A CHARACTERISTIC SUBGROUP OF A p-GROUP

CHARLES HOBBY

If x, y are elements and H, K subsets of the p-group G, we shall denote by $[x, y]$ the element $y^{-p}x^{-p}(xy)^p$ of G, and by $[H, K]$ the subgroup of G generated by the set of all $[h, k]$ for h in H and k in K. We call a p-group G *p-abelian* if $(xy)^p = x^py^p$ for all elements x, y of G. If we let $\theta(G) = [G, G]$ then $\theta(G)$ is a characteristic subgroup of G and $G/\theta(G)$ is p-abelian. In fact, $\theta(G)$ is the minimal normal subgroup N of G for which G/N is p-abelian. It is clear that $\theta(G)$ is contained in the derived group of G, and $G/\theta(G)$ is *regular* in the sense of P. Hall [3]

Theorem 1 lists some elementary properties of p-abelian groups. These properties are used to obtain a characterization of p-groups G (for $p \geq 3$) in which the subgroup generated by the pth powers of elements of G coincides with the Frattini subgroup of G (Theorems 2 and 3). A group G is said to be metacyclic if there exists a cyclic normal subgroup N with G/N cyclic. Theorem 4 states that a p-group G, for $p > 2$, is metacyclic if and only if $G/\theta(G)$ is metacyclic. Theorems on metacyclic p-groups due to Blackburn and Huppert are obtained as corollaries of Theorems 3 and 4.

The following notation is used: G is a p-group; $G^{(n)}$ is the nth derived group of G; G_n is the nth element in the descending central series of G; $P(G)$ is the subgroup of G generated by the set of all x^p for x belonging to G; $\Phi(G)$ is the Frattini subgroup of G; $\langle x, y, \cdots \rangle$ is the subgroup generated by the elements $x, y, \cdots$; $Z(G)$ is the center of G; $(h, k) = h^{-1}k^{-1}hk$; if H, K are subsets of G, then (H, K) is the subgroup generated by the set of all (h, k) for $h \in H$ and $k \in K$.

THEOREM 1. *If G is p-abelian, then*

$$P(G^{(1)}) = P(G)^{(1)}\ , \tag{1.1}$$

$$P(G) \subseteq Z(G)\ , \tag{1.2}$$

$$\Phi(G^{(1)}) = \Phi(G)^{(1)} = G^{(2)}\ . \tag{1.3}$$

Proof of (1.1). $\theta(G) = \langle 1 \rangle$ implies that $(xyx^{-1}y^{-1})^p = x^py^px^{-p}y^{-p}$ for all x, y in G. (1.1) follows immediately.

Proof of (1.2). Let x be an arbitrary element of G, and suppose the order of x is p^n. Let $u = x^{1+p+\cdots+p^{n-1}}$. Then, for any y in G,

Received July 30, 1959. This work was supported by a National Science Foundation pre-doctaral fellowship.

$$uy^p u^{-1} = (uyu^{-1})^p = u^p y^p u^{-p} ,$$

where the last equality follows from $\theta(G) = \langle 1 \rangle$. Therefore $u^{1-p} y^p u^{p-1} = y^p$. But $u^{1-p} = x^{1-p^n} = x$, hence $xy^p x^{-1} = y^p$, and (1.2) follows.

Proof of (1.3). It is easy to see that $\Phi(G) = P(G)G^{(1)}$, hence $\Phi(G)^{(1)} \supseteq P(G)^{(1)}G^{(2)}$. Thus, by (1.1), $\Phi(G)^{(1)} \supseteq P(G^{(1)})G^{(2)} = \Phi(G^{(1)}) \supseteq G^{(2)}$. It remains to show that $G^{(2)} \supseteq \Phi(G)^{(1)}$. But if x, y belong to $\Phi(G)$, we can write $x = x'u, y = y'v$ for x', y' in $P(G)$ and u, v in $G^{(1)}$ (since $\Phi(G) = P(G)G^{(1)}$). By (1.2), x' and y' belong to $Z(G)$, hence $xyx^{-1}y^{-1} = uvu^{-1}v^{-1}$ is an element of $G^{(2)}$. Thus $\Phi(G)^{(1)} \subseteq G^{(2)}$, and the proof is complete.

COROLLARY 1.1. $P(G^{(1)}) \subseteq \theta(G)$.

Proof. It suffices to show that $\theta(G) = \langle 1 \rangle$ implies $P(G^{(1)}) = \langle 1 \rangle$. But, if $\theta(G) = \langle 1 \rangle$, it follows from (1.1) and (1.2) that $P(G^{(1)}) = P(G)^{(1)}$ and $P(G) \subseteq Z(G)$. Thus $P(G^{(1)}) = \langle 1 \rangle$.

REMARK 1. P. Hall [3] has shown that

$$(xy)^p = x^p y^p cd$$

whenever x, y belong to a p-group G, where c is a product of pth powers of elements of $\langle x, y \rangle^{(1)}$ and d is a product of elements contained in the pth element of the descending central series of $\langle x, y \rangle$. We have, as an immediate consequence, $\theta(G) \subseteq P(G^{(1)})G_p$.

We shall now investigate p-groups G for which $P(G) = \Phi(G)$. The following lemma will be useful.

LEMMA 1. *Suppose $p \neq 2$. If $P(G) = \Phi(G)$ and $P(G^{(1)}) = \langle 1 \rangle$, then $G_3 = \langle 1 \rangle$.*

Proof. If $x, y \in G$, then

$$\begin{aligned}(y^p, x) &= y^{-p}(x^{-1}y^p x) = y^{-p}(x^{-1}yx)^p \\ &= y^{-p}\{y(y, x)\}^p \\ &= (y, x)^p[y, (y, x)] = [y, (y, x)] ,\end{aligned}$$

where the last equality follows from $P(G^{(1)}) = \langle 1 \rangle$. Therefore $G_3 \subseteq (G, P(G)) \subseteq [G, G^{(1)}] \subseteq [G, P(G)]$. We complete the proof by showing that $[G, P(G)] \subseteq G_4$.

We first observe that $(x, y^p) \in G_3$, hence

$$(xy^p)^p = x^p y^{p^2} (x, y^p)^{(p-1)/2} z$$

for some $z \in G_4$. Since $p \neq 2$ and $P(G^{(1)}) = \langle 1 \rangle$, we have $[x, y^p] \in G_4$ for every $x, y \in G$. It follows that $[G, P(G)] \subseteq G_4$.

THEOREM 2. *If* $P(G) = \Phi(G)$, *then* $P(G^{(k)}) = \Phi(G^{(k)})$ *for* $k = 1, 2, \cdots$.

Proof. Suppose G is a group of minimal order for which $P(G) = \Phi(G)$ but $P(G^{(k)}) \neq \Phi(G^{(k)})$ for some $k \geq 1$. If $P(G^{(1)}) = \Phi(G^{(1)})$, then we must have $P(G^{(k)}) = \Phi(G^{(k)})$ for all $k \geq 1$ since the order of $G^{(1)}$ is less than the order of G. Thus $P(G^{(1)}) \neq \Phi(G^{(1)})$. We assert that $P(G^{(1)})$ must be $\langle 1 \rangle$. For, if $P(G^{(1)}) \neq \langle 1 \rangle$, we let $H = G/P(G^{(1)})$. Then it is easy to see that $P(H) = \Phi(H)$. Thus, since H has smaller order than $G, P(H^{(1)}) = \Phi(H^{(1)})$. Also, $P(H^{(1)}) = \langle 1 \rangle$. Therefore

$$\langle 1 \rangle = \Phi(H^{(1)}) = \Phi(G^{(1)}/P(G^{(1)})) = \Phi(G^{(1)})P(G^{(1)})/P(G^{(1)}) .$$

That is, $P(G^{(1)}) \supseteq \Phi(G^{(1)})$, and hence $P(G^{(1)}) = \Phi(G^{(1)})$, which contradicts our assumption.

If $p = 2$ it follows from $P(G^{(1)}) = \langle 1 \rangle$ that $G^{(1)}$ is abelian. If $p \neq 2$, then by Lemma 1, $G_3 = \langle 1 \rangle$ and $G^{(1)}$ is again abelian. Therefore $P(G^{(1)}) = \Phi(G^{(1)})$, contrary to our choice of G.

COROLLARY 2.1. *If* $p \neq 2$ *and* $P(G) = \Phi(G)$, *then* $P(G^{(1)}) = \Phi(G^{(1)}) = \theta(G) \supseteq G_3$.

Proof. By Corollary 1.1, $P(G^{(1)}) \subseteq \theta(G)$. By Lemma 1, $G_3 \subseteq P(G^{(1)})$. Therefore $P(G^{(1)})G_p = P(G^{(1)})$ since $p \neq 2$. It follows from Remark 1 that $P(G^{(1)}) = \theta(G)$. By Theorem 2, $P(G^{(1)}) = \Phi(G^{(1)})$, and the proof is complete.

COROLLARY 2.2. *Let* $p \neq 2$ *and* $P(G) = \Phi(G)$. *Then* $P(G^{(1)}) \subseteq G^{(2)}$ *implies* $G_3 = \langle 1 \rangle$, *and hence* $G^{(2)} = \langle 1 \rangle$.

Proof. By Corollary 2.1, $G_3 \subseteq P(G^{(1)})$, thus $G_3 \subseteq G^{(2)}$. It is known [3, Theorem 2.54] that $G^{(2)} \subseteq G_4$. Therefore $G_3 = G_4 = G^{(2)} = \langle 1 \rangle$.

THEOREM 3. *Suppose* $p \neq 2$ *and let* $x_1, x_2, \cdots, x_k$ *be coset representatives of a minimal basis of the abelian group* $G/G^{(1)}$. *Then* $P(G) = \Phi(G)$ *if, and only if, there exist integers* $n(i)$ *such that*

$$G^{(1)} = \langle x_1^{p^{n(1)}}, x_2^{p^{n(2)}}, \cdots, x_k^{p^{n(k)}} \rangle .$$

Proof. If such integers $n(i)$ exist, then $G^{(1)} \subseteq P(G)$ and it follows that $P(G) = \Phi(G)$.

Suppose $P(G) = \Phi(G)$, and let $H = G/\theta(G)$. Then $\theta(H) = \langle 1 \rangle$, and $H = \langle y_1, y_2, \cdots, y_k \rangle$ where y_i is the image of x_i under the homomorphism mapping G onto $G/\theta(G)$. Since $\theta(H) = \langle 1 \rangle$, $P(H) = \langle y_1^p, y_2^p, \cdots, y_k^p \rangle$, and $P(H) \subseteq Z(H)$. Also, $P(H) = \Phi(H) \supseteq H^{(1)}$, hence every element of $H^{(1)}$ can be expressed in the form $y_1^{pu} y_2^{pv} \cdots y_k^{pw}$ for suitable integers $u, v, \cdots, w$. Since the y_i are independent generators of H modulo $H^{(1)}$, it follows that there exist integers $n_1, n_2, \cdots, n_k$ such that $H^{(1)} = \langle y_1^{pn_1}, y_2^{pn_2}, \cdots, y_k^{pn_k} \rangle$. By Corollary 2.1, $\Phi(G^{(1)}) = \theta(G)$, thus $H^{(1)} = G^{(1)}/\theta(G) = G^{(1)}/\Phi(G^{(1)})$. Thus we can use the Burnside Basis Theorem [6, page 111] to obtain $G^{(1)} = \langle x_1^{pn_1}, x_2^{pn_2}, \cdots x_k^{pn_k} \rangle$. The proof follows if we let $n(i)$ be the largest positive integer n for which p^n divides pn_i.

COROLLARY 3.1. *Suppose* $p \neq 2$ *and* $P(G) = \Phi(G)$. *If* G *can be generated by* k *elements, then* $G^{(r)}$ *can be generated by* k *elements for* $r = 1, 2, 3, \cdots$.

Proof. Follows immediately from Theorems 2 and 3.

LEMMA 2. *If* $p \neq 2$ *and* $G/\Phi(G^{(1)})G_3$ *is metacyclic, then*

$$\Phi(G^{(1)})G_3 = \theta(G) .$$

Proof. Since $p > 2$ it follows from Remark 1 that $\theta(G) \subseteq P(G^{(1)})G_3$ and hence $\theta(G) \subseteq \Phi(G^{(1)})G_3$. The lemma will follow if it is shown that $\Phi(G^{(1)})G_3 \subseteq \theta(G)$. We may assume $\theta(G) = \langle 1 \rangle$. Then, by Corollary 1.1, $P(G^{(1)}) = \langle 1 \rangle$, thus $\Phi(G^{(1)})G_3 = G_3$. If $G_3 \neq \langle 1 \rangle$ we may assume $G_3 = \langle z \rangle$, where z is an element of order p in $Z(G)$. Since G/G_3 is metacyclic, there exist elements a, b such that $G = \langle a, b \rangle$ and $G^{(1)}$ is generated modulo G_3 by a^{p^k} for some integer $k > 0$. By (1.2), a^{p^k} belongs to $Z(G)$. But then $G^{(1)} = \langle a^{p^k}, z \rangle \subseteq Z(G)$ and $G_3 = \langle 1 \rangle$.

Blackburn [1] showed that a p-group G is metacyclic if, and only if, $G/\Phi(G^{(1)})G_3$ is metacyclic. Our next theorem follows immediately from Lemma 2 and this result of Blackburn. We shall give a simple direct proof of Theorem 4, and obtain Blackburn's result for $p > 2$ as Corollary 4.2.

THEOREM 4. *Suppose* $p > 2$. *Then* G *is metacyclic if, and only if,* $G/\theta(G)$ *is metacyclic.*

Proof. Since any factor group of a metacyclic group is again metacyclic, we need only show that $G/\theta(G)$ metacyclic implies G is matacyclic.

Suppose G is a non-metacyclic group of minimal order for which $G/\theta(G)$ is metacyclic. Then $\theta(G) \neq \langle 1 \rangle$ and hence we can find an element z in $\theta(G)$ such that z has order p and belongs to $Z(G)$. If we let $H = G/\langle z \rangle$, then $H/\theta(H) = (G/\langle z \rangle)/(\theta(G)/\langle z \rangle) \cong G/\theta(G)$ is metacyclic, and consequently H is itself metacyclic since H has smaller order than G. Thus we can find $\bar{a}, \bar{b}$ in H such that $H = \langle \bar{a}, \bar{b} \rangle$ and $H^{(1)} = \langle \bar{a}^{p^k} \rangle$ for some $k > 0$. If we let a, b be coset representatives in G of $\bar{a}, \bar{b}$, then it follows from the Burnside Basis Theorem that $G = \langle a, b \rangle$ and hence $G^{(1)} = \langle a^{p^k}, z \rangle$. In particular, if we let $c = a^{-1}b^{-1}ab$, there exist integers, n and m such that $c = a^{np^k}z^m$. Since z belongs to $Z(G)$, it is clear that $a^{-1}c^{-1}ac = 1$, and

$$b^{-1}cb = b^{-1}a^{np^k}bz^m = (b^{-1}ab)^{np^k}z^m = (a^{1+np^k}z^m)^{np^k}z^m ,$$

thus

$$c^{-1}b^{-1}cb = a^{n^2p^{2k}}z^{mnp^k} = a^{n^2p^{2k}}$$

where the last equality follows from $z^p = 1$. Similarly, $b^{-1}a^{p^k}b = a^{p^k+np^{2k}}$. Thus G_3, which is generated by $c^{-1}b^{-1}cb, a^{-1}c^{-1}ac$, and the various conjugates of these elements, is contained in $\langle a^{p^k} \rangle$. Since $P(G^{(1)}) \subseteq \langle a^{p^k} \rangle$, it follows from Remark 1 that $\theta(G) \subseteq \langle a^{p^k} \rangle$. But z belongs to $\theta(G)$, hence $G^{(1)} = \langle a^{p^k} \rangle$ and G is metacyclic.

REMARK 2. If $p = 2$, it follows from $\theta(G) = \langle 1 \rangle$ that $(xy)^2 = x^2y^2$ and hence $x^{-1}yxy^{-1} = 1$ for all x, y in G. Thus $\theta(G) = G^{(1)}$ and $G/\theta(G)$ is metacyclic whenever G can be generated by two elements. Since there exist non-metacyclic 2-groups having two generators we see that Theorem 4 is false for $p = 2$.

The following result was established by Huppert [5, Hauptsatz 1].

COROLLARY 4.1. *Suppose $p \neq 2$ and G can be generated by two elements. Then G is metacyclic if, and only if, $P(G) = \Phi(G)$.*

Proof. It is clear that $P(G) = \Phi(G)$ if G is metacyclic. Suppose $P(G) = \Phi(G)$. Since G can be generated by two elements, $G^{(1)}$ is cyclic modulo G_3 [3, Theorem 2.81]. We see from Theorem 3 that, if $G = \langle a, b \rangle$, then $G^{(1)} = \langle a^{p^n}, b^{p^m} \rangle$ for some integers m and n. It follows that one of a^{p^n}, b^{p^m} is mapped on a generator of $G^{(1)}/G_3$ by the natural homomorphism. Thus G/G_3 is metacyclic. By Corollary 2.1, $\theta(G) \supseteq G_3$, hence $G/\theta(G)$ is metacyclic. It follows from Theorem 4 that G is metacyclic.

The next corollary is an immediate consequence of Lemma 2 and Theorem 4.

COROLLARY 4.2. *If $p \neq 2$, then G is metacyclic if, and only if, $G/\Phi(G^{(1)})G_3$ is metacyclic.*

REMARK 3. We define $\theta_1(G) = \theta(G)$ and $\theta_n(G) = \theta(\theta_{n-1}(G))$ for $n > 1$. The series $\theta_1(G) \supset \theta_2(G) \supset \cdots \supset \theta_k(G) = \langle 1 \rangle$ can be considered a generalization of the derived series of G. Corresponding generalizations of the ascending and descending central series of G can be obtained as follows: let $\Gamma_1(G)$ be the subgroup of G generated by the set of all x in G such that $(xy)^p = x^p y^p$ for every element y of G, and define $\Gamma_n(G)$ for $n > 1$ as the subgroup of G mapped onto $\Gamma_1(G/\Gamma_{n-1}(G))$ by the natural homomorphism; let $\Psi_1(G) = G$, and $\Psi_n(G) = [G, \Psi_{n-1}(G)]$ for $n > 1$. These series have an important property in common with the ascending and descending central series. Namely, if we define the lengths $l(\Gamma)$ and $l(\Psi)$ of the Γ and Ψ series as, respectively, the smallest integers m and n for which $\Gamma_m(G) = G$ and $\Psi_{n+1}(G) = \langle 1 \rangle$, it is easy to see that $l(\Gamma) = l(\Psi)$.

The group $\Gamma_1(G)$ has been studied by Grun [2]. The groups $\theta_n(G)$ and $\Psi_m(G)$ have not appeared in the literature, however the following result is an immediate consequence of earlier work [4, Remark 1].

THEOREM 5. *A non-abelian group with cyclic center cannot be one of the subgroups $\theta_n(G)$ or $\Psi_m(G)$ (for $m > 1$) of a p-group G.*

REFERENCES

1. N. Blackburn, *On prime power groups with two generators*, Proc. Camb. Phil. Soc. **54** (1958), 327–337.

2. O. Grun, *Beiträge zur Gruppentheorie, V.* Osaka Math. J. **5** (1953), 117–146.

3. P. Hall, *A contribution to the theory of groups of prime-power orders*, Proc. Lond. Math. Soc. (2) **36** (1933), 29–95.

4. C. Hobby, *The Frattini subgroup of a p-group.* Pacific J. Math. **10** (1960), 209–212.

5. B. Huppert, *Uber das Product von paarweise vertauschbaren zyklischen Gruppen*, Math. Z. **58** (1953), 243–264.

6. H. Zassenhaus, *Theory of Groups* (trans.), New York, Chelsea, 1949.

CALIFORNIA INSTITUTE OF TECHNOLOGY