Bull. Aust. Math. Soc. **98** (2018), 434–438
doi:10.1017/S0004972718000576

MINIMAL EXCEPTIONAL *p*-GROUPS

ROBERT CHAMBERLAIN

(Received 18 May 2018; accepted 25 May 2018; first published online 1 August 2018)

Abstract

For a finite group G, denote by $\mu(G)$ the degree of a minimal permutation representation of G. We call G exceptional if there is a normal subgroup $N \trianglelefteq G$ with $\mu(G/N) > \mu(G)$. To complete the work of Easdown and Praeger ['On minimal faithful permutation representations of finite groups', *Bull. Aust. Math. Soc.* **38**(2) (1988), 207–220], for all primes $p \geq 3$, we describe an exceptional group of order p^5 and prove that no exceptional group of order p^4 exists.

2010 *Mathematics subject classification*: primary 20B05.

Keywords and phrases: permutation representation, finite p-group.

1. Introduction

For a finite group G, denote by $\mu(G)$ the degree of a minimal permutation representation of G. We call G exceptional if there is a normal subgroup $N \trianglelefteq G$ with $\mu(G/N) > \mu(G)$. In this case N and G/N are called a distinguished subgroup and a distinguished quotient of G, respectively.

Easdown and Praeger [1] prove that an exceptional 2-group of least order is of order 2^5 and give examples of exceptional groups of order 2^5. They note the existence of an exceptional group of order p^6 for any prime p and raise the question whether an exceptional group of order p^5 exists. In this note, for all primes $p \geq 3$, we describe an exceptional group of order p^5 and prove that no exceptional group of order p^4 exists.

2. There are no exceptional groups of order p^4

Easdown and Praeger [1] deal with the case $p = 2$. Fix a prime $p \geq 3$.

Easdown and Praeger note that distinguished quotients cannot be cyclic or elementary abelian. If G is a p-group of order at most p^3 then for any nontrivial $N \trianglelefteq G$ we have $|G/N| \leq p^2$, which implies that G/N is either cyclic or elementary abelian, so not distinguished. Therefore any exceptional p-group G has order at least p^4.

For the remainder of this section, assume that G is exceptional of order p^4 with N a distinguished subgroup of G. Similar to the argument above, if $|N| > p$ then G/N is either cyclic or elementary abelian and therefore not distinguished, so we must have $|N| = p$. Fix a minimal faithful permutation representation of G, $\rho : G \to \mathrm{Sym}(X)$, with orbits $X_1, \ldots, X_k$, so that $\mu(G) = \sum_{i=1}^{k} |X_i|$.

Lemma 2.1. *$|X_i| = p^2$ for each i.*

Proof. By [1, Lemma 1.2], N acts intransitively and nontrivially on each X_i. The orbit–stabiliser theorem tells us that $|X_i|$ divides $|G| = p^4$. If $|X_i| = p$ then the action of N on X_i would either be transitive or trivial, so $|X_i| \geq p^2$. Also, as N is distinguished, $|X_i| \leq \mu(G) < \mu(G/N)$. The action of G/N on itself by right multiplication gives $\mu(G/N) \leq |G/N|$, so $|X_i| < \mu(G/N) \leq |G/N| = p^3$. Hence $|X_i| = p^2$. □

Theorem 2.2. *There are no exceptional groups of order p^4.*

Proof. Since $|X_i| = p^2$ for each i, we must have $\mu(G) \geq p^2$. Using $|G/N| = p^3$, we consider the five possible isomorphism classes of G/N, which can be found, for example, in [2].

As noted by Easdown and Praeger, distinguished quotients cannot be cyclic or elementary abelian. This excludes $G/N \cong C_p \times C_p \times C_p$ and $G/N \cong C_{p^3}$.

If $G/N \cong C_{p^2} \rtimes C_p$ with generators x, y and $x^y = x^{1+p}$, then $\langle y \rangle$ is a core-free subgroup of G/N (for example, $y^{x^{-1}} = yx^y x^{-1} = yx^p$). Therefore G/N acts faithfully on the right cosets of $\langle y \rangle$, giving $\mu(G/N) \leq [G/N : \langle y \rangle] = p^2 \leq \mu(G)$, so N is not distinguished.

If $G/N \cong (C_p \times C_p) \rtimes C_p$ with generators x, y, z and $x^z = xy$, $y^z = y$, then $\langle x \rangle$ is a core-free subgroup of G/N. As in the last case, this implies that N is not distinguished.

So we are left with $G/N \cong C_{p^2} \times C_p$. The minimal degree for abelian groups is well known (see, for example, [1]). In this case $\mu(G/N) = p^2 + p$. Consider the preimage H of C_{p^2} in G. Since N is central and C_{p^2} is cyclic, H is abelian of order p^3 containing an element of order p^2. This means $H \cong C_{p^3}$ or $H \cong C_{p^2} \times C_p$. In either case $\mu(G) \geq \mu(H) \geq p^2 + p = \mu(G/N)$ so N is not distinguished. □

3. An exceptional group of order p^5

Fix a prime $p \geq 3$. For this section, let G be the group generated by g, h subject to the relations

$$g^{p^2} = h^{p^2} = [g, h]^p = 1,$$
$$[[g, h], g] = [[g, h], h] = g^p.$$

Also, let N be the subgroup generated by $g^p h^p$. We show that $|G| = p^5$, $N \leq Z(G)$, $\mu(G) \leq 2p^2$ and $\mu(G/N) = p^3$. Thus G is exceptional with distinguished subgroup N. For $p = 2$, two exceptional groups of order p^5 exist and are given in [1].

Proposition 3.1. *G can be identified with $(C_{p^2} \rtimes C_p) \rtimes C_{p^2}$ where the two copies of C_{p^2} are generated by g and h respectively, and C_p is generated by $[g, h]$. In particular, $|G| = p^5$.*

https://doi.org/10.1017/S0004972718000576 Published online by Cambridge University Press

Proof. Straightforward calculations give $g^{[g,h]} = g[g,[g,h]] = g[[g,h],g]^{-1}$, so the relations on G give $g^{[g,h]} = g^{1-p}$. Thus $[g,h]$ normalises $\langle g \rangle$. Moreover, $\langle [g,h] \rangle$ is simple and $[g,h]$ does not commute with g, so $\langle [g,h] \rangle \cap \langle g \rangle$ is trivial and $\langle g,[g,h] \rangle \cong C_{p^2} \rtimes C_p$.

A similar calculation gives $g^h = g[g,h]$ and $[g,h]^h = [g,h][[g,h],h] = [g,h]g^p$. To see that $\langle g,[g,h] \rangle \cap \langle h \rangle$ is trivial, notice that $G/\langle g,[g,h] \rangle$ has generator h and relations $h^{p^2} = 1$, so $h^p \notin \langle g,[g,h] \rangle$. Hence $G \cong (C_{p^2} \rtimes C_p) \rtimes C_{p^2}$. □

Proposition 3.2. $\langle g^p, h^p \rangle = Z(G)$. *In particular,* $N \leq Z(G)$.

Proof. We begin by showing that $g^p \in Z(G)$. Using the identification in Proposition 3.1, it is a standard result that $Z(C_{p^2} \rtimes C_p) = \langle g^p \rangle$. (To see this, one can check that $g^p \in Z(C_{p^2} \rtimes C_p)$, then note that $|Z(C_{p^2} \rtimes C_p)| = p$ otherwise $C_{p^2} \rtimes C_p$ would be abelian.) Now, $Z(C_{p^2} \rtimes C_p) = \langle g^p \rangle$ is characteristic in $C_{p^2} \rtimes C_p$, so fixed by h under conjugation. There are no automorphisms of $\langle g^p \rangle$ of order p, so h must commute with g^p. Therefore $g^p \in Z(G)$.

We show by induction on i that $g^{h^i} = g[g,h]^i g^{(1/2)i(i-1)p}$. Therefore $g^{h^p} = g$ and $h^p \in Z(G)$. Recall from the proof of Proposition 3.1 that $[g,h]^h = [g,h]g^p$. Then

$$\begin{aligned} g^{h^{i+1}} &= (g[g,h]^i g^{(1/2)i(i-1)p})^h \\ &= g^h([g,h]^i)^h g^{(1/2)i(i-1)p} \\ &= g[g,h]^{i+1} g^{ip} g^{(1/2)i(i-1)p} \\ &= g[g,h]^{i+1} g^{(1/2)i(i+1)p}. \end{aligned}$$

For $\langle g^p, h^p \rangle = Z(G)$, consider $G/\langle g^p, h^p \rangle$. It is easy to see that this is isomorphic to $(C_p \times C_p) \rtimes C_p$, where the generators of the C_p are the images of g, $[g,h]$ and h. Following a similar argument as for $C_{p^2} \rtimes C_p$, it follows that $Z(G/\langle g^p, h^p \rangle)$ is the cyclic group generated by the image of $[g,h]$. If $|Z(G)| > p^2$ then this implies $[g,h] \in Z(G)$, but this is not true (for example, $[[g,h],h] = g^p$). So $Z(G) = \langle g^p, h^p \rangle$. □

Proposition 3.3. $\mu(G) \leq 2p^2$.

Proof. To show this, we describe a faithful representation of G of degree $2p^2$.

Let $H_1 = \langle g,[g,h] \rangle$ and $H_2 = \langle gh^{-1},[g,h] \rangle$. Consider the natural action of G on the set of right cosets $G/H_1 \sqcup G/H_2$. This is faithful if and only if $\mathrm{core}_G(H_1 \cap H_2)$ is trivial.

Recall from the proof of Proposition 3.2 that $G/Z(G) = (C_p \times C_p) \rtimes C_p$. It is a standard result that this group has exponent p, so $(gh^{-1})^p \in Z(G)$. Following the identification in Proposition 3.1, $(gh^{-1})^p$ is nontrivial as its image in $G/(C_{p^2} \times C_p)$ is nontrivial, so gh^{-1} has order p^2.

From the above, it follows that $H_1 \cap H_2 = \langle [g,h] \rangle$ so $\mathrm{core}_G(H_1 \cap H_2)$ is trivial, and that $|H_1| = |H_2| = p^3$ so $|G/H_1 \sqcup G/H_2| = 2p^2$ as required. □

https://doi.org/10.1017/S0004972718000576 Published online by Cambridge University Press

Proposition 3.4. $\mu(G/N) = p^3$.

Proof. The quotient G/N can be described with generators $a = Ng, b = Nh$ and relations

$$a^{p^2} = b^{p^2} = a^p b^p = [a, b]^p = 1,$$
$$[[a, b], a] = [[a, b], b] = a^p.$$

Following an argument similar to the calculation of $Z(G)$ in the proof of Proposition 3.2, $Z(G/N) = \langle a^p \rangle$. Since any normal subgroup of a p-group intersects the centre nontrivially, this means any nontrivial normal subgroup of G/N contains $Z(G/N)$. Therefore any minimal representation of G/N is given by the coset action of G/N on some core-free subgroup of G/N of largest order.

Suppose that K is some such subgroup. Noting that $\langle [a, b] \rangle$ is core-free, we must have $|K| \geq p$. If K meets $\langle a \rangle$ or $\langle b \rangle$ nontrivially then it meets $Z(G/N)$ nontrivially.

Consider $K \cap \langle a, [a, b] \rangle$, this must be trivial or cyclic of order p. If it is trivial then K is isomorphic to its image in $(G/N)/\langle a, [a, b] \rangle$ which has order p, so $\mu(G) = [G : K] = p^3$. So suppose that $K \cap \langle a, [a, b] \rangle$ is generated by $a^i [a, b]^j$ for some i, j. If $p \nmid i$ then, using $a^{a^{-1}b} = a[a, b]$ and $[a, b]^{a^{-1}b} = [a, b]$, we can find an appropriate conjugate of K in G containing a^i, contradicting the fact that K is core-free. Therefore $K \cap \langle a, [a, b] \rangle = \langle a^{ip} [a, b] \rangle$ for some i. Since $[a, b]^b = [a, b] a^p$, we may consider instead $K^{b^{p-i}}$, so we may assume that $K \cap \langle a, [a, b] \rangle = \langle [a, b] \rangle$.

Now suppose that $K > \langle [a, b] \rangle$. If $|K| = p^3$ then K is maximal and therefore normal in G/N, contrary to assumption. Therefore $|K| = p^2$, so K is abelian. In particular, $K \leq C_{G/N}([a, b])$. Clearly $[a, b], a^p \in C_{G/N}([a, b])$ and it is easy to check that $ab^{-1} \in C_{G/N}([a, b])$, so $C_{G/N}([a, b]) = \langle [a, b], ab^{-1}, a^p \rangle$ and $K = \langle [a, b], ab^{-1} x \rangle$ for some $x \in Z(G/N)$.

It is noted as a result of Corollary 12.3.1 in [2] that if $|H| = p^k$ for some group H with $k \leq p$ then H is regular. That is, if $u, v \in H$ then $(uv)^p = u^p v^p c^p$ for some $c \in [H, H]$. For $p \geq 5$ we may apply this to G, noting that $[G, G] = \langle [a, b], a^p \rangle \cong C_p \times C_p$, to obtain $(ab^{-1})^p = a^p b^{-p} = a^{p^2}$. In the case $p = 3$ we can calculate $(ab^{-1})^3$ as follows:

$$\begin{aligned}
a^b &= a[a, b] \\
a^{b^2} &= a^b [a, b]^b \\
&= a[a, b]^2 a^3 \\
(ab^{-1})^3 &= a a^b a^{b^2} b^{-3} \\
&= a^2 [a, b] a [a, b] a^3 b^{-3} \\
&= a^3 [a, b]^a [a, b] a^3 b^{-3} \\
&= a^3 [a, b] a^3 [a, b] a^3 b^{-3} = b^{-3}.
\end{aligned}$$

In either case, $(ab^{-1}x)^p = (ab^{-1})^p \notin \langle [a, b] \rangle$, contradicting the earlier result that $|K| = p^2$. Therefore $K = \langle [a, b] \rangle$ and $\mu(G/N) = [G : K] = p^3$. □

https://doi.org/10.1017/S0004972718000576 Published online by Cambridge University Press

References

[1] D. Easdown and C. E. Praeger, ‘On minimal faithful permutation representations of finite groups’, *Bull. Aust. Math. Soc.* **38**(2) (1988), 207–220.

[2] M. Hall Jr., *The Theory of Groups* (Chelsea Publishing Co., New York, 1976), reprint of the 1968 edition.

ROBERT CHAMBERLAIN, Mathematics Institute,
University of Warwick, Coventry, CV4 7AL, UK
e-mail: r.m.chamberlain@warwick.ac.uk

https://doi.org/10.1017/S0004972718000576 Published online by Cambridge University Press