FUSION SYSTEMS ON p-GROUPS WITH AN EXTRASPECIAL SUBGROUP OF INDEX p

by

RAÚL MORAGUES MONCHO

A thesis submitted to
the University of Birmingham
for the degreee of
DOCTOR OF PHILOSOPHY

School of Mathematics
College of Engineering and Physical Sciences
University of Birmingham
August 2018

Abstract

In this thesis we classify saturated fusion systems on p-groups S containing an extraspecial subgroup of index p for an arbitrary odd prime p. We prove that if $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$ then either $|S| \leq p^6$ or S is isomorphic to a unique group of order p^{p-1}. We either classify the fusion systems or cite references to show that $\mathcal{F}$ is known in all cases except when S is a Sylow p-subgroup of $SL_4(p)$, which remains as future work. When $|S| = p^{p-1}$ with $p \geq 11$ we describe new infinite exotic families related to those constructed by Parker and Stroth.

A mis padres Consuelo y Juan José.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my supervisor Professor Chris Parker, for his invaluable guidance and patience. Thanks for the suggestion of this project and incisive comments throughout its development, which have been vital to the completion of this thesis.

I am very grateful for the support of my family and friends, for all their support throughout these years. To my parents Consuelo and Juan José, to whom I dedicate this thesis, as well as Pablo, Yassin and Hao among many others.

My thanks to the colleagues of the Algebra Group with whom I have shared these last four years, for many fruitful conversations. A special mention to Valentina and Ryan, who were always helpful and could brighten my day. Thanks also to the people of the School of Mathematics, from the everyday work and the great times playing football, badminton, or whichever activity someone cooked up. Thanks to David, Alessandro, Rob, Gemma, Chloe, Alberto, and to all the people I have met over these four years, for having made this a great experience.

Finally, I thankfully acknowledge financial support from the University of Birmingham.

CONTENTS

LIST OF TABLES

LIST OF NOTATION

Throughout this thesis p denotes a prime, all groups are finite, and we write maps on the right hand side. Our notation is conventional except where stated otherwise.

- $C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$.
- $N_G(H) = \{g \in G \mid H^g = H\}$.
- $[x, y] = x^{-1}y^{-1}xy$ is the commutator of x and y.
- $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$.
- $\gamma_2(G) = G' = [G, G]$, the derived subgroup of G, and $\gamma_{i+1}(G) = [\gamma_i(G), G]$.
- $Z_1(G) = Z(G)$ and $Z_i(G)$ is the i-th term of the upper central series of G.
- $\Phi(G)$ is the Frattini subgroup of G.
- $\mathrm{Syl}_p(G)$ is the set of Sylow p-subgroups of G.
- $O_p(G) = \bigcap_{S \in \mathrm{Syl}_p(G)} S$ is the largest normal p-subgroup of G.
- $O_{p'}(G)$ is the largest normal subgroup of G of order coprime to p.
- $O^p(G)$ is the smallest normal subgroup of G of order p-power index.

- $O^{p'}(G) = \langle S \mid S \in \mathrm{Syl}_p(G) \rangle$, the normal closure in G of S is the smallest normal subgroup of G of index coprime to p.
- $\Omega_i(G) = \langle g \in G \mid g^{p^i} = 1 \rangle$.
- $\mho^i(G) = G^{p^i} = \langle g^{p^i} \mid g \in G \rangle$.
- $m_p(G)$ is the p-rank of G, that is, $p^{m_p(G)}$ is order of the largest elementary abelian subgroup of G. Not to confuse with the rank of a p-group $|P/\Phi(P)|_p$.
- $F^*(G)$ is the generalised Fitting subgroup of G.
- $\mathrm{Hom}(G, H)$ is the set of group homomorphisms $\phi : G \to H$.
- $\mathrm{Aut}(G)$ is the group of automorphisms $\phi : G \to G$.
- $\mathrm{Inn}(G)$ is the group of inner automorphisms of G.
- For $g \in G$ the map $c_g \in \mathrm{Inn}(G)$ is defined by $h \mapsto hc_g = h^g = g^{-1}hg$.
- $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is the outer automorphism group of G.
- $A \times B$ is the direct product of A and B.
- $A^n = A \times \cdots \times A$ is the direct product of n copies of A.
- $A \circ_C B$ is a central product of A and B with $C = A \cap B \leq Z(A \circ_C B)$.
- $A.B$ denotes a group extension of A by B where $A \trianglelefteq A.B$ and $A.B/A \cong B$.
- $A \rtimes_\phi B$ or $A : B$ denote a semidirect product or split extension of A by B with nontrivial action (if specified) $\phi : B \to \mathrm{Aut}(A)$, except in Appendix A, where we write $B \ltimes_\phi A$.

- $A{\cdot}B$ denotes an extension of A by B which does not split.

The following will denote specific groups:

- C_n is a cyclic group of order n.
- If p is odd, p_+^{1+2n} is the extraspecial group of order p^{1+2n} and exponent p.
- If p is odd, p_-^{1+2n} is the extraspecial group of order p^{1+2n} and exponent p^2.
- D_n is the dihedral group of order n.
- S_n is the symmetric group of degree n.
- A_n is the alternating group of degree n.
- We denote the versions of the classical groups as in [KL90], and those of the finite groups of Lie type as in [GLS98]. Where there are various notations in the literature we specify our choice. $GF(p^k)$ is the finite field of order p^k.
- $GU_n(p^k)$ is the general unitary group over $GF(p^{2k})$.
- In the Suzuki and Ree groups the exponents will be odd rather than fractional, for example $Sz(2^{2n+1}) = {}^2B_2(2^{2n+1})$ the Suzuki group over $GF(2^{2n+1})$.
- J_n denotes a Jordan block of size n with all eigenvalues 1.
- $H_{s,k} = C_{p^s} \wr C_p \wr \cdots \wr C_p$ is the wreath product with k wreathed factors.
- $\mathcal{A}(P) = \{A \leq P \mid A \text{ is elementary abelian of maximal order in } P\}$.
- $<n, a>$ denotes the a-th group of order n in the Magma [BCP97] SmallGroups library.

INTRODUCTION

In this thesis we initiate the classification of all saturated fusion systems $\mathcal{F}$ on p-groups S with an extraspecial subgroup of index p which contain no normal p-subgroups. We mostly assume that p is an odd prime, although results could be generalised to include $p = 2$. In group theory, the theory of fusion studies how the conjugation action of a group G on a subgroup S merges conjugacy classes of elements of S. As a consequence of Sylow's Theorems, the case when S is a Sylow p-subgroup of G is particularly important, and gives rise to the fusion category of a group usually denoted by $\mathcal{F}_S(G)$. Results about the fusion category date back to Burnside, who showed that if S is abelian then all G-fusion in S happens in $N_G(S)$.

The notion of fusion was first generalised beyond finite groups by Puig in the nineties with his *Frobenius categories*, but not published until [Pui06], as a tool in modular representation theory. The Frobenius categories he introduced were later rediscovered and rephrased by Broto, Levi and Oliver in [BLO03], who introduced them into topology to study p-completed classifying spaces and called them *saturated fusion systems*. This terminology has become standard in most of the literature. Fusion systems are used in finite group theory since some results seem to be easier to prove in the category of saturated fusion systems instead of in the finite groups themselves, for example see the proposed programme to improve and simplify portions of the classification of the finite simple groups by Aschbacher in [Asc11, Introduction] with $p = 2$. There is also a programme of Meierfrankenfeld, Stellmacher and Stroth to simplify parts of the classification by understanding the p-local structure of finite simple groups of local characteristic p in [MSS03].

An active area of research is the search for *exotic* fusion systems, which are saturated fusion systems that are not fusion categories of a finite group on its Sylow p-subgroups. When $p = 2$, the Benson-Solomon systems, encountered by Solomon and constructed by Levi and Oliver in [LO02], form the only known family of simple exotic fusion systems, but for odd primes they are more common, which suggested the following open problem from [AKO11, III.7.4].

Try to better understand how exotic fusion systems arise at odd primes; or (more realistically) look for patterns which explain how certain large families arise.

In this direction, exotic fusion systems have been found while classifying saturated fusion systems on extraspecial groups of order p^3 and exponent p when $p = 7$ by Ruiz and Viruel in [RV04], and many families of simple fusion systems on p-groups with an abelian subgroup of index p for all odd p have been described by Oliver [Oli14], Craven, Oliver and Semeraro [COS17], and Oliver and Ruiz [OR17].

The abelian subgroup of index p in these examples plays a role in controlling the fusion, which suggested attempting to use certain nonabelian p-groups to play an analogous role, such as *extraspecial* p-groups Q, which satisfy $Z(Q) = \Phi(Q) = Q'$ of order p, hence are nonabelian but $Q/Z(Q)$ has the structure of a symplectic vector space. In this direction some exotic fusion systems on p-groups with an extraspecial subgroup of index p have been constructed by Parker and Stroth in [PS15], which suggested the research problem in this thesis. The case of a Sylow

p-subgroup of $G_2(p)$, which if $p \geq 5$ contains an extraspecial subgroup of index p, has been classified in [PS18]. Many exotic fusion systems arose when $p = 7$. These systems are related to the Monster sporadic group and the Parker-Stroth constructions.

In saturated fusion systems we have many analogous concepts as in finite group theory, for example normal p-subgroups (see Definition 2.23). We denote by $O_p(\mathcal{F})$ the largest normal p-subgroup of $\mathcal{F}$ (see Lemma 2.24).

For each prime p there are many p-groups with an extraspecial subgroup of index p, and it is remarkable that the first main result that we prove greatly reduces the cases to be studied to at most four p-groups under the assumption that $|S| \geq p^6$.

Main Theorem (Theorem 4.27)**.** *Let p be an odd prime, let S be a p-group with an extraspecial subgroup Q of index p, and let $\mathcal{F}$ be a saturated fusion system on S satisfying $O_p(\mathcal{F}) = 1$. Suppose that $|S| \geq p^6$. Then S is isomorphic to one of the following:*

1. *a Sylow p-subgroup of $SL_4(p)$;*
2. *a Sylow p-subgroup of $SU_4(p)$;*
3. *a Sylow p-subgroup of $G_2(p)$ with $p \geq 5$;*
4. *the unique p-group of order p^{p-1}, maximal nilpotency class and exponent p whenever $p \geq 11$.*

We note that in cases (1), (2) and (3) we have $|S| = p^6$, and if $|S| < p^6$ then $|S| = p^4$ which we consider separately. When $p = 2$ we plan on adapting this reduction to prove that $|S| \leq 2^6$, at which point [Oli16, Theorem A] will conclude this case. Hence we assume that p is odd.

Most of the remainder of the thesis is then dedicated to studying the cases of the Main Theorem, and some have been already classified.

In Case (1), that is when S is a Sylow p-subgroup of $SL_4(p)$, we have not obtained a complete answer, and it remains as future work. Some results in this direction are Lemma 5.4 (2) and Proposition 5.5, which determine all the $\mathcal{F}$-essential candidates. The case $p = 3$ is being studied by Parker and Semeraro.

Case (2) is the object of Chapter 5, where we prove the following result.

Theorem 1 (Theorem 5.1)**.** *Suppose $p \geq 5$ and S is a Sylow p-subgroup of $SU_4(p)$. Then there is a one-to-one correspondence between saturated fusion systems $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$ and groups G with $SU_4(p) \leq G \leq \mathrm{Aut}(SU_4(p))$ which realise them. In particular, there are no such exotic fusion systems on S.*

This case is completed by [BFM], where the case $p = 3$ is considered and they show that there are no exotic fusion systems either. In this case however more finite almost simple groups appear, with socles $PSU_4(3)$, McL, Co_2, and $PSL_6(q)$ and $PSU_6(q)$ for suitable q coprime to 3.

In case (3), that of a Sylow p-subgroup of $G_2(p)$, the saturated fusion systems $\mathcal{F}$ with $O_p(\mathcal{F}) = 1$ have been classified in [PS18, Theorem 1.1], and they are either realisable by finite almost simple groups, or $p = 7$ where there arises a subsystem of the 7-fusion system of the Monster sporadic simple group and many examples related to case (4), as $|S| = 7^{7-1}$. The case $p = 3$ is also considered in [PS18], but does not arise in our situation as it does not contain extraspecial subgroups of index 3.

We study case (4) in Chapter 6, where we prove the following theorem.

Theorem 2 (Theorems 6.7 and 6.8)**.** *Suppose $p \geq 11$, S is as in Case (4) of the Main Theorem, and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. Let Q be the unique extraspecial subgroup of index p in S, and let $\mathcal{X} = \{M_1, \dots, M_{p-1}\}$ be the set of maximal subgroups of S of maximal class. Then $\mathcal{F}$ is one of the following, all of which are exotic:*

1. *A unique fusion system $\mathcal{F}_Q$ where $\mathrm{Out}_{\mathcal{F}}(Q) \cong GL_2(p)$ and $\mathrm{Aut}_{\mathcal{F}}(E) \cong SL_2(p)$ for all self-centralising subgroups E of order p^2 in S, described in [PS15, Proposition 3.5]; or*

2. *A subsystem $\mathcal{F}$ satisfying $\mathcal{F}_0^J = O^{p'}(\mathcal{F}) \subseteq \mathcal{F} \subset \mathcal{F}_Q$ which is an extension of p'-index of $\mathcal{F}_0^J$ which is determined by the set of $\mathcal{F}_0^J$-essential subgroups consisting of those self-centralising subgroups of order p^2 contained in M_{j_i} whenever $\emptyset \neq J = \{M_{j_1}, \dots M_{j_l}\} \subseteq \mathcal{X}$. Each $\mathcal{F}$-essential subgroup E satisfies $\mathrm{Aut}_{\mathcal{F}}(E) \cong SL_2(p)$, and $\mathcal{F}_0^J \cong \mathcal{F}_0^K$ if and only if $K = \{M_{j_1x}, \dots, M_{j_lx}\}$ for some $x \in \{1, \dots, p-1\}$. For each p there are at least $\frac{2^{p-1}-1}{p-1}$ isomorphism classes of $\mathcal{F}_0^J$.*

Putting together the Main Theorem and Theorem 2 we obtain the following.

Corollary 1. *Assume p is odd, S is a p-group with an extraspecial subgroup of index p and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. If $|S| > p^6$ then $\mathcal{F}$ is known.*

We can summarise the situation of the research problem thus far as follows, using the results of [PS18] and [BFM].

Corollary 2. *Assume p is odd, S is a p-group with an extraspecial subgroup of index p and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. If $|S| \geq p^6$ then either $\mathcal{F}$ is known or S is a Sylow p-subgroup of $SL_4(p)$.*

Since the Main Theorem assumes that $|S| \geq p^6$, it remains to consider the case with $|S| = p^4$, which behaves differently to the rest, and has been studied in [COS17], [Oli14], and [OR17] but due to the generality of their results the fusion systems were not written explicitly. We do this in Chapter 7, the main result of which is the following, where we note that there is no need to assume that S contains an extraspecial subgroup Q of index p.

Theorem 3 (Theorem 7.1)**.** *Suppose p is odd, $|S| = p^4$ and $\mathcal{F}$ is a simple fusion system on S. Then S has extraspecial subgroups of index p and $\mathcal{F}$ is one of the fusion systems described in Tables 7.1 and 7.2.*

Hence in all cases except when $S \in \mathrm{Syl}_p(SL_4(p))$ we obtain a complete list of the isomorphism types of saturated fusion systems considered. The remaining case $S \in \mathrm{Syl}_p(SL_4(p))$ will be the object of future work. We now describe the structure of the thesis.

In Chapter 1 we introduce the group theoretic notation and background results that we will use. We begin by defining some basic concepts and important subgroups, before introducing regular p-groups and extraspecial p-groups. Afterwards, we present the well-known isomorphisms between small classical groups and alternating groups. We then prove some results about p-groups containing an extraspecial subgroup of index p and its relation with p-groups with abelian subgroup of index p, and consider certain iterated wreath products of cyclic groups. We then use standard results about group extensions found in Appendix A to obtain results about isomorphism classes of p-groups with extraspecial subgroups of index p and prove some results about the ones we will encounter.

We then move onto actions of groups on p-groups. Of particular importance for us are the cases of coprime and quadratic action, and the specialisation to transvections. We then introduce strongly p-embedded subgroups and prove some of their properties, including a list of those almost simple groups with p-rank at least 2 containing one, and the structure of groups generated by transvections and containing a strongly p-embedded subgroup. We finally consider subgroups of $GL_r(p)$ with $r \leq 4$ containing strongly p-embedded subgroups. Our main sources for group theoretic background are [Gor80, Hup67, DH92, GLS96].

In Chapter 2 we give an introduction to the theory of saturated fusion systems, mainly following [AKO11, Part I] and using standard notation. We introduce the fusion category $\mathcal{F}_S(G)$ of a group G on a Sylow p-subgroup S and the more general fusion systems, immediately specialising to saturated fusion systems, as well as discussing extension of morphisms. Afterwards we introduce isomorphisms of fusion systems. We then present Alperin's Fusion Theorem, which is the starting point of the attempts to classify saturated fusion systems, by showing that any saturated fusion system $\mathcal{F}$ can be generated by compositions of restrictions of automorphisms in $\mathcal{F}$ of a class of subgroups, denoted *$\mathcal{F}$-essential*, which are introduced in Definition 2.13.

We then prove basic properties of these $\mathcal{F}$-essential subgroups, before proceeding to the local theory of fusion systems. Analogous concepts to those in group theory of normal p-subgroups and subsystems, as well as simple fusion systems are defined. The Model Theorem, which guarantees realisability of constrained fusion systems, is stated, and we present some properties about the smallest normal subsystem of

$\mathcal{F}$ on S, denoted by $O^{p'}(\mathcal{F})$.

We finally explore the relationship between simple fusion systems, reduced fusion systems, and those $\mathcal{F}$ containing no normal p-subgroups, that is, having $O_p(\mathcal{F}) = 1$, which are all assumptions in various classification results.

In Chapter 3 we study small p-groups and determine which isomorphism types can appear as $\mathcal{F}$-essential subgroups. We determine the isomorphism types of abelian p-groups of rank at most 2 which can be $\mathcal{F}$-essential in Proposition 3.4 and that of p-groups of order p^4 in Proposition 3.10.

It is in Chapter 4 that we begin the study of fusion systems on p-groups with an extraspecial subgroup of index p and prove the Main Theorem. The final step in each of the cases will be via results from Appendix A about group extensions. We begin with the following setup.

Hypothesis A. *S is a p-group with an extraspecial subgroup Q of index p, $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$.*

We use Hypothesis A to prove some general statements about S, such as Theorem 4.2.

Theorem 4 (Theorem 4.2)**.** *Assume Hypothesis A. Then $Z(S) = Z(Q)$.*

In its proof we already see that the cases $|S| = p^4$ and $|S| \geq p^6$ behave differently, so we restrict our attention to $|S| \geq p^6$, hence we may refine our setup using Theorem 4.

Hypothesis B. *Assume Hypothesis A, $|S| \geq p^6$, and set $Z := Z(S) = Z(Q)$.*

Then we prove that Q indeed mimics the role of an abelian subgroup as desired.

Theorem 5 (Theorem 4.4)**.** *Assume Hypothesis B. If $E \leq Q$ is $\mathcal{F}$-essential then $E = Q$.*

We define

$$\mathcal{M} := \{E \leq S \mid E \text{ is } \mathcal{F}\text{-essential and } Z \text{ is not normalised by } \operatorname{Aut}_{\mathcal{F}}(E)\},$$

which is nonempty since there must be some $\mathcal{F}$-essential subgroup that moves Z. We split the cases according to the structure of $Z_E := \langle Z(S)^{\operatorname{Aut}_{\mathcal{F}}(E)} \rangle$.

Hypothesis C. *Assume Hypothesis B and that there is $E \in \mathcal{M}$ such that $Z_E \leq Q$.*

Hypothesis D. *Assume Hypothesis B and that for all $E \in \mathcal{M}$ we have $Z_E \not\leq Q$.*

In Section 4.2 we consider the situation when Hypothesis C holds, and we prove that one of case (1) or (3) of the Main Theorem holds.

Proposition 1 (Proposition 4.9)**.** *Assume Hypothesis C and let $E \in \mathcal{M}$ with $Z_E \leq Q$. Then $|S| = p^6$, E is maximal in S, and either $|\Phi(E)| = p^2$ and S is isomorphic to a Sylow p-subgroup of $SL_4(p)$ or $p \geq 5$, $|\Phi(E)| = p^3$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$.*

To prove this proposition we first show that $|Z_E| = p^2$ and $C_S(Z_E)$ is maximal in S using McLaughlin's results on groups generated by transvections, and we have $O^{p'}(\operatorname{Out}_{\mathcal{F}}(C_S(Z_E))) \cong SL_2(p)$, which yields an abelian subgroup F_E of index p^2 in Q forcing $|Q| \leq p^{1+4}$, and then we prove that $E = C_S(Z_E)$. Then we consider the possibilities for $\Phi(E)$, which yields the upper and lower central series of S. If $|\Phi(E)| = p^3$ we prove that S has maximal class, Q has exponent p and there is a complement to Q in S, whence we conclude using Proposition 1.32 that S is isomorphic to a Sylow p-subgroup of $G_2(p)$. If $|\Phi(E)| = p^2$ we deal with the case $p = 3$ separately via a Magma computation, whereas if $p \geq 5$ we find $C_p^4 \cong V \trianglelefteq S$ and a complement to V in S, and conclude again by Proposition 1.32.

In Section 4.3 we consider the remaining case, concluding the Main Theorem.

Proposition 2 (Proposition 4.21)**.** *Assume Hypothesis D and let $E \in \mathcal{M}$. Then either S is isomorphic to a Sylow p-subgroup of $SU_4(p)$ and $|E| = p^4$ with $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong PSL_2(p^2)$, or $p \geq 7$, $|E| = p^2$ and $|S| = p^{p-1}$ where S has maximal class and is unique up to isomorphism.*

A first step in proving this proposition is showing that E and $N_S(E)/E$ are elementary abelian, after which we use Thompson's Replacement Theorem to obtain that either $E \trianglelefteq S$ is the unique elementary abelian subgroup of maximal order in S or E admits a quadratic action. We consider first the case where E has maximal possible order, that is $E \cap Q$ is maximal abelian in Q, which determines $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong PSL_2(p^2)$. A study of the module structure of E under the action of $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$ and a comparison with a parabolic subgroup of $SU_4(p)$ then show S to be isomorphic to a Sylow p-subgroup of $SU_4(p)$ via the Model Theorem. Afterwards we assume $E \cap Q$ is not maximal abelian in Q and, by considering the action of E on Q/Z, we show that $|N_S(E)/E| = p$. Then we prove that this action on Q/Z has a single non-trivial Jordan block and, since it can be seen as a subgroup of $\mathrm{Out}(Q) \cong CSp_{2n}(p)$, it forces E to be an $\mathcal{F}$-pearl. A result of Grazian ([Gra18, Theorem 3.14]) then implies that $|S| = p^{p-1}$ and has exponent p, whence we conclude by Proposition 1.31.

In Theorem 4.27 we gather the previous results of this chapter and conclude the Main Theorem, which contains extra information about the elements of $\mathcal{M}$

and their $\mathcal{F}$-automorphism groups which will be used in the cases to be considered.

We note that the reduction as presented depends on the Classification of Finite Simple Groups, which is assumed in Theorem 1.59 to obtain the list of groups with a strongly p-embedded subgroup with noncyclic Sylow p-subgroups, as well as to obtain Sambale's bound [Sam14, Proposition 6.10] for $|N_S(E)/E|$ in terms of the rank of E, which is used in Lemma 4.6 and Proposition 4.23 (Hypothesis D) to show that $|S| = p^6$ and that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong PSL_2(p^2)$, while showing that S is isomorphic to a Sylow p-subgroup of $SU_4(p)$.

Once the reduction is complete, we proceed to study the cases that arise.

Chapter 5 is devoted to the study of Case (2) of the Main Theorem and the proof of Theorem 1, that is when S isomorphic to a Sylow p-subgroup of $SU_4(p)$. Since the Sylow p-subgroups of $SU_4(p)$ are very similar to those of $SL_4(p)$, we begin by describing both isomorphism types of S and their automorphism groups together. We show that if the subgroups studied in the Main Theorem are $\mathcal{F}$-essential, they are always in $\mathcal{M}$, and then prove that Q is the only subgroup which can $\mathcal{F}$-essential but not in $\mathcal{M}$.

Then we specialise to the case $p \geq 5$, as we apply a generalisation of the result of Meierfrankenfeld ([Che04, Lemma 2.8]) to determine $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$, whereas when $p = 3$ there are more groups acting appropriately. We then study the natural $\Omega_4^-(p)$-module. It is at this point that we specialise to a Sylow p-subgroup of $SU_4(p)$. We show that both Q and $V := C_S(S')$ must be $\mathcal{F}$-essential, and translate the earlier module description to results about the action of $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$ on V. We then study the interaction between isomorphisms in $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ to determine the smallest possible $\mathrm{Aut}^0_{\mathcal{F}}(S)$ and determine its uniqueness, which involves some delicate calculations.

We then put together the results to determine a subsystem $\mathcal{F}_0$, then show that $PSU_4(p)$ realises $\mathcal{F}_0$, which shows that $\mathcal{F}_0$ is saturated and therefore $\mathcal{F}_0 = O^{p'}(\mathcal{F})$, before finally obtaining the one-to-one correspondence in Theorem 1.

The case where $p = 3$ is studied in [BFM], since a Sylow 3-subgroup of the sporadic finite simple group McL is isomorphic to a Sylow 3-subgroup of $SU_4(3)$.

In Chapter 6 we study case (4) of the Main Theorem and prove Theorem 2. This chapter begins with a construction of S and a finite group B as in [PS15], which enables us to calculate explicitly in the candidates for $\mathrm{Aut}_{\mathcal{F}}(S)$. Then we study the action of $\mathrm{Aut}(S)$ on the sets $\mathcal{X}$ and $\mathcal{P}$ of maximal subgroups of S of maximal nilpotency class and corresponding self-centralising subgroups of order p^2, before determining that every $\mathcal{F}$-essential subgroup is either Q or an element E of $\mathcal{P}$, that is an $\mathcal{F}$-pearl, and describe $\mathrm{Aut}_{\mathcal{F}}(E)$ and $\mathrm{Out}_{\mathcal{F}}(Q)$. If Q is $\mathcal{F}$-essential then we determine uniquely $N_{\mathcal{F}}(Q)$ and find a model for it before determining $\mathcal{F}$ in Theorem 6.7. If Q is not $\mathcal{F}$-essential, the situation is much more complicated and described before Theorem 6.8, where we prove saturation and exoticity of the fusion systems constructed. We note that in this case we obtain a lower bound of $\frac{2^{p-1}-1}{p-1}$ on the number of reduced fusion systems, since we have 2^{p-1} nonempty subsets $J \subseteq \{1, \ldots, p-1\}$ to choose from, and each orbit has length at most $p-1$, hence there are at least $\frac{2^{p-1}-1}{p-1}$ such orbits, hence the same number of reduced fusion systems $\mathcal{F}_0^J$.

The snippet of Magma code in Appendix C.1 calculates the number of orbits for a given prime, but due to the large number of calculations necessary, it is only practical up to $p = 19$. The total number of fusion systems with $O_p(\mathcal{F}) = 1$ is slightly larger due to the p'-extensions that also arise.

Since throughout the reduction we assume that $|S| \geq p^6$, we consider the case when $|S| = p^4$ separately in Chapter 7, where we prove Theorem 3. As groups of order p^4 always contain an abelian subgroup of index p, we use the results from [Oli14, COS17, OR17], where a recipe for obtaining the fusion systems is described. We use their results to give explicit descriptions of the fusion systems in Tables 7.1 and 7.2, and note that only the simple fusion systems are described in this case. We also encounter a family of fusion systems described in [CP10]. Our strategy in this chapter follows that of [Oli14, COS17], by considering first the case where A is not $\mathcal{F}$-essential, and considering the various cases that arise, before moving to the case where A is $\mathcal{F}$-essential, in which case it is elementary abelian and we follow the results from [COS17]. Throughout this chapter the cases $p = 3$ and $p = 5$ require different arguments, whereas whenever $p \geq 7$ a uniform description is possible.

In Chapter 8 we conclude with the state of the research question, which is almost complete. We also consider the strongly closed subgroups of $\mathcal{F}$ and determine that $\mathcal{F} = O^p(\mathcal{F})$ in most cases. There is a case left to consider, which is that of S a Sylow p-subgroup of $SL_4(p)$.

Appendix A presents background material used in the problem of determining group extensions of N by H, which is used in some propositions that appear in Chapter 1, and are used in the proof of the Main Theorem to determine the uniqueness up to isomorphism of the p-groups in question.

When the group extensions split or when N is abelian, this is well-known and depends on the conjugacy class of $\mathrm{Aut}(N)$, but in our case $N = Q = p_+^{1+2n}$ is nonabelian, and it is easier to study conjugacy in $\mathrm{Out}(N) \cong Sp_{2n}(p) \rtimes C_{p-1}$. For this reason we have to deal with group extensions in a more complicated setting. We follow mainly the treatment in [ML63, Chapter IV].

We begin by describing the notation of diagrams and exact sequences, and prove a version of the short five lemma, before moving onto semidirect products and their characterisations. While in the rest of the thesis we use the standard notation of having the normal subgroup on the left, in this chapter we write the normal subgroup on the right due to our maps acting on the right. Then we consider the problem of group extensions in more general terms, which induces only a homomorphism $\psi : H \to \mathrm{Out}(N)$. We introduce congruence of extensions, which is an equivalence relation preserving ψ which used to classify group extensions, slightly weaker than isomorphism of the resulting groups. Then we state some results relating low dimensional group cohomology to group extensions, and calculate an explicit example for C_p by C_p in Lemma A.15. We finally consider the general theory with *abstract kernels*, and sketch a proof of MacLane's classification (Theorem A.18).

With this result we show that $\mathrm{Aut}(N)$ being a split extension of $\mathrm{Inn}(N)$ by a subgroup isomorphic to $\mathrm{Out}(N)$ guarantees the existence of extensions of abstract kernels, and that $\mathrm{Out}(N)$-conjugate homomorphisms give rise to isomorphic groups. These results are applied in Section 1.6 to study the extensions of $Q \cong p_+^{1+2n}$ by C_p in the relevant cases.

In Appendix B we study which Sylow p-subgroups of finite simple groups contain an extraspecial subgroup of index p and prove Proposition B.1, which also considers the isomorphism types of their fusion categories. We then present some corollaries exploring the possibilities for each of the Sylow p-subgroups.

We begin by presenting some consequences of the Main Theorem which reduce the cases to be considered. We first consider the groups of Lie type in defining characteristic, where we obtain the four infinite families of groups, $PSL_4(p)$,

$PSU_4(p)$, $G_2(p)$ and $Sp_4(p)$, except $G_2(3)$. We then consider the symmetric and alternating groups, which yield only small examples. Then we study the groups of Lie type in cross characteristic, except when $p = 2$. We then consider the finite sporadic simple groups.

If $p > 7$, the four groups of Lie type in characteristic p are the only finite simple groups whose Sylow p-subgroups have the required property. Our main sources for results about the finite simple groups used are [Wei55], [GLS98], [CCN$^+$85] and [Car72]. The only p-groups other than the Sylow p-subgroups of the four infinite families above have order 3^4.

In Section B.5, we consider the fusion categories of the finite simple groups up to isomorphism, and complete the proof of Proposition B.1. Finally, in Section B.6, we show that no more examples can arise from almost simple groups when $p \geq 5$.

In Appendix C certain Magma programs used in the thesis can be found. These give a program to calculate the orbits of the multiplicative action of $GF(p)^\times$ on $GF(p)^\times$, a reduction to a Sylow 3-subgroup of $SL_4(3)$, and a program to obtain $\mathcal{F}_S(G)$-essential candidates given a finite group G, a Sylow p-subgroup and p.

CHAPTER 1

GROUP THEORY BACKGROUND

In this chapter we introduce definitions, notation and results about finite groups, as well as some methods which will be important when working with fusion systems. The notation that we use is mostly standard, and our main sources are [Gor80, Hup67, DH92]. Our groups are always finite, p is a prime number, and we write maps on the right.

1.1 Conjugation and commutators

Let G be a finite group. Given $g \in G$, the *conjugation map by* g is $c_g : G \to G$ defined by $h \mapsto hc_g = h^g = g^{-1}hg$. For $g, h \in G$ we denote the *commutator* of g and h by $[g, h] = g^{-1}h^{-1}gh = g^{-1}(gc_h)$.

When $H, K \leq G$ we denote $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$, the *commutator* of H and K. We write $G' = [G, G]$ for the *derived subgroup* of G.

We denote by $O_p(G)$ the largest normal p-subgroup of G, by $O_{p'}(G)$ the largest normal subgroup of G of order not divisible by p.

We also denote by $O^p(G)$ the intersection of all $K \trianglelefteq G$ of index a power of p, and by $O^{p'}(G)$ the smallest normal subgroup of index coprime to p, which is the subgroup generated by all Sylow p-subgroups of G.

If G, H are groups then we denote by $\mathrm{Hom}(G, H)$ the set of group homomorphisms with domain G and codomain H. We write $\mathrm{Aut}(G)$ for the group of automorphisms of G, $\mathrm{Inn}(G)$ for the subgroup of inner automorphisms of G, and $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is the outer automorphism group of G.

If $g \in G$ and $\alpha \in \mathrm{Aut}(G)$ then we denote by $[h, \alpha] = h^{-1}(h\alpha)$. Note that if α is a conjugation map c_g then this becomes $h^{-1}(hc_g) = h^{-1}g^{-1}hg = [h, g]$. If $H \leq G$ and $A \leq \mathrm{Aut}(G)$ then we write $[H, A] := \langle [h, \alpha] \mid h \in H, \alpha \in A \rangle$. Similarly when $\alpha \in \mathrm{Aut}(G)$ we write $[H, \alpha] := \langle h^{-1}(h\alpha) \mid h \in H \rangle$.

The *derived series* of G, denoted by $G^{(i)}$, is defined by $G^{(0)} = G$ and iteratively $G^{(i+1)} = [G^{(i)}, G^{(i)}] = G^{(i)\prime}$. If $G^{(n)} = 1$ for some $n \in \mathbb{N}$, G is *solvable* and the *derived length* of G is the smallest k such that $G^{(k)} = 1$.

The *upper central series* of G is the sequence of subgroups

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_i(G) \trianglelefteq \cdots$$

defined by $Z_0(G) = 1$ and $Z_i(G)$ is the preimage in G of $Z(G/Z_{i-1}(G))$. That is, $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. In particular, $Z_1(G) = Z(G)$. We call $Z_2(G)$ the *second centre* of G.

Analogously, the *lower central series* of G is the sequence of subgroups

$$G \trianglerighteq \gamma_2(G) \trianglerighteq \cdots \trianglerighteq \gamma_i(G) \trianglerighteq \cdots$$

where $\gamma_i(G) = [\gamma_{i-1}(G), G]$. A group is *nilpotent* if the lower central series (equivalently, the upper central series) terminates, that is $\gamma_n(G) = 1$ for some $n \in \mathbb{Z}$. The least n such that $\gamma_{n+1}(G) = 1$ (equivalently $Z_n(G) = G$) is the *nilpotency class* of G.

The *Frattini subgroup* of G, denoted $\Phi(G)$ is the intersection of all maximal subgroups of G.

The *socle* of G, denoted by $soc(G)$, is the subgroup generated by all minimal normal subgroups of G.

We will denote by $|G|_p = \nu$ the p-part of $|G|$, that is, the the highest exponent ν such that p^ν divides $|G|$, that is, p^ν is the order of a Sylow p-subgroup of G.

The *generalised Fitting subgroup* $F^*(G)$ is the subgroup generated by the components of G, which are the quasisimple subnormal subgroups of G, and the Fitting subgroup, which is the largest normal nilpotent subgroup of G. More details about this subgroup can be found in [GLS96, §3].

From now on, we assume that P is a p-group.

Then P is called *elementary abelian* if it is abelian of exponent p, in other words $P \cong C_p^n$ for some $n \in \mathbb{Z}_{\geq 0}$.

For each $i \in \mathbb{Z}_{\geq 0}$ we define the subgroups $\Omega_i(P) = \langle g \in P \mid g^{p^i} = 1 \rangle$ and $\mho^i(P) = G^{p^i} = \langle g^{p^i} \mid g \in P \rangle$.

We then have $\Phi(P) = P'\mho^1(P)$, and $\Phi(P)$ is the smallest subgroup of G such that $P/\Phi(P)$ is elementary abelian.

The *rank* of P is $|P/\Phi(P)|_p$.

The *p-rank* of P, denoted by $m_p(P)$, is the largest rank of an elementary abelian p-subgroup.

Every p-group P of order p^n is nilpotent and has nilpotency class at most $n-1$.

We say P has *maximal class* if it has nilpotency class $n-1$.

We will repeatedly use the Frattini Argument.

Theorem 1.1 ([Gor80, Theorem 1.3.7]). *If $H \trianglelefteq G$ and $P \in \mathrm{Syl}_p(H)$ then*

$$G = N_G(P)H.$$

The following is a useful number-theoretic result to prove that certain groups do not embed into other groups.

Theorem 1.2 (Zsigmondy, [Zsi92]). *Let q and n be integers with $q \geq 2$ and $n \geq 3$. Provided $(q,n) \neq (2,6)$, there is a prime s such that $s \mid q^n - 1$ but s does not divide $q^i - 1$ for $i < n$.*

The following is a well-known way to prove a p-group has maximal nilpotency class.

Proposition 1.3 ([Ber08, Proposition 1.8]). *Let S be a nonabelian p-group. If $A < S$ of order p^2 is such that $C_S(A) = A$ then S is of maximal nilpotency class.*

1.2 Regular p-groups

We now present some results about regular p-groups, which were introduced by Hall in [Hal34] and generalise some properties of abelian groups. They will allow us to complete the determination of the structure of certain p-groups when p is large enough, leaving some small primes to be checked separately.

Definition 1.4. *A p-group S is called* regular *if for every $x, y \in S$ we have $x^p y^p = (xy)^p w$ for some $w \in \mho^1(\langle x, y\rangle')$.*

Proposition 1.5 ([Hup67, III.10.2 Satz]). *Let S be a p-group.*

1. *If the nilpotency class of S is less than p then S is regular.*

2. *If $|S| \leq p^p$ then S is regular.*

3. *If S' is cyclic and $p > 2$ then S is regular.*

4. *If S has exponent p then S is regular.*

The lemma above shows that there are fewer regular p-groups when p is small. Next we note some properties of p-groups for $p = 2, 3$, as well as present a family of smallest irregular groups.

Proposition 1.6 ([Hup67, III.10.3 Satz]).

1. *Every regular 2-group is abelian.*

2. *If S is a regular 3-group with two generators then S' is cyclic.*

3. *The Sylow p-subgroups of the symmetric group S_{p^2} are irregular of order p^{p+1}.*

The Sylow p-subgroups of S_{p^2} will be studied later in Lemma 1.28, have nilpotency class p, order p^{p+1} and exponent p^2, which shows that the bounds in Proposition 1.5 (1,2,4) are best possible. The main reason we use regular p-groups is because their structure with respect to p-powers is well-behaved.

Theorem 1.7 ([Hup67, III.10.5 Hauptsatz, III.10.7 Satz]). *Let S be a regular p-group and $k \in \mathbb{Z}_{\geq 0}$. Then*

1. *If $x^{p^k} = y^{p^k} = 1$ then $(xy)^{p^k} = 1$. In particular $\Omega_k(S) = \{x \mid x^{p^k} = 1\}$.*

2. *For every $x, y \in S$ there exists $z \in S$ such that $x^{p^k} y^{p^k} = z^{p^k}$. That is, $\mho^k(S) = \{x^{p^k} \mid x \in S\}$.*

3. $|S/\Omega_k(S)| = |\mho^k(S)|$.

1.3 Extraspecial p-groups

Definition 1.8. *A p-group Q is called* extraspecial *if $Z(Q) = Q' = \Phi(Q)$ and $|Z(Q)| = p$.*

Note that by definition $Q/Z(Q)$ is elementary abelian, and Q has nilpotency class 2, so if p is odd Q is regular. The case $p = 2$ is slightly different to the case when p is odd. We begin by describing the normal subgroups of Q.

Lemma 1.9. *Let Q be an extraspecial group. A nontrivial subgroup $H \leq Q$ is normal in Q if and only if $Z(Q) \leq H$.*

Proof. If $1 \neq H \leq Q$ with $Z(Q) \leq H$ then $[H, Q] \leq Q' = Z(Q) \leq H$ so $H \trianglelefteq Q$. Conversely if $1 \neq H \trianglelefteq Q$ then as $|Z(Q)| = p$ either $[H, Q] = 1$ and $H \leq Z(Q)$, or $Z(Q) = Q' = [H, Q] \leq H$. □

Lemma 1.10 ([KS98, (5.1.8)])**.** *Let A and B be subgroups of a p-group P satisfying $[A, B] \leq A \cap B$ and $|[A, B]| \leq p$. Then $|A : C_A(B)| = |B : C_B(A)|$.*

An exposition of results about extraspecial p-groups can be found in [DH92, A.20]. The smallest examples of nonabelian p-groups are extraspecial. In fact, every p-group of order p^3 is either abelian or extraspecial.

Lemma 1.11 ([DH92, A.20.γ])**.** *The following groups are extraspecial of order p^3, and every extraspecial group of order p^3 is isomorphic to one of the following:*

$p_+^{1+2} := \langle x, y \mid x^p = y^p = 1, [[x,y],x] = [[x,y],y] = 1\rangle$ *for p odd,*

$p_-^{1+2} := \langle x, y \mid x^{p^2} = y^p = 1, [x,y] = x^p\rangle$ *for p odd,*

$D_8 = \langle x, y \mid x^4 = y^2 = 1, y^{-1}xy = x^{-1}\rangle$, *or*

$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk\rangle$.

These groups are the building blocks of extraspecial groups.

Lemma 1.12 ([DH92, Lemma A.20.4])**.** *If Q is an extraspecial group satisfying $Z(Q) = \langle z\rangle$ then $Q/Z(Q)$ is a vector space over $GF(p)$ endowed with a symplectic form defined by $(xZ(Q), yZ(Q)) = k$ whenever $[x,y] = z^k$ for some $1 \le k < p$. If $p = 2$ the map $\mathfrak{q} : Q/Z(Q) \to GF(2)$ given by $xZ(Q)\mathfrak{q} = b$ whenever $x^2 = z^b$ is a non-degenerate quadratic form on $Q/Z(Q)$ associated with the symplectic form above. Every extraspecial group has order p^{1+2n} for some $n \in \mathbb{Z}_{>0}$ and is a central product of n extraspecial groups of order p^3.*

Theorem 1.13 ([DH92, Theorem A.20.5])**.** *An extraspecial group Q of order p^{1+2n} satisfies exactly one of the following:*

$p \neq 2$, $Q \cong p_+^{1+2n}$ has exponent p and is a central product of n copies of p_+^{1+2};

$p \neq 2$, $Q \cong p_-^{1+2n}$ has exponent p^2 and is a central product of $n-1$ copies of p_+^{1+2} and a copy of p_-^{1+2};

$p = 2$, $Q \cong 2_+^{1+2n}$ is a central product of n copies of D_8; or

$p = 2$, $Q \cong 2_-^{1+2n}$ is a central product of $n-1$ copies of D_8 and a copy of Q_8.

Their automorphism groups are also well-known.

Theorem 1.14 ([Win72, Theorem 1],[DH92, Theorem A.20.8-9])**.** *Let Q be an extraspecial group of order p^{1+2n}. Denote by $A = \mathrm{Aut}(Q)$, $B = C_A(Z(Q))$, and $C = C_B(Q/Z(Q))$. Then we have:*

1. *$C = \mathrm{Inn}(Q) \cong Q/Z(Q)$ is elementary abelian of order p^{2n};*

2. $A = BT$ is the semidirect product of B with a cyclic group T of order $p-1$;

3. B/C is isomorphic to the following subgroup of $Sp_{2n}(p)$.

(a) If p is odd and $Q \cong p_+^{1+2n}$ then $B/C \cong Sp_{2n}(p)$;

(b) If p is odd and $Q \cong p_-^{1+2n}$ then B/C is isomorphic to a semidirect product of a normal extraspecial group of order p^{2n-1} with $Sp_{2n-2}(p)$. If $n = 1$ then $|B/C| = p$;

(c) If $p = 2$ then $B/C \cong O(\mathfrak{q})$, the orthogonal group for the quadratic form $\mathfrak{q}$ associated with Q in Lemma 1.12.

Corollary 1.15. *Let p be odd and $Q \cong p_-^{1+2n}$. Then Q contains characteristic subgroups $\Omega_1(Q)$ of index p and $Z(\Omega_1(Q))$ of order p^2.*

Proof. As Q is a central product of extraspecial groups of order p^3 where all but one can be taken to have exponent p by Theorem 1.13, it contains a maximal subgroup of exponent p. But as Q has nilpotency class 2 and p is odd, it is a regular p-group by Proposition 1.5 (1), therefore by Theorem 1.7 it is not generated by elements of order p and $\Omega_1(Q) < Q$. Hence $\Omega_1(Q)$ contains all elements of order p and thus is a characteristic subgroup of Q of index p, and it is the unique maximal subgroup of Q of exponent p. Then $Z(\Omega_1(Q))$ has order p^2 by Lemma 1.10. Further, $Z(\Omega_1(Q))$ is characteristic in $\Omega_1(Q)$, which is normal in Q, hence $Z(\Omega_1(Q))$ is characteristic in Q. $\square$

When p is odd, $\mathrm{Aut}(Q)$ is a semidirect product of $\mathrm{Inn}(Q)$ by a group isomorphic to $\mathrm{Out}(Q)$, and we now explain this when Q has exponent p. We recall that a group G is a semidirect product if there exist $H, N \leq G$ with $N \trianglelefteq G$, $H \cap N = 1$, and $G = NH$. They will be considered in more detail in Appendix A.

We denote by $CSp_{2n}(p)$ the group of similarities of a symplectic vector space V over $GF(p)$, that is those elements preserving a symplectic form up to scalars. We have $CSp_{2n}(p) \cong Sp_{2n}(p) \rtimes C_{p-1}$, and $\mathrm{Out}(p_+^{1+2}) \cong CSp_{2n}(p)$ when p is odd by Theorem 1.14.

Lemma 1.16. *If p is odd and $Q \cong p_+^{1+2n}$ then $\mathrm{Aut}(Q) = \mathrm{Inn}(Q) \rtimes CSp_{2n}(p)$, that is $\mathrm{Aut}(Q)$ is a semidirect product of $\mathrm{Inn}(Q)$ by $\mathrm{Out}(Q)$.*

Proof. Note that $\mathrm{Inn}(Q) \trianglelefteq \mathrm{Aut}(Q)$, and by Theorem 1.14 we have $\mathrm{Out}(Q) \cong CSp_{2n}(p)$. Consider a group $\mathrm{Inn}(Q) \leq B \leq \mathrm{Aut}(Q)$ such that $\overline{B} = B/\mathrm{Inn}(Q) \leq Z(\mathrm{Out}(Q))$ has order 2, that is, the nontrivial element of $\overline{B}$ is the central involution of $CSp_{2n}(p)$. Let $T \in \mathrm{Syl}_2(B)$, then $|T| = 2$. Note that $B \trianglelefteq \mathrm{Aut}(Q)$ as $\overline{B} \leq Z(\mathrm{Out}(Q))$. Then by the Frattini argument (Theorem 1.1) we have $\mathrm{Aut}(Q) = N_{\mathrm{Aut}(Q)}(T)B$, and since $T \leq N_{\mathrm{Aut}(Q)}(T) \cap B$, it follows that $\mathrm{Aut}(Q) = N_{\mathrm{Aut}(Q)}(T)\,\mathrm{Inn}(Q)$. But the nontrivial element of T inverts $\mathrm{Inn}(Q)$, so that $1 = C_{\mathrm{Inn}(Q)}(T) = N_{\mathrm{Aut}(Q)}(T) \cap \mathrm{Inn}(Q)$, which means that $N_{\mathrm{Aut}(Q)}(T)$ is a complement to $\mathrm{Inn}(Q)$ in $\mathrm{Aut}(Q)$. Therefore $\mathrm{Aut}(Q)$ is a semidirect product of $\mathrm{Inn}(Q)$ by $N_{\mathrm{Aut}(Q)}(T)$ as claimed. □

We now consider the maximal abelian subgroups of Q and its p-rank.

Lemma 1.17 ([Hup67, III.13.7, III.13.8])**.** *Let Q be an extraspecial group of order p^{1+2n}. Then its maximal abelian subgroups all have order p^{1+n}. Furthermore, Q has p-rank $1+n$, unless $p = 2$ and $Q \cong 2_-^{1+2n} \cong D_8^{n-1} \circ Q_8$, which has 2-rank n.*

We remark that abelian subgroups of an extraspecial group Q correspond to singular (isotropic) subspaces in the symplectic (orthogonal) space $Q/Z(Q)$ via the symplectic (quadratic) form given in Lemma 1.12.

Finally, we consider the representation theory of extraspecial groups.

Lemma 1.18. *Let Q be an extraspecial group of order p^{1+2n}. Let K be an algebraically closed field of characteristic $r \neq p$. Then Q has p^{2n} linear irreducible representations over K and every nonlinear irreducible representation has degree p^n over K. There are $p-1$ such representations.*

Proof. $|Z(Q)| = p$ so there are p central conjugacy classes of size 1, and $Q/Z(Q)$ is elementary abelian, so every other conjugacy class corresponds to a coset of $Z(Q)$ and has size p. There are $(p^{1+2n} - p)/p = (p^{2n} - 1)$ such. Thus there are $p^{2n} + p - 1$ conjugacy classes and irreducible representations of Q. Now $|Q/Z(Q)| = p^{2n}$ and is abelian, so we have p^{2n} linear characters by [Hup67, V.6.5]. Therefore there are $p - 1$ nonlinear characters, and their degrees are p^k for some $k \in \mathbb{N}$ since Q is a p-group.

Now $p^{1+2n} = |Q| = \sum_{\chi \in Irr(Q)} \chi(1)^2 = p^{2n} + \sum_{\chi \in Irr(Q), \chi(1)>1} \chi(1)^2$. Thus as $\sum_{\chi \in Irr(Q), \chi(1)>1} \chi(1)^2 = p^{2n}(p-1)$ has $p-1$ terms the average value is $\chi(1) = p^n$. However if there is some χ such that $\chi(1) > p^n$ then $\chi(1) \geq p^{1+n}$ and thus $\chi(1)^2 \geq p^{2+2n} > |Q|$. Hence all nonlinear representations must have degree p^n. $\square$

1.4 Isomorphisms between small classical groups

We will often encounter classical groups, and we have the following well-known isomorphisms between them.

Proposition 1.19 ([KL90, Proposition 2.9.1])**.** *The following groups are isomorphic:*

1. $SL_2(q) \cong Sp_2(q) \cong SU_2(q)$.

2. *For q odd, $PSL_2(q) \cong \Omega_3(q)$.*

3. $O_2^{\pm}(q) \cong D_{2(q\mp 1)}$, $SO_2^{\pm}(q) \cong C_{q\mp 1} \rtimes C_{(2,q)}$ *and* $\Omega_2^{\pm} \cong C_{(q\mp 1)/(2,q-1)}$.

4. $\Omega_4^+(q) \cong SL_2(q) \circ SL_2(q) \cong C_{(2,q-1)}.(PSL_2(q) \times PSL_2(q))$.

5. $\Omega_4^-(q) \cong PSL_2(q^2)$.

6. *For q odd, $PSp_4(q) \cong \Omega_5(q)$.*

7. $P\Omega_6^+(q) \cong PSL_4(q)$ *and* $P\Omega_6^-(q) \cong PSU_4(q)$.

8. $PSL_2(2) \cong S_3$ *(also $SL_2(2)$ and $GL_2(2)$).*

9. $PSL_2(3) \cong A_4$.

10. $PSL_2(4) \cong PSL_2(5) \cong A_5$.

11. $PSL_2(7) \cong PSL_3(2)$.

12. $PSL_2(9) \cong A_6$.

13. $PSL_4(2) \cong A_8$.

14. $PSU_3(2) \cong C_3^2 \rtimes Q_8$.

15. $PSU_4(2) \cong PSp_4(3)$.

16. $Sp_4(2) \cong S_6$.

1.5 p-groups with an extraspecial subgroup of index p

In this section we assume that S is a p-group containing an extraspecial subgroup Q with $|S : Q| = p$. We begin with some results about abelian subgroups of index p, which we can find in $S/Z(Q)$. We use the easy fact that if $X/Z(X)$ is cyclic then X is abelian ([Gor80, Lemma 1.3.4]), and note that since extraspecial groups have order at least p^3, the smallest examples satisfy $|S| = p^4$.

Lemma 1.20. *Suppose S is a p-group of order p^4. Then S contains an abelian subgroup of index p.*

Proof. As S is a p-group, it contains $H \trianglelefteq S$ of order p^2, hence H is abelian. Now $S/C_S(H) = N_S(H)/C_S(H)$ embeds into $\mathrm{Aut}(H)$ which in turn embeds into $GL_2(p)$, so $S/C_S(H)$ has order at most p. Therefore either $H \leq Z(S)$, in which case every maximal subgroup containing H is abelian, or $C_S(H)$ is abelian of index p in S. $\square$

Lemma 1.21 ([Oli14, Lemma 1.9])**.** *Suppose S is a nonabelian p-group with an abelian subgroup A of index p. Then $|S/Z(S)| = p|S'|$ and either*

1. *$|S'| = p$, $S/Z(S) \cong C_p^2$ and S contains exactly $p+1$ abelian subgroups of index p; or*
2. *$|S'| \geq p^2$ and A is the unique abelian subgroup of index p in S.*

We now move onto p-groups with an extraspecial subgroup of index p.

Lemma 1.22. *Suppose S is a finite p-group with an extraspecial subgroup Q of index p. Then either $Z(S) = Z(Q)$ or $S = QZ(S)$ and $|Z(S)| = p^2$.*

Proof. As $|Z(Q)| = p$ and $Z(Q) \trianglelefteq S$, we have $Z(Q) \leq Z(S)$. Thus either $Z(S) = Z(Q)$ or $Z(S) \nleq Q$, so $S = QZ(S)$ and since $|S : Q| = p$ we have $|Z(S)| = p^2$. $\square$

Lemma 1.23. *Suppose S is a p-group with an extraspecial subgroup Q of index p. Then $|S| = p^{2+2n}$ for some $n \in \mathbb{Z}_{>0}$, S has derived length at most 3, and S has exponent at most p^3.*

Proof. By Lemma 1.12 $|Q| = p^{1+2n}$ for some $n \in \mathbb{Z}_{>0}$. As $|S : Q| = p$, we have $|S| = p^{2+2n}$. We have $S' \leq Q$, so $S^{(2)} = [S', S'] \leq Q' \leq Z(S)$ is abelian and $S^{(3)} = [S^{(2)}, S^{(2)}] = 1$.

If $q \in Q$ then by Theorem 1.13 q has order at most p^2. As $|S : Q| = p$ if $g \in S \setminus Q$ then $g^p \in Q$ so g has order at most p^3. $\square$

Lemma 1.24. *Suppose S is a p-group with an extraspecial subgroup Q of index p. Then S has an abelian subgroup A of index p if and only if $|S| = p^4$.*

Proof. Suppose S has an abelian subgroup A and an extraspecial Q both of index p. Then $Q \cap A$ is abelian of index p in Q, so by Lemma 1.17 $|Q| = p^3$ and $|S| = p^4$. The converse follows by Lemma 1.20. $\square$

The outer automorphism group of an extraspecial group is closely related to the symplectic groups by Theorem 1.14. Hence, we now present a result on the conjugacy classes of p-elements in symplectic groups, which will help determine the upper and lower central series of p-groups as well as help classify extensions of extraspecial groups by a cyclic group of order p.

Theorem 1.25 ([LS12, Theorems 3.1 and 7.1])**.** *Let $G \cong Sp_{2n}(K)$ where K is algebraically closed field of characteristic p. Let $G_\sigma \cong Sp_{2n}(p)$. Let $u = \oplus_i J_i^{r_i}$ be a unipotent element in G. Then*

1. *Two unipotent elements of G are G-conjugate if and only if they are $GL_{2n}(K)$-conjugate (i.e. they have the same Jordan form).*
2. *r_i is even for each odd i.*
3. *$u^G \cap G_\sigma$ splits into 2^k G_σ-conjugacy classes where $k = |\{i : i \text{ even}, r_i > 0\}|$.*
4. *$C_{G_\sigma}(u) = V_\sigma R_\sigma$ where $R_\sigma = \prod_{i \text{ odd}} Sp_{r_i}(p) \times \prod_{i \text{ even}} O_{r_i}^{\epsilon_i}(p)$ where $\epsilon_i = \pm 1$.*

An application of this result is to obtain information about the upper and lower central series of S, as follows.

Lemma 1.26. *Suppose S is a p-group of order $p^{2+2n} \geq p^6$ with Q an extraspecial subgroup of index p and $|Z(S)| = p$. Then the following hold.*

1. *$|S/S'| = p^2$ if and only if S has maximal nilpotency class.*
2. *If $|S| = p^6$ and $|S'| = p^3$ then $S' = Z_2(S)$ and S has nilpotency class 3.*

In both cases Q is the unique extraspecial subgroup of index p and is characteristic in S.

Proof. Assume $|S/S'| = p^2$ and consider $\overline{S} := S/Z(S)$. Then $\overline{S}$ has an abelian subgroup $\overline{Q}$ of index p so Lemma 1.21 implies that $\overline{Q}$ is the unique abelian subgroup of index p in $\overline{S}$ and $|Z(\overline{S})| = |S/S'|/p = p$, hence $|Z_2(S)| = p^2$. The same argument applied to $S/Z_i(S)$ yields $|Z_{i+1}(S)| = p^{i+1}$ for $i \in \{2, \ldots, 2n-1\}$, hence $|Z_{2n}(S)| = p^{2n}$ and S has nilpotency class at least $2n+1$. But since S has order

p^{2+2n}, this is maximal nilpotency class. Conversely, if S has maximal nilpotency class then $|S/S'| = p^2$.

Now assume $|S| = p^6$ and $|S'| = p^3$. We can again apply Lemma 1.21 as $\overline{S}$ contains an abelian subgroup of index p, so $p|\overline{S}'| = |S/Z_2(S)|$ and $|Z_2(S)| = p^3$. Thus an element c_x of $S/Q \cong \mathrm{Out}_S(Q) \leq \mathrm{Out}_{\mathcal{F}}(Q)$, which embeds into $CSp_4(p)$ by Theorem 1.14, acts on $\overline{Q}$ with order p and kernel $\overline{Z_2(S)}$, hence its Jordan form has 2 nontrivial blocks and is either $J_3 \oplus J_1$ or $J_2 \oplus J_2$. However $J_3 \oplus J_1$ is not a symplectic element as it contains an odd number of blocks of a given odd size by Theorem 1.25 (2). Thus c_x has Jordan form $J_2 \oplus J_2$, acts quadratically on $\overline{Q}$, and $S' = Z_2(S)$. Therefore $Z_3(S) = S$, hence S has nilpotency class 3.

Now if R was a second extraspecial subgroup of index p then $S/Z(S)$ would contain two abelian subgroups of index p, whence Lemma 1.21 (1) implies that $|(S/Z(S))'| = p$ and $|S'| = p^2$, which does not hold in either case above. $\square$

We remark that the Sylow p-subgroups of $SL_4(p)$ and $SU_4(p)$ have the property described in Lemma 1.26 (2), and those of $G_2(p)$ have that of part (1) when $|S| = p^6$ unless $p = 3$.

Lemma 1.27. *Suppose S is a p-group with an extraspecial subgroup Q of index p. Let $H \trianglelefteq S$ and assume $S \ncong Q \times H$. Then either $H \leq Q$ and S/H has elementary abelian subgroups of index p or $H \nleq Q$ and S/H is elementary abelian.*

Proof. If $S \ncong Q \times H$ then $1 \neq H \cap Q \trianglelefteq Q$ so, by Lemma 1.9, $Z(Q) \leq H$. If $H \nleq Q$ then $S/H = QH/H \cong Q/(H \cap Q)$ which is elementary abelian as $\Phi(Q) = Z(Q) \leq H \cap Q$. On the other hand if $H \leq Q$ then S/H contains Q/H which is elementary abelian of index p. $\square$

The following p-groups will arise as Sylow p-subgroups of classical groups.

Lemma 1.28. *Let $H_{s,k} = C_{p^s} \wr C_p \wr \ldots \wr C_p$ with k wreathed factors. Then S contains an extraspecial subgroup of index p if and only if $p = 3$ and $H_{s,k} = H_{1,2} = C_3 \wr C_3$.*

Proof. By [Hup67, Satz III.15.3] $H_{1,k}$ is a Sylow p-subgroup of the symmetric group S_{p^k} and has derived length k and exponent p^k. Note also that $H_{1,k} \leq H_{s,k'}$ if $k \leq k'$. Therefore if $H_{s,k}$ has an extraspecial subgroup of index p then $k \leq 3$ and $s \leq 3$ by Lemma 1.23.

If $k = 1$ then $H_{s,1}$ is abelian. If $k = 2$ then $H_{s,2}$ has an abelian subgroup of index p so by Lemma 1.24 we need $p^4 = |H_{s,2}| = p^{1+sp}$, and $s = 1$, $p = 3$ is the only option. This is $H_{1,2} = C_3 \wr C_3$.

If $k = 3$ then $|H_{s,3}| = p^{1+p+sp^2}$ whereas by Lemma 1.23 $|H_{s,3}| = p^{2+2n}$, so p is odd, $s = 2$, and $n = \frac{-1+p+2p^2}{2}$. But $H_{2,3} = C_{p^2} \wr C_p \wr C_p$ has a homocyclic abelian subgroup of exponent p^2 and rank p^2, thus order p^{2p^2}, so we need $2p^2 \leq 2 + n$ by Lemma 1.17. Thus $4p^2 \leq 4 - 1 + p + 2p^2$. Therefore $2p^2 \leq 3 + p \leq 2p$, which is impossible.

$C_3 \wr C_3$ contains subgroups of index 3 and order 3^3 that are not abelian, and every group of order p^3 is either abelian or extraspecial, hence it contains extraspecial subgroups of index 3. □

Lemma 1.29. *Suppose $S = A \times B$ is a p-group with A, B nontrivial and S contains an extraspecial subgroup Q of index p. Then $S \cong Q \times C_p$.*

Proof. As $S = A \times B$, there is $C_p \times C_p \leq Z(S)$. Hence, since $|Z(Q)| = p$, there exists $x \in Z(S) \setminus Q$ of order p and, as $|S/Q| = p$, we have $S = Q \times \langle x \rangle \cong Q \times C_p$. □

1.6 Isomorphism classes of p-groups with an extraspecial subgroup of index p

In this section we use concepts and results from the theory of group extensions to study p-groups S containing an extraspecial subgroup Q of index p and exponent p. We follow [ML63] and refer to Appendix A for the definitions and results used.

Proposition 1.30. *Let p be odd. Suppose Q is an extraspecial group of exponent p, $K \cong C_p$ and $\psi : K \to \mathrm{Out}(Q)$ is a homomorphism. Then the abstract kernel (K, Q, ψ) has p congruence classes of extensions. There are at most p isomorphism classes of groups realising these extensions, one of which is split. The isomorphism type of the groups of this split extension is unique up to conjugacy of $K\psi$ in $\mathrm{Out}(Q)$.*

Proof. Let $|Q| = p^{1+2n}$. By assumption we have an abstract kernel (K, Q, ψ). By Lemma 1.16, $\mathrm{Aut}(Q) \cong \mathrm{Inn}(Q) \rtimes CSp_{2n}(p)$ via a splitting map ρ, so that the abstract kernel (K, Q, ψ) has a split extension $Q \rtimes_{\psi\rho} K$ by Lemma A.19.

Thus by Theorem A.18 the set of congruence classes of extensions of Q by K via ψ is in one-to-one correspondence with $H^2(K, Z(Q))$, which has order p by Lemma A.15. Since a congruence of extensions gives an isomorphism of the groups in the extensions by the Short Five Lemma A.3, there are at most p isomorphism classes of such groups S. By the remark after the statement of Theorem A.18 these extensions differ by the choice of f, which can be chosen to be trivial in a split extension. Hence there is a unique congruence class, thus there is a unique isomorphism type of split group extensions of the given abstract kernel.

We have proven that given K, Q and ψ there is a unique split extension of the abstract kernel (K, Q, ψ), and Lemma A.20 shows that this is independent of the conjugacy class representative of $K\psi$ in $\mathrm{Out}(Q)$. $\square$

Note that given a conjugacy class of $K\psi \leq \mathrm{Out}(Q)$ there are, for each element, $|\,\mathrm{Inn}(Q)|$ choices of coset representatives. These differ by some inner automorphism of Q and are not always in the same $\mathrm{Aut}(Q)$-conjugacy class. It is for this reason that we are considering homomorphisms into $\mathrm{Out}(Q) \cong CSp_{2n}(p)$. To obtain the conjugacy classes, we use Theorem 1.25 to obtain the corresponding ones in $Sp_{2n}(p)$, and then follow discussion in the proof of [GLO17, Proposition 2.3] for details of the relationship between conjugacy classes of $Sp_{2n}(p)$ and $CSp_{2n}(p)$.

As in Lemma 1.26, the Jordan form of $u = \oplus J_i^{r_i}$ given by $K\psi \leq \mathrm{Out}(Q) \cong CSp_{2n}(p)$ also determines the upper and lower central series of $S = Q \rtimes_{\psi\rho} K$ as follows. Let $m_j := \sum_{i \geq j} r_i$, the number of blocks in u of size at least j. Then

$$|\gamma_i(S) : \gamma_{i+1}(S)| = |Z_{i+1}(S) : Z_i(S)| = p^{m_i}$$

for $1 \leq i \leq c-1$ where c is the nilpotency class of S.

We now consider to p-groups of maximal class.

Proposition 1.31. *There exists a unique isomorphism class of p-groups S of maximal class containing an extraspecial subgroup $Q \cong p_+^{1+2n}$ and a complement $K \cong C_p$ to Q in S if and only if $1 + 2n \leq p$.*

Proof. S is an extension of the abstract kernel (K, Q, ψ) where the image of $K\psi$ in $CSp_{2n}(p)$ has a single Jordan block of size J_{2n}, which has order p if and only if $2n < p$. Thus S exists by Proposition 1.30 and the number of isomorphism classes of S with these properties coincides with the number of conjugacy classes of matrices with Jordan form J_{2n} in $CSp_{2n}(p)$.

By Theorem 1.25, if $1 \leq l \leq n$ and we have an element u with a single Jordan block of even size J_{2l}, then $k = 1$, and u^G splits into two conjugacy classes in $Sp_{2k}(G)$, and the centraliser of the two conjugacy classes have isomorphic centralisers. Further, by [GLO17, Proposition 2.3], they are fused in $CSp_{2n}(p)$, and conjugacy class representatives can be chosen to be u and u^α for α a nonsquare modulo p.

Therefore there is a unique conjugacy class of elements with Jordan form J_{2n} in $CSp_{2n}(p)$. Thus S is unique up to isomorphism whenever it exists, which is if and only if $1 + 2n \leq p$. □

We now consider p-groups of order p^6.

Proposition 1.32. *If $p \geq 5$ there are five isomorphism types of p-groups S of order p^6 containing an extraspecial subgroup $Q \cong p_+^{1+4}$ and a complement K to Q in S. If $p = 3$ there are four such groups. Information about the structure for all odd primes is as follows, where l is the number of $CSp_4(p)$-conjugacy classes corresponding to the given Jordan form and c is the nilpotency class of S. They have exponent p as long as $p > c$.*

<table>
<tr><th>Jordan form</th><th>k</th><th>l</th><th>Sylow of</th><th>c</th><th>Central series</th><th>Notes</th></tr>
<tr><td>J_4</td><td>1</td><td>1</td><td>$G_2(p)$</td><td>5</td><td>Maximal class</td><td>$p \geq 5$</td></tr>
<tr><td rowspan="2">J_2^2</td><td rowspan="2">1</td><td rowspan="2">2</td><td>$SL_4(p)$</td><td rowspan="2">3</td><td rowspan="2">$Z_2(S) = S'$, $|S'| = p^3$</td><td rowspan="2"></td></tr>
<tr><td>$SU_4(p)$</td></tr>
<tr><td>$J_2 \oplus J_1^2$</td><td>1</td><td>1</td><td></td><td>3</td><td>$|S'| = p^2$, $|Z_2(S)| = p^4$</td><td></td></tr>
<tr><td>$J_1^4 = I_4$</td><td>0</td><td>1</td><td></td><td>2</td><td>$S' = Q'$, $Z(S) = Z(Q) \times K$</td><td>$Q \times K$</td></tr>
</table>

Table 1.1: Split extensions of $Q \cong p_+^{1+4}$ by $K \cong C_p$.

Proof. By Proposition 1.30, such groups are in one-to-one correspondence with conjugacy classes of p-elements of order p in $\mathrm{Out}(Q) \cong CSp_4(p)$. By Theorem 1.25, these conjugacy classes have Jordan form J_4, J_2^2, $J_2 \oplus J_1^2$ or $J_1^4 = I_4$, where all except J_1^4 have $k = 1$. Thus there are two conjugacy classes of each nontrivial Jordan form in $Sp_4(p)$.

As in Proposition 1.31, the Jordan forms J_4 and $J_2 \oplus J_1^2$ contain a single Jordan block of even size, and we can again follow the argument in [GLO17, Proposition 2.3] to obtain that the two $Sp_4(p)$-conjugacy classes with each of the Jordan forms J_4 and $J_2 \oplus J_1^2$ are conjugate in $CSp_4(p)$.

On the other hand, if $1 \leq l \leq n/2$, the two $Sp_{2n}(p)$ conjugacy classes of matrices with Jordan form J_{2l}^2 have centralisers of distinct orders as, by Proposition 1.19 (3), $|O_2^+(p)| = 2(p-1) \neq 2(p+1) = |O_2^-(p)|$, hence they cannot fuse in $CSp_{2n}(p)$. Thus, the two conjugacy classes with form J_2^2 are not fused in $CSp_4(p)$. In the remaining case $J_1^4 = I_4$ centralises Q, hence it gives rise to $Q \times K$.

Note that if $p = 3$ then, as $4 \geq 3$, the Jordan block J_4 has order 9 and the corresponding ψ is not a homomorphism, and so there is no split group in this case.

By [GLS98, Theorem 2.2.9], the Sylow p-subgroups of $G_2(p)$ ($p \geq 5$), $SL_4(p)$ and $SU_4(p)$ have order p^6. If $p \geq 5$, the Sylow p-subgroups of $G_2(p)$ contain an extraspecial subgroup of index p by [PS18, Lemma 3.1]. For any prime, the Sylow p-subgroups of $SL_4(p)$ and $SU_4(p)$ also contain an extraspecial subgroup of index p which we can observe in the parabolic subgroups $p^{1+4} : (GL_2(p) \times (p-1))$ and $p^{1+4} : SU_2(p) : (p^2-1)$ described in [BHRD13, Tables 8.8 and 8.10] respectively.

Let $c = 5$ for $G_2(p)$ and $c = 3$ for $SL_4(p)$ and $SU_4(p)$. Then c is the nilpotency class of the Sylow p-subgroups by [GLS98, Proposition 3.3.1] and their upper and lower central series coincide. If $p > c$ then the Sylow p-subgroups have exponent p as $G_2(p)$ embeds into $SO_7(p)$ by [Wil09, p121], and $SL_4(p) \leq GL_p(p)$ and $SU_4(p) \leq GL_p(p^2)$, thus Q has exponent p and a complement $K \cong C_p$. In the remaining cases $G_2(5)$, $SL_4(3)$ and $SU_4(3)$ [GLS98, Proposition 3.3.1] (or a short

Magma check) their Sylow p-subgroups have exponent p^2 but have Q maximal of exponent p and a subgroup $R = C_S(Z_2(S))$ in $G_2(5)$ or $V = J(S)$ in $SL_4(3)$ and $SU_4(3)$ of exponent p, that is an element of order p outside Q. Thus in all cases they satisfy the conditions of S above with Jordan form J_4, J_2^2 and J_2^2 respectively.

The p-group corresponding to the Jordan form $J_2 \oplus J_1^2$ is isomorphic to a central product of a Sylow p-subgroup of $Sp_4(p)$, which is isomorphic to $p_+^{1+2} \rtimes K$ where K acts as J_2, and a Sylow p-subgroup of $SL_3(p)$, which is isomorphic to p_+^{1+2}. Hence in the central product K acts on $p_+^{1+4} \cong p_+^{1+2} \circ p_+^{1+2}$ as $J_2 \oplus J_1^2$. $\square$

Hence, in the situation of Proposition 1.32, the upper or lower central series of S determines S up to isomorphism, except in the case where S has nilpotency class 3 and K acts on Q/Z with Jordan form J_2^2, which gives rise to both the Sylow p-subgroups of $SL_4(p)$ and those of $SU_4(p)$, which are not isomorphic to each other. These two p-groups are very similar, as their exponent, nilpotency class and many more invariants coincide. A way to distinguish between them is by considering the maximal subgroups of S containing the unique abelian subgroup V of largest order. We first consider a module structure which will be relevant.

Lemma 1.33. *Let $X \cong SL_2(p^2)$, choose $T \in \mathrm{Syl}_p(X)$ and assume $E \cong C_p^4$ is a $GF(p)X$-module with $|C_E(T)| = p$. Then E is irreducible and a natural $\Omega_4^-(p)$-module for X. In particular every p-element of X acts on E with Jordan form $J_3 \oplus J_1$ if $p \neq 2$.*

Proof. As $|E| = p^4 \leq p^6$, [PR02, Lemma 3.12] implies that the irreducible components of E are one of the following modules:

1. A natural $SL_2(p^2)$-module, where $|C_E(T)| = p^2$.

2. A natural $\Omega_3(p^2)$-module with p odd, but this is 3-dimensional over $GF(p^2)$ and thus has order p^6 and $|C_E(T)| = p^2$.

3. A natural $\Omega_4^-(p)$-module with $|C_E(T)| = p$.

4. A triality module $V \otimes V^\sigma \otimes V^{\sigma^2}$ where σ is a field automorphism of order 3, which is impossible as we have $X = SL_2(p^2)$, and $GF(p^2)$ does not have field automorphisms of order 3.

Thus the only irreducible submodule of E is a natural $\Omega_4^-(p)$-module for X, which coincides with E as $|E| = p^4$, hence E is irreducible and a natural $\Omega_4^-(p)$-module for X.

Let x be a p-element of $\Omega_4^-(p)$. It acts on E with Jordan form is $J_3 \oplus J_1$ by [LS12, Theorem 3.1 (ii)], since it must have an even number of blocks of each even size and at least one block of odd size. $\square$

We can now prove the following result.

Lemma 1.34. *Suppose p is odd and S is a Sylow p-subgroup of $SL_4(p)$ or of $SU_4(p)$. Then S contains a unique abelian subgroup V of order p^4, and any maximal subgroup M of S containing V has $|Z(M)| = |M'| = p^2$.*

If S is a Sylow p-subgroup of $SL_4(p)$ then two such maximals satisfy $Z(M) = M'$ and the remaining $p-1$ are all isomorphic and have $Z(M) \neq M'$.

If S is a Sylow p-subgroup of $SU_4(p)$ then all $p+1$ maximal subgroups M of S containing V are isomorphic and have $Z(M) \neq M'$ with $|Z(M)| = |M'|$.

Proof. The structure of the maximal parabolic subgroups of $SL_4(p)$ and $SU_4(p)$ is given by [BHRD13, Tables 8.8 and 8.10]. In $SL_4(p)$ we have a maximal parabolic subgroup with shape $C_p^4 : (SL_2(p) \times SL_2(p)) : C_{p-1}$, whereas in $SU_4(p)$ the corresponding maximal parabolic has shape $C_p^4 : SL_2(p^2) : C_{p-1}$, both of which contain the corresponding Sylow p-subgroups. Thus S as in the statement contains an elementary abelian subgroup of order p^4, which we denote by V.

Note that V is the unique abelian subgroup of order p^4 in S as if W was a second one then $V \cap W \leq Z(VW)$. Hence, as $|Z(S)| = p$, $VW < S$ and $(VW)' = Z$ which implies $Z(S/Z) \geq Q/Z \cap VW/Z$, a contradiction since $|Z_2(S)| = p^3$.

A Sylow p-subgroup S of $SL_4(p)$ is given by the subgroup of lower triangular matrices with 1 on the diagonal, and $S/V \cong C_p \times C_p$ by Lemma 1.27, hence there are $p+1$ maximal subgroups of S containing V, which are given by

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ * & * & 1 & 0 \\ * & * & * & 1 \end{pmatrix}, \; M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & 1 & 0 & 0 \\ * & * & 1 & 0 \\ * & * & 0 & 1 \end{pmatrix} \text{ and } M_{(a)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ * & * & 1 & 0 \\ * & * & 1 & 1 \end{pmatrix}$$

where $a \in \{1, \ldots, p-1\}$. Then $Z(M_1) = M_1'$, $Z(M_2) = M_2'$ but $Z(M_{(a)}) \neq M_{(a)}'$. Further, there is an automorphism of S given by conjugation by a diagonal matrix with eigenvalues $(-1, \lambda, -1, 1)$ of order $p-1$ which normalises M_1 and M_2, but permutes the $M_{(a)}$, hence all $M_{(a)}$ are isomorphic.

On the other hand, in $SU_4(p)$, since the maximal parabolic considered above has shape $C_p^4 : SL_2(p^2) : C_{p-1}$, there exists an element θ of order p^2-1 in $SL_2(p^2)$ normalising a Sylow p-subgroup T of $SL_2(p^2)$ which is a complement to V in S, hence θ normalises V and a complement to V in S, and θ^{p-1} acts transitively on the $p+1$ maximal subgroups of S containing V. Further, as p is odd, Lemma 1.33 implies that every element of T acts on V with Jordan form $J_3 \oplus J_1$ hence the corresponding maximal subgroups M of S containing V have $Z(M) \neq M'$ with

$|Z(M)| = |M'| = p^2$. □

1.7 Actions of groups on p-groups

In the next sections we gather various results about groups acting on groups. Whenever we are talking about groups acting on groups we use multiplicative notation, but when we are considering actions on modules we use additive notation. We begin with an easy observation.

Lemma 1.35. *Let $K \trianglelefteq H$ be groups, $A \leq \mathrm{Aut}(H)$ with K normalised by A. If $[H, A] \leq K$ then A acts as the identity on H/K.*

Proof. Let $h \in H$, $\phi \in A$. Then, as $[H, A] \leq K$ we have $[h^{-1}, \phi] = h(h^{-1}\phi) \in K$ and $(Kh)\phi = (K\phi)(h\phi) = K(h\phi) = K[h^{-1}, \phi](h\phi) = Kh(h^{-1}\phi)(h\phi) = Kh$. □

We now consider coprime action, that is having automorphisms of order not divisible by p acting on p-groups. The following result of Burnside is a starting point.

Theorem 1.36 ([Gor80, 5.1.4 (Burnside)])**.** *Let ψ be a p'-automorphism of the p-group P which induces the identity on $P/\Phi(P)$. Then ψ is the identity automorphism of P.*

Lemma 1.37 ([Gor80, 5.3.3])**.** *Fix a prime p, a finite p-group S, and a group $G \leq \mathrm{Aut}(S)$ of automorphisms of S. Let $S_0 \trianglelefteq S_1 \trianglelefteq \cdots \trianglelefteq S_m = S$ be a sequence of subgroups, all normal in S and normalised by G, such that $S_0 \leq \Phi(S)$. Let $H \leq G$ be the subgroup of those $g \in G$ which act via the identity on S_i/S_{i-1} for each $1 \leq i \leq m$. Then H is a normal p-subgroup of G.*

Proof. By definition H is a normal subgroup of G. With the assumptions in the statement H stabilises the series $S_0 \trianglelefteq \ldots \trianglelefteq S_m$ in the sense of [Gor80, (5.3)], so by [Gor80, Corollary 5.3.3] H is a p-group. $\square$

We now see that coprime automorphisms also allow us to decompose p-groups.

Theorem 1.38 ([Gor80, Theorems 5.2.3, 5.3.5])**.** *Let A be a p'-group of automorphisms of the p-group P. Then $P = C_P(A)[P, A]$, and if P is abelian then $P = C_P(A) \times [P, A]$.*

We will need to consider submodules of cyclic modules, which satisfy the following lemma. We use additive notation as we are working with modules, and the result could also be phrased in multiplicative notation with respect of an element acting with a single Jordan block.

Lemma 1.39. *Let $Z = \langle x \rangle \cong C_p$ and K be a field of characteristic p. Suppose M is a cyclic KZ-module. Then $|M| \leq p^p$ and M has a unique maximal submodule $M(x-1)$ which is cyclic.*

Proof. Assume N is a maximal KZ-submodule of M, and note that we have $M(x-1)^p = M(x^p - 1) = M \cdot 0 = 0$. Choose l minimal such that $M(x-1)^l \leq N$. Then $M = N + M(x-1)^{l-1}$ as N is maximal. Hence

$$M(x-1) = N(x-1) + M(x-1)^l \leq N.$$

As M is cyclic, let m generate M. Then $m(x-1)$ generates $M(x-1)$ so $M(x-1)$ is also cyclic. Consider $M/M(x-1) = \langle m + M(x-1) \rangle$. Thus $\operatorname{codim}(M(x-1)) = 1$ and $M(x-1) = N$. $\square$

The next corollary follows from the proof above by induction.

Corollary 1.40. *In the situation of Lemma 1.39 if N is a submodule of M with M cyclic then $N = M(x-1)^s$ for some $s \in \mathbb{Z}_{\geq 0}$.*

1.8 Transvections

Definition 1.41. *Let V be a vector space of dimension $n \geq 2$ over a field K. An element $h \in SL(V)$ is a* transvection *if $[V,h] \leq C_V(h)$ with $\dim([V,h]) = 1$ and $\dim(C_V(h)) = n-1$.*

We will use the characterisation of groups generated by transvections by McLaughlin. The theorems depend on whether or not p is even.

Theorem 1.42 ([McL67, Theorem])**.** *Suppose $K = GF(p) \neq GF(2)$, $\dim(V) \geq 2$, and that G is a subgroup of $SL(V)$ which is generated by transvections. Suppose also that $O_p(G) = 1$. Then for some $s \geq 1$, $V = V_0 \oplus V_1 \oplus ... \oplus V_s$, $G = G_1 \times ... \times G_s$, and*

1. *The V_i are stable for the G_j.*
2. *$G_i|_{V_j} = 1$ if $i \neq j$. In particular $[V_0, G] = 1$.*
3. *$G_i|_{V_i} = SL(V_i)$ or $Sp(V_i)$.*

Theorem 1.43 ([McL69, Theorem])**.** *Let V be a vector space of dimension $n \geq 2$ over $GF(2)$, and let G be an irreducible subgroup of $SL(V)$ which is generated by transvections. If $G \neq SL(V)$ then $n \geq 4$ and G is one of the following subgroups of $Sp_n(V)$: $Sp_n(V)$, $O_n^-(V)$, $O_n^+(V)$ (except at $n=4$), S_{n+2}, or S_{n+1}.*

The exception arises because $O_4^+(V) \cong (S_3 \times S_3) : C_2$ via Proposition 1.19 (4,8), where transvections generate the subgroup $\Omega_4^+(V)$ which is not irreducible.

In particular we will be interested in the cases where the Sylow p-subgroups of G are elementary abelian, so we look more closely at this case.

Lemma 1.44. *Suppose V is a vector space over $GF(p)$, $\dim(V) \geq 2$. Let G be an irreducible subgroup of $SL(V)$ generated by transvections with elementary abelian Sylow p-subgroups. Then $V = V_1$ has dimension 2 and $G \cong SL_2(p)$.*

Proof. In the situation of the Lemma, $O_p(G) = 1$ so if p is odd we can apply Theorem 1.42 to obtain $V = V_0 \oplus V_1 \oplus ... \oplus V_s$. As G acts irreducibly on V, $s = 1$, V_0 is trivial and, as the Sylow p-subgroups of $SL_3(p)$ and $Sp_4(p)$ are nonabelian, V_1 is 2-dimensional.

If $p = 2$ we consider the minimal examples that arise. Since $SL_3(2)$ has nonabelian Sylow 2-subgroups, neither do any groups containing it, such as $O_6^+(2)$, since $\Omega_6^+(2) \cong PSL_4(2) \cong GL_4(2)$ by Proposition 1.19 (7). Note that $Sp_4(2) \cong S_6$ by Proposition 1.19 (16), and the smallest symmetric group that arises is S_5, with Sylow 2-subgroups isomorphic to $C_2 \wr C_2 \cong D_8$. Now $\Omega_4^-(2) \cong PSL_2(4) \cong A_5$ by Proposition 1.19 (5,10), which have index 2 in $O_4^-(2) \cong S_5$. Thus the only remaining case is $SL_2(2^k)$, which has elementary abelian Sylow 2-subgroups. $\square$

1.9 Quadratic action and Thompson Replacement Theorem

Transvections are a particular case of quadratic action, which we now introduce.

Definition 1.45 ([GLS96, 25.1])**.** *Let p be a prime, X be a group, and $A \leq X$ a*

p-subgroup. If P is an A-invariant p-subgroup of X with $[P, A, A] = 1$, we say that A acts quadratically *on P. If V is a faithful $GF(p)X$-module, $A \leq GL(V)$ and $[V, A, A] = 0$ and $A \neq 1$ then we say that V is a* quadratic X-module.

If G is a group with $O_p(G) = 1$ (p odd), a faithful representation ϕ of G on a vector space V over $GF(p^n)$ is called p-stable *provided no p-element of $G\phi$ has a quadratic minimal polynomial. The group G is* p-stable *if all such faithful representations are p-stable.*

We note that if $p = 2$ then every element of order 2 acting faithfully on a vector space V over $GF(2)$ has minimal polynomial $x^2 + 1 = x^2 + 2x + 1 = (x + 1)^2$, hence quadratic action becomes interesting when p is odd.

Lemma 1.46. *Suppose $A \leq X$ is a group which acts quadratically on a faithful $GF(p)X$-module V. Then A is elementary abelian.*

Proof. Since $[V, A, A] = 0$, we have $[A, V, A] = 0$ and by the Three Subgroup Lemma $[A, A, V] = 0$, so as A acts faithfully it follows that $[A, A] = 1$, that is A is abelian. Now let $a \in A$ and $v \in V$, then $[v, a, a] = 0$ so $[v, a] \in C_V(a)$ and hence $[v, a^2] = [v, a]^a + [v, a] = 2[v, a]$, thus for $m \geq 2$ we have $[v, a^m] = m[v, a]$. In particular $p[v, a] = 0$ and as V is a faithful $GF(p)$-module this means that $a^p = 1$, so A is elementary abelian. □

The concepts above are closely linked to $SL_2(p)$, as the following result demonstrates.

Theorem 1.47 ([Gor80, Theorem 3.8.3])**.** *Let p be odd and G be a group with $O_p(G) = 1$. If G is not p-stable then there are subgroups $K \trianglelefteq H \leq G$ such that $H/K \cong SL_2(p)$.*

Lemma 1.50 will be useful when studying $\mathrm{Aut}_{\mathcal{F}}(Q)$. It uses standard techniques and is similar to [Che04, Lemma 2.8 (U. Meierfrankenfeld)]. Note that it does not work for $p \leq 3$. We will need it when discussing the automisers of essential subgroups when S is a Sylow p-subgroup of $SL_4(p)$ or $SU_4(p)$.

Lemma 1.48. *Let G be a group, K be a field, $S \in \mathrm{Syl}_p(G)$, and V_1, V_2 be KG-modules. Let $\theta : V_1 \to V_2$ be a KG-module isomorphism. Then the eigenvalues of $r \in N_G(S)$ on $C_{V_1}(S)$ and on $C_{V_2}(S)$ are the same.*

Proof. Let $v \in C_{V_1}(S)$, then $(v\theta)s = (vs)\theta = v\theta$ for all $s \in S$, so $C_{V_1}(S)\theta = C_{V_2}(S)$. Further, let v be a λ-eigenvector for r, then $(v\theta)r = (vr)\theta = (\lambda v)\theta = \lambda(v\theta)$, so $v\theta$ is a λ-eigenvector for r. The same argument with θ^{-1} gives this property for θ^{-1}, hence the lemma is proved. □

Lemma 1.49. *Let $H \cong SL_2(p)$ and $S \in \mathrm{Syl}_p(H)$, let V be the natural module for H and let $r \in N_H(S) \setminus S$. Then there exists $h \in H \backslash N_H(S)$ such that r normalizes S^h. Moreover, if $o(r) \neq 2$, the subspaces $C_V(S)$ and $C_V(S^h)$ are eigenspaces of r for distinct eigenvalues λ and λ^{-1}.*

Proof. By Sylow's Theorems, we may assume that S consists of unipotent lower triangular matrices. Then, as $N_H(S) \cong C_p \rtimes C_{p-1}$ contains a unique conjugacy class of complements to S and $r \in N_H(S) \setminus S$, we may assume $r = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ for some $\lambda \in GF(p)$, hence r normalises the subgroup of unipotent upper triangular matrices, which is another Sylow p-subgroup of H and hence is S^h for some $h \in H \setminus N_H(S)$. Further, r has eigenspaces $C_V(S)$ and $C_V(S^h)$ with respective eigenvalues λ and λ^{-1}, which are distinct unless $\lambda^2 = 1$, that is $o(r) = 2$. □

Lemma 1.50. *Let $p > 3$, G be a group with $S \in \mathrm{Syl}_p(G)$ of order p, $O_p(G) = 1$, and let V be a 4-dimensional faithful $GF(p)G$-module with $C_V(S) = [V, S]$ of dimension 2. Then $O^{p'}(G) \cong SL_2(p)$ and V is a direct sum of two natural $SL_2(p)$-modules.*

Proof. Since G acts faithfully on V, G embeds into $\mathrm{Aut}(V) \cong GL_4(p)$. Assume G is a minimal counterexample to the lemma, that is, $S \le G \le GL_4(p)$ with $|G|$ minimal such that $O_p(G) = 1$ and if $S \le L < G$ with $O_p(L) = 1$ then $O^{p'}(L) \cong SL_2(p)$ and V is a direct sum of two natural $SL_2(p)$-modules for L.

Let $S = \langle s \rangle$. Since $C_V(S) = [V, S]$, we have $[V, s, s] = 0$, and, as $O_p(G) = 1$, $s \in G \setminus O_p(G)$. Because V is a faithful G-module, [Che04, Lemma 2.4] yields G has a subgroup H such that $H = \langle s^H \rangle \cong SL_2(p)$, and $V = [V, H] \oplus C_V(O^p(H))$ where $[V, H]$ is a direct sum of natural $SL_2(p)$-modules for H. Since $p > 3$, $O^p(H) = H$, so $C_V(O^p(H)) = 0$, as otherwise $\dim([V, s]) = 1$. Hence $V = [V, H]$ has dimension 4. Furthermore, as an H-module, $V = [V, H]$ is a direct sum of two natural $SL_2(p)$-modules. In particular, the central involution $t \in Z(H)$ negates V and so $t = -I_4 \in Z(GL_4(p))$ and $t \in Z(G)$. Therefore

$$C_V(G) \le C_V(H) \le C_V(t) = 0.$$

Let $T \in \mathrm{Syl}_p(H) \setminus \{S\}$. Then $H = \langle S, T \rangle$. Since G is a counterexample to the lemma, $H \neq O^{p'}(G)$ and so H is not normal in G.

Let $U \in \mathrm{Syl}_p(G) \setminus \{S\}$ and set $L = \langle S, U \rangle$. Since $S \neq U$, $O_p(L) = 1$. Assume that $C_V(S) \cap C_V(U) \neq 0$. Then

$$C_V(L) = C_V(S) \cap C_V(U) > 0 = C_V(G)$$

and so $L < G$. Since L satisfies the hypothesis of the lemma, induction implies $L = O^{p'}(L) \cong SL_2(p)$, $V|_L$ is a direct sum of two natural $SL_2(p)$-modules for L. But this means $C_V(L) = 0$, a contradiction.

Therefore, if $R, U \in \mathrm{Syl}_p(G)$ with $R \neq U$, then

$$C_V(R) \cap C_V(U) = 0. \tag{\dagger}$$

In particular,

$$|\bigcup_{R \in \mathrm{Syl}_p(G)} C_V(R)| = |\mathrm{Syl}_p(G)|(p^2 - 1) + 1 \leq p^4.$$

Hence $\left|\mathrm{Syl}_p(G)\right| \leq p^2 + 1$.

We investigate $N_G(S)$. Since $\mathrm{Aut}(S)$ is abelian, we have $N_G(S)' \leq C_G(S)$. Furthermore, $N_G(S)$ acts on $C_V(S)$ and so $N_G(S)/C_{N_G(S)}(C_V(S))$ is isomorphic to a subgroup of $\mathrm{Aut}(C_V(S)) \cong GL_2(p)$. Observe that $N_H(S)C_{N_G(S)}(C_V(S))/C_{N_G(S)}(C_V(S))$ acts on $C_V(S)$ as scalars by Lemma 1.48 (the eigenvalues of elements of $N_H(S)$ on $C_V(S)$ are equal). It follows that

$$[N_H(S), N_G(S)] \leq C_{N_G(S)}(C_V(S)) \cap N_G(S)' \leq C_{N_G(S)}(C_V(S)) \cap C_G(S).$$

Assume that $x \in [N_H(S), N_G(S)]$ has p'-order. Then $[V, S, x] = [[V, S], x] = 0$ and so the Three Subgroups Lemma implies $[V, x, S] = 0$. Hence $[V, x, x] = 0$ and so x centralizes V by coprime action. It follows by [Gor80, Theorem 5.3.6] that $x = 1$. Hence $[N_H(S), N_G(S)]$ is a p-group. As $[N_H(S), N_H(S)] = S$ and $S \in \mathrm{Syl}_p(G)$, we conclude that

$$[N_H(S), N_G(S)] = S \leq N_H(S)$$

and so $N_H(S)$ is normal in $N_G(S)$.

Assume that no two distinct conjugates of H contain S. Then, by Sylow's Theorem, for $k, \ell \in G$ with $H^k \neq H^\ell$, $|H^k \cap H^\ell|$ is coprime to p. Suppose K is a conjugate of H with $H \neq K$. Then, as $S \leq H$ and $S \in \mathrm{Syl}_p(G)$, S does not normalise K, as otherwise $p^2 \mid |SK|$. Hence $|\{K^s \mid s \in S\}| = p$ and, for all $s \in S$, p does not divide $|K^s \cap K|$. Thus

$$\begin{aligned} |\mathrm{Syl}_p(G)| &\geq |\mathrm{Syl}_p(H)| + \sum_{s \in S} |\mathrm{Syl}_p(K^s)| = p + 1 + p(p+1) \\ &= p^2 + 2p + 1 > p^2 + 1 \geq |\mathrm{Syl}_p(G)|, \end{aligned}$$

a contradiction.

Let K be a conjugate of H with $K \neq H$ and $S \leq H \cap K$. Then $K = H^g$ for some $g \in G$ and so $S, S^g \leq K$. By Sylow's Theorem, there exists $k \in K$ such that $S^{gk} = S$. Now $H^{gk} = K^k = K$. Hence we may assume that $g \in N_G(S)$. In particular, as $N_H(S)$ is normal in $N_G(S)$, $N_H(S) = N_H(S)^g \leq H^g = K$. Hence $N_H(S) = N_K(S)$. Let X be a complement to S in $N_H(S)$ which normalizes T. Then X is cyclic of order $p-1$, $X \leq N_K(S)$ and X normalizes some $U \in \mathrm{Syl}_p(K) \setminus \{S\}$. Let x be a generator of X and note that by the assumption $p > 3$, x is not an involution. Therefore Lemma 1.49 yields x has exactly two eigenvalues λ and λ^{-1} on V and the corresponding eigenspaces are $C_V(S)$ and $C_V(T)$. Since $C_V(S) \cap C_V(U) = 0$ and X acts on $C_V(U)$, there is an eigenvector for x in $C_V(U)$ which is not in $C_V(S)$. It follows that $C_V(U) \cap C_V(T) \neq 0$. By (†), we conclude that

$T = U$. But then $K = \langle S, U \rangle = \langle S, T \rangle = H$, a contradiction. This contradiction proves G is not a counterexample and proves the lemma. $\square$

A way to find quadratic actions is given by Thompson's Replacement Theorem, which does not require that p be odd.

Definition 1.51. *We define*

$$\mathcal{A}(P) := \{A \leq P \mid A \textit{ is elementary abelian of maximal order in } P\}.$$

Theorem 1.52 (Thompson's Replacement Theorem [GLS96, Theorem 25.2])**.** *Let P be a p-group and V a normal elementary abelian subgroup of P. Suppose that $A \in \mathcal{A}(P)$ but V does not normalise A. Then there exists $A^* \in \mathcal{A}(P)$ such that $A \cap V < A^* \cap V$ and $[A, A^*] \leq A$. Moreover, there exists some $A_1 \in \mathcal{A}(P)$ with $[V, A_1, A_1] = 1$ and $[V, A_1] \neq 1$.*

We will use it as follows.

Lemma 1.53. *Assume S is a p-group and $F \leq S$ is elementary abelian such that $C_S(F) = F$. Then either $F \trianglelefteq S$ is the unique elementary abelian subgroup of maximal order in S or F admits quadratic action.*

Proof. If $\mathcal{A}(N_S(F)) = \{F\}$ then F is characteristic in $N_S(F)$ and normal in $N_S(N_S(F))$. Thus $N_S(N_S(F)) = N_S(F) = S$ and $F \trianglelefteq S$. Then $\mathcal{A}(S) = \mathcal{A}(N_S(F)) = \{F\}$ and F is the unique elementary abelian subgroup of maximal order in S.

Otherwise, there is $A \in \mathcal{A}(N_S(F)) \setminus \{F\}$. If F does not normalise A, then by Theorem 1.52 there exists some $A_1 \in \mathcal{A}(N_S(F)) \setminus \{F\}$ acting quadratically on F.

If F normalises A, then $1 \neq [F, A] \leq A$ since $C_S(F) \leq F$, and $[F, A, A] = 1$, so F admits a quadratic action in both cases. □

1.10 Strongly p-embedded subgroups

Strongly p-embedded subgroups play an important role in saturated fusion systems, hence we study some of their properties, which can be found in [GLS96, Section 17].

Definition 1.54. *Suppose G is a finite group and let p be a prime. A proper subgroup H of G is* strongly p-embedded *in G if p divides $|H|$ and for all $x \in G \backslash H$, p does not divide $|H \cap H^x|$.*

Lemma 1.55 ([GLS96, Proposition 17.11])**.** *G has a strongly p-embedded subgroup H if and only if $C_G(x) \leq H$ for all elements of order p in H and $N_G(P) \leq H$ for $P \in \mathrm{Syl}_p(H)$.*

The following corollary is also well-known and can be found in [GLS96, Proposition 17.11].

Corollary 1.56. *1. H is strongly p-embedded in G if and only if $N_G(P) \leq H$ for all nontrivial p-subgroups $P \leq H$;*

2. A strongly p-embedded subgroup of G contains a Sylow p-subgroup of G;

3. If G has a strongly p-embedded subgroup then $O_p(G) = 1$;

4. If G has a cyclic Sylow p-subgroup P and $O_p(G) = 1$, then $N_G(\Omega_1(P))$ is strongly p-embedded in G.

In particular, if $P \cong C_p$ then either $N_G(P) = G$ or $N_G(P) < G$ is strongly p-embedded in G.

Proof. 1. Suppose H is strongly p-embedded in G. If there is a p-group $P \leq H$, such that $N_G(P) \nleq H$, then there is a $g \in G$ with $g \in N_G(P) \setminus H$. Then $P = P^g \cap P \leq H^g \cap H$ and, therefore, p divides $|H^g \cap H|$, a contradiction. Thus $N_G(P) \leq H$ for all p-subgroups $P \leq H$.

Conversely, note that if $N_G(P) \leq H$ for all p-subgroups $P \leq H$ then for any element x of order p in H we have $C_G(x) \leq N_G(\langle x \rangle) \leq H$, and if $S \in \mathrm{Syl}_p(H)$ then $N_G(S) \leq H$ by assumption, so by Lemma 1.55 H is strongly p-embedded in G.

2. Follows by (1) as if $R \in \mathrm{Syl}_p(H)$ and $R \notin \mathrm{Syl}_p(G)$ then $H \geq N_P(R) > R$ where $R \leq P \in \mathrm{Syl}_p(G)$.

3. Suppose $H < G$ is strongly p-embedded. We know that $O_p(G)$ is contained in every Sylow p-subgroup of G and thus by (2) $O_p(G) \leq H$. If $O_p(G) \neq 1$, by (1) $G = N_G(O_p(G)) \leq H < G$, a contradiction. Hence $O_p(G) = 1$.

4. Assume $P \in \mathrm{Syl}_p(G)$ is cyclic and set $H = N_G(\Omega_1(P)) < G$ as $O_p(G) = 1$. Then $P \leq H$. Let $1 \neq Q \leq H$ be a p-group. Then $Q \leq P^g$ for some $g \in H$. As P^g is cyclic, $\Omega_1(Q) = \Omega_1(P^g) = \Omega_1(P)^g = \Omega_1(P)$ so we have $N_G(Q) \leq N_G(\Omega_1(Q)) = N_G(\Omega_1(P)) = H$ and H is strongly p-embedded in G by (1).

In particular, if $P \cong C_p$ then $\Omega_1(P) = P$ and the last part follows.

$\square$

By Corollary 1.56 (4), there is no hope of classifying all groups with strongly p-embedded subgroups when the group has Sylow p-subgroups which are cyclic. However, if they have p-rank at least 2 then the structure of G is close to being simple. We will use the following lemma. We recall that a group G is almost simple if there exists a nonabelian finite simple group T such that $T \leq G \leq \mathrm{Aut}(T)$.

Lemma 1.57. *Suppose G is a finite group with $T \trianglelefteq G$ a nonabelian simple group that is the unique minimal normal subgroup of G. Then G is almost simple.*

Proof. As $T \trianglelefteq G$ we have a map $\phi : G \to \mathrm{Aut}(T)$ such that $g\phi = c_g|_T$. Then $\ker \phi = C_G(T) \trianglelefteq N_G(T) = G$, but $C_G(T) \cap T = Z(T) = 1$ as T is nonabelian simple. Thus since T is the unique minimal normal subgroup of G, we have $C_G(T) = 1$ and ϕ is injective, so G is isomorphic to a subgroup of $\mathrm{Aut}(T)$. We have $T\phi = \mathrm{Inn}(T)$, so $T \leq G \leq \mathrm{Aut}(T)$ and G is almost simple. □

Theorem 1.58. *Assume that G is a finite group, $H < G$ is strongly p-embedded and H contains an elementary abelian subgroup of order p^2. Then $O_{p'}(G) \leq H$, $H/O_{p'}(G)$ is strongly p-embedded in $G/O_{p'}(G)$, and $O^{p'}(G/O_{p'}(G))$ is a nonabelian almost simple group.*

Proof. Assume that H is strongly p-embedded in G. Let $\overline{G} = G/O_{p'}(G)$. Assume T is a normal p'-subgroup of G. Let $A \leq H$ be elementary abelian of order p^2. Then by [Gor80, Theorem 6.2.4] we have $T = \langle C_T(a) \mid a \in A \setminus 1 \rangle$.

As H is strongly p-embedded in G, we have by Lemma 1.55 $T \leq H$. In particular, $O_{p'}(G) \leq H$. Then for any p-group $\overline{P} \leq \overline{H} = H/O_{p'}(G)$, we have $\overline{P} = R/O_{p'}(G)$ for some $R \leq H$ with $O_{p'}(G) \leq R$. Let $P \in \mathrm{Syl}_p(R)$. Then by the Frattini Argument (Theorem 1.1) $N_G(R) = N_G(P)R \leq H$ as H is strongly

p-embedded in G. Therefore $N_{\overline{G}}(\overline{P}) = \overline{N_G(R)} \leq \overline{H}$ and, by Corollary 1.56 (1), $\overline{H}$ is strongly p-embedded in $\overline{G}$.

So now assume $O_{p'}(G) = 1$, fix $S \in \mathrm{Syl}_p(G)$, and let T be a minimal normal subgroup of G. As G has a strongly p-embedded subgroup H, $O_p(G) = 1$ by Corollary 1.56 (3). Then T is not a p-group and not a p'-group either as $O_{p'}(G) = 1$. As T is minimal normal, it is characteristically simple. Thus, as T is nonabelian, T is a direct product of isomorphic nonabelian simple groups $T = L_1 \times \ldots \times L_k$ by [Asc86, Lemma 8.2].

If $k > 1$ let $S_1 = S \cap L_1 \in \mathrm{Syl}_p(L_1)$ and $S_2 = S \cap (L_2 \times ... \times L_k)$ which is in $\mathrm{Syl}_p(L_2 \times ... \times L_k)$. As $O_{p'}(G) = 1$, S_1 and S_2 are nontrivial. Hence $L_1 \leq N_G(S_2)$ and $L_2 \times ... \times L_k \leq N_G(S_1)$. Since H is strongly p-embedded in G then $N_G(S_i) \leq H$, so $T = L_1 \times L_2 \times ... \times L_k \leq H$. Then if $S_0 = S \cap T \in \mathrm{Syl}_p(T)$ we have, by the Frattini Argument $N_G(S_0)T = G$, but $N_G(S_0)T \leq H \neq G$, a contradiction. Thus $k = 1$ and T is nonabelian simple.

Further, assume there are two minimal normal subgroups T_1, T_2. Denote by $S_1 = S \cap T_1 \in \mathrm{Syl}_p(T_1)$ and $S_2 = S \cap T_2 \in \mathrm{Syl}_p(T_2)$. Then $[T_1, T_2] \leq T_1 \cap T_2 = 1$ and $T_1 \times T_2 \leq soc(G) \leq G$. So $T_1 \leq N_G(S_2)$, $T_2 \leq N_G(S_1)$, and thus $T_1T_2 \leq H$. Then by the Frattini Argument $N_G(S_1)T_1 = G$, but $N_G(S_1)T_1 \leq H \neq G$, a contradiction.

Thus T is the unique minimal normal subgroup of G, and is a nonabelian simple group. Then G is almost simple by Lemma 1.57. □

As a consequence of the Classification of Finite Simple Groups we have a list of the almost simple groups below, which is stated in [GLS98] in the setting of the known finite simple groups.

Theorem 1.59 ([GLS98, Theorem 7.6.1])**.** *Assume that G is a finite group, $H < G$*

is strongly p-embedded and H contains an elementary abelian subgroup of order p^2. Then $O^{p'}(G/O_{p'}(G))$ is one of the following nonabelian almost simple groups:

1. *$PSL_2(p^n)$ for any p and $n \geq 2$.*

2. *$PSU_3(p^n)$ for any p and $p^n \geq 3$.*

3. *$Sz(2^{2n+1}) = {}^2B_2(2^{2n+1})$ for $p = 2$ and $n \geq 1$.*

4. *${}^2G_2(3^{2n-1})$ for $p = 3$ and $n \geq 1$.*

5. *A_{2p} for $p \geq 5$.*

6. *$PSL_3(4)$, M_{11}, $PSL_2(8) : C_3$ for $p = 3$.*

7. *$Sz(32) : C_5$, ${}^2F_4(2)'$, McL, Fi_{22} for $p = 5$.*

8. *J_4 for $p = 11$.*

Proof. By Theorem 1.58 $O^{p'}(G/O_{p'}(G))$ is a nonabelian almost simple group. If p is odd, by [GL83, (24-1)] we get all cases above except $PSL_2(8) : C_3$ for $p = 3$, $Sz(32) : C_5$ for $p = 5$, which are found in [GL83, (24-4)] or [GLS15]. Case (i) of (24-1) is ruled out by [GLS98, Theorem 7.5.5].

When $p = 2$ the result follows from the Bender-Suzuki Theorem [Ben71, Satz 1], which says that if a group G has a strongly 2-embedded subgroup then either its Sylow 2-subgroups are cyclic or quaternionic, hence of 2-rank 1, or $O^{p'}(G/O_{p'}(G))$ is one of $PSL_2(q)$, $Sz(q)$, $PSU_3(q)$ for $q = 2^n \geq 4$. □

Corollary 1.60. *The structure of the Sylow p-subgroups S of the groups in Theorem 1.59 is as follows.*

1. *If $O^{p'}(G/O_{p'}(G)) \cong PSL_2(p^n)$ then $S \cong C_p^n$ for any p and $n \geq 2$;*

2. *If $O^{p'}(G/O_{p'}(G))$ is one of A_{2p} for $p \geq 5$, $PSL_3(4)$ and M_{11} for $p = 3$, ${}^2F_4(2)'$ and Fi_{22} for $p = 5$ then $S \cong C_p^2$;*

3. *If $O^{p'}(G/O_{p'}(G)) \cong PSU_3(p^n)$ then S has order p^{3n} and nilpotency class 2;*

4. *If $O^{p'}(G/O_{p'}(G)) \cong Sz(2^{2n+1})$ then S has order $(2^{2n+1})^2$ and nilpotency class 2;*

5. *If $O^{p'}(G/O_{p'}(G)) \cong {}^2G_2(3^{2n+1})$ then S has order $(3^{2n+1})^3$ and nilpotency class 2;*

6. *$S \cong p_+^{1+2}$ when $O^{p'}(G/O_{p'}(G))$ is either McL for $p = 5$ or J_4 for $p = 11$;*

7. *$S \cong p_-^{1+2}$ when $O^{p'}(G/O_{p'}(G))$ is either $PSL_2(8) : C_3$ for $p = 3$, $Sz(32) : C_5$ for $p = 5$.*

Proof. The groups in question are finite simple groups (or almost simple in case (7)), so all facts can be deduced from [GLS98] or [CCN+85].

For the groups of Lie type and Lie rank r the orders are given by [GLS98, Theorem 2.2.9], and the nilpotency class equals r by [GLS98, Theorem 3.3.1] when it is nonsingular, which in the cases above is always true. Hence we see that $PSL_2(p^n) \cong A_1(p^n)$ has abelian (hence elementary abelian) Sylow p-subgroups and part (1) holds. The result applied to $PSU_3(p^n) \cong {}^2A_2(p^n)$, $Sz(2^{2n+1}) \cong {}^2B_2(2^{2n+1})$ and ${}^2G_2(3^{2n-1})$ proves parts (3), (4) and (5).

Case (2) holds as we assume $C_p^2 \leq S$ in Theorem 1.59 and the corresponding Sylow p-subgroups have order p^2.

Case (6) holds as both McL and J_4 have $|S| = p^3$, they contain maximal subgroups of shape $5^{1+2} : C_3 : C_8$ and $11^{1+2} : (C_5 \times 2S_4)$ respectively, and no elements of order p^2 by [WWT+05].

Finally, by [GLS98, Theorem 3.3.2(d)], ${}^2G_2(3) \cong L_2(8)$ with $p = 3$ and $Sz(32)$ with $p = 5$ have Sylow p-subgroups cyclic of order p^2 and which become nonabelian of order p^3 in the automorphism groups $L_2(8) : C_3$ and $Sz(32) : C_5$ as can be seen in the maximal subgroups $C_9 : C_6$ and $C_{25} : C_{20}$ (which are $C_{p^2} : \mathrm{Aut}(C_{p^2})$) in [WWT+05]. Hence case (7) holds and the corollary is proved. □

We now prove that normal subgroups whose order is divisible by p also contain a strongly p-embedded subgroup.

Lemma 1.61. *Assume that G is a finite group, H is strongly p-embedded in G, and $K \leq G$ with $p \mid |K|$. Then either $K \leq H^g$ for some $g \in G$ or $H \cap K$ is strongly p-embedded in K. In particular, if $p \mid |K|$ and $K \trianglelefteq G$ then $H \cap K$ is strongly p-embedded in K.*

Proof. Let $T \in \mathrm{Syl}_p(K)$ and $S \in \mathrm{Syl}_p(G)$ such that $T \leq S$. By Corollary 1.56 (2) and Sylow's Theorems there exists $l \in G$ such that $S \leq H^l$. Now let $H_0 = H^l \cap K$, then $T \leq H_0$ so $p \mid |H_0|$. Further, unless $K \leq H^g$ for some $g \in G$, we have $H_0 = H^l \cap K < K$. Now let $k \in K \setminus H_0$, then $k \in G \setminus H$ so p does not divide $|H^l \cap H^{lk}|$, hence it does not divide $|H_0 \cap H_0^k|$ either, that is H_0 is strongly p-embedded in K as claimed.

Finally, if $K \trianglelefteq G$, then we have $G = KN_G(T) \leq KH$ by Frattini's Argument (Theorem 1.1) and Corollary 1.56 (1). As $H < G$ by assumption, we have $K \not\leq H$, so for all $g \in G$ we have $K = K^g \not\leq H^g$ and by the previous part $H \cap K$ is strongly p-embedded in K. □

We now consider which groups can contain a subgroup which is both generated by transvections and contains a strongly p-embedded subgroup.

Lemma 1.62. *Suppose that p is odd, $K = GF(p)$, V is a vector space over K, $G \leq SL(V)$ is generated by transvections and G contains a strongly p-embedded subgroup H. Then $V = V_0 \oplus V_1$, $G \cong SL_2(p)$, V_1 is 2-dimensional, and $[V_0, G] = 1$.*

Proof. As G has a strongly p-embedded subgroup, Corollary 1.56 (3) implies that $O_p(G) = 1$. Then, as G is generated by transvections and $O_p(G) = 1$, Theorem 1.42 implies that $V = V_0 \oplus V_1 \oplus \cdots \oplus V_s$ and $G = G_1 \times G_2 \times \cdots \times G_s$, where $[V_0, G] = 1$. By assumption $p \mid |G|$, so we may assume that $p \mid |G_1|$. Let $S \in \mathrm{Syl}_p(G)$. If $p \mid |G_i|$ for some $1 < i \leq s$ then let $S_1 = S \cap G_1 \in \mathrm{Syl}_p(G_1)$ and $S_i = S \cap G_i \in \mathrm{Syl}_p(G_i)$. Then $G_2 \times \cdots \times G_s \leq C_G(S_1)$ and $G_1 \leq C_G(S_i)$, hence $G = N_G(S_1)N_G(S_2) \leq H$, contradicting Corollary 1.56 (1). Thus $p \nmid |G_i|$, and Theorem 1.42 (3) implies that $G_i = 1$ and $V_i = 1$, as $p \mid |SL_n(p)|$ and $p \mid |Sp_n(p)|$ for all $n \geq 2$. Thus $V = V_0 \oplus V_1$ and $G = G_1$. If $n \geq 3$ then the groups $SL_n(p)$ and $Sp_n(p)$ do not contain a strongly p-embedded subgroup. This can be seen as in these situations the Sylow p-subgroups have rank at least two, hence Theorem 1.58 implies that $O^{p'}(G/O_{p'}(G))$ is almost simple. In this situation, $O^{p'}(G/O_{p'}(G))$ is isomorphic to $PSL_n(p)$ or $PSp_n(p)$ respectively, both of which are known finite simple group not appearing in [GLS98, Theorem 7.6.1], hence they do not contain a strongly p-embedded subgroup. On the other hand the Sylow p-subgroups of $SL_2(p) = Sp_2(p)$ have order p and are not normal in G, hence $SL_2(p)$ contains a strongly p-embedded subgroup by Corollary 1.56 (4). We therefore conclude that $G \cong SL_2(p)$, and V_1 is 2-dimensional. $\square$

1.11 Subgroups of $GL_r(p)$ with a strongly p-embedded subgroup

We will be interested in knowing which subgroups of $GL_r(p)$ have a strongly p-embedded subgroup when $r \leq 4$.

Lemma 1.63. *Assume G is isomorphic to a subgroup of $X = GL_2(p)$ and $p \mid |G|$. Then either $O_p(G) \neq 1$ or $SL_2(p) = X' \leq G$. In particular, if $O_p(G) = 1$, then G has a strongly p-embedded subgroup.*

Proof. We may assume $O_p(G) = 1$. Then we can choose $S_1, S_2 \in \mathrm{Syl}_p(G)$ distinct. By [KS98, (8.6.7)] we have $\langle S_1, S_2 \rangle = SL_2(p) = X'$, so $X' \leq G$. As $|S_1| = p$ and it is not normal in G, Corollary 1.56 (4) implies that $N_G(S_1)$ is strongly p-embedded in G. □

Proposition 1.64. *Let V be a 3-dimensional vector space over the field $GF(p)$ and let $G \leq Aut(V) \cong GL_3(p)$. Suppose that G has a strongly p-embedded subgroup H. Then one of the following holds:*

1. *$O^{p'}(G) \cong SL_2(p)$ and $G \leq \mathrm{Aut}(U) \times \mathrm{Aut}(W) \cong GL_2(p) \times GL_1(p)$, for unique subspaces $U, W \subset V$;*
2. *p is odd, $O^{p'}(G) \cong PSL_2(p)$ and G acts irreducibly on V;*
3. *$p = 3$, $O^{p'}(G) \cong C_{13} : C_3$ and G acts irreducibly on V.*

In particular, $p \mid |G|$ but $p^2 \nmid |G|$. If G acts irreducibly on V then every p-element has Jordan form J_3, whereas if G acts reducibly then the Jordan form of every p-element is $J_2 \oplus J_1$.

Proof. When p is odd, all but the last claim are in [Gra18, Theorem 1.10]. For the last claim in all cases we have $O^{p'}(G) = \langle s, s^g \rangle$ for some $s \in G$ of order p and a conjugate element. Hence if s does not have Jordan form J_3 we have $|C_V(s)| \geq p^2$, thus $C_V(O^{p'}(G)) = C_V(s) \cap C_V(s^g)$ is nontrivial, and $O^{p'}(G)$ acts reducibly on V with $O^{p'}(G) \cong SL_2(p)$.

If $p = 2$ we consider the maximal subgroups of $GL_3(2) \cong PSL_2(7)$ (by Proposition 1.19 (11)) of order $2^3 \cdot 3 \cdot 7$, which are isomorphic to either S_4 or $C_7 : C_3$, the latter of which has odd order. We have $O_2(S_4) \cong C_2 \times C_2 \neq 1$, and its maximal subgroups M are A_4, D_8 and $S_3 \cong SL_2(2)$ (by Proposition 1.19 (8)), only the last of which has $O_2(M) = 1$. Finally, the only further subgroups are either 2-groups or have odd order, so by Corollary 1.56 (3) the result follows. Further, recall that an element of order 2 acting nontrivially has Jordan form $J_2 \oplus J_1$, as it satisfies $x^2 - 1 = (x-1)^2$ as its minimal polynomial. □

Proposition 1.65. *Suppose $G \leq GL_4(p)$ has a strongly p-embedded subgroup and G has p-rank at least 2. Then $O^{p'}(G)$ is isomorphic to either $SL_2(p^2)$ or $PSL_2(p^2)$.*

Proof. Under the assumptions above, Theorem 1.58 implies that $K := O^{p'}(G/O_{p'}(G))$ is almost simple, and we can use Theorem 1.59 to obtain a list of candidates for K. Let $T \in \mathrm{Syl}_p(K)$, we first rule out all candidates except $PSL_2(p^2)$, then show that $O_{p'}(G)$ centralises $O^{p'}(G)$, so that the result follows.

Claim 1.65.1. *$K \cong PSL_2(p^2)$.*

Proof of claim. Note that a Sylow p-subgroup S of $GL_4(p)$ has order p^6, nilpotency class 3, and K must be isomorphic to a section of $GL_4(p)$, in particular, $|K|$ must divide $|GL_4(p)| = p^6(p^4-1)(p^3-1)(p^2-1)(p-1)$. We obtain the candidates for K from Theorem 1.59 and the structure of T from Corollary 1.60.

If $K \cong PSU_3(p^n)$, with $p^n \geq 3$, then T has order p^{3n}, so we must have $n \leq 2$. If $n = 2$ then T has order p^6, so we need $S \cong T$, but T has nilpotency class 2, so it cannot happen. Finally, if $n = 1$, we have $p^6 - 1 \mid |PSU_3(p)|$ and Zsigmondy's Theorem (Theorem 1.2) implies that there exists a prime q such that $q \mid p^6 - 1$ but $q \nmid p^k - 1$ for $k < 6$ unless $p = 2$, but we have $p^n \geq 3$, so that case does not happen and we have $|K| \nmid |GL_4(p)|$.

If $K \cong Sz(2^{2n+1})$ then $|T| = (2^{2n+1})^2 \leq 2^6$, so we must have $n = 1$, but then $T \cong S$. However T has nilpotency class 2 while S has nilpotency class 3, so this case does not happen either.

If $K \cong {}^2G_2(3^{2n+1})$ then $|T| = (3^{2n+1})^3 > 3^6$, a contradiction.

If $K \cong A_{2p}$ with $p \geq 5$ then we must have $p \leq 17$, as otherwise we observe that $|A_{2p}| = (2p)!/2 \geq p^{17} > p^{16} \geq (p^4-1)(p^3-1)(p^2-1)(p-1)p^6 = |GL_4(p)|$, so it cannot embed. For the remaining primes $p = 5, 7, 11, 13$, we have, respectively, the primes $q = 7, 13, 17, 23$ such that $q \mid |A_{2p}|$ but $q \nmid |GL_4(p)|$, so this case does not happen. Note that if $p = 3$ then $A_6 \cong PSL_2(9)$ by Proposition 1.19 (12), which we consider later.

For the remaining cases other than $PSL_2(p^n)$ there is always a prime dividing $|K|$ that does not divide $|GL_4(p)|$. If $p = 3$, we have $7, 11 \nmid |GL_4(3)|$ but $7 \mid |PSL_3(4)|$, $7 \mid |PSL_2(8)|$ and $11 \mid |M_{11}|$. If $p = 5$, none of $11, 13, 41$ divide $|GL_4(5)|$ but 11 divides $|McL|$ and $|Fi_{22}|$, $13 \mid |{}^2F_4(2)'|$, and $41 \mid |\operatorname{Aut}(Sz(32))|$. And for $p = 11$, we have 43 does not divide the order of the sporadic Janko group J_4, but $43 \nmid |GL_4(11)|$.

Finally, if $K \cong PSL_2(p^n)$ then $|K| = \epsilon(p^{2n} - 1)p^n$ by [Gor80, Theorem 2.8.1] where $\epsilon = 1$ if $p = 2$ and $\epsilon = 1/2$ if p is odd. Then, if $n \geq 3$, we have again by Theorem 1.2 a prime q such that $q \mid p^{2n} - 1$ and $q \nmid p^k - 1$ for any $k < 2n$ unless $p = 2$ and $n = 3$. In this case, we are looking at $PSL_2(8)$ embedding into

$GL_4(2)$. But the Sylow 3-subgroups of $PSL_2(8)$ are cyclic of order 9 whereas those in $GL_4(2)$ are isomorphic to $C_3 \times C_3$, so this embedding does not happen either. The Sylow p-subgroups of $PSL_2(p)$ are cyclic, so we cannot have $n = 1$.

Therefore we must have $K \cong PSL_2(p^2) \cong \Omega_4^-(p)$ by Proposition 1.19 (5), which embeds into $GL_4(p)$. ■

Claim 1.65.2. *If p is odd then $O_{p'}(G) \leq Z(O^{p'}(G))$.*

Proof of claim. We have $K = O^{p'}(G/O_{p'}(G)) \cong PSL_2(p^2)$. Let $R := O_{p'}(G)$ and $T \in \mathrm{Syl}_p(G)$. Then $T \cong C_p \times C_p$ so pick $x \in T$ of order p, and consider $H := R\langle x \rangle \leq G$. H is p-solvable as $R \trianglelefteq H$ is a p'-group and $H/R \cong \langle x \rangle$ is a p-group. Consider the action of x on the natural $GL_4(p)$-module. The Jordan form of x has largest Jordan block of size at most 4, so that its minimal polynomial is $(X-1)^r$ for some $r \leq 4$.

Then, if $O_p(H) = 1$, we have by the Hall-Higman Theorem ([Gor80, Theorem 11.1.1]) that $p - 1 \leq r \leq p$. This means that if $p \geq 7$ or $p = 5$ and $r \leq 3$ then $O_p(H) \neq 1$. Thus $H = R \times \langle x \rangle$, and R centralises x. Since we can do this for any subgroup of any Sylow p-subgroup of G, we conclude that R acts trivially on $O^{p'}(G)$ and therefore $R \leq Z(O^{p'}(G))$ and $O^{p'}(G)$ is a central extension of $PSL_2(p^2)$. The Schur multiplier of $PSL_2(p^2)$ has order 2 if $p \geq 5$ and its universal covering group is $SL_2(p^2)$ by [Hup67, V.25.7 Satz], so in this case the result follows.

The remaining cases are $p = 3$, or $p = 5$ and $x \in T$ has Jordan form J_4.

As $O^{p'}(G) < O^{p'}(GL_4(p))$, there is some maximal subgroup M of $SL_4(p)$ such that $O^{p'}(G) \leq M$. Hence, if $p = 3$, we consider the maximal subgroups of $SL_4(3)$ from [BHRD13, Table 8.8]. The maximal subgroups $C_3^3 : GL_3(3)$, $C_3^4 : SL_2(3)^2 : C_2$ and $SO_4^+(3).C_2$ have order not divisible by 5, whereas the maximal subgroup

$SL_2(9).C_4.C_2$ satisfies $O^{3'}(M) \cong SL_2(9)$, and $SO_4^-(3).C_2 \cong (PSL_2(9) \times C_2).C_2$ has $O^{3'}(M) \cong PSL_2(9)$. The last maximal subgroup $Sp_4(3).C_2$ requires more attention via its own maximal subgroups, given in [BHRD13, Table 8.12]. Thus the maximal subgroups of $Sp_4(3).C_2$ are isomorphic to one of $3_+^{1+2} : (C_2 \times Sp_2(3))$, $C_3^3 : GL_2(3)$, $(Sp_2(3) \times Sp_2(3)) : C_2$, $2_-^{1+4}.A_5$, none of which have order divisible by $|A_6|$, or $Sp_2(9) : C_2$, in which case $O^{3'}(G) \cong Sp_2(9) \cong SL_2(9)$ by Proposition 1.19 (1). Thus if $p = 3$ then the claim holds, and both cases appear.

Note that a very similar argument also gives the result for $p = 5$.

Finally, if $p = 5$, and x has Jordan form J_4 then, $T \leq C = C_{GL_4(5)}(x)$, and C has shape $C_5^3 : C_4$ by [LS12, Theorem 7.1]. We claim there is no subgroup of the centraliser of order 5^2 with only elements with Jordan form J_4. This is because a Sylow 5-subgroup of C is generated by matrices

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \; x_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \; x_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

so that the subgroup generated by x_2 and x_3 contains no element with Jordan form J_4. Any subgroup of order p^2 in $C_{GL_4(5)}(x)$ must intersect this subgroup nontrivially, hence it must contain some nonidentity element y with Jordan form distinct from J_4. Then as before R must centralise y by Hall-Higman. Note that the subgroup $\langle y^G \rangle = O^{p'}(G)$, since $O^{p'}(G/O_{p'}(G))$ is almost simple, so that R centralises $O^{p'}(G)$ in this case as well. Thus in every case $O^{p'}(G)$ is a central extension of $PSL_2(p^2)$. ■

If $p = 2$, the following Magma code proves the claim. It enumerates those subgroups H of $GL_4(2)$ with $O_2(H) = 1$ and elementary abelian Sylow 2-subgroups.

It outputs groups in the SmallGroups notation.

```
> [IdentifyGroup(i`subgroup) : i in Subgroups(GL(4,2) :
> OrderMultipleOf := 4) | 1 eq #pCore(i`subgroup, 2) and
> IsElementaryAbelian(Sylow(i`subgroup,2))];
[ <36, 10>, <36, 10>, <60, 5>, <60, 5>, <180, 19> ]
```

Out of the outputted groups, the group $H = <36, 10>$ satisfies $H \cong S_3 \times S_3$ and does not contain a strongly p-embedded subgroup, as the only group containing the centralisers of all involutions is H itself, contradicting Lemma 1.55, whereas $<60, 5> \cong A_5 \cong PSL_2(4)$ and $<180, 19> \cong GL_2(4)$ have a strongly 2-embedded subgroup by [GLS98, Theorem 7.6.1].

The proposition now follows, and both cases arise for all primes. $\square$

CHAPTER 2

AN INTRODUCTION TO FUSION SYSTEMS

In this chapter we present some basic definitions about fusion systems and the results which we use to work with them. We use the notation and terminology from [AKO11], our main source. We begin by setting up the notation necessary for the definition, following the motivating example of a fusion category of a finite group G on a Sylow p-subgroup S. Recall that we write maps on the right.

Definition 2.1. *Given a finite group G and two subgroups P, Q, we define*

$$\mathrm{Hom}_G(P,Q) := \{\phi \in \mathrm{Hom}(P,Q) \mid \phi = c_g \textit{ for some } g \in G \textit{ such that } P^g \leq Q\},$$

where c_g is the conjugation map induced by g, that is $c_g : x \mapsto g^{-1}xg$. Further, if $P = Q$, we define the automiser *of P in G to be*

$$\mathrm{Aut}_G(P) := \mathrm{Hom}_G(P,P) \cong N_G(P)/C_G(P).$$

We also will denote $\mathrm{Out}_G(P) := \mathrm{Aut}_G(P)/\mathrm{Inn}(P)$.

Definition 2.2. *Suppose G is a finite group, p is a prime and S a Sylow p-subgroup* *of G. The* fusion category $\mathcal{F}_S(G)$ *of G on S is the category whose objects are all subgroups of S and, given $P, Q \leq S$, the morphisms between P and Q are given by* $\mathrm{Mor}_{\mathcal{F}_S(G)}(P, Q) = \mathrm{Hom}_G(P, Q)$.

Thus the maps in $\mathcal{F}_S(G)$ are conjugation maps by elements of G with specified domain and codomain. As such, they are injective maps, that is, isomorphisms followed by inclusions, and inclusion maps are in $\mathcal{F}_S(G)$ as conjugation by the identity element of G with appropriate domain and codomain.

A way to generalise this structure to a more abstract setting is to forget the group G, and consider maps between subgroups of the p-group S that act on subgroups of S with some of the properties above. This leads us to the following definition.

Definition 2.3. *A* fusion system $\mathcal{F}$ *on a (finite) p-group S is a category whose object set consists of the set of all subgroups of S and where, given two subgroups P, Q of S, the collection of morphisms between P and Q, denoted by* $\mathrm{Hom}_{\mathcal{F}}(P, Q)$*, satisfies:*

1. $\mathrm{Hom}_S(P, Q) \subseteq \mathrm{Hom}_{\mathcal{F}}(P, Q) \subseteq \mathrm{Inj}(P, Q)$;
2. *composition in the category is composition of maps; and*
3. *any map $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, Q)$ is the composite of an isomorphism in the category followed by an inclusion from the category.*

We write $\mathrm{Aut}_{\mathcal{F}}(Q) := \mathrm{Hom}_{\mathcal{F}}(Q, Q)$ for the *automiser* in $\mathcal{F}$ of Q, and its quotient $\mathrm{Out}_{\mathcal{F}}(Q) := \mathrm{Aut}_{\mathcal{F}}(Q)/\,\mathrm{Inn}(Q)$.

Note that $\mathcal{F}_S(G)$ is a fusion system, and by Definition 2.3 (1), $\mathcal{F}_S(S)$ is contained in every fusion system on S. In particular, $\mathrm{Aut}_S(P) \leq \mathrm{Aut}_{\mathcal{F}}(P) \leq \mathrm{Aut}(P)$ and

$\mathrm{Out}_S(P) \leq \mathrm{Out}_{\mathcal{F}}(P) \leq \mathrm{Out}(P)$.

We are interested in not only capturing the properties of conjugation maps, but also those extra properties satisfied S is a Sylow p-subgroup of G, so we restrict the definition by mimicking certain consequences of Sylow's Theorems for finite groups. We begin with some notation necessary for the definitions.

Definition 2.4. *Let $\mathcal{F}$ be a fusion system on a p-group S, and $P \leq S$.*

1. *A subgroup Q of S is $\mathcal{F}$-*conjugate *to P if they are isomorphic in $\mathcal{F}$. Let $P^{\mathcal{F}}$ denote the set of isomorphic images of P in $\mathcal{F}$.*

2. *P is* fully $\mathcal{F}$-normalised *if $|N_S(P)| \geq |N_S(Q)|$ for all $Q \in P^{\mathcal{F}}$.*

3. *P is* fully $\mathcal{F}$-centralised *if $|C_S(P)| \geq |C_S(Q)|$ for all $Q \in P^{\mathcal{F}}$.*

4. *P is* $\mathcal{F}$-centric *if $C_S(Q) = Z(Q)$ for all $Q \in P^{\mathcal{F}}$.*

5. *P is* fully $\mathcal{F}$-automised *if $\mathrm{Aut}_S(P) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(P))$.*

Definition 2.5. *Given an isomorphism $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, Q)$, define its* extension control subgroup *to be $N_\phi := \{g \in N_S(P) \mid \phi^{-1} c_g \phi \in \mathrm{Aut}_S(Q)\}$.*

We say that $Q \leq S$ is $\mathcal{F}$-receptive *if for every isomorphism $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, Q)$ there exists a map $\bar{\phi} \in \mathrm{Hom}_{\mathcal{F}}(N_\phi, S)$ such that $\bar{\phi}|_P = \phi$. We say ϕ* extends *or* lifts *to N_ϕ and that $\bar{\phi}$* extends *ϕ.*

We can now define saturation and an equivalent characterisation.

Definition 2.6. *A fusion system $\mathcal{F}$ on a finite p-group S is* saturated *if and only if for every subgroup P of S there is a subgroup $Q \in P^{\mathcal{F}}$ that is fully $\mathcal{F}$-automised and $\mathcal{F}$-receptive.*

Theorem 2.7 ([RS09, Theorem 5.2])**.** *A fusion system $\mathcal{F}$ on a p-group S is saturated if and only if:*

1. *Each subgroup $P \leq S$ which is fully $\mathcal{F}$-normalised is also fully $\mathcal{F}$-centralised and fully $\mathcal{F}$-automised;*

2. *Each subgroup $P \leq S$ which is fully $\mathcal{F}$-centralised is also $\mathcal{F}$-receptive.*

The conditions which define a saturated fusion system are motivated by similar properties that a fusion category of G on S has when $S \in \mathrm{Syl}_p(G)$. In particular, by [AKO11, Theorem 2.3 (Puig)], if $S \in \mathrm{Syl}_p(G)$ then $\mathcal{F}_S(G)$ is saturated.

The group N_ϕ controls when an isomorphism ϕ in $\mathcal{F}$ extends to a homomorphism between larger subgroups, so we consider some of its elementary properties.

Lemma 2.8. *Let $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, Q)$ be an isomorphism. Then*

$$PC_S(P) \leq N_\phi \leq N_S(P).$$

Proof. $N_\phi \leq N_S(P)$ by definition. If $g \in P$ and $x \in Q$ then

$$x\phi^{-1}c_g\phi = (g^{-1}(x\phi^{-1})g)\phi = (g^{-1}\phi)((x\phi^{-1})\phi)(g\phi) = xc_{g\phi}$$

so $\phi^{-1}c_g\phi = c_{g\phi} \in \mathrm{Aut}_S(Q)$. If $g \in C_S(P)$ then $\phi^{-1}c_g\phi = 1 \in \mathrm{Aut}_S(Q)$. □

Lemma 2.9. *Let $\mathcal{F}$ be a saturated fusion system on the p-group S. Suppose that $E \leq S$ is fully $\mathcal{F}$-normalised. Then every element of $N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$ lifts to an element of $\mathrm{Aut}_{\mathcal{F}}(N_S(E))$.*

Proof. Let $\theta \in N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$. As E is fully $\mathcal{F}$-normalised, by Theorem 2.7, E is $\mathcal{F}$-receptive so θ extends to N_θ. By Lemma 2.8, $N_\theta \leq N_S(E)$. Now if

$g \in N_S(E)$ then, as θ normalises $\mathrm{Aut}_S(E)$, we have $\theta^{-1}c_g\theta \in \mathrm{Aut}_S(E)$, so $g \in N_\theta$ and $N_\theta = N_S(E)$. Thus θ lifts to a map $\bar{\theta} \in \mathrm{Aut}_{\mathcal{F}}(N_S(E))$. □

We call a saturated fusion system $\mathcal{F}$ *realisable* if $\mathcal{F} = \mathcal{F}_S(G)$ for some finite group G with a Sylow p-subgroup S. Even with the properties that we require, there are saturated fusion systems on p-groups S which cannot be realised in this way. We will call such fusion systems *exotic*.

We now consider morphisms between fusion systems.

Definition 2.10. *Let $\mathcal{F}$, $\widetilde{\mathcal{F}}$ be two fusion systems on p-groups S, $\widetilde{S}$ respectively. A* morphism $\alpha : \mathcal{F} \to \widetilde{\mathcal{F}}$ *is a collection $(\alpha, \alpha_{P,Q} : P, Q \in \mathcal{F})$ such that $\alpha : S \to \widetilde{S}$ is a group homomorphism and $\alpha_{P,Q} : \mathrm{Hom}_{\mathcal{F}}(P,Q) \to \mathrm{Hom}_{\widetilde{\mathcal{F}}}(P\alpha, Q\alpha)$ is a function such that for all $\phi \in \mathrm{Hom}_{\mathcal{F}}(P,Q)$ we have $\phi\alpha = \alpha(\phi\alpha_{P,Q})$.*

The morphism α is an isomorphism *if $\alpha : S \to \widetilde{S}$ is an isomorphism and every $\alpha_{P,Q} : \mathrm{Hom}_{\mathcal{F}}(P,Q) \to \mathrm{Hom}_{\widetilde{\mathcal{F}}}(P\alpha, Q\alpha)$ is bijective. We write $\mathcal{F} \cong \widetilde{\mathcal{F}}$.*

In particular, for $\alpha \in \mathrm{Aut}(S)$, the fusion system $\mathcal{F}^\alpha$ on S is defined by

$$\mathrm{Hom}_{\mathcal{F}^\alpha}(P,Q) = \{\alpha^{-1}\phi\alpha \mid \phi \in \mathrm{Hom}_{\mathcal{F}}(P\alpha^{-1}, Q\alpha^{-1})\} = \mathrm{Hom}_{\mathcal{F}}(P\alpha^{-1}, Q\alpha^{-1})^\alpha$$

and is isomorphic to $\mathcal{F}$.

If the collection $(\alpha, \alpha_{P,Q})$ is a morphism, then the maps $\alpha_{P,Q}$ are uniquely determined by α and the given property, so we sometimes refer to α as the isomorphism. In particular, we can identify the group $\mathrm{Aut}(\mathcal{F})$ of automorphisms of $\mathcal{F}$ with a subgroup of $\mathrm{Aut}(S)$.

If an isomorphism α as above is between fusion systems of finite groups $\mathcal{F}_S(G)$ and $\mathcal{F}_{\widetilde{S}}(\widetilde{G})$ then we say it is *fusion preserving*. There is a notion of two fusion systems being *isotypically equivalent* if there is an equivalence of categories that has a natural isomorphism of functors. It is shown in [BMO12, Proposition 1.3] that two fusion systems $\mathcal{F}_S(G)$ and $\mathcal{F}_{\widetilde{S}}(\widetilde{G})$ are isotypically equivalent if and only if there is a fusion preserving isomorphism between S and $\widetilde{S}$. We now present some results of isomorphisms between fusion systems of finite groups.

Lemma 2.11. *Let G be a finite group, $S \in \mathrm{Syl}_p(G)$. Let $N \trianglelefteq G$ with $p \nmid |N|$, $\bar{G} = G/N$, $\bar{S} \in \mathrm{Syl}_p(\bar{G})$. Then $\mathcal{F}_S(G) \cong \mathcal{F}_{\bar{S}}(\bar{G})$.*

Proof. Since $p \nmid |N|$ we have $S \cong \bar{S}$, with isomorphism $\alpha : S \to \bar{S}$ such that for any $s \in S$, $s\alpha = sN$. Now define $\alpha_{P,Q} : \mathrm{Hom}_{\mathcal{F}_S(G)}(P,Q) \to \mathrm{Hom}_{\mathcal{F}_{\bar{S}}(\bar{G})}(P\alpha, Q\alpha)$ for $P, Q \leq S$ by $c_g\alpha_{P,Q} = c_{gN}$. Then

$$sc_g\alpha = s^g\alpha = s^gN = sN^{gN} = sNc_{gN} = (s\alpha)(c_g\alpha_{P,Q}),$$

so $c_g\alpha = \alpha(c_g\alpha_{P,Q})$ and α is an morphism of fusion systems. Finally, given $\phi_1, \phi_2 \in \mathrm{Hom}_{\mathcal{F}_S(G)}(P,Q)$, there are $g, h \in G$ with $P^g = P^h = Q$, such tht $\phi_1 = c_g$, and $\phi_2 = c_h$. Hence, since $\alpha : P \to P\alpha$ is an isomorphism, $c_{g\alpha} = c_{h\alpha}$ on $P\alpha$ if and only if $c_g = c_h$ on P. Thus $\alpha_{P,Q}$ is bijective for all $P, Q \leq S$, and $(\alpha, \alpha_{P,Q})$ is an isomorphism of fusion systems. $\square$

Lemma 2.12. *Suppose G_1 and G_2 and $\alpha : G_1 \to G_2$ is an isomorphism and let $S \in \mathrm{Syl}_p(G_1)$. Then $S\alpha \in \mathrm{Syl}_p(G_2)$, and $\mathcal{F}_S(G_1) \cong \mathcal{F}_{S\alpha}(G_2)$.*

Proof. As α is an isomorphism, $\ker(\alpha) = 1$, so $\alpha|_S : S \to S\alpha$ is an isomorphism. Let $P, Q \leq S$, $c_g \in \mathrm{Hom}_{\mathcal{F}_S(G_1)}(P,Q)$, and define $\alpha_{P,Q}$ by $c_g\alpha_{P,Q} := c_{g\alpha}$. Since $\alpha^{-1}c_g\alpha = c_{g\alpha}$, we have $c_g\alpha = \alpha(c_g\alpha_{P,Q})$, so $(\alpha, \alpha_{P,Q})$ is a morphism of fusion systems $\mathcal{F}_S(G_1) \to \mathcal{F}_{S\alpha}(G_2)$. Finally, as α is an isomorphism, given $g, h \in G$ such that $P^g = P^h = Q$, we have $c_g, c_h \in \mathrm{Hom}_{\mathcal{F}_S(G)}$, and $c_g = c_h$ on P if and only if $c_{g\alpha} = c_{h\alpha}$ on $P\alpha$, and each $\alpha_{P,Q}$ is bijective for all $P, Q \leq S$. Hence $(\alpha, \alpha_{P,Q})$ is an isomorphism of fusion systems. $\square$

2.1 Alperin's fusion theorem

Alperin's fusion theorem will allow us to generate saturated fusion systems in terms of automorphisms of some collection of subgroups. We begin by defining the elements of such a collection.

Definition 2.13. *Given a fusion system $\mathcal{F}$ on a p-group S, a proper subgroup $E < S$ is* $\mathcal{F}$-essential *if:*

1. *E is $\mathcal{F}$-centric;*
2. *E is fully $\mathcal{F}$-normalised;*
3. *$\mathrm{Out}_{\mathcal{F}}(E) = \mathrm{Aut}_{\mathcal{F}}(E)/\mathrm{Inn}(E)$ has a strongly p-embedded subgroup.*

We will denote by $\mathbf{E}_{\mathcal{F}}$ the set of $\mathcal{F}$-essential subgroups.

The key property of $\mathcal{F}$-essential subgroups is (3), which implies that there are some isomorphisms that do not extend to any overgroups.

Proposition 2.14 ([AKO11, Proposition I.3.3])**.** *Let $\mathcal{F}$ be a saturated fusion system on a p-group S. Let $P < S$ be fully $\mathcal{F}$-normalised, and let $H_P \leq \mathrm{Aut}_{\mathcal{F}}(P)$ be the subgroup generated by those $\alpha \in \mathrm{Aut}_{\mathcal{F}}(P)$ which extend to $\mathcal{F}$-isomorphisms between strictly larger subgroups of S. Then either P is not $\mathcal{F}$-essential and $H_P = \mathrm{Aut}_{\mathcal{F}}(P)$ or P is $\mathcal{F}$-essential and $H_P/\mathrm{Inn}(P)$ is strongly p-embedded in $\mathrm{Out}_{\mathcal{F}}(P)$.*

Before stating Alperin's Theorem, we make precise what generating means in a fusion system.

Definition 2.15 ([AKO11, Definition I.3.4]). *For any set X of monomorphisms between subgroups of S and/or fusion systems on subgroups of S, the* fusion system generated by X, *denoted $\langle X\rangle_S$ (or $\langle X\rangle$ if the group S is clear), is the smallest fusion system on S which contains X. Equivalently $\langle X\rangle_S$ is the intersection of all fusion systems on S which contain X. The morphisms in $\langle X\rangle_S$ are the composites of restrictions of homomorphisms in X or in $\mathrm{Aut}_S(S)$ and their inverses.*

We note that this notion is slightly different to generation of a group. For example, in a group of Lie type the $\mathcal{F}$-essential subgroups are the p-cores of the minimal parabolics, and the maximal parabolics generate the whole group. However, if we consider the p-cores of the maximal parabolics, not every map of $\mathcal{F}_S(G)$ is in the fusion system generated by their normalisers, as there are maps among larger subgroups which would be extensions of these generators, whereas we only allow for restrictions of the maps given.

Theorem 2.16 (Alperin-Goldschmidt Fusion Theorem [AKO11, Theorem I.3.5]). *Suppose $\mathcal{F}$ is a saturated fusion system on a p-group S. Then*

$$\mathcal{F} = \langle \mathrm{Aut}_{\mathcal{F}}(S), \mathrm{Aut}_{\mathcal{F}}(E) \mid E \textit{ is } \mathcal{F}\textit{-essential}\rangle_S.$$

We now use Frattini's argument to slightly refine Alperin's fusion theorem, noting that an analogous result holds with $O^p(\mathrm{Aut}_{\mathcal{F}}(E))$.

Lemma 2.17 ([BCG+07, Lemma 3.4]). *If $\mathcal{F}$ is saturated then*

$$\mathcal{F} = \langle O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)), \mathrm{Aut}_{\mathcal{F}}(S) \mid E \in \mathbf{E}_{\mathcal{F}}\rangle.$$

Proof. By Alperin's Theorem $\mathcal{F} = \langle \mathrm{Aut}_{\mathcal{F}}(E), \mathrm{Aut}_{\mathcal{F}}(S) \mid E \in \mathbf{E}_{\mathcal{F}} \rangle$, by Frattini's argument for each $E \in \mathbf{E}_{\mathcal{F}}$ we have $\mathrm{Aut}_{\mathcal{F}}(E) = O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$, and by Lemma 2.9 any element $\phi \in N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$ extends to an isomorphism $\overline{\phi} \in \mathrm{Aut}_{\mathcal{F}}(N_S(E))$, which again by Alperin's Theorem is a composition of maps $\overline{\phi} = \phi_1\phi_2 \ldots \phi_k$ where $\phi_i \in \mathrm{Aut}_{\mathcal{F}}(E_i)$ for some $E_i \in \mathbf{E}_{\mathcal{F}} \cup \{S\}$ satisfying $E_i \geq N_S(E)$. We can thus apply the same argument to each E_i until E_i is maximal among the $\mathcal{F}$-essential subgroups, at which point every lift of a map $\widetilde{\phi_i}$ is a composition of $\psi_i \in \mathrm{Aut}_{\mathcal{F}}(S)$, and thus every homomorphism can be obtained as a composition of restrictions of maps which are in either $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$ for some $E \in \mathbf{E}_{\mathcal{F}}$ or in $\mathrm{Aut}_{\mathcal{F}}(S)$, which concludes the lemma. □

The following are some straightforward properties of $\mathcal{F}$-essential subgroups.

Lemma 2.18. *Let $\mathcal{F}$ be a fusion system on S.*

1. *If $H \leq S$ is $\mathcal{F}$-centric then $Z(S) \leq H$.*
2. *If $H \leq S$ is $\mathcal{F}$-centric and abelian then it is maximal abelian in S.*
3. *(Burnside) If S is abelian then $\mathcal{F} = \langle \mathrm{Aut}_{\mathcal{F}}(S) \rangle$.*

Proof. Suppose H is $\mathcal{F}$-centric. Then $C_S(H) = Z(H)$, hence $Z(S) \leq C_S(H) \leq H$. If H is also abelian then we have $C_S(H) = Z(H) = H$, which is equivalent to H being maximal abelian in S. Finally, if S is abelian then every proper subgroup is abelian and not maximal abelian, so there are no $\mathcal{F}$-essential subgroups and $\mathcal{F} = \langle \mathrm{Aut}_{\mathcal{F}}(S) \rangle$. □

Lemma 2.19. *If $E < S$ is $\mathcal{F}$-essential then E is not cyclic.*

Proof. Suppose $E \cong C_{p^n}$. Then $\mathrm{Aut}(E)$ is abelian by [Gor80, Lemma 1.3.10 (i)], with $\mathrm{Inn}(E) = 1$ as E is abelian. If E is $\mathcal{F}$-essential then it is $\mathcal{F}$-centric, in particular $C_S(E) = E$, and as $E < S$ is a p-group, we have $N_S(E) > E$. Thus $\mathrm{Aut}_{\mathcal{F}}(E)$ and $\mathrm{Out}_{\mathcal{F}}(E)$ are abelian and have a nontrivial p-part. In particular, $O_p(\mathrm{Out}_{\mathcal{F}}(E)) \neq 1$ and $\mathrm{Out}_{\mathcal{F}}(E)$ does not have a strongly p-embedded subgroup by Corollary 1.56 (3), contradicting our assumption. Thus, no cyclic group E can be $\mathcal{F}$-essential. □

As an application of coprime action, we have the following result.

Lemma 2.20. *If $E \leq S$ with $O_p(\mathrm{Out}_{\mathcal{F}}(E)) = 1$ then $C_{\mathrm{Aut}_{\mathcal{F}}(E)}(E/\Phi(E)) = \mathrm{Inn}(E)$. In particular, if E is $\mathcal{F}$-essential then $\mathrm{Out}_{\mathcal{F}}(E)$ acts faithfully on $E/\Phi(E)$ and embeds into $GL_r(p)$ where $|E/\Phi(E)| = p^r$.*

Proof. As $\Phi(E)$ is characteristic in E, any map in $\mathrm{Aut}_{\mathcal{F}}(E)$ normalises it, so acts on $E/\Phi(E)$. Consider the map $\psi : \mathrm{Aut}_{\mathcal{F}}(E) \to \mathrm{Aut}_{\mathcal{F}}(E/\Phi(E))$ given by projection. Then $\ker \psi = C_{\mathrm{Aut}_{\mathcal{F}}(E)}(E/\Phi(E)) \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(E)$, and by Theorem 1.36 $C_{\mathrm{Aut}_{\mathcal{F}}(E)}(E/\Phi(E))$ is a p-group. Now $\mathrm{Inn}(E) \leq C_{\mathrm{Aut}_{\mathcal{F}}(E)}(E/\Phi(E))$ as $E/\Phi(E)$ is elementary abelian. Since $O_p(\mathrm{Out}_{\mathcal{F}}(E)) = 1$, we have $O_p(\mathrm{Aut}_{\mathcal{F}}(E)) = \mathrm{Inn}(E)$, thus $\mathrm{Inn}(E) = C_{\mathrm{Aut}_{\mathcal{F}}(E)}(E/\Phi(E))$, and $\mathrm{Out}_{\mathcal{F}}(E) = \mathrm{Aut}_{\mathcal{F}}(E)/\mathrm{Inn}(E)$ acts faithfully on $E/\Phi(E)$. Hence $\mathrm{Out}_{\mathcal{F}}(E)$ embeds into $\mathrm{Aut}(E/\Phi(E)) \cong GL_r(p)$. Finally, if E is $\mathcal{F}$-essential then $\mathrm{Out}_{\mathcal{F}}(E)$ has a strongly p-embedded subgroup, hence Corollary 1.56 (3) implies that $O_p(\mathrm{Out}_{\mathcal{F}}(E)) = 1$ and we can apply the preceding argument to obtain the same conclusion. □

When determining which subgroups can be $\mathcal{F}$-essential, the action of their overgroups will be important. For example, the following result will be used when F is extraspecial.

Lemma 2.21. *Suppose that E is $\mathcal{F}$-essential, $E \le F \le S$, $[E,F] \le Z(F)$ and $[E,F]$ is normalised by* $\mathrm{Aut}_{\mathcal{F}}(E)$*. Then $E = F$.*

Proof. As $[E,F] \le Z(F) \le C_S(E) \le E$, we have $[E,F] \trianglelefteq E$. Consider the chain $1 \trianglelefteq [E,F] \trianglelefteq E$ of subgroups normal in E, with $[E,F]$ normalised by $\mathrm{Aut}_{\mathcal{F}}(E)$. Then $F/Z(E)$ normalises the chain and acts on the quotients as the identity, so by Lemma 1.37 we have $F/Z(E) \le O_p(\mathrm{Aut}_{\mathcal{F}}(E)) = \mathrm{Inn}(E) = E/Z(E)$. Since $E \le F$, we have $E = F$. □

The smallest $\mathcal{F}$-essential subgroups, which we will encounter, have been defined as $\mathcal{F}$-pearls in [Gra18]. In Chapter 3 we consider $\mathcal{F}$-essential subgroups of order at most p^4.

Definition 2.22. *An $\mathcal{F}$-essential subgroup of S which is either elementary abelian of order p^2 or nonabelian of order p^3 is called an* $\mathcal{F}$-pearl.

2.2 Local theory of fusion systems

Many concepts about finite groups can be generalised to the theory of saturated fusion systems. We begin with normal p-subgroups. Throughout this section, $\mathcal{F}$ will always be a fusion system on a finite p-group S.

Definition 2.23.

1. *A subgroup $T \le S$ is* strongly closed *in $\mathcal{F}$ if no element of T is $\mathcal{F}$-conjugate to an element of $S \setminus T$.*
2. *A subgroup $T \le S$ is* normal *in $\mathcal{F}$ if $T \trianglelefteq S$ and for all $P, R \le S$ and all $\phi \in \mathrm{Hom}_{\mathcal{F}}(P,R)$, ϕ extends to a morphism $\bar{\phi} \in \mathrm{Hom}_{\mathcal{F}}(PT, RT)$ such that $T\bar{\phi} = T$. We denote T being normal in $\mathcal{F}$ by $T \trianglelefteq \mathcal{F}$.*

Lemma 2.24. *There is a unique maximal normal p-subgroup of a saturated fusion system $\mathcal{F}$, which we denote by $O_p(\mathcal{F})$.*

Proof. Suppose $N, M \trianglelefteq \mathcal{F}$. Then as $N, M \trianglelefteq S$ we have $NM \trianglelefteq S$. Further, any $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, R)$ extends to a morphism $\overline{\phi} \in \mathrm{Hom}_{\mathcal{F}}(PN, RN)$ such that $N\overline{\phi}|_N = N$, which then extends to a morphism $\widetilde{\phi} \in \mathrm{Hom}_{\mathcal{F}}(PNM, RNM)$ such that $NM\widetilde{\phi}|_{NM} = NM$. Hence $NM \trianglelefteq \mathcal{F}$. The product of all normal subgroups is the unique maximal normal p-subgroup of $\mathcal{F}$. $\square$

The main assumption throughout our reduction theorem (Theorem 4.27) will be that $O_p(\mathcal{F}) = 1$, that is, there is no nontrivial subgroup H of S with H normal in $\mathcal{F}$. We will often use the following characterisation of normal subgroups of a fusion system.

Proposition 2.25 ([AKO11, Proposition I.4.5]). *Let $\mathcal{F}$ be a saturated fusion system on a p-group S. Then, for any $H \leq S$, the following conditions are equivalent:*

- *H is normal in $\mathcal{F}$.*
- *H is strongly closed in $\mathcal{F}$, and $H \leq P$ for each P that is $\mathcal{F}$-centric with $O_p(\mathrm{Out}_{\mathcal{F}}(P)) = 1$.*
- *If $P \leq S$ is $\mathcal{F}$-essential or $P = S$, then $P \geq H$ and H is $\mathrm{Aut}_{\mathcal{F}}(P)$-invariant.*

We now introduce subsystems, and the normaliser fusion system of a p-subgroup of S, which we will use as a way to construct realisable fusion subsystems via the Model Theorem, allowing us to uniquely determine parts of the fusion systems we construct by realising them as fusion categories of finite groups. A *fusion subsystem* of $\mathcal{F}$ is a subcategory $\mathcal{E} \subseteq \mathcal{F}$ which is itself a fusion system on a subgroup $T \leq S$.

Definition 2.26 ([Cra11, Definition 4.26]). *The* normaliser *of Q in $\mathcal{F}$ is a category $N_{\mathcal{F}}(Q)$ which has as objects all subgroups of $N_S(Q)$ and has morphisms* $\mathrm{Hom}_{N_{\mathcal{F}}(Q)}(R, S)$ *given by all $\phi \in \mathrm{Hom}_{\mathcal{F}}(R, S)$ such that ϕ extends to a map $\overline{\phi} \in \mathrm{Hom}_{\mathcal{F}}(QR, QS)$ with $\overline{\phi}|_Q \in \mathrm{Aut}_{\mathcal{F}}(Q)$.*

Note that by definition the normaliser $N_{\mathcal{F}}(Q)$ is the largest subsystem of $\mathcal{F}$ in which Q is normal. We now consider when $N_{\mathcal{F}}(Q)$ is saturated.

Theorem 2.27 ([Cra11, Theorem 4.28]). *Let $\mathcal{F}$ be a fusion system on S, and $Q \leq S$. Then $N_{\mathcal{F}}(Q)$ is a fusion system on $N_S(Q)$, and if $\mathcal{F}$ is saturated and Q is fully $\mathcal{F}$-normalised then $N_{\mathcal{F}}(Q)$ is saturated.*

Definition 2.28. *Let $\mathcal{F}$ be a saturated fusion system on a p-group S. Then*

- *$\mathcal{F}$ is* constrained *if there exists $Q \trianglelefteq \mathcal{F}$ which is $\mathcal{F}$-centric.*
- *If $\mathcal{F}$ is constrained, a* model *for $\mathcal{F}$ is a finite group G such that $S \in \mathrm{Syl}_p(G)$, $\mathcal{F}_S(G) = \mathcal{F}$, and $C_G(O_p(G)) \leq O_p(G)$.*

We can now state the Model Theorem, the proof of which involves cohomological methods.

Theorem 2.29 (Model Theorem [AKO11, Theorem III.5.10]). *Let $\mathcal{F}$ be a constrained fusion system on S. Fix $Q \trianglelefteq \mathcal{F}$ that is $\mathcal{F}$-centric. Then the following hold:*

1. *There are models for $\mathcal{F}$.*
2. *For any finite group G with $S \in \mathrm{Syl}_p(G)$ such that $Q \trianglelefteq G$, $C_G(Q) \leq Q$ and $\mathrm{Aut}_G(Q) = \mathrm{Aut}_{\mathcal{F}}(Q)$, there is $\beta \in \mathrm{Aut}(S)$ such that $\beta|_Q = 1$ and $\mathcal{F}_S(G) = \mathcal{F}^{\beta}$. Thus there is a model for $\mathcal{F}$ which is isomorphic to G.*

3. *The model G is unique in the following strong sense: if G_1 and G_2 are two models for $\mathcal{F}$ then there is an isomorphism $\phi : G_1 \to G_2$ such that $\phi|_S = 1$. If ϕ and ϕ' are two such isomorphisms then $\phi' = \phi c_z$ for some $z \in Z(S)$.*

We now introduce normal subsystems as well as simplicity of a fusion system.

Definition 2.30. 1. *A fusion subsystem $\mathcal{E} \subseteq \mathcal{F}$ on $T \trianglelefteq S$ is* normal*, denoted by $\mathcal{E} \trianglelefteq \mathcal{F}$, if*

- *both $\mathcal{E}$ and $\mathcal{F}$ are saturated,*
- *T is strongly closed in $\mathcal{F}$,*
- *$\mathcal{E}^\alpha = \mathcal{E}$ for each $\alpha \in \mathrm{Aut}_{\mathcal{F}}(T)$ (invariance condition), that is, for each $P \leq Q \leq T$, $\phi \in \mathrm{Hom}_{\mathcal{E}}(P, Q)$, we have $\alpha^{-1}\phi\alpha \in \mathrm{Hom}_{\mathcal{E}}(P\alpha, T)$,*
- *for each $P \leq T$ and each $\phi \in \mathrm{Hom}_{\mathcal{F}}(P, T)$, there are $\alpha \in \mathrm{Aut}_{\mathcal{F}}(T)$ and $\phi_0 \in \mathrm{Hom}_{\mathcal{E}}(P, T)$ such that $\phi = \phi_0\alpha$ (Frattini condition), and*
- *each $\alpha \in \mathrm{Aut}_{\mathcal{E}}(T)$ extends to some $\bar{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(TC_S(T))$ such that $[C_S(T), \bar{\alpha}] \leq Z(T)$ (extension condition).*

2. *A fusion system is* simple *if it contains no proper nontrivial normal fusion subsystems.*

When classifying fusion systems in search for exotic ones, it is more suitable to consider the larger class of reduced fusion system which was introduced by Andersen, Oliver and Ventura in [AOV12]. In order to define them, we need to introduce some types of subsystems of $\mathcal{F}$.

Definition 2.31. 1. *The* focal subgroup $\mathfrak{foc}(\mathcal{F}) \leq S$ *and* hyperfocal subgroup

$\mathfrak{hyp}(\mathcal{F}) \leq S$ *of* $\mathcal{F}$ *are defined by*

$$\mathfrak{foc}(\mathcal{F}) := \langle g^{-1}(g\alpha) \mid g \in P \leq S, \alpha \in \mathrm{Aut}_{\mathcal{F}}(P) \rangle \leq S,$$
$$\mathfrak{hyp}(\mathcal{F}) := \langle g^{-1}(g\alpha) \mid g \in P \leq S, \alpha \in O^p(\mathrm{Aut}_{\mathcal{F}}(P)) \rangle \leq S.$$

2. *A fusion subsystem* $\mathcal{E} \subseteq \mathcal{F}$ *on* $T \leq S$ *has* p-power index *in* $\mathcal{F}$ *if* $T \geq \mathfrak{hyp}(\mathcal{F})$, *and* $\mathrm{Aut}_{\mathcal{E}}(P) \geq O^p(\mathrm{Aut}_{\mathcal{F}}(P))$ *for each* $P \leq S$.

3. *A fusion subsystem* $\mathcal{E} \subseteq \mathcal{F}$ *on* $T \leq S$ *has* index prime to p *in* $\mathcal{F}$ *if* $T = S$ *and* $\mathrm{Aut}_{\mathcal{E}}(P) \geq O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P))$ *for each* $P \leq S$.

Among the subsystems of p-power index or index prime to p there are unique smallest subsystems.

Theorem 2.32 ([AKO11, Theorems I.7.4 and I.7.7])**.** *There is a unique minimal saturated fusion subsystem of p-power index on $\mathfrak{hyp}(\mathcal{F})$, which we denote by $O^p(\mathcal{F})$. There is a unique minimal saturated fusion subsystem of index prime to p on S, which we denote by $O^{p'}(\mathcal{F})$.*

We now describe how to determine each of them. We consider $O^p(\mathcal{F})$ first, which can be determined via the following result.

Proposition 2.33 ([AKO11, Lemma I.7.2 and Corollary I.7.5])**.** *For any saturated fusion system $\mathcal{F}$ on a p-group S, we have $\mathfrak{foc}(\mathcal{F}) = \mathfrak{hyp}(\mathcal{F}) \cdot S'$. Further, we have*

$$O^p(\mathcal{F}) = \mathcal{F} \iff \mathfrak{hyp}(\mathcal{F}) = S \iff \mathfrak{foc}(\mathcal{F}) = S.$$

The determination of $O^{p'}(\mathcal{F})$ is a bit more complicated, and requires some notation. Recall that, by Lemma 2.17, if $\mathcal{F}$ is saturated, we have

$$\mathcal{F} = \langle O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)), \mathrm{Aut}_{\mathcal{F}}(S) \mid E \in \mathbf{E}_{\mathcal{F}} \rangle.$$

Definition 2.34. *Suppose $\mathcal{F}$ is saturated. We define the following.*

1. *If $E \in \mathbf{E}_{\mathcal{F}}$ then* $\mathrm{Aut}^E_{\mathcal{F}}(S) := \langle \alpha \in \mathrm{Aut}_{\mathcal{F}}(S) \mid \alpha|_E \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \rangle$.

2. $\mathrm{Aut}^0_{\mathcal{F}}(S) := \langle \mathrm{Aut}^E_{\mathcal{F}}(S),\ \mathrm{Inn}(S) \mid E \in \mathbf{E}_{\mathcal{F}} \rangle$.

3. $\mathcal{F}_0 := \langle O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)), \mathrm{Aut}^0_{\mathcal{F}}(S) \rangle \subseteq \mathcal{F}$.

4. $\Gamma_{p'}(\mathcal{F}) := \mathrm{Aut}_{\mathcal{F}}(S)/\,\mathrm{Aut}^0_{\mathcal{F}}(S)$.

Thus $\mathrm{Aut}^E_{\mathcal{F}}(S) \leq \mathrm{Aut}^0_{\mathcal{F}}(S)$ is the subgroup of automorphisms that are contributed to $\mathrm{Aut}_{\mathcal{F}}(S)$ by $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$. Note that by definition and Alperin's Theorem, $\mathcal{F}_0$ is the smallest fusion system on S which contains $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P))$ for each $P \leq S$, and $\mathcal{F}_0 \subseteq O^{p'}(\mathcal{F})$. We have $\mathcal{F} = \langle \mathcal{F}_0, \mathrm{Aut}_{\mathcal{F}}(S) \rangle$, so we will often construct this fusion system $\mathcal{F}_0$, show it is saturated by finding a group realising it, determine the largest possible candidate for $\mathrm{Aut}_{\mathcal{F}}(S)$, and then use the following result to obtain all subsystems of p'-index as intermediate fusion systems.

Theorem 2.35 ([Asc11, Theorem 8])**.**

1. *The map $\mathcal{E} \mapsto \mathrm{Aut}_{\mathcal{E}}(S)/\,\mathrm{Aut}^0_{\mathcal{F}}(S)$ is a bijection between the set of normal subsystems of $\mathcal{F}$ on S and the set of normal subgroups of $\Gamma_{p'}(\mathcal{F})$.*

2. *$\mathcal{F} = O^{p'}(\mathcal{F})$ if and only if $\mathrm{Aut}_{\mathcal{F}}(S) = \mathrm{Aut}^0_{\mathcal{F}}(S)$.*

3. *$\mathcal{F}$ is simple if and only if the following hold:*

(a) For each normal subsystem $\mathcal{D}$ of $\mathcal{F}$ on a subgroup D of S, we have $D = S$ or $D = 1$.

(b) $\operatorname{Aut}_{\mathcal{F}}(S) = \operatorname{Aut}^0_{\mathcal{F}}(S)$.

We now define a reduced fusion system.

Definition 2.36. *A saturated fusion system is* reduced *if $O_p(\mathcal{F}) = 1$, $O^p(\mathcal{F}) = \mathcal{F}$ and $O^{p'}(\mathcal{F}) = \mathcal{F}$. In other words a saturated fusion system is reduced if has no nontrivial normal p-subgroups, no proper subsystem of p-power index, and no proper subsystem of index prime to p.*

We now use a special case of the surjectivity property (see [Cra11, §6.1] for details), which is another equivalent formulation of saturation. This result will allow us to determine $\operatorname{Aut}^E_{\mathcal{F}}(S)$ from $O^{p'}(\operatorname{Aut}_{\mathcal{F}}(E))$ and vice versa.

Lemma 2.37. *If $\mathcal{F}$ is a saturated fusion system on S and $E \trianglelefteq S$ is $\mathcal{F}$-centric and normalised by $\operatorname{Aut}_{\mathcal{F}}(S)$, then there are isomorphisms*

$$\operatorname{Aut}_{\mathcal{F}}(S)/C_{\operatorname{Inn}(S)}(E) \cong N_{\operatorname{Aut}_{\mathcal{F}}(E)}(\operatorname{Aut}_S(E)),$$
$$\operatorname{Out}_{\mathcal{F}}(S) \cong N_{\operatorname{Aut}_{\mathcal{F}}(E)}(\operatorname{Aut}_S(E))/\operatorname{Aut}_S(E), \text{ and}$$
$$\operatorname{Out}^E_{\mathcal{F}}(S) \cong N_{O^{p'}(\operatorname{Aut}_{\mathcal{F}}(E))}(\operatorname{Aut}_S(E))/\operatorname{Aut}_S(E).$$

Proof. Since E is normalised by $\operatorname{Aut}_{\mathcal{F}}(S)$, there is a map given by restriction $\theta : \operatorname{Aut}_{\mathcal{F}}(S) \to N_{\operatorname{Aut}_{\mathcal{F}}(E)}(\operatorname{Aut}_S(E))$. As $E \trianglelefteq S$, by Lemma 2.9 every map in $N_{\operatorname{Aut}_{\mathcal{F}}(E)}(\operatorname{Aut}_S(E))$ is a restriction of an element of $\operatorname{Aut}_{\mathcal{F}}(S)$, hence θ is surjective.

Now let $\alpha \in \ker(\theta)$. Then $\alpha \in \operatorname{Aut}_{\mathcal{F}}(S)$ with $\alpha|_E = 1 \in \operatorname{Aut}(E)$ so α centralises $\operatorname{Aut}_S(E) \cong S/E$. We thus have $[S, \alpha] \leq S \cap C_{\operatorname{Aut}_{\mathcal{F}}(S)}(E) \leq C_S(E) \leq E$, so

$[S, \alpha, \alpha] = 1$ and $\ker(\theta)$ centralises the chain $1 \trianglelefteq E \trianglelefteq S$, so by Lemma 1.37 we have $\ker(\theta) \leq O_p(\mathrm{Aut}_{\mathcal{F}}(S)) = \mathrm{Aut}_S(S) = \mathrm{Inn}(S)$.

Hence $\ker(\theta) = C_{\mathrm{Inn}(S)}(E) \cong Z(E)/Z(S)$, which gives an isomorphism

$$\mathrm{Aut}_{\mathcal{F}}(S)/\ker(\theta) \cong N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E)).$$

Note that $\mathrm{Aut}_S(S)\theta = \mathrm{Aut}_S(E) \trianglelefteq N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$, so we also obtain

$$\mathrm{Out}_{\mathcal{F}}(S) = \mathrm{Aut}_{\mathcal{F}}(S)/\mathrm{Inn}(S) \cong N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))/\mathrm{Aut}_S(E).$$

The third statement follows from restricting θ to $\mathrm{Aut}_{\mathcal{F}}^E(S)$. □

We now study the relationship between reduced, simple fusion systems, and fusion systems with no normal p-subgroups, as in some of the results that we use will refer to various of these concepts. Note that by definition a fusion system being reduced implies, in particular, that $O_p(\mathcal{F}) = 1$, and we now prove that simplicity is the strongest condition.

Lemma 2.38. *Any simple fusion system is reduced.*

Proof. By [AOV12, Proposition 1.25], for any saturated fusion system $\mathcal{F}$, $O^p(\mathcal{F})$ and $O^{p'}(\mathcal{F})$ are normal subsystems of $\mathcal{F}$. Also, by a remark in [AKO11, I.6 after Proposition 6.2], if $H \trianglelefteq S$, then $H \trianglelefteq \mathcal{F}$ if and only if $\mathcal{F}_H(H) \trianglelefteq \mathcal{F}$. Thus if a fusion system is not reduced, it is not simple. □

Reduced fusion systems in general are not simple, but we have the following sufficient condition as a corollary of Theorem 2.35. We note that containing no proper non-trivial strongly $\mathcal{F}$-closed subgroups implies that $O^p(\mathcal{F}) = \mathcal{F}$.

Corollary 2.39. *If a fusion system $\mathcal{F}$ satisfies $O^{p'}(\mathcal{F}) = \mathcal{F}$ and contains no proper non-trivial strongly $\mathcal{F}$-closed subgroups then it is simple.*

Proof. We have $O^{p'}(\mathcal{F}) = \mathcal{F}$, which by Theorem 2.35 (2) is equivalent to condition (b) of Theorem 2.35 (3), which is $\mathrm{Aut}_{\mathcal{F}}(S) = \mathrm{Aut}^0_{\mathcal{F}}(S)$. Condition (a) holds since every normal subsystem $\mathcal{D}$ of $\mathcal{F}$ is constructed on a strongly closed subgroup $D \leq S$, but by assumption we have $D = S$, so the result follows. $\square$

Our hypothesis during the reduction phase of our argument only assumes that $O_p(\mathcal{F}) = 1$. In fact, during most of the reduction, we only assume that Z is not strongly closed in $\mathcal{F}$, but in order to narrow down the isomorphism classes of S we use some other potential normal subgroups. As a consequence of the reduction, we will prove that in almost all cases $O^p(\mathcal{F}) = \mathcal{F}$, whereas $O^{p'}(\mathcal{F})$ will be considered while constructing the fusion systems. Our strategy to classify saturated fusion systems $\mathcal{F}$ on a given p-group S is as follows.

1. Find which subgroups E of S can be $\mathcal{F}$-essential for some $\mathcal{F}$.
2. For each such E determine the possibilities for $O^{p'}(\mathrm{Out}_{\mathcal{F}}(E))$.
3. Determine $\mathbf{E}_{\mathcal{F}}$ by identifying which combinations of $\mathcal{F}$-essential subgroups and $\mathcal{F}$-automisers are consistent.
4. For each $E \in \mathbf{E}_{\mathcal{F}}$ determine $\mathrm{Aut}^E_{\mathcal{F}}(S)$ to construct $\mathrm{Aut}^0_{\mathcal{F}}(S)$.
5. Construct $\mathcal{F}_0 \subseteq O^{p'}(\mathcal{F})$ up to isomorphism and attempt to realise it.
6. Consider the largest possible $\mathrm{Aut}_{\mathcal{F}}(S)$ and attempt to construct a corresponding fusion system.

7. Determine the intermediate subsystems of prime index, using the bijection in Theorem 2.35.

8. Prove that the fusion systems constructed exist, are saturated, check uniqueness up to isomorphism and check their exociticy.

To check simplicity of the fusion systems constructed, we require to determine the possibilities of strongly closed subgroups, which will be further work.

CHAPTER 3

SMALL $\mathcal{F}$-ESSENTIAL CANDIDATES

In this chapter we assume that S is a p-group and $\mathcal{F}$ is a saturated fusion system on S, and we determine which p-groups $H \leq S$ satisfying either order at most p^4, abelian with rank at most 2 or of maximal nilpotency class can be $\mathcal{F}$-essential. We rule most cases out by finding a chain of characteristic subgroups to which we apply Lemma 1.37 to show that we cannot have $O_p(\mathrm{Out}_{\mathcal{F}}(H)) = 1$, contradicting the strongly p-embedded condition of $\mathrm{Out}_{\mathcal{F}}(H)$ whenever H is $\mathcal{F}$-essential. Recall that Lemma 2.19 shows that H cannot be cyclic. We begin by recalling well-known results about groups of order p^2 and p^3.

Lemma 3.1. *If H is $\mathcal{F}$-essential with $|H| = p^2$ then $H \cong C_p \times C_p$. Further, $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(H)) \cong SL_2(p)$ is uniquely determined.*

Proof. There are two isomorphism types of p-groups of order p^2 which are $C_p \times C_p$ and C_{p^2}, and cyclic groups cannot be $\mathcal{F}$-essential by Lemma 2.19, so $H \cong C_p \times C_p$. Then $\mathrm{Aut}(H) \cong GL_2(p)$, so the second claim follows from Lemma 1.63. □

Lemma 3.2. *Suppose $H \leq S$ is $\mathcal{F}$-essential of order p^3. Then H is isomorphic to one of C_p^3, p_+^{1+2} with p odd, or Q_8 when $p = 2$.*

Proof. There are five p-groups of order p^3, three abelian and two extraspecial by [Bur97, pp. 93-94 and pp. 100-101]. C_{p^3} is cyclic, so it cannot be $\mathcal{F}$-essential by Lemma 2.19. If $H \cong C_{p^2} \times C_p$ then we have a chain of characteristic subgroups $1 \trianglelefteq \Phi(H) \trianglelefteq \Omega_1(H) \trianglelefteq H$. Similarly if $H \cong p_-^{1+2}$ and p is odd then by Corollary 1.15 there is a characteristic subgroup of K order p^2, giving a chain $1 \trianglelefteq \Phi(H) \trianglelefteq K \trianglelefteq H$ as before. In either case each subgroup in the chain is characteristic in H with each of index p in the next, so each quotient is normalised by $\mathrm{Aut}(H)$ and centralised by $T \in \mathrm{Syl}_p(\mathrm{Aut}(H))$. Then Lemma 1.37 implies that $T \trianglelefteq \mathrm{Aut}(H)$, which as $|T| \neq 1$ contradicts $\mathrm{Out}_{\mathcal{F}}(H)$ having a strongly p-embedded subgroup by Corollary 1.56 (3). We thus conclude that no $\mathrm{Out}_{\mathcal{F}}(H)$ can have a strongly p-embedded subgroup and H cannot be $\mathcal{F}$-essential. The remaining isomorphism types of groups of order p^3 are C_{p^3} and if p is odd also p_+^{1+2}, which can be $\mathcal{F}$-essential, the latter being an $\mathcal{F}$-pearl.

If $p = 2$ the extraspecial groups of order 8 are D_8, which contains a characteristic C_4, and Q_8, which satisfies $\mathrm{Aut}(Q_8) \cong \mathrm{Inn}(Q_8) \rtimes S_3$ where $S_3 \cong SL_2(2)$ has a strongly p-embedded subgroup by Corollary 1.56 (4), therefore only Q_8 can be $\mathcal{F}$-essential. □

We now consider p-groups of maximal class.

Lemma 3.3 ([Gra18, Corollary 1.8])**.** *Suppose $H \leq S$ has maximal nilpotency class and order at least p^4. Then $O_p(\mathrm{Aut}(H)) \in \mathrm{Syl}_p(\mathrm{Aut}(H))$. In particular H cannot be $\mathcal{F}$-essential.*

Proof. Since H has maximal class we have $|H : \Phi(H)| = p^2$ and $|Z(H)| = p$, so since $|H| \geq p^4$, $Z(H) < \Phi(H)$. Thus the characteristic subgroup defined by $\gamma_1(H) = C_H(\gamma_2(H)/\gamma_4(H)))$ described just before [Bla58, Lemma 2.5] has index

p in H hence gives us a chain of characteristic subgroups $\Phi(H) \trianglelefteq \gamma_1(H) \trianglelefteq H$ to which we apply Lemma 1.37 to conclude the first claim. The second claim follows as $\mathcal{F}$-essential subgroups have $O_p(\mathrm{Out}_{\mathcal{F}}(H)) = 1$ by Corollary 1.56 (3). $\square$

3.1 Abelian p-groups of rank 2

We now consider abelian p-groups of rank two, beginning with $C_{p^2} \times C_{p^2}$. Our goal is to prove the following proposition, which we note coincides with [DRV07, Proposition 3.13] where $C_{p^n} \times C_{p^n}$ is ruled out whenever $p > 3$ and $n > 1$, and is the abelian part of [Sam14, Proposition 6.11] where the possibilities for $\mathcal{F}$-essential subgroups of rank at most 2 are determined, including $p = 2$.

Proposition 3.4. *Suppose H has rank at most 2 and is abelian. If H is $\mathcal{F}$-essential in some $\mathcal{F}$ then either $H \cong C_p \times C_p$, or $p \leq 3$ and $H \cong C_{p^k} \times C_{p^k}$.*

Outline of proof. If H has rank 1 then H is cyclic so by Lemma 2.19 is not $\mathcal{F}$-essential. Thus H has rank 2 and is abelian. We rule out non-homocyclic groups in Lemma 3.5 and consider homocyclic p-groups in Lemma 3.8, where we prove that either $p \leq 3$ or H is elementary abelian. $\square$

We begin by ruling out non-homocyclic abelian groups of rank 2.

Lemma 3.5. *If H is abelian of rank 2 and not homocyclic then $O_p(\mathrm{Out}_{\mathcal{F}}(H)) \neq 1$.*

Proof. $H \cong C_{p^a} \times C_{p^b}$ with respective generators x and y where we can choose $a > b$. As $\Phi(H) = \mho^1(H)H'$ and H is abelian, $\Phi(H) = \mho^1(H) = \langle x^p, y^p \rangle$. Hence we have $|H/\Phi(H)| = p^2$, and H contains $p+1$ maximal subgroups, generated by $\Phi(H)$ and $x^i y^j$ for some $i, j \in \{0, \ldots, p-1\}$. Out of these, the p with $i \neq 0$ have exponent p^a and the remaining one $M = \langle \Phi(H), y \rangle$ has exponent p^{a-1}, hence is characteristic in H. Thus we have a chain $\Phi(H) \trianglelefteq M \trianglelefteq H$ as in Lemma 1.37 and $O_p(\mathrm{Aut}(H)) \in \mathrm{Syl}_p(\mathrm{Aut}(H))$. $\square$

We now start studying the homocyclic case by calculating in $GL_2(\mathbb{Z}/p^2\mathbb{Z})$.

Lemma 3.6. *Suppose* $x = \begin{pmatrix} a+1 & b \\ c+1 & d+1 \end{pmatrix} \in GL_2(\mathbb{Z}/p^2\mathbb{Z})$ *with* $p \mid a, b, c, d$. *Then* $x^k = \begin{pmatrix} ka + 1 + T_{k-1}b & kb \\ T_{k-1}(a+d) + k(c+1) + b_{k-2}b & kd + 1 + T_{k-1}b \end{pmatrix}$ *where*

$$T_k = \Sigma_{i=1}^k i = k(k+1)/2 \text{ and } b_k = \Sigma_{i=1}^k T_i = (k+2)(k+1)k/6$$

are respectively the k-th triangular number, and the k-th tetrahedral number. If $p \geq 5$ *then* $x^p = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$ *and* x *can have order* p *if and only if* $p \leq 3$.

Proof.

$$x^{k+1} = \begin{pmatrix} ka + 1 + T_{k-1}b & kb \\ T_{k-1}(a+d) + k(c+1) + b_{k-2}b & kd + 1 + T_{k-1}b \end{pmatrix} \begin{pmatrix} a+1 & b \\ c+1 & d+1 \end{pmatrix} =$$

$$\begin{pmatrix} (ka + 1 + T_{k-1}b)(a+1) + kb(c+1) & (ka + 1 + T_{k-1}b)b + kb(d+1) \\ (T_{k-1}(a+d) + k(c+1) + b_{k-2}b)(a+1) & (T_{k-1}(a+d) + k(c+1) + b_{k-2}b)b \\ +(kd + 1 + T_{k-1}b)(c+1) & +(kd + 1 + T_{k-1}b)(d+1) \end{pmatrix} =$$

$$\begin{pmatrix} a + ka + 1 + T_{k-1}b + kb & b + kb \\ ka + T_{k-1}(a+d) + k(c+1) & \\ +b_{k-2}b + c + kd + 1 + T_{k-1}b & kb + d + kd + 1 + T_{k-1}b \end{pmatrix} =$$

$$\begin{pmatrix} (k+1)a + 1 + T_k b & (k+1)b \\ T_k(a+d) + (k+1)(c+1) + b_{k-1}b & (k+1)d + 1 + T_k b \end{pmatrix}$$

Note that we take $b_i = 0 = T_i$ when $i \leq 0$. We proceed by induction. If $k = 1$ then $T_0 = 0$ and $b_{-1} = 0$, so $x^1 = x$. The calculation above shows that x^{k+1} has form as claimed if x^k does too, where, as $x \in GL_2(\mathbb{Z}/p^2\mathbb{Z})$, any elements divisible by p^2 are 0, so the elements quadratic in p, a, b, c, d in calculations vanish and we are only left with elements where at most one copy of p, a, b, c and d appears.

In particular, when $k = p$, we see that $T_p = p(p+1)/2$ and $b_{p-2} = p(p-1)(p-2)/6$ are divisible by p whenever $p \geq 5$, so that the bottom left entry of x^p is

$$T_{p-1}(a+d) + p(c+1) + b_{p-2}b \equiv p \pmod{p^2}$$

and x does not have order p. If $p = 3$, we see $b_1 = 1$ so it is possible to take $b = 6$ to obtain the bottom left entry $T_2(a+d) + 3(c+1) + b_1 b \equiv 3 + 6 \equiv 0 \pmod 9$; therefore x can have order 3. If $p = 2$ then $T_1 = 1$ and $b_0 = 0$, so we can choose $a = 2$, $d = 0$ to obtain $T_1(a+d) + 2(c+1) + b_0 b \equiv a + d + 2 \equiv 0 \pmod 4$, thus x can have 2. $\square$

For any $\mathcal{F}$-essential subgroup H of rank 2, $\mathrm{Out}_{\mathcal{F}}(H)$ embeds into $GL_2(p)$ by Lemma 2.20. Thus, we now proceed inductively to determine when there is a subgroup isomorphic to $SL_2(p)$ in $GL_2(\mathbb{Z}/p^k\mathbb{Z})$, where Lemma 3.6 serves as a base case.

Lemma 3.7. *For each $k \in \mathbb{Z}_{\geq 2}$ let $G_k = GL_2(\mathbb{Z}/p^k\mathbb{Z})$ and $\psi_{k-1} : G_k \to G_{k-1}$ given by restriction modulo p^{k-1} of each entry of $A \in G_k$. Then $G_k \cong C_p^4.G_{k-1}$, and G_k contains a subgroup isomorphic to $SL_2(p)$ if and only if $p \in \{2, 3\}$.*

Proof. Note that $G_k = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}/p^k\mathbb{Z},\ p \nmid ad - bc \right\}$. For each k

we consider the map $\psi_{k-1} : G_k \to G_{k-1}$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ where we define $\overline{x} = x \pmod{p^{k-1}}$. The kernel of ψ_{k-1} is

$$K_{k-1} = \ker \psi_{k-1} = \left\{ \begin{pmatrix} a+1 & b \\ c & d+1 \end{pmatrix} \mid a,b,c,d \equiv 0 \pmod{p^{k-1}} \right\}.$$

K_{k-1} is generated by four commuting elements of order p which can be chosen to have exactly one of a, b, c, d equal to p^{k-1} and the rest equal to 0. Note that

$$\begin{aligned} \begin{pmatrix} 1 & -p^{k-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{k-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & p^{k-1} \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 - p^{2(k-1)} & -p^{k-1} \\ p^{k-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & p^{k-1} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 - p^{2(k-1)} & -p^{3(k-1)} \\ p^{k-1} & p^{2(k-1)} + 1 \end{pmatrix}, \end{aligned}$$

so that $\begin{pmatrix} 1 & p^{k-1} \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ p^{k-1} & 1 \end{pmatrix}$ commute whenever $p^{2(k-1)} = 0$, as it does in $\mathbb{Z}/p^k\mathbb{Z}$. We can similarly check that the remaining four generators commute, hence $K_{k-1} \cong C_p^4$, thus as ψ_{k-1} is surjective we have $G_k \cong C_p^4.G_{k-1}$.

Thus K_{k-1} is an elementary abelian normal subgroup of G_k. Then G_k splits over K_{k-1} if and only if it splits over a Sylow p-subgroup of K_{k-1} by [Hup67, I.17.4 (Gaschütz)], and we proceed inductively to show that G_k splits over K_1 if and only if G_k splits over a Sylow p-subgroup of K_1.

Thus if there is a complement to K_{k-1} in G_k, then there is an element $x \in G_k$ such that $\langle x \rangle$ is a Sylow p-subgroup of $GL_2(p)$, that is an element of order p such that $(x\psi_{k-1}\ldots\psi_2)\psi_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Thus $(x\psi_{k-1}\ldots\psi_2) = \begin{pmatrix} a+1 & b \\ c+1 & d+1 \end{pmatrix}$ with $a, b, c, d \equiv 0 \pmod p$ as in Lemma 3.6, which is possible if and only if $p \leq 3$. □

And now we use the calculation above to conclude.

Lemma 3.8. *Let H_k be homocyclic of rank 2 and exponent k. Then $SL_2(p)$ embeds into $\mathrm{Aut}(H_k)$ if and only if $k = 1$ or $p \leq 3$.*

Proof. We have $H_k \cong C_{p^k} \times C_{p^k}$. If $k = 1$ then $\mathrm{Aut}(H_k) \cong GL_2(p)$ and by Lemma 1.63 $SL_2(p) \leq GL_2(p)$ is a subgroup with a strongly p-embedded subgroup. If $k \geq 2$ then $\mathrm{Aut}(H_k) \cong GL_2(\mathbb{Z}/p^k\mathbb{Z})$, hence by Lemma 3.7 the condition is satisfied if and only if $p \leq 3$. □

3.2 p-groups of order p^4

We now turn our attention to p-groups of order p^4. These were enumerated by Burnside in [Bur97, pp. 100-102], and are available in the SmallGroups library [BEO02]. We first consider nonabelian p-groups.

Lemma 3.9. *Suppose $H \leq S$ of order p^4 is nonabelian and $O_p(\mathrm{Out}_{\mathcal{F}}(H)) = 1$ then either p is odd and $H \cong p_+^{1+2} \times C_p$ or $p = 2$ and $H \cong Q_8 \times C_2$ or $H \cong D_8 \circ C_4$.*

Proof. Let H of order p^4 be nonabelian with $O_p(\mathrm{Out}_{\mathcal{F}}(H)) = 1$. Lemma 3.3 rules out H of maximal nilpotency class, hence H has nilpotency class 2 and $H' \leq Z(H)$. If $Z(H) = H'$ of order p then, as H is not extraspecial by Lemma 1.12, we have $|\Phi(H)| = p^2$ and a chain $1 \trianglelefteq Z(H) \trianglelefteq \Phi(H) \trianglelefteq C_H(\Phi(H))$ as in Lemma 1.37. Hence $|Z(H)| = p^2$ and we cannot have any characteristic subgroup of index p

in H, so any characteristic subgroup of order p^2 coincides with $Z(H)$. Now H has nilpotency class 2, so if p is odd then H is regular by Proposition 1.5 (1), hence Proposition 1.7 (3) implies $|H/\Omega_1(H)| = |\mho^1(H)|$. Therefore either H has exponent p or $|\Omega_1(H)| = |\mho^1(H)| = p^2$, so that $\Phi(H) = \Omega_1(H) = \mho^1(H) = Z(H)$ and [Hup67, III.11.4 Satz] implies H is metacyclic. In this case $\mho^2(H) = 1$, so H has exponent p^2 and is an extension of C_{p^2} by C_{p^2}. As $\mathrm{Aut}(C_{p^2}) \cong C_{p^2-p}$, it contains a unique subgroup of index p, and there is only one nontrivial extension up to isomorphism, the group with presentation $\langle x, y \mid x^{p^2}, y^{p^2}, [x,y] = x^p \rangle$, which contains a characteristic subgroup $\langle x, y^p \rangle$ of index p.

The remaining case with p odd is H of exponent p, nilpotency class 2, and $|Z(H)| = p^2$. Hence $H = \langle x_1, x_2, x_3, x_4 \rangle$ such that $x_i^p = 1$, $Z(H) = \langle x_3, x_4 \rangle$, and $H' = \langle [x_1, x_2] \rangle \leq Z(H)$ has order p. Thus $\langle x_1, x_2 \rangle \cong p_+^{1+2}$ which commutes with the remaining generator hence $H \cong p_+^{1+2} \times C_p$ as claimed.

If $p = 2$ then, as regular 2-groups are abelian by Proposition 1.6 (1), H is not regular, so we use the SmallGroups Library [BEO02]. We see that the only candidates of 2-groups of order $16 = 2^4$ with nilpotency class 2 (and $|Z(H)| = 4$) are in the SmallGroups notation $H_i = <16, i>$ where $i \in \{3, 4, 6, 11, 12, 13\}$. Out of these, the only H_i where $\mathrm{Aut}(H_i)$ is not a 2-group are H_{12} and H_{13}. We have $H_{12} \cong Q_8 \times C_2$ and $H_{13} \cong D_8 \circ C_4 \cong Q_8 \circ C_4$, with automorphism groups $2^5.S_3$ and $C_2 \times S_4$ respectively. As $GL_2(2) = SL_2(2) \cong S_3$ acts on a section $Q_8/Z(Q_8)$ of H_i, both H_{12} and H_{13} are candidates. A Magma snippet checks this.

```
> S1 := [H : H in SmallGroups(2^4) | NilpotencyClass(H) eq 2];
> [<FactoredOrder(PermutationGroup(AutomorphismGroup(H))),
> IdentifyGroup(H)> : H in S1];
```

```
[
    <[ <2, 5> ], <16, 3>>,
    <[ <2, 5> ], <16, 4>>,
    <[ <2, 4> ], <16, 6>>,
    <[ <2, 6> ], <16, 11>>,
    <[ <2, 6>, <3, 1> ], <16, 12>>,
    <[ <2, 4>, <3, 1> ], <16, 13>>
]
```

□

We can now describe the $\mathcal{F}$-essential candidates of order p^4.

Proposition 3.10. *Suppose $H \leq S$ and H is an $\mathcal{F}$-essential subgroup of order p^4 for some saturated fusion system $\mathcal{F}$ on S. Then H is isomorphic to one of the following:*

1. *C_p^4 or $C_{p^2} \times C_p \times C_p$ for all p;*
2. *$C_{p^2} \times C_{p^2}$ with $p \in \{2, 3\}$;*
3. *$p_+^{1+2} \times C_p$ with p odd; or*
4. *$Q_8 \times C_2$ and $D_8 \circ C_4$ when $p = 2$.*

Proof. In Lemma 3.9 we showed that the proposition holds whenever H is non-abelian. If H is abelian then Proposition 3.4 shows that if it has p-rank at most 2 then $p \leq 3$ and $H \cong C_{p^2} \times C_{p^2}$. The elementary abelian group C_p^4 has $\mathrm{Aut}(C_p^4) \cong GL_4(p)$, which contains subgroups with a strongly p-embedded subgroup (even with Sylow p-subgroups of order p^2 by Proposition 1.65). The only remaining candidates have rank 3, hence they correspond to a partition of 4 with 3 non-zero elements. There is a unique such partition: $(2, 1, 1)$, hence $H \cong C_{p^2} \times C_p \times C_p$, whose automorphism group contains a subgroup isomorphic to $GL_2(p)$ and we have not ruled it out as an $\mathcal{F}$-essential candidate. $\square$

We finally show how to distinguish between certain groups of order p^4, which will appear in Chapter 7.

Lemma 3.11. *Let S be a p-group of order p^4 containing a unique abelian subgroup A of index p. Then the following hold.*

1. *If every nonabelian maximal subgroup of S has exponent p then either $p = 3$, $S \cong <3^4, 9>$ and $A \cong C_9 \times C_3$, or $p > 3$, S has exponent p and $S \cong <p^4, 7>$.*

2. *If $p = 3$, S satisfies $|Z(S)| = 3$ and S contains a unique maximal subgroup isomorphic to 3^{1+2}_+, then either $S \cong <3^4, 7>$ with $A \cong C_3^3$ or $S \cong <3^4, 8>$ with $A \cong C_9 \times C_3$.*

Proof. If $p > 3$ then as $|S| = p^4 < p^p$, S is regular by Proposition 1.5 (2). Hence if S contains at least 2 maximal subgroups of exponent p, S is generated by elements of order p and Theorem 1.7 implies that S has exponent p. Thus S is a split extension of $A \cong C_p^3$ by an element of x order p, that is $S \cong C_p^3 \rtimes C_p$. As A is the unique abelian subgroup of index p in S we have $|S'| = p^2$ and $|Z(S)| = p$ by Lemma 1.21, that is S has maximal class and x has Jordan form J_3 and is unique up to conjugacy in $\mathrm{Aut}(A) \cong GL_3(p)$. Hence Lemma A.6 implies that S is unique up to isomorphism. In the SmallGroups notation $S \cong <p^4, 7>$, and the Sylow p-subgroups of $PSp_4(p)$ have this property. If $p = 3$, however, S is not regular, but the following Magma snippets prove the claims, where $3_+^{1+2} \cong <3^3, 3>$, $C_3^3 \cong <3^3, 5>$ and $C_9 \times C_3 \cong <3^3, 2>$, and $A = C_S(S')$.

```
[IdentifyGroup(i) : i in SmallGroups(3^4) | 3 eq #[M : M in
MaximalSubgroups(i) | IsIsomorphic(M`subgroup,
SmallGroup(3^3, 3))]];
```

outputs: `[ <81, 9> ]`

Case (1) does not arise when $p = 2$ since 2-groups of exponent 2 are abelian.

Similarly the second claim is proved by the following snippet.

```
[<IdentifyGroup(i), IdentifyGroup(Centraliser(i,
DerivedSubgroup(i)))>: i in SmallGroups(3^4) | #Centre(i) eq 3 and
1 eq #[M : M in MaximalSubgroups(i) | IsIsomorphic(M`subgroup,
SmallGroup(3^3, 3))]];
```

outputs: `[ <<81, 7>, <27, 5>>, <<81, 8>, <27, 2>> ]` □

CHAPTER 4

FUSION SYSTEMS ON p-GROUPS WITH AN EXTRASPECIAL SUBGROUP OF INDEX p: REDUCTION

We begin by setting up some notation that we use throughout this chapter.

Hypothesis A. *Let p be an odd prime, S a p-group with an extraspecial subgroup Q of index p, and let $\mathcal{F}$ be a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. Denote $Z := Z(S)$, and $|S| = p^{2+2n}$.*

We begin by proving that if $Z(Q) \neq Z(S)$ then there is some subgroup of S which is normal in $\mathcal{F}$, which contradicts $O_p(\mathcal{F}) = 1$. We first adapt the proof of [Oli14, Theorem 2.1] when $|S| = p^4$, and then consider the general case.

Lemma 4.1. *Assume Hypothesis A and $|S| = p^4$. Then $Z(S) = Z(Q)$.*

Proof. Assume for a contradiction that $Z(S) \neq Z(Q)$. Then we have $|Z(S)| = p^2$ by Lemma 1.22, so that, as $|S| = p^4$, we have $|S/Z(S)| = p^2$ and $S/Z(S)$ is elementary abelian by [Gor80, Lemma 1.3.4]. In this case the only proper subgroups of S containing $Z(S)$ properly are abelian subgroups of index p in S, and there is exactly $p + 1$ of them which we denote by $E_1, \ldots, E_{p+1}$. Thus, by Lemma 2.18 (1), the E_i

are the only candidates for $\mathcal{F}$-essential subgroups. By Lemma 3.2 those E_i that are $\mathcal{F}$-essential are isomorphic to C_p^3. Fix one E_i.

Note $S' = (QZ(S))' = Q'$ has order p, so that $[S, E_i] = S'$ has order p and $C_{E_i}(S) = Z(S)$ has order p^2. Hence $\mathrm{Aut}_S(E)$ is generated by transvections over $GF(p)$, and so is its normal closure $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(E)$, which by Lemma 1.61 contanins a strongly p-embedded subgroup. Hence Lemma 1.62 implies that $H_i := O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong SL_2(p)$ and $E_i = W_i \times U_i$ where $U_i = [E_i, H_i]$ is a faithful 2-dimensional H_i-module and $W_i = C_{E_i}(H_i)$ is 1-dimensional. We have $U_i \cap Z(S) = S'$, thus $Z(S) = S' \times W_i$, and W_i is the unique subgroup of $Z(S)$ which is a complement to S' and is normalised by $N_{H_i}(\mathrm{Aut}_S(E_i)) = \mathrm{Aut}_S(E_i) \rtimes D_i$ of order $p(p-1)$. The subgroup D_i consists of diagonal matrices in $N_{H_i}(\mathrm{Aut}_S(E_i))$ hence acts faithfully on S' and permutes the $p-1$ other maximal subgroups of $Z(S)$. Now every element $d \in D_i$ extends to $\overline{d} \in \mathrm{Aut}_{\mathcal{F}}(S)$ with $\overline{d}|_{E_i} = d$ by Lemma 2.9. Further, as $Z(S)$ is characteristic in S, $\overline{d}|_{Z(S)} \in \mathrm{Aut}_{\mathcal{F}}(Z(S))$. Therefore the only maximal subgroups of $Z(S)$ which can be normalised by $\mathrm{Aut}_{\mathcal{F}}(Z(S))$ are S' and W_i. Since $\mathrm{Aut}_{\mathcal{F}}(Z(S))$ is a p' group and normalises S', it cannot act transitively on the remaining p maximal subgroups of $Z(S)$, so there is some complement to S' in $Z(S)$ that is normalised. Thus W_i is normalised by $\mathrm{Aut}_{\mathcal{F}}(Z(S))$.

Further, as every element of $\mathrm{Aut}_{\mathcal{F}}(S)$ restricts to $\mathrm{Aut}_{\mathcal{F}}(Z(S))$ and $\mathrm{Aut}_{\mathcal{F}}(Z(S))$ normalises W_i, so does $\mathrm{Aut}_{\mathcal{F}}(S)$. Thus $W_i = W_j$ for all i, j with E_i, E_j $\mathcal{F}$-essential, and W_i is normalised by $\mathrm{Aut}_{\mathcal{F}}(S)$ for all (potential) $\mathcal{F}$-essential subgroups of S as well as $\mathrm{Aut}_{\mathcal{F}}(S)$, so $W_i \trianglelefteq \mathcal{F}$ by Proposition 2.25, which contradicts our assumption that $O_p(\mathcal{F}) = 1$. $\square$

Now we deal with the general case.

Theorem 4.2. *Assume Hypothesis A. Then $Z(S) = Z(Q)$.*

Proof. Suppose $Z(S) \neq Z(Q)$. Then by Lemma 1.22 we have $S = QZ(S)$ and $|Z(S)| = p^2$. If $|S| = p^4$ the result is Lemma 4.1, hence we may assume $|Q| > p^3$. We have $S' = (QZ(S))' = Q' = Z(Q)$, and $\Phi(S) = S^p S' = Q^p Z(S)^p Q' = Z(Q)$.

We will show that $Z(Q) \trianglelefteq \mathcal{F}$, contradicting our assumptions. Note that $Z(Q) \leq Z(S)$ by Lemma 1.22, so Lemma 2.18 (1) implies that $Z(Q) \leq E$ for all $\mathcal{F}$-centric subgroups E. Hence, if $Z(Q) \ntrianglelefteq \mathcal{F}$, then H is not strongly closed in $\mathcal{F}$ by Lemma 2.25, that is there is some $\gamma \in \mathrm{Hom}_{\mathcal{F}}(Z(Q), S)$ such that $Z(Q) \neq Z(Q)\gamma$. Note that $Z(Q) = S'$ is characteristic in S, so it is normalised by $\mathrm{Aut}_{\mathcal{F}}(S)$. Then, by Alperin's Theorem (Theorem 2.16), there is some $\mathcal{F}$-essential subgroup E with $Z(Q) \leq E$ and $\alpha \in \mathrm{Aut}_{\mathcal{F}}(E)$ such that $Z(Q)\alpha \neq Z(Q)$. In particular, $Z(Q)$ is not a characteristic subgroup of E.

If E is not elementary abelian then $1 \neq \Phi(E) \leq \Phi(S) = Z(Q)$, which is cyclic of order p, so $\Phi(E) = Z(Q)$ is characteristic in E, a contradiction. Thus, any $\mathcal{F}$-essential subgroup E with $\beta \in \mathrm{Aut}_{\mathcal{F}}(E)$, such that $Z(Q) \neq Z(Q)\beta$, is elementary abelian. Further, $E \trianglelefteq S$ as $S' = Z(Q) \leq E$. Also $[E, S] = Z(Q)$, and E is $\mathcal{F}$-centric, so $1 \neq [E, S] \leq S' = Z(Q)$.

Claim 4.2.1. *Let $\alpha \in \mathrm{Aut}_{\mathcal{F}}(E)$ such that $Z(Q)\alpha \neq Z(Q)$. Then*

$$|C_S(Z(Q)\alpha)| = |C_Q(Z(Q)\alpha)|p \in \{|S|, |S|/p\}.$$

Proof of claim. Let $x \in Z(Q)\alpha$. Since $S = QZ(S)$ we have $x = qz$ for some $q \in Q$, $z \in Z(S)$, so $C_S(Z(Q)\alpha) = C_S(\langle q \rangle)$ with $\langle q \rangle \leq Q$. Let $K := \langle q, Z(Q) \rangle$, we have $|K| \in \{p, p^2\}$, and $Z(Q) \leq K$ so $|Q : C_Q(K)| = |K : Z(Q)| \in \{1, p\}$ by Lemma

1.10. Thus as

$$C_S(K) = C_S(\langle q \rangle) \cap C_S(Z(Q)) = C_S(\langle q \rangle) \cap S = C_S(\langle q \rangle)$$

we have $|C_S(Z(Q)\alpha)| = |C_S(\langle q \rangle)| = |C_S(K)| = |C_Q(K)|p \in \{|S|, |S|/p\}$. ■

Then as $|Q| > p^3$, the maximal abelian subgroups of Q have index at least p^2 in Q by Lemma 1.17, so $C_S(Z(Q)\alpha)$ is not abelian. In particular, as E is abelian, $C_S(Z(Q)\alpha) > E$ so $C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha) \neq 1$ and $[E, C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha)] \neq 1$.

Now consider $\mathrm{Aut}_{\mathcal{F}}(E)$. As $E \trianglelefteq S$, E is fully $\mathcal{F}$-normalised and we have $S/E \cong \mathrm{Aut}_S(E) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(E))$. Consider $\mathrm{Aut}_S(E)^\alpha \leq \mathrm{Aut}_{\mathcal{F}}(E)$.

By Sylow's Theorem, as $\mathrm{Aut}_S(E)^\alpha \cap C_{\mathrm{Aut}_{\mathcal{F}}(E)}(Z(Q)\alpha) \in \mathrm{Syl}_p(C_{\mathrm{Aut}_{\mathcal{F}}(E)}(Z(Q)\alpha))$ and $C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha)$ is a p-group, there exists $\beta \in C_{\mathrm{Aut}_{\mathcal{F}}(E)}(Z(Q)\alpha)$ such that:

1. $C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha) \leq [\mathrm{Aut}_S(E)^\alpha \cap C_{\mathrm{Aut}_{\mathcal{F}}(E)}(Z(Q)\alpha)]^\beta \leq (\mathrm{Aut}_S(E))^{\alpha\beta}$ and

2. $Z(Q)\alpha\beta = Z(Q)\alpha$.

Now consider $[E, C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha)] \leq [E, \mathrm{Aut}_S(E)] = [E, S] = Z(Q)$.

On the other hand,

$$\begin{aligned}[E, C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha)] \leq [E, (\mathrm{Aut}_S(E))^{\alpha\beta}] &= [E\alpha\beta, (\mathrm{Aut}_S(E))^{\alpha\beta}] \\ &= [E, S]\alpha\beta = Z(Q)\alpha\beta = Z(Q)\alpha.\end{aligned}$$

Thus, $1 \neq [E, C_{\mathrm{Aut}_S(E)}(Z(Q)\alpha)] \leq Z(Q) \cap Z(Q)\alpha$, so $Z(Q) = Z(Q)\alpha$, a contradiction. Hence $\mathrm{Aut}_{\mathcal{F}}(E)$ fixes $Z(Q)$.

Therefore, all maps in $\mathcal{F}$ normalise $Z(Q)$, and $Z(Q)$ is strongly closed in $\mathcal{F}$. As $Z(Q) \leq Z(S) \leq E$ for all $\mathcal{F}$-essential subgroups E, by Proposition 2.25 $Z(Q)$ is normal in $\mathcal{F}$. Thus $O_p(\mathcal{F}) \neq 1$, a contradiction as claimed. Thus we must have $Z(S) = Z(Q)$. $\square$

If $|S| = p^4$ then by Lemma 1.20 S has an abelian subgroup of index p. The simple fusion systems on these p-groups have been classified in [Oli14], [COS17] and [OR17]. We will look at them more closely in Chapter 7. Hence from now on we may assume the following.

Hypothesis B. *Assume Hypothesis A, $|S| \geq p^6$, and $Z = Z(S) = Z(Q)$.*

4.1 $\mathcal{F}$-essential subgroups contained in Q

Next we show that under Hypothesis B an extraspecial subgroup Q of index p in S plays a role analogous to an abelian subgroup of index p, in the sense that no proper subgroup of Q can be $\mathcal{F}$-essential. In general the only subgroups of extraspecial groups which can be $\mathcal{F}$-essential are elementary abelian.

Lemma 4.3. *Let $\mathcal{F}$ be a saturated fusion system on S. Suppose E is $\mathcal{F}$-essential and $E < R \leq S$ with R extraspecial. Then E is elementary abelian.*

Proof. Suppose $E < R$ is not elementary abelian. Then, as R is extraspecial, we have $1 \neq \Phi(E) \leq [E, R] \leq R' = Z(R)$, so $\Phi(E) = [E, R]$ is characteristic in E, and thus normalised by $\mathrm{Aut}_{\mathcal{F}}(E)$. However then by Lemma 2.21 we have $E = R$, a contradiction. Thus E is elementary abelian. $\square$

Note that the result above does not assume that R has index p in S. Now we look more closely at the case where Q does have index p in S.

Theorem 4.4. *Assume Hypothesis B. Suppose $E \leq Q$ is an $\mathcal{F}$-essential subgroup. Then $E = Q$.*

Proof. Let $|Q| = p^{1+2n}$, where $n \geq 2$ as $|S| \geq p^6$, and assume $E < Q$. Then E is elementary abelian by Lemma 4.3. By Lemma 2.18, E is maximal abelian in S. Therefore we have $|E| = p^{1+n}$ and $\mathrm{Aut}(E) \cong GL_{n+1}(p)$. Since E is maximal abelian in Q we have $Z(Q) \leq E$, so $E \trianglelefteq Q$ by Lemma 1.9. Thus $|\mathrm{Aut}_S(E)| \in \{p^n, p^{n+1}\}$. Note $1 \neq [E, Q] \leq Q' = Z$, so $[E, Q] = Z$.

Let $x \in Q \setminus E$. Then $|E/C_E(x)| = |[E, x]| = |Z| = p$, so c_x acts on E a transvection over $GF(p)$, hence $\mathrm{Aut}_Q(E) \cong Q/E$ is generated by transvections, and so are its conjugates in $\mathrm{Aut}_{\mathcal{F}}(E)$. Therefore $N := \langle \mathrm{Aut}_Q(E)^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(E)$ is generated by transvections. Further, as $\mathrm{Aut}_{\mathcal{F}}(E)$ contains a strongly p-embedded subgroup, by Lemma 1.61 so does N, hence Lemma 1.62 implies that $N \cong SL_2(p)$. In particular $|\mathrm{Aut}_Q(E)| = p$, contradicting $|Q/E| = p^n \geq p^2$. Therefore if $E \leq Q$ is $\mathcal{F}$-essential and $|S| \geq p^6$ then $E = Q$. $\square$

Remark 4.5. *Using the fact that $|\mathrm{Aut}_S(E)| \in \{p^n, p^{n+1}\}$, we could use that $\mathrm{Aut}_{\mathcal{F}}(E) \cong \mathrm{Out}_{\mathcal{F}}(E)$ has a strongly p-embedded subgroup and apply [Sam14, Proposition 6.10], which states that if E is $\mathcal{F}$-essential of rank r then $|N_S(E)/E| \leq p^{\lfloor r/2 \rfloor}$ to obtain the same result. However, we have chosen to supply a direct proof rather than one which depends on the Classification of Finite Simple Groups.*

Next we look at possible $\mathcal{F}$-essential subgroups not contained in any extraspecial subgroup of index p. If there is an $\mathcal{F}$-essential subgroup which is both abelian and normal in S we use Sambale's bounds as follows.

Lemma 4.6. *Let S be a p-group with an extraspecial subgroup Q of index p, and $\mathcal{F}$ a saturated fusion system on S. Suppose $E \trianglelefteq S$ with $E \not\leq Q$ abelian and*

$\mathcal{F}$*-essential. Then* $|S| = p^{2+2n} \leq p^6$ *and* E *is elementary abelian of index* p^n*.*

Proof. Let $|E| = p^l$. Then E is abelian and has rank $r \leq l$, and if $|S| = p^{2+2n}$ then $l \leq n+2$ by Lemma 1.17. As $E \not\leq Q$ and $E \trianglelefteq S$, Lemma 1.27 implies that S/E is elementary abelian, then we have $|\operatorname{Aut}_S(E)| = |S/E| \leq p^{\lfloor r/2 \rfloor}$ by [Sam14, Proposition 6.10]. Hence $p^{2+2n} = |S| = |E||S/E| \leq p^{l+\lfloor r/2 \rfloor}$ so

$$2 + 2n \leq l + \lfloor r/2 \rfloor \leq n + 2 + \lfloor n/2 \rfloor + 1.$$

Thus $n \leq 1 + n/2$, which implies $n \leq 2$. Therefore, $|S| = p^{2+2n} \leq p^6$. If $n = 2$ then, by Lemma 1.24, S does not contain an abelian subgroup of index p, thus $r = l = 4$ and E is elementary abelian. If $n = 1$ then $l = 3$, so, by Lemma 3.2, E is elementary abelian. □

We will use $O_p(\mathcal{F}) = 1$ to restrict the structure of Z as follows.

Lemma 4.7. *Assume Hypothesis B. Then there is some* $\mathcal{F}$*-essential* $E \leq S$ *such that* $\operatorname{Aut}_{\mathcal{F}}(E)$ *moves* Z*.*

Proof. If every map in $\mathcal{F}$ fixes Z then, as $Z \leq E$ for any $\mathcal{F}$-essential subgroup E and $Z \leq S$, by Lemma 2.25 $Z \trianglelefteq \mathcal{F}$, so $Z \leq O_p(\mathcal{F})$. Then by Alperin's Theorem 2.16 we need some $\mathcal{F}$-essential E such that $\operatorname{Aut}_{\mathcal{F}}(E)$ moves Z. □

Lemma 4.7 motivates the following definition.

Definition 4.8. *Assume Hypothesis B. Define by* $\mathcal{M}$ *the set of* $\mathcal{F}$*-essential subgroups of* S *such that* $\operatorname{Aut}_{\mathcal{F}}(E)$ moves Z*. That is,*

$$\mathcal{M} := \{E \leq S \mid E \textit{ is } \mathcal{F}\textit{-essential and } Z \textit{ is not normalised by } \operatorname{Aut}_{\mathcal{F}}(E)\}.$$

For $E \in \mathcal{M}$, define $Z_E := \langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle$ and $C_E := C_S(Z_E)$.

Note that $\mathcal{M}$ is nonempty by Lemma 4.7, and $E \in \mathcal{M}$ implies $E \not\leq Q$ by Theorem 4.4. We will split the discussion according to whether there is $E \in \mathcal{M}$ such that $Z_E \leq Q$, or $Z_E \not\leq Q$ for all $E \in \mathcal{M}$. Thus, we set up the following Hypotheses.

Hypothesis C. *Assume Hypothesis B and that there is $E \in \mathcal{M}$ such that $Z_E \leq Q$.*

Hypothesis D. *Assume Hypothesis B and that for all $E \in \mathcal{M}$ we have $Z_E \not\leq Q$.*

We discuss Hypothesis C and D each in their own section.

4.2 Hypothesis C: some $\mathcal{F}$-essential subgroup $E \in \mathcal{M}$ has $Z_E \leq Q$

In this section we study the case where Hypothesis C holds. That is, S is a p-group with an extraspecial subgroup Q of index p, where $|S| \geq p^6$ and $Z = Z(S) = Z(Q)$. $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$, and there is an $\mathcal{F}$-essential subgroup E such that Z is not normalised by $\mathrm{Aut}_{\mathcal{F}}(E)$ and $Z_E = \langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle \leq Q$. Important subgroups will be $C_E = C_S(Z_E)$ and $F_E := \bigcap_{\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)} C_Q(Z_E)\alpha$.

In this section we prove the following result.

Proposition 4.9. *Assume Hypothesis C. Let $E \in \mathcal{M}$ with $Z_E \leq Q$. Then $|S| = p^6$, E is maximal in S with $\Phi(E) \in \{Z_E, F_E\}$, and either S is isomorphic to a Sylow p-subgroup of $SL_4(p)$, or $p \geq 5$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$.*

Outline of proof. In Proposition 4.13 we prove that $|S| = p^6$ and C_E is maximal in S with $\Phi(C_E) \in \{Z_E, F_E\}$ and $Z_E = Z(E)$, then we show $E = C_E$ in Lemma

4.14. At that stage we split the discussion according to whether $\Phi(E) = Z_E$ or $\Phi(E) = F_E$. We then apply Lemma 1.26 to obtain the upper and lower central series of S.

In the case where $\Phi(E) = F_E$ we show that Q has exponent p in Lemma 4.16 and, in Proposition 4.17, we prove that $p \geq 5$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$.

We then prove that if $\Phi(E) = Z(E)$ and $p \neq 3$ then S is a semidirect product of C_p^4 by C_p^2 in Lemma 4.18, and conclude in Proposition 4.20 that S is isomorphic to a Sylow p-subgroup of $SL_4(p)$. Lemma 4.19 deals with the case $p = 3$. $\square$

We begin by studying Z_E.

Lemma 4.10. *Assume Hypothesis C. Then Z_E is normal in S, elementary abelian, fully $\mathcal{F}$-automised and $\mathcal{F}$-receptive.*

Proof. As $Z \leq Z(E)$, we have $Z_E = \langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle \leq Z(E)$, so $Z_E \trianglelefteq E$ is abelian and generated by elements of order p, hence it is elementary abelian. As $Z \leq Z_E \leq Q$, we have $Z_E \trianglelefteq Q$ by Lemma 1.9. Thus, $Z_E \trianglelefteq EQ = S$, and Z_E is fully $\mathcal{F}$-normalised. Then, by Theorem 2.7, Z_E is fully $\mathcal{F}$-centralised, fully $\mathcal{F}$-automised and $\mathcal{F}$-receptive. $\square$

Lemma 4.11. *Assume Hypothesis C, then Z is not invariant under $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$, $Z_E = \langle Z^{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))} \rangle$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ acts irreducibly on Z_E.*

Proof. As every map in $\mathrm{Aut}_{\mathcal{F}}(E)$ moving Z restricts to a map of Z_E, we observe $Z_E = \langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle = \langle Z^{\mathrm{Aut}_{\mathcal{F}}(Z_E)} \rangle$. Then, as Z_E is fully $\mathcal{F}$-automised by Lemma 4.10, we have $\mathrm{Aut}_S(Z_E) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(Z_E))$, so $\mathrm{Aut}_S(Z_E)$ is a Sylow p-subgroup of $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$. Further, as $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E)) \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(Z_E)$, we have, by the Frattini

Argument (Theorem 1.1), $\mathrm{Aut}_{\mathcal{F}}(Z_E) = O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))N_{\mathrm{Aut}_{\mathcal{F}}(Z_E)}(\mathrm{Aut}_S(Z_E))$. As $Z_E \trianglelefteq S$, it is fully $\mathcal{F}$-normalised, hence every element $\alpha \in N_{\mathrm{Aut}_{\mathcal{F}}(Z_E)}(\mathrm{Aut}_S(Z_E))$ lifts to $N_S(Z_E) = S$ by Lemma 2.9. Thus α normalises Z, so Z is not invariant under $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$, and any image of Z under $\mathrm{Aut}_{\mathcal{F}}(Z_E)$ can be attained by some $\alpha \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$. Hence $Z_E = \langle Z^{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))}\rangle$.

Assume there is $N \leq Z_E$ normalised by $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$. As $Z_E \leq Q$ we have $N \trianglelefteq Q$, as otherwise there would be $q \in Q$ such that $Nc_q \neq N$ and $c_q|_{Z_E} \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$, a contradiction. Thus, $Z \leq N$ by Lemma 1.9, and we have $Z_E = \langle Z^{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))}\rangle \leq N$. Therefore, $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ acts irreducibly on Z_E. $\square$

We now determine the structure of Z_E and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$.

Lemma 4.12. *Assume Hypothesis C. Then $|Z_E| = p^2$ and Z_E is a natural module for $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E)) \cong SL_2(p)$.*

Proof. By Lemma 4.10, Z_E is elementary abelian and fully $\mathcal{F}$-automised. Thus as $Z_E \leq Q$, we have $Q/C_Q(Z_E) \cong S/C_E \cong \mathrm{Aut}_S(Z_E) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(Z_E))$, and $\mathrm{Aut}_{\mathcal{F}}(Z_E)$ has elementary abelian Sylow p-subgroups, hence so does $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$. Also recall that $Z_E \leq Z(E)$, so E centralises Z_E, that is $E \leq C_E$.

If $x \in S = EQ$ with $x = eq$ then the action of $c_x \in \mathrm{Aut}_{\mathcal{F}}(Z_E)$ is that of c_q, so let $q \in Q \setminus C_Q(Z_E)$. Thus $1 \neq [Z_E, c_q] \leq Z$, has dimension 1 over $GF(p)$. Further, $C_{Z_E}(c_q) = C_{Z_E}(q)$, and as $|Q : C_Q(q)| = p$, we have $|Z_E : C_{Z_E}(q)| = p$, so c_q acts as a transvection over $GF(p)$ on Z_E. Then $S/C_E \cong \mathrm{Aut}_S(Z_E) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ is generated by transvections and so are its conjugates. Hence, as $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ is generated by its Sylow p-subgroups and all the Sylow p-subgroups are generated by transvections, $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ is generated by transvections.

Then we have $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ that is generated by transvections and has elementary abelian Sylow p-subgroups acting irreducibly on Z_E by Lemma 4.11. Thus we conclude that Z_E is 2-dimensional over $GF(p)$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E)) \cong SL_2(p)$ by Lemma 1.44. $\square$

We can now heavily restrict the structure of S and C_E as follows. Recall that $F_E := \bigcap_{\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)} C_Q(Z_E)\alpha$.

Proposition 4.13. *Assume Hypothesis C and fix $E \in \mathcal{M}$ with $Z_E \leq Q$. Then*

1. *$C_E = C_S(Z_E)$ is maximal in S, $\mathcal{F}$-essential, and $Z(C_E) = Z_E$.*
2. *$\mathrm{Out}_{\mathcal{F}}(C_E)$ acts as a subgroup of $GL_2(p)$ on both C_E/F_E and Z_E. Further, $O^{p'}(\mathrm{Out}_{\mathcal{F}}(C_E)) \cong SL_2(p)$ acts on C_E/F_E as a natural $SL_2(p)$-module. In particular, $|C_E : F_E| = p^2$.*
3. *$|S| = p^6$, $F_E \cong C_p^3$, $\Phi(C_E) \in \{Z_E, F_E\}$, $|S'| = p|\Phi(C_E)|$ and $p^3 \leq |E| \leq p^5$.*

Proof. We begin by considering the extensions of elements of $\mathrm{Aut}_{\mathcal{F}}(Z_E)$ to C_E, and then we consider $\mathrm{Aut}_{\mathcal{F}}(C_E)$ and $C_{\mathrm{Aut}_{\mathcal{F}}(C_E)}(\mathrm{Aut}_{\mathcal{F}}(Z_E))$ and show that $F_E \leq C_E$ is abelian. Finally, we deduce some facts about the structure of S.

Claim 4.13.1. *$C_E = C_S(Z_E)$ is maximal in S, $\mathcal{F}$-essential, and $Z(C_E) = Z_E$.*

Proof of Claim. By Lemma 4.12, we have that $|Z_E| = p^2$, $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E)) \cong SL_2(p)$. Thus, $|Q : C_Q(Z_E)| = |Z_E : Z| = p$ by Lemma 1.10. Therefore, as $C_Q(Z_E)E \leq C_E$, we have $|S : C_E| = p$, and C_E is a maximal subgroup of S.

Let $\phi \in \mathrm{Aut}_{\mathcal{F}}(E)$. By definition, $\mathrm{Aut}_{\mathcal{F}}(E)$ normalises Z_E, so $\phi|_{Z_E} \in \mathrm{Aut}_{\mathcal{F}}(Z_E)$. As Z_E is $\mathcal{F}$-receptive by Lemma 4.10, $\phi|_{Z_E}$ extends to $\bar{\phi} : N_{\phi|_{Z_E}} \to S$. Note $C_S(Z_E) = C_E \leq N_{\phi|_{Z_E}}$ by Lemma 2.8. Then $\widetilde{\phi} := \bar{\phi}|_{C_E} : C_E \to S$. Finally, Z is characteristic in S, so any map in $\mathrm{Aut}_{\mathcal{F}}(S)$ normalises it, hence $N_{\phi|_{Z_E}} < S$, and as C_E is maximal in S, we obtain that $N_{\phi|_{Z_E}} < C_E$.

If $C_E\widetilde{\phi} \neq C_E$ then, as $Z(Z\widetilde{\phi}) \leq Z(C_E)$, we have $(Z\widetilde{\phi})(Z\widetilde{\phi}\widetilde{\phi}) \leq Z(C_E\widetilde{\phi})$. Therefore, $Z\widetilde{\phi} \leq Z(C_E(C_E\widetilde{\phi})) = Z(S)$, a contradiction. Hence, $C_E\widetilde{\phi} = C_E$, $\widetilde{\phi} \in \mathrm{Aut}_{\mathcal{F}}(C_E)$ and $\widetilde{\phi}$ cannot extend to a map in $\mathrm{Aut}_{\mathcal{F}}(S)$, in particular it does not extend to an $\mathcal{F}$-isomorphism between strictly larger subgroups of S. Therefore, the subgroup $H_{C_E} \leq \mathrm{Aut}_{\mathcal{F}}(C_E)$ as in Proposition 2.14, which is generated by those $\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)$ which extend to $\mathcal{F}$-isomorphisms between strictly larger subgroups of S, does not contain $\widetilde{\phi}$, so Proposition 2.14 implies that $H_{C_E} < \mathrm{Aut}_{\mathcal{F}}(C_E)$ and C_E is $\mathcal{F}$-essential.

In particular, $C_E \trianglelefteq S$ is fully $\mathcal{F}$-normalised and, by Theorem 2.7, C_E is fully $\mathcal{F}$-automised. Thus $\mathrm{Out}_{\mathcal{F}}(C_E)$ has Sylow p-subgroups of order p. As $|Q| \geq p^5$ by assumption, $C_Q(Z_E) = C_E \cap Q$ is nonabelian by Lemma 1.17.

Now $Z(C_E) \cap Q \leq Z(C_E \cap Q) = Z_E$ by Lemma 1.10, so if $Z(C_E) \neq Z_E$ we have $Z(C_E) \nleq Q$. In this case $C_E = (C_E \cap Q)Z(C_E)$ and $C_E' = Z$, a contradiction as $\mathrm{Aut}_{\mathcal{F}}(C_E)$ does not normalise Z. Thus we have $Z(C_E) = Z_E$. This completes the proof of part (1). ■

We now study the subgroups $F_E = \bigcap_{\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)} C_Q(Z_E)\alpha$ and $\Phi(C_E) \leq F_E$ of C_E. Note that F_E is elementary abelian, since otherwise, as $F_E \leq Q$, we would have $\Phi(F_E) = Z$ normalised by all $\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)$, a contradiction.

Claim 4.13.2. *$\mathrm{Out}_{\mathcal{F}}(C_E)/C_{\mathrm{Out}_{\mathcal{F}}(C_E)}(Z_E)$ has a subgroup isomorphic to $SL_2(p)$ acting on Z_E as on a natural $SL_2(p)$-module. Further, $O^{p'}(\mathrm{Out}_{\mathcal{F}}(C_E)) \cong SL_2(p)$ acts on C_E/F_E as on a natural $SL_2(p)$-module. In particular, $|C_E : F_E| = p^2$.*

Proof of claim. As $Z_E = Z(C_E)$ is characteristic in C_E, every $\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)$

restricts to $\alpha|_{Z_E} \in \mathrm{Aut}_{\mathcal{F}}(Z_E)$, so $\theta : \mathrm{Aut}_{\mathcal{F}}(C_E) \to \mathrm{Aut}_{\mathcal{F}}(Z_E)$ given by restriction is a homomorphism. Note that θ is surjective, since every $\phi \in \mathrm{Aut}_{\mathcal{F}}(Z_E)$ extends to some $\overline{\phi} : N_\phi \to S$ with $\overline{\phi}\theta = \overline{\phi}|_{Z_E} = \phi$ where $N_\phi \geq C_E$, and if $C_E\overline{\phi} \neq C_E$ then $Z_E\overline{\phi} \neq Z_E$.

Note that $\mathrm{Inn}(C_E) \leq \ker(\theta) = C_{\mathrm{Aut}_{\mathcal{F}}(C_E)}(Z_E)$, so we can consider the projection map $\widetilde{\theta} : \mathrm{Out}_{\mathcal{F}}(C_E) \to \mathrm{Out}_{\mathcal{F}}(Z_E) \cong \mathrm{Aut}_{\mathcal{F}}(Z_E)$. Thus $\mathrm{Out}_{\mathcal{F}}(C_E)/\ker(\widetilde{\theta})$ contains a subgroup isomorphic to $SL_2(p)$. Note that $\ker(\widetilde{\theta}) = C_{\mathrm{Out}_{\mathcal{F}}(C_E)}(Z_E)$. Since $S/C_E \cong \mathrm{Out}_S(C_E) \in \mathrm{Syl}_p(\mathrm{Out}_{\mathcal{F}}(C_E))$ has order p, and $\mathrm{im}(\widetilde{\theta})$ contains a subgroup isomorphic to $SL_2(p)$, $|\ker(\widetilde{\theta})| = |\mathrm{Out}_{\mathcal{F}}(C_E)|/|\mathrm{im}(\widetilde{\theta})|$ is not divisible by p, that is, $\ker(\widetilde{\theta})$ is a p'-group. Note that, by [PS15, Lemma 3.5 and Remark afterwards], $\ker(\widetilde{\theta})$ is not necessarily trivial.

Recall that $1 \neq \Phi(C_E) \leq F_E = \bigcap_{\alpha \in \mathrm{Aut}_{\mathcal{F}}(C_E)} C_Q(Z_E)\alpha$. We consider the action of $\mathrm{Out}_{\mathcal{F}}(C_E)$ on $V := C_E/\Phi(C_E)$, an elementary abelian quotient of order at least p^2.

As C_E is $\mathcal{F}$-essential, $O_p(\mathrm{Out}_{\mathcal{F}}(C_E)) = 1$ so Lemma 2.20 implies that we have $C_{\mathrm{Aut}_{\mathcal{F}}(C_E)}(V) = C_{\mathrm{Aut}_{\mathcal{F}}(C_E)}(C_E/\Phi(C_E)) = \mathrm{Inn}(C_E)$, and $\mathrm{Out}_{\mathcal{F}}(C_E)$ acts faithfully on V. Consider $G := O^{p'}(\mathrm{Out}_{\mathcal{F}}(C_E))$, which is generated by elements of order p, hence contained in $SL(V)$. We have $\mathrm{Out}_S(C_E) \cong S/C_E \cong Q/(Q \cap C_E)$ which does not centralise V, but centralises $C_Q(Z_E)/\Phi(C_E)$ of index p in V. Since $\mathrm{Out}_S(C_E)$ has order p and centralises a hyperplane, its nontrivial elements act on V as transvections over $GF(p)$, hence G is generated by transvections. In particular, $[C_E, Q] = [C_E, \mathrm{Out}_S(C_E)]$ and $S' = C_E'Q'[C_E, Q]$, thus $|S'| = p|\Phi(C_E)|$. Further, G contains a strongly p-embedded subgroup by Lemma 1.61, so Lemma 1.62 implies that $V = V_0 \oplus V_1$, where $|V_1| = p^2$, $G \cong SL_2(p)$, and V_1 is a natural $SL_2(p)$-module for G.

Since $Q/\Phi(C_E) \leq C_V(S)$, we have $V_0 \leq Q$. Thus $V_0 \leq Q \cap C_E$ and is normalised by $\mathrm{Aut}_{\mathcal{F}}(C_E)$, so $V_0 = F_E$, hence $|C_E/F_E| = |Q/F_E| = p^2$. Thus, part (2) is proven. ■

Now F_E is abelian and contained in Q with $|Q| = p^{1+2n}$, so $|Q : F_E| \geq p^n$ by Lemma 1.17, so $n \leq 2$. Since we assumed $|S| \geq p^6$, we have $n \geq 2$, therefore $n = 2$, $|Q| = p^5$ and $|S| = p^6$. In particular, $|F_E| = p^3$ and, as F_E is elementary abelian, we have $F_E \cong C_p^3$.

We have $Z \leq \Phi(C_E)$, so $Z_E \leq \Phi(C_E) \leq F_E$ and $\Phi(C_E) \in \{Z_E, F_E\}$ has order p^2 or p^3, so that $|S'| \in \{p^3, p^4\}$. Finally, E satisfies $Z_E < E \leq C_E$, so that $p^3 \leq |E| \leq p^5$, which completes the proof of the proposition. □

We show C_E plays a similar role to Q in that no proper subgroups can be $\mathcal{F}$-essential.

Lemma 4.14. *Assume Hypothesis C and adopt the notation of Proposition 4.13. If $K \leq C_E$ is $\mathcal{F}$-essential then $K = C_E$. In particular, $E = C_E$.*

Proof. Suppose that $K \leq C_E$ is an $\mathcal{F}$-essential subgroup. We thus have $Z_E < K \leq C_E$. Assume that $\Phi(C_E) = Z_E$. As $[K, Z_E] = 1$, $C_E/C_S(K)$, which is isomorphic to a subgroup of $\mathrm{Aut}(K)$, normalises the subgroups $1 \trianglelefteq Z_E \trianglelefteq K$ and centralises K/Z_E and Z_E, so if $Z_E \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(K)$ then Lemma 1.37 implies that $C_E/C_S(K) \leq O_p(\mathrm{Aut}(K)) = \mathrm{Inn}(K)$. Therefore, if $Z_E \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(K)$, we have $K = C_E$.

If $Z_E \ntrianglelefteq \mathrm{Aut}_{\mathcal{F}}(K)$ then we have $\Phi(C_E) = Z_E \leq K \leq C_E$, so $K \trianglelefteq C_E$ and thus, if $|K| < p^4$, Proposition 1.64 yields a contradiction. Hence $|K| = p^4$ and, as $Z_E \leq Z(K)$ is not characteristic in K, we have $Z(K) > Z_E$, which implies

$K = Z(K)$ by [Gor80, Lemma 1.3.4]. Then, as K is abelian of index p in C_E and $|C_E|' = p^2$, Lemma 1.21 implies that K is the unique abelian subgroup of index p in C_E, hence K is characteristic in C_E. Thus $K \trianglelefteq S$, therefore Proposition 1.64 implies that K is elementary abelian, and Proposition 1.65 implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(K))$ is isomorphic to either $SL_2(p^2)$ or $PSL_2(p^2)$. Let $T \in \mathrm{Syl}_p(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(K)))$. Then, as $|Z(S)| = p$, we have $|C_K(T)| = p$, so that Lemma 1.33 implies that K is a natural $\Omega_4^-(p)$-module for $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(K))$ and every p-element acts on K with Jordan form $J_3 \oplus J_1$. In particular every maximal subgroup M of S containing K has $M' \neq Z(M)$, which contradicts the existence of C_E. Therefore we have $Z_E \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(K)$ and we can conclude that $K = C_E$.

Now assume $\Phi(C_E) = F_E$ and $K < C_E$. Then by Theorem 4.4 $K \not\leq Q$. We have $K \leq M < C_E$ for some maximal subgroup $M \neq C_E \cap Q$ of C_E. As $\Phi(C_E) = F_E$, no maximal subgroup of C_E is normalised by $\mathrm{Out}_{\mathcal{F}}(C_E)$, and $C_E \cap Q$ is the only maximal subgroup of C_E that is normalised by $\mathrm{Out}_S(C_E)$ by Proposition 4.13 (2). Thus M is $\mathcal{F}$-conjugate to $Q \cap C_E$, and K is $\mathcal{F}$-conjugate to some $L \leq Q$ with $Q' = Z \leq L$, hence $L \trianglelefteq Q$. Further, $|N_S(K)| \geq |N_S(L)| \geq |Q|$ since K is fully $\mathcal{F}$-normalised.

Any fully $\mathcal{F}$-normalised subgroup that is $\mathcal{F}$-conjugate to an $\mathcal{F}$-essential subgroup is $\mathcal{F}$-essential, so if $N_S(K) < S$ then $L < Q$ is $\mathcal{F}$-essential too, which contradicts Theorem 4.4. On the other hand if $N_S(K) = S$ we have $K\Phi(C_E) \trianglelefteq S$ so, as $K < C_E$, we have $K\Phi(C_E) < C_E$, hence $M = K\Phi(C_E) = C_E \cap Q$, a contradiction. □

Therefore, if Hypothesis C holds, the situation is as follows.

Proposition 4.15. *Assume Hypothesis C and that $E \in \mathcal{M}$ has $Z_E \leq Q$. Then $|S| = p^6$, $E = C_S(Z_E)$ has order p^5, $Z_E = Z(E)$ with $|Z_E| = p^2$, $\Phi(E) \in \{Z_E, F_E\}$*

and $|S'| = p|\Phi(E)|$*. Further,* $\mathrm{Out}_{\mathcal{F}}(E)$ *acts on* Z_E *and* E/F_E *as a subgroup of* $GL_2(p)$ *containing* $SL_2(p)$*.*

Proof. Follows from Lemmas 4.12, 4.13 and 4.14. $\square$

We note that in $SL_4(p)$ we have E with $Z_E = \Phi(E) = E' = Z(E)$, hence E is special, and in $G_2(p)$ we have E with $\Phi(E) = F_E$. We organise the reduction depending on $\Phi(E)$, and subsequently $|S'|$. We consider $\Phi(E) = F_E$ in Subsection 4.2.1, and $\Phi(E) = Z_E$ in Subsection 4.2.2.

4.2.1 $\Phi(E) = F_E$ leads to a Sylow p-subgroup of $G_2(p)$

If $\Phi(E) = F_E$, we know that $|S'| = p^4$, so, by Lemma 1.26 (1), S has maximal nilpotency class. Hence we show that Q has exponent p and that there is a complement to Q in S in order to apply Proposition 1.32 to conclude that there is a unique p-group with these properties, which is isomorphic to a Sylow p-subgroup of $G_2(p)$.

Lemma 4.16. *Assume Hypothesis C and adopt the notation of Proposition 4.15. If* $\Phi(E) = F_E$ *then* Q *has exponent* p*.*

Proof. As $\Phi(E) = F_E$ we have $|S'| = p|\Phi(E)| = p^4$, so by Lemma 1.26 (1) S has maximal nilpotency class. If Q does not have exponent p then $Q \cong p_-^{1+4}$ and, by Corollary 1.15, there is a characteristic subgroup H of Q of order p^2. Then $H \trianglelefteq S$, but, since S has maximal class, we must have $H = Z_2(S) = Z(E)$ by [Bla58, Lemma 2.2], so $Z_2(S)$ is characteristic in Q, S and E.

In this case $Z_2 := Z_2(S)$ is normalised by the $\mathcal{F}$-automorphism groups of S, Q and E and contained in them. Thus, by Proposition 2.25, if Z_2 is not normal in $\mathcal{F}$, we need some $\mathcal{F}$-essential subgroup K that either does not contain Z_2 or such that $\mathrm{Aut}_{\mathcal{F}}(K)$ does not normalise Z_2.

By Lemma 4.14 if $K \leq E$ then $K = E$, so that $K \not\leq Q$ and $K \not\leq E = C_S(Z_2)$. Then by [Gra18, Lemma 3.4] K is an $\mathcal{F}$-pearl (that is, K is isomorphic to either C_p^2 or p_+^{1+2}), but then [Gra18, Theorem 3.14] implies that Q has exponent p, a contradiction as we were assuming Q had exponent p^2.

Thus Q must have exponent p. □

Proposition 4.17. *Assume Hypothesis C and adopt the notation of Proposition 4.15. If $\Phi(E) = F_E$ then $p \geq 5$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$.*

Proof. If $\Phi(E) = F_E$ then $|S'| = p|\Phi(E)| = p^4$ by Proposition 4.13 (3), so S has maximal class by Lemma 1.26 (1). By Lemma 4.16 Q has exponent p. Now let $\alpha \in \mathrm{Aut}_{\mathcal{F}}(E)$ with $Q \cap E \neq (Q \cap E)\alpha$. Then $(Q \cap E)\alpha \not\leq Q$ so there is an element of order p in $S \setminus Q$ and Q has a complement K in S. Then Proposition 1.32 implies that $p \geq 5$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$. □

In the case above we can therefore use the results of [PS18]. The remaining case has $\Phi(E) = Z_E$.

4.2.2 $\Phi(E) = Z_E$ leads to a Sylow p-subgroup of $SL_4(p)$

Our strategy in this case differs when $p = 3$. We begin by finding an abelian subgroup V of order p^4 and find a complement to V in S. Then if $p \neq 3$ we show that V and hence S has exponent p, and use Lemma 1.26 (2) to determine the upper and lower central series of S, then use Proposition 1.32 to reduce S to either a Sylow p-subgroup of $SL_4(p)$ or one of $SU_4(p)$, the latter of which does not contain a maximal subgroup isomorphic to E.

If $p = 3$ we cannot use the arguments about exponent, so we perform a computer calculation.

Lemma 4.18. *Assume Hypothesis C and adopt the notation of Proposition 4.15. If $\Phi(E) = Z_E$ then there exists $V \trianglelefteq S$ abelian of order p^4 and $\widetilde{\tau} \in \mathrm{Aut}_{\mathcal{F}}(S)$ such that $V = [S, \widetilde{\tau}]$ has a complement $C_S(\widetilde{\tau})$ in S, that is, $S = [S, \widetilde{\tau}] \rtimes C_S(\widetilde{\tau})$. Further, $C_S(\widetilde{\tau})$ is elementary abelian and $V = C_S(S')$ is either elementary abelian or $p = 3$ and $V \cong C_9 \times C_9$.*

Proof. Recall that by Proposition 4.13 (2), $H = O^{p'}(\mathrm{Out}_{\mathcal{F}}(E)) \cong SL_2(p)$, in particular $|Z(H)| = 2$. Choose $\tau \in \mathrm{Aut}_{\mathcal{F}}(E)$ of order 2 such that its image in $\mathrm{Out}_{\mathcal{F}}(E)$ is the central involution of H. As $\Phi(E) = Z_E$, E/Z_E is elementary abelian, so $E/Z_E \cong C_{E/Z_E}(\tau) \times [E/Z_E, \tau]$ by Theorem 1.38. Thus τ inverts E/F_E and since τ has determinant 1, $|C_{E/Z_E}(\tau)| = p$. The restriction of τ to Z_E is central and has order 2 in $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Z_E)) \cong SL_2(p)$ hence it inverts every nontrivial element of Z_E.

Now let V be the preimage in S of $[E/Z_E, \tau]$, then V has order p^4. Then τ acts fixed point freely on V so by [Gor80, Theorem 10.1.4] V is abelian. Note V has index p in E.

Suppose W is abelian of index p in E, then by Lemma 1.21 either we have $V \cap W \leq Z(E)$ of order p^3 or $V = W$. Since $Z(E)$ has order p^2, V is the unique abelian subgroup of index p in E. Thus V is characteristic in E and in particular $V \trianglelefteq S$.

Now consider $\widetilde{\tau} \in \mathrm{Aut}_{\mathcal{F}}(S)$, a lift of τ to S, which exists by Lemma 2.9. Then

$\widetilde{\tau}|_E = \tau$, so that $\widetilde{\tau}|_E\tau^{-1} = 1_{\mathrm{Aut}_{\mathcal{F}}(E)}$.

Note that $\widetilde{\tau}$ acts on $S/E \cong \mathrm{Out}_S(E)$ via a map ψ. Let $\overline{\tau}$ be the image of τ in $\mathrm{Out}_{\mathcal{F}}(E)$ and consider the action of $\gamma = \psi\overline{\tau}^{-1}$ on $\mathrm{Out}_S(E)$. If it is not trivial then $\gamma \in \mathrm{Out}_{\mathcal{F}}(E)$ such that its preimage in $\mathrm{Aut}_{\mathcal{F}}(E)$ does not belong to $\mathrm{Inn}(E)$. Then γ does not act trivially on E. But $\widetilde{\tau}|_E\tau^{-1} = \tau\tau^{-1} = 1_{\mathrm{Aut}_{\mathcal{F}}(E)}$, a contradiction and γ and thus $\widetilde{\tau}$ centralises S/E.

Thus $|C_S(\widetilde{\tau})| = p^2$. By Theorem 1.38 we have $S = C_S(\widetilde{\tau})[S, \widetilde{\tau}]$. Since $\widetilde{\tau}|_V = \tau$, we have that $\widetilde{\tau}$ acts on V by inverting every nontrivial element, and we have $C_S(\widetilde{\tau}) \cap V = 1$, so $S = C_S(\widetilde{\tau})V$ and $C_S(\widetilde{\tau}) \cong S/V$ is a complement to V in S. Note that $S/V = QV/V \cong Q/(V \cap Q)$ is elementary abelian by Lemma 1.27, thus $C_S(\widetilde{\tau})$ is elementary abelian. Thus $S' \leq V$, and since $C_Q(S') = S'$ as $|S'| = p^3$, we have $C_S(S') = V$.

Consider $\Phi(V)$. We have $\Phi(V) \leq \Phi(E) = Z_E$ so $\Phi(V) \in \{1, Z_E\}$. If $\Phi(V) = Z_E$ then $V \cong C_{p^2} \times C_{p^2}$ and there is a subgroup isomorphic to $SL_2(p)$ in $\mathrm{Aut}(V)$, so Proposition 3.4 implies that $p \leq 3$. Thus if $p > 3$ then V is elementary abelian. $\square$

When $p = 3$ we determine the isomorphism type of S computationally.

Lemma 4.19. *Assume Hypothesis C and adopt the notation of Proposition 4.15. If $\Phi(E) = Z_E$ and $p = 3$ then S is isomorphic to a Sylow 3-subgroup of $SL_4(3)$.*

Proof. A Magma algorithm that proves the Lemma is in Appendix C.2. Below we prove that the algorithm does as claimed. We use the SmallGroups library to examine groups of order 3^6 and, using the fact that there is E maximal in S such that $\Phi(E) = E' = Z_E = Z(E)$ of order 3^2 and $|S'| = 3^3$, we reduce to seven candidates which are stored in the sequence C.

By Lemma 4.18 there is a homocyclic subgroup $V = C_S(S')$ of order 3^4. In the notation of the SmallGroups library this means that V is isomorphic to either $C_3^4 \cong <81, 15>$ or $C_9^2 \cong <81, 2>$. Further, we have $S = [S, \tau] \rtimes C_S(\tau)$, that is, there exists an involution in $\mathrm{Aut}(S)$ that centralises exactly nine elements of S, exactly one of which is in V (the identity element of S). This is what we use to prune C to the subsequence CC, which contains one element which we then check is isomorphic to a Sylow p-subgroup of $SL_4(3)$. Thus the code in Appendix C.2 proves the lemma. □

Proposition 4.20. *Assume Hypothesis C and adopt the notation of Lemma 4.15. If $\Phi(E) = Z_E$ then S is isomorphic to a Sylow p-subgroup of $SL_4(p)$.*

Proof. If $p = 3$ this is Lemma 4.19. On the other hand, if $p \neq 3$ then, by Lemma 1.26 (2), $|S'| = p^3$ and S has nilpotency class 3, so S is a regular p-group. By Lemma 4.18 both V and $C_S(\tau)$ have exponent p, so S is generated by elements of order p and thus has exponent p by Theorem 1.7.

Therefore, S contains an extraspecial subgroup $Q \cong p_+^{1+4}$, and a complement K to Q in S. Thus, by Proposition 1.32, S is isomorphic to a Sylow p-subgroup of either $SL_4(p)$ or $SU_4(p)$. But by Lemma 1.34 a Sylow p-subgroup of $SU_4(p)$ does not contain a subgroup isomorphic to E, whereas a Sylow p-subgroup of $SL_4(p)$ does. Thus S is isomorphic to a Sylow p-subgroup of $SL_4(p)$. □

All cases have been checked and the proof of Proposition 4.9 is finished.

4.3 Hypothesis D: every $\mathcal{F}$-essential subgroup $E \in \mathcal{M}$ has $Z_E \nleq Q$

Now we consider the case where Hypothesis D holds, that is, S is a p-group with an extraspecial subgroup Q of index p, where $|S| \geq p^6$ and $Z = Z(S) = Z(Q)$. Further, $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$, and $Z_E \nleq Q$ for all $E \in \mathcal{M}$. In this case we prove the following result.

Proposition 4.21. *Assume Hypothesis D. Let $E \in \mathcal{M}$. Then either S is isomorphic to a Sylow p-subgroup of $SU_4(p)$ and $|E| = p^4$ satisfies $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong PSL_2(p^2)$, or $p \geq 7$, $|E| = p^2$, and $|S| = p^{p-1}$, where S has maximal class and is unique up to isomorphism.*

Outline of proof. We show that E and $\mathrm{Aut}_S(E)$ are elementary abelian, then use Thompson's Replacement Theorem in Lemma 1.53 to obtain that either $E \trianglelefteq S$ or E admits a quadratic action in Lemma 4.22. We then split the discussion according to whether $E \cap Q$ is maximal abelian in Q or not.

In the first case we use Lemma 4.6 to prove $|S| = p^6$ and restrict $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$, then in Proposition 4.23 we determine that S is isomorphic to a Sylow p-subgroup of $SU_4(p)$ with $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong PSL_2(p^2)$.

In the second case we show in Lemma 4.24 that there is a subgroup of $\mathrm{Aut}_{\mathcal{F}}(E)$ generated by transvections, which implies that $|\mathrm{Aut}_S(E)| = p$. Then we bound the order of S and E in Lemma 4.25 and finally in Proposition 4.26 we show that E is an $\mathcal{F}$-pearl and use a result from [Gra18] to determine the order of S before proving uniqueness using Proposition 1.31. $\square$

We begin by showing that E is elementary abelian and splitting the problem into two cases which we will study separately.

Lemma 4.22. *Assume Hypothesis D and let $E \in \mathcal{M}$. Then E and $N_S(E)/E$ are elementary abelian. Either $E \cap Q$ is maximal abelian in Q and $E \trianglelefteq S$, or $E \cap Q < C_Q(E \cap Q)$ and E admits quadratic action.*

Proof. Let $E \in \mathcal{M}$. As $Z \leq \Omega_1(Z(E))$, $Z_E = \langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle \leq \Omega_1(Z(E))$, so Z_E is elementary abelian. If $E = Z_E(E \cap Q)$ is not elementary abelian, we have

$$\begin{aligned} 1 \neq \Phi(E) = E^p E' = & \ (Z_E(E \cap Q))^p [Z_E(E \cap Q), Z_E(E \cap Q)] \\ = & \ \ Z_E^p (E \cap Q)^p (E \cap Q)' \leq \Phi(Q) = Z, \end{aligned}$$

so $Z = \Phi(E)$ is characteristic in E, a contradiction since we assumed $\mathrm{Aut}_{\mathcal{F}}(E)$ moves Z. Thus E is elementary abelian. Note that

$$N_S(E)/E = N_Q(E)E/E \cong N_Q(E)/(E \cap N_Q(E)) = N_Q(E)/(E \cap Q) \leq Q/(E \cap Q)$$

and since $\Phi(Q) = Z \leq E \cap Q$, $N_S(E)/E$ is elementary abelian too.

Now if $C_Q(E \cap Q) > E \cap Q$ then Lemma 1.17 implies that there exists an elementary abelian subgroup $A \leq Q$ with $|A| \geq |E|$, in which case by Lemma 1.53 E admits quadratic action. Otherwise, we must have $C_Q(E \cap Q) = E \cap Q$, that is $E \cap Q$ is maximal abelian in Q, and $E = C_S(E \cap Q) \trianglelefteq N_S(E \cap Q) = S$. □

We first consider the case $C_Q(E \cap Q) = E \cap Q$.

4.3.1 $E \cap Q$ maximal abelian in Q leads to a Sylow p-subgroup of $SU_4(p)$

In this case we have already proven the results that we need.

Proposition 4.23. *Assume Hypothesis D and suppose that $E \in \mathcal{M}$ satisfies $C_Q(E \cap Q) = E \cap Q$. Then S is isomorphic to a Sylow p-subgroup of $SU_4(p)$.*

Proof. By Lemma 4.22, $E \trianglelefteq S$ is elementary abelian so that we can apply Lemma 4.6 to obtain $|S| = p^6$, $E \cong C_p^4$, hence $\mathrm{Aut}_{\mathcal{F}}(E) \leq GL_4(p)$ and, by Proposition 1.65, $A := O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$ is isomorphic to either $SL_2(p^2)$ or $PSL_2(p^2)$. Hence E is an X-module for $X \cong SL_2(p^2)$ of dimension 4 over $GF(p)$, where $Z(X)$ may act trivially. Note that $PSL_2(p^2) \cong \Omega_3(p^2) \cong \Omega_4^-(p)$ and $PSL_2(9) \cong A_6$ by parts (2,5,12) of Proposition 1.19.

Consider $N_{\mathcal{F}}(E)$, which is saturated by Theorem 2.27, and has $E \trianglelefteq N_{\mathcal{F}}(E)$ by definition. As E is $\mathcal{F}$-centric, $N_{\mathcal{F}}(E)$ is constrained, and as A acts transitively on the proper subgroups of S containing E, we have $E = O_p(N_{\mathcal{F}}(E))$. Hence, by the Model Theorem (Theorem 2.29), there exists a model G for $N_{\mathcal{F}}(E)$, that is a finite group G such that $E = O_p(G)$, $S \in \mathrm{Syl}_p(G)$, and $C_G(E) = E$. Then G is a semidirect product of E by $\mathrm{Aut}_G(E)$, where $\mathrm{Aut}_G(E)$ acts faithfully on E, and $O^{p'}(G) \cong E \rtimes O^{p'}(\mathrm{Aut}_G(E)) \cong E \rtimes A$ where, as $|C_E(S/E)| = p$, Lemma 1.33 implies that E is a natural $\Omega_4^-(p)$-module for A.

Let P be a parabolic maximal subgroup of $SU_4(p)$ of shape $C_p^4 : SL_2(p^2) : C_{p-1}$, of which there is a unique conjugacy class by [BHRD13, Table 8.10], and let $R \in Syl_p(P)$. Consider $O^{p'}(P) \cong C_p^4 : SL_2(p^2)$, where we have again that $O_p(P) \cong C_p^4$ is a $GF(p)X$-module of dimension 4, and we have $|Z(R)| = p$ by Proposition 1.32. Hence Lemma 1.33 implies that $\mathrm{Aut}_{O^{p'}(P)}(O_p(P)) \cong SL_2(p^2)$ acts on $O_p(P)$ as a natural $\Omega_4^-(p)$-module.

By Theorem A.13 there is a bijection between the set of equivalence classes of extensions of E by A giving rise to the given action of A on E and the 2-

cohomology $H^2(A, E)$. By [Küs79, Theorem 3.2] $H^2(\Omega_4^-(q), E) = 0$ for all odd q. Thus $O^{p'}(P) \cong O^{p'}(G)$, and in particular S is isomorphic to R and hence to a Sylow p-subgroup of $SU_4(p)$. $\square$

4.3.2 $E \cap Q$ not maximal abelian in Q

In this situation we begin by proving that $|\operatorname{Aut}_S(E)| = p$.

Lemma 4.24. *Assume Hypothesis D and $E \in \mathcal{M}$ with $C_Q(E \cap Q) > E \cap Q$. Then $|\operatorname{Aut}_S(E)| = p$.*

Proof. Let $|E| = p^r$ and assume for a contradiction that $|\operatorname{Aut}_S(E)| \geq p^2$. Since E is elementary abelian by Lemma 4.22, E can be considered as a vector space over $GF(p)$ and so $\operatorname{Aut}_{\mathcal{F}}(E) \leq GL_r(p)$.

Since $C_S(E \cap Q) = EC_Q(E \cap Q)$ and $C_Q(E \cap Q) > E \cap Q$ by assumption, we have $E < C_S(E \cap Q)$, so $N_{C_S(E\cap Q)}(E) > E$. Hence choose $h \in N_{C_S(E\cap Q)}(E) \setminus E$, then $c_h \in \operatorname{Aut}_S(E)$ has order p and centralises $E \cap Q$, so c_h acts on E as a transvection over $GF(p)$. Let $G := \operatorname{Aut}_{\mathcal{F}}(E)$, which contains a strongly p-embedded subgroup H. We consider $N := \langle c_h^{\operatorname{Aut}_{\mathcal{F}}(E)} \rangle \trianglelefteq G$, which is generated by elements with determinant 1, hence $N \leq O^{p'}(\operatorname{Aut}(E)) \cong SL_r(p)$. N is generated by conjugates of a transvection, hence it is generated by transvections and, by Lemma 1.61, N contains a strongly p-embedded subgroup. Then Lemma 1.62 implies that $N \cong SL_2(p)$, in particular $p^2 \nmid |N|$. As $N \trianglelefteq G$, we have $G/(NC_G(N)) \leq \operatorname{Out}(N)$. Further, by [CCN+85, Table 5], we have $|\operatorname{Out}(N)| = 2$, hence $p^2 \mid |NC_G(N)|$. Let $T \in \operatorname{Syl}_p(C_G(N))$ and $P = \langle c_h \rangle \in \operatorname{Syl}_p(N)$, then $N \leq C_G(T) \leq N_G(T)$ and $C_G(N) \leq C_G(P) \leq N_G(P)$, so, by Corollary 1.56 (1), we have $G \leq NC_G(N) \leq N_G(T)N_G(P) \leq H < G$, a contradiction. Therefore, we conclude that $|\operatorname{Aut}_S(E)| = p$. $\square$

We now study the action of E on Q/Z.

Lemma 4.25. *Assume Hypothesis D, and $E \in \mathcal{M}$ with $C_Q(E\cap Q) > E\cap Q$. Then $|E| \leq p^3$, $|S| \leq p^{3+p}$ and elements of E act on Q/Z either trivially or with Jordan form $J_k \oplus L$ where L is trivial if $|E| = p^2$ and $L = J_1$ if $|E| = p^3$.*

Proof. Lemma 4.22 implies that E is elementary abelian, and Lemma 4.24 shows that $|\operatorname{Aut}_S(E)| = p$. Since $E \cap Q$ acts trivially on $Q/(E \cap Q)$, the action of E on $Q/(E \cap Q)$ is that of a cyclic group of order p. We claim that if $e \in E \setminus E \cap Q$ then c_e acts on $Q/(E \cap Q)$, with Jordan form consisting of a single Jordan block. Otherwise, c_e acts with Jordan form $J_k \oplus J$ where J_k is a Jordan block of size k and J is nontrivial. In particular, $C_{Q/(E\cap Q)}(E) = C_{J_k}(E) \oplus C_J(E)$, which has order at least p^2. Let $x, y \in Q$ be such that $x(E \cap Q) \in C_{J_k}(E)$ and $y(E \cap Q) \in C_J(E)$. Then $[E, x] \leq E \cap Q \leq E$, and $[E, y] \leq E \cap Q \leq E$, so $x, y \in N_S(E)$. But then $|N_S(E)/E| \geq p^2$, a contradiction.

Further, $(E \cap Q)/Z$ is centralised by $QE = S$, so the action of e on Q/Z has Jordan form $J_k \oplus J_1 \oplus J_1 \oplus ... \oplus J_1$.

Assume $|E| > p^2$, and consider T, W of order p^2 with $Z \leq T \leq E \cap Q$ and $Z \leq W \leq E \cap Q$. Then T, W are normal in Q and E, hence also in S, thus $C_Q(T)$ and $C_Q(W)$ contain $E \cap Q$. By Lemma 1.10 both $C_Q(T)$ and $C_Q(W)$ have index p in Q, are normal in S, and have $T = Z(C_Q(T))$ and $W = Z(C_Q(W))$ respectively. As the action of e on $Q/(E \cap Q)$ has a single Jordan block, $Q/(E \cap Q)$ is a cyclic S-module, hence Lemma 1.39 implies that it has a unique S-invariant subgroup of index p, thus $C_Q(T) = C_Q(W)$. Then $T = Z(C_Q(T)) = Z(C_Q(W)) = W$. Thus $E \cap Q = T$ and has order p^2. So $|E| \leq p^3$ and $|(E \cap Q)/Z| \leq p$.

Hence $Q/Z = C \oplus D_1$, with C a cyclic module and $|D_1| \leq p$, hence Q/Z

has order at most p^{1+p} as cyclic modules have order at most p^p by Lemma 1.39. Thus $|S| \leq p^{1+p+2}$ and $|E| \leq p^3$, where D_1 is trivial if $|E| = p^2$ and $|D_1| = p$ if $|E| = p^3$. □

And we can now conclude this case.

Proposition 4.26. *Assume Hypothesis D and $E \in \mathcal{M}$ with $C_Q(E \cap Q) > E \cap Q$. Then $p \geq 7$, $|E| = p^2$, $|S| = p^{p-1}$ has maximal class and S is unique up to isomorphism.*

Proof. If $|E| = p^3$ then Lemma 4.25 implies that there is $e \in E \setminus (E \cap Q)$ such that c_e acts on Q/Z with Jordan form $J_k \oplus J_1$. Note that c_e centralises Z, and recall that $C_{\mathrm{Out}(Q)}(Z)$ is isomorphic to a subgroup of $Sp_{2n}(p)$ by Theorem 1.14. But then Theorem 1.25 (2) implies that either $k = 1$, or $c_e \notin Sp_{2n}(p)$, as we have $r_1 = 1$. If $k = 1$ then we have $|S| = p^{1+k+k+1} = p^4$, which contradicts the assumption of $|S| \geq p^6$ from Hypothesis D. In this situation we would also have $C_Q(E \cap Q) = E \cap Q$. Therefore we have $|E| = p^2$.

Then $E \cong C_p \times C_p$ is an $\mathcal{F}$-pearl, so S has maximal class by Proposition 1.3. As Q is extraspecial, [Gra18, Theorem 3.14] implies that $|S| = p^{p-1}$, $p \geq 7$ and S has exponent p. In particular it is a split extension of Q by C_p and then Proposition 1.31 implies that S is unique up to isomorphism. □

4.4 Summary of the reduction

We have covered all cases and we now finish proving the following first Main Theorem, and we also determine the candidates for elements of $\mathcal{M}$.

Theorem 4.27. *Suppose S is a p-group with an extraspecial subgroup Q of index p and $|S| \geq p^6$, let $\mathcal{F}$ be a saturated fusion system on S with $O_p(\mathcal{F}) = 1$, and define*

$$\mathcal{M} := \{E \leq S \mid E \text{ is } \mathcal{F}\text{-essential and } Z \text{ is not normalised by } \operatorname{Aut}_{\mathcal{F}}(E)\}.$$

If S has maximal nilpotency class we define $R := C_S(Z_2(S))$ and

$$\mathcal{P} := \{P_x = \langle Z(S), x\rangle \mid x \in S \setminus (Q \cup R)\}.$$

Then $\mathcal{M}$ is nonempty and S is isomorphic to one of the following.

1. *A Sylow p-subgroup of $SL_4(p)$. In this case $\mathcal{M} \subseteq \{M_1, M_2\}$ where $M_1 \cong M_2$ are the two maximal subgroups of S with $Z(M_i) = M_i'$ of order p^2.*
2. *A Sylow p-subgroup of $SU_4(p)$. In this case $\mathcal{M} = \{V\}$ where V is the unique elementary abelian subgroup of order p^4 in S and $O^{p'}(\operatorname{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$.*
3. *A Sylow p-subgroup of $G_2(p)$ with $p \geq 5$ and $p \neq 7$. Then $\mathcal{M} = \{R\}$.*
4. *A Sylow 7-subgroup of $G_2(7)$, where $\mathcal{M} \subseteq \{R\} \cup \mathcal{P}$.*
5. *The unique p-group of order p^{p-1}, maximal nilpotency class, exponent p and Q extraspecial of index p. In this case $p \geq 11$, and $\mathcal{M} \subseteq \mathcal{P}$.*

If $E \in \mathcal{M}$ and $|E| \neq p^4$ then $O^{p'}(\operatorname{Out}_{\mathcal{F}}(E)) \cong SL_2(p)$.
In all cases Q is the unique extraspecial subgroup of index p in S.
Further, if $E < L$ where $L \in \{Q\} \cup \mathcal{M}$ then E cannot be $\mathcal{F}$-essential.

Proof. We have proved in Propositions 4.9 and 4.21 that S is isomorphic to one of the p-groups above. We now complete the determination of candidates in $\mathcal{M}$ in each of the cases, which is nonempty by Lemma 4.7. Let $E \in \mathcal{M}$, and note that we must have $E \not\leq Q$ by Theorem 4.4. If $|S| = p^6$ then $p^2 \leq |E| \leq p^5$.

If $|S| = p^{p-1}$ we use [Gra18, Theorem 5.4] to obtain that the $\mathcal{F}$-essential candidates are Q, $P \in \mathcal{P}$, or $E \leq R$ with $p^3 \leq |E| \leq p^5$, and if $|E| \geq p^4$ then E is not abelian. Hence $E \in \mathcal{M}$ also satisfies $|E| \leq p^5$ in this case.

If $|E| \leq p^3$ then $Z_E = E \not\leq Q$ so E is abelian and Hypothesis D holds. Since $|S| \geq p^6$ we have $C_Q(E \cap Q) > E \cap Q$, hence Proposition 4.26 implies that we are in the case $|S| = p^{p-1}$ with $|E| = p^2$. Then as $E = C_S(E)$ we have $E \not\leq Q$ and $E \not\leq R$, so $E \in \mathcal{P}$.

If $|E| = p^4$ and $Z_E \leq Q$ then, as $Z_E \leq Z(E)$, we have $E \leq C_S(Z_E) = C_E$. Then Lemma 4.14 implies that $E = C_S(Z_E)$ of order p^5, so this case is not possible. Hence $Z_E \not\leq Q$ and E is elementary abelian by Lemma 4.22, so $Z_2(S) \geq E \cap Q$ and S does not have maximal nilpotency class, so Proposition 4.21 implies that $E \cap Q = C_Q(E \cap Q)$ and S is a Sylow p-subgroup of $SU_4(p)$ with $E \trianglelefteq S$. Then Lemma 1.34 implies that E is the unique abelian subgroup of order p^4 and we denote it by V.

Finally, if $|E| = p^5$ then both cases in Hypothesis C appear, and if Hypothesis D holds then $p = 7$ and S is isomorphic to a Sylow p-subgroup of $G_2(7)$ by Proposition 4.21 and [Gra18, Theorem 5.4].

Thus if S is a Sylow p-subgroup of $SU_4(p)$ then Proposition 4.23 implies that $\mathcal{M} = \{V\}$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$. If $|S| = p^{p-1}$ we have shown $\mathcal{M} \subseteq \mathcal{P}$ unless $p = 7$. Hence parts (2) and (5) are proven.

If S is isomorphic to a Sylow p-subgroup of $SL_4(p)$ then $|E| = p^5$ satisfying $E' = \Phi(E) = Z_E = Z(E)$. There are exactly two maximal subgroups of S with this property by Lemma 1.34, which we will denote by M_1 and M_2. Therefore

$\mathcal{M} \subseteq \{M_1, M_2\}$ in this case and (1) follows. $O^{p'}(\mathrm{Out}_{\mathcal{F}}(M_i)) \cong SL_2(p)$ follows by Proposition 4.13 (2).

Finally, if S is isomorphic to a Sylow p-subgroup of $G_2(p)$ then R is the only candidate when $p \neq 7$ as every other maximal subgroup of S is either Q or a p-group of maximal nilpotency class by [Gra18, Corollary 2.14]. If $p = 7$ we have $|S| = 7^6 = p^{p-1}$ so we can also obtain $\mathcal{F}$-pearls. Hence $\mathcal{M} \subseteq \{R\} \cup \mathcal{P}$. Again Proposition 4.13 (2) implies that $O^{p'}(\mathrm{Out}_{\mathcal{F}}(R)) \cong SL_2(p)$, and finally every $P \in \mathcal{P}$ is isomorphic to $C_p \times C_p$ hence $O^{p'}(\mathrm{Out}_{\mathcal{F}}(P)) \cong SL_2(p)$ by Lemma 1.63.

The uniqueness of Q follows by Lemma 1.26 (1) in cases (3), (4) and (5), and by Lemma 1.26 (2) in cases (1) and (2) of the Theorem.

The final statement follows from Lemma 2.18 (2) if L is abelian and from Theorem 4.4 if $L = Q$. The remaining cases are M_i in a Sylow p-subgroup of $SL_4(p)$ or R in $G_2(p)$, that is Hypothesis C holds and $L = C_E$ whence Lemma 4.14 proves that no proper subgroup can be $\mathcal{F}$-essential.

This completes the proof. $\square$

We have now completed the proof of the Main Theorem, as well as gathered some extra information about $\mathcal{M}$ to be used to classify the fusion systems. Case (1) will be the object of study of future work, with some preliminary results in Chapter 5. Case (2) is studied in Chapter 5 when $p \geq 5$, and [BFM] when $p = 3$. Cases (3) and (4) have been classified in [PS18], and Case (5) is studied in Chapter 6.

CHAPTER 5

FUSION SYSTEMS ON A SYLOW p-SUBGROUP OF $SU_4(p)$

In this chapter we classify, for $p \geq 5$, the saturated fusion systems $\mathcal{F}$ on S a Sylow p-subgroup of $SU_4(p)$ satisfying $O_p(\mathcal{F}) = 1$. We assume this hypothesis and adopt this notation throughout the chapter. The case where $p = 3$ has been studied by Baccanelli, Franchi and Mainardis in [BFM]. This is case (2) of Theorem 4.27.

The Sylow p-subgroups of $SL_4(p)$ and $SU_4(p)$ are very similar, as discussed before Lemma 1.34, in which we establish a way to differentiate between them. Hence we begin the discussion of both p-groups together, determine the $\mathcal{F}$-essential candidates and $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q))$, before determining the fusion systems for each type of group separately. We will refer to case **U** for a Sylow p-subgroup of $SU_4(p)$ and case **L** for a Sylow p-subgroup of $SL_4(p)$.

In case **U** we prove the following.

Theorem 5.1. *Assume $p \geq 5$ and S is a Sylow p-subgroup of $SU_4(p)$. Then there is a one-to-one correspondence between saturated fusion systems $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$ and groups G with $SU_4(p) \leq G \leq \mathrm{Aut}(SU_4(p))$ which realise them. In particular, there are no exotic fusion systems $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$.*

Outline of proof. In Lemma 5.2 we describe S and the p'-structure of $\mathrm{Aut}(S)$ in Lemma 5.3. Then in Proposition 5.5 and Lemma 5.8 we determine the $\mathcal{F}$-essential subgroups to be V and Q. We determine the isomorphism type of $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q))$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ in Lemmas 5.6 and 5.9, and use lifts from these described in Lemmas 5.10 and 5.11 to determine $\mathrm{Aut}^0_{\mathcal{F}}(S)$ in Lemma 5.12. With the information about morphisms obtained thus far, we determine uniqueness of $\mathcal{F}_0 = \langle O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)), O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q)), \mathrm{Aut}^0_{\mathcal{F}}(S)\rangle$ up to isomorphism in Lemma 5.14, and realise it via $PSU_4(p)$ in Lemma 5.15. Finally, Proposition 5.16 concludes the proof. $\square$

5.1 Structure of S for both $SL_4(p)$ and $SU_4(p)$

Let S be in either case **U** or **L**. In Proposition 1.32 we build these two p-groups as semidirect products of $Q \cong p_+^{1+4}$ by an element of $Sp_4(p)$ with Jordan form J_2^2. Note that from the parabolic structure of $SU_4(p)$ and $SL_4(p)$ taken from [BHRD13, Tables 8.8, 8.10] we can also describe S as $V \rtimes T$ where $V \cong C_p^4$ and T is a Sylow p-subgroup of $\Omega_4^-(p)$ in case **U** or $\Omega_4^+(p)$ in case **L**, as described in [PR10, Lemma 2.11]. The following properties of S can be deduced from these descriptions.

Lemma 5.2. *1. The order of S is p^6.*

2. *S has nilpotency class 3, and the terms of its upper and lower central series are $Z := Z(S) = [S,S,S]$ of order p and $Z_2(S) = \Phi(S) = S'$ of order p^3.*

3. *If $p \geq 5$ then S has exponent p.*

4. *Q is the unique maximal subgroup of S with $|Q'| = p$. In particular, Q is the*

unique extraspecial subgroup of index p in S, and Q is characteristic in S.

5. *V is the unique abelian subgroup of order p^4 in S, in particular, V is characteristic in S.*

6. *Let $\mathcal{X} := \{M \leq S \mid V < M < S\}$. Then $|\mathcal{X}| = p+1$, every $M \in \mathcal{X}$ has $|Z(M)| = |M'| = p^2$ and cases **L** and **U** can be distinguished by the structure of $\mathcal{X}$. In case **L** the set $\mathcal{X}$ has two isomorphism classes of subgroups, one with two elements M_1 and M_2 satisfying $Z(M_i) = M_i'$, and the other with the remaining $p-1$ elements which satisfy $Z(M) \neq M'$. In case **U** there is an element of $\mathrm{Aut}(S)$ of order $p+1$ which permutes transitively the elements of $\mathcal{X}$. In particular, the elements of $\mathcal{X}$ are all isomorphic and have $Z(M) \neq M'$.*

7. *Let $M \leq S$ be a maximal subgroup with $M \notin \mathcal{X}$. Then $Z(M) = Z(S)$.*

Proof. Parts (1), (2) and (3) are proved in Proposition 1.32. Parts (5) and (6) are proved in Lemma 1.34. Part (4) follows from part (2), as if there was another maximal subgroup M of S with $|M'| = p$, then $M' = Z$, and $Z(S/Z) \geq Q/Z \cap M/Z$, which has order p^3. This contradicts $|Z_2(S)| = p^3$.

Finally, we turn to part (7). Since $S' \leq M \leq C_S(Z(M))$, we have that $Z(M) \leq C_S(S') = V$, hence $C_S(Z(M)) \geq VM = S$, so $Z(M) = Z(S)$. □

We use this information to describe $\mathrm{Aut}(S)$.

Lemma 5.3. 1. *In case **U**, we have $|\mathrm{Aut}(S)| = p^a 2(p+1)(p-1)^2$ for some $a \in \mathbb{Z}_{\geq 0}$. $\mathrm{Out}_{\mathcal{F}}(S)$ is a subgroup of $\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S) \cong C_{p-1} \times (C_{p^2-1} : C_2)$ up to $\mathrm{Out}(S)$-conjugacy.*

2. *In case **L**, we have $|\mathrm{Aut}(S)| = p^a 2(p-1)^3$ for some $a \in \mathbb{Z}_{\geq 0}$, and $\mathrm{Out}_{\mathcal{F}}(S)$ is $\mathrm{Out}(S)$-conjugate to a subgroup of $\mathrm{Out}_{\mathrm{Aut}(SL_4(p))}(S) \cong C_{p-1} \times (C_{p-1}^2 : C_2)$.*

Proof. Consider the chain $\mathcal{C} : \Phi(S) \trianglelefteq V \trianglelefteq S$ of characteristic subgroups of S. The stabiliser of this chain is a normal p-subgroup of $\mathrm{Aut}(S)$ by Lemma 1.37, and any other element of $\mathrm{Aut}(S)$ acts nontrivially on this chain. In particular, since $|\Phi(S)| = p^3$, $\mathrm{Aut}(S)/C_{\mathrm{Aut}(S)}(\mathcal{C})$ embeds into $GL_1(p) \times GL_2(p)$. To describe which subgroup of $GL_2(p)$ we obtain in each case we consider the action of $\mathrm{Aut}(S)$ on S/V.

In case **U**, Lemma 5.2 (6) implies that all $p+1$ elements of $\mathcal{X}$ are isomorphic with $M' \neq Z(M)$ and there is an element of order $p+1$ permuting them. This element acts transitively on the $p+1$ nontrivial proper subgroups of $S/V \cong C_p^2$, hence its only overgroups in $GL_2(p)$ are either $GL_2(p)$ or contained in $C_{p^2-1} \rtimes C_2$, the normaliser in $GL_2(p)$ of a Singer cycle by [Hup67, II.7.3 and II.8.5]. There are no p-elements in $\mathrm{Aut}(S)/C_{\mathrm{Aut}(S)}(\mathcal{C})$, as one such would normalise some $M \in \mathcal{X}$ and permute transitively the remaining elements N of $\mathcal{X}$, all of which satisfy $N' \neq Z(N)$. Hence the p-element would normalise $C_S(M') \in \mathcal{X} \setminus \{M\}$, a contradiction. Hence $|\mathrm{Aut}(S)|_{p'} \mid 2(p-1)^2(p+1)$. To obtain equality we observe that in $\mathrm{Aut}(SU_4(p))$ we have $|\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S)| = 2(p-1)^2(p+1)$ by [BHRD13, Table 8.10] and [KL90, Table 2.1.C], hence $|\mathrm{Aut}(S)| = p^a 2(p+1)(p-1)^2$ as claimed, and the isomorphism type of $\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S)$ is $C_{p-1} \times (C_{p^2-1} \rtimes C_2)$.

In case **L**, Lemma 5.2 (6) implies that there are two isomorphism classes of maximal subgroups of S containing V, one with 2 elements and the other with the remaining $p-1$, hence $\mathrm{Out}(S)$ embeds into the subgroup of $GL_2(p)$ preserving this structure, which by [Hup67, II.7.2] is isomorphic to $C_{p-1}^2 \rtimes C_2$ acting on S/V. Therefore $|\mathrm{Aut}(S)| \leq p^a 2(p-1)^3$. As before we note that in $\mathrm{Aut}(SL_4(p))$ we have $|\mathrm{Out}_{\mathrm{Aut}(SL_4(p))}(S)| = 2(p-1)^3$, and the isomorphism type of $\mathrm{Out}_{\mathrm{Aut}(SL_4(p))}(S)$ is $C_{p-1} \times (C_{p-1}^2 \rtimes C_2)$.

In both cases $\mathrm{Aut}(S)$ is solvable, and as $\mathrm{Out}_{\mathcal{F}}(S)$ is a p'-group, it is $\mathrm{Out}(S)$-conjugate to a subgroup of $\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S)$ or $\mathrm{Out}_{\mathrm{Aut}(SL_4(p))}(S)$ respectively by Hall's Theorem [Gor80, Theorem 6.4.1]. □

5.2 $\mathcal{F}$-essential subgroups

In this section we complete the determination of the $\mathcal{F}$-essential subgroups of S. Recall that in Theorem 4.27 we described

$$\mathcal{M} := \{E \leq S \mid E \text{ is } \mathcal{F}\text{-essential and } Z \text{ is not normalised by } \mathrm{Aut}_{\mathcal{F}}(E)\}.$$

We proved that in case **L** we have $\mathcal{M} \subseteq \{M_1, M_2\}$ where $Z(M_i) = M_i'$ and $V \leq M_i$, whereas in case **U** we have $\mathcal{M} = \{V\}$. In both cases if $E < L$ where $L \in \{Q\} \cup \mathcal{M}$ then E cannot be $\mathcal{F}$-essential. In particular, any further $\mathcal{F}$-essential subgroups must normalise Z and not be contained in Q.

We begin with a lemma regarding the subgroups from $\mathcal{M}$.

Lemma 5.4. *1. In Case **U**, if $E = V$ is $\mathcal{F}$-essential then $E \in \mathcal{M}$.*

*2. In Case **L**, if $E \in \{M_1, M_2\}$ if $\mathcal{F}$-essential then $E \in \mathcal{M}$.*

Proof. If case **U** holds and $E = V$ is $\mathcal{F}$-essential but $E \notin \mathcal{M}$ then $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ preserves a 1-dimensional subspace and thus embeds into a parabolic subgroup P of shape $p^3 : GL_3(p) : (p-1)$ in $GL_4(p)$, with $|P| = p^6(p^3-1)(p^2-1)(p-1)^2$. However, $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$ by Theorem 4.27, hence $(p^4-1)/2 \mid |O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))|$, but by Zsigmondy's Theorem (Theorem 1.2) there exists a prime q dividing p^4-1 which does not divide $p^k - 1$ for $k < 4$, hence $q \mid |O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))|$ but $q \nmid |P|$, so

$O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ cannot embed into P, a contradiction. Therefore, if V is $\mathcal{F}$-essential, then $V \in \mathcal{M}$.

Now assume case **L** holds and let $M = E = M_i$ for $i \in \{1, 2\}$. Then $Z(M) = M'$ of order p^2 and $V \leq M$ is characteristic in both M and S, so $\mathrm{Out}_{\mathcal{F}}(M)$ embeds into $GL_2(p) \times GL_1(p)$ and Lemma 1.63 then implies $O^{p'}(\mathrm{Out}_{\mathcal{F}}(M)) \cong SL_2(p)$ acts on $M/Z(M)$ by centralising M/V and as a natural $SL_2(p)$-module on $V/Z(M)$.

In particular, there exists $\alpha \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(M))$ of order $p+1$ centralising M/V and acting transitively on the 1-dimensional subspaces of $V/Z(M)$. Therefore $C_{M/Z(M)}(\alpha)$ has order p, and $C_{M/Z(M)}(\alpha) = C_M(\alpha)Z(M)/Z(M)$ by coprime action (Theorem 1.38). Let $m \in C_M(\alpha)$, then $M = \langle V, m \rangle$, and consider the morphism $\theta : V \to Z(M)$ defined by $v\theta = [v, m]$. Then θ is a homomorphism as we have $(vw)\theta = [vw, m] = [v, m]^w[w, m] = [v, m][w, m] = (v\theta)(w\theta)$ for $v, w \in V$ since $[v, m] \in M' = Z(M)$. As α centralises m, we have

$$v\theta\alpha = [v, m]\alpha = [v\alpha, m\alpha] = [v\alpha, m] = v\alpha\theta$$

and so θ preserves the action of α in M. Since $\ker\theta = Z(M)$, it follows that $V/Z(M) \cong Z(M)$ as $\langle\alpha\rangle$-modules. Therefore α acts transitively on the subgroups of $Z(M)$ of order p, in particular $Z\alpha \neq Z$ and $M \in \mathcal{M}$. $\square$

Now we proceed to determine the $\mathcal{F}$-essential subgroups.

Proposition 5.5. *If $E \leq S$ is $\mathcal{F}$-essential and $E \notin \mathcal{M}$ then $E = Q$.*

Proof. Suppose E is $\mathcal{F}$-essential but $E \notin \mathcal{M} \cup \{Q\}$.

If $|E| \leq p^3$ then $|N_S(E)/E| = p$ by Lemmas 1.63 and 1.64, which implies

$|E^S| = |S : N_S(E)| \geq p^2$. Notice that as $Z \leq E$ and $Z_2(S) = S'$, we have

$$EZ_2(S) \leq N_S(E) \trianglelefteq S,$$

so every $F \in E^S$ has $F \leq N_S(E)$. In each case we will find a subgroup of index p^2 in $N_S(E)$ normal in S which is contained in E, which, as $|N_S(E)/E| = p$, shows that we have $|E^S| \leq p+1$, a contradiction. If $|E| = p^2$ then $Z \leq E$ works, whereas if $|E| = p^3$ we can take $E \cap Z_2(S) \trianglelefteq S$, since $[E \cap Z_2(S), S] \leq Z \leq E \cap Z_2(S)$.

If $|E| = p^4$ then as $E \neq V$, E is nonabelian, so by Proposition 3.10 we have $E \cong p_+^{1+2} \times C_p$ and Lemma 1.64 implies that $N_S(E)$ is maximal in S. If $E' \neq Z$ then, as $E' < Z(E)$, we have $Z(E) = ZE' < S'$, so $Z(N_S(E)) = Z(E)$, hence $N_S(E) = C_S(Z(E)) > V$. Then, by the final statement of Theorem 4.27, we cannot have $N_S(E)' = Z(N_S(E))$, which implies that $E' \leq N_S(E)' \cap Z(N_S(E)) = Z$, a contradiction. Thus, we have $E' = Z$, so that $Z_2(S)$ centralises the chain $1 \leq Z \leq E$, which, as $O_p(\mathrm{Out}_{\mathcal{F}}(E)) = 1$, implies $S' = Z_2(S) \leq E$, therefore $E \trianglelefteq S$, a contradiction.

The remaining subgroups have $|E| = p^5$ and are maximal in S. Let $M = E$ be a maximal subgroup of S. If $M \in \mathcal{X}$ then $Z(M) \neq M'$ by Lemma 5.4 with both of order p^2. We therefore have a chain $M' \trianglelefteq Z(M)M' \trianglelefteq C_M(M') \trianglelefteq M$ of characteristic subgroups of M with successive indices p, contradicting Lemma 1.37.

It only remains to consider candidates $M \notin \mathcal{X}$, that is, with $V \nleq M$. Then Lemma 5.2 (7) implies that $Z(M) = Z(S)$. If $\Phi(M) = Z$ then $M' = Z$ hence $M = Q$ by Lemma 5.2 (4). Thus, any remaining maximal subgroup has $\Phi(M) > Z$. If $\Phi(M) = S'$ then S acts trivially on M/S', contradicting Lemma 2.20. Thus $|\Phi(M)| = p^2$. Note that $Z_2(M)$ has index at least p^2 in M, so $S' = Z_2(S) = Z_2(M)$.

We can therefore build a chain $\Phi(M) \trianglelefteq Z_2(M) \trianglelefteq C_M(\Phi(M)) \trianglelefteq M$ each with index p in the next one, contradicting Lemma 1.37. We have now ruled out all subgroups other than Q, hence the proposition follows. $\square$

We now determine $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q))$ when $p \neq 3$ in both cases **L** and **U**.

Lemma 5.6. *Suppose $p \geq 5$ and Q is $\mathcal{F}$-essential. Then $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$ and $Q/Z(Q)$ is a direct sum of two natural $SL_2(p)$-modules.*

Proof. We know $Q/Z(Q)$ is a 4-dimensional faithful $\mathrm{Out}_{\mathcal{F}}(Q)$-module by Lemma 2.20, where $\mathrm{Out}_{\mathcal{F}}(Q) \leq \mathrm{Out}(Q) \cong CSp_4(p) \leq GL_4(p)$ with $\mathrm{Out}_S(Q) \cong S/Q$ of order p. As Q is $\mathcal{F}$-essential, $\mathrm{Out}_{\mathcal{F}}(Q)$ has a strongly p-embedded subgroup, so Corollary 1.56 (3) implies $O_p(\mathrm{Out}_{\mathcal{F}}(Q)) = 1$. Finally, as $Z_2(S) = S'$ of order p^3 and $[S, S, S] = Z$ by Lemma 5.2 (2), we have $C_{Q/Z(Q)}(S) = [Q/Z(Q), S]$ of dimension 2. Hence we can apply Lemma 1.50 to obtain $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$ and $Q/Z(Q)$ is a direct sum of two natural $SL_2(p)$-modules. $\square$

5.3 Natural $\Omega_4^-(p)$-module calculations

Lemma 5.7. *Suppose $G \cong \Omega_4^-(p) \leq GL_4(p)$ acts on the natural $\Omega_4^-(p)$-module V, let $R \in \mathrm{Syl}_p(G)$ and $K = \langle t \rangle$ be a complement to R in $N_G(R)$. Then $|R| = p^2$,*

1. *R preserves exactly p non-degenerate quadratic forms on V up to scalars.*
2. *$V = V_1 \oplus V_2 \oplus V_3$ as a K-module with V_i irreducible, $\dim(V_1) = \dim(V_3) = 1$ and $\dim(V_2) = 2$. $V_3 = C_V(R)$ and $[V, R] = V_2 \oplus V_3$. The element t has order $(p^2 - 1)/2$ and acts as an element of order $p - 1$ on V_1 and V_3, and as an element of order $p + 1$ on V_2.*

3. $C_K(C_V(R)) = \langle t^{p-1} \rangle \cong C_{(p+1)/2}$.

4. *Let* $i = t^{(p^2-1)/4}$ *be the unique involution in* K*. If* $4 \mid p+1$ *then* i *centralises* V_1 *and* V_3 *and inverts* V_2*, whereas if* $4 \mid p-1$ *then* i *centralises* V_2 *and inverts* V_1 *and* V_3*. In either case* i *inverts* R*.*

5. *If* $p \geq 5$ *then there is a unique non-degenerate quadratic form up to a scalar which is preserved by both* R *and* t*.*

Proof. Since $G \cong \Omega_4^-(p)$, it leaves invariant a quadratic form with matrix F. Then as G has type $-$, F has Witt index 1 and [Asc86, 21.2] implies $V = QD$ where Q is a 2-dimensional definite orthogonal space and D a hyperbolic plane. Therefore there is a basis $\{v_1, v_2, v_3, v_4\}$ of V such that [Asc86, 19.2 and 21.1] show that $F = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ where $-\alpha$ generates $GF(p)$, so that every $g \in G$ satisfies $gFg^T = F$ by [Asc86, 19.7]. Fix this basis. Recall that as $\Omega_4^-(p) \cong PSL_2(p^2)$ by Proposition 1.19 (5), we have $|R| = p^2$ and $N_G(R) = R \rtimes K \cong C_p^2 \rtimes C_{(p^2-1)/2}$, and we can find R as lower triangular matrices. We now calculate which lower triangular matrices preserve the quadratic form given by F. Let $a, b, c, d, e, f \in GF(p)$. Then

$$F = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & c & 1 & 0 \\ d & e & f & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & a & b & d \\ 0 & 1 & c & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & a \\ 0 & c & \alpha & b \\ 1 & e & \alpha f & d \end{pmatrix} \begin{pmatrix} 1 & a & b & d \\ 0 & 1 & c & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & c & e+a \\ 0 & c & c^2+\alpha & ec+\alpha f+b \\ 1 & a+e & b+ce+\alpha f & d+e^2+\alpha f^2+d \end{pmatrix}$$

therefore any such matrix satisfies $c = 0$, $e = -a$, $b = -\alpha f$, and $d = -(a^2 + f^2)/2$, so that we have generators $r_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1/2 & -1 & 0 & 1 \end{pmatrix}$ and $r_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -\alpha & 0 & 1 & 0 \\ -\alpha/2 & 0 & 1 & 1 \end{pmatrix}$.
Hence $R = \langle r_1, r_2 \rangle$ is the group of lower triangular matrices preserving F, and by comparing orders we see $R \in \mathrm{Syl}_p(G)$. Note that we can see that with respect to this basis, $C_V(R) = \langle v_4 \rangle$ and $[V, R] = \langle v_2, v_3, v_4 \rangle$. Hence we will denote $V_1 = \langle v_1 \rangle$, $V_2 = \langle v_2, v_3 \rangle$ and $V_3 = \langle v_4 \rangle = C_V(R)$. In particular $[V, R] = V_2 \oplus V_3$.

We now consider how many non-degenerate quadratic forms R leaves invariant. Suppose there is a quadratic form L which is invariant under R, then we have $L = r_i L r_i^T$ for $i = 1, 2$, hence

$$L = \begin{pmatrix} a & b & c & d \\ b & e & f & g \\ c & f & h & i \\ d & g & i & j \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1/2 & -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c & d \\ b & e & f & g \\ c & f & h & i \\ d & g & i & j \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & -1/2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c & d \\ a+b & b+e & c+f & d+g \\ c & f & h & i \\ -a/2-b+d & -b/2-e+g & -c/2-f+i & -d/2-g+j \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & -1/2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a & a+b & c & -a/2-b+d \\ a+b & a+2b+e & c+f & x_1 \\ c & c+f & h & -c/2-f+i \\ -a/2-b+d & x_1 & -c/2-f+i & x_2 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & e & f & g \\ c & f & h & i \\ d & g & i & j \end{pmatrix}$$

where $x_1 = -a/2 - b + d - b/2 - e + g$, $x_2 = -d/2 + e - g - d/2 - g + j$. We see that $a + b = b$, so $a = 0$, then $a + 2b + e = 2b + e = e$, so $b = 0$. Further, since $c + f = f$, we have $c = 0$ too, and as $-c/2 - f + i = i$, we see that $f = 0$ as well. As $x_1 = d - e + g = g$ we deduce $d = e$, and as $x_2 = -d + e - 2g + j = j$, we see that $g = 0$, so that $L = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & h & i \\ d & 0 & i & j \end{pmatrix}$. To determine h, i, j we perform a very similar computation

$$L = r_2 L r_2^T = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & h & h - \alpha d + i \\ d & 0 & -\alpha d + h + i & -\alpha d/2 + h + i - \alpha d/2 + i + j \end{pmatrix}$$

which shows that $h = \alpha d$, $i = 0$, and puts no restrictions on j. Hence the non-degenerate quadratic forms fixed by R have matrix $L = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & \alpha d & 0 \\ d & 0 & 0 & j \end{pmatrix}$, and up to scalars there are p such forms and part (1) holds.

We now consider $N_G(R) = R \rtimes K$ where K is cyclic of order $(p^2-1)/2$, and we claim that $K = \langle t \rangle$ where $t = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$ satisfying $\lambda\gamma = 1$ with λ a primitive element of $GF(p)$. We note that as $t \in G$, $\det(t) = 1$, so that the submatrix $M = \left(\begin{smallmatrix} a & b \\ c & e \end{smallmatrix}\right)$ preserves the quadratic form $N = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ of type $-$ and has determinant 1, hence embeds into $SO_2^-(p) \cong C_{p+1}$ by Proposition 1.19 (3), and can be chosen to have order $p+1$. In order to preserve the form N, it must satisfy $a^2 + b^2\alpha = 1$, $ca + be\alpha = 0$ and $c^2 + e^2\alpha = \alpha$. Hence we have $t^{(p+1)(p-1)/\gcd(p+1,p-1)} = 1$ and t has order $(p^2-1)/2$.

We see $t \in G$ when the above holds as it preserves F:

$$tFt^T = \begin{pmatrix} 0 & 0 & 0 & \lambda\gamma \\ 0 & a^2 + b^2\alpha & ca + be\alpha & 0 \\ 0 & ca + be\alpha & c^2 + e^2\alpha & 0 \\ \lambda\gamma & 0 & 0 & 0 \end{pmatrix} = F.$$

We see that t normalises R as follows:

$$t^{-1}r_1t = \begin{pmatrix} \lambda^{-1} & 0 & 0 & 0 \\ 0 & e & -b & 0 \\ 0 & -c & a & 0 \\ 0 & 0 & 0 & \gamma^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1/2 & -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} =$$

$$\begin{pmatrix} \lambda^{-1} & 0 & 0 & 0 \\ e & e & -b & 0 \\ -c & -c & a & 0 \\ -\gamma^{-1}/2 & -\gamma^{-1} & 0 & \gamma^{-1} \end{pmatrix} \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \lambda e & 1 & 0 & 0 \\ -\lambda c & 0 & 1 & 0 \\ -\lambda\gamma^{-1}/2 & -\gamma^{-1}a & -\gamma^{-1}b & 1 \end{pmatrix}$$

is a lower triangular matrix in G as $t, r_1 \in G$, and therefore $t^{-1}r_1t \in R$ as claimed. A similar calculation works for r_2. Note that we get $e = a$ and $c = -\alpha b$.

Now $t \in N_G(R)$ acts on $V_1 = \langle v_1 \rangle$ and on $V_3 = C_V(R) = \langle v_4 \rangle$ as an element of order $p-1$, and as an element of order $p+1$ on V_2 of order p^2, hence irreducibly. We have shown parts (2) and (3) hold.

We can further see that the action of the involution $i := t^{(p^2-1)/4}$ on V depends on the value of $p \pmod 4$. If $4 \mid p+1$ then $p-1 \mid (p^2-1)/4$ and $p+1 \nmid (p^2-1)/4$, hence $t^{(p^2-1)/4}$ centralises V_1 and V_3 while inverting V_2, whereas if $4 \mid p-1$ the divisibility conditions are swapped, hence $t^{(p^2-1)/4}$ centralises V_2 while inverting V_1 and V_3. Hence $i = \begin{pmatrix} \epsilon & 0 & 0 & 0 \\ 0 & -\epsilon & 0 & 0 \\ 0 & 0 & -\epsilon & 0 \\ 0 & 0 & 0 & \epsilon \end{pmatrix}$, where $\epsilon = 1$ if $4 \mid p+1$ and $\epsilon = -1$ if $4 \mid p-1$. In either case we have $ir_ki = r_k^{-1}$ for $k = 1, 2$, which establishes part (4).

We now consider which quadratic forms are preserved simultaneously by t and R. In part (1) we showed that any non-degenerate quadratic form preserved by R is of the form $L = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & \alpha d & 0 \\ d & 0 & 0 & j \end{pmatrix}$, and we have $t = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$. We calculate

$$L = tLt^T = \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & \alpha d & 0 \\ d & 0 & 0 & j \end{pmatrix} \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & c & 0 \\ 0 & b & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} =$$

$$\begin{pmatrix} 0 & 0 & 0 & \lambda d \\ 0 & ad & \alpha bd & 0 \\ 0 & cd & \alpha de & 0 \\ d\gamma & 0 & 0 & \gamma j \end{pmatrix} \begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & a & c & 0 \\ 0 & b & e & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & \gamma\lambda d \\ 0 & a^2d + \alpha b^2 d & acd + \alpha bde & 0 \\ 0 & acd + \alpha bde & c^2d + \alpha de^2 & 0 \\ \lambda\gamma d & 0 & 0 & \gamma^2 j \end{pmatrix}.$$

The middle 2×2 submatrix is I_2 by the constraints t satisfies, and we only obtain $j = \gamma^2 j$, which must hold for each nonzero $\gamma \in GF(p)$, so unless $p = 3$, we must have $j = 0$.

Therefore $K = \begin{pmatrix} 0 & 0 & 0 & d \\ 0 & d & 0 & 0 \\ 0 & 0 & \alpha d & 0 \\ d & 0 & 0 & 0 \end{pmatrix}$ is the unique non-degenerate quadratic form that is preserved by $N_G(R)$, and d can be chosen to be 1, hence in these circumstances claim (5) holds. $\square$

5.4 Classification of the fusion systems on a Sylow p-subgroup of $SU_4(p)$

At this stage we restrict our attention to case **U**, that is, S is a Sylow p-subgroup of $SU_4(p)$. We show that both remaining candidates Q and V for $\mathcal{F}$-essential subgroups must be $\mathcal{F}$-essential in order to have $O_p(\mathcal{F}) = 1$.

Lemma 5.8. *In case **U**, if $O_p(\mathcal{F}) = 1$ then the $\mathcal{F}$-essential subgroups of S are Q and V.*

Proof. By Theorem 4.27 (2) and Proposition 5.5, the $\mathcal{F}$-essential candidates are Q and V, both of which are characteristic in S, hence normalised by $\mathrm{Aut}_{\mathcal{F}}(S)$. If $L \in \{Q, V\}$ is the only $\mathcal{F}$-essential subgroup then Alperin's Theorem 2.16 shows that $\mathcal{F} = \langle \mathrm{Aut}_{\mathcal{F}}(S), \mathrm{Aut}_{\mathcal{F}}(L)\rangle$, where L is normalised by $\mathrm{Aut}_{\mathcal{F}}(S)$ and $\mathrm{Aut}_{\mathcal{F}}(L)$, hence by Theorem 2.25 we have $L \trianglelefteq \mathcal{F}$, which contradicts $O_p(\mathcal{F}) = 1$. Thus both V and Q are $\mathcal{F}$-essential. $\square$

We now determine $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ and $\mathrm{Aut}^V_{\mathcal{F}}(S)$ as in Definition 2.34.

Lemma 5.9. *Assume case **U** holds. Then $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$ acts on V as a natural $\Omega_4^-(p)$-module. Let $K = \langle t_V\rangle$ be a complement to $\mathrm{Aut}_S(V)$ in $N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))}(\mathrm{Aut}_S(V))$. Then we have:*

1. *t_V acts on Z and V/S' and S'/Z. Furthermore, all the actions are irreducible.*
2. *$\mathrm{Inn}(S)\langle \widetilde{t}_V\rangle = \mathrm{Aut}^V_{\mathcal{F}}(S) \leq \mathrm{Aut}_{\mathcal{F}}(S)$ where $\widetilde{t}_V$ has order $(p^2-1)/2$, $\widetilde{t}_V|_V = t_V$, and $\widetilde{t}_V|_Q \in \mathrm{Aut}_{\mathcal{F}}(Q)$ acting on Z and S/Q as an automorphism of order $p-1$.*

3. *The element* $\widetilde{t_V}^{(p^2-1)/4} \in \mathrm{Aut}_{\mathcal{F}}^V(S)$ *is an involution which centralises* Z *and* V/S' *and inverts* S'/Z *when* $4 \mid p+1$ *whereas when* $4 \mid p-1$ *it centralises* S'/Z *and inverts* Z *and* V/S'*. In both cases it inverts* S/V*.*

Proof. The structure of V as an $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$-module was described in Lemma 5.7. We extract the notation from there. In particular, Lemma 5.7 (2) implies that there is an element t_V generating K and acting on V in the way described in part (1). Note that t_V lifts to an element of $\mathrm{Aut}_{\mathcal{F}}(S)$ by Lemma 2.9, that is, there exists $\widetilde{t_V} \in \mathrm{Aut}_{\mathcal{F}}(S)$ such that $\widetilde{t_V}|_V = t_V \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$, so that $\widetilde{t_V} \in \mathrm{Aut}_{\mathcal{F}}^V(S)$. Then $Z = C_V(S) = C_V(\mathrm{Aut}_S(V)) = V_3$ and $[V,S] = [V, \mathrm{Aut}_S(V)] = S' = V_2 \oplus V_3$ as in Lemma 5.7 (2), so that part (2) follows.

Finally, for part (3), the action of $\widetilde{t_V}^{(p^2-1)/4}$ on V and $S/V \cong \mathrm{Aut}_S(V)$ is described in Lemma 5.7 (4). $\square$

Using very similar arguments, we obtain $C_{\mathrm{Aut}_{\mathcal{F}}^V(S)}(Z)$, which will help us determine $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q))$ uniquely (not just up to conjugacy).

Lemma 5.10. *Fix a subgroup* $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$ *and assume* $p \geq 5$*. Then* $C_{\mathrm{Aut}_{\mathcal{F}}^V(S)}(Z) = \mathrm{Inn}(S)\langle \widetilde{t_V}^{p-1} \rangle$ *where* $\langle \widetilde{t_V}^{p-1} \rangle$ *is cyclic of order* $(p+1)/2$*. The image* u *of the generator* $\widetilde{t_V}^{p-1}$ *acting on* Q/Z *is uniquely determined in a complement* $\mathrm{Out}_{\mathcal{F}}(Q)$ *to* $\mathrm{Inn}(Q)$ *in* $\mathrm{Aut}_{\mathcal{F}}(Q)$ *and is in the* $Sp_4(p)$*-conjugacy class* $B_6(2)$ *of [Sri68].*

Proof. By Lemma 5.7 (3) we have $C_K(C_V(\mathrm{Aut}_S(V))) \cong \langle t_V^{p-1} \rangle \cong C_{(p+1)/2}$, that is, with the notation of Lemma 5.9, a complement to $\mathrm{Aut}_S(V)$ in the subgroup of $N_{\mathrm{Aut}_{\mathcal{F}}(V)}(\mathrm{Aut}_S(V))$ centralising Z and generated by $\widetilde{t_V}^{p-1}$. As $\widetilde{t_V}^{p-1}$ has order $(p+1)/2$ and $p \geq 5$, its eigenvalues are in $GF(p^2) \setminus GF(p)$ and are $\eta^{\pm 2}$, where

$\eta = \theta^{p-1}$ for θ a primitive element of $GF(p^2)$. (This notation is taken from [Sri68], which we will use later to determine the conjugacy class of $\widetilde{t_V}^{p-1}$ in its action on Q/Z.)

Note that the lift $\widetilde{t_V}^{p-1}$ needs to be consistent with the commutator structure of S, and that $\widetilde{t_V}^{p-1}$ restricts to $u := \widetilde{t_V}^{p-1}|_Q \in C_{\mathrm{Aut}(Q)}(Z)$, centralising $S/Q \cong V/S'$. Let $s \in V \setminus S'$, then $su = s$ by Lemma 5.7 (2), and let $q, r \in Q$ and $x \in S'$. We again consider a homomorphism $\theta : Q \to S'/Z$ defined by $q\theta = [q,s]Z$. Then $qr\theta = [qr,s]Z = [q,s]^r[r,s]Z = [q,s][r,s]Z = q\theta r\theta$, hence θ is a homomorphism. Further, θ preserves the action of u as $q\theta u = [q,s]Zu = [qu,su]Z = [qu,s]Z = qu\theta$ since u centralises s and Z. Since $\ker\theta = C_Q(V) = S'$, we conclude that Q/S' and S'/Z are isomorphic as $\langle u \rangle$-modules and the eigenvalues of the projection of u to Q/Z, which are η^2, η^2, η^{-2}, η^{-2}. This determines the conjugacy class of u as an element of $C_{\mathrm{Out}(Q)}(Z) \cong Sp_4(p)$ by Theorem 1.14 to be the class $B_6(2)$ in the notation of [Sri68], which has $|C_{Sp_4(p)}(u)| = p(p+1)(p^2-1) = |GU_2(p)|$. $\square$

We now consider lifts of elements from $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))$ to $\mathrm{Aut}_{\mathcal{F}}(S)$ and when these maps can coincide with the lifts of maps from $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ to $\mathrm{Aut}_{\mathcal{F}}(S)$ determined in Lemmas 5.9 and 5.10.

Lemma 5.11. *Assume $p \geq 5$ and let $K = \langle t_Q \rangle$ be a complement to $\mathrm{Aut}_S(Q)$ in $N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))}(\mathrm{Aut}_S(Q))$. Then $\mathrm{Inn}(S)\langle \widetilde{t_Q} \rangle = \mathrm{Aut}_{\mathcal{F}}^Q(S) \leq \mathrm{Aut}_{\mathcal{F}}(S)$ where the element $\widetilde{t_Q} \in \mathrm{Aut}_{\mathcal{F}}^Q(S)$ has order $p-1$ and $\widetilde{t_Q}|_Q = t_Q$. The projection of t_Q to Q/Z is in the $Sp_4(p)$-conjugacy class $B_3(1,1)$ of [Sri68].*

Proof. By Lemma 5.6, $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$ and acts on Q/Z as a direct sum of two natural $SL_2(p)$-modules. As Q is characteristic in S, Lemma 2.9 implies that there exists a map $\widetilde{t_Q} \in \mathrm{Aut}_{\mathcal{F}}^Q(S)$ satisfying $\widetilde{t_Q}|_Q = t_Q$, whence Lemma 2.37

implies that $\mathrm{Out}_{\mathcal{F}}^{Q}(S) \cong N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))}(\mathrm{Aut}_S(Q))/\mathrm{Aut}_S(Q) \cong C_{p-1}$. As in the proof of Lemma 1.50 we see that t_Q acts on Q/Z as an element of $C_{\mathrm{Aut}(Q)}(Z) \cong Sp_4(p)$ has eigenvalues $\{\lambda, \lambda, \lambda^{-1}, \lambda^{-1}\}$ where $\langle \lambda \rangle = GF(p)$, so that its conjugacy class is given by $B_3(1,1)$ in [Sri68]. $\square$

We now consider the lifts from both $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))$ obtained to $\mathrm{Aut}_{\mathcal{F}}(S)$ together to calculate $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$, which, together with $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$, will generate the fusion system $\mathcal{F}_0$ on S.

Lemma 5.12. *Assume $p \geq 5$ and case **U** holds. Then*

$$\mathrm{Aut}_{\mathcal{F}}^{0}(S) = \mathrm{Inn}(S)\,\mathrm{Aut}_{\mathcal{F}}^{Q}(S)\,\mathrm{Aut}_{\mathcal{F}}^{V}(S) \cong \mathrm{Inn}(S) \rtimes (C_{p-1} \circ_D C_{(p^2-1)/2}),$$

where $D = \mathrm{Aut}_{\mathcal{F}}^{Q}(S) \cap \mathrm{Aut}_{\mathcal{F}}^{V}(S)$ has order $\gcd(4, p+1)/2$.

Proof. Lemma 5.9 yields a group $\langle \widetilde{t_V} \rangle$ with $\mathrm{Inn}(S)\langle \widetilde{t_V} \rangle = \mathrm{Aut}_{\mathcal{F}}^{V}(S) \leq \mathrm{Aut}_{\mathcal{F}}^{0}(S)$ of order $(p^2-1)/2$ such that only the subgroup $C_{\mathrm{Aut}_{\mathcal{F}}^{V}(S)}(Z) = \mathrm{Inn}(S)\langle \widetilde{t_V}^{p-1} \rangle$ studied in Lemma 5.10 centralises Z. Recall that $\widetilde{t_V}^{(p-1)k}$ is in $Sp_4(p)$-conjugacy class $B_6(2k)$, that is its eigenvalues over $GF(p^2)$ are $\{\eta^{2k}, \eta^{2k}, \eta^{-2k}, \eta^{-2k}\}$.

From Lemma 5.11 we similarly get $\langle \widetilde{t_Q} \rangle$ with $\mathrm{Inn}(S)\langle \widetilde{t_Q} \rangle = \mathrm{Aut}_{\mathcal{F}}^{Q}(S) \leq \mathrm{Aut}_{\mathcal{F}}^{0}(S)$ of order $p-1$ which centralises Z. Since the only $\mathcal{F}$-essential subgroups are Q and V, $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$ is generated by $\mathrm{Aut}_{\mathcal{F}}^{Q}(S)$, $\mathrm{Aut}_{\mathcal{F}}^{V}(S)$ and $\mathrm{Inn}(S)$ by definition. It remains to consider $\mathrm{Aut}_{\mathcal{F}}^{Q}(S) \cap \mathrm{Aut}_{\mathcal{F}}^{V}(S)$. Any power of $\widetilde{t_V}$ which coincides with some power of $\widetilde{t_Q}$ must centralise Z, hence is in $C_{\mathrm{Aut}_{\mathcal{F}}^{V}(S)}(Z) = \mathrm{Inn}(S)\langle \widetilde{t_V}^{p-1} \rangle$.

We saw that the action induced by $\widetilde{t_Q}$ on Q/Z is in $Sp_4(p)$-conjugacy class $B_3(1,1)$, that is has eigenvalues $\{\lambda, \lambda, \lambda^{-1}, \lambda^{-1}\}$, so any element $\widetilde{t_V}^{k(p-1)}$ inducing the same action must have its eigenvalues in $GF(p)$. In other words, if θ is a generator of $GF(p^2)$, we must have $\eta^{2k} = \theta^{2k(p-1)} \in GF(p)$. Now $\theta^l \in GF(p)$ when $p+1 \mid l$, so we must have $p+1 \mid 2k(p-1)$. Since $\gcd(p+1, p-1) = 2$, this means $p+1 \mid 4k$, in other words $(p+1)/4 \mid k$. As $k \in \mathbb{Z}$, if $4 \nmid p+1$ (hence $4 \mid p-1$) then only $k = (p+1)/2$ works, but $\widetilde{t_V}^{(p^2-1)/2} = 1_{\mathrm{Aut}_{\mathcal{F}}(S)}$ by Lemma 5.9 (2). On the other hand, if $4 \mid p+1$ then $k = n(p+1)/4 \in \mathbb{Z}$ and $\widetilde{t_V}^{(p^2-1)/4}$ has eigenvalues in $GF(p)$. Furthermore, Lemma 5.9 (3) implies that $\widetilde{t_V}^{(p^2-1)/4}$ centralises Z and S/Q and inverts Q/Z, in other words, it coincides with $\widetilde{t_Q}^{(p-1)/2}$, as seen in the calculation in Lemma 1.50.

Therefore, if $\gcd(4, p+1) = 2$, the only elements of $\mathrm{Aut}_{\mathcal{F}}^{Q}(S)$ and $\mathrm{Aut}_{\mathcal{F}}^{V}(S)$ which can coincide are in $\mathrm{Inn}(S)$, and $\mathrm{Inn}(S)\,\mathrm{Aut}_{\mathcal{F}}^{Q}(S)\,\mathrm{Aut}_{\mathcal{F}}^{V}(S)$ is isomorphic to $\mathrm{Inn}(S) \rtimes (C_{p-1} \times C_{(p^2-1)/2})$ in $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$. On the other hand, if $\gcd(4, p+1) = 4$ then $\mathrm{Aut}_{\mathcal{F}}^{Q}(S)\,\mathrm{Aut}_{\mathcal{F}}^{V}(S) \cong \mathrm{Inn}(S) \rtimes (C_{p-1} \circ_D C_{(p^2-1)/2})$ where $D = \mathrm{Aut}_{\mathcal{F}}^{Q}(S) \cap \mathrm{Aut}_{\mathcal{F}}^{V}(S)$ has order 2. We can also see this as the elements in the $Sp_4(p)$-conjugacy classes $B_6(2)$ and $B_3(1,1)$ both power up to the central involution of $Sp_4(p)$ in these circumstances.

Hence the order and isomorphism type of $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$ is determined. □

We now determine uniqueness of $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$ as a subgroup of $\mathrm{Aut}_{\mathrm{Aut}(SU_4(p))}(S)$.

Lemma 5.13. *There is a unique subgroup H of $\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S)$ isomorphic to $C_{p-1} \times C_{(p^2-1)/2}$. Further, H has two subgroups isomorphic to $C_{p-1} \circ_{C_2} C_{(p^2-1)/2}$, only one of which contains an element of order $(p^2-1)/2$ acting via an element of order $p-1$ on S/Q. In particular, $\mathrm{Aut}_{\mathcal{F}}^{0}(S)$ is uniquely determined as a subgroup of $\mathrm{Aut}_{\mathrm{Aut}(SU_4(p))}(S)$.*

Proof. Since $\mathrm{Aut}_{\mathcal{F}}^{0}(S) \geq \mathrm{Inn}(Q)$ and by Lemma 2.20, we work in the p'-group $\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S)$ via its faithful action on $S/\Phi(S)$. We fix generators x, y, z of

$\mathrm{Out}_{\mathrm{Aut}(SU_4(p))}(S) \cong C_{p-1} \times D_{2(p^2-1)}$ such that

$$\mathrm{Out}_B(S) = \langle x, y, z \mid x^{p-1}, y^{p^2-1}, z^2, y^z = y^{-1} \rangle.$$

As in Lemma 5.3, we see that x acts on S/Q and centralises $Q/\Phi(S)$ whereas $\langle y, z\rangle$ centralises S/Q and act on $Q/\Phi(S) \cong S/V$ as the normaliser in $GL_2(p)$ of a Singer cycle, which is a dihedral group by [Hup67, II.8.4]. We consider subgroups of index 4, noting that $H = \langle x, y^2 \rangle$ is one such.

We also see that since $p > 3$, z does not centralise $y^{(p^2-1)/4}$, hence z is not contained in the subgroups in question. There are three subgroups of index 2 in $\langle x, y\rangle$, which contain $\langle x^2, y^2\rangle$: $H_1 = \langle x^2, y\rangle$, $H_2 = \langle x, y^2\rangle$ and $H_3 = \langle x^2, y^2, xy\rangle$. Now H_1 and H_3 contain an element of order $p^2 - 1$, hence are not of the required shape and thus $H = H_2$ is the unique subgroup of the given isomorphism type. We note that if $4 \mid p - 1$ then uniqueness of $\mathrm{Aut}^0_{\mathcal{F}}(S)$ follows, whereas if $4 \mid p + 1$ we require a bit more work as $|D| = 2$.

In the latter case, we consider subgroups K_i of index 2 in H, which must contain $\langle x^2, y^4\rangle$. Hence there are again 3 such: $K_1 = \langle x^2, y^2\rangle$, $K_2 = \langle x^2, y^4, xy^2\rangle$ and $K_3 = \langle x, y^4\rangle$. Since the ones we are interested are $K_i \cong C_{p-1} \circ_{C_2} C_{(p^2-1)/2}$, such K_i contain an element of order $(p^2 - 1)/2$; hence $K_i \cong C_{(p-1)/2} \times C_{(p^2-1)/2}$. However, K_3 has exponent $(p^2 - 1)/4$; hence it is not an option, but both K_1 and K_2 are isomorphic to $C_{(p-1)/2} \times C_{(p^2-1)/2}$, as required. We again consider the action on $S/\Phi(S)$ to observe that in $\mathrm{Aut}^0_{\mathcal{F}}(S)$ we have an element $\widetilde{t_V}$ which by Lemma 5.9 acts on S/Q as an element of order $p - 1$, whereas in K_1 there is no such element. Thus K_2 is the only subgroup that we can have, and since the element $xy^2 \in K_2$ acts on $S/\Phi(S)$ as desired, and the lemma is complete. □

We finally prove uniqueness of the subsystem $\mathcal{F}_0$.

Lemma 5.14. *If case **U** holds and $p \geq 5$ then $\mathcal{F}_0$ is unique up to isomorphism.*

Proof. We have determined $\mathrm{Aut}_{\mathcal{F}_0}(S) \cong \mathrm{Inn}(S) \rtimes (C_{p-1} \circ_D C_{(p^2-1)/2})$ uniquely as a subgroup of $\mathrm{Aut}_{PSU_4(p)}(S)$ in Lemmas 5.12 and 5.13. Fix this subgroup. Then, since we are determining $\mathcal{F}_0$ up to isomorphism, and by Frattini's Argument $\mathrm{Aut}_{\mathcal{F}_0}(E) = O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(E))N_{\mathrm{Aut}_{\mathcal{F}_0}(E)}(\mathrm{Aut}_S(E))$, we need to determine $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(Q))$ and $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(V))$ uniquely.

As V is characteristic in S, we consider as in Lemma 2.37 the restriction map $\theta : \mathrm{Aut}_{\mathcal{F}_0}(S) \to N_{\mathrm{Aut}_{\mathcal{F}_0}(V)}(\mathrm{Aut}_S(V))$, which is surjective by Lemma 2.9.

Recall that $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(V)) \cong \Omega_4^-(p)$, where $\mathrm{Aut}_S(V) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}_0}(V))$ we see $N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(V))}(\mathrm{Aut}_S(V))$ of order $p^2(p^2-1)/2$. As $\widetilde{t}_V$ is determined uniquely, we have $t_V = \widetilde{t}_V\theta \in N_{\mathrm{Aut}_{\mathcal{F}_0}(V)}(\mathrm{Aut}_S(V))$, hence as $p \geq 5$ Lemma 5.7 (5) implies that there is a unique non-degenerate symmetric form which is preserved by $\mathrm{Aut}_S(V)$ and t_V, that is a unique $\Omega_4^-(p)$ which satisfies the required conditions. Thus $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(V))$ is uniquely determined.

We now turn our attention to Q. Recall that $\mathrm{Out}(Q) \cong CSp_4(p)$ by Theorem 1.14 and that Lemma 5.8 implies that the $\mathcal{F}$-essential subgroups are exactly Q and V and $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q)) \cong SL_2(p)$ by Lemma 5.6. As $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(V)) \cong PSL_2(p^2)$ is uniquely determined, Lemma 5.9 (2) yields a unique element of $\mathrm{Aut}_{\mathcal{F}_0}(Q)$ which acts on Z as an automorphism of order $p-1$, hence we can restrict our attention to $C_{\mathrm{Aut}(Q)}(Z(Q))/\mathrm{Inn}(Q) \cong Sp_4(p)$.

By Lemma 5.10 we have a uniquely determined element $u \in \mathrm{Out}_{\mathcal{F}_0}(Q)$ which acts on Q/Z via a matrix $u \in \mathrm{Out}_{\mathcal{F}_0}(Q)$ in $Sp_4(p)$ with eigenvalues $\{\eta^2, \eta^{-2}, \eta^2, \eta^{-2}\}$ in an extension field $GF(p^2)$, and centralises Z and S/Q.

Since $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q)) \trianglelefteq \mathrm{Out}_{\mathcal{F}_0}(Q)$, u normalises $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q)) \cong SL_2(p)$. As $\mathrm{Aut}(SL_2(p)) \cong PGL_2(p)$ and if $T \in \mathrm{Syl}_p(PGL_2(p))$ then $T = C_{PGL_2(p)}(T)$, and u centralises $\mathrm{Out}_S(Q)$, u centralises $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q))$, and has order $(p+1)/2$ by Lemma 5.10. Hence unless $(p+1)/2 \mid p-1$, which can only hold if $(p+1)/2 \mid 2$, that is $p = 3$, u is in $Sp_4(p)$-conjugacy class $B_6(2)$. As we assume $p \geq 5$, u centralises $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q))$.

Hence by [Sri68] we have $|C_{Sp_4(p)}(u)| = p(p+1)(p^2-1) = |GU_2(p)|$. Note that $C_{Sp_4(p)}(u)$ normalises an extension field, hence it is contained in a maximal subgroup M in Aschbacher's family $\mathscr{C}_3$. Hence, as $p \geq 5$, we deduce from [BHRD13, Table 8.12] that M is a subgroup of shape either $Sp_2(p^2) : C_2$ or $GU_2(p).C_2$, only the second of which has elements of order $(p+1)/2$ centralising a normal subgroup which is isomorphic to $SL_2(p)$. Hence $M \cong GU_2(p).C_2$.

If there was some $H \not\leq M$ containing $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q))$ as a normal subgroup, then $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q)) \trianglelefteq HM = C_{\mathrm{Out}(Q)}(Z) \cong Sp_4(p)$, a contradiction. Hence given u, M is the unique maximal subgroup of $Sp_4(p)$ which can contain both $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q))$ and u with the required properties. Further, note that M contains a unique subgroup isomorphic to $SL_2(p)$, hence $O^{p'}(\mathrm{Out}_{\mathcal{F}_0}(Q))$ is uniquely determined in $\mathrm{Out}(Q)$, and so is $O^{p'}(\mathrm{Aut}_{\mathcal{F}_0}(Q))$.

As $\mathcal{F}_0 = \langle O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)), O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q)), \mathrm{Aut}^0_{\mathcal{F}}(S)\rangle$ by definition, we have shown that fixing $\mathrm{Aut}^0_{\mathcal{F}}(S)$ uniquely determines $\mathcal{F}_0$, and the Lemma is proved. $\square$

At this stage we determine the fusion system of $PSU_4(p)$. Recall that the fusion systems of $SU_4(p)$ and $PSU_4(p)$ coincide by Lemma 2.11.

Lemma 5.15. *$\mathcal{F}_S(PSU_4(p))$ is isomorphic to $\mathcal{F}_0$ whenever $p \geq 5$. In particular $\mathcal{F}_0$ is saturated and $\mathcal{F}_0 = O^{p'}(\mathcal{F})$.*

Proof. By the Borel-Tits Theorem and [GLS98, Corollary 3.1.6], the Alperin-Goldschmidt conjugation family for $PSU_4(p)$ ($\mathcal{F}$-essential family) consists of the subgroups $O_p(P)$ as P ranges over the minimal parabolic subgroups of $PSU_4(p)$.

Note that by [KL90, Table 2.1.D and Proposition 2.3.5], we obtain

$$d := |Z(SU_4(p))| = |SU_4(p)|/|PSU_4(p)| = \gcd(4, p+1).$$

In [BHRD13, Table 8.10] we see two maximal subgroups of $SU_4(p)$ with structure $N_{SU_4(p)}(Q) \sim p^{1+4} : SU_2(p) : C_{p^2-1}$ and $N_{SU_4(p)}(V) \sim C_p^4 : SL_2(p^2) : C_{p-1}$, whose intersection is the Borel subgroup $N_{SU_4(p)}(V)$ of shape $S : (C_{p-1} \times C_{p^2-1})$. Note that these all contain $Z(SU_4(p))$.

We observe now that for $H \in \{S, V, Q\}$, $|N_{PSU_4(p)}(H)/H| = |\operatorname{Out}_{\mathcal{F}_0}(H)|$, and $O^{p'}(\operatorname{Aut}_{PSU_4(p)}(H))$ is isomorphic to $O^{p'}(\operatorname{Aut}_{\mathcal{F}_0}(H))$. Let $X = \operatorname{Aut}(SU_4(p))$. In Lemma 5.3 (1) we proved that $\operatorname{Out}_{\mathcal{F}}(S)$ is $\operatorname{Out}(S)$-conjugate to a subgroup of $\operatorname{Out}_X(S)$, hence the same is true for the respective automisers and, up to conjugacy in $\operatorname{Aut}(S)$, we may assume that $\operatorname{Aut}_{\mathcal{F}_0}(S) \leq \operatorname{Aut}_X(S)$. Therefore Lemma 5.13 determines that $\operatorname{Aut}_{\mathcal{F}_0}(S)^\alpha = \operatorname{Aut}_{PSU_4(p)}(S)$ for some isomorphism $\alpha \in \operatorname{Aut}(S)$. Further, by Lemma 5.14, this determines $\mathcal{F}_S(PSU_4(p))$ uniquely, whence $\mathcal{F}_0^\alpha$ is isomorphic to $\mathcal{F}_S(PSU_4(p))$. In particular $\mathcal{F}_0 \cong \mathcal{F}_0^\alpha$ is saturated, and thus we have $\mathcal{F}_0 = O^{p'}(\mathcal{F})$ $\square$

We have now constructed and realised the unique smallest possible fusion system $\mathcal{F}_0$ with $O_p(\mathcal{F}) = 1$ on S in case **U**. Recall that any saturated fusion system on S with $O_p(\mathcal{F}) = 1$ satisfies $\mathcal{F} = \langle \mathcal{F}_0, \operatorname{Aut}_{\mathcal{F}}(S)\rangle$ by Lemma 2.17. We now consider the largest possible $\operatorname{Aut}_{\mathcal{F}}(S)$, which by Lemma 5.3 has $|\operatorname{Aut}_{\mathcal{F}}(S)| = p^5 2(p+1)(p-1)^2$, to conclude the following.

Proposition 5.16. *Assume S is a Sylow p-subgroup of $SU_4(p)$ and $p \geq 5$. Then there is a one-to-one correspondence between saturated fusion systems $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$ and groups G with $PSU_4(p) \leq G \leq \mathrm{Aut}(PSU_4(p))$ which realise them. In particular, there are no exotic fusion systems $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$.*

Proof. In Lemma 5.14 we uniquely determined $\mathcal{F}_0$ up to isomorphism, which Lemma 5.15 shows is realised by $PSU_4(p)$. We can thus assume

$$\mathrm{Aut}_{\mathcal{F}_0}(S) = \mathrm{Aut}_{PSU_4(p)}(S) \leq \mathrm{Aut}_{\mathrm{Aut}(PSU_4(p))}(S),$$

and for any $\mathcal{F}$ on S with $O_p(\mathcal{F}) = 1$, $\mathrm{Out}_{\mathcal{F}}(S)$ is a subgroup of $\mathrm{Out}_{\mathrm{Aut}(PSU_4(p))}(S)$ containing $\mathrm{Out}_{\mathcal{F}_0}(S)$ by Lemma 5.3, hence $\mathrm{Aut}^0_{\mathcal{F}}(S) \leq \mathrm{Aut}_{\mathcal{F}}(S) \leq \mathrm{Aut}_{\mathrm{Aut}(PSU_4(p))}(S)$, and by Lemma 5.12 and [KL90, Theorem 2.1.4 and Table 2.1.D] we have

$$|\mathrm{Aut}_{\mathrm{Aut}(SU_4(p))}(S)/\mathrm{Aut}^0_{\mathcal{F}}(S)| = 2\gcd(4, p+1) = |\mathrm{Aut}(PSU_4(p))/PSU_4(p)| = 2d.$$

We now note that $\mathcal{F} := \mathcal{F}_S(\mathrm{Aut}(PSU_4(p)))$ is a saturated fusion system with $O_p(\mathcal{F}) = 1$ on S containing $\mathcal{F}_0$ and with $\mathrm{Aut}_{\mathrm{Aut}(PSU_4(p))}(S)$ largest possible. The bijective correspondence $N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))/\mathrm{Aut}_S(E) \cong \mathrm{Out}_{\mathcal{F}}(S)$ from Lemma 2.37 determines also $\mathrm{Aut}_{\mathcal{F}}(E)$ for $E \in \{V, Q\}$ to be largest possible.

Hence Theorem 2.35 implies that there is a one-to-one correspondence between saturated fusion subsystems between $\mathcal{F}_0 \leq \mathcal{E} \leq \mathcal{F}$ and intermediate subgroups $\mathrm{Aut}_{\mathcal{E}}(S)$, each of which is realised by a corresponding intermediate subgroup between $PSU_4(p)$ and $\mathrm{Aut}(PSU_4(p))$, as claimed. Any other saturated fusion system $\mathcal{K}$ on S with $O_p(\mathcal{F}) = 1$ would contain $O^{p'}(\mathcal{K}) \cong \mathcal{F}_0$ by Lemma 5.14, hence it would be one of the above considered. Thus this classification is complete. $\square$

CHAPTER 6

FUSION SYSTEMS ON S OF ORDER p^{p-1}

In this chapter we study the case of Theorem 4.27 (5), that is $p \geq 11$, S has maximal class, order p^{p-1} and exponent p, and Q is the unique extraspecial subgroup of index p in S. In this situation, Proposition 1.31 implies that S is unique up to isomorphism. We note that there are constructions of p-groups which have these properties in [PS15] with $p = m + 4$ and in [LGM02, Example 3.1.5(v)] when $t = (p-1)/2$, hence they are isomorphic to S. From the construction in [LGM02] we see that not all 2-step centralisers coincide, and denote $R := K_{2t-2} = C_S(Z_2(S))$, a maximal subgroup of S with $Q \neq R$.

If $p = 7$ then $|S| = 7^6$ and Proposition 1.32 implies that S is a Sylow p-subgroup of $G_2(7)$, hence it is dealt with in [PS18], and our proof here follows a similar structure as their case when R is not $\mathcal{F}$-essential, in [PS18, Theorems 5.13 and 5.15].

Recall that in Theorem 4.27 (5) we showed that $\mathcal{M} \subseteq \mathcal{P}$ where

$$\mathcal{M} := \{E \leq S \mid E \text{ is } \mathcal{F}\text{-essential and } Z \text{ is not normalised by } \mathrm{Aut}_{\mathcal{F}}(E)\},$$

$$\mathcal{P} := \{P_x = \langle Z(S), x \rangle \mid x \in S \setminus (Q \cup R)\}.$$

We again define

$$\mathcal{X} = \{PS' \mid P \in \mathcal{P}\} = \{M \mid M \text{ is maximal in } S,\ Q \neq M \neq R\}.$$

We now give a sketch of the construction of S following [PS15]. Note that by [PS15, Proposition 2.4] we have $\mathbb{F} = GF(p)$.

Let V_{p-4} be the simple $(p-3)$-dimensional $\mathbb{F}$-vector space of homogeneous polynomials of degree $p-4$ in two variables. As $p-4$ is odd, V_{p-4} can be equipped with an alternating form β_{p-4}, which determines a multiplication making $Q = V_{p-4} \times \mathbb{F}^+$ extraspecial by [PS15, Lemma 2.2] and has order $|Q| = p^{p-2}$.

Define $L = \mathbb{F}^\times \times GL_2(\mathbb{F})$, which acts on V_{p-4} via

$$X^aY^b \cdot (t, \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)) = t(\alpha X + \beta Y)^a(\gamma X + \delta Y)^b, \tag{6.1}$$

and L acts on Q via $(v,z)^{(t,A)} = (t(v \cdot A), t^2(\det A)^{p-4}z)$. We build $P := Q \rtimes L$ with the action of L on Q having kernel $K := C_L(Q) = \{\left(\mu^{-(p-4)}, \left(\begin{smallmatrix} \mu & 0 \\ 0 & \mu \end{smallmatrix}\right)\right) \mid \mu \in \mathbb{F}^\times\}$ by [PS15, Lemma 2.3 (1)]. As $K \leq Z(L)$, we have $K = C_P(S)$. Note that $L/C_L(Q/Z) \cong GL_2(p)$.

Further, we define $B_0 = \mathbb{F}^\times \times \{\left(\begin{smallmatrix} \alpha & 0 \\ \gamma & \delta \end{smallmatrix}\right)\} \leq L$ and $S_0 = \{1\} \times \{\left(\begin{smallmatrix} 1 & 0 \\ \gamma & 1 \end{smallmatrix}\right)\} \leq L$.

Let $S = QS_0 \in \mathrm{Syl}_p(P)$, then we have $N_P(S) = B = QB_0$. Further,

$$\mathrm{Out}_B(S) = N_B(S)/SC_B(S) = B/SK \cong C_{p-1} \times C_{p-1}. \tag{6.2}$$

In particular $(p-1)^2 \mid |\mathrm{Aut}(S)|$. Note that $K = O_{p'}(P)$, so by Lemma 2.11 we have $\mathcal{F}_S(B) = \mathcal{F}_S(B/K)$. We claim S has the properties desired.

We have $|S| = |Q||S_0| = p^{p-1}$. As the action of S_0 on V_{p-4} is indecomposable, the Jordan form of S_0 has a single Jordan block of size $p-3$ and S has maximal class as in Proposition 1.31. As $|S| < p^p$ and Q and S_0 have exponent p, S is regular by Proposition 1.5 (2) and has exponent p by Theorem 1.7.

We now identify certain subgroups that will be important. Let $Z = Z(S)$ of order p, and by [PS15, Lemma 2.3 (ii)] we have

$$Z_2(S) = C_Q(S_0) = \langle (\mu X^{p-4}, \lambda) \mid \lambda, \mu \in \mathbb{F} \rangle$$

of order p^2, and $R := C_S(Z_2(S)) = S_0 C_Q(Z_2(S))$ is maximal in S with $Q \ncong R$ as $|Z(Q)| \neq |Z(R)|$. Further, $\Phi(S) = S' = Q \cap R = C_Q(Z_2(S))$.

We will use the following elements of S: $q := (-Y^{p-4}, 0) \in Q \setminus S'$, and $e := (1, \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)) \in R \setminus S'$ as generators.

Then Q and R are maximal subgroups of S, and any other maximal subgroup has maximal class by [LGM02, Exercise 3.1(1)] or [VLL91, Lemma 1.2]. In particular, Q and R are characteristic in S, and since by (6.2) we have $\mathrm{Out}_B(S) \cong C_{p-1} \times C_{p-1}$ acting faithfully on $S/\Phi(S) \cong C_p^2$, there is an element of order $p-1$ acting transitively on the maximal subgroups of S of maximal class. Thus all $p-1$ maximal subgroups of maximal class must be isomorphic and so $\mathrm{Aut}(S)$ acts transitively on $\mathcal{X}$.

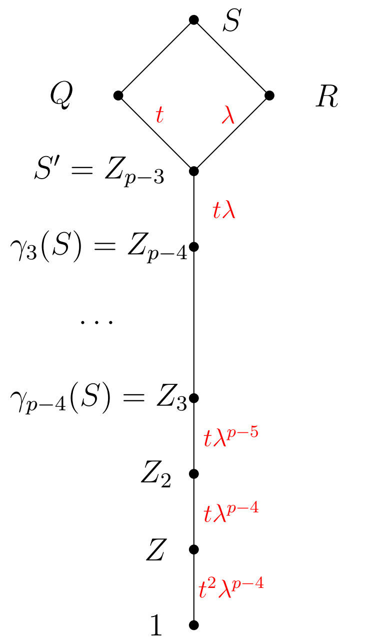


Figure 6.1: Action of $d \in B$ on S

Throughout this chapter we let S be the group just defined. Now we calculate in $\mathrm{Aut}(S)$, generalising [PS18, Lemmas 3.6, 4.8].

Lemma 6.1. *1. $Aut(S)/C_{\mathrm{Aut}(S)}(S/\Phi(S)) \cong C_{p-1} \times C_{p-1}$ is isomorphic to the subgroup of diagonal matrices in $GL_2(p)$. In particular, $|Aut(S)| = p^a(p-1)^2$ for some $a \in \mathbb{Z}_{\geq 0}$ and $\mathrm{Aut}(S) = \mathrm{Aut}_B(S)C_{\mathrm{Aut}(S)}(S/\Phi(S))$.*

2. $\mathrm{Out}_{\mathcal{F}}(S)$ is conjugate in $\mathrm{Out}(S)$ to a subgroup of diagonal matrices in $GL_2(p)$ and we may assume $\mathrm{Out}_{\mathcal{F}}(S) \leq \mathrm{Out}_B(S)$.

3. An element of the form $d = (t, (\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix})) \in B$ with $t, \lambda \in GF(p)^\times$ acts via c_d on S via the map induced by $qc_d = q^t$ and $ec_d = e^\lambda$ where $q := (-Y^{p-4}, 0)$, and $e := (1, (\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}))$. The element d acts on $\gamma_i(S)/\gamma_{i+1}(S)$ as $t\lambda^{i-1}$ for each $i \in \{2, \ldots, p-2\}$ and on Z via $t^2\lambda^{p-4}$.

4. In particular, if a p'-element in $\mathrm{Aut}(S)$ centralises $Z_2(S)$ then it has order dividing $(3, p-1)$.

Proof. Consider the projection $\pi : \mathrm{Aut}(S) \to \mathrm{Aut}(S/\Phi(S))$. Note that as S has maximal class, $\mathrm{Aut}(S/\Phi(S))$ embeds into $GL_2(p)$. Then

$$\ker(\pi) = C_{\mathrm{Aut}(S)}(S/\Phi(S)) \leq O_p(\mathrm{Aut}(S))$$

by Burnside's Theorem (Theorem 1.36). Let $\theta \in \mathrm{Aut}(S)$. Since the maximal subgroups of S are Q, R, and $p-1$ groups of maximal class by [Gra18, Corollary 2.14], $\theta\pi$ normalises the subgroups $Q/\Phi(S)$ and $R/\Phi(S)$, hence acts as diagonal matrices, thus as a subgroup of $C_{p-1} \times C_{p-1}$. By Equation (6.2) we see that $\mathrm{Aut}_B(S)\pi$ is isomorphic to $C_{p-1} \times C_{p-1}$ hence so is $\mathrm{Aut}(S)\pi$. In particular, as $\mathrm{Out}_{\mathcal{F}}(S)$ is a p'-group by saturation, it embeds into $\mathrm{Out}_B(S) \cong C_{p-1}^2$. Further, by Hall's Theorem ([Gor80, Theorem 6.4.1]), as $|\operatorname{Out}(S)| = p^a(p-1)^2$, $\operatorname{Out}_{\mathcal{F}}(S)$ is conjugate in $\operatorname{Out}(S)$ to a subgroup of $\operatorname{Out}_B(S)$. An element $d = (t, (\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}))$ as above acts on $q = (-Y^{p-4}, 0)$ via $qc_d = (-Y^{p-4}, 0)^d = (-tY^{p-4}, 0) = q^t$, and on $e = (1, (\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}))$ as $ec_d = (1, (\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}))^d = (1, (\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix})) = e^\lambda$. Note that $q \in Q \setminus S'$ and $e \in R \setminus S'$ so $S = \langle q, e \rangle$ and we have the following structure.

$s_2 = z_{p-3} := [q, e] \in S' \setminus \gamma_3(S)$ satisfies $s_2c_d = [qc_d, ec_d] = [q^t, e^\lambda] = s_2^{t\lambda}y$ for some $y \in S'$ and $s_i = z_{p-1-i} := [s_{i-1}, e] = [q, e, \dots, e] \in \gamma_i(S) \setminus \gamma_{i+1}(S)$ satisfies $s_ic_d = s_i^{t\lambda^{i-1}}y_i$ for $i \in \{3, \dots, p-3\}$ and some $y_i \in \gamma_{i+1}(S)$. Finally, $z := [q, z_2] \in Z$ satisfies $zc_d = [qc_d, z_2c_d] = [q^t, z_2^{t\lambda^{p-4}}] = z^{t^2\lambda^{p-4}}$.

In particular d acts on $Z_2(S)/Z$ via $\lambda^{p-4}t$ and on Z via $\lambda^{p-4}t^2$ so if it centralises both then $\lambda^{p-4}t^2 = \lambda^{p-4}t = 1$ thus $t = 1$ and $\lambda^{p-4} = 1 = \lambda^{p-1}$, hence $\lambda^3 = 1$ and d has order $(3, p-1)$. $\square$

The action of the element d above will be used to immediately know how any p'-element of $\operatorname{Aut}_{\mathcal{F}}(S)$ acts on the successive quotients of the upper central series of S. We now study the action of $\operatorname{Aut}(S)$ on $\mathcal{X}$ and on $\mathcal{P}$.

Lemma 6.2. *There are $p-1$ S-conjugacy classes in $\mathcal{P}$. $E_1, E_2 \in \mathcal{P}$ are S-conjugate if and only if $E_1S' = E_2S' \in \mathcal{X}$. $\operatorname{Aut}_B(S)$ acts transitively on $\mathcal{P}$ and $\mathcal{X}$.*

Proof. A subgroup E_x of S of order p^2 is in $\mathcal{P}$ if and only if it is not contained in $Q \cup R$, and $E_x = E_{x'}$ if and only if $x' \in E_x \setminus Z$. We thus have, as S has exponent p,

$$|\mathcal{P}| = \frac{|S| - |Q| - |R| + |R \cap Q|}{|E_x| - |Z|} = \frac{p^{p-1} - 2p^{p-2} + p^{p-3}}{p(p-1)} = p^{p-4}(p-1).$$

Let $E \in \mathcal{P}$. Then $N_S(E) = EZ_2$, so $|E^S| = |S : N_S(E)| = p^{p-4}$, hence $\mathcal{P}$ contains $p-1$ S-conjugacy classes of subgroups as claimed. As $E \nleq \Phi(S)$, it is contained in a unique maximal subgroup of S. As $\Phi(S) = S'$ is characteristic in S, two subgroups E_1, E_2 in $\mathcal{P}$ are S-conjugate if and only if E_1S' and E_2S' are S-conjugate, and as they are maximal and normal in S, they coincide. Now by Lemma 6.1 (1) $\mathrm{Aut}(S)$ acts transitively on the maximal subgroups of S distinct from Q and R, so the last claim follows. $\square$

We now complete the determination of the $\mathcal{F}$-essential candidates in a fusion system $\mathcal{F}$ on S.

Proposition 6.3. *Assume $p \geq 11$, S is as above and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. Let E be an $\mathcal{F}$-essential subgroup of S, then $E \in \{Q\} \cup \mathcal{M}$ with $\mathcal{M} \subseteq \mathcal{P}$.*

Proof. We proved that $\mathcal{M} \subseteq \mathcal{P}$ in Theorem 4.27 (5), and if $E \in \mathcal{P}$ is $\mathcal{F}$-essential then Lemma 1.63 implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong SL_2(p)$ and E moves Z, so $E \in \mathcal{M}$. Hence any further $\mathcal{F}$-essential subgroup E normalises Z and if $E \leq Q$ then $E = Q$ by Theorem 4.4. Assume $E \neq Q$, then [Gra18, Lemma 5.3 and Theorem 5.4] imply that $E \leq R$ is one of:

1. $E/Z_2(S) \cong p_+^{1+2}$ with Z not normalised by $\mathrm{Aut}_{\mathcal{F}}(E)$;
2. $E \cong C_p \times p_+^{1+2}$ with $E \cap Q = Z_3(S)$ and $Z(E) = Z_2(S)$; or
3. $E \cong C_p \times C_p \times C_p$.

We will prove that the cases do not happen in three claims.

Claim 6.3.1. *Case (1) does not occur.*

Proof of claim. In Case (1) Z not normalised by $\mathrm{Aut}_{\mathcal{F}}(E)$, hence $E \in \mathcal{M}$, which contradicts Theorem 4.27. ∎

Claim 6.3.2. *Case (2) does not occur.*

Proof of claim. If $|E| = p^4$ then we have $E \cong C_p \times p_+^{1+2}$ and $Z(E) = Z_2(S)$ by the previous discussion. We consider E', of order p. If $E' = Z$ then

$$Z_2(S) = [Z_3(S), S] = [E \cap Q, EQ] = [E \cap Q, E]Z \leq E'Z$$

so $E' \geq Z_2(S)$ of order p^2, a contradiction. Thus $E' \neq Z$ and $Z_2(S) = ZE'$. Now $O^{p'}(\mathrm{Out}_{\mathcal{F}}(E))$ acts faithfully on $E/\Phi(E)$ which has order p^3 and centralises $Z(E)/\Phi(E)$, hence it embeds into $GL_2(p) \times GL_1(p)$ as $O_p(\mathrm{Out}_{\mathcal{F}}(E)) = 1$, thus $O^{p'}(\mathrm{Out}_{\mathcal{F}}(E)) \cong SL_2(p)$ by Lemmas 1.63, 1.64 acting on $E/Z(E)$. Therefore $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))$, which is generated by p-elements which centralise $Z(E)$, centralises $Z(E)$.

Let $\delta \in O^{p'}(\mathrm{Out}_{\mathcal{F}}(E))$ be an element which normalises $\mathrm{Out}_S(E)$ and acts as $\left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ on $E/Z(E)$ of order $p-1$. Then consider a corresponding element $\delta_E \in N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E))}((\mathrm{Aut}_S(E)))$, which acts on E by centralising $Z(E)$ and acting as λ^{-1} on E/Z_3 and λ on Z_3/Z_2. As no overgroups of E are $\mathcal{F}$-essential and $\mathcal{F}$ is saturated, by Alperin's Theorem, δ_E extends to a map in $\overline{\delta} \in \mathrm{Aut}_{\mathcal{F}}(S)$ of order $p-1$ which centralises $Z(E) = Z_2(S)$ as $\overline{\delta}|_E = \delta_E$. However this contradicts Lemma 6.1 (4), hence E cannot be $\mathcal{F}$-essential as $p - 1 \nmid 3$. ∎

It remains to prove that $|E| \neq p^3$, which we do in the following claim.

Claim 6.3.3. *Case (3) does not occur.*

Proof of claim. We have $E \cong C_p^3$ and as $E \cap Q \trianglelefteq EQ = S$, $E \cap Q = Z_2(S)$ so $E \leq R$. Note that no overgroup of E can be $\mathcal{F}$-essential, as $E \nleq Q$ by Claim (2). Recall that Theorem 4.27 (5) implies that $E \notin \mathcal{M}$, that is $\mathrm{Aut}_{\mathcal{F}}(E)$ must normalise

Z. Thus, as $\mathrm{Aut}_S(E)$ is a p-group, it centralises Z. Now as $p \geq 11$, we have $N_S(N_S(E)) > N_S(E)$, so let $x \in N_S(N_S(E))) \setminus N_S(E)$ (note that this fails when $p = 5$, as can be seen in Chapter 7). Then $E \neq E^x \leq N_S(E)$, so $[E, E^x, E^x] = 1$ and as $c_x \in \mathrm{Aut}_S(E)$, the Jordan form of an element of $\mathrm{Aut}_S(E) \leq GL_3(p)$ is $J_2 \oplus J_1$, whence Proposition 1.64 implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong SL_2(p)$. Let τ be the unique involution in $Z(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)))$. Then τ centralises Z and inverts $Z_2(S)/Z$ and $E/Z_2(S)$. As $\tau \in N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$ and there are no $\mathcal{F}$-essential subgroups containing E, τ extends to a map $\widetilde{\tau} \in \mathrm{Aut}_{\mathcal{F}}(S)$. Now let $e \in E \setminus Z_2(S)$, then $e\tau \equiv e^{-1} \pmod{Z}$. Since $E/Z_2(S) = E/(E \cap S') \cong ES'/S' = R/S'$, we observe that $\widetilde{\tau}$ acts on R/S' by inverting every nontrivial element.

Let $z_2 \in Z_2(S) \setminus Z$, then $z_2\widetilde{\tau} = z_2^{-1}z^b$ for some $0 \leq b \leq p-1$. Then, as $C_Q(z_2) = C_Q(Z_2(S)) = S'$, for any $q \in Q \setminus S'$ we have $[q, z_2] = z^a \in Z \setminus 1$ and $q\widetilde{\tau} = q^l y$ for some $1 \leq l \leq p-1$ and $y \in S' = C_Q(Z_2(S))$. Then

$$z^a = z^a\widetilde{\tau} = [q, z_2]\widetilde{\tau} = [q\widetilde{\tau}, z_2\widetilde{\tau}] = [q^l y, z_2^{-1}z^b] = [q^l, z_2^{-1}] = [q, z_2]^{l(p-1)} = z^{al(p-1)},$$

hence $l = -1$ and $\widetilde{\tau}$ inverts Q/S'.

Hence Lemma 6.1 (3) implies that $\widetilde{\tau}$ corresponds to $(-1, \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) \in B$, and using Figure 6.1 we see that $z\widetilde{\tau} = z^{t^2\lambda} = z^{-1}$, a contradiction as $\widetilde{\tau}|_E = \tau$, which centralises Z. ∎

Combining Claims 6.3.1, 6.3.2 and 6.3.3 we conclude that the only candidates for $\mathcal{F}$-essential subgroups are Q or $E \in \mathcal{P}$ as claimed. □

Now we determine $\mathrm{Aut}_{\mathcal{F}}(E)$ for $E \in \mathcal{P}$.

Lemma 6.4. *If $E \in \mathcal{P}$ is $\mathcal{F}$-essential then $\mathrm{Aut}_{\mathcal{F}}(E) = O^{p'}(\mathrm{Aut}(E)) \cong SL_2(p)$ is* *uniquely determined in* $\mathrm{Aut}(E)$. *Let* $\delta = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right)$ *be an element of order* $p-1$ *in* $N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$. *Then* δ *extends to a map* $\widetilde{\delta} \in \mathrm{Aut}_{\mathcal{F}}(S)$ *which acts as conjugation by* $d = (\lambda^{-1}, \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)) \in B$ *and restricts to an element of* $N_{\mathrm{Aut}_{\mathcal{F}}(Q)}(\mathrm{Aut}_S(Q))$ *of order* $p-1$ *which acts as an automorphism of order* $p-1$ *on* S/Q *and* Z. *For every* $E \in \mathcal{P}$ *the subgroup* $\Delta := N_{\mathrm{Aut}_{\mathcal{F}}(S)}(\mathrm{Aut}(E)) \operatorname{Inn}(S)/\operatorname{Inn}(S)$ *is generated by the images of* c_d *as above as* $\lambda \in GF(p)^{\times}$ *independently of the choice of* E.

Furthermore, $\Delta \leq \mathrm{Out}_{\mathcal{F}}(S)$ *is the stabiliser in* $\mathrm{Out}_B(S)$ *of* $\mathcal{X}$ *and has order* $p-1$. *In particular,* $\mathcal{P}$ *is the union of* $(p-1)^2/|\mathrm{Out}_{\mathcal{F}}(S)|$ $\mathcal{F}$*-conjugacy classes of subgroups.*

Proof. As E is $\mathcal{F}$-essential and $\mathrm{Aut}(E) \cong GL_2(p)$, $\mathrm{Aut}_{\mathcal{F}}(E)$ is isomorphic to a subgroup of $GL_2(p)$ with $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong SL_2(p)$ by Lemma 1.63.

Let $N := N_{\mathrm{Aut}_{\mathcal{F}}(E)}(\mathrm{Aut}_S(E))$ of order $p(p-1)$. Let $\delta \in N$ have order $p-1$, then it acts on E/Z via λ^{-1} and on Z via λ for some generator λ of $GF(p)$. As by Proposition 6.3 no overgroup of E is $\mathcal{F}$-essential, Proposition 2.14 implies that δ extends to some $\widetilde{\delta} \in \mathrm{Aut}_{\mathcal{F}}(S)$ with $\widetilde{\delta}|_E = \delta$ and by Lemma 6.1 (2) we may assume that $\widetilde{\delta}$ acts as c_d for some $d = (t, \left(\begin{smallmatrix} \mu & 0 \\ 0 & 1 \end{smallmatrix}\right))$. Then $\widetilde{\delta}$ normalises Q, R and the unique maximal subgroup of S containing E, so $\widetilde{\delta}$ normalises all subgroups of S/S' and acts on S/S' as a scalar matrix. Hence $t = \mu = \lambda^{-1}$ by Lemma 6.1, and $d = (\lambda^{-1}, \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right))$. Note that this is independent of the choice of $E \in \mathcal{P}$.

Further, $\widetilde{\delta}$ restricts to $\overline{\delta} \in \mathrm{Aut}_{\mathcal{F}}(Q)$ as Q is characteristic in S. We define $U := S/Q = EQ/Q \cong E/(E \cap Q) = E/Z$, then the projection of $\overline{\delta}$ to $\mathrm{Out}_{\mathcal{F}}(Q)$ is an element of order $p-1$ normalising U. Now

$$\widetilde{\delta} \in \Delta = N_{\mathrm{Aut}_{\mathcal{F}}(S)}(\mathrm{Aut}(E)) \operatorname{Inn}(S)/\operatorname{Inn}(S) = \bigcap_{X \in \mathcal{X}} N_{\mathrm{Aut}_{\mathcal{F}}(S)}(X) \operatorname{Inn}(S)/\operatorname{Inn}(S),$$

hence $|\Delta| \leq p-1$, and since we obtain $|\langle\widetilde{\delta}\rangle| = p-1$, we have equality at each point E. Thus $\mathrm{Aut}_{\mathcal{F}}(E) \cong SL_2(p)$ and $|\Delta| = p-1$.

The final statements then follow as Δ stabilises $\mathcal{X}$. By Lemma 6.2, since $|\operatorname{Out}_B(S)/\Delta| = p-1$, Δ must be the stabiliser of $\mathcal{X}$ in $\operatorname{Out}_B(S)$. $\square$

Now we determine $\operatorname{Out}_{\mathcal{F}}(Q)$ when Q is $\mathcal{F}$-essential.

Lemma 6.5. *Suppose that Q is $\mathcal{F}$-essential. Then $\operatorname{Out}_{\mathcal{F}}(Q) \cong GL_2(p)$ is unique up to Out(Q)-conjugacy and acts on Q/Z as the module V_{p-4} described in (6.1).*

Proof. Following the notation in [COS17], we let $\mathscr{G}_p$ be the class of finite groups whose Sylow p-subgroups are not normal and have order p. Let $\mathscr{G}_p^\wedge$ be the class of all $G \in \mathscr{G}_p$ such that $|\operatorname{Aut}_G(U)| = p-1$ for $U \in \operatorname{Syl}_p(G)$. Note that as $|U| = p$, $|\operatorname{Aut}(U)| = p-1$, so the assumption is equivalent to $\operatorname{Aut}(U) = \operatorname{Aut}_G(U)$.

Let $G := \operatorname{Out}_{\mathcal{F}}(Q)$, $U := \operatorname{Out}_S(Q) \cong S/Q$. As Q is $\mathcal{F}$-essential, Q is fully $\mathcal{F}$-automised, that is $S/Q \cong U \in \operatorname{Syl}_p(G)$. Further, G contains a strongly p-embedded subgroup, so we have $U \ntrianglelefteq G$, hence $G \in \mathscr{G}_p$. Since $O_p(\mathcal{F}) = 1$, Lema 4.7 implies $\mathcal{M}$ is empty, and by Lemma 6.4 we have $\delta \in N_{\operatorname{Aut}_{\mathcal{F}(Q)}}(\operatorname{Aut}_S(Q))$ acting as $p-1$ on S/Q and Z, hence $|\operatorname{Aut}_G(U)| = p-1$, and $G \in \mathscr{G}_p^\wedge$.

We can therefore use the results from [COS17] to obtain $\operatorname{Out}_{\mathcal{F}}(Q)$. Note that we do not know whether our groups satisfy the conditions of [COS17, Corollary 2.10].

We consider the elementary abelian group $V := Q/Z$. As $Z = \Phi(Q)$, by Lemma 2.20 G acts faithfully on V. Recall that Proposition 1.31 implies that $S = Q \rtimes \langle s\rangle$ where $s \in Sp_{p-3}(p)$ has a single Jordan block of size $p-3$. Hence V is a minimally active, faithful, indecomposable $GF(p)(G)$-module of dimension $p-3 \geq 8$ (as $p \geq 11$).

Let $G_0 = F^*(G)$. Then [COS17, Proposition 5.4] implies that, as $p \geq 11$ and $\dim(V) < p$, the image $\overline{G}$ of G in $PGL(V)$ is almost simple, and $p \mid |F^*(G)|$. These cases are classified in [COS17, Sections 6-11]. In Proposition 6.1 the groups of Lie type in defining characteristic p are considered, with the only example with $|U| = p$ being $PSL_2(p)$, and we obtain the unique simple module $V|_{G_0} \cong V_{p-4}|_{G_0}$, which is exactly the module of homogeneous polynomials of degree $p-4$ in two variables described in [PS15], and can also be described as the $(p-4)$th symmetric power of the natural module (note that it is denoted by V_{p-3} in [COS17]).

The remaining almost simple groups $\overline{G}$ are considered as follows: the case when $\overline{G}$ is sporadic is ruled out by [COS17, Proposition 7.1], the alternating groups are eliminated in [COS17, Proposition 8.1], and the groups of Lie type in cross characteristic are considered in [COS17, Propositions 8.1, 10.1, 10.2, 10.3, 10.4 and 11.1], which rule out the linear, unitary, symplectic, orthogonal and exceptional ones respectively.

Hence V is (isomorphic to) the module described above, and further as in [COS17, Proposition 4.2] as V is simple and even dimensional, we have $G_0 = SL_2(p)$ acting faithfully on V as we require, and $G \leq \overline{G} = N_{\mathrm{Aut}(V)}(G_0) \cong GL_2(p)$.

Note that as $G_0 = O^{p'}(\overline{G}) \leq Sp_{p-3}(p) \cong C_{\mathrm{Aut}(Q)}(Z(Q))$ and by Lemma 6.4 we have $\theta \in N_{\mathrm{Aut}_{\mathcal{F}}(Q)}(\mathrm{Aut}_S(Q))$ acting on Z via an element of order $p-1$, we deduce that $G = \overline{G} \cong GL_2(p)$ and [BHRD13, Proposition 5.3.6] implies that $G = \mathrm{Out}_{\mathcal{F}}(Q)$ is unique up to conjugacy in $\mathrm{Out}(Q)$. Thus we conclude that $G \cong GL_2(p)$, which preserves the symplectic form of Q, is unique up to conjugacy in $\mathrm{Out}(Q) \cong CSp_{p-3}(p)$. $\square$

Now we work with the subsystem $N_{\mathcal{F}}(Q)$ to determine the remaining uniqueness properties.

Lemma 6.6. *Assume Q is $\mathcal{F}$-essential. Then $N_{\mathcal{F}}(Q)$ is uniquely determined up to isomorphism, $\mathcal{F}_S(P/C_L(Q)) = N_{\mathcal{F}}(Q)$, and, in particular, $\mathrm{Aut}_{\mathcal{F}}(Q)$ and $\mathrm{Aut}_{\mathcal{F}}(S)$ are uniquely determined.*

Proof. By Proposition 6.3 the only $\mathcal{F}$-essential candidates are Q and $E \in \mathcal{P}$. Note $Q \trianglelefteq N_{\mathcal{F}}(Q)$, so only Q is $N_{\mathcal{F}}(Q)$-essential by Proposition 2.25. Then Lemma 6.5 implies that $\mathrm{Out}_{\mathcal{F}}(Q) \cong GL_2(p)$ is unique up to $\mathrm{Out}(Q)$-conjugacy, hence $\mathrm{Aut}_{\mathcal{F}}(Q)$ is determined uniquely up to conjugacy in $\mathrm{Aut}(Q)$.

In particular, $N_{\mathrm{Out}_{\mathcal{F}}(Q)}(\mathrm{Out}_S(Q)) \cong C_p : C_{p-1}^2$, and by Lemma 2.9 every map in $N_{\mathrm{Aut}_{\mathcal{F}}(Q)}(\mathrm{Aut}_S(Q))$ extends to a map in $\mathrm{Aut}_{\mathcal{F}}(S) \leq \mathrm{Aut}(S)$ giving us a subgroup of size $\mathrm{Aut}_B(S)$ by Lemma 6.1 (2), hence the order and isomorphism type of $\mathrm{Aut}_{\mathcal{F}}(S)$ is known.

Further, under the assumption that $\mathcal{F}$ is saturated, $N_{\mathcal{F}}(Q)$ is saturated by Theorem 2.27. $N_{\mathcal{F}}(Q)$ is further constrained as $Q \trianglelefteq N_{\mathcal{F}}(Q)$ and Q is $\mathcal{F}$-centric. We have $K = C_B(Q)$, hence by applying the Model Theorem 2.29 we obtain a model $P/C_L(Q)$ for $\mathcal{F}$ which is unique up to isomorphism, hence $N_{\mathcal{F}}(Q) = \mathcal{F}_S(P/C_L(Q))$. Therefore $\mathrm{Aut}_{\mathcal{F}}(S) = \mathrm{Aut}_{P/C_L(Q)}(S) \cong \mathrm{Aut}_B(S)$ is uniquely determined. □

Now we show that if Q is $\mathcal{F}$-essential we obtain a unique fusion system.

Theorem 6.7. *Suppose $p \geq 11$ and Q is $\mathcal{F}$-essential. Then there is a unique saturated fusion system $\mathcal{F}_Q$ on S with $O_p(\mathcal{F}) = 1$ up to isomorphism, which is exotic. Then $\mathcal{F}$ is the fusion system described in [PS15, Proposition 3.5].*

Proof. As $O_p(\mathcal{F}) = 1$, Theorem 4.27 (5) implies that there is $E \in \mathcal{P}$ which is $\mathcal{F}$-essential. As Q is $\mathcal{F}$-essential, Lemma 6.6 implies that $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_B(Q)$

and $\mathrm{Aut}_{\mathcal{F}}(S) = \mathrm{Aut}_B(S)$ are uniquely determined. Since $\mathrm{Aut}_{\mathcal{F}}(S) = \mathrm{Aut}_B(S)$, Lemmas 6.2 and 6.4 imply that $\mathrm{Aut}_{\mathcal{F}}(S)$ acts transitively on $\mathcal{P}$, that is all $E \in \mathcal{P}$ are $\mathcal{F}$-conjugate. Since they are all fully $\mathcal{F}$-normalised, they are all $\mathcal{F}$-essential.

Further, Lemma 6.4 shows that each $E \in \mathcal{P}$ satisfies $\mathrm{Aut}_{\mathcal{F}}(E) = O^{p'}(\mathrm{Aut}(E))$ which is uniquely determined. Thus, there is at most one $\mathcal{F}$ up to isomorphism. It satisfies the conditions of [PS15, Proposition 3.5], hence the fusion system exists, is saturated and exotic. This concludes the case where Q is $\mathcal{F}$-essential. $\square$

It remains to consider the case when Q is not $\mathcal{F}$-essential, which we do as follows. Note that we prove the result before stating it, since the notation is involved and defined throughout the proof.

Assume Q is not $\mathcal{F}$-essential, then the set of $\mathcal{F}$-essential subgroups is a union of conjugacy classes of members of $\mathcal{P}$, and by Lemma 6.2, as each S-conjugacy class of elements of $\mathcal{P}$ is contained in the same maximal subgroup of S, this corresponds to a subset of $\mathcal{X}$. As we can label $\mathcal{X}$ by $M_1, ..., M_{p-1}$, we can identify each configuration with a nonempty subset of $\mathcal{J} = \{1, \ldots, p-1\}$. Recall that by Lemma 6.1 (2), $\mathrm{Aut}_{\mathcal{F}}(S) \leq \mathrm{Aut}_B(S)$ and we have $\Delta \leq \mathrm{Out}_{\mathcal{F}}(S)$ by Lemma 6.4. Now $\mathrm{Out}_B(S)/\Delta$, which has order $p-1$, acts on $\mathcal{X}$ as $C_{p-1} \cong \mathbb{F}_p^\times = GF(p)^\times$. Hence a nonempty subset J of $\mathcal{J}$ determines uniquely a fusion system with $\mathrm{Aut}_{\mathcal{F}}(E) = O^{p'}(\mathrm{Aut}(E))$ if $E \leq M_j$ where $j \in J$, and $\mathrm{Aut}_{\mathcal{F}}(E) = N_{O^{p'}(\mathrm{Aut}(E))}(\mathrm{Aut}_S(E))$ otherwise, all of which is uniquely determined.

Some of the configurations described will give rise to isomorphic fusion systems. This is the case when the subsets J_1, J_2 of $\mathcal{J}$ which determine the $\mathcal{F}$-essential subgroups are $\mathrm{Aut}_B(S)$-conjugate. Hence in order to uniquely determine a fusion system up to isomorphism we require a subset $J \subseteq \mathcal{J}$ corresponding to the S-orbits which are $\mathcal{F}$-essential, and a subgroup of $\mathrm{Aut}_B(S)$ containing Δ and stabilising J. Hence, given an orbit representative J, we define $B_J := Stab_{\mathrm{Aut}_B(S)}(J)$ and

$$\mathcal{F}_0^J = \langle O^{p'}(\mathrm{Aut}(E)), \Delta \mid E \leq M_k, k \in J\rangle,$$

which is the smallest fusion system on S containing the given set of $\mathcal{F}$-essential subgroups by Lemma 2.17.

Finally, we define $\mathcal{F}^J = \langle \mathcal{F}_0^J, B_J\rangle$, which is the largest fusion system with J corresponding to the set of $\mathcal{F}$-essential subgroups. Note $O^{p'}(\mathcal{F}^J) = \mathcal{F}_0^J$, and $\Gamma_{p'}(\mathcal{F}^J) = B_J/\Delta$. Hence the result follows by Theorem 2.35.

With this notation we have showed the first part of the following Theorem.

Theorem 6.8. *Suppose $p \geq 11$, S is as in Theorem 4.27 (5) and Q is not $\mathcal{F}$-essential. Then $\mathcal{F}$ is isomorphic to a subsystem of p'-index of $\mathcal{F}^J$ containing $\mathcal{F}_0^J = O^{p'}(\mathcal{F}^J)$ where J is a nonempty $\mathrm{Aut}(S)$-orbit on $\mathcal{X}$. Furthermore, these fusion systems are saturated and exotic, and no two of them are isomorphic. There are at least $\frac{2^{p-1}-1}{p-1}$ such fusion systems. All these fusion systems are subsystems of the fusion system in Theorem 6.7.*

Proof. It remains to prove saturation and exoticity of $\mathcal{F}^J$. To prove saturation we begin with $\mathcal{E}^J = \langle \mathrm{Aut}_{\mathcal{F}}(S)\rangle \leq \mathcal{F}^J$, which is saturated. Let $\{E_j : j \text{ in } \mathcal{J}\}$ be $\mathcal{F}^J$-conjugacy representatives of the $\mathcal{F}^J$-essential subgroups. As $E_i \in \mathcal{P}$ and E_i is $\mathcal{F}^J$-essential, the E_i are fully $\mathcal{E}^J$-normalised, $\mathcal{E}^J$-centric, and no proper subgroups of the E_i are $\mathcal{F}^J$-centric or $\mathcal{F}^J$-essential. Then $\mathcal{F}^J$ is saturated by [Sem14, Theorem C].

To prove $\mathcal{F}^J$ is exotic, assume $\mathcal{F}^J = \mathcal{F}_S(G)$ for some finite group G with $S \in \mathrm{Syl}_p(G)$, where we may assume $O_{p'}(G) = 1$, as Lemma 2.11 implies that

$\mathcal{F}_S(G) \cong \mathcal{F}_{SO_{p'}(G)/O_{p'}(G)}(G/O_{p'}(G))$. Let N be a minimal normal subgroup of G. Then $1 \neq S \cap N \trianglelefteq S$, so $Z(S) \leq N$. Let $E \in \mathcal{P}$ be $\mathcal{F}^J$-essential. Then $E = \langle Z^{\mathrm{Aut}_{\mathcal{F}}^J(E)} \rangle = \langle Z^{N_G(E)} \rangle \leq N$, where $N_G(E)/C_G(E) \cong SL_2(p)$. Thus

$$ES' = E[E,Q] \leq E[E,S] = \langle E^S \rangle \leq N,$$

therefore $(N \cap N_G(E))C_G(E)/C_G(E)$ contains a Sylow p-subgroup of $N_G(E)/C_G(E)$ and so $N \cap N_G(E) \trianglelefteq N_G(E)$ and $N_G(E)/C_G(E) \cong SL_2(p)$. This implies that $N_G(E) = (N \cap N_G(E))C_G(E)$, hence $\mathcal{F}_S(NS)$ must contain some $\mathcal{F}_0^J$, so by Lemma 6.4 $[S, \mathrm{Out}_{NS}(S)] = S$, that is $S \leq N$ thus $S \in \mathrm{Syl}_p(N)$. Now as $|Z(S)| = p$, N is nonabelian simple and the unique minimal normal subgroup of G, whence Lemma 1.57 implies that G is almost simple. Now as $p \geq 11$, we have $|S| > p^6$ so Proposition B.1 implies that there is no finite simple group N with $S \in \mathrm{Syl}_p(N)$. Therefore $\mathcal{F}^J$ is exotic.

It remains to consider the orbits of the action of $GF(p)^\times$ on the subsets of $GF(p)^\times$, for which we see that there are $2^{p-1} - 1$ nonempty subsets $J \subseteq \mathcal{J}$ to choose from, and each orbit has length at most $p - 1$, hence there are at least $\frac{2^{p-1}-1}{p-1}$ such orbits, hence the same number of saturated fusion systems $\mathcal{F}_0^J$. There is a snippet of Magma code in Appendix C.1 which calculates the number of orbits for a given representatives, but due to the large number of calculations necessary, it is not very fast. It yields 107 fusion systems when $p = 11$, 351 when $p = 13$, 4115 when $p = 17$, and 14601 when $p = 19$, taking over 25 minutes in the latter case. We note that the result appears not to be very far from the lower bound above, which gives 102.3, 341.25, 4096, and 14563.5 respectively, and gives a lower bound of 190650 when $p = 23$, which is too large to calculate. The case $p = 7$ is considered in [PS18, Notation 5.14], where there are 13 orbits whereas our bound gives at least 10.5. □

We note that when $\mathcal{F}$ contains is a unique S-conjugacy class as $\mathcal{F}$-essential subgroups with E a representative, we can construct a saturated fusion system $\mathcal{F}_{N_i} = \langle \mathrm{Aut}_{\mathcal{F}}(E), \mathrm{Aut}_{\mathcal{F}}(S)|_{N_i} \rangle$ on N_i where $N_1 = N_S(E)$ and $N_{i+1} = N_S(N_i)$ for $i \in \{2, \ldots, p-4\}$. Further, in this case, $N_{p-4} = ES'$ is strongly closed in $\mathcal{F}$.

CHAPTER 7

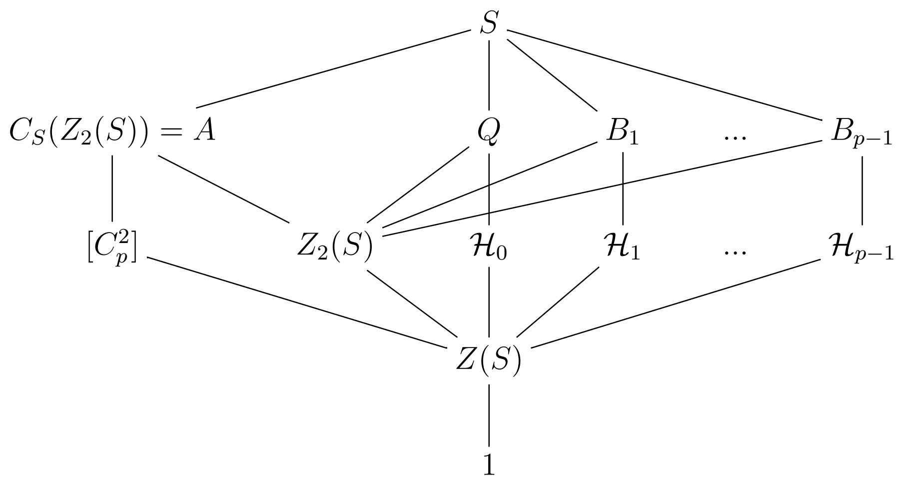
SIMPLE FUSION SYSTEMS WHEN $|S| = p^4$

In this chapter we consider the case when p is odd and $|S| = p^4$. In this case S contains an abelian subgroup of index p by Lemma 1.20. The simple (reduced) fusion systems on S with abelian subgroup of index p have been classified by Oliver, Craven, Semeraro and Ruiz in [Oli14, COS17, OR17]. In [Oli14] the case where the abelian subgroup A of index p is not $\mathcal{F}$-essential was studied, in [COS17] they considered the case where A is $\mathcal{F}$-essential and elementary abelian, and in [OR17] the remaining case was dealt with, but not a classification given. The latter will not be required in our situation. Our goal is to prove the following.

Theorem 7.1. *Assume p is odd, S is a p-group of order p^4 and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. If $\mathcal{F}$ is simple then $\mathcal{F}$ is one of the fusion systems described in Tables 7.1 and 7.2.*

We now establish some notation to synchronise with the results form [Oli14, COS17, OR17] and describe Tables 7.1 and 7.2.

Notation 7.2. We denote by $\mathbf{E}_{\mathcal{F}}$ the set of $\mathcal{F}$-essential subgroups of S, with A being the unique maximal subgroup of S that is abelian. $Q = B_0 \cong p_+^{1+2}$ is the extraspecial subgroup of index p that is normalised by every p'-element of $\mathrm{Aut}(S)$, which exists by [Oli14, Lemma 2.6]. We denote by $B_1, \ldots, B_{p-1}$ the other maximal subgroups of S. They are all extraspecial. $\mathcal{H}_i$ denotes the S-conjugacy class of S-centric subgroups of B_i, which are elementary abelian if they are $\mathcal{F}$-essential. In particular, members of $\mathcal{H}_0$ are subgroups of Q, and we denote $\mathcal{H}_* = \bigcup_{i=1}^{p-1} \mathcal{H}_i$ for the remaining ones. When we write "union of $\mathcal{H}_i$", there are p isomorphism classes of simple fusion systems, each with $\mathbf{E}_\mathcal{F}$ consisting a different number of conjugacy classes $\mathcal{H}_0 \cup \mathcal{H}_*$, none of which are $\mathcal{F}$-conjugate. The cases are labelled J.(x) where J = I when $A \notin \mathbf{E}_\mathcal{F}$ and J=II otherwise, and (x) refers to the subsection of [Oli14, Theorem 2.8] and [COS17, Theorem 2.8 and Table 2.1] in which they are described. If $\mathcal{F}$ is realisable, $\mathcal{F}_l$ represents its name in Proposition B.1 and Table B.1. S is given in the SmallGroups notation, for example $<3^4, 7> \cong C_3 \wr C_3$, $<p^4, 7> \in \mathrm{Syl}_p(Sp_4(p))$. The lattice of conjugacy classes subgroups of S containing $Z = Z(S)$ is described in the following picture.



p	Case	S	$E \in \mathbf{E}_{\mathcal{F}} \cup \{S\}$	$\mathrm{Out}_{\mathcal{F}}(E)$	Realisable or exotic
3,5	I.(a)(i)	$<3^4, 9>$, $<5^4, 7>$	$\mathcal{H}_0$	$SL_2(p)$	$\mathcal{F}_a$, $PSU_3(8)$ if $p = 3$, all $\mathcal{H}_i$ $\mathcal{F}$-essential Exotic otherwise
			Union of $\mathcal{H}_i$	$SL_2(p)$	
			S	C_{p-1}	
3,5	I.(a)(ii)	$<3^4, 9>$, $<5^4, 7>$	Q	$GL_2(p)$	$\mathcal{F}_b$, ${}^3D_4(2)$ for $p = 3$ Exotic for $p = 5$ from [PS15]
			$\mathcal{H}_*$	$SL_2(p)$	
			S	C_{p-1}^2	
$p \geq 7$	I.(a)(iv)	$<p^4, 7>$	$\mathcal{H}_0$	$SL_2(p)$	Exotic
			S	C_{p-1}	
3	I.(b)	$<3^4, 7>$, $<3^4, 8>$	$\mathcal{H}_0$	$SL_2(3)$	Exotic
			S	C_2	

Table 7.1: Simple fusion systems on p-groups of order p^4 with A not $\mathcal{F}$-essential.

p	Case	S	$E \in \mathbf{E}_{\mathcal{F}} \cup \{S\}$	$\mathrm{Out}_{\mathcal{F}}(E)$	Realisable or exotic
3	II.(iii)	$<3^4, 7>$	A	$S_4 \cong PGL_2(3)$	$\mathcal{F}_3$, A_9
			$\mathcal{H}_0$	$SL_2(3)$	
			S	C_2	
5	II.(ii)	$<5^4, 7>$	A	$(C_4 \times A_5) : C_2$	Co_1
			Q	$GL_2(5)$	
			$\mathcal{H}_*$	$2A_5 \cong SL_2(5)$	
			S	C_4^2	
5	II.(iii)	$<5^4, 7>$	A	$PGL_2(5) \cong S_5$	$\mathcal{F}_c$, $PSU_5(4)$ if all $\mathcal{H}_i$ $\mathcal{F}$-essential Exotic otherwise
			Union of $\mathcal{H}_i$	$SL_2(5)$	
			S	C_4	
$p \geq 7$	II.(iii)	$<p^4, 7>$	A	$PSL_2(p) : C_{2(p-1)/d}$	Exotic [CP10] $d = \gcd(4, p-1)$
			$\mathcal{H}_0$	$SL_2(p) : C_{(p-1)/d}$	
			S	$C_{p-1} \times C_{(p-1)/d}$	
p	II.(iv)	$<p^4, 7>$	A	$GL_2(p)/\{\pm I_2\}$	$PSp_4(p)$
			Q	$SL_2(p) : C_{(p-1)/2}$	
			S	$C_{p-1} \times C_{(p-1)/2}$	$\mathcal{F}_1$ when $p = 3$

Table 7.2: Reduced fusion systems on p-groups of order p^4 with A $\mathcal{F}$-essential.

We gather here the remaining relevant notation.

Notation 7.3 ([COS17, Notation 2.4 and 2.9]). We will denote by $Z = Z(S)$ and $Z_0 = Z \cap S'$, which in our case coincide, and $A_0 = ZS' = S'$.

Let $\Delta = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$, and $\Delta_i = \{(r, r^i) \mid r \in (\mathbb{Z}/p\mathbb{Z})^\times\} \leq \Delta$, and consider the action of Δ on S/A and Z. Define $\mu : \mathrm{Aut}(S) \to \Delta$ and its projection $\hat{\mu} : \mathrm{Out}(S) \to \Delta$ by setting, for $\alpha \in \mathrm{Aut}(S)$ (respectively $[\alpha] \in \mathrm{Out}(S)$),

$$\alpha\mu = [\alpha]\hat{\mu} = (r, s) \text{ if } \begin{cases} x\alpha = x^r A \text{ for } x \in S \setminus A \\ g\alpha = g^s \text{ for } x \in Z. \end{cases}$$

We also define $\mathrm{Aut}^\vee_{\mathcal{F}}(S) := \{\alpha \in \mathrm{Aut}_{\mathcal{F}}(S) \mid [\alpha, Z] \leq Z\}$, and note that in our case $\mathrm{Aut}^\vee_{\mathcal{F}}(S) = \mathrm{Aut}_{\mathcal{F}}(S)$, its projection $\mathrm{Out}^\vee_{\mathcal{F}}(A) = \mathrm{Aut}^\vee_{\mathcal{F}}(S)/\,\mathrm{Inn}(S)$, and $\mathrm{Aut}^\vee_{\mathcal{F}}(A) := \{\alpha|_A \mid \alpha \in \mathrm{Aut}^\vee_{\mathcal{F}}(S)\}$.

We will sometimes consider A as a $GF(p)G_0$-module, which we will then denote by V, and define $G = \mathrm{Aut}_{\mathcal{F}}(A)$, $G^\vee = \mathrm{Aut}^\vee_{\mathcal{F}}(A)$ and $\mu_V = \mu_A : G^\vee \to \Delta$ the restriction of μ to $G^\vee$, and let $G_0 = F^*(G) = O^{p'}(G)$, and σ is a certain element of S which we will need not use, but appears in the tables. In this context $\mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$, and we will consider $V = A$ as a quotient module of $\mathbb{Z}[\mathbf{U}]$ by a suitable ideal. Further, $G_0 \leq \overline{G} \leq N_{GL(V)}(G_0)$ is a suitable overgroup of G.

We now proceed to the proof of Theorem 7.1.

Proof of Theorem 7.1. S contains an abelian subgroup of index p by Lemma 1.20, and we use the results of [Oli14] and [COS17] to obtain the simple/reduced fusion systems. Then [Oli14, Theorem 2.1] implies there is a unique abelian subgroup of S of index p in S, which we denote by A, hence the remaining maximal subgroups of S are extraspecial, and S contains extraspecial subgroups of index p. Thus Hypothesis A holds and Lemma 4.1 implies that $Z = Z(S) = Z(Q)$ has order p. Further, Lemmas 3.1 and 3.2 imply that the only possible $\mathcal{F}$-essential subgroups are isomorphic to p_+^{1+2} or elementary abelian, and we divide the classification as in [Oli14] according to whether A is $\mathcal{F}$-essential or not.

We have $m = log_p(|A|) = 3$. In both cases the classification depends on the value of $3 \pmod{p-1}$ so it behaves differently when $p = 3, 5$ than when $p \geq 7$. Recall that in the SmallGroups notation $<p^4, 7> \cong T \in \mathrm{Syl}_3(PSp_4(p))$, $<3^4, 7> \cong C_3 \wr C_3$ and $<3^4, 9> \cong T \in \mathrm{Syl}_p({}^3D_4(2))$. The map $\hat{\mu} : \mathrm{Out}(S) \to \Delta \cong C_{p-1}^2$ will be very important.

Case I. We assume that A is not $\mathcal{F}$-essential, and we use [Oli14, Theorem 2.8]. As $m = 3$, if $3 \equiv -1 \pmod{p-1}$ then $p - 1 \mid 4$ and $p \in \{3, 5\}$. So cases I.(a)(i) and I.(a)(ii) only happen if $p \leq 5$. Note that $3 \equiv 0 \pmod{p-1}$ is not possible as p is odd. Thus we are in case I.(a)(iv) if and only if $p \geq 7$. The remaining case I.(b) only happens when $3 = m = k(p-1) + 1$, that is $k = 1$ and $p = 3$.

In case I.(a) all $\mathcal{H}_i$ can be $\mathcal{F}$-essential, so they are all elementary abelian hence $B_i \cong p_+^{1+2}$ for all $i \in \{0, \ldots, p\}$. Therefore Lemma 3.11 (1) implies that either $p = 3$ and $S \cong <3^4, 9>$ or $p \geq 5$ and $S \cong <5^4, 7>$.

In case I.(b) we look more closely at the structure of S. We have $k = 1$, $p = 3$, $|Z(S)| = 3$, and $A \cong \mathbb{Z}[\mathbf{U}]/I$ where $I = \langle p\sigma, p + l\sigma \rangle$ for $\sigma = 1 + u + u^2 \in \mathbb{Z}[\mathbf{U}]$ and some $l \in \mathbb{Z}$ such that $p \nmid l + 1$. As $p\sigma \in I$, only the value $l \pmod 3$ matters and there are 2 possible choices, which can be taken to be $l = 0$ or $l = 1$. If $l = 0$ then $I = \langle p\sigma, p \rangle = \langle 3 \rangle$, so A has exponent 3, that is $A \cong C_3^3$. If however $l = 1$, then $3 \notin I = \langle p\sigma, p + \sigma \rangle$ (otherwise $\sigma = (3 + \sigma) - 3 \in I$, which contradicts $\sigma\Psi \neq 1$ in this case, see Step 3, Case 3 of the proof of [Oli14, Theorem 2.8]), hence the image of $1 \in \mathbb{Z}[\mathbf{U}]$ in S has order 9. In particular, A does not have exponent 3, and $A \cong C_9 \times C_3$. Further, in Step 3, Case 3 of the proof of [Oli14, Theorem 2.8], it is shown that out of the three nonabelian maximal subgroups of S, one has exponent p and the remaining two have exponent 9. Thus, Lemma 3.11 (2) implies that either $S \cong {<}3^4, 7{>} \cong C_3 \wr C_3$ or $S \cong {<}3^4, 8{>}$, and we have shown that both cases arise according to the choice of l.

In every case except I.(a)(i) (and for each choice of S) we then get a unique fusion system up to isomorphism. In case I.(a)(i) we have $\mathrm{Out}_{\mathcal{F}}(S)\hat{\mu} = \Delta_{-1}$, thus [Oli14, Lemma 2.6 (b)] implies that none of the $\mathcal{H}_i$ are $\mathcal{F}$-conjugate and that $\mathcal{H}_0$ is normalised by every $\alpha \in \mathrm{Aut}_{\mathcal{F}}(S)$. The situation here is slightly different to that of Chapter 6, as in this case there are p S-conjugacy class of pearls, there is an element of order p in $\mathrm{Aut}(S)$ permuting the $\mathcal{H}_i$ transitively, and $\mathcal{H}_0$ is not characteristic in S. This can be observed when $p = 5$ via an embedding of S into $K := C_5 \wr C_5$, and by embedding S into $K := C_9 \wr C_3$ when $p = 3$, where the only maximal subgroup of S normal in $N_K(S)$ is A. In particular, $\mathrm{Aut}(S)$ acts 2-transitively on $\{\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{p-1}\}$ and there is a unique isomorphism class of reduced $\mathcal{F}$ for each choice of number of $\mathcal{F}$-essential classes. Hence there are p reduced fusion systems up to isomorphism arising from case I.(a)(i).

Whether $\mathcal{H}_0 \subseteq \mathbf{E}_{\mathcal{F}}$ or not does not affect the reduced fusion systems, but different extensions arise in each of the cases. When $p = 3$ all saturated fusion systems on ${<}3^4, 9{>}$ were constructed in [DRV07, Table 2].

Therefore one of the following holds:

1. $p = 3$. There are 3 simple fusion systems up to isomorphism from I.(a)(i), one from I.(a)(ii) and one from I.(b) for each choice of S. Note that $S \cong {<}3^4, 9{>}$

in case I.(a), whereas in case I.(b) we have $S \cong C_3 \wr C_3$ or $S \cong <3^4, 8>$.

2. $p = 5$, $S \cong <5^4, 7> \in \mathrm{Syl}_5(PSp_4(5))$ and there are 6 simple fusion systems up to isomorphism. These are 5 from I.(a)(i) and one from I.(a)(ii), which is the exotic fusion system described in [PS15].

3. $p \geq 7$, $S \cong <p^4, 7>$ and there is a unique simple fusion system from case I.(a)(iv).

In each case [Oli14, Theorem 2.8] determines both $\mathrm{Out}_{\mathcal{F}}(H_i) \cong SL_2(p)$ and $\mathrm{Out}_{\mathcal{F}}(Q) \cong GL_2(p)$ whenever H_i or Q are $\mathcal{F}$-essential. Further, as $\hat{\mu}|_{\mathrm{Out}_{\mathcal{F}}(S)}$ is injective, $\mathrm{Out}_{\mathcal{F}}(S) \cong C_{p-1}^i$ where $i = 1$ if $\hat{\mu}|_{\mathrm{Out}_{\mathcal{F}}(S)} = \Delta_{-1}$ (that is $\mathbf{E}_{\mathcal{F}} \subseteq \mathcal{H}_0 \cup \mathcal{H}_*$) and $i = 2$ if $\hat{\mu}|_{\mathrm{Out}_{\mathcal{F}}(S)} = \Delta$ (that is $Q \in \mathbf{E}_{\mathcal{F}}$). By the second bullet point in the statement of [Oli14, Theorem 2.8] the fusion systems above are all exotic except when $p = 3$ in case I.(a)(ii), in which case it is realised by ${}^3D_4(q)$ for q coprime to 3 and in case from I.(a)(i) when all 3 conjugacy classes $\mathcal{H}_i$ are $\mathcal{F}$-essential, which is realised by $PSL_3(q)$ or $PSU_3(q)$ for appropriate q. These are $\mathcal{F}_b$ and $\mathcal{F}_a$ respectively in the notation of Table B.1.

This completes the proof of Case I, that is when A is not $\mathcal{F}$-essential, and Table 7.1 is correct.

Case II. If $A \in \mathbf{E}_{\mathcal{F}}$ then then by Lemma 3.2 A is elementary abelian and the reduced fusion systems $\mathcal{F}$ are studied in [COS17, Theorem 2.8, Theorem 4.1], and they are all simple. They are either realised by one of the groups in [COS17, Table 2.2] or exotic. Most of the relevant information can be found in [COS17, Tables 2.1 and 4.1], hence we now reproduce the relevant parts of these tables.

We have $n = m = dim(A) = 3$, which reduces the modules to consider to special cases of the first and fifth rows of [COS17, Table 4.1], with the fifth row appearing only when $p = n = 3$. Note that for reduced $\mathcal{F}$ we require also [COS17, Table 4.2], which contains no 3-dimensional modules, hence we need not consider it.

	$(\mathrm{Aut}_{\mathcal{F}}^{\vee}(A))\mu_A$	$G = O^{p'}(G)X$ where	$m \pmod{p-1}$	σ	$\mathbf{E}_{\mathcal{F}} \setminus \{A\}$
(i)	Δ	$X = \mathrm{Aut}_{\mathcal{F}}^{\vee}(A)$	$\equiv 0$	$\sigma \in \Phi(Z)$	$\mathcal{H}_0 \cup \mathcal{B}_*$
(ii)	Δ	$X = \mathrm{Aut}_{\mathcal{F}}^{\vee}(A)$	$\equiv -1$	$\sigma \in \Phi(Z)$	$\mathcal{B}_0 \cup \mathcal{H}_*$
(iii)	$\geq \Delta_{-1}$	$X = \Delta_{-1}\mu_A^{-1}$	$\equiv -1$	$\sigma \in \Phi(Z)$	union of $\mathcal{H}_i$'s
			—	—	$\mathcal{H}_0$
(iv)	$\geq \Delta_0$	$X = \Delta_0\mu_A^{-1}$	$\equiv 0$	$\sigma \in \Phi(Z)$	union of $\mathcal{B}_i$'s
		Z_0 not G-invariant	—	—	$\mathcal{B}_0$

Table 7.3: [COS17, Table 2.1]

R	p	G_0	$\dim(V)$	$\overline{G}$	$\overline{G}^{\vee}\mu_V$	$G_0^{\vee}\mu_V$	E, R
1	p	$SL_2(p)$ or $PSL_2(p)$ $(p \geq 5)$	$3 \leq n \leq p^{(\mathbf{4.2})}$ socle of dim. i	$GL_2(p)$ or $PGL_2(p) \times C_{p-1}$	Δ	$\{(u^2, u^{i-1})\}$	ER
5	p	—	$n^{(\mathbf{4.4(b)})}$	$C_{p-1} \wr S_n$ $(n \geq p)$	Δ	—	ER

Table 7.4: [COS17, Table 4.1, rows 1 and 5]

We begin by considering the case $p = 3$, which satisfies $n = 3 \equiv -1 \pmod{p-1}$. Since A is elementary abelian and $|Z(S)| = 3$ (by Lemma 4.1), we have $S \cong C_3 \wr C_3$ by Lemma 3.11. S has maximal class, hence four maximal subgroups: A, $Q \cong 3_+^{1+2}$ and the remaining two are isomorphic to 3_-^{1+2}. Hence the only possible $\mathcal{F}$-essential subgroups are A, $Q = B_0$ and the conjugacy class $\mathcal{H}_0$ of $E \leq Q$, $E \cong C_3^2$ with $C_S(E) = E$, S-conjugate to H_0. Both Q and E cannot be $\mathcal{F}$-essential in the same fusion system, since if Q is $\mathcal{F}$-essential then $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$ from Lemma 1.63, hence $\mathrm{Aut}_{\mathcal{F}}(Q)$ acts transitively on the maximal subgroups of Q. In particular, E is $\mathcal{F}$-conjugate to $Z_2(S)$, hence E is not fully $\mathcal{F}$-normalised and not $\mathcal{F}$-essential. Thus either $\mathbf{E}_{\mathcal{F}} = \{A, Q\}$ or $\mathbf{E}_{\mathcal{F}} = \{A, E\}$. We also obtain that $O^{p'}(\mathrm{Out}_{\mathcal{F}}(E)) \cong SL_2(p)$ from Lemma 1.63 if $E \in \mathbf{E}_{\mathcal{F}}$. It remains to consider $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A))$, which is in described in the first row or in the fifth row of [COS17, Table 4.1] reproduced above as Table 7.4.

In the first row we see that $i = 3$, so $G_0^{\vee}\mu_V = \{(u^2, u^2)\} \leq \Delta \cong C_2^2$ is the trivial subgroup, which means that there are no elements in $G_0 = O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A))$ which extend to $\mathrm{Aut}_{\mathcal{F}}(S)$. This is only possible if $N_{O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A))}(\mathrm{Aut}_S(A)) = \mathrm{Aut}_S(A)$, which since $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A)) = G_0$ implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A)) \cong PSL_2(3)$, which also follows from [COS17, Proposition 4.2]. In the fifth row $\mathrm{Aut}_{\mathcal{F}}(A) \leq \overline{G} = C_2 \wr S_3$, and $O^{3'}(C_2 \wr S_3) \cong PSL_2(3)$, hence in every situation $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A)) \cong PSL_2(3)$, and no p'-elements of $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A))$ extend to S, in other words $\mathrm{Aut}_{\mathcal{F}}^A(S) = \mathrm{Inn}(S)$. This means that if $O^{p'}(\mathcal{F}) = \mathcal{F}$, we have $\mathrm{Aut}_{\mathcal{F}}(E) \cong SL_2(p)$ or $\mathrm{Out}_{\mathcal{F}}(Q) \cong SL_2(p)$.

Thus when $p = 3$ there are exactly two reduced fusion systems which correspond to the cases (iii) and (iv) of [COS17, Table 2.1], corresponding to each of the first and last rows of Table 7.2. Now Lemma B.19 implies that there are 4 saturated fusion systems on S up to isomorphism which are realisable by finite simple groups, which can be chosen to be the fusion systems of $\mathcal{F}_1 = \mathcal{F}_S(PSp_4(3))$, $\mathcal{F}_2 = \mathcal{F}_S(PSL_6(2))$, $\mathcal{F}_3 = \mathcal{F}_S(A_9)$, $\mathcal{F}_4 = \mathcal{F}_S(A_{11})$. Note that $A_9 \leq A_{11}$. Further, $PSU_4(2) \cong PSp_4(3)$ by Proposition 1.19 (15), which implies that $PSp_4(3) \cong PSU_4(2) \leq PSL_6(2)$. Hence we see see that $\mathcal{F}_1$ and $\mathcal{F}_3$ are subsystems of $\mathcal{F}_2$ and $\mathcal{F}_4$, respectively (of index 2). Thus $\mathcal{F}_2$ and $\mathcal{F}_4$ are not reduced, but they satisfy $O_p(\mathcal{F}) = 1$. Hence the only reduced fusion systems on S are $\mathcal{F}_1$ and $\mathcal{F}_3$, which agrees with [COS17, Table

2.2]. We note here that despite $\mathrm{Aut}_{A_9}(A) \cong \mathrm{Aut}_{PSp_4(3)}(A) \cong PGL_2(3)$, we have $N_{A_9}(A) \not\cong N_{PSp_4(3)}(A)$, in other words $\mathrm{Aut}_{\mathcal{F}}(A)$ acts slightly differently in the two fusion systems.

Γ	p	conditions	$G = \mathrm{Aut}_\Gamma(A)$	$\mathbf{E}_{\mathcal{F}} \setminus \{A\}$	Table B.1
A_9	3	$n = p = 3$	$\frac{1}{2}C_2 \wr S_3$	$\mathcal{H}_0$	$\mathcal{F}_3$
$Sp_4(p)$	p	—	$GL_2(p)/\{\pm I\}$	$\mathcal{B}_0$	$\mathcal{F}_1$ if $p = 3$
$PSL_5(q)$	5	$v_p(q-1) = 1$	S_5	$\mathcal{H}_0 \cup \mathcal{H}_*$	$\mathcal{F}_c$
$PSL_4(q)$	3	$v_p(q-1) = 1$	S_4	$\mathcal{B}_0$	$\mathcal{F}_1$
$P\Omega_6^+(q)$	3	$v_p(q-1) = 1$	$C_2^2 \rtimes S_3$	$\mathcal{B}_0$	$\mathcal{F}_1$
Co_1	5	—	$4 \times S_5$	$\mathcal{B}_0 \cup \mathcal{H}_*$	

Table 7.5: [COS17, Table 2.2] with $rk(A) = m = 3$, $e = 1$.

When $p \geq 5$ we are in the case of the first row of [COS17, Table 4.1], with A elementary abelian. As $O_p(\mathcal{F}) = 1$ and A is $\mathrm{Aut}(S)$-invariant, by Proposition 2.25 there is some $\mathcal{F}$-essential subgroup other than A, hence there is an element x of order p in $S \setminus A$. Therefore $S \cong p_+^{1+2} \rtimes C_p \cong <p^4, 7>$ by Lemma 3.11. In this case Lemma 1.64 implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A))$ is isomorphic to either $SL_2(p)$ or $PSL_2(p)$. But since A is simple as a $GF(p)G_0$-module and odd-dimensional, the simple composition factors of A are odd dimensional and [COS17, Proposition 4.2] implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A)) \cong PSL_2(p)$.

When $p = 5$ we have $3 \equiv -1 \pmod{p-1}$, so we need to consider cases (ii), (iii), (iv) of [COS17, Table 2.1], and this case is discussed just before the end of Chapter 4 in [COS17], and collated in the second row of [COS17, Table 4.3], which we reproduce here for $p = 5$. Note the rows correspond to cases (ii), (iii) and (iv) from top to bottom.

<table>
<tr><th>p</th><th>G_0</th><th>$\dim(V)$</th><th>$G_0^\vee\mu_V$</th><th>G</th><th>$G^\vee\mu_V$</th><th>$\mathbf{E}_\mathcal{F}\setminus\{A\}$</th><th>Group/Exotic</th></tr>
<tr><td rowspan="3">5</td><td rowspan="3">$PSL_2(5)$</td><td rowspan="3">3</td><td rowspan="3">$\frac{1}{2}\Delta_{-1}$</td><td>$G_0.C_2\times C_4$</td><td>Δ</td><td>$\mathcal{B}_0\cup\mathcal{H}_*$</td><td>$Co_1$</td></tr>
<tr><td>$PGL_2(5)$</td><td>Δ_{-1}</td><td>$\bigcup\mathcal{H}_i$</td><td>E or $PSL_5(11)$</td></tr>
<tr><td>$G_0.C_2\times C_2$</td><td>$\Delta_0.C_2$</td><td>$\mathcal{B}_0$</td><td>$Sp_4(5)$</td></tr>
</table>

Table 7.6: [COS17, Table 4.3, row 2] for $p=5$.

There is a unique fusion system of type (ii) which is realised by Co_1 as seen by comparing with [COS17, Table 2.2] or by the local subgroups $5^{1+2}:GL_2(5)$, $C_5^3:(C_4\times A_5).C_2$ and $C_5^2:2A_5$[1] from [WWT$^+$05], which show that Q, A and at least one H_i are $\mathcal{F}_S(Co_1)$-essential, and the only candidate fusion system is the one from (ii). In particular, as $\mathrm{Aut}_\mathcal{F}^\vee(A)\mu_A=\Delta$, by [COS17, Lemma 2.5 (c)], we have that $\mathrm{Out}_\mathcal{F}(S)\cong\Delta\cong C_{p-1}^2$ fuses all the conjugacy classes in $\mathcal{H}_*$.

In case (iii), the $\mathcal{F}$-essential subgroups can be any nonempty union of $\mathcal{H}_i$'s. As by [COS17, Table 4.3, row 2] we have $G^\vee\mu_A=\Delta_{-1}$, the $\mathcal{H}_i$ are not $\mathcal{F}$-conjugate by [Oli14, Lemma 2.6 (b)], and as $O_p(\mathcal{F})=1$ there must be some $\mathcal{F}$-essential subgroup other than A by Proposition 2.25. Hence we have the same 5 possibilities for $\mathbf{E}_\mathcal{F}\setminus\{A\}$ as when A is not $\mathcal{F}$-essential. According to [COS17, Table 2.2] these are all exotic except the one with every conjugacy class $\mathcal{H}_i$ being $\mathcal{F}$-essential, which is realised by $PSL_5(q)$, $PSU_5(q)$ for suitable q.

Since we have $G_0^\vee\mu_V=\{(u^2,u^2)\}\subseteq\Delta_{-1}=\{(u,u^{-1})\}$ again by the first row of [COS17, Table 4.1] (as $u^2=u^{-2}$), we have $\mathrm{Aut}_\mathcal{F}(H_i)\cong SL_2(p)$ and $\mathrm{Aut}_\mathcal{F}(A)\cong PGL_2(p)$, so $\mathrm{Out}_\mathcal{F}(S)\cong C_{p-1}$. This complicated situation is again related to the examples in [PS15] and the case $|S|=p^{p-1}$, and this particular situation is even richer than the general case due to there being p S-conjugacy

[1] The ATLAS [CCN$^+$85] gives this as $C_5^2:4A_5$ but it is a known error, see [Wil17, Section 4].

classes of $\mathcal{H}_i$ being potentially $\mathcal{F}$-essential. Further, $A = C_S(Z_2(S))$ can also be $\mathcal{F}$-essential, which can be seen as analogous to the role of $R = C_{S_7}(Z_2(S_7))$ for $S_7 \in \mathrm{Syl}_7(G_2(7))$.

In case (iv) there is a unique fusion system for $p = 5$ that can be seen to be realised by $PSp_4(p)$ by comparing with [COS17, Table 2.2].

At this stage it only remains to establish the last two rows of Table 7.2 whenever $p \geq 7$, in which case we only need consider the first row of [COS17, Table 4.1], and we have $3 \not\equiv 0, -1 \pmod{p-1}$ hence there are exactly two reduced fusion systems corresponding to cases (iii) and (iv) of [COS17, Table 2.1]. In this situation [COS17, Proposition 4.2] implies that $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(A)) \cong PSL_2(p)$ and $G_0^{\vee}\mu_V = \{(u^2, u^2)\}$. Each $\mathcal{F}$ has exactly one $\mathcal{F}$-conjugacy class of $\mathcal{F}$-essential subgroups other than A, either $\mathcal{H}_0$ in case (iii), or $\mathcal{B}_0 = \{Q\}$ in case (iv). The fusion system $\mathcal{F}$ with $\mathbf{E}_{\mathcal{F}} = \{A, Q\}$ is realised by $PSp_4(p)$, since $Sp_4(p)$ has p-local subgroups of shapes $p^{1+2} : (C_{p-1} \times Sp_2(p))$ and $C_p^3 : GL_2(p)$ by [BHRD13, Table 8.12], concluding the last row of Table 7.2. On the other hand the fusion system $\mathcal{F}$ with $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{H}_0$ is exotic, since it does not appear in [COS17, Table 2.2]. This exotic $\mathcal{F}$ has $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(E)) \cong SL_2(p)$ whenever $E \in \mathcal{H}_0$, by Lemma 1.63, which gives us $\mathrm{Aut}_{\mathcal{F}}^{E}(S)\mu = \Delta_{-1}$, and can be found in [CP10, Theorem 5.1].

It remains to consider the relationship between the subgroups of Δ determined by $\mathrm{Aut}_{\mathcal{F}}^{E}(S)\mu = \Delta_{-1}$ and $G_0^{\vee}\mu_V = \{(u^2, u^2)\}$, which depends on the value of $p \pmod 4$. Let $d \in \Delta_{-1}$, then $d = (u^k, u^{-k})$ for some $k \in \mathbb{Z}$, so in order to have $d \in G_0^{\vee}\mu_V$ we need $u^k = u^{-k}$ with k even, that is u is an involution and $k = (p-1)/2$ even. Thus if $4 \mid p-1$ then $\Delta_{-1} \cap \{(u^2, u^2)\}$ has order 2, whereas if $4 \mid p+1$ then $\Delta_{-1} \cap \{(u^2, u^2)\}$ is trivial. Notice that if $p = 5$ we saw this earlier, and if $p = 3$ the intersection is trivial, since u has order $p - 1 = 2$, so this coincides with the previous cases of II.(iii), which are in different rows of Table 7.2 due to their complexity.

We thus see that $\mathrm{Out}_{\mathcal{F}}(S) \cong C_{p-1} \times C_{(p-1)/\gcd(4,p-1)}$, $\mathrm{Aut}_{\mathcal{F}}(A)$ has shape $PSL_2(p) : C_{2(p-1)/\gcd(4,p-1)}$ and the shape of $\mathrm{Aut}_{\mathcal{F}}(E)$ is $SL_2(p) : C_{(p-1)/\gcd(4,p-1)}$.

Further, all the reduced fusion systems in Case II are simple by [COS17, Theorem 2.8], so we have classified both the reduced and simple fusion systems in this case.

We have now considered all possible cases and completely determined Tables 7.1 and 7.2. We further note that all the relevant known fusion systems of finite simple groups from Table B.1 ($\mathcal{F}_1$, $\mathcal{F}_3$ and $\mathcal{F}_c$ in Case II, $\mathcal{F}_a$ and $\mathcal{F}_b$ in Case I) have been described, as well as all of the relevant ones in [COS17, Table 2.2]. $\mathcal{F}_2$ and $\mathcal{F}_4$ do not appear since they are not reduced, as they are extensions of $\mathcal{F}_1$ and $\mathcal{F}_3$ respectively of order 2, with $O^{p'}(\mathcal{F}_i) = \mathcal{F}_{i-1}$ for $i = 2, 4$. $\square$

CHAPTER 8

CONCLUSION

After the results in this thesis, the problem of classifying saturated fusion systems with $O_p(\mathcal{F}) = 1$ on p-groups with an extraspecial subgroup of index p is at an advanced stage. In Theorem 4.27 we reduced the situation when p is odd and $|S| \geq p^6$ to a few cases, all but one of which have been classified Chapters 5 and 6 of this thesis, [BFM] and [PS18]. The case when $|S| = p^4$ was determined in Chapter 7 using the classifications in [Oli14] and [COS17]. Finally, the case of a Sylow p-subgroup of $SL_4(p)$ remains future work.

In the proof of the Reduction Theorem 4.27 we assume that $p \neq 2$, but we believe that this assumption can be removed. Removing this assumption will involve modifying the applications of McLaughlin's results on groups generated by transvections, but appears doable. In the case $p = 2$ we only need to show that $|S| \leq 2^6$, as then we can conclude by [Oli16, Theorem A].

When S is a Sylow p-subgroup of $SL_4(p)$ there are some partial results in Chapter 5 and we will attempt to proceed in a similar manner, although there are 3 $\mathcal{F}$-essential subgroups instead of just 2 to worry about in the uniqueness arguments. The case $p = 3$, as in a Sylow p-subgroup of $SU_4(p)$, will require different arguments.

We did not prove which of the fusion systems satisfying $O^{p'}(\mathcal{F}) = \mathcal{F}$ constructed are simple, but we have the following partial results using strongly closed subgroups.

Lemma 8.1. *The saturated fusion systems $\mathcal{F}$ obtained in Theorems 6.7 and 6.8 contain no proper non-trivial strongly closed subgroups unless $\mathbf{E}_{\mathcal{F}}$ consists of a unique S-conjugacy of $\mathcal{F}$-pearls, in which case the unique maximal subgroup containing them is strongly closed in $\mathcal{F}$. In particular, $\mathcal{F}$ is simple whenever $O^{p'}(\mathcal{F}) = \mathcal{F}$ except possibly for the exception above.*

Proof. Assume $X \leq S$ is strongly closed. Then $X \trianglelefteq S$, which implies that $Z \leq X$. Let $E \in \mathbf{E}_{\mathcal{F}} \cap \mathcal{P}$, then $\langle Z^{\mathrm{Aut}_{\mathcal{F}}(E)} \rangle \geq E$ so $E \leq X$ and as $X \trianglelefteq S$ we have $ES' \leq X$, so X is the only candidate for a strongly closed subgroup and is strongly closed if the only $\mathcal{F}$-essential subgroups are the S-conjugates of E. If there is another $\mathcal{F}$-essential subgroup then $X = S$ and there are no proper non-trivial strongly closed subgroups in $\mathcal{F}$. The second part follows from Corollary 2.39 as $O^{p'}(\mathcal{F}) = \mathcal{F}$ and $\mathcal{F}$ contains no proper non-trivial strongly closed subgroups. □

Lemma 8.2. *If $p \geq 5$, S is a Sylow p-subgroup of $SU_4(p)$, and $\mathcal{F}$ is a saturated fusion system on $\mathcal{F}$ with $O_p(\mathcal{F}) = 1$ and $O^{p'}(\mathcal{F}) = \mathcal{F}$ then there are no proper non-trivial strongly $\mathcal{F}$-closed subgroups. In particular $\mathcal{F}$ is simple.*

Proof. With the assumptions above Lemmas 5.8 and 5.9 imply that V is $\mathcal{F}$-essential and V is a natural $\Omega_4^-(p)$-module for $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))$, hence V is irreducible and we have $\langle Z^{\mathrm{Aut}_{\mathcal{F}}(V)} \rangle = V$, so any strongly closed subgroup in $\mathcal{F}$ is a maximal subgroup containing V. By Lemma 1.34 there is $p+1$ such, all of which are isomorphic. Further, by Lemmas 5.7 and 5.9, we have an element $\widetilde{t}_V \in \mathrm{Aut}_{\mathcal{F}}(S)$ of order $(p^2-1)/2$ normalising V, hence acting on S/V as an element of order $(p+1)/2$, and in $PSU_4(p)$ we see that this element acts on the $p+1$ maximal subgroups of S containing V with two orbits of size $(p+1)/2$, hence does not normalise any of them and they cannot be strongly closed in $\mathcal{F}$. Thus, there are no proper non-trivial strongly closed subgroups in S, and, as $O^{p'}(\mathcal{F}) = \mathcal{F}$, Corollary 2.39 implies that $\mathcal{F}$ is simple. $\square$

With regards to the subsystem $O^p(\mathcal{F})$, we now prove that, unless $p = 3$, all saturated fusion systems on S with $O_p(\mathcal{F}) = 1$ satisfy $O^p(\mathcal{F}) = 1$.

Lemma 8.3. *Suppose S is a p-group with an extraspecial subgroup Q of index p and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. Then $O^p(\mathcal{F}) = \mathcal{F}$ unless $p = 3$ and either $S \in \mathrm{Syl}_3(SL_4(3))$ or $|S| = 3^4$ and all $\mathcal{F}$-essential subgroups have order 3^3.*

Proof. By Proposition 2.33 we have $O^p(\mathcal{F}) = \mathcal{F} \iff \mathfrak{hyp}(\mathcal{F}) = S \iff \mathfrak{foc}(\mathcal{F}) = S$. Now S contains an extraspecial subgroup Q of index p and $O_p(\mathcal{F}) = 1$, so if $|S| \geq p^6$ we apply Theorem 4.27 to obtain the structure of S and $\emptyset \neq \mathcal{M} \subseteq \mathbf{E}_{\mathcal{F}}$.

If S is a Sylow p-subgroup of $SL_4(p)$ then $\mathcal{M} \subseteq \{M_1, M_2\}$ and as $\mathcal{M}$ is not empty $M_i \in \mathbf{E}_{\mathcal{F}}$ for either $i = 1$ or $i = 2$. Now as $M_1 \cap M_2 = V$ is characteristic in S by Lemma 5.2 (5), since $O_p(\mathcal{F}) = 1$ by using Proposition 5.5 we see that Q is $\mathcal{F}$-essential. If $p \geq 5$ then Lemma 5.6 implies that $O^{p'}(\mathrm{Out}_{\mathcal{F}}(Q)) \cong SL_2(p)$ acts on $Q/Z(Q)$ as a direct sum of 2 natural $SL_2(p)$-modules. Thus $[Q, O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q))] = Q$, and there is a complement K to $\mathrm{Aut}_S(Q)$ in $N_{\mathrm{Aut}_S(Q)}(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(Q)))$ of order $p-1$ which acts on S/Q with kernel $Z(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(M_i)))$ of order 2. Thus as $p \geq 5$ we obtain $\mathfrak{foc}(\mathcal{F}) > Q$, and $\mathfrak{foc}(\mathcal{F}) = S$.

If $S \in \mathrm{Syl}_p(G_2(p))$ we have $p \geq 5$, so if $R \in \mathcal{M}$ then we can use Proposition 4.13 to obtain that $O^{p'}(\mathrm{Out}_{\mathcal{F}}(R)) \cong SL_2(p)$ acts on a $R/\Phi(R)$ as a natural $SL_2(p)$-

module, thus we have $\mathfrak{foc}(\mathcal{F}) \geq [R, \mathrm{Aut}_{\mathcal{F}}(R)] = R$, and there is a cyclic group $\langle\alpha\rangle$ of order $p-1$ in $N_{O^{p'}(\mathrm{Out}_{\mathcal{F}}(R))}(\mathrm{Out}_S(R))$ acting on $\mathrm{Out}_S(R) \cong S/R$ with kernel $Z(O^{p'}(\mathrm{Out}_{\mathcal{F}}(R)))$ of order 2. Let $g \in S \setminus R$, then $gR\alpha = g^{\lambda^2}R$ for some $\lambda \in GF(p)$, so taking an appropriate $\widetilde{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(S)$ we see that $g\widetilde{\alpha} = g^{\lambda^2}x$ for some $x \in R$, so $g^{-1}g\widetilde{\alpha} = g^{\lambda^2-1}x \notin R$. We thus have $\mathfrak{foc}(\mathcal{F}) > R$, hence $\mathfrak{foc}(\mathcal{F}) = S$.

If $S \in \mathrm{Syl}_p(SU_4(p))$ then $\mathcal{M} = \{V\}$ with $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)) \cong PSL_2(p^2)$ acting on V as a natural $\Omega_4^-(p)$-module by Proposition 4.23, hence we see by Lemma 5.7 (2) that $[V, R]$ has index p in V for each $R \in \mathrm{Syl}_p(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V)))$, thus $[V, O^{p'}(\mathrm{Aut}_{\mathcal{F}}(V))] = V$. There further is an element $t \in \mathrm{Aut}_{\mathcal{F}}(S)$ of order $(p^2-1)/2$ which inverts S/V, that is for $xV \in S/V$ we have $xV^{-1}(xVt) = xV^{-2}$ and thus $\mathfrak{foc}(\mathcal{F}) \geq V[S, \langle t\rangle] = S$.

If $|S| = p^{p-1}$ (including when $p = 7$ with $S \in \mathrm{Syl}_7(G_2(7))$ and $R \notin \mathbf{E}_{\mathcal{F}}$) then there exists $P \in \mathcal{P} \cap \mathbf{E}_{\mathcal{F}}$, hence P is an $\mathcal{F}$-pearl, a natural $SL_2(p)$-module for $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P)) \cong SL_2(p)$, and we have $[P, \mathrm{Aut}_{\mathcal{F}}(P)] = P$. Further, Lemma 6.4 implies that there exists $\Delta \leq \mathrm{Out}_{\mathcal{F}}(S)$ of order $p-1$ whose elements act on S/S' as diagonal elements as before, hence, as $p \geq 5$, $\mathfrak{foc}(S) \geq PS'[S, \Delta] = M_P[S, \Delta] = S$, since $[S, \Delta] \nleq M_P$, where M_P is the unique maximal subgroup containing P in S by Lemma 6.2.

Finally, we consider the case when $|S| = p^4$. By Lemma 1.20, S contains an abelian subgroup A of index p and we use [Oli14, Lemma 2.2(a)] to obtain that $\mathbf{E}_{\mathcal{F}} \subseteq \{A\} \cup \mathcal{B}_0 \cup \mathcal{B}_* \cup \mathcal{H}_0 \cup \mathcal{H}_*$ (see Notation 7.2). Now if $A \notin \mathbf{E}_{\mathcal{F}}$ then as $O_p(\mathcal{F}) = 1$ we have $(\mathcal{H}_0 \cup \mathcal{H}_*) \cap \mathbf{E}_{\mathcal{F}} \neq \emptyset$. Let $H \in (\mathcal{H}_0 \cup \mathcal{H}_*) \cap \mathbf{E}_{\mathcal{F}}$. Then since $O^{p'}(\mathrm{Aut}_{\mathcal{F}}(H)) \cong SL_2(p)$ we have $[H, \mathrm{Aut}_{\mathcal{F}}(H)] = H$, and we have an action on $\mathrm{Out}_S(H)$ as before, hence $\mathrm{Aut}_{\mathcal{F}}(S)\mu \geq \Delta_{-1}$. As $|S| = p^4$ we have $m = 3$, and in the proof of [Oli14, Theorem 2.8] it is proved that

$$O^p(\mathcal{F}) = \mathcal{F} \iff \mathrm{Aut}_{\mathcal{F}}(S)\mu \nleq \Delta_{m-1} = \Delta_2 \text{ or } (\mathcal{H}_* \cup \mathcal{B}_*) \cup \mathbf{E}_{\mathcal{F}} \neq \emptyset.$$

Now we have $\Delta_{-1} = \{(r, r^{-1}) \mid r \in (\mathbb{Z}/p)^\times\} \nleq \Delta_2 = \{(r, r^2) \mid r \in (\mathbb{Z}/p)^\times\}$, unless $r^{-1} = r^2$, that is $r^3 = 1$, whereas r has order dividing $p-1$, thus in this case we always have $O^p(\mathcal{F}) = \mathcal{F}$.

If A is $\mathcal{F}$-essential we instead use [COS17, Lemma 2.7(b)] to obtain that $O^p(\mathcal{F}) = \mathcal{F}$ if and only if $[A, \mathrm{Aut}_{\mathcal{F}}(A)] = A$. We see from the proof of [COS17, Lemma 2.7(b)] that if $O^p(\mathcal{F}) \neq \mathcal{F}$ then $(\mathrm{Out}_{\mathcal{F}}(S))\hat{\mu} \leq \Delta_2$, whereas $E \in \mathbf{E}_{\mathcal{F}} \setminus \{A\}$ forces $(\mathrm{Out}_{\mathcal{F}}(S))\hat{\mu} \geq \Delta_t$ where $t = 0$ if $|E| = p^3$ and $t = -1$ if $|E| = p^2$. The only way that $\Delta_t \leq \Delta_2$ is when $p = 3$ and $t = 0$, where we have

$$\Delta_0 = \{(r, r^0) \mid r \in (\mathbb{Z}/p)^\times\} = \Delta_2 = \{(r, r^2) \mid r \in (\mathbb{Z}/p)^\times\}$$

as $r^2 = r^0 = 1$. Thus the lemma is proved. $\square$

A possible extension of the problem considered is to study the situation for Sylow p-subgroups of Chevalley groups in defining characteristic p in higher dimensions, where we know that the finite groups in question will give rise to examples. Under the assumption that the $\mathcal{F}$-essential subgroups coincide with those in the above situation, it seems reasonable to attempt to prove that when p is large enough these are the only examples arising, or find counterexamples. Another question to tackle is whether there will arise other possible $\mathcal{F}$-essential subgroups, which we answer negatively for $SL_4(p)$ and $SU_4(p)$ but has a positive answer in for example $SL_3(p)$, where the Sylow p-subgroups are extraspecial p^{1+2}_+.

Another extension of the problem would involve considering the classical groups considered over larger fields, where similar questions arise.

APPENDIX A

GROUP EXTENSIONS

We are studying p-groups S containing an extraspecial subgroup Q of index p, thus $Q \trianglelefteq S$, and $S/Q \cong C_p$. This is a group extension of Q by C_p, hence we look at groups with this structure. We begin by describing some notation about homomorphisms and diagrams, then consider the less complicated case of the semidirect product, before considering more general group extensions. When the group being extended is abelian this has a straightforward solution, but when it is nonabelian as in our case the situation is a bit more complicated. We work in full generality until Theorem A.18 and afterwards we focus on the case of interest. Standard references on this topic in order of importance are [ML63, Chapter IV], [Bro94, Chapter IV] and [Ben91, §3.7].

Our goal is to prove the following result, which we will do as Propositions 1.31 and 1.32.

Proposition A.1. *Suppose $Q \cong p_+^{1+2n}$ is an extraspecial group of exponent p and $K \cong C_p$. Then*

1. *There exists a unique isomorphism class of split group extensions S of Q by*

K of maximal nilpotency class if and only if $1+2n \leq p$.

In particular, if $n=2$, then $p \geq 5$ and S is isomorphic to a Sylow p-subgroup of $G_2(p)$.

2. *If $n=2$, then there exist exactly two isomorphism classes of split group extensions S of Q by K with $|S'| = p^3$. One is isomorphic to a Sylow p-subgroup of $SL_4(p)$ and the other to a Sylow p-subgroup of $SU_4(p)$.*

A.1 Diagrams and the short five lemma

We begin with some background notation that we will use.

Definition A.2. *A pair of homomorphisms (α, β) with $\alpha : A \to B$ and $\beta : B \to C$ is* exact *at B if $\ker \beta = \operatorname{im} \alpha$.*

A sequence of homomorphisms $G_1 \xrightarrow{\alpha_1} G_2 \xrightarrow{\alpha_2} G_3 \xrightarrow{\alpha_3} \ldots \xrightarrow{\alpha_{n-2}} G_{n-1} \xrightarrow{\alpha_{n-1}} G_n$ is exact *if (α_{i-1}, α_i) is exact at G_i for $i \in \{2, \ldots, n-1\}$.*

A short exact sequence *is an exact sequence of the form*

$$1 \to G_2 \xrightarrow{\alpha_2} G_3 \xrightarrow{\alpha_3} G_4 \to 1.$$

In particular α_2 is injective, α_3 is surjective and $G_3/G_2\alpha_2 \cong G_4$.

A diagram of groups and homomorphisms is said to be commutative *if any two directed paths from one group to another yield the same composite homomorphism.*

The following result, the Short Five Lemma, is very familiar in the literature for abelian groups and abelian categories, but the version we present here deals with arbitrary groups. It is a particular case which in the terms of category theory has been shown to hold exactly in those categories that are protomodular, as in [Bou91]. We take the proof from [ML63, Lemma I.3.1].

Lemma A.3. *Assume the commutative diagram*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\alpha"'] & B \arrow[r, "\pi"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & 1 \\
1 \arrow[r] & A' \arrow[r, "\iota'"] & B' \arrow[r, "\pi'"] & C' \arrow[r] & 1
\end{tikzcd}$$

of (not necessarily abelian) groups has both rows exact.

1. *If α and γ are monomorphisms, then so is β.*

2. *If α and γ are epimorphisms, then so is β.*

In particular, if α and γ are isomorphisms then so is β.

Proof. We "chase the arrows". For (1), assume α and γ are injective and let $b \in \ker \beta$. As the right square is commutative, $b\pi\gamma = b\beta\pi' = 1_{C'}$, and as γ is injective we have $b\pi = 1_C$. As the top row is exact, $\ker \pi = \operatorname{im} \iota$ so there is $a \in A$ with $a\iota = b$. Now since the left square is commutative $a\alpha\iota' = a\iota\beta = b\beta = 1_{B'}$. As the bottom row is exact ι' is injective, which means that $a\alpha = 1_{A'}$. Since α is injective, $a = 1_A$. Hence $b = a\iota = 1_B$. Thus β is injective.

For (2), assume α and γ are surjective. We consider $b' \in B'$ and apply π'. As γ is surjective there is $c \in C$ such that $c\gamma = b'\pi'$. As the top row is exact, π is surjective. Hence there is $b \in B$ with $b\pi = c$. As the right square is commutative $b\beta\pi' = b\pi\gamma = c\gamma = b'\pi'$. Therefore $((b\beta)b'^{-1})\pi' = 1_{C'}$. Thus as the bottom row is exact, $\ker \pi' = \operatorname{im} \iota'$ and there is $a' \in A'$ such that $a'\iota' = (b\beta)b'^{-1}$. As α is surjective there is $a \in A$ with $a\alpha = a'$, and since the left square is commutative $b\beta b'^{-1} = a'\iota' = a\alpha\iota' = a\iota\beta$ so that $b' = ((a\iota)^{-1}\beta)(b\beta) = ((a\iota)^{-1}b)\beta$. Therefore β is surjective.

The last claim follows from parts (1) and (2). □

A.2 Semidirect products

We now consider a well-known construction on groups which generalises the direct product by introducing an action. As with direct products it can be seen both as an internal and an external construction. Note that, as we write maps on the right, we write the normal subgroup on the right throughout this chapter.

Definition A.4. *We say a group G is the* internal semidirect product *of N by H if G is the product of subgroups $G = HN$, where N is normal in G and $H \cap N = 1$. We denote it by $G = H \ltimes N$. Any such H is called a* complement *to N in G.*

If N, H are groups and $\phi : H \to \mathrm{Aut}(N)$ is a group homomorphism, the external semidirect product *$H \ltimes_\phi N$ of N by H with respect to ϕ is defined as a group with underlying set $H \times N$ where the multiplication in $H \ltimes_\phi N$ is defined by $(h_1, n_1)(h_2, n_2) = (h_1 h_2, (n_1(h_2\phi))n_2)$ for $h_1, h_2 \in H$ and $n_1, n_2 \in N$.*

With this notation the external direct product corresponds to the external semidirect product $H \ltimes_\phi N$ with $\phi : H \to \mathrm{Aut}(N)$ the trivial homomorphism, that is $h\phi = 1_{\mathrm{Aut}(N)}$ for all $h \in H$. As in the direct product case, both definitions of semidirect products are equivalent, so we will refer to a semidirect product for either. This is sensible due to the following.

Lemma A.5. *A group S is an internal semidirect product if and only if it is isomorphic to an external semidirect product $H \ltimes_\phi N$ where for every $h \in H$ we have $h\phi = c_h|_N \in \mathrm{Aut}(N)$.*

Proof. Suppose S is an internal semidirect product. Then there are $N \trianglelefteq S$, $H \leq S$ such that $S = HN$ and $H \cap N = 1$. Then every element s of S can be written uniquely in the form $s = hn$ where $h \in H$ and $n \in N$. As $N \trianglelefteq S$ we have $\theta_h \in \mathrm{Aut}(N)$ where $n\theta_h = n^h \in N$.

We define $\phi : H \to \mathrm{Aut}(N)$ such that $h\phi = \theta_h = c_h|_N$. Then ϕ is a homomorphism as $(hk)\phi = \theta_{hk} = \theta_h\theta_k = h\phi k\phi$. Hence we can build the external semidirect product $H \ltimes_\phi N$. We define $\psi : H \ltimes_\phi N \to S$ by $(h, n)\psi = hn$. Then

$$\begin{aligned}((h_1, n_1)(h_2, n_2))\psi = (h_1h_2, (n_1(h_2\phi))n_2)\psi &= (h_1h_2(n_1^{h_2})n_2)\\ &= (h_1n_1)(h_2n_2) = (h_1, n_1)\psi(h_2, n_2)\psi.\end{aligned}$$

Hence ψ is a homomorphism. If $(h, n) \in \ker\psi$ then $1_S = (h, n)\psi = hn$ so that $h^{-1} = n \in H \cap N = 1$ and $\ker\psi$ is trivial. Thus ψ is an isomorphism.

Conversely assume $S = H \ltimes_\phi N$. Then we have $\overline{N} = \{(1_H, n) \mid n \in N\} \trianglelefteq S$ and $\overline{H} = \{(h, 1_N) \mid h \in H\} \leq S$ such that $S = \overline{HN}$ and $\overline{H} \cap \overline{N} = 1$ so that S is an internal semidirect product of N by H. $\square$

By definition given groups Q, K the semidirect products of Q by K are determined by the maps $\psi : K \to \mathrm{Aut}(Q)$. There are many choices which give rise to isomorphic groups. Below we present a sufficient condition for $K \ltimes_{\phi_1} Q$ to be isomorphic to $K \ltimes_{\phi_2} Q$. There are other ways to find isomorphisms involving changing the normal subgroup or complement.

Lemma A.6. *Suppose K, Q are groups, $\psi_1, \psi_2 : K \to \mathrm{Aut}(Q)$ are homomorphisms and there exist $\mu \in \mathrm{Aut}(K)$ and $\sigma \in \mathrm{Aut}(Q)$ such that*

$$\begin{tikzcd} K \arrow[r, "\psi_1"] \arrow[d, "\mu"'] & \mathrm{Aut}(Q) \arrow[d, "c_\sigma"'] \\ K \arrow[r, "\psi_2"] & \mathrm{Aut}(Q) \end{tikzcd}$$

commutes. Then $K \ltimes_{\psi_1} Q \cong K \ltimes_{\psi_2} Q$. In particular $\mathrm{Aut}(Q)$*-conjugate maps give rise to isomorphic semidirect products.*

Proof. Define $\theta : K \ltimes_{\psi_1} Q \to K \ltimes_{\psi_2} Q$ via $(k, q)\theta = (k\mu, q\sigma)$. To check that θ is a homomorphism we compare:

$$\begin{aligned} ((k, q)(k_1, q_1))\theta = (kk_1, (q(k_1\psi_1))q_1)\theta &= ((kk_1)\mu, ((q(k_1\psi_1))q_1)\sigma) \\ &= (k\mu k_1\mu, (q(k_1\psi_1)\sigma)(q_1\sigma)) \end{aligned}$$

and

$$(k, q)\theta(k_1, q_1)\theta = (k\mu, q\sigma)(k_1\mu, q_1\sigma) = (k\mu k_1\mu, (q\sigma(k_1\mu\psi_2))(q_1\sigma)).$$

Both expressions coincide whenever $q\sigma[\sigma^{-1}(k_1\psi_1)\sigma] = q(k_1\psi_1)\sigma = q\sigma(k_1\mu\psi_2)$. Hence as $\mu\psi_2 = \psi_1 c_\sigma$ by assumption, θ is a homomorphism. The inverse of θ is $\phi : K \ltimes_{\psi_2} Q \to K \ltimes_{\psi_1} Q$ defined by $(k, q)\phi = (k\mu^{-1}, q\sigma^{-1})$. Hence the lemma holds. $\square$

A.3 Group extensions

Now we look at general group extensions. A group extension contains a normal subgroup, but may not contain a subgroup isomorphic to the quotient group as in the semidirect product. They can be defined in terms of subgroups and short exact sequences, and both concepts coincide.

Definition A.7. *Given groups A and C a* group extension *of A by C is a group B such that B has a normal subgroup $A\iota$ isomorphic to A and $B/A\iota \cong C$ via a projection map π.*

A group extension splits *if π has a one-sided inverse ρ, that is a homomorphism $\rho : C \to B$ such that $\rho\pi = 1_C$. A* nonsplit extension *is an extension that does not split.*

A group extension B of A by C determines a short exact sequence of groups

$$E: \quad 1 \longrightarrow A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 1$$

and such a short exact sequence determines a group extension B of A by C. We refer to both the group B and the short exact sequence E as a group extension.

A group extension E induces an action $\theta : B \to \mathrm{Aut}(A)$ given by $b \mapsto \iota\, c_b\, \iota|_{A\iota}^{-1}$ as B acts on $A\iota \trianglelefteq B$ by conjugation and ι is injective.

If a group extension splits then the diagram becomes

$$\begin{tikzcd} E: \quad 1 \arrow[r] & A \arrow[r, "\iota"] & B \arrow[r, "\pi"] & C \arrow[r] \arrow[l, bend left, "\rho"] & 1 \end{tikzcd}$$

and there is a subgroup $C\rho \leq B$ isomorphic to C, but in general C may not embed in B. We make the statement precise below.

Lemma A.8. *An extension E splits if and only if B is a semidirect product of A by C.*

Proof. If $E : 1 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 1$ splits then $A\iota \trianglelefteq B$ and by definition there exists $\rho : C \to B$ such that $\rho\pi = 1_C$, therefore $C\rho \leq B$, $C\rho \cap A\iota = 1$ and $B/A\iota = B/\operatorname{im}\iota = B/\ker\pi \cong \operatorname{im}\pi = C$ so $C\rho$ is a complement to $A\iota$ in B hence B is an internal semidirect product of $A\iota$ and $C\rho$.

Conversely if B is an internal semidirect product of A by C then $B = CA$ such that $A \trianglelefteq B$ and $C \cap A = 1$, so that $B/A \cong C$ which gives a short exact sequence $1 \to A \to B \to B/A \cong C \to 1$. As C embeds into B, the inclusion map gives us our splitting. $\square$

When classifying extensions we do it according to the following equivalence which is called congruence.

Definition A.9. *A* morphism *of extensions* $\Gamma : E \to E'$ *is a triple*

$$\Gamma = (\alpha, \beta, \gamma) \in \mathrm{Hom}(A, A') \times \mathrm{Hom}(B, B') \times \mathrm{Hom}(C, C')$$

such that the following diagram is commutative:

$$\begin{tikzcd} E : 1 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\alpha"'] & B \arrow[r, "\pi"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & 1 \\ E' : 1 \arrow[r] & A' \arrow[r, "\iota'"] & B' \arrow[r, "\pi'"] & C' \arrow[r] & 1 \end{tikzcd}$$

Two group extensions are congruent *if* $A = A'$, $C = C'$ *and there exists a morphism* $(1_A, \beta, 1_C) : E \to E'$. *In this case the previous diagram becomes*

$$\begin{tikzcd} & & B \arrow[dd, "\beta"'] \arrow[dr, "\pi"] & & \\ 1 \arrow[r] & A \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & & C \arrow[r] & 1. \\ & & B' \arrow[ur, "\pi'"'] & & \end{tikzcd}$$

Note that if two group extensions E, E' are congruent then β is an isomorphism by the Short Five Lemma A.3.

Lemma A.10. *Congruence of group extensions is an equivalence relation.*

Proof. E is congruent to itself via $(1_A, 1_B, 1_C)$. If E is congruent to E' then β is an isomorphism by Lemma A.3, so E' is congruent to E via $(1_A, \beta^{-1}, 1_C)$, hence congruence is symmetric. Further, congruence is transitive via composition of morphisms as we now show.

$$\begin{tikzcd}
 & & B \arrow[d, "\beta"] \arrow[dr, "\pi"] & & \\
1 \arrow[r] & A \arrow[ur, "\iota"] \arrow[r, "\iota'"] \arrow[dr, "\iota''"'] & B' \arrow[r, "\pi'"] \arrow[d, "\beta'"] & C \arrow[r] & 1 \\
 & & B'' \arrow[ur, "\pi''"'] & &
\end{tikzcd}$$

If E, E' and E', E'' are congruent extensions we have a diagram as above. Since E, E' are congruent $\iota\beta = \iota'$ and $\beta\pi' = \pi$ and since E', E'' are congruent $\iota'\beta' = \iota''$ and $\beta'\pi'' = \pi'$, so that $\iota\beta\beta' = \iota'\beta' = \iota''$ and $\beta\beta'\pi'' = \beta\pi' = \pi$. Thus $(1_A, \beta\beta', 1_C)$ makes the diagram commutative therefore E and E'' are congruent. $\square$

We note that if there is an isomorphism of extensions then, since $\alpha\iota'$ is injective and $\pi'\gamma^{-1}$ is surjective, we can build a congruence between the extensions as follows.

$$\begin{tikzcd}
E : 1 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\alpha"'] \arrow[dr, "\alpha\iota'"] & B \arrow[r, "\pi"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 1 \\
E' : 1 \arrow[r] & A' \arrow[r, "\iota'"] & B' \arrow[r, "\pi'"] \arrow[ur, "\pi'\gamma^{-1}"] & C' \arrow[r] & 1
\end{tikzcd}$$

Thus isomorphism and congruence classes of extensions coincide. However two group extensions can have B isomorphic to B' despite not being congruent, as for example with extensions of C_p by C_p where all $p-1$ nonsplit group extensions are isomorphic to C_{p^2}. Thus the number of isomorphism classes of groups B which are a group extension of A by C is smaller than the number of congruence classes of extensions of A by C.

The theory of group extensions with an abelian normal subgroup A is well known and involves cohomology groups in dimension 2. We refer to [Bro94, Section

IV.3] for the general details and will present some results in the next section. For A nonabelian it is less familiar. A crucial difference is the following, arising from the fact that $\mathrm{Aut}(A) \cong \mathrm{Out}(A)$ if and only if A is abelian.

Recall that a group extension E induces an action $\theta : B \to \mathrm{Aut}(A)$ given by $b \mapsto \iota\, c_b\, \iota|_{A\iota}^{-1}$ as B acts on $A\iota \trianglelefteq B$ by conjugation and ι is injective. The action of θ on A is given by $(a)(b\theta)\iota = (a\iota)c_b$. Note that $A\iota\theta = \mathrm{Inn}(A)$. Hence there is a projection $\widetilde{\theta} : B/A\iota \to \mathrm{Aut}(A)/\mathrm{Inn}(A) = \mathrm{Out}(A)$. We have $\ker\theta = C_B(A\iota)$ so that $\ker\theta \cap A\iota = C_{A\iota}(A\iota) = Z(A\iota)$. As the sequence is exact, $A\iota = \mathrm{im}\,\iota = \ker\pi$ so the projection $\widetilde{\pi} : B/A\iota \to C$ is an isomorphism, hence there is $\widetilde{\pi}^{-1} : C \to B/A\iota$.

Therefore from the group extension a homomorphism is obtained satisfying $\psi = \widetilde{\pi}^{-1}\widetilde{\theta} : C \to \mathrm{Out}(A)$ given by $c \mapsto \iota\, c_b\, \iota|_{A\iota}^{-1}\,\mathrm{Inn}(A)$. This is the information that we will use when studying group extensions, as opposed to a homomorphism $\phi = \rho\theta : C \to \mathrm{Aut}(A)$ which we have in the semidirect product (split extension). Note that if A is abelian we have $\mathrm{Aut}(A) \cong \mathrm{Out}(A)$, so that $\widetilde{\theta}$ also gives an action $\phi : C \to \mathrm{Aut}(A)$.

We note now that congruent extensions give rise to the same induced action.

Lemma A.11. *If E and E' are congruent extensions then they induce the same homomorphism $\psi : C \to \mathrm{Out}(A)$.*

Proof. The congruent extensions E and E' determine the commutative diagram

$$\begin{tikzcd}
& & B \arrow[dd, "\beta"] \arrow[dr, "\pi"] & & \\
1 \arrow[r] & A \arrow[ur, "\iota"] \arrow[dr, "\iota'"'] & & C \arrow[r] & 1 \\
& & B' \arrow[ur, "\pi'"'] & &
\end{tikzcd}$$

We should compare $\psi = \widetilde{\pi}^{-1}\widetilde{\theta} : C \to \mathrm{Out}(A)$ with $\psi' = \widetilde{\pi}'^{-1}\widetilde{\theta}' : C \to \mathrm{Out}(A)$.

Let $c \in C$, we show that $c\psi = c\psi'$. Recall that $c\psi = \iota c_b \iota|_{A\iota}^{-1} \operatorname{Inn}(A)$ for some $b \in B$ with $b\pi = c$ and $c\psi' = \iota' c_{b'} \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A)$ for some $b' \in B'$ with $b'\pi' = c$.

As the diagram is commutative $\pi = \beta\pi'$, so that $b\beta\pi' = b\pi = c = b'\pi'$ and $(b\beta)^{-1}b' \in \ker \pi'$. That is there is $a \in A$ such that $b' = (b\beta)(a\iota')$. Similarly $\iota = \iota'\beta^{-1}$, and as $\operatorname{Inn}(A) \trianglelefteq \operatorname{Aut}(A)$ we have $\iota' c_{a\iota'} \iota'|_{A\iota'}^{-1} \in \operatorname{Inn}(A)$. Thus we have

$$\begin{aligned} c\psi' &= \iota' c_{b'} \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A) = \iota' c_{(b\beta)(a\iota')} \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A) = \iota' c_{b\beta} \iota'|_{A\iota'}^{-1} \iota' c_{a\iota'} \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A) \\ &= \iota' c_{b\beta} \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A) = \iota' \beta^{-1} c_b \beta \iota'|_{A\iota'}^{-1} \operatorname{Inn}(A) = \iota c_b \iota|_{A\iota}^{-1} \operatorname{Inn}(A) = c\psi \end{aligned}$$

and Lemma A.11 is proven. □

A.4 Low dimensional cohomology

As noted above, the problem of determining group extensions involves the cohomology groups in small dimension. We require them them for group extensions of $Z(Q)$, so we state them for abelian groups. Note that when we have a group extension of an abelian group A by G with action $\phi : G \to \operatorname{Aut}(A)$, the action ϕ makes A into a $\mathbb{Z}G$-module. Here we present the characterisations that we will use before applying them to our particular case.

Proposition A.12 ([Ben91, Proposition 3.7.2]). *Given a group G and a $\mathbb{Z}G$-module M, the cohomology group $H^1(G, M)$ is in one-to-one correspondence with the set of conjugacy classes of complements to the subgroup M in the split extension $G \ltimes M$.*

Theorem A.13 ([Bro94, Theorem IV.3.12]). *Let G be a group and M a $\mathbb{Z}G$-*

module. Then the set of congruence classes of extensions of M by G giving rise to the given homomorphism $\phi : G \to \mathrm{Aut}(M)$ is in bijection with $H^2(G, M)$. Under this bijection the split extension corresponds to the zero element of $H^2(G, M)$.

The higher dimensional interpretations get contrived, but in the case of finite cyclic groups they can be recovered from the results above.

Theorem A.14 ([ML63, Theorem IV.7.1]). *For a finite cyclic group C_m, a $\mathbb{Z}C_m$-module A and $n \geq 2$, $H^{2n}(C_m, A) = H^2(C_m, A)$ and $H^{2n-1}(C_m, A) = H^1(C_m, A)$.*

In the case in which we are interested we have $M = Z(Q) \cong C_p$, and $G \cong C_p$, so that since $p \nmid |\mathrm{Aut}(M)|$, G acts trivially on M. In particular, we can talk about $H^n(G, M)$ without needing to specify the action.

Lemma A.15. *Suppose $Z \cong C_p$ and $K \cong C_p$. Then Z is a trivial $\mathbb{Z}K$-module, and $H^1(K, Z) \cong H^2(K, Z) \cong H^3(K, Z) \cong C_p$.*

Proof. Note that K acts trivially on Z. Thus the split extension is the direct product $P \cong C_p \times C_p$. Therefore P contains $p + 1$ subgroups of order p, one of which is Z, hence there are p conjugacy classes of complements to Z in P. Proposition A.12 then implies that $H^1(K, Z) \cong C_p$.

For the determination of $H^2(K, Z)$ we look at group extensions of Z by K. Recall that K acts trivially on Z. Fix a generator z of Z and a generator k of K. For each $0 \leq a \leq p - 1$ we define a group

$$G_a = \langle l_a, c_a \mid c_a^p = 1, [l_a, c_a] = 1, l_a^p = c_a^a \rangle$$

and homomorphisms $\iota_a : Z \to G_a$ such that $z\iota_a = c_a$ and $\pi_a : G_a \to K$ with $l_a\pi_a = k$. Then each G_a is a group extension of Z by K hence it determines a short exact sequence

$$1 \to Z \xrightarrow{\iota_a} G_a \xrightarrow{\pi_a} K \to 1.$$

Now let $a, b \in \{0, \ldots, p-1\}$ and suppose G_a and G_b are congruent extensions. Then there is an isomorphism $\theta : G_a \to G_b$

$$\begin{tikzcd}
 & & G_a \arrow[dd, "\theta"] \arrow[dr, "\pi_a"] & & \\
1 \arrow[r] & Z \arrow[ur, "\iota_a"] \arrow[dr, "\iota_b"'] & & K \arrow[r] & 1 \\
 & & G_b \arrow[ur, "\pi_b"'] & &
\end{tikzcd}$$

so that $c_a\theta = z\iota_a\theta = z\iota_b = c_b$ and $l_a\theta\pi_b = l_a\pi_a = k = l_b\pi_b$ and therefore $l_a\theta l_b^{-1} \in \ker \pi_b = \langle c_b \rangle$. Thus $l_a\theta = l_b z^m$ for some $m \in \{0, \ldots p-1\}$.

Then $c_b^a = c_a^a\theta = (l_a)^p\theta = (l_a\theta)^p = l_b^p z^{mp} = c_b^b$, which requires $a \equiv b \pmod{p}$ and the p constructed groups are pairwise not congruent. Thus there are at least p congruence classes of group extensions of Z by K and $|H^2(K, Z)| \geq p$ by Theorem A.13.

Now consider an arbitrary group extension G of Z by K given by

$$1 \to Z \xrightarrow{\iota} G \xrightarrow{\pi} K \to 1.$$

Pick $l \in G$ such that $l\pi = k$. As K acts trivially on Z we have $[z\iota, l] = 1$. As $Z \cong C_p \cong K$ we have $(z\iota)^p = 1$ and $l^p \in \ker \pi$, that is $l^p = z^m$ for some $m \in \{0, \ldots p-1\}$. Thus G is a congruent extension to G_m via $\theta : G \to G_m$ determined by $z\iota\theta = c_m$ and $l\theta = l_m$. Hence any group extension of Z by K is congruent to one of the p above, and there are exactly p congruence classes of extensions of Z by K. Thus by Theorem A.13 $|H^2(K, Z)| = p$.

Finally, $H^3(K, Z) = H^1(K, Z)$ by Theorem A.14. $\square$

A.5 Extensions with nonabelian normal subgroup

Now we have all the tools we require to state the results used in the extension problem.

Definition A.16. *An* abstract kernel *is a triple* (C, A, ψ) *where* C *and* A *are (not necessarily abelian) groups and a homomorphism* $\psi : C \to \mathrm{Out}(A)$.

The problem becomes classifying all group extensions arising from a given abstract kernel. Recall that a group extension determines a map $\psi : C \to \mathrm{Out}(A)$ induced by the conjugation action $\theta : B \to \mathrm{Aut}(A)$ and so determines an abstract kernel. Here we consider the converse, that is when the given homomorphism $\psi : C \to \mathrm{Out}(A)$ extends to a homomorphism $\theta : B \to \mathrm{Aut}(A)$ and then how many extensions it yields which give rise to $\phi : C \to \mathrm{Aut}(A)$. In [ML63, §IV.8] this question is studied in detail. We offer a sketch.

For each $c \in C$, pick a map $c\phi \in \mathrm{Aut}(A)$ which is in the coset $c\psi \in \mathrm{Out}(A)$ and specify that $1_C\phi = 1_C$. Then $(x\phi)(y\phi)(xy\phi)^{-1}$ is an inner automorphism of A which we denote by $(x, y)f$. Thus $f : C \times C \to \mathrm{Aut}(A)$ is a map measuring how ϕ differs from a homomorphism from C into $\mathrm{Aut}(A)$. Studying the group axioms, particularly the associative law, gives rise to an *obstruction*, a map $k : C \times C \times C \to Z(A)$ satisfying the properties of a 3-cocycle [ML63, IV.(8.5'), p. 126]. That is k is an element of $H^3(C, Z(A))$ up to a quotient.

Note that since $Z(A)$ is abelian, the restriction of $c\psi$ to $Z(A)$ gives $Z(A)$ the structure of a C-module where $\mathrm{Inn}(A)$ acts trivially, so that any choice of automorphism $c\phi \in \mathrm{Aut}(A)$ which is a coset representative of the automorphism induced by $c\psi$ will give rise to the same action on $Z(A)$.

Theorem A.17 ([ML63, Theorem IV.8.7])**.** *Let* (C, A, ψ) *be an abstract kernel and* *interpret the centre $Z(A)$ as a C-module as above. The assignment to this abstract kernel of the cohomology class of any one of its obstructions yields a well-defined element of $H^3(C, Z(A))$. Furthermore, the abstract kernel has an extension if and only if one of its obstructions is 0.*

Theorem A.18 ([ML63, Theorem IV.8.8])**.** *Fix an abstract kernel (C, A, ψ). Then the group $H^2(C, Z(A))$ acts on the set of extensions of the abstract kernel simply transitively, so that given an extension any other extension can be obtained by operation with exactly one element of $H^2(C, Z(A))$.*

In particular, the set of congruence classes of extensions $1 \to A \to G \to C \to 1$ giving rise to $\psi : C \to \mathrm{Out}(A)$ is either empty or in one-to-one correspondence with $H^2(C, Z(A))$.

A note from the proof of Theorem A.18 is that non-congruent extensions give rise to different maps f, which can be chosen to be identically 0 in a split extension, and in particular, if the abstract kernel has an extension, it has a unique split extension.

Remark: if A is abelian then $A = Z(A)$ and Theorem A.18 reduces to Theorem A.13. A sufficient condition to guarantee the existence of group extensions of an abstract kernel is the following.

Lemma A.19. *Suppose $\mathrm{Aut}(A)$ splits over $\mathrm{Inn}(A)$. Then every abstract kernel (C, A, ψ) has $|H^2(C, Z(A))|$ extensions.*

Proof. As $\mathrm{Aut}(A)$ splits over $\mathrm{Inn}(A)$ we have $\rho : \mathrm{Out}(A) \to \mathrm{Aut}(A)$ such that $\mathrm{Out}(A)\rho \leq \mathrm{Aut}(A)$ and $\rho\pi = 1_{\mathrm{Out}(A)}$ where $\pi : \mathrm{Aut}(A) \to \mathrm{Out}(A)$ is the projection map. Hence for any element $c\psi \in \mathrm{Out}(A)$ we have $c\psi\rho \in \mathrm{Aut}(A)$, that is we have

$\psi\rho : C \to \mathrm{Aut}(A)$ and we can build a split extension $C \ltimes_{\psi\rho} A$ of the abstract kernel (C, A, ψ). Thus by Theorem A.18 it has $|H^2(C, Z(A))|$ extensions. $\square$

Lemma A.20. *Suppose (C, A, ψ) and (C, A, ψ_2) are two abstract kernels, let $\chi \in \mathrm{Out}(A)$ and $\mu \in \mathrm{Aut}(C)$ be such that the diagram*

$$\begin{tikzcd} C \arrow[r, "\psi"] \arrow[d, "\mu"'] & \mathrm{Out}(A) \arrow[d, "c_\chi"'] \\ C \arrow[r, "\psi_2"] & \mathrm{Out}(A) \end{tikzcd}$$

commutes. If $\mathrm{Aut}(A)$ *splits over* $\mathrm{Inn}(A)$ *then both abstract kernels have a split extension whose groups are isomorphic.*

In particular, the isomorphism type of the split extension of an abstract kernel (C, A, ψ) is unique up to conjugacy of $C\psi$ in $\mathrm{Out}(A)$*.*

Proof. We have $C\mu\psi_2 = C\psi c_\chi$. Since $\mathrm{Aut}(A)$ splits over $\mathrm{Inn}(A)$, with ρ the inverse of π, we define $\phi := \psi\rho : C \to \mathrm{Aut}(A)$ and $\phi_2 := \psi_2\rho : C \to \mathrm{Aut}(A)$, as in Lemma A.19.

Let $\sigma = \chi\rho$ be an element in $\mathrm{Aut}(A)$ which is in the coset of χ. Then $c_\sigma \in \mathrm{Inn}(\mathrm{Aut}(A))$ and $\mu \in \mathrm{Aut}(C)$ build a commuting diagram

$$\begin{tikzcd} C \arrow[r, "\phi"] \arrow[d, "\mu"'] & \mathrm{Aut}(A) \arrow[d, "c_\sigma"'] \\ C \arrow[r, "\phi_2"] & \mathrm{Aut}(A) \end{tikzcd}$$

as in Lemma A.6, which implies that $C \ltimes_\phi A \cong C \ltimes_{\phi_2} A$.

Now it $C \ltimes_{\phi_2} A$ is a split extension of the abstract kernel (C, A, ψ_2), that is that the projection $\phi_2\pi = \psi_2 : C \to \mathrm{Out}(A)$, which follows since $\phi_2\pi = \psi_2\rho\pi = \psi_2$ as $\rho\pi = id_{\mathrm{Out}(A)}$ by definition of the splitting of $\mathrm{Aut}(A)$ over $\mathrm{Inn}(A)$.

It remains to show that given an abstract kernel (with extension), only one of the extensions is split. This can be seen via the map $f : C \times C \to \mathrm{Aut}(A)$

mentioned earlier which can be seen to be 0 if the extension splits, and is different in each of the extensions by the proof of [ML63, Theorem 8.8].

Thus abstract kernels (C, A, ψ) and (C, A, ψ_2) give rise to the same isomorphism type of split extension. $\square$

APPENDIX B

FINITE SIMPLE GROUPS WHOSE SYLOW p-SUBGROUPS CONTAIN AN EXTRASPECIAL SUBGROUP OF INDEX p

The finite simple groups are the primary source of examples of saturated fusion systems which satisfy $O_p(\mathcal{F}) = 1$, and indicate part of the behaviour that arises when considering saturated fusion systems, as well as being required to determine which fusion systems are exotic or realisable. Our main goal in this chapter is to prove the following propositions.

Proposition B.1. *Suppose p is odd and G is a finite simple group whose Sylow p-subgroups S contain an extraspecial subgroup Q of index p. Then $|S| \leq p^6$, G is in Table B.1 and $\mathcal{F}_S(G)$ is isomorphic to one of the following.*

1. $\mathcal{F}_{S_p}(PSL_4(p))$, $\mathcal{F}_{S_p}(PSU_4(p))$, $\mathcal{F}_{S_p}(PSp_4(p))$, *$p$ odd; or* $\mathcal{F}_{S_p}(G_2(p))$, $p \neq 3$;
2. $\mathcal{F}_a = \mathcal{F}_S(PSU_3(8))$ *or* $\mathcal{F}_b = \mathcal{F}_S({}^3D_4(2))$ *with* $S \cong \langle 3^4, 9 \rangle$;
3. $\mathcal{F}_2 = \mathcal{F}_S(PSL_6(2))$, $\mathcal{F}_3 = \mathcal{F}_S(A_9)$, *or* $\mathcal{F}_4 = \mathcal{F}_S(A_{11})$ *with* $S \in \mathrm{Syl}_3(PSp_4(3))$;[1]

[1] $\mathcal{F}_1 = \mathcal{F}_S(PSp_4(3))$

4. $\mathcal{F}_S(PSL_5(11))$ *or* $\mathcal{F}_S(Co_1)$ *with* $S \in \mathrm{Syl}_5(PSp_4(5))$*;*

5. $\mathcal{F}_S(F_4(2))$ *or* $\mathcal{F}_S(HN)$ *with* $S \in \mathrm{Syl}_3(PSL_4(3))$*;*

6. $\mathcal{F}_S(PSL_6(4))$, $\mathcal{F}_S(McL)$, $\mathcal{F}_S(Co_2)$ *with* $S \in \mathrm{Syl}_3(PSU_4(3))$*;*

7. $\mathcal{F}_S(Ly)$, $\mathcal{F}_S(HN)$, $\mathcal{F}_S(BM)$ *with* $S \in \mathrm{Syl}_5(G_2(5))$*;*

8. $\mathcal{F}_S(M)$ *with* $S \in \mathrm{Syl}_7(G_2(7))$*.*

We note that if G is not a classical group of Lie type in characteristic p then $p \leq 7$

Outline of proof. G is determined for the alternating groups in Lemma B.10, groups of Lie type in characteristic p in Proposition B.9, and in cross characteristic (when p is odd) in Propositions B.13 (Classical) and B.14 (exceptional), and the sporadic groups are considered in Proposition B.15 and Table B.4. Then in Section B.5 we determine the isomorphism types of the fusion systems as follows: Lemma B.18 determines part (2), Lemma B.19 deals with part (3), part (4) is covered by Lemma B.20. Lemma B.21 proves parts (5) and (6), and finally Lemma B.22 concludes parts (7) and (8). Part (1) is determined as a collation of the Lemmas above. □

If $p = 2$ and G is not a group of Lie type in odd characteristic then we prove the following.

Proposition B.2. *If* $p = 2$ *and* G *is a finite simple group that is not a group of Lie type in odd characteristic with* $S \in \mathrm{Syl}_2(p)$ *containing an extraspecial subgroup of index* 2 *then* G *is one of* $PSL_4(2) \cong A_8$, A_9, $PSU_4(2)$, M_{11}, M_{12}, *and* $\mathcal{F}_S(G)$ *is isomorphic to exactly one of* $\mathcal{F}_S(PSL_4(2))$, $\mathcal{F}_S(PSU_4(2))$, $\mathcal{F}_S(M_{11})$ *or* $\mathcal{F}_S(M_{12})$.

G	p	S	Congruences	Notes
$PSL_4(p)$	all	$<p^6, a_1>$		
$PSU_4(p)$	all	$<p^6, a_2>$		
$PSp_4(p)$	all	$<p^4, 7>$		
$G_2(p)$	$p \geq 5$	$<p^6, a_3>$		
A_9, A_{10}	3	$<3^4, 7>$		$\mathcal{F}_3$
A_{11}	3	$<3^4, 7>$		$\mathcal{F}_4$
$PSL_3(q)$	3	$<3^4, 9>$	$q \equiv 10, 19 \pmod{27}$	$\mathcal{F}_a$
$PSL_4(q)$	3	$<3^4, 7>$	$q \equiv 4, 7 \pmod 9$	$\mathcal{F}_1$
$PSL_6(q)$	3	$<3^6, 321>$	$q \equiv 4, 7 \pmod 9$	$\mathcal{F}_D$
$PSL_6(q)$	3	$<3^4, 7>$	$q \equiv 2, 5 \pmod 9$	$\mathcal{F}_2$
$PSL_7(q)$	3	$<3^4, 7>$	$q \equiv 2, 5 \pmod 9$	$\mathcal{F}_2$
$PSL_5(q)$	5	$<5^4, 7>$	$q \equiv 6, 11, 16, 21 \pmod{25}$	$\mathcal{F}_c$
$PSU_3(q)$	3	$<3^4, 9>$	$q \equiv 8, 17 \pmod{27}$	$\mathcal{F}_a$
$PSU_4(q)$	3	$<3^4, 7>$	$q \equiv 2, 5 \pmod 9$	$PSU_4(2) \cong PSp_4(3)$. $\mathcal{F}_1$
$PSU_6(q)$	3	$<3^6, 321>$	$q \equiv 2, 5 \pmod 9$	$\mathcal{F}_D$
$PSU_6(q)$	3	$<3^4, 7>$	$q \equiv 4, 7 \pmod 9$	$\mathcal{F}_2$
$PSU_7(q)$	3	$<3^4, 7>$	$q \equiv 4, 7 \pmod 9$	$\mathcal{F}_2$
$PSU_5(q)$	5	$<5^4, 7>$	$q \equiv 4, 9, 14, 19 \pmod{25}$	$\mathcal{F}_c$
$PSp_6(q)$	3	$<3^4, 7>$	$q \equiv 2, 4, 5, 7 \pmod 9$	$PSp_6(2) \cong P\Omega_7(2)$. $\mathcal{F}_2$
$P\Omega_7(q)$	3	$<3^4, 7>$	$q \equiv 2, 4, 5, 7 \pmod 9$	$\mathcal{F}_2$
$P\Omega_6^+(q)$	3	$<3^4, 7>$	$q \equiv 4, 7 \pmod 9$	$\mathcal{F}_1$
$P\Omega_6^-(q)$	3	$<3^4, 7>$	$q \equiv 2, 5 \pmod 9$	$\mathcal{F}_1$
$P\Omega_8^-(q)$	3	$<3^4, 7>$	$q \equiv 2, 4, 5, 7 \pmod 9$	$\mathcal{F}_2$
${}^3D_4(q)$	3	$<3^4, 9>$	$q \equiv 2, 4, 5, 7 \pmod 9$	$\mathcal{F}_b$
$F_4(q)$	3	$<3^6, 307>$	$q \equiv 2, 4, 5, 7 \pmod 9$	$\mathcal{F}_E$
$E_6(q)$	3	$<3^6, 307>$	$q \equiv 2, 5 \pmod 9$	$F_4(q) \leq E_6(q)$. $\mathcal{F}_E$
${}^2E_6(q)$	3	$<3^6, 307>$	$q \equiv 4, 7 \pmod 9$	$F_4(q) \leq {}^2E_6(q)$. $\mathcal{F}_E$
$\boldsymbol{Co_1}$	5	$<5^4, 7>$		
$\boldsymbol{McL}$	3	$<3^6, 321>$		$PSU_4(3) \leq_{Max} McL$
$\boldsymbol{Co_2}$	3	$<3^6, 321>$		$McL \leq_{Max} Co_2$
$\boldsymbol{Ly}$	5	$<5^6, 643>$		$G_2(5) \leq_{Max} Ly$
$\boldsymbol{HN}$	3	$<3^6, 307>$		$S \cong S_3(PSL_4(3))$
$\boldsymbol{HN}$	5	$<5^6, 643>$		$S \cong S_5(G_2(5))$
$\boldsymbol{BM}$	5	$<5^6, 643>$		$HN \leq BM$
$\boldsymbol{M}$	7	$<7^6, 807>$		$S \cong S_7(G_2(7))$

Table B.1: Finite simple groups whose Sylow p-subgroups have an extraspecial subgroup of index p when p is odd.

We remark that the groups $G_2(2) \cong PSU_3(3) : C_2$ and $PSp_4(2) \cong S_6$ also contain Sylow 2-subgroups with Q extraspecial of index 2, but they are not simple.

Outline of proof. The possibilities for G are determined in Lemma B.10, Proposition B.9 and Proposition B.15, and those for $\mathcal{F}_S(G)$ in Lemma B.16. $\square$

We now gather some particular cases of S in their own corollaries, as well as setting up notation. Note for example that when p is odd Corollary B.3 coincides with [PS18, Theorem 2.11].

Corollary B.3. *Suppose G is a finite simple group with $S \in \mathrm{Syl}_p(G)$ isomorphic to a Sylow p-subgroup of $G_2(p)$. Then either $G \cong G_2(p)$ or one of the following holds:*

1. *$p = 2$ and G is either M_{12} or a group of Lie type in odd characteristic;*
2. *$p = 5$, and G is one of B, HN, Ly;*
3. *$p = 7$ and $G \cong M$.*

When $|S| = p^4$ all but two examples of finite simple groups are on a Sylow p-subgroup of $PSp_4(p)$, hence we have the following, where we omit $p = 2$ since its Sylow 2-subgroups are isomorphic to $D_8 \times C_2$, and any examples will arise from groups of Lie type in odd characteristic.

Corollary B.4. *Suppose $p \neq 2$, G is a finite simple group and $S \in \mathrm{Syl}_p(G)$ is isomorphic to a Sylow p-subgroup of $PSp_4(p)$. Then either $G \cong PSp_4(p)$ or one of the following holds:*

1. *p=3 and we get the following groups with $S \cong C_3 \wr C_3$:*

when $q \equiv 4, 7 \pmod 9$*:* $PSL_4(q)$*,* $PSU_6(q)$*,* $PSU_7(q)$*,* $P\Omega_6^+(q)$*;*

when $q \equiv 2, 5 \pmod 9$*:* $PSU_4(q)^1$*,* $PSL_6(q)$*,* $PSL_7(q)$*,* $P\Omega_6^-(q)$*;*

when $q \equiv 2, 4, 5, 7 \pmod 9$*:* $PSp_6(q)$*,* $P\Omega_7(q)$*,* $P\Omega_8^-(q)$*;*

A_9*,* A_{10}*,* A_{11}*.*

2. $p = 5$ *and* G *is* $PSL_5(q)$ *for* $q \equiv 6, 11, 16, 21 \pmod{25}$*;* $PSU_5(q)$ *whenever* $q \equiv 4, 9, 14, 19 \pmod{25}$*; or* Co_1*.*

3. $p > 5$ *and* $G \cong PSp_4(p)$*.*

When there may be confusion about which prime a Sylow p-subgroup of G is over, we will write it as $S_p(G)$. We will show in Lemma B.17 that every row in the table gives rise to a single isomorphism class of fusion systems. We will denote the cross characteristic fusion systems by $\mathcal{F}_a \cong \mathcal{F}_{S_3}(PSL_3(19))$, and $\mathcal{F}_b \cong \mathcal{F}_{S_3}({}^3D_4(2))$ when $S \cong <3^4, 9>$; by $\mathcal{F}_c \cong \mathcal{F}_{S_5}(PSL_5(11))$ that with $p = 5$; and by $\mathcal{F}_D \cong \mathcal{F}_{S_3}(PSL_6(4))$ and $\mathcal{F}_E \cong \mathcal{F}_{S_3}(F_4(2))$ those with $|S| = 3^6$. When $S \cong C_3 \wr C_3$ we will denote the fusion systems in Table B.1 by $\mathcal{F}_1 \cong \mathcal{F}_{S_3}(PSp_4(3))$, $\mathcal{F}_2 \cong \mathcal{F}_{S_3}(PSL_6(2))$, $\mathcal{F}_3 \cong \mathcal{F}_{S_3}(A_9)$, and $\mathcal{F}_4 \cong \mathcal{F}_{S_3}(A_{11})$. It will also be determined that the fusion systems of the sporadic simple groups are not isomorphic to any other fusion system on the table.

If a fusion system $\mathcal{F}$ is simple and realisable, then we have the following result about the smallest groups realising $\mathcal{F}$.

Theorem B.5 ([Cra11, Theorem 5.71]). *Let* $\mathcal{F}$ *be a simple fusion system on a p-group* P*, and suppose that* $\mathcal{F}$ *is realised by a finite group* G*. Suppose that*

[1] $PSp_4(3) \cong PSU_4(2)$ by Proposition 1.19 (15)

$O_{p'}(G) = 1$ and that $\mathcal{F}_P(G) \neq \mathcal{F}_P(H)$ for any proper subgroup H of G containing P. Then G is simple.

Thus if a simple fusion system $\mathcal{F}$ comes from a finite group G, and G is chosen smallest possible, then G is a simple group. However not all fusion systems of finite simple groups are simple, but we have the following, which is a consequence of a result of Flores and Foote [FF09] and allows us to use the Reduction Theorem 4.27 to restrict the structure of S when p is odd. We begin with a piece of notation.

Definition B.6. *A nonabelian finite simple group G is p-Goldschmidt if $N_G(S)$ controls p-fusion in G, that is $\mathcal{F}_S(G) = \mathcal{F}_S(N_G(S))$.*

Proposition B.7. *Suppose G is a nonabelian finite simple group, $S \in \mathrm{Syl}_p(G)$ and S contains an extraspecial subgroup of index p. Then $O_p(\mathcal{F}_S(G)) = 1$.*

Proof. Let $H := O_p(\mathcal{F}_S(G))$ and suppose $H \neq 1$. Then $H \trianglelefteq \mathcal{F}_S(G)$, where $\mathcal{F}_S(G)$ is a saturated fusion system on S, and $N_G(H)$ controls p-fusion in G (that is $\mathcal{F}_S(G) = \mathcal{F}_S(N_G(H))$). Thus if $H = S$ then G is p-Goldschmidt by definition. Otherwise $1 \neq H < S$ so H is a proper nontrivial subgroup of S strongly closed in S with respect to $\mathcal{F}_S(G)$ by Proposition 2.25, and $H \leq E$ for every $\mathcal{F}_S(G)$-essential subgroup E. Then [Asc11, Theorem 15.8 (Flores-Foote)] ([AKO11, Theorem II.12.12]) implies that either G is p-Goldschmidt, or $p = 3$, $G \cong G_2(q)$ with $q \equiv \pm 1 \pmod 9$, and $H = Z(S)$ has order 3. In this case $|G| = q^6(q^6 - 1)(q^2 - 1) = q^6(q+1)(q^2 - q + 1)(q - 1)(q^2 + q + 1)(q + 1)(q - 1)$. Let a be the largest power such that $3^a \mid q \pm 1$, then a is even as $q \equiv \pm 1 \pmod 9$, so $|S| = 3^{1+2a}$ has odd exponent and S cannot have an extraspecial subgroup of index p.

If G is p-Goldschmidt then [Asc11, Theorems 15.6 and Remark 15.7] together imply that either S is abelian, G is a group of Lie type in characteristic p of Lie rank 1, $S \cong p^{1+2}$, or $G = J_3$ for $p = 3$ (where $|S| = 3^5$ by [CCN$^+$85]). The group S cannot have an extraspecial subgroup of index p in any of these cases, which we now justify in the rank 1 case. These are:

1. $PSL_2(p^n)$, with S abelian;

2. $PSU_3(p^n)$, with S special;

3. ${}^2B_2(2^{2n+1})$, where $|Z(S)| = 2^{2n+1}$, whereas ${}^2B_2(2) \cong C_5$ ([GLS98, Theorem 2.2.7]);

4. ${}^2G_2(3^{2n+1})$, with $|S| = 3^{6n+3}$.

Hence none of the above S have an extraspecial subgroup of index p, and the proposition follows. $\square$

This result allows us to use Theorem 4.27 to conclude.

Corollary B.8. *Suppose p is odd, G is a finite simple group with $S \in \mathrm{Syl}_p(G)$ containing an extraspecial subgroup Q of index p. Then $|Z(S)| = p$ and either $|S| \in \{p^4, p^6\}$ or $p \geq 11$, $|S| = p^{p-1}$ and S has maximal nilpotency class and exponent p.*

Proof. Let G be a finite simple group and $S \in \mathrm{Syl}_p(G)$. If G is abelian then S cannot contain an extraspecial subgroup of index p. If G is nonabelian then Proposition B.7 implies that $O_p(\mathcal{F}_S(G)) = 1$, and Theorem 4.2 implies that $Z(S) = Z(Q)$ has order p. If $|S| = p^4$ we are done, so we may assume $|S| \geq p^6$, and $\mathcal{F} = \mathcal{F}_S(G)$ satisfies all properties of Theorem 4.27. If S is in cases (1), (2), (3) or (4) then

$|S| = p^6$, whereas in case (5) we have $p \geq 11$, S has order p^{p-1}, maximal nilpotency class and exponent p. Thus in all cases the corollary holds. $\square$

We now consider each of the families of finite simple groups separately, with p being an arbitrary prime except in the groups of Lie type in cross characteristic, where we assume that p is odd.

B.1 Groups of Lie type in defining characteristic

Proposition B.9. *Suppose G is a finite simple group of Lie type in characteristic p and let $S \in \mathrm{Syl}_p(G)$. Then S contains an extraspecial subgroup of index p if and only if G is one of $A_3(p) \cong PSL_4(p)$, ${}^2A_3(p) \cong PSU_4(p)$, $B_2(p) \cong PSp_4(p)$ for any prime p, or $G_2(p)$ for $p \geq 5$.*[1]

Proof. We use notation from [GLS98]. Consider $N_G(X_{-\alpha_*})$, the normaliser in $G \in Lie(p)$ of the lowest root $-\alpha_*$ with respect to a fundamental root system Π of G. Let $S \in \mathrm{Syl}_p(G)$, as in [GLS98, Example 3.2.6 and Theorem 3.3.1], which imply that we have $X_{-\alpha_*} \leq U_a \leq Z(S) \leq S$, so $S \leq N_G(X_{-\alpha_*})$. Thus, by Lemma 1.27, either $S \cong Q \times O_p(N_G(X_{-\alpha_*}))$, or $S/O_p(N_G(X_{-\alpha_*}))$ is elementary abelian, or $O_p(N_G(X_{-\alpha_*})) \leq Q$. The direct product does not happen since $Z(S) \cap Q \neq 1$. We now consider the case $O_p(N_G(X_{-\alpha_*})) \leq Q$, where we have

$$X_{-\alpha_*} \leq O_p(N_G(X_{-\alpha_*})) \cap Z(S) \leq Q \cap Z(S) = Z(Q)$$

so, as $X_{-\alpha_*} \neq 1$, we have $X_{-\alpha_*} = Z(Q)$. Then $[Q, O_p(N_G(X_{-\alpha_*}))] \leq [Q, Q] = Z(Q) = X_{-\alpha_*}$, thus Q centralises the normal chain $1 \trianglelefteq X_{-\alpha_*} \trianglelefteq O_p(N_G(X_{-\alpha_*}))$,

[1]Note that $G_2(2)$ and $PSp_4(2)$ are not simple, but S has an extraspecial subgroup of index 2.

and by Lemma 1.37 we have $Q \leq O_p(N_G(X_{-\alpha_*}))$. In this case they are equal, so $S/O_p(N_G(X_{-\alpha_*}))$ is abelian of order p. Thus in any case $S/O_p(N_G(X_{-\alpha_*}))$ is elementary abelian.

From [GLS98, Example 3.2.6] we can see that $I_{-\alpha*} = N_G(X_{-\alpha_*}) = P_J$ where $J = \Pi \cap \alpha_*^\perp$. By the same discussion we see that J is the root system associated to the affine Dynkin diagram in [GLS98, Table 1.8] left when removing the darkened vertex (corresponding to the lowest root) and any adjacent ones. Thus, since $S/O_p(N_G(X_{-\alpha_*}))$ is elementary abelian and nontrivial, the remaining Dynkin diagram cannot have any edges. The only possible diagrams are A_3, B_2, B_3, G_2 and D_4, and the groups with those diagrams are $A_3(q)$, $B_2(q)$, $B_3(q)$, $G_2(q)$, $D_4(q)$, and the twisted groups ${}^2A_4(q)$, ${}^2A_3(q)$, ${}^2D_4(q)$ and ${}^3D_4(q)$ by [Car72, Section 13.3]. Now if G is not one of $G_2(p^k)$ for $p = 2, 3$, $B_2(2^k)$, ${}^2B_2(2^{2m+1})$, ${}^2G_2(3^{2m+1})$, we can apply [GLS98, Theorem 3.3.1 (a)] to see that $\mathbb{F} \leq Z(S) = U_J^a \leq U_J^2 = \Phi(S) \leq Q$, so we need the field to have order p, otherwise the centre is too big.

For the exceptions above, we have the following.

For $G_2(2^k)$ we can use part (b) of [GLS98, Theorem 3.3.1] to still obtain that $\mathbb{F} \leq Z(S) = U_a \leq U_2 \leq \Phi(S) \leq Q$, so we need the field to have order 2. But by [GLS98, Theorems 2.2.7 and 2.2.10] $G_2(2)$ is not simple and $G_2(2)' \cong {}^2A_2(3)$ has Sylow 2-subgroups of order 2^5. Thus none of the $G_2(2^k)$ with $k \geq 2$ has any extraspecial subgroups of index p. However the Sylow 2-subgroups of $G_2(2) \cong PSU_3(3) : C_2$ do contain an extraspecial subgroup of index 2, checked computationally via:

```
#[i:i in MaximalSubgroups(Sylow(G2(2),2))|IsExtraSpecial(i`subgroup)];
1
```

In $G_2(3^k)$ we have $|Z(S)| = 3^{2k}$ by [GLS98, Theorem 3.3.1 (c)] so we need $k = 1$. But $G_2(3)$ has $Z(S) \cong C_3 \times C_3$, which contradicts Corollary B.8.

$B_2(2^k)$: Similarly we have $|Z(S)| = 2^{2k}$ so we need $k = 1$. But $B_2(2) \cong S_6$ is not simple, and $B_2(2)' \cong A_6$ by [GLS98, Theorem 2.2.10], which has Sylow 2-subgroups of order 2^3, so it cannot have an extraspecial subgroup of index 2. We note however that $B_2(2) \cong S_6$ does have Sylow 2-subgroups isomorphic to $C_2 \wr C_2 \times C_2 = D_8 \times C_2$, which do contain an extraspecial subgroup D_8 of index 2. In the SmallGroups notation it is $<2^4, 11>$.

${}^2B_2(2^{2m+1})$ has Sylow 2-subgroups whose centre has order 2^{2m+1}, so we need $m = 0$. This gives ${}^2B_2(2)$ which is not simple, and ${}^2B_2(2)' \cong C_5$ by [GLS98, Theorem 2.2.7].

${}^2G_2(3^{2m+1})$ has $|S| = 3^{6m+3}$, whose order has odd exponent, thus no extraspecial subgroups of index 3.

In the cases it remains to consider the field has order p, hence they are $A_3(p)$, $D_4(p)$, $B_2(p)$ for $p \geq 3$, $B_3(p)$, $G_2(p)$ for $p \geq 5$, and the twisted ones ${}^2A_3(p)$, ${}^2A_4(p)$, ${}^2D_4(p)$ and ${}^3D_4(p)$.

For $A_3(p)$ note that $|S| = p^6$. Consider a positive system of roots with fundamental subsystem $\Pi = \{a, b, c\}$. Let $J = \{a, c\}$. Then by [GLS98, Theorem 3.2.2] we see that U_J has nilpotency class 2, $|U_J^1| = p^5$, $|U_J^2| = p$ and $U_{\{a+b+c\}} = U_J^2 = \Phi(U_J) = U_J' = Z(U_J)$. Thus U_J is extraspecial of index p in S.

In ${}^2A_3(p)$ we have by [Wil09, Theorem 3.9 (ii)] with $k = 1$ a subgroup of type $p^{1+4}.SU_2(p)$ as the stabiliser of a totally isotropic 1-space, where we can see an extraspecial subgroup of index p in its Sylow p-subgroups. Note that the statement in the book is not correct, but the amended version can be found in `http://www.maths.qmul.ac.uk/~raw/TFSG.html`. Hence we always have an extraspecial subgroup of index p in this case.

For $B_2(p) \cong PSp_4(p)$ we note that $|S| = p^4$. If $p \geq 3$ we can again use [GLS98, Theorem 3.2.2] with a positive root system with fundamental subsystem $\Pi = \{a, b\}$ where a is short. Let $J = \{a\}$, then U_J has nilpotency class 2, $|U_J^1| = p^3$, $|U_J^2| = p$ and $U_{\{2a+b\}} = U_J^2 = \Phi(U_J) = U_J' = Z(U_J)$. Thus U_J is extraspecial of index p in S. If $p \geq 5$ then $|S| = p^4 \leq p^p$ so S is regular by Lemma 1.5 (2), thus as it is generated by elements of order p, it has exponent p by Theorem 1.7. Then Lemma 3.11 implies $S \cong \langle p^4, 7\rangle$. When $p = 3$ a Magma calculation checks that $S \cong C_3 \wr C_3 \cong \langle 3^4, 7\rangle$:

```
> IdentifyGroup(Sylow(PSp(4,3),3));
<81, 7>
```

Similarly for $G_2(p)$ note that $|S| = p^6$. If $p \geq 5$ then G is $\overline{U}$-nonsingular, hence we can apply [GLS98, Theorem 3.2.2] with positive root system with fundamental subsystem $\Pi = \{a, b\}$ with a short and $J = \{b\}$ to see again that U_J has nilpotency class 2, $|U_J^1| = p^5$, $|U_J^2| = p$ and $U_{\{3a+2b\}} = U_J^2 = \Phi(U_J) = U_J' = Z(U_J)$. Thus U_J is again extraspecial of index p in S.

In $B_3(p) \cong PSp_6(p)$ the Sylow p-subgroups have order p^9, which has odd exponent, hence no extraspecial subgroups of index p.

If $G = {}^{\epsilon}D_4(p)$ for $\epsilon \in \{1, 2\}$ then there is respectively parabolic subgroups of shape $C_p^6.(GL_1(p) \times GO_6^+(p))$ and $C_p^6.(GL_1(p) \times GO_6^-(p))$, hence the Sylow p-subgroups of $GO_6^+(p)$ and $GO_6^-(p)$ must contain abelian subgroups of index p by Lemma 1.27 do not contain any abelian subgroups of index p by Lemma 1.24. However we have $P\Omega_6^+(q) \cong PSL_4(q)$ and $P\Omega_6^-(q) \cong PSU_4(q)$ by Proposition 1.19 (7), hence their Sylow p-subgroups contain no abelian subgroups of index p

and we have a contradiction. Thus S has no extraspecial subgroups of index p.

Now ${}^3D_4(p)$ has $|S| = p^{12}$ and has p-rank 5 by [GLS98, Theorem 3.3.3], which is too small since an extraspecial subgroup of index p would have p-rank 6 by Lemma 1.17.

In ${}^2A_4(p)$ we similarly contain a subgroup M of shape $H.SU_3(p)$ where $H \cong p^{1+6}$, but in this case a Sylow p-subgroup S has order p^{10}. If S contained $Q \cong p_{\pm}^{1+8}$, since the Sylow p-subgroups of $PSU_3(p)$ are not elementary abelian, by Lemma 1.27 $H \leq Q$. But then Q centralises the normal chain $1 \trianglelefteq Z(H) \trianglelefteq H$ so by Lemma 1.37 $Q \leq O_p(M) = H$, a contradiction. Thus there cannot be any extraspecial subgroup of index p in S.

Therefore the only (simple) groups of Lie type in characteristic p whose Sylow p-subgroups contain an extraspecial subgroup of index p are $A_3(p) \cong PSL_4(p)$, ${}^2A_3(p) \cong PSU_4(p)$, $B_2(p) \cong PSp_4(p)$ when $p \geq 3$, $G_2(p)$ when $p \geq 5$. We claim their Sylow p-subgroups are pairwise non-isomorphic except $S_2(A_3(2)) \cong S_2({}^2A_3(2))$. Those of $PSp_4(p)$ have order p^4, whereas the rest have $|S| = p^6$, and those of $G_2(p)$ have nilpotency class 5 (if $p \geq 5$), whereas the Sylow p-subgroups of $PSL_4(p)$ and $PSU_4(p)$ have nilpotency class 3. Finally, the latter two can be distinguished when p is odd by Lemma 1.34.

When $p = 2$ we can check computationally that $S_2(A_3(2)) \cong S_2({}^2A_3(2))$ and they are not isomorphic to $S_2(G_2(2))$:

```
> IdentifyGroup(Sylow(PSL(4,2),2));
<64, 138>
> IdentifyGroup(Sylow(PSU(4,2),2));
<64, 138>
```

```
> IdentifyGroup(Sylow(G2(2),2));
<64, 134>
```

□

B.2 Alternating groups

We now consider the symmetric and alternating groups. We note for completeness that $PGL_2(9)$ and M_{10}, which are maximal subgroups of $\mathrm{Aut}(A_6)$ have respectively dihedral and semidihedral Sylow 2-subgroups of order 16, which contain extraspecial subgroups of index 2.

Lemma B.10. *Suppose that $G = A_n$ is an alternating group or $G = S_n$ a symmetric group. The only Sylow p-subgroups of G with an extraspecial p-group of index p are those of A_9, A_{10}, A_{11}, S_9, S_{10}, S_{11} with $S \cong C_3 \wr C_3$ when $p = 3$, those of S_6 and S_7 with $S \cong D_8 \times C_2$ when $p = 2$, and those of A_8, A_9, with S isomorphic to a Sylow 2-subgroup of $PSL_4(2)$ also when $p = 2$.*

Proof. By [Hup67, Theorem III.15.3] a Sylow p-subgroup of S_n is a direct product of Sylow p-subgroups of S_{p^k} which are of the form $B_k := C_p \wr C_p \wr ... \wr C_p$ (k wreathed factors). If we have more than one B_k factor, then Lemma 1.29 implies that $S = Q \times C_p = B_{k_1} \times B_{k_2}$, which is only possible if $p = 2$, $B_{k_1} = B_2 = C_2 \wr C_2 \cong D_8$ and $B_{k_2} = C_2$, which happens only in S_6 and S_7. This can also be seen as $S_6 \cong PSp_4(2)$. Otherwise S does not have an extraspecial subgroup of index p by Lemma 1.29 and we can focus on the B_k.

If $p \neq 2$ then B_k is also a Sylow p-subgroup of A_{p^k}. By Lemma 1.28 then $p = 3$ and $S \cong C_3 \wr C_3$. This happens only in S_9, S_{10}, S_{11}, A_9, A_{10} and A_{11}, all of which have isomorphic Sylow 3-subgroups.

If $p = 2$ the Sylow 2-subgroups H of A_{2^k} have index 2 in B_k. Since any cycle of even length is an odd permutation, the exponent of $S \in \mathrm{Syl}_2(A_{2^k})$ is 2^{k-1}, so $k \leq 4$ by Lemma 1.23. If $k \leq 2$ then $|H| \leq 2^{1+2-1}$ which is too small, and if $k = 3$ we get $|H| = p^6$, and by Proposition 1.19 (13) we have $A_8 \cong PSL_4(2)$, so by Proposition B.9 it has an extraspecial subgroup of index 2. A_9 has isomorphic Sylow 2-subgroups to those of A_8.

If $k = 4$ we look at A_{16}, which has an irreducible section of the natural permutation representation in characteristic 0 of dimension 15. But since its Sylow 2-subgroups have order 2^{14}, an extraspecial subgroup Q of order 2^{13} would have its smallest nonlinear representations of dimension $2^6 = 64$ by Lemma 1.18, a contradiction. Thus this does not happen. $\square$

B.3 Groups of Lie type in cross characteristic when $p \neq 2$

B.3.1 Classical groups

Throughout this section we assume $p \neq 2$.

Lemma B.11. *Suppose $b, c, p \in \mathbb{Z}_{>0}$. Let $n_b := \left\lfloor \frac{c}{b} \right\rfloor$. Then for all $a > 0$ we have $n_a \geq p n_{ap}$.*

Proof. We can write $c = an_a + t$ with $0 \leq t < a$, and $c = apn_{ap} + ka + s$ where $0 \leq k < p$, $0 \leq s < a$. Thus $a(n_a - pn_{ap}) = c - t - (c - ka - s) = ka + s - t$. Then, if $k = 0$, this gives two expressions of c/a with residues s and t, so we have $s = t$ and $n_a - pn_{ap} = 0$. If $k \geq 1$ then $a(n_a - pn_{ap}) = ka + s - t \geq a - a = 0$.

In either case the lemma holds. $\square$

Lemma B.12. *Suppose that $p \neq 2$. Let G be a finite classical group of Lie type in characteristic $r \neq p$, and X be the corresponding classical simple group. Then the Sylow p-subgroups of X and those of G are isomorphic except when $G \cong GL_n(q)$ and $p \mid q-1$ or $G \cong GU_n(q)$ and $p \mid q+1$.*

Proof. If $G \cong GL_n(q)$ then $X \cong PSL_n(q) = SL_n(q)/Z(SL_n(q))$ where we have $|GL_n(q) : SL_n(q)| = q-1$ and $|Z(SL_n(q))| = (n, q-1)$ by [GLS98, Theorem 2.2.7] or [KL90, Tables 2.1C and 2.1D]. Thus if $p \nmid q-1$ the Sylow p-subgroups of G and X are isomorphic.

If $G \cong GU_n(q)$ then $X \cong PSU_n(q) = SU_n(q)/Z(SU_n(q))$ where we have $|GU_n(q) : SU_n(q)| = q+1$ and $|Z(SU_n(q))| = (n, q+1)$ by [GLS98, Theorem 2.2.7], so if $p \nmid q+1$ the Sylow p-subgroups of G and X are isomorphic.

If $G \cong O_n^\epsilon(q)$ then $X \cong P\Omega_n^\epsilon(q)$. By [CCN+85, Section 2.4, p. xi-xii] we have that any $M \in O_n^\epsilon(q)$ satisfies $MM^T = 1$ hence $\det(M) = \pm 1$ and $|O_n^\epsilon(q) : SO_n^\epsilon(q)| = 2$. Further, $|Z(SO_n^\epsilon(q))| = (2, q-1)$. Also $|SO_n^\epsilon(q) : \Omega_n^\epsilon(q)| \leq 2$, and X is its image in $PSO_n^\epsilon(q)$ of index at most 2. Thus $|O_n^\epsilon(q)|$ and $|P\Omega_n^\epsilon(q)|$ differ by a factor of a power of 2 and their Sylow p-subgroups are isomorphic.

If $G \cong Sp_{2m}(q)$ then $X \cong PSp_{2m}(q)$ and by [GLS98, Theorem 2.2.7] we have $|Z(Sp_{2m}(q))| = 2$ and the Sylow p-subgroups of $Sp_{2m}(q)$ and $PSp_{2m}(q)$ are isomorphic. $\square$

Proposition B.13. *Suppose that $p \neq 2$. If a Sylow p-subgroup S of a classical simple group G of Lie type in characteristic r for $p \neq r$ contains an extraspecial subgroup of index p, then G, S, p, $q = r^v$ are as follows:*

- *In the linear case $PSL_n(q)$ we have one of:*

$p = 3$: $n = 3$ and $q \equiv 10, 19 \pmod{27}$ with $S \cong <81, 9>$;

$n = 4$ and $q \equiv 4, 7 \pmod 9$, with $S \cong C_3 \wr C_3$;

$n = 6$ and $q \equiv 4, 7 \pmod 9$ with $S \cong S_3(PSU_4(3)) \cong S_3(^2A_3(3))$;

$n = 6, 7$ and $q \equiv 2, 5 \pmod 9$ with $S \cong C_3 \wr C_3$.

Or $p = 5$, $n = 5$ and $q \equiv 6, 11, 16, 21 \pmod{25}$ with $S \cong <625, 7>$.

- *In the unitary case $PSU_n(q)$ we get the following list:*

  For $p = 3$: $n = 3$ and $q \equiv 8, 17 \pmod{27}$ with $S \cong <81, 9>$;

  $n = 4$ and $q \equiv 2, 5 \pmod 9$, with $S \cong C_3 \wr C_3$;

  $n = 6$ and $q \equiv 2, 5 \pmod 9$ with $S \cong S_3(PSU_4(3)) \cong S_3(^2A_3(3))$;

  $n = 6, 7$ and $q \equiv 4, 7 \pmod 9$, with $S \cong C_3 \wr C_3$.

  For $p = 5$, $n = 5$ and $q \equiv 4, 9, 14, 19 \pmod{25}$ with $S \cong <625, 7>$.

- *In the symplectic case $PSp_n(q)$ we get: $p = 3$, $S \cong C_3 \wr C_3$ whenever G is$PSp_6(q)$ and $q \equiv 2, 4, 5, 7 \pmod 9$.*

- *In the orthogonal case $P\Omega_n^{\pm}(q)$ we get $p = 3$ and $S \cong C_3 \wr C_3$ in the cases:*

  $P\Omega_6^+(q)$ when $q \equiv 4, 7 \pmod 9$,

  $P\Omega_6^-(q)$ when $q \equiv 2, 5 \pmod 9$,

  $P\Omega_7(q)$ when $q \equiv 2, 4, 5, 7 \pmod 9$,

  $P\Omega_8^-(q)$ when $q \equiv 2, 4, 5, 7 \pmod 9$.

Proof. We follow the construction and notation of [Wei55] except for $GU_n(q)$ where he denotes this group by $U_n(q^2)$. Let e be minimal such that $p \mid q^e - 1$, (which by Fermat's Little Theorem satisfies $e \leq p - 1$) and s maximal such that $p^s \mid q^e - 1$.

Choose a such that $c + ea = n$ with $0 \leq c < e$ in case $GL_n(q)$ and if e is even in cases $GU_n(q)$, $Sp_{2m}(q)$ with $2m = n$, $O_{2m+1}(q)$ with $2m + 1 = n$. Choose b such that $c + 2eb = n$ with $0 \leq c < e$ if e is odd in cases $GU_n(q)$, $Sp_{2m}(q)$ with $2m = n$, $O_{2m+1}(q)$ with $2m + 1 = n$. Denote by $\Sigma_n(q)$ an arbitrary classical group. We will denote $a = \Sigma a_i p^i$, $b = \Sigma b_i p^i$, and $\mu_i(p) = 1 + p + \cdots + p^{i-1}$.

By [Wei55, Final statement] $GL_n(q)$, $GU_n(q)$, $O_n^\epsilon(q)$, $Sp_{2m}(q)$ all have Sylow p-subgroups isomorphic to a direct product of the $H_{s,k} = C_{p^s} \wr C_p \wr \cdots \wr C_p$ with $k \geq 0$ wreathed factors where $s > 0$, as in Lemma 1.28. Note that $H_{s,0}$ is homocyclic.

By Lemma B.12 the Sylow p-subgroups of the simple classical groups are isomorphic to the $H_{s,k}$ as above whenever we do not have $PSL_n(q)$ with $p \mid q - 1$ or $PSU_n(q)$ with $p \mid q + 1$. Thus in all these cases Lemma 1.28 implies that $p = 3$ and $S \cong C_3 \wr C_3$, and $s = 1$.

Thus in $PSL_n(q)$ if $p \nmid q - 1$ the Sylow p-subgroups are isomorphic to those of $GL_n(q)$ and the only possibility is $C_3 \wr C_3$ by Lemma 1.28, when $a = 3$. Then as $1 < e < p$ we have $e = 2$ since $e < p$, and $c \in \{0, 1\}$, so this Sylow appears when $n = c + ea \in \{6, 7\}$ and $q \equiv 2, 5 \pmod 9$.

For $PSU_n(q)$ we similarly get when $p \nmid q + 1$ isomorphic Sylow p-subgroups to those of $GU_n(q)$. As we need $p = 3$ and $s = 1$, we have $e = 1$ ($e = 2$ means $p \nmid p - 1$ and $p \mid p^2 - 1$, thus $p \mid p + 1$, a contradiction), hence $q \equiv 4, 7 \pmod 9$ and $n = c + 2b \in \{6, 7\}$ since the blocks now have degree 2. Thus $PSU_6(q)$ and $PSU_7(q)$ have Sylow 3-subgroups isomorphic to $C_3 \wr C_3$.

In the symplectic case as $e < p = 3$ we have either $e = 2$ and $Sp_n(q)$ shares its Sylow p-subgroups with $GL_n(q)$, in which case the only possibility is $Sp_6(q)$ for $q \equiv 2, 5 (\bmod\ 9)$; or $e = 1$ and from the construction in [Wei55, Section 3, p.531] we see that $n = d + 2b$, so $4 = M = sb + \sum b_i \mu_i(p) \geq b_0 s + b_1(1 + 3s) + b_2(1 + 3 + 9s)$.

Then as $s = 1$, the only possibility is $b = 3$, that is $Sp_6(q)$ for $q \equiv 4, 7 \pmod 9$. Thus $PSp_6(q)$ appears whenever $q \equiv 2, 4, 5, 7 \pmod 9$.

For odd degree orthogonal groups again $C_3 \wr C_3$ is the only possible Sylow, and either $e = 2$ and $O_{2m+1}(q)$ has Sylow p-subgroups isomorphic to those of $GL_{2m+1}(q)$, which gives us $O_7(q)$ for $q \equiv 2, 5 \pmod 9$; or $e = 1$, and we obtain $2m+1 = d+2b$ and as before $4 = M = sb + \sum b_i \mu_i(p)$ so $b = 3$ and $2m + 1 = 1 + 6 = 7$, that is $O_7(q)$ when $q \equiv 4, 7 \pmod 9$. Thus we obtain $P\Omega_7(q)$ when $q \equiv 2, 4, 5, 7 \pmod 9$.

Note that $|O^+_{2m}(q)| = q^{m(m-1)}(q^2 - 1)(q^4 - 1) \dots (q^{2m-2} - 1)(q^m - 1)$,
$|O^-_{2m}(q)| = q^{m(m-1)}(q^2 - 1)(q^4 - 1) \dots (q^{2m-2} - 1)(q^m + 1)$, and
$|O_{2m+1}(q)| = q^{m(m-1)}(q^2 - 1)(q^4 - 1) \dots (q^{2m-2} - 1)(q^{2m} - 1)$ and these have isomorphic Sylow p-subgroups with those of $P\Omega^{\pm}_n(q)$ by Lemma B.12, so we get the following:

$[O^+_{2m+2}(q) : O_{2m+1}(q)] = q^{m+1} - 1$, $[O_{2m+1}(q) : O^+_{2m}(q)] = q^m + 1$.

$[O^-_{2m+2}(q) : O_{2m+1}(q)] = q^{m+1} + 1$, $[O_{2m+1}(q) : O^-_{2m}(q)] = q^m - 1$.

Thus, since the Sylow 3-subgroups need to coincide with those of $O_7(q)$, $m = 3$. We have that $q^4 \equiv 1 \pmod 3$ so $O^-_8(q)$ has Sylow p-subgroups isomorphic to $C_3 \wr C_3$ for $q \equiv 2, 4, 5, 7 \pmod 9$ and so does $P\Omega^-_8(q)$. Similarly we get $P\Omega^+_6(q)$ when $q \equiv 4, 7 \pmod 9$ and also $P\Omega^-_6(q)$ when $q \equiv 2, 5 \pmod 9$.

The above covers the cases when the quotient of the orders is coprime to p. When p divides this index we get a subgroup of index p^s and a quotient by the centre of order $p^t = (n, q-1)$ in $PSL_n(q)$ or $p^t = (n, q+1)$ in $PSU_n(q)$. Note that $t \leq s$ by definition.

Now we have in $GL_n(q)$ a homocyclic group of exponent p^s and rank a which becomes in $SL_n(q)$ a homocyclic group of exponent p^s and rank $a-1$. In $PSL_n(q)$ we lose p^t from $Z(SL_n(q))$. Thus in $PSL_n(q)$ we have $|S| = p^{2+2k} = p^N$ and containing an abelian subgroup of order $p^{sa-s-t} \leq p^{2+k}$ and of index

$$j = \sum a_i \mu_i(p) \leq \sum_{i=0}^{\infty} \frac{a}{p} \left(\frac{1}{p}\right)^i = \frac{a}{p(1-1/p)} = \frac{a}{p-1},$$

which yields the following inequality:

$$sa - 2s - 2 \leq sa - s - t - 2 \leq k \leq j \leq \frac{a}{p-1}.$$

This gives us $a \leq \frac{(p-1)(2s+2)}{s(p-1)-1}$, and $k \leq \frac{2+2s}{s(p-1)-1}$ which satisfies $k \leq 4$ for $p = 3$, $k < 2$ for $p = 5$ and $k < 1$ for $p \geq 7$. So the only possibilities are either $p = 5$, $s = 1$ and $|S| = 5^4$; or $p = 3$, $s = 1$ and $|S| \leq 3^{10}$; or $p = 3$, $s \geq 2$ and $|S| \leq 3^6$.

Thus any further examples have either $p = 3, 5$ and $|S| = p^4$ or $p = 3$ and $|S| \leq 3^{10}$. We note that by Theorem 4.27 we have $|S| \leq p^6$.

For $PSL_n(q)$ we have $e = 1$ since $p \mid q - 1$. Its Sylow p-subgroups then have order $p^{N-s-t} \leq p^6$ and as 7 is not divisible by 3 or 5 in $PSL_7(q)$ contains a homocyclic subgroup $C_{p^s}^6$, hence we have $n \leq 6$.

When $n = 6$ we are considering $PSL_6(q)$, where we observe if $p = 5$ a homocyclic $C_{p^s}^5$, which is too big. If $p = 3$ this becomes a $C_{p^s}^4$, which implies $s = 1$. Therefore $q \equiv 4, 7 \pmod 9$, where S does have an extraspecial subgroup of index 3. In $GL_6(q)$ the Sylow 3-subgroups are $T \cong (C_3 \wr C_3) \times (C_3 \wr C_3)$, of nilpotency class 3. This contains $3_+^{1+2} \times 3_+^{1+2}$ of index p^2, which is contained in the subgroup $T \cap SL_6(q)$, and contains $Z(SL_6(q)) \cap T$ of order 3. Then $S = (T \cap SL_6(q))/(Z(SL_6(q) \cap T))$ has a subgroup $3_+^{1+2} \circ 3_+^{1+2} \cong 3_+^{1+4}$ which is extraspecial by Theorem 1.13 and has index 3 in S. Thus S is isomorphic to a Sylow 3-subgroup of either $PSL_4(3)$ or $PSU_4(3)$. Since this description does not depend on the particular value of q, just modulo 9, we can then check with $q = 4$, and a Magma computation shows

$S \cong T \in \mathrm{Syl}_3(PSU_4(3))$:

```
> IsIsomorphic(Sylow(PSU(4,3),3),(Sylow(PSL(6,4),3))) eq true;
true
```

If $n = 5$ and $p = 3$ then $|S| = 3^{4s+1}$, hence there can be no extraspecial subgroup of index 3. If $p = 5$, we have $|S| = 5^4$ and observe a $C_{5^s}^3$, hence $s = 1$ and the only case is $PSL_5(q)$ when $q \equiv 6, 11, 16, 21 \pmod{25}$ where the Sylow 5-subgroups of $GL_5(q)$ are $T \cong C_5 \wr C_5$ and those of $PSL_5(q)$ a subquotient of order 5^4 with extraspecial subgroups of index 5. Now $Z(T) = T^5$, thus S has exponent 5, hence $S \cong <5^4, 7>$ by Lemma 3.11.

If $n < p$ then the Sylow p-subgroups of $GL_n(q)$ are abelian, thus there are no more examples with $p = 5$. It remains to consider $n \in \{3, 4\}$ for $p = 3$.

If $n = 4$ then the Sylow p-subgroups of $PSL_4(q)$ and $SL_4(q)$ are isomorphic, hence we have $S \leq C_{3^s} \wr C_3 \times C_3$ of index 3, and we must have $s = 1$. That is $q \equiv 4, 7 \pmod 9$, where the Sylow p-subgroups of $SL_4(q)$ are $S \cong C_3 \wr C_3$ and have extraspecial subgroups of index 3 by Lemma 1.28.

Finally, $GL_3(q)$ has Sylow p-subgroups isomorphic to $C_{3^s} \wr C_3$, and we observe in $SL_3(q)$ a homocyclic $C_{3^s}^2 : C_3$ which in $PSL_3(q)$ becomes $(C_{3^s} \times C_{3^{s-1}}) : C_3$ containing an abelian subgroup of index p, therefore $|S| = 3^4$ by Lemma 1.24, which implies $s = 2$. Hence we are considering $PSL_3(q)$ when $q \equiv 10, 19 \pmod{27}$, where $S \cong (C_9 \times C_3) : C_3$ has at least one extraspecial subgroup $3_+^{1+2} \cong (C_3 \times C_3) : C_3$ and index 3. We determine the isomorphism type of S via:

```
> IdentifyGroup(Sylow(PSL(3,19),3));
<81, 9>
```

This covers all cases of $PSL_n(q)$.

In the case of $PSU_n(q)$ we need $p \mid q+1$ for subgroups or subquotients to appear, that is $e = 2$ since in [Wei55] the notation is with $q^{1/2}$. Then $e = 2\epsilon$ so $\epsilon = 1$ and the Sylow p-subgroups coincide with $GL_n(q^2)$. Then like in the linear case we can get the same order N and the indices s, t correspond when using $p \mid q+1$, instead of $p \mid q-1$, so we get the same cases as in $PSL_n(q)$ with the analogous congruences. $\square$

B.3.2 Exceptional groups

Type	$\prod \Phi_i^{n_i}$	$\lvert Z(K_u)\rvert$
A_ℓ	$\Phi_1^\ell \prod_{m>1} \Phi_m^{\left[\frac{\ell+1}{m}\right]}$	$(l+1, q-1)$
${}^2\mathrm{A}_\ell$	$\Phi_2^\ell \prod_{m\not\equiv 2 \pmod 4} \Phi_m^{\left[\frac{\ell+1}{\mathrm{lcm}(2,m)}\right]} \prod_{m\equiv 2 \pmod 4,\, m>2} \Phi_m^{\left[\frac{2(\ell+1)}{m}\right]}$	$(l+1, q+1)$
B_ℓ	$\prod_{m\geq 1} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]}$	$(2, q-1)$
C_ℓ	$\prod_{m\geq 1} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]}$	$(2, q-1)$
D_ℓ	$\prod_{m\nmid 2\ell \text{ or } m\mid\ell} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]} \prod_{m\mid 2\ell \text{ and } m\nmid\ell} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]-1}$	$\begin{cases}(2,q-1)^2 \text{ if } 2\mid l\\(4,q^l-1) \text{ if } 2\nmid l\end{cases}$
${}^2\mathrm{D}_\ell$	$\prod_{m\nmid\ell} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]} \prod_{m\mid\ell} \Phi_m^{\left[\frac{2\ell}{\mathrm{lcm}(2,m)}\right]-1}$	$(4, q^l+1)$
${}^2B_2$	$\Phi_1\Phi_4$	1
${}^3D_4$	$\Phi_1^2\Phi_2^2\Phi_3^2\Phi_6^2\Phi_{12}$	1
G_2	$\Phi_1^2\Phi_2^2\Phi_3\Phi_6$	1
${}^2G_2$	$\Phi_1\Phi_2\Phi_6$	1
F_4	$\Phi_1^4\Phi_2^4\Phi_3^2\Phi_4^2\Phi_6^2\Phi_8\Phi_{12}$	1
${}^2F_4$	$\Phi_1^2\Phi_2^2\Phi_4^2\Phi_6\Phi_{12}$	1
E_6	$\Phi_1^6\Phi_2^4\Phi_3^3\Phi_4^2\Phi_5\Phi_6^2\Phi_8\Phi_9\Phi_{12}$	$(3, q-1)$
${}^2E_6$	$\Phi_1^4\Phi_2^6\Phi_3^2\Phi_4^2\Phi_6^3\Phi_8\Phi_{10}\Phi_{12}\Phi_{18}$	$(3, q+1)$
E_7	$\Phi_1^7\Phi_2^7\Phi_3^3\Phi_4^2\Phi_5\Phi_6^3\Phi_7\Phi_8\Phi_9\Phi_{10}\Phi_{12}\Phi_{14}\Phi_{18}$	$(2, q-1)$
E_8	$\Phi_1^8\Phi_2^8\Phi_3^4\Phi_4^4\Phi_5^2\Phi_6^4\Phi_7\Phi_8^2\Phi_9\Phi_{10}^2\Phi_{12}^2\Phi_{14}\Phi_{15}\Phi_{18}\Phi_{20}\Phi_{24}\Phi_{30}$	1

Table B.2: Cyclotomic polynomials expressing the r'-part of the orders of universal versions of Lie type groups and their centres.

Lemma B.14. *Assume that p is odd. Suppose G is an exceptional finite simple group of Lie type in characteristic r for $r \neq p$ and q is a power of r. Then G has Sylow p-subgroups S with an extraspecial subgroup of index p if and only if $p = 3$ and G is one of:*

- $F_4(q)$ *for* $q \equiv 2, 4, 5, 7 \pmod 9$*;*
- $E_6(q)$ *for* $q \equiv 2, 5 \pmod 9$*;*
- ${}^2E_6(q)$ *for* $q \equiv 4, 7 \pmod 9$*;*
- ${}^3D_4(q)$ *for* $q \equiv 2, 4, 5, 7 \pmod 9$.

where $S \cong T \in \mathrm{Syl}_3(PSL_4(3))$ in the first three cases and $S \cong <3^4, 9>$ in the last one.

Proof. For exceptional groups of Lie type, using the notation from [GLS98, Theorem 4.10.2] and Table B.2, in S we get a homocyclic subgroup of exponent p^a, rank n_{m_0} and index b, where n_i denotes the exponent of $\Phi_i(q)$ in Table B.2, which is taken from [GL83, Tables 10:1, 10:2] and [GLS98, Table 2.2 and Theorem 2.5.12], m_0 is the multiplicative order of q modulo p, p^a is the p-part of $\Phi_{m_0}(q)$, and $b = \sum_{i=p^c m_0, c>0} n_i$. We note that for S to be nonabelian we need p to divide the order of the Weyl group associated with G. Thus $|S| = p^{an_{m_0}+b}$. We recall that $an_{m_0} + b = 2 + 2k$ must be even by Lemma 1.23 and $b \geq k$ by Lemma 1.17. Hence we need $b \neq 0$ to have nonabelian Sylow p-subgroups, and we look at the values of chains $p^c m_0$. Thus we need p to divide some index in the expression in Table B.2, which reduces to $p = 3, 5, 7$.

For example we have $|F_4(q)| = q^{24}\Phi_1(q)^4\Phi_2(q)^4\Phi_3(q)^2\Phi_4(q)^2\Phi_6(q)^2\Phi_8(q)\Phi_{12}(q)$ so the only nonabelian Sylow p-subgroups are for $p = 3$ since p is the only odd prime dividing the possible indices. Then $m_0 = 1$, or $m_0 = 2$, and in both cases $n_{m_0} = 4$, hence $|S| = 3^{an_{m_0}+b} = 3^{4a+2}$. Since $b = 2$, this forces S to have an abelian subgroup of index 3^2, so $|S| \leq 3^6$ by Lemma 1.17. Thus we need $a = 1$, and $|S| = 3^6$. Now $F_4(q)$ contains $3^3.SL_3(3)$ by [CLSS92, Theorem 1]. By the previous result and [CCN+85] we see that $3^3.SL_3(3) < PSL_4(3) < F_4(2)$, thus the Sylow 3-subgroups of $F_4(q)$ (which are isomorphic to those of $F_4(2)$ by the uniform construction) are isomorphic to those of $PSL_4(3)$ that have an extraspecial subgroup of index 3 by Proposition B.9. This happens whenever $a = 1$, that is $q \equiv 2, 4, 5, 7 \pmod 9$.

Next we consider $E_6(q)$:

$$|E_6(q)| = \frac{1}{(3, q-1)} q^{36}\Phi_1(q)^6\Phi_2(q)^4\Phi_3(q)^3\Phi_4(q)^2\Phi_5(q)\Phi_6(q)^2\Phi_8(q)\Phi_9(q)\Phi_{12}(q),$$

so the possible chains arise when $p = 3$ or $p = 5$.

When $p = 3$, $m_0 = 1, 2$ according to $q \equiv \pm 1 \pmod 3$, and we can have $b = 3 + 1 = 4$ or $b = 2$. Then $|S|$ is respectively $3^{an_{m_0}+b}$, so 3^{6a+4} or 3^{4a+2}. Those with $q \equiv -1 \pmod 3$ appear as by [LS04, Theorem 1], $F_4(q)$ is isomorphic to a subgroup of $E_6(q)$, so when $|S| = 3^6$, that is $q \equiv 2, 5 \pmod 9$, $F_4(q)$ and $E_6(q)$ have isomorphic Sylow 3-subgroups which have an extraspecial subgroup of index 3. When $q \equiv 1 \pmod 3$ then $3 \mid |Z(K_u)|$ and the Sylow p-subgroups of the simple group have size 3^9, so no extraspecial subgroups of index p.

When $p = 5$, as the only index divisible by 5 appearing is 5 itself with multiplicity 1, the only possibility is $b = 1$. But then as $m_0 \in \{1, 2, 4\}$, we have $n_{m_0} \in \{6, 4, 2\}$ hence $|S| = 5^{an_{m_0}+1}$ which has odd exponent, so no extraspecial subgroups of index p.

The case of ${}^2E_6(q)$ is similar. We have

$$|{}^2E_6(q)| = \frac{1}{(3,q+1)} q^{36}\Phi_1(q)^4\Phi_2(q)^6\Phi_3(q)^2\Phi_4(q)^2\Phi_6(q)^3\Phi_8(q)\Phi_{10}(q)\Phi_{12}(q)\Phi_{18}(q),$$

so $p = 3$, and either $m_0 = 1$, $b = 2$ or $m_0 = 2$, $b = 3+1 = 4$. When $q \equiv -1 \pmod 3$ we have $p \mid |Z(K_u)|$ and the Sylow 3-subgroups have order 3^9, a contradiction. When $q \equiv 1 \pmod 3$ we have by [LS04, Theorem 1] $F_4(q) \leq {}^2E_6(q)$, so their Sylow 3-subgroups are isomorphic and have an extraspecial subgroup of index 3. This happens when $q \equiv 4, 7 \pmod 9$.

$E_7(q)$ has $b \neq 0$ for $p = 3, 5, 7$. If $p = 5$ or $p = 7$ then we get an abelian subgroup of order $p^7 \leq p^{2+k}$, which is too big since in this case $k \leq b = 1$. For $p = 3$ we get $|S| = 3^{7a+4} \geq 3^{11}$ so we again get an abelian group of order 3^{7a} and index 3^4, hence there are no extraspecial subgroups of index 3 either.

$E_8(q)$ has $b \leq 5$ with equality when $p = 3$ for $m_0 = 1, 2$, so $|S| \leq p^{12}$. However the orders of the Sylow p-subgroups are 3^{8a+5}, 5^{4a+1}, 7^{8a+1} which have odd exponent, or 5^{8a+2} but in this case we have $b = 2$ so $|S| \leq 5^6$, a contradiction. Thus we don't have extraspecial subgroups of index p in any case.

We now consider the remaining small cases. For ${}^2B_2(2^{2r+1})$, ${}^2G_2(3^{2r+1})$ only $p = 2, 3$ appear, which is either defining characteristic or $p = 2$, so for any other p we have $b = 0$ and all relevant Sylow p-subgroups are abelian.

${}^2F_4(2^{2r+1})$ has $b \leq 1$ with $p = 3$ so $|S| \leq p^4$. However as the corresponding polynomials are Φ_1^2 and Φ_2^2, we have $|S| = 3^{2a+1}$, a contradiction.

$G_2(q)$ has two chains for $p = 3$, but its Sylow 3-subgroups have order 3^{2a+1}, a contradiction.

${}^3D_4(q)$: the only chains with $b \neq 0$ are for $p = 3$, which is an exception in

[GLS98, Theorem 4.10.2]. Using the Weyl group we see that $b = 1$, so the only possibility is $a = 1$, $S \cong (C_3 \times C_9) : C_3$ of order p^4. This happens whenever $q \equiv 2, 4, 5, 7 \pmod 9$. Since the description of S does not depend any further on q, we calculate in Magma that in ${}^3D_4(2)$ we have $S \cong <3^4, 9>$ via:

```
> IdentifyGroup(Sylow(ChevalleyGroup("3D",4,2),3));
<81, 9>
```

Hence the same holds for the remaining ${}^3D_4(q)$. $\square$

B.4 Sporadic groups

The necessary information about orders, maximal subgroups and number of elements of a given order was obtained and uses the notation of the ATLAS in its book and online versions [CCN+85] and [WWT+05]. The p-rank information is taken from [GLS98, Proposition 5.6.1].

Proposition B.15. *Suppose G is a sporadic simple group and $S \in \mathrm{Syl}_p(G)$ has an extraspecial subgroup of index p. Then G and $|S|$ are as in the final rows of Table B.1.*

Proof. Recall that for S to have an extraspecial subgroup of index p it is necessary that its order must be p^{2+2k} for some $k \in \mathbb{Z}_{>0}$ by Lemma 1.23. This reduces the primes to be considered to those in the second column of Table B.4, with the third column giving the respective orders. Further, by Corollary B.8, as in every case $p \leq 7$, we obtain that $|S| \leq 3^6$, which rules out Fi_{24}', Th and M for $p = 3$.

Name	p	$\lvert S\rvert$	Extraspecial index p	Notes
$\boldsymbol{M_{11}}$	2	2^4	Yes	$S \cong SD_{16}$
$\boldsymbol{M_{12}}$	2	2^6	Yes	$S \cong T \in \mathrm{Syl}_2(G_2(2))$
M_{22}, M_{23}	none	-	-	-
M_{24}	2	2^{10}	No	-
J_1, J_2, J_3, J_4	none	-	-	-
$\boldsymbol{Co_1}$	5	5^4	Yes	$S \cong T \in \mathrm{Syl}_5(PSp_4(5))$
$\boldsymbol{McL}$	3	3^6	Yes	$PSU_4(3) \leq_{Max} McL$
$\boldsymbol{Co_2}$	2,3	$2^{18}, 3^6$	2 No, 3 Yes	$McL \leq_{Max} Co_2$
Co_3	2	2^{10}	No	-
Fi_{22}	none	-	-	-
Fi_{23}	2	2^{18}	No	-
Fi'_{24}	3	3^{16}	No	-
HS	none	-	-	-
Suz	none	-	-	-
He	2	2^{10}	No	-
Ru	2	2^{14}	No	-
$O'N$	3	3^4	No	-
$\boldsymbol{Ly}$	2,5	2^8, 5^6	2 No, 5 Yes	$G_2(5) \leq_{Max} Ly$
Th	3	3^{10}	No	-
$\boldsymbol{HN}$	2,3,5	$2^{14}, 3^6, 5^6$	2 No, 3 Yes, 5 Yes	$S_3 \cong T \in \mathrm{Syl}_3(PSL_4(3))$ $S_5 \cong T \in \mathrm{Syl}_5(G_2(5))$
$\boldsymbol{BM}$	5	5^6	Yes	$HN : 2 \leq_{Max} BM$
$\boldsymbol{M}$	2,3,7	$2^{46}, 3^{20}, 7^6$	2 No, 3 No, 7 Yes	$S \cong T \in \mathrm{Syl}_7(G_2(7))$

Table B.3: Sporadic finite simple groups whose Sylow p-subgroups have an extraspecial subgroup of index p.

We now consider each of the cases left.

M_{11}: when $p = 2$, M_{11} has a maximal subgroup $2S_4 \cong GL_2(3) \cong Q_8 : S_3$, so its Sylow 2-subgroups are isomorphic to $Q_8 : C_2 \cong SD_{16} \cong <16, 8>$ and contain an extraspecial subgroup of index 2.

M_{12}: when $p = 2$ M_{12} has a maximal subgroup of shape $2_+^{1+4}{:}S_3$ containing a Sylow 2-subgroup with an extraspecial subgroup of index 2. We check that S is isomorphic to a Sylow 2-subgroup of $G_2(2)$, that is $<2^6, 134>$ via:

```
> load "m12";
Loading "/Applications/Magma/libs/pergps/m12"
M12 - Mathieu group on 12 letters - degree 12
Order 95 040 = 2^6 * 3^3 * 5 * 11;  Base 1,2,3,4,5
Group: G
> IsIsomorphic(Sylow(G,2), Sylow(G2(2),2)) eq true;
true
```

The group M_{24} when $p = 2$ has $|S| = 2^{10}$. It contains $H{:}C_3{}^{\cdot}S_6$ as a maximal subgroup where $H \cong C_2^6$, and since the Sylow 2-subgroups of S/H are not abelian, by Lemma 1.27 we need $H \leq Q$, but this is too big since $|Q| = 2^9$ and the maximal abelian subgroups have order 2^5 by Lemma 1.17. Hence we see that there are no extraspecial subgroups of index 2.

For the group Co_1, $p = 5$ is the only possible prime. It has a maximal subgroup $5_+^{1+2}{:}GL_2(5)$, so it has an extraspecial subgroup of index p. The remaining 5-local maximal subgroups have shape $C_5^3 : (C_4 \times A_5).C_2$ and $C_5^2 : 2A_5$, in particular, S is generated by elements of order p, and thus its Sylow p-subgroups are isomorphic to those of $PSp_4(5)$ (see e.g. Lemma 3.11).

The group McL contains a maximal subgroup isomorphic to $PSU_4(3)$ so the Sylow 3-subgroups of $PSU_4(3)$ and McL are isomorphic and have an extraspecial subgroup of index 3 by Proposition B.9.

For the group Co_2 we need to examine $p = 2, 3$. When $p = 2$ the Sylow 2-subgroups do not have an extraspecial subgroup of index 2. This can be seen since there is a maximal subgroup M with shape $H{:}M_{22}{:}C_2$ with $H \cong C_2^{10}$, and we take $S \in \mathrm{Syl}_2(Co_2)$ such that $S \leq M$. As M/H has nonabelian Sylow 2-subgroups,

$H \leq Q$ by Lemma 1.27. However by Lemma 1.17 maximal abelian subgroups of Q have order at most 2^9, a contradiction. If $p = 3$, as McL is a maximal subgroup of Co_2, and they have Sylow 3-subgroups of order 3^6, they are isomorphic, so as above they have an extraspecial subgroup of index 3.

The group Co_3 contains a maximal subgroup $M \cong C_2^4{}^{\cdot}A_8$ which contains a Sylow 2-subgroup S of Co_3. Let $H = O_2(M) \leq S$. As the Sylow 2-subgroups of A_8 have order 2^6 and an extraspecial subgroup of index 2, by Lemma 1.24 S/H does not contain an abelian subgroup of index 2. Then, by Lemma 1.27, S does not contain any extraspecial subgroup of index 2.

For Fi_{23} we have $p = 2$ to consider, but Fi_{23} has an abelian subgroup $H \cong C_2^{11}$ observed in the maximal subgroup $H{}^{\cdot}M_{23}$. But if it had an extraspecial subgroup Q of index 2 then $|H \cap Q| \geq 2^{10}$, whereas the maximal abelian subgroups of Q would have order 2^9 by Lemma 1.17.

The group He has $p = 2$ to consider, with Sylow 2-subgroups of order 2^{10}, but we have a maximal subgroup $C_2^6{:}C_3.S_6 \geq S$, and we can argue as for M_{24}.

The group Ru has $p = 2$ as the only possibility. If Ru had an extraspecial subgroup of index 2 then exponent of the Sylow would be at most 8 by Lemma 1.23, but Ru has elements of order 16.

The group $O'N$ has $p = 3$ as the only possibility. But we can see in the maximal subgroup $C_3^4{:}2^{1+4}.D_{10}$ that it has elementary abelian Sylow 3-subgroups, so no extraspecial subgroup of index 3.

The Lyons group Ly has possible primes $p = 2, 5$. For $p = 2$ we have the maximal subgroup $2.A_{11}$ containing S. Then either $S \cong Q \times C_2$ or by Lemma 1.27 S/C_2 should have either elementary abelian subgroups of index 2 or be elementary abelian. But the Sylow 2-subgroups of A_{11} have index 2 in those of S_{11}, isomorphic to $C_2 \wr C_2 \wr C_2 \times C_2$ as in Lemma B.10, hence they are not abelian nor extraspecial nor do they contain an abelian subgroup of index 2. Thus S does not contain any extraspecial subgroups of index 2. For $p = 5$, $G_2(5)$ is a maximal subgroup of Ly, and their Sylow 5-subgroups are isomorphic and have an extraspecial subgroup of index 5 by Proposition B.9.

For HN we need to consider $p = 2, 3, 5$. We consider a $2A$ involution t, which has centraliser $2.HS.2$ of order 2^{11}. If this involution is in Q, then by Lemma 1.10 applied to $\langle Z(S), t\rangle$, its centraliser would have index at most 2 in Q, hence $|C_S(t)| \geq 2^{12}$, so t is not in Q. On the other hand as $|S : Q| = 2$, every square of an element of 2-power order is in Q, but we can see from the character table in [CCN+85] that t is the square of some elements in classes $4A$ and $4B$, so $t \in Q$, a contradiction. Thus S does not contain an extraspecial subgroup of index 2.

For $p = 3$, the maximal subgroup $M_3 = 3^{1+4}_{+}{:}C_4.A_5$ shows that there is an extraspecial subgroup of index 3. Its other 3-local subgroup N_3 has shape $C_3^4 : C_2 : (A_4 \times A_4).C_4$, which shows that S contains an elementary abelian C_3^4, hence a complement to $Q \cong 3^{1+4}_{+}$ in S. Thus Proposition 1.32 implies that S is isomorphic to either a Sylow p-subgroup of $SL_4(3)$ or that of $SU_4(3)$. Further, Proposition 1.19 (4,9) implies that $C_2.(A_4 \times A_4) \cong \Omega_4^+(3)$, whence N_3 is isomorphic to a parabolic subgroup of $PSL_4(3)$, and therefore S is isomorphic to a Sylow 3-subgroup of $PSL_4(3)$. For $p = 5$, we have the maximal 5-local subgroups $M_5 = 5^{1+4}_{+}{:}2^{1+4}_{-}.C_5.C_4$ and $N_5 = C_5^2 : 5^{1+2}_{+}.C_4.A_5$, which are $\mathcal{F}_{S_5}(HN)$-essential subgroups, and we can see an extraspecial subgroup of index 5. From N_5 we observe that $Z_{O_5(N_5)} \leq Q$, and $|\Phi(O_5(N_5))| = 5^3$, so Hypothesis C holds and Proposition 4.17 implies that S_5 is isomorphic to a Sylow 5-subgroup of $G_2(5)$.

BM has $p = 5$ as the only possible prime. But it has maximal subgroup $HN{:}C_2$, so it contains HN and their Sylow 5-subgroups are isomorphic.

And finally, in M the primes left to consider are $p = 2, 7$. For $p = 2$, we see that M contains elements of order $32 = 2^5$, thus there can be no extraspecial of index 2 in its Sylow 2-subgroups by Lemma 1.23.

For $p = 7$ we have an extraspecial of index p, as seen in the maximal subgroup $M_7 = 7_+^{1+4}{:}(C_3 \times 2S_7)$. The remaining 7-locals of M are $N_7 = 7^{2+1+2} : GL_2(7)$ and $P_7 = C_7^2 : SL_2(7)$, thus there is a self-centralising subgroup $O_7(P_7)$ of order 7^2, thus Proposition 1.3 implies that $S \in \mathrm{Syl}_7(M)$ has maximal nilpotency class whence we see that S is isomorphic to a Sylow 7-subgroup of $G_2(7)$ by Proposition 1.32. $\square$

B.5 Fusion systems of the finite simple groups

Even though we have an infinite number of finite simple groups from whose Sylow p-subgroups contain an extraspecial subgroup of index p in Proposition B.1, they only give rise to a small number of isomorphism types of fusion systems in addition to the 4 infinite families of groups of Lie type in defining characteristic. We now classify the isomorphism types on each S. We begin with the known cases with $p = 2$, which does not include all groups of Lie type in odd characteristic.

Lemma B.16. *Suppose $p = 2$ and G is a finite simple group which is not a group of Lie type in odd characteristic. If $S \in \mathrm{Syl}_2(G)$ contains an extraspecial subgroup of index 2 then S and G are, up to isomorphism of $\mathcal{F}_S(G)$, one of the following, with $\mathcal{F}_S(G)$ always simple:*

1. *$S \cong SD_{16}$ and $G = M_{11}$;*
2. *$S \in \mathrm{Syl}_2(PSL_4(2))$ and $G = PSL_4(2) \cong A_8$ or $G = PSU_4(2) \cong PSp_4(3)$.*

3. *S is of type M_{12} and $G = M_{12}$.*

We remark that in this situation $G_2(2)$ has Sylow 2-subgroups as in (3), and $PSp_4(2)$ has $C_8 \times C_2$, but they are not simple groups. As S has sectional rank at most 4, we can use [Oli16, Theorem A] to see that $G_2(q)$ will arise in case (3) for q with $v_2(q \pm 1) = 2$, as well as $PSL_3(q)$ where $q \equiv 2^2 - 1 \pmod{2^3}$ ($v_2(q \pm 1) = 2$) in case (1), and $PSp_4(q)$ when $v_2(q^2 - 1) = 3$ in case (2).

Proof. Proposition B.2 implies that G is one of $PSL_4(2) \cong A_8$, A_9, $PSU_4(2)$, M_{11} or M_{12}. In Proposition B.15 we showed that if $G = M_{11}$ then $S \cong SD_{16}$ and if $G = M_{12}$ then $S \cong T \in \mathrm{Syl}_2(G_2(2))$, whereas in Lemma B.10 we showed that $PSL_4(2) \cong A_8$, A_9 have isomorphic Sylow 2-subgroups. Further, the following easy Magma computation checks that the Sylow 2-subgroups of $PSL_4(2)$ and $PSU_4(2)$ are isomorphic.

```
> IsIsomorphic(Sylow(PSU(4,2),2), Sylow(PSL(4,2),2)) eq true;
true
```

Finally, the fusion systems of A_8 and A_9 at $p = 2$ coincide since the normalisers of 2-groups do not grow. Each $\mathcal{F}_S(G)$ is simple by [Oli16, Theorem A]. $\square$

We recall before stating the next lemma that isotypically equivalent implies that the fusion systems are isomorphic, as per the discussion just after Definition 2.10 where isomorphism of fusion systems is introduced.

Lemma B.17. *Out of the groups of Lie type in cross characteristic from Table B.1, the following have isotypically equivalent fusion systems on $S \in \mathrm{Syl}_p(G)$:*

1. *Every family of groups in the same row independently of the characteristic.*

2. The $PSL_n(q)$ and $PSU_{n'}(q')$ where $n = n'$ and $q \equiv -q' \pmod p$.

3. The $P\Omega_6^{\pm}(q)$.

4. The groups $F_4(q)$, $E_6(q)$ and ${}^2E_6(q)$ for all q as in the table.

Proof. All the parts follow from [BMO12, Theorem A].

From [BMO12, Theorem A (a)] we see that whenever $q \equiv q' \pmod p$ we have $\mathcal{F}_p(G(q)) \simeq \mathcal{F}_p(G(q'))$, which gives all of (1) except the cases $PSp_6(q)$, $P\Omega_7(q)$, $P\Omega_8^-(q)$, ${}^3D_4(q)$ and $F_4(q)$, all of which follow from part [BMO12, Theorem A (c)].

From part (c) we get all cases of (1) whenever W contains an element inverting all elements of the torus, that is if G is not one of A_m $(m > 1)$, D_{2m+1} $(m \geq 1)$, E_6. In those cases we have only one congruence class of $q \pmod p$ so part (a) (or (b) in the twisted cases) completes (1).

Part (d) gives us parts $(2), (3)$ and those of ${}^\epsilon E_6$ in (4) since we have the twists exactly when $q \equiv -q' \pmod p$.

$\mathcal{F}_{S_3}(F_4(q)) \simeq \mathcal{F}_{S_3}({}^2E_6(q))$ from [BMO12, Example 4.5 (b)] as the second ones appear only when $q \equiv 1 \pmod 3$. Hence (4) follows as well. □

At this stage we know that, except for the rows of groups of Lie type in defining characteristic, for each row of Table B.1 there is a unique fusion system $\mathcal{F}_S(G)$ up to isomorphism, and that certain rows give rise to isomorphic fusion systems. In each of the cases we can take the smallest candidate for q and we have a particular group with which we can compute in Magma, hence we can run the code in Appendix C.3 to obtain a list of potential $\mathcal{F}_S(G)$-essential subgroups E, and $\mathrm{Out}_G(E) = N_G(E)/E$, which allow us to easily check that certain fusion systems are not isomorphic. We note that in Appendix C.3 we do not only return the $\mathcal{F}_S(G)$-

essentials, but rather those E with $O_p(\mathrm{Out}_G(E)) = 1$, but when $|Out_S(E)| = p$ this is sufficient by Corollary 1.56 (4).

All fusion systems on the sporadic simple groups in Proposition B.1 are simple by [Asc11, (16.8) and (16.10)].[1]

The only p-groups on which we still have more than one fusion system arising from a group of Lie type in cross characteristic are $C_3 \wr C_3$ and $<3^4, 9>$, which are labelled $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4$, and $\mathcal{F}_a$, $\mathcal{F}_b$ respectively, and we consider them now.

Lemma B.18. *Suppose G is a finite simple group with $S \in \mathrm{Syl}_3(G)$ isomorphic to $<3^4, 9>$. Then $\mathcal{F}_S(G)$ is isomorphic to either $\mathcal{F}_a = \mathcal{F}_S(PSL_3(19))$, or $\mathcal{F}_b = \mathcal{F}_S({}^3D_4(2))$.*

Proof. By Proposition B.1 and Lemma B.17 there are at most the two fusion systems $\mathcal{F}_a = \mathcal{F}_S(PSU_3(8)) \cong \mathcal{F}_S(PSL_3(8))$ and $\mathcal{F}_b = \mathcal{F}_S({}^3D_4(2))$ on S, which we now show are not isomorphic. In $PSL_3(19)$ (or $PSU_3(8)$) we check computationally using Appendix C.3 that the $\mathcal{F}_S(PSL_3(19))$-essential subgroups are exactly the 3 S-conjugacy classes of self-centralising subgroups of order 3^2, whereas in ${}^3D_4(2)$ there is a 3-local subgroup $3_+^{1+2} : 2S_4$ using [WWT+05]. Thus these two fusion systems are not isomorphic. □

Lemma B.19. *Suppose G is a finite simple group with $S \in \mathrm{Syl}_3(G)$ isomorphic to $C_3 \wr C_3$. Then $\mathcal{F}_S(G)$ is isomorphic to exactly one of $\mathcal{F}_{S_3}(A_9)$, $\mathcal{F}_{S_3}(A_{11})$, $\mathcal{F}_{S_3}(PSp_4(3))$, or $\mathcal{F}_{S_3}(PSL_6(2))$.*

Proof. The groups with S as in the statement are listed in Corollary B.4 (1).

For the alternating groups we can see that A_9 and A_{10} give rise to the same fusion system since the normalisers of 2-groups do not grow, as opposed to A_{11},

[1] The 5-fusion system of Co_1 is said not to be simple, but there is an error. We describe it in Lemma B.20 and Table 7.6

where $S_9 \leq A_{11}$ but $S_9 \not\leq A_9, A_{10}$, the fusion systems will be different as in the two instances $\mathrm{Aut}_{S_9}(S) \not\cong \mathrm{Aut}_{A_9}(S)$. Hence we have two non-isomorphic fusion systems $\mathcal{F}_{S_3}(A_9)$ and $\mathcal{F}_{S_3}(A_{11})$.

By Lemma B.17 the cases left to consider are $PSU_4(2)$, $PSL_6(2)$, $PSL_7(2)$, $PSp_6(2)$, $P\Omega_7(2)$, $P\Omega_6^+(4)$, $P\Omega_8^-(2)$.

Since Proposition 1.19 (15) implies that $PSU_4(2) \cong PSp_4(3)$ and [KL90, Proposition 2.5.1] or [Car72, p.11] we have $PSp_6(2) \cong P\Omega_7(2)$, their fusion systems are isomorphic.

Further, we have that $PSp_6(2) \leq PSL_6(2) \leq PSL_7(2)$, and $PSp_6(2) \leq P\Omega_8^-(2)$, and in all cases above we checked using the Magma program from Appendix C.3 that the $\mathcal{F}_S(G)$-essential candidates are $A \cong C_3^3$ and $Q \cong 3_+^{1+2}$, which have isomorphic normalisers in all the inclusions above. Then in all cases the $\mathcal{F}$-essential subgroups are C_3^3 or 3_+^{1+2}, and $SL_2(p) \cong O^{p'}(\mathrm{Out}_{\mathcal{F}}(E)) \leq \mathrm{Out}_{\mathcal{F}}(E) \leq \mathrm{Out}(E) \cong GL_2(p)$ is uniquely determined by its isomorphism type, so by Alperin's fusion theorem their fusion systems are isomorphic to $\mathcal{F}_{S_3}(PSL_6(2)) \cong \mathcal{F}_{S_3}(PSp_6(2))$.

It only remains to consider $P\Omega_6^+(4)$. We have $PSL_4(4) \leq P\Omega_6^+(4)$, and we similarly established using Magma that the fusion systems are isomorphic and of index 2 in the previous ones, in particular to those of $PSU_4(2)$ by Lemma B.17 (1), and thus to $\mathcal{F}_{S_3}(PSp_4(3))$ since $PSU_4(2) \cong PSp_4(3)$.

Hence any fusion system on a finite simple group with $S_3 \cong C_3 \wr C_3$ is isomorphic to one of $\mathcal{F}_{S_3}(A_9)$, $\mathcal{F}_{S_3}(A_{11})$, $\mathcal{F}_{S_3}(PSp_4(3))$, or $\mathcal{F}_{S_3}(PSL_6(2))$.

These are all pairwise non-isomorphic since $N_{PSp_4(3)}(S_3) \cong C_2$ whereas we have$N_{PSL_6(2)}(S_3) \cong C_2 \times C_2$, and in the alternating cases there is an $\mathcal{F}$-essential subgroup of type $C_3 \times C_3$ whereas in the rest they all have order 3^3. $\square$

We have now considered all p-groups of order p^4 except for $<5^4, 7>$, which we study now.

Lemma B.20. *Suppose G is a finite simple group with $S \in \mathrm{Syl}_5(G)$ isomorphic to $<5^4, 7> \cong T \in \mathrm{Syl}_5(PSp_4(5))$. Then $\mathcal{F}_S(G)$ is isomorphic to exactly one of $\mathcal{F}_S(PSp_4(5))$, $\mathcal{F}_S(PSL_5(11))$ or $\mathcal{F}_S(Co_1)$.*

Proof. The groups in question are listed in Corollary B.4 (2) and are $PSp_4(5)$; $PSL_5(q)$ for $q \equiv 6, 11, 16, 21 \pmod{25}$; $PSU_5(q)$ for $q \equiv 4, 9, 14, 19 \pmod{25}$; or Co_1. Lemma B.17 (2) implies that all the cross characteristic groups give rise to isomorphic fusion systems. Thus there are at most the 3 fusion systems in the statement, which we consider now. In Co_1 the maximal 5-local subgroups have shapes $5^{1+2} : GL_2(5)$, $C_5^3 : (C_4 \times A_5).C_2$ and $C_5^2 : 2A_5$, which shows that there are $\mathcal{F}$-essentials of order 5^2, that is $\mathcal{F}_S(Co_1)$-pearls, as well as the unique abelian subgroup $A \cong C_5^3$ of index 5 in S, and an extraspecial subgroup 5_+^{1+2}.

In $PSp_4(5)$ the only maximal 5-local subgroups are of shapes $5^{1+2} : 2A_5 : C_2$ and $C_5^3 : (C_2 \times A_5).C_2$, thus there are no $\mathcal{F}_S(PSp_4(5))$-pearls.

Finally, in the cross characteristic case, we consider $PSU_5(4)$, the smallest example, in which the code in Appendix C.3 outputs as essential candidates 5 conjugacy classes of C_5^2 and the unique abelian subgroup A of index 5 in S. In particular, there is no nonabelian $\mathcal{F}_S(PSU_5(4))$-essential, and all three fusion systems are pairwise nonisomorphic. This information is also contained in Table 7.6 □

We now consider Sylow p-subgroups of order p^6 with p odd. When $p = 3$ we have two isomorphism classes of Sylow 3-subgroups, isomorphic to the Sylow 3-subgroups of $PSL_4(3)$ and $PSU_4(3)$ respectively. We see from the discussion above that in the first case we have at most 3 fusion systems up to isomorphism, those of $\mathcal{F}_{S_3}(PSL_4(3))$, $\mathcal{F}_{S_3}(F_4(2))$, and $\mathcal{F}_{S_3}(HN)$, while in the second case we have at most 4, any being isomorphic to one of $\mathcal{F}_{S_3}(PSU_4(3))$, $\mathcal{F}_{S_3}(PSL_6(4)) \cong \mathcal{F}_{S_3}(PSU_6(2))$, $\mathcal{F}_{S_3}(Co_2)$ or $\mathcal{F}_{S_3}(McL)$.

Lemma B.21. *1. $\mathcal{F}_{S_3}(PSL_4(3))$, $\mathcal{F}_{S_3}(F_4(2))$, and $\mathcal{F}_{S_3}(HN)$ are pairwise non-isomorphic.*

2. $\mathcal{F}_{S_3}(PSU_4(3))$, $\mathcal{F}_{S_3}(PSL_6(4)) \cong \mathcal{F}_{S_3}(PSU_6(2))$, $\mathcal{F}_{S_3}(Co_2)$ or $\mathcal{F}_{S_3}(McL)$ are pairwise non-isomorphic.

Proof. We show that $N_G(Q)$ has different shapes for each G. We have that $N_{PSL_4(3)}(Q) \sim Q : GL_2(3)$, $N_{F_4(2)}(Q) \sim Q : ((Q_8 \times Q_8) : C_3) : C_2$ (Appendix C.3 takes around 100 seconds to run and gives $N_{F_4(2)}(Q)/Q \cong <384, 18131>$, then GAP's StructureDescription yields the above) and $N_{HN}(Q) \sim Q : 4^{\cdot}A_5$ from [WWT+05].

In the $PSU_4(3)$ Sylow we have $N_{PSU_4(3)}(Q) \sim Q : 2S_4$ as in [CCN+85, p.52], $N_{PSU_6(2)}(Q) \sim Q : (Q_8 \times Q_8) : S_3$, $N_{McL}(Q) \sim Q : 2.S_5$ and $N_{Co_2}(Q) \sim Q.2^{1+4}.S_5$, obtained from [WWT+05]. Thus none of the 4 fusion systems above are isomorphic.

□

We notice that the fusion systems on the two Sylow 3-subgroups above are more complicated to classify than in the general cases. A source of complications is the different nature of quadratic modules for $p = 3$, which yields some extra modules seen above. We also have $PSL_2(9) \cong A_6$, yielding extra automorphisms, hence the p'-extensions are harder to classify, and some arise from almost simple groups such as $\Omega_8^+(2) : S_3 < F_4(2)$. S a Sylow 3-subgroup of $PSU_4(3)$ is classified in [BFM].

We now consider the case with $p > 3$ and $|S| = p^6$, where there are always 3 isomorphism classes of Sylow p-subgroups, those of $PSL_4(p)$, $PSU_4(p)$ and $G_2(p)$. In this situation these G are the only finite simple groups that have Sylow p-subgroups isomorphic to one of the above except for a Sylow p-subgroup of $G_2(5)$ and $G_2(7)$, which we consider now, as in Corollary B.3.

Lemma B.22. *1. The fusion systems $\mathcal{F}_S(G_2(5))$, $\mathcal{F}_S(HN)$, $\mathcal{F}_S(Ly)$, $\mathcal{F}_S(BM)$ are pairwise non-isomorphic.*

2. The fusion systems $\mathcal{F}_S(M)$ and $\mathcal{F}_S(G_2(7))$ are not isomorphic.

Proof. Corollary B.3 implies that there are 3 sporadic groups HN, Ly and BM for $p = 5$, and only M for $p = 7$. For $p = 5$ by the maximal subgroups from [CCN+85] we have: $N_{G_2(5)}(Q) \sim Q : GL_2(5)$, $N_{HN}(Q) \sim Q : 2_-^{1+4}.C_5.C_4$, $N_{Ly}(Q) \sim Q : C_4.S_6$, and $N_B(Q) \sim Q : 2_-^{1+4}.A_5.C_4$. For $p = 7$ we have $N_{G_2(7)}(Q) \sim Q : GL_2(7)$ (computed using Magma as $G_2(7)$ is not in [CCN+85]) and $N_M(Q) \sim Q : (C_3 \times 2S_7)$. Hence all these groups give rise to non-isomorphic fusion systems. $\square$

At this stage all isomorphism types of fusion systems arising from Proposition B.1 as in Table B.1 have been classified.

B.6 Almost simple groups

In the above we have only considered the simple groups. We now use Lemma 8.3 to prove that if $p \neq 3$ and $\mathcal{F}$ is realised by an almost simple group G then $O^{p'}(\mathcal{F})$ is realised by a finite simple group, hence we do we need not consider the almost simple groups. When $p = 3$, $O^3(\mathcal{F})$ may be smaller than $\mathcal{F}$, as in the group

$G = \Omega_8^+(2) : C_3$, which has Sylow 3-subgroups isomorphic to those of $SL_4(3)$, and $\mathfrak{foc}(\mathcal{F}_S(G))$ is a Sylow 3-subgroup of $\Omega_8^+(2)$ and has index 3 in S.

Lemma B.23. *Suppose S is a p-group with an extraspecial subgroup Q of index p and $\mathcal{F}$ is a saturated fusion system on S with $O_p(\mathcal{F}) = 1$. Suppose $\mathcal{F}$ is realised by an almost simple group G with socle X. Then, unless $p = 3$ and either $S \in \mathrm{Syl}_3(SL_4(3))$ or $|S| = 3^4$ and all $\mathcal{F}$-essential subgroups have order 3^3, $O^{p'}(\mathcal{F})$ is a fusion system on S realised by a finite simple group and is reduced.*

Proof. As $X \trianglelefteq G$, we have $\mathcal{F}_T(X) \trianglelefteq \mathcal{F}_S(G)$ by [AKO11, Proposition I.6.2] where $T = S \cap X$. Now as G is almost simple by the Schreier conjecture $G/X \leq \mathrm{Out}(X)$ is solvable, and there is a series of normal subgroups $X \trianglelefteq X_1 \trianglelefteq X_2 \trianglelefteq \cdots \trianglelefteq X_n = G$, where X_i/X_{i-1} is cyclic of prime order. In particular, if $T \neq S$ at some point $X_i/X_{i-1} \cong C_p$, whence $O^p(\mathcal{F}_{S_i}(X_i)) \neq \mathcal{F}_{S_i}(X_i)$. However, by Proposition B.7 $O_p(\mathcal{F}_S(X)) = 1$, so also $O_p(\mathcal{F}_{S_i}(X_i)) = 1$, and we can apply Lemma 8.3 to obtain that $O^p(\mathcal{F}) = \mathcal{F}$, a contradiction. Thus $T = S$ and $\mathcal{F}_S(X)$ has index prime to p in $\mathcal{F}_S(G)$, and Theorem 2.35 and the discussion immediately before it show that $O^{p'}(\mathcal{F}_S(G)) = \mathcal{F}_S(X)$, and $\mathcal{F}_S(X)$ is reduced. $\square$

APPENDIX C

Magma CODE

C.1 Orbits calculation

```
p := 11; P :=[1..p-1]; T := [];
time for i in P do
    "----------";
    Q := []; R := []; S := [];
    time for N in Subsets({1..p-1},i) do
        if N notin Q then
            LL := [];
            for l in P do L := SequenceToSet([(m*l) mod p : m in N]);
                if L notin Q then
                Append(~Q,L);  Append(~R, N); Append(~LL, L);
            end if;  end for;
        Length := #LL; Append(~S, Length);
        Append(~T, SequenceToSet(R));
        if Length notin {0, p-1} then N;
    end if; end if; end for;
i, #Subsets({1..p-1},i)/(p-1), #SequenceToSet(R), Multiset(S), #T;
end for;
```

C.2 Reduction to $SL_4(3)$

```
//Find groups of order $3^6$ with $|S'| = 3^3$, $Q$ extraspecial
//of index $p$ and $E$ as in Hypothesis C.
SG := SmallGroups(3^6);
time C := [S : S in SG |#DerivedSubgroup(S) eq 3^3 and
0 ne #[j : j in MaximalSubgroups(S) | IsExtraSpecial(j`subgroup)]
and 0 ne #[j : j in MaximalSubgroups(S) | Centre(j`subgroup)
eq DerivedSubgroup(j`subgroup) and #Centre(j`subgroup) eq 3^2]];
#C;

//Find involutions in $Aut(S)$ which centralise 9 elements of $S$
//only one of which is in $V$, which is homocyclic. This reduces
//to a Sylow $p$-subgroup of $SL(4,3)$.

CC:= [];
for i in C do
    A := AutomorphismGroup(i);
    V := Centraliser(i, DerivedSubgroup(i));
    phi, P := PermutationRepresentation(A);
    T := Sylow(P,2);
    maps := [Inverse(phi)(k) : k in T ];
    for k in maps do
        if Order(k) eq 2 then
            if (IsIsomorphic(V, SmallGroup(81,15)) or
                IsIsomorphic(V, SmallGroup(81,2))) and
                #[s: s in i | k(s) eq s] eq 9 and
                #[s: s in i | k(s) eq s and s in V] eq 1
            then IdentifyGroup(i);
            Append(~CC, i);
            //CC := []; Append(~CC, <i,k>);
            end if;
        end if;
    end for;
end for;
#CC; IsIsomorphic(CC[1], Sylow(SL(4,3),3)) eq true;
```

C.3 Magma code to find subgroups that can be $\mathcal{F}_S(G)$-essential

```
/*Function Essentials: Given a group $G$, a Sylow $p$-subgroup $S$
*of $G$ and the prime $p$, returns a list E of possible
*$\FF_S(G)$-essential subgroups and $S$, and in NN their
*corresponding $\Out_G(E)$.*/
Essentials := function(G,S,p);
    j := 0;NN := []; E := [];
    for i in Subgroups(S) do H := i`subgroup;
//Check H is $\FF_S(G)$-centric:
        if Centraliser(S,H) subset Centre(H) then
            q,pi := Normaliser(S,H)/FrattiniSubgroup(H);
            if Centraliser(q,pi(H)) subset pi(H) and
                pi(H) subset Centraliser(q,pi(H)) then
                N := Normaliser(G,H)/H;
//Check $O_p(Out_G(H)) = 1$ so that it can have a strongly
//$p$-embedded subgroup:
                if Order(pCore(N,p)) eq 1 then
                    j+:=1; E[j] := H; NN[j] := N;
                end if;
            end if;
        end if;
    end for;
return E, NN;
end function;
```

LIST OF REFERENCES

[AKO11] Michael Aschbacher, Radha Kessar, and Bob Oliver. *Fusion systems in algebra and topology*, volume 391 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2011.

[AOV12] Kasper K. S. Andersen, Bob Oliver, and Joana Ventura. Reduced, tame and exotic fusion systems. *Proc. Lond. Math. Soc. (3)*, 105(1):87–152, 2012.

[Asc86] Michael Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[Asc11] Michael Aschbacher. The generalized Fitting subsystem of a fusion system. *Mem. Amer. Math. Soc.*, 209(986):vi+110, 2011.

[BCG$^+$07] Carles Broto, Natàlia Castellana, Jesper Grodal, Ran Levi, and Bob Oliver. Extensions of p-local finite groups. *Trans. Amer. Math. Soc.*, 359(8):3791–3858, 2007.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[Ben71] Helmut Bender. Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt. *J. Algebra*, 17:527–554, 1971.

[Ben91] David J. Benson. *Representations and Cohomology I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991.

[BEO02] Hans U. Besche, Bettina Eick, and Eamonn A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[Ber08] Yakov Berkovich. *Groups of prime power order. Vol. 1*, volume 46 of *De Gruyter Expositions in Mathematics*. Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[BFM] Elisa Baccanelli, Clara Franchi, and Mario Mainardis. Fusion systems on a Sylow 3-subgroup of the McLaughlin group. In preparation.

[BHRD13] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013.

[Bla58] Norman Blackburn. On a special class of p-groups. *Acta Math.*, 100:45–92, 1958.

[BLO03] Carles Broto, Ran Levi, and Bob Oliver. The homotopy theory of fusion systems. *J. Amer. Math. Soc.*, 16(4):779–856, 2003.

[BMO12] Carles Broto, Jesper M. Møller, and Bob Oliver. Equivalences between fusion systems of finite groups of Lie type. *J. Amer. Math. Soc.*, 25(1):1–20, 2012.

[Bou91] Dominique Bourn. Normalization equivalence, kernel equivalence and affine categories. *Category theory*, pages 43–62, 1991.

[Bro94] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Bur97] William Burnside. *Theory of groups of finite order*. Cambridge University Press, 1897.

[Car72] Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney, 1972. Pure and Applied Mathematics, Vol. 28.

[CCN$^+$85] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker, and Robert A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985.

[Che04] Andrew Chermak. Quadratic pairs. *J. Algebra*, 277(1):36–72, 2004.

[CLSS92] Arjeh M. Cohen, Martin W. Liebeck, Jan Saxl, and Gary M. Seitz. The local maximal subgroups of exceptional groups of Lie type, finite and algebraic. *Proc. London Math. Soc. (3)*, 64(1):21–48, 1992.

[COS17] David A. Craven, Bob Oliver, and Jason Semeraro. Reduced fusion systems over p-groups with abelian subgroup of index p: II. *Adv. Math.*, 322:201–268, 2017.

[CP10] Murray Clelland and Christopher Parker. Two families of exotic fusion systems. *J. Algebra*, 323(2):287–304, 2010.

[Cra11] David A. Craven. *The theory of fusion systems: an algebraic approach*, volume 131 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2011.

[DH92] Klaus Doerk and Trevor Hawkes. *Finite soluble groups*, volume 4 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 1992.

[DRV07] Antonio Díaz, Albert Ruiz, and Antonio Viruel. All p-local finite groups of rank two for odd prime p. *Trans. Amer. Math. Soc.*, 359(4):1725–1764, 2007.

[FF09] Ramón J. Flores and Richard M. Foote. Strongly closed subgroups of finite groups. *Adv. Math.*, 222(2):453–484, 2009.

[GL83] Daniel Gorenstein and Richard Lyons. The local structure of finite groups of characteristic 2 type. *Mem. Amer. Math. Soc.*, 42(276):vii+731, 1983.

[GLO17] Samuel Gonshaw, Martin W. Liebeck, and Eamonn A. O'Brien. Unipotent class representatives for finite classical groups. *J. Group Theory*, 20(3):505–525, 2017.

[GLS96] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups. Number 2. Part I. Chapter G*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1996.

[GLS98] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups. Number 3. Part I. Chapter A*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998.

[GLS15] Danieil Gorenstein, Richard Lyons, and Ronald Solomon. Errata for the classifcation of the finite simple groups, a.m.s. surveys and monographs 40. 2015.

[Gor80] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.

[Gra18] Valentina Grazian. Fusion systems containing pearls. *Journal of Algebra*, 510:98 – 140, 2018.

[Hal34] Philip Hall. A contribution to the theory of groups of prime power order. *Proceedings of the London Mathematical Society*, s2-36(1):29–95, 1934.

[Hup67] Bertram Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.

[Jam80] Rodney James. The groups of order p^6 (p an odd prime). *Math. Comp.*, 34(150):613–637, 1980.

[KL90] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[KS98] Hans Kurzweil and Bernd Stellmacher. *Theorie der endlichen Gruppen.* Springer-Verlag, Berlin, 1998.

[Küs79] Ayse S. Küsefoglu. The second degree cohomology of finite orthogonal groups. I. *J. Algebra*, 56(1):207–220, 1979.

[LGM02] Charles R. Leedham-Green and Susan McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series.* Oxford University Press, Oxford, 2002.

[LO02] Ran Levi and Bob Oliver. Construction of 2-local finite groups of a type studied by Solomon and Benson. *Geom. Topol.*, 6:917–990, 2002.

[LS04] Martin W. Liebeck and Gary M. Seitz. The maximal subgroups of positive dimension in exceptional algebraic groups. *Mem. Amer. Math. Soc.*, 169(802):vi+227, 2004.

[LS12] Martin W. Liebeck and Gary M. Seitz. *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, volume 180 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2012.

[McL67] Jack McLaughlin. Some groups generated by transvections. *Arch. Math. (Basel)*, 18:364–368, 1967.

[McL69] Jack McLaughlin. Some subgroups of $\mathrm{SL}_n(\mathbf{F}_2)$. *Illinois J. Math.*, 13:108–115, 1969.

[ML63] Saunders Mac Lane. *Homology*. Die Grundlehren der mathematischen Wissenschaften, Bd. 114. Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[MSS03] Ulrich Meierfrankenfeld, Bernd Stellmacher, and Gernot Stroth. Finite groups of local characteristic p: an overview. In *Groups, combinatorics & geometry (Durham, 2001)*, pages 155–192. World Sci. Publ., River Edge, NJ, 2003.

[Oli14] Bob Oliver. Simple fusion systems over p-groups with abelian subgroup of index p: I. *J. Algebra*, 398:527–541, 2014.

[Oli16] Bob Oliver. Reduced fusion systems over 2-groups of sectional rank at most 4. *Mem. Amer. Math. Soc.*, 239(1131):v+100, 2016.

[OR17] Bob Oliver and Albert Ruiz. Reduced fusion systems over p-groups with abelian subgroup of index p: III. *arXiv preprint arXiv:1708.08710*, 2017.

[PR02] Christopher Parker and Peter Rowley. *Symplectic amalgams*. Springer Monographs in Mathematics. Springer-Verlag London, Ltd., London, 2002.

[PR10] Christopher Parker and Peter Rowley. A 3-local characterization of Co_2. *J. Algebra*, 323(3):601–621, 2010.

[PS15] Chris Parker and Gernot Stroth. A family of fusion systems related to the groups $\mathrm{Sp}_4(p^a)$ and $\mathrm{G}_2(p^a)$. *Arch. Math. (Basel)*, 104(4):311–323, 2015.

[PS18] Chris Parker and Jason Semeraro. Fusion systems over a Sylow p-subgroup of $\mathrm{G}_2(p)$. *Math. Z.*, 289(1-2):629–662, 2018.

[Pui06] Lluis Puig. Frobenius categories. *J. Algebra*, 303(1):309–357, 2006.

[RS09] Kieran Roberts and Sergey Shpectorov. On the definition of saturated fusion systems. *J. Group Theory*, 12(5):679–687, 2009.

[RV04] Albert Ruiz and Antonio Viruel. The classification of p-local finite groups over the extraspecial group of order p^3 and exponent p. *Math. Z.*, 248(1):45–65, 2004.

[Sam14] Benjamin Sambale. *Blocks of finite groups and their invariants*, volume 2127 of *Lecture Notes in Mathematics*. Springer, Cham, 2014.

[Sem14] Jason Semeraro. Trees of fusion systems. *J. Algebra*, 399:1051–1072, 2014.

[Sri68] Bhama Srinivasan. The characters of the finite symplectic group Sp(4, q). *Trans. Amer. Math. Soc.*, 131:488–525, 1968.

[VLL91] Antonio Vera López and Begoña Larrea. On p-groups of maximal class. *J. Algebra*, 137(1):77–116, 1991.

[Wei55] A. J. Weir. Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p. *Proc. Amer. Math. Soc.*, 6:529–533, 1955.

[Wil09] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

[Wil17] Robert A. Wilson. Maximal subgroups of sporadic groups. In *Finite simple groups: thirty years of the atlas and beyond*, volume 694 of *Contemp. Math.*, pages 57–72. Amer. Math. Soc., Providence, RI, 2017.

[Win72] David L. Winter. The automorphism group of an extraspecial p-group. *Rocky Mountain J. Math.*, 2(2):159–168, 1972.

[WWT+05] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Steve Linton, John Bray, and Rachel Abbott. Atlas of finite group representations-version 3, 2005.

[Zsi92] Karl Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.