MINIMAL DEGREES ASSOCIATED WITH SOME WREATH PRODUCTS OF GROUPS

IBRAHIM ALOTAIBI AND DAVID EASDOWN

ABSTRACT. We investigate minimal degrees of groups associated with certain wreath products. We construct sequences of groups with the property that some proper quotients are isomorphic to subgroups having the same minimal degree, thus having the so-called *almost exceptional* property. We show that it is possible to have an almost exceptional group with an arbitrarily long chain of normal subgroups with respect to which the quotients all have the same minimal degree, whilst at the same time having arbitrarily many subgroups, also with the same minimal degree, but which are pairwise incomparable. The results depend on a theory of semidirect products, where the base group is a k-dimensional vector space over the field with p elements, where p is a prime and k is a positive integer, extended by a cyclic group of order p, represented by a $k \times k$ matrix. This theory uncovers a large class of nonabelian groups of exponent p. A final application is made to construct sequences of groups with the property that the direct products have minimal degrees that grow as a linear function of the number n of factors, whilst their respective quotients, realised as central products, have minimal degrees that grow as an exponential function of n, generalising a result of Peter Neumann.

1. INTRODUCTION

Throughout this paper, all groups will be finite, C_n denotes a cyclic group of order n, $Z(G)$ denotes the centre of a group G, and $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ is the field with p elements for a prime p. Addition and subtraction of subscripts should be interpreted modulo p.

The *minimal (faithful) degree* $\mu(G)$ of a group G is the least nonnegative integer such that G embeds in the symmetric group $\mathrm{Sym}(n)$ of permutations on a set of size n. If G is nontrivial then $\mu(G)$ is the minimal sum of indexes for any non-empty collection of subgroups $\mathscr{C} = \{H_1, \ldots, H_k\}$ with a trivial core intersection, in which case we say that $\mathscr{C}$ *affords a minimal (faithful) representation of* G. In this case, the subgroups $H_1, \ldots, H_k$ become the stabilisers of points in the respective orbits for the permutation action of G, and the orbits may be identified with the sets of cosets of $H_1, \ldots, H_k$ in G respectively. When $k = 1$, there is a single orbit and the representation is transitive. One of the earliest results is due to Karpilovsky [9], which calculates minimal degrees of abelian groups, and which will be used implicitly throughout:

Theorem 1.1. [9] *If $G = C_{p_1^{i_1}} \ldots C_{p_n^{i_n}}$ is an abelian group where $n, i_1, \ldots, i_n$ are positive integers and $p_1, \ldots, p_n$ are primes, then $\mu(G) = p_1^{i_1} + \ldots + p_n^{i_n}$.*

Johnson [8] proved a number of seminal results, including the following:

AMS subject classification (2010): 20B35.

Keywords: permutation groups, wreath products, semidirect products, minimal degrees.

Theorem 1.2. [8, Theorem 3] *If p is an odd prime and G is a nontrivial p-group whose centre is minimally generated by d elements, then any minimal faithful representation of G is afforded by a collection of d subgroups. In particular, if the centre is cyclic then a minimal representation of G must be transitive.*

Proposition 1.3. [8, Proposition 3] *If p is an odd prime and G is a p-group whose centre is cyclic or elementary abelian then $\mu(G) \geq p\mu\big(Z(G)\big)$.*

Wright [14] proved that taking minimal degrees is additive with respect to taking direct products of nilpotent groups (for which Theorem 1.1 becomes a special case):

Theorem 1.4. [14, Corollary 2] *If G and H are nilpotent then $\mu(G\times H) = \mu(G)+\mu(H)$.*

Clearly if H is a subgroup of G then $\mu(H) \leq \mu(G)$. However if N is a normal subgroup then $\mu(G/N)$ may be greater than $\mu(G)$. Neumann [13] observed that if $G = D_8^n$ is a direct product of n copies of the dihedral group D_8 then

$$\mu(G) \;=\; 4n\,, \tag{1}$$

whilst

$$\mu(G/N) \;=\; 2^{n+1} \tag{2}$$

if N is chosen so that G/N becomes (isomorphic to) the n-fold central product of n copies of D_8. This shows that the minimal degree of the direct product of n groups may grow as a linear function of n, whilst the minimal degree of at least one of its quotients grows as an exponential function of n. In fact, (1) follows from Theorem 1.4 and the fact that $\mu(D_8) = 4$, whilst (2) follows from Theorem 1.2, and a simple induction, since the central product has cyclic centre and a transitive representation of a 2-group has degree a power of 2. This idea is adapted for odd primes p in Theorem 7.2 below and is also captured in [5, Theorem 2.1].

Easdown and Praeger in [5] refer to a group G as *exceptional* if G has a normal subgroup N such that $\mu(G/N) > \mu(G)$, in which case N is called a *distinguished subgroup* and (any group isomorphic to) G/N is called a *distinguished quotient*. They prove that the smallest exceptional groups have order 32 and exhibit several classes of exceptional groups. Other examples and classes of exceptional groups have been studied, for example, by Lemieux [12], Britnell, Saunders and Skyner [1] and Chamberlain [2]. By (1) and (2), Neumann's example, $G = D_8^n$, is exceptional, with an n-fold central product as distinguished quotient, if and only if $n \geq 3$. In the case $n = 2$, (1) and (2) yield

$$\mu(D_8\times D_8) \;=\; \mu(D_8 * D_8) \;=\; 8\,. \tag{3}$$

We say that a group G is *almost exceptional* if G has a nontrivial normal subgroup N such that $\mu(G/N) = \mu(G)$, in which case N is referred to as an *almost distinguished subgroup* and (any group isomorphic to) G/N an *almost distinguished quotient*. Thus, by (3), the group $D_8\times D_8$ is almost exceptional of order 64 with almost distinguished quotient $D_8 * D_8$. It is not difficult to prove that the smallest almost exceptional group is D_8, of order 8, with almost distinguished quotient $C_2\times C_2$:

$$\mu(D_8) \;=\; \mu(C_2\times C_2) \;=\; 4\,. \tag{4}$$

Kovacs and Praeger [10] classify almost exceptional groups with abelian quotients, of which (4) is also the smallest example, and conjecture that no exceptional group exists with a distinguished abelian quotient. Progress towards resolving this conjecture, constraining properties of any hypothetical counterexample, has been made in [11], [7] and [3].

The group D_8 is also (isomorphic to) the smallest instance of a nontrivial wreath product $C_p \wr C_p$, when $p = 2$. In Lemmas 6.5 and 6.6 below, we describe all sections of $C_p \wr C_p$, when p is any prime, and prove, in Theorem 6.7 that all of the nonabelian sections of order at least p^4 are almost exceptional of minimal degree p^2. The development of Theorem 6.7 and its supporting lemmas relies on an analysis of groups that decompose as semidirect products of finite dimensional vector spaces over $\mathbb{Z}_p$ extended by C_p, adapting a technique and notation introduced in [6], and related to the fact that indecomposable C_p-modules over $\mathbb{Z}_p$ form a chain (see, for example, [4]). This technique also provides a large class of nonabelian groups of exponent p, all of which are sections of $C_p \wr C_p$ (see Corollary 4.4, Corollary 4.10 and Theorem 4.11). The lattice of normal subgroups of $C_p \wr C_p$ is fully described (see Figure 1), demonstrating that it is possible to exhibit a single group with an arbitrarily long chain of normal subgroups, yielding quotients all with the same minimal degree, whilst at the same time exhibiting an arbitrarily large number of pairwise incomparable subgroups all with the same minimal degree. Theorem 7.2, in the final section, provides an analogue of (1) and (2), but using arbitrary combinations of nonabelian sections of $C_p \wr C_p$, for p an odd prime.

Section 2 records identities involving binomial coefficients, which may be of independent interest, and used to prove Theorem 4.2, which is a key to the later sections of the paper, by establishing isomorphisms between sections and subgroups of $C_p \wr C_p$.

Section 3 introduces two large classes of almost exceptional groups that arise as wreath products. The first class (see Theorem 3.3) involves groups whose orders are divisible by two distinct primes, relying on results from [6], whilst the second class (see Theorem 3.5) involves p-groups, the simplest case of which is $C_p \wr C_p$, which is examined in forensic detail in Sections 5 and 6.

Section 4 develops a theory of semidirect products, whose base groups are k-dimensional vector spaces over the field with p elements, extended by the cyclic group of order p, whose generator is represented by a $k \times k$ matrix, where $k \leq p$. All of the groups that arise turn out to be sections of the wreath product $C_p \wr C_p$ and have exponent p or p^2, and the results are then applied in Sections 5 and 6. Section 7 gives a final application, constructing sequences of p-groups, with direct products that have minimal degrees that grow as a linear function of the number n of factors, whilst their quotients, formed using central products, grow as an exponential function of n.

In case it is useful for future potential research, we have included, as an appendix, data related to wreath products of orders up to 500. The calculations were made with the assistance of GAP and MAGMA computer algebra software, and the group identification numbers are common to both systems. This table includes examples where, in some cases, nonabelian or noncyclic groups are used to build the base group or the extending group.

2. Identities involving binomial coefficients

In this short section we highlight identities involving binomial coefficients, which may be of independent interest, and which are used in the proof of Theorem 4.2 below. These identities are easy to prove directly using a simple counting argument, and are surely well-known. The short proof we provide here however exploits the polynomial $(\lambda - 1)^k$, which is part of the apparatus, in Section 4, leading to the definition of an extension of a vector space by the cyclic group generated by its companion matrix, so it is perhaps not surprising that the identities arise in one of the main proofs.

Lemma 2.1. *Let i, k and ℓ be positive integers such that $i, \ell < k$. Then the following hold:*

(i) *If $\ell < i$ then*

$$\binom{k}{\ell} = \sum_{m=0}^{\ell} \binom{k-i}{\ell-m}\binom{i}{m} .$$

(ii) *If $i \leq \ell$ then*

$$\binom{k}{\ell} - \binom{k-i}{\ell-i} = \sum_{m=M}^{i-1} \binom{k-i}{\ell-m}\binom{i}{m}$$

where $M = \max\{0, \ell+i-k\}$.

Proof. Observe that the following (real) polynomial equation holds:

$$\begin{aligned}(\lambda-1)^k - \lambda^i(\lambda-1)^{k-i} &= (\lambda-1)^{k-i}\big((\lambda-1)^i - \lambda^i\big) \\ &= (\lambda-1)^{k-i}\left(\sum_{m=0}^{i-1}(-1)^{i+m}\binom{i}{m}\lambda^m\right) .\end{aligned}$$

The identities in (i) and (ii) follow by comparing binomial expansions on each side. □

3. Wreath products with elementary abelian base group

Let p be a prime and $n \geq 2$ an integer. Suppose in this section that G is a finite group represented faithfully using permutations of n letters, so we may identify G with a subgroup of $\mathrm{Sym}(n)$. Form the wreath product

$$W = C_p \wr G = C_p^n \rtimes G .$$

We may write W as an internal semidirect product of an elementary abelian base group $B \cong C_p^n$ by an extending group also identified with G

$$W \equiv BG = B_1 \dots B_n G ,$$

where B is an internal direct product of $B_1, \dots, B_n$, where

$$B_k = \langle a_k \rangle \cong C_p$$

for $1 \leq k \leq n$. Elements α of W may then be expressed uniquely in the form

$$\alpha = \Big(\prod_{k=1}^{n} a_k^{i_k}\Big) g$$

for some $g \in G$ and $i_1, \dots, i_n \in \mathbb{Z}_p$. Thus, if α and β are elements of W, say

$$\alpha = \Big(\prod_{k=1}^{n} a_k^{i_k}\Big) g \qquad \text{and} \qquad \beta = \Big(\prod_{k=1}^{n} a_k^{j_k}\Big) h$$

for some $g, h \in G$ and $i_1, \dots, i_n, j_1, \dots, j_n \in \mathbb{Z}_p$, then the product $\alpha\beta$ in W, involving the wreath action, becomes

$$\alpha\beta = \Big(\prod_{k=1}^{n} a_k^{i_k + j_{kg}}\Big) gh . \tag{5}$$

Note that

$$\beta^{-1} = \Big(\prod_{k=1}^{n} a_k^{-j_{kh^{-1}}}\Big) h^{-1} , \tag{6}$$

and we get the following conjugation action:

$$\alpha^{\beta} \;=\; \Big(\prod_{k=1}^{n} a_k^{-j_{kh^{-1}}+i_{kh^{-1}}+j_{kh^{-1}g}}\Big) g^h \,. \tag{7}$$

In particular (as an instance of (7), taking $g = 1$ and $\beta = h$), we get the following conjugation action of an element h from G on an element of the base group::

$$\Big(\prod_{k=1}^{n} a_k^{i_k}\Big)^h \;=\; \prod_{k=1}^{n} a_k^{i_{kh^{-1}}} \,. \tag{8}$$

Since C_p may be regarded as a permutation group on p letters, it follows quickly that W is isomorphic to a permutation group on pn letters, so that $\mu(W) \leq pn$. But B is a subgroup of W, and $\mu(B) = \mu(C_p^n) = pn$, so, also, $\mu(W) \geq pn$, whence

$$\mu(W) \;=\; np \,. \tag{9}$$

Note that the minimal degree of W is determined by the base group B only, regardless of whether or not the wreathing group G is represented minimally as a permutation group.

Suppose that G has m orbits, say $\Omega_1, \ldots, \Omega_m$. For $1 \leq i \leq m$ put

$$\delta_i \;=\; \prod_{k \in \Omega_i} a_k \,,$$

which is clearly central in W (since any element of G permutes subscripts of generators associated with any given orbit by conjugation). Consider also

$$\delta \;=\; a_1 \ldots a_n \;=\; \prod_{i=1}^{m} \delta_i \,.$$

Then δ is also central in W, being a product of central elements, and $\delta = \delta_1$ if G is transitive. Put

$$D \;=\; \langle \delta \rangle \;\cong\; C_p \,,$$

which is a central subgroup of W. The following result is probably well-known and the proof is straightforward.

Lemma 3.1. *The centre of W is*

$$Z(W) \;=\; \langle \delta_1, \ldots, \delta_m \rangle \,.$$

In particular, $Z(W) = D$ if and only if G is transitive.

We work now towards showing, in certain cases, that the quotient group W/D is isomorphic to a subgroup of W. Let ν be the mapping from W into $\mathbb{Z}_p$, referred to as the *evaluation map*, given by the following rule:

$$\nu : \Big(\prod_{k=1}^{n} a_k^{i_k}\Big) g \;\mapsto\; \sum_{k=1}^{n} i_k \,, \tag{10}$$

for any $g \in G$ and $i_1, \ldots, i_n \in \mathbb{Z}_p$. By (5), it follows quickly that ν is a group homomorphism from the multiplicative group W onto the additive group $\mathbb{Z}_p$. Consider the following subgroup of B:

$$K \;=\; \Big\{ \prod_{k=1}^{n} a_k^{i_k} \;\Big|\; i_1 + \ldots + i_n = 0 \mod p \Big\} \;=\; \langle a_1 a_2^{-1}, \ldots, a_1 a_n^{-1} \rangle \,.$$

It follows from (8) that K is a normal subgroup of W. Now put

$$\overline{W} \;=\; KG \,,$$

Clearly, $\overline{W} = \ker \nu$ is a normal subgroup of W of index p. Since K intersects trivially with G, we have, further, that $\overline{W}$ decomposes as an internal semidirect product:

$$\overline{W} \;=\; KG \;=\; K \rtimes G \,.$$

We now prove that $\overline{W}$ is isomorphic to the quotient group W/D under certain conditions. We first record a large class of cases. If n is not divisible by p then $\overline{W}$ is a complement for D in W so that W decomposes as an internal direct product $W = \overline{W}D = \overline{W} \times D$, and we have the following:

Lemma 3.2. *If p and n are coprime, then $\overline{W} \cong W/D$.*

We can now identify a large class of almost exceptional groups:

Theorem 3.3. *Suppose that p and q are distinct primes and let s be the order of p modulo q. Suppose that $s \geq 2$ (so that p is not congruent to 1 modulo q) and that $q < p^{s-1}$. Put $W = C_p \wr C_q$. Then*

$$\mu(W) \;=\; pq \,.$$

and W is almost exceptional with almost distinguished normal subgroup $Z(W) \cong C_p$.

Proof. We use the notation of this section, where $n = q$ and the generator of $G \cong C_q$ may be identified with the cyclic permutation $(1\; 2\; \ldots\; q)$. We have $\mu(W) = pq$ immediately from (9). By Lemma 3.1, since G is transitive,

$$Z(W) \;=\; D \,,$$

and, by Lemma 3.2,

$$W/Z(W) \;=\; W/D \;\cong\; \overline{W} \,.$$

Observe that, inherited from the wreath action,

$$\overline{W} \;\cong\; V \rtimes T \,,$$

using the notation of [6], where V is a vector space over $\mathbb{Z}_p$ of dimension $q-1$ and T is an invertible matrix of order q with the following minimal polynomial (coinciding with the characteristic polynomial):

$$\chi(\lambda) \;=\; 1 + \lambda + \ldots + \lambda^{q-1} \,,$$

Since $s \geq 2$, observe that $\chi(\lambda)$ decomposes as a product of irreducible factors each of degree s. Since $q < p^{s-1}$, it follows from the second alternative in [6, Theorem 4.7] that

$$\mu\big(W/Z(W)\big) \;=\; \mu(\overline{W}) \;=\; \mu(V \rtimes T) \;=\; pq \,.$$

This coincides with $\mu(W)$, which shows that W is almost exceptional with almost distinguished normal subgroup $Z(W)$, completing the proof of the theorem. □

Another sufficient condition for $\overline{W}$ to be isomorphic to W/D occurs when G is a transitive cyclic permutation group of order n, but the proof is more delicate.

Lemma 3.4. *Suppose that $G \cong C_n$ where the generator of G may be identified with the cyclic permutation $(1\; 2\; \ldots\; n)$, so that the action of G is transitive on $\{1, \ldots, n\}$. Then $\overline{W} \cong W/D$.*

Proof. It is important to note, interpreting subtraction modulo n, that the mapping

$$k \mapsto k-1 \qquad \text{for} \qquad k \in \{1,\dots,n\}\,,$$

which is the inverse of the cyclic permutation $(1\;2\;\dots\;n)$, commutes with all elements of G. Let φ be the mapping from W into $\overline{W}$ given by the rule

$$\varphi : \Big(\prod_{k=1}^{n} a_k^{i_k}\Big) g \;\mapsto\; \Big(\prod_{k=1}^{n} a_k^{i_k - i_{k-1}}\Big) g\,,$$

for $g \in G$ and $i_1,\dots,i_n \in \mathbb{Z}_p$, where it is understood that $i_{k-1} = i_n$ when $k=1$. Observe that this rule is well-defined because

$$\sum_{k=1}^{n}(i_k - i_{k-1}) \;=\; \Big(\sum_{k=1}^{n} i_k\Big) - \Big(\sum_{k=1}^{n} i_{k-1}\Big) \;=\; \Big(\sum_{k=1}^{n} i_k\Big) - \Big(\sum_{k=1}^{n} i_k\Big) \;=\; 0\,.$$

The mapping is a homomorphism, because if

$$\alpha \;=\; \Big(\prod_{k=1}^{n} a_k^{i_k}\Big) g \qquad \text{and} \qquad \beta \;=\; \Big(\prod_{k=1}^{n} a_k^{j_k}\Big) h$$

for some $g,h \in G$ and $i_1,\dots,i_n,j_1,\dots,j_n \in \mathbb{Z}_p$, then, by (5), and the fact that the action of g commutes with subtraction by 1 modulo n,

$$\begin{aligned}
(\alpha\beta)\varphi \;&=\; \Big(\Big(\prod_{k=1}^{n} a_k^{i_k + j_{kg}}\Big) gh\Big)\varphi \;=\; \Big(\prod_{k=1}^{n} a_k^{i_k + j_{kg} - i_{k-1} - j_{(k-1)g}}\Big) gh \\
&=\; \Big(\prod_{k=1}^{n} a_k^{i_k - i_{k-1} + j_{kg} - j_{(k-1)g}}\Big) gh \;=\; \Big(\prod_{k=1}^{n} a_k^{i_k - i_{k-1} + j_{kg} - j_{(kg)-1}}\Big) gh \\
&=\; \Big(\Big(\prod_{k=1}^{n} a_k^{i_k - i_{k-1}}\Big) g\Big)\Big(\Big(\prod_{k=1}^{n} a_k^{j_k - j_{k-1}}\Big) h\Big) \;=\; (\alpha\varphi)(\beta\varphi)\,.
\end{aligned}$$

Observe that

$$\delta\varphi \;=\; (a_1 \dots a_n)\varphi \;=\; (a_1 a_2^{-1})(a_2 a_3^{-1})\dots(a_{n-1}a_n^{-1})(a_n a_1^{-1}) \;=\; \delta\delta^{-1} \;=\; 1\,,$$

so that $\delta \in \ker\varphi$. Hence

$$D \;=\; \langle \delta \rangle \;\subseteq\; \ker\varphi\,.$$

Suppose that $\alpha \in \ker\varphi$. If $\alpha \notin B$ then $\alpha = bg$ for some $b \in B$ and $g \in G$ with $g \neq 1$, so that

$$\alpha\varphi \;=\; (b\varphi)g \;\neq\; 1\,,$$

since $b\varphi \in B$ and $g \neq 1$, contradicting that $\alpha \in \ker\varphi$. Hence $\alpha \in B$, say

$$\alpha \;=\; \prod_{k=1}^{n} a_k^{i_k}$$

for some $i_1,\dots,i_n \in \mathbb{Z}_p$. But then

$$1 \;=\; \alpha\varphi \;=\; \prod_{k=1}^{n} a_k^{i_k - i_{k-1}}\,,$$

so that $i_k - i_{k-1} = 0$ for each k, yielding

$$i_1 \;=\; i_n \;=\; i_{n-1} \;=\; \dots \;=\; i_2\,.$$

Hence $\alpha = \delta^{i_1} \in D$. This proves that $\ker\varphi \subseteq D$, so that, combined with $D \subseteq \ker\varphi$, from before, we have

$$\ker\varphi \;=\; D\,.$$

Observe that, all elements of G are fixed by φ, so lie in the image, and, for each $k = 1,\dots,n-1$,

$$a_k\varphi \;=\; a_k a_{k+1}^{-1}\,.$$

Hence

$$\overline{W} \;=\; KG \;=\; \langle a_1a_2^{-1}, a_2a_3^{-1}, \dots, a_{n-1}a_n^{-1}\rangle G \;\subseteq\; \operatorname{im}\varphi \;\subseteq\; \overline{W}\,,$$

whence

$$\overline{W} \;=\; \operatorname{im}\varphi \;\cong\; W/\ker\phi \;= W/D\,,$$

completing the proof of the lemma. □

Now we can now identify another class of almost exceptional groups.

Theorem 3.5. *Let $n = p^\ell$ be a nontrivial power of an odd prime p and put $W = C_p \wr C_n$, where the wreath action of the cyclic group is transitive, acting on a set of size n. Then*

$$\mu(W) \;=\; np \;=\; p^{\ell+1}\,.$$

and W is almost exceptional with almost distinguished normal subgroup $Z(W) \cong C_p$.

Proof. Let $G = \langle g\rangle \cong C_n$ where $g = (1\;2\;\dots\;n)$, so that the wreath action is transitive and we may regard $W = C_p \wr C_n$ as an internal semidirect product

$$W \;=\; \langle a_1,\dots,a_n\rangle \rtimes \langle g\rangle\,.$$

We then have

$$\overline{W} \;=\; \left\{a_1^{i_1}\dots a_n^{i_n}g^j \;\middle|\; i_1,\dots,i_n \in \mathbb{Z}_p\,,\; i_1+\dots+i_n = 0\,,\; j \in \{0,\dots,n-1\}\right\}.$$

As before, we put $\delta = a_1\dots a_n$ and $D = \langle\delta\rangle$. Then, as before (see Lemma 3.1), δ is central in W. Since n is congruent to 0 modulo p, we have $\delta \in \overline{W}$, so that δ is also central in $\overline{W}$. Thus

$$D \;\subseteq\; Z(\overline{W})\,.$$

Let $\alpha \in Z(\overline{W})$, so

$$\alpha \;=\; a_1^{i_1}\dots a_n^{i_n}g^j$$

for some $i_1,\dots,i_n \in \mathbb{Z}_p$ such that $i_1+\dots+i_n = 0$ and for some $j \in \{0,\dots,n-1\}$. If $j > 0$, then, since α is central in $\overline{W}$, and interpreting addition of subscripts modulo p,

$$a_1a_2^{-1} \;=\; (a_1a_2^{-1})^\alpha \;=\; a_{j+1}a_{2+j}^{-1} \;\neq\; a_1a_2^{-1}\,,$$

which is a contradiction. Hence $j = 0$, so that

$$\alpha \;=\; a_1^{i_1}a_2^{i_2}\dots a_n^{i_n}\,.$$

Since α is central,

$$\alpha \;=\; \alpha^g \;=\; a_1^{i_n}a_2^{i_1}\dots a_n^{i_{n-1}}\,,$$

from which it follows quickly that $i_1 = i_2 = \dots = i_n$, so that $\alpha = \delta^{i_1} \in D$. This shows that $Z(\overline{W}) \subseteq D$, so that

$$Z(\overline{W}) \;=\; D\,.$$

In particular, $Z(\overline{W})$ is cyclic. But $\overline{W}$ is a p-group, so that, by Theorem 1.2, a minimal faithful representation of $\overline{W}$ must be transitive of degree a power of p. However, W contains a copy of C_p^{n-1}, so that

$$\mu(\overline{W}) \;\geq\; \mu(C_p^{n-1}) \;=\; (n-1)p \;=\; (p^\ell - 1)p \;=\; p^{\ell+1} - p \;>\; p^\ell \;,$$

from which it follows that $\mu(\overline{W}) \geq p^{\ell+1}$. Now we have

$$p^{\ell+1} \;\leq\; \mu(\overline{W}) \;\leq\; \mu(W) \;=\; p^{\ell+1} \;,$$

so that

$$\mu(W) \;=\; \mu(\overline{W}) \;=\; \mu(W/D) \;=\; p^{\ell+1} \;,$$

completing the proof of the theorem. □

In the following three sections we investigate the special case when $W = C_p \wr C_p$, culminating in a proof that, for odd primes p, all nonabelian sections of W of order at least p^4 are almost exceptional with minimal faithful degree p^2.

4. Extension of a vector space by a cyclic group

Throughout this section, p is a prime and k is a fixed integer such that $1 \leq k \leq p$. We also fix a k-dimensional vector space V over the field $\mathbb{Z}_p$, which becomes an elementary abelian group with respect to addition. We will create a semidirect product in a natural way, extending the additive group V by a multiplicative cyclic group of order p. The technique is adapted from [6].

The special case $k = p$ will be important, as the group extension will become isomorphic to the wreath product $C_p \wr C_p$. When $k = 1$, the extension trivialises. When $1 < k < p$, the extension will correspond to a nonabelian section of the wreath product.

Working over $\mathbb{Z}_p$, let T_k be the companion matrix of the monic polynomial

$$\chi_k(\lambda) \;=\; (\lambda - 1)^k \;=\; a_0 + a_1\lambda + \ldots + a_{k-1}\lambda^{k-1} + \lambda^k \;,$$

where, for $0 \leq i \leq k-1$,

$$a_i \;=\; (-1)^{k+i}\binom{k}{i} \;, \tag{11}$$

noting that, since the characteristic of the field is p,

$$\chi_p(\lambda) \;=\; (\lambda - 1)^p \;=\; \lambda^p - 1 \;.$$

Then

$$T_k \;=\; \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{k-2} & -a_{k-1} \end{bmatrix} ,$$

interpreted so that $T_1 = [1]$, and, when $k = p$, this becomes a permutation matrix:

$$T_p \;=\; \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} . \tag{12}$$

The characteristic and minimal polynomials of T_k coincide with $\chi_k(\lambda)$, so that, by the Cayley-Hamilton Theorem, $(T_k - I_k)^k$ is the zero matrix. Now put

$$M_k \;=\; T_k - I_k \;=\; \begin{bmatrix} -1 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 \\ 0 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-2} & -1-a_{n-1} \end{bmatrix} ,$$

which is nilpotent of index k. For example, when $p = 3$, we have $\chi_2(\lambda) = 1 + \lambda + \lambda^2$ and the following sequence of matrices:

$$M_1 \;=\; \begin{bmatrix} 0 \end{bmatrix} , \qquad M_2 \;=\; \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} , \qquad M_3 \;=\; \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{bmatrix} .$$

When $p = 5$, we have

$$\chi_2(\lambda) = 1 + 3\lambda + \lambda^2 , \qquad \chi_3(\lambda) = 4 + 3\lambda + 2\lambda^2 + \lambda^3 , \qquad \chi_4(\lambda) = 1 + \lambda + \lambda^2 + \lambda^3 + \lambda^4 ,$$

and the following sequence of matrices:

$$M_1 \;=\; \begin{bmatrix} 0 \end{bmatrix} , \qquad M_2 \;=\; \begin{bmatrix} 4 & 1 \\ 4 & 1 \end{bmatrix} , \qquad M_3 \;=\; \begin{bmatrix} 4 & 1 & 0 \\ 0 & 4 & 1 \\ 1 & 2 & 2 \end{bmatrix} .$$

$$M_4 \;=\; \begin{bmatrix} 4 & 1 & 0 & 0 \\ 0 & 4 & 1 & 0 \\ 0 & 0 & 4 & 1 \\ 4 & 4 & 4 & 3 \end{bmatrix} , \qquad M_5 \;=\; \begin{bmatrix} 4 & 1 & 0 & 0 & 0 \\ 0 & 4 & 1 & 0 & 0 \\ 0 & 0 & 4 & 1 & 0 \\ 0 & 0 & 0 & 4 & 1 \\ 1 & 0 & 0 & 0 & 4 \end{bmatrix} .$$

Suppose henceforth that $k > 1$ (since in the case $k = 1$ the matrix T_k trivialises). To decongest the notation, write

$$T \;=\; T_k \qquad \text{and} \qquad M \;=\; M_k \, .$$

Observe that, since $k \leq p$,

$$T^p - I \;=\; (T-I)^p \;=\; (T-I)^{p-k}(T-I)^k \;=\; (T-I)^{p-k}0 \;=\; 0 \, ,$$

so that $T^p = I$. Hence T is an invertible matrix generating a cyclic group of order p under matrix multiplication:

$$\langle T \rangle \;\cong\; C_p \, .$$

We may regard V as the vector space of k-tuples, also identified with row vectors:

$$V \;=\; \left\{(w_1,\dots,w_k)\;\middle|\; w_1,\dots,w_k \in \mathbb{Z}_p\right\} \;\equiv\; \left\{\begin{bmatrix} w_1 \;\dots\; w_k\end{bmatrix}\;\middle|\; w_1,\dots,w_k \in \mathbb{Z}_p\right\} .$$

Then T acts on V as a linear transformation by matrix multiplication on the right. The unique eigenvalue of T is $\lambda = 1$, with a one-dimensional eigenspace. It is well-known (see, for example, [4]) that, up to isomorphism, V is the unique indecomposable C_p-module of degree k with respect to a field of characteristic p. For $1 \le i \le k$, put

$$\mathbf{e}_i \;=\; (0,\dots,0,1,0,\dots 0) ,$$

with 1 in the ith position and 0 in all other positions, so

$$\{\mathbf{e}_1,\dots,\mathbf{e}_k\} \tag{13}$$

is a (standard) basis for V. Then

$$\left\{\mathbf{e}_1\, ,\, \mathbf{e}_1 M\, ,\, \dots,\, \mathbf{e}_1 M^{k-1}\right\} \tag{14}$$

is also a basis for V. It may be instructive to work through the details in a particular case. Suppose, for example that $p = 5$. If $k = 2$ then (14) becomes

$$\{(1,0)\, ,\, (4,1)\} .$$

If $k = 3$ then (14) becomes

$$\{(1,0,0)\, ,\, (4,1,0)\, ,\, (1,3,1)\} .$$

If $k = 4$ then (14) becomes

$$\{(1,0,0,0)\, ,\, (4,1,0,0)\, ,\, (1,3,1,0)\, ,\, (4,3,2,1)\} .$$

If $k = 5$ then (14) becomes

$$\{(1,0,0,0,0)\, ,\, (4,1,0,0,0)\, ,\, (1,3,1,0,0)\, ,\, (4,3,2,1,0)\, ,\, (1,1,1,1,1)\} .$$

We now form the following extension, which is a semidirect product, combining the additive group V with the multiplicative group $\langle T\rangle \cong C_p$:

$$V \rtimes T \;=\; V \rtimes \langle T\rangle \;=\; \{(\mathbf{v},T^i) \mid \mathbf{v} \in V\, ,\; i \in \mathbb{Z}_p\} ,$$

using the notation and terminology of [6], but using row vectors and matrix action on the right. The rule (adapted from [6]) for group multiplication in $V \rtimes T$ becomes the following:

$$(\mathbf{v},T^i)(\mathbf{w},T^j) \;=\; (\mathbf{v}+\mathbf{w}T^{-i},T^{i+j}) . \tag{15}$$

The reader should be careful to distinguish between action of a matrix on a row vector, given by matrix multiplication, and the binary group operation in the semidirect product. When $k = p$, the action of the permutation matrix T on the additive group V corresponds to the wreath action of the permutation $(1\ 2\ \dots\ p)$, generating a copy of C_p, on the multiplicative group C_p^p, so that, in this case,

$$V \rtimes T \;=\; V_p \rtimes T_p \;\cong\; C_p \wr C_p . \tag{16}$$

Consider, for general k, where $1 < k \le p$, a T-invariant subspace S of V. One may form the quotient vector space V/S, on which T acts on the left, so that we may form the semidirect product

$$(V/S) \rtimes T \;=\; \left\{\left(S+\mathbf{v},T^i\right)\;\middle|\; \mathbf{v} \in V\, ,\;\; i \in \mathbb{Z}\right\} . \tag{17}$$

On the other hand, we may identify S with

$$S \rtimes I \;\equiv\; \{(\mathbf{v}, I) \mid \mathbf{v} \in S\}\;,$$

which becomes a normal subgroup of $V \rtimes T$, and then form the quotient group

$$(V \rtimes T)/(S \rtimes I) \;=\; \Big\{ (S \rtimes I)(\mathbf{v}, T^i) \;\Big|\; \mathbf{v} \in V\,,\;\; i \in \mathbb{Z}_p \Big\}\,. \tag{18}$$

The identification

$$\big(S + \mathbf{v}, T^i\big) \;\equiv\; (S \rtimes I)(\mathbf{v}, T^i)$$

is easily seen to be an isomorphism between the groups (17) and (18), so, in what follows, we may identify them:

$$(V/S) \rtimes T \;\equiv\; (V \rtimes T)/(S \rtimes I)\,. \tag{19}$$

The normal subgroups of $V \rtimes T$ contained in the base group $V \equiv V \rtimes I$ are just the T-invariant subspaces of V, which form a chain, namely

$$\{\mathbf{0}\} \;=\; V_0 \;\subseteq V_1 \;\subseteq\; \ldots \;\subseteq\; V_{k-1} \;\subseteq\; V_k \;=\; V\;, \tag{20}$$

where, for $0 \le i \le k$,

$$V_i \;=\; \ker M^i \;=\; VM^{k-i}\,. \tag{21}$$

The set containments in (20) are strict, and, for $1 \le i \le k$, a basis for V_i may be taken to be the following linearly independent set with i elements:

$$\big\{\, \mathbf{e}_1 M^{k-i}, \, \mathbf{e}_1 M^{k-i+1}, \;\ldots, \;\mathbf{e}_1 M^{k-1} \big\}\,. \tag{22}$$

In particular, for each $i > 0$, we have

$$\dim V_i \;=\; i\;, \tag{23}$$

and, for $0 \le i \le k-2$,

$$\dim(V_{i+1}/V_i) \;=\; 1 \qquad \text{and} \qquad \dim(V/V_i) \;=\; k - i \;\ge\; 2\,. \tag{24}$$

Note that the one-dimensional eigenspace of T is V_1 with basis

$$\big\{\mathbf{e}_1 M^{k-1}\big\}\,. \tag{25}$$

It should be remarked that in (14), (22) and (25), we may, if we wish, replace $\mathbf{e}_1$ uniformly throughout by any one of the standard basis vectors. We provided before, at (13) and (14), two different bases for V. The following lemma, used to prove Theorem 4.2 below, provides an alternative basis for V_i for $1 \le i \le k$, and follows from (13) by a simple induction, and for which both (13) and (25) become extreme special cases:

Lemma 4.1. *For $1 \le i \le k$, a basis for V_i is*

$$\big\{\, \mathbf{e}_1 M^{k-i}, \, \mathbf{e}_2 M^{k-i}, \;\ldots, \;\mathbf{e}_i M^{k-i} \big\}\,, \tag{26}$$

and, for $1 \le j \le i$,

$$\mathbf{e}_j M^{k-i} \;=\; \sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{j+\ell}\,. \tag{27}$$

It follows from Lemma 4.1 (or by direct calculation) that

$$V_{k-1} \;=\; \langle \mathbf{e}_2-\mathbf{e}_1\,,\,\mathbf{e}_3-\mathbf{e}_2\,,\,\ldots\,,\,\mathbf{e}_k-\mathbf{e}_{k-1}\rangle \;=\; \{(\alpha_1,\ldots,\alpha_p)\mid \alpha_1+\ldots+\alpha_p=0\}\,, \tag{28}$$

and, in the special case that $k=p$,

$$V_1 \;=\; \langle \mathbf{e}_1+\ldots+\mathbf{e}_p\rangle\,. \tag{29}$$

We may now take each of the T-invariant subspaces in the chain (20) and form semidirect products, with multiplication (15) inherited from $V\rtimes T$:

$$V_i\rtimes T \;\equiv\; V_i\rtimes\langle T\rangle\,,$$

for $0\le i\le k$, and obtain a chain of subgroups of $V\rtimes T$, with strict set containments:

$$\langle T\rangle \;\equiv\; V_0\rtimes T \;\subseteq\; V_1\rtimes T \;\subseteq\; \ldots \;\subseteq\; V_{k-1}\rtimes T \;\subseteq V_k\rtimes T \;=\; V\rtimes T\,. \tag{30}$$

For $0\le i\le j\le k$, define a mapping

$$\Psi_{i,j}: V_j\rtimes T\to V_i\rtimes T$$

by the rule

$$(\mathbf{v},T^{\ell}) \;\mapsto\; (\mathbf{v}M^{j-i},T^{\ell})$$

for $\mathbf{v}\in V_j$ and $\ell\in\mathbb{Z}_p$. It follows from (21) that this rule is well-defined, and from (15) and the fact that M and T commute under matrix multiplication that $\Psi_{i,j}$ is a group homomorphism. It follows quickly, again using (21), that

$$\ker\Psi_{i,j} \;=\; V_{j-i}\rtimes I\,. \tag{31}$$

Clearly also $\Psi_{i,j}$ is surjective. The first isomorphism (32) in the following theorem asserts that certain sections of $V\rtimes T$ associated with the chain (20) of invariant subspaces are isomorphic to subgroups. The second and third isomorphisms, (33) and (34), document cases when the action of T is trivial. The fourth isomorphism (35) is involved (when $2\le i\le k$), allowing us to replace k-tuples by i-tuples, acted on by T_i, instead of by T_k.

Theorem 4.2. *Suppose that* $0\le i\le j\le k$ *(noting the blanket assumption that* $k>1$*). Then*

$$(V_j/V_{j-i})\rtimes T_k \;\cong\; V_i\rtimes T_k\,. \tag{32}$$

If $i=0$ *then*

$$V_i\rtimes T_k \;=\; V_0\rtimes T_k \;=\; \{\mathbf{0}\}\times\langle T_k\rangle\cong\; C_p\,. \tag{33}$$

If $i=1$ *then*

$$V_i\rtimes T_k \;=\; V_1\rtimes T_k \;=\; V_1\times\langle T_k\rangle \;\cong\; C_p\times C_p\,. \tag{34}$$

If $i\ge 2$ *then*

$$V_i\rtimes T_k \;\cong\; \overline{V_i}\rtimes T_i\,, \tag{35}$$

where $\overline{V_i}$ *is the vector space of i-tuples drawn from* $\mathbb{Z}_p$ *(noting that* V_i *is a subspace of* V_k*, elements of which are k-tuples).*

Proof. The isomorphism (32) follows from (31), the fundamental homomorphism theorem and the fact that $\Psi_{i,j}$ is surjective. The isomorphisms (33) and (34) are immediate from the definitions. Suppose that $i \geq 2$. If $i = k$ then $V_k = \overline{V_i}$, so that (35) is immediate. We may suppose, therefore, that $i < k$. Let $\overline{\mathbf{e}}_1, \ldots, \overline{\mathbf{e}}_i$ be standard basis vectors for $\overline{V_i}$. Note that T_i is the companion matrix for the polynomial $(\lambda - 1)^i$ (whilst T_k, by contrast, is the companion matrix for $(\lambda - 1)^k$). By Lemma 4.1, (26) and (27), $\{\mathbf{f}_1, \ldots, \mathbf{f}_i\}$ is a basis for V_i where, for $1 \leq j \leq i$,

$$\mathbf{f}_j \;=\; \sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{j+\ell}\,. \tag{36}$$

Let $\varphi : \ V_i \to \overline{V_i}$ be the linear transformation with the rule

$$\varphi : \alpha_1 \mathbf{f}_1 + \ldots + \alpha_i \mathbf{f}_i \;\mapsto\; \alpha_1 \overline{\mathbf{e}}_1 + \ldots + \alpha_i \overline{\mathbf{e}}_i$$

for $\alpha_1, \ldots, \alpha_i \in \mathbb{Z}_p$, and let $\Phi : V_i \rtimes T_k \to \overline{V_i} \rtimes T_i$ be the mapping with the rule

$$\Phi : \ \big(\mathbf{v}\,,\, T_k^{\ell}\big) \;\mapsto\; \big(\mathbf{v}\varphi\,,\, T_i^{\ell}\big)$$

for $\mathbf{v} \in V_i$ and $\ell \in \mathbb{Z}_p$. Clearly φ and Φ are bijective. To show that Φ is a group isomorphism, using the multiplication rule in $V_k \rtimes T_k$ defined by (15), and the corresponding rule for $\overline{V_i} \rtimes T_k$, it suffices to check that φ respects the actions of T_k and T_i on V_i and $\overline{V_i}$ respectively. Because φ is a linear transformation, it is sufficient to consider actions on the basis elements. Observe, first, for $1 \leq j < i$, using (36) and the fact that $j + \ell < k$ if $0 \leq \ell \leq k - i$,

$$\begin{aligned}
\mathbf{f}_j T_k \;&=\; \left(\sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{j+\ell}\right) T_k \;=\; \sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \Big(\mathbf{e}_{j+\ell} T_k\Big) \\
&=\; \sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{j+1+\ell} \;=\; \mathbf{f}_{j+1}\,,
\end{aligned}$$

so that $\big(\mathbf{f}_j \varphi\big) T_i = \overline{\mathbf{e}}_j T_i = \overline{\mathbf{e}}_{j+1} = \mathbf{f}_{j+1}\varphi = \big(\mathbf{f}_j T_k\big)\varphi$. Next observe that

$$\begin{aligned}
\mathbf{f}_i T_k \;&=\; \left(\sum_{\ell=0}^{k-i} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{i+\ell}\right) T_k \;=\; \left(\left(\sum_{\ell=0}^{k-i-1} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{i+\ell}\right) + \mathbf{e}_k\right) T_k \\
&=\; \left(\sum_{\ell=0}^{k-i-1} (-1)^{k-i+\ell} \binom{k-i}{\ell} \Big(\mathbf{e}_{i+\ell} T\Big)\right) + \mathbf{e}_k T_k \\
&=\; \left(\sum_{\ell=0}^{k-i-1} (-1)^{k-i+\ell} \binom{k-i}{\ell} \mathbf{e}_{i+\ell+1}\right) - \Big(a_0 \mathbf{e}_1 + \ldots + a_{k-1} \mathbf{e}_k\Big) \\
&=\; \left(\sum_{\ell=i}^{k-1} (-1)^{k+\ell} \binom{k-i}{\ell-i} \mathbf{e}_{\ell+1}\right) - \left(\sum_{\ell=0}^{k-1} (-1)^{k+\ell} \binom{k}{\ell} \mathbf{e}_{\ell+1}\right) \\
&=\; \left(\sum_{\ell=i}^{k-1} (-1)^{k+\ell} \left(\binom{k-i}{\ell-i} - \binom{k}{\ell}\right) \mathbf{e}_{\ell+1}\right) - \left(\sum_{\ell=0}^{i-1} (-1)^{k+\ell} \binom{k}{\ell} \mathbf{e}_{\ell+1}\right) \\
&=\; \left(\sum_{\ell=0}^{i-1} (-1)^{k+\ell+1} \binom{k}{\ell} \mathbf{e}_{\ell+1}\right) + \left(\sum_{\ell=i}^{k-1} (-1)^{k+\ell+1} \left(\binom{k}{\ell} - \binom{k-i}{\ell-i}\right) \mathbf{e}_{\ell+1}\right)\,.
\end{aligned}$$

Write $(\lambda - 1)^i \;=\; b_0 + b_1 \lambda + \ldots + b_{i-1} \lambda^{i-1} + \lambda^i$ where, for $0 \leq j \leq i - 1$,

$$b_j \;=\; (-1)^{i+j} \binom{i}{j}\,,$$

and $-b_0, \ldots, -b_{i-1}$ are the entries, in that order, of the last row of T_i. Then, manipulating bionomial coeffecients, using Lemma 2.1, we have

$$\begin{aligned}
\big(\overline{\mathbf{e}}_i T_i\big)\varphi^{-1} &= \big(-b_0\overline{\mathbf{e}}_1 - \ldots - b_{i-1}\overline{\mathbf{e}}_i\big)\varphi^{-1} = \Big(\sum_{j=0}^{i-1}(-1)^{i+j+1}\binom{i}{j}\overline{\mathbf{e}}_{j+1}\Big)\varphi^{-1} \\
&= \sum_{j=0}^{i-1}(-1)^{i+j+1}\binom{i}{j}\mathbf{f}_{j+1} = \sum_{j=0}^{i-1}(-1)^{i+j+1}\binom{i}{j}\Big(\sum_{m=0}^{k-i}(-1)^{k-i+m}\binom{k-i}{m}\mathbf{e}_{j+m+1}\Big) \\
&= \sum_{j=0}^{i-1}\sum_{m=0}^{k-i}(-1)^{j+k+m+1}\binom{i}{j}\binom{k-i}{m}\mathbf{e}_{j+m+1} = \sum_{\ell=0}^{k-1}(-1)^{k+\ell+1}\sum_{\substack{0\le j\le i-1\\ 0\le m\le k-i}}^{j+m=\ell}\binom{i}{j}\binom{k-i}{m}\mathbf{e}_{\ell+1} \\
&= \Big(\sum_{\ell=0}^{i-1}(-1)^{k+\ell+1}\sum_{j=0}^{\ell}\binom{i}{j}\binom{k-i}{\ell-j}\mathbf{e}_{\ell+1}\Big) + \Big(\sum_{\ell=i}^{k-i-1}(-1)^{k+\ell+1}\sum_{j=0}^{i-1}\binom{i}{j}\binom{k-i}{\ell-j}\mathbf{e}_{\ell+1}\Big) \\
&\qquad + \Big(\sum_{\ell=k-i}^{k-1}(-1)^{k+\ell+1}\sum_{\ell+i-k}^{i-1}\binom{i}{j}\binom{k-i}{\ell-j}\mathbf{e}_{\ell+1}\Big) \\
&= \Big(\sum_{\ell=0}^{i-1}(-1)^{k+\ell+1}\binom{k}{\ell}\mathbf{e}_{\ell+1}\Big) + \Big(\sum_{\ell=i}^{k-i-1}(-1)^{k+\ell+1}\Big(\binom{k}{\ell} - \binom{k-i}{\ell-i}\Big)\mathbf{e}_{\ell+1}\Big) \\
&\qquad + \Big(\sum_{\ell=k-i}^{k-1}(-1)^{k+\ell+1}\Big(\binom{k}{\ell} - \binom{k-i}{\ell-i}\Big)\mathbf{e}_{\ell+1}\Big) \\
&= \mathbf{f}_i T_k\ .
\end{aligned}$$

This proves that

$$\big(\mathbf{f}_i\varphi\big)T_i = \overline{\mathbf{e}}_i T_i = \big(\mathbf{f}_i T_k\big)\varphi\ ,$$

completing the verification that φ respects the group actions. This suffices to prove (35), completing the proof of the theorem. □

Remark 4.3. That an isomorphism exists yielding (35) follows from the fact that indecomposable C_p-modules over $\mathbb{Z}_p$ are characterised up to isomorphism by dimension (see, for example, [4]). The above proof however is direct. An alternative proof can also be found indirectly by forming the group algebra $\mathscr{A} = \mathbb{Z}C_p \equiv \mathbb{Z}[\lambda]$, where λ is also used to denote the generator of C_p, so that $\lambda^p = 1$ and $\lambda - 1$ is nilpotent in $\mathscr{A}$ of index p. One can show that V_i with the action of T_k is module-isomorphic to the submodule $\mathscr{S}$ of $\mathscr{A}$ spanned by

$$(\lambda-1)^{p-i},\ \lambda(\lambda-1)^{p-i},\ \ldots,\ \lambda^{i-1}(\lambda-1)^{p-i}$$

whilst $\overline{V_i}$ with the action of T_i is module-isomorphic to $\mathscr{S}' = \mathscr{A}/(\lambda-1)^i\mathscr{A}$ with natural basis

$$1+(\lambda-1)^i\mathscr{A}\ ,\ \lambda+(\lambda-1)^i\mathscr{A}\ ,\ \ldots,\ \lambda^{i-1}+(\lambda-1)^i\mathscr{A}\ ,$$

in both cases using module action induced by multiplication in $\mathscr{A}$ by λ. One then forms a module isomorphism from $\mathscr{S}$ to $\mathscr{S}'$ by extending the map

$$\lambda^j(\lambda-1)^{p-i} \mapsto \lambda^j+(\lambda-1)^i\mathscr{A} \qquad\qquad (0\le j\le i-1)$$

and checking that the module actions match. The trickiest part of the action to check, corresponding to the difficult case in the previous proof, is to observe that, working in $\mathscr{A}$, where $(\lambda-1)^p = 0$,

$$\Big(\lambda^{i-1}(\lambda-1)^{p-i}\Big)\lambda = \lambda^i(\lambda-1)^{p-i} = \lambda^i(\lambda-1)^{p-i} - (\lambda-1)^p = \Big((\lambda^i - (\lambda-1)^i\Big)(\lambda-1)^{p-i}\ ,$$

and then use the binomial expansion of $\lambda^i - (\lambda - 1)^i$. The coefficients in that expansion match the negatives of the entries of the companion matrix T_i in the previous proof. This particular manipulation of formal polynomials also features in the proof of Lemma 2.1, explaining the connection with summation formulae used in the direct proof of (35).

Corollary 4.4. *The semidirect product $V_k \rtimes T_k$ embeds in the wreath product $C_p \wr C_p$. In particular, all sections of $V_k \rtimes T_k$ are sections of $C_p \wr C_p$.*

Proof. We have $V_p \rtimes T_p \cong C_p \wr C_p$ by (16). Using (35) of Theorem 4.2, but with p for k, and k for i, and interpreting V_k, in this context, as consisting of k-tuples (not p-tuples if $k < p$), we get that $V_k \rtimes T_k$ is isomorphic to a subgroup of $C_p \wr C_p$, and the corollary follows. □

Lemma 4.5. *The centre of $V_k \rtimes T_k$ is cyclic of order p, namely,*

$$Z(V_k \rtimes T_k) \;=\; V_1 \;=\; \langle \mathbf{e}_1 M_k^{k-1} \rangle \, . \tag{37}$$

and $\mu(V_k \rtimes T_k) = p^2$.

Proof. Note that the action of $T = T_k$ is nontrivial, since $\mathbf{e}_1 T = \mathbf{e}_2 \neq \mathbf{e}_1$, and $V = V_k$ is an abelian group (under addition). Hence the centre of $V \rtimes T$ consists precisely of elements from V that are fixed by the action of T, that is, elements of the eigenspace of T with respect to the eigenvalue 1. Hence (37) follows from (25) . By Proposition 1.3,

$$\mu(V \times T) \;\geq p\mu\big(Z(V \rtimes T)\big) \;=\; p\mu(C_p) \;=\; p^2 \, .$$

Let S be the subspace of V of codimension 1 generated by $\mathbf{e}_1, \ldots, \mathbf{e}_{k-1}$, which becomes a subgroup of $V \rtimes T$ of index p^2. The core of S is a T-invariant subspace of V, so must be one of the subspaces appearing in the chain (20). Suppose that the core of S is nontrivial. Then S must contain V_1, the atom of (20), which we have just observed is the centre of $V \rtimes T$. Hence S contains some nonzero central element $\mathbf{v}$, must have the form

$$\mathbf{v} \;=\; \alpha_1 \mathbf{e}_1 + \alpha_2 \mathbf{e}_2 + \ldots + \alpha_{k-1} \mathbf{e}_{k-1} \, ,$$

for some $\alpha_1, \ldots, \alpha_{k-1} \in \mathbb{Z}_p$, where at least one of $\alpha_1, \ldots, \alpha_{k-1}$ is nonzero. Hence there is some largest $\ell \leq k-1$, such that $\alpha_\ell \neq 0$ and

$$\mathbf{v} \;=\; \alpha_1 \mathbf{e}_1 + \alpha_2 \mathbf{e}_2 + \ldots + \alpha_\ell \mathbf{e}_\ell \, .$$

But then, by centrality of $\mathbf{v}$ and the form of the matrix T,

$$\mathbf{v} \;=\; \mathbf{v} T^{k-\ell-1} \;=\; \alpha_1 \mathbf{e}_{k-\ell+1} + \alpha_2 \mathbf{e}_{k-\ell+2} + \ldots + \alpha_\ell \mathbf{e}_k \, ,$$

which contradicts that $\mathbf{v}$ is a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_{k-1}$. Hence the core of S must be trivial, so that S affords a faithful permutation representation of $V \rtimes T$ of degree

$$|V \rtimes T : S| \;=\; p^2 \, .$$

Hence $\mu(V \rtimes T) \leq p^2$, so that $\mu(V \rtimes T) = p^2$, completing the proof of the lemma. □

Corollary 4.6. *Let i and j be integers such that $0 \leq i \leq j-2 \leq k-2$. Then the group $(V_j/V_i) \rtimes T_k$ has cyclic centre V_{i+1}/V_i of order p and minimal degree p^2.*

Proof. Put $\ell = j-i$, so that $\ell \geq 2$. By Theorem 4.2 and isomorphisms (32) and (35),

$$(V_j/V_i) \rtimes T_k \;\cong\; V_\ell \rtimes T_k \;\cong\; \overline{V_\ell} \rtimes T_\ell \;,$$

and the result follows by Lemma 4.5, using ℓ in place of k. □

Theorem 4.7. *If $k \geq 3$ then $V_k \rtimes T_k$ is almost exceptional of minimal degree p^2.*

Proof. Suppose that $k \geq 3$. Put $G = V_k \rtimes T_k$ and $N = Z(G)$. Then $N = V_1$ and $\mu(G) = p^2$, by Lemma 4.5. By (32) and (35) of Theorem 4.2,

$$G/N \;=\; (V_k/V_1) \rtimes T_k \;\cong\; V_{k-1} \rtimes T_k \;\cong \overline{V}_{k-1} \rtimes T_{k-1} \;.$$

But $k-1 > 1$, so that, applying Lemma 4.5, with $k-1$ in place of k, we get

$$\mu(G/N) \;=\; \mu\big(\overline{V}_{k-1} \rtimes T_{k-1}\big) \;=\; p^2 \;=\; \mu(G) \;,$$

completing the proof that G is almost exceptional. □

Corollary 4.8. *Let i and j be integers such that $0 \leq i \leq j-3 \leq k-3$. Then the group $(V_j/V_i) \rtimes T_k$ is almost exceptional of minimal degree p^2.*

Proof. Put $\ell = j-i$, so that $\ell \geq 3$. Again

$$(V_j/V_i) \rtimes T_k \;\cong\; \overline{V_\ell} \rtimes T_\ell \;,$$

and the result now follows by Theorem 4.7, with ℓ in place of k. □

Lemma 4.9. *Elements of $V_p \rtimes T_p$ have order 1, p or p^2. An element α has order p^2 if and only if $\alpha \notin V_p \cup (V_{p-1} \rtimes T_p)$, that is,*

$$\alpha \;=\; (\mathbf{v}, T_p^i)$$

for some $\mathbf{v} \in V_p \backslash V_{p-1}$ and $i \in \mathbb{Z}_p \backslash \{0\}$, in which case α^p is a nontrivial element of V_1, the centre of $V_p \rtimes T_p$.

Proof. Write, as usual, $T = T_p$, $I = I_p$, $V = V_p$ and put $G = V \rtimes T$. The subgroup V is elementary abelian, so all of its elements have order 1 or p. Thus if an element of G does not have order 1 or p then it must belong to $G \backslash V$. Let α be an element of $G \backslash V$, so

$$\alpha \;=\; (\mathbf{v}, T^i)$$

for some $\mathbf{v} \in V$ and $i \in \mathbb{Z}_p \backslash \{0\}$. We show that α has order p if $\mathbf{v} \in V_{p-1}$ and order p^2 otherwise. We may write

$$\mathbf{v} \;=\; \lambda_1 \mathbf{e}_1 + \lambda_2 \mathbf{e}_2 + \ldots + \lambda_p \mathbf{e}_p$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_p \in \mathbb{Z}_p$. Using the multiplication rule (15) for G, we have

$$\alpha^p \;=\; (\mathbf{w}, I) \;\equiv\; \mathbf{w} \;,$$

where

$$\mathbf{w} \;=\; \mathbf{v} + \mathbf{v}T^{-i} + \mathbf{v}T^{-2i} + \ldots + \mathbf{v}T^{-(p-1)i} \;.$$

Recall from (12) that $T = T_p$ is a permutation matrix, so the effect of applying T^{-i} to $\mathbf{v}$ is to subtract i from the subscripts of the coefficients modulo p, that is,

$$\mathbf{v}T^{-i} \;=\; \lambda_1 \mathbf{e}_{1-i} + \lambda_2 \mathbf{e}_{2-i} + \ldots + \lambda_p \mathbf{e}_{p-i} \;.$$

Observe that, for any $k \in \{1, \ldots, p\}$, the sequence

$$k\,,\; k-i\,,\; k-2i\,,\; \ldots\,,\; k-(p-1)i$$

reproduces the sequence $1, 2, \ldots, p$, in some order, when evaluated modulo p. Hence we may rewrite $\mathbf{w}$, gathering together and reordering coefficients, as

$$\begin{aligned} \mathbf{w} &= (\lambda_1 + \ldots + \lambda_p)\mathbf{e}_1 + (\lambda_1 + \ldots + \lambda_p)\mathbf{e}_2 + \ldots + (\lambda_1 + \ldots + \lambda_p)\mathbf{e}_p \\ &= (\lambda_1 + \ldots + \lambda_p)(\mathbf{e}_1 + \ldots + \mathbf{e_p})\,. \end{aligned}$$

We may now apply (28) (when $k = p$). If $\mathbf{v} \in V_{p-1}$ then $\lambda_1 + \ldots + \lambda_p = 0$ in $\mathbb{Z}_p$, so that $\mathbf{w} = \mathbf{0}$ and α has order p. On the other hand, if $\mathbf{v} \notin V_{p-1}$ then $\lambda_1 + \ldots + \lambda_p \neq 0$, giving $\mathbf{w} \neq \mathbf{0}$, so that $\mathbf{w}$ has order p and α has order p^2, in which case $\alpha^p \equiv \mathbf{w}$ is a nonzero scalar multiple of the generator of $Z(G) = V_1$, by (29). This completes the proof of the lemma. □

Corollary 4.10. *The exponent of $V_p \rtimes T_p$ is p^2 and the exponent of $V_{p-1} \rtimes T_p$ is p.*

Proof. By Lemma 4.9, elements of $V_p \rtimes T_p$ have order dividing p^2, and elements in the set $(V_p \rtimes T_p) \backslash (V_p \cup (V_{p-1} \rtimes T_p)$ have order p^2. Hence the exponent of $V_p \rtimes T_p$ is p^2. By Lemma 4.9, elements of $V_{p-1} \rtimes T_p$ have order dividing p, so the exponent of $V_{p-1} \rtimes T_p$ is p, completing the proof of the corollary. □

Theorem 4.11. *The exponent of $V_k \rtimes T_k$ is* $\begin{cases} p^2 & \textit{if } k = p, \\ p & \textit{if } k < p. \end{cases}$

Proof. Put $G = V_k \rtimes T_k$. If $k = p$ then the exponent of G is p^2, by Corollary 4.10. Suppose that $k < p$. For the purposes of applying Theorem 4.2, let V_k denote the vector space consisting of p-tuples, which is a T_p-invariant subspace of V_p of dimension k defined by (21) and appearing in the corresponding chain (20) of subspaces. Let $\overline{V_k}$, using the overline notation of Theorem 4.2, now denote the vector space of k-tuples, acted on by T_k. With this shift in notation, $G = \overline{V_k} \rtimes T_k$. By Theorem 4.2 and (35) (interpreted with p for k, and k for i, in this application), we now have

$$G \;=\; \overline{V_k} \rtimes T_k \;\cong\; V_k \rtimes T_p\;,$$

the latter being a nontrivial subgroup of $V_{p-1} \rtimes T_p$, since $k \leq p-1$, which has exponent p, by Corollary 4.10. Hence G also has exponent p, completing the proof of the theorem. □

5. THE WREATH PRODUCT $C_p \wr C_p$

Let p be a prime and put $W = C_p \wr C_p$. Recall, by identifying the second copy of the cyclic group C_p with the permutation group $\langle (1\;2\;\ldots\;p) \rangle$ we have the isomorphism

$$W \;=\; C_p \wr C_p \;\cong\; V_p \rtimes T_p$$

where T_p is the permutation matrix given by (12). As observed previously, $\mu(W) = p^2$, and W may be identified with the following permutation group on p^2 letters:

$$W \;\cong\; \langle (x_{11}\, x_{12}\, \ldots\, x_{1p}), (x_{11}\, x_{21} \ldots x_{p1})(x_{12}\, x_{22} \ldots x_{p2}) \ldots (x_{1p}\, x_{2p} \ldots x_{pp}) \rangle\;.$$

We may also give W the following presentation, which will be identified with W in what follows:

$$W \;\equiv\; \langle a_1, \ldots, a_p, c \mid a_i^p = [a_i, a_j] = c^p = 1\,, a_i^c = a_{i+1}\; (1 \leq i, j \leq p, i \neq j) \rangle \qquad (38)$$

where it is understood that $a_{p+1} \equiv a_1$. Put

$$B \;=\; \langle a_1, \ldots, a_p \rangle \;\cong\; C_p \times \ldots \times C_p \;,$$

which becomes the base group, extended by the cyclic group $C = \langle c \rangle$, so that W becomes an internal semidirect product

$$W \;=\; BC \;=\; B \rtimes C \;.$$

For $i = 0, \ldots, p$, let A_i correspond to V_i, under the isomorphism between $W = B \rtimes C$ and $V_p \rtimes T_p$. Then (20) corresponds to the following chain, which becomes a complete list of distinct normal subgroups of W contained in the base group B:

$$\{1\} \;=\; A_0 \;\subseteq A_1 \;\subseteq\; A_2 \;\subseteq\; \ldots \;\subseteq\; A_{p-2} \;\subseteq\; A_{p-1} \;\subseteq\; A_p \;=\; B\;. \tag{39}$$

In particular, we have the following analogues of (29) and (28):

$$A_1 \;=\; \langle a_1 a_2 \ldots a_p \rangle \tag{40}$$

and

$$A_{p-1} \;=\; \langle a_1 a_2^{-1}\,,\, a_2 a_3^{-1}\,,\, \ldots\,,\, a_{p-1} a_p^{-1} \rangle \;=\; \left\{ a_1^{\alpha_1} \ldots a_p^{\alpha_p} \;\middle|\; \alpha_1 + \ldots + \alpha_p = 0 \right\}\;. \tag{41}$$

Observe that A_{p-1} is the kernel of the evaluation homomorphism ν from A to the additive group $\mathbb{Z}_p$ with the rule

$$\nu :\; a_1^{\alpha_1} \ldots a_p^{\alpha_p} \;\mapsto\; \alpha_1 + \ldots + \alpha_p \;.$$

Henceforth, to decongest the notation in what follows, put

$$K \;=\; A_{p-1}\;.$$

We may form W/A_i, for each i, and, by analogy with (19) identify this with $(A/A_i) \rtimes C$. The result of Corollary 4.6 now translates to the following:

$$Z(W/A_i) \;=\; A_{i+1}/A_i\;, \tag{42}$$

for each $0 \le i \le p-2$, which is cyclic, because the vector space V_{i+1}/V_i is one-dimensional.

Consider now a proper normal subgroup N of W that is not contained in the base group B. Then N must contain an element x that has, as a factor, a nontrivial power of the generator c, with respect to the presentation (38). By replacing x by a suitable power, there is no loss of generality in assuming

$$x \;=\; ac \;\in\; N \tag{43}$$

for some $a \in A$. But now, because N is normal in W, we have, for each $i < p$,

$$[x, a_i] \;=\; [ac, a_i] \;=\; [c, a_i] \;=\; a_i^{-c} a_i \;=\; a_{i+1}^{-1} a_i \;=\; a_i a_{i+1}^{-1} \;\in\; N\;,$$

so that, by (41),

$$K \;\subseteq\; N\;. \tag{44}$$

It follows quickly, using the action of c on generators of A, that

$$(ac)^p \;=\; (a_1 \ldots a_n)^{a\nu}\;. \tag{45}$$

But the index of K in W is p^2, so that, since N is a proper subgroup of W not contained in A, it follows that N has index p in W and decomposes as a product of subgroups:

$$N \;=\; \langle K \cup \{x\} \rangle \;=\; K\langle x \rangle\;. \tag{46}$$

This product becomes an internal semidirect product with these factors if and only if x has order p, which occurs, by (45), if and only if $a\nu = 0$, that is, if and only if $a \in K$, in which case

$$N \;=\; \langle K \cup \{ac\}\rangle \;=\; \langle K \cup \{c\}\rangle \;=\; K\langle c\rangle \;=\; K \rtimes \langle c\rangle\,. \tag{47}$$

Observe further that

$$(aa_1^{-a\nu})\nu \;=\; a\nu - a\nu \;=\; 0\,,$$

so that $aa_1^{-a\nu} \in K$, so that, by (43) and (44),

$$a_1^{a\nu}x \;=\; (aa_1^{-a\nu})^{-1}ax \;\in\; N\,.$$

But $a\nu \in \mathbb{Z}_p$, so, there is no loss in generality, in assuming, instead of (43), that

$$x \;=\; a_1^j c \;\in\; N\,, \tag{48}$$

for some $j \in \mathbb{Z}_p$. When $j = 0$, we have (47). For $j \neq 0$, we have, in place of (46), the following:

$$N \;=\; K\langle a_1^j c\rangle\,. \tag{49}$$

Putting all of this together, using (39), (47) and (49), we obtain the lattice of all normal subgroups of $W = C_p \wr C_p$, depicted in the Hasse diagram of Figure 1.

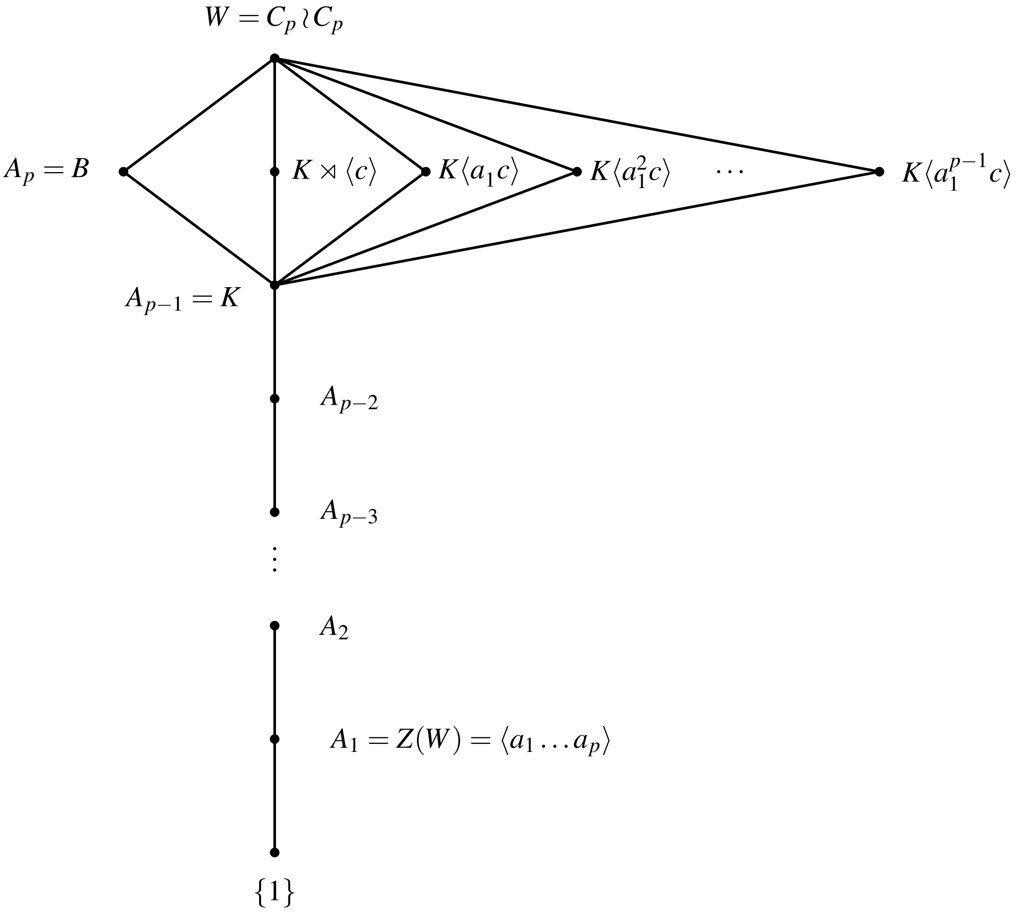
$W = C_p \wr C_p$
$A_p = B$
$K \rtimes \langle c\rangle$
$K\langle a_1 c\rangle$
$K\langle a_1^2 c\rangle$
$\cdots$
$K\langle a_1^{p-1} c\rangle$
$A_{p-1} = K$
A_{p-2}
A_{p-3}
$\vdots$
A_2
$A_1 = Z(W) = \langle a_1 \ldots a_p\rangle$
$\{1\}$

FIGURE 1. Lattice of normal subgroups of $C_p \wr C_p$

The following corollary now follows quickly from results of the previous section, which shows that it is possible to have almost exceptional groups with arbitrarily many nonisomorphic almost distinguished quotients. In fact, the normal subgroups form an arbitrarily long chain, so that the quotients have different orders.

Corollary 5.1. *Let p be any prime. The group $W = C_p \wr C_p$ is almost exceptional of minimal faithful degree p^2. If p is odd then W contains a chain of $p-2$ nontrivial normal subgroups, such that the respective quotients have the same minimal faithful degree.*

Proof. If $p = 2$ then $W \cong D_8$, which we have noted is almost exceptional at (4). Suppose henceforth that p is odd. By Theorem 4.7 and Corollary 4.8, taking $k = j = p$, we have

$$\mu(W) \;=\; \mu(W/A_i) \;=\; p^2$$

for $1 \leq i \leq p-2$. By observing that $A_1, \ldots, A_{p-2}$ (exhibited in Figure 1) form a chain of distinct normal subgroups, the proof is complete. □

6. Sections of the wreath product

Again we put $W = C_p \wr C_p$, and, as in the previous section, we identify elements and subgroups associated with the presentation (38), and adopt the notation $B = A_p$ for the base group and $K = A_{p-1}, A_{p-2}, \ldots, A_1 = Z(W), A_0 = \{1\}$ for the chain of normal subgroups properly contained in B.

Lemma 6.1. *Suppose that $w \in W \backslash B$. Then $w^p \in Z(W)$. Further $w^p \neq 1$ if and only if $w = ac^j$ for some $a \in B \backslash K$ and for some $j \in \{1, \ldots, p-1\}$, in which case $Z(W) = \langle w^p \rangle$. In particular, w has order p or p^2.*

Proof. This is a translation of Lemma 4.9 and corresponding facts about $V_p \rtimes T_p \cong W$. □

Lemma 6.2. *Suppose that H is a subgroup of W such that H is not contained in B. Then*

$$H \;=\; A_\ell \langle ac \rangle \tag{50}$$

for some $\ell \in \{0, \ldots, p\}$ and $a \in B$. If $a \in A_\ell$ then H becomes an internal semidirect product

$$H \;=\; A_\ell \langle c \rangle \;=\; A_\ell \rtimes \langle c \rangle \;\cong\; C_p^\ell \rtimes C_p \,. \tag{51}$$

If $a \in K$ then H becomes an internal semidirect product

$$H \;=\; A_\ell \rtimes \langle ac \rangle \;\cong\; C_p^\ell \rtimes C_p \,. \tag{52}$$

Proof. Because $H \not\subseteq A$, there exists $w \in H$ of the form

$$w \;=\; ac$$

for some $a \in B$. Clearly $H \cap B \subseteq B = A_p$, so there is some least $\ell \leq p$, such that

$$H \cap B \;\subseteq\; A_\ell \,.$$

Let $v \in H$. If $v \in B$ then $v \in H \cap B \subseteq A_\ell$, so that $v \in A_\ell \langle w \rangle$. Suppose now that $v \notin B$, so that

$$v \;=\; bc^i$$

for some $b \in B$ and $i \in \{1, \ldots, p-1\}$. Then

$$w^i \;=\; dc^i$$

for some $d \in B$, so that

$$v^{-1}w^i \;=\; c^{-i}b^{-1}dc^i \;=\; (b^{-1}d)^{c^i} \;\in\; H \cap B \;\subseteq\; A_\ell\;,$$

so that $v \in A_\ell\langle w\rangle$. This proves that

$$H \;\subseteq\; A_\ell\langle w\rangle\;. \tag{53}$$

We claim that

$$H \cap B \;=\; A_\ell\;. \tag{54}$$

First note that (54) holds trivially if $\ell = 0$. Suppose now that $\ell > 0$. By minimality of ℓ, there exists $b \in H$ with $b \in A_\ell \backslash A_{\ell-1}$. Regarding A_ℓ as a vector space over $\mathbb{Z}_p$, on which w acts by conjugation, b generates a submodule of A_ℓ, and this is contained in H. Since $b \notin A_{\ell-1}$, this submodule must coincide with A_ℓ, since the submodules form a chain, so that

$$A_\ell \;\subseteq\; H \cap B \;\subseteq\; A_\ell\;,$$

whence $H \cap B = A_\ell$. This shows that (54) holds for all ℓ, and so

$$A_\ell\langle w\rangle \;=\; (H \cap B)\langle w\rangle \;\subseteq\; H\;. \tag{55}$$

By (53) and (55), we conclude that

$$H \;=\; A_\ell\langle w\rangle\;,$$

proving (50). If $a \in A_\ell$ then, immediately, $A_\ell \cap \langle c\rangle = \{1\}$, yielding an internal semidirect product

$$H \;=\; A_\ell\langle ac\rangle \;=\; A_\ell\langle c\rangle \;=\; A_\ell \rtimes \langle c\rangle\;,$$

verifying (51). If $a \in K$ then, by Lemma 6.1, the order of w is p, so that $A_\ell \cap \langle w\rangle = \{1\}$, whence H is an internal semidirect product of A_ℓ by $\langle w\rangle$, verifying (52). This completes the proof of the lemma. □

Lemma 6.3. *Suppose that* $0 \le m \le \ell - 2 \le p - 2$, $a \in B$ *and put*

$$H \;=\; A_\ell\langle ac\rangle/A_m\;.$$

Then

$$Z(H) \;=\; A_{m+1}/A_m$$

is cyclic of order p *and* $\mu(H) = p^2$.

Proof. Consider the subgroup

$$H' \;=\; A_\ell\langle c\rangle/A_m\;,$$

so that $H' = H$ if $a = 1$, and $H' \cong H$ if $|a| = p$. Observe that if $b \in B$ then b commutes with c if and only if b commutes with ac, from which it follows that

$$Z(H) \;=\; Z(H')\;.$$

Under the isomorphism between $W = C_p \wr C_p$ and $V_p \rtimes T_k$, we have that H' corresponds to

$$(V_\ell/V_m) \rtimes T_p\;,$$

which, by Corollary 4.6, has minimal degree p^2 and centre

$$Z\big((V_\ell/V_m) \rtimes T_p\big) \;=\; V_{m+1}/V_m\;,$$

which, in turn, using the inverse of the isomorphism, corresponds to

$$Z(H') \;=\; A_{m+1}/A_m\;.$$

The statement of the lemma is then immediate if $a = 1$ or $|a| = p$. Suppose then that $a \neq 1$ and $|a| \neq p$. By Lemma 6.1, $a \in A_p \backslash A_{p-1}$ and $|a| = p^2$. We have

$$\mu(H) \;\geq\; \mu\big(\langle ac\rangle\big) \;=\; \mu(C_{p^2}) \;=\; p^2 \,,$$

and, again by Corollary 4.6,

$$\mu(H) \;\leq\; \mu\big((A_p/A_m)\langle c\rangle\big) \;=\; \mu(V_p/V_m) \rtimes T) \;=\; p^2 \,,$$

whence $\mu(H) = p^2$, completing the proof of the lemma. □

Lemma 6.4. *Suppose that $S = H/N$ is a section of W such that N is not contained in B. Then S is trivial or cyclic of order p.*

Proof. Suppose that S is nontrivial. By Lemma 6.2 and (54), we have

$$N \;=\; A_\ell\langle ac\rangle \qquad \text{and} \qquad N \cap B \;=\; A_\ell$$

for some $\ell \in \{0,\ldots,p\}$ and $a \in B$. But H also is not contained in A, so, again, by Lemma 6.2 and (54), we have

$$H \;=\; A_m\langle bc\rangle \qquad \text{and} \qquad H \cap B \;=\; A_m$$

for some $m \in \{0,\ldots,p\}$ and $b \in B$. But

$$a^{-1}b \;=\; c(c^{-1}a^{-1}bc)c^{-1} \;=\; \big((ac)^{-1}bc)\big)^{bc} \;\in\; H \cap B \;=\; A_m \,,$$

so we also have

$$H \;=\; A_m\langle bc\rangle \;=\; A_m\langle ab^{-1}bc\rangle \;=\; A_m\langle ac\rangle \,.$$

Further, since $H \neq N$, we have

$$m \;>\; \ell \,.$$

Suppose that $m > \ell + 1$, so that A_m properly contains $A_{\ell+1}$. By Corollary 4.6, the group $(V_m/V_\ell) \rtimes T_p$ has cyclic centre of order p, which must be the unique minimal normal subgroup $V_{\ell+1}/V_\ell$, so that, correspondingly,

$$Z(A_m\langle c\rangle/A_\ell) \;=\; A_{\ell+1}/A_\ell \,.$$

Choose any $d \in A_m \backslash A_{\ell+1}$. But N is normal in H, so that

$$[d,c] \;=\; [d,ac] \;\in\; N \cap B \;=\; A_\ell \,.$$

Hence the coset $A_\ell\, d$ commutes with the coset $A_\ell\, c$, so that

$$A_\ell d \;\in\; Z(A_m\langle c\rangle/A_\ell) \;=\; A_{\ell+1}/A_\ell \,,$$

whence $d \in A_{\ell+1}$. But this contradicts that $d \notin A_{\ell+1}$. This proves that $m = \ell + 1$, so that

$$H \;=\; A_{\ell+1}\langle ac\rangle \,,$$

and $N = A_\ell\langle ac\rangle$ has index p in H. Hence $S = H/N$ is cyclic of order p, and the lemma is proved. □

Lemma 6.5. *Let S be an abelian section of $W = C_p \wr C_p$ Then either*

(i) *S is elementary abelian of rank at most p, in which case $\mu(S) = kp$ for some k such that $0 \leq k \leq p$, or*

(ii) *S is cyclic of order p^2, in which case $\mu(S) = p^2$.*

Case (ii) *occurs if and only if $S = \langle ac\rangle$ for some $a \in B\backslash K$.*

Proof. Clearly (i) holds if S is trivial, so we may assume that S is nontrivial. If S is a section of B then immediately S must be elementary abelian of rank at most p and (i) holds. Hence we may suppose that $S = H/N$ is not a section of B, say for some subgroup H of G not contained in B. If N is not contained in B then, by Lemma 6.4, S is trivial or cyclic of order p, so that (i) holds. We may suppose, therefore, that N is contained in B, so is an elementary abelian subgroup of rank r, say. By Lemma 6.2 and (54), we have

$$H \;=\; A_\ell\langle ac\rangle \qquad \text{and} \qquad H\cap B \;=\; A_\ell$$

for some $\ell \in \{0,\dots,p\}$ and $a \in A$. Since $N \subseteq H\cap B = A_\ell$, we have

$$r \;\le\; \ell\;,$$

whence $N = A_r$, since A_r is the unique normal subgroup of H contained in A_ℓ of rank r. If $r \le \ell-2$ then

$$S \;=\; A_\ell\langle ac\rangle/A_r$$

is nonabelian, since $Z(S) = A_{r+1}/A_r$, by Lemma 6.3, which is impossible. Hence $r=\ell$ or $\ell-1$. Suppose that $r=\ell-1$. Then $\ell\ge 1$ and

$$S = \;A_\ell\langle ac\rangle/A_{\ell-1}\;.$$

If $\ell \ge 2$ then S is elementary abelian of order p^2, noting that

$$(ac)^p \;\in\; Z(W) \;=\; A_1 \;\subseteq\; A_{\ell-1}\;,$$

by Lemma 6.1, and (i) holds. If $\ell=1$ then

$$S \;=\; A_1\langle ac\rangle/A_0 \;\equiv\; Z(W)\langle ac\rangle \;=\; \begin{cases}\langle ac\rangle \;\cong\; C_{p^2} & \text{if } a\in B\backslash K\;,\\ Z(W)\times\langle ac\rangle \;\cong\; C_p\times C_p & \text{if } a\in K\;,\end{cases}$$

by Lemma 6.1, so that (ii) or (i) hold respectively. Suppose finally that $r=\ell$. If $\ell\ge 1$ then

$$S \;=\; A_\ell\langle ac\rangle/A_\ell \;\cong\; \langle ac\rangle\;,$$

which is cylic of order p, noting that $(ac)^p \in Z(W) = A_1 \subseteq A_\ell$, by Lemma 6.1, and (i) holds. If $\ell=0$ then

$$S \;=\; A_0\langle ac\rangle/A_0 \;\equiv\; \langle ac\rangle \;\cong\; \begin{cases} C_{p^2} & \text{if } a\in B\backslash K\;,\\ C_p & \text{if } a\in K\;,\end{cases}$$

by Lemma 6.1, so that (ii) or (i) hold respectively. Note, from just two subcases in the above analysis, that (ii) holds if and only if $S = \langle ac\rangle$ with $a\in B\backslash K$, completing the proof of the lemma. □

Lemma 6.6. *Let S be a nonabelian section of $W = C_p \wr C_p$ Then*

$$S \;=\; A_m\langle ac\rangle/A_\ell$$

for some $a\in A$, and $\ell \le m-2$ such that $0\le\ell\le p-2$ and $2\le m\le p$. Furthermore,

$$\mu(S) \;=\; p^2\;.$$

Proof. Suppose that $S = H/N$ for some H and N. If N is not contained in B, then, by Lemma 6.4, S is trivial or cyclic of order p, contradicting that S is nonabelian. Hence N is contained in B so is an elementary abelian subgroup of rank ℓ, say. If H is also contained in B then S would be elementary abelian, again a contradiction. Hence H is not contained in B, so that, by Lemma 6.2 and (54), we have

$$H \;=\; A_m\langle ac\rangle \qquad \text{and} \qquad H\cap B \;=\; A_m$$

for some $m \in \{0,\dots,p\}$ and $a \in B$. Since $N \subseteq H\cap B = A_\ell$, we have

$$\ell \;\leq\; m\,.$$

Note that N is closed under conjugation by ac, so also under conjugation by c, so that N is normal in W. Hence $N = A_\ell$, since A_ℓ is the unique normal subgroup of W contained in A_m of rank ℓ. If $\ell = m$ or $\ell = m-1$, then S is abelian, by the proof of the previous lemma, which is a contradiction. Hence $\ell \leq m-2$, so that $\ell \leq p-2$ and $2 \leq m$. By Lemma 6.3, we have

$$Z(S) = A_{\ell+1}/A_\ell\;,$$

which is cyclic of order p, so that, by Proposition 1.3,

$$\mu(S) \;\geq\; p\mu\big(Z(S)\big) \;=\; p^2\,.$$

But S is a subgroup of W and $\mu(W) = p^2$, so that $\mu(S) = p^2$, completing the proof of the lemma. □

Theorem 6.7. *Let p be any odd prime. A section S of $C_p \wr C_p$ is almost exceptional if and only if S is nonabelian of order at least p^4, in which case $\mu(S) = p^2$ and S is isomorphic to an extension of a k-dimensional vector space over $\mathbb{Z}_p$ by a cyclic group of order p with a nontrivial conjugation action, for some k such that* $3 \leq k \leq p$.

Proof. Put $W = C_p \wr C_p$ and suppose that S is a section of W. If S is abelian then S cannot be exceptional (by Theorem 1.1).

Suppose that S is nonabelian. In the following, we show that $|S| \geq p^3$ and S is almost exceptional if and only if $|S| \geq p^4$. By Lemma 6.6,

$$S \;=\; A_m\langle ac\rangle/A_\ell$$

for some $a \in A$, and $\ell \leq m-2$ such that $0 \leq \ell \leq p-2$ and $2 \leq m \leq p$, and $\mu(S) = p^2$. Then A_m/A_ℓ is an elementary abelian normal subgroup of S of rank $m-\ell \geq 2$, which may be regarded as a vector space of dimension $m-\ell$ over $\mathbb{Z}_p$. By Lemma 6.1, we have $(ac)^p \in A_1 \subseteq A_m$, so that S is an extension of A_m/A_ℓ by

$$S/(A_m/A_\ell) \;\cong\; A_m\langle ac\rangle/A_m \;\cong\; \langle ac\rangle/(\langle ac\rangle\cap A_m) \;=\; \langle ac\rangle/\langle (ac)^p\rangle \;\cong\; C_p\;,$$

noting, again by Lemma 6.1, that ac has order p or p^2. This shows that S is an extension of a k-dimensional vector space by a cyclic group of order p. The wreath action, inherited from W, guarantees that the conjugation action is nontrivial. Put

$$k \;=\; m-\ell\,,$$

so that $k \geq 2$. If $k = 2$ then

$$S \;=\; A_m\langle ac\rangle/A_{m-2}\;,$$

$|S| = p^3$, and the nontrivial quotients of S are elementary abelian, by the proof of Lemma 6.5, of minimal degree less that p^2, so that S is not almost exceptional. Suppose that $k \geq 3$, so A_{m-2}/A_ℓ is a nontrivial normal subgroup of S. Then

$$A_m\langle ac\rangle/A_{m-2} \;\cong\; S/(A_{m-2}/A_\ell)$$

is a nontrivial quotient of S of minimal degree p^2, so that S is almost exceptional. Observe that

$$|S| \;=\; |A_m\langle ac\rangle/A_\ell| \;=\; p^{m-\ell+1} \;=\; p^{k+1} \;\geq\; p^4\,,$$

completing the proof of the theorem. □

7. Application to central products

Recall that if H and K are groups such that Z_1 is a subgroup of $Z(H)$ and Z_2 is a subgroup of $Z(K)$, and $\varphi : Z_1 \to Z_2$ is an isomorphism, then the *external central product of H and K via φ* is the group

$$H * K \;=\; (H \times K)/N$$

where

$$N \;=\; \{(h^{-1}, h\varphi) \mid h \in Z_1\}\,.$$

Recall that a group G is an *internal central product* of subgroups H and K if $G = HK$ and elements of H commute with elements of K, in which case G is isomorphic to the *external central product* of H and K via the identity map applied to $H \cap K$. The external central product $H * K$ above, via $\varphi : Z_1 \to Z_2$, may be identified with an internal central product HK in a natural way, by identifying H with $(H \times \{1\})N/N$, K with $(\{1\} \times K)N/N$ and $H \cap K$ with

$$\{N(h,1) \mid h \in Z_1\} \;=\; \{N(1, h\varphi \mid h \in Z_1\}\,.$$

We use the notation $H * K$ to denote both the external and associated internal central products of H and K. In this section, we will only be considering central products, in terms of the above notation for the external central product, where p is an odd prime, H and K are p-groups and

$$Z_1 \;=\; Z(H) \;\cong\; C_p \;\cong\; Z(K) \;=\; Z_2\,. \tag{56}$$

It follows from (56), regarded as an internal central product, and the definitions, that

$$Z(H * K) \;=\; H \cap K \;\cong\; C_p\,. \tag{57}$$

Hence, we may iterate taking central products and have, as a consequence of (57), the following result:

Lemma 7.1. *Let p be an odd prime and $n \geq 2$ an integer. Suppose that $G_1, \ldots, G_n$ are nonabelian p-groups such that*

$$Z(G_i) \;\cong\; C_p$$

for $1 \leq i \leq n$. Then

$$Z(G_1 * \ldots * G_n) \;\cong\; C_p\,. \tag{58}$$

For $1 \leq i \leq n$,

$$\mu(G_i) \;=\; p^{\alpha_i} \tag{59}$$

for some positive integer α_i, and

$$\mu(G_1 * \ldots * G_n) \;=\; p^{\alpha} \tag{60}$$

for some positive integer $\alpha \geq \max\{\alpha_1,\dots,\alpha_n\}+1$.

Proof. Put $G = G_1 * \ldots * G_n$. That $Z(G) \cong C_p$ follows from (57), so that (58) holds. By Theorem 1.2, each of $\mu(G_1),\dots,\mu(G_n),\mu(G)$ must be a power of p, since the minimal representations are transitive. In particular, there are positive integers $\alpha_1,\dots,\alpha_n,\alpha$ such that (59) and (60) hold. Certainly

$$\mu(G) \;\geq\; \max\{\mu(G_1),\dots,\mu(G_n)\} \;=\; p^{\max\{\alpha_1,\dots,\alpha_n\}}\;,$$

since G_i embeds in G for $1 \leq i \leq n$. Reordering the groups, if necessary, we may suppose that

$$\mu(G_1) \;=\; \max\{\mu(G_1),\dots,\mu(G_n)\}\;,$$

so that $\alpha_1 = \max\{\alpha_1,\dots,\alpha_n\}$ and

$$p^{\alpha} \;=\; \mu(G) \;\geq\; \mu(G_1) \;=\; p^{\alpha_1}\;,$$

so that $\alpha \geq \alpha_1$. Suppose that $\alpha = \alpha_1$, so that $\mu(G) = \mu(G_1)$. Observe that G may be regarded as an internal central product $G = G_1H$ where $H \cong G_2 * \ldots * G_n$ is a nonabelian group and

$$Z(G) \;=\; Z(G_1) \;=\; Z(H) \;=\; G_1 \cap H \;\cong\; C_p\;.$$

In particular, H is noncyclic so H contains a nontrivial subgroup S such that

$$S \cap G_1 \;=\; S \cap (G_1 \cap H) \;=\; S \cap Z(G) \;=\; S \cap Z(H) \;= \{1\}\;.$$

Hence, because all elements of G_1 commute with all elements of H, the subgroup G_1S of G is an internal direct product, so that, by Theorem 1.4,

$$\mu(G) \;\geq\; \mu(G_1S) \;=\; \mu(G_1)+\mu(S) \;>\; \mu(G_1) \;=\; \mu(G)\;,$$

which is a contradiction. Hence $\alpha \geq \alpha_1 + 1$, completing the proof of the lemma. □

We can now exhibit a proliferation of sequences of exceptional p-groups with the property that taking the minimal faithful degree of successive direct products grows as a linear function of the number of factors, compared with exponential growth of the minimal faithful degree of the associated central products (which are quotients of the respective direct products).

Theorem 7.2. *Suppose that* p *is an odd prime and* $n \geq 1$ *is an integer. Suppose that* $G_1,\dots,G_n$ *are nonabelian sections of* $C_p \wr C_p$. *Then*

$$\mu(G_1 \times \ldots \times G_n) \;=\; np^2\;, \tag{61}$$

whilst

$$\mu(G_1 * \ldots * G_n) \;=\; p^{n+1}\;. \tag{62}$$

In particular, for $n \geq 2$, *the group* $G_1 \times \ldots \times G_n$ *is exceptional with minimal faithful degree that is a linear function of* n, *with distinguished quotient* $G_1 * \ldots * G_n$, *which has minimal faithful degree that is an exponential function of* n.

Proof. By Lemma 6.6, $\mu(G_i) = p^2$ for $1 \leq i \leq n$ and, by Theorem 1.4,

$$\mu(G_1 \times \ldots \times G_n) \;=\; \mu(G_1)+\ldots+\mu(G_n) \;=\; np^2\;,$$

verifying (61). We verify (62) by induction. The induction starts trivially, so suppose (62) holds for $n \geq 1$ and that G_{n+1} is a nonabelian section of $C_p \wr C_p$. Put

$$H \;=\; G_1 * \ldots * G_n$$

and

$$G \;=\; H * G_{n+1}\;.$$

We may regard G as an internal central product $G = HG_{n+1}$, where

$$Z(G) \;=\; Z(H) \;=\; Z(G_{n+1}) \;=\; H \cap G_{n+1}\;.$$

By the inductive hypothesis, $\mu(H) = p^{n+1}$ and, by Lemma 6.6, $\mu(G_{n+1}) = p^2$, so that

$$\max\{p^{n+1}, p^2\} \;=\; p^{n+1}\;.$$

By Lemma 7.1,

$$\mu(G) \;\geq\; p^{(n+1)+1} \;=\; p^{n+2}\;.$$

To establish the inductive step, it suffices to find a faithful representation of G of degree p^{n+2}. By Lemmas 6.3 and 6.6, the centres of $G_1, \ldots, G_{n+1}$ are cyclic of order p. By Lemma 7.1, H also has a cyclic centre of order p. By Theorem 1.2, H and G_{n+1} have transitive faithful minimal representations afforded by some subgroups S_1 for H and S_2 for G_{n+1} respectively. By faithfulness,

$$S_1 \cap Z(H) \;=\; S_2 \cap Z(G_{n+1}) \;=\; \{1\}\;.$$

In particular,

$$\{1\} \;=\; S_1 \cap Z(H) \;=\; S_1 \cap H \cap G_{n+1} \;=\; S_1 \cap G_{n+1}\;,$$

which implies that

$$S_1 \cap S_2 \;=\; \{1\}\;.$$

Elements of H commute with elements of G_n, so that S_1S_2 is a subgroup of G, which becomes an internal direct product. Hence $|S_1S_2| = |S_1||S_2|$, so that

$$|G : S_1S_2| \;=\; \frac{|G|}{|S_1S_2|} \;=\; \frac{|H||G_{n+1}|}{p|S_1||S_2|} \;=\; \frac{1}{p}\mu(H)\mu(G_{n+1}) \;=\; p^{n+1+2-1} \;=\; p^{n+2}\;.$$

We now verify that S_1S_2 has trivial core in G. Let

$$x \;\in\; S_1S_2 \cap Z(G) \;=\; S_1S_2 \cap (H \cap G_{n+1})\;,$$

so that $x = st$ for some $s \in S$ and $t \in T$. But then, since $x, t \in G_{n+1}$, we have

$$s \;=\; xt^{-1} \;\in\; S_1 \cap G_{n+1} \;=\; S_1 \cap (H \cap G_{n+1}) \;=\; S_1 \cap Z(H) \;=\; \{1\}\;,$$

and, also, since $x, s \in H$, we have

$$t \;=\; xs^{-1} \;\in\; S_2 \cap H \;=\; S_2 \cap (H \cap G_{n+1}) \;=\; S_2 \cap Z(G_{n+1}) \;=\; \{1\}\;.$$

This shows that $x = s = t = 1$, so that the core of S_1S_2 in G must be trivial. This shows that S_1S_2 is a core-free subgroup of G of index p^{n+2}, so that

$$\mu(G) \;\leq\; p^{n+2}\;,$$

whence $\mu(G) = p^{n+2}$, establishing the inductive step, so that (62) holds always. Observe that, for $n \geq 2$,

$$p^{n+2} \;>\; np^2\;,$$

so that $G_1 \times \ldots \times G_n$ is exceptional with distinguished quotient $G_1 * \ldots * G_n$, completing the proof of the theorem. □

8. Appendix: Wreath Products of Orders up to 500

$\mathscr{Q}$: G is almost exceptional, i.e. $\exists$ nontrivial $N \lhd G$ such that $\mu(G) = \mu(G/N)$

$\mathscr{E}$: G is exceptional, i.e. $\exists\, N \lhd G$ such that $\mu(G) < \mu(G/N)$

$\mathscr{D}$: Decreasing quotients, i.e. $\mu(G/N) < \mu(G)$ for all nontrivial $N \lhd G$

$\mathscr{S}$: $\exists$ proper $S \leq G$ such that $\mu(G) = \mu(S)$

$\mathscr{N}$: G is nilpotent

Groups	**Order. ID**	$\mu(G)$	$\mathscr{N}$	$\mathscr{S}$	$\mathscr{Q}$	$\mathscr{E}$	$\mathscr{D}$
$C_2 \wr C_2$	8.3	4	✓	✓	✓	×	×
$C_3 \wr C_2$	18.3	6	×	✓	×	×	✓
$C_2 \wr C_3$	24.13	6	×	✓	×	×	✓
$C_4 \wr C_2$	32.11	8	✓	✓	✓	×	×
$C_2^2 \wr C_2$	32.27	8	✓	✓	×	×	✓
$C_2 \wr S_3$	48.48	6	×	✓	×	×	✓
$C_5 \wr C_2$	50.3	10	×	✓	×	×	✓
$C_2 \wr C_4$	64.32	8	✓	✓	✓	×	×
$C_2 \wr C_2^2$	64.138	8	✓	✓	✓	×	×
$C_6 \wr C_2$	72.30	10	×	✓	×	×	✓
$S_3 \wr C_2$	72.40	6	×	✓	×	×	✓
$C_3 \wr C_3$	81.7	9	✓	✓	✓	×	×
$C_7 \wr C_2$	98.3	14	×	✓	×	×	✓
$C_8 \wr C_2$	128.67	16	✓	✓	✓	×	×
$(C_2 \times C_4) \wr C_2$	128.628	12	✓	✓	✓	×	×
$D_8 \wr C_2$	128.928	8	✓	✓	✓	×	×
$Q_8 \wr C_2$	128.937	16	✓	✓	×	×	✓
$C_2^3 \wr C_2$	128.1578	12	✓	✓	×	×	✓
$C_2 \wr C_5$	160.235	10	×	✓	✓	×	×
$C_9 \wr C_2$	162.3	18	×	✓	×	×	✓

Continued on next page

Table 1 – *continued from previous page*

Groups	**Order. ID**	$\mu(G)$	$\mathscr{N}$	$\mathscr{S}$	$\mathscr{Q}$	$\mathscr{E}$	$\mathscr{D}$
$C_3 \wr S_3$	162.10	9	×	✓	✓	×	×
$C_3^2 \wr C_2$	162.52	12	×	✓	✓	×	×
$C_4 \wr C_3$	192.188	12	×	✓	✓	×	×
$C_2 \wr A_4$	192.201	8	×	✓	✓	×	×
$C_2^2 \wr C_3$	192.1540	12	×	✓	×	×	✓
$C_{10} \wr C_2$	200.31	14	×	✓	×	×	✓
$D_{10} \wr C_2$	200.43	10	×	✓	×	×	✓
$C_{11} \wr C_2$	242.3	22	×	✓	×	×	✓
$C_{12} \wr C_2$	288.239	14	×	✓	✓	×	×
$Dic_3 \wr C_2$	288.389	14	×	✓	×	×	✓
$(C_2 \times C_6) \wr C_2$	288.724	14	×	✓	×	×	✓
$D_{12} \wr C_2$	288.889	10	×	✓	×	×	✓
$A_4 \wr C_2$	288.1025	8	×	✓	×	×	✓
$C_2 \wr D_{10}$	320.1636	10	×	✓	✓	×	×
$C_3 \wr C_4$	324.162	12	×	✓	×	×	✓
$C_3 \wr C_2^2$	324.167	12	×	✓	×	×	✓
$C_{13} \wr C_2$	338.3	26	×	✓	×	×	✓
$C_5 \wr C_3$	375.6	15	×	✓	✓	×	×
$C_{14} \wr C_2$	392.27	18	×	✓	×	×	✓
$D_{14} \wr C_2$	392.37	14	×	✓	×	×	✓
$C_{15} \wr C_2$	450.29	16	×	✓	×	×	✓

REFERENCES

[1] J.R. Britnell, N. Saunders and T. Skyner. On exceptional groups of order p^5. *J. Pure App. Algebra*, 221 (2017), 2647–2665.

[2] R. Chamberlain. Minimal exceptional p-groups. *Bull. Aust. Math. Soc.* 98 (2018), 434–438.

[3] R. Chamberlain. Subgroups with no abelian composition factors are not distinguished. *Bull. Aust. Math. Soc.* 101 (2020), 446–452.

[4] H.E.A. Campbell and D.L. Wehlau. *Modular Invariant Theory.* Berlin, Heidelberg: Springer Nature, 2011.

[5] D. Easdown and C.E.. Praeger. On minimal permutation representations of finite groups. *Bull. Aust. Math. Soc.*, 38 (1988), 207–220.

[6] D. Easdown and M. Hendriksen. Minimal permutation representations of semidirect products of groups. *J. Group Theory*, 19(6) (2016), 1017–1048.

[7] C. Franchi. On minimal degrees of permutation representations of abelian quotients of finite groups. *Bull. Aust. Math. Soc.* 84 (2011), 408–413.

[8] D. Johnson. Minimal permutation representations of finite groups. *Am. J. Math.*, 93 (1971), 857–866.

[9] G.I. Karpilovsky. The least degree of a faithful representation of abelian groups. *Vestni Khar'kov Gos. Univ.*, 53 (1970), 107-115.

[10] L. Kovacs and C.E.. Praeger. Finite permutation groups with large abelian quotients. *Pacific J. Math.* 136 (1989), 283–292.

[11] L. Kovacs and C.E.. Praeger. On minimal faithful permutation representations of finite groups. *Bull. Aust. Math. Soc.*, 62 (2000), 311–317.

[12] S. Lemieux. Finite exceptional p-groups of small order. *Comm. Algebra*, 35 (2007), 1890–1894.

[13] P. Neumann. Some algorithms for computing with finite permutation groups. In E. Robertson and C. Campbell (Eds.), Groups (St Andrews 1985), London Math. Soc. Lecture Note Ser. 121. Cambridge University Press, Cambridge (1987), 59–92.

[14] D. Wright. Degrees of minimal embeddings for some direct products. *Am. J. Math.*, 97 (1976), 897–903.

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SYDNEY, NSW 2006, AUSTRALIA
E-mail address: `ialo9634@uni.sydney.edu.au, ialotaibi@tvtc.gov.sa`

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF SYDNEY, NSW 2006, AUSTRALIA
E-mail address: `david.easdown@sydney.edu.au`