A COHOMOLOGICAL PROPERTY OF FINITE p-GROUPS

PETER J. CAMERON AND THOMAS W. MÜLLER

ABSTRACT. We define and study a certain cohomological property of finite p-groups (to be of 'Frobenius type'), which is implicit in Frobenius' theorem (Berl. Sitz. 1895, 981–993) concerning the equation $X^m = 1$ and Philip Hall's subsequent work (Proc. London Math. Soc. 40, 468–501) on equations in finite groups. Hall's twisted version (loc. cit., Theorem 1.6) of Frobenius' theorem implies that each cyclic group of prime power order is of Frobenius type. We show that this property in fact pertains to every finite p-group.

1. INTRODUCTION

One of the most beautiful results of Philip Hall's seminal paper [4] provides a twisted version of Frobenius' well-known theorem[1] concerning the equation $X^m = 1$ in finite groups. Hall's original result [4, Theorem 1.6], which is expressed in terms of solution numbers of a certain type of equation over finite groups, can be restated, in terms more germane to the present investigation, as follows.

Proposition. *Let $\mathfrak{C}$ be a finite cyclic group, $\mathfrak{H}$ a finite group, and let $\alpha : \mathfrak{C} \to \mathrm{Aut}(\mathfrak{H})$ be an action by automorphisms of $\mathfrak{C}$ on $\mathfrak{H}$. Then*

$$|\mathrm{Der}_\alpha(\mathfrak{C}, \mathfrak{H})| \equiv 0 \mod \gcd(|\mathfrak{C}|, |\mathfrak{H}|).$$

Hall's theorem reduces to Frobenius' result upon setting $\alpha = 1$. Recall the concept of a derivation (in a non-commutative setting): given groups $\mathfrak{G}$ and $\mathfrak{H}$, and a fixed action $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$ by automorphisms of $\mathfrak{G}$ on $\mathfrak{H}$, a map $d : \mathfrak{G} \to \mathfrak{H}$ is called a *derivation* (with respect to the action α), if

$$d(g_1 g_2) = \big(d(g_1)\big)^{\alpha(g_2)} d(g_2) \quad (g_1, g_2 \in \mathfrak{G}).$$

Note that, for a derivation $d : \mathfrak{G} \to \mathfrak{H}$ with respect to α, we have $d(1) = 1$ and, consequently,

$$\big(d(g^{-1})\big)^{\alpha(g)} = (d(g))^{-1} \quad (g \in \mathfrak{G}). \tag{1}$$

We denote by $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ the set of all derivations $d : \mathfrak{G} \to \mathfrak{H}$ with respect to a given action $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$.

Definition. *Let p be a prime.*

(i) *A non-trivial finite p-group $\mathfrak{G}$ is termed* **admissible**, *if, for each finite group $\mathfrak{H}$ with $p \big| |\mathfrak{H}|$ and every action $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$, the corresponding set $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ of derivations $d : \mathfrak{G} \to \mathfrak{H}$, formed with respect to this action α, has cardinality a multiple of p.*

(ii) *A finite p-group $\mathfrak{G}$ is said to be of* **Frobenius type**, *if every subgroup $\mathfrak{U} > 1$ of $\mathfrak{G}$ is admissible.*

[1] See [1, § 2, Theorem II] and [3].

In this terminology, Hall's result above immediately implies the following.

Corollary. *Every cyclic group of prime power order is of Frobenius type.*

The question addressed in the present note is: which finite groups of prime power order are of Frobenius type? This problem was raised in [6], having arisen implicitly in [5] in connection with a descent principle in modular subgroup arithmetic. The main result of this paper provides a somewhat surprising answer to this problem.

Theorem. *Every group of prime power order is of Frobenius type.*

The proof is contained in the next two sections.

2. The untwisted case

In order to establish our theorem, we first have to deal with the untwisted case ($\alpha = 1$).

Lemma. *Let p be a prime, $\mathfrak{G}$ a non-trivial finite p-group, and let $\mathfrak{H}$ be a finite group of order divisible by p. Then* $|\mathrm{Hom}(\mathfrak{G},\mathfrak{H})| \equiv 0 \mod p$.

Proof. Classifying homomorphisms by their kernel, and applying the isomorphism theorem, we find that

$$|\mathrm{Hom}(\mathfrak{G},\mathfrak{H})| = \sum_{\mathfrak{V}\trianglelefteq\mathfrak{G}} |\mathrm{Inj}(\mathfrak{G}/\mathfrak{V},\mathfrak{H})|. \tag{2}$$

We now make use of the facts that (i) every subgroup of index p in a finite p-group is normal, (ii) the automorphism group of $\mathfrak{G}/\mathfrak{V}$ contains an element of order p, provided $|\mathfrak{G}/\mathfrak{V}| > p$, and (iii) $\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})$ acts freely on the set $\mathrm{Inj}(\mathfrak{G}/\mathfrak{V},\mathfrak{H})$, provided the latter is non-empty. The second fact follows, for instance, from Gaschütz's theorem [2] asserting the existence of an outer automorphism of order p; however, since we only need to know that $p\big||\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ for $|\mathfrak{G}/\mathfrak{V}| > p$, we can get by with a more elementary argument. Indeed, if $\mathfrak{G}/\mathfrak{V}$ is non-abelian, then it has an inner automorphism of order p. If, on the other hand, $\mathfrak{G}/\mathfrak{V}$ is abelian and $|\mathfrak{G}/\mathfrak{V}| > p$, then $\mathfrak{G}/\mathfrak{V}$ must contain a direct summand of one of the forms $\mathfrak{C}_{p^\sigma}$ or $\sigma\mathfrak{C}_p$ with $\sigma \geq 2$. In the first case, $|\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ is divisible by

$$|\mathrm{Aut}(\mathfrak{C}_{p^\sigma})| = \varphi(p^\sigma) = p^{\sigma-1}(p-1) \equiv 0 \mod p,$$

where φ is Euler's totient function, while, in the second case, $|\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ must be divisible by

$$|\mathrm{Aut}(\sigma\mathfrak{C}_p)| = |\mathrm{GL}_\sigma(p)| = (p^\sigma-1)(p^\sigma-p)\cdots(p^\sigma-p^{\sigma-1}) \equiv 0 \mod p.$$

Hence, evaluating (2) modulo p, we get

$$|\mathrm{Hom}(\mathfrak{G},\mathfrak{H})| \equiv 1 + s_p(\mathfrak{G})|\mathrm{Inj}(\mathfrak{C}_p,\mathfrak{H})| \mod p.$$

We have $s_p(\mathfrak{G}) \equiv 1 \bmod p$ by Frobenius' generalization of Sylow's third theorem and the fact that $\mathfrak{G} \neq 1$. (Alternatively, one might compute

$$s_p(\mathfrak{G}) = \frac{p^{r(\overline{\mathfrak{G}})}-1}{p-1} = 1 + p + p^2 + \cdots + p^{r(\overline{\mathfrak{G}})-1} \equiv 1 \mod p,$$

where $r(\overline{\mathfrak{G}})$ is the rank of the factor group $\overline{\mathfrak{G}} = \mathfrak{G}/\Phi(\mathfrak{G})$, since every subgroup of $\mathfrak{G}$ of index p contains $\Phi(\mathfrak{G})$. Moreover, by Frobenius' theorem concerning the equation $X^m = 1$ in finite groups and the fact that $p \big| |\mathfrak{H}|$, we have

$$|\mathrm{Inj}(\mathfrak{C}_p, \mathfrak{H})| \equiv -1 \mod p,$$

whence the lemma. □

3. Proof of the theorem

Let p be a prime, $\mathfrak{G}$ a non-trivial finite p-group, $\mathfrak{H}$ a finite group of order divisible by p, and let $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$ be an action by automorphisms of $\mathfrak{G}$ on $\mathfrak{H}$, where multiplication in the group $\mathrm{Aut}(\mathfrak{H})$ is given by the rule

$$(\sigma_1 \cdot \sigma_2)(h) := \sigma_2(\sigma_1(h)) \quad (\sigma_1, \sigma_2 \in \mathrm{Aut}(\mathfrak{H}),\ h \in \mathfrak{H}).$$

We have to show that

$$|\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})| \equiv 0 \mod p. \tag{3}$$

Let

$$\mathcal{F}(\mathfrak{G}, \mathfrak{H}) = \mathfrak{H}^{\mathfrak{G}}$$

be the set of all functions from $\mathfrak{G}$ to $\mathfrak{H}$. We make $\mathfrak{G}$ act (from the right) on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ by setting

$$(\mathfrak{f} \circledast g)(x) := \big(\mathfrak{f}(gxg^{-1})\big)^{\alpha(g)} \quad \big(g, x \in \mathfrak{G},\ \mathfrak{f} \in \mathcal{F}(\mathfrak{G}, \mathfrak{H})\big).$$

For $g_1, g_2, x \in \mathfrak{G}$ and $\mathfrak{f} \in \mathcal{F}(\mathfrak{G}, \mathfrak{H})$,

$$\begin{aligned}\big((\mathfrak{f} \circledast g_1) \circledast g_2\big)(x) &= \big((\mathfrak{f} \circledast g_1)(g_2 x g_2^{-1})\big)^{\alpha(g_2)} \\ &= \big(\mathfrak{f}(g_1 g_2 x g_2^{-1} g_1^{-1})\big)^{\alpha(g_1 g_2)} \\ &= \big(\mathfrak{f} \circledast (g_1 g_2)\big)(x),\end{aligned}$$

as well as $\mathfrak{f} \circledast 1 = \mathfrak{f}$, and we have indeed defined an action of $\mathfrak{G}$ on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$. In what follows, two distinguished subsets of $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ will play a role: the set $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ of derivations $d : \mathfrak{G} \to \mathfrak{H}$ with respect to α, and the set $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$ of anti-homomorphisms from $\mathfrak{G}$ to $\mathfrak{H}$. Note that

$$|\mathrm{Hom}(\mathfrak{G}, \mathfrak{H})| = |\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})|, \tag{4}$$

a bijection being given by the map

$$\psi \mapsto \psi^*, \quad \psi^*(g) := (\psi(g))^{-1} \quad \big(g \in \mathfrak{G},\ \psi \in \mathrm{Hom}(\mathfrak{G}, \mathfrak{H})\big).$$

We have to check that the action of $\mathfrak{G}$ on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ defined above restricts to an action of $\mathfrak{G}$ on the subsets $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ and $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$. Indeed, for $g, x, y \in \mathfrak{G}$ and $d \in \mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$, we have

$$\begin{aligned}(d \circledast g)(xy) &= \big(d(gxyg^{-1})\big)^{\alpha(g)} \\ &= \big(d(gxg^{-1})\big)^{\alpha(gy)} \big(d(gyg^{-1})\big)^{\alpha(g)} \\ &= \big((d \circledast g)(x)\big)^{\alpha(y)} (d \circledast g)(y),\end{aligned}$$

that is, $d \circledast g : \mathfrak{G} \to \mathfrak{H}$ is again a derivation with respect to α. Similarly, for $g,x,y \in \mathfrak{G}$ and $\psi^* \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})$,

$$\begin{aligned}(\psi^* \circledast g)(xy) &= \big(\psi^*(gxyg^{-1})\big)^{\alpha(g)} \\ &= \big(\psi^*(gyg^{-1})\big)^{\alpha(g)}\big(\psi^*(gxg^{-1})\big)^{\alpha(g)} \\ &= (\psi^* \circledast g)(y)(\psi^* \circledast g)(x).\end{aligned}$$

Denote by $\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}$ and $\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}$ the fixed point sets of $\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})$ and $\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})$, respectively, under the respective $\mathfrak{G}$-action, so that

$$|\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})| \equiv |\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}| \mod p \tag{5}$$

and

$$|\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})| \equiv |\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}| \mod p. \tag{6}$$

The decisive point in the proof is the fact that

$$\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} = \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}) \cap \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H}) = \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}. \tag{7}$$

Indeed, let $d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})$. Then

$$d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} \iff \big(d(gxg^{-1})\big)^{\alpha(g)} = d(x) \quad (g,x \in \mathfrak{G}).$$

Now, using (1),

$$\begin{aligned}\big(d(gxg^{-1})\big)^{\alpha(g)} &= \Big(\big(d(gx)\big)^{\alpha(g^{-1})} d(g^{-1})\Big)^{\alpha(g)} \\ &= d(gx)\big(d(g^{-1})\big)^{\alpha(g)} \\ &= d(gx)\big(d(g)\big)^{-1},\end{aligned}$$

hence

$$d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} \iff d \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H}), \quad d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}).$$

Similarly, if $\psi^* \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})$, then

$$\begin{aligned}\psi^* \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} &\iff \psi^*(g^{-1}xg) = \big(\psi^*(x)\big)^{\alpha(g)} \quad (g,x \in \mathfrak{G}) \\ &\iff \psi^*(xg)\psi^*(g^{-1}) = \big(\psi^*(x)\big)^{\alpha(g)} \quad (g,x \in \mathfrak{G}) \\ &\iff \psi^* \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}),\end{aligned}$$

whence (7). In view of equations (4)–(7) and the lemma, we now find that, modulo p,

$$\begin{aligned}|\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})| &\equiv |\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}| \\ &= |\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}) \cap \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})| \\ &= |\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}| \\ &\equiv |\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})| \\ &= |\mathrm{Hom}(\mathfrak{G},\mathfrak{H})| \equiv 0,\end{aligned}$$

whence (3), and the proof of the theorem is complete.

REFERENCES

[1] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Berliner Sitzungsber.* (1895), 981–993.
[2] W. Gaschütz, Nichtabelsche p-Gruppen besitzen äußere p-Automorphismen, *J. Algebra* **4** (1966), 1–2.
[3] I. M. Isaacs and G. R. Robinson, On a theorem of Frobenius: solutions of $x^n = 1$ in finite groups, *Am. Math. Monthly* **99** (1992), 352–354.
[4] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* **40** (1936), 468–501.
[5] T. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.
[6] T. Müller, Modular subgroup arithmetic, in: Proc. 2001 Durham Symposium on Groups, Geometries, and Combinatorics (A. Ivanov, M. Liebeck, and J. Saxl eds.), World Scientific, to appear.

SCHOOL OF MATHEMATICAL SCIENCES
QUEEN MARY, UNIVERSITY OF LONDON
MILE END ROAD
LONDON E1 4NS
UNITED KINGDOM
E-mail: P.J.Cameron@qmul.ac.uk
and T.W.Muller@qmul.ac.uk