NEARLY REGULAR p-GROUPS

C. R. HOBBY

A finite p-group G is said to be regular if for every pair of elements a, b in G,

$$(ab)^p = a^p b^p c^p, \tag{1}$$

where c is an element of the derived group of the subgroup generated by a and b. We shall say that G is *nearly regular* if (i) there is a central element z of order p such that $G/\langle z\rangle$ is regular, and (ii) the subgroup generated by x and y is regular whenever $x \in G$ and $y \in G'$, the derived group of G.

It is easy to see that the property of being nearly regular is inherited by subgroups and factor groups. The power structure of nearly regular groups is much more complicated than that of regular groups. For instance, if G is a regular group in which the subgroup generated by pth powers has order p, then the elements of order p form a subgroup of index p in G. However, if $H_1, \ldots, H_m$ are m copies of the wreath product of two groups of order p, and if G is constructed by taking the direct product of the H_i and then amalgamating their centres, then it is not hard to see that G is a nearly regular group in which the subgroup generated by pth powers has order p, yet the largest subgroup consisting of elements of order p has index p^m.

If G is not regular, then there are elements x, y such that there is no c in $\langle x, y\rangle'$ for which $(xy)^p = x^p y^p c^p$. We shall show that if G is nearly regular, then we can always find elements a, b such that $\langle x, y\rangle = \langle a, b\rangle$, where a, b satisfy the regularity condition (1).

THEOREM. *Suppose G is a nearly regular p-group where p is an odd prime. If $x, y \in G$, then there are elements a, b in G such that $\langle x, y\rangle = \langle a, b\rangle$ and $(ab)^p = a^p b^p c^p$, where c is an element of the derived group of the group $\langle a, b\rangle$.*

All regular 2-groups are abelian; therefore, the nearly regular 2-groups are those with a derived group of order at most 2. Thus if the theorem were true for 2-groups we would have $\langle x, y\rangle = \langle a, b\rangle$, where $(ab)^2 = a^2 b^2$; hence $ba = ab$, so $xy = yx$. This would imply that all nearly regular 2-groups are abelian, a contradiction. Therefore the restriction $p > 2$ in the theorem is necessary.

Proof. Suppose that G is a counterexample of minimal order. Let x, y be a pair of elements such that $\langle x, y\rangle$ cannot be generated by any pair of elements a, b which satisfy (1). Then $\langle x, y\rangle$ is a counterexample, and hence $G = \langle x, y\rangle$.

Received January 19, 1966. This work was supported in part by the National Science Foundation under Grant No. GP–3919, and by the U.S. Air Force, Grant AF–AFOSR–937–65.

Let N be the subgroup generated by all pth powers of elements of G'. Suppose $N \neq 1$. Then the theorem is true for G/N, so $G/N = \langle \bar{a}, \bar{b} \rangle$, where $(\bar{a}\bar{b})^p = \bar{a}^p\bar{b}^p\bar{c}^p$ for $\bar{c} \in G'/N$. Thus, if a, b, c are pre-images in G of $\bar{a}$, $\bar{b}$, $\bar{c}$, we have $(ab)^p = a^pb^pc^p \cdot d$ for some $d \in N$. Clearly N is contained in the Frattini subgroup of G, so G is generated by a, b. It only remains to show that c^pd is the pth power of an element of G'. But the derived group of a nearly regular group is regular, so c^pd is a pth power since it is a product of pth powers. This completes the proof if $N \neq 1$.

Suppose now that $N = 1$. Since G is regular modulo $\langle z \rangle$ and $N = 1$, we have $(ab)^p = a^pb^pz^t$ for every pair $a, b \in G$, where t depends on a, b. Also, the subgroup generated by pth powers of the elements of G is central modulo $\langle z \rangle$; hence $a^pb^p = b^pa^p$ for all $a, b \in G$.

For $1 \leqslant s, t \leqslant p - 1$, we define $\alpha(s, t)$ by

$$(x^s y^t)^p = x^{ps} y^{pt} z^{\alpha(s,t)}, \tag{2}$$

where $1 \leqslant \alpha(s, t) \leqslant p$. If $\alpha(s, t) = p$, we take $a = x^s$, $b = y^t$ and the proof is complete. In fact, we may suppose that the mapping $s \to \alpha(s, 1)$ is a permutation of $1, 2, \ldots, p - 1$, for, if $\alpha(s, 1) = \alpha(s_1, 1)$, where $s \not\equiv s_1 \bmod p$, we set $r = s - s_1$ and observe that

$$\begin{aligned}(x^s y)^p &= x^{ps} y^p z^{\alpha(s,1)} \\ &= x^{pr} x^{ps_1} y^p z^{\alpha(s,1)} \\ &= x^{pr} (x^{s_1} y)^p z^{-\alpha(s_1,1)+\alpha(s,1)};\end{aligned}$$

hence $(x^r \cdot x^{s_1} y)^p = x^{pr}(x^{s_1} y)^p$ and the proof is complete if we set $a = x^r$, $b = x^{s_1} y$.

A similar argument shows that the mapping $t \to \alpha(1, t)$ is a permutation of $1, 2, \ldots, p - 1$.

Next, we show that $\alpha(s, t)$ is homogeneous. That is, if $1 \leqslant k \leqslant p - 1$, then $\alpha(ks, kt) = k\alpha(s, t)$. We carry out the computation as follows:

$$\begin{aligned}(x^{ks} y^{kt})^p &= x^{pks} y^{pkt} z^{\alpha(ks,kt)} \\ &= (x^{ps} y^{pt})^k z^{\alpha(ks,kt)} \\ &= \{(x^s y^t)^p z^{-\alpha(s,t)}\}^k z^{\alpha(ks,kt)} \\ &= (x^s y^t)^{kp} z^{\alpha(ks,kt)-k\alpha(s,t)},\end{aligned}$$

where we have used the fact that pth powers commute. It only remains to show that $(x^{ks} y^{kt})^p = (x^s y^t)^{kp}$. But $(x^s y^t)^k = (x^{ks} y^{kt}) \cdot g$ for some $g \in G'$, and, by hypothesis, $\langle (x^{ks} y^{kt}), g \rangle$ is regular. The result follows since $N = 1$, so α is homogeneous.

The assumption that G is a minimal counterexample has led to the existence of a homogeneous function $\alpha(s, t)$ on $1, 2, \ldots, p - 1$ such that the mappings

https://doi.org/10.4153/CJM-1967-044-8 Published online by Cambridge University Press

$s \to \alpha(s, 1)$ and $t \to \alpha(1, t)$ are permutations. But, for p odd, there is no such function, since by Wilson's theorem

$$-1 \equiv \prod_s \alpha(s, 1) \equiv \prod_s s\alpha(1, 1/s)$$

$$\equiv \prod_s s \prod_t \alpha(1, t) \equiv (-1)\cdot(-1) \equiv 1,$$

a contradiction. This completes the proof of the theorem.

If $p = 3$, the same result can be obtained under the weaker assumption that $G/\langle z\rangle$ is regular for some central z of order p. As before, a minimal counter-example can be generated by two elements, say x, y. But a regular 3-group which can be generated by two elements has a cyclic derived group; hence $G'/\langle z\rangle$ is cyclic, so G' is abelian. One may now argue as before that $N = 1$. It follows that G' has order at most 9; hence, if $a \in G$, $g \in G'$, we have $\langle a, g\rangle$ regular. Thus G is nearly regular and the result follows. It is an open question whether the hypothesis of the theorem can be weakened for general p.

Reference

1. Marshall Hall, *The theory of groups* (New York, 1959).

University of Washington,
Seattle