Groups of prime power order with cyclic Frattini subgroup

by T. R. Berger, L. G. Kovács and M. F. Newman

University of Minnesota, Minneapolis, U.S.A.,
Australian National University, Canberra,
Australian National University, Canberra

Communicated by Prof. T. A. Springer at the meeting of February 24, 1979

A well-known theorem attributed to P. Hall (see, for example, Huppert [2] III.13.10) describes the structure of the groups of prime power order in which every abelian characteristic subgroup is cyclic. Van der Waall [4] has recently observed that for odd primes p the same groups G arise if one assumes only that $Z(\Phi(G))$ and $Z(\Omega_1(G))$ are cyclic – notation follows Huppert. (This result is implicit in Huppert's proof of III.13.10.). The first aim of this note is to point out that for all primes p the same groups G are obtained by asking that just one abelian characteristic subgroup, namely $Z(\Omega_1(C_G(\Phi(G))))$, be cyclic, and to give a short proof of the structure theorem, with only this assumption, in a form which solves the isomorphism problem for these groups. (P. Hall is reported to have given a result of this kind in his lectures in Cambridge.) The second aim is to describe the structure of those groups G of prime power order in which $Z(\Phi(G))$ is cyclic. (From this one can read off an answer to the question posed at the end of van der Waall's paper.) The starting point of both arguments is, as in Huppert's book and in van der Waall's paper, an application of a theorem of Hobby [1] (III.7.8c in [2]): if G is a finite p-group and $Z(\Phi(G))$ is cyclic, then $\Phi(G)$ is cyclic. (For another generalization of van der Waall's paper, see [3].)

Only finite p-groups will be considered. The structure of the groups will be described in terms of direct products and central products. The terminology of central products will be used in a restricted sense. We

say that G is a *central product* of its subgroups A and B if A and B commute elementwise and together generate G, *provided also that $A \cap B$ is the centre of (at least) one of the factors A, B.* Routine verifications of this extra condition will be omitted. In most central products we look at, each central factor has cyclic centre, and all automorphisms of this centre are restrictions of automorphisms of the whole factor. All central products formed from one family of such factors (subject, of course, to the extra proviso above) are isomorphic. Only in this case do we write $A \curlyvee B$ for a representative of the well-defined isomorphism class of central products of A and B.

THEOREM 1. *If G is a finite p-group with $Z(\Omega_1(C_G(\Phi(G))))$ cyclic, then*

$$G = G_0 \curlyvee G_1 \curlyvee \dots \curlyvee G_s$$

where G_0 is cyclic, dihedral, semidihedral, or generalized quaternion; $G_1, \dots, G_s$ are nonabelian groups of order p^3, of exponent p for p odd and dihedral for $p=2$; and $|G_0|>2$ if $s>0$.

REMARKS. (a) It is straightforward to check that every group with such a central decomposition has all its abelian characteristic subgroups cyclic.

(b) It can be shown that G uniquely determines s and the isomorphism type of G_0. We leave this to the reader (but beware of the proof of III.13.8b in [2]).

PROOF. We begin with two familiar facts which will be used repeatedly.

(1) *If $\Phi(C)$ is cyclic and central, then $|C'| \leq p$.* The proof is that of III.13.7a in [2].

(2) *If $|D'| \leq p$, then every nonabelian 2-generator subgroup $\langle x, y\rangle$ is a central factor in D.* For, each of x and y has centralizer of index p in D, so $|D: C_D(\langle x, y\rangle)| \leq p^2$, but $|\langle x, y\rangle : Z(\langle x, y\rangle)| \geq p^2$, and hence

$$D = \langle x, y\rangle C_D(\langle x, y\rangle).$$

Put $C_G(\Phi(G)) = C$; by assumption, $Z(\Omega_1(C))$ is cyclic. As $\Omega_1(Z(C)) \leq Z(\Omega_1(C))$, we get that $\Omega_1(Z(C))$, and hence $Z(C)$, is cyclic. Since $Z(\Phi(G)) \leq Z(C)$ a result of Hobby (III.7.8c in [2]) yields that $\Phi(G)$ is cyclic; so $\Phi(C) \leq \Phi(G) \leq Z(C)$.

A major step is to establish that

(3) $\quad C = C_0 \curlyvee C_1 \curlyvee \dots \curlyvee C_s$

where C_0 is either nonabelian of order 8 or cyclic, and $C_1, \dots, C_s$ are nonabelian groups of order p^3, of exponent p for odd p and dihedral for $p=2$.

If $C = Z(C)$ this is so (with $s=0$); otherwise we have from (1) that $|C'|=p$. Write $C = D \curlyvee E$ with E of largest possible order subject to the restriction that it is a central product of nonabelian groups of order p^3,

each of exponent p for p odd and dihedral for $p=2$; if C has no such decomposition, put $D=C$ and $E=C'$. Observe that $Z(D)$ is cyclic, for $Z(D)=Z(C)$. If D has no noncentral element of order p then D has only one subgroup of order p so (by III.8.2 in [2]) D is cyclic or generalized quaternion: in the latter case $|C'|=2$ forces D to have order 8, and in either case we are done with $D=C_0$ and $E=C_1 \curlyvee \dots \curlyvee C_s$ or $s=0$. Suppose then that x is a noncentral element of order p in D. As $\langle x\rangle\Omega_1(Z(C))$ cannot lie in the cyclic $Z(\Omega_1(C))$, there must be an element of order p in C which does not commute with x; take such an element in the form yz with $y \in D$, $z \in E$. Now $[x, yz] \neq 1$ while $[x, z]=1$, so $[x, y] \neq 1$. Also, $1=(yz)^p=y^p z^p$ so $y^p=z^{-p} \in E^p < E' < C'$; as $|C'|=p$ it follows that $\langle x, y\rangle$ is a nonabelian group of order p^3. For $p=2$ this group is dihedral because $|x|=p$; for $p>2$, it has exponent p, since then $y^p \in E^p=1$. From (2) we know that $\langle x, y\rangle$ is a central factor of D; hence C is the central product of $C_D(\langle x, y\rangle)$ and $\langle x, y\rangle \curlyvee E$, contrary to the maximal choice of E. This completes the proof of (3).

Observe that if $|\Phi(G)|<p$ then $C=G$ and the theorem follows from (3). We have $Z(C)^p < \Phi(G) < Z(C)$. Consider first the case $\Phi(G)=Z(C)$. If $\Phi(G)=G^p$ then $\Phi(G)=\langle g^p\rangle$ for some g in G, but then $g \in C$ so now $Z(C)=\Phi(G)=C^p$ and (3) yields $|\Phi(G)|<p$. The alternative is that $\Phi(G)=$ $=G'>G^p$ and then, of course, p is odd. In this case (3) shows that $|C: Z(C)^p\Omega_1(C)|<p$. On the other hand, $|G/C|<p$ because G/C is isomorphic to an elementary abelian subgroup of the automorphism group of $\Phi(G)$ and that automorphism group is cyclic (see I.13.19 in [2]). Thus $Z(C)^p\Omega_1(C)$ is a normal subgroup of index at most p^2 in G; as such it must contain G' which is now $\Phi(G)$. Therefore $Z(C)=\Phi(G)<\Omega_1(C)$ and again $|\Phi(G)|<p$.

It remains to consider the case $\Phi(G)=Z(C)^p$: say, $Z(C)=\langle g\rangle$, $\Phi(G)=\langle g^p\rangle$. Let $h \in G\backslash C$. Since $\langle g\rangle$ is normal in G and $h^p \in \langle g\rangle$, the subgroup $\langle g, h\rangle$ has a cyclic maximal subgroup $\langle g\rangle$ with $[g^p, h] \neq 1$. On inspecting the list of groups with cyclic maximal subgroups (I.14.9 in [2]) we find that $p=2$ and $\langle g, h\rangle$ is dihedral, semidihedral, or generalized quaternion. In each case, h acts invertingly on $\langle g^2\rangle$, so all elements of $G\backslash C$ act the same way on $\Phi(G)$: thus $|G/C|=2$ and $G=\langle h\rangle C$. Also, as $|g|>8$, in (3) we must have $C_0=\langle g\rangle$. If $s=0$ we are done; otherwise for each i with $1<i<s$ let a_i, b_i be a pair of involutions generating C_i. Since $G'=\langle g^2\rangle$, we have that a_i^h is an involution in the coset $a_i\langle g^2\rangle$, so it is either a_i or $a_i^{b_i}$. After a similar observation concerning b_i^h, we find that there is an element c_i (namely 1 or a_i or b_i or a_ib_i) in C_i such that $a_i^h=a_i^{c_i}$ and $b_i^h=b_i^{c_i}$. Put $h'=hc_1^{-1}c_2^{-1}\dots c_s^{-1}$; then h' centralizes $C_1 \curlyvee C_2 \curlyvee \dots \curlyvee C_s$ and since, like h, it is an element of $G\backslash C$, we have that $\langle g, h'\rangle$ is dihedral, semidihedral, or generalized quaternion (though not necessarily isomorphic to $\langle g, h\rangle$). Thus Theorem 1 holds with $G_0=\langle g, h'\rangle$ and $G_i=C_i$ for $1<i<s$. ||

The main task in determining the structure of p-groups G with $Z(\Phi(G))$ cyclic is to find the directly and centrally indecomposable groups of this kind. Two interesting types come to attention: both are factor groups of

$$\langle a, b, c \mid a^{2^{n+1}} = b^2 = 1,\ a^b = a^{-1+2^n},\ a^c = a^{1+2^n},\ bc = cb \rangle$$

with $n > 1$; one obtains $D^+(2^{n+3})$ by adding the relation $c^2 = 1$, and $Q^+(2^{n+3})$ by adding $c^2 = a^{2^n}$ instead. Of course, the cyclic groups $C(p^m)$ of order p^m, the various nonabelian groups of order p^3, and the nonabelian groups with cyclic maximal subgroups and orders greater than p^3, all make their appearance. The latter also occur as subgroups of the groups mentioned above: just to fix notation, observe that the dihedral group $D(2^{n+2})$ of order 2^{n+2} is $\langle a, bc \rangle$ in $D^+(2^{n+3})$, the semidihedral group $S(2^{n+2})$ of that order is $\langle a, b \rangle$ in either group, and the generalized quaternion group $Q(2^{n+2})$ is $\langle a, bc \rangle$ in $Q^+(2^{n+3})$. The fourth type is $\langle a, c \rangle$ in either group, but it is also needed for odd p: for $m > 1$, put

$$M(p^{m+2}) = \langle a, d \mid a^{p^{m+1}} = d^p = 1,\ a^d = a^{1+p^m} \rangle.$$

One may also note (although this paragraph will not be used in the sequel) that $\langle a \rangle$ is normal and its own centralizer in both groups, and both induce on it the unique fours subgroup of its automorphism group. While D^+ splits over $\langle a \rangle$, Q^+ cannot, on account of the generalized quaternion subgroup $\langle a, bc \rangle$. It is easy to see that if $\langle x \rangle$ is any cyclic subgroup of order 2^{n+1}, other than $\langle a \rangle$, in $Q^+(2^{n+3})$, then $\langle a, x \rangle = \langle a, c \rangle$, and hence that $\langle x \rangle = \langle ac \rangle$: since $\langle ac, bc \rangle$ is also generalized quaternion, Q^+ cannot split over $\langle x \rangle$ either, and so cannot be isomorphic to D^+. It will be a consequence of Theorem 2 that every extension of a cyclic 2-group by a fours group with faithful action is isomorphic to D^+ or Q^+.

THEOREM 2. *If G is a finite p-group with $Z(\Phi(G))$ cyclic, then*

$$G = E \times (G_0 \curlyvee G_1 \curlyvee \dots \curlyvee G_s)$$

where E is elementary abelian, $G_1, \dots, G_s$ are nonabelian of order p^3, of exponent p for p odd and dihedral for $p = 2$, while $G_0 > 1$ if $E > 1$, $|G_0| > 2$ if $s > 0$, and G_0 has one of the following types: cyclic, nonabelian with a cyclic maximal subgroup, $D(2^{n+2}) \curlyvee C(4)$, $\cancel{S(2^{n+2}) \curlyvee C(4),}$ $D^+(2^{n+3})$, $Q^+(2^{n+3})$, $D^+(2^{n+3}) \curlyvee C(4)$ (all with $n > 1$). Conversely, every such group has cyclic Frattini subgroup.

REMARK. It can be shown that G uniquely determines s and the isomorphism types of E and G_0: we leave this to the reader.

The converse part is trivial. Towards the direct statement, Hobby's result (loc. cit.) implies that $\Phi(G)$ is cyclic; this property is conveniently inherited by all subgroups and factor groups. If $\Phi(G) < Z(G)$, we have from (1) and (2) that either G is abelian or it has a 2-generator nonabelian central factor. We show below that

(4) *if H is any nonabelian 2-generator group with cyclic $\Phi(H)$, then either H has a cyclic maximal subgroup or $|H|=p^3$.*

Beyond this, the proof of the case $\Phi(G)<Z(G)$ of Theorem 2 will be left to the reader. (Typical steps are $Q(8)\curlyvee Q(8)\cong D(8)\curlyvee D(8)$, and, for $m>n>1$, $M(p^{m+2})\curlyvee M(p^{n+2})\cong M(p^{m+2})\curlyvee N$ where N is nonabelian of order p^3, with exponent p for odd p and dihedral for $p=2$.)

Towards the case $\Phi(G)\not\leq Z(G)$ we shall prove the following.

(5) *If $\Phi(G)$ is cyclic and noncentral then $p=2$, and if G has no nonabelian central factor of order 8 then G is a central product of an abelian group and a group which is dihedral, semidihedral, generalized quaternion, a $D^+(2^{n+3})$ or a $Q^+(2^{n+3})$.*

The rest will again be left to the reader. It just needs the well known

$$Q(2^{n+2})\curlyvee C(4)\cong D(2^{n+2})\curlyvee C(4), \quad \cong S(2^{n+2})\curlyvee C(4)$$

two results implicit in Theorem 1, namely

$$Q(2^{n+2})\curlyvee Q(8)\cong D(2^{n+2})\curlyvee D(8),$$
$$S(2^{n+2})\curlyvee Q(8)\cong S(2^{n+2})\curlyvee D(8),$$

and the similarly straightforward

$$Q^+(2^{n+3})\curlyvee C(4)\cong D^+(2^{n+3})\curlyvee C(4),$$
$$Q^+(2^{n+3})\curlyvee Q(8)\cong D^+(2^{n+3})\curlyvee D(8).$$

PROOF OF (4). Note that under these assumptions $|H:\Phi(H)|=p^2$. If $\Phi(H)=H^p$ then $\Phi(H)=\langle h^p\rangle$ for some h, and $\langle h\rangle$ is maximal. Thus if H has no cyclic maximal subgroup we must have $H^p<H'=\Phi(H)$, and then $p>2$. As in the second last paragraph of the proof of Theorem 1, we deduce that $|H:C_H(\Phi(H))|<p$, so $C_H(\Phi(H))$ contains some maximal subgroup M of H. Since M is abelian but not cyclic, it is the direct product of $\Phi(H)$ and some group N of order p; let L be a maximal subgroup of H not containing N. Put $\Omega_1(\Phi(H))=P$; then $PN=\Omega_1(M)\lhd H$. Now H/P is the product of the disjoint normal subgroups L/P and PN/P: so it is a 2-generator p-group with a proper direct decomposition and hence abelian. Thus $H'=P$; as we are considering the case $\Phi(H)=H'$, it follows that $|H|=p^3$.

PROOF OF (5). Put $C_G(\Phi(G))=C$; by assumption, $C<G$, and so $|\Phi(G)|>p^2$. If $\Phi(G)\neq G^p$ then $\Phi(G)=G'=\langle[g,h]\rangle$ for some g and h in G; since $|[g,h]|>p^2$, we know from (4) that $\langle g,h\rangle$ has a cyclic maximal subgroup, and then $[g,h]\in\langle g,h\rangle^p$ contradicts $\Phi(G)\neq G^p$. Thus $\Phi(G)=G^p=\langle a^p\rangle$ for some a in G; put $|a|=p^{n+1}$ and note $n>1$. Let h be any element of G outside C; then $\langle a,h\rangle$ has a cyclic maximal subgroup (namely $\langle a\rangle$) and $[a^p,h]\neq 1$, so the list of such groups (I.14.9 in [2]) shows that $p=2$. Now $\langle a\rangle$ is normal in G and $G/\langle a\rangle$ has exponent 2; therefore every nontrivial automorphism induced on $\langle a\rangle$ by G has order 2, so its restriction

to $\langle a^2\rangle$ is trivial or inverting: thus $|G: C|=2$. Put $C_G(a)=A$; as $A<C$ and $\langle a\rangle$ has only one nontrivial automorphism which is trivial on $\langle a^2\rangle$, we have $|C: A|<2$. Put $C_G(h)=B$. Every conjugate of h in G lies in the coset hG' and $G'=\langle a^2\rangle$, so $|G: B|<2^n$; on the other hand, $|\langle a\rangle : \langle a\rangle \cap B|=2^n$, so $\langle a\rangle B=G$. It follows that $C=\langle a\rangle(B\cap C)$ and $\langle a, h\rangle(B\cap C)=\langle h, C\rangle=G$. Observe that $\Phi(B\cap C)<\langle a\rangle \cap B=\langle a^{2^n}\rangle$; so if D is any 2-generator nonabelian subgroup in $B\cap C$ then $|D|=8$. By (1) and (2), such a D would be a central factor in C, so we would have $DC_G(D)>C$: in fact, as $h\in C_G(D)$, we would have $DC_G(D)>\langle h\rangle C=G$, contrary to the assumption that G has no central factor of order 8. Thus $B\cap C$ is abelian. Consequently $B\cap A$ is centralized by $\langle a, h\rangle$ and by $B\cap C$, so $B\cap A<Z(G)$. If $B\cap A=B\cap C$ we have that G is a central product of $\langle a, h\rangle$ and $(B\cap A)$, and we are done. If $B\cap A<B\cap C$ then $|B\cap C: B\cap A|=2$, for we have observed that $a^c=a^{1+2^n}$ for any c in C but not in A: choose such a c from $B\cap C$. Now $B\cap C=\langle c\rangle(B\cap A)$ and $G=\langle a, h\rangle(B\cap C)=\langle a, h, c\rangle(B\cap A)=\langle a, h, c)Z(G)$. Note also that $c^2\in\Phi(G)\cap B=\langle a^{2^n}\rangle$. If $\langle a, h\rangle$ is semidihedral, there is an element b of order 2 (namely h or $a^{2^{n-1}}h$) such that $\langle a, b\rangle=\langle a, h\rangle$. If $\langle a, h\rangle$ is dihedral or generalized quaternion, $\langle a, hc\rangle$ is semidihedral and there is an element b of order 2 (namely hc or $a^{2^{n-1}}hc$) such that $\langle a, b\rangle=\langle a, hc\rangle$. In each case $\langle a, b, c\rangle=\langle a, h, c\rangle$ and $|a|=2^{n+1}$, $b^2=1$, $a^b=a^{-1+2^n}$, $a^c=a^{1+2^n}$, $bc=cb$, while c^2 is 1 or a^{2^n}, so $\langle a, b, c\rangle$ is $D^+(2^{n+3})$ or $Q^+(2^{n+3})$. As $G=\langle a, h, c\rangle Z(G)=\langle a, b, c\rangle Z(G)$, this completes the proof. ||

REFERENCES

1. Hobby, Charles – The Frattini subgroup of a p-group. Pacific J. Math. 10, 209–212 (1960).
2. Huppert, B. – Endliche Gruppen I, (Die Grundlehren der mathematischen Wissenschaften, 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967).
3. Laffey, Thomas J. – Centralizers of elementary abelian subgroups in finite p-groups, J. Alg. 51, 88–96 (1978).
4. Waall, Robert W. van der – On finite p-groups whose commutator subgroups are cyclic. Nederl. Akad. Wetensch. Proc. Ser. A 76=Indag. Math. 35, 342–345 (1973).