*Proceedings of the Royal Society of Edinburgh*, **150**, 1187–1239, *2020*
DOI:10.1017/prm.2018.107

# Reduced fusion systems over $p$-groups with abelian subgroup of index $p$: III

**Bob Oliver**
LAGA, Institut Galilée,
Av. J-B Clément, 93430 Villetaneuse, France
(bobol@math.univ-paris13.fr)

**Albert Ruiz**
Departament de Mathemàtiques, Edifici C,
Universitat Autònoma de Barcelona,
08193 Bellaterra, Spain (albert@mat.uab.cat)

(MS Received 30 August 2017; accepted 12 January 2018)

We finish the classification, begun in two earlier papers, of all simple fusion systems over finite nonabelian $p$-groups with an abelian subgroup of index $p$. In particular, this gives many new examples illustrating the enormous variety of exotic examples that can arise. In addition, we classify all simple fusion systems over infinite nonabelian discrete $p$-toral groups with an abelian subgroup of index $p$. In all of these cases (finite or infinite), we reduce the problem to one of listing all $\mathbb{F}_pG$-modules (for $G$ finite) satisfying certain conditions: a problem which was solved in the earlier paper [15] using the classification of finite simple groups.

*Keywords:* finite groups; fusion; finite simple groups; modular representations; Sylow subgroups

2010 *Mathematics subject classification:* Primary 20D20
Secondary 20C20; 20D05; 20E45

A *saturated fusion system* over a finite $p$-group $S$ is a category whose objects are the subgroups of $S$, and whose morphisms are injective homomorphisms between the subgroups, and which satisfy some additional conditions first formulated by Puig (who called them 'Frobenius $S$-categories' in [24]) and motivated in part by the Sylow theorems for finite groups. For example, if $G$ is a finite group and $S \in \mathrm{Syl}_p(G)$, then the category $\mathcal{F}_S(G)$, whose objects are the subgroups of $S$ and whose morphisms are the homomorphisms between subgroups defined via conjugation in $G$ is a saturated fusion system over $S$. We refer to [24], [7, Part I], or [14] for the basic definitions and properties of saturated fusion systems.

A saturated fusion system is *realizable* if it is isomorphic to $\mathcal{F}_S(G)$ for some finite group $G$ and some $S \in \mathrm{Syl}_p(G)$; it is *exotic* otherwise. Here, by an isomorphism of fusion systems we mean an isomorphism of categories that is induced by an isomorphism between the underlying $p$-groups. Exotic fusion systems over finite $p$-groups seem to be quite rare for $p = 2$ (the only known examples are those constructed in

[21] and others easily derived from them), but many examples of them are known for odd primes $p$.

A *discrete $p$-torus* is a group of the form $(\mathbb{Z}/p^\infty)^r$ for some $r \geqslant 0$, where $\mathbb{Z}/p^\infty$ is the union of the cyclic groups $\mathbb{Z}/p^k$ via the obvious inclusions $\mathbb{Z}/p^k < \mathbb{Z}/p^{k+1}$. A *discrete $p$-toral group* is a group containing a discrete $p$-torus as a normal subgroup of $p$-power index. Saturated fusion systems over discrete $p$-toral groups were defined and studied in [10], motivated by the special case of fusion systems for compact Lie groups and $p$-compact groups.

A fusion system is *simple* if it is saturated and contains no proper nontrivial normal fusion subsystems (see definition 1.4). As a special case, very rich in exotic examples, we have been looking at simple fusion systems $\mathcal{F}$ over finite nonabelian $p$-groups $S$ with an abelian subgroup $A$ of index $p$. By [6, proposition 5.2(a)], if $p = 2$, then $S$ is dihedral, semidihedral, or a wreath product of the form $C_{2^k} \wr C_2$, and hence $\mathcal{F}$ is isomorphic to the fusion system of $PSL_2(q)$ or $PSL_3(q)$ for some odd $q$. Fusion systems over extraspecial groups of order $p^3$ and exponent $p$ were listed in [25], and by [23, theorem 2.1], these include the only simple fusion systems over nonabelian $p$-groups containing more than one abelian subgroup of index $p$. The other cases where $p$ is odd and $A$ is not essential (equivalently, not radical) in $\mathcal{F}$ were handled in [23, theorem 2.8], while those where $A$ is essential and of exponent $p$ was handled in [15]. So it remains to describe those cases where $A$ is essential and not elementary abelian (and the unique abelian subgroup of index $p$). This, together with analogous results about simple fusion systems over infinite discrete $p$-toral groups with abelian subgroup of index $p$, are the main results of this paper.

To simplify the following summary of our results, we use the term 'index-$p$-triple' to denote a triple $(\mathcal{F}, S, A)$, where $S$ is a nonabelian discrete $p$-toral group (finite or infinite) with abelian subgroup $A$ of index $p$, and $\mathcal{F}$ is a simple fusion system over $S$. Our main results are shown in §§ 4 and 5, where we handle separately the finite and infinite cases. In each of these sections, we first list, in theorems 4.5 and 5.11, all index-$p$-triples $(\mathcal{F}, S, A)$, for $S$ finite or infinite, in terms of the pair $(G, A)$ where $G = \mathrm{Aut}_{\mathcal{F}}(A)$ and $A$ is regarded as a $\mathbb{Z}_pG$-module. Theorem 4.5 is taken directly from [15, theorem 2.8], while theorem 5.11 is new. For completeness in the infinite case, we also show that each index-2-triple $(\mathcal{F}, S, A)$ with $|S| = \infty$ is isomorphic to that of $SO(3)$ or $PSU(3)$ (theorem 5.6), and that for each $p$ there is (up to isomorphism) a unique index-$p$-triple $(\mathcal{F}, S, A)$ where $|S| = \infty$ and $A$ is not essential (theorem 5.12).

The main theorems, theorems A and B, appear at the ends of §§ 4 and 5, respectively. In theorem A, for $p$ odd, we prove that each index-$p$-triple $(\mathcal{F}, S, A)$, where $A$ is finite, essential in $\mathcal{F}$, and not elementary abelian, is determined by $G = \mathrm{Aut}_{\mathcal{F}}(A)$, $V = \Omega_1(A)$ regarded as an $\mathbb{F}_pG$-module, the exponent of $A$, and some additional information needed when $A$ is not homocyclic. In all cases, $\mathrm{rk}(A) \geqslant p - 1$, and $A$ is homocyclic whenever $\mathrm{rk}(A) \geqslant p$. Also, $A$ is always isomorphic to some quotient of a $\mathbb{Z}_pG$-lattice.

Theorem B can be thought of as a 'limiting case' of the classification in theorem A. It says that each index-$p$-triple $(\mathcal{F}, S, A)$ such that $A$ is infinite and essential in $\mathcal{F}$ is determined by the pair $(G, V)$, where $G = \mathrm{Aut}_{\mathcal{F}}(A)$, and $V = \Omega_1(A)$ is regarded

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

as an $\mathbb{F}_pG$-module. In all such cases, $A$ is a discrete $p$-torus of rank at least $p-1$. We also determine which of the fusion systems we list are realized as fusion systems of compact Lie groups or $p$-compact groups.

Theorems A and B reduce our classification problems to questions about $\mathbb{F}_pG$-modules with certain properties. These questions were already studied in [**15**], using the classification of finite simple groups, and the results in that paper that are relevant in this one are summarized in § 6. Theorems A and B together with proposition 6.1 and table 6.1 allow us to completely list all simple fusion systems over nonabelian discrete $p$-toral groups (finite or infinite) with an abelian subgroup of index $p$ that is not elementary abelian. In particular, as in the earlier papers [**15**, **23**], we find a very large, very rich variety of exotic fusion systems over finite $p$-groups (at least for $p \geqslant 5$).

This work was motivated in part by the following questions and problems, all of which are familiar to people working in this field.

**Q1:** For a fixed odd prime $p$, a complete classification of all simple fusion systems over finite $p$-groups, or even a conjecture as to how they could be classified, seems way out of reach for now. But based on the many examples already known, is there any meaningful way in which one could begin to systematize them; for example, by splitting up the problem into simpler cases? Alternatively, is there a class of simple fusion systems over finite $p$-groups, much less restrictive than the one we look at here, for which there might be some chance of classifying its members?

**Q2:** Find some criterion which can be used to prove that some (or at least one!) of the examples constructed here or earlier (over *finite* $p$-groups for odd primes $p$) are exotic, without invoking the classification of finite simple groups.

**Q3:** A *torsion linear group* in defining characteristic $q$ is a subgroup $\Gamma \leqslant GL_n(K)$, for some $n \geqslant 1$ and some field $K$ of characteristic $q$, such that all elements of $\Gamma$ have finite order. If $p$ is a prime and $\Gamma$ is a torsion linear group in defining characteristic different from $p$, then by [**10**, § 8], there is a maximal discrete $p$-toral subgroup $S \leqslant \Gamma$, unique up to conjugation, and $\mathcal{F}_S(\Gamma)$ is a saturated fusion system. Are there any saturated fusion systems over discrete $p$-toral groups (for any prime $p$) which we can prove are *not* fusion systems of torsion linear groups?

The notation used in this paper is mostly standard. We let $A \circ B$ denote a central product of $A$ and $B$. When $g$ and $h$ are in a group $G$, we set ${}^gh = ghg^{-1}$ and $h^g = g^{-1}hg$. When $A$ is an abelian group and $\beta \in \mathrm{Aut}(A)$, we write $[\beta, A] = \langle \beta(x)x^{-1} \,|\, x \in A \rangle$. When $P$ is a $p$-group, we let $\mathrm{Fr}(P)$ denote its Frattini subgroup, and for $k \geqslant 1$ set

$$\Omega_k(P) = \langle g \in P \,|\, g^{p^k} = 1 \rangle \quad \text{and} \quad \mho^k(P) = \langle g^{p^k} \,|\, g \in P \rangle.$$

We would like to thank the Centre for Symmetry and Deformation at Copenhagen University, and the Universitat Autònoma de Barcelona, for their hospitality in allowing us to get together on several different occasions.

## 1. Background

We first recall some of the definitions and standard terminology used when working with fusion systems. Recall that a *discrete $p$-toral group* is a group that contains a normal subgroup of $p$-power index isomorphic to $(\mathbb{Z}/p^\infty)^r$ for some $r \geqslant 0$. A *fusion system* over a discrete $p$-toral group $S$ is a category $\mathcal{F}$ whose objects are the subgroups of $S$, and where for each $P, Q \leqslant S$, the set $\mathrm{Hom}_{\mathcal{F}}(P,Q)$ is a set of injective homomorphisms from $P$ to $Q$ that includes all those induced by conjugation in $S$, and such that for each $\varphi \in \mathrm{Hom}_{\mathcal{F}}(P,Q)$, we have $\varphi \in \mathrm{Hom}_{\mathcal{F}}(P,\varphi(P))$ and $\varphi^{-1} \in \mathrm{Hom}_{\mathcal{F}}(\varphi(P),P)$.

Define the *rank* $\mathrm{rk}(S)$ of a discrete $p$-torus $S$ by setting $\mathrm{rk}(S)=r$ if $S \cong (\mathbb{Z}/p^\infty)^r$. If $S$ is a discrete $p$-toral group with normal discrete $p$-torus $S_0 \trianglelefteq S$ of $p$-power index, then we refer to $S_0$ as the *identity component* of $S$, and set $|S| = \big(\mathrm{rk}(S_0), |S/S_0|\big)$, where such pairs are ordered lexicographically. Thus if $T$ is another discrete $p$-toral group with identity component $T_0$, then $|S| \leqslant |T|$ if $\mathrm{rk}(S_0) < \mathrm{rk}(T_0)$, or if $\mathrm{rk}(S_0) = \mathrm{rk}(T_0)$ and $|S/S_0| \leqslant |T/T_0|$. Note that the identity component of $S$, and hence $|S|$, are uniquely determined since a discrete $p$-torus has no proper subgroups of finite index.

Definition 1.1. Fix a prime $p$, a discrete $p$-toral group $S$, and a fusion system $\mathcal{F}$ over $S$.

- For each $P \leqslant S$ and each $g \in S$, $P^{\mathcal{F}}$ denotes the set of subgroups of $S$ which are $\mathcal{F}$-conjugate (isomorphic in $\mathcal{F}$) to $P$, and $g^{\mathcal{F}}$ denotes the $\mathcal{F}$-conjugacy class of $g$ (the set of images of $g$ under morphisms in $\mathcal{F}$).
- A subgroup $P \leqslant S$ is *fully normalized* in $\mathcal{F}$ (*fully centralized* in $\mathcal{F}$) if $|N_S(P)| \geqslant |N_S(Q)|$ ($|C_S(P)| \leqslant |C_S(Q)|$) for each $Q \in P^{\mathcal{F}}$.
- A subgroup $P \leqslant S$ is *fully automized* in $\mathcal{F}$ if $\mathrm{Out}_{\mathcal{F}}(P) \overset{\mathrm{def}}{=} \mathrm{Aut}_{\mathcal{F}}(P)/\mathrm{Inn}(P)$ is finite and $\mathrm{Out}_S(P) \in \mathrm{Syl}_p(\mathrm{Out}_{\mathcal{F}}(P))$. The subgroup $P$ is *receptive* in $\mathcal{F}$ if for each $Q \in P^{\mathcal{F}}$ and each $\varphi \in \mathrm{Iso}_{\mathcal{F}}(Q,P)$, there is $\bar{\varphi} \in \mathrm{Hom}_{\mathcal{F}}(N_\varphi, S)$ such that $\bar{\varphi}|_P = \varphi$, where
$$N_\varphi = \big\{ g \in N_S(Q) \,\big|\, \varphi c_g \varphi^{-1} \in \mathrm{Aut}_S(P) \big\}.$$
- The fusion system $\mathcal{F}$ is *saturated* if
  - *(Sylow axiom)* each fully normalized subgroup of $S$ is fully automized and fully centralized;
  - *(extension axiom)* each fully centralized subgroup of $S$ is receptive; and
  - *(continuity axiom, when $|S| = \infty$)* if $P_1 \leqslant P_2 \leqslant P_3 \leqslant \cdots$ is an increasing sequence of subgroups of $S$ with $P = \bigcup_{i=1}^\infty P_i$, and $\varphi \in \mathrm{Hom}(P,S)$ is such that $\varphi|_{P_i} \in \mathrm{Hom}_{\mathcal{F}}(P_i, S)$ for each $i \geqslant 1$, then $\varphi \in \mathrm{Hom}_{\mathcal{F}}(P,S)$.

The above definition of a saturated fusion system is the one given in [9] and [10, definition 2.2]. It will not be used directly in this paper (saturation of the fusion systems we construct will be shown using later theorems), but we will frequently refer to the extension axiom as a property of saturated fusion systems.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

We now need some additional definitions, to describe certain subgroups in a saturated fusion system.

Definition 1.2. Fix a prime $p$, a discrete $p$-toral group $S$, and a saturated fusion system $\mathcal{F}$ over $S$. Let $P \leqslant S$ be any subgroup. Note that by definition 1.1, $\mathrm{Out}_{\mathcal{F}}(P)$ is finite whether or not $P$ is fully normalized (see also [10, proposition 2.3]).

- $P$ is *$\mathcal{F}$-centric* if $C_S(Q) = Z(Q)$ for each $Q \in P^{\mathcal{F}}$, and is *$\mathcal{F}$-radical* if $O_p(\mathrm{Out}_{\mathcal{F}}(P)) = 1$.
- $P$ is *$\mathcal{F}$-essential* if $P < S$, $P$ is $\mathcal{F}$-centric and fully normalized in $\mathcal{F}$, and $\mathrm{Out}_{\mathcal{F}}(P)$ contains a strongly $p$-embedded subgroup. Here, a proper subgroup $H < G$ of a finite group $G$ is *strongly $p$-embedded* if $p\big||H|$, and $p\nmid|H \cap gHg^{-1}|$ for each $g \in G\smallsetminus H$. Let $\mathbf{E}_{\mathcal{F}}$ denote the set of all $\mathcal{F}$-essential subgroups of $S$.
- $P$ is *normal in $\mathcal{F}$* ($P \trianglelefteq \mathcal{F}$) if each morphism $\varphi \in \mathrm{Hom}_{\mathcal{F}}(Q, R)$ in $\mathcal{F}$ extends to a morphism $\bar{\varphi} \in \mathrm{Hom}_{\mathcal{F}}(PQ, PR)$ such that $\bar{\varphi}(P) = P$. The maximal normal $p$-subgroup of a saturated fusion system $\mathcal{F}$ is denoted $O_p(\mathcal{F})$.
- $P$ is *strongly closed in $\mathcal{F}$* if for each $g \in P$, $g^{\mathcal{F}} \subseteq P$.

Proposition 1.3. *Let $\mathcal{F}$ be a saturated fusion system over a discrete $p$-toral group $S$.*

(a) *Each morphism in $\mathcal{F}$ is a composite of restrictions of elements in* $\mathrm{Aut}_{\mathcal{F}}(P)$ *for $P \leqslant S$ that is fully normalized in $\mathcal{F}$, $\mathcal{F}$-centric and $\mathcal{F}$-radical.*

(b) *Each morphism in $\mathcal{F}$ is a composite of restrictions of elements in* $\mathrm{Aut}_{\mathcal{F}}(P)$ *for $P \in \mathbf{E}_{\mathcal{F}} \cup \{S\}$.*

(c) *For each $Q \trianglelefteq S$, $Q \trianglelefteq \mathcal{F}$ if and only if for each $P \in \mathbf{E}_{\mathcal{F}} \cup \{S\}$, $Q \leqslant P$ and $Q$ is* $\mathrm{Aut}_{\mathcal{F}}(P)$*-invariant.*

*Proof.* Point (a) is shown in [10, theorem 3.6].

By [10, proposition 2.3], $\mathrm{Out}_{\mathcal{F}}(P) = \mathrm{Aut}_{\mathcal{F}}(P)/\mathrm{Inn}(P)$ is always finite. For each such $P < S$ that is not $\mathcal{F}$-essential, $\mathrm{Aut}_{\mathcal{F}}(P)$ is generated by automorphisms that can be extended to strictly larger subgroups: this is shown in [7, proposition I.3.3] in the finite case, and the same argument applies when $S$ is infinite. Point (b) now follows from (a) and induction, and (in the infinite case) since there are only finitely many $S$-conjugacy classes of subgroups of $S$ that are $\mathcal{F}$-centric and $\mathcal{F}$-radical [10, corollary 3.5].

Point (c) follows easily from (b), just as in the finite case [7, proposition I.4.5]. □

Definition 1.4. Let $\mathcal{F}$ be a saturated fusion system over a discrete $p$-toral group $S$. A saturated fusion subsystem $\mathcal{E}$ over $T \leqslant S$ is *normal* in $\mathcal{F}$ ($\mathcal{E} \trianglelefteq \mathcal{F}$) if

- $T$ is strongly closed in $\mathcal{F}$ (in particular, $T \trianglelefteq S$);
- (invariance condition) each $\alpha \in \mathrm{Aut}_{\mathcal{F}}(T)$ is fusion preserving in the sense that it extends to an automorphism of $\mathcal{E}$;

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

- (Frattini condition) for each $P \leqslant T$ and each $\varphi \in \mathrm{Hom}_{\mathcal{F}}(P,T)$, there are $\alpha \in \mathrm{Aut}_{\mathcal{F}}(T)$ and $\varphi_0 \in \mathrm{Hom}_{\mathcal{E}}(P,T)$ such that $\varphi = \alpha \circ \varphi_0$; and
- (extension condition) each $\alpha \in \mathrm{Aut}_{\mathcal{E}}(T)$ extends to some $\bar{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(TC_S(T))$ such that $[\bar{\alpha}, C_S(T)] \leqslant Z(T)$.

The fusion system $\mathcal{F}$ is *simple* if it contains no proper nontrivial normal subsystems.

For further discussion of the definition and properties of normal fusion subsystems, we refer to [**7**, § I.6] or [**14**, §§ 5.4 & 8.1] (when $S$ and $T$ are finite) and to [**18**, definition 2.8] (in the general case). Note, in particular, the different definition used in [**14**] and in [**18**]: a saturated fusion subsystem $\mathcal{E} \leqslant \mathcal{F}$ over a subgroup $T$ that is strongly closed in $\mathcal{F}$ is normal if the extension condition holds, and also the *strong invariance condition*: for each $P \leqslant Q \leqslant T$, and each $\varphi \in \mathrm{Hom}_{\mathcal{E}}(P,Q)$ and $\psi \in \mathrm{Hom}_{\mathcal{F}}(Q,T)$, $\psi \circ \varphi \circ (\psi|_P)^{-1} \in \mathrm{Hom}_{\mathcal{E}}(\psi(P),T)$. When $S$ is finite, this is equivalent to the above definition by [**7**, proposition I.6.4], and a similar argument (made more complicated because there can be infinitely many subgroups) applies when $S$ and $T$ are $p$-toral.

Our definition of a simple fusion system also differs from that used by González [**18**, definition 3.1]: he allows the possibility of finite normal subsystems in a simple fusion system over an infinite discrete $p$-toral group. However, that definition seems to make sense only in the context of Lie groups and their analogues. In our situation, it seems more natural to require there to be no nontrivial normal subsystems at all.

Since the Frattini condition will be important in § 5, we work here with the above definition. However, none of the examples over infinite discrete $p$-toral groups considered here contains a nontrivial proper strongly closed subgroup (see lemma 5.8), so these details make no difference as to which of them are simple or not.

Proposition 1.5. *Fix a prime $p$, and let $\mathcal{F}$ be a saturated fusion system over an infinite discrete $p$-toral group $S$. Let $S_0$ be the identity component of $S$, and assume that each element of $S$ is $\mathcal{F}$-conjugate to an element of $S_0$.*

(a) *If $\mathcal{F}$ is realized by a compact Lie group $G$ with identity connected component $G_0$, then $G/G_0$ has order prime to $p$. If in addition, $\mathcal{F}$ is simple, then $\mathcal{F}$ is realized by the connected, simple group $G_0/Z(G_0)$, where $Z(G_0)$ is finite of order prime to $p$.*

(b) *If $\mathcal{F}$ is realized by a $p$-compact group $X$, then $X$ is connected. If in addition, $\mathcal{F}$ is simple, then so is $X$.*

*In either case, if $\mathcal{F}$ is simple, then the action of the Weyl group $\mathrm{Aut}_{\mathcal{F}}(S_0)$ on the $\mathbb{Q}_p$-vector space $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(S_0, \mathbb{Q}_p/\mathbb{Z}_p)$ is irreducible and generated by pseudoreflections.*

*Proof.* If $\mathcal{F} = \mathcal{F}_S(G)$ where $G$ is a compact Lie group with identity connected component $G_0$ and maximal discrete $p$-toral subgroup $S$, then $S \cap G_0$ is strongly closed in $\mathcal{F}$ since $G_0 \trianglelefteq G$, $S_0 \leqslant S \cap G_0$, and so $S \leqslant G_0$. Hence $G/G_0$ has order prime to $p$. Also, $\mathcal{F}_S(G_0) \trianglelefteq \mathcal{F}_S(G)$: the invariance and extension conditions are easily checked, and the Frattini condition holds since $G = G_0 N_G(S)$ by the Frattini argument.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

If in addition, $\mathcal{F}$ is simple, then $\mathcal{F}_S(G_0) = \mathcal{F}_S(G) = \mathcal{F}$, and $Z(G_0)$ is finite of order prime to $p$ since $Z(\mathcal{F}) = 1$. Hence $\mathcal{F}$ is also realized by $G_0/Z(G_0)$, which is simple.

If $\mathcal{F} \cong \mathcal{F}_S(X)$ for some $p$-compact group $X$ with $S \in \mathrm{Syl}_p(X)$, then $X$ is connected by [19, proposition 4.8(a)]. Then $X$ is a central product of connected, simple $p$-compact groups, and hence is simple if $\mathcal{F}$ is simple.

Whenever $\mathcal{F}$ is realized by a connected $p$-compact group $X$ (possibly a compact connected Lie group), then by [16, theorem 9.7(ii)], the action of the Weyl group $\mathrm{Aut}_{\mathcal{F}}(S_0)$ on $\mathbb{Q} \otimes_{\mathbb{Z}} H^2(BS_0; \mathbb{Z}_p)$ is generated by pseudoreflections, where

$$H^2(BS_0; \mathbb{Z}_p) \cong H^2(S_0; \mathbb{Z}_p) \cong H^1(S_0; \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}(S_0, \mathbb{Q}_p/\mathbb{Z}_p).$$

If this is not irreducible as a group generated by pseudoreflections, then by the classification of connected $p$-compact groups in [4, theorem 1.2] (for $p$ odd) and in [3, theorem 1.1] or [22, corollary 1.2] (for $p = 2$), $X$ must be a nontrivial central product of simple factors, and hence $\mathcal{F}$ is not simple. □

We also recall the definition of a *reduced* fusion system, but only for fusion systems over finite $p$-groups. Recall [7, § I.7] that in this setting, $O^p(\mathcal{F})$ and $O^{p'}(\mathcal{F})$ are the smallest (normal) fusion systems in $\mathcal{F}$ of $p$-power index and of index prime to $p$, respectively.

Definition 1.6. A saturated fusion system $\mathcal{F}$ over a finite $p$-group $S$ is *reduced* if $O_p(\mathcal{F}) = 1$, and $O^p(\mathcal{F}) = \mathcal{F} = O^{p'}(\mathcal{F})$.

For each saturated fusion system $\mathcal{F}$ over a finite $p$-group $S$, $\mathcal{F}_{O_p(\mathcal{F})}(O_p(\mathcal{F}))$, $O^p(\mathcal{F})$, and $O^{p'}(\mathcal{F})$ are all normal fusion subsystems. Hence $\mathcal{F}$ is reduced if it is simple. Conversely, if $\mathcal{E} \trianglelefteq \mathcal{F}$ is any normal subsystem over the subgroup $T \trianglelefteq S$, then by definition of normality, $T$ is strongly closed in $\mathcal{F}$. Since each normal fusion subsystem over $S$ itself has index prime to $p$, a reduced fusion system is simple if it has no proper nontrivial strongly closed subgroups.

When $\mathcal{F}$ is a saturated fusion system over an infinite discrete $p$-toral group $S$, there are well defined normal subsystems $O^p(\mathcal{F})$ (see [18, appendix B]), and $O^{p'}(\mathcal{F})$ (see [19, A.10–A.12]), with the same properties as in the finite case. So we could define reduced fusion systems in this context just as in the finite case. However, to simplify the discussion, and because we do not know whether or not infinite reduced fusion systems have the same properties that motivated the definition in the finite case (see [5, theorems A & B]), we restrict attention to simple fusion systems in the infinite setting.

## 2. Reduced or simple fusion systems over nonabelian discrete $p$-toral groups with index $p$ abelian subgroup

In this section, $p$ is an arbitrary prime. We want to study simple fusion systems over nonabelian discrete $p$-toral groups (possibly finite) which contain an abelian subgroup of index $p$. Most of the results here were shown in [15], but only in the case where $|A| < \infty$ and $p$ is odd.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

We first fix some notation which will be used throughout the rest of the paper. As usual, for a group $S$, we define $Z_m(S)$ for all $m \geqslant 1$ by setting $Z_1(S) = Z(S)$, and setting $Z_m(S)/Z_{m-1}(S) = Z(S/Z_{m-1}(S))$ for $m \geqslant 2$.

NOTATION 2.1. *Fix a nonabelian discrete $p$-toral group $S$ with a unique abelian subgroup $A$ of index $p$, and a saturated fusion system $\mathcal{F}$ over $S$. Define*

$$S' = [S,S] = [S,A], \quad Z = Z(S) = C_A(S), \quad Z_0 = Z \cap S', \quad Z_2 = Z_2(S)\,.$$

*Thus $Z_0 \leqslant Z \leqslant Z_2$ and $Z_0 \leqslant S' \leqslant A$. Also, set*

$$\mathcal{H} = \bigl\{Z\langle x\rangle \bigm| x \in S{\smallsetminus}A\bigr\} \qquad\qquad G = \mathrm{Aut}_{\mathcal{F}}(A)$$
$$\mathcal{B} = \bigl\{Z_2\langle x\rangle \bigm| x \in S{\smallsetminus}A\bigr\} \qquad\qquad \mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)\,.$$

Recall that by [**23**, theorem 2.1], if $p$ is odd, and $S$ is finite and nonabelian and has more than one abelian subgroup of index $p$, then either $S$ is extraspecial of order $p^3$ (and the reduced fusion systems over $S$ were described in [**25**]), or there are no reduced fusion systems over $S$. So in the finite case, the restriction about the uniqueness of $A$ is just a convenient way to remove certain cases that have already been handled. We will show later (corollary 5.2) that in the infinite case (also when $p = 2$), $A$ is unique whenever $O_p(\mathcal{F}) = 1$.

LEMMA 2.2. *Assume notation 2.1. Then $\mathbf{E}_{\mathcal{F}} \subseteq \{A\} \cup \mathcal{H} \cup \mathcal{B}$, and $|N_S(P)/P| = p$ for each $P \in \mathbf{E}_{\mathcal{F}}$. If $\mathbf{E}_{\mathcal{F}} \nsubseteq \{A\}$, then $Z_2 \leqslant A$ and $|Z_2/Z| = p$.*

*Proof.* Fix some $P \in \mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$. Then $P \nleq A$ since $P$ is $\mathcal{F}$-centric. Set $P_0 = P \cap A$, and fix some element $x \in P{\smallsetminus}P_0$. Since $\mathrm{Out}_{\mathcal{F}}(P)$ is finite (definition 1.1) and contains a strongly $p$-embedded subgroup, we have that $O_p(\mathrm{Out}_{\mathcal{F}}(P)) = 1$ (cf. [**7**, proposition A.7(c)]).

We must show that $P \in \mathcal{H} \cup \mathcal{B}$, $|N_S(P)/P| = p$, $Z_2 \leqslant A$, and $|Z_2/Z| = p$. (Clearly, $|N_S(P)/P| = p$ if $P = A$.)

**Case 1:** Assume $P$ is nonabelian. Since $Z \leqslant P$ ($P$ is $\mathcal{F}$-centric), $Z(P) = C_{P_0}(x) = Z$. For each $g \in N_A(P){\smallsetminus}P$, $c_g$ is the identity on $P_0$ and on $P/P_0$. If $P_0$ is characteristic in $P$, then $c_g \in O_p(\mathrm{Aut}_{\mathcal{F}}(P))$ by lemma A.1, which is impossible since $O_p(\mathrm{Out}_{\mathcal{F}}(P)) = 1$. Thus $P_0$ is not characteristic in $P$, and hence is not the unique abelian subgroup of index $p$ in $P$. So by lemma A.3, $|P_0/Z| = p$ and $|[P,P]| = |[x,P_0]| = p$. Also, $P/Z$ is abelian since $|P/Z| = p^2$, so $[x,P_0] \leqslant Z$, and hence $P_0 \leqslant Z_2$. Note that $P_0 > Z$, since $P$ is nonabelian.

If $P_0 < Z_2$, then for $y \in Z_2 \smallsetminus P$, $[y,P] \leqslant Z = Z(P)$, so $y \in N_S(P) \smallsetminus P$ and $c_y \in O_p(\mathrm{Aut}(P))$, contradicting the assumption that $P$ is $\mathcal{F}$-essential. Thus $P_0 = Z_2$, so $P \in \mathcal{B}$, $Z_2 \leqslant A$, and $|Z_2/Z| = p$. Finally, $|N_S(P)/P| = p$ by lemma A.6, applied with $\mathrm{Out}_{\mathcal{F}}(P)$ in the role of $G$, $\mathrm{Out}_S(P) \cong N_S(P)/P$ in the role of $S$, and $P/Z_0$ (if $P \in \mathcal{B}$) in the role of $A$. Note that $[P,P] = [x,Z_2] \leqslant Z_0$ and $C_{P/Z_0}(N_S(P)) = Z_2/Z_0$.

**Case 2:** If $P \in \mathbf{E}_{\mathcal{F}}$ is abelian, then $P_0 = Z$: it contains $Z$ since $P$ is centric, and cannot be larger since then $P$ would be nonabelian. Hence $P = Z\langle x\rangle \in \mathcal{H}$. Also, $\mathrm{Aut}_A(P) = \mathrm{Aut}_S(P) \in \mathrm{Syl}_p(\mathrm{Aut}_{\mathcal{F}}(P))$ centralizes $P_0$. The conditions of lemma A.6 thus hold (with $P$ and $\mathrm{Aut}_{\mathcal{F}}(P)$ in the roles of $A$ and $G$), so $|N_S(P)/P| =$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

$|\mathrm{Aut}_S(P)| = p$. Since $[S{:}P] = |A/Z| > p$ by lemma A.3 and since $A$ is the unique abelian subgroup of index $p$, this implies that $S/Z$ is nonabelian, so $[x, A] \nleqslant Z$, and $Z_2 \leqslant A$.

For each $g \in A$, $g \in N_S(P)$ if and only if $[g, x] \in P_0 = Z$, if and only if $gZ \in C_{A/Z}(x) = Z(S/Z) = Z_2/Z$. Thus $N_A(P) = Z_2$, $N_S(P) = Z_2\langle x\rangle = Z_2P$, and $|Z_2/Z| = |N_S(P)/P| = p$. □

Lemma 2.3. *Let $S$, $\mathcal{F}$, etc. be as in notation 2.1. If, for some $x \in S \smallsetminus A$, $Z_2\langle x\rangle \in \mathbf{E}_{\mathcal{F}}$, then $Z\langle x\rangle$ is not $\mathcal{F}$-centric, and hence $Z\langle x\rangle \notin \mathbf{E}_{\mathcal{F}}$.*

*Proof.* Assume $x \in S \smallsetminus A$ and $Z_2\langle x\rangle \in \mathbf{E}_{\mathcal{F}}$, and set $P = Z_2\langle x\rangle \in \mathcal{B}$. In particular, $Z_2 < A$ since $Z_2\langle x\rangle < S$. Also, $|Z_2/Z| = p$ by lemma 2.2, so $|P/Z| = p^2$, and $Z_2$ is not normalized by $\mathrm{Aut}_{\mathcal{F}}(P)$ since $P$ is essential.

Let $\mathcal{P}$ be the set of all subgroups of index $p$ in $P$ which contain $Z$. Then $\mathcal{P} \supsetneqq \{Z_2\}$, so $P/Z \cong C_p^2$ (i.e., is not cyclic), and $\mathrm{Aut}_S(P)$ permutes transitively the $p$ members of $\mathcal{P} \smallsetminus \{Z_2\}$. So $\mathrm{Aut}_{\mathcal{F}}(P)$ must act transitively on $\mathcal{P}$, hence $Z\langle x\rangle$ is $\mathcal{F}$-conjugate to $Z_2$, and is not $\mathcal{F}$-centric (recall $Z_2 < A$). So $Z\langle x\rangle \notin \mathbf{E}_{\mathcal{F}}$ in this case. □

Lemma 2.4. *Assume notation 2.1, and also $A \ntrianglelefteq \mathcal{F}$ ($\iff$ $\mathbf{E}_{\mathcal{F}} \nsubseteq \{A\}$). Then $|Z_0| = p$, and $|Z_i(S)/Z_{i-1}(S)| = p$ for all $i > 1$ such that $Z_i(S) < S$. If $|A| < \infty$, then $|A/ZS'| = p$.*

*Proof.* Fix $x \in S \smallsetminus A$. Let $\psi \in \mathrm{End}(A)$ be the homomorphism $\psi(g) = [g, x]$. Thus $\mathrm{Ker}(\psi) = Z$ and $\mathrm{Im}(\psi) = S'$.

By lemma 2.2 and since $\mathbf{E}_{\mathcal{F}} \nsubseteq \{A\}$, $(\mathcal{H} \cup \mathcal{B}) \cap \mathbf{E}_{\mathcal{F}} \neq \varnothing$, $Z_2 \leqslant A$, and $|Z_2/Z| = p$. Since $Z_2/Z = C_{A/Z}(x)$, $Z_2 = \psi^{-1}(Z)$, and so $\psi$ sends $Z_2$ onto $Z_0 = Z \cap S'$ with kernel $Z$. Thus $|Z_0| = |Z_2/Z| = p$.

Set $Z_i = Z_i(S)$ for each $i \geqslant 0$, and let $k > 2$ be the smallest index such that $Z_k = S$. Thus $S/Z_{k-2}$ is nonabelian, so $Z_{k-2} \leqslant A$, and $Z_{k-1}/Z_{k-2} = Z(S/Z_{k-2}) \leqslant A/Z_{k-2}$. Hence $Z_i \leqslant A$, and $Z_i = \psi^{-1}(Z_{i-1})$, for all $i < k$. In particular, $\psi$ induces a monomorphism from $Z_i/Z_{i-1}$ into $Z_{i-1}/Z_{i-2}$ for each $3 \leqslant i < k$, so $|Z_i/Z_{i-1}| \leqslant p$, with equality since $Z_i(S) > Z_{i-1}(S)$ whenever $Z_{i-1}(S) < S$.

If $|A| < \infty$, then $|ZS'| = |Z|{\cdot}|S'|/|Z_0| = |A|/|Z_0|$, and hence $ZS'$ has index $p$ in $A$. □

Lemma 2.5. *Let $A \trianglelefteq S$, $\mathcal{F}$, $\mathcal{H}$, $\mathcal{B}$, and so on, be as in notation 2.1. Assume $P \in \mathbf{E}_{\mathcal{F}}$ where $P \in \mathcal{H} \cup \mathcal{B}$, and set $X = 1$ if $P \in \mathcal{H}$ and $X = Z_0$ if $P \in \mathcal{B}$. Define $P_1, P_2 \leqslant P$ by setting*

$$P_1/X = C_{P/X}(O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P))) \quad \text{and} \quad P_2 = [O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P)), P].$$

*Then $O^{p'}(\mathrm{Out}_{\mathcal{F}}(P)) \cong SL_2(p)$, and the following hold.*

(a) *If $P \in \mathcal{H}$, then $P_1 < Z$, $Z = P_1 \times Z_0$, $Z_0 < P_2 \cong C_p^2$, and $P = P_1 \times P_2$. If $p$ is odd, then $P_1$ is the unique $\mathrm{Aut}_{\mathcal{F}}(Z)$-invariant subgroup of $Z$ such that $Z = P_1 \times Z_0$.*

(b) *If $P \in \mathcal{B}$, then $P_1 = Z$, $P_2$ is extraspecial of order $p^3$, $P_2 \cong Q_8$ if $p = 2$ while $P_2$ has exponent $p$ if $p$ is odd, and $P_1 \cap P_2 = Z(P_2) = Z_0 = [P, P]$. Thus $P = P_1 \times_{Z_0} P_2$.*

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

*Proof.* To simplify notation, set $H = \mathrm{Out}_{\mathcal{F}}(P)$, $H_0 = O^{p'}(H)$, and $T = \mathrm{Out}_S(P) \in \mathrm{Syl}_p(H)$.

If $P \in \mathcal{B}$, then $[P, P] \leqslant Z(P) \cap S' = Z \cap S' = Z_0$, with equality since $|Z_0| = p$ by lemma 2.4. Thus $P/X$ is abelian in both cases. Also, $[N_S(P), P/X] = Z_0$ (if $P \in \mathcal{H}$) or $Z_2/Z_0$ (if $P \in \mathcal{B}$), and thus has order $p$ in both cases. So by proposition A.7, applied to the $H$-action on $P/X$, we have $H_0 \cong SL_2(p)$, $P/X = (P_1/X) \times (P_2/X)$, and $P_2/X \cong C_p^2$.

If $P \in \mathcal{H}$ (so $X = 1$), then $P_1 = C_P(H_0) \leqslant C_P(T) = Z$, and $[Z{:}P_1] = p$ since $[P{:}P_1] = p^2$. Also, $P_2 \geqslant [T, P] = Z_0$, so $P_1 \cap Z_0 = 1$, and $Z = P_1 \times Z_0$. If $p$ is odd, then $N_{H_0}(T)$ is a semidirect product of the form $C_p \rtimes C_{p-1}$. Fix $\alpha \in N_{H_0}(T)$ of order $p - 1$; then $\alpha$ acts on $Z_0 = [T, P]$ with order $p - 1$ and acts trivially on $P_1$. Thus $\alpha|_Z \in \mathrm{Aut}_{\mathcal{F}}(Z)$, and $P_1$ is the only subgroup which is a complement to $Z_0$ in $Z$ and could be normalized by $\mathrm{Aut}_{\mathcal{F}}(Z)$. Since $\mathrm{Aut}_{\mathcal{F}}(Z)$ has order prime to $p$, there is at least one such subgroup, and hence $P_1$ is $\mathrm{Aut}_{\mathcal{F}}(Z)$-invariant.

If $P \in \mathcal{B}$, then $X = Z_0$, and $P_2/Z_0 \cong C_p^2$. Also, $H_0 \cong SL_2(p)$ acts faithfully on $P_2$, and this is possible only if $Z(P_2) = Z_0$, and $P_2 \cong Q_8$ (if $p = 2$) or $P_2$ is extraspecial of exponent $p$ (if $p$ is odd). Also, $P_1$ has index $p^2$ in $P$ since $P_1 \cap P_2 = Z_0$, $P_1 \leqslant Z(P)$ since $P = P_1 \times_{Z_0} P_2$ is a central product, and hence $P_1 = Z(P) = Z$. □

Corollary 2.6. *In the situation of notation 2.1, if $A \ntrianglelefteq \mathcal{F}$ (i.e., if $\mathbf{E}_{\mathcal{F}} \nsubseteq \{A\}$) and $p$ is odd, then $S$ splits over $A$: there is $x \in S \smallsetminus A$ of order $p$.*

*Proof.* Fix $P \in \mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$. By lemma 2.2, $P \in \mathcal{H} \cup \mathcal{B}$. In either case, by lemma 2.5, there is $x \in P \smallsetminus A$ of order $p$. □

We now restrict to the case where $p$ is odd. Recall that $G = \mathrm{Aut}_{\mathcal{F}}(A)$ by notation 2.1.

Lemma 2.7. *Assume notation 2.1, and also that $p$ is odd and $A \ntrianglelefteq \mathcal{F}$. Then $O_p(\mathcal{F}) = 1$ if and only if either there are no nontrivial $G$-invariant subgroups of $Z$, or $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} \neq \varnothing$ and $Z_0$ is the only $G$-invariant subgroup of $Z$.*

*Proof.* The following proof is essentially the same as the proof in [**15**, lemma 2.7(a)] in the finite case.

Assume first that $Q \overset{\mathrm{def}}{=} O_p(\mathcal{F}) \neq 1$. Since $A \ntrianglelefteq \mathcal{F}$, there is $P \in \mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} \subseteq \mathcal{B} \cup \mathcal{H}$. If $P \in \mathcal{H}$, then $Q \leqslant Z$: the intersection of the subgroups $S$-conjugate to $P$. If $P \in \mathcal{B}$, then $Q \leqslant Z_2$ by a similar argument, and then $Q \leqslant Z$ since that is the intersection of the subgroups in the $\mathrm{Aut}_{\mathcal{F}}(P)$-orbit of $Z_2$. Thus $Q$ is a non-trivial $G$-invariant subgroup of $Z$. If $Q = Z_0$, then $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing$, since for $P \in \mathbf{E}_{\mathcal{F}} \cap \mathcal{H}$, $Z_0$ is not normalized by $\mathrm{Aut}_{\mathcal{F}}(P)$. This proves one implication.

Conversely, assume that $1 \neq R \leqslant Z$ is $G$-invariant. For each $\alpha \in \mathrm{Aut}_{\mathcal{F}}(S)$, $\alpha(A) = A$ since $A$ is the unique abelian subgroup of index $p$, so $\alpha|_A \in G$, and thus $\alpha(R) = R$. Since each element of $\mathrm{Aut}_{\mathcal{F}}(Z)$ extends to $S$ by the extension axiom, $R$ is also normalized by $\mathrm{Aut}_{\mathcal{F}}(Z)$. Also, for each $P \in \mathbf{E}_{\mathcal{F}} \cap \mathcal{B}$, $Z = Z(P)$ is characteristic in $P$ and so $R$ is also normalized by $\mathrm{Aut}_{\mathcal{F}}(P)$. In particular, if $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing$, then $R \trianglelefteq \mathcal{F}$, and so $O_p(\mathcal{F}) \neq 1$.

Now assume that $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} \neq \varnothing$, and also that $R \neq Z_0$. By [**15**, lemma 2.3(b)] (the argument easily extends to the infinite case), there is a unique $\mathrm{Aut}_{\mathcal{F}}(Z)$-invariant

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

factorization $Z = Z_0 \times \widetilde{Z}$. Set $\widetilde{R} = R \cap \widetilde{Z}$. If $R \geqslant Z_0$, then $R = \widetilde{R} \times Z_0$. Otherwise, $R \cap Z_0 = 1$ (recall $|Z_0| = p$), and since $R$ is $\mathrm{Aut}_{\mathcal{F}}(Z)$-invariant, the uniqueness of the splitting implies that $R \leqslant \widetilde{Z}$ and hence $R = \widetilde{R}$. Since $R \neq Z_0$, we have $\widetilde{R} \neq 1$ in either case.

For each $\varphi \in \mathrm{Aut}_{\mathcal{F}}(A) = G$, $\varphi(\widetilde{R}) \leqslant R \leqslant Z$, so by the extension axiom, $\varphi|_{\widetilde{R}}$ extends to some $\bar{\varphi} \in \mathrm{Aut}_{\mathcal{F}}(S)$, and $\varphi(\widetilde{R}) = \bar{\varphi}(\widetilde{R}) = \widetilde{R}$ since $\widetilde{R}$ is $\mathrm{Aut}_{\mathcal{F}}(Z)$-invariant. So by the same arguments as those applied above to $R$, $\widetilde{R}$ is normalized by $\mathrm{Aut}_{\mathcal{F}}(P)$ for each $P \in (\{S\} \cup \mathbf{E}_{\mathcal{F}}) \smallsetminus \mathcal{H}$. If $P \in \mathbf{E}_{\mathcal{F}} \cap \mathcal{H}$, then for each $\alpha \in \mathrm{Aut}_{\mathcal{F}}(P)$, $\alpha(\widetilde{Z}) = \widetilde{Z}$ by [**15**, lemma 2.3(b)], so $\alpha|_{\widetilde{Z}}$ extends to an element of $\mathrm{Aut}_{\mathcal{F}}(S)$ and hence of $\mathrm{Aut}_{\mathcal{F}}(Z)$, and in particular, $\alpha(\widetilde{R}) = \widetilde{R}$. Thus $1 \neq \widetilde{R} \trianglelefteq \mathcal{F}$, and hence $O_p(\mathcal{F}) \neq 1$. □

Without the assumption that $p$ be odd in lemma 2.7, the 2-fusion system $\mathcal{F}$ of $P\Sigma L_2(q^2)$ is a counterexample for each prime power $q \equiv \pm 1 \pmod 8$. Here, $P\Sigma L_2(q^2) = PSL_2(q^2)\langle\theta\rangle$ where $\theta$ acts on $PSL_2(q^2)$ as a field automorphism of order 2 (and $\theta^2 = 1$). Then $O_2(\mathcal{F}) = 1$, $S \cong D_{2^m} \times C_2$ for some $m \geqslant 4$ depending on $q$, $A \cong C_{2^{m-1}} \times C_2$, $Z = Z(S) = \Omega_1(A)$, and $G = \mathrm{Aut}_S(A)$ acts trivially on $Z$ (so that all subgroups of $Z$ are $G$-invariant).

Lemma 2.8. *Assume notation 2.1, and also that $p$ is odd and $O_p(\mathcal{F}) = 1$. Let $A_2 \leqslant A_1 \leqslant A$ be $G$-invariant subgroups such that $A_1 \leqslant ZA_2$. Then either $A_1 = A_2$, or $A_1 = Z_0 \times A_2$ and $Z_0$ is $G$-invariant.*

*Proof.* Fix a class $xA_2 \in A_1/A_2$. By assumption, we can assume $x \in Z$. Since $G$ acts on $A_1/A_2$ and $\mathbf{U}$ acts trivially on this quotient, $G_0 = O^{p'}(G)$ also acts trivially. Hence $\alpha(x) \in xA_2$ for each $\alpha \in G_0$. Let $\alpha_1, \ldots, \alpha_k \in G_0$ be left coset representatives for $\mathbf{U}$ (so $p \nmid k = [G_0{:}\mathbf{U}]$), and set $y = \left(\prod_{i=1}^{k} \alpha_i(x)\right)^{1/k}$. Then $y \in xA_2$ since $\alpha_i(x) \in xA_2$ for each $i$, and $y \in C_A(G_0)$. This shows that $A_1 \leqslant C_A(G_0)A_2$.

Now, $C_A(G_0)$ is a subgroup of $Z = C_A(\mathbf{U})$ normalized by $G$. So by lemma 2.7 and since $O_p(\mathcal{F}) = 1$, $C_A(G_0) \leqslant Z_0$. Thus $A_1 \leqslant Z_0A_2$. If $A_1 > A_2$, then $A_1 = A_2 \times Z_0$ since $|Z_0| = p$, and $Z_0 = C_A(G_0)$ is $G$-invariant. □

The following notation, taken from [**15**, notation 2.4], will be used throughout the rest of the paper.

Notation 2.9. *Assume notation 2.1, and also that $|Z_0| = p$. Set*

$$\Delta = (\mathbb{Z}/p)^\times \times (\mathbb{Z}/p)^\times, \quad \text{and} \quad \Delta_i = \{(r, r^i) \mid r \in (\mathbb{Z}/p)^\times\} \leqslant \Delta \quad (\text{for } i \in \mathbb{Z}).$$

*Set*

$$\begin{aligned}
\mathrm{Aut}^\vee(S) &= \{\alpha \in \mathrm{Aut}(S) \mid [\alpha, Z] \leqslant Z_0\} \\
\mathrm{Aut}^\vee(A) &= \{\alpha|_A \mid \alpha \in \mathrm{Aut}^\vee(S)\} \\
\mathrm{Aut}^\vee_{\mathcal{F}}(S) &= \mathrm{Aut}^\vee(S) \cap \mathrm{Aut}_{\mathcal{F}}(S) \\
\mathrm{Aut}^\vee_{\mathcal{F}}(A) &= \mathrm{Aut}^\vee(A) \cap \mathrm{Aut}_{\mathcal{F}}(A) = \{\beta \in N_{\mathrm{Aut}_{\mathcal{F}}(A)}(\mathrm{Aut}_S(A)) \mid [\beta, Z] \leqslant Z_0\}.
\end{aligned}$$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

*Define*

$$\mu\colon \mathrm{Aut}^\vee(S) \longrightarrow \Delta \quad \text{and} \quad \mu_A\colon \mathrm{Aut}^\vee(A) \longrightarrow \Delta$$

*by setting, for* $\alpha \in \mathrm{Aut}^\vee(S)$,

$$\mu(\alpha) = (r,s) \quad \text{if} \quad \begin{cases} \alpha(x) \in x^r A & \text{for } x \in S \smallsetminus A \\ \alpha(g) = g^s & \text{for } g \in Z_0 \end{cases}$$

*and* $\mu_A(\alpha|_A) = \mu(\alpha)$ *if* $\alpha \in \mathrm{Aut}^\vee_{\mathcal{F}}(S)$.

## 3. Minimally active modules

In the earlier paper [15], the concept of ‘minimally active’ modules played a central role when identifying the pairs $(A, \mathrm{Aut}_{\mathcal{F}}(A))$ that can occur in a simple fusion system $\mathcal{F}$ over a $p$-group $S$ that contains an elementary abelian group $A$ with index $p$. Before continuing to study the structure of such $\mathcal{F}$, we need to recall some of the notation and results in that paper, beginning with [15, definitions 3.1 & 3.3], and describe how they relate to the more general situation here.

Definition 3.1. For each prime $p$,

- $\mathscr{G}_p$ is the class of finite groups $\varGamma$ with $U \in \mathrm{Syl}_p(\varGamma)$ such that $|U| = p$ and $U \ntrianglelefteq \varGamma$; and
- $\mathscr{G}_p^\wedge$ is the class of those $\varGamma \in \mathscr{G}_p$ such that $|\mathrm{Out}_\varGamma(U)| = p-1$ for $U \in \mathrm{Syl}_p(\varGamma)$.

For $\varGamma \in \mathscr{G}_p$, an $\mathbb{F}_p\varGamma$-module is *minimally active* if its restriction to $U \in \mathrm{Syl}_p(\varGamma)$ has exactly one Jordan block with nontrivial action.

The next lemma explains the importance of minimally active modules here. In particular, it means that many of the tables and results in [15, § 4–5] can be applied to get information about $\mathrm{Aut}_{\mathcal{F}}(A)$ and $\Omega_1(A)$.

Lemma 3.2. *Assume notations 2.1 and 2.9, and also that* $p$ *is odd,* $A \in \mathbf{E}_{\mathcal{F}}$, *and* $O_p(\mathcal{F}) = 1$. *Set* $V = \Omega_1(A)$ *and*

$$\begin{aligned} \mathrm{Aut}^\vee_{\mathcal{F}}(V) &= \bigl\{\beta \in N_{\mathrm{Aut}_{\mathcal{F}}(V)}(\mathrm{Aut}_S(V)) \bigm| [\beta, \Omega_1(Z)] \leqslant Z_0\bigr\} \\ &= \bigl\{\alpha|_V \bigm| \alpha \in \mathrm{Aut}_{\mathcal{F}}(S),\ [\alpha, \Omega_1(Z)] \leqslant Z_0\bigr\}, \end{aligned}$$

*and define* $\mu_V\colon \mathrm{Aut}^\vee_{\mathcal{F}}(V) \longrightarrow \Delta$ *by setting* $\mu_V(\alpha|_V) = \mu(\alpha)$. *Then*

(a) $G = \mathrm{Aut}_{\mathcal{F}}(A) \in \mathscr{G}_p^\wedge$;

(b) $V$, *and* $A/\mathrm{Fr}(A)$ *if* $|A| < \infty$, *are both faithful, minimally active, and indecomposable as* $\mathbb{F}_pG$*-modules; and*

(c) $$\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}}(A)) = \begin{cases} \mu_V(\mathrm{Aut}^\vee_{\mathcal{F}}(V)) & \text{if } Z_0 \nleq \mathrm{Fr}(A) \\ \mu_V(\mathrm{Aut}^\vee_{\mathcal{F}}(V)) \cap \Delta_0 & \text{if } Z_0 \leqslant \mathrm{Fr}(A). \end{cases}$$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

*Proof.* **(a)** By assumption, $\mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$ has order $p$. Since $A \in \mathbf{E}_{\mathcal{F}}$, $\mathbf{U}$ is not normal in $G = \mathrm{Aut}_{\mathcal{F}}(A)$, and hence $G \in \mathscr{G}_p$.

Since $O_p(\mathcal{F}) = 1$, there is $P \in \mathbf{E}_{\mathcal{F}} \cap (\mathcal{H} \cup \mathcal{B})$. By lemma 2.5(a,b), $O^{p'}(\mathrm{Out}_{\mathcal{F}}(P)) \cong SL_2(p)$. Choose $\alpha \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P))$ of order $p-1$ whose class in $\mathrm{Out}_{\mathcal{F}}(P)$ normalizes $\mathrm{Out}_S(P) \cong C_p$; then $\alpha$ extends to an element of $\mathrm{Aut}_{\mathcal{F}}(N_S(P))$ and hence (since $P$ is maximal among $\mathcal{F}$-essential subgroups) to some $\bar{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(S)$. Then $\bar{\alpha}|_A$ normalizes $\mathbf{U}$ and its class in $\mathrm{Aut}_G(\mathbf{U})$ has order $p-1$, so $G \in \mathscr{G}_p^{\wedge}$.

**(b)** Set $\overline{A} = A/\mathrm{Fr}(A)$. If $|A| < \infty$, then since $G$ acts faithfully on $A$, [20, theorems 5.2.4 & 5.3.5] imply that $C_G(V)$ and $C_G(\overline{A})$ are both normal $p$-subgroups of $G$. Since $\mathbf{U}$ is not normal by (a), $G$ acts faithfully on $V$ and on $\overline{A}$ in this case. If $|A| = \infty$, then $G$ acts faithfully on $\Omega_m(A)$ for $m$ large enough, and hence acts faithfully on $V$ by the above argument.

Since $|Z_0| = p$ by lemma 2.4, where $Z_0 = S' \cap Z = [\mathbf{U}, V] \cap C_V(\mathbf{U})$, the $\mathbb{F}_p\mathbf{U}$-module $V|_{\mathbf{U}}$ has exactly one Jordan block with nontrivial action of $\mathbf{U}$. So $V$ is minimally active. If $|A| < \infty$, then $ZS' = C_A(\mathbf{U})[\mathbf{U}, A]$ has index $p$ in $A$ by lemma 2.4, so $C_{\overline{A}}(\mathbf{U})[\mathbf{U}, \overline{A}]$ has index at most $p$ in $\overline{A}$, and hence $\overline{A}$ is minimally active.

If $V = V_1 \times V_2$, where each $V_i$ is a nontrivial $\mathbb{F}_pG$-submodule, then by [15, lemma 3.4(a)], we can assume (after exchanging indices if needed) that $V_1 \leqslant Z$ and (since it is a summand) $V_1 \cap Z_0 = 1$. But this contradicts lemma 2.7.

Assume $|A| < \infty$. If $\overline{A} = \overline{X} \times \overline{Y}$ where $\overline{X}, \overline{Y} \leqslant \overline{A}$ are $\mathbb{F}_pG$-submodules, then by the Krull-Schmidt theorem, one of the factors, say $\overline{X}$, contains a nontrivial Jordan block, while $\mathbf{U}$ acts trivially on the other factor. Thus $\overline{X} \geqslant [\mathbf{U}, \overline{A}]$ and $\overline{X} \nleqslant ZS'/\mathrm{Fr}(A)$. Let $X \leqslant A$ be such that $\mathrm{Fr}(A) \leqslant X$ and $X/\mathrm{Fr}(A) = \overline{X}$. Then $X \geqslant S'$ and $X \nleqslant ZS'$, so $XZ = A$. By lemma 2.8, either $X = A$ (and $\overline{X} = \overline{A}$) or $A = X \times Z_0$ (which is impossible since $Z_0 \leqslant S' \leqslant X$). Thus $\overline{X} = \overline{A}$, and $\overline{A}$ is indecomposable.

**(c)** By definition, the restriction to $V$ of each element in $\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)$ lies in $\mathrm{Aut}^{\vee}_{\mathcal{F}}(V)$, and hence $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)) \leqslant \mu_V(\mathrm{Aut}^{\vee}_{\mathcal{F}}(V))$. If $Z_0 \leqslant \mathrm{Fr}(Z)$, then choose $z \in Z$ such that $1 \neq z^p \in Z_0$. For each $\beta \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(A)$, $\beta(z) = z^{pk+1}$ for some $k$ since $[\beta, Z] \leqslant Z_0$, and hence $\beta|_{Z_0} = \mathrm{Id}$ and $\mu_A(\beta) \in \Delta_0$. Thus $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A))$ is contained in the right-hand side in (c).

Now assume that $\beta \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(V)$, where $\beta = \alpha|_V$ for $\alpha \in \mathrm{Aut}_{\mathcal{F}}(S)$. If $Z_0 \leqslant \mathrm{Fr}(A)$, then assume also that $\mu_V(\beta) \leqslant \Delta_0$; that is, that $\beta|_{Z_0} = \mathrm{Id}$. Upon replacing $\beta$ by $\beta^{p^k}$ and $\alpha$ by $\alpha^{p^k}$ for appropriate $k$, we can also assume that $\alpha$ has order prime to $p$ without changing $\mu(\alpha)$. Then $Z = C_Z(\alpha) \times [\alpha, Z]$ by [20, theorem 5.2.3] and since $Z$ is the union of the finite abelian $p$-groups $\Omega_i(Z)$, and $[\alpha, \Omega_1(Z)] = [\beta, \Omega_1(Z)] \leqslant Z_0$ since $\beta \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(V)$. Also, $\Omega_1([\alpha, Z]) = [\alpha, \Omega_1(Z)] \leqslant Z_0$ (since it canot be any larger). If $Z_0 \nleqslant \mathrm{Fr}(Z)$, then this implies that $[\alpha, Z] \leqslant Z_0$, hence that $\alpha \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(S)$. If $Z_0 \leqslant \mathrm{Fr}(Z)$, then $\Omega_1([\alpha, Z]) \leqslant Z_0 \leqslant C_Z(\alpha)$ implies that $\Omega_1([\alpha, Z]) = 1$ and hence $[\alpha, Z] = 1$, so again $\alpha \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(S)$. Thus $\mu_V(\beta) = \mu_A(\alpha|_A) \in \mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A))$, and the right-hand side in (c) is contained in $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A))$. □

The following basic properties of minimally active indecomposable modules, taken from [15], play an important role in the rest of the paper.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Lemma 3.3 ([15, proposition 3.7]). *Fix an odd prime $p$, a finite group $\Gamma \in \mathscr{G}_p$, and $U \in \mathrm{Syl}_p(\Gamma)$. Let $V$ be a faithful, minimally active, indecomposable $\mathbb{F}_p\Gamma$-module. Then*

(a) *$\dim(V) \leqslant p$ implies that $V|_U$ is indecomposable and thus contains a unique Jordan block;*

(b) *$\dim(V) \geqslant p+1$ implies that $V|_U$ is the direct sum of a Jordan block of dimension $p$ and a module with trivial action of $U$; and*

(c) *$\dim(C_V(U)) = 1$ if $\dim(V) \leqslant p$, while $\dim(C_V(U)) = \dim(V) - p + 1$ if $\dim(V) \geqslant p$.*

The next lemma is closely related to [15, lemma 1.11].

Lemma 3.4. *Fix an odd prime $p$, let $\Gamma$ be a finite group such that $U \in \mathrm{Syl}_p(\Gamma)$ has order $p$, and set $N = N_\Gamma(U)$. Let $V$ be a faithful, minimally active, indecomposable $\mathbb{F}_p\Gamma$-module such that $\dim(V) \leqslant p$. Then $C_V(U)$ and $V/[U,V]$ are both 1-dimensional, and the following hold.*

(a) *If $\dim(V) = p$, then $V/[U,V]$ and $C_V(U)$ are 1-dimensional, and isomorphic as $\mathbb{F}_p[N/U]$-modules.*

(b) *The projective cover and the injective envelope of $V|_N$ are both $p$-dimensional.*

(c) *If $\dim(V) = p-1$, and there is an $\mathbb{F}_p\Gamma$-submodule $V_0 < V$ with $\dim(V_0) = 1$, then there is a projective $\mathbb{F}_p\Gamma$-module $W$ such that $\dim(W) = p$ and $W$ has a submodule isomorphic to $V$.*

(d) *Let $W$ be another $\mathbb{F}_p\Gamma$-module such that $\dim(W) = \dim(V)$, and assume that $C_W(U) \cong C_V(U)$ as $\mathbb{F}_p[N_\Gamma(U)/U]$-modules. Then $W \cong V$ as $\mathbb{F}_p[N_\Gamma(U)]$-modules, and as $\mathbb{F}_p\Gamma$-modules if $\dim(V) < p$.*

*Proof.* **(a)** By lemma 3.3, $U$ acts on $V$ with only one Jordan block, so $\dim(C_V(U)) = 1$ and $\dim(V/[U,V]) = 1$. By [15, lemma 1.11(b)], if $g \in N_\Gamma(U)$ and $t \in (\mathbb{Z}/p)^\times$ are such that $g$ acts on $V/[U,V]$ via multiplication by $t$, then for some $r \in (\mathbb{Z}/p)^\times$, $g$ acts on $C_V(U)$ via multiplication by $tr^{m-1} = tr^{p-1} = t$. Thus $V/[U,V]$ and $C_V(U)$ are isomorphic as $\mathbb{F}_p[N_\Gamma(U)/U]$-modules.
**(b)** By the Schur-Zassenhaus theorem, there is $H < N$ of index $p$ such that $N = HU$. Set $V_0 = C_V(U)$, regarded as an $\mathbb{F}_p[N/U]$-module, and also as an $\mathbb{F}_pH$-module via the natural isomorphism $H \cong N/U$. Set $\widehat{V} = \mathrm{Ind}_H^N(V_0)$: a projective and injective $p$-dimensional $\mathbb{F}_pN$-module. Then

$$\widehat{V}/[U,\widehat{V}] \cong \mathbb{F}_p[N/U] \otimes_{\mathbb{F}_pN} \mathbb{F}_pN \otimes_{\mathbb{F}_pH} V_0 \cong \mathbb{F}_p[N/U] \otimes_{\mathbb{F}_pH} V_0 \cong V_0,$$

and so $C_{\widehat{V}}(U) \cong V_0$ by (a). Thus $\widehat{V}$ is the injective envelope of $V_0$ when regarded as an $\mathbb{F}_pN$-module. In particular, an isomorphism $C_V(U) \cong C_{\widehat{V}}(U)$ extends to an $\mathbb{F}_pN$-linear homomorphism $V \longrightarrow \widehat{V}$ which is injective since it sends the socle $C_V(U)$ injectively. Thus $\widehat{V}$ is an injective envelope of $V|_N$. The statement about projective covers is shown in a similar way (or by dualizing).

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

**(c)** Assume that $\dim(V) = p - 1$, and that there is an $\mathbb{F}_p\Gamma$-submodule $V_0 < V$ with $\dim(V_0) = 1$. Then $V_0 = C_V(U)$, since this is the unique 1-dimensional submodule of $V$ as an $\mathbb{F}_pU$-module. By (b), there is an injective (hence projective) $\mathbb{F}_pN$-module $\widehat{W}$ containing $V|_N$ as a submodule. By (a), $\widehat{W}/V \cong V_0|_N$ as $\mathbb{F}_pN$-modules.

Consider the homomorphisms

$$\operatorname{Ext}^1_{\mathbb{F}_p\Gamma}(V_0, V) \xrightarrow{\Phi_1} \operatorname{Ext}^1_{\mathbb{F}_pN}(V_0, V) \xrightarrow{\Phi_2} \operatorname{Ext}^1_{\mathbb{F}_pU}(V_0, V)$$

induced by restrictions of rings. Since $U$ has index prime to $p$ in $\Gamma$, $\Phi_1$ and $\Phi_2$ are injective, and the images of $\Phi_2$ and $\Phi_2\Phi_1$ are certain subgroups of stable elements (see [8, proposition 3.8.2] for this version of the stable elements theorem). Since $\operatorname{Ext}^1_{\mathbb{F}_p}(V_0, V) = 0$, we need to only consider the stability of elements with respect to automorphisms of $U$, and hence $\operatorname{Im}(\Phi_2) = \operatorname{Im}(\Phi_2\Phi_1)$.

Thus $\Phi_1$ is an isomorphism. Interpreted in terms of extensions, this implies that there is an extension $0 \longrightarrow V \longrightarrow W \longrightarrow V_0 \longrightarrow 0$ of $\mathbb{F}_p\Gamma$-modules such that $W|_N \cong \widehat{W}$. In particular, $W$ is projective since $\widehat{W}$ is projective as an $\mathbb{F}_pN$-module.

**(d)** By (b), the injective envelope $\widehat{V}$ of $V|_N$ is $p$-dimensional. Hence $C_{\widehat{V}}(U) \cong C_V(U) \cong C_W(U)$, so $\widehat{V}$ is also the injective envelope of $C_W(U)$, and hence of $W|_N$ since $C_W(U)$ is its socle. Since $\dim(V) = \dim(W)$, and $\widehat{V}$ contains a unique $\mathbb{F}_pN$-submodule of each dimension $m \leqslant p$, we conclude that $V \cong W$ is isomorphic as $\mathbb{F}_pN$-modules.

If $\dim(V) < p$, then $U$ is a vertex of $V$ and of $W$ and they are the Green correspondents of $V|_N$ and $W|_N$, respectively (see [8, § 3.12]). So $V \cong W$ as $\mathbb{F}_p\Gamma$-modules. □

Point (d) need not hold if $\dim(V) = p$. As an example, fix $p \geqslant 5$, set $\Gamma = SL_2(p)$ and choose $U \in \operatorname{Syl}_p(\Gamma)$, let $V$ be the simple $p$-dimensional $\mathbb{F}_p\Gamma$-module, and let $W$ be the projective cover of the trivial 1-dimensional $\mathbb{F}_p\Gamma$-module. Using the fact that $V$ is the $(p-1)$-st symmetric power of the natural 2-dimensional $\mathbb{F}_p\Gamma$-module, it is not hard to see that $C_V(U)$ is 1-dimensional with trivial $N_\Gamma(U)/U$-action. The same holds for $W$ by construction, where $\dim(W) = p$. We refer to [2, pp. 48–52] or the discussion in [15, § 6] for more detail.

A minimally active indecomposable $\mathbb{F}_p\Gamma$-module of dimension at least $p+2$ is simple by [15, proposition 3.7(c)]. This is not true for modules of dimension $p+1$, but the following lemma gives some information about such modules.

Lemma 3.5. *Fix a finite group $\Gamma \in \mathscr{G}_p$ with $U \in \operatorname{Syl}_p(\Gamma)$. Let $V$ be a finite, minimally active, indecomposable $\mathbb{F}_p\Gamma$-module of rank $p+1$. If $0 \neq V_0 < V$ is a proper nontrivial submodule, then $V_0|_U$ and $(V/V_0)|_U$ are both indecomposable $\mathbb{F}_pU$-modules with nontrivial action. In particular, $2 \leqslant \dim(V_0) \leqslant p-1$.*

*Proof.* Recall $|U| = p$ since $\Gamma \in \mathscr{G}_p$. By [15, proposition 3.7(a)], $V|_U \cong \mathbb{F}_pU \oplus \mathbb{F}_p$; that is, $V|_U$ has Jordan blocks of dimension $p$ and 1.

Fix a proper nontrivial submodule $0 \neq V_0 < V$, and assume that $V_0|_U$ is decomposable or has trivial action as an $\mathbb{F}_pU$-module. We will first show that $V_0$ always has a 1-dimensional $\mathbb{F}_p\Gamma$-submodule, and then show that this is impossible. In particular, this shows that $\dim(V_0) \geqslant 2$. The corresponding results for $V/V_0$ then follow by dualizing.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

If $V_0|_U$ is decomposable with nontrivial action, then $V_0|_U$ is the sum of a 1-dimensional module with trivial action and an indecomposable module of dimension at most $p-1$. By [15, proposition 3.7(a)], $V_0$ is decomposable as an $\mathbb{F}_p\Gamma$-module, and thus has a 1-dimensional summand.

If $U$ acts trivially on $V_0$, then $\dim(V_0) \leqslant 2$ and $O^{p'}(\Gamma)$ (the normal closure of $U$ in $\Gamma$) acts trivially on $V_0$. If $\dim(V_0)=2$, then $V_0 = C_V(U)$, and $[U,V]\cap V_0$ is a 1-dimensional subspace normalized by $N_\Gamma(U)$. Since $\Gamma = O^{p'}(\Gamma)N_\Gamma(U)$ by the Frattini argument, $[U,V]\cap V_0$ is a 1-dimensional $\mathbb{F}_p\Gamma$-submodule.

We are thus reduced to the case where $\dim(V_0)=1$. If $V_0 \neq [U,V]$, then $(V/V_0)|_U$ is indecomposable (consists of one Jordan block), and hence is $\mathbb{F}_pU$-free. So $V/V_0$ is projective, contradicting the assumption that $V$ is indecomposable.

Thus $V_0=[U,V]$ is an $\mathbb{F}_p\Gamma$-submodule, and $V/V_0$ has Jordan blocks of length 1 and $p-1$. So by [15, proposition 3.7(a)], it is decomposable: there are submodules $W_1, W_2 < V$ such that $V/V_0 = (W_1/V_0)\oplus(W_2/V_0)$, where $\dim(W_1)=p$, and $(W_1/V_0)|_U$ is an (indecomposable) Jordan block. If $[U,W_1]=0$, then $[U,W_2]=V_0$, and $V|_U$ contains Jordan blocks of dimension $p-1$ and 2, which we saw is impossible. Thus $[U,W_1]=V_0$, so $W_1|_U$ is indecomposable, $W_1$ is projective and injective, and this again contradicts the assumption that $V$ is indecomposable.

This proves that $U$ acts nontrivially on $V_0$, and in particular, $\dim(V_0)\geqslant 2$. A similar argument applied to the dual $V^*$ shows that $U$ acts nontrivially on $V/V_0$, and that $\dim(V_0)\leqslant p-1$. □

The following definitions will be useful.

Definition 3.6. For a finite group $\Gamma$, a *$\mathbb{Z}_p\Gamma$-lattice* is a finitely generated $\mathbb{Z}_p\Gamma$-module that is free as a $\mathbb{Z}_p$-module (hence a lattice in a finitely generated $\mathbb{Q}_p\Gamma$-module). A *discrete $\Gamma$-$p$-torus* is a discrete $p$-torus equipped with an action of $\Gamma$ by automorphisms.

Let $\mathbb{Q}_p(\zeta)\supseteq\mathbb{Z}_p[\zeta]$ denote the extensions of $\mathbb{Q}_p\supseteq\mathbb{Z}_p$ by a primitive $p$-th root of unity $\zeta$. When $U$ is a group of order $p$, we regard $\mathbb{Q}_p(\zeta)$ and $\mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_pU$-modules under some choice of identification $U\cong\langle\zeta\rangle$.

Lemma 3.7. *Fix an odd prime $p$, a group $\Gamma\in\mathscr{G}_p$, and $U\in\mathrm{Syl}_p(\Gamma)$.*

(a) *Let $\Lambda$ be a $\mathbb{Z}_p\Gamma$-lattice such that $\Lambda/p\Lambda$ is faithful and minimally active as an $\mathbb{F}_p\Gamma$-module. Then $\Lambda/C_\Lambda(U)\cong\mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_pU$-modules, and $[U,\Lambda]+C_\Lambda(U)$ has index $p$ in $\Lambda$.*

(b) *Let $A$ be a discrete $\Gamma$-$p$-torus such that $\Omega_1(A)$ is faithful and minimally active as an $\mathbb{F}_p\Gamma$-module. Then $A/C_A(U)\cong\mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_pU$-modules, and $|[U,A]\cap C_A(U)|=p$.*

(c) *Let $X$ be a finite, faithful $\mathbb{Z}_p\Gamma$-module. Then $\Gamma$ acts faithfully on $\Omega_1(X)$ and on $X/pX$. Among the following conditions:*
(1) *$\Omega_1(X)$ is minimally active as an $\mathbb{F}_p\Gamma$-module.*

(2) *$X/pX$ is minimally active as an $\mathbb{F}_p\Gamma$-module.*

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

(3) $|[U,X]\cap C_X(U)|=p$.

(4) *$[U,X]+C_X(U)$ has index $p$ in $X$.*
*we have* (1) $\Longleftarrow$ (3) $\Longleftrightarrow$ (4) $\Longrightarrow$ (2). *If $X\cong\Lambda/\Lambda_0$ for some $\mathbb{Z}_p\Gamma$-lattice $\Lambda$ and some submodule $\Lambda_0\leqslant p\Lambda$, then all four conditions are equivalent.*

(d) *If $X$ is a finite, faithful $\mathbb{Z}_p\Gamma$-module such that condition* (c.4) *holds, then for each $x\in X\smallsetminus([U,X]+C_X(U))$, $X=C_X(U)+\mathbb{Z}_pU{\cdot}x$.*

*Proof.* Fix a generator $u\in U$.
**(a)** Set $M=\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\Lambda$. By lemma A.5(a), $M/C_M(U)$ is isomorphic, as a $\mathbb{Q}_pU$-module, to a sum of copies of $\mathbb{Q}_p(\zeta)$, where $\zeta$ is a primitive $p$-th root of unity. In particular, each Jordan block for the action of $U$ on $\Lambda/(C_\Lambda(U)+p\Lambda)$ has length at most $p-1$. Since $\Lambda/p\Lambda$ is minimally active, it follows that $M/C_M(U)\cong\mathbb{Q}_p(\zeta)$, since otherwise $\Lambda/(C_\Lambda(U)+p\Lambda)$ would have ranked at least $2(p-1)$ and hence $U$ would be fixed by a submodule of rank at least $p\geqslant 3$. Hence $\Lambda/C_\Lambda(U)\cong\mathbb{Z}_p[\zeta]$ by lemma A.5(c).

Consider the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & C_\Lambda(U) \arrow[r, "\mathrm{incl}"] & \Lambda \arrow[r, "\varphi"] & {[U,\Lambda]} \arrow[r] & 0, \end{tikzcd}$$

where $\varphi(x)=u(x)-x$ for all $x\in\Lambda$. We just saw that $[U,\Lambda]\cong\mathbb{Z}_p[\zeta]$. Under this identification, $\varphi|_{[U,\Lambda]}$ is multiplication by $1-\zeta$, and so its image has index $p$ in $[U,\Lambda]$. Thus $C_\Lambda(U)+[U,\Lambda]$ has index $p$ in $\Lambda$.
**(b)** Let $A$ be a discrete $\Gamma$-$p$-torus such that $\Omega_1(A)$ is faithful and minimally active as an $\mathbb{F}_p\Gamma$-module. Set $\Lambda=\mathrm{Hom}_{\mathbb{Z}_p}(A,\mathbb{Q}_p/\mathbb{Z}_p)$, regarded as a $\mathbb{Z}_p\Gamma$-lattice. Then $\Omega_1(A)\cong\Lambda/p\Lambda$ by proposition A.4, so $\Lambda/p\Lambda$ is minimally active. We just saw, in the proof of (a), that this implies that $\Lambda/C_\Lambda(U)\cong\mathbb{Z}_p[\zeta]$. So after taking tensor products with $\mathbb{Q}_p/\mathbb{Z}_p$ and applying proposition A.4 again, we get that $A/(\mathbb{Q}_p/\mathbb{Z}_p\otimes_{\mathbb{Z}_p}C_\Lambda(U))\cong\mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$. Hence $A/C_A(U)\cong\mathbb{Q}_p(\zeta)/R$ for some $\mathbb{Z}_pU$-lattice $R<\mathbb{Q}_p(\zeta)$ that contains $\mathbb{Z}_p[\zeta]$ with finite index. Then $R\cong\mathbb{Z}_p[\zeta]$ by lemma A.5(c), $\mathbb{Q}_p(\zeta)=\mathbb{Q}_p{\cdot}R$, and so $A/C_A(U)\cong\mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$.

Consider the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & C_A(U) \arrow[r, "\mathrm{incl}"] & A \arrow[r, "\varphi"] & {[U,A]} \arrow[r] & 0, \end{tikzcd}$$

where $\varphi(x)=u(x)-x$ for all $x\in A$. We just saw that $[U,A]\cong\mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$. Under this identification, $\varphi|_{[U,A]}$ is multiplication by $1-\zeta$, and so its kernel has order $p$. Thus $|C_A(U)\cap[U,A]|=p$.
**(c)** We have $|X|=|C_X(U)|{\cdot}|[U,X]|$: $X$ is finite, and $[U,X]$ is the image of the homomorphism $X\xrightarrow{1-u}X$ while $C_X(U)$ is its kernel. Hence (3) and (4) are equivalent.

If (3) holds, then $[U,\Omega_1(X)]\cap C_{\Omega_1(X)}(U)$ also has order $p$ (since it cannot be trivial). Since the rank of this intersection is the number of Jordan blocks in $\Omega_1(X)$ with nontrivial $U$-action, we see that $\Omega_1(X)$ is minimally active in this case. So (3) implies (1); and a similar argument shows that (4) implies (2).

Assume that $\Lambda_0<\Lambda$ are $\mathbb{Z}_p\Gamma$-lattices such that $\Lambda_0\leqslant p\Lambda$ and $\Lambda/\Lambda_0\cong X$. In particular, $\Lambda/p\Lambda\cong X/pX$. So if $X/pX$ is minimally active, then $[U,\Lambda]+C_\Lambda(U)$ has

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

index $p$ in $\Lambda$ by (a), and hence $[U,X]+C_X(U)$ has index $p$ in $X$ (since it cannot be all of $X$). Thus (2) implies (4) in this case.

We continue to assume that $X\cong\Lambda/\Lambda_0$, and set $R_p=\mathbb{Q}_p/\mathbb{Z}_p$ for short. We have an exact sequence

$$0\longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}(R_p,X)\longrightarrow R_p\otimes_{\mathbb{Z}_p}\Lambda_0\longrightarrow R_p\otimes_{\mathbb{Z}_p}\Lambda\longrightarrow R_p\otimes_{\mathbb{Z}_p}X\longrightarrow 0.$$

Also, by tensoring the short exact sequence $0\to\mathbb{Z}_p\to\mathbb{Q}_p\to R_p\to 0$ by $X$ and using the fact that $\mathbb{Q}_p$ is flat over $Z_p$, we see that $R_p\otimes_{\mathbb{Z}_p}X=0$, and $\mathrm{Tor}_{\mathbb{Z}_p}(R_p,X)\cong X$ as $\mathbb{Z}_p\Gamma$-modules. Thus $X$ is isomorphic to a subgroup of the discrete $\Gamma$-$p$-torus $A=R_p\otimes_{\mathbb{Z}_p}\Lambda_0$ (see proposition A.4), where $\Omega_1(X)\cong\Omega_1(A)$. With the help of (b), we now see that (1) implies (3).

**(d)** Set $\overline{X}=X/pX$ for short. By (c), $\overline{X}$ is minimally active as an $\mathbb{F}_p\Gamma$-module. Hence there is $\bar{y}\in\overline{X}$ such that $\overline{X}=C_{\overline{X}}(U)+\mathbb{F}_pU{\cdot}\bar{y}$. Thus $[U,\overline{X}]=(1-u)\mathbb{F}_pU{\cdot}\bar{y}$. Choose $y\in X$ whose class modulo $p$ is $\bar{y}$; then $[U,X]\leqslant(1-u)\mathbb{Z}_pU{\cdot}y+pX$.

By assumption, $X=C_X(U)+[U,X]+\mathbb{Z}_p{\cdot}x$. So there are $\xi\in\mathbb{Z}_pU$ and $r\in\mathbb{Z}_p$ such that $y\in rx+(1-u)\xi{\cdot}y+C_X(U)+pX$. Then $(1-(1-u)\xi)y\in rx+C_X(U)+pX$, where $1-(1-u)\xi$ is invertible in $\mathbb{Z}_pU$ since $(1-u)^p\in p\mathbb{Z}_pU$. Thus $y\in\mathbb{Z}_pU{\cdot}x+C_X(U)+pX$, and hence $X=\mathbb{Z}_pU{\cdot}x+C_X(U)+pX$. Since $pX$ is the Frattini subgroup of $X$, it now follows that $X=\mathbb{Z}_pU{\cdot}x+C_X(U)$. □

In the rest of the section, we look at questions of existence and uniqueness of finite $\mathbb{Z}_p\Gamma$-modules or discrete $\Gamma$-$p$-tori $A$ for which $\Omega_1(A)$ is isomorphic to a given minimally active, indecomposable $\mathbb{F}_p\Gamma$-module.

PROPOSITION 3.8. *Fix an odd prime $p$ and a group $\Gamma\in\mathscr{G}_p$, and let $V$ be a faithful, minimally active, indecomposable $\mathbb{F}_p\Gamma$-module.*

(a) *If $\dim(V)\geqslant p-1$, then there is a $\mathbb{Q}_p\Gamma$-module $M$ and a $\mathbb{Z}_p\Gamma$-lattice $\Lambda\leqslant M$ such that $V\cong\Lambda/p\Lambda$.*

(b) *If $\dim(V)=p$, and there is an $\mathbb{F}_p\Gamma$-submodule $V_1<V$ of dimension 1, then $M$ and $\Lambda$ can be chosen as in (a) such that $M$ contains a 1-dimensional $\mathbb{Q}_p\Gamma$-submodule.*

*Proof.* Fix $U\in\mathrm{Syl}_p(\Gamma)$, and let $u\in U$ be a generator. Let $\zeta$ be a $p$-th root of unity, and regard $\mathbb{Q}_p(\zeta)$ as a $\mathbb{Q}_pU$-module where $u$ acts by multiplication by $\zeta$. Thus $\mathbb{Z}_p[\zeta]$ is a $\mathbb{Z}_pU$-lattice in $\mathbb{Q}_p(\zeta)$. We also write $\mathbb{F}_p[\zeta]=\mathbb{Z}_p[\zeta]/p\mathbb{Z}_p[\zeta]$. Thus $\mathbb{F}_p[\zeta]\cong\mathbb{F}_p[u]/\langle(1-u)^{p-1}\rangle$, and $V|_U\cong\mathbb{F}_p[\zeta]$ since $V$ is minimally active and indecomposable [**15**, proposition 3.7(a)].

**(a)** If $\dim(V)\geqslant p$, then $V$ is a trivial source module by [**15**, proposition 3.7(b)], and hence $V$ is the mod $p$ reduction of some $\mathbb{Z}_p\Gamma$-lattice (see [**8**, corollary 3.11.4.i]). So for the rest of the proof, we assume that $\dim(V)=p-1$.

Set $\widehat{\Lambda}=\mathrm{Ind}_U^\Gamma(\mathbb{Z}_p[\zeta])$ and $\widehat{V}=\mathrm{Ind}_U^\Gamma(V|_U)$. Then $\widehat{V}\cong\widehat{\Lambda}/p\widehat{\Lambda}$. Since induction of representations is adjoint to restriction, the identity on $V$ extends to a surjective $\mathbb{F}_p\Gamma$-linear homomorphism $\alpha\colon\widehat{V}\longrightarrow V$. This is split by an $\mathbb{F}_pU$-linear map, and hence (by averaging over cosets of $U$) by an $\mathbb{F}_p\Gamma$-linear homomorphism $\beta\colon V\longrightarrow\widehat{V}$.

Set $e_0 = \beta\alpha \in \operatorname{End}_{\mathbb{F}_p\Gamma}(\widehat{V})$. Thus $e_0$ is an idempotent in this endomorphism ring, and $e_0\widehat{V} \cong V$.

We want to lift $e_0$ to an idempotent in $\operatorname{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda})$. By the Mackey double coset formula,

$$\widehat{\Lambda}|_U = \bigl(\operatorname{Ind}_U^\Gamma(\mathbb{Z}_p[\zeta])\bigr)\big|_U \cong \bigl(\mathbb{Z}_p[\zeta]\bigr)^m \times \bigl(\mathbb{Z}_pU\bigr)^n$$

as $\mathbb{Z}_pU$-modules for some $m, n \geqslant 0$. Hence as $\mathbb{Z}_p$-modules,

$$\begin{aligned}\operatorname{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda}) \cong \operatorname{Hom}_{\mathbb{Z}_pU}(\mathbb{Z}_p[\zeta], \widehat{\Lambda}) &\cong \bigl(\operatorname{End}_{\mathbb{Z}_pU}(\mathbb{Z}_p[\zeta])\bigr)^m \times \bigl(\operatorname{Hom}_{\mathbb{Z}_pU}(\mathbb{Z}_p[\zeta], \mathbb{Z}_pU)\bigr)^n \\ &\cong (\mathbb{Z}_p[\zeta])^m \times ((1-u)\mathbb{Z}_pU)^n\end{aligned}$$

where the last isomorphism follows upon sending a homomorphism $\varphi$ to $\varphi(1)$. Since

$$\operatorname{End}_{\mathbb{F}_p\Gamma}(\widehat{\Lambda}) \cong (\mathbb{F}_p[\zeta])^m \times ((1-u)\mathbb{F}_pU)^n$$

by a similar argument, the natural homomorphism from $\operatorname{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda})$ to $\operatorname{End}_{\mathbb{F}_p\Gamma}(\widehat{V})$ is surjective (and reduction mod $p$). So $e_0$ lifts to an idempotent $e \in \operatorname{End}_{\mathbb{Z}_pU}(\widehat{\Lambda})$ (see [8, proposition 1.9.4]).

Now set $\Lambda = e\widehat{\Lambda}$. Then $\Lambda/p\Lambda \cong V$, and $\Lambda$ is a $\mathbb{Z}_p\Gamma$-lattice in the $\mathbb{Q}_p\Gamma$-module $M = Q_p \otimes_{\mathbb{Z}_p} \Lambda$.

**(b)** We repeat the proof of (a) but keeping control of the submodule as well as $V$. Set $V_2 = V$ and $V_3 = V_2/V_1$, and set $\widehat{V}_i = \operatorname{Ind}_U^\Gamma(V_i|_U)$ for $i = 1, 2, 3$. We thus have short exact sequences

$$0 \longrightarrow V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3 \longrightarrow 0 \quad \text{and} \quad 0 \longrightarrow \widehat{V}_1 \xrightarrow{\widehat{f}} \widehat{V}_2 \xrightarrow{\widehat{g}} \widehat{V}_3 \longrightarrow 0.$$

Let $\alpha_i\colon \widehat{V}_i \longrightarrow V_i$ be the natural map, and let $\beta_i\colon V_i \longrightarrow \widehat{V}_i$ be the $\mathbb{F}_p\Gamma$-linear splitting of $\alpha_i$ obtained by taking the natural $\mathbb{F}_pU$-linear inclusion and then averaging over cosets of $U$ in $\Gamma$. Thus $\alpha_i \circ \beta_i = \operatorname{Id}_{V_i}$ (upon composing from right to left), while $e_i \overset{\text{def}}{=} \beta_i \circ \alpha_i$ is an idempotent in $\operatorname{End}_{\mathbb{F}_p\Gamma}(\widehat{V}_i)$. All of these commute with the natural homomorphisms $f$, $\widehat{f}$, $g$, and $\widehat{g}$, and so we get a commutative diagram with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \widehat{V}_1 \arrow[r, "\widehat{f}"] \arrow[d, "e_1"'] & \widehat{V}_2 \arrow[r, "\widehat{g}"] \arrow[d, "e_2"'] & \widehat{V}_3 \arrow[r] \arrow[d, "e_3"'] & 0 \\ 0 \arrow[r] & \widehat{V}_1 \arrow[r, "\widehat{f}"] & \widehat{V}_2 \arrow[r, "\widehat{g}"] & \widehat{V}_3 \arrow[r] & 0\,. \end{tikzcd} \tag{1}$$

Now set $\Lambda_1^0 = \mathbb{Z}_p$, $\Lambda_2^0 = \mathbb{Z}_pU$, $\Lambda_3^0 = \mathbb{Z}_p[\zeta]$, and let $\varphi$ and $\psi$ be such that

$$0 \longrightarrow \Lambda_1^0 \xrightarrow{\varphi} \Lambda_2^0 \xrightarrow{\psi} \Lambda_3^0 \longrightarrow 0$$

is a short exact sequence of $\mathbb{Z}_pU$-modules. We identify $V_i|_U = \Lambda_i^0/p\Lambda_i^0$ in such a way that $f$ and $g$ are the reductions modulo $p$ of $\varphi$ and $\psi$, respectively. Set $\widehat{\Lambda}_i = \operatorname{Ind}_U^\Gamma\left(\Lambda_i^0\right)$, so that $\widehat{V}_i = \widehat{\Lambda}_i/p\widehat{\Lambda}_i$ as $\mathbb{F}_p\Gamma$-modules, and let $\widehat{\varphi}$ and $\widehat{\psi}$ be the

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

homomorphisms induced by $\varphi$ and $\psi$. We claim that the $e_i$ can be lifted to elements $\varepsilon_i \in \mathrm{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda}_i)$ that make the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & \widehat{\Lambda}_1 \arrow[r, "\widehat{\varphi}"] \arrow[d, "\varepsilon_1"'] & \widehat{\Lambda}_2 \arrow[r, "\widehat{\psi}"] \arrow[d, "\varepsilon_2"'] & \widehat{\Lambda}_3 \arrow[r] \arrow[d, "\varepsilon_3"'] & 0 \\
0 \arrow[r] & \widehat{\Lambda}_1 \arrow[r, "\widehat{\varphi}"] & \widehat{\Lambda}_2 \arrow[r, "\widehat{\psi}"] & \widehat{\Lambda}_3 \arrow[r] & 0\,.
\end{tikzcd} \tag{2}$$

To see this, we identify

$$\mathrm{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda}_i) \cong \mathrm{Hom}_{\mathbb{Z}_pU}\left(\Lambda_i^0, \left(\mathrm{Ind}_U^\Gamma\left(\Lambda_i^0\right)\right)|_U\right),$$

where by the Mackey double coset formula, for some indexing sets $J$ and $K$ independent of $i \in \{1,2,3\}$,

$$\left(\mathrm{Ind}_U^\Gamma\left(\Lambda_i^0\right)\right)|_U \cong \bigoplus_{j\in J}\Lambda_i^0 \oplus \bigoplus_{k\in K}(\mathbb{Z}_pU \otimes_{\mathbb{Z}_p} \Lambda_i^0).$$

Fix $\varepsilon_2 \in \mathrm{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda}_2)$, and set $\varepsilon_2(1) = \big((u_j)_{j\in J}, (v_k)_{k\in K}\big)$ with respect to the above decomposition (and where 1 is the identity in $\Lambda_2^0 = \mathbb{Z}_pU$). Then $\varepsilon_2$ induces endomorphisms $\varepsilon_1$ and $\varepsilon_3$ such that (2) commutes if and only if $\sum_{i=0}^{p-1} u^i(v_k) \in \mathrm{Ker}(\widehat{\psi})$ for each $k \in K$. Note that $\widehat{\psi}$, after restriction to the summands for some $k \in K$, is a surjection of one free $\mathbb{Z}_pU$-module onto another. Hence $\varepsilon_2$ can always be chosen (as a lifting of $e_2$) to induce $\varepsilon_1$ and $\varepsilon_3$ since the above condition holds modulo $p$ by the commutativity of (1).

Since $\varepsilon_i$ is a lifting of the idempotent $e_i$, we have $\varepsilon_i^2 \equiv \varepsilon_i \pmod p$. Hence $(\varepsilon_i)^{2p^k} \equiv (\varepsilon_i)^{p^k} \pmod{p^{k+1}}$ for each $k \geqslant 1$. Upon replacing $\varepsilon_i$ by the limit of the $(\varepsilon_i)^{p^k}$, we can arrange that each $\varepsilon_i$ is an idempotent in $\mathrm{End}_{\mathbb{Z}_p\Gamma}(\widehat{\Lambda}_i)$ (and that the above diagram still commutes). Set $\Lambda = \varepsilon_2\widehat{\Lambda}_2$ and $M = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \Lambda$. Thus $M$ is a $\mathbb{Q}_p\Gamma$-module with a 1-dimensional submodule, and has a $\mathbb{Z}_p\Gamma$-lattice $\Lambda$ such that $\Lambda/p\Lambda \cong V$. □

We now turn to questions of uniqueness, looking first at the finite case. When $R$ is a ring and $M$ is an $R$-module, we let $\mathrm{Ann}_R(x)$ denote the annihilator of an element $x \in M$.

Proposition 3.9. *Fix an odd prime $p$, a finite group $\Gamma \in \mathscr{G}_p$, and $U \in \mathrm{Syl}_p(\Gamma)$. Let $A_1$ and $A_2$ be finite $\mathbb{Z}_p\Gamma$-modules, and assume that $\left|C_{A_i}(U) \cap [U, A_i]\right| = p$ for $i = 1,2$. Set $\sigma = \sum_{u\in U} u \in \mathbb{Z}_pU$.*

*Assume that there is a $\mathbb{Z}_pU$-linear isomorphism $\varphi\colon A_1 \longrightarrow A_2$ whose reduction modulo $p$ is $\mathbb{F}_p\Gamma$-linear. Then $A_1 \cong A_2$ as $\mathbb{Z}_p\Gamma$-modules. In particular, this happens if $A_1/pA_1 \cong A_2/pA_2$ and either*

(a) *$A_1$ and $A_2$ are homocyclic of the same exponent and $\sigma{\cdot}A_i \nleq pA_i$ for $i = 1,2$; or*

(b) *there are elements* $\mathbf{a}_1\in A_1$ *and* $\mathbf{a}_2\in A_2$ *such that* $A_1=\mathbb{Z}_pU\cdot\mathbf{a}_1$, $A_2=\mathbb{Z}_pU\cdot\mathbf{a}_2$, *and* $\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_1)=\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_2)$.

*Proof.* Set $\overline{A}_i=A_i/pA_i$ for $i=1,2$. For each $X\leqslant A_i$ and $g\in A_i$, set $\overline{X}=(X+pA_i)/pA_i$ and $\bar g=g+pA_i$. Set $Z_i=C_{A_i}(U)$ and $S_i'=[U,A_i]$. By assumption, $|Z_i\cap S_i'|=p$, and hence $|A_i/(Z_i+S_i')|=p$ by lemma 3.7(c).

Assume $\varphi\colon A_1\longrightarrow A_2$ is a $\mathbb{Z}_pU$-linear isomorphism whose reduction $\bar\varphi\colon\overline{A}_1\longrightarrow\overline{A}_2$ modulo $p$ is $\mathbb{F}_p\varGamma$-linear. Let $g_1,\dots,g_k$ be a set of representatives for the left cosets $gU$ in $\varGamma$ (where $k=|\varGamma/U|$ is prime to $p$), and define $\psi\colon A_1\longrightarrow A_2$ by setting $\psi(\lambda)=\frac{1}{k}\bigl(\sum_{j=1}^k g_j\varphi(g_j^{-1}\lambda)\bigr)$. Then $\psi$ is $\mathbb{Z}_p\varGamma$-linear, its reduction modulo $p$ is equal to $\bar\varphi$ since $\bar\varphi$ is $\mathbb{F}_p\varGamma$-linear, it is surjective since the reduction mod $p$ is surjective, and is an isomorphism since $|A_1|=|A_2|$.

It remains to prove that each of (a) and (b) implies the existence of the homomorphism $\varphi$. Fix an $\mathbb{F}_p\varGamma$-linear isomorphism $\bar\varphi\colon\overline{A}_1\longrightarrow\overline{A}_2$.

**(a)** Assume $A_1$ and $A_2$ are homocyclic of the same exponent $p^k$, and for $i=1,2$, $\sigma\cdot A_i\not\leqslant pA_i$. Choose $\mathbf{a}_1\in A_1$ such that $\sigma\cdot\mathbf{a}_1\notin pA_1$, and let $\mathbf{a}_2\in A_2$ be such that $\bar\varphi(\bar{\mathbf{a}}_1)=\bar{\mathbf{a}}_2$. Thus for $i=1,2$, $\overline{\sigma\cdot\mathbf{a}_i}\neq 0$, and so $\{u(\bar{\mathbf{a}}_i)\,|\,u\in U\}$ is a basis for $\mathbb{F}_pU\cdot\bar{\mathbf{a}}_i$, and $\mathrm{Ann}_{\mathbb{F}_pU}(\bar{\mathbf{a}}_i)=0$. Note that $\mathbf{a}_i\notin Z_i+S_i'$, since $\sigma\cdot Z_i\leqslant pZ_i$ and $\sigma\cdot S_i'=0$.

We claim that each element of $C_{\overline{A}_i}(U)$ lifts to an element of $C_{A_i}(U)$; that is,

$$C_{\overline{A}_i}(U)=\overline{Z}_i. \tag{1}$$

To see this, let $g\in A_i$ be such that $\bar g\in C_{\overline{A}_i}(U)$. By lemma 3.7(d), $g=\xi\cdot\mathbf{a}_i+z$ for some $\xi\in\mathbb{Z}_pU$ and $z\in Z_i$. Then $\overline{\xi\cdot\mathbf{a}_i}$ is fixed by $U$ since $\bar g$ is, and $C_{\overline{\mathbb{Z}_pU\cdot\mathbf{a}_i}}(U)=\langle\overline{\sigma\cdot\mathbf{a}_i}\rangle$ since $\mathrm{Ann}_{\mathbb{F}_pU}(\bar{\mathbf{a}}_i)=0$. Hence there is $k\in\mathbb{Z}$ such that $\overline{k\sigma\cdot\mathbf{a}_i}=\overline{\xi\cdot\mathbf{a}_i}$; and $\bar g=\overline{k\sigma\cdot\mathbf{a}_i+z}$ where $k\sigma\cdot\mathbf{a}_i+z\in Z_i$. This proves (1).

Set $m=\mathrm{rk}(A_1)-p=\mathrm{rk}(A_2)-p$ (possibly $m=0$). By (1), we can choose elements $x_1,\dots,x_m\in Z_1$ such that $\overline{A}_1=\mathbb{F}_pU\cdot\bar{\mathbf{a}}_1\oplus\langle\bar x_1,\dots,\bar x_m\rangle$. By (1) again, there are elements $y_1,\dots,y_m\in Z_2$ such that $\bar\varphi(\bar x_i)=\bar y_i$ for each $i$. Then

$$\{u(\bar{\mathbf{a}}_1)\,|\,u\in U\}\cup\{\bar x_1,\dots,\bar x_m\}\quad\text{and}\quad\{u(\bar{\mathbf{a}}_2)\,|\,u\in U\}\cup\{\bar y_1,\dots,\bar y_m\}$$

are bases for $\overline{A}_1$ and $\overline{A}_2$, respectively, and $\bar\varphi$ sends the first basis to the second. Since $A_1$ and $A_2$ are both homocyclic of exponent $p^k$, the sets $\{u(\mathbf{a}_1),x_1,\dots,x_m\,|\,u\in U\}$ and $\{u(\mathbf{a}_2),y_1,\dots,y_m\,|\,u\in U\}$ are bases for $A_1$ and $A_2$, respectively, as $\mathbb{Z}/p^k$-modules. Thus $\bar\varphi$ lifts to a $\mathbb{Z}_pU$-linear isomorphism $\varphi\colon A_1\longrightarrow A_2$, defined by setting $\varphi(u(\mathbf{a}_1))=u(\mathbf{a}_2)$ for $u\in U$ and $\varphi(x_i)=y_i$ for each $i$.

**(b)** Let $\mathbf{a}_i\in A_i$ (for $i=1,2$) be such that $\mathbb{Z}_pU\cdot\mathbf{a}_i=A_i$ and $\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_1)=\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_2)$. Let $\xi\in\mathbb{Z}_pU$ be such that $\bar\varphi(\bar{\mathbf{a}}_1)=\overline{\xi\cdot\mathbf{a}_2}$. Thus $\overline{\xi\cdot\mathbf{a}_2}$ generates $\overline{A}_2$ as an $\mathbb{F}_pU$-module, and since $(1-u)A_2\leqslant S_2'$ for $1\neq u\in U$, $\xi$ is not in the ideal $(1-u)\mathbb{Z}_pU+p\mathbb{Z}_pU$ of index $p$ in $\mathbb{Z}_pU$. Since this is the unique maximal ideal in $\mathbb{Z}_pU$, $\xi$ is invertible, and we can replace $\mathbf{a}_2$ by $\xi\cdot\mathbf{a}_2$ without changing $\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_2)$.

Let $\varphi\colon A_1\longrightarrow A_2$ be the unique $\mathbb{Z}_pU$-linear homomorphism such that $\varphi(\mathbf{a}_1)=\mathbf{a}_2$. Its reduction modulo $p$ is $\bar\varphi$, since $\bar\varphi(\bar{\mathbf{a}}_1)=\bar{\mathbf{a}}_2$ and $\bar\varphi$ is $\mathbb{F}_pU$-linear. □

It remains to prove the analogous uniqueness result for discrete $p$-tori.

LEMMA 3.10. *Fix an odd prime $p$, a finite group $\mathit{\Gamma} \in \mathscr{G}_p$, and $U \in \mathrm{Syl}_p(\mathit{\Gamma})$. Let $A_1$ and $A_2$ be discrete, $\mathit{\Gamma}$-$p$-tori, and assume that*

(i) *$\Omega_1(A_1)$ and $\Omega_1(A_2)$ are faithful, minimally active, and indecomposable as $\mathbb{F}_p\mathit{\Gamma}$-modules; and*

(ii) *$\Omega_1(A_1) \cong \Omega_1(A_2)$ as $\mathbb{F}_p\mathit{\Gamma}$-modules.*

*Then $A_1 \cong A_2$ as $\mathbb{Z}_p\mathit{\Gamma}$-modules.*

*Proof.* By lemma 3.7(b), we also have that

(a) $[U, A_i] \cap C_{A_i}(U)$ has order $p$ for $i = 1, 2$.

Assume, for each $k \geqslant 1$, that $\Omega_k(A_1) \cong \Omega_k(A_2)$ as $\mathbb{Z}_p\mathit{\Gamma}$-modules, and let $X_k$ be the set of $\mathbb{Z}_p\mathit{\Gamma}$-linear isomorphisms $\Omega_k(A_1) \xrightarrow{\cong} \Omega_k(A_2)$. Then $X_k$ is finite since the $\Omega_k(A_i)$ are finite, $X_k \neq \varnothing$ by assumption, and if $k \geqslant 2$, restriction to $\Omega_{k-1}(A_i)$ defines a map $X_k \longrightarrow X_{k-1}$. So the inverse limit of the $X_k$ is nonempty, and each element in the inverse limit determines a $\mathbb{Z}_p\mathit{\Gamma}$-linear isomorphism $A_1 \cong A_2$.

It remains to show that $\Omega_k(A_1) \cong \Omega_k(A_2)$ for each $k$. Since $\Omega_k(A_i)/p\Omega_k(A_i) \cong \Omega_1(A_i)$ as $\mathbb{F}_p\mathit{\Gamma}$-modules (multiplication by $p^{k-1}$ defines an isomorphism), we have $\Omega_k(A_1)/p\Omega_k(A_1) \cong \Omega_k(A_2)/p\Omega_k(A_2)$, and both are faithful, minimally active, and indecomposable.

Set $\sigma = \sum_{u \in U} u \in \mathbb{Z}_pU$, as usual. If $\mathrm{rk}(A_i) \geqslant p$, then by lemma 3.3(a,b), $\sigma{\cdot}\Omega_k(A_i) \nleq p\Omega_k(A_i)$. Since $\Omega_k(A_1)$ and $\Omega_k(A_2)$ are both homocyclic of exponent $p^k$, they are isomorphic as $\mathbb{Z}_p\mathit{\Gamma}$-modules by proposition 3.9(a).

If $\mathrm{rk}(A_i) = p - 1$ for $i = 1, 2$, then by proposition A.4, $A_i \cong (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda_i$ for some $(p-1)$-dimensional $\mathbb{Z}_p\mathit{\Gamma}$-lattice $\Lambda_i$. Since $\mathit{\Gamma}$ acts faithfully on the lattices, $\Lambda_1 \cong \Lambda_2 \cong \mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_pU$-modules by lemma A.5(a,c) (where $\zeta$ is a primitive $p$-th root of unity). Hence for $i = 1, 2$, $A_i \cong \mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$, and $\Omega_k(A_i) \cong \mathbb{Z}_p[\zeta]/p^k\mathbb{Z}_p[\zeta]$, as $\mathbb{Z}_pU$-modules. So there is $\mathbf{a}_i \in \Omega_k(A_i)$ such that $\mathbb{Z}_pU{\cdot}\mathbf{a}_i = \Omega_k(A_i)$ and $\mathrm{Ann}_{\mathbb{Z}_pU}(\mathbf{a}_i)$ is the ideal generated by $p^k$ and $\sigma$. Proposition 3.9(b) now applies to conclude that $\Omega_k(A_1) \cong \Omega_k(A_2)$ as $\mathbb{Z}_p\mathit{\Gamma}$-modules. □

## 4. Reduced fusion systems over finite nonabelian *p*-groups with index *p* abelian subgroup (*p* odd)

Throughout this section, $p$ is an odd prime, and $A$ is finite. As noted in the introduction, the corresponding question for finite 2-groups was answered in [**6**, proposition 5.2(a)].

LEMMA 4.1 ([**15**, lemma 2.2(d,e,f)]). *Assume the notation and hypotheses of 2.1, and also that $p$ is odd and $|A| < \infty$. Set $A_0 = ZS'$. Then the following hold.*

(a) *If $A \ntrianglelefteq \mathcal{F}$, then there are elements $\mathbf{x} \in S{\smallsetminus}A$ and $\mathbf{a} \in A{\smallsetminus}A_0$ such that $A_0\langle\mathbf{x}\rangle$ and $S'\langle\mathbf{a}\rangle$ are normalized by $\mathrm{Aut}_{\mathcal{F}}(S)$. If some element of $S{\smallsetminus}A$ has order $p$, then we can choose $\mathbf{x}$ to have order $p$.*

(b) *For each $P \in \mathbf{E}_{\mathcal{F}}$ and each $\alpha \in N_{\mathrm{Aut}_{\mathcal{F}}(P)}(\mathrm{Aut}_S(P))$, $\alpha$ extends to some $\bar{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(S)$.*

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

(c) *For each $x \in S \smallsetminus A$ and each $g \in A_0$, $Z\langle x\rangle$ is $S$-conjugate to $Z\langle gx\rangle$, and $Z_2\langle x\rangle$ is $S$-conjugate to $Z_2\langle gx\rangle$.*

We now fix some more notation, based on lemma 4.1.

Notation 4.2. *Assume notation 2.1. Assume also that $p$ is odd, $S$ is finite, and $A \ntrianglelefteq \mathcal{F}$, and hence that $|Z_0| = |A/ZS'| = p$ by lemma 2.4. Fix $\mathbf{a} \in A \smallsetminus ZS'$ and $\mathbf{x} \in S \smallsetminus A$, chosen such that $ZS'\langle \mathbf{x}\rangle$ and $S'\langle \mathbf{a}\rangle$ are each normalized by $\mathrm{Aut}_{\mathcal{F}}(S)$, and such that $\mathbf{x}^p = 1$ if any element of $S \smallsetminus A$ has order $p$ (lemma 4.1(a)). For each $i = 0, 1, \ldots, p-1$, define*

$$H_i = Z\langle \mathbf{x}\mathbf{a}^i\rangle \in \mathcal{H} \quad \text{and} \quad B_i = Z_2\langle \mathbf{x}\mathbf{a}^i\rangle \in \mathcal{B}\,.$$

*Let $\mathcal{H}_i$ and $\mathcal{B}_i$ denote the $S$-conjugacy classes of $H_i$ and $B_i$, respectively, and set*

$$\mathcal{H}_* = \mathcal{H}_1 \cup \cdots \cup \mathcal{H}_{p-1} \quad \text{and} \quad \mathcal{B}_* = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{p-1}.$$

*For each $P \leqslant S$, set*

$$\mathrm{Aut}_{\mathcal{F}}^{(P)}(S) = \bigl\{\alpha \in \mathrm{Aut}_{\mathcal{F}}(S) \bigm| \alpha(P) = P,\ \alpha|_P \in O^{p'}(\mathrm{Aut}_{\mathcal{F}}(P))\bigr\}.$$

When $|Z_0| = p$, then by lemma 4.1(c), $\mathcal{H} = \mathcal{H}_0 \cup \mathcal{H}_*$ and $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_*$. Note that for $x, x' \in S \smallsetminus A$, $Z\langle x\rangle$ is $S$-conjugate to $Z\langle x'\rangle$ or $Z_2\langle x\rangle$ is $S$-conjugate to $Z_2\langle x'\rangle$ only if $x'x^{-1} \in ZS'$. So in fact, each of the sets $\mathcal{H}$ and $\mathcal{B}$ is a union of $p$ distinct $S$-conjugacy classes: the classes $\mathcal{H}_i$ and $\mathcal{B}_i$ for $0 \leqslant i \leqslant p-1$.

Lemma 4.3 ([**15**, lemma 2.5(a,b)]). *Let $p$ be an odd prime, let $S$ be a finite nonabelian $p$-group with a unique abelian subgroup $A \trianglelefteq S$ of index $p$, and let $\mathcal{F}$ be a saturated fusion system over $S$ such that $A \ntrianglelefteq \mathcal{F}$. We use the conventions of notations 2.1 and 2.9, set $A_0 = ZS'$, and let $m \geqslant 3$ be such that $|A/Z| = p^{m-1}$. Then the following hold.*

(a) *$\widehat{\mu}|_{\mathrm{Out}_{\mathcal{F}}^{\vee}(S)}$ is injective.*

(b) *Fix $\alpha \in \mathrm{Aut}(S)$, set $(r, s) = \mu(\alpha)$, and let $t$ be such that $\alpha(g) \in g^t A_0$ for each $g \in A \smallsetminus A_0$. Then $s \equiv tr^{m-1}$ (mod $p$).*

Lemma 4.4 ([**15**, lemma 2.6(a)]). *Let $p$ be an odd prime, let $S$ be a finite nonabelian $p$-group with a unique abelian subgroup $A \trianglelefteq S$ of index $p$, and let $\mathcal{F}$ be a saturated fusion system over $S$. We use the notation of notations 2.1 and 2.9. Let $m$ be such that $|A/Z| = p^{m-1}$. Fix $P \in \mathcal{H} \cup \mathcal{B}$, and set*

$$H_P = N_{\mathrm{Aut}_{\mathcal{F}}(S)}(P), \quad \widehat{H}_P = \bigl\{\alpha|_P \bigm| \alpha \in H_P\bigr\}, \quad \text{and} \quad t = \begin{cases} -1 & \text{if } P \in \mathcal{H} \\ 0 & \text{if } P \in \mathcal{B}. \end{cases}$$

*If $P \in \mathbf{E}_{\mathcal{F}}$, then $\mathrm{Aut}_{\mathcal{F}}^{(P)}(S) \leqslant \mathrm{Aut}_{\mathcal{F}}^{\vee}(S)$ and $\mu\left(\mathrm{Aut}_{\mathcal{F}}^{(P)}(S)\right) = \Delta_t$. If $P \in \mathcal{H}_*$ or $P \in \mathcal{B}_*$, then $m \equiv t$ (mod $p-1$).*

Theorem 4.5 ([**15**, theorem 2.8]). *Fix an odd prime $p$, and a finite nonabelian $p$-group $S$ which contains a unique abelian subgroup $A \trianglelefteq S$ of index $p$. Let $\mathcal{F}$ be a*

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Table 4.1. *Summary of the cases in theorem 4.5.*

| | $\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}}(A))$ | $G = O^{p'}(G)X$ | $m \pmod{p-1}$ | $\sigma{\cdot}A$ | $\mathbf{E}_0$ |
|---|---|---|---|---|---|
| (i) | $\Delta$ | $X = \mathrm{Aut}^\vee_{\mathcal{F}}(A)$ | $\equiv 0$ | $\leqslant \mathrm{Fr}(Z)$ | $\mathcal{H}_0 \cup \mathcal{B}_*$ |
| (ii) | $\Delta$ | $X = \mathrm{Aut}^\vee_{\mathcal{F}}(A)$ | $\equiv -1$ | $\leqslant \mathrm{Fr}(Z)$ | $\mathcal{B}_0 \cup \mathcal{H}_*$ |
| (iii′) | $\geqslant \Delta_{-1}$ | $X = \mu_A^{-1}(\Delta_{-1})$ | $\equiv -1$ | $\leqslant \mathrm{Fr}(Z)$ | $\bigcup_{i\in I} \mathcal{H}_i$ |
| (iii″) | | | – | – | $\mathcal{H}_0$ |
| (iv′) | $\geqslant \Delta_0$ | $X = \mu_A^{-1}(\Delta_0)$ | $\equiv 0$ | $\leqslant \mathrm{Fr}(Z)$ | $\bigcup_{i\in I} \mathcal{B}_i$ |
| (iv″) | | $Z_0$ not $G$-invariant | – | – | $\mathcal{B}_0$ |

*reduced fusion system over $S$ for which $A$ is $\mathcal{F}$-essential. We use the notation of 2.1, 2.9, and 4.2, and also set $A_0 = ZS'$, $\mathbf{E}_0 = \mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$, and $G = \mathrm{Aut}_{\mathcal{F}}(A)$. Thus $\mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$. Let $m \geqslant 3$ be such that $|A/Z| = p^{m-1}$. Then the following hold:*

(a) *$Z_0 = C_A(\mathbf{U}) \cap [\mathbf{U}, A]$ has order $p$, and hence $A_0 = C_A(\mathbf{U})[\mathbf{U}, A]$ has index $p$ in $A$.*

(b) *There are no nontrivial $G$-invariant subgroups of $Z = C_A(\mathbf{U})$, aside (possibly) from $Z_0$.*

(c) *$[G, A] = A$.*

(d) *One of the conditions (i)–(iv) holds, described in table 4.1, where $\sigma = \sum_{u\in\mathbf{U}} u \in \mathbb{Z}_p\mathbf{U}$.*

*Conversely, for each $G$, $A$, $\mathbf{U} \in \mathrm{Syl}_p(G)$, and $\mathbf{E}_0 \subseteq \mathcal{H} \cup \mathcal{B}$ which satisfy conditions (a)–(d), where $|\mathbf{U}| = p$ and $\mathbf{U} \ntrianglelefteq G$, there is a simple fusion system $\mathcal{F}$ over $A \rtimes \mathbf{U}$ with $\mathrm{Aut}_{\mathcal{F}}(A) = G$ and $\mathbf{E}_{\mathcal{F}} = \mathbf{E}_0 \cup \{A\}$, unique up to isomorphism. When $A$ is not elementary abelian, all such fusion systems are exotic, except for the fusion systems of the simple groups listed in table 4.2.*

*Such a fusion system $\mathcal{F}$ has a proper strongly closed subgroup if and only if $A_0 = C_A(\mathbf{U})[\mathbf{U}, A]$ is $G$-invariant, and $\mathbf{E}_0 = \mathcal{H}_i$ or $\mathcal{B}_i$ for some $i$, in which case $A_0H_i = A_0B_i$ is strongly closed.*

We now look for a more precise description of the group $A$ when it is finite but not elementary abelian. The following notation will be useful when describing more precisely, the elements and subgroups of $A$.

Notation 4.6. *Assume notations 2.1 and 4.2, and set $\mathbf{u} = c_{\mathbf{x}} \in \mathbf{U} = \mathrm{Aut}_S(A)$. Set $\sigma = 1 + \mathbf{u} + \mathbf{u}^2 + \cdots + \mathbf{u}^{p-1} \in \mathbb{Z}_p\mathbf{U}$. Regard $A$ as a $\mathbb{Z}_p\mathbf{U}$-module, and define*

$$\Psi\colon \mathbb{Z}_p\mathbf{U} \longrightarrow A$$

*by setting $\Psi(\xi) = \xi{\cdot}\mathbf{a}$. Thus $\Psi\bigl(\sum_{i=0}^{p-1} n_i\mathbf{u}^i\bigr) = \prod_{i=0}^{p-1} \mathbf{u}^i(\mathbf{a})^{n_i}$ for $n_i \in \mathbb{Z}_p$.*

Table 4.2. *In this table, $e$ is such that $p^e$ is the exponent of $A$, and we restrict to the cases where $e \geqslant 2$. In all cases except when $\Gamma \cong PSL_p(q)$, $A$ is homocyclic*

| $\Gamma$ | $p$ | conditions | $\mathrm{rk}(A)$ | $e$ | $m$ | $G = \mathrm{Aut}_\Gamma(A)$ | $\mathbf{E}_0$ |
|---|---|---|---|---|---|---|---|
| $PSL_p(q)$ | $p$ | $p^2 \mid (q-1),\ p>3$ | $p-1$ | $v_p(q-1)$ | $e(p-1)-1$ | $\Sigma_p$ | $\mathcal{H}_0 \cup \mathcal{H}_*$ |
| $PSL_n(q)$ | $p$ | $p^2 \mid (q-1),\ p<n<2p$ | $n-1$ | $v_p(q-1)$ | $e(p-1)+1$ | $\Sigma_n$ | $\mathcal{B}_0$ |
| $P\Omega_{2n}^+(q)$ | $p$ | $p^2 \mid (q-1),\ p \leqslant n<2p$ | $n$ | $v_p(q-1)$ | $e(p-1)+1$ | $C_2^{n-1} \rtimes \Sigma_n$ | $\mathcal{B}_0$ |
| ${}^2F_4(q)$ | 3 | ——— | 2 | $v_3(q+1)$ | $2e$ | $GL_2(3)$ | $\mathcal{B}_0 \cup \mathcal{B}_*$ |
| $E_n(q)$ | 5 | $n=6,7,\ p^2 \mid (q-1)$ | $n$ | $v_5(q-1)$ | $4e+1$ | $W(E_n)$ | $\mathcal{B}_0$ |
| $E_n(q)$ | 7 | $n=7,8,\ p^2 \mid (q-1)$ | $n$ | $v_7(q-1)$ | $6e+1$ | $W(E_n)$ | $\mathcal{B}_0$ |
| $E_8(q)$ | 5 | $v_5(q^2+1) \geqslant 2$ | 4 | $v_5(q^4-1)$ | $4e$ | $(4 \circ 2^{1+4}).\Sigma_6$ | $\mathcal{B}_0 \cup \mathcal{B}_*$ |

*Set $\zeta = e^{2\pi i/p}$, $R = \mathbb{Z}_p[\zeta]$, and $\mathfrak{p} = (1-\zeta)R$. Thus $\mathfrak{p}$ is the unique maximal ideal in $R$. We identify $R = \mathbb{Z}_p\mathbf{U}/\sigma\mathbb{Z}_p\mathbf{U}$, by sending $\zeta \in R$ to the class of $\mathbf{u}$ modulo $\langle\sigma\rangle$.*

The basic properties of $\Psi$, and the role of $\Psi(\sigma)$, are described in the following lemma. Recall that $\mho^k(P) = \langle g^{p^k} \mid g \in P\rangle$, when $P$ is a $p$-group and $k \geqslant 1$.

Lemma 4.7. *Assume notations 2.1 and 4.6, where $A \in \mathbf{E}_\mathcal{F}$, and $A \ntrianglelefteq \mathcal{F}$ is finite and not elementary abelian. Let $m$ be such that $|A/Z| = p^{m-1}$. Then*

(a) $\mathrm{Im}(\Psi) \cap Z = Z_0\langle\Psi(\sigma)\rangle$;

(b) $\Psi$ *induces an isomorphism $A/Z \cong R/\mathfrak{p}^{m-1}$ via the identification $R = \mathbb{Z}_p\mathbf{U}/\langle\sigma\rangle$; and*

(c) $\Psi((1-\mathbf{u})^m) = 1$ *and* $Z_0 = \langle\Psi((\mathbf{u}-1)^{m-1})\rangle$.

*Furthermore, the following all hold.*

(d) *The homomorphism $\Psi$ is surjective if and only if $\mathrm{rk}(A) \leqslant p$, if and only if $Z$ is cyclic. If $\Psi(\sigma) \in \mathrm{Fr}(A)$, then $\mathrm{rk}(A) < p$ and $\Psi$ is surjective.*

(e) *Either*
- $\Psi(\sigma) = 1$, *in which case $\mathrm{rk}(A) = p-1$, $Z = Z_0$, and $\Psi$ induces an isomorphism $A \cong R/\mathfrak{p}^m$ via the identification $R = \mathbb{Z}_p\mathbf{U}/\langle\sigma\rangle$; or*
- $\Psi(\sigma) \notin \mathrm{Fr}(Z)$, *in which case $\mathbf{E}_\mathcal{F} \subseteq \{A\} \cup \mathcal{H}_0$ or $\mathbf{E}_\mathcal{F} \subseteq \{A\} \cup \mathcal{B}_0$.*

(f) *If $\Psi(\sigma) \neq 1$ and $\Psi(\sigma) \in Z_0$, then $m \equiv 1 \pmod{p-1}$. If $\Psi(\sigma) \notin Z_0$, then $\mu(\mathrm{Aut}_\mathcal{F}^\vee(S)) = \Delta_{m-1}$; and either $m \equiv 1 \pmod{p-1}$ and $\mathbf{E}_\mathcal{F} \smallsetminus \{A\} = \mathcal{B}_0$, or $m \equiv 0 \pmod{p-1}$ and $\mathbf{E}_\mathcal{F} \smallsetminus \{A\} = \mathcal{H}_0$.*

(g) *If $\Psi$ is not surjective, then $A$ is homocyclic.*

*Proof.* Set $\bar{A} = A/\mathrm{Fr}(A)$ for short. For $B \leqslant A$ or $g \in A$, let $\bar{B} \leqslant \bar{A}$ or $\bar{g} \in \bar{A}$ denote their images in $\bar{A}$ under projection. Let $\bar{\Psi}\colon \mathbb{Z}_p\mathbf{U} \longrightarrow \bar{A}$ be the composite of $\Psi$ followed by projection to $\bar{A}$.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

indent**(a)** Since $(1-\mathbf{u})\mathbb{Z}_p\mathbf{U}+\sigma\mathbb{Z}$ has index $p$ in $\mathbb{Z}_p\mathbf{U}$,

$$\mathrm{Im}(\Psi)=\Psi\big((1-\mathbf{u})\mathbb{Z}_p\mathbf{U}\big)\langle\Psi(\sigma)\rangle\langle\Psi(1)\rangle=S'\langle\Psi(\sigma)\rangle\langle\mathbf{a}\rangle,$$

where $\mathbf{a}^p\in S'\langle\Psi(\sigma)\rangle$. Since $\mathbf{a}\notin Z$ and $\Psi(\sigma)\in Z$, we have

$$\mathrm{Im}(\Psi)\cap Z=C_{\mathrm{Im}(\Psi)}(\mathbf{U})=C_{S'\langle\Psi(\sigma)\rangle}(\mathbf{U})=(S'\cap Z){\cdot}\langle\Psi(\sigma)\rangle=Z_0\langle\Psi(\sigma)\rangle.$$

**(b,c)** Since $\Psi(\sigma)\in Z$, $\Psi$ induces a homomorphism from $\mathbb{Z}_p\mathbf{U}/\langle\sigma\rangle\cong R$ to $A/Z$, which is onto since $A=Z{\cdot}\mathrm{Im}(\Psi)$ by lemma 3.7(d). Since $|A/Z|=p^{m-1}$ by assumption (and since $\mathfrak{p}$ is the unique maximal ideal in $R$ that contains $p$), we have $A/Z\cong R/\mathfrak{p}^{m-1}$. Hence $\Psi((\mathbf{u}-1)^{m-1})\in Z$ and $\Psi((\mathbf{u}-1)^{m-2})\notin Z$, and the latter implies that $\Psi((\mathbf{u}-1)^{m-1})\neq 1$. Thus in all cases (and since $|Z_0|=p$), $\Psi((\mathbf{u}-1)^{m})=1$ and $\langle\Psi((\mathbf{u}-1)^{m-1})\rangle=Z_0$.

**(d)** If $\mathrm{rk}(A)\leqslant p$, then $\mathrm{rk}(\bar{A})\leqslant p$, and by [**15**, proposition 3.7(a)], $\bar{A}|_{\mathbf{U}}$ is indecomposable. Hence $\bar{\Psi}$ is onto in this case, and so $\Psi$ is also onto. Conversely, if $\mathrm{rk}(A)>p=\mathrm{rk}(\mathbb{Z}_p\mathbf{U})$, then $\Psi$ is clearly not surjective.

By lemmas 3.2(b) and 3.3(c), $\Omega_1(Z)=C_{\Omega_1(A)}(\mathbf{U})$ has rank 1 if and only if $\mathrm{rk}(\Omega_1(A))\leqslant p$. Hence $Z$ is cyclic if and only if $\mathrm{rk}(A)\leqslant p$.

If $\Psi(\sigma)\in\mathrm{Fr}(A)$, then $\mathrm{rk}(\mathrm{Im}(\bar{\Psi}))\leqslant p-1$. Hence $\bar{A}$ has no nontrivial Jordan block of rank $p$, and by [**15**, proposition 3.7(a)] again, $\bar{A}$ is indecomposable as an $\mathbb{F}_p\mathbf{U}$-module. So $\mathrm{rk}(A)=\mathrm{rk}(\bar{A})<p$, and $\Psi$ is onto.

**(e)** If $\Psi(\sigma)\in\mathrm{Fr}(Z)\leqslant\mathrm{Fr}(A)$, then $\Psi$ is surjective by (a), so $Z=Z_0\langle\Psi(\sigma)\rangle\leqslant Z_0{\cdot}\mathrm{Fr}(Z)$, and hence $Z=Z_0$ and $\Psi(\sigma)\in\mathrm{Fr}(Z_0)=1$. Thus $\Psi$ factors through a surjection $\Psi^*\colon\mathbb{Z}_p\mathbf{U}/\langle\sigma\rangle\cong R\longrightarrow A$, and induces an isomorphism $A\cong R/I$ for some ideal $I$ in $R$. Since $\mathfrak{p}$ is the only prime ideal in $R$ of $p$-power index (and $|R/\mathfrak{p}|=p$), and since $|A|=p^{m-1}|Z|=p^m$ (recall $Z=Z_0$ by (a)), we have $I=\mathfrak{p}^m$.

Since $\mathbf{E}_{\mathcal{F}}\nsubseteq\{A\}$ (notation 4.6), $\mathbf{x}^p=1$ by notation 4.6 and lemma 4.1. For each $b\in A$,

$$(b\mathbf{x})^p=(b\mathbf{x})^p\mathbf{x}^{-p}=b{\cdot}{}^{\mathbf{x}}b{\cdot}{}^{\mathbf{x}^2}b\cdots{}^{\mathbf{x}^{p-1}}b=\textstyle\prod_{i=0}^{p-1}\mathbf{u}^i(b).$$

If $\Psi(\sigma)=\prod_{i=0}^{p-1}\mathbf{u}^i(\mathbf{a})\notin\mathrm{Fr}(Z)$, then $\prod_{i=0}^{p-1}\mathbf{u}^i(b)\neq 1$ for each $b\in A\smallsetminus ZS'=\bigcup_{i=1}^{p-1}\mathbf{a}^iZS'$. So by lemma 2.5, no member of $\mathcal{H}_*\cup\mathcal{B}_*$ can be essential, and $\mathbf{E}_{\mathcal{F}}\subseteq\{A\}\cup\mathcal{H}_0\cup\mathcal{B}_0$.

**(f)** Assume $A\ntrianglelefteq\mathcal{F}$, and thus $\mathbf{E}_{\mathcal{F}}\nsubseteq\{A\}$. Fix $P\in\mathbf{E}_{\mathcal{F}}\cap(\mathcal{H}\cup\mathcal{B})$ and $\alpha\in\mathrm{Aut}_{\mathcal{F}}^{(P)}(S)\leqslant\mathrm{Aut}_{\mathcal{F}}^{\vee}(S)$ (lemma 4.4).

Set $\mu(\alpha)=(r,s)$, and let $t$ be as in lemma 4.3(b). Thus $s\equiv tr^{m-1}\pmod p$ and $\alpha(\mathbf{a})\equiv\mathbf{a}^t\pmod{ZS'}$, so $\alpha(\mathbf{a})=\Psi(\xi)$ for some $\xi\equiv t\pmod{\langle 1-\mathbf{u},p\rangle}$. Also, $\alpha(\mathbf{x})\in\mathbf{x}^rA$, so $\alpha(\mathbf{u}^i(g))=\mathbf{u}^{ri}(\alpha(g))$ for all $i$ and $g\in A$. Thus

$$\begin{aligned}\alpha(\Psi(\sigma))=\prod_{i=0}^{p-1}\alpha(\mathbf{u}^i(\mathbf{a}))=\prod_{i=0}^{p-1}\mathbf{u}^{ri}(\alpha(\mathbf{a}))=\Psi\left(\sum_{i=0}^{p-1}\xi\mathbf{u}^{ri}\right)\qquad(1)\\ =\Psi(\xi\sigma)\equiv\Psi(t\sigma).\quad\pmod{\Psi(p\sigma)}\end{aligned}$$

In other words, $\alpha(\Psi(\sigma))\equiv\Psi(\sigma)^t\pmod{\langle\Psi(\sigma)^p\rangle}$.

If $\Psi(\sigma) \neq 1$ and $\Psi(\sigma) \in Z_0$, then $t \equiv s \pmod{p}$ by (1) (and by definition of $\mu$), and hence $r^{m-1} \equiv 1 \pmod{p}$. Since this holds for arbitary $\alpha$ and hence for arbitary $r$ prime to $p$ by [**15**, lemma 2.6(a)] and since $P \in \mathbf{E}_{\mathcal{F}} \cap (\mathcal{H} \cup \mathcal{B})$, it follows that $m \equiv 1 \pmod{p-1}$.

Now assume $\Psi(\sigma) \notin Z_0$. By (1) and since $[\alpha, Z] \leqslant Z_0$, we have $t \equiv 1$ and $s \equiv r^{m-1}$. Since this holds for arbitrary $\alpha \in \mathrm{Aut}_{\mathcal{F}}^{(P)}(S)$ (in particular, for arbitrary $r$ prime to $p$), it follows that $\mu\left(\mathrm{Aut}_{\mathcal{F}}^{(P)}(S)\right) \leqslant \mu(\mathrm{Aut}_{\mathcal{F}}^{\vee}(S)) \leqslant \Delta_{m-1}$, with equality by lemma 4.4. So by lemma 4.4, $P \notin \mathcal{H}_* \cup \mathcal{B}_*$, and either $P \in \mathcal{H}_0$ and $\Delta_{m-1} = \Delta_{-1}$ (so $m \equiv 0 \pmod{p-1}$); or $P \in \mathcal{B}_0$ and $\Delta_{m-1} = \Delta_0$ (so $m \equiv 1 \pmod{p-1}$).

**(g)** Assume that $\Psi$ is not onto, and hence by (d) that $\mathrm{rk}(A) \geqslant p+1$ and $\Psi(\sigma) \notin \mathrm{Fr}(A)$. Let $k \geqslant 2$ be such that $A$ has exponent $p^k$. If $A/Z$ has strictly smaller exponent, then $1 \neq \mho^{k-1}(A) \leqslant Z$, and thus $\mho^{k-1}(A)$ is an $\mathbb{F}_pG$-submodule of the minimally active, indecomposable module $\Omega_1(A)$ upon which $\mathbf{U}$ acts trivially. If $\mathrm{rk}(A) = p+1$, this contradicts lemma 3.5, while if $\mathrm{rk}(A) \geqslant p+2$, this is impossible since $\Omega_1(A)$ is simple by [**15**, proposition 3.7(c)]. Thus $A/Z \cong R/\mathfrak{p}^{m-1}$ also has exponent $p^k \geqslant p^2$, and hence $m-1 \geqslant p$. So by (c), and since $(\mathbf{u}-1)^p \in p\mathbb{Z}_p\mathbf{U}$, we have $Z_0 = \langle \Psi((\mathbf{u}-1)^{m-1}) \rangle \leqslant \mathrm{Fr}(A)$.

Now, $\mathrm{rk}(A/Z) = \mathrm{rk}(R/\mathfrak{p}^{m-1}) = p-1$ since $m \geqslant p$, and $\mathrm{rk}(Z) = \mathrm{rk}(C_{\Omega_1(A)}(\mathbf{U})) = \mathrm{rk}(A) - (p-1)$ by lemma 3.3(c). If $Z_0$ is a direct factor in $Z$, then $\mathrm{rk}(Z/Z_0) = \mathrm{rk}(Z) - 1$, so $\mathrm{rk}(A/Z_0) \leqslant \mathrm{rk}(A/Z) + \mathrm{rk}(Z/Z_0) = \mathrm{rk}(A) - 1$. Thus no minimal generating set for $A/Z_0$ lifts to a generating set for $A$, so $Z_0 \nleqslant \mathrm{Fr}(A)$, which contradicts what we just showed. Thus $Z_0$ is not a direct factor in $Z$, and so $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing$ by lemma 2.5(a).

In particular, $m \equiv 1 \pmod{p-1}$ by (f), and hence $A/Z \cong R/\mathfrak{p}^{m-1}$ is homocyclic of rank $p-1$ and exponent $p^k$. Thus $A$ and $A/Z$ are both $\mathbb{Z}/p^k$-modules and $A/Z$ is free, so $A \cong Z \times (A/Z)$ as abelian groups. Since $\mho^{k-1}(A) \cap Z = C_{\mho^{k-1}(A)}(\mathbf{U}) \neq 1$, this shows that $\mathrm{rk}(\mho^{k-1}(A)) \geqslant p$.

If $A$ is not homocyclic, then $\mho^{k-1}(A) < \Omega_1(A)$ is a nontrivial proper $\mathbb{F}_pG$-submodule, where $\Omega_1(A)$ is faithful, minimally active, and indecomposable by lemma 3.2(b). Hence $\mathrm{rk}(A) = \dim(\Omega_1(A)) = p+1$, since $\Omega_1(A)$ is simple if $\dim(\Omega_1(A)) \geqslant p+2$ by [**15**, proposition 3.7(c)]. So $\dim(\mho^{k-1}(A)) \leqslant p-1$ by lemma 3.5. This contradicts what was shown in the last paragraph, and we conclude that $A$ is homocyclic. □

Lemma 4.8. *Let $p$ be an odd prime, let $\mathbf{U}$ be a group of order $p$, and set $\sigma = \sum_{u \in \mathbf{U}} u \in \mathbb{Z}\mathbf{U}$. Then for each $1 \neq u \in \mathbf{U}$ and each $k \geqslant 1$,*

$$(u-1)^{k(p-1)} \equiv (-1)^{k-1}(p^{k-1}\sigma - p^k) \pmod{p^k(u-1)\mathbb{Z}\mathbf{U}}.$$

*Proof.* Since $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for each $0 \leqslant k \leqslant p-1$, we have $(u-1)^{p-1} \equiv \sigma \pmod{p\mathbb{Z}\mathbf{U}}$. Hence

$$(u-1)^{p-1} \equiv \sigma - p \pmod{p(u-1)\mathbb{Z}\mathbf{U}} \tag{1}$$

since they are congruent modulo $p$ and modulo $u-1$. This proves the lemma when $k = 1$.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Table 4.3. *Summary of the cases in proposition 4.9.*

| Case | (a) | (b) | (c) |
|---|---|---|---|
| $\Psi(\sigma)$ | $\Psi(\sigma)=1$ | $\Psi(\sigma)\notin \mathrm{Fr}(Z)$ | |
| $A$ homocyclic? | yes if $(p-1)\mid m$<br>no if $(p-1)\nmid m$ | yes | no |
| $\Psi$ onto? | yes | yes if $\mathrm{rk}(A)=p$<br>no if $\mathrm{rk}(A)>p$ | yes |
| $\mathrm{rk}(A)$ | $p-1$ | $r\geqslant p$ | $p-1$ |
| $\mathrm{Ker}(\Psi)$ | $\langle(\mathbf{u}-1)^m,\sigma\rangle$ | $p^k\mathbb{Z}_p\mathbf{U}$ | $\langle p^k,p^{k-1}-\ell\sigma\rangle\ \ (p\nmid\ell)$ |
| $A$ | $\cong R/\mathfrak{p}^m$ | $\cong (C_{p^k})^r$ | $\cong (C_{p^{k-1}})^{p-2}\times C_{p^k}$ |
| $Z$ | $=Z_0$ | $\cong (C_{p^k})^{r-p+1}$ | $=Z_0$ |
| $Z_0$ | $\langle\Psi((\mathbf{u}-1)^{m-1})\rangle$ | $\langle\Psi(p^{k-1}\sigma)\rangle$ | $\langle\Psi(p^{k-1})\rangle=\langle\Psi(\sigma)\rangle$ |
| $m$ | | $k(p-1)+1$ | $(k-1)(p-1)+1$ |
| $\mathbf{E}_{\mathcal{F}}\smallsetminus\{A\}$ | (see Table 4.1) | $\mathcal{B}_0$ | $\mathcal{H}_0$ |

When $k>1$, (1) together with the congruence for $(u-1)^{(k-1)(p-1)}$ give

$$\begin{aligned}
(u-1)^{k(p-1)} &= (u-1)^{p-1}\cdot(u-1)^{(k-1)(p-1)}\\
&\equiv (u-1)^{p-1}\cdot(-1)^{k-2}(p^{k-2}\sigma-p^{k-1}) \quad \pmod{(u-1)^{p-1}\cdot p^{k-1}(u-1)}\\
&\equiv (\sigma-p)\cdot(-1)^{k-2}(p^{k-2}\sigma-p^{k-1}) \qquad \pmod{p(u-1)(p^{k-2}\sigma-p^{k-1})}\\
&= (-1)^{k-1}(p^{k-1}\sigma-p^k);
\end{aligned}$$

and the congruences hold modulo $p^k(u-1)$ since $p(u-1)$ divides $(u-1)^p$ and $(u-1)\sigma=0$. □

Proposition 4.9. *Assume the notation of 2.1, 2.9, 4.2, and 4.6. Assume also that $A$ is finite and not elementary abelian, that $A\in\mathbf{E}_{\mathcal{F}}$, and that $O_p(\mathcal{F})=1$. Let $m\geqslant 3$ be such that $|A/Z|=p^{m-1}$, and let $k\geqslant 2$ be such that $A$ has exponent $p^k$. Then one of the following holds, as summarized in table 4.3, where $G=\mathrm{Aut}_{\mathcal{F}}(A)$.*

(a) *If $\Psi(\sigma)=1$, then $\Psi$ is onto, $\mathrm{Ker}(\Psi)=\langle\sigma,(\mathbf{u}-1)^m\rangle$, $\mathrm{rk}(A)=p-1$, $Z=Z_0=\langle\Psi((\mathbf{u}-1)^{m-1})\rangle$, and $A\cong R/\mathfrak{p}^m$ as $\mathbb{Z}_p\mathbf{U}$-modules.*

(b) *If $\Psi(\sigma)\notin\mathrm{Fr}(Z)$ and $A$ is homocyclic, then $\mathrm{rk}(A)\geqslant\mathrm{rk}(\mathrm{Im}(\Psi))=p$, $\mathrm{rk}(Z)=\mathrm{rk}(A)-p+1$, and $\mathrm{Im}(\Psi)$ and $Z$ are both direct factors in $A$ and homocyclic of exponent $p^k$. Also, $\mathbf{E}_{\mathcal{F}}=\{A\}\cup\mathcal{B}_0$. Either $\Psi$ is onto and $\mathrm{rk}(A)=p$, or $\Psi$ is not onto and $\mathrm{rk}(A)>p$. If $\mathrm{rk}(A)\geqslant p+2$, then $A/\mathrm{Fr}(A)\cong\Omega_1(A)$ are irreducible $\mathbb{F}_p[\mathrm{Aut}_{\mathcal{F}}(A)]$-modules.*

(c) *If $\Psi(\sigma)\notin\mathrm{Fr}(Z)$ and $A$ is not homocyclic, then $\Psi$ is onto, $\mathrm{rk}(A)=p-1$, $m\equiv 1\pmod{p-1}$, $\mathrm{Ker}(\Psi)=\langle p^k,p^{k-1}-\ell\sigma\rangle$ for some $\ell$ prime to $p$, and $\mathbf{E}_{\mathcal{F}}=\{A\}\cup\mathcal{H}_0$. Also, $A\cong(C_{p^{k-1}})^{p-2}\times C_{p^k}$, where $\mho^{k-1}(A)=Z=Z_0=\langle\Psi(\sigma)\rangle$. If $k=2$, then $\ell\not\equiv 1\pmod{p}$.*

*Proof.* If $\mathbf{E}_{\mathcal{F}}=\{A\}$, then $A\trianglelefteq\mathcal{F}$ by proposition 1.3(c), contradicting the assumption that $O_p(\mathcal{F})=1$. Thus $\mathbf{E}_{\mathcal{F}}\supsetneqq\{A\}$.

**Case 1: $\Psi(\sigma) \in \mathrm{Fr}(Z)$.** In this case, $\Psi$ is surjective by lemma 4.7(d) and since $\mathrm{Fr}(Z) \leqslant \mathrm{Fr}(A)$. By lemma 4.7(e), $\Psi(\sigma) = 1$, $\mathrm{rk}(A) = p-1$, $Z = Z_0$, and $A \cong R/\mathfrak{p}^m$. In particular, $\mathrm{Ker}(\Psi) = \langle \sigma, (\mathbf{u}-1)^m \rangle$, while $Z_0 = \langle \Psi((\mathbf{u}-1)^{m-1}) \rangle$ by lemma 4.7(c). We are thus in the situation of (a).

**Case 2: $\Psi(\sigma) \notin \mathrm{Fr}(Z)$ and $A$ is homocyclic.** Recall that $k \geqslant 2$ is such that $A$ has exponent $p^k$.

If $\mathrm{rk}(A) < p$, then $\Psi$ is onto by lemma 4.7(d), and $\Omega_1(Z) = C_{\Omega_1(A)}(\mathbf{U})$ has rank 1 by lemma 3.3(c) and since $\Omega_1(A)$ is minimally active and indecomposable by lemma 3.2(b). Thus $Z$ is cyclic, and since $A$ is homocyclic of rank at least 2, $A/Z \cong R/\mathfrak{p}^{m-1}$ also has exponent $p^k \geqslant p^2$. Hence $\mathrm{rk}(A) = \mathrm{rk}(A/Z) = p-1$. Also, $(A/Z)/\mho^{k-1}(A/Z) \cong (C_{p^{k-1}})^{p-1}$, so $|Z| = p$, and $Z = Z_0$. Thus $|A| = |A/Z| \cdot |Z| = p^m$, and $m \equiv 0 \pmod{p-1}$ since $A$ is homocyclic of rank $p-1$. But then $\Psi(\sigma) \notin Z_0$ by lemma 4.7(f), a contradiction.

Thus $\mathrm{rk}(A) \geqslant p$, and $\Psi(\sigma) \notin \mathrm{Fr}(A)$ by lemma 4.7(d). So the homomorphism $\bar{\Psi}\colon \mathbb{F}_p\mathbf{U} \longrightarrow A/\mathrm{Fr}(A)$ is injective, and $A/\mathrm{Fr}(A)$ contains a Jordan block $\mathrm{Im}(\bar{\Psi})$ of rank $p$. Since $A$ is homocyclic of exponent $p^k$, $|\mathrm{Im}(\Psi)| \geqslant p^{pk}$, and thus $\mathrm{Ker}(\Psi) = p^k\mathbb{Z}_p\mathbf{U}$. So $\mathrm{Im}(\Psi) \cong \mathbb{Z}/p^k\mathbf{U}$. Also,

$$p^{m-1} = |A/Z| = |\mathrm{Im}(\Psi)/\langle \Psi(\sigma) \rangle| = p^{k(p-1)},$$

and so $m = k(p-1)+1 \equiv 1 \pmod{p-1}$.

Now, $Z_0 = \langle \Psi(p^{k-1}\sigma) \rangle$, and $\Psi(\sigma) \notin Z_0$ since $k \geqslant 2$. Hence $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{B}_0$ by lemma 4.7(f). Also, $\Psi$ is surjective if and only if $\mathrm{rk}(A) = p$ (lemma 4.7(d)), and we are in the situation of case (b).

**Case 3: $\Psi(\sigma) \notin \mathrm{Fr}(Z)$ and $A$ is not homocyclic.** Set $k' = [m/(p-1)]$. Since $m \equiv 0, 1 \pmod{p-1}$ by lemma 4.7(f), $A/Z \cong R/\mathfrak{p}^{m-1}$ has exponent $p^{k'}$, and hence $\mho^{k'}(A) \leqslant Z$. So $p^{k'}(\mathbf{u}-1) \in \mathrm{Ker}(\Psi)$.

Now, $\Psi$ is onto by lemma 4.7(g), and hence $\mathrm{rk}(A) \leqslant p$ and $Z$ is cyclic by lemma 4.7(d). If $\Psi(\sigma) \notin Z_0$, then $Z_0 < Z$ and is not a direct factor, so $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing$ by lemma 2.5(a). Thus

$$\Psi \text{ onto} \quad \Longrightarrow \quad \Psi(\sigma) \in Z_0 \text{ or } \mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing. \tag{1}$$

**Case 3.1: $\mho^{k'}(A) \neq 1$.** Since $\mho^{k'}(A) \leqslant Z$ is invariant under the action of $G = \mathrm{Aut}_{\mathcal{F}}(A)$, lemma 2.7 implies that $\mho^{k'}(A) = Z_0$ and $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} \neq \varnothing$. In particular, $\mho^{k'}(A) = \langle \Psi(p^{k'}) \rangle$ has order $p$, and $\Psi(\sigma) \in Z_0$ by (1). Thus $\langle \Psi(\sigma) \rangle = Z_0 = \langle \Psi(p^{k'}) \rangle$, so $p^{k'} - \ell\sigma \in \mathrm{Ker}(\sigma)$ for some $\ell$ prime to $p$.

Now, $\mathrm{rk}(A) < p$ by lemma 4.7(d) and since $\Psi(\sigma) \in Z_0 \leqslant \mathrm{Fr}(A)$. Also, $Z = Z_0\langle \Psi(\sigma) \rangle = Z_0$ by lemma 4.7(a), and $m \equiv 1 \pmod{p-1}$ by lemma 4.7(f) and since $\Psi(\sigma) \in Z_0$. So $|A| = |A/Z| \cdot |Z| = p^m = p^{k'(p-1)+1}$, and $A/\mho^{k'}(A)$ has exponent $k'$, rank at most $p-1$, and order $p^{k'(p-1)}$. This proves that $A/\mho^{k'}(A)$ is homocyclic of rank $p-1$ and exponent $p^{k'}$, and hence that $A \cong (C_{p^{k'}})^{p-2} \times C_{p^{k'+1}}$. Thus $k' = k-1$ (recall $A$ has exponent $p^k$). This also shows that $\langle p^{k-1}, \sigma \rangle$ has index $p$ in $\mathrm{Ker}(\Psi)$, and hence (since $p^{k-1} - \ell\sigma$ is in the kernel) that $\mathrm{Ker}(\Psi) = \langle p^k, p^{k-1} - \ell\sigma \rangle$.

If $k = 2$ and $\ell \equiv 1 \pmod{p}$, then $\mathrm{Ker}(\Psi) = \langle p^2, p-\sigma \rangle$, and $(\mathbf{u}-1)^{p-1} \in \mathrm{Ker}(\Psi)$ by lemma 4.8. But then $\Psi((\mathbf{u}-1)^{p-2}) \in Z$ where $Z = Z_0 = \mho^1(A)$, and this is impossible since $A/\mho^1(A)$ has rank $p-1$.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Finally, $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{H}_0$ by lemma 4.7(e) and since $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} \neq \varnothing$. We are thus in the situation of case (c).

**Case 3.2: $\boldsymbol{\mho^{k'}(A) = 1}$.** Since $\Psi(\sigma) \in Z_0 \smallsetminus 1$ or $\mathbf{E}_{\mathcal{F}} \cap \mathcal{H} = \varnothing$ by (1), we have $m \equiv 1 \pmod{p-1}$ by lemma 4.7(f). Thus $m-1 = k'(p-1)$, so $1 \neq Z_0 = \langle \Psi((1-\mathbf{u})^{m-1}) \rangle = \langle \Psi(p^{k'-1}\sigma) \rangle$ by lemma 4.8. Since $p^{k'-1}\sigma \notin \mathrm{Ker}(\Psi)$, we have $|Z| \geqslant |\Psi(\sigma)| = p^{k'}$, and $|A| = |A/Z| {\cdot} |Z| \geqslant p^{m-1+k'} = p^{k'p}$. Hence $A = \mathrm{Im}(\Psi)$ is homocyclic of rank $p$ and exponent $p^{k'}$, contradicting our assumption. □

We now give some examples to show that all cases listed in proposition 4.9 can occur.

Example 4.10. We list here some examples of pairs $(G, A)$ satisfying the hypotheses of theorem 4.5. In all cases, we assume that $G \in \mathscr{G}_p^{\wedge}$ and $\mathbf{U} \in \mathrm{Syl}_p(G)$. By lemma 3.2(b), $\Omega_1(A)$ and $A/\mathrm{Fr}(A)$ must be minimally active and indecomposable.

(a) Each $\mathbb{Q}_pG$-module of dimension $p-1$ whose restriction to $\mathbf{U}$ is isomorphic to the canonical action on $\mathbb{Q}_p(\zeta)$ can be used to construct homocyclic examples of arbitrary exponent, by adding scalars as needed to meet one of the conditions in table 4.1.

More interesting are examples where $A$ is not homocyclic. By proposition 4.9, $\Omega_1(A)$ and $A/\mathrm{Fr}(A)$ must be not only minimally active and indecomposable of dimension $p-1$, but also not simple. By table 6.1, this occurs only when $A_p \leqslant G \leqslant \Sigma_p \times C_{p-1}$, $SL_2(p) \leqslant G \leqslant GL_2(p)$, or $PSL_2(p) \leqslant G \leqslant PGL_2(p) \times C_{p-1}$. By proposition 3.8(a), for each minimally active, indecomposable $\mathbb{F}_pG$-module $V$ of dimension $p-1$, there is a $\mathbb{Z}_pG$-lattice $\Lambda$ such that $\Lambda/p\Lambda \cong V$. If $0 \neq V_0 < V$ is a nontrivial proper $\mathbb{F}_pG$-submodule, and $\Lambda_0 < \Lambda$ is such that $p\Lambda < \Lambda_0$ and $\Lambda_0/p\Lambda \cong V_0$, then we can take $A \cong \Lambda_0/p^k\Lambda$ for arbitrary $k \geqslant 2$.

(b) These are homocyclic, and there are many such examples, obtained from the $\mathbb{F}_pG$-modules in table 6.1 of dimension at least $p$ (all of them are reductions of lattices in $\mathbb{Q}_pG$-modules). Lemma 3.2(c) together with theorem 4.5 imply, very roughly, that each $\mathbb{F}_pG$-module that yields simple fusion systems with elementary abelian $A$ and with $\mathbf{E}_{\mathcal{F}} \subseteq \{A\} \cup \mathcal{B}$ will also give simple fusion systems with $A$ of exponent $p^k$ for arbitary $k > 1$. Some of the resulting fusion systems are realizable (see table 4.2), while 'most' are exotic.

(c) Fix an odd prime $p$, $k \geqslant 2$, and $\ell$ prime to $p$ such that $\ell \not\equiv 1 \pmod{p}$ if $k = 2$. Set $\overline{G} = \Sigma_p \times C_{p-1}$ and $G_0 = O^{p'}(\overline{G}) \cong A_p$, and set $\mathbf{U} = \big\langle (1\,2 \cdots p) \big\rangle \in \mathrm{Syl}_p(\overline{G})$. Let $\Lambda \cong (\mathbb{Z}_p)^p$ be the $\mathbb{Z}_p\overline{G}$-lattice upon which $\Sigma_p$ acts by permuting a $\mathbb{Z}_p$-basis $\{e_1, \ldots, e_p\}$, and where the factor $C_{p-1}$ acts via multiplication by $(p-1)$-st roots of unity in $\mathbb{Z}_p^\times$. Now define

$$A = \Lambda \big/ \big\langle p^k\Lambda, p^{k-1}e_i - \ell(e_1 + \cdots + e_p) \,\big|\, 1 \leqslant i \leqslant p \big\rangle,$$

and let $\bar{e}_i \in A$ be the class of $e_i \in \Lambda$. This defines a finite $\mathbb{Z}_p\overline{G}$-module of rank $p-1$ and exponent $p^k$, as described in the last column in table 4.3, where $\Psi \colon \mathbb{Z}_p\mathbf{U} \longrightarrow A$ is defined by setting $\Psi(\xi) = \xi {\cdot} \bar{e}_1$.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Table 4.4. *The sets in the last column are as defined in notations 2.1 and 4.2.*

<table>
<tr><th>Tbl.4.1</th><th>Tbl.4.3</th><th>$\dim(V)$</th><th>$r=\dim(V_0)$</th><th>$\mathrm{Ker}(\Psi)$</th><th>$\mu_V(G^\vee_{(V)})$</th><th>$G=$</th><th>$\mathbf{E}_\mathcal{F}\smallsetminus\{A\}$</th></tr>
<tr><td rowspan="2">(iv$''$)</td><td>(b)</td><td>$\geqslant p$</td><td>$V_0=V$</td><td>$\langle p^k\rangle$</td><td rowspan="3">$\geqslant \Delta_0$</td><td rowspan="3">$O^{p'}(G)\mu_V^{-1}(\Delta_0)$</td><td rowspan="2">$\mathcal{B}_0$</td></tr>
<tr><td rowspan="6">(a)</td><td rowspan="6">$p-1$</td><td>$1\leqslant r\leqslant p-1$</td><td rowspan="6">$\langle p^k,\sigma,$<br>$p^{k-1}(\mathbf{u}-1)^r\rangle$</td></tr>
<tr><td>(iv$'$)</td><td rowspan="2">$V_0=V$</td><td>$\bigcup_{i\in I}\mathcal{B}_i$</td></tr>
<tr><td>(i)</td><td>$\Delta$</td><td>$O^{p'}(G){\cdot}G^\vee_{(V)}$</td><td>$\mathcal{H}_0\cup\mathcal{B}_*$</td></tr>
<tr><td>(ii)</td><td rowspan="2">$r=p-2$</td><td>$\Delta$</td><td>$O^{p'}(G){\cdot}G^\vee_{(V)}$</td><td>$\mathcal{B}_0\cup\mathcal{H}_*$</td></tr>
<tr><td>(iii$'$)</td><td rowspan="3">$\geqslant \Delta_{-1}$</td><td rowspan="3">$O^{p'}(G)\mu_V^{-1}(\Delta_{-1})$</td><td>$\bigcup_{i\in I}\mathcal{H}_i$</td></tr>
<tr><td rowspan="2">(iii$''$)</td><td>$1\leqslant r\leqslant p-1$</td><td rowspan="2">$\mathcal{H}_0$</td></tr>
<tr><td>(c)</td><td>$p-1$</td><td>$r=1$</td><td>$\langle p^k,p^{k-1}-\ell\sigma\rangle$</td></tr>
</table>

Set $Z=C_A(\mathbf{U})$. Note that $|p^{k-1}A|=p$, and $A/p^{k-1}A\cong\Lambda/\langle p^{k-1}\Lambda,\bar{e}_1+\cdots+\bar{e}_p\rangle\cong\mathbb{Z}_p[\zeta]/(p^{k-1})$. Hence $Z\geqslant p^{k-1}A$, and $|Z|>p$ only if $p^{k-2}(\bar{e}_1+2\bar{e}_2+\cdots+p\bar{e}_p)\in Z$. But this last is the case only if $p^{k-2}((\bar{e}_1+\cdots+\bar{e}_p)-p\bar{e}_1)=0$, which is not possible since we assumed that either $k\geqslant 3$ or $\ell\not\equiv 1 \pmod p$. Thus $|Z|=p$ in all cases.

Now set $S=A\rtimes\mathbf{U}$, and set $\overline{G}^\vee=N_{\overline{G}}(\mathbf{U})$. (Note that $Z=Z_0$ in the notation of 2.1.) Define $\mu_A\colon\overline{G}^\vee\longrightarrow\Delta$ as in notation 2.9. One easily checks that $\mu_A(\overline{G}^\vee)=\Delta$. Set $G=G_0\mu_A^{-1}(\Delta_{-1})$. This now defines an action which satisfies the conditions in theorem 4.5, including condition (d.iii$''$).

We now combine theorem 4.5 with proposition 4.9 to prove our main result on simple fusion systems over finite $p$-groups with an abelian subgroup of index $p$ and exponent at least $p^2$. Recall that $\mathbf{E}_\mathcal{F}$ is the set of essential subgroups in a fusion system $\mathcal{F}$ (definition 1.2), and that $\mathscr{G}_p^\wedge$ is a certain class of finite groups (definition 3.1).

Theorem A. *Fix an odd prime $p$.*

(a) *Let $\mathcal{F}$ be a simple fusion system over a finite nonabelian $p$-group $S$ with an abelian subgroup $A<S$ of index $p$ such that $A\in\mathbf{E}_\mathcal{F}$. Let $k$ be such that $A$ has exponent $p^k$, and assume $k\geqslant 2$ ($A$ is not elementary abelian). Set $G=\mathrm{Aut}_\mathcal{F}(A)$, $\mathbf{U}=\mathrm{Aut}_S(A)\in\mathrm{Syl}_p(G)$, $V=\Omega_1(A)$, and $V_0=\mho^{k-1}(A)\leqslant V$. Let $G^\vee_{(V)}=\big\{\alpha\in N_G(\mathbf{U})\,\big|\,[\alpha,C_V(\mathbf{U})]\leqslant[\mathbf{U},V]\big\}$ and $\mu_V\colon G^\vee_{(V)}\longrightarrow\Delta$ be as in notation 2.9. Let $\Psi\colon\mathbb{Z}_p\mathbf{U}\longrightarrow A$ be as in notation 4.6. Then $G\in\mathscr{G}_p^\wedge$, restriction defines an isomorphism $G\cong\mathrm{Aut}_\mathcal{F}(V)$, and*

> *$V$ is a faithful, minimally active, indecomposable $\mathbb{F}_pG$-module, and $[G,V_0]=V_0$. Also, one of the cases in table 4.4 holds, where $V$ has no $1$-dimensional submodule in cases (iv$'$) and (iv$''$).* $(*_{\mathrm{fin}})$

(b) *Conversely, assume that $G\in\mathscr{G}_p^\wedge$ and $\mathbf{U}\in\mathrm{Syl}_p(G)$, and that $V$ is a faithful, minimally active, indecomposable $\mathbb{F}_pG$-module satisfying $(*_{\mathrm{fin}})$ for some submodule $0\neq V_0\leqslant V$, where $G^\vee$ is the subgroup of all elements $g\in N_G(\mathbf{U})$*

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

*such that $[g, C_V(\mathbf{U})] \leqslant [\mathbf{U}, V]$. Then for each $k \geqslant 2$, there is a simple fusion system $\mathcal{F}$ over a finite $p$-group $S$ containing an abelian subgroup $A$ of index $p$, and such that $G \cong \mathrm{Aut}_{\mathcal{F}}(A)$, $A$ has exponent $p^k$, $\Omega_1(A) \cong V$ and $\mho^{k-1}(A) \cong V_0$ as $\mathbb{F}_pG$-modules, and with $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$ as described in table 4.1. Furthermore, any other simple fusion system with these properties, and with the same essential subgroups, is isomorphic to $\mathcal{F}$.*

*Proof.* **(a)** Set $\mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$ and $Z = C_A(\mathbf{U})$.

Under the above assumptions, $G \in \mathscr{G}_p^\wedge$ by lemma 3.2(a), $V$ is faithful, minimally active, and indecomposable by lemma 3.2(b), and $\dim(V) = \mathrm{rk}(A) \geqslant p-1$ by proposition 4.9. In particular, restriction induces a monomorphism $G = \mathrm{Aut}_{\mathcal{F}}(A) \longrightarrow \mathrm{Aut}_{\mathcal{F}}(V)$, and this is an isomorphism by the extension axiom (definition 1.1) and since $A = C_S(V)$. From now on, we identify $G = \mathrm{Aut}_{\mathcal{F}}(V)$.

Set $G^\vee_{(A)} = \bigl\{\alpha \in N_G(\mathbf{U}) \bigm| [\alpha, C_A(\mathbf{U})] \leqslant [\mathbf{U}, A]\bigr\}$. Thus $G^\vee_{(A)} \leqslant G^\vee_{(V)}$, and $\mu_A\colon G^\vee_{(A)} \longrightarrow \Delta$ is as in notation 2.9. For some $\Delta_x \in \{\Delta, \Delta_0, \Delta_{-1}\}$, $\mu_A(G^\vee_{(A)}) \geqslant \Delta_x$ and $G = O^{p'}(G)\mu_A^{-1}(\Delta_x)$ by theorem 4.5(d). So the same holds if we replace $G^\vee_{(A)}$ by $G^\vee_{(V)}$ and $\mu_A$ by $\mu_V$.

Assume we are in case (a) of table 4.3. Then $Z = Z_0$ has order $p$, so $|A| = p^m$, and $m \equiv 0 \pmod{p-1}$ if and only if $A$ is homocyclic. Also, $\Psi(\sigma) = 1$. Thus we are in case (i), (iii$''$), (iv$'$), or (iv$''$) of table 4.1 if $A$ is homocyclic, or in case (ii), (iii$'$), (iii$''$), or (iv$''$) if $A$ is not homocyclic. Since $m \equiv 0 \pmod{p-1}$ and $\Psi(\sigma) = 1$ when $A$ is homocyclic, (iv$''$) is a special case of (iv$'$). The other information follows from the two earlier tables.

Now assume we are in case (b) or (c) in table 4.3. Then $\Psi(\sigma) \notin \mathrm{Fr}(Z)$, so this corresponds to case (iii$''$) or (iv$''$) in table 4.1. Since $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{H}_0$ in cases (c) and (iii$''$), and $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{B}_0$ in cases (b) and (iv$''$), these are the only possible correspondences. In case (b), $A$ is homocyclic, and so we have $V_0 = V$ in table 4.4. In case (c), $A \cong (C_{p^{k-1}})^{p-2} \times C_{p^k}$, so $V = \Omega_1(A)$ has a submodule $V_0 = \mho^k(A)$ of rank 1.

There is a surjective homomorphism $\psi\colon A \longrightarrow V_0$ of $\mathbb{Z}_pG$-modules, defined by setting $\psi(a) = a^{p^{k-1}}$. Since $[G, A] = A$ by theorem 4.5(c), we have $[G, V_0] = V_0$.

If $V = \Omega_1(A)$ has a 1-dimensional $\mathbb{F}_pG$-submodule $W$, then $W \in C_V(\mathbf{U}) \leqslant C_A(\mathbf{U})$, so $W = Z_0 = C_A(\mathbf{U}) \cap [\mathbf{U}, A]$ by theorem 4.5(b), which is impossible in cases (iv$'$) and (iv$''$) of theorem 4.5(d).

**(b)** Fix $G \in \mathscr{G}_p^\wedge$ and $\mathbf{U} \in \mathrm{Syl}_p(G)$, and let $V$ be an $\mathbb{F}_pG$-module that satisfies $(*_{\mathrm{fin}})$, where $G^\vee$ is the subgroup of all elements $g \in N_G(\mathbf{U})$ such that $[g, C_V(\mathbf{U})] \leqslant [\mathbf{U}, V]$. Fix $k \geqslant 2$.

Assume we have chosen a finite $\mathbb{Z}_pG$-module $A$ such that $\Omega_1(A) \cong V$ as $\mathbb{F}_pG$-modules, and such that either $\dim(V) = p-1$ and $|C_A(\mathbf{U})| = p$, or $\dim(V) \geqslant p$ and $A$ is homocyclic. Let $G^\vee_{(A)} \leqslant G^\vee_{(V)}$ be as in the proof of (a). If $\mathrm{rk}(V) = \mathrm{rk}(A) = p-1$, then since $C_A(\mathbf{U}) \cong C_V(\mathbf{U})$ has order $p$, $G^\vee_{(A)} = G^\vee_{(V)} = N_G(\mathbf{U})$ and $\mu_A = \mu_V$. So the properties of $G^\vee_{(V)}$ and $\mu_V$ in table 4.4 also hold for $G^\vee_{(A)}$ and $\mu_A$.

If $\mathrm{rk}(V) = \mathrm{rk}(A) \geqslant p$ and $A$ is homocyclic, then $\mu_V(G^\vee_{(V)}) \geqslant \Delta_0$, and $G = O^{p'}(G)\mu_V^{-1}(\Delta_0)$. In such cases, we could have $G^\vee_{(A)} < G^\vee_{(V)}$, but for each $\alpha \in \mu_V^{-1}(\Delta_0)$ of order prime to $p$, $\alpha$ acts trivially on $C_V(\mathbf{U}) \cong \Omega_1(C_A(\mathbf{U}))$ by definition of $\mu_V$ (and lemma A.1), and hence also acts trivially on $C_A(\mathbf{U})$ (see [**20**, theorem 5.2.4]). Thus $\mu_V^{-1}(\Delta_0) = \mu_A^{-1}(\Delta_0)$, and so the information in table 4.4 still holds if we replace $G_{(V)}^\vee$ and $\mu_V$ by $G_{(A)}^\vee$ and $\mu_A$.

**Cases 4.9(a,b):** Assume that we are in Case (a) or (b) in proposition 4.9. By proposition 3.8(a), there is a $\mathbb{Z}_pG$-lattice $\Lambda$ such that $\Lambda/p\Lambda \cong V$ as $\mathbb{F}_pG$-modules. Let $\Lambda_0 \leqslant \Lambda$ be such that $\Lambda_0 \geqslant p\Lambda$ and $\Lambda_0/p\Lambda \cong V_0$, and set $A = \Lambda_0/p^k\Lambda$. Set $S = A \rtimes \mathbf{U}$, $Z = Z(S) = C_A(\mathbf{U})$, $S' = [S,S] = [\mathbf{U}, A]$, and $Z_0 = Z \cap S'$.

We first check that conditions (a)–(d) in theorem 4.5 all hold. Condition (d) follows immediately from ($*_{\text{fin}}$). Condition (a) ($|Z_0| = p$) follows from lemma 3.7(c) and since $A$ is defined to be a quotient group of a $\mathbb{Z}_pG$-lattice.

Assume $1 \neq B \leqslant Z$ is $G$-invariant; we claim that $B = Z_0$. If $\text{rk}(A) = p-1$, then $Z = Z_0$, and there is nothing to prove. If not, then $\text{rk}(A) \geqslant p$, we are in case (iv$''$), and so $V$ has no 1-dimensional $\mathbb{F}_pG$-submodule. Thus $\text{rk}(Z) \geqslant \text{rk}(B) \geqslant 2$, and hence $\dim(V) \geqslant p+1$. If $\dim(V) = p+1$, then by lemma 3.5, every nontrivial $\mathbb{F}_pG$-submodule has nontrivial action of $\mathbf{U}$, contradicting the assumption $B \leqslant Z$. If $\dim(V) \geqslant p+2$, then $V$ is simple by [**15**, proposition 3.7(c)]. So Condition 4.5(b) holds in all cases.

If $\text{rk}(A) \geqslant p$, then $V_0 = V$, $A/\text{Fr}(A) \cong V_0$, and so $[G, A] = A$ since $[G, V_0] = V_0$. If $\text{rk}(A) = p-1$, then by lemma A.5(a–c), $\Lambda_0|_{\mathbf{U}} \cong \mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_p\mathbf{U}$-modules, and the radical of $\Lambda_0|_{\mathbf{U}}$ has index $p$. Thus $p\Lambda$ is contained in the radical, and in $[G, A] = A$ since $V_0 \cong \Lambda_0/p\Lambda$ and $[G, V_0] = V_0$. This proves 4.5(c).

By theorem 4.5, there is a unique simple fusion system $\mathcal{F}$ over $A \rtimes \mathbf{U}$ such that $G = \text{Aut}_{\mathcal{F}}(A)$, $A \in \mathbf{E}_{\mathcal{F}}$, and $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$ is as described in table 4.4. Since $A$ is unique (up to isomorphism of $\mathbb{Z}_pG$-modules) by proposition 3.9(a) (in case 4.9(b)) or 3.9(b) (in case 4.9(a)), this shows that $\mathcal{F}$ is uniquely determined by $V$.

**Case 4.9(c):** Assume that we are in Case (c) in proposition 4.9. In particular, $\dim(V) = p-1$ and $\dim(V_0) = 1$. By lemma 3.4(c), there is a projective, minimally active $\mathbb{F}_pG$-module $W > V$ such that $\dim(W) = p$ and thus $\dim(W/V) = 1$.

By proposition 3.8(b), there is a $\mathbb{Z}_pG$-lattice $\Lambda$ such that $\Lambda/p\Lambda \cong W$, and such that $\Lambda$ has a $\mathbb{Z}_pG$-submodule $\Lambda_0 = C_\Lambda(G_0)$ of rank 1. In particular, $\Lambda$ is free as a $\mathbb{Z}_p\mathbf{U}$-module since $W$ is free as an $\mathbb{F}_p\mathbf{U}$-module. Let $\Lambda_V < \Lambda$ be the $\mathbb{Z}_pG$-sublattice of index $p$ such that $\Lambda_V/p\Lambda \cong V$. Define

$$\widehat{A} = \Lambda/\big(p^k\Lambda + p^{k-1}\Lambda_V + p\Lambda_0\big) \cong C_{p^k} \times (C_{p^{k-1}})^{p-2} \times C_p\,.$$

Then $\Omega_1(\widehat{A})$ is a $p$-dimensional $\mathbb{F}_pG$-module, and contains a 2-dimensional submodule

$$\begin{aligned}\widehat{A}_0 &= \big(p^{k-1}\Lambda + \Lambda_0\big)/\big(p^k\Lambda + p^{k-1}\Lambda_V + p\Lambda_0\big)\\ &\cong \big(p^{k-1}\Lambda/(p^k\Lambda + p^{k-1}\Lambda_V)\big) \oplus \big(\Lambda_0/p\Lambda_0\big) \cong (W/V) \oplus V_0\,.\end{aligned}$$

Now, $V_0 \cong W/V$ as $\mathbb{F}_p[N_G(\mathbf{U})]$-modules by lemma 3.4(a) and since $\dim(W) = p$. Also, $O^{p'}(G)$ acts trivially on each of them and $G = O^{p'}(G)N_G(\mathbf{U})$ by the Frattini argument, so $V_0$ and $W/V$ are isomorphic as $\mathbb{F}_pG$-modules, and any $\mathbb{F}_p$-linear isomorphism is $\mathbb{F}_pG$-linear. Hence for fixed $a \in \Lambda \smallsetminus \Lambda_V$ and fixed $\ell$ prime to $p$ such

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

that $\ell \not\equiv 1 \pmod p$ if $k = 2$, the quotient group

$$A = \widehat{A}/\widehat{A}_1 \quad \text{where} \quad \widehat{A}_1 = \langle [p^{k-1}a - \ell\sigma{\cdot}a] \rangle \leqslant \widehat{A}_0$$

is a quotient group of $\widehat{A}$ where the two summands of $\widehat{A}_0$ have been identified, and hence is a $\mathbb{Z}_pG$-module. Here, as usual, $\sigma = \sum_{u\in\mathbf{U}} u \in \mathbb{Z}_p\mathbf{U}$. Note that $\widehat{A}_1$ is independent of the choice of $a$, and depends on $\ell$ only modulo $p$.

Since $\widehat{A}/\widehat{A}_0 \cong \Lambda/(p^{k-1}\Lambda + \Lambda_0)$, where $\Lambda/\Lambda_0 \cong \mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_p\mathbf{U}$-modules by lemma A.5(c), we have that $|C_{\widehat{A}/\widehat{A}_0}(\mathbf{U})| = p$, and is generated by the class of $p^{k-2}(u-1)^{p-2}a$ for $1 \neq u \in \mathbf{U}$. The class of $p^{k-2}(u-1)^{p-2}a$ in $A$ is fixed by $\mathbf{U}$ if and only if as classes in $\widehat{A}$,

$$[p^{k-2}(u-1)^{p-1}a] = [p^{k-2}(\sigma - p)a] = [p^{k-2}\sigma{\cdot}a] - [p^{k-1}a] \in \widehat{A}_1$$

(where the second equality holds by lemma 4.8). But this fails to hold under our hypotheses: either $k > 2$, in which case $[p^{k-2}\sigma{\cdot}a] = 0$ and $[p^{k-1}a] \neq 0$ in $\widehat{A}$; or $k = 2$ and $\ell \not\equiv 1 \pmod p$, in which case $[\sigma{\cdot}a] - [pa] \notin \widehat{A}_1$. Thus in all such cases, $C_A(\mathbf{U}) = \widehat{A}_0/\widehat{A}_1$ and has order $p$.

Since $V_0 \cong \Lambda_0/p\Lambda_0 \cong \widehat{A}_0/\widehat{A}_1 = C_A(\mathbf{U})$ as $\mathbb{F}_pG$-modules, and since $V$ and $\Omega_1(A)$ are both $(p-1)$-dimensional minimally active $\mathbb{F}_pG$-modules, lemma 3.4(d) applies to show that $V \cong \Omega_1(A)$ as $\mathbb{F}_pG$-modules.

By construction, $(G, A)$ satisfies all of the conditions in case (c) of proposition 4.9, as well as condition (d.iii$''$) of theorem 4.5. Since $|Z| = |C_A(\mathbf{U})| = p$, conditions (a) and (b) in 4.5 also hold: $|Z_0| = p$, and no nontrivial subgroup of $Z$ is $G$-invariant except possibly $Z_0 = Z$. Finally, 4.5(c) holds ($[G, A] = A$) since $A/[\mathbf{U}, A] = A/\Omega_{k-1}(A)$ has order $p$, and has nontrivial action of $G$ since $G$ acts nontrivially on $Z_0 = \mho^{k-1}(A)$ (since $\mu_A(G^\vee) \geqslant \Delta_{-1}$).

By theorem 4.5, there is a unique simple fusion system $\mathcal{F}$ over $A \rtimes \mathbf{U}$ such that $G = \mathrm{Aut}_{\mathcal{F}}(A)$, $A \in \mathbf{E}_{\mathcal{F}}$, and $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{H}$. Since $A$ is unique up to isomorphism of $\mathbb{Z}_pG$-modules by proposition 3.9(b), this shows that $\mathcal{F}$ is uniquely determined by $V$. □

## 5. Simple fusion systems over nonabelian discrete *p*-toral groups with an abelian subgroup of index *p*

We now focus on the case where $A$ and $S$ are infinite. Since most of the results in § 2 assume notation 2.1, and in particular, that $S$ contains a unique abelian subgroup of index $p$, we begin by proving that this always holds when $O_p(\mathcal{F}) = 1$.

Lemma 5.1. *Let $\mathcal{F}$ be a saturated fusion system over an infinite discrete $p$-toral group $S$ with an abelian subgroup $A$ of index $p$. Assume also that $O_p(\mathcal{F}) = 1$. Then $|A/Z(S)| = \infty$.*

*Proof.* Let $S_0 \trianglelefteq S$ denote the identity component of $S$. If $|A/Z(S)| < \infty$, then $S_0 \leqslant Z(S)$, so $S_0$ is contained in (and is characteristic in) each $P \in \mathbf{E}_{\mathcal{F}}$. Thus

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

$S_0 \trianglelefteq \mathcal{F}$ by proposition 1.3(c), so $S_0 \leqslant O_p(\mathcal{F}) = 1$, contradicting the assumption that $|A| = \infty$. □

Corollary 5.2. *If $\mathcal{F}$ is a saturated fusion system over an infinite discrete p-toral group $S$ with an abelian subgroup $A$ of index $p$, and $O_p(\mathcal{F}) = 1$, then $A$ is the only abelian subgroup of index $p$ in $S$.*

*Proof.* Since $|A/Z(S)| = \infty$ by lemma 5.1, this follows from lemma A.3. □

Lemma 5.3. *Assume notation 2.1. If $|A| = \infty$ and $O_p(\mathcal{F}) = 1$, then $A/Z$ and $S'$ are both discrete p-tori of rank $p - 1$.*

*Proof.* Since $|A/Z| = \infty$ by lemma 5.1 and $C_{A/Z}(\mathbf{U}) = Z_2/Z$ has order $p$ by lemma 2.4, $A/Z \cong (\mathbb{Z}/p^\infty)^{p-1}$ by lemma A.5(d). Also, $A/Z \cong S'$ by lemma A.3. □

Lemma 5.4. *Assume notation 2.1. If $|A| = \infty$ and $O_p(\mathcal{F}) = 1$, then $A = ZS'$. As one consequence, each of the sets $\mathcal{B}$ and $\mathcal{H}$ consists of one S-conjugacy class.*

*Proof.* Fix a generator $u \in \mathbf{U}$, and define $\chi\colon A/Z \longrightarrow A/Z$ by setting $\chi(aZ) = [a, u]Z$. Then $\mathrm{Im}(\chi) = ZS'/Z$, and $\mathrm{Ker}(\chi) = Z_2/Z$ has order $p$ by lemma 2.4. Since $A/Z$ is a discrete $p$-torus by lemma 5.3, $\chi$ must be onto, and hence $ZS' = A$.

Thus if $P = Z\langle x\rangle$ and $Q = Z\langle y\rangle$ are two members of $\mathcal{H}$, where $yx^{-1} \in A$, then there are $z \in Z$ and $a \in A$ such that $yx^{-1} = axa^{-1}x^{-1}z$. Then $y \in {}^axZ$, so $Q = {}^aP$, and $P$ and $Q$ are $S$-conjugate. A similar argument shows that all members of $\mathcal{B}$ are $S$-conjugate. □

Part of the next lemma follows from lemma 2.7 when $p$ is odd. But since we also need it here when $p = 2$, we prove it independently of the earlier lemma.

Lemma 5.5. *Assume notation 2.1, and also that $|A| = \infty$, $O_p(\mathcal{F}) = 1$, and $A \notin \mathbf{E}_\mathcal{F}$. Then $Z = Z_0$, $\mathbf{E}_\mathcal{F} = \mathcal{H}$, and $A = S'$ is a discrete p-torus of rank $p - 1$.*

*Proof.* Since $A \notin \mathbf{E}_\mathcal{F}$, lemmas 2.2 and 2.3 imply that $\mathbf{E}_\mathcal{F} = \mathcal{B}$ or $\mathbf{E}_\mathcal{F} = \mathcal{H}$. If $\mathbf{E}_\mathcal{F} = \mathcal{B}$, then since $Z = Z(S)$ is normalized by $\mathrm{Aut}_\mathcal{F}(S)$ and by $\mathrm{Aut}_\mathcal{F}(P)$ for each $P \in \mathcal{B}$ ($Z$ is characteristic in $P$ by lemma 2.5(b)), $Z \trianglelefteq \mathcal{F}$ by proposition 1.3(c), contradicting the assumption that $O_p(\mathcal{F}) = 1$. Thus $\mathbf{E}_\mathcal{F} = \mathcal{H}$.

For $P = Z\langle x\rangle \in \mathcal{H}$, by lemma 2.5(a), $P = P_1 \times P_2$, where $P_1 = C_P(O^{p'}(\mathrm{Aut}_\mathcal{F}(P))) < Z$, $Z = P_1 \times Z_0$, and $Z_0 < P_2 \cong C_p \times C_p$, and where each factor $P_i$ is normalized by $\mathrm{Aut}_\mathcal{F}(P)$. If $P^* \in \mathcal{H}$ is another member, then $P^* = {}^gP$ for some $g \in S$ by lemma 5.4, and $P_1 = {}^gP_1 = C_{{}^gP}(O^{p'}(\mathrm{Aut}_\mathcal{F}({}^gP)))$ is also normalized by $\mathrm{Aut}_\mathcal{F}({}^gP)$. Finally, $P_1$ is normalized by $\mathrm{Aut}_\mathcal{F}(S)$ since $\mathrm{Aut}_\mathcal{F}(S) = \mathrm{Inn}(S){\cdot}N_{\mathrm{Aut}_\mathcal{F}(S)}(P)$ by the Frattini argument, and thus $P_1 \trianglelefteq \mathcal{F}$ by proposition 1.3(c). So $P_1 \leqslant O_p(\mathcal{F}) = 1$, and hence $Z = Z_0$.

Since $Z = Z_0$, we have $A = S'$ by lemma 5.4, and so $A$ is a discrete $p$-torus of rank $p - 1$ by lemma 5.3. □

When $A$ is finite and $p$ is odd, it was shown in [**23**, lemma 2.4] that $O_p(\mathcal{F}) = 1$ and $A \notin \mathbf{E}_\mathcal{F}$ imply $Z = Z_0$. When $A$ is finite and $p = 2$, this is not true: for each odd prime $p$, the 2-fusion system of $PSL_2(p^2)\langle\phi\rangle$, where $\phi$ is a field automorphism of

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

order 2, is a counterexample. Note that in this case, $S \cong D \times C_2$ for some dihedral 2-group $D$ (whose order depends on $p$).

The case $p = 2$ is now very easy to handle.

Theorem 5.6. *Let $S$ be an infinite nonabelian discrete 2-toral group with an abelian subgroup $A < S$ of index 2. Let $\mathcal{F}$ be a saturated fusion system over $S$ such that $O_2(\mathcal{F}) = 1$. Then $\mathcal{F}$ is isomorphic to the 2-fusion system of $SO(3)$ (if $A$ is not $\mathcal{F}$-essential) or of $PSU(3)$ (if $A$ is $\mathcal{F}$-essential).*

*Proof.* Recall that $A$ is the unique abelian subgroup of index 2 in $S$ by corollary 5.2. So we can use notation 2.1. Also, $|Z_0| = 2$ by lemma 2.4, and $\mathbf{E}_\mathcal{F} \smallsetminus \{A\} = \mathcal{H}$ or $\mathcal{B}$ by lemmas 2.2 and 5.4 (and since $A \trianglelefteq \mathcal{F}$ if $\mathbf{E}_\mathcal{F} \subseteq \{A\}$).

**Case 1:** Assume first that $A \notin \mathbf{E}_\mathcal{F}$. Then by lemma 5.5, $\mathbf{E}_\mathcal{F} = \mathcal{H}$, $Z = Z_0$, and $A = S'$ is a discrete $p$-torus of rank 1. Thus $A \cong \mathbb{Z}/2^\infty$, where this group is inverted by the action of $S/A$. Also, for each $P \in \mathbf{E}_\mathcal{F} = \mathcal{H}$, $P \cong C_2 \times C_2$ and hence $\mathrm{Aut}_\mathcal{F}(P) = \mathrm{Aut}(P) \cong \Sigma_3$. Thus there is a unique choice of fusion system $\mathcal{F}$ on $S$, and it must be isomorphic to the fusion system of $SO(3)$.

**Case 2:** Now assume that $A$ is $\mathcal{F}$-essential, and set $G = \mathrm{Aut}_\mathcal{F}(A)$. Then $\mathrm{Aut}_S(A) \in \mathrm{Syl}_2(G)$ has order 2, so $|G| = 2m$ for some odd $m$. By proposition A.7, we can write $G = G_1 \times G_2$ and $A = A_1 \times A_2$, where $G_i$ acts faithfully on $A_i$ and trivially on $A_{3-i}$ for $i = 1, 2$, where $|G_1|$ is odd, $G_2 \cong \Sigma_3$, and $A_2 \cong C_{2^k} \times C_{2^k}$ for some $1 \leqslant k \leqslant \infty$.

Now, $|A_2| = \infty$ since $A_1 \leqslant Z$ and $|A/Z| = \infty$ (lemma 5.1). Hence $Z_0$ is not a direct factor in $Z$, so $\mathcal{H} \cap \mathbf{E}_\mathcal{F} = \varnothing$ by lemma 2.5(a), and $\mathbf{E}_\mathcal{F} = \{A\} \cup \mathcal{B}$. Each $\alpha \in \mathrm{Aut}_\mathcal{F}(S)$ normalizes $A$ and hence normalizes $A_1$. For each $P \in \mathcal{B}$ and each $\alpha \in \mathrm{Aut}_\mathcal{F}(P)$, $\alpha(Z) = Z$ since $Z = Z(P)$, $\alpha|_Z \in \mathrm{Aut}_\mathcal{F}(Z)$ extends to $\bar{\alpha} \in \mathrm{Aut}_\mathcal{F}(S)$, and thus $\alpha(A_1) = A_1$. So $A_1 \trianglelefteq \mathcal{F}$, and $A_1 \leqslant O_2(\mathcal{F}) = 1$.

Thus $A \cong (\mathbb{Z}/2^\infty)^2$ and $\mathrm{Aut}_\mathcal{F}(A) = G \cong \Sigma_3$. For each $P \in \mathcal{B} = \mathbf{E}_\mathcal{F} \smallsetminus \{A\}$, $P \in (\mathbb{Z}/2^\infty) \times_{C_2} Q_8$, and the subgroup isomorphic to $Q_8$ is unique. Hence $\mathrm{Out}_\mathcal{F}(P) \cong \Sigma_3$ is uniquely determined, and $\mathcal{F}$ is determined uniquely by $\mathrm{Aut}_\mathcal{F}(A)$. So $\mathcal{F}$ is the 2-fusion system of $PSU(3)$. □

We now focus on the cases where $p$ is odd.

Proposition 5.7. *Assume notation 2.1. Assume also that $p$ is odd, $|A| = \infty$, and $O_p(\mathcal{F}) = 1$. Then $A$ is a discrete $p$-torus. If $\mathrm{rk}(A) \geqslant p$, then $Z$ is also a discrete $p$-torus, and has rank $\mathrm{rk}(A) - p + 1$.*

*Proof.* We first apply lemma 2.8, with $A_1 = A$ and $A_2$ the identity component of $A$. Since $S'$ is a discrete $p$-torus by lemma 5.3, we have $A_2Z \geqslant ZS' = A = A_1$ by lemma 5.4. So by lemma 2.8, $A \leqslant A_2Z_0 = A_2$, the last equality since $Z_0 \leqslant S' \leqslant A_2$. Thus $A$ is a discrete $p$-torus.

Set $G = \mathrm{Aut}_\mathcal{F}(A)$ and $V = \Omega_1(A)$, and choose $1 \neq u \in \mathbf{U} \in \mathrm{Syl}_p(G)$. By lemma 3.2(a,b), $G \in \mathscr{G}_p^\wedge$ (so $|\mathbf{U}| = p$), and $V$ is faithful, minimally active, and indecomposable as an $\mathbb{F}_pG$-module. So if $\dim(V) = \mathrm{rk}(A) \geqslant p$, then by lemma 3.3(a,b), the action of $u$ on $V$ has a Jordan block of length $p$, and hence $\dim(\Omega_1(Z)) = \dim(C_V(\mathbf{U})) = \mathrm{rk}(A) - p + 1$.

Let $Z_1, Z_2 \leqslant Z$ be such that $Z_1$ is a discrete $p$-torus, $Z_2$ is a finite abelian $p$-group, and $Z = Z_1 \times Z_2$. Since $\mathrm{rk}(A/Z) = p - 1$ by lemma 5.3, $\mathrm{rk}(Z_1) = \mathrm{rk}(A) - p + 1 = \dim(\Omega_1(Z))$. So $Z_2 = 1$, and $Z = Z_1$ is a discrete $p$-torus. □

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Lemma 5.8. *Assume notation 2.1, and also that $p$ is odd, $|A| = \infty$, and $O_p(\mathcal{F}) = 1$. Then no proper nontrivial subgroup of $S$ is strongly closed in $\mathcal{F}$. Thus $\mathcal{F}$ is simple if and only if it contains no proper normal subsystem over $S$.*

*Proof.* Assume that $1 \neq Q \leqslant S$ is strongly closed in $\mathcal{F}$. If $Q \leqslant Z$, then $Q$ is contained in all $\mathcal{F}$-essential subgroups, so $Q \trianglelefteq \mathcal{F}$ by proposition 1.3(c), contradicting the assumption that $O_p(\mathcal{F}) = 1$. Thus $Q \nleqslant Z$.

Now, $(QZ/Z) \cap Z(S/Z) \neq 1$ since $Q \trianglelefteq S$, so $Q \cap Z_2 \nleqslant Z$. Fix $g \in (Q \cap Z_2) \smallsetminus Z$. Then $Q \geqslant [g, S] = Z_0$ since $Q \trianglelefteq S$.

Fix $P \in \mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} \subseteq \mathcal{B} \cup \mathcal{H}$ (recall $A \ntrianglelefteq \mathcal{F}$). If $P \in \mathcal{B}$, then the $\mathrm{Aut}_{\mathcal{F}}(P)$-orbit of $g \in (Q \cap Z_2) \smallsetminus Z$ is not contained in $A$. If $P \in \mathcal{H}$, then the $\mathrm{Aut}_{\mathcal{F}}(P)$-orbit of $Z_0 \leqslant Q$ is not contained in $A$. So in either case, $Q \nleqslant A$. Hence $Q \geqslant [Q, S] \geqslant [\mathbf{U}, A] = S'$.

Set $G_0 = O^{p'}(G)$. Since $Q \cap A$ is normalized by the action of $G$, and contains $[\mathbf{U}, A]$ where $G_0$ is the normal closure of $\mathbf{U}$ in $G$, $Q \geqslant [G_0, A]$. Since $C_A(G_0) \leqslant C_A(\mathbf{U}) = Z$ and $C_A(G_0)$ is normalized by $G$, $C_A(G_0) \leqslant Z_0 \leqslant [\mathbf{U}, A]$ by lemma 2.7. So by lemma A.2, $[G_0, A] \geqslant C_A(\mathbf{U}) = Z$. Thus $Q \geqslant ZS' = A$, and so $Q = S$ since $Q \nleqslant A$.

The last statement is immediate. □

Lemma 5.9. *Assume notations 2.1 and 2.9, and also that $|A| = \infty$ and $S$ splits over $A$.*

(a) *The kernel of $\mu\colon \mathrm{Aut}^{\vee}(S) \longrightarrow \Delta$ does not contain any elements of finite order prime to $p$.*

(b) *Fix $Q \in \mathcal{B} \cup \mathcal{H}$, and set $t = 0$ if $Q \in \mathcal{B}$, $t = -1$ if $Q \in \mathcal{H}$. Assume that $\mu(\mathrm{Aut}^{\vee}_{\mathcal{F}}(S)) \geqslant \Delta_t$. Then there are unique subgroups $\widetilde{Z} \leqslant Z$ and $\widetilde{Q} \geqslant Q \cap S'$ which are normalized by $N_{\mathrm{Aut}_{\mathcal{F}}(S)}(Q)$, and are such that the following hold.*

(i) *If $Q \in \mathcal{H}$, then $Q = \widetilde{Z} \times \widetilde{Q}$ and $\widetilde{Q} \cong C_p \times C_p$.*

(ii) *If $Q \in \mathcal{B}$, then $\widetilde{Z} = Z$, $Q = Z\widetilde{Q}$, $Z \cap \widetilde{Q} = Z_0 = Z(\widetilde{Q})$, and $\widetilde{Q}$ is extraspecial of order $p^3$ and exponent $p$.*

(iii) *Thus in all cases, $\mathrm{Out}(\widetilde{Q}) \cong GL_2(p)$. If $\alpha \in \mathrm{Aut}(Q)$ is such that $\alpha|_{\widetilde{Z}} = \mathrm{Id}$, $\alpha(\widetilde{Q}) = \widetilde{Q}$, $\alpha(Q \cap A) = Q \cap A$, and $\alpha|_{\widetilde{Q}} \in O^{p'}(\mathrm{Aut}(\widetilde{Q}))$, then $\alpha$ extends to some $\bar{\alpha} \in N_{\mathrm{Aut}^{\vee}_{\mathcal{F}}(S)}(Q)$.*

*Proof.* **(a)** Fix $\alpha \in \mathrm{Ker}(\mu)$ of finite order prime to $p$. Then $\alpha$ induces the identity on $Z/Z_0$ since $\alpha \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(S)$, and on $Z_0$ and $S/A$ since $\mu(\alpha) = (1, 1)$. In particular, $\alpha|_Z = \mathrm{Id}$ by lemma A.1, and $\alpha|_A$ is $\mathbb{Z}_p\mathbf{U}$-linear.

Fix $x \in S \smallsetminus A$, and let $\psi \in \mathrm{End}(A)$ be the homomorphism $\psi(g) = [g, x]$. Then $\psi$ commutes with $\alpha|_A$ since $\alpha(x) \in xA$, and $\psi$ induces an injection from $Z_i(S)/Z_{i-1}(S)$ into $Z_{i-1}(S)/Z_{i-2}(S)$ for each $i \geqslant 2$. Since $\alpha|_Z = \mathrm{Id}$, this shows that $\alpha$ induces the identity on $Z_i(S)/Z_{i-1}(S)$ for each $i$, and hence that $\alpha|_{Z_i(S)} = \mathrm{Id}$ for each $i$ by lemma A.1 again. Thus $\alpha|_{\Omega_1(A)} = \mathrm{Id}$ since $\Omega_1(A) \leqslant Z_i(S)$ for some $i$, so $\alpha|_{\Omega_m(A)} = \mathrm{Id}$ for each $m \geqslant 1$ by [**20**, theorem 5.2.4]. So $\alpha|_A = \mathrm{Id}$, and $\alpha = \mathrm{Id}_S$ by lemma A.1 again.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

**(b)** This proof is essentially the same as that of [15, lemma 2.6(b)] (a similar result but with $|A| < \infty$). We sketch an alternative argument here.

Set $K = N_{\mathrm{Aut}_{\mathcal{F}}^{\vee}(S)}(Q)$ for short. By the Frattini argument and since all members of the $\mathrm{Aut}(S)$-orbit of $Q$ are $S$-conjugate to $Q$ (lemma 5.4), $\mathrm{Aut}_{\mathcal{F}}^{\vee}(S) = \mathrm{Inn}(S){\cdot}K$. Hence $\mu(K) \geqslant \Delta_t$. Also, $|N_{\mathrm{Inn}(S)}(Q)| \leqslant |N_S(Q)/Z| < \infty$ since $|N_S(Q)/Q| = p$ by lemma 2.2, and $N_{\mathrm{Inn}(S)}(Q) = \mathrm{Aut}_{N_S(Q)}(S)$ is normal of index prime to $p$ in $K$ since $\mathrm{Inn}(S) \trianglelefteq \mathrm{Aut}_{\mathcal{F}}(S)$ has finite index prime to $p$ by the Sylow axiom.

By the Schur-Zassenhaus theorem, there is $K_0 < K$ of order prime to $p$ such that $K = K_0{\cdot}\mathrm{Aut}_{N_S(Q)}(S)$. Set $\widetilde{Z} = C_Q(K_0)$ and $\widetilde{Q} = [K_0, Q]$.

- If $Q \in \mathcal{H}$ and $\mu(K_0) = \mu(K) \geqslant \Delta_{-1}$, then $K_0$ acts nontrivially on $Q/Z$ and on $Z_0$, and trivially on $Z/Z_0$. Hence $\widetilde{Z} \leqslant Z$ and $\widetilde{Q} \cap A = Z_0$. Also, $Q = \widetilde{Z} \times \widetilde{Q}$ and $Z = \widetilde{Z} \times Z_0$ by [20, theorem 5.2.3] (applied to the subgroups $\Omega_m(Q)$ for $m \geqslant 1$), and $\widetilde{Q} \cong C_p \times C_p$ since $S$ splits over $A$. In particular, $\mathrm{Out}(\widetilde{Q}) \cong GL_2(p)$.

  If $\beta \in K_0$ is such that $\mu(\beta)$ generates $\Delta_{-1}$, then $\mu(\beta) = (r, r^{-1})$ for some generator $r$ of $(\mathbb{Z}/p)^{\times}$, so $\beta|_{\widetilde{Q}}$ acts on $\widetilde{Q} \cong C_p \times C_p$ as the matrix $\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right)$ for an appropriate choice of basis. Thus $\mathrm{Aut}_S(\widetilde{Q})\langle \beta|_{\widetilde{Q}} \rangle = N_{O^{p'}(\mathrm{Aut}(\widetilde{Q}))}(Z_0)$ where $O^{p'}(\mathrm{Aut}(\widetilde{Q})) \cong SL_2(p)$, proving (iii) in this case.

- If $Q \in \mathcal{B}$ and $\mu(K_0) = \mu(K) \geqslant \Delta_0$, then $\alpha$ acts nontrivially on $Q/Z_2$, and trivially on $Z_0$ and $Z/Z_0$. Hence $\alpha$ acts trivially on $Z$ by lemma A.1, nontrivially on $Z_2/Z$, and so $\widetilde{Z} = Z$ and $\widetilde{Q} \cap A = Z_2 \cap S'$. Also, $\widetilde{Q}$ is extraspecial of order $p^3$ and (since $S$ splits over $A$) exponent $p$. In particular, $\mathrm{Out}(\widetilde{Q}) \cong GL_2(p)$. By [20, theorem 5.2.3], applied to the abelian $p$-groups $\Omega_m(Q/Z_0)$ for $m \geqslant 1$, $Q = \widetilde{Z}\widetilde{Q}$ and $\widetilde{Z} \cap \widetilde{Q} = Z_0$.

  If $\beta \in K_0$ is such that $\mu(\beta)$ generates $\Delta_0$, then $\mu(\beta) = (r, 1)$ for some generator $r$ of $(\mathbb{Z}/p)^{\times}$, so $[\beta|_{\widetilde{Q}}]$ has order $(p-1)$ in $O^{p'}(\mathrm{Aut}(\widetilde{Q}))/\mathrm{Inn}(\widetilde{Q}) \cong SL_2(p)$. So $\mathrm{Aut}_S(\widetilde{Q})\langle \beta|_{\widetilde{Q}} \rangle = N_{O^{p'}(\mathrm{Aut}(\widetilde{Q}))}(Q \cap A)$ in this case, again proving (iii).

Since $\widetilde{Z} \leqslant Z \leqslant C_Q(N_S(Q))$ and $\widetilde{Q} \geqslant Q \cap S' \geqslant [N_S(Q), Q]$ in all cases, we have $\widetilde{Z} = C_Q(K)$ and $\widetilde{Q} = [K, Q]$. Thus $\widetilde{Z}$ and $\widetilde{Q}$ are independent of the choice of $K_0$, and are normalized by $K = N_{\mathrm{Aut}_{\mathcal{F}}^{\vee}(S)}(Q)$. Since $\mathrm{Aut}_{\mathcal{F}}^{\vee}(S)$ is normal in $\mathrm{Aut}_{\mathcal{F}}(S)$ (the kernel of a homomorphism to $\mathrm{Aut}(Z/Z_0)$), we see that $K$ is normal in $N_{\mathrm{Aut}_{\mathcal{F}}(S)}(Q)$, and hence $\widetilde{Z}$ and $\widetilde{Q}$ are also normalized by $N_{\mathrm{Aut}_{\mathcal{F}}(S)}(Q)$. These are easily seen to be the unique subgroups that satisfy the required conditions. □

When $\mathcal{F}$ is a fusion system over a discrete $p$-toral group $S$, then for each $Q \leqslant S$, we define another subgroup $Q^{\bullet} \leqslant S$ as follows. Let $T$ be the identity component of $S$. If $m \geqslant 0$ is the smallest integer such that $g^{p^m} \in T$ for each $g \in S$, and $Q^{[m]} = \mho^m(Q) = \langle g^{p^m} \mid g \in Q \rangle$, then $Q^{\bullet} \overset{\mathrm{def}}{=} Q{\cdot}I(Q^{[m]})_0$, where $I(Q^{[m]}) = C_T(C_{\mathrm{Aut}_{\mathcal{F}}(T)}(Q^{[m]}))$ and $I(Q^{[m]})_0$ is its identity component. Thus $Q \leqslant Q^{\bullet} \leqslant QT$ for each $Q$. See [10, definition 3.1] or [11, definition 3.1] for more detail, as well as the motivation for this construction.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Lemma 5.10. *Assume the notation and hypotheses of 2.1, and also that $|A| = \infty$. For each $Q \in \mathcal{B} \cup \mathcal{H} \cup \{A, S\}$, $Q^\bullet = Q$.*

*Proof.* By proposition 5.7, $A$ is the identity component of $S$. Thus $A$ and $G$ play the role of $T$ and $W = \mathrm{Aut}_{\mathcal{F}}(T)$ in [**11**, definition 3.1]. Since $Q \leqslant Q^\bullet \leqslant QA$ for each $Q \leqslant S$, we have $A^\bullet = A$ and $S^\bullet = S$.

Now assume $Q \in \mathcal{H} \cup \mathcal{B}$. By assumption, $S/A$ has exponent $p = p^1$. Since $Q/Z \cong C_p$ or $C_p^2$ (lemma 2.5), $Q^{[1]} \overset{\mathrm{def}}{=} \langle g^p \mid g \in Q \rangle \leqslant Z$. Hence $C_G(Q^{[1]}) \geqslant \mathbf{U}$, and $I(Q^{[1]}) \overset{\mathrm{def}}{=} C_A(C_G(Q^{[1]})) \leqslant C_A(\mathbf{U}) = Z$. It follows that $Q^\bullet \leqslant Q{\cdot}I(Q^{[1]}) = Q$. □

We are now ready to prove our main theorem used to construct simple fusion systems over infinite discrete $p$-toral groups with an abelian subgroup of index $p$.

Theorem 5.11. *Fix an odd prime $p$. Let $S$ be an infinite nonabelian discrete $p$-toral group which contains an abelian subgroup $A \trianglelefteq S$ of index $p$, and let $\mathcal{F}$ be a simple fusion system over $S$. Assume notations 2.1 and 2.9 (where the uniqueness of $A$ follows from corollary 5.2). Then the following hold:*

(a) $\mathbf{U} \in \mathrm{Syl}_p(G)$ *and $S$ splits over $A$.*

(b) *$A$ is a discrete $p$-torus of rank at least $p-1$, $Z_0 = C_A(\mathbf{U}) \cap [\mathbf{U}, A]$ has order $p$, and $A = C_A(\mathbf{U}){\cdot}[\mathbf{U}, A]$.*

(c) *There are no non-trivial $G$-invariant subgroups of $Z = C_A(\mathbf{U})$, aside (possibly) from $Z_0$.*

(d) *Either*
   (i) $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{H}$, $\mathrm{rk}(A) = p-1$, $\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}}(A)) \geqslant \Delta_{-1}$, *and* $G = O^{p'}(G){\cdot}\mu_A^{-1}(\Delta_{-1})$; *or*

   (ii) $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{B}$, $\mathrm{rk}(A) \geqslant p-1$, $\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}}(A)) \geqslant \Delta_0$, $\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}}(A)) = \Delta_0$ *if* $\mathrm{rk}(A) \geqslant p$, $G = O^{p'}(G){\cdot}\mu_A^{-1}(\Delta_0)$, *and $Z_0$ is not $G$-invariant.*

   *Here, we regard $\mu_A$ as a homomorphism defined on* $\mathrm{Aut}^\vee_{\mathcal{F}}(A)$.

*Conversely, let $S$ be an infinite discrete $p$-toral group containing a unique abelian subgroup $A \trianglelefteq S$ of index $p$, let $G \leqslant \mathrm{Aut}(A)$ be such that $\mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$, and adopt the notation in 2.1 and 2.9. Assume that (a)–(d) hold, with $\mathrm{Aut}^\vee_{\mathcal{F}}(A)$ replaced by $G \cap \mathrm{Aut}^\vee(A)$ and $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$ replaced by $\mathbf{E}_0 = \mathcal{H}$ or $\mathcal{B}$ in (d). Then there is a unique simple fusion system $\mathcal{F}$ over $S$ such that $G = \mathrm{Aut}_{\mathcal{F}}(A)$ and $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathbf{E}_0$.*

*Proof.* We prove in Steps 1 and 3 that conditions (a)–(d) are necessary, and prove the converse in Step 2.

**Step 1:** Assume that $\mathcal{F}$ is a simple fusion system over $S$. We must show that conditions (a)–(d) hold. By corollary 5.2, $A$ is the unique abelian subgroup of index $p$ in $S$.

**(a,b,c)** Point (a) holds by corollary 2.6 and since $A$ is fully automized. The last two statements in (b) hold by lemmas 2.4 and 5.4, and (c) holds by lemma 2.7 and since $O_p(\mathcal{F}) = 1$. Finally, $A$ is a discrete $p$-torus by proposition 5.7, and $\mathrm{rk}(A) \geqslant p-1$ by lemma 5.3.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

**(d)** Since $A \ntrianglelefteq \mathcal{F}$, there is $P \in \mathbf{E}_{\mathcal{F}} \cap (\mathcal{H} \cup \mathcal{B})$. Set $t = 0$ if $P \in \mathcal{B}$, and $t = -1$ if $P \in \mathcal{H}$.

Set $H = \mathrm{Aut}_{\mathcal{F}}(P)$ and $H_0 = O^{p'}(H)$. By lemma 2.5, $H_0/\mathrm{Inn}(P) \cong SL_2(p)$, and acts trivially on $Z/Z_0$. Since $\mathrm{Aut}_S(P) \in \mathrm{Syl}_p(H) = \mathrm{Syl}_p(H_0)$, we can choose $\alpha \in N_{H_0}(\mathrm{Aut}_S(P))$ of order $p-1$ in $H/\mathrm{Inn}(P)$. By the extension axiom, $\alpha$ extends to an element of $\mathrm{Aut}_{\mathcal{F}}(N_S(P))$, and since $P$ is maximal among $\mathcal{F}$-essential subgroups by lemmas 2.2 and 2.3, $\alpha = \widehat{\alpha}|_P$ for some $\widehat{\alpha} \in \mathrm{Aut}_{\mathcal{F}}(S)$. Set $\alpha_0 = \widehat{\alpha}|_A \in G$.

Now, $\alpha_0$ induces the identity on $Z/Z_0$ since $\alpha$ does, and $\alpha_0 \in N_G(\mathbf{U})$ since it extends to $S$. Thus $\alpha_0 \in \mathrm{Aut}^{\vee}_{\mathcal{F}}(A)$. By lemma 2.5, $\alpha$ acts as an element of $SL_2(p)$ on $P/Z \cong C_p^2$ (if $P \in \mathcal{B}$) or on $P/P_1 \cong C_p^2$ where $Z = P_1 \times Z_0$ (if $P \in \mathcal{H}$). Hence for some $s \in (\mathbb{Z}/p)^{\times}$ of order $p-1$, $\mu_A(\alpha_0) = (s, s^{-1})$ if $P \in \mathcal{H}$, or $\mu_A(\alpha_0) = (s, 1)$ if $P \in \mathcal{B}$. Thus $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)) \geqslant \Delta_t$ in either case.

Assume $\mathrm{rk}(A) \geqslant p$. By proposition 5.7, $Z$ is a discrete $p$-torus. Hence each element of $\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)$ induces the identity on $Z_0$ since it induces the identity on $Z/Z_0$, and $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)) \leqslant \Delta_0$.

Set $G_0 = O^{p'}(G){\cdot}\mu_A^{-1}(\Delta_t)$. Since $\mathrm{Ker}(\mu_A|_{\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)}) = \mathbf{U}$ by lemma 5.9(a), and since $\mu_A(\mathrm{Aut}^{\vee}_{\mathcal{F}}(A)) \geqslant \Delta_t$ by assumption, we have $G \geqslant \mu_A^{-1}(\Delta_t)$, and hence $G \geqslant G_0$. We will show in Step 3 (with the help of the constructions in Step 2) that $G = G_0$, thus finishing the proof of (d).

**Step 2:** Now assume that $S$, $A$, and $G$ are as above, and set $G^{\vee} = G \cap \mathrm{Aut}^{\vee}(A)$. Assume that (a) and (b) hold, and also that $\mu_A(G^{\vee}) \geqslant \Delta_t$ for some $t \in \{0, -1\}$. (Note that $G^{\vee} \leqslant N_G(\mathbf{U})$ since each element is the restriction of an automorphism of $S$.) We must show that these are realized by a unique saturated fusion system $\mathcal{F}$, which is simple if (c) and (d) hold. Set $\mathbf{E}_0 = \mathcal{H}$ if $t = -1$, or $\mathbf{E}_0 = \mathcal{B}$ if $t = 0$.

Set $\Gamma = A \rtimes G$, and identify $S = A \rtimes \mathbf{U} \in \mathrm{Syl}_p(\Gamma)$. Choose a generator $\mathbf{x} \in \mathbf{U} < S$. Set $Z = Z(S)$, $Z_2 = Z_2(S)$, as in notation 2.1.

Set $Q = Z\langle \mathbf{x} \rangle$ if $\mathbf{E}_0 = \mathcal{H}$, or $Q = Z_2\langle \mathbf{x} \rangle$ if $\mathbf{E}_0 = \mathcal{B}$. Thus $Q \in \mathbf{E}_0$, and each member of $\mathbf{E}_0$ is $S$-conjugate to $Q$ by lemma 5.4. Set $K = \mathrm{Aut}_{\Gamma}(Q)$. By assumption, there is $\alpha \in N_{G^{\vee}}(\mathbf{U})$ such that $\mu_A(\alpha)$ generates $\Delta_t$, and $\alpha$ extends to some $\bar{\alpha} \in \mathrm{Aut}^{\vee}(S)$ such that $\bar{\alpha}(\mathbf{x}) \in \mathbf{U}$. In particular, $\bar{\alpha}(Q) = Q$, and $\bar{\alpha} \in \mathrm{Aut}_{\Gamma}(S)$.

By lemma 5.9(b), applied with $\mathcal{F}_S(\Gamma)$ in the role of $\mathcal{F}$, there are unique subgroups $\widetilde{Z} \leqslant Z$ and $\widetilde{Q} \geqslant Q \cap S'$, both normalized by $N_{\mathrm{Aut}_{\Gamma}(S)}(Q)$, and such that $Q = \widetilde{Z} \times \widetilde{Q}$ and $\widetilde{Q} \cong C_p \times C_p$ if $Q \in \mathcal{H}$; or $\widetilde{Z} = Z$, $Q = Z\widetilde{Q}$, $Z \cap \widetilde{Q} = Z_0$, and $\widetilde{Q}$ is extraspecial of order $p^3$ and exponent $p$ if $Q \in \mathcal{B}$. Let $\Theta \leqslant \mathrm{Aut}(Q)$ be the unique subgroup containing $\mathrm{Inn}(Q)$ that acts trivially on $\widetilde{Z}$, normalizes $\widetilde{Q}$, and is such that $\Theta/\mathrm{Inn}(Q) \cong SL_2(p)$.

We next claim that

(1) each $\alpha \in \mathrm{Aut}_{\Gamma}(Q)$ extends to some $\bar{\alpha} \in N_{\mathrm{Aut}_{\Gamma}(S)}(Q)$;

(2) $\mathrm{Aut}_{\Gamma}(Q)$ normalizes $\Theta$;

(3) $\mathrm{Aut}_S(Q) \in \mathrm{Syl}_p(\Theta) = \mathrm{Syl}_p(\Theta\mathrm{Aut}_{\Gamma}(Q))$; and

(4) $N_{\Theta}(\mathrm{Aut}_S(Q)) \leqslant \mathrm{Aut}_{\Gamma}(Q)$.

Point (1) holds since $S = QA$ where $A \trianglelefteq \Gamma$, and hence $N_{\Gamma}(Q) \leqslant N_{\Gamma}(S)$. By assumption, each element of $N_{\mathrm{Aut}_{\Gamma}(S)}(Q)$ normalizes $\widetilde{Z}$ and $\widetilde{Q}$, and hence normalizes $\Theta$.

Thus (2) follows from (1). Since $|\mathrm{Out}_S(Q)| = |N_S(Q)/Q| = p$ by lemma 2.2, this acts trivially on $Z \geqslant \widetilde{Z}$ and normalizes $\widetilde{Q}$, and $\mathrm{Out}(\widetilde{Q}) \cong GL_2(p)$ where $\mathrm{Syl}_p(GL_2(p)) = \mathrm{Syl}_p(SL_2(p))$, we see that $\mathrm{Out}_S(Q) \in \mathrm{Syl}_p(\Theta/\mathrm{Inn}(Q))$ and hence that $\mathrm{Aut}_S(Q) \in \mathrm{Syl}_p(\Theta)$. Also, $\Theta$ has index prime to $p$ in $\Theta\mathrm{Aut}_\Gamma(Q)$ since $\mathrm{Aut}_S(Q) \in \mathrm{Syl}_p(\mathrm{Aut}_\Gamma(Q))$, and this proves (3). Finally, (4) follows from lemma 5.9(b.iii).

Set $\mathcal{F} = \langle \mathcal{F}_S(\Gamma), \Theta\rangle$: the smallest fusion system over $S$ which contains $\mathcal{F}_S(\Gamma)$ and such that $\mathrm{Aut}_\mathcal{F}(Q) \geqslant \Theta$. Set $\mathcal{K} = \{S, A\} \cup \mathbf{E}_0$. Then $\mathcal{K}$ is invariant under $\mathcal{F}$-conjugacy, and is closed in the space of all subgroups of $S$ [**11**, definition 1.11]. Thus condition (i) in [**11**, theorem 4.2] holds for $\mathcal{K}$; and condition (iii) holds ($P \in \mathcal{K}$ and $P \leqslant Q \leqslant P^\bullet$ imply $Q \in \mathcal{K}$) since $P = P^\bullet$ for each $P \in \mathcal{K}$ (lemma 5.10).

By lemma 2.3, if $\mathbf{E}_0 = \mathcal{B}$, then the members of $\mathcal{H}$ are not $\mathcal{F}$-centric. So in all cases, if $P \leqslant S$ is $\mathcal{F}$-centric and $P \notin \mathcal{K}$, then $P$ is not contained in any member of $\mathbf{E}_\mathcal{F} = \mathbf{E}_0 \cup \{A\}$, and hence $\mathrm{Out}_S(P) \trianglelefteq \mathrm{Out}_\mathcal{F}(P)$. This proves condition (iv) in [**11**, theorem 4.2]:

$$O_p(\mathrm{Out}_\mathcal{F}(P)) \cap \mathrm{Out}_S(P) \neq 1$$

whenever $P \leqslant S$ is $\mathcal{F}$-centric and not in $\mathcal{K}$.

We refer to [**11**, definition 1.11] for the definitions of '$\mathcal{K}$-generated' and '$\mathcal{K}$-saturated'. By construction, $\mathcal{F}$ is $\mathcal{K}$-generated. To show that $\mathcal{F}$ is $\mathcal{K}$-saturated, we must prove that each $P \in \mathcal{K}$ is fully automized and receptive in $\mathcal{F}$ (definition 1.1). If $P = A$ or $P = S$, then $\mathrm{Aut}_\mathcal{F}(P) = \mathrm{Aut}_\Gamma(P)$, and this is easily checked. So it remains to show this when $P = Q$. By (2), $\mathrm{Aut}_\mathcal{F}(Q) = \Theta{\cdot}\mathrm{Aut}_\Gamma(Q)$. So $Q$ is fully automized by (3). If $\alpha \in N_{\mathrm{Aut}_\mathcal{F}(Q)}(\mathrm{Aut}_S(Q))$, then $\alpha \in \mathrm{Aut}_\Gamma(Q)$ by (4), and hence extends to some $\bar{\alpha} \in \mathrm{Aut}_\Gamma(S)$ by (1). So $Q$ is also receptive. This finishes the proof of condition (ii) in [**11**, theorem 4.2], and hence $\mathcal{F}$ is saturated by that theorem.

Now assume (c) and (d) hold; we must prove that $\mathcal{F}$ is simple. By (c), there are no non-trivial $G$-invariant subgroups of $Z$ except possibly for $Z_0$. Also, $\mathbf{E}_\mathcal{F} \supseteq \mathcal{H}$ in case (d.i), and $Z_0$ is not $G$-invariant in case (d.ii). Hence $O_p(\mathcal{F}) = 1$ by lemma 2.7. By lemma 5.8, $\mathcal{F}$ is simple if there are no proper normal fusion subsystems in $\mathcal{F}$ over $S$.

Assume $\mathcal{F}_0 \trianglelefteq \mathcal{F}$ is a normal fusion subsystem over $S$, and set $G_0 = \mathrm{Aut}_{\mathcal{F}_0}(A)$. Then $G_0 \trianglelefteq G$, and $G_0 \geqslant O^{p'}(G)$ since it is the normal closure of $\mathbf{U} = \mathrm{Aut}_S(A)$. Also, $\mu_A(\mathrm{Aut}^\vee_{\mathcal{F}_0}(A)) \geqslant \Delta_t$ by Step 1, applied with $\mathcal{F}_0$ in the role of $\mathcal{F}$. Since $\mu_A$ is injective on $G^\vee/\mathrm{Aut}_S(A)$ by lemma 5.9(a), we have $G_0 \geqslant O^{p'}(G){\cdot}\mu_A^{-1}(\Delta_t) = G$. Thus $G_0 = G$, and $\mathrm{Aut}_{\mathcal{F}_0}(S) = \mathrm{Aut}_\mathcal{F}(S)$ by the extension axiom, so $\mathcal{F}_0 = \mathcal{F}$ by the Frattini condition on a normal subsystem (see definition 1.4). This finishes the proof that $\mathcal{F}$ is simple.

The uniqueness of $\mathcal{F}$ follows from the uniqueness of $\widetilde{Z}$ and $\widetilde{Q}$ in lemma 5.9(b).

**Step 3:** We return to the situation of Step 1, where it remains only to prove that $G_0 = G$. By Step 2, there is a unique saturated fusion subsystem $\mathcal{F}_0 \leqslant \mathcal{F}$ over $S$ such that $\mathbf{E}_{\mathcal{F}_0} = \mathbf{E}_\mathcal{F}$ and $\mathrm{Aut}_{\mathcal{F}_0}(A) = G_0$. The invariance condition on $\mathcal{F}_0 \leqslant \mathcal{F}$ (definition 1.4) holds by the uniqueness of $\mathcal{F}_0$, and the Frattini condition holds since $G = O^{p'}(G)N_G(\mathbf{U}) \leqslant G_0N_G(\mathbf{U})$ (where each element of $N_G(\mathbf{U})$ extends to an element of $\mathrm{Aut}_\mathcal{F}(S)$ by the extension axiom). Thus $\mathcal{F}_0 \trianglelefteq \mathcal{F}$, so $\mathcal{F}_0 = \mathcal{F}$ since $\mathcal{F}$ is simple, and hence $G_0 = G$. □

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

As a special case, we next show that for each prime $p$, there is (up to isomorphism) a unique simple fusion system over an infinite discrete $p$-toral group with an abelian subgroup of index $p$ which is not essential.

Theorem 5.12. *For each odd prime $p$, there is, up to isomorphism, a unique simple fusion system $\mathcal{F}$ over an infinite nonabelian discrete $p$-toral group $S$ which contains an abelian subgroup $A < S$ of index $p$ that is not $\mathcal{F}$-essential. The following hold for each such $p$, $\mathcal{F}$, $S$, and $A$:*

(a) *The group $A$ is a discrete $p$-torus of rank $p-1$, and $S$ splits over $A$. Also, $\mathrm{Aut}_{\mathcal{F}}(A) \cong C_p \rtimes C_{p-1}$, $\mathrm{Out}_{\mathcal{F}}(S) \cong C_{p-1}$, and $\mathbf{E}_{\mathcal{F}} = \mathcal{H}$ (defined as in notation 2.1).*

(b) *Fix a prime $q \neq p$, set $\Gamma = PSL_p(\bar{\mathbb{F}}_q)$, let $\widetilde{A} < \Gamma$ be the subgroup of classes of diagonal matrices of $p$-power order, and set $\widetilde{S} = \widetilde{A}\langle\widetilde{x}\rangle \in \mathrm{Syl}_p(\Gamma)$ for some permutation matrix $\widetilde{x}$ of order $p$. Then there is an isomorphism $S \cong \widetilde{S}$ that restricts to an isomorphism $A \cong \widetilde{A}$, and induces isomorphisms $\mathrm{Aut}_{\mathcal{F}}(S) \cong \mathrm{Aut}_{\Gamma}(\widetilde{S})$ and $\mathrm{Aut}_{\mathcal{F}}(A) \cong \mathrm{Aut}_{N_{\Gamma}(\widetilde{S})}(\widetilde{A})$.*

(c) *If $p = 3$, then $\mathcal{F}$ is isomorphic to the 3-fusion system of $PSU(3)$, and also to the 3-fusion system of $PSL_3(\bar{\mathbb{F}}_q)$ for each prime $q \neq 3$. For $p \geqslant 5$, $\mathcal{F}$ is not realized by any compact Lie group, nor by any $p$-compact group.*

*Proof.* We use the notation of 2.1 and 2.9. In particular, $G = \mathrm{Aut}_{\mathcal{F}}(A)$.
**(a,b)** Assume $\mathcal{F}$ is a simple fusion system over an infinite discrete $p$-toral group $S$ with an abelian subgroup $A < S$ of index $p$ such that $A \notin \mathbf{E}_{\mathcal{F}}$. By lemma 5.5, $Z = Z_0$, $\mathbf{E}_{\mathcal{F}} = \mathcal{H}$, and $A = S'$ is a discrete $p$-torus of rank $p-1$. In particular, $|Z| = |Z_0| = p$. Also, $S$ splits over $A$ by corollary 2.6.

It remains to describe $G = \mathrm{Aut}_{\mathcal{F}}(A)$ and $\mathrm{Aut}_{\mathcal{F}}(S)$ and prove (b). Since $A \notin \mathbf{E}_{\mathcal{F}}$, $\mathbf{U} \trianglelefteq G$, and $\mathrm{Out}_{\mathcal{F}}(S) \cong G/\mathbf{U}$. (Each $\alpha \in \mathrm{Aut}_{\mathcal{F}}(A)$ extends to $\mathrm{Aut}_{\mathcal{F}}(S)$ by the extension axiom.)

Since $S$ splits over $A$, each $\alpha \in N_{\mathrm{Aut}(A)}(\mathbf{U})$ extends to an automorphism of $S$. Since $Z = Z_0$, this implies that $N_{\mathrm{Aut}(A)}(\mathbf{U}) = \mathrm{Aut}^{\vee}(A)$. Also, $\mu_A(G) = \Delta_{-1}$ by theorem 5.11(d) and since $O^{p'}(G) = \mathbf{U} \leqslant \mathrm{Ker}(\mu_A)$.

Let $R = \mathbb{Z}_p[\zeta]$ and $\mathfrak{p} = (1-\zeta)R$ be as in notation 4.6, regarded as $\mathbb{Z}_p\mathbf{U}$-modules. By proposition A.4, $A \cong (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda$ and $\Lambda \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A)$ for some $(p-1)$-dimensional $\mathbb{Z}_pG$-lattice $\Lambda$, and $\Lambda|_{\mathbf{U}} \cong R$ as $\mathbb{Z}_p\mathbf{U}$-modules by lemma A.5(c). These isomorphisms induce isomorphisms of automorphism groups

$$\begin{aligned}\mathrm{Aut}^{\vee}(A) = N_{\mathrm{Aut}(A)}(\mathbf{U}) &\cong N_{\mathrm{Aut}(R)}(\mathbf{U}) \cong C_{\mathrm{Aut}(R)}(\mathbf{U}) \rtimes \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\\ &\cong R^{\times} \rtimes \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\\ &\cong \big((1+\mathfrak{p}) \times \mathbb{F}_p^{\times}\big) \rtimes \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p),\end{aligned}$$

and these send $\mathrm{Ker}(\mu_A) \leqslant \mathrm{Aut}^{\vee}(A)$ (the group of automorphisms of $A$ that commute with $\mathbf{U}$ and are the identity on $Z = Z_0$) onto $1+\mathfrak{p}$, and send the subgroup $\mathrm{sc}(\mathbb{F}_p^{\times}) \leqslant \mathrm{Aut}^{\vee}(A)$ of scalar multiplication by $(p-1)$-st roots of unity onto $\mathbb{F}_p^{\times}$.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Thus

$$\mathrm{Aut}^{\vee}(A) = N_{\mathrm{Aut}(A)}(\mathbf{U}) = \big(\mathrm{Ker}(\mu_A) \times \mathrm{sc}(\mathbb{F}_p^{\times})\big) \rtimes W$$

for a certain subgroup $W \cong C_{p-1}$. Set $\overline{G} = (\mathbf{U} \times \mathrm{sc}(\mathbb{F}_p^{\times}))\cdot W < \mathrm{Aut}^{\vee}(A)$: a subgroup of order $p(p-1)^2$.

Since $\mathrm{Aut}^{\vee}(A)/\mathrm{Ker}(\mu_A)$ has order $(p-1)^2$, and since $\mathrm{Ker}(\mu_A) \cong (1+\mathfrak{p})$ is an abelian pro-$p$-group and hence uniquely $m$-divisible for each $m$ prime to $p$, we have $H^i(H;\mathrm{Ker}(\mu_A)) = 0$ for each $H \leqslant \mathrm{Aut}^{\vee}(A)/\mathrm{Ker}(\mu_A)$ and each $i > 0$. Hence for each subgroup $K < \mathrm{Aut}^{\vee}(A)$ of order prime to $p$, $K \cap \mathrm{Ker}(\mu_A) = 1$ since $\mathrm{Ker}(\mu_A)$ is a pro-$p$-group, $\mathrm{Ker}(\mu_A)\cdot K$ splits over $\mathrm{Ker}(\mu_A)$ with a splitting unique up to conjugacy, and thus $K$ is conjugate by an element of $\mathrm{Ker}(\mu_A)$ to a subgroup of $\mathrm{sc}(\mathbb{F}_p^{\times})\cdot W$. In particular, $G$ is conjugate to a subgroup of $\overline{G}$, and we can assume (without changing the isomorphism type of $\mathcal{F}$) that $G \leqslant \overline{G}$. Finally, one easily sees that $\mu_A$ sends $\overline{G}$ onto $\Delta$ with kernel $\mathbf{U}$, and hence that $G = (\mu_A|_{\overline{G}})^{-1}(\Delta_{-1}) \cong C_p \rtimes C_{p-1}$ is uniquely determined.

A natural isomorphism $A \cong \widetilde{A}$ is most easily seen by identifying $\Gamma = PGL_p(\overline{\mathbb{F}}_q)$, so that $\widetilde{A}$ is the quotient of $(\mathbb{Z}/p^{\infty})^p$ by the diagonal $\mathbb{Z}/p^{\infty} \cong O_p(Z(\Gamma))$, with the permutation action of $\mathrm{Aut}_{\Gamma}(\widetilde{A}) \cong \Sigma_p$. This then extends to an isomorphism of $S \cong A \rtimes \mathbf{U}$ with $\widetilde{S} = \widetilde{A}\langle\widetilde{x}\rangle$, and of $\mathrm{Aut}_{\mathcal{F}}(A)$ with $\mathrm{Aut}_{N_{\Gamma}(\widetilde{S})}(\widetilde{A})$.

**Existence and uniqueness of $\mathcal{F}$:** Let $A$, $\mathbf{U} \trianglelefteq G$, and $S = A \rtimes \langle x\rangle$ be as described in the proof of (b). Since $\mu_A(G) = \Delta_{-1}$, conditions (a)–(d) in theorem 5.11 all hold with $\mathbf{E}_{\mathcal{F}} = \mathcal{H}$. So such an $\mathcal{F}$ exists by that theorem. It is unique up to isomorphism by the uniqueness in the theorem and by the restrictions shown in the proof of (b).

**(c)** If $\mathcal{F}$ is realized by a compact Lie group or a $p$-compact group, then by proposition 1.5 and since all elements in $S$ are $\mathcal{F}$-conjugate to elements in $A$, $\mathcal{F}$ is realized by a connected, simple $p$-compact group, and the action of the Weyl group $\mathrm{Aut}_{\mathcal{F}}(A)$ on $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by pseudoreflections. But if $p \geqslant 5$, then $\mathrm{Aut}_{\mathcal{F}}(A) \cong C_p \rtimes C_{p-1}$ contains no pseudoreflections other than the identity. So $p = 3$, and we easily check that $\mathcal{F}$ is realized by $PSU(3)$, or by $PSL_3(\overline{\mathbb{F}}_q)$ for $q \neq 3$. □

We can now describe the simple fusion systems over discrete $p$-toral groups with discrete $p$-torus of index $p$ in terms of the classification of certain faithful, minimally active, indecomposable modules carried out in [15].

Theorem B. *Fix an odd prime $p$.*

(a) *Let $\mathcal{F}$ be a simple fusion system over an infinite nonabelian discrete $p$-toral group $S$ with an abelian subgroup $A < S$ of index $p$. Assume also that $A$ is $\mathcal{F}$-essential. Set $G = \mathrm{Aut}_{\mathcal{F}}(A)$ and $V = \Omega_1(A)$, let $\mathcal{H}$ and $\mathcal{B}$ be as in notation 2.1, and let $G^{\vee} = \mathrm{Aut}_{\mathcal{F}}^{\vee}(A)$ and $\mu_A \colon G^{\vee} \longrightarrow \Delta$ be as in notation 2.9. Then*

*$A$ is a discrete $p$-torus, $S$ splits over $A$, $G \in \mathscr{G}_p^\wedge$, and for some $t \in \{0, -1\}$,*

$$\text{\textit{$V$ is a faithful, minimally active, indecomposable $\mathbb{F}_pG$-module. Either $\dim(V) = p-1$, $\mu_A(G^\vee) \geqslant \Delta_t$ and $G = O^{p'}(G)\mu_A^{-1}(\Delta_t)$; or $\dim(V) \geqslant p$, $t=0$, $\mu_A(G^\vee) = \Delta_0$, and $G = O^{p'}(G){\cdot}G^\vee$. Also, $\mathbf{E}_\mathcal{F} = \{A\} \cup \mathcal{H}$ if $t=-1$, while $\mathbf{E}_\mathcal{F} = \{A\} \cup \mathcal{B}$ if $t=0$. If $t=0$, then $V$ contains no 1-dimensional $\mathbb{F}_pG$-submodule.}} \tag{$*_\infty$}$$

(b) *Conversely, assume that $G \in \mathscr{G}_p^\wedge$, $\mathbf{U} \in \mathrm{Syl}_p(G)$, and $t \in \{0, -1\}$, and that $V$ is an $\mathbb{F}_pG$-module that satisfies $(*_\infty)$, where $G^\vee$ is the subgroup of all elements $\alpha \in N_G(\mathbf{U})$ such that $[\alpha, C_V(\mathbf{U})] \leqslant [\mathbf{U}, V]$. Then there are a discrete $G$-$p$-torus $A$ and a simple fusion system $\mathcal{F}$ over $S = A \rtimes \mathbf{U}$ such that $\mathrm{Aut}_\mathcal{F}(A) = \mathrm{Aut}_G(A) \cong G$, such that $\Omega_1(A) \cong V$ as $\mathbb{F}_pG$-modules, and such that $\mathbf{E}_\mathcal{F} = \{A\} \cup \mathcal{H}$ if $t=-1$, or $\mathbf{E}_\mathcal{F} = \{A\} \cup \mathcal{B}$ if $t=0$. Furthermore, any other simple fusion system with these properties is isomorphic to $\mathcal{F}$.*

(c) *Among the fusion systems specified in (b), the only ones that are realized as fusion systems of compact Lie groups or of $p$-compact groups are those listed in table 5.1.*

*Proof.* **(a)** Set $\mathbf{U} = \mathrm{Aut}_S(A) \in \mathrm{Syl}_p(G)$ and $Z = C_A(\mathbf{U})$.

Under the above assumptions, $A$ is a discrete $p$-torus by proposition 5.7, $G \in \mathscr{G}_p^\wedge$ by lemma 3.2(a), $V$ is faithful, minimally active, and indecomposable by lemma 3.2(b), and $\mathrm{rk}(V) = \mathrm{rk}(A) \geqslant p-1$ by lemma 5.3. Also, for some $t \in \{0, -1\}$, $\mu_A(G^\vee) \geqslant \Delta_t$ and $G = O^{p'}(G)\mu_A^{-1}(\Delta_t)$, and $\mathbf{E}_\mathcal{F}$ is as described in $(*_\infty)$, by theorem 5.11(d). Since $A \ntrianglelefteq \mathcal{F}$, $S$ splits over $A$ by corollary 2.6. If $t=0$ and $V_0 < V$ is a 1-dimensional $\mathbb{F}_pG$-submodule, then $V_0 \leqslant C_V(\mathbf{U}) \leqslant Z$, which is impossible by theorem 5.11(c,d.ii).

Assume $\mathrm{rk}(V) = \mathrm{rk}(A) \geqslant p$. Since $V$ is minimally active and indecomposable, $V|_\mathbf{U}$ is the direct sum of a free module $\mathbb{F}_p\mathbf{U}$ and an $\mathbb{F}_p$-vector space with trivial $\mathbf{U}$-action by lemma 3.3, and hence $\Omega_1(Z) = C_V(\mathbf{U})$ has rank $\mathrm{rk}(A) - p + 1$. Also, $Z$ is a discrete $p$-torus by proposition 5.7, so for each $\alpha \in G^\vee = \mathrm{Aut}_\mathcal{F}^\vee(A)$, $\alpha$ acts via the identity on $Z_0$ since it acts via the identity on $Z/Z_0$ (see notation 2.9). Thus $\mu_A(\alpha) \in \Delta_0$ by definition of $\mu_A$, so $t=0$ and $\mu_A(G^\vee) = \Delta_0$ in this case, finishing the proof of $(*_\infty)$.

**(b)** Fix $G \in \mathscr{G}_p^\wedge$, $\mathbf{U} \in \mathrm{Syl}_p(G)$, and $t \in \{0, -1\}$, and let $V$ be an $\mathbb{F}_pG$-module that satisfies $(*_\infty)$, where $G^\vee$ is the subgroup of all elements $g \in N_G(\mathbf{U})$ such that $[g, C_V(\mathbf{U})] \leqslant [\mathbf{U}, V]$. By proposition 3.8(a), there is a $\mathbb{Z}_pG$-lattice $\Lambda$ such that $\Lambda/p\Lambda \cong V$ as $\mathbb{F}_pG$-modules. Set $A = (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda$: a discrete $G$-$p$-torus where $\Omega_1(A) \cong V$ as $\mathbb{F}_pG$-modules (see proposition A.4). To simplify notation, we identify $V = \Omega_1(A)$. Set $S = A \rtimes \mathbf{U}$. Set $Z = Z(S) = C_A(\mathbf{U})$, $S' = [S, S] = [\mathbf{U}, A]$, and $Z_0 = Z \cap S'$.

We next check that conditions (a)–(d) in theorem 5.11 all hold. Conditions (a) and (d) follow immediately from $(*_\infty)$, and (b) ($|Z_0| = p$) was shown in lemma 3.7(b).

Table 5.1. *The sixth column lists a compact Lie group or a $p$-compact group that realizes the fusion system $\mathcal{F}$ described in the first five columns. Here, $X(m,m,n)$ denotes the $p$-compact group with Weyl group $G(m,m,n)$ in the notation of* [**26**, § *2*], *and $X_k$ the one with Weyl group number $k$ in* [**26**, *table VII*]. *In the last column, we give, in some cases, a torsion linear group that realizes $\mathcal{F}$: $q \neq p$ is prime, $K \subseteq \bar{\mathbb{F}}_2$ is the union of the odd degree extensions of $\mathbb{F}_2$, and $\gamma \in \mathrm{Aut}(F_4(K))$ is a graph automorphism of order 2. In the fourth column, $B.C$ means an extension of $B$ by $C$, and the subscripts in the entry $6_1{\cdot}PSU_4(3).2_2$ are* Atlas *notation* [**13**, *p. 52*].

| $p$ | conditions | $\mathrm{rk}(A)$ | $G = \mathrm{Aut}_{\mathcal{F}}(A)$ | $\mathbf{E}_0$ | $p$-cpct. gp. | tors. lin. gp. |
|---|---|---|---|---|---|---|
| $p$ | $p \geqslant 5$ | $p{-}1$ | $\Sigma_p$ | $\mathcal{H}$ | $PSU(p)$ | $PSL_p(\bar{\mathbb{F}}_q)$ |
| $p$ | $p < n < 2p$ | $n{-}1$ | $\Sigma_n$ | $\mathcal{B}$ | $PSU(n)$ | $PSL_n(\bar{\mathbb{F}}_q)$ |
| $p$ | $p \leqslant n < 2p,\ n \geqslant 4$ | $n$ | $C_2^{n-1} \rtimes \Sigma_n$ | $\mathcal{B}$ | $PSO(2n)$ | $P\Omega_{2n}(\bar{\mathbb{F}}_q)$ |
| $p$ | $2 < m \mid (p-1)$<br>$p \leqslant n < 2p,\ n \geqslant 4$ | $n$ | $(C_m)^{n-1} \rtimes \Sigma_n$ | $\mathcal{B}$ | $X(m,m,n)$ | |
| 5 | $n = 6, 7$ | $n$ | $W(E_n)$ | $\mathcal{B}$ | $E_n$ | $E_n(\bar{\mathbb{F}}_q)$ |
| 7 | $n = 7, 8$ | $n$ | $W(E_n)$ | $\mathcal{B}$ | $E_n$ | $E_n(\bar{\mathbb{F}}_q)$ |
| 3 | | 2 | $GL_2(3)$ | $\mathcal{B}$ | $X_{12}$ | $C_{F_4(K)}(\gamma)$ |
| 5 | | 4 | $(4 \circ 2^{1+4}).\Sigma_5$ | $\mathcal{B}$ | $X_{29}$ | |
| 5 | | 4 | $(4 \circ 2^{1+4}).\Sigma_6$ | $\mathcal{B}$ | $X_{31}$ | $E_8(K)$ |
| 7 | | 6 | $6_1{\cdot}PSU_4(3).2_2$ | $\mathcal{B}$ | $X_{34}$ | |

Assume $1 \neq B \leqslant Z$ is $G$-invariant. If $\mathrm{rk}(A) = p-1$, then $Z = Z_0$ has order $p$, so $B = Z_0$. Otherwise, by $(*_\infty)$, $t = 0$, and $V$ contains no 1-dimensional $\mathbb{F}_pG$-submodule. Thus $\dim(\Omega_1(B)) \geqslant 2$, so $\dim(V) = \mathrm{rk}(A) \geqslant p+1$. If $\dim(V) \geqslant p+2$, then $V$ is simple by [**15**, proposition 3.7(c)], while if $\dim(V) = p+1$, then $V$ contains no nontrivial $\mathbb{F}_pG$-submodule with trivial $\mathbf{U}$-action by lemma 3.5. Thus $B = Z_0$, and this proves condition 5.11(c).

By theorem 5.11, there is a unique simple fusion system $\mathcal{F}$ over $S$ such that $G = \mathrm{Aut}_{\mathcal{F}}(A)$, and $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\} = \mathcal{H}$ (if $t = -1$) or $\mathcal{B}$ (if $t = 0$). Since $A$ is unique (up to isomorphism of $\mathbb{Z}_pG$-modules) by lemma 3.10, this shows that $\mathcal{F}$ is uniquely determined by $V$.

**(c)** If $\mathcal{F}$ is realized by a compact Lie group or a $p$-compact group, then by proposition 1.5 and since all elements in $S$ are $\mathcal{F}$-conjugate to elements in $A$, $\mathcal{F}$ is realized by a connected, simple $p$-compact group, and the action of the Weyl group $G = \mathrm{Aut}_{\mathcal{F}}(A)$ on $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is irreducible as a group generated by pseudoreflections. Using the list of pseudoreflection groups and their realizability over $\mathbb{Q}_p$ compiled by Clark & Ewing [**12**], as well as the assumption that $v_p(|G|) = 1$, we see that $G$ must be one of the groups listed in table 5.1, or else one of the other groups $G(m,d,n)$ (of index $d$ in $C_m \wr \Sigma_n$) for $d \mid m \mid (p-1)$ with $d < m$. The latter are eliminated by the condition $G = O^{p'}(G){\cdot}\mu_A^{-1}(\Delta_0)$ in (d.ii) (i.e., the fusion systems of the corresponding $p$-compact groups are not simple), and so we are left with the groups listed in the table.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Table 5.2. *Summary of the cases in theorem B.*

| $\dim(V)$ | $\mathbf{E}_{\mathcal{F}} \smallsetminus \{A\}$ | $\mu_A(G^\vee)$ | $G =$ | Condition |
|---|---|---|---|---|
| $p-1$ | $\mathcal{H}$ | $\geqslant \Delta_{-1}$ | $O^{p'}(G)\cdot\mu_A^{-1}(\Delta_{-1})$ | – |
| | $\mathcal{B}$ | $\geqslant \Delta_0$ | $O^{p'}(G)\mu_A^{-1}(\Delta_0)$ | $V$ contains no 1-dimensional $\mathbb{F}_pG$-submodule |
| $\geqslant p$ | $\mathcal{B}$ | $= \Delta_0$ | | |

Since a $p$-compact group is determined by its Weyl group by [**4**, theorem 1.1], it remains only to check, when $\mathrm{rk}(A) = p-1$ and based on the constructions of these groups, whether $\mathcal{B} \subseteq \mathbf{E}_{\mathcal{F}}$ or $\mathcal{H} \subseteq \mathbf{E}_{\mathcal{F}}$. This situation occurs only in the last four cases listed in the table, in which cases the $p$-compact group was constructed by Aguadé [**1**, §§ 5–7, 10], and the use of $SU(p)$ in his construction shows that extraspecial groups of order $p^3$ and exponent $p$ appear as essential subgroups.

In those cases where a torsion linear group is given in table 5.1, it is a union of a sequence of finite groups that by table 4.2 realize a sequence of finite fusion subsystems of $\mathcal{F}$. □

The different situations handled in theorem B are partly summarized in table 5.2.

## 6. Examples

Recall definition 3.1: for a given prime $p$, $\mathscr{G}_p$ is the class of finite groups $G$ with $\mathbf{U} \in \mathrm{Syl}_p(G)$ of order $p$ and not normal, and $\mathscr{G}_p^\wedge$ is the class of those $G \in \mathscr{G}_p$ such that $\mathrm{Aut}_G(\mathbf{U}) = \mathrm{Aut}(\mathbf{U})$. It remains now to describe explicitly which finite groups $G \in \mathscr{G}_p^\wedge$ and $\mathbb{F}_pG$-modules $V$ can appear in theorems A and B. This follows immediately from the work already done in [**15**], and is stated in proposition 6.1 and table 6.1. As in [**15**], when $p$ is a fixed prime, we define, for each odd integer $i$ prime to $p$,

$$\Delta_{i/2} = \{(r^2, r^i) \,|\, r \in (\mathbb{Z}/p)^\times\}\,.$$

(Compare with the definition of $\Delta_i$ in notation 2.9.)

Proposition 6.1. *Assume that $G \in \mathscr{G}_p^\wedge$, and that $V$ is a faithful, minimally active, indecomposable $\mathbb{F}_pG$-module such that $\dim(V) \geqslant p-1$. If $\dim(V) \geqslant p$, then assume also that $\mu_V(G^\vee) \geqslant \Delta_0$; and if $\dim(V) = p$, then assume that $V$ contains no 1-dimensional $\mathbb{F}_pG$-submodule. Then either*

(a) *the image of $G$ in $PGL(V)$ is not almost simple, and $G \leqslant \overline{G}$ with the given action on $V$ for one of the pairs $(\overline{G}, V)$ listed in table 6.1 with no entry $G_0$; or*

(b) *the image of $G$ in $PGL(V)$ is almost simple, and $G_0 \leqslant G \leqslant \overline{G}$ with the given action on $V$ for one of the triples $(G_0, \overline{G}, V)$ listed in table 6.1.*

*In all cases, the entry under $\dim(V)$ gives the dimensions of the composition factors of $V$; thus a single number means that $V$ is simple.*

*Proof.* We take as starting point the information in [**15**, table 4.1]. We drop from that table those cases where $\dim(V) < p-1$, and also those cases where $\dim(V) \geqslant p$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Table 6.1. *Pairs $(G, V)$, where $G \in \mathscr{G}_p^\wedge$, $G \leqslant \overline{G}$, $G \geqslant G_0$ when a quasisimple group $G_0$ is given, and where $V$ is a minimally active indecomposable module of dimension at least $p-1$, such that $\mu_V(G^\vee) \geqslant \Delta_0$ if* $\dim(V) \geqslant p$, *and such that $V$ does not have a 1-dimensional submodule if* $\dim(V) = p$. *In all cases,* $\dim(V)$ *gives the dimensions of the composition factors in $V$. Also, $\mathbb{F}_p^{\times 2} = \{r^2 \,|\, r \in \mathbb{F}_p^\times\}$. The notation $B.C$, $B{:}C$, and $B{\cdot}C$ for extensions is as in the* Atlas [13, *p. xx*], *as well as the subscripts used to make precise certain central extensions or automorphism groups.*

| $p$ | $G_0$ | $\dim(V)$ | $\overline{G}$ | $\mu_V(\overline{G}^\vee)$ | $\mu_V(G_0^\vee)$ |
|---|---|---|---|---|---|
| $p$ | $SL_2(p)$ or $PSL_2(p)$ $(p \geqslant 5)$ | $p-1,\ p$ | $GL_2(p)$ or $PGL_2(p) \times C_{p-1}$ | $\Delta$ | $\Delta_{-1/2},\ \frac{1}{2}\Delta_0$ |
| | | $(p{-}n{-}1)/n$ | | $\Delta$ | $\{(u^2, u^{n-1})\}$ |
| $p$ | $A_p \quad (p \geqslant 5)$ | $(p{-}2)/1$ | $\Sigma_p \times C_{p-1}$ | $\Delta$ | $\frac{1}{2}\Delta_0$ |
| | | $1/(p{-}2)$ | | $\Delta$ | $\frac{1}{2}\Delta_{-1}$ |
| $p$ | $A_{p+1} \quad (p \geqslant 5)$ | $p$ | $\Sigma_{p+1} \times C_{p-1}$ | $\Delta$ | $\frac{1}{2}\Delta_0$ |
| $p$ | $A_n\ (p{+}2 \leqslant n \leqslant 2p{-}1)$ | $n-1$ | $\Sigma_n \times C_{p-1}$ | $\Delta_0$ | $\frac{1}{2}\Delta_0$ |
| $p$ | — | $n$ | $C_{p-1} \wr S_n\ (n \geqslant p)$ | $\Delta$ | — |
| 3 | — | 2 | $GL_2(3)$ | $\Delta$ | — |
| 5 | $2{\cdot}A_6$ | 4 | $4{\cdot}S_6$ | $\Delta$ | $\Delta_{1/2}$ |
| 5 | — | 4 | $(C_4 \circ 2^{1+4}).S_6$ | $\Delta$ | — |
| 5 | $PSp_4(3) = W(E_6)'$ | 6 | $W(E_6) \times 4$ | $\Delta_0.2$ | $\frac{1}{2}\Delta_0$ |
| 5 | $Sp_6(2) = W(E_7)'$ | 7 | $G_0 \times 4$ | $\Delta_0$ | $\frac{1}{2}\Delta_0$ |
| 7 | $6{\cdot}PSL_3(4)$ | 6 | $G_0.2_1$ | $\Delta$ | $\mathbb{F}_p^{\times 2} \times \mathbb{F}_p^\times$ |
| 7 | $6_1{\cdot}PSU_4(3)$ | 6 | $G_0.2_2$ | $\Delta$ | $\mathbb{F}_p^{\times 2} \times \mathbb{F}_p^\times$ |
| 7 | $PSU_3(3)$ | 6 | $G_0.2 \times 6$ | $\Delta$ | $\frac{1}{2}\Delta_1$ |
| 7 | $PSU_3(3)$ | 7 | $G_0.2 \times 6$ | $\Delta$ | $\frac{1}{2}\Delta_0$ |
| 7 | $SL_2(8)$ | 7 | $G_0{:}3 \times 6$ | $\Delta$ | $\frac{1}{3}\Delta_1$ |
| 7 | $Sp_6(2) = W(E_7)'$ | 7 | $G_0 \times 6$ | $\Delta$ | $\Delta_3$ |
| 7 | $2{\cdot}\Omega_8^+(2) = W(E_8)'$ | 8 | $W(E_8) \times 3$ | $\Delta_0.2$ | $\Delta_3$ |
| 11 | $PSU_5(2)$ | 10 | $G_0.2 \times 10$ | $\Delta$ | $\frac{1}{2}\Delta_2$ |
| 11 | $2{\cdot}M_{12}$ | $10,\ 10$ | $G_0.2 \times 5$ | $\Delta$ | $\Delta_{1/2},\ \Delta_{7/2}$ |
| 11 | $2{\cdot}M_{22}$ | $10,\ 10$ | $G_0.2 \times 5$ | $\Delta$ | $\Delta_{1/2},\ \Delta_{7/2}$ |
| 13 | $PSU_3(4)$ | 12 | $G_0.4 \times 12$ | $\Delta$ | $\frac{1}{3}\Delta_1$ |

and $\mu_V(G^\vee) \ngeqslant \Delta_0$, or where $\dim(V) = p$ and $V$ contains a 1-dimensional $\mathbb{F}_pG$-submodule.

Since the table in [15] is restricted to representations of dimension at least 3, we must add those representations of dimension 2 that appear. Since $\dim(V) \geqslant p-1$, this occurs only for $p = 3$, and thus $G \leqslant GL_2(3)$. Since this group is solvable, the

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

image of $G$ in $PGL(V)$ cannot be almost simple, and so this case is covered by the unique row of the table restricted to $p = 3$. □

We now give two examples, in terms of the pairs $(\overline{G}, V)$ that appear in table 6.1, to illustrate how this table can be used to list explicit fusion systems as described by theorems A and B. When $V$ is an $\mathbb{F}_p$-vector space, we set $\mathrm{Aut}_{\mathrm{sc}}(V) = Z(\mathrm{Aut}(V)) \cong \mathbb{F}_p^\times$: the group of automorphisms given by scalar multiplication.

Example 6.2. Fix an odd prime $p \geqslant 5$ and a finite group $\overline{G} \in \mathscr{G}_p^\wedge$, and choose $\mathbf{U} \in \mathrm{Syl}_p(\overline{G})$. Let $V$ be a simple, $(p-1)$-dimensional, minimally active $\mathbb{F}_p\overline{G}$-module, and assume that $\mathrm{Aut}_{\overline{G}}(V) \geqslant \mathrm{Aut}_{\mathrm{sc}}(V)$. Then $\mu_V(\overline{G}^\vee) = \Delta$ by [**15**, proposition 3.13(a)]. Let $\Lambda$ be a $\mathbb{Z}_p\overline{G}$-lattice such that $\Lambda/p\Lambda \cong V$ (see proposition 3.8(a)).

(a) By case (i–a) in table 4.4, for each $k \geqslant 2$, there is a unique simple fusion systems $\mathcal{F}$ over $(\Lambda/p^k\Lambda) \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}}(\Lambda/p^k\Lambda) \cong \overline{G}$, and such that $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{H}_0 \cup \mathcal{B}_*$.

(b) By case (iv′–a) in table 4.4, for each $k \geqslant 2$ and each $\varnothing \neq I \subseteq \{0, 1, \ldots, p-1\}$, there is a unique simple fusion system $\mathcal{F}_I$ over $(\Lambda/p^k\Lambda) \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}_I}(\Lambda/p^k\Lambda) = G_0\mu_V^{-1}(\Delta_0)$, and such that $\mathbf{E}_{\mathcal{F}_I} = \{A\} \cup \big(\bigcup_{i\in I} \mathcal{B}_i\big)$.

(c) By case (iii″–a) in table 4.4, for each $k \geqslant 2$, there is a unique simple fusion system $\mathcal{F}$ over $(\Lambda/p^k\Lambda) \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}}(\Lambda/p^k\Lambda) = G_0\mu_V^{-1}(\Delta_{-1})$, and such that $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{H}_0$.

(d) Set $A = (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda$, regarded as a discrete $\overline{G}$-p-torus. By theorem B, there are unique simple fusion systems $\mathcal{F}_B$ and $\mathcal{F}_H$ over $A \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}_B}(A) \cong O^{p'}(\overline{G})\mu_V^{-1}(\Delta_0)$ and $\mathbf{E}_{\mathcal{F}_B} = \{A\} \cup \mathcal{B}$, and $\mathrm{Aut}_{\mathcal{F}_H}(A) \cong O^{p'}(\overline{G})\mu_V^{-1}(\Delta_{-1})$ and $\mathbf{E}_{\mathcal{F}_H} = \{A\} \cup \mathcal{H}$.

Since $V$ is simple (since there is no $(p-2)$-dimensional submodule), none of the cases (ii–a), (iii′–a), or (iii″–c) in table 4.4 can occur with $G_0 \leqslant G \leqslant \overline{G}$ and $V \cong \Omega_1(A)$. Since $\dim(V) < p$, case (iv″–b) in table 4.3 cannot occur.

The last column in table 6.1 can be used to help determine the subgroups $O^{p'}(\overline{G})\mu_V^{-1}(\Delta_t)$ for $i = 0, -1$. For example:

- When $p = 5$, $G_0 \cong 2{\cdot}A_6$, and $\dim(V) = 4$, we have $\mu_V(G_0^\vee) = \Delta_{1/2}$: the subgroup of order 4 in $\Delta = (\mathbb{Z}/5)^\times \times (\mathbb{Z}/5)^\times$ generated by the class of $(4, 2)$. Since $\Delta_{1/2}\Delta_t = \Delta$ for $t = 0, -1$, we have $G_0\mu_V^{-1}(\Delta_t) = \overline{G}$.

- When $p = 7$, $G_0 \cong 6{\cdot}PSL_3(4)$ or $6{\cdot}PSU_4(3)$, and $\dim(V) = 6$, we have that $\mu_V(G_0^\vee)$ has index 2 in $\Delta$ and does not contain $\Delta_t$ for any $t$. So in all cases, $G_0\mu_V^{-1}(\Delta_t) = \overline{G}$: an extension of the form $G_0.2$.

- If $p = 7$, $G_0 \cong PSU_3(3)$, and $\dim(V) = 6$, then $\mu_V(G_0^\vee) = 1/2\Delta_1$: a subgroup of order 3 that intersects trivially with $\Delta_t$ for $t = 0, -1$. So in this case, $G_0\mu_V^{-1}(\Delta_t)$ has the form $G_0.2 \times 3$ (where the precise extension depends on $t$).

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

We now look at one case where the $\mathbb{F}_p G$-module $V$ is not simple.

Example 6.3. Let $p$, $\overline{G}$, $\mathbf{U}$, $V$, and $\Lambda$ be as in example 6.2, except that we assume that $V$ is indecomposable but not simple, and contains a $(p-2)$-dimensional submodule $V_0 < V$. Let $\Lambda_0 < \Lambda$ be a $\mathbb{Z}_p\overline{G}$-sublattice of index $p$ such that $\Lambda_0/p\Lambda \cong V_0$.

- There are simple fusion systems exactly as described in cases (a), (b), (c), and (d) in example 6.2. In addition, we have:

(e) By case (ii–a) in table 4.4, for each $k \geqslant 2$, there is a unique simple fusion systems $\mathcal{F}$ over $(\Lambda_0/p^k\Lambda) \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}}(\Lambda_0/p^k\Lambda) \cong \overline{G}$, and such that $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{B}_0 \cup \mathcal{H}_*$.

(f) By case (iii′–a) in table 4.4, for each $k \geqslant 2$ and each $\varnothing \neq I \subseteq \{0, 1, \ldots, p-1\}$, there is a unique simple fusion system $\mathcal{F}_I$ over $(\Lambda_0/p^k\Lambda) \rtimes \mathbf{U}$, with $\mathrm{Aut}_{\mathcal{F}_I}(\Lambda_0/p^k\Lambda) = O^{p'}(\overline{G})\mu_V^{-1}(\Delta_{-1})$, and such that $\mathbf{E}_{\mathcal{F}_I} = \{A\} \cup \big(\bigcup_{i\in I} \mathcal{H}_i\big)$.

Since there is no 1-dimensional submodule, case (iii″–c) in table 4.4 cannot occur with $G_0 \leqslant G \leqslant \overline{G}$ and $V \cong \Omega_1(A)$. Since $\dim(V) < p$, case (iv″–b) in table 4.3 cannot occur.

If we chose to restrict the above examples to the case $\dim(V) = p-1$, this is because when $\dim(V)$ is larger, there are far fewer possibilities. By table 4.4, $A \cong \Lambda/p^k\Lambda$ for some $k \geqslant 2$, and $\mathbf{E}_{\mathcal{F}} = \{A\} \cup \mathcal{B}_0$. Similarly, by table 5.2, there is only one possibility for $\mathcal{F}$ when $A$ is a discrete $p$-torus with $\Omega_1(A) \cong V$.

**Acknowledgements**

B. Oliver is partially supported by UMR 7539 of the CNRS. A. Ruiz is partially supported by MICINN-FEDER project number MTM2016-80439-P.

## Appendix A. Background on groups and representations

We collect here some miscellaneous group theoretic results which were needed earlier. We begin with a few elementary properties of discrete $p$-toral groups that are easily reduced to the analogous statements about finite $p$-groups.

Lemma A.1. *Fix a prime $p$, a discrete $p$-toral group $P$, and a finite group $G \leqslant \mathrm{Aut}(P)$ of automorphisms of $P$. Let $1 = P_0 \trianglelefteq P_1 \trianglelefteq \cdots \trianglelefteq P_m = P$ be a sequence of subgroups, all normal in $P$ and normalized by $G$. Let $H \leqslant G$ be the subgroup of those $g \in G$ which act via the identity on $P_i/P_{i-1}$ for each $1 \leqslant i \leqslant m$. Then $H$ is a normal $p$-subgroup of $G$, and hence $H \leqslant O_p(G)$.*

*Proof.* See, for example, [**10**, lemma 1.7(a)]. □

Lemma A.2. *Fix an abelian group $A$ each of whose elements has $p$-power order. Let $G \leqslant \mathrm{Aut}(A)$ be a finite group of automorphisms, and choose $\mathbf{U} \in \mathrm{Syl}_p(G)$. Then*

$$C_A(\mathbf{U}) \leqslant [G, A] \iff C_A(G) \leqslant [G, A] \iff C_A(G) \leqslant [\mathbf{U}, A]\,.$$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

*Proof.* This is shown in [**15**, lemma 1.9] when $A$ is a finite abelian $p$-group, and the proof given there also applies when $A$ is infinite and $p$-power torsion. □

Lemma A.3. *Let $S$ be a nonabelian discrete $p$-toral group, with an abelian subgroup $A < S$ of index $p$, and set $Z = Z(S) = C_S(A)$ and $S' = [S, S] = [S, A]$. Then $S' \cong A/Z$. Also, $A$ is the unique abelian subgroup of index $p$ in $S$ if and only if $|S'| = |A/Z| > p$.*

*Proof.* Choose $1 \neq u \in \mathrm{Aut}_S(A)$, and define $\varphi\colon A \longrightarrow A$ by setting $\varphi(a) = a - u(a)$. Then $Z = \mathrm{Ker}(\varphi)$ and $S' = \mathrm{Im}(\varphi)$, so $A/Z \cong S'$.

If $|A/Z| = p$, then $S/Z \cong C_p \times C_p$ (it cannot be cyclic since $S$ is nonabelian), and each subgroup of index $p$ in $S$ containing $Z$ is abelian. Conversely, if $B$ is a second abelian subgroup of index $p$, then $Z = A \cap B$ since $S = AB$, so $|A/Z| = p$. □

We now turn attention to discrete $p$-toral groups and discrete $G$-$p$-tori. We start with the well known equivalence between discrete $G$-$p$-tori and $\mathbb{Z}_pG$-lattices (see definition 3.6).

Proposition A.4. *Fix a prime $p$ and a finite group $G$. Then there is a natural bijection*

$$\left\{\begin{array}{l}\text{isomorphism classes of dis-}\\ \text{crete } G\text{-}p\text{-tori}\end{array}\right\} \underset{\longleftarrow}{\xrightarrow{\cong}} \left\{\begin{array}{l}\text{isomorphism classes of } \mathbb{Z}_pG\text{-lattices in}\\ \text{finitely generated } \mathbb{Q}_pG\text{-modules}\end{array}\right\}$$

$$A \longmapsto \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A)$$

$$(\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda \longleftarrow\!\shortmid \Lambda$$

*If $A$ is a discrete $G$-$p$-torus and $\Lambda = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A)$, then for each $n \geqslant 1$, evaluation at $[1/p^n] \in \mathbb{Q}_p/\mathbb{Z}_p$ defines an $\mathbb{F}_pG$-linear isomorphism $\Lambda/p^n\Lambda \xrightarrow{\cong} \Omega_n(A)$.*

*Proof.* If $\Lambda$ is a $\mathbb{Z}_pG$-lattice, then $(\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda$ is a discrete $G$-$p$-torus, and if $A$ is a discrete $G$-$p$-torus, then $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A)$ is a $\mathbb{Z}_pG$-lattice. It is an easy exercise to show that the natural homomorphisms

$$(\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, A) \xrightarrow{\text{eval}} A$$

and

$$\Lambda \xrightarrow{\lambda \mapsto (r \mapsto r \otimes \lambda)} \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathbb{Q}_p/\mathbb{Z}_p, (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Lambda\big)$$

are isomorphisms for each $\mathbb{Z}_pG$-lattice $\Lambda$ and each discrete $G$-$p$-torus $A$. The last statement now follows from the short exact sequence

$$0 \longrightarrow (p^{-n}\mathbb{Z}_p)/\mathbb{Z}_p \xrightarrow{\text{incl}} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{(x \mapsto p^n x)} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0. \qquad \square$$

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

The next lemma is mostly a well-known result in elementary number theory.

LEMMA A.5. *Fix a prime $p$, and let $\mathbf{U}$ be a group of order $p$. Let $\zeta$ be a primitive $p$-th root of unity, and regard $\mathbb{Q}_p(\zeta)$ and $\mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_p\mathbf{U}$-modules via some choice of isomorphism $\mathbf{U} \cong \langle\zeta\rangle$.*

(a) *There are exactly two irreducible $\mathbb{Q}_p\mathbf{U}$-modules up to isomorphism: a 1-dimensional module with trivial $\mathbf{U}$-action, and a $(p-1)$-dimensional module isomorphic to $\mathbb{Q}_p(\zeta)$.*

(b) *The ring $\mathbb{Z}_p[\zeta]$ is a local ring with maximal ideal $\mathfrak{p} = (1-\zeta)\mathbb{Z}_p[\zeta]$. Also, $p\mathbb{Z}_p[\zeta] = \mathfrak{p}^{p-1}$.*

(c) *Let $M$ be a $(p-1)$-dimensional irreducible $\mathbb{Q}_p\mathbf{U}$-module, and let $\Lambda < M$ be a $\mathbb{Z}_p\mathbf{U}$-lattice. Then $\Lambda \cong \mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_p\mathbf{U}$-modules, and hence $\Lambda/p\Lambda \cong \mathbb{Z}_p[\zeta]/\mathfrak{p}^{p-1}$ is indecomposable as an $\mathbb{F}_p\mathbf{U}$-module.*

(d) *Let $B$ be an infinite abelian discrete $p$-toral group (written additively), upon which $\mathbf{U}$ acts with $|C_B(\mathbf{U})| = p$. Assume also that $\prod_{u\in\mathbf{U}} u(x) = 1$ for each $x \in B$. Then $B$ is a discrete $p$-torus of rank $p-1$, and $B \cong \mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta]$ as $\mathbb{Z}_p\mathbf{U}$-modules.*

*Proof.* **(a,b)** By [17, proposition 6-2-6], $(1-\zeta)\mathbb{Z}[\zeta]$ is the only prime ideal in $\mathbb{Z}[\zeta]$ containing $p\mathbb{Z}[\zeta] = (1-\zeta)^{p-1}\mathbb{Z}[\zeta]$. Hence $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta) = \mathbb{Q}_p(\zeta)$, so $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p(\zeta)) = p-1$, and $\mathbb{Z}_p[\zeta]$ is a local ring with maximal ideal $\mathfrak{p} = (1-\zeta)\mathbb{Z}_p[\zeta]$ where $\mathfrak{p}^{p-1} = p\mathbb{Z}_p[\zeta]$. This proves (b), and also that $\mathbb{Q}_p(\zeta)$ is an irreducible $(p-1)$-dimensional $\mathbb{Q}_p\mathbf{U}$-module. So the only other irreducible $\mathbb{Q}_p\mathbf{U}$-module is $\mathbb{Q}_p$ with the trivial action.
**(c)** By (a), we can assume that $M = \mathbb{Q}_p(\zeta)$. Thus $\Lambda$ is a $\mathbb{Z}_p\mathbf{U}$-lattice in $\mathbb{Q}_p(\zeta)$, so $p^m\Lambda \leqslant \mathbb{Z}_p[\zeta]$ is an ideal for $m$ large enough. Hence $p^m\Lambda = \mathfrak{p}^k = (1-\zeta)^k\mathbb{Z}_p[\zeta]$ for some $k$, and $\Lambda$ is isomorphic to $\mathbb{Z}_p[\zeta]$ as a $\mathbb{Z}_p\mathbf{U}$-module.
**(d)** Since $\prod_{u\in\mathbf{U}} u(x) = 1$ for each $x \in B$, we can regard $B$ as a $\mathbb{Z}_p[\zeta]$-module. For each $n \geqslant 1$, $\bigl|\Omega_n(B)/(1-\zeta)\Omega_n(B)\bigr| = |C_{\Omega_n(B)}(\mathbf{U})| = |C_B(\mathbf{U})| = p$, and so by (b), there is $r_n \in \Omega_n(B)$ that generates $\Omega_n(B)$ as a $\mathbb{Z}_p[\zeta]$-module. Let $R_n$ be the set of all such generators of $\Omega_n(B)$, and let $\varphi_n\colon R_n \longrightarrow R_{n-1}$ be the map $\varphi_n(r_n) = (r_n)^p$. The $(R_n, \varphi_n)$ thus form an inverse system of nonempty finite sets. An element $(r_n)_{n\geqslant 1}$ in the inverse limit defines an isomorphism $\mathbb{Q}_p(\zeta)/\mathbb{Z}_p[\zeta] \cong (\mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta] \xrightarrow{\quad} B$ of $\mathbb{Z}_p[\zeta]$-modules (hence of $\mathbb{Z}_p\mathbf{U}$-modules), where $(1/p^n) \otimes \xi$ is sent to $\xi{\cdot}r_n$. □

LEMMA A.6. *Fix a prime $p$, an abelian discrete $p$-toral group $A$ and a finite group of automorphisms $G \leqslant \mathrm{Aut}(A)$. Assume, for $S \in \mathrm{Syl}_p(G)$, that $S \ntrianglelefteq G$ and $|A/C_A(S)| = p$. Then $|S| = p$.*

*Proof.* This is shown in [23, lemma 1.10] when $A$ is finite, and the general case follows since $G$ acts faithfully on $\Omega_k(A)$ for $k$ large enough. □

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

Proposition A.7. *Fix an abelian discrete $p$-toral group $A$, and a subgroup $G \leqslant \mathrm{Aut}(A)$. Assume the following.*

(i) *Each Sylow $p$-subgroup of $G$ has order $p$ and is not normal in $G$.*

(ii) *For each $x \in G$ of order $p$, $[x, A]$ has order $p$, and hence $C_A(x)$ has index $p$.*

*Set $H = O^{p'}(G)$, $A_1 = C_A(H)$, and $A_2 = [H, A]$. Then $G$ normalizes $A_1$ and $A_2$, $A = A_1 \times A_2$, and $H \cong SL_2(p)$ acts faithfully on $A_2 \cong C_p^2$. There are groups of automorphisms $G_i \leqslant \mathrm{Aut}(A_i)$ $(i = 1, 2)$, such that $p \nmid |G_1|$, $G_2 \geqslant \mathrm{Aut}_H(A_2) \cong SL_2(p)$, and $G \trianglelefteq G_1 \times G_2$ (as a subgroup of $\mathrm{Aut}(A)$) with index dividing $p - 1$.*

*Proof.* This is shown in [23, lemma 1.11] when $A$ is finite. The general case then follows by regarding $A$ as the union of the groups $\Omega_k(A)$ for $k \geqslant 1$. □

## References

1 J. Aguadé. Constructing modular classifying spaces. *Israel J. Math.* **66** (1989), 23–40.

2 J. L. Alperin. *Local representation theory. Modular representations as an introduction to the local representation theory of finite groups.* Cambridge Studies in Advanced Mathematics, 11 (Cambridge: Cambridge University Press, 1986).

3 K. Andersen and J. Grodal. The classification of 2-compact groups. *J. Amer. Math. Soc.* **22** (2009), 387–436.

4 K. Andersen, J. Grodal, J. Møller and A. Viruel. The classification of $p$-compact groups for $p$ odd. *Ann. Math.* **167** (2008), 95–210.

5 K. Andersen, B. Oliver and J. Ventura. Reduced, tame, and exotic fusion systems. *Proc. London Math. Soc.* **105** (2012), 87–152.

6 K. Andersen, B. Oliver and J. Ventura. Fusion systems and amalgams. *Math. Z.* **274** (2013), 1119–1154.

7 M. Aschbacher, R. Kessar and B. Oliver. *Fusion systems in algebra and topology.* London Mathematical Society Lecture Note Series, 391 (Cambridge: Cambridge University Press, 2011).

8 D. J. Benson. *Representations and cohomology. I. Basic representation theory of finite groups and associative algebras.* Cambridge Studies in Advanced Mathematics, 30 (Cambridge: Cambridge University Press, 1991).

9 C. Broto, R. Levi and B. Oliver. The homotopy theory of fusion systems. *J. Amer. Math. Soc.* **16** (2003), 779–856.

10 C. Broto, R. Levi and B. Oliver. Discrete models for the $p$-local homotopy theory of compact Lie groups and $p$-compact groups. *Geom. Topol.* **11** (2007), 315–427.

11 C. Broto, R. Levi and B. Oliver. An algebraic model for finite loop spaces. *Algebr. Geom. Topol.* **14** (2014), 2915–2981.

12 A. Clark and J. Ewing. The realization of polynomial algebras as cohomology rings. *Pacific J. Math.* **50** (1974), 425–434.

13 J. H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson and Atlas of finite groups. *Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray* (Eynsham: Oxford University Press, 1985).

14 D. Craven. *The theory of fusion systems. An algebraic approach.* Cambridge Studies in Advanced Mathematics, 131 (Cambridge; Cambridge University Press, 2011).

15 D. Craven, B. Oliver and J. Semeraro. Reduced fusion systems over $p$-groups with abelian subgroup of index $p$: II. *Adv. Math.* **322** (2017), 201–268.

16 W. Dwyer and C. Wilkerson. Homotopy fixed-point methods for Lie groups and finite loop spaces. *Ann. Math.* **139** (1994), 395–442.

17 L. Goldstein. *Analytic number theory* (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1971).

18 A. González. The structure of $p$-local compact groups of rank 1. *Forum Math.* **28** (2016), 219–253.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press

19 A. González, T. Lozano and A. Ruiz. Some new examples of $p$-local compact groups. *Publ. Mat.*, (to appear), arXiv:1512.00284v5 [math.AT].

20 D. Gorenstein. *Finite groups* (New York/London: Harper & Row, Publishers, 1968).

21 R. Levi and B. Oliver. Construction of 2-local finite groups of a type studied by Solomon and Benson. *Geometry & Topology* **6** (2002), 917–990.

22 J. Møller. $N$-determined 2-compact groups. I. *Fund. Math.* **195** (2007), 11–84.

23 B. Oliver. Simple fusion systems over $p$-groups with abelian subgroup of index $p$: I. *J. Algebra* **398** (2014), 527–541.

24 L. Puig. Frobenius categories. *J. Algebra* **303** (2006), 309–357.

25 A. Ruiz and A. Viruel. The classification of $p$-local finite groups over the extraspecial group of order $p^3$ and exponent $p$. *Math. Z.* **248** (2004), 45–65.

26 G. Shephard and J. Todd. Finite unitary reflection groups. *Canadian J. Math.* **6** (1954), 274–304.

https://doi.org/10.1017/prm.2018.107 Published online by Cambridge University Press