Irish Math. Soc. Bulletin
Number 86, Winter 2020, 107–108
ISSN 0791-5578

Some shorter proofs for p-groups

ROBERT HEFFERNAN AND DESMOND MACHALE

Abstract. We give short proofs of elementary results about groups of prime power order.

One of the prettiest results in elementary group theory is the following:

Theorem 1. *If p is a prime number and G is a group with $|G| = p^2$, then G is abelian.*

The usual proof of this result runs like this:

Proof. $|Z(G)|$, being a divisor of $|G|$ is either 1, p of p^2. By a well-known result, since G is a p-group, $|Z(G)|$ is non-trivial, so $|Z(G)| = 1$ is ruled out. Next, if $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic. But, if $G/Z(G)$ is cyclic, then G is abelian, a contradiction. [Alternatively, if $|Z(G)| = p$, choose $a \in G, a \notin Z(G)$. Then $C_G(a) \supseteq \langle Z(G), a\rangle = G$, so $a \in Z(G)$, a contradiction.]
Thus $|Z(G)|$ must be p^2 and G is abelian. □

However, there is a shorter proof using group representation theory. We use the facts that

$$|G| = \sum_{i=1}^{k} d_i^2$$

where the d_i are the degrees of the irreducible complex representations of G; each d_i is a divisor of $|G|$, and the number of representations of degree 1 is $(G : G')$, where G' is the commutator subgroup of G.

The degree equation $|G| = \sum_{i=1}^{k} d_i^2$ gives

$$p^2 = (G : G') + tp^2$$

for some integer t. This is impossible unless $t = 0$ and $G' = \{1\}$, forcing G to be abelian.

We remark that groups of order n^2 are not necessarily abelian if n is not a prime. A minimal counterexample for $n = 4$ is given by D_8, the dihedral group of order 16. For p odd, there are non-abelian groups of order $81 = 9^2$, for example $G(27) \times C_3$, where $G(27)$ is a non-abelian group of order 27.

In general, the degree equation is in many ways a dual of the class equation of a group. Just as the class equation can be used to show that the centre of a p-group is non-trivial, the degree equation can be used to show that the commutator subgroup of a non-abelian p-group cannot have index 1 or p.

Theorem 2. *If G is a non-abelian p-group, then $(G : G') = 1$ or $(G : G') = p$ are not possible.*

Proof. (i) Suppose that $(G : G') = 1$. Then, for $n > 2$, $p^n = (G : G') + \sum p^{2i}$, for $i > 0$. So, $p^n = 1 + \sum p^{2i}$, which is a contradiction. [The usual method of proof of this is to show that G has a normal subgroup H with $(G : H) = p$. Thus, G/H is abelian, so $H \supseteq G'$, a contradiction.]

2020 *Mathematics Subject Classification.* 20-01.
Key words and phrases. groups, p-groups.
Received on 8-6-2020.

©2020 Irish Mathematical Society

(ii) Suppose that $(G : G') = p$. Then, for $n > 2$, we have $p^n = (G : G') + \sum p^{2i}$, for $i > 0$ or $p^n = p + \sum p^{2i}$ and $p^{n-1} = 1 + \sum p^{2i-1}$, a contradiction.

□

We note that D_4, the dihedral group of order 8, and $G(27)$ show that $(G : G') = p^2$ is possible and that the above results can be extended to finite nilpotent groups, which are the direct product of p-groups.

Robert Heffernan is a Lecturer in the Department of Mathematics at Cork Institute of Technology. His mathematical interests are primarily in group theory.
Desmond MacHale is Emeritus Professor of Mathematics at University College Cork where he taught for nearly forty years. His mathematical interests are in abstract algebra but he also works in number theory, geometry, combinatorics and the history of mathematics. His other interests include humour, geology and words.

(Robert Heffernan) Department of Mathematics, Cork Institute of Technology, Ireland

(Desmond MacHale) Department of Mathematics, University College Cork, Ireland
E-mail address, R. Heffernan: robert.heffernan@cit.ie
E-mail address, D. MacHale: d.machale@ucc.ie