GLASNIK MATEMATIČKI
Vol. 43(63)(2008), 59 – 95

ON THE NUMBER OF SUBGROUPS OF GIVEN TYPE IN A FINITE p-GROUP

Yakov Berkovich
University of Haifa, Israel

Abstract. In §1 we study the p-groups G containing exactly $p+1$ subgroups of order p^p and exponent p. A number of counting theorems and results on subgroups of maximal class and p-groups with few subgroups of given type are also proved. Counting theorems play crucial role in the whole paper.

This paper is a continuation of [Ber1, Ber3, Ber4, BJ2]. We use the same notation, however, for the sake of convenience, we recall it in the following paragraph.

In what follows, p is a prime, n, m, k, s, t are natural numbers, G is a finite p-group of order $|G|$, $o(x)$ is the order of $x \in G$, $\Omega_n(G) = \langle x \in G \mid o(x) \leq p^n \rangle$, $\Omega_n^*(G) = \langle x \in G \mid o(x) = p^n \rangle$ and $\mho_n(G) = \langle x^{p^n} \mid x \in G \rangle$. A p-group G is said to be *absolutely regular* if $|G/\mho_1(G)| < p^p$. Let $e_p(G)$ be the number of subgroups of order p^p and exponent p in G and $\mathrm{c}_n(G)$ the number of cyclic subgroups of order p^n in G. A p-group G of order p^m is said to be of *maximal class* if $m > 2$ and $\mathrm{cl}(G) = m-1$. As usually, G', $\Phi(G)$, $\mathrm{Z}(G)$ denote the derived subgroup, Frattini subgroup and center of G, respectively. Let $\Gamma_i = \{H < G \mid \Phi(G) \leq H, |G : H| = p^i\}$ so that Γ_1 is the set of maximal subgroups of G. If $H < G$, then $\Gamma_1(H)$ is the set of maximal subgroups of H. Let $\mathrm{K}_n(G)$ be the n-th member of the lower central series of G. If $M \subseteq G$, then $\mathrm{C}_G(M)$ ($\mathrm{N}_G(M)$) is the centralizer (normalizer) of M in G. Next, $\mathrm{K}_n(G)$ and $\mathrm{Z}_n(G)$ is the nth member of the lower and upper central series of G, respectively. Given $n > 2$ and $n > 3$ for $p = 2$, let $\mathrm{M}_{p^n} = \langle a, b \mid a^{p^{n-1}} = b^p = 1, a^b = a^{1+p^{n-2}} \rangle$. Let D_{2^m}, Q_{2^m} and SD_{2^m} be dihedral, generalized quaternion and semidihedral groups of order 2^m, and let C_{p^n}, E_{p^n} be cyclic and elementary abelian groups

2000 *Mathematics Subject Classification.* 20D15.
Key words and phrases. p-groups of maximal class, regular and absolutely regular p-groups.

of order p^n. We write $\eta(G)/\mathrm{K}_3(G) = \mathrm{Z}(G/\mathrm{K}_3(G))$; clearly, $G' \leq \eta(G)$. Let $\mathrm{H}_p(G) = \langle x \in G \mid o(x) > p\rangle$ be the H_p-subgroup of G. Let $\mu_n(G)$ be the number of subgroups of maximal class and order p^n in G.

In Lemma J we gathered some known results which are due to P. Hall, N. Blackburn and the author (proofs all of them are presented in [Ber1-4, Bla1-2, Hal1-2]).

LEMMA J. *Let G be a nonabelian p-group of order p^m.*

(a) *(Blackburn) If G has no normal subgroup of order p^p and exponent p, it is either absolutely regular or of maximal class.*

(b) *(Berkovich, Blackburn, independently) If G is neither absolutely regular nor of maximal class, then $\mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-1} \pmod{p^p}$, $\mathrm{c}_n(G) \equiv 0 \pmod{p^{p-1}}$ $(n > 1)$ and $e_p(G) \equiv 1 \pmod{p}$.*

(c) *(Berkovich) If $B \leq G$ is nonabelian of order p^3 and $\mathrm{C}_G(B) < B$, then G is of maximal class.*

(d) (i) *(Berkovich) If $H < G$ and $\mathrm{N}_G(H)$ is of maximal class, then G is also of maximal class.*

 (ii) *(Blackburn) Let G be of maximal class. Then, for $i \in \{2, \dots, m\}$, G has exactly one normal subgroup of index p^i. If, in addition, $m \geq p+1$, then G is irregular and $|G/\mho_1(G)| = p^p$.*

(e) (i) *If G is irregular of maximal class and $H < G$ is of order p^p and exponent p, then H is a maximal regular subgroup of G, $\mathrm{N}_G(H)$ is of maximal class and $\Omega_1(\Phi(G)) < H$.*

 (ii) *[Ber3, Theorem 10.1] If R be a maximal regular subgroup of order p^p of an irregular p-group G, then G is of maximal class.*

(f) *If G is of maximal class, $M \lhd G$ and $|G : M| > p$, then $M \leq \Phi(G)$ is absolutely regular and $|\mathrm{Z}(M)| > p$, unless $|M| \leq p$. If $p > 2$ and $m > 3$, then G has no normal cyclic subgroup of order p^2.*

(g) *(Berkovich) If $H < G$ is of order $\leq p^{p-1}$ and exponent p and G is neither absolutely regular nor of maximal class, then the number of subgroups of order $p|H|$ and exponent p between H and G is $\equiv 1 \pmod{p}$.*

(h) *(Blackburn) Let G be irregular of maximal class; then $m > p$. If G has a normal subgroup of order p^p and exponent p, then $m = p+1$. If $m = p+2$, then all maximal subgroups of G have exponent p^2. If $m > p+1$, then exactly p maximal subgroups of G are of maximal class and one maximal subgroup, which we denote by G_1 (the fundamental subgroup of G), is absolutely regular. If $n > 2$, then $c_n(G) = c_n(G_1)$.*

(i) *[Ber1, Theorem 7.4] Let H be a subgroup of maximal class and index p in G. If $\mathrm{d}(G) = 2$, then G is also of maximal class. Now let $\mathrm{d}(G) = 3$ and $m > p+1$. Then $G/\mathrm{K}_p(G)$ is of order p^{p+1} and exponent p and exactly $p+1$ members, say $T_1, \dots, T_{p+1}$ of the set Γ_1, are neither absolutely regular nor of maximal class and exactly p^2 members of the* *set* Γ_1 *are irregular of maximal class. We have* $|G : \bigcap_{i=1}^{p+1} T_i| = p^2$ *and* $|T_i/T_i'| > p^2$ *for* $i = 1, \dots, p+1$.

(j) *(Berkovich, Blackburn, independently) If* $m > p+1$*, then an irregular group* G *is of maximal class if and only if* $\mathrm{c}_1(G) \equiv 1 + p + \cdots + p^{p-2} \pmod{p^p}$.

(k) *(Hall) If* G *is regular of exponent* $\geq p^n$*, then*

$$\exp(\Omega_n(G)) = p^n,\ \Omega_n^*(G) = \Omega_n(G),\ \mathrm{c}_n(G) = \frac{|\Omega_n(G) - \Omega_{n-1}(G)|}{p^{n-1}(p-1)}.$$

If $\mathrm{cl}(G) < p$ *or* $\exp(G) = p$*, then* G *is regular.*

(l) *(Berkovich) If* G *has an absolutely regular maximal subgroup* A *and irregular subgroup* M *of maximal class, then* G *is also of maximal class.*

(m) *(Burnside, 1897) Let a nonabelian* p*-group* G *contain a cyclic subgroup of index* p*. Then* G *is either* M_{p^n} *or a 2-group of maximal class.*

(n) *(Blackburn) Let* G *be neither absolutely regular nor of maximal class. If* $H \in \Gamma_1$ *is absolutely regular, then* $G = H\Omega_1(G)$*, where* $|\Omega_1(G)| = p^p$.

(o) *(Suzuki) If* $A < G$ *is of order* p^2 *and* $\mathrm{C}_G(A) = A$*, then* G *is of maximal class.*

(p) *[Ber1, Theorem 5.2] If* $p > 2$*,* G *is of maximal class and* $H < G$ *is such that* $\mathrm{d}(H) > p-1$*, then* $G \cong \Sigma_{p^2}$*, a Sylow* p*-subgroup of the symmetric group of degree* p^2.

(q) *(Hall) If* G *is irregular, then* G' *contains a characteristic subgroup of order* $\geq p^{p-1}$ *and exponent* p.

(r) *(Huppert) If* $p > 2$ *and* $|G/\mho_1(G)| \leq p^2$*, then* G *is metacyclic.*

(s) *[Ber1, Lemma 2.1] Suppose that* $|\Omega_2(G)| = p^3$*. Then* G *is one of the following groups:*
   (i) *abelian of type* (p^{m-1}, p),
   (ii) $\mathrm{M}_{\mathrm{p^m}}$,
   (iii) $p = 2$ *and* $G = \langle a, b \mid a^{2^{m-2}} = 1, b^4 = a^{2^{m-3}}, a^b = a^{-1}\rangle$.

(t) *(Redei) If* G *is minimal nonabelian, then* $G = \langle a, b\rangle$ *and one of the following holds:*
   (i) $a^{p^u} = b^{p^v} = 1,\ a^b = a^{1+p^{u-1}} (u + v = m)$,
   (ii) $a^{p^u} = b^{p^v} = 1,\ c = [a, b],\ [a, c] = [b, c] = 1 (u + v + 1 = m)$,
   (iii) $G \cong \mathrm{Q}_8$.

It follows from Lemma J(f) the following easy but important fact. If G is a p-group of maximal class, $M \in \Gamma_1$ is of maximal class and order $> p^3$ and M_1 is the fundamental subgroup of M, then $M \cap G_1 = M_1$. Indeed, M_1 is characteristic in M so normal in G. Since $|G : M_1| = p^2$, we get $M_1 = \Phi(G) < G_1$.

The paper is self contained modulo Lemma J and few results from [Ber1–Ber4].

1. p-groups with exactly $p+1$ subgroups of order p^p and exponent p

In view of Lemma J(b), it is natural to investigate the p-groups G satisfying $e_p(G) = 1 + kp$ for $k = 0$ and 1. The case $k = 0$ has been treated only for $p = 2$ in the fundamental paper [Jan1]. In Theorems 1.1–1.3 we analyze the structure of p-groups G satisfying $e_p(G) = p + 1$. Below we consider the p-groups G satisfying $e_p(G) < p + 1$.

Case 1. Let $e_p(G) = 0$. Then G has no subgroup of order p^p and exponent p so G is either absolutely regular or of maximal class (Lemma J(a)); in that case, $|\Omega_1(G)| < p^p$.

Case 2. Let $e_p(G) = 1$. Then $|\Omega_1(G)| = p^p$. Indeed, let H be the unique subgroup of G of order p^p and exponent p and $D < H$ be G-invariant of index p in H. Assume that there is $x \in G - H$ of order p. Then $U = \langle x, D\rangle$ is of order p^p and exponent p (Lemma J(k)) and $U \neq H$, a contradiction.

Case 3. Let $1 < e_p(G) \le p$. Then, by Lemma J(b), G is of maximal class since it is not regular, by Lemma J(k). If, in addition, $e_p(G) < p$, then G has a normal subgroup of order p^p and exponent p so $|G| = p^{p+1}$ (Lemma J(f)). Now let $e_p(G) = p$, $m > p + 1$ and let $H < G$ be a subgroup of order p^p and exponent p. Since H is not normal in G (Lemma J(e,h)), we get $|G : \mathrm{N}_G(H)| = p$. Then $\mathrm{N}_G(H)$ is of maximal class and order p^{p+1} (Lemma J(e)(i)) so $m = p+2$. (Note that $\mathrm{e}_2(\mathrm{SD}_{2^4}) = 2$.) Clearly, $e_p(\mathrm{N_G(H)}) = \mathrm{e_p(G)}$.

Remark 1.1. Suppose that a p-group G is not of maximal class. We claim that if $|\Omega_1(G)| = p^{p+1}$, then $\exp(\Omega_1(G)) = p$. Assume that this is false. Then $\Omega_1(G)$ is of maximal class so it has exactly $p + 1$ maximal subgroups. Obviously, all $e_p(G)$ subgroups of order p^p and exponent p are maximal subgroups of $\Omega_1(G)$. However, by hypothesis, $e_p(G) > 1$ so $e_p(G) \ge p+1$ (Lemma J(b)); then $\exp(\Omega_1(G)) = p$, contrary to Lemma J(h).

Remark 1.2. We claim that if G is a p-group with $1 < e_p(G) < p^2+p+1$, then intersection of all its subgroups of order p^p and exponent p has order p^{p-1}. Indeed, let $R \lhd G$ be of order p^{p-1} and exponent p (R exists, by Lemma J(a)) and let $S < G$ be of order p^p and exponent p such that $R \not\le S$. Set $H = RS$; then $|H| \ge p^{p+1}$. Assume that $|H| = p^{p+1}$. Then $\mathrm{d}(H) \ge 3$, $\mathrm{cl}(H) < p$ and $\exp(H) = p$ so all $\ge p^2 + p + 1$ maximal subgroups of order H have order p^p and exponent p, contrary to the hypothesis. Now we let $|H| > p^{p+1}$. Set $D = R \cap S$; then $|S/D| = p^n \ge p^3$. Let $U_1/D, \dots, U_k/D$ be all subgroups of order p in S/D, $k = 1 + p + \cdots + p^{n-1} \ge p^2 + p + 1$. Set $S_i = RU_i$, $i = 1, \dots, k$. Then $S_1, \dots, S_k$ are pairwise distinct and have order p^p and exponent p, contrary to the hypothesis since $e_p(G) < p^2 + p + 1$. Thus, R is contained in all subgroups of G of order p^p and exponent p. In particular, R is the unique normal subgroup of order p^{p-1} in G.

REMARK 1.3. Let G be a p-group of order $> p^{p+1}$ with $e_p(G) = 1$. Then $R = \Omega_1(G)$ is the unique subgroup of G of order p^p and exponent p (see Case 2). Then one of the following holds: (a) $R \leq \Phi(G)$, (b) all members of the set Γ_1 not containing R, are absolutely regular, (c) all p^2 members of the set Γ_1 not containing R, are of maximal class. Indeed, the group G is not of maximal class since $|G| > p^{p+1}$ (Lemma J(f)). Assume that $R \not\leq \Phi(G)$. Let $R \not\leq M \in \Gamma_1$; then $\Omega_1(M) = R \cap M$ is of order p^{p-1} so M is either absolutely regular or of maximal class (Lemma J(a)). Assume that M is of maximal class and let $R \not\leq K \in \Gamma_1$. By Lemma J(l), K is not absolutely regular. Thus, all members of the set Γ_1 not containing R, are of maximal class, and the number of such members equals p^2 (Lemma J(i)). This argument also shows that if M is absolutely regular, then the set Γ_1 has no members of maximal class. This supplements Lemma J(n).

REMARK 1.4. Suppose that G is a p-group and $R \leq G$ is of order p^p and exponent p. We claim that then $\Omega_1(G)$ is generated by subgroups of order p^p and exponent p. Indeed, it follows from Lemma J(g,i) that G has a normal subgroup D of order p^{p-1} and exponent p. If $x \in G - D$ is of order p, then $U = \langle x, D \rangle$ is of order p^p so it is regular. Since $|U| = p^p$ and $\Omega_1(U) = U$, we get $\exp(U) = p$ (Lemma J(k)), and our claim follows.

THEOREM 1.5. *Let G be a p-group of order $> p^{p+3}$ with $e_p(G) = p + 1$, and let $R_1, \ldots, R_{p+1}$ be all its subgroups of order p^p and exponent p. Set $H = \Omega_1(G)$. Then one of the following holds:*

(a) *H is of order p^{p+1} and exponent p and $\mathrm{d}(H) = 2$.*

(b) *$|H| = p^{p+2}$, $\exp(H) = p^2$, $\mathrm{d}(H) = 3$, $\cap_{i=1}^{p+1} R_i = \Phi(H)$. One may assume that $R = R_1 \triangleleft G$. Then*

  (b1) *$\Gamma_1(H) = \{M_1, \ldots, M_{p^2}, T_1, \ldots, T_{p+1}\}$, where $M_1, \ldots, M_{p^2}$ are of maximal class, $T_1, \ldots, T_{p+1}$ are regular with $|\Omega_1(T_i)| = p^p$. Exactly one of subgroups T_i, say T_1, is normal in G.*

  (b2) *$H \not\leq \Phi(G)$.*

  (b3) *If $H \not\leq M \in \Gamma_1$, then $e_p(M) = 1$. In particular, M is not of maximal class.*
  In what follows we assume that $R = R_1$ is the unique normal subgroup of order p^p and exponent p in G. Set $N = \mathrm{N}_G(R_2)$; then $|G : N| = p$ so $N \in \Gamma_1$.

  (b4) *$R < T_1 \cap \Phi(G)$ so, if $M \in \Gamma_1$ does not contain H, then $\Omega_1(M) = R$.*

  (b5) *$RR_2, \ldots, RR_{p+1}$ are distinct conjugate subgroups of maximal class and order p^{p+1} with $e_p(RR_i) = 2$ for $i = 2, \ldots, p + 1$.*

  (b6) *$T_2, \ldots, T_{p+1}$ are conjugate in G. One can choose numbering so that $\Omega_1(T_i) = R_i$ for $i = 2, \ldots, p + 1$.*

(b7) *Let* $K \in \Gamma_1(H)$ *be of maximal class. Assume that* $K < L < G$ *but* $H \not\leq L \not\leq N$. *Then* L *is of maximal class and order* p^{p+2} *and* $e_p(L) = e_p(K) \in \{0, p\}$.

(b8) *If* $K \in \Gamma_1(H)$ *is of maximal class and* $0 < e_p(K) < p$, *then* K *is not normal in* G.

(b9) *Suppose that there is* $K \in \Gamma_1(H)$ *with* $e_p(K) = p$. *Then* $K \triangleleft G$ *is of maximal class. In that case,* H *contains exactly* $p-1$ *maximal subgroups* L *such that* $e_p(L) = 0$, *and all these* L *are* G*-invariant. Exactly* p^2-p *members of the set* $\Gamma_1(H)$ *of maximal class are not normal in* G *and their normalizers are all equal to* N.

Proof. Since the set $\{R_i\}_1^{p+1}$ of cardinality $p+1$ is G-invariant, one may assume that $R = R_1 \triangleleft G$. Then, by Lemma J(h), G is not of maximal class. By Remark 1.2, $D = \bigcap_{i=1}^{p+1} R_i$, where D is the unique normal subgroup of order p^{p-1} and exponent p in G. If G has a subgroup of order p^{p+1} and exponent p, then that subgroup contains all R_i so coincides with $\Omega_1(G)$ (Remark 1.4), and G is as stated in part (a). Next we assume that G has no subgroup of order p^{p+1} and exponent p.

Set $N = \mathrm{N}_G(R_2)$. Then, since R_2 has at most p conjugates, we get $|G : N| \leq p$ so N is normal in G. In any case, all $R_i < N$. Indeed, $R < N$ since $|RR_2| = p^{p+1}$ so R normalizes R_2. Our claim is obvious if $R_2 \triangleleft G$ since then all $R_i \triangleleft G$. If R_2 is not normal in G, then $R_2, \ldots, R_{p+1}$ are conjugate in G, and again $R_i < N$ for $i > 1$ since $N \triangleleft G$. Since $\mathrm{N}_G(R_i) = N$ for all $i > 1$, $R_s R_t < G$ and $R_s R_t$ is of maximal class and order p^{p+1} for $s \neq t$, $1 \leq s, t \leq p+1$ (indeed, $R_s \cap R_t = D$, by the previous paragraph). By Lemma J(n), the set Γ_1 has no absolutely regular member.

Since G has no subgroup of order p^{p+1} and exponent p, then $\exp(\Omega_1(G)) > p$ and $|\Omega_1(G)| > |\bigcup_{i=1}^{p+1} R_i| = p^{p+1}$. One may assume that $R_3 \not\leq RR_2$. Set $H = RR_2R_3$; then $|H| = p^{p+2}$ since $R_3 \cap RR_2 = D$, and so $H/D \cong \mathrm{E}_{p^3}$; then $\exp(H) = p^2$ (see the first paragraph) and $\mathrm{d}(H) = 3$ since $\mathrm{d}(RR_2) = 2$. By Lemma J(b), $e_p(H) \equiv 1 \pmod p$ so $e_p(H) = p+1$ since $e_p(H) > 1$. It follows that $H = \Omega_1(G)$ (Remark 1.4). Thus, $|\Omega_1(G)| = |H| = p^{p+2}$.

By Lemma J(f), H is not of maximal class, therefore $\Gamma_1(H)$ is such as given in (b1) (Lemma J(i)). Let $\Gamma_1(H) = \{U_1, \ldots, U_{p^2}, T_1, \ldots, T_{p+1}\}$, all U_i's are of maximal class and all T_i's are regular. One may assume that $T_1 \triangleleft G$.

Assume that $H \leq \Phi(G)$. In that case, $|R \cap \mathrm{Z}(\Phi(G))| > p$ (indeed, every G-invariant subgroup of R of order p^2 is contained in $\mathrm{Z}(\Phi(G))$). Then $R \cap \mathrm{Z}(\Phi(G)) \leq \mathrm{Z}(RR_2)$, a contradiction since RR_2 is of maximal class. Thus, $H \not\leq \Phi(G)$, proving (b2).

Suppose that $H \not\leq M \in \Gamma_1$. As we have noticed, M is not absolutely regular. Since $e_p(M) < e_p(H) = p+1$, it follows that $e_p(M) \leq p$ so either $|\Omega_1(M)| = p^p$ or M is of maximal class (Lemma J(b)). Assume that M is of maximal class. Since $|M| > p^{p+2}$, M has no normal subgroup of order p^p and exponent p. Write $F = M \cap H \triangleleft M$; then $|F| = p^{p+1}$. Assume that $F = T_i$ for some i. Since T_i is not absolutely regular, $\Omega_1(T_i) \triangleleft G$ is of order p^p and exponent p, a contradiction. If $F = U_j$, then $|M : F| = p$ (Lemma J(f)) so $|M| = p^{p+2}$, contrary to the hypothesis. Thus, M is not of maximal class so $|\Omega_1(M)| = p^p$. As by product, we established that if R is the unique normal subgroup of G of order p^p and exponent p, then $R \le \Phi(G)$.

In what follows we assume that R_2 is not normal in G; then R is the unique normal subgroup of G of order p^p and exponent p and $R_2, \dots, R_{p+1}$ are conjugate in G. By the previous paragraph, $R \le \Phi(G)$ and $|G : N| = p$. Next, $R_2, \dots, R_{p+1} \not\le \Phi(G)$.

Since $\mathrm{d}(RR_2) = 2$ and $\exp(RR_2) > p$, not all conjugates of R_2 are contained in RR_2 so RR_2 is not normal in G. Then $\mathrm{N}_G(RR_2) = N = \mathrm{N}_G(R_2)$ and $RR_2, \dots, RR_{p+1}$ is a class of p conjugate subgroups of G. Since $RR_i \cap RR_j = R$ for $i, j > 1$ and $i \ne j$, we get $e_p(RR_i) = 2$ for all $i > 1$ since $e_p(G) = p + 1$, and the proof of (b5) is complete.

Since G has no subgroup of order p^{p+1} and exponent p, we get $\exp(T_i) = p^2$. By Lemma J(n) applied to H, T_i is not absolutely regular so $\Omega_1(T_i)$ is of order p^p and exponent p. By assumption, $T_1 \triangleleft G$ so $\Omega_1(T_1) = R$. Since $H/R \cong \mathrm{E}_{p^2}$, R is contained in exactly $p+1$ maximal subgroups of H, namely, in $T_1, RR_2, \dots, RR_{p+1}$. Therefore, if $i > 1$, then T_i is not normal in G since $R \ne \Omega_1(T_i)$. Without loss of generality, one may assume that $\Omega_1(T_i) = R_i$ for all i (indeed, if $R_j < T_i$ for $j \ne i$, then regular subgroup $T = R_i R_j$ is of exponent p).

Let $H \not\le M \in \Gamma_1$. Then, by the above, $\Omega_1(M) = R$ so $\Omega_1(\Phi(G)) = R$. Since $H \cap M \triangleleft G$ and maximal in H, it follows that $H \cap M = T_1$ since T_1 is the unique G-invariant member X of the set $\Gamma_1(H)$ such that $\Omega_1(X) = R$. Thus, T_1 is contained in all members of the set Γ_1 so $T_1 \le \Phi(G)$, and the proof of (b4) is complete.

Let $K \in \Gamma_1(H)$ be of maximal class. Assume that $K < L < G$ but $H \not\le L$. Then $L \cap H = K \triangleleft L$ so $e_p(L) = e_p(K) = s \le p$. If $s > 1$, then L is of maximal class (Lemma J(b)) so $|L| = p^{p+2}$ (Lemma J(f)) and $R \not\le L$. Now let $s = 1$ and $R \not\le K$. In that case, $e_p(L) = 1$ so $L \le \mathrm{N}_G(\Omega_1(K)) = N$ since $\Omega_1(K) \ne R$, and this completes the proof of (b7).

Let $K \in \Gamma_1(H)$ be of maximal class and $1 \le e_p(K) < p$. Then K is not normal in G. This is clear if $R < K$, by (b5). If $R \not\le K$ and $K \triangleleft G$, then all subgroups of order p^p and exponent p in K are normal in G, a contradiction since R is the unique G-invariant subgroup of order p^p and exponent p. This proves (b8).

Assume that $K \in \Gamma_1(H)$ and $e_p(K) = p$. Then $R \not\le K$ (see (b5)) and $R_i R_j = K$ for distinct $i, j > 1$. If $i > 1$, then R_i is contained in exactly $p - 1$ maximal subgroups of H distinct of K and T_i (all these $p-1$ subgroups are of maximal class). Therefore, the set $\Gamma_1(H)$ contains exactly $p(p-1)$ pairwise distinct members M of maximal class different of K and such that $e_p(M) > 0$. All remaining $p-1$ members L of maximal class of the set $\Gamma_1(H)-\{K\}$ satisfy $e_p(L) = 0$, and all these L are G-invariant. Indeed, since $\{R_2, \dots, R_{p+1}\}$ is the class of conjugate in G subgroups, it follows that $K = R_2 \dots R_{p+1} \triangleleft G$. Next, all above mentioned $p(p-1)$ members of the set $\Gamma_1(H)$, by (b5), are not normal in G (otherwise, $R_2, \dots, R_{p+1}$ are normal in G). It follows that $p-1$ subgroups $L \in \Gamma_1(H)$ with $e_p(L) = 0$ are G-invariant, completing the proof of (b9). ∎

Let G be a group of Theorem 1.5(b). Taking into account that $D = \bigcap_{i=1}^{p+1} R_i$ is of order p^{p-1}, we get

$$\begin{aligned} \mathrm{c}_1(G) &= \mathrm{c}_1(D) + \sum_{i=1}^{p+1}(\mathrm{c}_1(R_i) - \mathrm{c}_1(D)) = 1 + p + \cdots + p^{p-2} + (p+1)p^{p-1} \\ &= 1 + p + \cdots + p^p. \end{aligned} \tag{1.1}$$

Therefore, the following result is of some interest.

THEOREM 1.6. *Let G be a p-group with $\exp(\Omega_1(G)) > p$. Then the following conditions are equivalent:*

(a) $e_p(G) = p + 1$.
(b) $\mathrm{c}_1(G) = 1 + p + \cdots + p^p$.

By (1.1), (a) $\Rightarrow$ (b). The reverse implication is a consequence of the following

LEMMA 1.7. *Let G be a p-group, $\exp(G) > p$, $\Omega_1(G) = G$ and $\mathrm{c}_1(G) = 1 + p + \cdots + p^p$. Then*

(a) *G is irregular of order p^{p+2}; all members of the set Γ_1 have exponent p^2.*
(b) *$\mathrm{d}(G) = 3$, $\Phi(G) = G'$ is of order p^{p-1} and exponent p.*
(c) *$G/\mho_1(G)$ is of order p^{p+1} so $\mho_1(G) = \mathrm{K}_p(G)$ is of order p.*
(d) *$\mathrm{c}_2(G) = p^p$.*
(e) *$\Gamma_1 = \{M_1, \dots, M_{p^2}, T_1, \dots, T_{p+1}\}$, where $M_1, \dots, M_{p^2}$ are of maximal class, $T_1, \dots, T_{p+1}$ are regular of exponent p^2 and $\eta(G) = \bigcap_{i=1}^{p+1} T_i$ has exponent p^2 and index p^2 in G.*
(f) *$e_p(G) = p + 1$, all subgroups of order p^p and exponent p contain $\Phi(G)$ so these subgroups are normal in G.*
(g) *Exactly p^2 subgroups of G of order p^p, containing $\Phi(G)$, have exponent p^2.*
(h) *Let $L \in \Gamma_2$. If $L \neq \eta(G)$, then exactly p members of the set Γ_1, containing L, are of maximal class.*

PROOF. We have $|G| > |\{x \in G \mid o(x) \le p\}| = 1 + (p-1)\mathrm{c}_1(G) = p^{p+1}$ since $\exp(G) > p$. By Lemma J(k), G is irregular. By Lemma J(j), G is not of maximal class so there is $R \triangleleft G$ of order p^p and exponent p (Lemma J(a)).

(a) Set $\sigma(G) = [p^{-p} \cdot \mathrm{c}_1(G)]$, where $[x]$ is the integer part of a real number x; then $\sigma(G) = 1$. By [BJ2, Theorem 2.1], $|G| \le p^{p+1+\sigma(G)} = p^{p+2}$ whence $|G| = p^{p+2}$. It follows from $\Omega_1(G) = G$ that $G/R \cong \mathrm{E}_{p^2}$ so $\exp(G) = p^2$ and $\exp(H) = p^2$ for all $H \in \Gamma_1$ since $\mathrm{c}_1(G) > \mathrm{c}_1(H)$.

(b) If $x \in G - R$ is of order p and $M = \langle x, R\rangle$, then $\exp(M) > p$, by the previous two paragraphs, so $M \in \Gamma_1$ is of maximal class (Lemma J(k)); then $\mathrm{d}(G) = 3$, by Lemma J(i), and we conclude that $\Phi(G) = G' = \Phi(M) = M'$ has exponent p.

(c) follows from Lemma J(i).

(d) By (a), $\mathrm{c}_2(G) = \frac{|G|-(p-1)\mathrm{c}_1(G)-1}{\varphi(p^2)} = p^p$ (here $\varphi(*)$ is Euler's totient function).

(e) The first assertion follows from Lemma J(i). Assume that $\exp(\eta(G)) = p$. If $x \in G - \eta(G)$ is of order p, then $\mathrm{cl}(\langle x, \eta(G)\rangle) < p$ so the subgroup $\langle x, \eta(G)\rangle \in \Gamma_1$ is regular of order p^{p+1} and exponent p (Lemma J(k)), contrary to (a).

(f) Assume that S is a nonnormal subgroup of order p^p and exponent p in G; then $\Phi(G) = G' \not\le S$ so $H = S\Phi(G) \in \Gamma_1$. We have $\Omega_1(H) = H$ and, by (a), $\exp(H) = p^2$ so H is irregular, i.e., H is of maximal class (Lemma J(k)); in that case, as we have proved, $\Phi(G) = \Phi(H)$. Then, since $S \in \Gamma_1(H)$, we get $\Phi(G) = \Phi(H) < S$, contrary to the assumption. Thus, all subgroups of order p^p and exponent p are normal in $G(= \Omega_1(G))$ so contain $G' = \Phi(G)$. If $e_p(G) = t$, then

$$\begin{aligned} 1 + p + \cdots + p^{p-2} + (p+1)p^{p-1} &= \mathrm{c}_1(G) = \mathrm{c}_1(\Phi(G)) + tp^{p-1} \\ &= 1 + p + \cdots + p^{p-2} + tp^{p-1} \end{aligned}$$

so $t = p + 1$.

(g) follows from (a), (b) and (f).

(h) By (e), the intersection of two distinct regular members of the set Γ_1 coincides with $\eta(G)$. Let $L \ne \eta(G)$ be a normal subgroup of index p^2 in G; then L is contained in at most one regular maximal subgroup of G and $G/L \cong \mathrm{E}_{p^2}$ since $G = \Omega_1(G)$. Let D be a G-invariant subgroup of index p^2 in L. Set $C = \mathrm{C}_G(L/D)$; then $|G : C| \le p$. Let $L < H \le C$, where $H \in \Gamma_1$; then H is regular since H/D is abelian of order p^3 (Lemma J(k)). It follows that L is contained in exactly one regular member of the set Γ_1 so it contained in exactly p irregular members of that set. ∎

Let $G = D * C$, where D is of maximal class and order p^{p+1}, C is cyclic of order p^2 and $D \cap C = \mathrm{Z}(D)$; then $e_p(G) = p+1$. Indeed, by [Ber2, Appendix 16, Exercise A], we have $\mathrm{c}_1(G) = 1 + p + \cdots + p^p$ so $\Omega_1(G) = G$, and then, by Lemma 1.7, $e_p(G) = p + 1$.

Proof of Theorem 1.6. It remains to show that (b) $\Rightarrow$ (a). Let $H = \Omega_1(G)$; then $\exp(H) > p$, by hypothesis. As in the proof of Lemma 1.7(a), we get $|H| \le p^{p+2}$. By Remark 1.1, however, $|H| > p^{p+1}$. Thus, $|H| = p^{p+2}$. Next, H has no maximal subgroup which has exponent p (indeed, if F is such a subgroup, then $\mathrm{c}_1(G) > \mathrm{c}_1(F) = 1 + p + \cdots + p^p$). In that case, by Lemma 1.7, applied to H, we get $e_p(H) = p + 1$. But $e_p(G) = e_p(H)$. $\square$

2. p-groups G with small $|\Omega_i(G)|$ $(i = 1, 2)$

We begin with the following remark which deals with a partial case of Proposition 2.2.

Remark 2.1. Let G be a p-group of exponent $> p$ such that $|\Omega_2(G)| = p^{p+2}$, $\Omega_1(G) = F < H = \Omega_2(G)$, $e_p(G) > p + 1$. Then $\mathrm{d}(F) > 2$ so F is of order p^{p+1} and exponent p, and we conclude that G is not of maximal class [Bla]. Then $H/F = \Omega_1(G/F)$ is of order p so G/F is either cyclic or generalized quaternion.

The p-groups G satisfying $|\Omega_2(G)| = p^{p+1}$ are classified in [Ber1, Lemma 2.1]. Now we consider the p-groups G, $p > 2$, satisfying $|\Omega_2(G)| = p^{p+2}$. (The 2-groups G satisfying $|\Omega_2(G)| = 2^4$, are classified in [Jan3].)

Proposition 2.2. *Let G be a p-group, $p > 2$, $|G| > p^{p+2} = |\Omega_2(G)|$. Then*

(a) *G has a normal subgroup $E \cong \mathrm{E}_{p^3}$.*
(b) *G/E is either absolutely regular or irregular of maximal class.*
(c) *Let G/E be irregular of maximal class. Then $p = 3$, $\Omega_1(G/E) \cong \mathrm{E}_{3^2}$ and E is the unique normal subgroup $\cong \mathrm{E}_{3^3}$ in G. Next, E is a maximal normal subgroup of exponent 3 in G.*
(d) *If $M \lhd G$ is of order p^{p+1} and exponent p, then G/M is cyclic.*
(e) *If $p > 3$, then G/E is absolutely regular.*
(f) *If $p = 3$ and G/E is irregular of order $\ge 3^5$, then $E \le \mathrm{Z}(\Omega_2(G))$ so $cl(\Omega_2(G)) \le 2$ and $E = \Omega_1(G)$. Next, $E < \Phi(G)$.*

Proof. (a) In view of $\Omega_2(G) < G$, G is not of maximal class; then $\Omega_2(G)$ is not of maximal class as well [Ber1, Remark 7.8]. It follows from $p + 2 \ge 3 + 2 = 5$ that G has a normal subgroup $E \cong \mathrm{E}_{p^3}$, by Blackburn's Theorem (see [Ber3, Theorem 6.1]).

(b) By hypothesis, $|\Omega_1(G/E)| < p^p$, so G/E is either absolutely regular or irregular of maximal class (Lemma J(a)).

(c,e) Suppose that G/E is irregular of maximal class; then $|G/E| \ge p^{p+1}$ (Lemma J(k)). Assume that $E < U \lhd G$, where U is of order p^4 and exponent p (Lemma J(g)). Then $|\Omega_1(G/U)| < p^{p-1}$ so G/U is absolutely regular (Lemma J(a,q)) and $|G/U| \ge p^p$, contrary to Lemma J(d). Thus, E is a maximal normal subgroup of G of exponent p. It follows from Lemma J(a) that $p = 3$. Assume that E_1 is another normal elementary abelian subgroup of G of order 3^3. Then $\mathrm{cl}(EE_1) \le 2$, by Fitting's Lemma so $\exp(EE_1) = 3$ (Lemma J(k)), contrary to what has just been proved. The proof of (c) is complete. Now, (b) and (c) imply (e).

(d) follows since $\Omega_1(G/M) = \Omega_2(G)/M$ is of order p.

(f) Let L/E be the fundamental subgroup of G/E; then L/E is metacyclic but has no cyclic subgroup of index 3 [Ber2, Theorem 9.6] so $\Omega_1(L/E) = \Omega_2(G)/E \cong \mathrm{E}_{3^2}$. In that case, $L/\mathrm{C}_L(E)$ is isomorphic to a subgroup of E_{3^2} since a Sylow 3-subgroup of $\mathrm{Aut}(E)$ is nonabelian of order 3^3 and exponent 3, and we conclude that $\Omega_2(G) \leq \mathrm{C}_L(E)$. Then $\mathrm{cl}(\Omega_2(G)) \leq 2$ so $\Omega_1(G) = \Omega_1(\Omega_2(G)) = E$, by (c).

Assume that $E \not\leq \Phi(G)$. Then $G = EM$ for some $M \in \Gamma_1$. In that case, M has no G-invariant subgroup $\cong \mathrm{E}_{3^3}$ so, by [Ber4, Theorem 6], M has no normal subgroup $\cong \mathrm{E}_{3^3}$. Then, M is of maximal class since $M/(M \cap E) \cong G/E$ is irregular. In that case, by [Ber1, Remark 7.8], $M = \Omega_2(M) \leq \Omega_2(G)$, a contradiction, since $|M| = 3^2|G/E| \geq 3^7 > 3^5 = |\Omega_2(G)|$. □

Proposition 2.3. *Let G be a p-group, $p > 2$. Suppose that $|\Omega_1(\mathrm{Z}(G))| = p^n$. Let $\mathcal{E}_k$ be the set of elementary abelian subgroups of order p^k in G. Then*

(a) If $k \leq n$, then $|\mathcal{E}_k| \equiv 1 \pmod p$.

(b) If $\Omega_1(\mathrm{Z}(G)) < \Omega_1(G)$, then $|\mathcal{E}_{n+1}| \equiv 1 \pmod p$.

Proof. One may assume in (a) that $\Omega_1(\mathrm{Z}(G)) < \Omega_1(G)$; then every maximal elementary abelian subgroup U of G has order at least p^{n+1}. Suppose that we have proved that $|\mathcal{E}_{k-1}| \equiv 1 \pmod p$. Write

$$\mathcal{E}_{k-1} = \{A_1, \dots, A_r\},\ \mathcal{E}_k = \{B_1, \dots, B_s\},\ V = \Omega_1(\mathrm{Z}(G)).$$

If $A_i \leq V$, then, taking $x \in \Omega_1(G) - V$, we see that $A_i < \langle x, A_i\rangle \in \mathcal{E}_k$. If $A_i \not\leq V$, then $A_i < B_j \in \mathcal{E}_k$, where $B_j = \langle x, A_i\rangle$ for $x \in V - A_i$. Thus, in any case, $A_i < B_j$ for some j. By assumption, $r \equiv 1 \pmod p$. Let α_i be the number of members of the set $\mathcal{E}_k$, containing A_i, and let β_j be the number of members of the set $\mathcal{E}_{k-1}$ contained in B_j. By [Ber4, Theorem 1], $\alpha_i \equiv 1 \pmod p$ for all i. By Sylow's Theorem, $\beta_j \equiv 1 \pmod p$ for all j. Therefore, by double counting, $1 \equiv r \equiv \alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s \equiv s \pmod p$. Part (a) is proved. The same argument also suits for proof of (b). □

Proposition 2.3 is not true for $p = 2$ as the group $G \cong \mathrm{D}_8$ shows.

The following result supplements the previous one.

Proposition 2.4. *Let G be a nonabelian p-group, $|\mathrm{Z}(G)| = p^n$ and let $k \leq n+1$. Let $\mathcal{A}_i$ be the set of normal abelian subgroups of order p^i in G. Then $|\mathcal{A}_k| \equiv 1 \pmod p$.*

Proof. Write $\mathcal{A}_{k-1} = \{U_1, \dots, U_r\}$, $\mathcal{A}_k = \{V_1, \dots, V_s\}$. Since $k \leq n+1$, the sets $\mathcal{A}_{k-1}$ and $\mathcal{A}_k$ are nonempty. We have to prove that $s \equiv 1 \pmod p$. We use induction on k. By induction, $r \equiv 1 \pmod p$. Let α_i be the number of members of the set $\mathcal{A}_k$ that contain U_i and let β_j be the number of members of the set $\mathcal{A}_{k-1}$ that contained in V_j. By Sylow, $\beta_j \equiv 1 \pmod p$. Let $U_i \leq \mathrm{Z}(G)$

and let $T/U_i \triangleleft G/U_i$ be of order p; then $T = V_j \in \mathcal{A}_k$ for some j. If $U_i \not\leq \mathrm{Z}(G)$ and $T/U_i \leq U_i\mathrm{Z}(G)/U_i$ is of order p, then $T = V_j \in \mathcal{A}_k$. It follows, by the double counting, that $\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s \equiv s \pmod p$ so it suffices to prove that $\alpha_i \equiv 1 \pmod p$ for all i. Let $\mathcal{M}_i$ be the set of all members of the set $\mathcal{A}_k$ that contain U_i; then $|\mathcal{M}_i| = \alpha_i$. All members of the set $\mathcal{M}_i$ are contained in $\mathrm{C}_G(U_i)$. Therefore, without loss of generality, one may assume that $\mathrm{C}_G(U_i) = G$. Let $D = \langle H \mid H \triangleleft G \in \mathcal{M}_i\rangle$; then D/U_i is elementary abelian. If $V/U_i \leq D/U_i$ is of order p, then $V \in \mathcal{M}_i$ since $D/U_i \leq \mathrm{Z}(G/U_i)$, so $\alpha_i \equiv |\mathcal{M}_i| = \mathrm{c}_1(D/U_i) \equiv 1 \pmod p$, and we are done. ☐

Proposition 2.5. *Let p^p be the maximal order of subgroups of exponent p in a p-group G. Then either $|\Omega_1(G)| = p^p$ or the intersection K of all subgroups of order p^p and exponent p in G has order p^{p-1}, and K is the unique normal subgroup of order p^{p-1} and exponent p in G.*

Proof. If $e_p(G) = 1$, then $|\Omega_1(G)| = p^p$ (see Case 2, preceding Theorem 1.5). Now we let $e_p(G) > 1$; then G is irregular (indeed, let R and S be two distinct subgroups of G of order p^p and exponent p and $V = \langle R, S\rangle$; then $\exp(V) > p$, by hypothesis, and the claim follows, by Lemma J(k)). One may assume that G is not of maximal class since for such groups the assertion is true, by Lemma J(e)(i). Then G contains a normal subgroup R of order p^p and exponent p (Lemma J(a)). We have $R < \Omega_1(G)$. Now let F_0 be a subgroup of order p^p and exponent p in G, $F_0 \neq R$. Let R_0 be a G-invariant subgroup of R minimal such that $R_0 \not\leq F_0$. Set $F = F_0R_0$; then $\Omega_1(F) = F$ and $|F| = p^{p+1}$. By hypothesis, $\exp(F) > p$ so F is irregular hence it is of maximal class (Lemma J(k)). In that case, $|R_0| = p^p = |R|$ (otherwise, if $|R_0| < p^p$, then $R_0 \leq \Phi(F) < F_0$, and we get $F = R_0F_0 = F_0 < F$) so $R_0 = R$. In particular, F_0 contains all proper G-invariant subgroups of R so that $F_0 \cap R = K = \Phi(F)$. Thus, K is the intersection of all subgroups of order p^p and exponent p in G. Since every G-invariant subgroup of order p^{p-1} and exponent p is contained in at least two distinct subgroups of order p^p and exponent p, it coincides with K. ☐

3. Groups and subgroups of maximal class

In this section we study subgroups of maximal class in a p-group. We also prove a number of new assertions on p-groups of maximal class.

Theorem 3.1. *Let G be a p-group and $M < G$ be of maximal class.*

(a) *Write $D = \Phi(M)$, $N = \mathrm{N}_G(M)$ and $C = \mathrm{C}_N(M/D)$. Let t be the number of subgroups $K \leq G$ of maximal class such that $M < K$ and $|K : M| = p$. Then t equals the number of subgroups of order p in N/M not contained in C/M. If $C = M$, then G is of maximal class. If $C > M$, then t is a multiple of p.*

(b) *Suppose, in addition, that M is irregular and G is not of maximal class. Let a positive integer k be fixed. Then the number t of subgroups $L < G$ of maximal class and order $p^k|M|$ such that $M < L$, is a multiple of p.*

PROOF. (a) All subgroups of G of order $p|M|$ that contain M, are contained in N. Note that $|N : C| \leq |\mathrm{Aut}(M/D)|_p = p$. First assume that $M < C$. If K/M is a subgroup of order p in C/M, then K/D is abelian of order p^3 so K is not of maximal class. Now let K/M be a subgroup of order p in N/M not contained in C/M. Then K/D is nonabelian of order p^3. Since $D = \Phi(M) \leq \Phi(K)$, it follows that $\mathrm{d}(K) = \mathrm{d}(K/D) = 2$ so K is of maximal class, by Lemma J(i). If $C = N$, then $t = 0$. If $C = M$, then $|N : M| = p$ and N is of maximal class, by the above; then G is also of maximal class (Lemma J(d)). Now let $M < C < N$; then the number of subgroups of order p in C/M is $\equiv 1 \pmod p$ so the number of subgroups $L/M < N/M$ of order p not contained in C/M, is a multiple of p (Sylow); since L, by the above, is of maximal class, we get $t \equiv 0 \pmod p$.

(b) Let $\mathcal{M}$ be the set of all wanted subgroups. One may assume that $\mathcal{M} \neq \emptyset$.

If $k = 1$, the assertion follows from (a). Indeed, assume that p does not divide t. It follows from (a) that then $C = M$ and N is of maximal class so G is also of maximal class (Lemma J(d)), contrary to the hypothesis. Now let $k > 1$. We proceed by induction on k. Let $\mathcal{N} = \{P_1, \dots, P_u\}$ be the set of subgroups of maximal class and order $p^{k-1}|M|$ in G containing M (by Lemma J(h), $\mathcal{N} \neq \emptyset$ since $\mathcal{M} \neq \emptyset$). By induction, $u \equiv 0 \pmod p$. Let $\mathcal{M}_i = \{V_1, \dots, V_a\}$ and $\mathcal{M}_j = \{W_1, \dots, W_b\}$ be the sets of those subgroups of maximal class and order $p|P_1|$ in G which contain P_i and P_j, respectively, $i \neq j$. By (a), a and b are multiples of p. Assume that $X \in \{V_1, \dots, V_a\} \cap \{W_1, \dots, W_b\}$. Then P_i and and P_j are distinct subgroups of index p in X so $X = P_iP_j$. Since X is of maximal class, we get $\mathrm{d}(X) = 2$ so $P_i \cap P_j = \Phi(X)$. Since $M \leq P_i \cap P_j = \Phi(X)$ and $\Phi(X)$ is absolutely regular (Lemma J(f)) and M is irregular, we get a contradiction. Thus, $\{V_1, \dots, V_a\} \cap \{W_1, \dots, W_b\} = \emptyset$. Clearly, in this way we have counted all members of the set $\mathcal{M}$. It follows that $\mathcal{M} = \bigcup_{i=1}^{u} \mathcal{M}_i$ is a partition, and we conclude that $t = \sum_{i-1}^{u} |\mathcal{M}_i| \equiv 0 \pmod p$. ∎

If $M < G$ are irregular p-groups of maximal class and $p^k \leq |G : M|$, then the number of subgroups of G of maximal class and order $p^k|M|$ that contain M, equals 1. Indeed, if M_1 and M_2 are distinct irregular subgroups of maximal class and the same order in G, then $M_1 \cap M_2$ is absolutely regular.

REMARK 3.2. Let $A < G$, where G is a p-group. If every subgroup of G of order $p|A|$ containing A, is of maximal class, then G is also of maximal class (here we do not assume, as in Theorem 3.1(a), that A is of maximal class; obviously, $|A| > p$). Indeed, assume that G is not of maximal class. By Lemma J(d), $N = \mathrm{N}_G(A)$ is not of maximal class. Then, by hypothesis, $|N : A| > p$. To obtain a contradiction, it suffices to assume that $N = G$; then $A \triangleleft G$. Let D be a G-invariant subgroup of index p^2 in A. Set $C = \mathrm{C}_G(A/D)$; then $|G : C| \le p$ so $A < C$. If B/A is a subgroup of order p in C/A, then B/D is abelian of order p^3 so B is not of maximal class, contrary to the hypothesis.

Theorem 3.1(b) is also true if $|M| = p^p$. Indeed, consider part (b) for $k > 1$ since case $k = 1$ follows from part (a). In that case, $p > 2$ and $M \not\le \Phi(X)$, where X is such as in the proof of the theorem since $\Phi(X)$ is absolutely regular (Lemma J(f)). Now the proof is continued as in the proof of Theorem 3.1(b).

Theorem 3.3. *Suppose that a subgroup of maximal class H is normal in a p-group G and G/H is cyclic of order $> p$. If $|H| > p^{p+1}$, then G has only one normal subgroup of order p^p and exponent p.*

Proof. The group G is not of maximal class since $G/G' \ncong \mathrm{E}_{p^2}$. Set $\Phi = \Phi(H)$, $C = \mathrm{C}_G(H/\Phi)$; then $|G : C| \le p$ and C/Φ is abelian of rank 3 since, if $L/H = \Omega_1(G/H)$, then L is not of maximal class so $\mathrm{d}(L) = 3$, by Lemma J(i). Since C is neither absolutely regular nor of maximal class, it contains a G-invariant subgroup R of order p^p and exponent p (Lemma J(b)). Since $|H| > p^{p+1}$, we get $R \not\le H$ (Lemma J(h)).

Let H_1 be the fundamental subgroup of H; then H_1 is characteristic in H so normal in G. Since G/H is cyclic of order $> p$, we get $\Omega_1(G) \le HR$ and $|HR| = p|H|$ so $H \cap R = H_1 \cap R$ has order p^{p-1} hence $|H_1 R| = p|H_1| = |H|$, by the product formula. Next, $\Omega_1(H_1 R) = R$ (Lemma J(n)) since $H_1 R$ is neither absolutely regular nor of maximal class and absolutely regular subgroup $H_1 \in \Gamma_1(H_1 R)$ (Lemma J(h)). Assume that G has another normal subgroup R_1 of order p^p and exponent p. Then $R_1 H = RH$ since $R_1 < \Omega_1(G) \le RH$, and $R \cap R_1 = H \cap R = H_1 \cap R$ is of order p^{p-1} (indeed, H has exactly one normal subgroup of order p^{p-1}, namely, $\Omega_1(H_1)$). By Lemma J(b), $e_p(G) \ge p+1$.

Assume that $R_2 \triangleleft G$ is of order p^p and exponent p such that $R_2 \not\le RR_1$. We have $R \cap R_2 = R \cap R_1 = R \cap H$ (see the previous paragraph). Then $H \cap RR_1 = H \cap RR_2 = T$, where T is absolutely regular of order p^p (note that $RR_1, RR_2 \le \Omega_1(G) \le HR$). In that case, $TR_1 = TR = RR_1$, $TR_2 = TR$ so $TR_1 = TR_2 = RR_1$, hence $R_2 < RR_1$, contrary to the assumption. Thus, $R_2 < RR_1$, i.e., all G-invariant subgroups of order p^p and exponent p are contained in RR_1. As we know, $|RR_1| = p^{p+1}$. Since H has no normal subgroup of order p^p and exponent p, $\exp(H \cap (RR_1)) > p$ so $\exp(RR_1) > p$. By Lemma J(k), RR_1 is irregular so of maximal class whence $\mathrm{d}(RR_1) = 2$. Since all $e_p(G) \ge p+1$ normal subgroups of order p^p and exponent p are maximal subgroups of the 2-generator group RR_1, by what has just been proved, we conclude that $\exp(RR_1) = p$, a contradiction. Thus, R_1 does not exist. ∎

Let $H \in \mathrm{Syl}_p(\mathrm{S}_{p^2})$, $p > 2$. As $G = H \times \mathrm{C}_{p^2}$ shows, Theorem 3.3 is not true for $|H| = p^{p+1}$.

Let $\mathcal{M}_n(G)$ be the set of subgroups of maximal class and order p^n in a p-group G of order p^m, and write $\mu_n(G) = |\mathcal{M}_n(G)|$. By Lemma J(i), if $m > 3$, then $\mu_{m-1}(G) \equiv 0 \pmod{p^2}$, unless G is of maximal class. By Mann's Theorem 5.3 below, we also have $\mu_3(G) \equiv 0 \pmod{p^2}$ provided $m \geq 5$. Therefore, it is natural to study the p-groups G satisfying $\mu_n(G) = p^2$ for $n \geq 3$. Note that, if G is of maximal class and $n > p$, then $G = \langle A \mid A \in \mathcal{M}_n(G)\rangle$.

Theorem 3.4. *Let G be a group of order p^m, $3 \leq n < m$ and $\mu_n(G) = p^2$. Take $S \in \mathcal{M}_n(G)$ and set $N = \mathrm{N}_G(S)$, $D = \langle A \mid A \in \mathcal{M}_n(G)\rangle$. Then one of the following holds:*

(a) $G = D$ is of maximal class and $m = n + 2$.

(b) $|D| = p^{n+1}$, $\mathrm{d}(D) = 3$, $\mathrm{c}_1(N/S) = 1$, i.e., N/S is either cyclic or generalized quaternion.

Proof. We use the notation introduced in the statement of the theorem. We have $|G : N| \leq \mu_n(G) = p^2$. Set $C = \mathrm{C}_N(S/\Phi(S))$.

(i) Suppose that $|N : S| > p$. Then $C/\Phi(S) > S/\Phi(S)$ in view of $|N : C| \leq |\mathrm{Aut}(S/\Phi(S))|_p = p$. Take a subgroup U/S of order p in C/S; then $U/\Phi(S)$ is abelian of order p^3 so U is not of maximal class. In that case, by Lemma J(i), $|\mathcal{M}_n(U)| = p^2 = |\mathcal{M}_n(G)|$ so $U = D$, $|D| = p^{n+1}$, $\mathrm{d}(D) = 3$. It follows that $\mathrm{c}_1(N/S) = 1$. Indeed, let V/S be a subgroup of order p in N/S and $V \neq U (= D)$. Since all members of the set $\mathcal{M}_n(G)$ are contained in U, S is the unique member of the set $\mathcal{M}_n(G)$, which contained in V, and this is impossible (Lemma J(i)). Thus, $\mathrm{c}_1(N/S) = 1$, i.e., N/S is either cyclic or generalized quaternion, and G is as stated in (b).

(ii) Now let $|N : S| = p$ for all $S \in \mathcal{M}_n(G)$ (then N/S is cyclic).

(ii1) Suppose that $\mathrm{d}(N) = 2$. Then N is of maximal class (Lemma J(i)) so G is also of maximal class (Lemma J(d)). Since $1 < \mu_n(N) \leq p$, we get $N < D$ and D is of maximal class (Lemma J(d)). Assume that $|G : N| = p^2$; then all members of the set $\mathcal{M}_n(G)$ are conjugate in G so $D \in \Gamma_1$ and $|G| = |G : N||N| = p^{n+3}$. If $n > p$, then $D = G$ (see the paragraph, preceding the theorem), a contradiction. Therefore, if $D < G$, we get $D \in \Gamma_1$ and $n \leq p$ so $p > 2$. Since $\mu_{m-1}(G) > 1$, there is $T \in \Gamma_1 - \{D\}$ which is of maximal class. Since $\mu_{n+1}(T) > 1$, T contains a subgroup U of maximal class and index p which is not contained in D (indeed, $T = \langle K \mid K \in \mathcal{M}_n(T)\rangle$). Similarly, $\mu_n(U) > 1$ so U contains a subgroup V of maximal class and index p which is not contained in D, contrary to definition of D since $|V| = p^n$. Thus, $|G : N| = p$ so $D = G$, $m = n + 2$, and G is as stated in (a).

(ii2) Now let $\mathrm{d}(N) = 3$. Then $N = D$ since $\mu_n(N) = p^2$ (Lemma J(i)), and G is as stated in (b). ∎

Remark 3.5. Let $H < G$, where H is a nonnormal subgroup of G of order p^p and exponent p and let the p-group G be not of maximal class. Suppose that H^G, the normal closure of H in G, is irregular of maximal class. We claim that then G has a normal subgroup F of order p^p and exponent p such that $|HF| = p^{p+1}$ and $H \cap F \triangleleft G$. Indeed, it follows from $|H^G| \geq p^{p+1}$ that $R = \Omega_1(\Phi(H^G))$ is G-invariant of order p^{p-1} and exponent p and $R < H$ (Lemma J(e)(i)). By Lemma J(g), $R < F$, where $F \triangleleft G$ is of order p^p and exponent p. Then $H \cap F = R \triangleleft G$ so $|HF| = p^{p+1}$, by the product formula.

Remark 3.6. Let G be a p-group of order p^m, $m > p+1$, and let $M \in \Gamma_1$. If G contains a subgroup H of order p^{p+1} such that $H \not\leq M$, and all such H are of maximal class, then G is also of maximal class. Indeed, if $m = p+2$, then $\mathcal{M}_{m-1}(G) = \Gamma_1 - \{M\}$ so $|\mathcal{M}_{m-1}(G)| \not\equiv 0 \pmod{p^2}$, hence G is of maximal class, by Lemma J(i). Now let $m > p+2$ and H be as above. Let $R \neq M \cap H$ be a maximal subgroup of H. Then R is a maximal regular subgroup of G, by hypothesis, and we conclude that G is of maximal class (Lemma J(e)(ii)) since $|R| = p^p$.

Remark 3.7. Let G be an irregular p-group of maximal class and order $> p^{p+1}$, $p > 2$. Let us estimate $p^a = \max\{|A| \mid A < G, A' = \{1\}, A \not\leq G_1\}$, where G_1 is the fundamental subgroup of G. It follows from description of subgroups of G ([Bla1] and [Ber2, Theorems 9.5 and 9.6]) that $a \leq p$. We claim that $a < p$. Assume that this is false, and let $A < G$ be an abelian subgroup of order $\geq p^p$ such that $A \not\leq G_1$. Then $|G : A| > p$ (otherwise, $A = G_1$). Let $A < M < G$, where $|M : A| = p$. Then M is of maximal class [Ber2, Theorem 13.19] so A is characteristic in M, by Fitting's Lemma. Since $\mathrm{N}_G(M)$ is of maximal class and order $\geq p^{p+2}$ and $\mathrm{N}_G(M) \leq \mathrm{N}_G(A)$ so $\mathrm{N}_G(A)$ is also of maximal class, we get, by Lemma J(f), $A \leq \Phi(\mathrm{N}_G(A)) \leq \Phi(G) < G_1$, a contradiction (in fact, according to the deep result from [Bla1], $a \leq 2$).

Remark 3.8. Let H is a nonnormal subgroup of a p-group G, $|G| > p^{p+1}$, $|H| > p^2$ and $\mathrm{N}_G(H)$ is of maximal class. Then G is also of maximal class (Lemma J(d)) and $H \not\leq G_1$, where G_1 is the (absolutely regular) fundamental subgroup of G (indeed, $|\mathrm{Z}(\mathrm{G}_1)| > \mathrm{p}$). We claim that $|\mathrm{N}_G(H) : H| = p$. Assume that this is false. Then H is characteristic in $\mathrm{N}_G(H)$ (Lemma J(d)) so $\mathrm{N}_G(H) = G$, contrary to the hypothesis. Let $K \neq H \cap G_1$ be maximal in H and assume that $\mathrm{N}_G(K) > H$. Let $H < F \leq \mathrm{N}_G(K)$, where $|F : H| = p$; then $F = \mathrm{N}_G(H)$ (compare orders) so F is of maximal class. Since $|F : K| = |F : H||H : K| = p^2$ and $K \triangleleft F$, we get $K = \Phi(F) < \Phi(G) < G_1$ so $K = H \cap G_1$, a contradiction.

Remark 3.9. Suppose that a p-group G satisfies the following conditions: (i) G contains a proper abelian subgroup A of order $\geq p^p$. (ii) Whenever $A < H \leq G$ and $|H : A| = p$, then $|\mathrm{Z}(H)| = p$. Then: (a) G is of maximal class. (b) If $p > 2$, then A has index p in G. Indeed, let $A < H \leq G$

with $|H : A| = p$. Then H is of maximal class, by [Ber2, Lemma 1.1] and induction, and (a) follows from Remark 3.2. Now let $p > 2$. Using induction, one may assume that $|G : A| = p^2$, and obtain a contradiction. Let H be as above. Then A is characteristic in H (Fitting's Lemma) so normal in G. It follows that $A = \Phi(G)$. Then, by hypothesis, all members of the set Γ_1 are of maximal class, a contradiction since $\mathrm{C}_G(\mathrm{Z}_2(G)) \in \Gamma_1$ is not of maximal class. Thus, $|G : A| = p$, as required.

REMARK 3.10. Let A be a proper absolutely regular subgroup of a p-group G, $p > 2$, $\exp(A) > p$ such that, whenever $A < B \leq G$ with $|B : A| = p$, then $\Omega_1(B) = B$. Then G is of maximal class. If, in addition, $|A| > p^p$, then $A = G_1$. Assume that the first assertion is false; then $\mathrm{N}_G(A)$ is not of maximal class (Lemma J(d)). Therefore, one may assume that $\mathrm{N}_G(A) = G$. If $B/A \leq G/A$ is of order p, then, in view of $\exp(B) \geq \exp(A) > p$ and $\Omega_1(B) = B$, we conclude that B is irregular (Lemma J(k)). Assume that B is not of maximal class. Since B is also not absolutely regular, we get $B = A\Omega_1(B)$, where $\Omega_1(B)(= B)$ is of exponent p (Lemma J(n)), contrary to the hypothesis. Thus, every subgroup of G of order $p|A|$, containing A, is of maximal class so G is of maximal class, by Remark 3.2. Let, in addition, $|A| > p^p$ and assume that $A \neq G_1$. Then $|G : A| > p$. Let $A < B < T \leq G$ with $|B : A| = p = |T : B|$. Then $A \triangleleft T$ since A is characteristic in B, and T is of maximal class. It follows that $A = \Phi(T) \leq \Phi(G) < G_1$, a contradiction.

PROPOSITION 3.11. *Let R be a subgroup of order p of a nonabelian p-group G. If there is only one maximal chain connecting R with G, then either $\mathrm{C}_G(R) \cong \mathrm{E}_{p^2}$ (then G is of maximal class, by Lemma J(o)) or $G \cong \mathrm{M}_{p^{n+2}}$.*

PROOF. We have $\mathrm{C}_G(R) = R \times Z$, where Z is cyclic of order, say p^n. Assume that $n > 1$. We have $\Omega_1(\mathrm{C}_G(R)) = U \cong \mathrm{E}_{p^2}$. Then $\mathrm{N}_G(U)/U$ is cyclic so $\mathrm{N}_G(U) \cong \mathrm{M}_{p^m}$ since $n > 1$. Since $U = \Omega_1(\mathrm{N}_G(U))$ is characteristic in $\mathrm{N}_G(U)$, we get $\mathrm{N}_G(U) = G$.

Now let $n = 1$. In that case, any subgroup of G, properly containing U, is of maximal class (Lemma J(o)). Let $U \leq B < G$. Then $\mathrm{N}_G(B)$ is of maximal class so $|\mathrm{N}_G(B) : B| = p$ (Lemma J(b)) so G satisfies the hypothesis. ☐

THEOREM 3.12. *Let G be a p-group. Then the number of irregular members of maximal class in the set Γ_2 is a multiple of p.*

PROOF. Let Γ_2' be the set of all irregular members of maximal class in the set Γ_2. We may assume that $\Gamma_2' \neq \emptyset$; then G is not of maximal class, $\mathrm{d}(G) \leq 4$ and $|G| \geq p^{p+3}$. Let $\mathcal{M}$ be the set of all normal (irregular) subgroups of maximal class and index p^2 in G. Since $\Phi(G) \notin \Gamma_2'$ (the center of each member of the set Γ_2' is of order p), we get $\mathrm{d}(G) > 2$.

By Lemma J(i), $p \mid |\mathcal{M}|$ (this is the only place where we use irregularity of all members of the set Γ_2). Therefore, we may assume that $\mathcal{M} \neq \Gamma_2'$ so there is $H \triangleleft G$ of maximal class such that $G/H \cong \mathrm{C}_{p^2}$.

Assume that $\mathrm{d}(G) = 4$. Let $L \in \mathcal{M}$. Since $|G : \Phi(L)| = |G : L||L : \Phi(L)| = p^4 = |G : \Phi(G)|$ and $\Phi(L) \leq \Phi(G)$, we get $\Phi(L) = \Phi(G)$ so $L \in \Gamma_2'$, $\Gamma_2' = \mathcal{M}$, contrary to the assumption. Thus, $\mathrm{d}(G) = 3$, $|G/G'| = p^4$ so G/G' is abelian of type (p^2, p, p) and $G' = H'$ (compare indices!).

Let $F \in \Gamma_2'$; then $G' = F'$ (compare indices!). Set $T/G' = \Omega_1(G/G')$; then $T/G' \cong \mathrm{E}_{p^3}$. Since $G/F \cong \mathrm{E}_{p^2}$, there is $M/F < G/F$ of order p such that $M \neq T$. We have $M' = F' = G'$ since $|F : F'| = p^2$ and $G' = F' \leq M' \leq G'$, and so M/G' is abelian of type (p^2, p). Let L be a G-invariant subgroup of index p in G'. Then F/L is nonabelian of order p^3 since F is of maximal class. The group M/L is minimal nonabelian since $L < G' = M' < \Phi(M)$ so $\mathrm{d}(M) = \mathrm{d}(M/L) = 2$ and $(M/L)'$ is of order p [BJ2, Lemma 3.2(a)]. This is a contradiction: M/L contains a proper nonabelian subgroup F/L. Thus, H does not exist so $\mathcal{M} = \Gamma_2'$, completing the proof. □

Theorem 3.13. *Let G be an irregular p-group of order $> p^{p+1}$. If $K = \Omega_1(G) < G$ is of maximal class, then one of the following holds:*

(a) *If K is irregular, then G is of maximal class and $|G : K| = p$.*
(b) *If K is regular, then $p > 2$, K is of order p^p and exponent p and all maximal subgroups of G not containing K, are absolutely regular.*

Proof. Since $|\mathrm{Z}(K)| = p$ and K is noncyclic, we get $K \not\leq \Phi(G)$.

(i) Suppose that K is irregular; then $|K| \geq p^{p+1}$. If $|K| = p^{p+1}$, then G is of maximal class (Remark 1.1). If $|K| > p^{p+1}$, then $\mathrm{e}_p(G) = e_p(K) \equiv 0 \pmod p$ so G is of maximal class (Lemma J(b)). In both cases, $|G : K| = p$, by Lemma J(f).

(ii) Now let K be regular. Then $\exp(K) = p$ (Lemma J(k)) so $p > 2$: K is nonabelian. Since G is irregular, we get $|K| \geq p^{p-1}$ (Lemma J(q)).

If $|K| = p^{p-1}$, then G is of maximal class (Lemma J(a)). In that case, $K \leq \Phi(G)$, and K is not of maximal class (Lemma J(f)), a contradiction.

Therefore, since the order of regular p-group of maximal class is at most p^p, we must have $|K| = p^p$. If G is of maximal class, then $|G| = p^{p+1}$ (Lemma J(h)), and in this case (b) is true. Next assume that G is not of maximal class; then $|G| > p^{p+1}$. Then K has a G-invariant abelian subgroup $R \cong \mathrm{E}_{\mathrm{p}^2}$. Setting $\mathrm{C}_G(R) = M$, we get $K \not\leq M$ so $|G : M| = p$. Then $\Omega_1(M) = K \cap M$ is of order p^{p-1} and exponent p (recall that $K = \Omega_1(G)$) so M is absolutely regular since it is not of maximal class (Lemma J(a)). Now let $F \in \Gamma_1$ be of maximal class. Since $M \in \Gamma_1$ is absolutely regular, it follows that G is of maximal class (Lemma J(l)), a contradiction. Taking, from the start, $F \not\geq K$, we see that F is absolutely regular. Thus, all maximal subgroups of G not containing K, are absolutely regular. □

Proposition 3.14. *Let G be a p-group of exponent $> p$ and $H < G$ be either absolutely regular or of maximal class.*

(a) *If* $\mathrm{H}_p(G) \le H < G$, *then* G *is of maximal class. In that case,* G *is irregular,* $|G : \mathrm{H}_p(G)| = p$ *and* H *is absolutely regular.*
(b) *Let* $\exp(H) > p$. *If* $H \cap Z = \{1\}$ *for each cyclic* $Z < G$ *with* $Z \not\le H$, *then* G *is of maximal class.*

PROOF. (a) The group G is irregular (otherwise, $\mathrm{H}_p(G) = G$).

(i) If H is absolutely regular, then each subgroup of G of order $p|H|$, containing H, is generated by elements of order p so G is of maximal class (Remark 3.10).

(ii) Now suppose that H is of maximal class but not absolutely regular. Since $\exp(H) = \exp(G) > p$, we get $|H| \ge p^{p+1}$ so H is irregular (Lemma J(h)). Assume that $|H| > p^{p+1}$. Then $\mathrm{c}_1(G) \equiv \mathrm{c}_1(H) \pmod{p^p}$ so G is of maximal class (Lemma J(b)). Now let $|H| = p^{p+1}$. Assume that G is not of maximal class. In view of Theorem 3.1(b), one may assume that $|G : H| = p$. Let $T_1, \dots, T_{p+1}$ be all regular members of the set Γ_1 (Lemma J(i)); then $\Omega_1(T_i) = T_i$ so $\exp(T_i) = p$ for all i. It follows from $G = \bigcup_{i=1}^{p+1} T_i$ (Lemma J(i)) that $\exp(G) = p$, a contradiction.

(b) If $H < M \le G$ with $|M : H| = p$, then $H \ge \mathrm{H}_p(M)$ so M is of maximal class, by (a). Thus, all containing H subgroups of G of order $p|H|$ are of maximal class so G is of maximal class, by Remark 3.2. □

In proofs of known Proposition 3.15 and Corollaries 3.16 and 3.17 we use the description of the set Γ_1 only.

PROPOSITION 3.15. *Suppose that a* p*-group* G *of maximal class,* $p > 3$, *contains two distinct elementary abelian subgroups of order* p^{p-1}. *Then* $|G| = p^{p+1}$. *In particular, if* G *contains* $> p+1$ *elementary abelian subgroups of order* p^{p-1}, *then* G *is isomorphic to a Sylow* p*-subgroup of the symmetric group of degree* p^2.

PROOF. By [Ber1, Theorem 7.14(b)], there is $\mathrm{E}_{p^{p-1}} \cong E \lhd G$. Let $E_1 < G$ be another elementary abelian subgroup of order p^{p-1} and set $H = EE_1$. Then $|G| > p^p$ (otherwise, $G = H$ and, by Fitting's Lemma, $\mathrm{cl}(G) \le 2 < p$) so G is irregular (Lemma J(d)). It follows that $E \le \Phi(G)$ (Lemma J(f)). We claim that H is regular. Assume that this is false. Then $|H| \ge p^{p+1}$ so H is of maximal class and we get $E \le \Phi(H)$ so $H = EE_1 = E_1$, a contradiction. Thus, $\exp(H) = p$ (Lemma J(k)) so $|H| = p^p$ (recall that a p-group of maximal class has no subgroup of order p^{p+1} and exponent p), and then $\mathrm{cl}(H) \le 2$, by Fitting's Lemma.

Assume that $|G| > p^{p+1}$. We have $E = \Omega_1(\Phi(G))$. Next, H is nonabelian (Lemma J(p); see also Remark 3.7) so $\mathrm{Z}(H) = E \cap E_1$ has index p^2 in H. Let $A < H$ be minimal nonabelian; then $|A| = p^3$ since $\exp(A) = p$ (Lemma J(t)). By the product formula, $H = A\mathrm{Z}(H)$ so, if $\mathrm{Z}(H) = \mathrm{Z}(A) \times E_0$, then $H = A \times E_0$ so $H' = A'$. Since all subgroups of G, that contain H, are of maximal class, it follows that $H' = \mathrm{Z}(G)$. Let $H < F < M \le G$, where

$|F:H| = p = |M:F|$; then F and M are of maximal class. By Lemma J(f), H is not normal in M. Therefore, $H_1 = H^x \neq H$ for every $x \in M - F$ and $H_1 < F$. As above, $H_1' = \mathrm{Z}(G)$. In that case, $H/\mathrm{Z}(G)$ and $H_1/\mathrm{Z}(G)$ are two distinct abelian maximal subgroups of $F/\mathrm{Z}(G)$ so $\mathrm{cl}(F/\mathrm{Z}(G)) \leq 2$ (Fitting's Lemma). In that case, $\mathrm{cl}(F) \leq 3$, a contradiction since F is of maximal class and order p^{p+1} so $\mathrm{cl}(F) = p \geq 5$. Thus, $|G| = p^{p+1}$.

Let, in addition, $\{E_1, \dots, E_k\}$ be the set of elementary abelian subgroups of order p^{p-1} in G, and $k > p+1$. To prove that $G \cong \Sigma_{p^2}$, it suffices to show that G has an elementary abelian subgroup of index p (Lemma J(p)). Assume that this is false. By the above, one may assume that $E_1 = \Phi(G)$. Then, for $i > 1$, E_i is not normal in G so $N_i = \mathrm{N}_G(E_i) \in \Gamma_1$ and all conjugates of E_i are contained in N_i. Then $\mathrm{cl}(N_i) \leq 2$, $i > 1$ (Fitting's Lemma) so $\exp(N_i) = p$. The subgroup N_i $(i > 1)$ is nonabelian (otherwise, $\mathrm{d}(N_i) = p$ so $G \cong \Sigma_{p^2}$, by Lemma J(p)). Then N_2 has at most $p+1$ abelian subgroups of index p so one may assume that $\mathrm{N}_G(E_{p+2}) = N_{p+2} \neq N_2$. Again $\mathrm{cl}(N_{p+2}) = 2$. Then, by Fitting's Lemma,

$$\mathrm{cl}(G) = \mathrm{cl}(N_2 N_{p+2}) \leq \mathrm{cl}(N_2) + \mathrm{cl}(N_{p+2}) = 2 + 2 = 4 < p = \mathrm{cl}(G),$$

a contradiction. □

COROLLARY 3.16. *Let $p > 3$ and suppose that a p-group G of maximal class contains an abelian subgroup A such that* $\mathrm{d}(A) = p-1$ *and* $\exp(A) > p$. *Then $A \leq G_1$, where G_1 is the fundamental subgroup of G, and there is a G-invariant abelian subgroup B of order p^p such that $\Omega_1(A) < B \leq G_1$.*

PROOF. We have $|A| \geq p^p$. If $|G| = p^{p+1}$, then $A = G_1$, and we are done. Now let $|G| > p^{p+1}$. Then, by Proposition 3.15, $\Omega_1(A)$ is the unique elementary abelian subgroup of order p^{p-1} in G so $\Omega_1(A) = \Omega_1(\Phi(G))$. Then $A \leq \mathrm{C_G}(\Omega_1(\mathrm{A})) \leq \mathrm{C_G}(\mathrm{Z_2(G)}) = \mathrm{G_1}$ (here $\mathrm{Z}_2(G)$ is the second member of the upper central series of G) so $A < G_1$. By [Ber4, Theorem 1], $\Omega_1(A) < B \lhd G$, where B is abelian of order p^p. Since $|G:B| > p$, we get $B \leq \Phi(G) < G_1$. (We have $\exp(B) = p^2$, unless G is a Sylow subgroup of the symmetric group of degree p^2; see [Ber1, Theorem 5.2]). □

COROLLARY 3.17. *Let $p > 3$ and suppose that a p-group G of maximal class contains an abelian subgroup A with* $\mathrm{d}(A) = p-1$, $\exp(A) = p^k > p$ *and* $|A| = p^{(p-1)k-\epsilon}$, $\epsilon \in \{0,1\}$. *If $\epsilon = 0$, then $A \lhd G$. If $\epsilon = 1$, then there exists in G a normal abelian subgroup B such that $|B| = |A|$ and* $\exp(B) = p^k$. *We also have $A, B \leq G_1$.*

PROOF. By Corollary 3.16, $A \leq \Omega_k(G_1)$, and we are done if $\epsilon = 0$. If $\epsilon = 1$, then $\Omega_k(G_1)$ contains $\equiv 1 \pmod p$ abelian subgroups of order $|A|$ since $|\Omega_k(G_1) : A| \leq p$. □

REMARK 3.18. If every maximal abelian subgroup of a nonabelian p-group G is either cyclic or of exponent p, then one of the following holds:

(a) $\exp(G) = p$, (b) G is a 2-group of maximal class, (c) $p > 2$ and G is of maximal class and order p^{p+1} at most. Indeed, suppose that $\exp(G) > p$ and G is not a 2-group of maximal class. Then G has a maximal abelian subgroup, say A, which is cyclic. Since $\mathrm{Z(G)} < \mathrm{C_G(A)} = \mathrm{A}$, the center $\mathrm{Z}(G)$ is cyclic. Let $R \triangleleft G$ be abelian of type (p, p) and set $C = \mathrm{C}_G(R)$. Then $\mho_1(A) < C$ since $|\mathrm{Aut}(R)|_p = p$ and so $|G : C| = p$. Every maximal abelian subgroup, say B, of C contains R so noncyclic. If $B \le D < G$, where D is maximal abelian in G, then $\exp(D) = p$. It follows that $\exp(B) = p$, and we get $\exp(C) = p$ so $A \cong \mathrm{C}_{p^2}$. It follows from $\mathrm{C}_G(A) = A$ that G is of maximal class (Lemma J(o)). Since G has no subgroup of order p^{p+1} and exponent p (by induction and Lemma J(i)), we get $|G| = p|C| \le p^{p+1}$.

Remark 3.19. Let G be a p-group of order $> p^{p+1}$ such that it is not of maximal class and $|G/\mathrm{K}_p(G)| = p^p$. Then $\mathrm{K}_p(G)/\mathrm{K}_{p+1}(G)$ is noncyclic. Assume that this is false. Then $p > 2$, by Taussky's Theorem. By [Ber1, Theorem 5.1(b)], $G/\mathrm{K}_{p+1}(G)$ is not of maximal class so $|\mathrm{K_p(G)/K_{p+1}(G)}| > \mathrm{p}$. By the way of contradiction, assume that $\mathrm{K}_p(G)/\mathrm{K}_{p+1}(G) \cong \mathrm{C}_{p^2}$ and $\mathrm{K}_{p+1}(G) = \{1\}$. Obviously, $G/\Omega_1(\mathrm{K}_p(G))$ must be of maximal class. Let $\mathrm{E}_{p^2} \cong R \triangleleft G$ and $\Omega_1(\mathrm{K}_p(G)) < R$. However, $\mathrm{E}_{p^2} \cong R\mathrm{K}_p(G)/\Omega_1(\mathrm{K}_p(G)) \le \mathrm{Z}(G/\Omega_1(\mathrm{K}_p(G)))$, a contradiction.

Remark 3.20. Suppose that a p-group G is neither absolutely regular nor of maximal class. Then one of the following holds: (a) G has a characteristic subgroup of order $\ge p^p$ and exponent p, (b) G has an irregular characteristic subgroup H of class p such that $\Phi(H)$ is of order p^{p-1} and H is generated by G-invariant subgroups of order p^p and exponent p containing a fixed ($= \Phi(H)$) characteristic subgroup of G of order p^{p-1} and exponent p. Indeed, if G is regular, then $|\Omega_1(G)| \ge p^p$, and (a) holds (Lemma J(k)). Therefore, in what follows we may assume that G is irregular. We also assume that (a) is not true. By Lemma J(q), G' has a characteristic subgroup R of order $\ge p^{p-1}$ and exponent p; then R is characteristic in G and $|R| = p^{p-1}$. Let $H = \langle M \triangleleft G \mid R < M, |M| = p^p, \exp(M) = p\rangle$; then $\Omega_1(H) = H$, H is characteristic in G and so $|H| > p^p$ so H is irregular and then $\mathrm{cl}(H) = p$ since H/R is elementary abelian. By Lemma J(q), $R = \Phi(H)$.

Remark 3.21. Let G be a group of exponent p and order $p^m > p^p$. We claim that then $G/\mathrm{K}_p(G)$ is not of maximal class. Assume that this is false. Then $\mathrm{K}_p(G) > \{1\}$. Passing to quotient group, one may assume that $\mathrm{K}_p(G)$ is of order p. In that case, $\mathrm{cl}(G) = p$ so G is of maximal class and order p^{p+1}, contrary to Lemma J(h).

We divide the p-groups of maximal class and order $> p^{p+1}$ in three disjoint families.

Definition 3.22. *Let G be a group of maximal class and order p^m, $m > p + 1$. Then G is said to be*

(i) *a* $\mathcal{Q}_p$*-group, if* $|\Omega_1(G)| = p^{p-1}$,
(ii) *a* $\mathcal{D}_p$*-group, if* $\Omega_1(G) = G$,
(iii) *an* $\mathcal{SD}_p$*-group, if* $|\Omega_1(G)| = p^{m-1}$.

Motivation: a $\mathcal{Q}_2$-group is generalized quaternion, a $\mathcal{D}_2$-group is dihedral and an $\mathcal{SD}_2$-group is semidihedral. It follows from Lemma J(f) that, if G is of maximal class and order $> p^{p+1}$, it is one of the above three types.

Definition 3.23. *Let* G *be a* $\mathcal{D}_p$*-group of maximal class. Then* G *is said to be a* $\mathcal{D}_p^0$*-group if* $G_1 = \mathrm{H}_p(G) < G$*, and a* $\mathcal{D}_p^1$*-group if* $G = \mathrm{H}_p(G)$*, where* $H_p(G) = \langle x \in G \mid o(x) > p\rangle$.

Note that D_{2^m} is a $\mathcal{D}_2^0$-group so $\mathcal{D}_2^1$-groups do not exist. If G is either a $\mathcal{Q}_p$- or $\mathcal{SD}_p$-group, then $G = \mathrm{H}_p(G)$ so a p-group G of maximal class and order $> p^{p+1}$ is a $\mathcal{D}_p^0$-group if and only if $\mathrm{H}_p(G) < G$.

If G is a $\mathcal{D}_p^0$-group, then $\mathrm{H}_p(G) = G_1$ so all members of the set $\Gamma_1 - \{G_1\}$ are also $\mathcal{D}_p^0$-groups since all elements of the set $G - G_1$ have order p. If G is a $\mathcal{D}_p^1$-group, then the set $G - G_1$ has an element of order p^2 (by [B2, Theorem 13.19], the set $G - G_1$ has no elements of order $> p^2$). If a p-group G is of maximal class and order $> p^{p+2}$, then $G/\mathrm{Z}(G)$ is a $\mathcal{D}_p^0$-group.

Theorem 3.24. *Let* G *be a* p*-group of maximal class and order* p^m, $p > 2$, $m > p+2$*, and let* $\Gamma_1 = \{G_1, G_2, \dots, G_{p+1}\}$*, where* G_1 *is the fundamental subgroup of* G*. Then*

(a) *If* G *is a* $\mathcal{Q}_p$*-group, then* $G_2, \dots, G_{p+1}$ *are* $\mathcal{Q}_p$*-groups.*
(b) *If* G *is a* $\mathcal{D}_p^0$*-group, then* $G_2, \dots, G_{p+1}$ *are* $\mathcal{D}_p^0$*-groups.*
(c) G *has no maximal subgroup which is an* $\mathcal{SD}_p$*-group.*
(d) *Let* G *be an* $\mathcal{SD}_p$*-group and let* $\Omega_1(G) = G_2$*. Then* G_2 *is a* $\mathcal{D}_p$*-group and* $G_3, \dots, G_{p+1}$ *are* $\mathcal{Q}_p$*-groups.*
(e) *If* G *is a* $\mathcal{D}_p$*-group, then at least two of subgroups* $G_2, \dots, G_{p+1}$ *are* $\mathcal{D}_p$*-groups.*

Proof. Since 2-groups of maximal class are classified and the theorem holds for them, one may assume that $p > 2$. If $i > 1$, then G_i is of maximal class and so (a) is obvious.

(b) We have $\mathrm{H}_p(G) = G_1$, the fundamental subgroup of G. If $i > 1$, then $\mathrm{H}_p(G_i) \le G_i \cap G_1 = \Phi(G) < G_i$ so G_i is a $\mathcal{D}_p^0$-group.

(c) Let $M \in \Gamma_1$ be not a $\mathcal{Q}_p$-group; then $\gamma(M) = |G : \Omega_1(M)| \le p^2$. If $\gamma(M) = p^2$, then $\Omega_1(M) = \Phi(G)$ is absolutely regular and order $\ge p^{p+1}$, which is impossible. Thus, $\Omega_1(M) = M$ so M is a $\mathcal{D}_p$-group. This argument shows that the set Γ_1 has no members which are $\mathcal{SD}_p$-groups.

(d) By definition, G_2 is a $\mathcal{D}_p$-group. Let $i > 2$; then G_i is not an $\mathcal{SD}_p$-group, by (c). Since $\Omega_1(G_i) \le G_i \cap G_2 = \Phi(G)$ is absolutely regular so of order p^{p-1}, it follows that G_i is a $\mathcal{Q}_p$-group.

(e) By hypothesis, $\Omega_1(G) = G$. Let $R < G$ be of order p^p and exponent p and let $R < M \in \Gamma_1$. Since M is neither absolutely regular nor a $\mathcal{Q}_p$-group, we conclude that M is a $\mathcal{D}_p$-group, by (c). Let $x \in G - M$ be of order p; then $R_1 = \langle x, \Omega_1(G_1)\rangle$ is of order p^p and exponent p. A maximal subgroup L of G such that $R_1 < L$, is a $\mathcal{D}_p$-group and $L \neq M$. □

Below we do not use deep properties of p-groups of maximal class.

Proposition 3.25. *Let $B < G$ be nonabelian of order p^3, G is a p-group and $C_G(B) < B$. Then G is of maximal class and*

(a) *$Z_2(G) < B$.*
(b) *Each maximal subgroup $K \neq \mathrm{Z}_2(G)$ of B satisfies $C_G(K) = K$.*

Proof. Obviously, $\mathrm{Z}(G) < B$. By Lemma J(c), all subgroups between B and G are of maximal class.

(a) We have $B \neq \mathrm{Z}_2(G)$ since $|B| > p^2 = |\mathrm{Z}_2(G)|$. Assume that $\mathrm{Z}_2(G) \not\leq B$. Set $H = B\mathrm{Z}_2(G)$; then H is of maximal class and order p^4. In that case, $\mathrm{Z}_2(G) = \Phi(H)$ so $H = B\Phi(H) = B$, a contradiction. Thus, $\mathrm{Z}_2(G) < B$.

(b) Assume that $\mathrm{C}_G(K) \neq K$. Since $B < \mathrm{N}_G(K)$ and $\mathrm{C}_G(K) \lhd \mathrm{N}_G(K)$, then B normalizes $C_G(K)$. Next, $\mathrm{Z}_2(G) \not\leq \mathrm{C}_G(K)$ since $\mathrm{Z}_2(G)K = B$ is nonabelian. Let $U/K \leq \mathrm{C}_G(K)/K$ be of order p and $U \lhd \mathrm{N}_G(K)$. Set $F = UB$; then F is of class 3 and order p^4. In that case, U and $\mathrm{C}_F(\mathrm{Z}_2(G))$ are two distinct abelian maximal subgroups of F so $\mathrm{cl}(F) \leq 2$ (Fitting's Lemma), a contradiction. Thus, $\mathrm{C}_G(K) = K$. □

Proposition 3.26. *Suppose that a nonabelian group G of order $p^m > p^3$ has only one normal subgroup N of index p^3 and let K be a G-invariant subgroup of index p in N. Then one of the following holds:*

(a) *$\mathrm{d}(G) = 2$ and $G' < \Phi(G)$. In that case, $K = \{1\}$ and $G \cong \mathrm{M}_{p^4}$.*
(b) *$p > 2$, $\mathrm{d}(G) = 2$, $G' = \Phi(G)$, $N = \mathrm{K}_3(G)$, G/N is nonabelian of exponent p. In that case, G/K is of maximal class.*
(c) *$p = 2$, G is a 2-group of maximal class.*
(d) *$\mathrm{d}(G) = 3$, $N = \Phi(G) = G'$. Then $\mathrm{Z}(G/K)$ is cyclic of order p^2 and $G/K = (E/K)\mathrm{Z}(G/K)$, where E/K is nonabelian of order p^3 and $\mathrm{Z}(G/K) \cong \mathrm{C}_{p^2}$. If, in addition, $p > 2$ and $E_1/K = \Omega_1(G/K)$, then E_1/K is nonabelian of order p^3 and exponent p and $G/K = (E_1/K)\mathrm{Z}(G/K)$.*

Proof. We have $|G/G'| \leq p^3$ so $\mathrm{d}(G) \leq 3$. The hypothesis is inherited by nonabelian epimorphic images of G. If a minimal nonabelian p-group X has only one normal subgroup of index p^3, then either $|X| = p^3$ or $X \cong \mathrm{M}_{p^4}$ (Lemma J(t)).

(i) Suppose that $\mathrm{d}(G) = 2$. In that case, $G/\mathrm{K}_3(G)$ is minimal nonabelian so either its order equals p^3 or $G/\mathrm{K}_3(G) \cong \mathrm{M}_{p^4}$, by the previous paragraph.

Let $|G/G'| = p^3$; then $N = G' < \Phi(G)$, G/G' is abelian of type (p^2, p). In that case, G/K is minimal nonabelian so $\cong \mathrm{M}_{p^4}$. Assume that $K > \{1\}$. Let L be a G-invariant subgroup of index p in K. Then G/L has two distinct cyclic subgroups A/L and B/L of index p, and we get $A \cap B = \mathrm{Z}(G)$ so G/L is minimal nonabelian of order p^5, a contradiction. We obtained the group from (a).

Let $|G : G'| = p^2$. Then $N = \mathrm{K}_3(G)$ so G/K is of maximal class and order p^4. If $p = 2$, then G itself is of maximal class, by Taussky's Theorem. If $p > 2$, then, as in the previous paragraph, $\exp(G/N) = p$. We obtained groups from (b) and (c).

(ii) Suppose that $\mathrm{d}(G) > 2$; then $G/G' \cong \mathrm{E}_{p^3}$ so $N = G' = \Phi(G)$. Let E/K be a minimal nonabelian subgroup in G/K; then $E < G$ since $\mathrm{d}(G/K) = 3 > 2 = \mathrm{d}(E/K)$. By Lemma J(c), $G/K = (E/K)\mathrm{Z}(G/K)$. Since G/K has only one normal subgroup of order p, we conclude that $\mathrm{Z}(G/K)$ is cyclic. Let $p > 2$ and set $E_1/K = \Omega_1(G/K)$. Then E_1/K is of order p^3 since G/K is regular. It follows that E_1/K is nonabelian since $G/K = (E_1/K)\mathrm{Z}(G/K)$.
□

If a group G of order 2^6 has only one normal subgroup of index 2^3, then one of the following holds: (i) G is cyclic, (ii) G is of maximal class, (iii) G is the Suzuki 2-group (see [HS]).

We claim that if a metacyclic p-group G of order $> p^3$ has only one normal subgroup of index p^3 if and only if one of the following holds: (i) G is cyclic, (ii) G is a 2-group of maximal class, (iii) $G \cong \mathrm{M}_{\mathrm{p}^4}$. Assume that G has no cyclic subgroup of index p. Then $\bar{G} = G/\mho_2(G)$ is metacyclic of order p^4 and exponent p^2. Then $\Omega_1(\mathrm{Z}(\bar{\mathrm{G}}) \cong \mathrm{E}_{\mathrm{p}^2}$ so $\bar{G}$ has two distinct normal subgroups A and B of order p. Since $|G : A| = p^3 = |G : B|$, we get a contradiction. Next, a p-group of order $> p^3$ contains a cyclic subgroup and has only one normal subgroup of index p^3 if and only if it is one of groups (i)-(iii).

Remark 3.27. Let $H < G$ be nonnormal, $|G| = p^m > p^{p+1}$, $|H| > p^2$ and $\mathrm{N}_G(H)$ is of maximal class. Then G is of maximal class (Lemma J(d)) and $H \not\leq G_1$ since $|\mathrm{Z}(G_1)| > p$. Let us prove that, if $K \neq H \cap G_1$ is maximal in H, then $\mathrm{N}_G(K) = H$. Indeed, $|\mathrm{N}_G(H) : H| = p$ (Lemma J(f)). Assume that $\mathrm{N}_G(K) > H$. Let $H < F \leq \mathrm{N}_G(K)$, where $|F : H| = p$. Then $F = \mathrm{N}_G(H)$ (compare the orders!). By the choice, $K \triangleleft F$ and F is of maximal class. Since $|F : K| = |F : H||H : K| = p^2$, we get $K = \Phi(F) < \Phi(G) < G_1$ so $K = H \cap G_1$, a contradiction.

Let G be a 3-group of maximal class and order $> 3^4$ and let $x \in G - G_1$; then $B = \langle x, \mathrm{Z}_2(G)\rangle$ is of order 3^3 [Ber2, Theorem 13.19] and nonabelian since $\mathrm{C}_G(\mathrm{Z}_2(G)) = G_1$. Assume that $\mathrm{C}_G(B) \not\leq B$. If $y \in \mathrm{C}_G(B) - B$, then $\mathrm{d}(\langle y, B\rangle) = 3$, which is impossible, by Lemma J(p).

4. p-GROUPS WITH EXACTLY ONE NONCYCLIC ABELIAN SUBGROUP OF ORDER p^3

In the proof of Theorem 4.2 we use the following

REMARK 4.1. If U is a cyclic subgroup of order p^2 of a nonabelian p-group G such that $\mathrm{C}_G(U) > U$ is cyclic, then $p = 2$ and G is a 2-group of maximal class. Indeed, if $\mathrm{C}_G(U) < H \leq G$ with $|H : \mathrm{C}_G(U)| = p$, then H is nonabelian with cyclic subgroup of index p. It follows from Lemma J(m) that $p = 2$ and H is of maximal class. Assuming that G is not of maximal class, we get $H < G$. Let $H < F \leq G$ with $|F : H| = 2$. Since $|H| > 8$, the subgroup U is characteristic in H so $U \triangleleft F$. In that case, $|F : \mathrm{C}_F(U)| = 2$ so $|\mathrm{C}_F(U)| = |H| > |\mathrm{C}_G(U)|$, a contradiction.

THEOREM 4.2. *Let G be the p-group of order $p^m > p^4$ with exactly one noncyclic abelian subgroup A of order p^3. Then one of the following holds:*

(a) *G is abelian of type (p^{m-1}, p).*

(b) *$G \cong \mathrm{M}_{\mathrm{p^m}}$.*

(c) *$p = 2$ and $G = \langle a, b \mid a^{2^{m-2}} = 1, b^4 = a^{2^{m-3}}, a^b = a^{-1} \rangle$.*

PROOF. Obviously $A \triangleleft G$ and G is not a 2-group of maximal class (all abelian subgroups of order 8 in a 2-group of maximal class are cyclic).

Assume that G is of maximal class, $p > 2$. Let $U \triangleleft G$ be of order p^2 and let $L < \mathrm{C_G(U)}$ be G-invariant of order p^4. If $p = 3$, then L is metacyclic of exponent 9 and either abelian or minimal nonabelian. In that case, L has $3+1$ distinct noncyclic abelian subgroups of order 3^3, contrary to the hypothesis. If $p > 3$, then $\exp(L) = p$ and L is nonabelian since, otherwise, it has > 1 (noncyclic) abelian subgroups of order p^3. Let $M < L$ be minimal nonabelian; then $U \not\leq M$. In that case, $L = M \times V$ for some subgroup $V < U$ of order p so L has $p+1$ distinct noncyclic abelian subgroups of order p^3, a contradiction. Thus, G is not of maximal class.

(i) If $B < G$ is nonabelian of order p^3, then $\mathrm{C}_G(B) < B$ (otherwise, $B * \mathrm{C_G(B)}$ has two distinct noncyclic abelian subgroups of order p^3). Then G is of maximal class (Lemma J(c)), contrary to the previous paragraph. Thus, G has no nonabelian subgroup of order p^3.

(ii) Let $U \leq G$ be minimal nonabelian. In that case (see (i) and Lemma J(t)), $U \cong M_{p^n}$, $n > 3$ so $A < U$ and $\Omega_1(A) \cong E_{p^2}$; then A is abelian of type (p^2, p) and $\Omega_1(A) \triangleleft G$.

(iii) Assume that there is $x \in G - A$ of order p. Then $B = \langle x, \Omega_1(A) \rangle$ is of order p^3. By (i), B is noncyclic abelian, a contradiction since $B \neq A$, by the choice of x. Thus, $\Omega_1(G) = \Omega_1(A)$.

(iii) Assume that there is $y \in G - A$ of order p^2. Write $Y = \langle y \rangle$. Set $H = \Omega_1(A)Y$; then $|H| = p^3$, by (iii), so H is noncyclic abelian, by (i), and $H \neq A$, by the choice of y, a contradiction.

Thus, $\Omega_2(G) = A$ so G is one of groups (a), (b), (c) (Lemma J(s)). ∎

Theorem 4.2 is not true for $m = 4$ and $p > 2$. Indeed, if G is a nonabelian subgroup of order p^4 of a Sylow p-subgroup of the symmetric group of degree p^2, then G, as a group of class 3, has exactly *one* noncyclic abelian subgroup A of order p^3 (Fitting's Lemma) and $A \cong \mathrm{E}_{p^3}$.

REMARK 4.3. Suppose that the 2-group G has exactly one abelian subgroup, say A, of type $(4, 2)$. We claim that then $\mathrm{c}_2(G) = 2$ (see [Ber1, Theorem 2.4] where such G are described). Clearly, G is not of maximal class, G has no abelian subgroups of types $(4, 2, 2)$ and $(4, 4)$ and it has no subgroup $\cong \mathrm{D}_8 * \mathrm{C}_4$ of order 16. Assume that $L < G$ be cyclic of order 4 such that $L \not\leq A$. If $\Phi(A) \not\leq L$, then $L \times \Phi(A) \neq A$ is abelian of type $(4, 2)$, a contradiction. Thus, $\Phi(A) < L$. Then LA of order 16 is nonabelian (otherwise, it must be of order 16 and exponent 4, and such group has two distinct abelian subgroups of type $(4, 2)$). Then, by Lemma J(o), $\mathrm{C}_A(L)$ is of order 4 since LA is not of maximal class, so $\mathrm{C}_A(L)L(\neq A)$ is abelian of type $(4, 2)$, a contradiction.

We claim that if an irregular p-group G of order $> p^{p+1}$ is neither absolutely regular nor of maximal class, then one of the following holds: (a) G has a subgroup E of order p^{p+1} and exponent p or (b) there is $H \in \Gamma_1$ such that $|\Omega_1(H)| = p^p$. Indeed, by Lemma J(a), there is $R \triangleleft G$ of order p^p and exponent p. Let D be a G-invariant subgroup of index p^2 in R. Set $C = \mathrm{C}_G(R/D)$. If an element $x \in C - R$ has order p, then $E = \langle x, R \rangle$ is of order p^{p+1} and class $\leq p - 1$ so regular; then $\exp(E) = p$. Now suppose that (a) is not true; then $|\Omega_1(C)| = p^p$. In that case, if $R/D < H/D \leq C/D$ and H/D is maximal in G/D (the equality $C = G$ is possible), then $R \leq \Omega_1(H) \leq \Omega_1(C) = R$ and (b) holds.

Let G be a p-group of maximal class. Then it contains a self centralizing subgroup H of order p^2 (Blackburn). We use this in Proposition 4.4.

PROPOSITION 4.4. *Let G be a group of maximal class and order $p^m > p^{p+1}$, $p > 2$. Set $\bar{G} = G/\mathrm{Z}(G)$. Let $\bar{D} < \bar{G}$ be of order p^2 such that $C_{\bar{G}}(\bar{D}) = \bar{D}$. Then*

(a) *D is nonabelian of order p^3 and $C_G(D) < D$.*
(b) *D has exactly p subgroups R of order p^2 such that $C_G(R) = R$.*

PROOF. Since $|\mathrm{Z}(G)| = p$, we get $|D| = p^3$. If $u \in G - D$ centralizes D, then $\bar{u}$ centralizes $\bar{D}$ and $\bar{u} \notin \bar{D}$, contrary to the choice of $\bar{D}$. Thus, $\mathrm{C}_G(D) \leq D$. Since $\bar{G}_1$ is not of maximal class, we get $\bar{D} \not\leq \bar{G}_1$ (Lemma J(o)) so $D \not\leq G_1$, where G_1 is the fundamental subgroup of G. Since $\mathrm{Z}(\bar{G}) < \bar{D}$, we get $\mathrm{Z}_2(G) < D$. Since $m > p + 1$, we get $\mathrm{C}_G(\mathrm{Z}_2(G)) = G_1$ (Lemma J(h)) so D is nonabelian, completing the proof of (a). Now (b) follows from Proposition 3.25. □

5. SOME COUNTING THEOREMS

The following proposition is known.

PROPOSITION 5.1. *Let G be a p-group of maximal class and order $> p^3$. Then*

(a) *G contains exactly one maximal subgroup, say A, such that $|A : A'| > p^2$.*
(b) *G contains exactly one maximal subgroup, say B, such that $|\mathrm{Z}(B)| > p$.*

PROOF. (a) Such A exists since group $G/\mathrm{K}_4(G)$ of order p^4 has *the* abelian maximal subgroup. Assume that $B \in \Gamma_1 - \{A\}$ is such that $|B : B'| > p^2$. Since $A', B' \lhd G$, one may assume that that $B' \le A'$ (Lemma J(d)). Then G/A' is of maximal class and order $\ge p^4$ containing two distinct abelian maximal subgroups B/A' and A/A'; in that case, however, $\mathrm{cl}(G/A') \le 2$ (Fitting's Lemma), a contradiction (clearly, $A = G_1$).

(b) Such B exists since $\mathrm{C}_G(\mathrm{Z}_2(G)) \in \Gamma_1$. Assume that $C \in \Gamma_1 - \{B\}$ is such that $|\mathrm{Z}(C)| > p$. Since $\mathrm{Z}(B), \mathrm{Z}(C) \lhd G$, one may assume that $\mathrm{Z}(C) \le \mathrm{Z}(B)$. Then $\mathrm{C}_G(\mathrm{Z}(C)) \ge BC = G$, a contradiction since $|\mathrm{Z}(G)| = p < |\mathrm{Z}(C)|$. (If $|G| > p^{p+1}$, then $B = G_1$ (Lemma J(h))). ∎

REMARK 5.2. (i) Let G be a p-group of order p^4. If $|\mathrm{Z}(G)| = p$, then $\mathrm{cl}(G) = 3$. If, in addition, $\mathrm{d}(G) = 3$ and G is nonabelian, then $\mu_3(G) = p^2$ (see [Ber5, §16]). (ii) If G is a p-group of maximal class and order p^5, then $\mu_4(G) = p$. Indeed, by Proposition 5.1(a), the set Γ_1 has exactly p members with centers of order p so the claim follows from (i). (iii) If $|G| = p^5$ and G is not of maximal class, then $\mu_4(G) \equiv 0 \pmod{p^2}$, by Lemma J(h).

We offer a new proof of the following nice counting theorem due to Mann [Man]. In his shorter proof of Theorem 5.3, Mann uses so called Eulerian function $\varphi_2(*)$.

THEOREM 5.3 ([Man]). *Let G be a p-group of order p^m, $m > 3$. Then $\mu_3(G) \equiv 0 \pmod{p^2}$, unless $m = 4$ and* $\mathrm{cl}(G) = 3$.

PROOF. One may assume that $\mu_3(G) > 0$; then G is nonabelian. By Hall's enumeration principle,

$$\mu_3(G) \equiv \sum_{H \in \Gamma_1} \mu_3(H) - p \sum_{H \in \Gamma_2} \mu_3(H) \pmod{p^2}. \tag{5.1}$$

(i) Let $m = 4$. If $\mathrm{cl}(G) = 3$, the result follows from Fitting's Lemma. If $\mathrm{d}(G) = 3$, the result follows from Remark 5.2.

(ii) Suppose that $m = 5$.

If $H \in \Gamma_1$ is not of maximal class, we have $\mu_3(H) \equiv 0 \pmod{p^2}$, by (i). If $H \in \Gamma_1$ is of maximal class, then $\mu_3(H) = p$, by (i). Next, $\mu_4(G) \equiv 0 \pmod{p}$, by Remark 5.2(ii,iii). Therefore,

$$\sum_{H \in \Gamma_1} \mu_3(H) \equiv 0 \pmod{p^2}. \tag{5.2}$$

If $\mathrm{d}(G) = 2$, then $\Phi(G)$ is abelian and $\Gamma_2 = \{\Phi(G)\}$ so, by (5.1) and (5.2), $\mu_3(G) \equiv 0 \pmod{p^2}$. It remains to consider the case $\mathrm{d}(G) > 2$. By (5.1) and (5.2), we get $\mu_3(G) \equiv 0 \pmod{p}$. Therefore, if $|\Phi(G)| = p$, all nonabelian subgroups of G contain $\Phi(G)$ so are members of the set Γ_2, and now the result follows from (5.1). Now we let $|\Phi(G)| = p^2$. We are done provided $\Phi(G) \leq \mathrm{Z}(G)$ since then all members of the set Γ_2 are abelian; therefore assume that $\Phi(G) \not\leq \mathrm{Z}(G)$. In that case, $|G : \mathrm{C_G(\Phi(G))}| = \mathrm{p}$ so $\mathrm{C}_G(\Phi(G))$ contains exactly $p+1$ (abelian) members of the set Γ_2. Thus, the set Γ_2 has exactly $|\Gamma_2| - (p+1) = p^2$ members of the set $\mathcal{M}_3(G)$, and we get, by (5.1), $\mu_3(G) \equiv 0 \pmod{p^2}$,

(iii) If $m > 5$, we use induction on m. If $H \in \Gamma_1$, then $\mu_3(H) \equiv 0 \pmod{p^2}$, by induction since $|H| \geq p^5$. If $H \in \Gamma_2$, then $\mu_3(H) \equiv 0 \pmod{p}$, by (i). Substituting this in (5.1), we complete the proof. ◻

Proposition 5.4. *Suppose that a p-group G of order $> p^{p+2}$ is neither absolutely regular nor of maximal class. If $R \lhd G$ is of order p, then one of the following holds:*

(a) The number of abelian subgroups of type (p,p) in G, containing R, is $\equiv 1 + p + \cdots + p^{p-2} \pmod{p^{p-1}}$.

(b) The number of cyclic subgroups of order p^2 in G, containing R, is a multiple of p^{p-1}.

Proof. (a) By Lemma J(b), $\mathrm{c}_1(G) = 1 + p + \cdots + p^{p-1} + ap^p$ for some integer $a \geq 0$. If $L \neq R$ is a subgroup of order p in G, then $RL = R \times L$ contains exactly p subgroups of order p different of R. We see that exactly p subgroups of order p, different of R, produce the same abelian subgroup of type (p,p) containing R. If $L_1 \not\in RL$ is of order p, then $RL \cap RL_1 = R$. Suppose that the required number equals s. Then $ps + 1 = \mathrm{c}_1(G)$ so $s = \frac{1}{p}[\mathrm{c}_1(G) - 1] = 1 + p + \cdots + p^{p-2} + ap^{p-1}$.

(b) If s is as in (a), then $s = 1 + p + \cdots + p^{p-2} + ap^{p-1}$ for some integer $a \geq 0$.

(i) Suppose that G/R is absolutely regular. Since G has a normal subgroup of order p^p and exponent p, we get $|\Omega_1(G/R)| = p^{p-1}$ so $\mathrm{c}_1(G/R) = 1 + p + \cdots + p^{p-2}$. Thus, there are $1 + p + \cdots + p^{p-2}$ subgroups of order p^2 lying between R and G, and exactly $1 + p + \cdots + p^{p-2} + ap^{p-1}$ among them are noncyclic, by (a). It follows that $a = 0$ so in our case the desired number equals 0.

(ii) Let G/R be irregular of maximal class. Then $\mathrm{c}_1(G/R) = 1 + p + \cdots + p^{p-2} + bp^p$ for some integer $b \geq 0$ (Lemma J(j)). Thus, there are $1 + p + \cdots + p^{p-2} + bp^p$ subgroups of order p^2 between R and G, and exactly $1 + p + \cdots + p^{p-2} + ap^{p-1}$ among them are noncyclic, by (a). In that case, the desired number is $(1 + p + \cdots + p^{p-2} + bp^p) - (1 + p + \cdots + p^{p-2} + ap^{p-1}) = (bp - a)p^{p-1}$.

(iii) If G/R is neither absolutely regular nor of maximal class, then $\mathrm{c}_1(G/R) = 1+p+\cdots+p^{p-1}+dp^p$ for some integer $d \geq 0$ (Lemma J(b)), and so, by (a), the desired number is $(1+p+\cdots+p^{p-1}+dp^p) - (1+p+\cdots+p^{p-2}+ap^{p-1}) = (1+dp-a)p^{p-1}$. ∎

Proposition 5.5. *Let $n > 1$ and suppose that a p-group G is not absolutely regular and $\mathrm{c}_n(G) = p^{p-2}$. Then one and only one of the following holds:*

(a) *$p = 2$, $n = 2$, G is dihedral.*
(b) *$p = 2$, $n > 2$, G is an arbitrary 2-group of maximal class.*
(c) *$p > 2$, $n = 2$, G is of maximal class and order p^{p+1} with exactly one absolutely regular subgroup of index p.*

Proof. Groups (a)-(c) satisfy the hypothesis.

If $p = 2$, then G has exactly one cyclic subgroup of order 2^n. In that case, if $n = 2$, then G is dihedral, and if $n > 2$, then G is an arbitrary 2-group of maximal class (Lemma J(b)).

Now let $p > 2$; then, by Lemma J(k), G is irregular (otherwise, $\mathrm{c}_n(G)$ is a multiple of p^{p-1} by Lemma J(b)), and so, by Lemma J(j), G is of maximal class. Assume that $|G| > p^{p+1}$. Let G_1 be the fundamental subgroup of G; then G_1 is absolutely regular with $|\Omega_{n-1}(G_1)| = p^{(n-1)(p-1)}$. If $n > 2$, then

$$\begin{aligned}\mathrm{c}_n(G_1) &= \frac{|\Omega_n(G_1)| - |\Omega_{n-1}(G_1)|}{\varphi(p^n)} \geq \frac{p^{(n-1)(p-1)+1} - p^{(n-1)(p-1)}}{(p-1)p^{n-1}} \\ &= p^{(n-1)(p-2)} > p^{p-2},\end{aligned}$$

a contradiction. Now let $n = 2$ and $|G| > p^{p+1}$. Then $|\Omega_2(G_1)| \geq p^{p-1+2} = p^{p+1}$ so $\mathrm{c}_2(G_1) \geq \frac{p^{p+1}-p^{p-1}}{p(p-1)} = p^{p-2}(p+1) > p^{p-2}$, again a contradiction. Thus, $|G| = p^{p+1}$. Then, clearly, G has exactly one absolutely regular subgroup of index p. ∎

It follows from Proposition 5.5 the following result, essentially due to G.A. Miller in the case $p > 3$. Suppose that a p-group G, $p > 2$, has exactly p cyclic subgroups of order p^n (by Kulakoff's Theorem, we have $n > 1$). Then one of the following holds: (a) G is either abelian of type (p^m, p) or $\cong \mathrm{M}_{p^{m+1}}$, $m \geq n$. (b) $p = 3$, $n = 2$, G is a 3-group of maximal class and order 3^4 with $\mathrm{c}_1(G) = 1+3+3^3$.

Proposition 5.6. *Suppose that an irregular p-group G is neither minimal nonabelian nor absolutely regular nor of maximal class, $|G| = p^m > p^{p+1}$. Let all nonabelian members of the set Γ_1 be either absolutely regular or of maximal class. Then one of the following holds:*

(a) *$p = 2$, $G = D\mathrm{Z}(G)$ is of order 16, $|D| = 8$.*
(b) *$E = \Omega_1(G)$ is elementary abelian of order p^p, G/E is cyclic and $C_G(E)$ is maximal in G.*

Proof. Assume that the set Γ_1 has no abelian member. Let $R \triangleleft G$ be abelian of type (p,p); then any maximal subgroup H of G such that $R < H \leq C_G(R)$, must be absolutely regular (in that case, $p > 2$), and so, by Lemma J(n), we get $|\Omega_1(G)| = p^p$. It follows that all members of the set Γ_1 containing $\Omega_1(G)$, are of maximal class so $|G| = p^{p+2}$ whence G, by Remark 3.2, is of maximal class, contrary to the hypothesis.

Suppose that there are distinct abelian $A, B \in \Gamma_1$. Then $A \cap B = Z(G)$ so $\mathrm{cl}(G) = 2$ whence $p = 2$ since G is irregular. Since G is not minimal nonabelian, there is $D \in \Gamma_1$ of maximal class. Then $|D| = 2^3$ so $|G| = 2^4$. By Lemma J((c), $G = DZ(G)$.

Now let A be the unique abelian member of the set Γ_1. If $m = 4$, then $p = 2$ (by hypothesis, $m > p + 1$). Since G is not of maximal class, we get a contradiction. Next assume that $m > 4$.

Assume, in addition, that there is absolutely regular $H \in \Gamma_1$. By Lemma J(n), $G = EH$, where $E = \Omega_1(G)$ is of order p^p and exponent p. By Lemma J(l), the set Γ_1 has no member of maximal class. Then all members of the set Γ_1, containing $\Omega_1(G)$, are abelian. If $G/\Omega_1(G)$ is cyclic, then $C_G(\Omega_1(G)) \in \Gamma_1$, and we get case (b). Now assume that $G/\Omega_1(G)$ is noncyclic. Then $\mathrm{cl}(G) = 2$ so $p = 2$ since G is irregular. Since G has a cyclic subgroup of index 2, we conclude that $G \cong M_{2^n}$ is minimal nonabelian, contrary to the hypothesis.

Now let all nonabelian members of the set Γ_1 are of maximal class. Then $\mu_{m-1}(G) \equiv 0 \pmod{p^2}$ (Lemma J(i)) and, since the set Γ_1 has exactly one abelian member, we get $|\Gamma_1| \equiv 1 \pmod{p^2}$, a contradiction. ∎

6. Nonabelian 2-groups of order 2^n and exponent > 2 with maximal number of involutions

In this section we find all G of order 2^n and exponent > 2 with maximal possible number of involutions ($= c_1(\mathrm{G})$). We use the following fact. If G is of order 2^4 and exponent > 2, then $c_1(G) \leq 11$ with equality if and only if $G \cong D_8 \times C_2$ [Ber5, §16].

To clear up our path, we consider the following

Example 6.1. Let G be a group of order 2^5 and exponent > 2. We claim that then $c_1(G) \leq 23$ with equality if and only if $G \cong D_8 \times E_4$. Indeed, assume that $c_1(G) > 23$. Then $c_1(G) = 27$ (Lemma J(b)). In that case, G has exactly 4 elements of composite orders. It follows that $\exp(G) = 4$ and $c_2(G) = 2$ (indeed, if G has a cyclic subgroup of order 8, it is unique so G is of maximal class, and then $c_1(G) \leq 17$). We get a contradiction with [Ber4, Theorem 2.4]. Now assume that $c_1(G) = 23$. Using Frobenius-Schur formula for $c_1(G)$, we get $|G'| = 2$ and $\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\} = \{1, 2\}$ so G is not extraspecial (if G is extraspecial, then $c_1(G) \in \{11, 19\}$). If $G/G' \not\cong E_{2^4}$ and $H/G' = \Omega_1(G/G')$, then all involutions of G lie in H so $c_1(G) \leq |H| - 1 \leq 15$.

Thus, $G/G' \cong \mathrm{E}_{2^4}$. Since $|G/\mathrm{Z}(G)| = 2^{2k}$ for positive integer k, we get $k = 1$ or 2. Since G is not extraspecial, $k \neq 2$. Thus, $G/\mathrm{Z}(G) \cong \mathrm{E}_4$. Let $H_i/\mathrm{Z}(G)$, $i = 1, 2, 3$, be all subgroups of order 2 in $G/\mathrm{Z}(G)$. We have $23 = \mathrm{c}_1(G) = \sum_{i=1}^{3} \mathrm{c}_1(H_i) - 2\mathrm{c}_1(\mathrm{Z}(G))$. Since $\mathrm{d}(G) = 4$, $\mathrm{Z}(G)$ is noncyclic. If $\mathrm{Z}(G)$ is abelian of type $(4, 2)$, then $\mathrm{c}_1(H_i) \leq 7$, $i = 1, 2, 3$, and, by the formula for $\mathrm{c}_1(G)$, we get $\mathrm{c}_1(G) \leq 7 \cdot 3 - 2 \cdot 3 = 15 < 23$. Now let $\mathrm{Z}(G) \cong \mathrm{E}_{2^3}$. Let $A < G$ be minimal nonabelian. Since $G' = A'$, $G/G' \cong \mathrm{E}_{2^4}$ and $\mathrm{d}(A) = 2$, we get $|A| = 2^3$. We have $\mathrm{Z}(G) = (A \cap \mathrm{Z}(G)) \times E$, where $E \cong \mathrm{E}_4$. Then $G = A \times E$. It follows from $24 = 1 + \mathrm{c}_1(G) = (1 + \mathrm{c}_1(A))(1 + \mathrm{c}_1(E))$ that $\mathrm{c}_1(A) = 5$ so $A \cong \mathrm{D}_8$.

Theorem 6.2. *If G is a group of order 2^m, $m > 2$ and $G \not\cong \mathrm{E}_{2^m}$, then $\mathrm{c}_1(G) \leq 3 \cdot 2^{m-2} - 1$ with equality if and only if $G \cong \mathrm{D}_8 \times \mathrm{E}_{2^{m-3}}$.*

Proof. As we have noticed, the theorem is true for $m = 4, 5$. By Frobenius-Schur formula [BZ, Lemmas 4.11, 4.18],

$$1 + \mathrm{c}_1(G) \leq \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \leq |G : G'| + \frac{|G| - |G : G'|}{2^2} \cdot 2$$
$$= \frac{1}{2}|G| + \frac{1}{2}|G : G'| \leq 2^{m-1} + 2^{m-2} = 3 \cdot 2^{m-2}.$$

Indeed, the contribution of one irreducible character χ of degree $2^k > 2$ in the sum $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)$ equals 2^k, on the other hand, the contribution of 2^{2k-2} irreducible characters of degree 2 equals $2^{2k-1} > 2^k$ (the sum of squares of degrees of those characters is $2^2 \cdot 2^{2k-2} = (2^k)^2 = \chi(1)^2$).

Now suppose that $\mathrm{c}_1(G) = 3 \cdot 2^{m-2} - 1$. The same argument as in Example 6.1, shows that then $\mathrm{cd}(G) = \{1, 2\}$, $|G'| = 2$ and every irreducible character of G is afforded by a real representation. It follows that $\exp(G/G') = 2$. We have $|\mathrm{Irr}(G)| = 2^{m-1} + \frac{2^m - 2^{m-1}}{2^2} = 2^{m-1} + 2^{m-3} = 5 \cdot 2^{m-3}$. Let $|\mathrm{Z}(G)| = 2^s$. Then the class number $\mathrm{k}(G) = 2^s + \frac{2^m - 2^s}{2} = 2^{m-1} + 2^{s-1}$. Since $|\mathrm{Irr}(G)| = \mathrm{k}(G)$, we get $5 \cdot 2^{m-3} = |\mathrm{Irr}(G)| = \mathrm{k}(G) = 2^{m-1} + 2^{s-1}$, or $2^{m-3} = 2^{s-1}$ so $s = m - 2$. Thus, $|G : \mathrm{Z}(G)| = 4$. If A is a minimal nonabelian subgroup of G, then, as in Example 6.1, $|A| = 8$ and $G = A\mathrm{Z}(G)$ so $G/A \cong \mathrm{E}_{2^{m-3}}$. Assume that $\exp(\mathrm{Z}(G)) = 4$. Then $\mathrm{c}_1(AC) = 7$, where C is a cyclic subgroup of order 4 in $\mathrm{Z}(G)$ [BJ1, Appendix 16]. In that case, $G = (AC) \times E$, where $\mathrm{E}_{2^{m-4}} \cong E < \mathrm{Z}(G)$. Then, however, $\mathrm{c}_1(G) = 8 \cdot 2^{m-4} - 1 = 2 \cdot 2^{m-2} - 1 < 3 \cdot 2^{m-2} - 1$, a contradiction. Thus, $\exp(\mathrm{Z}(G)) = 2$ and $G = A \times E$, where $E \cong \mathrm{E}_{2^{m-3}}$. If $A \cong \mathrm{Q}_8$, then $\mathrm{c}_1(G) = 2^{m-2} - 1 < 3 \cdot 2^{m-2} - 1$, a contradiction. Thus, $A \cong \mathrm{D}_8$; then $\mathrm{c}_1(G) = 3 \cdot 2^{m-2} - 1$. ∎

7. p-groups close to Dedekindian

Here we prove the following

Theorem 7.1. *Let G be a nonabelian p-group of order $> p^3$ and exponent $> p > 2$, all of whose nonnormal abelian subgroups are cyclic of the same order p^ξ. Then $|G'| = p$ and one and only one of the following holds:*

(a) $\xi = 1$. *In that case, one of the following assertions is true:*
 (1a) $G = Z * G_0$, *where Z is cyclic and G_0 is nonabelian of order p^3 and exponent p, $Z \cap G_0 = \mathrm{Z}(G_0)$.*
 (2a) $G \cong \mathrm{M}_{p^n}$.

(b) $G = \langle a, b \mid a^{p^m} = b^{p^\xi} = 1, a^b = a^{p^{m-1}} \rangle$ *is a metacyclic minimal nonabelian group, $1 < \xi \le m$.*

Proof. Let $A < G$ be nonnormal cyclic; then $|A| = p^\xi$ and A is a maximal cyclic subgroup of G.

Let $U = \Omega_1(\mathrm{Z}(G))$ and assume that $|U| > p^2$. Then AU is abelian and noncyclic so $AU \triangleleft G$. Let B/A and C/A be distinct subgroups of order p in AU/A. Then B and C are normal in G since they are abelian and noncyclic so $A = B \cap C \triangleleft G$, contrary to the choice of A. Thus, $|U| \le p^2$.

(a) Let $\xi = 1$. Then all cyclic subgroups of composite orders are normal in G. By [Ber1, Proposition 11.1 and Supplement to Proposition 11.1 and Theorem 11.3], $|G'| = p$ and $\Phi(G)$ is cyclic. In that case, $\mathrm{cl}(G) = 2$ so G is regular. Let $M < G$ be nonabelian; then $M' = G'$ so $M \triangleleft G$. Thus, all subgroups of composite orders are normal in G so G is as stated in (a), by Passman's Theorem [Pas, Theorem 2.4]. It is easy to check that groups of (a) satisfy the hypothesis.

(b) Now let $\xi > 1$. Then $U = \Omega_1(G) \le \mathrm{Z}(G)$ and $|U| = p^2$, by the above, so G has no subgroup $\cong \mathrm{E}_{p^3}$. Since G is regular, we get $|G/\mho_1(G)| = |\Omega_1(G)| = p^2$ so, by Lemma J(r), G is metacyclic. If $L/U < G/U$ is cyclic, then L is noncyclic abelian so $L \triangleleft G$. Thus, G/U is abelian since $p > 2$ so $G' \le U \cong \mathrm{E}_{p^2}$ hence $|G'| = p$ since G' is cyclic. Then $G = \langle a, b \mid a^{p^m} = b^{p^\xi} = 1, a^b = a^{1+p^{m-1}} \rangle$ is minimal nonabelian [BJ2, Lemma 3.2(a)]; note that $o(b) = p^\xi$ since $\langle b \rangle$ is not normal in G. We have to show that G satisfies the hypothesis if and only if $\xi \le m$.

Let $H < G$ be nonnormal cyclic. Then $H \cap G' = \{1\}$ so $H \cap \langle a \rangle = \{1\}$. It follows that H is isomorphic to a subgroup of the group $G/\langle a \rangle$ so H is cyclic of order $\le p^\xi$. Assume that $\xi > m$. Then the cyclic subgroup $\langle ab^{p^{\xi-m}} \rangle$ is nonnormal and has order $p^m < p^\xi$, a contradiction. Thus, $\xi \le m$. Since $\Omega_{\xi-1}(G) \le \mathrm{Z}(G)$, all subgroups of G of order $< p^\xi$ lie in $\mathrm{Z}(G)$ so G-invariant, and G satisfies the hypothesis. $\square$

8. On the number of cyclic subgroups of order $p^k > p^2$ in a p-group

If a p-group G is neither absolutely regular nor of maximal class and $k > 1$, then $\mathrm{c}_k(G) \equiv 0 \pmod{p^{p-1}}$. Below we prove that if $k > 2$, then, as a rule, $\mathrm{c}_k(G) \equiv 0 \pmod{p^p}$ [Ber6].

Definition 8.1. *Let s be a positive integer. A p-group G is said to be an L_s-group if $\Omega_1(G)$ is of order p^s and exponent p and $G/\Omega_1(G)$ is cyclic of order $> p$.*

Definition 8.2. *A 2-group G is said to be a U_2-group if it contains a normal subgroup $R \cong \mathrm{E}_4$ (a kernel of G) such that G/R is of maximal class and, if T/R is a cyclic subgroup of index 2 in G/R, then $\Omega_1(T) = R$.*

It is easy to show that a U_2-group has only one kernel.

Remark 8.3. Let G be a U_2-group of order 2^m with kernel $R \cong \mathrm{E}_4$. Let T/R be a cyclic subgroup of index 2 in G/R. Then, if $k > 3$, we have $\mathrm{c}_k(G) = \mathrm{c}_k(T) = 2$. Now let $k = 3$. Set $|G/R| = 2^{n+1}$, where $n+1 = m-2$. If G/R is dihedral, then all elements in $G-T$ have order ≤ 4 so $\mathrm{c}_3(G) = \mathrm{c}_3(T) = 2$. Let $G/R \cong \mathrm{Q}_{2^{n+1}}$, $n \geq 2$. Then all elements in $G - T$ have order 8 so $\mathrm{c}_3(G) = \mathrm{c}_3(T) + \frac{|G-T|}{\varphi(8)} = 2+2^n \equiv 2 \pmod 4$. Now let $G/R \cong \mathrm{SD}_{2^{n+1}}$, $n \geq 3$. Let $M/R \cong \mathrm{Q}_{2^n}$ be maximal in G/R. Then $\mathrm{c}_3(G) = \mathrm{c}_3(M) = 2 + 2^{n-1} \equiv 2 \pmod 4$ since $n \geq 3$.

Remark 8.4. Let G be a 2-group and let $H \in \Gamma_1$ be of maximal class. Then H has a G-invariant cyclic subgroup T of index 2. We claim that T is contained in exactly two subgroups of maximal class and order $2|T|$. One may assume that G has no cyclic subgroup of index 2 (otherwise, G is of maximal class, by Lemma J(m), $T = \Phi(G)$, and we are done). Now assume that G is not of maximal class. Let $U < T$ be of index 4. Since H/U is nonabelian, G/U is not metacyclic. Indeed, otherwise $\exp(G/U) = 8$ [Ber1, Remark 1.3] so G/U has a cyclic subgroup F/U of index 2. Since $U < \Phi(T) \leq \Phi(F)$, it follows that F is cyclic, a contradiction. In particular, $G/T \cong \mathrm{E}_4$. Let $H/T = H_1/T, H_2/T, H_3/T$ be three distinct subgroups of G/T of order 2. Since G/U has an abelian subgroup of index 2, one may assume that H_3/U is abelian. It remains to show that H_2 is of maximal class. Since $T/U \not\leq \mathrm{Z}(G/U)$, it follows that H_2/T is nonabelian. Since H_2 has a cyclic subgroup T of index 2, it follows that H_2 is of maximal class (Lemma J(m)).

I am indebted to Zvonimir Janko drawing my attention to an inaccuracy in the first proof of part (iv) of the following

Theorem 8.5. *If an irregular p-group G is not of maximal class, $k > 2$, then $\mathrm{c}_k(G) \equiv 0 \pmod{p^p}$, unless G is an L_p- or U_2-group.*

Proof. Suppose that G is neither an L_p- or U_2-group (for these G we have $\mathrm{c}_k(G) \equiv p^{p-1} \pmod{p^p}$; for L_p-groups this is trivial, for U_2-groups this is proved in Remark 8.3). We proceed by induction on $|G|$. By Lemma J(a), G has a normal subgroup R of order p^p and exponent p. If G/R is cyclic and G is not an L_p-group, then $\Omega_1(G)$ is of order p^{p+1} and exponent p (Remark 1.1) and $\mathrm{c}_k(G) = p^p$. In what follows we assume that G/R is not cyclic. Then G/R contains a normal subgroup T/R such that G/T is abelian of type (p,p). Let $H_1/T, \dots, H_{p+1}/T$ be all maximal subgroups of G/T. Then we have

$$\mathrm{c}_k(G) = \sum_{i=1}^{p+1} \mathrm{c}_k(H_i) - p\mathrm{c}_k(T). \tag{8.1}$$

One may assume that $\exp(G) \geq p^k$. We claim that $\mathrm{c}_k(T) \equiv 0 \pmod{p^{p-1}}$. Assume that this is false; then $\exp(T) \geq p^k > p^2$. In that case, T is irregular of maximal class (Lemma J(b)) and, since $R < T$ (Lemma J(b)), we get $|T| = p^{p+1}$ (Lemma J(f)); then $\exp(T) = p^2 < p^k$, a contradiction. It follows that $p\mathrm{c}_k(T) \equiv 0 \pmod{p^p}$. Therefore, it remains to prove that

$$\sum_{i=1}^{p+1} \mathrm{c}_k(H_i) \equiv 0 \pmod{p^p}. \tag{8.2}$$

Assume that (8.2) is not true. Then p^p does not divide some $\mathrm{c}_k(H_i)$. We may assume that $i = 1$. By induction, H_1 is one of the following groups: (i) an absolutely regular p-group; (ii) a p-group of maximal class, (iii) an L_p-group, (iv) a U_2-group. We must consider these four possibilities separately. Since $R < H_1$ and $k > 2$, possibilities (i) and (ii) do not hold (Lemma J(f)). It remains to consider possibilities (iii) and (iv).

(iii) Suppose that H_1 is an L_p-group; then $\Omega_1(H_1) = R$. It follows from Lemma J(m) that exactly p groups among $H_1/R, \dots, H_{p+1}/R$ are cyclic, unless p=2 and G/R is of maximal class. First suppose that $H_1/R, \dots, H_p/R$ are cyclic and H_{p+1}/R is noncyclic; then H_{p+1}/R is abelian of type (p^n, p). Since $k > 2$, $K/R := \Omega_1(H_1/R) \leq \Phi(G/R) < H_i/R$ so $R = \Omega_1(H_1) = \Omega_1(K) = \Omega_1(H_i)$, and we conclude, that H_i is an L_p-group for all $i = 2, \dots, p$. It follows, for the same i, that $\mathrm{c}_k(H_i) = p^{p-1}$. Since a U_2-group has only one kernel, H_{p+1} is not a U_2-group. Therefore, by induction, $\mathrm{c}_k(H_{p+1}) \equiv 0 \pmod{p^p}$ so (8.2) is true. Now suppose that $p = 2$ and G/R is of maximal class. Since $\Omega_1(H_1) = R$ and H_1/R is a cyclic subgroup of index 2 in G/R, we conclude that G/R is a U_2-group, contrary to the assumption.

(iv) Now suppose that H_1 is a U_2-group; then $p = 2$. Since G is not a U_2-group, we conclude that G/R is not of maximal class (otherwise, G/R has a cyclic subgroup, say Z/R, of index 2; then, as in (iii), $\Omega_1(Z) = R$ so G is a U_2-group). Let T/R be a G-invariant cyclic subgroup of index 2 in H_1/R and $H_1/T, H_2/T, H_3/T$ be all subgroups of order 2 in G/T (note that G/T is noncyclic, by Theorem 3.1, since G/R is not of maximal class). By

Remark 8.4, one may assume that H_2/R is of maximal class and H_3/R is not of maximal class. It follows from $\Omega_1(T) = R$ (indeed, $T < H_1$) that H_2 is a U_2-subgroup. Clearly, H_3 is neither an L_2-subgroup since G/R has no cyclic subgroup of index 2 nor U_2-group. We have, by induction, $\mathrm{c}_k(H_3) \equiv 0 \pmod 4$. Since $\mathrm{c}_k(H_i) \equiv 2 \pmod 4$ $(i = 1, 2)$, by Remark 8.3, we get $\mathrm{c}_k(G) \equiv \mathrm{c}_k(H_1) + \mathrm{c}_k(H_2) + \mathrm{c}_k(H_3) \equiv 2 + 2 + 0 \equiv 0 \pmod 4$, so (8.2) is true. □

Janko [Jan2] has classified the 2-groups G with $\mathrm{c}_k(G) = 4$, $k > 2$. The proof of this boundary result, which is fairly involved, shows that the assertion of Theorem 8.5 is very strong.

If G be a group of exponent p^e, then

$$|G| = 1 + \sum_{i=1}^{e} \varphi(p^i)\mathrm{c}_i(G). \tag{8.3}$$

Theorem 8.5 and (8.3) imply the following

Corollary 8.6. *Suppose that an irregular p-group G is not of maximal class and $|G| > p^{p+1}$. Then $1 + (p-1)\mathrm{c}_1(G) + p(p-1)\mathrm{c}_2(G) \equiv 0 \pmod{p^{p+2}}$, unless G is an L_p or U_2-group.*

Indeed, if $i > 2$, then $\varphi(p^i)\mathrm{c}_i(G)$ is divisible by $p^{i-1} \cdot p^p \geq p^{p+2}$ (Theorem 8.5).

Proposition 8.7. *For a p-group G of order p^{n+2}, $n > 1$, the following conditions are equivalent:*

(a) $\mathrm{cl}(G) = n$ *and* $\mathrm{d}(G) = 3$.
(b) *G is not of maximal class but contains a subgroup of maximal class and index p.*

Proof. (a) ⇒ (b): By hypothesis, indices of the lower central series of G are $p^3, p, \dots, p$. Therefore, $K = \mathrm{K}_3(G) = [G, G, G]$ has index p in G'. Since G/K is of class 2 and order $p^4 = p^{1+3}$, it is not extraspecial so that $|\mathrm{Z}(G/K)| = p^2$. Set $\eta(G)/K = \mathrm{Z}(G/K)$; then $|\eta(G)/K| = p^2$. Let H/K be a minimal nonabelian subgroup of G/K (recall that $\mathrm{d}(G/K) = 3$ and the rank of minimal nonabelian p-groups equals 2). Then $G = H\eta(G)$ so, by Blackburn's Theorem [Ber2, Theorem 1.40], $\mathrm{cl}(H) = \mathrm{cl}(G) = n$ and, since $|H| = p^{n+1}$, we conclude that H is of maximal class.

(b) ⇒ (a): By Lemma J(h), G contains exactly p^2 subgroups of maximal class and index p so $\mathrm{d}(G) = 3$. Set $|G| = p^{n+2}$. Since $n = \mathrm{cl}(H) \leq \mathrm{cl}(G) \leq n$, we get $\mathrm{cl}(G) = n$, completing the proof of (a). □

Using Proposition 8.7, it is easy to classify the 2-groups G of order 2^{n+2} such that $\mathrm{cl}(G) = n$ and $\mathrm{d}(G) = 3$ (see also [Jam]).

9. Problems

Here we formulate some related problems. In what follows G is a p-group.

1. Classify the p-groups, $p > 2$, containing exactly one noncyclic abelian subgroup of order (p^2, p).

2. Let $\mathrm{d}(G) > 3$ and $2 < i < \mathrm{d}(G)$. Is it true that the number of irregular members of maximal class in the set Γ_i is a multiple of p (see Theorem 3.12)?

3. Let $H < G$ be irregular and $\Omega_1(G) \not\leq H$. Suppose that for each element $x \in G - H$ of order p, the subgroup $\langle x, H\rangle$ is of maximal class. Study the structure of G. (See Remark 3.2.)

4. It follows from Blackburn's theory of p-groups of maximal class [Bla1] that if a p-group G has no nonabelian subgroup of order p^3, then the coclass of G is > 1. Estimate the coclass of such groups.

5. Study the p-groups without normal cyclic subgroup of order p^2. [1]

6. Classify the p-groups of exponent p, whose 2-generator subgroups have orders $\leq p^3$.

7. Let R be a subgroup of order p^2 of a p-group G. Suppose that there is only one maximal chain connecting R with G. Describe the structure of G.

8. Study the p-groups G with $e_p(G) = 2p + 1$.

9. Let G be a group of Theorem 1.5(b). Study the structure of $G/\Omega_1(G)$.

10. Let G be a $\mathcal{D}_p$-group. Describe the members of the set Γ_1 (see Theorem 3.24).

References

[Ber1] Y. Berkovich, *On subgroups and epimorphic images of finite p-groups*, J. Algebra **248** (2002), 472-553.

[Ber2] Y. Berkovich, *Groups of Prime Power Order, Part I*, in preparation.

[Ber3] Y. Berkovich, *On subgroups of finite p-groups*, J. Algebra **240** (2000), 198-240.

[Ber4] Y. Berkovich, *On abelian subgroups of p-groups*, J. Algebra **199** (1998), 262-280.

[Ber5] Y. Berkovich, *Alternate proofs of some basic theorems of finite group theory*, Glas. Mat. **40** (2005), 207-233.

[[Ber5] Y. Berkovich, *On the number of elements of given order in a finite p-group*, Israel J. Math. **73** (1991), 107-112.

[BJ1] Y. Berkovich and Z. Janko, *Groups of Prime Power Order, Part II*, in preparation.

[BJ2] Y. Berkovich and Z. Janko, *Structure of finite p-groups with given subgroups*, Contemporary Mathematics **402** (2006), 13-93.

---

[1] The group $\Sigma_{p^n} \in \mathrm{Syl}_p(\mathrm{S}_{p^n})$, $n > 1$, has no normal cyclic subgroup of order p^2, unless $p^n = 4$. Indeed, assume that $p^n > 4$ and let L be a normal cyclic subgroup of order p^2 in $G_n = \Sigma_{p^n}$. Since G_2 is of maximal class, it has a normal abelian subgroup of type (p,p) so it has no normal cyclic subgroup of order p^2, by Lemma J(d)(ii), hence $n > 2$. Let $B = H_1 \times \cdots \times H_p$, where $H_i \cong \Sigma_{p^{n-1}}$ is the ith coordinate subgroup of the base B of the wreath product $G_n = G_{n-1} \operatorname{wr} \mathrm{C}_p$. Then $\Omega_1(L) = \mathrm{Z}(G)$ and so $L \cap H_i = \{1\}$ for all i. Assume that $L < B$; then $\mathrm{C}_G(L) \geq H_1 \times \cdots \times H_p = B$, a contradiction, since $\mathrm{Z}(B)$ is elementary abelian. Thus, $L \not\leq B$. Since $\mathrm{Z}(H_i)$ centralizes L (consider the semidirect product $L \cdot H_i$) so $\mathrm{C}_G(\mathrm{Z}(H_i)) \geq BL = G$, we get $\mathrm{Z}(H_i) \leq \mathrm{Z}(G)$ for all i, a contradiction since $|\mathrm{Z}(G)| = p$.

[Bla1] N. Blackburn, *On a special class of p-groups*, Acta Math. **1** (1958), 45-92.

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

[Hal1] P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc. **36** (1933), 29-95.

[Hal2] P. Hall, *On a theorem of Frobenius*, Proc. London Math. Soc. **40** (1936), 468–501.

[HS] M. Hall, Jr. and J.K. Senior, *The groups of order 2^n ($n \leq 6$)*, Macmillan, NY, 1964.

[Jam] R. James, *2-groups of almost maximal class*, J. Austral. Math. Soc. (Ser A) **19** (1975), 343-357; corrigendum, ibid. **35** (1983), 307.

[Jan1] Z. Janko, *A classification of finite 2-groups with exactly three involutions*, J. Algebra **291** (2005), 505-533.

[Jan2] Z. Janko, *Finite 2-groups with exactly four cyclic subgroups of order 2^n*, J. reine angew. Math. **566** (2004), 135-181.

[Jan3] Z. Janko, *Finite 2-groups G with* $|\Omega_2(G)| = 16$, Glas. Mat. **40**, 1 (2005), 71-86.

[Man] A. Mann, *Conjugacy classes in finite groups*, Israel J. Math. **31** (1978), 78-84.

[Pas] D.S. Passman, *Nonnormal subgroups of p-groups*, J. Algebra **15, 3** (1970), 352-370.

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

Received: 16.7.2006.
Revised: 30.8.2007.