p-Groups with a unique proper non-trivial characteristic subgroup

S.P. Glasby\textsuperscript{a}, P.P. Pálfy\textsuperscript{b}, Csaba Schneider\textsuperscript{c,\ast}

\textsuperscript{a} Department of Mathematics, Central Washington University, WA 98926-7424, USA
\textsuperscript{b} Alfréd Rényi Institute of Mathematics, 1364 Budapest, Pf. 127, Hungary
\textsuperscript{c} Centro de Álgebra da Universidade de Lisboa, Av. Prof. Gama Pinto, 2, 1649-003 Lisboa, Portugal

\begin{abstract}
We consider the structure of finite \( p \)-groups \( G \) having precisely three characteristic subgroups, namely 1, \( \Phi(G) \) and \( G \). The structure of \( G \) varies markedly depending on whether \( G \) has exponent \( p \) or \( p^2 \), and, in both cases, the study of such groups raises deep problems in representation theory. We present classification theorems for 3- and 4-generator groups, and we also study the existence of such \( r \)-generator groups with exponent \( p^2 \) for various values of \( r \). The automorphism group induced on the Frattini quotient is, in various cases, related to a maximal linear group in Aschbacher’s classification scheme.
\end{abstract}

1. Introduction

Taunt [Taunt55] considered groups having precisely three characteristic subgroups. As such groups have a unique proper non-trivial characteristic subgroup, he called these UCS-groups. He gave necessary, but not sufficient, conditions for the direct power of a UCS-group to be a UCS-group. Taunt discussed solvable UCS-groups in [Taunt55], and promised a forthcoming paper describing the structure of UCS \( p \)-groups. However, his article on UCS \( p \)-groups was never written. The present paper is devoted to the study of these groups.
In our experience UCS $p$-groups are rather elusive, and it is unlikely that a general classification could be given. However, the study of these groups does lead to the exploration of very interesting problems in representation theory, and some interesting, sometimes even surprising, theorems can be proved.

The main results of this paper can be summarized as follows.

**Theorem 1.** Let $G$ be a non-abelian UCS $p$-group where $|G/\Phi(G)| = p^7$.

(a) If $r = 2$, then $G$ belongs to a unique isomorphism class.

(b) If $r = 3$, then $G$ belongs to a unique isomorphism class if $p = 2$, and to one of two distinct isomorphism classes if $p > 2$.

(c) If $r = 4$ and either $p = 2$ or $G$ has exponent $p$, then $G$ belongs to one of eight distinct isomorphism classes.

(d) Suppose that $r = 4$ and $G$ has exponent $p^2$. Then $p \neq 5$. Further, if $p \equiv \pm 1 \pmod{5}$ then $G$ belongs to a unique isomorphism class; while if $p \equiv \pm 2 \pmod{5}$ then $G$ belongs to one of two distinct isomorphism classes.

(e) Let $p$ be an odd prime, and let $k$ be a positive integer. Then there exist non-abelian exponent-$p^2$ UCS-groups

(i) of order $p^{6k}$ for all $p$ and $k$;

(ii) of order $p^{10}$ if and only if $p^5 \equiv 1 \pmod{11}$;

(iii) of order $p^{14k}$ for all $p$ and $k$.

Parts (a) and (b) of Theorem 1 follow from Theorem 6, while part (c) follows from Theorems 8 and 9. Part (d) is verified in Theorem 17 and the proof of (e) can be found at the end of Section 7.

As UCS $p$-groups have precisely three characteristic subgroups, they must have exponent $p$ or $p^2$. Abelian UCS $p$-groups are all of the form $(C_p^2)^s$ where $p$ is a prime. Non-abelian UCS $p$-groups with exponent $p$ are quite common, and so we could investigate them only for small generator number ($r \leq 4$). However, it seems that non-abelian UCS $p$-groups with exponent $p^2$ are less common, and we could even prove that for certain choices of the pair $(p, r)$ in Theorem 1 they do not exist. For instance Theorem 1(d) implies that there is no non-abelian UCS 5-group with 4 generators and exponent 25. In both cases, the study of such groups leads to challenging problems in representation theory. A well-written introduction to $p$-groups of Frattini length 2 can be found in [GQ06].

Let $p$ be an odd prime, and let $G$ be a non-abelian $r$-generator UCS $p$-group with exponent $p$. Then $G$ has the form $H/N$ where $H$ is the $r$-generator, free group with exponent $p$ and nilpotency class 2, and $N$ is a proper subgroup of $H'$. The groups $H/H'$ and $H'$ are elementary abelian, and so they can be considered as vector spaces over $F_p$. Moreover, the group $GL_r(p)$ acts on $H/H'$ in the natural action, and on $H'$ in the exterior square action. It is proved in Theorem 4 that $G$ is UCS if and only if the (setwise) stabilizer $K := GL_r(p)_N$ is irreducible on both $H/H'$ and $H'/N$. Conversely, an irreducible subgroup $K \leq GL_r(p)$ and an irreducible $K$-factor module $H'/N$ lead to a UCS $p$-group with exponent $p$ (see Theorem 5). Thus the investigation of the class of UCS $p$-groups with exponent $p$ is reduced to the study of irreducible subgroups $K$ of $GL_r(p)$ and the maximal $K$-submodules of the exterior square $\Lambda^2(F_p)^r$.

The study of UCS 2-groups poses different problems than the odd case. In this paper we concentrate on UCS groups of odd order, and prove only a few results about UCS 2-groups.

A non-abelian UCS $p$-group $G$ with odd order and exponent $p^2$, is a powerful $p$-group (i.e. $G' \leq G^p$). Moreover, $G$ has the form $H/N$ where $H$ is the $r$-generator free group with $p$-class 2 and exponent $p^2$ (that is, $\Phi(H) \leq Z(H)$ and $\Phi(H)^p = 1$) and $N$ is a subgroup of $\Phi(H)$. As above, $GL_r(p)$ acts on $H/\Phi(H)$ in the natural action and $\Phi(H) = H^p \oplus H'$ can also be viewed as a $GL_r(p)$-module. The commutator subgroup $G'$ is isomorphic to $H'/\langle H' \cap N \rangle$ and, as $G$ has one proper non-trivial characteristic subgroup, $G'$ must coincide with $G^p$. On the other hand, as the $p$-th power map $x \mapsto x^p$ is a homomorphism, the $GL_r(p)_N$-actions on $H/\Phi(H)$ and on $H'/\langle H' \cap N \rangle$ must be equivalent. Further $GL_r(p)_N$ must be irreducible on both $H/\Phi(H)$ and $H'/\langle H' \cap N \rangle$ (see Theorem 4 for the proof of the last two assertions). Therefore we found an irreducible subgroup $K$ of $GL_r(p)$ and a maximal $K$-submodule $N$ in $\Lambda^2(F_p)^r$ such that $\Lambda^2(F_p)^r/N$ is equivalent to the natural module of $K$. Conversely, such a group $K$ and a submodule $N$ lead to a UCS $p$-group with exponent $p^2$ (see...
Theorem 5). Thus UCS \( p \)-groups with odd exponent \( p^2 \) give rise to irreducible modules that are isomorphic to a quotient of the exterior square. We call these exterior self-quotient modules (or ESQ-modules).

In Sections 4 and 6, UCS \( p \)-groups with exponent \( p \) and generator number at most 4 are studied. We achieve a complete classification of 2- and 3-generator UCS \( p \)-groups and, for odd \( p \), a complete classification of 4-generator UCS \( p \)-groups with exponent \( p \). These classifications are made possible in these cases by our knowledge of the GL\(_r\)(\( p \))-module \( W = \Lambda^2(\mathbb{F}_p)^2 \). If \( r = 2 \) then \( W \) is a 1-dimensional module, and our problem is trivial. If \( r = 3 \), then \( W \) is equivalent to the dual of the natural module and the classification of UCS \( p \)-groups with exponent \( p \) is straightforward also in this case. However, the classification of 3-generator UCS \( p \)-groups with exponent \( p^2 \) is already non-trivial. The fact that there is, up to isomorphism, precisely one 3-generator UCS \( p \)-group with exponent \( p^2 \) is a consequence of the fact that the stabilizer in the general linear group GL\(_3\)(\( p \)) of a certain 3-dimensional subspace of \( (\mathbb{F}_p)^6 \) is the special orthogonal group SO\(_2\)(\( p \)) (see Lemma 7).

When \( r = 4 \), the Klein correspondence makes it possible to obtain the necessary information about the GL\(_r\)(\( p \))-module \( W \). In this case GL\(_r\)(\( p \)) preserves (up to scalar multiples) a quadratic form on \( W \). A \( p \)-group with exponent \( p \) corresponds to a subspace \( N \) of \( W \) as explained above. These observations and the classification of \( p \)-groups with order dividing \( p^2 \) (see [NOVL04,OVL05]) enable us to classify 4-generator UCS \( p \)-groups with exponent \( p \). We found it surprising that \( N \) leads to a UCS \( p \)-group if and only if the restriction of the quadratic form to \( N \) is non-degenerate. The details are presented in Section 6. A brief classification of 4-generator UCS 2-groups is given in Section 5.

Section 7 focuses on the construction of exterior self-quotient (ESQ) modules. As remarked above, this is directly related to the construction of UCS \( p \)-groups with odd exponent \( p^2 \). Our results for exponent-\( p^2 \) UCS groups are summarized in Theorem 1(d), (e), and proved in Section 7. Theorems 15, 16 are concerned with the structure of ESQ-modules in dimensions 4 and 5, and are of independent interest.

2. \( p \)-Groups with precisely 3 characteristic subgroups

We shall focus henceforth on the structure of a \( p \)-group \( G \) with precisely three characteristic subgroups. In such a group the Frattini subgroup \( \Phi(G) \) is non-trivial, otherwise \( G \) is elementary abelian and characteristicaly simple. Therefore the non-trivial, proper characteristic subgroup of \( G \) is \( \Phi(G) \). Since the terms of the lower central series and the subgroups \( G^p \) are characteristic in \( G \), we obtain that a UCS \( p \)-group has exponent at most \( p^2 \) and nilpotency class at most 2.

Let \( H_{p,r} \) denote the \( r \)-generator free group in the variety of groups that have exponent \( p^2 \), nilpotency class 2, and have the property that all \( p \)-th powers are central. Then \( H_{p,r} \) is a finite \( p \)-group and the quotient \( H_{p,r}/\Phi(H_{p,r}) \) is elementary abelian with rank \( r \). Further, the subgroup \( \Phi(H_{p,r}) \) is elementary abelian and central. Assume that the elements \( x_1, \ldots, x_r \) form a minimal generating set for \( H_{p,r} \). The Frattini subgroup \( \Phi(H_{p,r}) \) is minimally generated by the elements \( x_i^p \) and \( [x_j, x_k] \) with \( i, j, k \in \{1, \ldots, r\} \) and \( j < k \). Thus \( \Phi(H_{p,r}) \) has rank \( r(r - 1)/2 + r \). In 2-groups, the subgroup generated by the squares contains the commutator subgroup, so \( \Phi(H_{2,r}) = (H_{2,r})^2 \). On the other hand, if \( p \geq 3 \), then \( \Phi(H_{p,r}) = (H_{p,r})' \oplus (H_{p,r})^p \). In this case, the commutators \( [x_j, x_k] \) with \( j < k \) form a minimal generating set for \( (H_{p,r})' \), while the \( p \)-th powers \( x_i^p \) form a minimal generating set for \( (H_{p,r})^p \). Thus \( (H_{p,r})' \) and \( (H_{p,r})^p \) are elementary abelian with ranks \( r(r - 1)/2 \) and \( r \), respectively.

When investigating UCS \( p \)-groups we may conveniently assume that \( G \) is of the form \( H_{p,r}/N \) where \( N \leq \Phi(H_{p,r}) \).

Now we introduce some notation that will be used in the rest of the paper. If \( L \) is a group that acts on a vector space \( V \), then \( L^V \) denotes the image of \( L \) under this action. Hence \( L^V \leq \text{GL}(V) \). The stabilizer in \( L \) of an object \( X \) is denoted by \( L_X \). If \( G \) is a \( p \)-group, then \( G \) denotes \( G/\Phi(G) \). If \( G \) is a UCS \( p \)-group, then \( \Phi(G) \) and \( G \) can be considered as \( \mathbb{F}_p \)-vector spaces. We shall consider the linear groups \( \text{Aut}(G/\Phi(G)) \) and \( \text{Aut}(G/\Phi(G)) \).

The \( p \)-th power map \( x \mapsto x^p \) and the commutator map \( (x, y) \mapsto [x, y] \) can be used to define a \( \text{GL}(H_{p,r}) \)-action on \( H_{p,r} \) and hence the subgroup \( \Phi(H_{p,r}) \) can be viewed as a \( \text{GL}(H_{p,r}) \)-module, whose structure is described by the following lemma. For a proof, follow, for instance, the argument on page 26 in [Hig60].
Lemma 2. Set $H = H_{p,r}$. Then $H'$ is a $\text{GL}(\Pi)$-submodule of $\Phi(H)$ and $\Phi(H)/H' \cong \Pi$ as $\text{GL}(\Pi)$-modules. If $p \geq 3$, then $\Phi(H) = H' \oplus H^p$ is a direct sum of $\text{GL}(\Pi)$-modules. In particular, $\Pi \cong H^p$ as $\text{GL}(\Pi)$-modules if $p \geq 3$.

Next we give a description of the automorphism group of $G$ following [O’B90, Theorem 2.10]. If $G$ is of the form $H_{p,r}/N$, with some $N \leq \Phi(H_{p,r})$ then the spaces $H_{p,r}$ and $G$ can be identified, and this fact is exploited in the following lemma.

Lemma 3. Set $H = H_{p,r}$, let $N$ be a subgroup of $\Phi(H)$, and set $G = H/N$. Identifying $G$ and $\Pi$, we obtain that

$$\text{Aut}(G)^\Pi = \text{GL}(\Pi)\text{N} \quad \text{and} \quad \text{Aut}(G)^{\Phi(G)} = (\text{GL}(\Pi)\text{N})^{\Phi(H)/N}.$$ Further, the kernel $K$ of the action on $\Pi$ is an elementary abelian $p$-group of order $|\Phi(G)|^r$, and $K$ acts trivially on $\Phi(G)$.

Lemma 3 enables us to characterize UCS $p$-groups.

Theorem 4. Let $p$ be a prime, let $r$ be an integer, set $H = H_{p,r}$, and let $G = H/N$ where $N \leq \Phi(H)$. Then the following are equivalent:

(a) $G$ is a UCS $p$-group;
(b) both $\text{Aut}(G)^\Pi$ and $\text{Aut}(G)^{\Phi(G)}$ are irreducible;
(c) both $\text{GL}(\Pi)\text{N}$ and $(\text{GL}(\Pi)\text{N})^{\Phi(H)/N}$ are irreducible.

Further, if $p$ is odd and $G$ is a UCS $p$-group, then precisely one of the following must hold:

(i) $N = H'$ and $G$ is abelian;
(ii) $H^p \leq N$ and $G$ is non-abelian of exponent $p$;
(iii) $N \cap H^p = 1$, $\Pi$ and $H'/N$ are equivalent $\text{GL}(\Pi)\text{N}$-modules, $G$ is non-abelian of exponent $p^2$, and $|G| = p^{2r}$.

Proof. Assertions (b) and (c) are equivalent by Lemma 3. We now prove that (a) and (b) are equivalent. The following two observations show that (a) implies (b). First, inverse images of $\text{Aut}(G)^\Pi$-submodules of $\Pi$ correspond bijectively to characteristic subgroups of $G$ containing $\Phi(G)$. Second, $\text{Aut}(G)^{\Phi(G)}$-submodules of $\Phi(G)$ correspond bijectively to characteristic subgroups of $G$ contained in $\Phi(G)$. Assume now that (b) holds and that $L$ is a characteristic subgroup of $G$. As $L\Phi(G)$ is characteristic, it follows from the observation above that $L\Phi(G)$ equals $\Phi(G)$ or $G$. In the latter case, $L = G$ as $\Phi(G)$ comprises the set of elements of $G$ that can be omitted from generating sets. In the former case $L\Phi(G) = \Phi(G)$ and $L \leq \Phi(G)$. It follows from (b) that $L$ equals 1 or $\Phi(G)$. Thus (b) implies (a).

We now prove the second statement of the theorem. Suppose that $G$ is an abelian UCS $p$-group, where $p$ is odd. Then $H' \leq N$ and $G$ is a quotient of $H/H' \cong (C_p)^r$ which is homocyclic of rank $r$ and exponent $p^2$. The only $r$-generator UCS quotient of $H/H' \cong (C_p)^r$ is itself, and so $N = H'$ and (i) holds. Suppose now that $G$ is non-abelian. By Lemma 2, $H'N$ is invariant under $\text{GL}(\Pi)\text{N}$. By Lemma 3, $\text{Aut}(G)^{\Phi(G)} = (\text{GL}(\Pi)\text{N})^{\Phi(H)/N}$, which shows that $H'N/N$ is characteristic in $G$. Thus $H'N$ equals $\Phi(H)$ or $N$. As $G$ is non-abelian $H'N = \Phi(H)$ holds. As $p$ is odd, Lemma 2 implies that $H^p$ is invariant under $\text{GL}(\Pi)$, and so $H^p \cap N$ must be invariant under $\text{GL}(\Pi)$\text{N}. On the other hand, the first part of Theorem 4 shows that $\text{GL}(\Pi)\text{N}$ is irreducible on $\Pi$, and so, by Lemma 2, also on $H^p$. Thus either $N \cap H^p = H^p$ or $N \cap H^p = 1$. In the former case $H^p \leq N$, and case (ii) holds. In the latter case, we shall show below that case (iii) holds.

Suppose now that $H'N = \Phi(H)$, $N \cap H^p = 1$ and $p$ is odd. As $H^p$ is invariant under $\text{GL}(\Pi)$, the quotient $NH^p/N$ must be invariant under $\text{GL}(\Pi)$\text{N}. Thus Lemma 3 implies that $NH^p/N$ is characteristic
in $G$. Hence $N H^p = \Phi(H)$. As $N \cap H^p = 1$, we obtain the following isomorphisms between $GL(\bar{H})_N$-modules:

$$H^p \cong \frac{H^p}{N \cap H^p} \cong \frac{H^p N}{N} = \frac{\Phi(H)}{N} = \frac{H' N}{N} \cong \frac{H'}{N \cap H'}.$$ 

By Lemma 2, $H^p \cong H$, as $GL(\bar{H})$-modules, so $H$ and $H'/(N \cap H')$ are equivalent $GL(\bar{H})_N$-modules. It follows from the above displayed equation that $|N| = |H'| = p^{r \cdot (r-1)/2}$, and hence that $|G| = p^{2r}$. Thus case (iii) holds. \hfill $\Box$

3. The existence of UCS $p$-groups

In this section we study the question whether UCS $p$-groups exist with given parameters. We find that the existence of $r$-generator UCS $p$-groups is equivalent to the existence of certain irreducible groups of $GL_r(p)$.

Let $H = H_{p,r}$ be as above. Recall that the $GL(\bar{H})$-action on $H'$ is equivalent to the exterior square of the natural action. If $p$ is an odd prime and $G$ is an $r$-generator UCS $p$-group with exponent $p$, then $G$ is non-abelian and, by Theorem 4, $G \cong H/N$ where $H^p \subseteq N < \Phi(H)$. Furthermore, $GL(\bar{H})_N$ must be irreducible on both $\bar{H}$ and $\Phi(H)/N$. As $H' \not\subseteq N$, we obtain that

$$\frac{\Phi(H)}{N} = \frac{H' N}{N} \cong \frac{H'}{N \cap H'}.$$

Denote $\bar{G}$ by $V$. The argument above shows that an exponent-$p$ UCS $p$-group $G$ gives rise to an irreducible linear group $K := \text{Aut}(G)^G$ acting on $V$, and a maximal $K$-module $M$ of $\Lambda^2 V$.

The structure of UCS $p$-groups with exponent $p^2$ is, by Theorem 4(iii), intimately related to the following (apparently new) concept in representation theory.

**Definition.** An $FG$-module $V$ is called an *exterior self-quotient* module, briefly an ESQ-module, if there is an $FG$-submodule $U$ of $\Lambda^2 V$ such that $(\Lambda^2 V)/U$ is isomorphic to $V$. If $G$ acts faithfully on $V$, we call $G$ an ESQ-subgroup of $GL(V)$, or simply an ESQ-group.

By Theorem 4, $\text{Aut}(G)^G$ is an irreducible ESQ-group when $G$ is a non-abelian UCS $p$-group of exponent $p^2$ for odd $p$. In Section 7 we study exterior self-quotient modules, where it is natural to consider fields $F$ other than $\mathbb{F}_p$. When we consider necessary conditions for the existence of UCS $p$-groups then we usually take $F$ to be the prime field $\mathbb{F}_p$; however, for sufficient conditions, working over arbitrary (finite) fields is most natural.

Suppose that $V$ is a $d$-dimensional vector space over a field $\mathbb{F}_q$ where $q = p^k$ for some prime $p$ and integer $k$. We may consider $V$ as a vector space over the prime field $\mathbb{F}_p$ and also over the larger field $\mathbb{F}_q$. Thus we may take the exterior squares $\Lambda^2_{\mathbb{F}_p} V$ and $\Lambda^2_{\mathbb{F}_q} V$ over $\mathbb{F}_p$ and $\mathbb{F}_q$, respectively, where $\dim \Lambda^2_{\mathbb{F}_p} V = \binom{d}{2}$ and $\dim \Lambda^2_{\mathbb{F}_q} V = \binom{dk}{2}$. There is an $\mathbb{F}_p$-linear epimorphism $\varepsilon : \Lambda^2_{\mathbb{F}_p} V \to \Lambda^2_{\mathbb{F}_q} V$ satisfying $\varepsilon(u \wedge v) = u \wedge v$ for all $u, v \in V$.

**Theorem 5.** Let $p$ be an odd prime, let $r$ and $s$ be integers. Then assertions $(a1)$ and $(a2)$ are equivalent, and so are assertions $(b1)$ and $(b2)$.

(a1) There exists a UCS $p$-group $G$ with exponent $p$ such that $|\bar{G}| = p^r$ and $|\Phi(G)| = p^s$.

(a2) There exists an irreducible linear group $K$ acting on a vector space $V$ over $\mathbb{F}_p^k$, for some $k$, such that $\dim V = r/k$ and $\Lambda^2_{\mathbb{F}_p^k} V$ has a maximal $\mathbb{F}_p^k K$-submodule with codimension $s/k$. 

(b1) There exists a UCS $p$-group $G$ with exponent $p$ such that $|\bar{G}| = p^r$ and $|\Phi(G)| = p^s$.

(b2) There exists an irreducible linear group $K$ acting on a vector space $V$ over $\mathbb{F}_p^k$, for some $k$, such that $\dim V = r/k$ and $\Lambda^2_{\mathbb{F}_p^k} V$ has a maximal $\mathbb{F}_p^k K$-submodule with codimension $s/k$. 


(b1) There exists a UCS $p$-group $G$ with exponent $p^2$ such that $|G| = p^4$.

(b2) There exists an irreducible ESQ-module $V$ over a field $\mathbb{F}_{p^k}$ such that $\dim V = r/k$, and $V$ cannot be written over any proper subfields of $\mathbb{F}_{p^k}$.

**Proof.** Assume (a1) is true, and $G$ is an exponent-$p$ UCS-group. Then by Theorem 4 $K = \text{Aut}(G)$ is an irreducible linear group, so (a2) is true with $k = 1$. Assume now that (a2) holds and set $q = p^k$. Let $U$ be a maximal $\mathbb{F}_qK$-submodule of $\Lambda^2 V$ of codimension $s/k$. Let $Z$ denote the group of the non-zero scalar transformations $\{\lambda I \mid \lambda \in \mathbb{F}_q^*\}$ of $V$. Then $Z$ commutes with $K$ and so one can form the subgroup $ZK$. Since $K$ is irreducible on $V$ over $\mathbb{F}_q$ and the action of $\mathbb{F}_q^*$ on $V$ is realized by $Z$, we find that $ZK$ is irreducible on $V$ over $\mathbb{F}_q$. Thus we proved that (a1) and (a2) are equivalent, and let us next show that (b1) and (b2) are equivalent.

Let $H$ denote $H_{p,r}$. As the GL($H$)-action on $H'$ is equivalent to its action on $\Lambda^2 H$, we identify $V$ with $H_2 \Lambda^2 V$ with $H'$, and $\hat{U}$ with a $K$-invariant normal subgroup $N$ of index $p^2$ in $H'$. Set $G = H/(H^p N)$. As $p \geq 3$, Lemma 2 shows that $H^p$ and $H'$ are GL($H$)-submodules of $\Phi(H)$ such that $\Phi(H) = H' \oplus H^p$. Hence $K$ must stabilize $H^p N$ and so Lemma 3 gives that $K \leq \text{Aut}(G)$. Since $K$ is irreducible, so is $\text{Aut}(G)$. As $$\frac{\Phi(H)}{H^p N} = \frac{H^p H'}{H^p N} \cong \frac{H'}{N},$$ we obtain that $K$ and $\text{Aut}(G)$ are irreducible on $\Phi(H)/(H^p N)$. Now Theorem 4 implies that $G$ is a UCS $p$-group with exponent $p$.

Thus we proved that (a1) and (a2) are equivalent, and let us next show that (b1) and (b2) are equivalent.

The discussion at the beginning of this section shows that (b1) implies (b2) with $k = 1$. Before proving the converse, we argue that we may assume that $k = 1$. Suppose that $V$ is an ESQ $\mathbb{F}_qK$-module, and $U$ is an $\mathbb{F}_qK$-submodule satisfying $\Lambda^2 V / U \cong V$. Using the notation above, the $\mathbb{F}_p(ZK)$-homomorphism $\varepsilon : \Lambda^2_p V \to \Lambda^2_q V$ gives rise to an $\mathbb{F}_p(ZK)$-isomorphism $\Lambda^2_p V / \hat{U} \cong \Lambda^2_q V / U$ where $\hat{U} := \varepsilon^{-1}(U)$. Since $\Lambda^2 V / U \cong V$ is an $\mathbb{F}_pK$-isomorphism, it follows that $\Lambda^2_p V$ is ESQ. Moreover, $V$ is an irreducible $\mathbb{F}_pK$-module by [HB82, Theorem VII.11.6(e)]. In summary, viewing $V$ as a $K$-module over $\mathbb{F}_p$ of larger dimension allows us to assume that the hypotheses for (b2) hold for $k = 1$.

Suppose that $k = 1$. Set $H = H_{p,r}$. Take $K$ to be an irreducible subgroup of $\text{GL}(H)$, and $M$ to be a $K$-submodule of $H'$ such that $\overline{H}$ and $\overline{H'} / M$ are isomorphic. Specifically let $\varphi : \overline{H} \to H' / M$ be a $K$-module isomorphism. Set $$N = \{ x^p y \mid x \in H, \ y \in H' \text{ such that } \varphi(x \Phi(H)) = y M \},$$ and set $G = H / N$. As $p \geq 3$, one can easily check that $N$ is a subgroup of $\Phi(H)$ and that $H' / N = M$. Since the map $x \Phi(H) \to x^p$ is a $\text{GL}(H)$-isomorphism between $\overline{H}$ and $H^p$ (Lemma 2), we find that $N$ is a $K$-submodule. Therefore Lemma 3 implies that $K \leq \text{Aut}(G)$. As in the first part of the proof, one can show that $\text{GL}(\overline{H})_N$ is irreducible both on $\overline{H}$ and on $\Phi(H) / N$. Hence, by Theorem 4, $G$ must be a UCS $p$-group. Since $N \cap H^p = 1$, $G$ has exponent $p^2$. Thus (b2) implies (b1). \qed
4. UCS $p$-groups with generator number at most 3

In this section we classify 2- and 3-generator UCS $p$-groups. The main result of this section is the following theorem from which Theorem 1(a)–(b) follows.

**Theorem 6.** Let $G$ be an $r$-generated non-abelian UCS $p$-group.

(a) If $p = r = 2$, then $G$ is isomorphic to the quaternion group $Q_8$, and if $p = 2$ and $r = 3$, then $G \cong G_1$ where

$$G_1 = \langle x_1, x_2, x_3 \mid x_1^p, x_2^p, x_3^p, p\text{-class } 2 \rangle$$

has order $2^6$. Further, $\text{Aut}(Q_8)^G \cong \text{GL}_2(2)$ and $\text{Aut}(G_1)^G$ has order 21.

(b) If $p \geq 3$ and $r = 2$, then $G \cong G_2$ where $G_2 = \langle x_1, x_2 \mid x_1^p, x_2^p, p\text{-class } 2 \rangle$ is extraspecial of order $p^3$ and exponent $p$. Further, $\text{Aut}(G_2)^G \cong \text{GL}_3(p)$.

(c) If $p \geq 3$ and $r = 3$, then $G$ has order $p^6$ and $G \cong G_3$ or $G_4$ where

$$G_3 = \langle x_1, x_2, x_3 \mid x_1^p, x_2^p, x_3^p, p\text{-class } 2 \rangle,$$  
and

$$G_4 = \langle x_1, x_2, x_3 \mid x_1^p = [x_2, x_3], x_2^p = [x_3, x_1], x_3^p = [x_1, x_2], p\text{-class } 2 \rangle.$$  

Further, $\text{Aut}(G_3)^G \cong \text{GL}_3(p)$ and $\text{Aut}(G_4)^G \cong \text{SO}_3(p)$.

**Proof.** (a) If $p = 2$ and $r = 2$, then $|G'| = 2$ and so $|G| = 8$. The dihedral group of order 8 has a characteristic cyclic subgroup of order 4, so the only possibility is that $G \cong Q_8$. As is well known, $Q_8$ is indeed a UCS group and $\text{Aut}(Q_8)^Q \cong \text{GL}_2(2)$. Now suppose that $p = 2$ and $r = 3$. It can be checked that every irreducible subgroup of $\text{GL}_3(2)$ has order divisible by 7. All subgroups of order 7 are conjugate in $\text{GL}_3(2)$, so we may take an arbitrary one. Its action on $\Phi(H_{2.3})$ is the sum of two non-isomorphic irreducible 3-dimensional submodules, say $(H_{2.3})^\gamma$ and $N$. Hence $H_{2.3}/N$ is a non-abelian UCS-group. A direct calculation (or an application of a computational algebra system [GAP07, BCP97]) shows that $H_{2.3}/N \cong G_1$, and $\text{Aut}(G_1)^G \cong \text{GL}_3(2)$ is non-abelian of order 21.

(b) Suppose that $p$ is odd, and $H = H_{p,2}$. Let $N$ be a subgroup of $\Phi(H)$ such that $G = H/N$ is a non-abelian UCS $p$-group. As $G' = \Phi(G)$ has order $p$, it follows that $N = H^p$. Moreover, $H/H^p$ is an extraspecial group, and $\text{Aut}(G)^G \cong \text{GL}_3(2)$ is non-abelian of order 21.

This completes the proof of (a) and (b). The proof of (c) relies on the following lemma.

**Lemma 7.** Suppose that $V$ is a 3-dimensional vector space over a finite field $\mathbb{F}$, where $\text{char}(\mathbb{F}) \neq 2$. Let $U$ be a subspace of $V \oplus A^2V$ such that $\dim U = 3$, $U \cap V = U \cap A^2V = 0$ and that $\text{GL}(V)_U$ is irreducible on $V$. Then there exists a $g \in \text{GL}(V)$ such that $Ug = W$ where

$$W = \langle e_1 - e_2 \land e_3, e_2 - e_3 \land e_1, e_3 - e_1 \land e_2 \rangle,$$

and $e_1, e_2, e_3$ is a basis for $V$. Further, $\text{GL}(V)_U = g \text{GL}(V)_W g^{-1}$ and $\text{GL}(V)_W = \text{SO}_3(\mathbb{F})$.

**Proof.** Let $e_1, e_2, e_3$ be a basis for $V$, and let $e_2 \land e_3, e_3 \land e_1, e_1 \land e_2$ be the corresponding dual basis for $A^2V$. Concatenating these bases gives a basis for $V \oplus A^2V$. We view $g \in \text{GL}(V)$ as a $3 \times 3$ matrix relative to the basis $e_1, e_2, e_3$. An easy computation shows that the transformation $g \land g \in \text{GL}(A^2V)$ defined by $(u \land v)(g \land g) = (ug) \land (vg)$, has matrix $\text{det}(g)(g^{-1})^T = \text{det}(g)g^{-T}$ relative to the above dual basis. Thus $g$ acting on $V \oplus A^2V$ has matrix

$$\begin{pmatrix} g & 0 \\ 0 & g \land g \end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & \text{det}(g)g^{-T} \end{pmatrix}.$$  

(1)
The subspace $U$ has a basis of the form $e_1 - a_1, e_2 - a_2, e_3 - a_3$ where $a_1, a_2, a_3$ is a basis for $A^2 V$. We now calculate the stabilizer $GL(V)_U$. Let $U_A$ denote the $3 \times 6$ matrix $(I \mid -A)$ where $A$ is the invertible $3 \times 3$ matrix with $i$-th row

$$(a_{i1}, a_{i2}, a_{i3}) \quad \text{where} \quad a_i = a_{i1}e_2 \wedge e_3 + a_{i2}e_3 \wedge e_1 + a_{i3}e_1 \wedge e_2.$$ 

Note that the matrix $(I \mid -A)$ possesses two $3 \times 3$ sub-blocks. We shall view $U$ as the row space of $U_A$. Let $g$ be an arbitrary invertible $3 \times 3$ matrix. Then

$$(I \mid -A) \left( \begin{array}{cc} g & 0 \\ 0 & g^{-1}A \end{array} \right) = (g \mid -A(g \wedge g))$$

which has the same row space as $(I \mid -g^{-1}A(g \wedge g))$. Thus we have, by Eq. (1), that $(U_A)g = U_{g^{-1}A(g \wedge g)} = U_{det(g)g^{-1}Ag^{-T}}$. Hence $g \in GL(V)$ stabilizes $U = U_A$ if and only if $A = g^{-1}A(g \wedge g)$, or $A$ intertwines $g$ and $g \wedge g$. In summary, $g \in GL(V)_U$ if and only if $gAg^T = (det g)A$.

The stabilizer $GL(V)_U$ is contained in the subgroup

$$\Gamma = \{ g \in GL(V) \mid g(A - A^T)g^T = (det g)(A - A^T) \}.$$

However $\Gamma$, and hence $GL(V)_U$, fixes the null space

$$\{ v \in V \mid v(A - A^T) = 0 \}.$$

As $GL(V)_U$ acts irreducibly on $V$, $A - A^T$ is either 0 or invertible. Since

$$det(A - A^T) = det((A - A^T)^T) = det(A^T - A) = (-1)^3 det(A - A^T)$$

and $\text{char}(\mathbb{F}) \neq 2$, we see that $det(A - A^T) = 0$. Thus $A - A^T = 0$, and $A$ is symmetric. Given that $A$ is invertible, $gAg^T = (det g)A$ for $g \in GL(V)_U$ implies $det(g) = 1$. In summary, $GL(V)_U$ is the special orthogonal group

$$GL(V)_U = \{ g \in GL(V) \mid gAg^T = A \text{ and } det(g) = 1 \}.$$

In particular, if $A = I$ and $W = U_I$, then

$$GL(V)_W = \{ g \in GL(V) \mid gg^T = I \text{ and } det(g) = 1 \} = SO_3(\mathbb{F}).$$

The quadratic form $Q_A : V \rightarrow \mathbb{F} : v \mapsto \frac{1}{2} v A v^T$ determines (and is determined by) a non-degenerate symmetric bilinear form $\beta_A : V \times V \rightarrow \mathbb{F} : (v, w) \mapsto v A w^T$. By diagonalizing $\beta_A$ (see [Lam73, Chapter 1, Corollary 1.2.4]), there exists $g_1 \in GL(V)$ such that $g_1^{-1}A(g_1^{-1})^T$ is a non-zero scalar matrix. Thus $(U_A)g_1 = U_{g_1^{-1}A(g_1^{-1})} = U_{g_1}$ where $\lambda I$ is a non-zero scalar matrix. However, $(U_{g_1})(\lambda^{-1}I) = U_I$. Thus $U_A g = U_I = W$ where $g = g_1 \lambda^{-1}$. \square

**Proof of Theorem 6(c).** Let $p$ be an odd prime, set $H = H_{3,3}$ and let $G = H/N$ be a 3-generator UCS $p$-group. By Lemma 2, the $GL(\mathbb{F})$-modules $\mathbb{R}$ and $H^P$ are equivalent via the $p$-th power map. The action of $GL(\mathbb{F})$ on $H^P$ is equivalent to the exterior square action. In the proof of Lemma 7, the action of $GL(V)$ on $A^2 V$ was shown to be $g \mapsto det(g)(g^{-1})^T$. Thus by Lemma 2 and Theorem 4 the stabilizer $K := GL(\mathbb{F})_N$ acts irreducibly on $\mathbb{R} \cong H^P \cong V$ and on $H^P \cong A^2 V$.

If $G$ has exponent $p$, then $H^P \leq N$. By Lemma 2, $H'$ is invariant under $GL(\mathbb{F})$, and so the subspace $N \cap H'$ must be invariant under $GL(\mathbb{F})_N$. If $1 < N \cap H < H'$, then $GL(\mathbb{F})_N$ is reducible on $H'$ contradicting the previous paragraph. Thus, by Theorem 4, $N \cap H' = 1$, and $G = H/H^P$. Hence $G$ must be isomorphic to the group $G_3$ in the statement of the theorem, and $\text{Aut}(G_3)^{\mathbb{F}} \cong GL_3(p)$.
Suppose now that $G$ has exponent $p^2$. By Theorem 4(iii), $|N| = p^3$, $N \cap H^p = 1$ and $GL(H)_N$ is irreducible. As the $GL(H)$-actions on $H^p$ and $\Lambda^2 H$ are equivalent, Lemma 7 with $F = \mathbb{F}_p$ shows that a minimal generating set $x_1, x_2, x_3$ of $G$ can be chosen satisfying the relations of $G_4$. Lemma 7 also yields that $\text{Aut}(G_4) \cong \text{SO}_3(p)$. As $\text{SO}_3(p)$ acts irreducibly on both $G/G^p$ and $G^p$, we see that $G = G_4$ is a UCS-group, as required. \hfill \Box

5. 4-generator UCS 2-groups

In this brief section we describe a computer-based classification of 4-generator UCS 2-groups. Recall that $\{x_1, x_2, x_3, x_4\}$ is a fixed minimal generating set for $H_{2,4}$. Let $y_1, y_2, y_3, y_4$ denote the squares $x_1^2, x_2^2, x_3^2, x_4^2$, and let $z_1, z_2, z_3, z_4, z_5, z_6$ denote the commutators $[x_1, x_2], [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4], [x_3, x_4]$ in $H_{2,4}$, respectively. Each group below has the form $H_{2,4}/N$ where $N$ is a subgroup of the Frattini subgroup

$$\Phi(H_{2,4}) = \langle y_1, y_2, y_3, y_4, z_1, z_2, z_3, z_4, z_5, z_6 \rangle.$$

The following theorem proves the part of Theorem 1(c) with $p = 2$. The homocyclic abelian group $H_{2,4}/N_5$ below is not included in Theorem 1(c).

**Theorem 8.** A 4-generator UCS 2-group is isomorphic to the group $H_{2,4}/N$ where $N$ is precisely one of the 9 subgroups described below:

- $N_1 = \langle y_1, y_2, y_3, y_4, z_1 z_3, z_2, z_3 z_4, z_5, z_6 \rangle$;
- $N_2 = \langle y_1, y_2 y_3, y_3 z_4, y_4, z_1 z_3, z_2, z_3 z_4, z_5, z_6 \rangle$;
- $N_3 = \langle y_1 z_1, y_2 z_1, y_3, y_4, z_1 z_2 z_3, z_2 z_3 z_5, z_3 z_4, z_6 \rangle$;
- $N_4 = \langle y_1 z_1, y_2 z_2, y_3 z_2, y_4 z_1, z_1 z_5, z_2 z_3 z_5, z_3 z_4, z_6 \rangle$;
- $N_5 = \langle z_1, z_2, z_3, z_4, z_5, z_6 \rangle$;
- $N_6 = \langle y_1 z_3, y_2, y_3, y_4 z_5, z_6 \rangle$;
- $N_7 = \langle y_1 z_2, y_2 z_5, y_3, y_4, z_1 z_6, z_2 z_5 z_6 \rangle$;
- $N_8 = \langle y_1 z_2 z_4, y_2 y_4 z_3, y_3 y_4 z_4, y_4 z_1, z_1 z_6, z_2 z_5 z_6 \rangle$;
- $N_9 = \langle y_1 z_3, y_2 z_4, y_3 z_4, y_4 z_3, z_1 z_6, z_2 z_5 z_6 \rangle$.

**Proof.** The proof relies primarily on computer calculations. One can easily verify, using the command CharacteristicSubgroups in GAP [GAP07], that each of the above 9 quotient groups is UCS 2-group. Clearly, they all are 4-generator groups.

Suppose that $G$ is a 4-generator UCS 2-group. Then $G \cong H_{2,4}/N$ where $N \leq \Phi(H_{2,4})$. If $G$ is abelian, then $G^2$ is the non-trivial and proper characteristic subgroup of $G$. In this case, $G$ must be isomorphic to the homocyclic group $H_{2,4}/N_5 \cong (C_4)^4$.

Assume now that $G$ is non-abelian. As $\Phi(G) = G'$ and $\lvert (H_{2,4})' \rvert = 2^6$, we deduce that $\lvert G \rvert \leq 2^{10}$. The classification of 2-groups with order at most $2^{10}$ is part of the computational algebra systems MAGMA and GAP [BCP97,GAP07]. Suppose that $H$ is a 4-generator group with order dividing $2^9$, where $H' = \Phi(H) = Z(H)$. We used MAGMA to compute $\text{Aut}(H)$, and checked whether $\text{Aut}(H)^\Phi(H)$ are irreducible linear groups. By Theorem 4, $H$ is UCS if and only if both of these linear groups are irreducible. In this way one can verify that if $\lvert G \rvert$ divides $2^9$, then $G$ is precisely one of the 9 quotient groups above. Looping over the groups with order $2^9$ on a computer with a 1.8 GHz CPU and 512 MB memory took approximately 20 CPU minutes.
Theorem 4. We use the proper non-trivial subspaces of $Q$-group 2-groups. Computation with GAP \cite{GAP07} shows that the group 2-groups induce on the Frattini quotient the following irreducible subgroups of $GL(4)$:

\begin{align*}
\phi(H_2,4) \cong (F_2)^4, \text{ and } (H_2,4)' \cong \Lambda^2 V.
\end{align*}

As $|G| = |\Lambda^2 V| = 2^8$, we see that $N \cap \Lambda^2 V = 0$, and so $\phi(H_2,4)$ admits the $S$-module direct decomposition $\phi(H_2,4) = N \oplus \Lambda^2 V$. Further, since $\phi(H_2,4)/N \cong \Lambda^2 V$, the action of $S$ on $\Lambda^2 V$ is irreducible by Theorem 4. We use MAGMA to loop over all irreducible subgroups $R$ of $GL(V) \cong GL(4)$, and we find that either $R$ is reducible on $\Lambda^2 V$, or the $R$-action on $\phi(H_2,4)$ fixes no 4-dimensional subspace that could correspond to $N$. This contradiction proves that no such group $G$ exists. 

The GAP and MAGMA catalogue numbers of the 9 quotient groups in Theorem 8 are \cite{SageMath, Magma, GAP07}, \cite{MAGMA}, \cite{MAGMA2}, \cite{SageMath}, \cite{MAGMA}, \cite{MAGMA}, \cite{SageMath2}, \cite{Magma}, \cite{MAGMA}. As can be deduced by using GAP or MAGMA, the automorphism groups of the 9 USC 2-groups induce on the Frattini quotient the following irreducible subgroups of $GL(4)$: $O_4^+(2)$, $O_4^-(2)$, $GL(2) \otimes GL(2) \cong S_3 \times S_3$, $I_{1}(16)$, $GL(4)(2)$, $O_4^+(2)$, $C_5 \times C_4$, $C_5$, and $\Gamma L_2(4)$ respectively.

The indexing of groups in Theorem 9, as explained later, is related to the 18 orbits of $GL(V)$ on the proper non-trivial subspaces of $\Lambda^2 V$. The indexing of groups in Theorem 9, as explained later, is related to the 18 orbits of $GL(V)$ on the proper non-trivial subspaces of $\Lambda^2 V$.

Recall the definition of $H_{p,4}$ in Section 2. Theorem 9 is a qualitative version of Theorem 1(c), and its proof relies on the classification of 4-generator $p$-groups with exponent $p$ and nilpotency class 2. In order to present the classification here, we need some notation. Since $p$ is odd, a 4-generator $p$-group $G$ with nilpotency class 2 and exponent $p$ is isomorphic to $H_{p,4}/((H_{p,4})^p N)$ where $N$ is a subgroup of $(H_{p,4})'$. Since $(H_{p,4})'$ is an elementary abelian group, we view it as a vector space over $F_p$. Assume that $H_{p,4}$ is generated by $x_1, x_2, x_3, x_4$. View the subgroup $(H_{p,4})'$ as a 6-dimensional $F_p$-subspace with standard basis $[x_1, x_2], [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4], [x_3, x_4]$. We introduce a non-degenerate quadratic form on $(H_{p,4})'$:

\begin{align*}
Q'(\alpha_1 x_1, \alpha_2 x_2, \alpha_3 x_3, \alpha_4 x_4) = \alpha_1 \alpha_6 - \alpha_2 \alpha_5 + \alpha_3 \alpha_4.
\end{align*}

Fix $\alpha \in F_p^\times$ such that $F_p^\times = \{-\alpha\}$. The following is a complete and irredundant list of the isomorphism classes of 4-generator $p$-groups $G$ with exponent $p$ and nilpotency class 2.

\begin{align*}
\text{(i)} & \quad G_0 = H_{p,4}/(H_{p,4})^p; \\
\text{(ii)} & \quad G_2 = H_{p,4}/((H_{p,4})^p, [x_1, x_2][x_3, x_4], [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4]); \\
\text{(iii)} & \quad G_4 = H_{p,4}/(H_{p,4})^p, [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4]); \\
\text{(iv)} & \quad G_6 = H_{p,4}/((H_{p,4})^p, [x_1, x_2], [x_3, x_4], [x_2, x_3][x_1, x_4], [x_1, x_3][x_2, x_4]); \\
\text{(v)} & \quad G_8 = H_{p,4}/((H_{p,4})^p, [x_1, x_4], [x_2, x_3], [x_2, x_4][x_1, x_3], [x_3, x_4]); \\
\text{(vi)} & \quad G_{14} = H_{p,4}/((H_{p,4})^p, [x_1, x_2], [x_3, x_4]); \\
\text{(vii)} & \quad G_{16} = H_{p,4}/((H_{p,4})^p, [x_1, x_2], [x_3, x_4]); \\
\text{(viii)} & \quad G_{18} = H_{p,4}/((H_{p,4})^p, [x_1, x_4], [x_1, x_3][x_2, x_4], [x_1, x_3][x_2, x_4]^{-1}).
\end{align*}

The indexing of groups in Theorem 9, as explained later, is related to the 18 orbits of $GL(V)$ on the proper non-trivial subspaces of $\Lambda^2 V$.
The quadratic form $Q'$ induces a non-degenerate symmetric bilinear form:

$$(v_1, v_2) = Q'(v_1 + v_2) - Q'(v_1) - Q'(v_2).$$

If $U$ is a subgroup in $(H_{p,4})'$, then $U^\perp$ is defined as

$$U^\perp = \{ v \in (H_{p,4})' \mid (u, v) = 0 \text{ for all } u \in U \}.$$  

Let $\alpha$ be as in Theorem 9, and define the following subgroups in $(H_{p,4})'$:

$$N_0 = 1;$$

$$N_1 = \langle [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4], [x_3, x_4] \rangle;$$

$$N_2 = \langle [x_1, x_2], [x_3, x_4]^{-1}, [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4] \rangle;$$

$$N_3 = \langle [x_1, x_2], [x_1, x_4], [x_2, x_4], [x_3, x_4] \rangle;$$

$$N_4 = \langle [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4] \rangle;$$

$$N_5 = \langle [x_1, x_2], [x_2, x_4], [x_3, x_4], [x_2, x_3][x_1, x_4]^{-1} \rangle;$$

$$N_6 = \langle [x_1, x_2], [x_3, x_4], [x_2, x_3][x_1, x_4]^{-1}, [x_1, x_3]^{\alpha}[x_2, x_4] \rangle;$$

$$N_7 = \langle [x_1, x_4], [x_2, x_4], [x_3, x_4] \rangle;$$

$$N_8 = \langle [x_1, x_3], [x_1, x_4], [x_2, x_4] \rangle;$$

$$N_9 = \langle [x_2, x_3], [x_2, x_4], [x_3, x_4] \rangle;$$

$$N_{10} = \langle [x_1, x_3], [x_1, x_4], [x_3, x_4][x_1, x_2]^{-1} \rangle;$$

$$N_{11} = \langle [x_1, x_4], [x_2, x_3], [x_2, x_4][x_1, x_3]^{-1} \rangle;$$

$$N_{12} = \langle [x_1, x_4], [x_2, x_4][x_1, x_3]^{-\alpha}, [x_1, x_2][x_3, x_4]^{-1} \rangle.$$  

For $i = 13, \ldots, 18$ set $N_i = (N_{i-12})^\perp$. That is, $N_i$ is the subgroup perpendicular to $N_{i-12}$ with respect to the symmetric bilinear form $(\cdot, \cdot)$ associated to $Q'$. For $i = 0, \ldots, 18$, let $G_i$ denote the group $H_{p,4}/((H_{p,4})^p N_i)$. Our notation is consistent in the sense that the groups $G_i$ defined here coincide with those defined in Theorem 9.

**Lemma 10.** For $p \geq 3$, every 4-generator finite $p$-group with exponent $p$ and nilpotency class 2 is isomorphic to precisely one of the 19 groups $G_0, G_1, \ldots, G_{18}$.

**Proof.** Suppose that $i \in \{0, \ldots, 5\}$ and let $\mathcal{N}_i$ denote the set of subgroups with order $p^i$ in $(H_{p,4})'$. Then, for $M_1, M_2 \in \mathcal{N}_i$, we have $H_{p,4}/((H_{p,4})^p M_1) \cong H_{p,4}/((H_{p,4})^p M_2)$ if and only if $M_1$ and $M_2$ lie in the same $\text{GL}(\overline{H_{p,4}})$-orbit (see [O'B90, Theorem 2.8]). Therefore it suffices to show that the subgroups $N_0, \ldots, N_{18}$ form a complete and irredundant set of representatives of the $\text{GL}(\overline{H_{p,4}})$-orbits in $\bigcup \mathcal{N}_i$. A simple computation shows that $Q'$ is stabilized by $\text{GL}(\overline{H_{p,4}})$ up to scalar multiples (alternatively see [KLU90, Proposition 2.9.1(vii)]) Thus $M_1$ and $M_2$ lie in the same $\text{GL}(\overline{H_{p,4}})$-orbit if and only if $(M_1)^\perp$ and $(M_2)^\perp$ do. Therefore we only need to verify that the set $\{N_1, \ldots, N_{12}\}$ is a set of representatives of the $\text{GL}(\overline{H_{p,4}})$-orbits in $\mathcal{N}_5 \cup \mathcal{N}_4 \cup \mathcal{N}_3$. These orbits have long been known; they are listed already in Brahana’s paper [Bra40]. Our list above is taken from the recent classification of finite $p$-groups of order dividing $p^7$, see [NOVL04, OVL05]. \(\square\)
Recall that \( \{x_1, x_2, x_3, x_4\} \) is a fixed generating set for \( H_{p,4} \). Risking confusion, let \( V \) denote a 4-dimensional vector space over \( \mathbb{F}_p \), with basis \( x_1, x_2, x_3, x_4 \). This way the symbol \( x_i \) may refer to an element of \( H_{p,4} \), or to an element of \( V \). However, elements of the group \( H_{p,4} \) are written multiplicatively, while elements of \( V \) are written additively. There is a natural bijection \( \Psi : A^2V \rightarrow (H_{p,4})' \) mapping \( x_1 \wedge x_j \mapsto [x_i, x_j] \). Define a quadratic form \( Q \) on \( A^2V \) by \( Q(w) = Q'(\Psi(w)) \) for all \( w \in A^2V \). The value of the form \( Q \) is given by:

\[
Q(\alpha_1 x_1 \wedge x_2 + \alpha_2 x_1 \wedge x_3 + \alpha_3 x_1 \wedge x_4 + \alpha_4 x_2 \wedge x_3 + \alpha_5 x_2 \wedge x_4 + \alpha_6 x_3 \wedge x_4)
= \alpha_1 \alpha_6 - \alpha_2 \alpha_5 + \alpha_3 \alpha_4.
\]

Theorem 4 says that a subspace \( U \leq A^2V \) gives rise to an exponent-\( p \) UCS \( p \)-group \( G_U := H_{p,4}/((H_{p,4})'\Psi(U)) \) if and only if the stabilizer \( GL(V)_U \) is irreducible on both \( V \) and \( A^2V/U \). For \( i = 0, \ldots, 18 \), let \( U_i \) denote the subspace \( \Psi^{-1}(N_i) \). Therefore we can check which of the groups \( G_0, \ldots, G_{18} \) are UCS by checking, for \( i = 0, \ldots, 18 \), whether \( GL(V)_{U_i} \) is irreducible on \( V \) and on \( A^2V/U_i \). This is carried out in the rest of this section.

A subspace \( U \leq A^2V \) is said to be degenerate if \( U \cap U^\perp \neq \{0\} \); otherwise it is said to be non-degenerate. A subspace \( U \) is said to be totally isotropic if \( Q(u) = 0 \) for all \( u \in U \).

**Lemma 11.** If \( U \) is a degenerate subspace of \( A^2V \), then \( GL(V)_U \) acts reducibly on \( V \) or \( A^2V/U \), and thus the \( p \)-group \( G_U := H_{p,4}/((H_{p,4})'\Psi(U)) \) is not a UCS-group. Further, the subspaces \( U_i \) for \( i \in \{1, 3, 5, 7, 8, 9, 10, 12, 13, 15, 17\} \) are degenerate with respect to \( Q \).

**Proof.** Suppose that \( U \) is degenerate. Then \( U \cap U^\perp \neq \{0\} \), and \( U + U^\perp \) is a proper subspace of \( A^2V \). Thus if \( U \neq \{0\} \), then \( GL(V)_{U \perp} = GL(V)_{U^\perp} \) is reducible on \( A^2V/U \) as it fixes the proper non-zero subspace \( (U + U^\perp)/U \). Assume henceforth that \( U \perp \leq U \).

Lemma 10 says that there are precisely 19 different \( GL(V) \)-orbits on the proper subspaces of \( A^2V \), and representatives of the orbits are \( U_0, U_1, \ldots, U_{18} \). A straightforward calculation shows that \( U_i \) is degenerate if and only if \( i \in \{1, 3, 5, 7, 8, 9, 10, 12, 13, 15, 17\} \). Moreover, the only \( U_i \) satisfying \( U \leq U_i \) are \( U_1, U_3, U_7, U_9 \). It is possible to prove case-by-case that the group \( G_{U_i} \), for \( i \in \{1, 3, 7, 9\} \), is not UCS. Rather than exhibiting a case-by-case analysis, we offer a geometric proof, which we find more elegant.

We shall show that for each degenerate subspace \( U \leq A^2V \) with \( U \perp \leq U \), the stabilizer \( GL(V)_{U \perp} = GL(V)_{U \perp} \) is a reducible subgroup of \( GL(V) \). Since \( \dim(U^\perp) = 6 - \dim(U) \), we see that \( \dim(U^\perp) = 1, 2, 3 \) and \( U \) is a totally isotropic subspace of \( A^2V \). First, suppose that \( \dim(U^\perp) = 1 \). By [Tay92, p. 187], there exist linearly independent vectors \( v_1, v_2 \in V \) such that \( U^\perp = \langle v_1 \wedge v_2 \rangle \) and hence \( GL(V)_{U \perp} \) fixes \( \langle v_1, v_2 \rangle \) and so is reducible. Second, suppose that \( \dim(U^\perp) = 2 \). Then also by [Tay92, Lemma 12.15], \( U^\perp \) has the form \( \langle v_1 \wedge v_3, v_2 \wedge v_3 \rangle \) where \( v_1, v_2, v_3 \in V \) are linearly independent. Thus \( GL(V)_{U \perp} \) fixes \( \langle v_1, v_2, v_3 \rangle \). Finally, suppose that \( \dim(U^\perp) = 3 \), then by [Tay92, Theorem 12.16], \( U^\perp \) equals \( W_1 \wedge W_2 \) or \( W_3 \wedge W_3 \) where \( W_1, W_2 \) are subspaces of \( V \) of dimension 1 and 3 respectively. Thus \( GL(V)_{U \perp} \) fixes \( W_1 \) or \( W_2 \), and so is reducible. \( \square \)

The proof of the converse of Lemma 11 is substantially harder. It is noteworthy that in the proof of Lemma 12 below, \( Aut(G)_{\overline{Q}} \) is commonly a maximal group from one of Aschbacher’s [Asc84] classes.

**Lemma 12.** If \( U \) is a non-degenerate subspace of \( A^2V \), then \( GL(V)_{U \perp} \) acts irreducibly on \( V \) and \( A^2V/U \), and thus the \( p \)-group \( G_U := H_{p,4}/((H_{p,4})'\Psi(U)) \) is a UCS-group. Further, the subspaces \( U_i \) for \( i \in \{0, 2, 4, 6, 11, 14, 16, 18\} \) are non-degenerate with respect to \( Q \).

**Proof.** As remarked in the proof of Lemma 11, \( U_0, U_1, \ldots, U_{18} \) is a complete and irredundant list of representatives of \( GL(V) \)-orbits on the proper subspaces of \( A^2V \). Moreover, \( U_i \) is non-degenerate if
and only if \( i \in \{0, 2, 4, 6, 11, 14, 16, 18\} \). Denote the stabilizer \( \text{GL}(V)_{U_i} \) by \( K_i \). We prove below case-by-case that \( K_i \) acts irreducibly on \( V \) and \( \Lambda^2 V / U_i \) for \( i \in \{0, 2, 4, 6, 11, 14, 16, 18\} \). The groups \( K_i \) identified below are also of interest.

Since \( \text{GL}(V) \) is irreducible on \( V \) and \( \Lambda^2 V \), \( G_0 \) is a UCS-group. Suppose henceforth that \( U_i \neq 0 \). For non-degenerate \( U \), \( \Lambda^2 V = U \oplus U^\perp \) and \( \text{GL}(V)_{\perp} = \text{GL}(V)_{U \perp} \). Since \( U_{i+12} = U_i \perp \), for \( 1 \leq i \leq 6 \), we see that \( K_i = K_{i+12} \). Thus it suffices to prove that \( K_i \) is irreducible on the spaces \( V \), \( U_i \), and \( U_i^\perp \cong \Lambda^2 V / U_i \) for \( i \in \{2, 4, 6, 11\} \).

Consider first the stabilizer \( K_2 \). Note that \( U_2^\perp = U_{14} = (x_1 \wedge x_2 + x_3 \wedge x_4) \). View \( g \in \text{GL}(V) \) as a \( 4 \times 4 \) matrix with respect to the basis \( x_1, x_2, x_3, x_4 \) of \( V \). The equation

\[
(x_1 \wedge x_2 + x_3 \wedge x_4)(g \wedge g) = \alpha(x_1 \wedge x_2 + x_3 \wedge x_4)
\]

for some non-zero \( \alpha \in \mathbb{F}_p \), gives a linear system equivalent to the matrix equation

\[
g^T J g = \alpha J
\]

Thus \( g \in K_2 \) if and only if \( g \) preserves the alternating form \( J \) up to a scalar factor. In other words, \( K_2 \cong \text{Sp}_4(p) \). Clearly, \( \text{Sp}_4(p) \) is irreducible on \( V \), and on the 1-dimensional subspace \( U_{14} \). Additionally, the \( K_2 \)-action on \( U_2 \) is irreducible as \( K_2 \) contains a subgroup isomorphic to \( \Omega_5(p) \) (see [KL90, Proposition 2.9.1(vi)]) and \( \Omega_5(p) \) acts irreducibly on the 5-dimensional space \( U_2 \).

Consider now the stabilizer \( K_4 \). Set \( L_1 = (x_1, x_2) \) and \( L_2 = (x_3, x_4) \). Let \( H \) be the stabilizer of the decomposition \( V = L_1 \oplus L_2 \). Then \( H \cong \text{GL}_2(p) \rtimes C_2 \) and simple argument shows that \( H = K_4 \). We claim that \( K_4 \) is irreducible on \( V \), \( U_4 \), and on \( U_{16} \). Denote by \( K_4 \) the stabilizer in \( K_4 \) of the subspaces \( L_1 \) and \( L_2 \). Then \( K_4 \) coincides with the stabilizer of \( P_1 := (x_1 \wedge x_2) \) and \( P_2 := (x_3 \wedge x_4) \). The only proper and non-trivial \( K_4 \)-submodules of \( V \) are \( L_1 \) and \( L_2 \). These are swapped by \( K_4 \), and so \( K_4 \) is irreducible on \( V \). Suppose that \( g \in K_4 \) is represented by the block-matrix

\[
\begin{pmatrix}
A & 0 \\
0 & B
\end{pmatrix}
\]

Then the action of \( g \) on \( U_{16} \) relative to the basis \( x_1 \wedge x_2, x_3 \wedge x_4 \) corresponds to the diagonal matrix \( \text{diag}(\det A, \det B) \). Therefore the only proper, non-trivial \( K_4 \)-submodules of \( U_{16} \) are \( P_1 \) and \( P_2 \). However, \( K_4 \) contains an element that swaps \( P_1 \) and \( P_2 \), and thus \( K_4 \) is irreducible on \( U_{16} \). Recall that \( U_4 = (x_1 \wedge x_2, x_3 \wedge x_4) \). The action of \( K_4 \) on \( U_4 \) is equivalent to the action of \( \text{GL}_2(p) \times \text{GL}_2(p) \) on the tensor product \( (x_1, x_2) \otimes (x_3, x_4) \). The equivalence is realized by the map \( x_i \wedge x_j \mapsto x_i \otimes x_j \). Since \( \text{GL}_2(p) \) is absolutely irreducible, [Rob96, 8.4.2] can be used to obtain that the outer tensor product \( \text{GL}_2(p) \otimes \text{GL}_2(p) \) acts irreducibly on \( \mathbb{F}_p^4 \). Hence \( K_4 \), and therefore \( K_4 \), acts irreducibly on \( U_4 \).

The next stabilizer to consider is \( K_6 \). We shall show that \( K_6 \) acts irreducibly on \( V \), \( U_6 \) and \( U_{18} = U_6^\perp \). The definition of the subspace \( U_6 \) involves a fixed \( \alpha \in \mathbb{F}_p^\times \) such that \( -\alpha \) generates \( \mathbb{F}_p^\times \). Note that

\[
U_{18} = U_6^\perp = (x_1 \wedge x_4 + x_2 \wedge x_3, \alpha x_1 \wedge x_3 - x_2 \wedge x_4).
\]

(2)

We shall prove that \( K_6 = K_{18} \cong \Gamma L_2(p^2) \). Identify \( V \) with \( \mathbb{F}_p^2 \oplus \mathbb{F}_p^2 \) as follows. Since \( -\alpha \) is a non-square in \( \mathbb{F}_p \), its square roots, \( \pm \beta \), lie in \( \mathbb{F}_p^2 \setminus \mathbb{F}_p \). Then \( (1, 0), (\beta, 0), (0, 1), (0, \beta) \) is a \( \mathbb{F}_p \)-basis of \( \mathbb{F}_p^2 \oplus \mathbb{F}_p^2 \). Identify the elements \( x_1, x_2, x_3, x_4 \) with \( (1, 0), (\beta, 0), (0, 1), (0, \beta) \), respectively. We view \( \Gamma L_2(p^2) \) as a subgroup of \( \text{GL}_4(p) \) under the identification above.

Let \( \varepsilon : A_{p^2}^2 \to V \to A_{p^2}^2 V \) be the unique \( \mathbb{F}_p \)-linear map satisfying \( \varepsilon(u \wedge v) = u \wedge v \). Easy computation shows that \( U_6 \leq \ker \varepsilon \). On the other hand, by dimension counting, we have that \( \text{dim}(\ker \varepsilon) = 4 \), which
gives \( U_6 = \ker \varepsilon \). Suppose that \( U \) is a 2-dimensional \( F_p \)-subspace in \( V \). Then \( U \) is an \( F_p^2 \)-subspace of \( V \) if and only if \( \varepsilon(U \cup U) = 0 \); that is, \( U \cup U \leq U_6 \). Thus \( K_6 \) is the setwise stabilizer of the \( F_p^2 \)-subspaces of \( V \).

Clearly, the group \( \Gamma L_2(p^2) \) permutes the \( F_p^2 \)-subspaces of \( V \), and hence \( \Gamma L_2(p^2) \leq K_6 \). In order to prove the reverse containment, let \( g \in GL_4(p) \) and suppose that \( g \) stabilizes \( U_6 \). Then \( g \) permutes the \( F_p^2 \)-subspaces. Thus we have, for \( v \in V \) and \( \lambda \in F_p^2 \), that

\[
(\lambda v)g = \mu(vg)
\]

(3)

with some \( \mu \in F_p^2 \). Let \( v_1, v_2 \in V \) be linearly independent over \( F_p^2 \). Then, as \( g \) permutes the \( F_p^2 \)-subspaces, \( v_1g \) and \( v_2g \) are linearly independent over \( F_p^2 \). Let \( \mu_1, \mu_2 \in F_p^2 \) such that \( (\lambda v_1)g = \mu_1(v_1g) \) and \( (\lambda v_2)g = \mu_2(v_2g) \). Then there is some \( v \in F_p^2 \) such that \( (\lambda v_1 + \lambda v_2)g = v(v_1g + v_2g) \), but also \( (\lambda v_1 + \lambda v_2)g = \mu_1(v_1g) + \mu_2(v_2g) \). This shows that \( \mu_1 = \mu_2 \), and therefore \( \mu \) is independent of \( v \) in Eq. (3). Hence for all \( \lambda \in F_p^2 \) there is some \( \psi(\lambda) \in F_p^2 \) such that \( (\lambda v)g = \psi(\lambda)(vg) \). The map \( \psi \) is a field automorphism. Since \( \psi \) fixes \( F_p^2 \) pointwise, \( \psi \) is a member of the Galois group of \( F_p^2 \) over \( F_p \). Hence \( g \) is a semilinear transformation which gives that \( K_6 \leq \Gamma L_2(p^2) \). Therefore \( K_6 = \Gamma L_2(p^2) \), as claimed.

To show that \( K_6 \) acts irreducibly on \( U_6 \) and \( U_{18} \) let us take a Singer cycle, i.e., an element \( g \) of order \( p^4 - 1 \) in \( GL_2(p^2) \) \( < \) \( K_6 \). Let \( \varepsilon \in F_p^4 \) be an eigenvalue of \( g \). Then the eigenvalues of \( g \) are \( \varepsilon, \varepsilon p, \varepsilon p^2, \varepsilon p^3 \), and so the eigenvalues of \( g \wedge g \) on \( V \wedge V \) are \( \eta = \varepsilon^{1+p}, \eta p, \eta p^2, \eta p^3, \theta = \varepsilon^{1+p^2} \) and \( \theta p \). The order of \( \eta \) is \( (p^4 - 1)/(p + 1) > p^2 \), hence \( \eta, \eta p, \eta p^2, \eta p^3 \) are all different. Similarly, the order of \( \theta \) is \( p^2 - 1 \), so \( \theta \) and \( \theta p \) are distinct. This means that the characteristic polynomial of \( g \wedge g \) is the product of two irreducible factors, one of degree 4, the other of degree 2. Hence \( V \wedge V \) decomposes into a direct sum of a 4-dimensional and a 2-dimensional irreducible \( \langle g \wedge g \rangle \)-submodules. Since \( U_6 \) and \( U_{18} \) are invariant under \( g \wedge g \), we obtain that these are the irreducible summands.

Finally, consider \( K_{11} \). We identify \( V \) with the tensor product \( U_1 \otimes U_2 \) \( \subset \) \( \langle v_1, v_2 \rangle \) by assigning \( x_1, x_2, x_3, x_4 \) to \(-u_1 \otimes v_1, u_2 \otimes v_1, u_2 \otimes v_2, u_1 \otimes v_2 \), respectively. Hence the group \( GL_2(p) \times GL_2(p) \) acts on \( V \), and the action of the element

\[
\begin{pmatrix}
\alpha_{11} & \alpha_{12} \\
\alpha_{21} & \alpha_{22}
\end{pmatrix}
\otimes
\begin{pmatrix}
\beta_{11} & \beta_{12} \\
\beta_{21} & \beta_{22}
\end{pmatrix}
\]

is represented by the matrix

\[
\begin{pmatrix}
\alpha_{11}\beta_{11} & -\alpha_{12}\beta_{11} & -\alpha_{12}\beta_{12} & -\alpha_{11}\beta_{12} \\
-\alpha_{21}\beta_{11} & \alpha_{22}\beta_{11} & \alpha_{22}\beta_{12} & \alpha_{21}\beta_{12} \\
-\alpha_{21}\beta_{21} & \alpha_{22}\beta_{21} & \alpha_{22}\beta_{22} & \alpha_{21}\beta_{22} \\
-\alpha_{11}\beta_{21} & -\alpha_{12}\beta_{21} & -\alpha_{12}\beta_{22} & -\alpha_{11}\beta_{22}
\end{pmatrix}.
\]

(4)

The kernel of the action of \( GL_2(p) \times GL_2(p) \) on \( V \) equals \( \{ \lambda I \otimes \lambda^{-1} I \mid \lambda \in F_p^* \} \). Thus the central product \( GL_2(p) \circ GL_2(p) \) acts faithfully on \( V \). Let \( H \) denote the group of all matrices of the form (4). Elementary, but cumbersome, calculation shows that the group \( H \) is the stabilizer of \( U_{11} \), and so \( H = K_{11} \). In particular \( K_{11} \equiv GL_2(p) \circ GL_2(p) \). As \( GL_2(p) \) is absolutely irreducible on \( F_p^2 \), by [Rob96, 8.4.2], \( K_{11} \) is irreducible on \( V \).

Consider the subgroups \( T_1 \) and \( T_2 \) of \( K_{11} \) consisting of the elements of the form

\[
\begin{pmatrix}
\alpha_{11} & \alpha_{12} \\
\alpha_{21} & \alpha_{22}
\end{pmatrix}
\otimes
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\quad \text{and} \quad
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
\otimes
\begin{pmatrix}
\beta_{11} & \beta_{12} \\
\beta_{21} & \beta_{22}
\end{pmatrix}.
\]
Simple computation shows that the action of a generic element of $T_1$ on $U_{11}$ is represented by the matrix

$$
\begin{pmatrix}
\alpha_{11}^2 & -\alpha_{12}^2 & -\alpha_{12}\alpha_{11} \\
-\alpha_{21}^2 & \alpha_{22}^2 & \alpha_{22}\alpha_{21} \\
-2\alpha_{21}\alpha_{11} & 2\alpha_{22}\alpha_{12} & \alpha_{22}\alpha_{11} + \alpha_{12}\alpha_{21}
\end{pmatrix}.
$$

Since $T_1$ is isomorphic to $GL_2(p)$, the derived subgroup $(T_1)'$ is isomorphic to $SL_2(p)$ and simple computation shows that $(T_1)'$ induces a subgroup of $SL(U_{11})$. Moreover, $(T_1)'$ preserves the symmetric bilinear form

$$
(\alpha_1 x_1 \wedge x_4 + \alpha_2 x_2 \wedge x_3 + \alpha_3 (x_2 \wedge x_4 - x_1 \wedge x_3), \beta_1 x_1 \wedge x_4 + \beta_2 x_2 \wedge x_3 + \beta_3 (x_2 \wedge x_4 - x_1 \wedge x_3))
$$

$$
= -\alpha_1\beta_2 - \alpha_2\beta_1 - 2\alpha_3\beta_3.
$$

It is shown in [KL90, Proposition 2.9.1(ii)] that $(T_1)'$ induces $\Omega(\hat{Q})$, where $\hat{Q}$ is the quadratic form induced by the above bilinear form. As $\Omega(\hat{Q})$ is irreducible, we obtain that $K_{11}$ is irreducible on $U_{11}$. Replacing $T_1$ by $T_2$, the same argument shows that $K_{11}$ is irreducible on $U_{11}'$. \qed

The proof of Theorem 9 is now straightforward.

**The proof of Theorem 9.** As explained in Lemma 12, $G_i$ is UCS if and only if $GL(V)_{U_i}$ is irreducible on both $V$ and $A^2 V/U_i$. Hence Lemmas 11 and 12 imply Theorem 9. \qed

UCS $p$-groups with exponent $p^2$ are studied in the next section. It follows from Theorems 9 and 4 that a 4-generator exponent-$p^2$ UCS $p$-group is a quotient of either $H_{p,4}/N_{16}$ or $H_{p,4}/N_{18}$. Determining precisely which of these two cases leads to UCS $p$-groups involves subtle isomorphism problems which depend on the value of the prime $p$. This is illustrated in the next section.

7. Exterior self-quotient modules

The study of UCS $p$-groups with exponent $p^2$ is reduced by Theorem 5(b) to considering a problem in representation theory. Recall that the concepts of ESQ-modules and ESQ-groups were defined in Section 3. Unlike the property of irreducibility, the ESQ-property is preserved under subgroups and field extensions, as shown by the following lemma.

**Lemma 13.** Let $V$ be an ESQ $\mathbb{F}K$-module. Then

(a) every subgroup $H$ of $K$ is also an ESQ-subgroup of $GL(V)$;
(b) $V \otimes_{\mathbb{F}} E$ is an ESQ $EK$-module for every extension field $E$ of $\mathbb{F}$;
(c) $K$ contains no non-trivial scalar matrices, and $\dim(V) \geq 3$.

**Proof.** Parts (a) and (b) are routine to verify. If a scalar matrix $\lambda I$ lies in $K$, then it follows from $A^2 V/U \cong V$ that $\lambda^2 = \lambda$ and hence $\lambda = 1$. In addition, $\dim(A^2 V) \geq \dim(V)$ implies $\dim(V) \geq 3$. Hence part (c) holds. \qed

An irreducible ESQ-module can give rise to a smaller-dimensional irreducible module over a larger field which does not enjoy the ESQ-property. For example, an irreducible, but not absolutely irreducible, ESQ-subgroup of $GL_2(\mathbb{F}_q)$ gives rise to an irreducible subgroup of $GL_4(\mathbb{F}_{q^n})$ which is not an ESQ-subgroup by Lemma 13(c).

Let $r$ and $q$ be coprime integers. Denote the order of $q$ modulo $r$ by $\text{ord}_r(q)$. Then $\text{ord}_r(q)$ is the smallest positive integer $n$ satisfying $q^n \equiv 1 \pmod{r}$. **Warning:** The variables $p$ and $r$ have different meanings in the following discussion about ESQ-groups, to the previous discussion about UCS-groups.
Theorem 14. Let $p$ be a prime, $q$ a power of a prime (possibly distinct from $p$), and let $K$ be a minimal irreducible ESQ-subgroup of $GL_p(q)$. Then one of the following holds:

(a) $K$ is not absolutely irreducible, $r := |K|$ is prime, $\text{ord}_r(q) = p$ and there exist distinct $\alpha, \beta \in (q) \subseteq F_q^\times$ such that $\alpha + \beta = 1$;

(b) $K$ is an absolutely irreducible non-abelian simple group;

(c) $K$ is absolutely irreducible, $|K| = pr^s$ where $r$ is a prime different to $p$, $\text{ord}_r(q) = 1$, and $s = \text{ord}_p(r)$.

Moreover, $K'$ is an elementary abelian group of order $r^2$ and $K/K'$ has order $p$ and acts irreducibly on $K'$.

Proof. Denote by $V = (F_q)^p$ the corresponding ESQ $F_qK$-module. Here $p$ and $\text{char}(F_q)$ may be distinct primes. By Lemma 13(a), subgroups of ESQ-groups are ESQ-groups, and hence by the minimality of $K$, proper subgroups of $K$ act irreducibly on $V$. If $H$ is a non-trivial abelian normal subgroup of $K$, then by Clifford’s theorem either $H$ acts irreducibly on $V$, or $V = V_0 \oplus V_1 \oplus \cdots \oplus V_{p-1}$ is an internal direct sum of $p$ pairwise non-isomorphic 1-dimensional $H$-submodules. (If $V_0, V_1, \ldots, V_{p-1}$ were all isomorphic, then $H$ would contain non-trivial scalar matrices contrary to Lemma 13(c).)

(a) Suppose that $K$ does not act absolutely irreducibly on $V$. By Lemma 13(b) we may view $K$ as an ESQ-subgroup of $GL_p(E)$ where $E$ denotes the algebraic closure of $F_q$. The module $E^p = W \oplus \sigma(W) \oplus \cdots \oplus \sigma^{p-1}(W)$ where $\sigma : E \rightarrow E$ is the $q$-th power (Frobenius) automorphism, and $\sigma(W)$ denotes an $EK$-module algebraically conjugate irreducible 1-dimensional $K$-submodules by [HB82, Theorem VII.116]. This proves that $K$ is abelian. We argue that $r := |K|$ is prime. If not, then $K$ has a proper non-trivial normal subgroup $H$. By the first paragraph of the proof, $V$ decomposes as the sum of 1-dimensional $H$-modules. In particular, an element $h \in H$ has an eigenvalue, $\lambda$, say, in $E$. Since $h$ commutes with $K$, the linear transformation $h$ is a $K$-endomorphism of $V$, and so are the transformations $\lambda I$ and $h - \lambda I$. As $h - \lambda I$ is not invertible, Schur’s lemma shows that $h - \lambda I = 0$, and so $h$ coincides with the scalar matrix $\lambda I$. However, as, by Lemma 13(c), $K$ contains no non-trivial scalar matrices, we obtain that $h = I$. Hence the only proper subgroup of $K$ is the trivial subgroup, which shows that $r$ is prime.

Then $E^p = W \oplus \sigma(W) \oplus \cdots \oplus \sigma^{p-1}(W)$ where $\sigma : E \rightarrow E$ is the $q$-th power (Frobenius) automorphism, and $\sigma(W)$ denotes an $EK$-module algebraically conjugate irreducible 1-dimensional $K$-submodules by [HB82, Definition VII.113]. Further, $\sigma^p(W) \cong W$. The exterior square of $E^p$ is isomorphic to a direct sum $\bigoplus_{0 \leq i < j < p} \sigma^i(W) \wedge \sigma^j(W)$. Thus $W \cong \sigma^i(W) \wedge \sigma^j(W)$ for some $0 \leq i < j < p$, as $E^p$ is an ESQ-module. Suppose that $K = \langle g \rangle$. Then $g$ is conjugate in $GL_p(E)$ to a diagonal matrix $\text{diag}(\xi, \xi^q, \ldots, \xi^{q^{p-1}})$ where $\xi \in E^\times$ has order $r$. It follows from $q^{p-1} \equiv 1 \mod p$, that $\text{ord}_p(q) = 1$ or $p$. The first possibility does not arise as $g$ is not a scalar matrix. The condition $W \cong \xi^i(W) \wedge \xi^j(W)$ implies that $1 \equiv q^i + q^j \mod p$ where $\alpha = q^i$ and $\beta = q^j$ are distinct powers of $q$. This completes the proof of part (a).

(b) Suppose now that $K$ is a simple group acting absolutely irreducibly on $V$. Then $K$ must be non-abelian.

(c) Suppose now that $K$ acts absolutely irreducibly on $V$ and $K$ is not simple. Let $N$ be minimal normal subgroup of $K$. Then $N$ is a proper subgroup of $K$ and so acts reducibly. Let $V = V_0 \oplus \cdots \oplus V_{p-1}$ be a direct sum of $p$ irreducible 1-dimensional $N$-submodules. It follows that $N$ is abelian. Suppose that $|N| = r^n$ where $r$ is prime. By the first paragraph of this proof, $V_0, \ldots, V_{p-1}$ are pairwise non-isomorphic. Since $N$ has a non-trivial 1-dimensional module over $F_q$, it follows that $r$ divides $q - 1$, or $\text{ord}_p(q) = 1$.

By Clifford’s theorem, $K$ acts transitively on the set $\{V_0, \ldots, V_{p-1}\}$. Choose $g \in K$ that induces a $p$-cycle. By renumbering if necessary, assume that $V_1g = V_{1+i}$ where the subscripts are read modulo $p$. Choose $0 \neq e_0 \in V_0$ and set $e_i = e_0g^i$. Then $e_0g^p = \lambda e_0$ for some $\lambda \in F_q$. Since $g^p$ is the scalar matrix $\lambda I$, it follows from Lemma 13(c) that $\lambda = 1$. Since $\langle g \rangle N$ acts irreducibly on $V$, it follows by minimality that $K = \langle g \rangle N$ has order $p^r$. $K$ is a direct product of $C_r$ wr $C_p$. The base group $(C_p)^p$ may be identified with the vector space $(F_r)^p$, and $N$ may be identified with an irreducible $F_rC_p$-submodule of $(F_r)^p$. Since the derived subgroup $K'$ equals $N$, it follows that $r \neq p$. By Maschke’s theorem $(F_r)^p$ is a completely reducible $F_rC_p$-module. Since no $V_i$ is the trivial module, $N$ corresponds to an irreducible $F_rC_p$-submodule of $(F_r)^{p-1}$. However, $(F_r)^{p-1}$ is the direct sum of $(|p - 1|/\text{ord}_p(r))$ irreducible $F_rC_p$-submodules each of dimension $\text{ord}_p(r)$. This proves that $s = \text{ord}_p(r)$, and completes the proof. $\square$
In Theorem 14(a), (c), the order $|N| = r^4$ of a minimal normal subgroup of $K$ is restricted. For instance, if $p$ and $q$ are given, then $r^4$ must divide $|GL_p(F_q)|$. The following theorem shows that case (b) of Theorem 14 does not arise in dimension 5.

**Theorem 15.** Let $q$ be a prime power, and let $K$ be a minimal irreducible ESQ-subgroup of $GL_5(q)$. Then case (b) of Theorem 14 does not arise, and more can be said about cases (a) and (c):

(a) $K$ is not absolutely irreducible, $|K| = 11$, and ord$_{11}(q) = 5$,
(b) $K$ is absolutely irreducible of order 55 and ord$_{11}(q) = 1$.

Furthermore, both of these possibilities arise.

**Proof.** Assume that $K$ satisfies case (a) of Theorem 14. Then $|K| = r$ is prime, ord$_r(q) = 5$, and there exist $\alpha = q^i, \beta = q^j$ $(0 < i, j < 5)$ with $\alpha + \beta \equiv 1 \pmod{r}$. Let $C \in GL_5(F_r)$ be the permutation matrix corresponding to the cycle $(1, 2, 3, 4, 5)$, and let $v = (q^i, q^j, q^3, q, 1) \in F_r^5$. Then $vC = v\alpha$ and $v(I - C - C^t) = (1 - \alpha - \beta)v = 0$. Thus det$(I - C - C^t) = 0$. A direct calculation shows that det$(I - C - C^t)$ equals $-1$ when $i + j \equiv 0 \pmod{5}$, and $-11$ otherwise. Hence we have that $r = 11$.

As the subgroup $(q) \subseteq F_{11}^*$ has order $p = 5$, we have that $(q) = \{1, 3, 4, 5, 9\} = (F_{11}^*)^2$, and hence $q = 3, 4, 5, 9 \pmod{11}$. Note that $\alpha = 3$ and $\beta = 9$ satisfy $\alpha + \beta = 1$ in $F_{11}$. Conversely, if ord$_{11}(q) = 5$, then the cyclotomic polynomial $\Phi_{11}(x) = x^{10} + \cdots + x + 1$ factors over $F_q$ as a product of two distinct irreducible quintics. The companion matrix of either of these quintics generates an irreducible (but not absolutely irreducible) ESQ-subgroup of $GL_5(F_q)$ of order 11.

Suppose now that case (c) of Theorem 14 holds. Then we obtain, as above, that $r = 11$ and $s = \text{ord}_5(11) = 1$. Therefore $K \cong \langle g, n \mid g^2 = n^{11} = 1, g^{-1}ng = n^t \rangle$ where ord$_{11}(t) = 5$ and $|K| = 55$. By replacing $g$ by a power of itself, we may assume that $t = 3$. Conversely, there is an irreducible ESQ-subgroup $K$ of $GL_5(F_q)$ of order 55 if $q^5 \equiv 1 \pmod{11}$. To see this apply Theorem 18 below with $K = K_L$ where $L = (F_{11}^*)^2 = \{1, 3, 4, 5, 9\}$. Note that $\alpha = 3, \beta = 9$ satisfy $\alpha + \beta = 1$ in $F_{11}$, and the condition $q \in L$ is equivalent to $q^5 \equiv 1 \pmod{11}$. Here $K_L$ is a minimal ESQ-subgroup if an only if $q \equiv 1 \pmod{11}$.

Suppose now that case (b) of Theorem 14 holds, and $K$ is a non-abelian simple (absolutely) irreducible ESQ-subgroup of $GL_3(q)$ where $q = p^k$ and char$(F_q) = p$. As $K$ is non-abelian simple, we have $K \subseteq SL_3(q)$ and $K \cap Z(SL_3(q)) = 1$. Thus $K$ is isomorphic to an irreducible subgroup of $PSL_3(q)$. Consider first the case when $p = 2$. The irreducible subgroups of $PSL_3(2^k)$ were classified by Wagner [Wag78]. As $K$ is simple, it must be isomorphic to one of the following groups: $PSL_2(11), PSL_2(2^2)$ where $\ell | k$, or $PSL_3(4^t)$ where $2\ell | k$. We shall use Lemma 13(a) to show that none of these possibilities give irreducible ESQ-subgroups of $GL_3(q)$. Since $PSL_3(2) \leq PSL_3(2^t)$ and $PSL_2(11) \leq PSL_2(4^t)$ for all $\ell$, minimality implies that $K$ is an irreducible (and hence absolutely irreducible) group isomorphic to $PSL_2(11)$ or $PSL_3(2)$. The Atlas [WWT8] lists (up to isomorphism) the irreducible 5-dimensional modules for $PSL_2(11)$ and $PSL_5(2)$ in characteristic 2. There are four: two for $PSL_2(11)$ over $F_4$, and two for $PSL_5(2)$ over $F_2$. Straightforward computation shows that the exterior square of each of these is irreducible. Thus no ESQ-groups arise when $p = 2$.

Suppose now that $p > 2$. Here we use the classification of irreducible subgroups of $PSL_5(p^k)$ in [DMW79]. To prove that there are no non-abelian simple irreducible ESQ-subgroups of $PSL_5(p^k)$ (really $GL_5(p^k)$), it will be convenient by Lemma 13(b) to choose $q = p^k$ to be “sufficiently large.” It follows from [DMW79] that $K$ is isomorphic to one of the following: $PSL_5(p^r), PSL_5(p^{2k}), PSL_2(p^4), PSL_2(3), PSL_2(p^4), A_5, A_6, PSL_2(11), A_7, M_{11}$. Each of these groups contains a subgroup isomorphic to the alternating group $A_4$. Indeed, $PSL_2(p^4)$ contains such a subgroup by [Hop67, Satz II.8.18], and we also have

$$A_5 \leq PSL_2(11) \leq M_{11}, \quad A_5 \leq PSL_5(p) \leq PSL_5(p^t), \quad PSL_5(p) \leq PSU_5(p^{2k}), \quad A_5 \leq PSL_5(3).$$

As $A_4$ is a subgroup of $A_5$, the claim is valid.
Next we show that $A_4$ does not have a 5-dimensional faithful ESQ-module. Suppose that $V$ is a faithful 5-dimensional $A_4$-module over $\mathbb{F}_q$. Suppose first that $\text{char} \mathbb{F}_q \geq 5$, and so the $A_4$-modules are completely reducible. Assume by Lemma 13(b) that $\mathbb{F}_q$ is a splitting field. Then there are 4 pairwise non-isomorphic irreducible $A_4$-modules over $\mathbb{F}_q$, three of which are 1-dimensional, and one is 3-dimensional. Since $A_4$ is non-abelian, $V$ decomposes as $V = V_3 + V_1 + V'_1$ where the subscript denotes the dimension. Thus $\Lambda^2 V = \Lambda^2 (V_3 + V_1 + V'_1)$ contains three 3-dimensional and a 1-dimensional direct summand, and so it is not ESQ. If the characteristic of $\mathbb{F}_q$ is 3, then there are only two irreducible $A_4$-modules, one is 1-dimensional, and the other is 3-dimensional. Thus we may argue the same way as above, except we must use composition factors instead of direct summands. □

Next we determine the ESQ-subgroups in $\text{GL}_4(\mathbb{F})$ for fields $\mathbb{F}$ with $\text{char} \mathbb{F} \neq 2$. (We allow $|\mathbb{F}|$ to be non-prime, even $\text{char} \mathbb{F} = 0$.) The case $\text{char} \mathbb{F} = 2$ requires additional considerations and it is not relevant to Theorem 1(d).

Let $L = \text{AGL}_1(5)$ be the group of linear functions of the 5-element field considered as a permutation group of degree 5. We have $L = \langle a, b \rangle$, where $a = (0 \ 1 \ 2 \ 3 \ 4), b = (1 \ 2 \ 4 \ 3)$, and $|L| = 20$. Then $L$ naturally embeds into $\text{GL}_5(\mathbb{F})$ for any field $\mathbb{F}$. If $\text{char} \mathbb{F} \neq 5$, then the underlying module splits into a direct sum of submodules $\mathbb{F}^5 = V \oplus V_1$, where $V = \langle (x_0, \ldots, x_4) \mid x_0 + \cdots + x_4 = 0 \rangle$ and $V_1 = \langle (x, \ldots, x) \mid x \in \mathbb{F} \rangle$. The action of $L$ on $V$ is absolutely irreducible and it is the only faithful irreducible representation of $L$ over $\mathbb{F}$. In the following theorem $L$ and $V$ are as above.

**Theorem 16.** Let $\mathbb{F}$ be a field with $\text{char} \mathbb{F} \neq 2$ and let $K \leq \text{GL}_4(\mathbb{F})$ be a finite irreducible ESQ-subgroup. Then $\text{char}(\mathbb{F}) \neq 5$ and $K$ is isomorphic, as a linear group, to a subgroup of $L$. Moreover, 5 divides $|K|$, and if 5 is a square in $\mathbb{F}$ then $K \cong L$.

**Proof.** First recall [KL90, Proposition 5.5.10] that no finite non-abelian simple group has a non-trivial representation of degree two over a field of characteristic different from 2.

Let $M$ be a minimal normal subgroup of $K$. We first show that $M$ is abelian. If not, then $M$ is the direct product of pairwise isomorphic non-abelian simple groups. Let $S$ be one of the simple factors. Applying Clifford’s theorem twice for $S < M < K$, and considering that $S$ has no two-dimensional non-trivial representation, we conclude that $S$ is irreducible. Let $V = (\mathbb{F}_q)^4$. Since $(\Lambda^2 V)/U \cong V$ for some 2-dimensional $S$-submodule $U$, the remark in the first paragraph in this proof gives that $S$ acts trivially on $U$.

Let $V^*$ denote the dual space of $V$. Let $\psi: \text{Hom}(V, V^*) \to V \otimes V$ be defined as follows. Let $x_1, \ldots, x_4$ be a basis of $V$ and let $x_1^*, \ldots, x_4^*$ be the dual basis of $V^*$. If $f \in \text{Hom}(V, V^*)$ represented by the matrix $(a_{i,j})$ with respect to these bases, then let $\psi(f)$ be the element $\sum_{i,j} a_{i,j} x_i \otimes x_j$. It is easy to check that $\psi$ is a linear isomorphism. Now the group $S$ acts on both spaces $\text{Hom}(V, V^*)$ and $V \otimes V$: if $g \in S$, then the matrix of $f^g$ is $g^t (a_{i,j}) g$. An easy calculation shows that the isomorphism $\psi$ is an isomorphism of $S$-modules, and so the fixed points of $S$ in $V \otimes V$ correspond to intertwining operators between the $S$-modules $V$ and $V^*$. Identify $\Lambda^2 V$ with $(u \otimes v - v \otimes u \mid u, v \in V) \subseteq V \otimes V$. As $U$ is a 2-dimensional subspace of $\Lambda^2 V$ on which $S$ acts trivially, the dimension of these intertwining operators is at least 2. The dimension of the space of these intertwining operators is equal to the dimension of the centralizer algebra of the $S$-module $V$. On the other hand, by Schur’s lemma, the centralizer algebra is a quadratic extension field $\mathbb{F}$ of $\mathbb{F}_q$. Further, the $S$-module $V$ is also an ESQ-module. This means that $S$ can be viewed as a subgroup of $\text{GL}_2(\mathbb{E})$, which contradicts the first paragraph of the proof.

So we have that $M$ is an elementary abelian $r$-group for some prime $r$, which cannot be the characteristic of $\mathbb{F}$. Take an extension field $\mathbb{E} \supseteq \mathbb{F}$ containing primitive $r$-th roots of unity and consider $M \leq \text{GL}_4(\mathbb{E})$, which, by Lemma 13(a), (b), is an ESQ-group. Now $\mathbb{E}$ is a splitting field for $M$, so we can fix an eigenbasis $e_1, e_2, e_3, e_4 \in \mathbb{E}^4$ of $M$.

Suppose that $M$ contains an element without fixed points, i.e., an element $g \in M$ such that 1 is not an eigenvalue of $g$. Let the eigenvalues of $g$ be $\lambda_i \in \mathbb{E}$ ($1 \leq i \leq 4$). Then the eigenvalues of $g \wedge g$ are $\lambda_j \lambda_k$ ($1 \leq j < k \leq 4$). By the ESQ-property there is an injective map $i \mapsto P(i) = \{j, k\}$ such that $\lambda_i = \lambda_j \lambda_k$. Since 1 is not among the eigenvalues of $g$, we see that $i \notin P(i)$. Up to renumbering
the eigenvalues there are only two essentially different injective maps satisfying this property. So we arrive at two alternative systems of equations:

\[
\begin{align*}
\lambda_1 &= \lambda_2 \lambda_3, \\
\lambda_2 &= \lambda_3 \lambda_4, \\
\lambda_3 &= \lambda_4 \lambda_1, \\
\lambda_4 &= \lambda_1 \lambda_2; \\
\end{align*}
\]

and

\[
\begin{align*}
\lambda_1 &= \lambda_2 \lambda_3, \\
\lambda_2 &= \lambda_1 \lambda_4, \\
\lambda_3 &= \lambda_1 \lambda_2, \\
\lambda_4 &= \lambda_1 \lambda_3. \\
\end{align*}
\]

It is easy to solve these systems of equations. In the first case we obtain

\[
\begin{align*}
\lambda_1 &= \varepsilon, \\
\lambda_2 &= \varepsilon^2, \\
\lambda_3 &= \varepsilon^4, \\
\lambda_4 &= \varepsilon^3,
\end{align*}
\]

where \(\varepsilon^5 = 1\), and that implies \(r = 5\). In the second case the solutions have the form

\[
\begin{align*}
\lambda_1 &= \varepsilon^2, \\
\lambda_2 &= \varepsilon^3, \\
\lambda_3 &= \varepsilon^5, \\
\lambda_4 &= \varepsilon,
\end{align*}
\]

where \(\varepsilon^6 = 1\). However, non-trivial elements of \(M\) have prime order \(r\), hence either \(\lambda_1 = \varepsilon^2 = 1\) or \(\lambda_2 = \varepsilon^3 = 1\), contrary to our assumption that 1 is not an eigenvalue of \(g\). So the only possibility is that such an element has order 5 and its eigenvalues are all the four distinct primitive fifth roots of unity.

Now we treat the case when 1 is an eigenvalue of every element \(g \in M\) and show that this is impossible. As \(K\) is irreducible and \(M < K\), we have \(\{v \in F^4 \mid \forall g \in M : vg = v\} = 0\). This implies that the trivial module is not a direct summand in the \(M\)-module \(F^4\), and so it cannot be a direct summand in \(E^4\). Hence \(\{v \in E^4 \mid \forall g \in M : vg = v\} = 0\). Now for every fixed \(i\) (\(1 \leq i \leq 4\)) the number of elements \(g \in M\) with \(e_i g = e_i\) equals \(|M|/r\). If an element \(g \in M\) has a fixed point in \(E^4\) (that is, 1 is an eigenvalue of \(g\)) then \(g\) must fix one of the basis vectors \(e_i\). This shows, for \(r > 4\), that the number of elements in \(M\) without eigenvalue 1 is at least \(|M| - 4|M|/r > 0\), which is not possible. Hence \(r = 2\) or \(r = 3\). If \(M\) were cyclic, then all non-trivial elements of \(M\) would have non-trivial eigenvalues, hence \(M\) is non-cyclic in our present case. Then \(M\) intersects \(SL_4(F)\) non-trivially, so by the minimality of \(M\) we have that all matrices in \(M\) have determinant 1.

Let \(r = 2\). Let \(D\) denote the 8-element subgroup consisting of diagonal matrices (with respect to the basis \(e_1, e_2, e_3, e_4\)) with diagonal entries \(\pm 1\) and with determinant 1. We have \(M < D\). By Lemma 13(c), \(M\) cannot contain \(-I\). Now \(D\) has seven maximal subgroups, out of these three contain \(-I\) and the remaining four are the stabilizers of the four basis vectors \(e_i\) (\(1 \leq i \leq 4\)) in \(D\). So there remains no possibility for \(M\).

Let \(r = 3\), and denote by \(\omega \in E\) a primitive third root of unity. Let \(g \in M \leq SL_4(E)\) and suppose that \(g \neq 1\). Then 1 is an eigenvalue of \(g\). If the multiplicity of the eigenvalue 1 is one, then, as \(\det g = 1\), the eigenvalues of \(g\) are \(1, \omega, \omega, \omega\) or \(1, \omega^2, \omega^2, \omega^2\). In both cases 1 is not an eigenvalue of \(g \wedge g\) contradicting the ESQ-property. Hence for every \(1 \neq g \in M\) the multiplicity of the eigenvalue 1 is at least two, and then we infer that the eigenvalues of \(g\) are \(1, 1, \omega, \omega^2\). Now \(M\) is a proper subgroup of the group of diagonal matrices with order 3 and determinant 1, so it is generated by at most two subgroups. Since no basis vector can be fixed by both generators, each one of the basis vectors \(e_1, e_2, e_3, e_4\) is fixed by one generator, and the eigenvalue for the other generator on the same eigenvector must be \(\omega\) or \(\omega^2\). Then the product of the two generators does not have eigenvalue 1, contrary to our assumption.

In summary, we have proved that \(r = 5\) and there is a \(g \in M\) with \(g = \text{diag}(\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^3)\) with respect to the basis \(e_1, e_2, e_3, e_4 \in E^4\) (where \(\varepsilon \in E\) satisfies \(\varepsilon^5 = 1\)). Therefore \(g \wedge g = \text{diag}(\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^3, 1, 1, 1)\) with respect to the basis \(e_2 \wedge e_3, e_3 \wedge e_4, e_4 \wedge e_1, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_4\) of \(\Lambda^2 E^4\). Hence any isomorphism from the \((g)\)-module \(E^4\) into \(\Lambda^2 E^4\) maps \(e_i\) to a multiple of \(e_{i+1} \wedge e_{i+2}\) (where the indices are taken modulo 4).
Now take an element $h \in C_k(g) \leq GL_4(\mathbb{F})$. Since the eigenvalues of $g$ are distinct, $h$ is also diagonal with respect to the basis $e_1, e_2, e_3, e_4$, say, $h = \text{diag}(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. The matrix of $h \wedge h$ restricted to $\langle e_2 \wedge e_3, e_2 \wedge e_4, e_4 \wedge e_1, e_1 \wedge e_2 \rangle$ is $\text{diag}(\lambda_2 \lambda_3, \lambda_3 \lambda_4, \lambda_4 \lambda_1, \lambda_1 \lambda_2)$. From the ESQ-property it follows that the eigenvalues of $h$ satisfy the same system of Eqs. (5) as above, therefore $h$ is a power of $g$. Thus we have shown that $(g)$ is a self-centralizing subgroup of $K$. In particular, we obtain that $M = (g)$ is cyclic of order 5.

Since $M < K$ and $M$ is self-centralizing, $K$ is isomorphic to a subgroup in the holomorph of $M$, which is $L$. Since the characteristic polynomial of any element $g$ generating $M$ is $x^4 + x^3 + x^2 + x + 1$, $M \leq GL_4(\mathbb{F})$ is unique up to conjugacy. Hence $K$ can be embedded into a subgroup of $GL_4(\mathbb{F})$ that is isomorphic to $L$.

There are three subgroups of $L$ containing $M$; namely, $M$, a dihedral group $D_5$ of order 10, and $L$. If 5 has a square root in $\mathbb{F}$, then the dimensions of the irreducible representations of $D_5$ are at most two, hence proper subgroups of $L$ act reducibly on $\mathbb{F}^4$ in this case. □

Theorem 1(d) is an immediate consequence of the following results.

**Theorem 17.** Let $p$ be an odd prime, and let $\{x_1, x_2, x_3, x_4\}$ be a generating set for $H_{p,4}$.

(a) There is no 4-generator UCS 5-group with exponent $5^2$.

(b) If $p \equiv \pm 1 \pmod{5}$, then there is a unique isomorphism class of 4-generator UCS $p$-groups with exponent $p^2$, namely,

$$G_1 = H_{p,4}/\langle x_1^p z_{13} z_{41}^2 z_{23}^2 z_{42}^2 z_{43}^2, x_2^p z_{21}^2 z_{31}^2 z_{41}^2 z_{32}^2 z_{34}^2, x_3^p z_{21}^2 z_{14}^2 z_{23}^2 z_{24}^2, x_4^p z_{12}^2 z_{13}^2 z_{14}^2 z_{32}^2 z_{42}^2, z_{12} z_{14} z_{23} z_{24} \rangle$$

where $z_{ij}$ denotes $[x_i, x_j]$.

(c) If $p \equiv \pm 2 \pmod{5}$, then there are two isomorphism classes of 4-generator UCS $p$-groups with exponent $p^2$, namely, $G_1$ as in case (b) and another group $G_2$.

Moreover, $|\text{Aut}(G_1)| = |G_1| = 20$ and $|\text{Aut}(G_2)| = 5$.

**Proof.** Let $G$ be a 4-generator UCS group of exponent $p^2$, where $p$ is an odd prime. Let $K$ denote $\text{Aut}(G)/G \leq GL_4(p)$. By Theorem 5, $K$ is an irreducible ESQ-group. Theorem 16 implies that there are no 4-generator UCS groups of exponent $5^2$. Let us use the notation introduced before Theorem 16. In particular, let $L$ denote the group $AGL_1(5)$ acting on the vector space $V \cong \mathbb{F}^4$. By quadratic reciprocity, the number 5 is a square in the $p$-element field if and only if $p \equiv \pm 1 \pmod{5}$. For these primes we have $K = L$, for primes with $p \equiv \pm 2 \pmod{5}$ we can conclude that $K \leq L$ with 5 dividing the order of $K$.

First assume that $K = L$. Since $L$ has up to equivalence a unique faithful irreducible 4-dimensional representation, we can choose a generating set $x_1, x_2, x_3, x_4$ of $H = H_{p,4}$ such that the matrices of generators of $L$ acting on $H$ will be

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$ 

Choosing the basis $[x_1, x_2], [x_1, x_3], [x_1, x_4], [x_2, x_3], [x_2, x_4], [x_3, x_4]$ in $H'$ the action of $a$ and $b$ on $H'$ is described by the matrices

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$
of order 5. Let a\textsuperscript{p}exponent (tors.)

defining relations of this group. (In Theorem 17 we avoided inverses by reversing some commuta-

tions.)

For these primes the five-element cyclic group is an irreducible subgroup in \text{GL}_4


Using the transition matrix

\[ t = \begin{pmatrix}
0 & -1 & 1 & -2 & 2 & 2 \\
1 & 2 & 2 & 1 & 0 & -2 \\
2 & 0 & -2 & -1 & -2 & -1 \\
-2 & -2 & -1 & 2 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0
\end{pmatrix} \]

of determinant 25 \neq 0 we obtain

\[ ta't^{-1} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
-1 & -1 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}, \quad tb't^{-1} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}. \]

Let W denote the subspace generated by the first four rows of t, and U the subspace generated

by the last two rows. Then \( H' = W \oplus U \), furthermore V and W are isomorphic \( L \)-modules

via the isomorphism mapping \( x_i \) to the \( i \)-th row of \( t \) for \( i = 1, 2, 3, 4 \). Since V is an abso-

lute irreducible \( L \)-module, the isomorphism between V and W is determined up to a scalar factor.

Theorem 4(iii) implies that \( G = H/N \) for some \( K \)-invariant normal subgroup N such that

\( N \subseteq \Phi(H) \), \( H^p \cap N = 1 \), and \( \overline{H} \) and \( H'/(N \cap H') \) are equivalent \( K \)-modules. Therefore, there are exactly \( p-1 \) suitable normal subgroups N, but they can be mapped to one another using auto-

morphisms of \( H \) sending each \( x_i \) to \( x_i^{k} \) for some fixed \( k = 1, \ldots, p - 1 \). Hence there is a unique

isomorphism class of those 4-generating UCS groups \( G \) of exponent \( p^2 \) where the automorphism

group of \( G \) induces \( L \) on \( \overline{G} \). Using the matrices above it is straightforward to write down the

definitions relating to this group. (In Theorem 17 we avoided inverses by reversing some commuta-

tors.)

Now consider the case, when \( K \) is a proper subgroup of \( L \). This can happen only if \( p \equiv \pm 2 \) (mod 5).

For these primes the five-element cyclic group is an irreducible subgroup in \text{GL}_4(p). Let \( E = \mathbb{F}_p^* \)

and \( \varepsilon \in E \) a primitive fifth root of unity. Up to conjugation \( H = H_{p,4} \) has a unique automorphism \( a \) of order 5. Let \( M = \langle a \rangle \) and let \( W = \langle H', M \rangle \).

Then the 6-dimensional space \( H' \) decomposes as a direct sum \( H' = W \oplus C_{H'}(M) \).

The \( M \)-modules \( \overline{H} \), \( H^p \), and \( W \) are isomorphic, and they can be

identified with the additive group of \( E \) so that the action of \( a \) becomes the multiplication by \( \varepsilon \). Using

this identification every \( M \)-invariant normal subgroup \( N \triangleleft H \) such that \( H/N \) is an UCS group with

exponent \( p^2 \) has the form

\[ N_w = \{ (\vartheta, w\vartheta) \in H^p \oplus W \mid \vartheta \in E \} \oplus C_{H'}(M). \]

for \( w \in W \setminus \{0\} \). Let \( \gamma \) be a generator of the multiplicative group of \( E \). Multiplication by \( \gamma \) commutes

with multiplication by \( \varepsilon \), hence \( W \) and \( C_{H'}(M) \) are invariant under the action of any automorphism

of \( H \) that corresponds to multiplication by \( \gamma \) on \( \overline{H} \). The eigenvalues of the \( \mathbb{F}_p \)-linear transformation
determined by multiplication by \( \gamma \) on \( \overline{H} \cong E \) are \( \gamma, \gamma^p, \gamma^{p^2}, \gamma^{p^3} \), and hence its eigenvalues on \( H' \)

are \( \gamma^{p+i} \) for \( 0 \leq i < j \leq 3 \). Now \( \gamma^{1+p} \) has degree 4 over \( \mathbb{F}_p \), so we infer that the eigenvalues on \( W \)
are $γ^{(1+p)^i}$ for $i = 0, 1, 2, 3$. If $p \equiv 2 \pmod{5}$ then let $k = (1 + p)p$, while if $p \equiv 3 \pmod{5}$ then let $k = (1 + p)p^2$. In both cases we have $k \equiv 1 \pmod{5}$. Now multiplication by $γ^k$ on $E$ has the same eigenvalues as the action of $γ$ on $W$, moreover, $e^k = e$, hence the action of $γ$ on $W$ is multiplication by $γ^k$. Now $γ^n$ transforms $N_w$ to

$$\{ (φγ^n, w φy(nk−1)) ∈ H^p ⊕ W \mid φ ∈ E \} ⊕ C_H(M) = \{ (φ, w φy) ∈ H^p ⊕ W \mid φ ∈ E \} ⊕ C_H(M) = N_wγ^{nk−1}.$$

A simple calculation using the Euclidean algorithm yields that gcd$(k − 1, p^4 − 1) = 5$. Hence $N_w1$ and $N_w2$ determine isomorphic quotient groups $H/N_w1$, $H/N_w2$ provided $w_1$ and $w_2$ lie in the same coset of the multiplicative group of $E$ modulo the fifth powers. Field automorphisms of $E$ normalize $⟨γ⟩$, hence we can map $N_w$ to

$$\{ (φ^p, (w φ)^p) ∈ H^p ⊕ W \mid φ ∈ E \} ⊕ C_H(M) = \{ (φ, w φ^p) ∈ H^p ⊕ W \mid φ ∈ E \} ⊕ C_H(M) = N_wφ^p.$$

Now it follows that for $G_1 = H/N_1$ the automorphism group induces $L$ on $G_1$. Furthermore, the other four cosets modulo the subgroup of fifth powers are permuted cyclically by the Frobenius automorphism, since $p$ is a primitive root modulo 5. Hence for each $w ∈ E$ which is not a fifth power in $E$ the quotient groups $H/N_w$ are all isomorphic to each other, and this is the group $G_2$ in Theorem 17(c).

It is possible to write down explicit defining relations of $G_2$ using a generator element of the multiplicative group of $F_{p^4}$. However, we thought that a very complicated formula will not help the reader, so we were content with stating the existence of $G_2$.

In Theorem 14(a), (c) subgroups of the affine general linear group $AGL_1(F_r)$ are candidates for minimal irreducible ESQ-groups. We shall clarify when these examples arise, and construct larger ESQ-groups.

Let $t$ be a power of a prime $r$. Identify the 1-dimensional affine semilinear group $AGL_1(F_t)$ with the Cartesian product of sets

$$AGL_1(F_t) = \text{Gal}(F_t/F_r) × F_t^X × F_t.$$

Here $\text{Gal}(F_t/F_r)$ denotes the group of field automorphisms of $F_t$. Multiplication in $AGL_1(F_t)$ is defined by

$$(σ_1, λ_1, μ_1)(σ_2, λ_2, μ_2) = (σ_1σ_2, (λ_1σ_2)λ_2, (μ_1σ_2)λ_2 + μ_2)$$

where $σ_1, σ_2 ∈ \text{Gal}(F_t/F_r)$, $λ_1, λ_2 ∈ F_t^X$, and $μ_1, μ_2 ∈ F_t$. A 2-transitive action of $AGL_1(F_t)$ on $F_t$ is given by

$$α(σ, λ, μ) = (ασ)λ + μ$$

where $α ∈ F_t$, and $(σ, λ, μ) ∈ \text{Gal}(F_t/F_r) × F_t^X × F_t = AGL_1(F_t)$.

**Theorem 18.** Let $t, q$ be powers of distinct primes. Let $L \leq F_t^X$, and suppose that $q ∈ L$, and there exist distinct $α, β ∈ L$ such that $α + β = 1$. Define $G_{t1}$ to be the subgroup of $AGL_1(F_t)$ containing the elements $(σ, λ, μ)$ such that $μ ∈ F_t$, $λ ∈ L$, and $σ$ induces the identity automorphism $F_t^X/L → F_t^X/L$. Then there exist $|F_t^X:L|$ pairwise non-isomorphic absolutely irreducible ESQ $F_qGL_1$-modules of dimension $|L|$. In particular, $AGL_1(F_t)$ is an absolutely irreducible ESQ-subgroup of $GL_{t−1}(F_q)$ if $t > 3$ and gcd$(t, q) = 1$. 

---

Proof. Let \( V = (F_q)^t \) be the permutation module for \( \Gamma L_1(E) \) where \( E := F_t \) has (prime) characteristic \( r \). Let \((e_\alpha)_{\alpha \in E}\) be a basis for \( V \) indexed by \( \alpha \in E \). The action of \( \Gamma L_1(E) \) on \( V \) is given by

\[
e_\alpha(\sigma, \lambda, \mu) = e_{(\alpha \sigma) \lambda + \mu} \quad (\alpha \in E).
\]

Our proof has two cases. Assume first that \( q \equiv 1 \pmod{r} \). In this case the hypothesis \( q \in L \) holds trivially, as \( 1 \in L \) and \( q = 1 \) in \( E \). We show later that the second case when \( q \not\equiv 1 \pmod{r} \), reduces to this first case.

Let \( T : E \to F_r \) denote the absolute trace function: \( T(\alpha) = \sum \alpha \sigma \) where \( \sigma \) ranges over \( \text{Gal}(E/F_r) \).

Let \( \zeta \in F_q^\times \) have order \( r \), and define

\[
f_\alpha = \sum_{\mu \in E} \xi^{T(\alpha \mu)} e_\mu.
\]

Since \( |E|^{-1} \sum_{\alpha \in E} \xi^{T(\alpha \mu - \nu)} = 0 \) if \( \mu \neq \nu \), and 1 otherwise, we have

\[
|E|^{-1} \sum_{\alpha \in E} \xi^{-T(\nu \alpha)} f_\alpha = \sum_{\mu \in E} \left( |E|^{-1} \sum_{\alpha \in E} \xi^{T(\alpha \mu - \nu)} \right) e_\mu = e_\nu.
\]

Therefore \((f_\alpha)_{\alpha \in E}\) defines a new basis for \( V \). The action of \( \Gamma L_1(E) \) on the new basis is monomial, and given by

\[
f_\alpha(\sigma, \lambda, \mu) = \xi^{-T(\alpha \sigma \lambda - 1 \mu)} f_{(\alpha \sigma) \lambda - 1}.
\]

Consider the normal subgroup \( N = \{(1,1,\mu) \mid \mu \in E\} \) of \( G_L \). By Eq. (6), \( f_\alpha(1,1,\mu) = \xi^{-T(\alpha \mu)} f_\alpha \).

Thus each \((f_\alpha)\) is an irreducible \( F_q N \)-module. The non-degeneracy of the map \( E \times E \to F_r, (\alpha, \beta) \mapsto T(\alpha \beta) \) implies that there is an \( N \)-module isomorphism

\[
(f_\alpha) \cong (f_\beta) \quad \text{if and only if} \quad \alpha = \beta.
\]

Let \( \lambda' L \) be a coset of \( L \) in \( E^\times \), and set

\[
W(\lambda' L) = \{ f_\alpha \mid \alpha \in \lambda' L \} = \sum_{\alpha \in \lambda' L} (f_\alpha).
\]

It follows from Eq. (6) that \( W(\lambda' L) \) is a \( G_L \)-module. We shall show that it is irreducible. Set \( M = \{(1,\lambda, \mu) \mid \lambda \in L, \mu \in E\} \). Then \( M \) is a normal subgroup of \( G_L \), and by (7) the inertia subgroup of \((f_{\lambda'})\) in \( M \) is \( N \). Hence by Clifford’s theorem, the induced module \( \text{Ind}^M_N((f_{\lambda'})) = W(\lambda' L) \) is \( M \)-irreducible, and \emph{a fortiori} \( G_L \)-irreducible.

There are two decompositions of \( V \):

\[
V = \sum_{\alpha \in E} (f_\alpha) \quad \text{and} \quad V = (f_0) \oplus \sum_{\lambda' L \in E^\times / L} W(\lambda' L).
\]

The first is as a direct sum of irreducible \( F_q N \)-modules, and the second, a direct sum of irreducible \( F_q G_L \)-modules. If \( \alpha', \beta' \in \lambda' L \), then by Eq. (6)

\[
(f_{\alpha'} \wedge f_{\beta'})(\sigma, \lambda, \mu) = \xi^{-T((\alpha' + \beta') \sigma \lambda - 1 \mu)} f_{(\alpha' \sigma) \lambda - 1} \wedge f_{(\beta' \sigma) \lambda - 1}.
\]

Hence if \( \alpha' \neq \beta' \), then \((f_{\alpha'} \wedge f_{\beta'}) \cong (f_{\alpha' + \beta'}) \) as \( F_q N \)-modules by (6). Thus \( W(\lambda' L) \) is an ESQ-module if and only if \( \alpha' + \beta' \in \lambda' L \) for distinct \( \alpha', \beta' \in \lambda' L \). Equivalently, \( \alpha + \beta = 1 \) where \( \alpha = \alpha' / (\alpha' + \beta') \) and
\( \beta = \beta^* (\alpha^* + \beta^*) \) in \( L \) are distinct. Clearly \( W(\lambda') \cong W(\lambda'' \lambda') \) as \( N \)-modules if and only if \( \lambda' = \lambda'' \lambda' \). Therefore \( W(\lambda') \cong W(\lambda'' \lambda') \) as \( G_1 \)-modules if and only if \( \lambda' = \lambda'' \lambda' \). In summary, the \( W(\lambda') \) provide \( |E^X : L| \) pairwise non-isomorphic absolutely irreducible ESQ \( FqGL_L \)-modules of dimension \( |L| \).

Suppose now that \( q \not\equiv 1 \pmod{r} \), and \( q \in L \) holds. We temporarily enlarge the field of scalars from \( Fq \) to the finite field \( Fq(\zeta) \), where \( \zeta \) has order \( r \). View \( W(\lambda') \) as an absolutely irreducible ESQ \( Fq(\zeta)GL_L \)-module. We shall show that there exists an \( FqGL_L \)-module \( U(\lambda') \) which satisfies \( W(\lambda') \cong U(\lambda') \otimes FqGL_L(\zeta) \). It then follows that the \( U(\lambda') \) are pairwise non-isomorphic absolutely irreducible ESQ \( FqGL_L \)-modules of dimension \( |L| \). By a theorem of Brauer (see [H82, Theorem VII.1.17] and [GH97]), the module \( U(\lambda') \) exists if and only if the character \( \chi \) of \( W(\lambda') \) has values in \( Fq \). We shall show that \( \chi(\sigma, \lambda, \mu) \in Fq \) for all \( (\sigma, \lambda, \mu) \in GL \) by showing \( \chi(\sigma, \lambda, \mu)^q = \chi(\sigma, \lambda, \mu) \). By Eq. (6)

\[
\chi(\sigma, \lambda, \mu) = \sum_{|\alpha| = 1} \zeta^{-T((\alpha\sigma)\lambda^{-1}\mu)} = \sum_{|\alpha| = 1} \zeta^{-T(\alpha\mu)}.
\]

However, \( \{ \alpha \in \lambda' | (\alpha\sigma)\alpha^{-1} = \lambda \} = \{ \alpha \in \lambda' | ((\alpha\sigma)\alpha^{-1} = \lambda \} \) as \( q \) in \( L \) is fixed by \( \sigma \). Therefore \( \chi(\sigma, \lambda, \mu) = \chi(\sigma, \lambda, \mu)^q \) as desired.

If \( L = E^X \), then \( G_1 = \Gamma(L(\mathbb{E})) \). Moreover, \( q \in E^X \) holds as \( t, q \) are powers of distinct primes. If \( t > r \), then take \( \alpha \) to be an element of \( E^X \) not in \( Fq^r \), and so that \( \beta = 1 - \alpha \) satisfies \( \alpha + \beta = 1 \) and \( \alpha \neq \beta \). Clearly \( \alpha + \beta = 1 \) and \( \alpha \neq \beta \) provided \( r > 3 \). This proves that \( GL(\mathbb{E}) \) is an absolutely irreducible ESQ-subgroup of \( GL_{n-1}(Fq) \) if \( t > 3 \) and \( \gcd(t, q) = 1 \). □

We next prove Theorem 1(e).

**Proof of Theorem 1(e).** Consider parts (i) and (iii). Let \( p \) be an odd prime, and let \( q = p^k \). Let \( V = (Fq)^3 \) be the natural \( SO_3(q) \)-module. Choose a basis \( x_1, x_2, x_3 \) for \( V \), and the basis \( x_2 \wedge x_3, x_3 \wedge x_1, x_1 \wedge x_2 \) for \( A^2V \). The matrix of \( g \wedge g \) det \((g^{-1})^T \). As \( \text{det}(g) = 1 \) and \( g^{-1}g = 1 \), it follows that \( g \wedge g = g \) and so \( V \) is an irreducible ESQ \( SO_3(q) \)-module. By Theorem 5(b) there exists an exponent-\( p^2 \) UCS \( p \)-group of order \( q^6 \). This proves part (i). Similarly, by the last sentence of Theorem 18, \( \Gamma(L(\mathbb{E})) \) is an absolutely irreducible ESQ-subgroup of \( GL_{n-1}(Fq) \) for odd \( q \). Part (iii) now follows by Theorem 5(b).

Consider part (ii). Parts (a) and (b) of Theorem 5 are true with \( k = 1 \). Thus if \( G \) is an exponent-\( p^2 \) UCS-group of order \( q^{10} \), then \( \text{Aut}(G)^F \) is an irreducible ESQ-subgroup of \( GL_5(p) \). It follows from Theorem 15 (with \( q = p \)) that \( p^5 \equiv 1 \pmod{11} \). (Additionally, \( |\text{Aut}(G)^F| \) is divisible by 11.) Conversely, if \( p^5 \equiv 1 \pmod{11} \), or more generally if \( q = p^k \) satisfies \( q^{10} \equiv 1 \pmod{11} \), then there exists an exponent-\( p^2 \) UCS-group of order \( q^{10} \) by Theorems 15 and 5. This proves part (ii). □

Note that \( q^{12} = (q^2)^6 \) and so by Theorem 1(e)(i) there exist UCS-groups of order \( q^{12} \) and exponent \( p^2 \) for all powers \( q \) of an odd prime \( p \).

**Acknowledgments**

We are grateful to Eamonn O’Brien for making available to us a MAGMA [BCP97] database of class-2 \( p \)-groups with 4 generators and exponent \( p \); and to Pál Hegedűs for his valuable comments. The second and the third authors were supported by the Hungarian Scientific Research Fund (OTKA) grants NK72523 and NK72845. The third author began this work in the Computer and Automation Research Institute of the Hungarian Academy of Sciences (MTA SZTAKI), and later he was supported by the research grant PTDC/MAT/101993/2008 of the Fundação para a Ciência e a Tecnologia (Portugal).

**References**


[DMW79] L. Di Martino, A. Wagner, The irreducible subgroups of \(\text{PSL}(V, q)\), where \(q\) is odd, Results Math. 2 (1) (1979) 54–61.