THE NUMBER OF SUBGROUPS OF GIVEN ORDER IN A METACYCLIC *p*-GROUP

YAKOV BERKOVICH University of Haifa, Israel

ABSTRACT. This note was inspired by A. Mann's letter [M1] at June 28, 2009, in which the number of subgroups of given order in a metacyclic p-group for odd primes p was computed. Below we present another proof of that result. The offered proof is extended to so called quasi-regular metacyclic 2-groups. In Sec. 2 we compute the number of cyclic subgroups of given order in metacyclic 2-groups. In Sec. 3 we complete computation of the number of subgroups of given order in metacyclic 2-groups with small minimal nonabelian subgroups or sections.

Recall that a group G is said to be *metacyclic* if it contains a normal cyclic subgroup N such that G/N is cyclic. In this note we consider finite metacyclic p-groups only.

In the Lemma J we gathered some results which we use in what follows.

LEMMA J. Let G be a nonabelian metacyclic p-group.

- (a) If G is of order 2^4 and exponent 4, then $G \cong \mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle$ is minimal nonabelian and $G' = \langle a^2 \rangle$. All subgroups of order 2 are characteristic in G.
- (b) [B, Proposition 10.19] If G has a nonabelian subgroup of order p^3 , then it is of maximal class (in particular, if p > 2, then $|G| = p^3$).
- (c) If p = 2 and $L \triangleleft G$ is such that G/L is nonabelian of order 8, then L is characteristic in G.
- (d) [B, Theorem 1.2 and Lemma 1.6] There are exactly four series of nonabelian 2-groups with cyclic subgroup of index p: dihedral D_{2^n} , generalized quaternion Q_{2^n} , semidihedral SD_{2^n} , $M_{2^n} = \langle a, b \mid a^{2^{n-1}} =$

²⁰¹⁰ Mathematics Subject Classification. 20D15.

 $Key\ words\ and\ phrases.$ Metacyclic $p\mbox{-}{\rm groups},\ {\rm quasi-regular}\ {\rm metacyclic}\ p\mbox{-}{\rm groups},\ {\rm section},\ {\rm Hall's}\ {\rm enumeration}\ {\rm principle}.$

⁷⁹

 $b^2 = 1, a^b = a^{2^{n-2}+1}, n > 3$. The first three series exhaust 2-groups of maximal class.

(e) $|\Omega_1(G)| \neq p^2$ if and only if p = 2 and G is of maximal class.

Let us prove Lemma J(a). There is in G a normal cyclic subgroup $A = \langle a \rangle$ of order 4 such that G/A is cyclic. If $B = \langle b \rangle \langle G$ is cyclic and such that AB = G, then |B| = 4. Since $|G : C_G(A)| = 2$ and A has only one automorphism $a \to a^3$ of order 2, we obtain $a^b = a^3$ and so G has the same defining relations as in (a). The subgroup $G' = \langle a^2 \rangle$ is characteristic in G. Next, G has exactly three subgroups of order 2: $G' = \langle a^2 \rangle$, $U = \langle b^2 \rangle$ and $V = \langle a^2 b^2 \rangle$, and all these subgroups are central. Since $G/V \cong Q_8$ and G has no cyclic subgroup of index 2, it follows that a^2b^2 is the unique involution which is non-square in G. It follows that V is characteristic in G, and we conclude that U is also characteristic in G.

Let us prove Lemma J(c). Clearly, $\mathcal{O}_2(G) \leq L$. If $\mathcal{O}_2(G) = L$, it is nothing to prove. Now let $\mathcal{O}_2(G) < L$. Then $|G : \mathcal{O}_2(G)| = 2^4$, so $G/\mathcal{O}_2(G)$ is nonabelian metacyclic of order 2^4 and exponent 4, and the result follows from Lemma J(a).

1. MANN'S THEOREM ON THE NUMBER OF SUBGROUPS OF GIVEN ORDER IN CERTAIN METACYCLIC *p*-GROUPS

Let G be a metacyclic group of order p^n and exponent p^e and let f = n-e. We also write e = e(G) and f = f(G). This notation is also applicable to subgroups and epimorphic images of G.

DEFINITION 1.1. A metacyclic p-group G is said to be quasi-regular provided:

(QR1) If p = 2, then G has no nonabelian sections of order 8. (QR2) If H is a section of G, then $\mathcal{O}_1(H) = \{x^p \mid x \in H\}.$

Sections of quasi-regular *p*-groups are quasi-regular. Metacyclic *p*-groups, p > 2, are quasi-regular ([B, Theorem 7.2(c)]). If G is a quasi-regular (metacyclic) *p*-group of exponent p^e , then

(*)
$$\exp(\Omega_m(G)) \le p^m$$
 for all $m \le e$ and $\{x^p \mid x \in G\} = \mathcal{O}_1(G)$

(the first equality follows from Lemma J(e) and induction). The irregular groups M_{2^n} (see Lemma J(d)) are quasi-regular, but the group \mathcal{H}_2 (see Lemma J(a)) is not quasi-regular.

It is worth while to note that quasi-regular *p*-groups are powerful (see [B, §26]). This is obvious for p > 2. Now let p = 2 and set $\overline{G} = G/\mathcal{O}_2(G)$. We have to prove that \overline{G} is abelian. Assume that this is false. One has $|\overline{G}| \in \{2^3, 2^4\}$. By the definition, $|\overline{G}| \neq 2^3$. Then $G \cong \mathcal{H}_2$ (Lemma J(a)), and so G is not quasi-regular, by the previous paragraph.

Let $s_m(G) s'_m(G)$, $c_m(G)$ be the number of subgroups, noncyclic subgroups, cyclic subgroups of order p^m in G, respectively, and let c, e, f, m, n, tbe positive integers.

The main result of this section is the following

THEOREM 1.2 (Mann [M2] for p > 2). Let G be a quasi-regular metacyclic group of order p^n and exponent $p^e < p^n$, $m \le n$. Set f(G) = f = n - e (so that $f \geq 1$). Then one of the following holds:

- (a) If $m \le f$, then $s_m(G) = \frac{p^{m+1}-1}{p-1}$. (b) If $f < m \le e$, then $s_m(G) = \frac{p^{f+1}-1}{p-1}$. (c) If m > e, then $s_m(G) = \frac{p^{n-m+1}-1}{p-1}$.

As far as I know, this is a unique counting theorem for so wide class of *p*-groups.

Since our proof is inductive, it would be impossible to prove this theorem without previous knowledge of Mann's result obtained in another way.

LEMMA 1.3. Let G be a quasi-regular (metacyclic) group of order p^n and exponent p^e . Given a cyclic $A \leq G$ of order p^e , there is a cyclic $B \leq G$ such that G = AB and $A \cap B = \{1\}$.

PROOF. We use induction on |G|. One may assume that G is nonabelian and f = n - e > 1 (otherwise, either G is abelian or M_{p^m} , and then the assertion is known). In that case, $\mathcal{O}_1(G)$ is noncyclic of exponent p^{e-1} , by (QR2). We have $|A \cap \mathcal{O}_1(G)| = p^{e-1}$ so, by induction, $\mathcal{O}_1(G) = UV$, where $U = A \cap \mathcal{O}_1(G)$, V is cyclic and $U \cap V = \{1\}$. It follows that $A \cap V = \{1\}$. Let $V = \langle v \rangle$. Then, by (QR2), there is $b \in G$ such that $v = b^p$. Set $B = \langle b \rangle$. Then $A \cap B = \{1\}$ and G = AB since |A||B| = |G|.

Note that, for general abelian *p*-groups, cyclic subgroups of maximal order are complemented ([B, Introduction, Exercise 4]). As we see, this property also holds for quasi-regular (metacyclic) p-groups. This is not true, in general, for p = 2. However, it is not true that if p > 2 and $A \triangleleft G$ is cyclic and such that G/A is cyclic, then A is complemented in G. Example: G is abelian of type (p, p^n) , n > 2, and A is a cyclic subgroup of order p^2 not contained in $\Phi(G).$

PROOF OF THEOREM 1.2. One may assume that 1 < m < n (otherwise, the validity of the theorem is checked easily).

If f = 1, then G is either abelian of type (p^e, p) or $G = M_{p^n}$ (see [B, Theorem 1.2]). In both these cases, $s_m(G) = p + 1$, and the same result yield formulas in (a-c). Next we assume that f > 1; then G has no cyclic subgroup of index p.

By Lemma 1.3, G = AB, where A, B < G are cyclic of orders p^e, p^f , respectively, and $A \cap B = \{1\}$. Taking into account that G is quasi-regular and $f \leq e$, we get

(**)
$$|\Omega_k(G)| = p^{2k} \ (k \le f) \text{ and } G/\Omega_f(G) \cong \mathcal{C}_{p^{e-f}} = \mathcal{C}_{p^{n-2f}},$$

where C_{p^k} is cyclic of order p^k .

We have

(1.1)
$$\mathbf{s}_m(G) = \mathbf{s}'_m(G) + \mathbf{c}_m(G).$$

If $H \leq G$ is noncyclic, then $\Omega_1(G) \leq H$ since $|\Omega_1(G)| = p^2 = |\Omega_1(H)|$ (Lemma J(e)), and so

(1.2)
$$s'_m(G) = s_{m-2}(G/\Omega_1(G)).$$

Therefore, one can rewrite (1.1) as follows:

(1.3)
$$s_m(G) = s_{m-2}(G/\Omega_1(G)) + c_m(G)$$

(A) We first compute $c_m(G)$ for $m \leq e$ (if m > e, then $c_m(G) = 0$). Since G is quasi-regular, it follows that

(1.4)
$$c_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{p^{m-1}(p-1)}.$$

(i) Suppose that $m \leq f$. Then $|\Omega_m(G)| = p^{2m}$, $|\Omega_{m-1}(G)| = p^{2m-2}$ so that, by (1.4),

(1.5)
$$c_m(G) = \frac{p^{2m} - p^{2m-2}}{p^{m-1}(p-1)} = p^{m-1}(p+1)$$

(ii) Suppose that $f < m \leq e$. By (*), we have

 $|\Omega_m(G)| = p^{2f+m-f} = p^{m+f}$ and $|\Omega_{m-1}(G)| = p^{2f+m-1-f} = p^{m+f-1}$.

Therefore, by (1.4),

(1.6)
$$c_m(G) = \frac{p^{m+f} - p^{m+f-1}}{p^{m-1}(p-1)} = p^f.$$

(B) In view of (1.3), it remains to compute $s_{m-2}(G/\Omega_1(G))$. Here we use induction on m. We have

(1.7)

$$|G/\Omega_1(G)| = p^{n-2}, e_1 = e(G/\Omega_1(G)) = e - 1, f_1 = f(G/\Omega_1(G)) = f - 1.$$

(j) Let $m \le f$; then $m - 2 \le f - 2 < f - 1 = f(G/\Omega_1(G))$. By induction (see part (a) of the statement), $s_{m-2}(G/\Omega_1(G)) = \frac{p^{m-2+1}-1}{p-1} = \frac{p^{m-1}-1}{p-1}$ so that, by (1.3) and (1.5), we get

$$s_m(G) = \frac{p^{m-1} - 1}{p - 1} + p^{m-1}(p + 1) = \frac{p^{m+1} - 1}{p - 1},$$

completing this case.

(jj) Let $f < m \leq e$; then

$$f_1 = f(G/\Omega_1(G)) = f - 1 \le m - 2 \le e - 2 < e - 1 = e(G/\Omega_1(G)) = e_1$$

If $m-2 = f-1(=f_1)$ or, what is the same, m-1 = f, then, by induction (see part (a)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{m-2+1}-1}{p-1} = \frac{p^f-1}{p-1}$$

so, by (1.3) and (1.6), we obtain

$$s_m(G) = p^f + \frac{p^f - 1}{p - 1} = \frac{p^{f+1} - 1}{p + 1},$$

and we are done in this case.

Now let m-2 > f-1 or, what is the same, m > f+1. Then, by induction (see part (b)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{f-1+1}-1}{p-1} = \frac{p^f-1}{p-1},$$

so, by (1.3) and (1.6), we have

$$s_m(G) = p^f + \frac{p^f - 1}{p - 1} = \frac{p^{f+1} - 1}{p - 1},$$

completing case (jj).

(jjj) Now let $m \ge e+1$ or, what is the same, $m-2 \ge e-1 = e(G/\Omega_1(G)) = e_1$. Then $s_m(G) = s_{m-2}(G/\Omega_1(G))$ since all subgroups of G of order p^m are noncyclic so contain $\Omega_1(G)$.

Let
$$m-2 = e-1 = e_1$$
, i.e., $e+1 = m$; then, by induction (see part (b)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{(f-1)+1}-1}{p-1} = \frac{p^f-1}{p-1} = \frac{p^{n-e}-1}{p-1} = \frac{p^{n-m+1}-1}{p-1},$$

and this coincides with formula in (c).

Now let m-2 > e-1, i.e., m > e+1. Then, by induction (see part (c)),

$$s_{m-2}(G/\Omega_1(G)) = \frac{p^{(n-2)-(m-2)+1}-1}{p-1} = \frac{p^{n-m+1}-1}{p-1},$$

and this coincides with formula in (c). The proof is complete.

COROLLARY 1.4 (Mann [M2] for p > 2). If G, n, m, f, e are as in Theorem 1.2, then $s_m(G) = s_{n-m}(G)$.

PROOF. One may assume that 1 < m < n.

(i) Let $m \leq f$; then $n - m \geq n - f = e$.

If n - m = e, then m = n - e = f. We have, by Theorem 1.2(b,a),

$$s_{n-m}(G) = s_e(G) = \frac{p^{f+1} - 1}{p-1} = \frac{p^{m+1} - 1}{p-1} = s_m(G)$$

If n - m > e, then m < n - e = f. We have, by Theorem 1.2(c,a),

$$s_{n-m}(G) = \frac{p^{n-(n-m)+1}-1}{p-1} = \frac{p^{m+1}-1}{p-1} = s_m(G)$$

Y. BERKOVICH

(ii) Let $f < m \le e$; then $f = n - e \le n - m < n - f = e$. If n - m = f, then m = n - f = e. We have, by Theorem 1.2(a,b),

$$s_{n-m}(G) = s_f(G) = \frac{p^{f+1} - 1}{p-1} = s_e(G) = s_m(G)$$

If f < n - m < e, then, by Theorem 1.2(b),

$$s_{n-m}(G) = \frac{p^{f+1} - 1}{p-1} = s_m(G)$$

(iii) Let m > e, then n - m < n - e = f so, by Theorem 1.2(a,c),

$$s_{n-m}(G) = \frac{p^{n-m+1}-1}{p-1} = s_m(G),$$

and the proof is complete.

The group $G = \langle a, b \mid a^4 = b^4 = 1, a^b = a^3 \rangle \cong \mathcal{H}_2$ with n = 4, e = f = 2, is not quasi-regular, however, $s_m(G)$ is such as in Theorem 1.2.

2. The number of cyclic subgroups of given order in a metacyclic 2-group

In this section we find the number of cyclic subgroups of given order in metacyclic 2-group (for p > 2 this was done in 1°). In what follows we suppose that G is a metacyclic group of order 2^{n} . Set

$$w = w(G) = \max\{i \mid |\Omega_i(G)| = 2^{2i}\}$$
 but $|\Omega_{w+1}(G)| \neq 2^{2(w+1)}$

In that case, we write $R(G) = \Omega_w(G)$. Then $|R(G)| = 2^{2w}$ and G/R(G) is either cyclic or a 2-group of maximal class (Lemma J(e)). We retain this notation in what follows.

If w = 0, then either G is cyclic or of maximal class (Lemma J(e)). The maximal subgroups of such G are known. This allows us, using induction and Hall's enumeration principle ([B, Theorem 5.2]; see also (3.1), below), to prove the following known theorem, and this completes case w = 0.

THEOREM 2.1. Suppose that G is a 2-group of maximal class and order $2^n > 2^3$.

A. If n > m > 2, then $c_m(G) = 1$. (a) If $G \cong D_{2^n}$, then $c_1(G) = 2^{n-1} + 1$ and $c_2(G) = 1$. (b) If $G \cong Q_{2^n}$, then $c_1(G) = 1$ and $c_2(G) = 2^{n-2} + 1$. (c) If $G \cong SD_{2^n}$, then $c_1(G) = 2^{n-2} + 1$ and $c_2(G) = 2^{n-3} + 1$. B. We have $s_m(G) = 2^{n-m} + 1$ for $2 \le m < n$.

In what follows w = w(G) is a positive integer and G is metacyclic of order 2^n .

84

THEOREM 2.2. Suppose that R(G) = G; then $|G| = 2^n = 2^{2w}$. In that case, G = AB, where $A \triangleleft G$ and B are cyclic of the same order 2^w and $c_m(G) = 3 \cdot 2^{m-1}$ for all $m \in \{1, \ldots, w\}$.

PROOF. Since G is metacyclic, there is a cyclic $A \triangleleft G$ such that G/A is cyclic. It follows from $\exp(G) = 2^w$ and $|A| \leq 2^w$ that $|G:A| \geq 2^w = \exp(G) = 2^w$ so $|A| = 2^w$. If B < G is cyclic such that AB = G, then $|B| = 2^w$, $A \cap B = \{1\}$, and the first assertion is proven.

Since $|\Omega_t(G)| = 2^{2t}$ for all non-negative integers $t \leq w$, we get

$$c_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{2^{m-1}} = \frac{2^{2m} - 2^{2m-2}}{2^{m-1}} = 3 \cdot 2^{m-1},$$

completing the proof.

In view of Theorem 2.2, we suppose in what follows that $\Omega_w(G) = R(G) < G$. By Theorem 2.2, if $m \leq w$, then $c_m(G) = 3 \cdot 2^{m-1}$. Therefore, in the following two theorems we assume that m > w.

THEOREM 2.3. Let G/R(G) is nonidentity cyclic and m > w. Then $c_m(G) = 2^w$.

PROOF. We have

$$|\Omega_m(G)| = 2^{2w + (m-w)} = 2^{w+m}, \ |\Omega_{m-1}(G)| = 2^{2w + (m-1-w)} = 2^{w+m-1}.$$

Therefore,

$$c_m(G) = \frac{|\Omega_m(G) - \Omega_{m-1}(G)|}{2^{m-1}} = \frac{2^{w+m} - 2^{w+m-1}}{2^{m-1}} = 2^w,$$

and the proof is complete.

In what follows we assume that G/R(G) is of maximal class. If L/R(G) < G/R(G) is cyclic of order 2^s , s > 0, then $c_m(L) = 2^w$, by Theorem 2.3. If $L_1/R(G) < G/R(G)$ is another subgroup of order 2^s , then $L \cap L_1$ has no cyclic subgroups of order 2^{w+s} . If L < G is cyclic of order $2^m > 2^w$, then LR(G)/R(G) is cyclic of order 2^{m-w} since $|L \cap R(G)| = 2^w$. Therefore, we get

THEOREM 2.4. Suppose that G/R(G) is a 2-group of maximal class and m > w. Then $c_m(G) = 2^w \cdot c_{m-w}(G/R(G))$.

Since $c_{m-w}(G/R(G))$ is known (Theorem 2.1A), we completed computing $c_m(G)$ if G/R(G) is of maximal class. Thus, the number $c_m(G)$ is computed for all metacyclic 2-groups.

Y. BERKOVICH

3. The number of subgroups of given order in a metacyclic 2-group

In what follows G is a metacyclic 2-group of order 2^n with $R(G) > \{1\}$ or, what is the same, $w \ge 1$. In this section we compute the number $s_m(G)$ of subgroups of order 2^m in G. We first consider a metacyclic 2-group G = R(G)(see the second paragraph of §2).

THEOREM 3.1. If G is a metacyclic 2-group such that $G = R(G), w \ge 1$ (in that case, $|G| = 2^{2w}$), then

- (a) If $m \le w$, then $s_m(G) = 2^{m+1} 1$.
- (b) If $1 \le t \le w$, then $s_{w+t}(G) = 2^{w-t+1} 1$.

PROOF. It is easily checked that the theorem is true for w = 1 and t = w. Next we assume that w > 1 and t < w. As in the proof of Theorem 1.2, formulas (1.1), (1.2) and (1.3) hold. Therefore, in view of Theorem 2.2, it remains to find the number of noncyclic subgroups of order 2^m . If H < G is noncyclic, then $\Omega_1(G) \leq H$ so the number of noncyclic subgroups of order 2^m in G equals $s_{m-2}(G/\Omega_1(G))$.

(a) Suppose that $m \leq w$. In our case, $w' = w(G/\Omega_1(G)) = w - 1$, $|G/\Omega_1(G)| = 2^{2w-2}$. We have m-2 < w-1 = w'. Let H < G be of order 2^m . If H is noncyclic, then the number of such H in G equals $s_{m-2}(G/\Omega_1(G)) = 2^{(m-2)+1} - 1 = 2^{m-1} - 1$, by induction (see the previous paragraph). If H < G is cyclic, then the number of such H equals $c_m(\Omega_m(G)) = 3 \cdot 2^{2m-1}$ (Theorem 2.2) so, by (1.3), we obtain

$$s_m(G) = 3 \cdot 2^{m-1} + (2^{m-1} - 1) = 2^{m+1} - 1,$$

completing the proof of (a).

(b) In what follows we assume that m = w + t, where $1 \le t < m$. Since $\exp(G) = 2^w$, then $\exp(G/\Omega_t(G)) = 2^{w-t}$. If H < G is of order 2^{w+t} , then $\Omega_t(G) < H$ and $|H/\Omega_t(G)| = 2^{w-t}$, and so $s_{w+t}(G) = s_{w-t}(G/\Omega_t(G))$. As we know, $R(G/\Omega_t(G)) = G/\Omega_t(G)$; therefore, using the formula from the previous sentence and (a) for $G/\Omega_t(G)$, we get $s_{w+t}(G) = s_{w-t}(G/\Omega_t(G)) = 2^{w-t+1} - 1$, and the proof is complete.

It is easy to show that the groups of Theorem 3.1 coincide with metacyclic 2-groups G of order 2^{2w} and exponent 2^w . Indeed, if G is metacyclic of order 2^{2w} and exponent 2^w , then G is not of maximal class so $\Omega_1(G)$ is abelian of type (2, 2), by Lemma J(e), and now, by induction, $|\Omega_i(G/\Omega_1(G))| = 2^{2i}$ for all $i \leq m - 1$, and our claim follows.

It follows that the number $s_m(G)$ of Theorem 3.1 is computed by the same formulas as in Theorem 1.2. But 2-groups of these two theorems do not coincide.

A group G = AB of Theorem 3.1 has a noncyclic center. This is a case if one of subgroups A, B, say A, is normal in G since $\Omega_1(A) \leq Z(G)$ and, in view of $|\operatorname{Aut}(A)| = 2^{m-1}$, $\Omega_1(B)$ centralizes A so contained in Z(G). Now suppose that A and B are not normal in G. Then there exists $x \in G - N_G(A)$ such that $A^x \neq A$. By Ore, $AA^x \neq G$ so $A \cap A^x \geq \Omega_1(A) > \{1\}$ for all $x \in G$, by the product formula. It follows that $A_G = \bigcap_{x \in G} A^x > \{1\}$ so $Z(G) \geq \Omega_1(A) > \{1\}$. Similarly, $Z(G) \geq \Omega_1(B) > \{1\}$, and our claim follows since $\Omega_1(A) \times \Omega_1(B) \leq Z(G)$ is noncyclic.

Suppose that a metacyclic 2-group G is such that G/R(G) is nonidentity cyclic and $R(G) > \{1\}$. We claim that then G = AB, where A, B < G are cyclic and $A \cap B = \{1\}$. Indeed, suppose that $\exp(G) = 2^e$ and, as above, $\exp(R(G)) = p^w$; then w < e. Let A < G be cyclic of order 2^e ; then $A \cap R(G)$ is cyclic of order 2^w . By Theorem 2.2, we have $R(G) = (A \cap R(G))B$, where B < R(G) is cyclic of order 2^w and $(A \cap R(G)) \cap B = \{1\}$. It follows that $A \cap B = \{1\}$ so AB = G, by the product formula.

Let $\Gamma_1 = \{A, B, C\}$ be the set of maximal subgroups of a noncyclic metacyclic 2-group G. Then, supposing $2^m < |G|$, we have, by Hall's enumeration principle (see [B, Theorem 5.2]),

(3.1)
$$s_m(G) = s_m(A) + s_m(B) + s_m(C) - 2s_m(\Phi(G)),$$

where $\Phi(G)(=A \cap B \cap C)$ is the Frattini subgroup of G (note that equality (3.1) is easily proved without enumeration principle). If $2^{m+2} = |G| = 2^n$ and G has no cyclic subgroup of index 2, then, by (3.1)

$$s_m(G) = s_{n-2}(G) = 3 \cdot 3 - 2 \cdot 1 = 7 = 2^3 - 1 = 2^2 + 3,$$

(we shall use freely this fact in what follows). Next we retain the notation introduced in this paragraph.

Now we compute $s_m(G)$ for the case where G/R(G) is nonidentity cyclic. The following lemmas will help us to state the inductive hypothesis. If $m \leq w$, then $s_m(G) = s_m(R(G))$, and this number is computed in Theorem 3.1(a). Therefore, in what follows we consider case m > w only.

LEMMA 3.2. Suppose that G is a metacyclic 2-group such that |G/R(G)| = 2. If $1 \le t \le w+1$, then $s_{w+t}(G) = 2^{w-t+2} - 1$.

PROOF. If t = w + 1, then w + t = 2w + 1 = n, where $2^n = |G|$; then $s_{w+t}(G) = s_n(G) = 1 = 2^{w-(w+1)+2} - 1$, as in the statement. Next we assume that t < w + 1. We have $\exp(G) = 2^{w+1}$. If w = 1, then t = 1, G is abelian of type (4, 2) (indeed, if G is nonabelian of order 8, then $|\Omega_1(G)| \neq 4$), and so

$$s_{w+t}(G) = s_2(G) = 3 = 2^2 - 1 = 2^{1-1+2} - 1,$$

as in the statement. Next we also assume that w > 1.

In view of Theorem 3.1, $s_{w+t}(R(G)) = 2^{w-t+1} - 1$ so it suffices to find the number of subgroups H < G of order 2^{w+t} such that $H \leq R(G)$. Let Hbe such a subgroup; then $\exp(H) = 2^{w+1} = \exp(G)$. If H is cyclic, then m = w + 1 so t = 1, hence the number of such H is equal to $c_{w+1}(G) = 2^w$ (Theorem 2.3), and we get

$$s_{w+1}(G) = s_{w+1}(R(G)) + c_{w+1}(G) = (2^{w-1+1} - 1) + 2^w = 2^{w+1} - 1,$$

completing this case. Next we assume that $|H| = 2^{(w+1)+t}$, where 0 < t < w. In that case, H is noncyclic and $\Omega_t(G) < H$.

Suppose that $H \not\leq R(G)$. Since $\exp(H) = 2^{w+1} = \exp(G)$, then $H/\Omega_t(G)$ is of order $2^{w+t+1-2t} = 2^{w-t+1}$ and exponent 2^{w-t+1} hence $H/\Omega_t(G)$ is cyclic. We have $w(G/\Omega_t(G)) = w - t$. The number of such H equals $c_{w-t+1}(G/\Omega_t(G)) = 2^{w-t}$ (Theorem 2.3). Since $s_{w+1+t}(R(G)) = 2^{w-(t+1)+1} - 1 = 2^{w-t} - 1$ (Theorem 3.1(b)), we obtain

$$f_{w+t+1}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing t + 1 by t in the last equality, we get $s_{w+t}(G) = 2^{w-t+2} - 1$, as required.

LEMMA 3.3. Suppose that a metacyclic 2-group G is such that G/R(G) is cyclic of order 4.

- (a) $s_{w+1}(G) = 2^{w+1} 1.$
- (b) If $2 \le t \le w+2$, then $s_{w+t}(G) = 2^{w-t+3} 1$.

PROOF. (a) By Lemma 3.2,

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1$$

and (a) is proven.

(b) If t = w + 2, then $2^{w+t} = |G|$ so $s_{w+(w+2)}(G) = s_n(G) = 1 = 2^{w-(w+2)+3} - 1$. If t = w + 1, then $s_{w+t}(G) = s_{n-1}(G) = 3 = 2^2 - 1 = 2^{w-(w+1)+3} - 1$. Next we assume that t < w + 1. If w = 1, then $|G| = 2^4$ has cyclic subgroup of index 2, t = 2 (by hypothesis), $s_{1+t}(G) = s_3(G) = 3 = 2^2 - 1 = 2^{1-2+3} - 1$, and this coincides with the required result. Next we assume that w > 1.

Set $U = \Omega_{w+1}(G)$; then |U : R(G)| = 2 = |G : U|. Since $s_{w+t}(U) = 2^{w-t+2} - 1$ (Lemma 3.2), it suffices to compute the number of H < G of order 2^{w+t} such that $H \not\leq U$. Let H be such a subgroup. Then $\exp(H) = 2^{w+2} = \exp(G)$. If H is cyclic, then $|H| = 2^{w+2}$ (in that case, t = 2), and so the number of such H equals $c_{w+2}(G) = 2^w$ (Theorem 2.3), and we get

$$s_{w+2}(G) = c_{w+2}(G) + s_{w+2}(U) = 2^w + (2^{w-2+2} - 1) = 2^{w+1} - 1 = 2^{w-2+3} - 1,$$

and this coincides with the required result for t = 2 (note that if t = 2 and $H \leq U$, then H is cyclic).

Now let $|H| = 2^{(w+2)+t}$, where 0 < t < w. Then H is noncyclic of exponent $2^{w+2} = \exp(G)$, $\Omega_t(G) < H$ and $H/\Omega_t(G)$ is cyclic of order $2^{(w+t+2)-2t} = 2^{w-t+2}$ (cyclic since $|H/\Omega_t(G)| = \exp(H/\Omega_t(G))$. Since $\exp(R(G/\Omega_t(G)) = 2^{w-t}$, the number of such H equals $c_{w-t+2}(G/\Omega_t(G)) =$ 2^{w-t} (Theorem 2.3). Since $s_{w+t+2}(U) = 2^{w-(t+2)+2} - 1 = 2^{w-t} - 1$ (Lemma 3.2), we get

$$s_{w+t+2}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the last equality t + 2 by t, we get $s_{w+t}(G) = 2^{w-t+3} - 1$, and the proof is complete.

LEMMA 3.4. Suppose that G is a metacyclic 2-group such that G/R(G) is cyclic of order 2^3 , w > 0.

- (a) If t = 1, then $s_{w+1}(G) = 2^{w+1} 1$.
- (b) If t = 2, then $s_{w+2}(G) = 2^{w+1} 1$.
- (c) If $3 \le t \le w+3$, then $s_{w+t}(G) = 2^{w-t+4} 1$.

PROOF. (a) and (b) follow from Lemmas 3.2 and 3.3, respectively. Indeed, if t = 1, then, by Lemma 3.2,

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1.$$

Now let t = 2. Then, by Lemma 3.3,

$$s_{w+2}(G) = s_{w+2}(\Omega_{w+2}(G)) = 2^{w-2+3} - 1 = 2^{w+1} - 1.$$

Next we assume that $3 \le t \le w + 3$.

(c) One may assume that t < w + 3. If w = 1, then t = 3, by hypothesis, G has a cyclic subgroup of index 2 so $s_{1+3}(G) = 3 = 2^{1-3+4} - 1$. Set $U = \Omega_{w+2}(G)$.

Let H < G be of order 2^{w+3} . Since $s_{w+3}(U) = 2^{w-3+3} - 1 = 2^w - 1$ (Lemma 3.3), it suffices to count the number of H such that $H \not\leq U$. In this case, $\exp(H) = 2^{w+3}$ so H is cyclic; then the number of such H is equal to $c_{w+3}(G) = 2^w$ (Theorem 2.3). We get

$$s_{w+3}(G) = 2^w + (2^w - 1) = 2^{w+1} - 1 = 2^{w-3+4} - 1,$$

and this coincides with the required result for t = 3.

Now suppose that H < G be of order 2^{w+3+t} , where 0 < t < w, $H \not\leq U$. Then $\Omega_t(G) < H$, $H/\Omega_t(G)$ is cyclic of order 2^{w-t+3} . The number of such H equals $c_{w-t+3}(G/\Omega_t(G)) = 2^{w-t}$ since $\exp(R(G/\Omega_t(G))) = 2^{w-t}$ (Theorem 2.3). All such H are not contained in $U = \Omega_{t+2}(G)$ since $\exp(H) = 2^{w+3} > 2^{w+2} = \exp(U)$. Since $s_{w+3+t}(U) = 2^{w-(t+3)+3} - 1 = 2^{w-t} - 1$ (Lemma 3.3), we get

$$s_{w+3+t}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the last equality t + 3 by t, we get $s_{w+t}(G) = 2^{w-t+4} - 1$, completing the proof.

The proofs of the previous three lemmas are similar. Our goal there was to state inductive hypothesis and show as to attain this. In any case, Lemma 3.2 must be proved (it is the basis of induction). Now we are ready to prove the following

THEOREM 3.5. Suppose that G is a metacyclic 2-group of order 2^n such that w > 1 and G/R(G) is cyclic of order 2^c (in this case, n = 2w + c).

(a) If $1 \le t < c$, then $s_{w+t}(G) = 2^{w+1} - 1$.

(b) If $c \le t \le w + c$, then $s_{w+t}(G) = 2^{w-t+c+1} - 1$.

PROOF. We proceed by induction on c.

(i) First we prove (b): as we shall see, (a) follows from (b). Thus, $t \ge c$. As in three previous lemmas, one may assume that t < w + c. Set $U = \Omega_{w+c-1}(G)$; then $\exp(U) = 2^{w+c-1} = \frac{1}{2}\exp(G)$, |G:U| = 2 and U/R(U) = UR(G)/R(G) is cyclic of order $2^{c-1} > 1$.

The theorem holds for c = 1, 2, 3 (Lemmas 3.2–3.4) so one may assume that c > 3. We have $\exp(G) = 2^{w+c}$. By induction,

$$s_{w+t}(U) = 2^{w-t+(c-1)+1} - 1 = 2^{w-t+c} - 1$$

since

$$t > c - 1 = \log_2(|UR(G)/R(G)|)$$

Therefore, it suffices to find the number of those H < G of order 2^{w+t} that are not contained in U. All such H have the same exponent $2^{w+c} = \exp(G)$. If such H is cyclic, then $|H| = 2^{w+c}$ (in this case, t = c), and the number of such H in G is equal to $c_{w+c}(G) = 2^w$ (Theorem 2.3). Therefore, we get

$$s_{w+c}(G) = c_{w+c}(G) + s_{w+c}(U) = 2^w + (2^{w-c+c} - 1) = 2^{w+1} - 1$$

and this coincides with the required result for t = c.

Next we assume that $|H| = 2^{(w+c)+t}$, where 0 < t < w. Then $\Omega_t(G) < H$ and $H/\Omega_t(G)$ is of order $2^{w+c+t-2t} = 2^{w-t+c} = \exp(H/\Omega_t(G))$ hence $H/\Omega_t(G)$ is cyclic. We have

$$s_{w+c+t}(U) = 2^{w-(c+t)+(c-1)+1} - 1 = 2^{w-t} - 1,$$

by induction. Since $R(G/\Omega_t(G)) = R(G)/\Omega_t(G)$ and $\exp(R(G/\Omega_t(G))) = 2^{w-t}$, the number of such H equals $c_{w-t+c}(G/\Omega_t(G)) = 2^{w-t}$ (Theorem 2.3). Therefore,

$$s_{w+c+t}(G) = 2^{w-t} + (2^{w-t} - 1) = 2^{w-t+1} - 1.$$

Replacing in the displayed formula t + c by t, we get $s_{w+t} = 2^{w-t+c+1} - 1$, and the proof of (b) is complete.

(ii) It remains to prove (a); then t < c. In this case, $H < V = \Omega_{w+t}(G)$. The subgroup V/R(G) is cyclic of order 2^t . By part (b), applied to V, we get $s_{w+t}(V) = 2^{w-t+t+1} - 1 = 2^{w+1} - 1$. Since $s_{w+t}(G) = s_{w+t}(V)$, the proof of (a) is complete.

To complete computation of $s_m(G)$, it remains to consider the case where G/R(G) is of maximal class. There are three infinite series of 2-groups of maximal class and order 2^c , unless c = 3 (see Lemma J(d)). Note that all these 2-groups contain a cyclic subgroup of index 2 ([B, Theorem 1.2]). In the notation of (3.1) (namely, $\Gamma_1 = \{A, B, C\}$ is the set of maximal subgroups

of G), we assume in the sequel that C/R(G) is cyclic. These three cases will be covered in Theorems 3.9, 3.11 and 3.12 and supplements to them. In those theorems we consider case w > 1, $t \ge c - 1$. In supplements we consider cases w = 1 and t = 1 separately. In the case under consideration, $R(G) < \Phi(G)$ since d(G/R(G)) = 2 = d(G), where d(G) is the minimal number of generators of G.

The following two lemmas are induction bases for Theorems 3.9 and 3.11, respectively.

LEMMA 3.6. Let G be a metacyclic 2-group of order 2^n such that $G/R(G) \cong \mathbb{Q}_8$ and w+t > w > 1. $1 \le t \le w+3$ (then n = 2w+3).

(a) If t = 1, then $s_{w+1}(G) = 2^{w+1} - 1$.

(b) If $2 \le t \le w+3$, then $s_{w+t}(G) = 2^{w-t+4} - 1$.

PROOF. If t = w + 3, then w + t = n so $s_{w+t}(G) = 1 = 2^{w-(w+3)+4} - 1$, as in (b). If t = w + 2, then w + t = n - 1 so $s_{w+t}(G) = 3 = 2^2 - 1 = 2^{w-(w+2)+4} - 1$, as in (b). In what follows we assume that t < w + 2.

We have $R(A) = R(B) = R(C) = R(\Phi(G)) = R(G)$ and the quotient groups A/R(G), B/R(G) and C/R(G) are cyclic of order 4, $|\Phi(G)/R(\Phi(G))| = 2$.

If t = 1, then, by Lemma 3.2,

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = s_{w+1}(\Phi(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1,$$

and the proof of (a) is complete.

Now let t > 1. Then

$$s_{w+t}(A) = s_{w+t}(B) = s_{w+t}(C) = 2^{w-t+3} - 1$$
 (Lemma 3.3),
 $s_{w+t}(\Phi(G)) = 2^{w-t+2} - 1$ (Lemma 3.2)

so, by (3.1),

$$s_{w+t}(G) = 3 \cdot (2^{w-t+3} - 1) - 2 \cdot (2^{w-t+2} - 1) = 2^{w-t+4} - 1,$$

and the proof is complete.

LEMMA 3.7. Suppose that G is a metacyclic 2-group of order
$$2^n$$
 such that $G/R(G) \cong D_8$ and $w + t > w > 1$, $1 \le t \le w + 3$.

- (a) If t = 1, then $s_{w+1}(G) = 2^{w+3} 2^{w+1} 1 = 3 \cdot 2^{w+1} 1$.
- (b) If t > 1, then $s_{w+t}(G) = 2^{w-t+4} 1$.

PROOF. In the notation of identity (3.1), we have

$$R(A) = A, R(B) = B, \quad w(A) = w(B) = w + 1,$$

$$R(C) = R(\Phi(G)) = R(G), \quad w(C) = w(\Phi(G)) = w.$$

If t = w + 3, then w + t = n, and, as in the previous lemma, we have $s_{w+t}(G) = 1 = 2^{w-(w+3)+4} - 1$, as in (b). If t = w + 2, then

$$s_{w+t}(G) = 3 = 2^2 - 1 = 2^{w-(w+2)+4} - 1,$$

as in (b). Next we assume that t < w + 2.

For t = 1, we have

$$s_{w+1}(A) = s_{w+1}(B) = 2^{(w+1)+1} - 1 = 2^{w+2} - 1 \text{ (Theorem 3.1(a))},$$

$$s_{w+1}(C) = s_{w+1}(\Omega_{w+1}(C)) = s_{w+1}(\Phi(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1$$

(Lemma 3.2), so that, by (3.1),

$$s_{w+1}(G) = 2 \cdot (2^{w+2} - 1) + (2^{w+1} - 1) - 2(2^{w+1} - 1) = 3 \cdot 2^{w+1} - 1,$$

in (a)

as in (a).

If t > 1, then w + t = (w + 1) + (t - 1) so that

 $s_{w+t}(A) = s_{w+t}(B) = 2^{(w+1)-(t-1)+1} - 1 = 2^{w-t+3} - 1$ (Theorem 3.1(b)), $s_{w+t}(C) = 2^{w-t+3} - 1$ (Lemma 3.3), $s_{w+t}(\Phi(G)) = 2^{w-t+2} - 1$ (Lemma 3.2) so that, by (3.1),

$$s_{w+t}(G) = 3(2^{w-t+3} - 1) - 2(2^{w-t+2} - 1) = 2^{w-t+4} - 1,$$

completing the proof.

LEMMA 3.8. Let G be a metacyclic 2-group of order 2^n such that $G/R(G) \cong Q_{2^4}, w > 1 \text{ and } 1 \le t \le w + 4.$ Then

- (a) $s_{w+1}(G) = 2^{w+1} 1.$
- (b) If $2 \le t \le w + 4$, then $s_{w+t}(G) = 2^{w-t+5} 1$.

PROOF. If t = w + 4, then $s_{w+(w+4)}(G) = s_n(G) = 1 = 2^{w-(w+4)+5} - 1$, as in (b). If t = w + 3, then $s_{w+(w+3)}(G) = 3 = 2^2 - 1 = 2^{w-(w+3)+5} - 1$, as in (b). If t = 1, then

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1$$
 (Lemma 3.2),

as in (a).

We have w(M) = w for $M \in \{A, B, C, \Phi(G)\}$.

Now let t = 2. Then, by Lemmas 3.6, 3.4, 3.3, respectively, we have

$$s_{w+2}(A) = s_{w+2}(B) = 2^{w-2+4} - 1 = 2^{w+2} - 1,$$

 $s_{w+2}(C) = 2^{w-2+4} - 1 = 2^{w+2} - 1, s_{w+2}(\Phi(G)) = 2^{w-2+3} - 1 = 2^{w+1} - 1.$ Therefore, by (3.1), we get

$$s_{w+2} = 3(2^{w+2} - 1) - 2(2^{w+1} - 1) = 2^{w+3} - 1$$

as in (b) for t = 2. Next we assume that 2 < t < w + 3.

By Lemma 3.6, Theorem 3.5 and identity (3.1),

$$s_{w+t}(G) = 2(2^{w-t+4} - 1) + (2^{w-t+4} - 1) - 2(2^{w-t+3} - 1) = 2^{w-t+5} - 1,$$

ind the proof is complete.

and the proof is complete.

Now we are ready to prove the following

THEOREM 3.9. Let G be a metacyclic 2-group such that $G/R(G) \cong \mathbb{Q}_{2^c}$ and w + t > w > 1, $c - 1 \le t \le w + c$. Then $\mathfrak{s}_{w+t}(G) = 2^{w-t+c+1} - 1$.

PROOF. We use induction on c. The theorem is true for c = 3, 4 (Lemmas 3.6, 3.8) and $t \in \{w + c - 1, w + c\}$ (direct checking; see Lemma 3.8). Next assume that c > 4 and t < w + c - 1. As in Lemma 3.8, w(M) = w for $M \in \{A, B, C, \Phi(G)\}$. We have

$$A/R(G) \cong \mathbb{Q}_{2^{c-1}} \cong B/R(G), \ C/R(G) \cong \mathbb{C}_{2^{c-1}}, \ \Phi(G)/R(G) \cong \mathbb{C}_{2^{c-2}}.$$

Then, by induction, $s_{w+t}(A) = s_{w+t}(B) = 2^{w-t+c} - 1$. By Theorem 3.5, $s_{w+t}(C) = 2^{w-t+c} - 1$, $s_{w+t}(\Phi(G)) = 2^{w-t+c-1} - 1$. Therefore, by (3.1),

$$s_{w+t}(G) = 3(2^{w-t+c} - 1) - 2(2^{w-t+c-1} - 1) = 2^{w-t+c+1} - 1,$$

and the proof is complete.

There is no problem to compute $s_{w+t}(G)$ for t < c-1. Our method works also in this case.

Now suppose that w = 1 and G/R(G) is of maximal class and order 2^c . Taking into account that C and $\Phi(G)$ have cyclic subgroups of index 2, $\operatorname{cl}(C) \leq 2$ and $\Phi(G)$ is abelian (indeed, $\operatorname{C}_G(R(G)) \geq \Phi(G)$), we obtain $\operatorname{s}_{1+t}(C) = \operatorname{s}_{1+t}(\Phi(G)) = 3$. Therefore, by (3.1), we get

(3.2)
$$s_{1+t}(G) = s_{1+t}(A) + s_{1+t}(B) - 3$$

SUPPLEMENT 1 TO THEOREM 3.9. Let $G/R(G) \cong \mathbb{Q}_{2^c}$, w = 1, $|G| = 2^n = 2^{2+c}$, $1 \le t < c$. Then

(a)
$$s_2(G) = 3$$
 (in this case, $t = 1$).

(a) $S_2(G) = 0$ (in this case, t = 1). (b) If 1 < t < c, then $s_{1+t}(G) = 2^{1-t+c} + 3$.

PROOF. One may assume that 1 + t < n - 2 (= c) (we have $s_{n-2}(G) = 2^2 + 3 = 2^{1-t+c} + 3$, where t = n - 3 and c = n - 2; see the displayed formula following (3.1)). If t = 1, then $s_{1+1}(G) = s_2(\Omega_2(G)) = s_2(\Phi(G)) = 3$ since $\Omega_2(G)$ is abelian of type (4,2). Next we also assume that t > 1. By the same displayed formula following (2,1), if c = 3 and t = 2, then $s_3(G) = 2^2 + 3 = 2^{1-2+3} + 3$.

If c = 4, then t = 2 (by assumption, t < c) so, by (3.2) and the previous paragraph,

$$s_{1+2}(G) = 2(2^2 + 3) - 3 = 2^3 + 3 = 2^{1-2+4} + 3$$

If c = 5, then $t \in \{2, 3\}$ so, by (3.2),

 $s_{1+2}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-2+5} + 3$, by the previous paragraph,

 $s_{1+3}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-3+5} + 3$, by the first paragraph.

If c = 6, then $t \in \{2, 3, 4\}$. We have, by (3.2) and the previous paragraphs,

$$s_{1+2}(G) = 2(2^4 + 3) - 3 = 2^5 + 3 = 2^{1-2+6} + 3,$$

Y. BERKOVICH

$$s_{1+3}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-3+6} + 3,$$

$$s_{1+4}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-4+6} + 3.$$

Now let $|G/R(G)| = 2^c$, $t \in \{2, ..., c-1\}$, c > 3. We claim that $s_{1+t}(G) =$ $2^{1-t+c}+3$. We prove this by induction on c. By the above, this is true for c = 3, 4, 5, 6 so one may assume that c > 6. By induction and (3.2), we have

$$s_{1+t}(G) = 2(2^{1-t+c-1}+3) - 3 = 2^{1-t+c}+3,$$

and we are done.

We see that cases w = 1 and w > 1 are differed essentially.

SUPPLEMENT 2 TO THEOREM 3.9. Let $G/R(G) \cong \mathbb{Q}_{2^c}$, w > 1 and t =1. Then $s_{w+1}(G) = 2^{w+1} - 1$.

PROOF. For arbitrary $c \geq 3$, we have, by Lemma 3.2,

$$s_{w+1}(G) = s_{w+1}(\Omega_{w+1}(G)) = 2^{w-1+2} - 1 = 2^{w+1} - 1$$

as required.

LEMMA 3.10. Let G be a metacyclic 2-group such that $G/R(G) \cong D_{2^4}$, w > 1 and $3 \le t < w + 3$. Then $s_{w+t}(G) = 2^{w-t+5} - 1 = 2^{w-t+(4+1)} - 1$.

PROOF. It follows from the structure of maximal subgroups of G that w(M) = w for $M \in \{A, B, C, \Phi(G)\}$. By Lemmas 3.7, 3.3 and (3.1), we have

$$s_{w+t}(G) = 2(2^{w-t+4} - 1) + (2^{w-t+4} - 1) - 2(2^{w-t+3} - 1) = 2^{w-t+5} - 1,$$

and we are done.

Now we are ready to prove the following

THEOREM 3.11. Let G be a metacyclic 2-group such that $G/R(G) \cong D_{2^c}$, $w + t > w > 1, c - 1 \le t < w + c - 1.$ Then $s_{w+t}(G) = 2^{w-t+c+1} - 1.$

PROOF. We proceed by induction on c. The theorem holds for c = 3, 4(Lemmas 3.7 and 3.10). So one may assume that c > 4. As above, w(M) = wfor $M \in \{A, B, C, \Phi(G)\}$. Indeed, since c > 4, subgroups A/R(G) and B/R(G) have no normal abelian subgroups of type (2,2). By induction, Theorem 3.5 and (3.1), we have

$$s_{w+t}(G) = 2(2^{w-t+c} - 1) + (2^{w-t+c} - 1) - 2(2^{w-t+c-1} - 1) = 2^{w-t+c+1} - 1,$$

completing the proof.

npleting the p

Now we consider case $G/R(G) \cong D_{2^c}$, w = 1. As above, let $|G| = 2^n$.

SUPPLEMENT 1 TO THEOREM 3.11. Let $G/R(G) \cong D_{2^c}$, w = 1 (so that n = c + 2, $1 \le t < c$. Then $s_{1+t}(G) = 2^{1-t+c} + 3$.

¹If t = c, then $s_{1+c}(G) = |\Gamma_1| = 3$.

PROOF. By the paragraph containing (3.1), we have $s_{n-2}(G) = 2^2 + 3 =$ $2^{1-(n-3)+n-2}+3$ (here t=n-3 and c=n-2), as in the statement. Therefore, one may assume in the sequel that t < n - 3 = (c + 2) - 3 = c - 1.

Let t = 1. If H < G is of order 4 and $H \neq R(G)$, then HR(G) of order 8 contains exactly two $\neq R(G)$ subgroups of order 4 since HR(G) is abelian of type (p^2, p) , by Lemma J(b). Since $s_1(G/R(G)) = 2^{c-1} + 1$, we get

$$s_{1+1}(G) = 1 + 2(2^{c-1} + 1) = 2^c + 3 = 2^{1-1+c} + 3$$

as in the statement. In what follows we assume that t > 1; then c > 3. Let c = 4. Then t = 2. Using (3.2), we obtain

$$s_{1+2}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-2+4} + 3,$$

by the displayed formula following (3.1).

Let c = 5. Then $t \in \{2, 3\}$ and

$$s_{1+2}(G) = 2(2^3 + 3) - 3 = 2^4 + 3 = 2^{1-2+5} + 3,$$

$$S_{1+3}(G) = 2 \cdot (2^2 + 3) - 3 = 2^3 + 3 = 2^{1-3+5} + 3$$

(the first equality follows from the previous paragraph and the second one follows from the formula following (3.1)).

Now we will prove by induction on c that $s_{1+t}(G) = 2^{1-t+c} + 3$. This is true for c = 3, 4, 5 and t = 1. By induction, Theorem 3.5 and (3.2), we get

$$s_{1+t}(G) = 2(2^{1-t+c-1}+3) - 3 = 2^{1-t+c}+3,$$

as required.

SUPPLEMENT 2 TO THEOREM 3.11. Let $G/R(G) \cong D_{2^c}, w > 1$. Then $s_{w+1}(G) = 2^{w+c-1} + 2^{w+1} - 1.$

PROOF. Let

$$X_1/R(G), \dots, X_{2^{c-1}}/R(G), X_{2^{c-1}+1}/R(G) = \mathbb{Z}(G/R(G))$$

be all subgroups of order 2 in G/R(G). Then $R(X_i) = R(G)$, $s_{w+1}(X_i) =$ $2^{w-1+2}-1=2^{w+1}-1$ for all *i* (Lemma 3.2) and $s_{w+1}(R(G))=2^{w-1+1}-1=$ $2^w - 1$ (Theorem 3.1(b)). We have $X_i \cap X_j = R(G)$ for $i \neq j$ and, given H < G of order 2^{w+1} not contained in R(G), there is exactly one $i \leq 2^{c-1} + 1$ such that $H < X_i (= HR(G))$. Therefore,

$$s_{w+1}(G) = \sum_{i=1}^{2^{c-1}+1} s_{w+1}(X_i) - 2^{c-1} s_{w+1}(R(G))$$

= $(2^{c-1}+1)(2^{w+1}-1) - 2^{c-1}(2^w-1) = 2^{w+c-1} + 2^{w+1} - 1,$
proof is complete.²

and the

²It is easy to check that, for c = 3, the obtained result coincides with Lemma 3.7(a).

SUPPLEMENT 3 TO THEOREM 3.11. Let G be a metacyclic 2-group such that $G/R(G) \cong D_{2^c}$, w > 1 and t = 2. Then $s_{w+2}(G) = 2^{w+c-2} + 2^{w+1} - 1$.

PROOF. Suppose that $X_1/R(G), \ldots, X_{2^{c-2}}/R(G) < G/R(G)$ are abelian of type (2,2) and $X_{2^{c-2}+1}/R(G) = Y/R(G) < G/R(G)$ cyclic of order 4. We have $X_i \cap X_j = \Omega_{w+1}(Y)$ for $i \neq j$. Given H < G of order 2^{w+2} , there is $i \in \{1, \ldots, 2^{c-2} + 1\}$ such that $H < X_i$ since $|H \cap R(G)| \ge 2^w$. Therefore,

(3.3)
$$\mathbf{s}_{w+2}(G) = \sum_{i=1}^{2^{c-2}+1} \mathbf{s}_{w+2}(X_i) - 2^{c-2} \cdot \mathbf{s}_{w+2}(\Omega_{w+1}(Y)).$$

We have $R(X_i) = X_i$ for $i \le 2^{c-2}$ and R(Y) = R(G). By Theorem 3.1(b), $s_{w+2}(X_i) = s_{(w+1)+1}(X_i) = 2^{(w+1)-1+1} - 1 = 2^{w+1} - 1, \ i \le 2^{c-2},$

and, by Lemmas 3.3, 3.2, respectively (recall that $Y = X_{2^{c-2}+1}$), $s_{w+2}(Y) = 2^{w-2+3} - 1 = 2^{w+1} - 1$, $s_{w+2}(\Omega_{w+1}(Y)) = 2^{w-2+2} - 1 = 2^w - 1$. Therefore, we get, by (3.3),

 $\mathbf{s}_{w+2}(G) = 2^{c-2} \cdot (2^{w+1}-1) + (2^{w+1}-1) - 2^{c-2} \cdot (2^w-1) = 2^{w+c-2} + 2^{w+1} - 1,$ and the proof is complete.

Note that cases $t = 3, \ldots, c - 2$ of Supplement 3 are more difficult and, to treating them, one has to use the enumeration principle and induction on c for each value of t.

The cases $G/R(G) \in \{Q_{2^c}, SD_{2^c}\}, w > 1$ and t = 2, are considered similarly.

THEOREM 3.12. Let G be a metacyclic 2-group such that $G/R(G) \cong SD_{2^c}$ and w + t > w > 1, $c - 1 \le t \le w + c - 1$. Then $s_{w+t}(G) = 2^{w-t+c+1} - 1$.

PROOF. It is easily seen that the theorem holds for $t \in \{w + c - 1, w + c\}$. Next we assume that t < w + c - 1.

By Theorems 3.5, 3.9, 3.11 and (3.1), we have

 $s_{w+t}(G) = 3(2^{w-t+c}-1) - 2(2^{w-t+c-1}-1) = 2^{w-t+c+1}-1, \quad t > 1,$

and the proof is complete.

SUPPLEMENT 1 TO THEOREM 3.12. Let $G/R(G) \cong \mathrm{SD}_{2^c}, w = 1$ and $t \geq 1$. Then

(a) If t = 1, then $s_{1+1}(G) = s_2(G) = 2^{c-1} + 3$.

(b) If $1 < t \le c - 1$, then $s_{1+t}(G) = 2^{1-t+c} + 3$.

PROOF. If t = c - 1, the result follows from the displayed formula following (3.1). Now let t < c - 1.

By Supplements 1 to Theorems 3.9 and 3.11 and (3.2),

$$s_{1+1}(G) = s_2(G) = 3 + (2^{1-1+c-1}+3) - 3 = 2^{c-1}+3$$

$$A_{1+t}(G) = 2(2^{1-t+c-1}+3) - 3 = 2^{1-t+c} + 3$$
 for $1 < t < c$,
we the proof

completing the proof.

 \mathbf{S}

SUPPLEMENT 2 TO THEOREM 3.12. Let $G/R(G) \cong SD_{2^c}$, w > 1. Then $s_{w+1}(G) = 2^{w+c-2} + 2^{w+1} - 1$.

PROOF. We have

(3.4)
$$s_{w+1}(G) = s_{w+1}(A) + s_{w+1}(B) + s_{w+1}(C) - 2s_{w+1}(\Phi(G)).$$

Let $\{A/R(G), B/R(G)\} = \{D_{2^{c-1}}, Q_{2^{c-1}}\}$. By Supplements 2 to Theorems 3.11, 3.9 and Theorem 3.5(b), we have

$$s_{w+1}(A) = 2^{w+c-2} + 2^{w+1} - 1, \ s_{w+1}(B) = 2^{w+1} - 1, \ s_{w+1}(C)$$
$$= s_{w+1}(\Phi(G)) = 2^{w+1} - 1.$$

Substituting these results in (3.4), we get

$$s_{w+1}(G) = (2^{w+c-2} + 2^{w+1} - 1) + (2^{w+1} - 1) + (2^{w+1} - 1) - 2(2^{w+1} - 1)$$

= 2^{w+c-2} + 2^{w+1} - 1,

as was to be shown.

The lower restrictions for t in Theorems 3.9, 3.11 and 3.12 are made by technical causes (otherwise, statements of these theorems would be more complicated). However, if necessary, it is not difficult, using the above approach, consider cases $t \in \{2, ..., c-2\}$.

It is known that if G is a noncyclic p-group of order p^n such that $s_k(G) = 1$ for some $k \in \{1, \ldots, n-1\}$, then k = 1, p = 2 and G is a generalized quaternion group. By Sylow's theorem, $s_k(G) \equiv 1 \pmod{p}$ for the same k. It follows that if G is neither cyclic nor generalized quaternion and k < n, then $s_k(G) \ge 1+p$. Therefore, it is natural to classify the noncyclic p-groups G of order $p^n > p^3$ satisfying $s_k(G) = 1 + p$ for some fixed $k \in \{2, \ldots, n-2\}$ $(s_{n-1}(G) = 1 + p$ if and only if d(G) = 2).

PROPOSITION 3.13. Suppose that G is a group of order $p^n > p^3$ satisfying $s_k(G) = 1 + p$ for some fixed $k \in \{2, ..., n-2\}$. Then one of the following holds:

- (a) G is abelian of type (p^{n-1}, p) .
- (b) $G \cong \mathbf{M}_{p^n}$.

(c) p = 2, k = 2 and $G = \langle a, b \mid a^{2^{n-2}} = 1, n > 4, a^{2^{n-3}} = b^2 = 1, a^b = a^{-1} \rangle$ is metacyclic.

PROOF. By Theorem 2.1, G is not a 2-group of maximal class. Then G has a normal abelian subgroup R of type (p, p) (Lemma J(e)).

(i) Let k = 2. Assume that E < G is of order p^3 and exponent p; then E is nonabelian. It follows that all subgroups of G of order p^2 are contained in

E; then $\exp(G) = p$ so $s_2(G) \equiv 1 + p + 2p^2 \pmod{p^3}$ ([B, Theorem 5.9]), a contradiction. Thus, E does not exist.

Assume that G/R has two distinct subgroups X/R and Y/R of order p. Then X and Y contain together at least $s_2(X) + s_2(Y) - 1 = 2p + 1 > p + 1$ distinct subgroups of order p^2 , a contradiction. Thus, G/R is either cyclic or generalized quaternion. In the first case, G is one of groups (a), (b). If G/R is generalized quaternion, then $|\Omega_2(G)| = 2^3$ so G is as in (c), by [B, Lemma 42.1(c)].

(ii) Suppose that k > 2. Then, as in (i), G/R contains exactly one (proper since k < n-1) subgroup of order p^{k-1} . In this case, G/R is cyclic. The subgroup $C_G(R)$ is abelian with cyclic subgroup of index p and $|G : C_G(R)| \le p$. Then $\Omega_1(G) = R$ so G is as in (a) or in (b).

Now let $s_1(G) = 1 + p$. If p > 2, then G is either metacyclic or a 3-group of maximal class ([B, Theorems 12.1(b), 9.8(a) and 7.2(d)]). Such G is also described very well for p = 2, see [BJ, §82].

PROPOSITION 3.14. Let M be a metacyclic p-group and G a p-group of order $p^n > p^3$, p > 2. If $s_2(G) = s_2(M)$, then one of the following holds:

- (a) G is metacyclic.
- (b) G = EC, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent pand C is cyclic of order > p.
- (c) G is of maximal class and order p^4 , all maximal subgroups of G are two-generator.

PROOF. One may assume that M is noncyclic; then G is also noncyclic. We have $s_2(G) = s_2(M) = \{1 + p, 1 + p + p^2\}$ (Theorem 1.2). Assume that G is nonmetacyclic. Then $s_2(G) = 1 + p + p^2$, by Proposition 3.13, and so $\Omega_2(G)$ is nonmetacyclic ([B, Remark 41.2]).

(i) Assume that G has a subgroup E of order p^4 and exponent p. Then $s_2(E) = 1 + p + 2p^2 + sp^3$ for some nonnegative integer ([B, Theorem 5.9]) so $s_2(E) > 1 + p + p^2 = s_2(G)$, a contradiction.

(ii) Assume that G has an elementary abelian subgroup E of order p^3 . Then $s_2(E) = 1 + p + p^2$, so, by the first paragraph, all subgroups of G of order p^2 are contained in E. It follows that $\exp(G) = p$, and so, by (i), G = E is of order p^3 , contrary to the hypothesis.

(iii) It follows from (ii) that either G is a 3-group of maximal class or G = EC, where $E = \Omega_1(G)$ is nonabelian of order p^3 and exponent p and C is cyclic ([BJ, Theorem 69.4]). The group G = EC satisfies the hypothesis (note that one of such groups is of maximal class; then its order is equal to p^4).

Suppose that G is a 3-group of maximal class and order > 3⁴. Let G_1 be the fundamental subgroup of G (see [B, §9]); then G_1 is metacyclic without cyclic subgroup of index 3 ([B, §9]) so that $s_2(G_1) = 1 + 3 + 3^2 = s_2(M) =$ s₂(*G*). It follows that all subgroups of *G* of order 3^2 are contained in G_1 so that $\Omega_2(G) \leq G_1$. However (see [B, Proposition 13.14(b)]), $\Omega_2(G) = G > G_1$, and this is a contradiction. Thus, if *G* is a 3-group of maximal class, then n = 4. By (ii), *G* has no subgroup of type (3, 3, 3), and this holds if and only if *G* is not isomorphic to a Sylow 3-subgroup of the symmetric group of degree 9.

4. Metacyclic *p*-groups with small minimal nonabelian subgroups or sections

In the following four paragraphs G is a nonabelian metacyclic p-group.

If G, p > 2, has a proper subgroup $H = \langle a, b \mid a^{p^2} = b^{p^2} = 1$, $a^b = a^{1+p} \rangle$, then |G:H| = p. Indeed, setting $L = \langle b^p \rangle$ and $C = C_G(L)$, we see that $|G:C| \leq p$ and $H/L \leq C/L$ is nonabelian of order p^3 . By Lemma J(b), C/L = H/L so that C = H. Since C = H < G, we get |G:H| = p, as asserted.

If p > 2, $\{1\} < L < M < G$ and M/L is nonabelian of order p^3 , then $|\mathcal{N}_G(M) : M| = p$. Indeed, since $M/\mathcal{O}_2(M)$ is of exponent p^2 and $\mathcal{O}_2(M)$, being characteristic in M, is normal in $\mathcal{N}_G(M)$, the claim follows from the previous paragraph.

Let us prove that if every minimal nonabelian subgroup of G has a cyclic subgroup of index p, then G has an abelian subgroup of index p. One may assume that G is not a 2-group of maximal class; then there is in G a normal abelian subgroup R of type (p, p) and $R \not\leq Z(G)$. Also, G has no nonabelian subgroup of order p^3 (Lemma J(b)). Set $C = C_G(R)$; then |G : C| = p. Assume that C is nonabelian. Then C contains a minimal nonabelian subgroup A. Since $\Omega_1(G) \leq Z(C)$, it follows that $\Omega_1(G) = \Omega_1(A) \leq Z(A)$ so A/Z(A) is cyclic, a contradiction since A is nonabelian.

If every minimal nonabelian subgroup of G has no cyclic subgroup of index p, then $\Omega_1(G) \leq Z(G)$. Indeed, if $A \leq G$ is minimal nonabelian, then $\Omega_1(G) = \Omega_1(A) \leq Z(A)$ (Lemma J(b) and [BJ, Lemma 65.1]). Since G is generated by minimal nonabelian subgroups ([B, Theorem 10.28]), our claim follows.

Below G is a metacyclic 2-group. If G = R(G), then $R(\mathcal{O}_1(G)) = \mathcal{O}_1(G)$. We use this obvious fact in the proof of the following theorem.

THEOREM 4.1. Suppose that a metacyclic 2-group has a nonabelian section of order 8. If G is not of maximal class, then

(a) There is $R \triangleleft G$ such that $G/R \cong Q_8$. Next, G/G' is abelian of type (4,2) and there is a cyclic $C \triangleleft G$ such that G/C is cyclic of order 4.

(b) $\mathcal{O}_1(G)$ has no nonabelian section of order 8.

PROOF. (a) First we prove the existence of R such that G/R is nonabelian of order 8. We use induction on |G|. Let $L \triangleleft M \leq G$ be such that M/L is nonabelian of order 8. One may assume that M < G (otherwise, we are done with R = L). Let $M \leq H \in \Gamma_1$. Then, by induction, there is $S \triangleleft H$ such that H/S is nonabelian of order 8. By Lemma J(c), S is characteristic in H so normal in G. By Lemma J(b), G/S is of maximal class. Let R/S = Z(G/S); then G/R is nonabelian of order 8, as was to be shown.

Now let M = G. We claim that then $G/\mathcal{O}_2(G) \cong \mathcal{H}_2$. Clearly, $\mathcal{O}_2(G) \leq L$. If $\mathcal{O}_2(G) = L$, then |G : G'| = 4 so G is of maximal class, by Taussky's theorem, a contradiction. Thus, $|G/\mathcal{O}_2(G)| = 2^4$, and $G/\mathcal{O}_2(G) \cong \mathcal{H}_2$, by Lemma J(a).

Since G is not of maximal class, |G : G'| > 4. By hypothesis, G has no cyclic subgroup of index 2. It follows that $\mathcal{V}_2(G) < R$, where R is as in the first paragraph of the proof. Then $G/\mathcal{V}_2(G) \cong \mathcal{H}_2$ (Lemma J(a)). It follows that $\mathcal{V}_2(G) < G'$ so that G/G' is abelian of type (4, 2). Since G is metacyclic, there is a cyclic $C \triangleleft G$ such that G/C is cyclic. Since G' < C, we conclude that G/C is of order 4. Since $G/\mathcal{V}_2(G) \cong \mathcal{H}_2$ has an epimorphic image isomorphic to Q_8 , the proof of (a) is complete.

(b) Assume that $\mathcal{O}_1(G) = \Phi(G)$ has a nonabelian section of order 8. Then, by (a), there is $S \triangleleft \mathcal{O}_1(G)$ such that $\mathcal{O}_1(G)/S$ is nonabelian of order 8. By Lemma J(c), S is characteristic in $\mathcal{O}_1(G)$ so normal in G. By Lemma J(b), G/S is of maximal class (of order 2⁵). It follows that $\mathcal{O}_1(G/S) = \mathcal{O}_1(G)/S$ is cyclic of order 8, a contradiction since, by (a), $\mathcal{O}_1(G)/\mathcal{O}_1(G)'$ is abelian of type (4, 2).

Suppose that a metacyclic *p*-group *G* has a proper normal nonabelian subgroup *H* of order p^4 and exponent p^2 . Let $L < \Omega_1(H)$ be of order *p*, $L \neq H'$; then $C = C_G(L)$ has index $\leq p$ in *G* and C = G provided p = 2. Since $H/L \leq C/L$ is nonabelian of order p^3 , C = H for p > 2 and G/L is of maximal class if p = 2. In addition, G/G' is abelian of type (p^2, p) .

Problems

- 1. Study the metacyclic *p*-groups, p > 2, possessing a nonabelian section of order p^3 (see Theorem 4.1).
- 2. Find the number of subgroups of given order in nonmetacyclic minimal nonabelian *p*-group.
- 3. Let G be an abelian group of type $(p^{a_1}, \ldots, p^{a_k})$. Find the types of all maximal subgroups of G counting multiplicities.
- Find the number of subgroups of given order in abelian *p*-group of rank
 3.
- 5. Let G be a homocyclic p-group of rank d. (i) Find the number of subgroups of given order in G. (ii) Find the number of subgroups of rank 2 and given order in G.
- 6. Given a positive integer k > 1, classify the *p*-groups *G* such that there exists a metacyclic *p*-group *M* satisfying $s_k(G) = s_k(M)$.

- 7. Study the *p*-groups G such that $s_k(G) = s_k(A)$ for all positive integers k and some abelian *p*-group A.
- 8. Given p > 2 and n > p, does there exist an absolutely regular p-group A (see [B, §9]) and an irregular p-group G of the same order p^n satisfying $s_k(G) = s_k(A)$ for all $k \in \{2, \ldots, n-1\}$?

ACKNOWLEDGEMENTS.

I am indebted to Avinoam Mann who acquainted me with his paper [M2] prior its publication and for his interest to this note.

References

- [B] Y. Berkovich, Groups of prime power order. Vol. 1, Walter de Gruyter, Berlin, 2008.
- [BJ] Y. Berkovich and Z. Janko, Groups of prime power order. Vol. 2, Walter de Gruyter, Berlin, 2008.
- [M1] A. Mann, personal communication.
- [M2] A. Mann, The number of subgroups of metacyclic groups, in: Character theory of finite groups, Contemporary Mathematics 524, AMS, Providence, 2010, 93–95.

Y. Berkovich Department of Mathematics University of Haifa Mount Carmel, Haifa 31905 Israel Received: 19.9.2009. Revised: 15.2.2010.