Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2009, Article ID 245617, 12 pages
doi:10.1155/2009/245617

*Research Article*

# Automorphisms of Regular Wreath Product $p$-Groups

**Jeffrey M. Riedl**

*Department of Theoretical and Applied Mathematics, University of Akron, Akron, OH 44325-4002, USA*

Correspondence should be addressed to Jeffrey M. Riedl, riedl@uakron.edu

Received 12 July 2009; Revised 5 November 2009; Accepted 6 November 2009

Recommended by Alexander Rosa

We present a useful new characterization of the automorphisms of the regular wreath product group $P$ of a finite cyclic $p$-group by a finite cyclic $p$-group, for any prime $p$, and we discuss an application. We also present a short new proof, based on representation theory, for determining the order of the automorphism group $\mathrm{Aut}(P)$, where $P$ is the regular wreath product of a finite cyclic $p$-group by an arbitrary finite $p$-group.

Copyright © 2009 Jeffrey M. Riedl. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1. Introduction

Let $P$ denote the regular wreath product group $C \wr Q$, where $Q$ is an arbitrary nontrivial finite $p$-group, for some prime $p$, and where $C$ is an any finite cyclic $p$-group. Thus $P$ is the semidirect product $B \rtimes Q$, where $B$ is a direct product of $|Q|$ copies of $C$, and where $Q$ acts via automorphisms on $B$ by regularly permuting these direct factors.

In [1], Houghton determines some information on the structure of the automorphism group $\mathrm{Aut}(P)$. Using this work of Houghton (see also [2, Chapter 5]), it is possible to calculate the order of $\mathrm{Aut}(P)$. Our first result in this paper is to present an alternative method for calculating the order of $\mathrm{Aut}(P)$. Our approach to this calculation is to apply the Automorphism Counting Formula (established in [3]), a general formula for the order of the automorphism group $\mathrm{Aut}(G)$ of a monolithic finite group $G$ in terms of information about the complex characters of $G$ and information about how $G$ is embedded as a subgroup of a particular finite general linear group. A finite group is said to be monolithic if and only if it has a unique minimal normal subgroup. Thus a finite $p$-group is monolithic if and only if its center is cyclic. Let $|C| = p^e$ and $|Q| = p^n$. Throughout this paper we assume that $p^{en} \geq 3$, which excludes only the case where $p = 2$ and $e = n = 1$, for which $P$ is dihedral of order 8.

**Theorem 1.1.** $\mathrm{Aut}(P)$ *has order* $|\mathrm{Aut}(Q)|(p-1)p^a$, *where* $a = 2ep^n - e - 1$.

Because the dihedral group of order 8 has an automorphism group of order 8, the condition $p^{en} \geq 3$ is a necessary hypothesis for Theorem 1.1.

The next result is a step along the way to proving Theorem 1.1. We mention it here.

**Theorem 1.2.** *Let* $q$ *be any prime-power larger than* 1 *such that* $p^e$ *is the full* $p$*-part of* $q-1$. *Then the general linear group* $\mathrm{GL}(p^n, q)$ *has exactly one conjugacy class of subgroups whose members are isomorphic to* $P$.

Now suppose that the group $Q$ of order $p^n$ is cyclic. Since $\mathrm{Aut}(Q)$ has order $(p-1)p^{n-1}$, Theorem 1.1 yields $|\mathrm{Aut}(P)| = (p-1)^2 p^{2ep^n+n-e-2}$. Using knowledge of $|\mathrm{Aut}(P)|$ and little more than an elementary counting argument, we obtain a useful new characterization of the automorphisms of $P$. Before stating this characterization, we establish some notation.

*Hypothesis 1.3.* Assume that the group $Q$ of order $p^n$ is cyclic. Let $\mathrm{x}_0, \mathrm{x}_1, \ldots, \mathrm{x}_{p^n-1}$ be a collection of elements of order $p^e$ that constitutes a generating set for the homocyclic group $B$ of exponent $p^e$ and of rank $p^n$. Let w be a generator for the cyclic group $Q$ and suppose that $\mathrm{x}_u^{\mathrm{w}} = \mathrm{x}_{u-1}$ for each $u \in \{1, \ldots, p^n - 1\}$ and that $\mathrm{x}_0^{\mathrm{w}} = \mathrm{x}_{p^n-1}$.

Under Hypothesis 1.3, it is clear that $\{\mathrm{x}_{p^n-1}, \mathrm{w}\}$ is a generating set for the group $P$, and so every automorphism of $P$ is determined by where it maps these two elements.

Neumann [4] has characterized the regular wreath product groups (including infinite groups) for which the so-called base group is a characteristic subgroup. This general result of Neumann implies that $B$ is always a characteristic subgroup of $P$ for the particular class of wreath product groups $P$ considered in this paper. Nevertheless, in our proof of Theorem 1.1 we present our own brief argument (see Step 7) that $B$ is a characteristic subgroup of $P$. From this fact it follows that $[B, P]$ is a characteristic subgroup of $P$.

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

**Theorem A.** *Assume Hypothesis 1.3. Then the group* $B/[B,P]$ *is cyclic of order* $p^e$, *and therefore has a unique maximal subgroup which one denotes as* $D/[B,P]$, *and so* $D$ *is a characteristic subgroup of* $P$ *that satisfies* $|B : D| = p$. *Let* $\mathcal{E}$ *denote the set of all elements* $g \in P$ *of order* $p^n$ *that satisfy the condition* $P = \langle B, g \rangle$. *Then for each pair of elements* $(a, b)$ *such that* $a \in B - D$ *and* $b \in \mathcal{E}$, *there exists an automorphism of* $P$ *that maps* $x_{p^n-1}$ *to* $a$ *and maps* w *to* $b$. *Furthermore, every automorphism of* $P$ *is of this type.*

In the notation of Theorem A, the information that we have about the subgroup $D$ and the set $\mathcal{E}$ makes it clear that every automorphism of $P$ maps the set $B - D$ to itself and maps the set $\mathcal{E}$ to itself. It is not difficult to see that the element $\mathrm{x}_{p^n-1}$ belongs to the set $B - D$ and that the element w belongs to the set $\mathcal{E}$. From this perspective, we might summarize Theorem A as stating that every mapping that could possibly be an automorphism of $P$ actually is an automorphism of $P$.

Theorem A gives us a factorization of $A = \mathrm{Aut}(P)$, namely, $A = \mathbf{C}_A(\mathrm{w})\mathbf{C}_A(x')$ with $\mathbf{C}_A(\mathrm{w}) \cap \mathbf{C}_A(x') = 1$, where $x' = \mathrm{x}_{p^n-1}$. Houghton's main result in [1] is a factorization of $A$, namely, $A = \mathbf{C}_A(\mathrm{w})I \rtimes Q^*$ with $\mathbf{C}_A(\mathrm{w}) \cap I = 1$, where $I$ denotes the group of inner automorphisms of $P$ induced by elements of $B$, and where $Q^*$ is the image of the usual embedding of $\mathrm{Aut}(Q)$ in $A$ (see [2]). In particular $Q^* \cong \mathrm{Aut}(Q)$. Since $I \subseteq \mathbf{C}_A(x')$, these two factorizations are the same if and only if $Q^* \subseteq \mathbf{C}_A(x')$. However, $Q^*$ permutes the elements

$x_0, x_1, \ldots, x_{p^n-1}$ with $x' = x_{p^n-1}$ lying in a regular orbit, and so $Q^* \cap \mathbf{C}_A(x') = 1$. Hence these two factorizations are the same if and only if $Q^* = 1$, which happens only when $|Q| = 2$.

We now discuss an application of Theorem A. In [5] we classify up to isomorphism the nonabelian subgroups of the wreath product group $P = \mathbb{Z}_{p^e} \wr \mathbb{Z}_p$ for an arbitrary prime $p$ and positive integer $e$ such that $p^e \geq 3$. In [6] we use the characterization of the elements of $A = \mathrm{Aut}(P)$ that is provided by Theorem A to compute the index $|\mathbf{N}_A(H) : \mathbf{C}_A(H)|$ for each group $H$ of class 3 or larger appearing in this classification. For each such group $H$, we then observe that this index is equal to the order of the automorphism group $\mathrm{Aut}(H)$, from which we deduce that the group $\mathbf{N}_A(H)/\mathbf{C}_A(H)$ is isomorphic to $\mathrm{Aut}(H)$, which says that the full automorphism group $\mathrm{Aut}(H)$ is realized inside the group $A = \mathrm{Aut}(P)$.

In Section 3 we prove Theorems 1.1 and 1.2. In Section 4 we prove Theorem A. In Section 2 we discuss some preliminary results used in our proof of Theorem 1.1.

Let $\mathrm{Irr}(G)$ denote the set of irreducible ordinary characters of a finite group $G$.

## 2. Preliminaries

For each finite group $G$ and prime-power $q$, let $\mathrm{mindeg}(G, q)$ denote the smallest positive integer $m$ such that the general linear group $\mathrm{GL}(m, q)$ contains a subgroup that is isomorphic to $G$. Thus $\mathrm{mindeg}(G, q)$ is the minimal degree among all the faithful $F$-representations of the group $G$, where $F$ denotes the field with $q$ elements. For any groups $H$ and $G$ such that $H \subseteq G$, we have $\mathrm{mindeg}(H, q) \leq \mathrm{mindeg}(G, q)$.

*Definition 2.1.* Let $G$ be a monolithic finite group, let $q$ be a prime-power that is relatively prime to the order of $G$, and let $m = \mathrm{mindeg}(G, q)$. We say that the ordered triple $(G, q, m)$ is a *monolithic triple* in case every faithful irreducible ordinary character of $G$ has degree at least $m$. Assuming that $(G, q, m)$ is a monolithic triple, we define $\mathfrak{F}(G, q)$ to be the set of all faithful irreducible ordinary characters of $G$ of degree $m$. We say that the monolithic triple $(G, q, m)$ is *good* provided that every value of each character belonging to the set $\mathfrak{F}(G, q)$ is a $\mathbb{Z}$-linear combination of complex $(q-1)$st roots of unity.

The following is a special case of result that was proved in [3]. We call this result the Automorphism Counting Formula. It is the key to establishing Theorem 1.1.

**Theorem 2.2.** *Let $(G, q, m)$ be a good monolithic triple. Suppose that $\Gamma = \mathrm{GL}(m, q)$ has a unique conjugacy class of subgroups whose members are isomorphic to $G$. Let $H$ be any subgroup of $\Gamma$ that is isomorphic to $G$. Then $|\mathrm{Aut}(G)|(q-1) = |\mathfrak{F}(G, q)| \cdot |\mathbf{N}_\Gamma(H)|$.*

In our proof of Theorem 1.1, the idea is to define a good monolithic triple $(G, q, m)$ with $G = P$ that satisfies the hypothesis of Theorem 2.2. The conclusion of Theorem 2.2 would then yield $|\mathrm{Aut}(G)|$ provided that we know in advance $|\mathfrak{F}(G, q)|$ and $|\mathbf{N}_\Gamma(H)|$.

Given a monolithic group $G$, in order to define a good monolithic triple $(G, q, m)$ we must choose an appropriate prime-power $q$ and then calculate $\mathrm{mindeg}(G, q)$. The following result may be used to calculate $\mathrm{mindeg}(G, q)$ for certain groups $G$ and prime-powers $q$.

**Lemma 2.3.** *Let $G$ be any finite group containing an abelian $p$-subgroup $B$ of exponent $p^e$ and of rank $r$, where $p$ is a prime. Let $F$ be any field containing a primitive $p^e$th root of unity. If there exists a faithful $F$-representation of $G$ of degree $r$, then* $\mathrm{mindeg}(G, F) = r$.

*Proof.* The hypotheses yield $\text{mindeg}(B,F) \leq \text{mindeg}(G,F) \leq r$. It remains to show that $r \leq \text{mindeg}(B,F)$. The hypothesis on $F$ implies that every irreducible $F$-representation of $B$ has degree 1 and that the characteristic of the field $F$ is not $p$. Let $\mathcal{X}$ be any faithful $F$-representation of $B$, and let $n$ be its degree. By Maschke's theorem, $\mathcal{X}$ is similar to a faithful $F$-representation $\mathcal{Y}$ consisting of diagonal matrices. Let $E$ be the subgroup of $\text{GL}(n,F)$ consisting of all diagonal matrices of order dividing $p^e$. Then $\mathcal{Y}(B) \subseteq E$ while $E$ is homocyclic of exponent $p^e$ and of rank $n$. Since $\mathcal{Y}$ is faithful, indeed $\mathcal{Y}(B)$ is an abelian $p$-group of rank $r$. It follows that $r \leq n$. Therefore $\text{mindeg}(B,F) \geq r$, as desired. □

One of the hypotheses of Theorem 2.2 is that the general linear group $\text{GL}(m,q)$ has a unique conjugacy class of subgroups whose members are isomorphic to $G$. The following result (Lemma 4.5 in [3]) is useful for establishing this condition in certain situations.

**Lemma 2.4.** *Let $F$ be a field containing a primitive $p^e$th root of unity, where $p$ is some prime and $e$ is some positive integer. Let $G$ be any finite group containing an abelian normal $p$-subgroup $B$ of exponent $p^e$ and of rank $r$. Then every faithful $F$-representation of $G$ of degree $r$ is similar to a representation $\mathcal{Y}$ such that $\mathcal{Y}(B)$ consists of diagonal matrices and $\mathcal{Y}(G)$ consists of monomial matrices.*

Using Theorem 2.2 to calculate the order of the automorphism group $\text{Aut}(G)$ for a given monolithic triple $(G,q,m)$ requires that we know in advance the cardinality of the set $\mathcal{F}(G,q)$ that was defined in Definition 2.1. The following result is helpful for calculating the cardinality of the set $\mathcal{F}(G,q)$ in certain situations.

**Lemma 2.5.** *Let $p$ be a prime and let $P$ be a monolithic finite $p$-group. One defines the set $\mathcal{A} = \{\psi \in \text{Irr}(P) \mid \psi \text{ is faithful}\}$. Let $n$ be a nonnegative integer and suppose that every character belonging to the set $\mathcal{A}$ has degree $p^n$. Then $|\mathcal{A}| = |P|(p-1)/p^{2n+1}$.*

*Proof.* We define the set $\mathcal{B} = \text{Irr}(P) - \mathcal{A}$. Let $N$ be the unique minimal normal subgroup of $P$, and note that $\mathcal{B} = \{\psi \in \text{Irr}(P) \mid N \subseteq \ker\psi\}$. Hence the set $\mathcal{B}$ may be identified with the set $\text{Irr}(P/N)$. We have $|N| = p$, and so $|P/N| = |P|/p$. By Corollary 2.7 in [7], along with the fact that $\text{Irr}(P) = \mathcal{A} \cup \mathcal{B}$ is a disjoint union, we deduce that

$$|P| = \sum_{\psi\in\mathcal{A}} \psi(1)^2 + \sum_{\psi\in\mathcal{B}} \psi(1)^2 = |\mathcal{A}|p^{2n} + \frac{|P|}{p}. \tag{2.1}$$

Solving this equation for $|\mathcal{A}|$, we obtain the desired conclusion. □

Using Theorem 2.2 to calculate the order of the automorphism group $\text{Aut}(G)$ for a given monolithic triple $(G,q,m)$ requires that we know in advance the order of the normalizer of a certain subgroup $H$ in the general linear group $\text{GL}(m,q)$. The following result (which is part of Theorem 4.4 in [3]) is useful for this task in certain situations.

**Theorem 2.6.** *Let $\Gamma = \text{GL}(m,q)$ where $q > 1$ is any prime-power and $m$ is any positive integer. Let $F$ be the field with $q$ elements, let $F_0$ be any nontrivial subgroup of the multiplicative group $F^\times = F - \{0\}$, and let $E$ be the group of all diagonal matrices in $\Gamma$ having the property that each entry along the diagonal belongs to $F_0$. Let $S$ be the subgroup of $\Gamma$ consisting of all permutation matrices, and note that $S \cong \text{Sym}(m)$. Let $T$ be any transitive subgroup of the symmetric group $S$ and let $H = E \rtimes T$. If $E$ is a characteristic subgroup of $H$, then $|\mathbf{N}_\Gamma(H)| = |\mathbf{N}_S(T) : T| \cdot |H|(q-1)/|F_0|$.*

The following rather specialized result will be used in our proof of Theorem 1.1.

**Lemma 2.7.** *Let $p$ be any prime and let $e$, $n$, and $j$ be positive integers such that $j \leq n$. Then the condition $ep^{n-j}(p^j - 1) \leq j$ holds if and only if $p = 2$ and $e = n = j = 1$.*

*Proof.* First, an easy inductive argument shows that $2^j - 1 > j$ whenever $j \geq 2$. Now suppose that $ep^{n-j}(p^j - 1) \leq j$ holds. First we show that $j = 1$. Assuming instead that $j \geq 2$, we get $p^j - 1 \geq 2^j - 1 > j$, forcing $ep^{n-j}(p^j - 1) > j$, a contradiction. Hence $j = 1$, and so $ep^{n-1}(p^1 - 1) \leq 1$, which forces each of the positive integers $e$, $p^{n-1}$, and $p - 1$ to be 1. Therefore $e = n = 1$ and $p = 2$, as desired. The reverse implication is trivial. □

The next two results on permutation groups will be used later in this article.

**Lemma 2.8.** *Let $H_1$ and $H_2$ be isomorphic transitive subgroups of order $n$ of the symmetric group* $\mathrm{Sym}(n)$. *Then $H_1$ and $H_2$ are conjugate subgroups of* $\mathrm{Sym}(n)$.

*Proof.* For each $\alpha \in \Omega = \{1, \ldots, n\}$ and each $x \in \mathrm{Sym}(n)$, let $\alpha \cdot x$ denote the image of $\alpha$ under $x$. For $i \in \{1, 2\}$, the maps $f_i : H_i \to \Omega$ defined by $f_i(x) = 1 \cdot x$ are bijections. Let $\theta : H_1 \to H_2$ be an isomorphism. The composition $y = f_2 \theta f_1^{-1} : \Omega \to \Omega$ is an element of $\mathrm{Sym}(n)$. It suffices to show that $y^{-1}xy = \theta(x)$ for each $x \in H_1$. A straightforward calculation (left to the reader) yields $\alpha \cdot y^{-1}xy = \alpha \cdot \theta(x)$ for arbitrary $\alpha \in \Omega$. □

**Theorem 2.9.** *Let $H$ be any transitive subgroup of order $n$ in the symmetric group $S = \mathrm{Sym}(n)$. Then the normalizier $\mathbf{N}_S(H)$ is isomorphic to the holomorph $H \rtimes \mathrm{Aut}(H)$.*

The following basic lemma is needed for our proof of Theorem 2.9.

**Lemma 2.10.** *Let $G$ be a group of permutations of a set $\Omega$, let $H$ be a transitive subgroup of $G$, and let $C = \mathbf{C}_G(H)$. For each $\alpha \in \Omega$, the stabilizer subgroup $C_\alpha$ is trivial.*

*Proof.* Let $x \in C_\alpha$. To prove that $x = 1$, it suffices to show that $\beta \cdot x = \beta$ for arbitrary $\beta \in \Omega$, since $G$ acts faithfully. There exists $h \in H$ such that $\alpha \cdot h = \beta$. Since $x \in C$, we have $hx = xh$, and so $\beta \cdot x = (\alpha \cdot h) \cdot x = \alpha \cdot (hx) = \alpha \cdot (xh) = (\alpha \cdot x) \cdot h = \alpha \cdot h = \beta$. □

*Proof of Theorem 2.9.* Let $G$ be a group that is isomorphic to $H$. Let $V = G \rtimes A$ where $A = \mathrm{Aut}(G)$. First we identify a subgroup $D$ of $V$ that is isomorphic to $G$ and that centralizes $G$. The rule $x \mapsto \varphi_x x^{-1}$ defines an injective homomorphism $\theta : G \to V$, where $\varphi_x \in A$ is the inner automorphism induced by $x$. Let $D = \theta(G)$. For $x, y \in G$, observe that

$$\theta(x)^{-1} y \theta(x) = \left(x\varphi_x^{-1}\right) y \left(\varphi_x x^{-1}\right) = x\left(\varphi_x^{-1} y \varphi_x\right) x^{-1} = x\left(x^{-1} y x\right) x^{-1} = y. \tag{2.2}$$

Next we embed $V$ as a subgroup of $S$ in such a way that $G$ becomes a transitive (in fact regular) subgroup of $S$. Since $\mathrm{core}_V(A) = 1$, the action of $V$ on the set $\Omega$ consisting of the right cosets of $A$ in $V$ is faithful. We now argue that the action of $G$ on $\Omega$ is regular. Since $|G| = |\Omega|$, it suffices to show that each nonidentity element of $G$ fixes no element of $\Omega$. Let $x \in G$ and $Av \in \Omega$ such that $x$ fixes $Av$. Thus $Avx = Av$ and so $vxv^{-1} \in A$. Since $x \in G \lhd V$, we obtain $vxv^{-1} \in A \cap G = 1$, and so $x = 1$, as desired. Now label the members of $\Omega$ as the numbers $1, 2, \ldots, n$. In this way we regard $V$ as a subgroup of $S$.

Since $H$ and $G$ are isomorphic transitive subgroups of order $n$ in $S$, by Lemma 2.8 we may complete the proof by showing that $\mathbf{N}_S(G) = V$. Write $C = \mathbf{C}_S(G)$. Lemma 2.10 implies that every orbit in the action of $C$ on $\{1, \ldots, n\}$ has size $|C|$. Hence $|C|$ divides $n = |G| = |D|$. But since $D$ centralizes $G$, we have $D \subseteq C$. It follows that $D = C$.

Write $N = \mathbf{N}_S(G)$. By the $N$-Mod-$C$ Theorem, the integer $|N|/|C|$ divides $|A|$, which says that $|N|$ divides $|C| \cdot |A|$. Recalling that $|C| = |D| = |G|$, this says that $|N|$ divides $|G| \cdot |A| = |V|$. But since $G \lhd V \subseteq S$, we have $V \subseteq N$. It follows that $V = N$. □

## 3. Proof of Theorem 1.1

Let $\{x_u \mid u \in Q\}$ be a collection of elements of order $p^e$ that constitutes a generating set for the homocyclic group $B$ of exponent $p^e$ and of rank $|Q| = p^n$. We now define an action of the group $Q$ on the set $\{x_u \mid u \in Q\}$. For each pair $u, v \in Q$, we let $x_u^v = x_{uv}$, where the product $uv$ is computed in $Q$. This action naturally gives rise to an action of $Q$ via automorphisms on the group $B$. Let $P = B \rtimes Q$ denote the semidirect product group corresponding to this action. Let $\mathcal{F}$ denote the set consisting of all functions from $Q$ into the additive group $\mathbb{Z}_{p^e}$. For each function $f \in \mathcal{F}$, we define the element

$$x(f) = \prod_{u \in Q} x_u^{f(u)} \in B. \tag{3.1}$$

Each element of $B$ has the form $x(f)$ for some unique function $f \in \mathcal{F}$. We define the element $z \in B$ of order $p^e$ by letting $z$ denote the product of all the elements $x_u$ for $u \in Q$.

*Step 1.* For each subgroup $L$ of $Q$, the centralizer $\mathbf{C}_B(L)$ is equal to the set of all elements $x(f)$ such that the function $f \in \mathcal{F}$ is constant on each of the left cosets of $L$ in $Q$.

*Proof.* Let $T$ be a transversal for the left cosets of $L$ in $Q$. For each $t \in T$, observe that the set $\{x_u \mid u \in tL\}$ is an orbit in the action of $L$ on the set of generators $\{x_u \mid u \in Q\}$ for $B$. □

*Step 2.* The group $P$ is monolithic, and its center is the cyclic group $\langle z \rangle$ of order $p^e$.

*Proof.* Since $B$ is abelian and the action of $Q$ via automorphisms on $B$ is faithful, the center of $P = B \rtimes Q$ is $\mathbf{C}_B(Q)$. By Step 1, $\mathbf{C}_B(Q)$ is the cyclic group generated by the element $z$. Finally, since $P$ is a $p$-group whose center is cyclic, $P$ is indeed monolithic. □

Following standard notation (see [7]), we define the *inertia subgroup* of any character $\theta \in \mathrm{Irr}(B)$ as the subgroup $\mathbf{I}_P(\theta) = \{x \in P \mid \theta^x = \theta\}$.

*Step 3.* For each character $\theta \in \mathrm{Irr}(B)$ such that $\mathbf{I}_P(\theta) > B$, every irreducible constituent of the induced character $\theta^P$ is not faithful.

*Proof.* For each pair of functions $f, g \in \mathcal{F}$ we define the dot product $f \cdot g$ to be the value

$$f \cdot g = \sum_{u \in Q} f(u) g(u) \in \mathbb{Z}_{p^e}. \tag{3.2}$$

Let $\epsilon$ be any primitive complex $p^e$th root of unity. For each function $g \in \mathcal{F}$, we define the character $\varphi_g \in \mathrm{Irr}(B)$ by $\varphi_g(\mathrm{x}(f)) = \epsilon^{f\cdot g}$ for every function $f \in \mathcal{F}$. It is clear that every irreducible ordinary character of $B$ is of the form $\varphi_g$ for some function $g \in \mathcal{F}$.

Let $\theta \in \mathrm{Irr}(B)$ such that $\mathbf{I}_P(\theta) > B$. Since $\ker \theta^P$ is equal to the intersection of the kernels of the irreducible constituents of $\theta^P$, it suffices to show that $\ker \theta^P > 1$. Because $P = B \rtimes Q$, we have $\mathbf{I}_P(\theta) = B \rtimes L$ for some nontrivial subgroup $L$ of $Q$. Let $T$ be any transversal for the left cosets of $L$ in $Q$. Since $1 < L \subseteq Q$, the prime $p$ divides $|L|$. Since $\theta \in \mathrm{Irr}(B)$, we have $\theta = \varphi_g$ for some function $g \in \mathcal{F}$. Because the character $\theta$ is $L$-invariant, the function $g$ must be constant on each left coset of $L$ in $Q$. This says that for each $t \in T$, there exists a value $c_t \in \mathbb{Z}_{p^e}$ such that $g(u) = c_t$ for each element $u \in tL$.

By Step 2, $\langle z^{p^{e-1}} \rangle$ is the unique minimal normal subgroup of $P$. Note that $z^{p^{e-1}} = \mathrm{x}(f)$ for the constant function $f \in \mathcal{F}$ defined as $f(u) = p^{e-1}$ for $u \in Q$. Observe that

$$\theta\left(z^{p^{e-1}}\right) = \epsilon^{f\cdot g} \quad \text{where } f \cdot g = \sum_{u\in Q} f(u)g(u) = \sum_{t\in T}\sum_{u\in tL} f(u)g(u). \tag{3.3}$$

For each $t \in T$, using the fact that $|tL| = |L|$ is divisible by $p$, we deduce that

$$\sum_{u\in tL} f(u)g(u) = \sum_{u\in tL} p^{e-1}c_t = |L|p^{e-1}c_t = 0. \tag{3.4}$$

It follows that $f \cdot g = 0$, which yields $z^{p^{e-1}} = \mathrm{x}(f) \in \ker\theta$. Hence $\langle z^{p^{e-1}} \rangle \subseteq \ker\theta$. Using $\ker\theta^P = \mathrm{core}_P(\ker\theta)$ and $1 < \langle z^{p^{e-1}} \rangle \lhd P$, we obtain $1 < \langle z^{p^{e-1}} \rangle \subseteq \ker\theta^P$, as desired. □

We define the set $\mathcal{A} = \{\psi \in \mathrm{Irr}(P) \mid \psi \text{ is faithful}\}$.

*Step 4.* For each character $\chi \in \mathcal{A}$ we have $\chi(1) = p^n$, and for each element $x \in P$ the value $\chi(x)$ is a sum of complex $p^e$th roots of unity. Furthermore $|\mathcal{A}| = (p-1)|P|/p^{2n+1}$.

*Proof.* Let $\chi \in \mathcal{A}$ be arbitrary and let $\theta \in \mathrm{Irr}(B)$ be any irreducible constituent of the restriction $\chi_B$. Hence $\chi$ is an irreducible constituent of the induced character $\theta^P$. Since $B \subseteq \mathbf{I}_P(\theta)$ and since $\chi$ is faithful, Step 3 yields $\mathbf{I}_P(\theta) = B$. By the Clifford Correspondence [7, Theorem 6.11], it follows that $\theta^P$ is irreducible, and so $\chi = \theta^P$. Since $\theta \in \mathrm{Irr}(B)$ while $B$ is abelian, we have $\theta(1) = 1$. Therefore $\chi(1) = \theta^P(1) = |P : B|\theta(1) = |Q| = p^n$.

Since $\chi = \theta^P$ with $\theta \in \mathrm{Irr}(B)$ and $B \lhd P$, the character $\chi$ vanishes off $B$. Furthermore, because $B$ is an abelian $p$-group of exponent $p^e$, every value of $\theta$ is a complex $p^e$th root of unity. By Theorem 6.2 in [7], the restriction $\chi_B$ is a sum of conjugates of $\theta$ in $P$. Hence for each element $x \in B$, the value $\chi(x)$ is a sum of complex $p^e$th roots of unity.

Finally, Lemma 2.5 yields $|\mathcal{A}| = |P|(p-1)/p^{2n+1}$, as desired. □

Let $q > 1$ be any prime-power such that $p^e$ is the full $p$-part of $q - 1$. Let $\Gamma = \mathrm{GL}(p^n, F)$ where $F$ is the field with $q$ elements. Let $D$, $S$, and $M$ denote the subgroups of $\Gamma$ consisting of all diagonal matrices, permutation matrices, and monomial matrices, respectively. Note that $M = D \rtimes S$ and that $S$ is isomorphic to the symmetric group of degree $p^n$. Let $E$ denote the subgroup of $\Gamma$ consisting of all diagonal matrices of order dividing $p^e$. Thus $E$ is homocyclic of exponent $p^e$ and of rank $p^n$. Note that $E$ is the unique Sylow $p$-subgroup of the abelian group $D$, and that $E$ is a separator subgroup of $\Gamma$.

We will now define a faithful representation $\mathfrak{Z} : P \to \Gamma$. Recall that $\{x_u \mid u \in Q\}$ is a collection of elements of order $p^e$ that constitutes a generating set for the homocyclic group $B$ of exponent $p^e$ and of rank $|Q| = p^n$. We index the rows and the columns of the matrices in $\Gamma$ by the elements of the group $Q$. We choose an arbitrary element $\omega$ of order $p^e$ in the cyclic multiplicative group of nonzero elements in the field $F$. For each $u \in Q$, we define $\mathfrak{Z}(x_u)$ to be the diagonal matrix in $\Gamma$ whose $(u,u)$-entry is $\omega$, and each of whose other diagonal entries is 1. Thus $\mathfrak{Z}(B) = E$ consists of diagonal matrices. We define $\mathfrak{Z}|_Q : Q \to \Gamma$ to be the right regular representation of the group $Q$. Thus $\mathfrak{Z}(Q)$ consists of permutation matrices and is a regular subgroup of the symmetric group $S$. The action of $Q$ by conjugation on $B$ inside the group $P$ is similar to the action of $\mathfrak{Z}(Q)$ by conjugation on $\mathfrak{Z}(B)$ inside the group $\Gamma$. Thus, since $P = QB$ and $B \cap Q = 1$, we have a faithful representation $\mathfrak{Z} : P \to \Gamma$ whose image $\mathfrak{Z}(P) = \mathfrak{Z}(Q)\mathfrak{Z}(B)$ is a subgroup of $SE$.

*Step 5.* $\operatorname{mindeg}(P,F) = p^n$.

*Proof.* Recall that $\mathfrak{Z}$ is a faithful $F$-representation of $P$ of degree $p^n$; use Lemma 2.3. □

The next step establishes Theorem 1.2.

*Step 6.* Every faithful $F$-representation of $P$ of degree $p^n$ is similar to $\mathfrak{Z}$.

*Proof.* By Lemma 2.4, every faithful $F$-representation of $P$ of degree $p^n$ is similar to a faithful $F$-representation $\mathfrak{X}$ such that $\mathfrak{X}(B) \subseteq D$ and $\mathfrak{X}(P) \subseteq M$. Since $E$ is the unique Sylow $p$-subgroup of $D$, indeed $\mathfrak{X}(B) \subseteq E$. Since $\mathfrak{X}$ is faithful, the $p$-groups $\mathfrak{X}(B)$ and $E$ are homocyclic of exponent $p^e$ and of rank $p^n$. It follows that $\mathfrak{X}(B) = E$. That $E$ is the unique Sylow $p$-subgroup of $D$ yields $E \lhd \mathbf{N}_\Gamma(D)$. Satz II.7.2(a) in [8] yields $\mathbf{N}_\Gamma(D) = M$, so $E \lhd M = DS$. Let $R$ be a Sylow $p$-subgroup of $S$. Thus $ER$ is a Sylow $p$-subgroup of $M$. Since $\mathfrak{X}(P)$ is a $p$-subgroup of $M$, Sylow's theorem asserts that $\mathfrak{X}$ is similar (by a matrix in $M$) to a representation $\mathfrak{Y}$ such that $\mathfrak{Y}(P) \subseteq ER$. We have $\mathfrak{Y}(B) = E$, since $E \lhd M$. Thus $\mathfrak{Y}(P)/E$ and $\mathfrak{Z}(P)/E$ are regular subgroups of the symmetric group $ES/E \cong \operatorname{Sym}(p^n)$, and are both isomorphic to $Q$. By Lemma 2.8, conjugation by some element of $ES/E$ maps $\mathfrak{Y}(P)/E$ to $\mathfrak{Z}(P)/E$. Conjugation by the unique preimage of this element under the natural isomorphism $S \to ES/E$ maps $\mathfrak{Y}(P)$ to $\mathfrak{Z}(P)$. Hence $\mathfrak{Y}$ is similar to $\mathfrak{Z}$. □

*Step 7.* $B$ is a characteristic subgroup of $P$.

*Proof.* We argue that $B$ is the only abelian normal subgroup of index $p^n$ in $P$. Let $A$ be an abelian normal subgroup of $P$ such that $|P : A| = p^n$ and $A \neq B$. Write $|AB : B| = p^j$ with $j \in \{1, \ldots, n\}$ and let $L = AB \cap Q$. We now argue that $AB = B \rtimes L$. Since $L \subseteq Q$ while $B \cap Q = 1$, we have $B \cap L = 1$. Because $B \subseteq AB$, Dedekind's lemma yields $BL = AB \cap BQ = AB \cap P = AB$, and so $AB = B \rtimes L$. From this we obtain $|L| = |AB : B| = p^j$. Since $A$ and $B$ are abelian, we have $A \cap B \subseteq \mathbf{Z}(AB)$. It follows that $A \cap B \subseteq \mathbf{C}_B(L) \subseteq B$ and $|B : \mathbf{C}_B(L)| \leq |B : A \cap B| = p^j$. By Step 1, we have $|\mathbf{C}_B(L)| = (p^e)^{|Q:L|} = p^{ep^{n-j}}$. Since $|B| = p^{ep^n}$, it follows that $|B : \mathbf{C}_B(L)| = p^{ep^{n-j}(p^j-1)}$. Thus $ep^{n-j}(p^j - 1) \leq j$. By Lemma 2.7, this contradicts the hypothesis $p^{en} \geq 3$. □

*Step 8.* The normalizer $\mathbf{N}_\Gamma(\mathfrak{Z}(P))$ has order $(q-1)|P| \cdot |\operatorname{Aut}(Q)|/p^e$.

*Proof.* Using $P = B \rtimes Q$ and $E = \mathfrak{Z}(B)$, we obtain $\mathfrak{Z}(P) = E \rtimes \mathfrak{Z}(Q)$. By Step 7 and the fact that $\mathfrak{Z}$ is faithful, $E = \mathfrak{Z}(B)$ is a characteristic subgroup of $\mathfrak{Z}(P)$. Since $\mathfrak{Z}(Q)$ is a regular subgroup of the symmetric group $S$ and since $\mathfrak{Z}(Q) \cong Q$, Theorem 2.9 implies that the normalizer

$\mathbf{N}_S(\mathfrak{X}(Q))$ is isomorphic to the holomorph of $Q$. Therefore $|\mathbf{N}_S(\mathfrak{X}(Q)) : \mathfrak{X}(Q)| = |\mathrm{Aut}(Q)|$. The statement now follows from Theorem 2.6. □

*Step 9.* $|\mathrm{Aut}(P)| = (p-1)|\mathrm{Aut}(Q)|p^{2ep^n-e-1}$.

*Proof.* By Steps 2, 4, and 5, $(P, q, p^n)$ is a good monolithic triple and $\mathfrak{F}(P,q) = \mathcal{A}$. Thus Step 4 yields $|\mathfrak{F}(P,q)| = (p-1)|P|/p^{2n+1}$. By Step 6, $\mathfrak{X}(P)$ belongs to the unique conjugacy class of subgroups of $\Gamma$ whose members are isomorphic to $P$. In view of Step 8, Theorem 2.2 yields $|\mathrm{Aut}(P)| = (p-1)|\mathrm{Aut}(Q)| \cdot |P|^2/p^{e+2n+1}$ where $|P| = p^{ep^n+n}$. □

## 4. Proof of Theorem A

Assume Hypothesis 1.3. Let $\mathfrak{F}$ denote the set of all functions from the set $\mathcal{U} = \{0, 1, \ldots, p^n - 1\}$ into the additive group $\mathbb{Z}_{p^e}$. For each function $f \in \mathfrak{F}$, we define the element

$$\mathrm{x}(f) = \mathrm{x}_0^{f(0)}\mathrm{x}_1^{f(1)} \cdots \mathrm{x}_{p^n-1}^{f(p^n-1)} \in B. \tag{4.1}$$

Each element of $B$ has the form $\mathrm{x}(f)$ for some unique $f \in \mathfrak{F}$. The mapping $\varphi : B \to \mathbb{Z}_{p^e}$ defined by $\varphi(\mathrm{x}(f)) = f(0) + f(1) + \cdots + f(p^n - 1)$ is a surjective homomorphism. Hence $B/\ker\varphi$ is cyclic of order $p^e$. To establish Theorem A, our first task is to prove that $B/[B,P]$ is cyclic of order $p^e$. For this it suffices to show that $[B,P] = \ker\varphi$.

**Lemma 4.1.** *For each function $f \in \mathfrak{F}$, the commutator element $[x(f), \mathrm{w}]$ has the form*

$$x_0^{f(1)-f(0)}x_1^{f(2)-f(1)} \cdots x_{p^n-2}^{f(p^n-1)-f(p^n-2)}x_{p^n-1}^{f(0)-f(p^n-1)}. \tag{4.2}$$

*Proof.* Note that $[\mathrm{x}(f), \mathrm{w}] = \mathrm{x}(f)^{-1}\mathrm{x}(f)^{\mathrm{w}}$. Conjugating $\mathrm{x}(f)$ by w, we obtain

$$\begin{aligned}\mathrm{x}(f)^{\mathrm{w}} &= \left(\mathrm{x}_0^{\mathrm{w}}\right)^{f(0)}\left(\mathrm{x}_1^{\mathrm{w}}\right)^{f(1)}\left(\mathrm{x}_2^{\mathrm{w}}\right)^{f(2)} \cdots \left(\mathrm{x}_{p^n-1}^{\mathrm{w}}\right)^{f(p^n-1)} \\ &= \mathrm{x}_{p^n-1}^{f(0)}\mathrm{x}_0^{f(1)}\mathrm{x}_1^{f(2)} \cdots \mathrm{x}_{p^n-2}^{f(p^n-1)} = \mathrm{x}_0^{f(1)}\mathrm{x}_1^{f(2)} \cdots \mathrm{x}_{p^n-2}^{f(p^n-1)}\mathrm{x}_{p^n-1}^{f(0)}.\end{aligned} \tag{4.3}$$

Since $\mathrm{x}(f)^{-1} = \mathrm{x}_0^{-f(0)}\mathrm{x}_1^{-f(1)} \cdots \mathrm{x}_{p^n-2}^{-f(p^n-2)}\mathrm{x}_{p^n-1}^{-f(p^n-1)}$, the result follows. □

**Theorem 4.2.** $[B,P] = \ker\varphi$.

*Proof.* Let $[B, \mathrm{w}]$ denote the subgroup of $P$ that is generated by all elements of the form $[b, \mathrm{w}]$ with $b \in B$. Using $Q = \langle \mathrm{w} \rangle$, we can show that $[B, \mathrm{w}] = [B, Q]$. Since $P = BQ$ while $B$ is abelian, it is clear that $[B,Q] = [B,P]$. Hence it suffices to show that $[B, \mathrm{w}] = \ker\varphi$.

To show that $[B, \mathrm{w}] \subseteq \ker\varphi$, we must verify that $[\mathrm{x}(f), \mathrm{w}] \in \ker\varphi$ for each $f \in \mathfrak{F}$, but this is obvious by Lemma 4.1. Next we argue that $\ker\varphi \subseteq [B, \mathrm{w}]$. An arbitrary element of $\ker\varphi$ has the form $\mathrm{x}(g)$ for some function $g \in \mathfrak{F}$ satisfying $g(0)+g(1)+\cdots+g(p^n-1) = 0$. To establish that $\mathrm{x}(g) \in [B, \mathrm{w}]$, we will now define a particular function $f \in \mathfrak{F}$ such that $[\mathrm{x}(f), \mathrm{w}] = \mathrm{x}(g)$. Let $f(0) = 0$, and for each $u \in \{1, \ldots, p^n - 1\}$ let $f(u) = g(0) + g(1) + \cdots + g(u-1)$. It follows

that for each $u \in \{0, 1, \ldots, p^n - 2\}$ we have $f(u+1) - f(u) = g(u)$. Furthermore, using the condition $g(0) + g(1) + \cdots + g(p^n - 1) = 0$, we obtain

$$f(0) - f\left(p^n - 1\right) = 0 - \sum_{v=0}^{p^n-2} g(v) = g\left(p^n - 1\right). \tag{4.4}$$

By Lemma 4.1, we deduce that $[\mathrm{x}(f), \mathrm{w}] = \mathrm{x}(g)$. Therefore $\mathrm{x}(g) \in [B, \mathrm{w}]$, as desired. □

The cyclic group $\mathbb{Z}_{p^e}$ has a unique subgroup of index $p$, namely, $p\mathbb{Z}_{p^e} = \{pa \mid a \in \mathbb{Z}_{p^e}\}$. Let $D$ be the group consisting of all those elements $\mathrm{x}(f)$ in $B$ such that $\varphi(\mathrm{x}(f)) \in p\mathbb{Z}_{p^e}$. It is clear that $\ker\varphi \subseteq D \subseteq B$ and $|B : D| = p$.

**Corollary 4.3.** $\ker\varphi$ *and* $D$ *are characteristic subgroups of* $P$.

*Proof.* By Step 7 in the proof of Theorem 1.1, $B$ is a characteristic subgroup of $P$. It follows that $[B, P]$ is a characteristic subgroup of $P$. By Theorem 4.2, we deduce that $\ker\varphi$ is a characteristic subgroup of $P$. Since $B/\ker\varphi$ is cyclic, $D$ is the only subgroup of $P$ that satisfies the conditions $\ker\varphi \subseteq D \subseteq B$ and $|B : D| = p$. Because $B$ and $\ker\varphi$ are characteristic subgroups of $P$, it follows that $D$ is a characteristic subgroup of $P$. □

For the next result, we need a formula (due to Philip Hall) for raising the product of two group elements to an arbitrary positive integer power. For any positive integer $n$ and any elements $a$ and $b$ belonging to some group, the element $(ab)^n$ may be written as

$$a^n\left(a^{-(n-1)}ba^{(n-1)}\right)\left(a^{-(n-2)}ba^{(n-2)}\right)\cdots\left(a^{-2}ba^2\right)\left(a^{-1}ba^1\right)b. \tag{4.5}$$

This says that $(ab)^n = a^n b^{a^{n-1}} b^{a^{n-2}} \cdots b^{a^2} b^{a^1} b$. Furthermore, in case all the conjugates of $b$ by powers of $a$ commute with each other (which is automatically true if $b$ is contained in an abelian normal subgroup of any group containing $a$ and $b$), this formula becomes

$$(ab)^n = a^n b b^{a^1} b^{a^2} \cdots b^{a^{n-2}} b^{a^{n-1}} = a^n \prod_{j=0}^{n} b^{a^j}. \tag{4.6}$$

**Lemma 4.4.** *The set* $\mathcal{E}$ *has cardinality* $(p-1)p^{ep^n-e+n-1}$.

*Proof.* Each element $g$ of the group $P = B \rtimes Q$ has the form $g = \mathrm{w}^m\mathrm{x}(f)$ for a unique integer $m \in \{0, 1, \ldots, p^n - 1\}$ and a unique function $f \in \mathcal{F}$. We will argue that $g \in \mathcal{E}$ if and only if $\mathrm{x}(f) \in \ker\varphi$ while $p$ does not divide $m$. From this it will follow that, to construct an element $g \in \mathcal{E}$, there are $(p-1)p^{n-1}$ choices for $m$ and $|\ker\varphi| = p^{ep^n-e}$ choices for $f$.

Because $P/B$ is cyclic of order $p^n$, the condition $\langle B, g\rangle = P$ holds if and only if the coset $gB = \mathrm{w}^m\mathrm{x}(f)B = \mathrm{w}^m B$ has order $p^n$ as an element of $P/B$. Since the subgroups $Q = \langle \mathrm{w}\rangle$ and $B$ intersect trivially, the coset $\mathrm{w}^m B$ has order $p^n$ if and only if the element $\mathrm{w}^m$ has order $p^n$. Recalling that the element w has order $p^n$, we see that the element $\mathrm{w}^m$ has order $p^n$ if and only if $p$ does not divide $m$. Therefore the condition $\langle B, g\rangle = P$ holds if and only if $p$ does not divide $m$.

Also because $P/B$ is cyclic of order $p^n$, the condition $\langle B, g\rangle = P$ implies that the order of the element $g$ is divisible by $p^n$. Henceforth we suppose that $p$ does not divide $m$. To complete the proof, it suffices to show that $g^{p^n} = 1$ if and only if $\mathrm{x}(f) \in \ker\varphi$.

Write $y = \mathrm{w}^m$. Thus $g = y\mathrm{x}(f)$. Using Philip Hall's formula for raising the product of two elements to a power, along with the fact that $y^{p^n} = 1$, we obtain

$$\begin{aligned} g^{p^n} &= \prod_{j=0}^{p^n-1} \mathrm{x}(f)^{y^j} = \prod_{j=0}^{p^n-1}\left[\prod_{u\in\mathcal{U}} \mathrm{x}_u^{f(u)}\right]^{y^j} \\ &= \prod_{j=0}^{p^n-1}\left[\prod_{u\in\mathcal{U}} \left(\mathrm{x}_u^{y^j}\right)^{f(u)}\right] \\ &= \prod_{u\in\mathcal{U}}\left[\prod_{j=0}^{p^n-1} \left(\mathrm{x}_u^{y^j}\right)\right]^{f(u)}. \end{aligned} \tag{4.7}$$

We define the element $z = \mathrm{x}_0\mathrm{x}_1\cdots\mathrm{x}_{p^n-1} \in B$ of order $p^e$. Conjugation by w cyclically permutes the elements $\mathrm{x}_0, \mathrm{x}_1, \ldots, \mathrm{x}_{p^n-1}$. Since $p$ does not divide $m$, conjugation by $y = \mathrm{w}^m$ cyclically permutes the elements $\mathrm{x}_0, \mathrm{x}_1, \ldots, \mathrm{x}_{p^n-1}$ in some order. It follows that

$$\prod_{j=0}^{p^n-1}\left(\mathrm{x}_u^{y^j}\right) = z. \tag{4.8}$$

From our work above, we deduce that

$$g^{p^n} = \prod_{u\in\mathcal{U}} z^{f(u)} = z^s, \quad \text{where } s = \sum_{u\in\mathcal{U}} f(u) = \varphi(\mathrm{x}(f)). \tag{4.9}$$

Recalling that the element $z$ has order $p^e$, we deduce that $g^{p^n} = 1$ if and only if $\mathrm{x}(f) \in \ker\varphi$. □

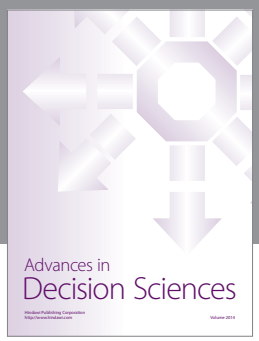
We will now complete the proof of Theorem A. Since $D \subseteq B$ while $D$ and $B$ are characteristic subgroups of $P$, every automorphism of $P$ maps the set $B - D$ to itself. Because $\mathrm{x}_{p^n-1} \in B$ and $\varphi(\mathrm{x}_{p^n-1}) = 1$, we have $\mathrm{x}_{p^n-1} \in B - D$. Since $B$ is a characteristic subgroup of $P$, every automorphism of $P$ maps the set $\mathcal{E}$ to itself. Note that $\mathrm{w} \in \mathcal{E}$. Thus for each automorphism $\sigma \in \mathrm{Aut}(P)$, we have $\mathrm{x}_{p^n-1}^{\sigma} \in B - D$ and $\mathrm{w}^{\sigma} \in \mathcal{E}$.

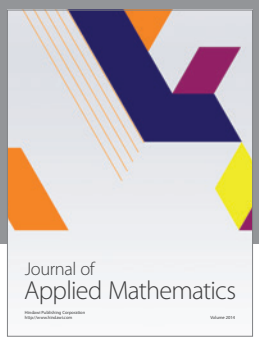
Let $\mathcal{S}$ be the set consisting of all ordered pairs $(a, b)$ such that $a \in B - D$ and $b \in \mathcal{E}$. We now define the mapping $\Psi : \mathrm{Aut}(P) \to \mathcal{S}$ as follows. For each automorphism $\sigma \in \mathrm{Aut}(P)$ we let $\Psi(\sigma) = (\mathrm{x}_{p^n-1}^{\sigma}, \mathrm{w}^{\sigma})$. By the last sentence of the preceding paragraph, the mapping $\Psi$ is well defined. Since $\{\mathrm{x}_{p^n-1}, \mathrm{w}\}$ is a generating set for the group $P$, every automorphism of $P$ is determined by where it maps the two elements $\mathrm{x}_{p^n-1}$ and w, and so the mapping $\Psi$ is injective. We now argue that $|\mathrm{Aut}(P)| = |\mathcal{S}|$, an equality that would force the mapping $\Psi$ to be a bijection, thereby completing the proof of Theorem A.

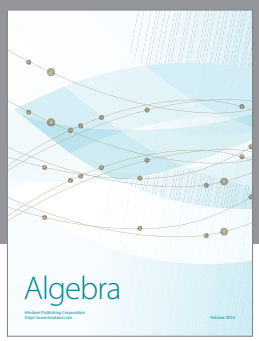
Using $|B : D| = p$ and $|B| = p^{ep^n}$, we obtain $|B - D| = (p-1)p^{ep^n-1}$. It is clear that $|\mathcal{S}| = |B - D| \cdot |\mathcal{E}|$, and so by Lemma 4.4 we deduce that $|\mathcal{S}| = (p-1)^2 p^{2ep^n+n-e-2}$. On the other hand, in the Introduction we calculated that $|\mathrm{Aut}(P)| = (p-1)^2 p^{2ep^n+n-e-2}$.

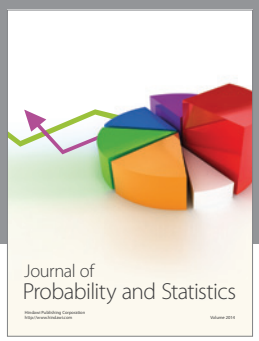
## References

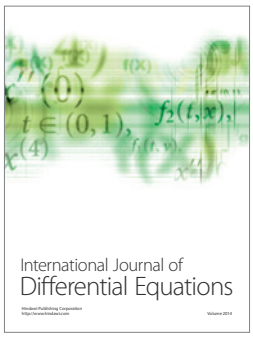
[1] C. H. Houghton, "On the automorphism groups of certain wreath products," *Publicationes Mathematicae Debrecen*, vol. 9, pp. 307–313, 1962.
[2] J. D. P. Meldrum, *Wreath Products of Groups and Semigroups*, vol. 74 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman, Harlow, UK, 1995.
[3] J. M. Riedl, "The number of automorphisms of a monolithic finite group," *Journal of Algebra*, vol. 322, pp. 4483–4497, 2009.
[4] P. M. Neumann, "On the structure of standard wreath products of groups," *Mathematische Zeitschrift*, vol. 84, pp. 343–373, 1964.
[5] J. M. Riedl, "Classification of the finite $p$-subgroups of GL($p$, $\mathbb{C}$) up to isomorphism," in preparation.
[6] J. M. Riedl, "Automorphism groups of subgroups of wreath product $p$-groups," in preparation.
[7] I. M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, NY, USA, 1994.
[8] B. Huppert, *Endliche Gruppen. I*, vol. 134 of *Die Grundlehren der Mathematischen Wissenschaften*, Springer, Berlin, Germany, 1967.

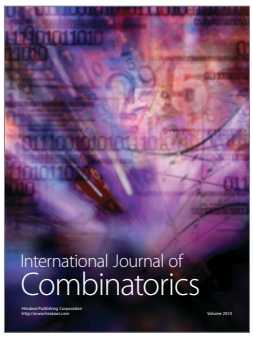


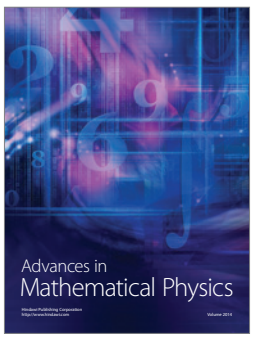


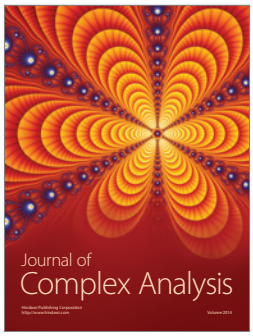


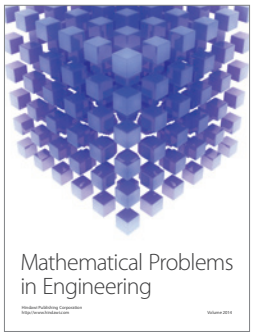


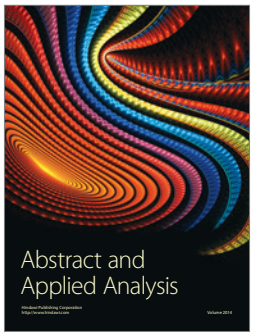


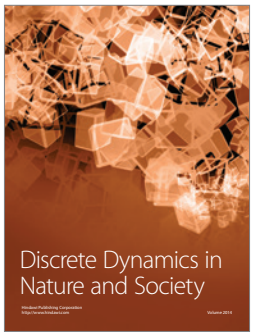


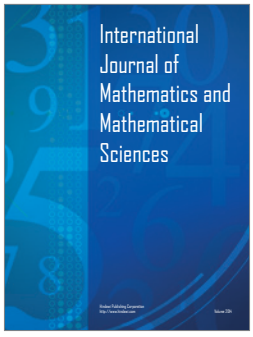


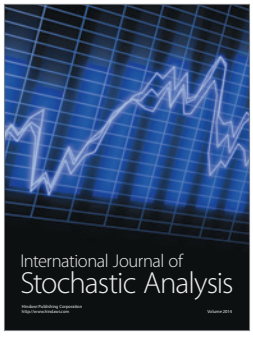












Hindawi
Submit your manuscripts at
http://www.hindawi.com