ON THE METACYCLIC EPIMORPHIC IMAGES OF FINITE p-GROUPS

Yakov Berkovich

University of Haifa, Israel

ABSTRACT. We prove that if G is a p-group of order $p^m > p^n$, where $n > 3$ for $p = 2$ and $n > 2$ for $p > 2$, then the number of normal subgroups D of G such that G/D is metacyclic of order p^n is a multiple of p, unless G is metacyclic. We also give a very short and elementary proof of the following result: representation groups of nonabelian metacyclic p-groups are metacyclic.

In this note only finite p-groups are considered, where p is a prime. We use standard notation usual for finite p-group theory. Thus, $\mathrm{d}(G)$ is the minimal number of generators of G, $o(x)$ the order of $x \in G$, $\Omega_n(G) = \langle x \in G \mid o(x) \leq p^n \rangle$, $\mho_n(G) = \langle x^{p^n} \mid x \in G \rangle$.

$1°$. In this section we prove the following[1]

THEOREM 1. *Let G be a nonmetacyclic p-group of order p^m and let $n < m$.*

(a) *Let $p = 2$ and $n > 3$. Then the number of normal subgroups D of G, such that G/D is metacyclic of order 2^n, is even.*

(b) *[Ber1, Theorem 6.3] Let $p > 2$ and $n > 2$. Then the number of normal subgroups D of G, such that G/D is metacyclic of order p^n, is a multiple of p.*

The proof of Theorem 1(b) is easy; in contrast, the proof of Theorem 1(a) is fairly involved. Part (b) is included in Theorem 1 for the sake of completeness.

[1]As I know, Theorem 1 is the first nontrivial result on counting epimorphic images of p-groups. Theorem 6.2 in [Ber2] is of the same kind but it is not so deep.

REMARK 2. Let G be a two-generator nonmetacyclic 2-group. Then all epimorphic images of G of order 8 are metacyclic. Since the number of normal subgroups of given index in a 2-group G is odd, it follows that Theorem 1(a) is not true for $n = 3$. As groups of order p^3 and exponent p show, Theorem 1 is not true for $n = 2$.

REMARK 3. Let G be an abelian group of rank 3 and order $p^m > p^3$. Let us check Theorem 1 for $n = m - 1$. Let $D < G$ be of order p. Then G/D is metacyclic if and only if $D \not\leq \Phi(G)$. Since both G and $\Phi(G)$ contain $\equiv 1$ (mod p) subgroups of order p, one can choose D in $\equiv 0$ (mod p) ways.

REMARK 4. Let $G = \langle a, b \mid a^4 = b^4 = c^2 = 1, c = [a, b], [a, c] = [b, c] = 1 \rangle$ be a nonmetacyclic minimal nonabelian group of order 2^5 (G is the unique minimal nonabelian group of order 2^5 and exponent 4). Let us check Theorem 1(a) for $n = 4$. Below we use the following obvious fact: If $X = \langle u, v \rangle$ and $\langle u \rangle \triangleleft X$, then X is metacyclic. Therefore, since $\Omega_1(G) = \Phi(G)$, our group G has no normal cyclic subgroup of order 4. The group G has exactly seven central subgroups of order 2:

$$X_1 = \langle a^2 \rangle, \quad X_2 = \langle b^2 \rangle, \quad X_3 = \langle a^2 b^2 \rangle, \quad X_4 = \langle c \rangle,$$

$$X_5 = \langle a^2 c \rangle, \quad X_6 = \langle b^2 c \rangle, \quad X_7 = \langle a^2 b^2 c \rangle$$

since $E_8 \cong \Omega_1(G) = Z(G)$. Then G/X_i is metacyclic for $i = 4, 5, 6, 7$ and nonmetacyclic for $i = 1, 2, 3$. This assertion is obvious for $i = 1, 2, 4$. Let us consider the case $i = 5$. The subgroup $U = \langle a, c \rangle = \langle a \rangle \times X_5 \triangleleft G$ so $C_4 \cong U/X_5 \triangleleft G/X_5$ and, since a generator of U/X_5 is a member of a minimal basis of the two-generator group G/X_5, it follows that G/X_5 is metacyclic, by what has just been said. Similarly, G/X_6 is metacyclic since $\langle b, c \rangle = \langle b \rangle \times X_6 \triangleleft G$. We have $(ab)^2 = a^2 b^2 c$ so $V = \langle ab, c \rangle = \langle ab \rangle \times X_7 \triangleleft G$ and, as above, G/X_7 is metacyclic and G/X_3 is not metacyclic. For $i = 4, 5, 6, 7$, we have $G/X_i \cong \langle x, y \mid x^4 = y^4 = 1, x^y = x^3 \rangle$; for $i = 1, 2, 3$, we have $G/X_i \cong \langle x, y \mid x^4 = y^2 = z^2 = 1, z = [x, y], [x, z] = [y, z] = 1 \rangle$. Thus, there are exactly four normal subgroups D of G such that G/D is metacyclic of order 2^4, and we have checked Theorem 1(a) in this partial case.

REMARK 5. Let $G = \langle a, b \mid a^{2^m} = b^2 = c^2 = 1, m > 2, c = [a, b], [a, c] = [b, c] = 1 \rangle$ be a nonmetacyclic minimal nonabelian group of order 2^{m+2}. Set $\alpha = a^{2^{m-1}}$; then $\{\langle c\alpha \rangle, \langle \alpha \rangle, \langle c \rangle\}$ is the set of minimal normal subgroups of G. In that case, $G/\langle c \rangle$ and $G/\langle c\alpha \rangle$ are metacyclic and $G/\langle \alpha \rangle$ is not metacyclic.

Let $Sc(G) = \Omega_1(Z(G))$ be the socle of a p-group G. For all i such that $p^i \leq |Sc(G)|$, let Δ_i denote the set of subgroups of order p^i in $Sc(G)$. Let $\mathcal{M}$ be a set of nonidentity normal subgroups of G. Given $H \in \Delta_0 \cup \Delta_1 \cup \Delta_2 \cup \cdots \cup \{Sc(G)\}$, let $\alpha(H)$ denote the number of members of the set $\mathcal{M}$ containing H; obviously, $|\mathcal{M}| = \alpha(\{1\})$. Set $|Sc(G)| = p^t$. We claim that the following identity holds

(see [Ber1, Theorem 6.1]):

$$(1) \qquad |\mathcal{M}| = \sum_{i=1}^{t} (-1)^{i-1} p^{i(i-1)/2} \sum_{H \in \Delta_i} \alpha(H).$$

Indeed, let $D \in \mathcal{M}$ and let $|D \cap \mathrm{Sc}(G)| = p^k$; then $k \geq 1$ since $D > \{1\}$. For natural numbers $u \geq v$, let $\varphi_{u,v}$ denote the number of subgroups of order p^v in the elementary abelian group of order p^u; then $|\Delta_i| = \varphi_{t,i}$, the number of subgroups of order p^i in $\mathrm{Sc}(G)$, the elementary abelian group of order p^t. The subgroup D is counted in the right-hand side of (1) exactly $\sum_{i=1}^{k} (-1)^{i-1} p^{i(i-1)/2} \varphi_{k,i}$ times (indeed, for $i \leq k$, D contains exactly $\varphi_{k,i}$ members of the set Δ_i), and that number equals 1, by Hall's identity (see [Hup, §III.5]). Since the contribution of D in the left-hand side of (1) is also equal 1, we are done. Identity (1), dual to Hall's enumeration principle, is the enumeration principle for counting of normal subgroups. It looks like Hall's enumeration principle. It follows from (1) the following congruence (only this congruence we use in the sequel):

$$(2) \qquad |\mathcal{M}| \equiv \sum_{H \in \Delta_1} \alpha(H) \pmod{p}.$$

To clear our path, we give one simplest application of (2).

REMARK 6. Let G be a noncyclic group of order p^m, $m > 2$ and $1 < n < m$. We claim that the number $\mathrm{c}(G)$ of normal subgroups N of G such that G/N is cyclic of order p^n, is a multiple of p. One may assume that $\mathrm{c}(G) > 0$. First let $n = m - 1$. By assumption, there is a normal subgroup N of order p such that G/N is cyclic. Then G is abelian of type (p^{m-1}, p) so $G = Z \times N$, where Z is cyclic of order $p^{m-1} = p^n$. If $N_1 < G$ is of order p, then G/N_1 is cyclic if and only if $N_1 \not\leq Z$ so $\mathrm{c}(G) = p$. Now let $n < m-1$. In that case, one can use (2) and the same notation as in (2). Let $H \in \Delta_1$. Suppose that G/H is cyclic; then G is abelian of type (p^{m-1}, p). The group G contains exactly $p+1$ subgroups of index p^n. If N is one of such subgroups, then G/N is cyclic if and only if $N \not\leq \Phi(G)$ so, since $\Phi(G)$ is cyclic, we get $\mathrm{c}(G) = p$. Next we assume that G is not abelian of type (p^{m-1}, p); then G/H is not cyclic for all $H \in \Delta_1$, therefore, by induction on m, we get $\alpha(H) \equiv 0 \pmod{p}$ so $\mathrm{c}(G) \equiv 0 \pmod{p}$, by (2).

REMARK 7. Let G be a group of order p^m and $p^n \leq |G : G'|$. We claim that then the number $\nu(G)$ of $N \triangleleft G$ such that G/N is nonabelian of order p^n is a multiple of p. One may assume that G is nonabelian and $\nu(G) > 0$; then $n \geq 3$. The number of normal subgroups of given index in G is $\equiv 1 \pmod{p}$ (Sylow). If $N \triangleleft G$ has index p^n, then G/N is nonabelian if and only if $G' \not\leq N$. Therefore, $\nu(G) \equiv 0 \pmod{p}$ (Sylow again; here we did not use (2)). It follows that if a 2-group G of order $2^m > 2^3$ is not of maximal class, then the number of $N \triangleleft G$ such that G/N is nonabelian of order 2^3 is even.

Indeed, we get $|G : G'| \geq 2^3$, by Taussky's theorem, and our claim follows from what has just been proved. Thus, [Ber1, Theorem 6.2] also holds for $p = 2$ and $n = 3$.

In Lemma 8 we gathered some known results which we use in what follows.

LEMMA 8.   (a) (Huppert; see [Ber2, Corollary 13]) *A p-group G, $p > 2$, is metacyclic if and only if $|G/\mho_1(G)| \leq p^2$.*
  (b) ([Ber1, Theorem 3.4]) *A 2-group G is metacyclic if and only if $G/\mho_2(G)$ is metacyclic.*[2]
  (c) ([Ber2, Theorem 2]) *If a nonabelian p-group G is nonmetacyclic and R is a proper G-invariant subgroup of G', then G/R is also nonmetacyclic.*
  (d) ([Tua]; see also the proof of [Isa2, Lemma 12.12]) *Let U be an abelian normal subgroup of a group G and $G/U = \langle xU \rangle$ is cyclic. Then $G' \cong U/C_U(x)$.*

Note that Lemma 8(c) is equivalent to known result of Blackburn [Bla1, Theorem 2.3] (the proof of that result, presented in [Bla1], is due to Philip Hall). Lemma 8(b) follows from Lemma 8(c).

This note is self contained modulo Lemma 8.

Now we are ready to prove Theorem 1.

PROOF OF THEOREM 1. Let $\mathcal{M}$ be the set of all normal subgroups D of G such that quotient group G/D is metacyclic of order p^n. One may assume that the set $\mathcal{M}$ is not empty. As above, in (1), $\alpha(H)$ denotes the number of members of the set $\mathcal{M}$ containing $H \in \Delta_1$.

A. Here we consider the most difficult case $n = m - 1$; then $\mathcal{M} \subseteq \Delta_1$. We have to prove that $|\mathcal{M}|$ is a multiple of p, or, what is the same, $|\Delta_1 - \mathcal{M}| \equiv 1 \pmod{p}$ since $|\Delta_1| \equiv 1 \pmod{p}$. In view of (2), we have to prove that

$$(3) \qquad (|\mathcal{M}| \equiv) \sum_{H \in \Delta_1} \alpha(H) \equiv 0 \pmod{p}.$$

If G is abelian, then $d(G) = 3$ since $\mathcal{M} \neq \emptyset$, and the result follows, by Remark 3. In what follows we assume that G is nonabelian.

(i) Let $p > 2$. Since G is not metacyclic, $|G/\mho_1(G)| \geq p^3$ (Lemma 8(a)). Take $D \in \mathcal{M}$; then G/D is metacyclic. Assuming that $|G/\mho_1(G)| \geq p^4$, we conclude that $G/D\mho_1(G)$ is of order $\geq p^3$ and exponent p so nonmetacyclic, a contradiction since $G/D\mho_1(G)$ is an epimorphic image of the metacyclic group G/D. Thus, $|G/\mho_1(G)| = p^3$. Let $U \in \Delta_1 - \mathcal{M}$; then G/U is not

---

[2]Given a p-group, set $\mho^2(G) = \mho_1(\mho_1(G))$. It follows from $\exp(G/\mho^2(G)) \leq p^2$ that $\mho_2(G) \leq \mho^2(G)$. Let G be a 2-group such that $G/\mho^2(G)$ is metacyclic. Let M be maximal in G. Then $\mho^2(G) = \mho_1(\mho_1(G)) = \Phi(\Phi(G)) < \Phi(M) < M$ so $d(M) = d(M/\mho^2(G)) \leq 2$. Since, obviously, $d(G) \leq 2$, it follows that G is metacyclic [Ber1, Theorem 3.3]. This improves Lemma 8(b).

metacyclic so $|(G/U)/\mho_1(G/U)| \geq p^3$ (Lemma 8(a)). If W is the inverse image of $\mho_1(G/U)$ in G, then G/W is of order $\geq p^3$ and exponent p so $W = \mho_1(G)$ since $|G/\mho_1(G)| = p^3$, and we get $U \leq \mho_1(G)$. Thus, all members of the set $\Delta_1 - \mathcal{M}$ are contained in $\mho_1(G)$. Conversely, if $V \in \Delta_1$ is contained in $\mho_1(G)$, then G/V is not metacyclic since its epimorphic image $G/\mho_1(G)$ is not metacyclic. Thus, $|\Delta_1 - \mathcal{M}|$ equals the number of those members of the set Δ_1 that are contained in $\mho_1(G)$. By Sylow, the last number is $\equiv 1 \pmod{p}$ so $|\mathcal{M}| \equiv |\Delta_1| - 1 = \varphi_{t,1} - 1 \equiv 0 \pmod{p}$, completing this case.

(ii) Let $p = 2$. Here we have to consider the nonmetacyclic quotient group $G/\mho_2(G)$ (see Lemma 8(b)), whose order is at least 2^4 since its exponent equals 4.

Assume that $|G/\mho_2(G)| = 2^4$. Then $\mho_2(G) > \{1\}$ since, by hypothesis, $m > n \geq 4$. The number of members of the set Δ_1 contained in $\mho_2(G)$, is odd (Sylow). Therefore, if all members of the set $\Delta_1 - \mathcal{M}$ are contained in $\mho_2(G)$, then $|\mathcal{M}|$ is even since $|\Delta_1|$ is odd, so, in what follows, we may assume that there is $U \in \Delta_1 - \mathcal{M}$ such that $U \not\leq \mho_2(G)$; then $\bar{G} = G/U$ is not metacyclic. It follows from Lemma 8(b) again, that $\bar{G}/\mho_2(\bar{G})$ is not metacyclic so its order is $\geq 2^4$. Write $\bar{H} = \mho_2(\bar{G})$; then $G/H(\cong \bar{G}/\bar{H})$ is not metacyclic of order $\geq 2^4$ and exponent 4. It follows that $H = \mho_2(G)$ (here we use the assumption that $|G/\mho_2(G)| = 2^4$), contrary to the choice of U: $U \not\leq \mho_2(G)$ and $U \leq H = \mho_2(G)$. Thus, $|G/\mho_2(G)| > 2^4$.

Take $D \in \mathcal{M}$; then $D \not\leq \mho_2(G)$ since the nonmetacyclic group $G/\mho_2(G)$ cannot be an epimorphic image of the metacyclic group G/D. We claim that $|G/\mho_2(G)| \leq 2^5$. Indeed, $G/D\mho_2(G)$, as an epimorphic image of (metacyclic) G/D and $G/\mho_2(G)$ (of exponent 4), is metacyclic of exponent 4 so its order $\leq 2^4$, and our claim follows since $D\mho_2(G) = D \times \mho_2(G)$, by the choice of D. Combining this with the result of the previous paragraph, we conclude that $|G/\mho_2(G)| = 2^5$. Since G/D is metacyclic, we have $|\mathrm{Sc}(G/D)| \leq 2^2$ so $|\mathrm{Sc}(G)| \leq |D||\mathrm{Sc}(G/D)| = 2^3$, and we conclude that $|\Delta_1| \in \{1, 3, 7\}$.

Since $|\Delta_1|$ is odd, to complete this case, it suffices to show that the number $|\Delta_1 - \mathcal{M}|$ is also odd. Let $D \in \mathcal{M}$; then G/D is metacyclic so D is not contained in G' (Lemma 8(c)) and hence G' is of index 2 in $DG' = D \times G'$. It follows that G' is cyclic since $G' \cong (G/D)'$.

Suppose that $\mathrm{d}(G) > 2$. If $D \in \mathcal{M}$, then $\mathrm{d}(G) = 3$ and $G = D \times M$ since $D \not\leq \Phi(G)$; here $M \cong G/D$ is a metacyclic maximal subgroup of G. If $|M \cap \mathrm{Sc}(G)| = 2$, then $|\mathrm{Sc}(G)| = 4$, $|\Delta_1| = 3$ and $|\mathcal{M}| = 2$ since there are exactly two members of the set Δ_1 not contained in M (both these members are directly complemented by M and form the set $\Delta_1 - \{D\}$). Now let $|M \cap \mathrm{Sc}(G)| = 4$; then $|\mathrm{Sc}(G)| = 8$. Take $U \in \Delta_1$. If $U < M$, then $G/U = (M/U) \times (DU/U)$ is not metacyclic (otherwise, M is abelian and so is G), and we get $U \notin \mathcal{M}$. If U is not contained in M, then $G = U \times M$ and $U \in \mathcal{M}$ since M is metacyclic. In that case, $|\mathcal{M}| = 4$.

In what follows, we assume that $\mathrm{d}(G) = 2$.

Let $D \in \mathcal{M}$ again. Set $\bar{G} = G/D$ and $\bar{H} = \mho_2(\bar{G})$. Since $G/D\mho_2(G)$ is metacyclic of order 16, we get $H = D\mho_2(G) = D \times \mho_2(G)$. Thus, for all $D \in \mathcal{M}$, we have $|\bar{G}/\mho_2(\bar{G})| = 2^4$ since $|G/\mho_2(G)| = 2^5$.

Suppose that $\mho_2(G) = \{1\}$; then G is nonmetacyclic of order 2^5 and exponent 4. It follows from $\mathrm{d}(G) = 2$ that G/G' is abelian of type $(4,2)$ or $(4,4)$. If $|G'| = 2$, then G is minimal nonabelian such as in Remark 4. Indeed, if $x, y \in G$, then, since $\mathrm{cl}(G) = 2$, we get $[x, y^2] = [x, y]^2 = 1$ so $\Phi(G) = \mho_1(G)G' \leq \mathrm{Z}(G)$ and, since $\Phi(G) = \mathrm{Z}(G)$ has index 4 in G, our claim follows. In that case, $|\mathcal{M}| = 4$ is even (Remark 4). It remains to consider the case $|G'| = 4$ (indeed, by Taussky's theorem, $|G : G'| > 4$ since G is not of maximal class: G is not metacyclic). By Lemma 8(c), all members of the set $\mathcal{M}$ are not contained in G'. As we have been established above, the derived subgroup G' is cyclic so it contains exactly one member of the set $\Delta_1 - \mathcal{M}$ (Lemma 8(c)). Now suppose that $V \in \Delta_1$ is not contained in G' (if V does not exist, we are done since then $\Delta_1 = \{\Omega_1(G')\}$). In that case, $|(G/V)'| = |G'| = 4$ hence $|(G/V) : (G/V)'| = 4$, and so, by Taussky's theorem, G/V is of maximal class. In that case, $\exp(G) \geq \exp(G/V) = 8 > 4 = \exp(G)$, a contradiction. Thus, if $\mho_2(G) = \{1\}$, then $\Delta_1 = \{\Omega_1(G')\}$ and $G/\Omega_1(G')$ is nonmetacyclic (Lemma 8(c)) so $|\mathcal{M}| = 0$, contrary to the assumption: $\mathcal{M} \neq \emptyset$.

In what follows we assume that $\mho_2(G) > \{1\}$; then $|G| \geq 2|G/\mho_2(G)| = 2 \cdot 2^5 = 2^6$.

Let $\mathcal{N}_0$ be the set of those members of the set Δ_1 that are contained in $\mho_2(G)$; then $|\mathcal{N}_0|$ is odd (Sylow) and $\mathcal{N}_0 \subseteq \Delta_1 - \mathcal{M}$. One may assume that $\mathcal{N}_0 \subset \Delta_1 - \mathcal{M}$ (otherwise, $|\mathcal{M}| = |\Delta_1| - |\mathcal{N}_0|$ is even, and we are done). In that case, there exists $U_1 \in \Delta_1 - (\mathcal{M} \cup \mathcal{N}_0)$; then $\bar{G} = G/U_1$ is not metacyclic. Write $\bar{H}_1 = \mho_2(\bar{G})$; then $\bar{G}/\bar{H}_1$ is not metacyclic (Lemma 8(b)) so its order is $\geq 2^4$ and, since $U_1\mho_2(G) \leq H_1$ and $U_1 \not\leq \mho_2(G)$, we get $H_1 = U_1 \times \mho_2(G)$ and $|G/H_1| = \frac{1}{2}|G/\mho_2(G)| = \frac{1}{2} \cdot 2^5 = 2^4$. If $V < H_1$ is a member of the set Δ_1, then G/V is nonmetacyclic since its epimorphic image $G/H_1 \cong \bar{G}/\bar{H}_1$ is not metacyclic. Let $\mathcal{N}_1$ be the set of members of the set $\Delta_1 - \mathcal{N}_0$ that are contained in H_1. Then $|\mathcal{N}_0 \cup \mathcal{N}_1| = |\mathcal{N}_0| + |\mathcal{N}_1|$, the number of members of the set Δ_1 contained in H_1, is odd (Sylow). It follows that the number $|\mathcal{N}_1|$ is even since the number $|\mathcal{N}_0|$ is odd. Since $U_1 \in \mathcal{N}_1$, we obtain $|\mathcal{N}_1| \geq 2$ so we get $|\mathcal{N}_0 \cup \mathcal{N}_1| \geq 1 + 2 = 3$. Assuming that $\mathcal{N}_0 \cup \mathcal{N}_1 \subset \Delta_1 - \mathcal{M}$ (otherwise, we are done), we add to the set $\mathcal{N}_0 \cup \mathcal{N}_1$ the set $\mathcal{N}_2$ (of even cardinality > 0) of new members of the set $\Delta_1 - \mathcal{M}$. Indeed, if $U_2 \in \Delta_1 - (\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{M})$, then, writing $H_2 = U_2\mho_2(G)$, we conclude, as above with U_1 and H_1, that G/H_2 is nonmetacyclic of order 2^4. We have $H_1 \cap H_2 = \mho_2(G)$ since $\mho_2(G) \leq H_1 \cap H_2$ has order $\frac{1}{2}|H_i|$, $i = 1, 2$ and H_1, H_2 are distinct, so $\mathcal{N}_2$ is the set of members of the set $\Delta_1 - (\mathcal{N}_0 \cup \mathcal{N}_1)$ contained in H_2 but not in H_1 and $|\mathcal{N}_2| > 0$ is even (if $V_i \in \mathcal{N}_i$, then $V_i\mho_2(G) = H_i$, $i = 0, 1, 2$). Thus, we get $|\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{N}_2| \geq 1 + 2 + 2 = 5$. We claim that then the set $\mathcal{N}_0 \cup \mathcal{N}_1 \cup \mathcal{N}_2$, which contains exactly five members, coincides

with the set $\Delta_1 - \mathcal{M}$. Indeed, otherwise, we can, acting as above, add to that sum-set at least two new members of the set $\Delta_1 - \mathcal{M}$, which is impossible since $|\Delta_1 - \mathcal{M}| \leq 6$: the set $\mathcal{M} \neq \emptyset$ and $|\Delta_1| = 7$. Thus, in any case, the number $|\Delta_1 - \mathcal{M}|$ is odd so that the number $|\mathcal{M}|$ is even, as was to be shown.

B. Now let $n < m - 1$. Here we consider cases $p = 2$ and $p > 2$ together. We proceed by induction on $|G|$. Take $H \in \Delta_1$. If G/H is metacyclic, then $\alpha(H) \equiv 1 \pmod{p}$ (Sylow). However, the number of such H, by part A of the proof, is a multiple of p. Therefore, the contribution of such H in the sum on the right-hand side of formula (2), is a multiple of p. Now let G/H be not metacyclic. Then, by induction, $\alpha(H) \equiv 0 \pmod{p}$. Therefore, the contribution of such H in the sum on the right-hand side of formula (2) is a multiple of p again, Thus, congruence (3) is proven, and this completes the proof.   □

We met, in part A of the proof of Theorem 1, a nonmetacyclic and nonabelian two-generator group, say F, of order 2^4. We claim that then $F = \langle a^4 = b^2 = c^2 = 1, c = [a, b], [a, c] = [b, c] = 1 \rangle$. Indeed, assume that $B < F$ is minimal nonabelian. In that case, $F = B\mathrm{Z}(G)$, by [Ber3, Proposition 19(a)]; then $\mathrm{d}(F) = 3$, a contradiction, Thus, B does not exist so F is minimal nonabelian, and we are done, by Redei's classification of minimal nonabelian p-groups.[3]

Next we state an analogue of Theorem 1(b). Following Blackburn, we call a p-group G *absolutely regular* provided $|G/\mho_1(G)| < p^p$. Absolutely regular 2-groups are cyclic. Absolutely regular p-groups are regular, by Hall's regularity criterion, so that, if G is irregular, then $|G/\mho_1(G)| \geq p^p$ (there are a lot of irregular p-groups G satisfying $|G/\mho_1(G)| = p^p$). Note that if $G/\mathrm{Z}(G)$ is absolutely regular, then G is regular (to prove this, it suffices to use Mann's description of irregular p-groups all of whose proper sections are regular; see [Man] or [Ber5, Theorem 7.5]).

PROPOSITION 9. *Let $m > n > p - 1$. Suppose that a p-group G of order p^m is not absolutely regular. Then the number of normal subgroups D of G, such that G/D is absolutely regular of order p^n, is a multiple of p.*

To prove this, we have to repeat, word for word (using also the results stated in the paragraph preceding the proposition), the proof of Theorem 1(b). The same proof works in the case of the following more general

SUPPLEMENT TO PROPOSITION 9. *Let $1 \leq k \leq p - 1$, $k < n < m$. Suppose that a p-group G of order p^m satisfies $|G/\mho_1(G)| > p^k$. Then the number of normal subgroups D of G such that $|(G/D)/\mho_1(G/D)| \leq p^k$ and $|G/D| = p^n$, is a multiple of p.*

---

[3]If $p > 2$, there exists a nonmetacyclic two-generator group of order p^4 which is not minimal nonabelian: this group must be of class 3.

Let $p > 2$. Putting $k = 2$ in Supplement to Proposition 9, we get Theorem 1(b) (see Lemma 8(a)). However, Theorem 1(b) is not a consequence of Proposition 9. Note that the Supplement also generalizes the result of Remark 6.

If n, m are such as in Theorem 1(a) (Proposition 9), then the group G of order 2^m (of order p^m) is metacyclic (absolutely regular) if and only if the number of normal subgroups D of G such that G/D is metacyclic of order 2^n (absolutely regular of order p^n) is not divisible by 2 (by p). Therefore, one can consider Theorem 1 (Proposition 9) as a characterization of metacyclic 2-groups (absolutely regular p-groups).

$2°$. In this section we prove that representation groups of nonabelian metacyclic p-groups are metacyclic.[4] Let us recall some definitions.

Let G be a finite group. Issai Schur [Sch] (see also [BZ, Chapter 6] and [Kar, Theorem 4.2.7]) has showed that there exists a pair $M < \Gamma$ of finite groups such that

(M1) $M \leq Z(\Gamma) \cap \Gamma'$.

(M2) $\Gamma/M \cong G$.

(M3) If a pair $M_0 \leq \Gamma_0$ satisfies (M1) and (M2), then $|\Gamma| \geq |\Gamma_0|$, or, what is the same, $|M| \geq |M_0|$.

A group M in the Schur's theorem is determined uniquely up to isomorphism (see, for example, [BZ, Chapter 6]) and is called the *Schur multiplier* of G; we write $M = M(G)$. A group Γ satisfying (M1)–(M3), is called a *representation group* of G (in [Kar], this group is termed a *covering group*). In most cases, a group G has > 1 representation groups[5]. In particular, all representation groups of given finite group have the same order. For a comprehensive treatment of questions related to Schur multipliers and representation groups, see fundamental monograph [Kar, Part II].

There is another definition of $M(G)$ in terms of cohomology groups [Kar, Theorem 4.2.6] which is used in most cases to find $M(G)$. But below we use the definition given above.

It follows from Burnside's theorem [Isa1, Theorem 9.13] that if Γ is a representation group of G, then the sets of prime divisors of $|G|$ and $|\Gamma|$ coincide, so that, all representation groups of a p-group are also p-groups. Schur has computed the multiplier of an arbitrary abelian group (see, for example, [Kar, Theorem 10.7.1]). There are few p-groups for which all representation

---

[4]It is not true that all representation groups of abelian p-groups rank 2 are metacyclic. Indeed, if G is abelian of type (p^m, p), $m \geq 1$, then $\Gamma = \langle a, b \mid a^{p^m} = b^p = c^p = 1, c = [a, b], [a, c] = [b, c] = 1 \rangle$ is a nonmetacyclic representation group of G. Moreover, each abelian p-group of rank 2 and order $> p^2$ has a nonmetacyclic representation group.

[5]For example, the dihedral group D_{2^n} of order 2^n has three nonisomorphic representation groups: $D_{2^{n+1}}$, $Q_{2^{n+1}}$, the generalized quaternion group of order 2^{n+1}, and $SD_{2^{n+1}}$, the semidihedral group of order 2^{n+1}; see below.

groups are known (however, Schur gave an upper estimate for the number of representation groups of an abelian p-group; see [Kar, Theorem 4.4.4]).

With such small prerequisites, we are ready to prove the following

THEOREM 10. *Let G be a nonabelian metacyclic p-group. Then all representation groups of G are also metacyclic.*[6]

PROOF. If Γ is a representation group of G, then there is in $Z(\Gamma) \cap \Gamma'$ a subgroup $M \cong M(G)$ such that $\Gamma/M \cong G$. Since G is nonabelian, we get $M < \Gamma'$. Since $\Gamma/M \cong G$ is metacyclic, it follows that Γ is also metacyclic (Lemma 8(c)). □

According to Isaacs' letter on January 10, 2006, he also proved Theorem 10. His proof is based on the following

LEMMA 11 (Isaacs). *Let G be a p-group and let $Z < G'$ be G-invariant of order p. If G/Z is metacyclic, then G is metacyclic.*

PROOF. Let U be normal in G with U/Z cyclic and G/U cyclic. Note that $|U/Z| > p$ since G/Z is not abelian. We want to show that U is cyclic. Otherwise, U has a subgroup W of order p and different from Z.

Now let $\langle xU \rangle = G/U$. Since U is abelian and normal in G and G/U is cyclic, we see that $G' = [U, x]$ is isomorphic to $U/C_U(x)$ (Lemma 8(d)). But Z is contained in $C_U(x)$ and U/Z is cyclic, and hence G' is cyclic as an epimorphic image of U/Z. Since Z is in cyclic subgroup G', we see that W is not in G'. Thus WZ/Z is not contained in G'/Z. But WZ/Z is the unique subgroup of order p in U/Z, and it follows that G'/Z intersects U/Z trivially. But G/U is abelian, so $G' < U$, and thus G'/Z is trivial, contrary to noncommutativity of G/Z. □

It appears that lemmas 8(c) and 11 are equivalent (however, their proofs are based on different ideas). Indeed, Lemma 11 follows from Lemma 8(c) immediately. Now, assuming that Lemma 11 holds, we deduce Lemma 8(c). To this end, we use induction on $|G|$. Let R be a G-invariant subgroup of index p in G'. Assuming that G/R is metacyclic, we want to prove that G is also metacyclic. Let $Z \leq R$ be a G-invariant subgroup of order p. Write $\bar{G} = G/Z$. Since $|\bar{G}| < |G|$, $\bar{G}$ is metacyclic, by induction in $\bar{G}$. In that case, G is metacyclic, by Lemma 11. In particular, the Isaacs' proof is the third one of [Bla1, Theorem 2.3] (the first proof, due to Hall, is reproduced in [Bla1], the second proof is presented in [Ber2, Theorem 2]).

The fact that Schur multipliers of metacyclic p-groups are cyclic, is known, their orders are also computed (the proof of this is fairly involved and uses a nontrivial cohomological machinery; see [Kar, Theorem 10.1.25]). It seems that the main assertion of Theorem 10 on representation groups is new.

---

[6]In particular, $M(G)$, the Schur multiplier of G, is cyclic.

It follows from Theorem 10 that representation groups of dihedral group of order 2^n coincide with three 2-groups of maximal class and order 2^{n+1}, and Schur multipliers of generalized quaternion and semidihedral groups are trivial. Indeed, if G is one of our groups of order 2^n and Γ of one of its representation groups, then $|\Gamma : \Gamma'| = 4$, and our claim follows from Taussky's theorem and the classification of 2-groups with cyclic subgroup of index 2. The same result follows from Theorem 10, without appealing to Taussky's theorem. Indeed, by Theorem 10, Γ is metacyclic so Γ' is cyclic of index 4 in Γ. However, $\Gamma' = \Phi(\Gamma) = \mho_1(\Gamma)$ so Γ has a cyclic subgroup of index 2.

Let $G = \mathrm{M}_{p^n} = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle$, where $n > 2$ and $n > 3$ for $p = 2$. We claim that $\mathrm{M}(G) = \{1\}$. Indeed, let Γ be a representation group of G and let $M \leq \Gamma' \cap \mathrm{Z}(\Gamma)$ be such that $M \cong \mathrm{M}(G)$ and $\Gamma/M \cong G$. Then Γ/M contains two distinct cyclic subgroups A/M and B/M of index p. Obviously, A and B are abelian, and so $A \cap B = \mathrm{Z}(\Gamma)$, hence $|\Gamma : \mathrm{Z}(\Gamma)| = p^2$, and we conclude that Γ is minimal nonabelian. Then $|\Gamma'| = p$ so $M = \{1\}$ since $M < \Gamma'$.

PROBLEM 1. Let G be a group of order p^m, $m > n \geq 3$. Find all possible numbers of normal subgroups N of G such that G/N is of maximal class and order p^n.[7]

PROBLEM 2. Let G be a group of order p^m, $m > n = 2k+1 > 3$. Find all possible numbers of normal subgroups N of G such that G/N is extraspecial of order p^n. (For $k = 1$, see Remark 7.)

PROBLEM 3. Describe the representation groups of abelian p-groups.

PROBLEM 4. Describe Schur multipliers and representation groups of (a) nonmetacyclic minimal nonabelian p-groups, (b) p-groups of maximal class. Describe the representation groups of extraspecial p-groups (multipliers of extraspecial p-groups are described; see [Kar, Theorem 11.8.23]).

REFERENCES

[Ber1] Y. Berkovich, *On subgroups and epimorphic images of finite p-groups*, J. Algebra **248** (2002), 472-553.
[Ber2] Y. Berkovich, *Short proofs of some basic characterization theorems of finite p-group theory*, Glas. Mat. Ser. III **41(61)** (2006), 239-258.
[Ber3] Y. Berkovich, *On abelian subgroups of p-groups*, J. Algebra **199** (1998), 262-280.
[Ber4] Y. Berkovich, *Alternate proofs of some basic theorems of finite group theory*, Glas. Mat. **40(60)** (2005), 207-233.

---

[7] For $n > p+1$, see [Ber1, Theorem 6.2]. For $p = 2$ and $n = 3$, see Remark 7. Obviously, the solution of this problem depends on the structure of all representation groups of G.

[Ber5] Y. Berkovich, *Groups of Prime Power Order, Part I*, in preparation.

[BZ]   Ya. G. Berkovich and E. M. Zhmud, Characters of Finite Groups, Part 1, American Mathematical Society, Providence, 1998.

[Bla1] N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. **54** (1958), 327-337.

[Bla2] N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. (3) **11** (1961), 1-22.

[Hup]   B. Huppert, Endliche Gruppen. I, Springer-Verlag, Berlin-New York, 1967.

[Isa1] I. M. Isaacs, Algebra. A Graduate Course, Brooks/Cole Publishing Co., Pacific Grove, 1994.

[Isa2] I. M. Isaacs, Character Theory of Finite Groups, Academic Press, New York-London, 1976.

[Kar]   G. Karpilovsky, Group Representations, Vol. 2, North-Holland Publishing Co., Amsterdam, 1993.

[Man]   A. Mann, *Regular p-groups*, Israel J. Math **10** (1971), 471-477.

[Sch]   I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **127** (1904), 20-50.

[Tua]   H. F. Tuan, A *theorem about p-groups with abelian subgroups of index p*, Acad. Sinica Science Record **3** (1950), 17-23.

Y. Berkovich
Department of Mathematics
University of Haifa
Mount Carmel, Haifa 31905
Israel
E-mail: `berkov@math.haifa.ac.il`