GROUPS IN WHICH ELEMENTS WITH
THE SAME p-POWER PERMUTE

M. BIANCHI - A. GILLIO BERTA MAURI - L. VERARDI

To the memory of Umberto Gasapina

We characterize finite groups satisfying the following property: if $x$, $y$ are two elements with the same $p$-power, then they permute.

Let $G$ be a group and $p$ a prime number. We say $\mathcal{C}_p$ the class of those groups $G$ such that if, $x, y \in G$ and $x^p = y^p$ then $xy = yx$. A $C_p$-group $G$ is a group in the class $\mathcal{C}_p$.

Of course, abelian groups are in $\mathcal{C}_p$ for all prime number $p$.

The case $p = 2$ was dealt in [3] and [2], where in particular one proves that such a group is always soluble.

Here we study the class $\mathcal{C}_p$ when $p > 2$ and, setting $\Omega(G) = \{ x \in G \mid x^p = 1 \}$, we will prove the following two main results:

**Theorem A.** If $p$ is an odd prime and if $G$ is a finite $p$-group then $G \in \mathcal{C}_p$ if and only if $\Omega(G) \subseteq Z(G)$. In particular, the nilpotency class of a $p$-group $G \in \mathcal{C}_p$ is not bounded.

Research partially supported by G.N.S.A.G.A. of C.N.R. and M.U.R.S.T. of Italy. 

*A.M.S. Classification:* 20D40, 20D08.
Theorem B. Let $G$ be a finite group whose order is a multiple of $p$. Then $G \in \mathcal{C}_p$ if and only if it possesses a normal Sylow $p$-subgroup $P \in \mathcal{C}_p$.

First of all, we observe that subgroups and direct products of $C_p$-groups are $C_p$-groups, while the same does not hold for factor groups of $C_p$-groups. The following lemma can be formulated and proved for $p = 2$ too.

Lemma 1. Let $G$ be a finite group and $p$ a prime number.

- a) Let $x, y \in G$ such that $x^p = y^p$. If $p$ does not divide the order of one of the two elements then $xy = yx$.
- b) If $p \nmid |G|$ then $G \in \mathcal{C}_p$.
- c) If $p \mid |G|$ and $G \in \mathcal{C}_p$ the set $\Omega(G)$ is an abelian normal subgroup of $G$.
- d) If $G \in \mathcal{C}_p$ is a simple non abelian group, then $p \nmid |G|$.

Proof. a) If $p \nmid o(x)$ it is $\langle x^p \rangle = \langle x \rangle$. So if $(o(x), p) = (o(y), p) = 1$ the two elements generate the same subgroup and so they permute. If $p \mid o(x)$ but $p \nmid o(y)$ it is

$$\langle y \rangle = \langle y^p \rangle = \langle x^p \rangle \leq \langle x \rangle,$$

so $xy = yx$.

b) It follows from a) for $p \nmid |G|$.

c) Of course, if $x, y \in \Omega(G)$ it is $x^p = y^p = 1$. So $xy = yx$ and this implies $(xy)^p = 1$, that is $xy \in \Omega(G)$. The result follows immediately.

d) It follows from c).

Lemma 2. Let $G$ be a $p$-group in $\mathcal{C}_p$.

- a) If $\exp(G) = p$ then $G$ is abelian.
- b) If $G$ has a maximal cyclic subgroup then $G$ is abelian.
- c) If $|G| = p^3$ then $G$ is abelian.

Proof. a) It follows immediately from Lemma 1.

b) If $p > 2$ and $G$ is not abelian then (see [6] 5.3.4) it has the following presentation:

$$G \simeq \langle a, x \mid a^{p^2 - 1} = x^p = 1, a^x = a^{1 + p^{n-2}} \rangle,$$

so $G$ is nilpotent of class 2 and it is $(ax)^x = a^p$, but $[a, ax] = a^{p^n - 1} \neq 1$.

If $p = 2$, because of Theorem 5.3.4 of [6], $G$ contains a subgroup of order 8 isomorphic either to the dihedral or to the quaternion group which are not in $\mathcal{C}_2$.

This means that $G \notin \mathcal{C}_2$ too.

c) If $p > 2$ the non-abelian groups of order $p^3$ have either exponent $p$ or they possess a cyclic maximal subgroup and they are not in $\mathcal{C}_p$ because of a) and b).
Proposition 3. Let $p$ be an odd prime, $1 < m, n, k \in \mathbb{N}$ such that $m + k > n$ and let
\[ G \cong \langle a, b \mid a^{p^k} = b^{p^m} = 1, a^b = a^{1+p^k} \rangle. \]
Then $G \in \mathcal{C}_p$. Besides $G$ has nilpotency class $c(G) \geq \lfloor n/k \rfloor - 1$. So the nilpotency class of a group $G$ in $\mathcal{C}_p$ is not bounded.

Proof. First of all $G = \langle \langle a \rangle \rangle \langle b \rangle$. From an element $x = b^i a^j \in G$, with some calculations, one obtains:
\[ x^p = (b^i a^j)^p = b^{pi} a^{j \left( \sum_{\lambda=0}^{p-1} (1+p^k)^{\lambda i} \right)}. \]
So, if $y = b^i a^s$, it is $x^p = y^p$ if and only if
\[ \begin{align*}
    pi & \equiv pr \quad (\text{mod} \ p^m) \\
    \left( \sum_{\lambda=0}^{p-1} (1+p^k)^{\lambda i} \right) & \equiv s \left( \sum_{\lambda=0}^{p-1} (1+p^k)^{\lambda r} \right) \quad (\text{mod} \ p^n).
\end{align*} \tag{*}
\]
In particular $i = r + tp^{m-1}$ for a suitable $t \in \mathbb{N}$.
As $m + k - 1 \geq n$, developing the following sum, we obtain:
\[ \sum_{\lambda=0}^{p-1} (1+p^k)^{\lambda i} = 1 + 1 + ip^k + \binom{i}{2} p^{2k} + \cdots + 1 + (2i) p^k + \binom{2i}{2} p^{2k} + \]
\[ \cdots + 1 + (p-1)ip^k + \binom{p-1+i}{2} p^{2k} + \cdots = p + i \binom{p}{2} p^k + \cdots = \]
\[ = p + r \binom{p}{2} p^k + tp^{m-1} \binom{p}{2} p^k + \cdots \equiv \sum_{\lambda=0}^{p-1} (1+p^k)^{\lambda r} \quad (\text{mod} \ p^n). \]

The two sums are of the same type $p(1+p^k q)$ for a suitable $q$, so after a division by $p$, they become invertible and congruent mod $p^{n-1}$. Thus they can be simplified and so $j \equiv s \pmod{p^{n-1}}$ that is $j = s + t' p^{n-1}$, $t' \in \mathbb{N}$.
It follows that:
\[ xy = (b^i a^j)(b^i a^s) = b^i r a^j (1+p^k)^{i+j} + s, \quad xy = (b^r a^s)(b^i a^j) = b^r + a^s (1+p^k)^{i+j}. \]

We observe that
\[ s(1+p^k)^i + j = s(1+ip^k + \ldots) + j = s(1+rp^k + tp^{m+k-1} + \ldots) + j \equiv \]
\[ \equiv s(1+rp^k) + j \pmod{p^n} \equiv s + j + sr p^k \pmod{p^n}. \]
\[ j(1 + p^k)^r + s = j(1 + rp^k + \ldots) + s = j(1 + ip^k + t'p^{m+k-1} + \ldots) + s \equiv j(1 + ip^k) + s \pmod{p^n} \equiv s + jip^k \pmod{p^n}. \]

But \( ip^k \equiv (r + tp^{m-1})(s + t'p^{n-1}) \pmod{p^n} \equiv rsp^k \pmod{p^n} \) as \( m + k - 1 \geq n \).

But then \( G \in \mathcal{G}_p \).

Set now \([a, b] = [a, b]\) and \([a, r+1 b] = [a, r b, b]\). By induction one easily proves that it is \([a, r b] \in \Gamma_r(G)\) and \([a, b] = a^{\rho^k}\).

So for \( r < n/k \) it is \( \Gamma_r(G) \neq 1 \) and \( c(G) \geq [n/k] - 1 \).

**Remark.** Among such groups, the smallest has order \( p^4 \) and it is the unique group of such order in \( \mathcal{G}_p \).

**Theorem A.** Let \( p > 2 \) and \( G \) a \( p \)-group. Then \( G \in \mathcal{G}_p \) if and only if \( \Omega(G) \leq Z(G) \).

**Proof.** Let \( G \in \mathcal{G}_p \). We prove that \( \Omega(G) \leq Z(G) \). If \( |G| \leq p^2 \) the result holds, so we use induction on \( |G| \). Let \( x \in G \), \( o(x) = p \) and let \( M \) be a maximal subgroup of \( G \) containing \( x \). Because of the inductive hypothesis, \( x \in Z(M) \). If \( M \) is the unique maximal subgroup, then \( G \) is cyclic and \( x \in Z(G) \).

Now let \( N \) be another maximal subgroup, \( N \neq M \).

If \( x \in N \), then \( G = MN \leq C_G(x) \). Consider now \( x \in M \setminus N \) and \( y \in N \setminus M \). Then \( G = M(y) \). If \( o(y) = p \) then \( xy = yx \) and therefore \( x \in Z(G) \). If \( o(y) > p \), consider \([x, y] \): as \( x \in M \triangleleft G \) then \([x, y] \in M \) and so it permutes with \( x \). It follows that for all \( n \in \mathbb{N} \), \([x^n, y] = [x, y]^n \), so from \( o(x) = p \) one gets \( o([x, y]) \leq p \). Being \( N \triangleleft G \), it follows \([x, y] \in N \) and, because of its order and of the inductive hypothesis, it belongs to \( Z(N) \), so it commutes with \( y \) too.

But then \( (xy)^n = x^n y^n[x, y]^n \) and, for \( n = p \), it is \((xy)^p = y^p \): this means \((xy) y = y(xy) \) so \( xy = yx \) and \( x \in Z(G) \).

Vice-versa, let \( G \) be a \( p \)-group such that \( \Omega(G) \leq Z(G) \); we want to prove that \( G \in \mathcal{G}_p \).

Deny and suppose that \( G \) is a minimal counterexample, i.e. \( \Omega(G) \leq Z(G) \), but there exist \( a, b \in G \) such that \( a^p = b^p \) with \( c = [a, b] \neq 1 \).

As the property \( \Omega(G) \leq Z(G) \) is inherited by subgroups, if it where \( \langle a, b \rangle < G \) one would get a contradiction. So \( G = \langle a, b \rangle \).

Now \((b^{-1}ab)^p = b^{-1}a^pb = b^{-1}b^p = a^p \). From \( b^{-1}ab = ac \in aG' \leq a\Phi(G) \) it follows \( \langle a, b^{-1}ab \rangle < G \), so \( a \) and \( a^b \) permute.

Therefore \( ac = b^{-1}ab = c^{-1}b^{-1}ab \) \( a \) = \( c \), that is \( c \) permutes with \( a \). In a similar way one proves that \([b, a] \) permutes with \( b \), so \( c = [b, a]^{-1} \) permutes with \( b \) too.

This means that \( c \in Z(G) \) and consequently \( 1 = [b^p, b][a^p, b] = [a, b]^p = c^p \) implies \( c \in \Omega(G) \).
Besides $b^{-1}a = ab^{-1}[b^{-1},a] = ab^{-1}c$, from which it follows $(ab^{-1})^p = a^pb^{-p}c^p(\frac{b}{a}) = 1$, so $ab^{-1} = z \in \Omega(G) \leq Z(G)$. But then $a = bz$ and $c = [a, b] = 1$. It follows that $G$ is abelian, a contradiction.

**Remark.** For $p = 2$ the result is false, as proved by the following counterexample:

$$G = \langle a, b \mid a^8 = b^2 = 1, a^2b = ba^2, (ab)^2 = (ba)^2 \rangle.$$ 

It is $G \in \mathcal{G}_2$ but $G$ has non-central elements of order 2 ($b$, namely).

**Proposition 4.** Let $G \in \mathcal{G}_p$ be a $p$-group with $p > 2$ and $1 \neq u \in G$. Then:

a) $\{ x \in G \mid x^p = u^p \} = u\Omega(G)$.  
b) If $o(u) = p^2$ then $u \in Z_2(G)$.  
c) If $o(u) = p^2$, $\langle u \rangle \lhd G$ then $(G/\langle u^p \rangle) \in \mathcal{G}_p$.

**Proof.** 
a) From $x^p = u^p$ it follows $xu = ux$ and so $(u^{-1}x)^p = 1$, that is $x \in u\Omega(G)$. The converse follows from $\Omega(G) \leq Z(G)$.

b) It is $u^p \in \Omega(G) \leq Z(G)$ so, for all $g \in G$, $(u^g)^p = (u^p)^g = u^p$, from which it follows $u^g = uc$ with $c \in \Omega(G)$.

Consequently $[u, g] = u^{-1}(u^g) = c \in Z(G)$, which implies $u \in Z_2(G)$.

c) Let $K = \langle u^p \rangle$ and consider $G/K$: for each couple $xK$, $yK$ of elements such that $(xK)^p = (yK)^p$, it is $x^p = y^pc$ with $c \in K$.

So there exists $v \in \langle u \rangle$ such that $c = v^p$ and this means $x^p = (yv)^p$. Being $\langle u \rangle \lhd G$ one gets $[v, x] \in \langle u \rangle$ and, moreover $[v, x] \in \langle u^p \rangle = K$ for $G$ is nilpotent.

Besides it is $xyv = yuv = yx[v, x] = yx[v, x]v$, which means $xy = yx[v, x]$. But then $xK yK = yxK$ and so $G/K \in \mathcal{G}_p$.

**Remarks.** a) One of Thompson’s theorems states that if $G$ is a $p$-group where $\Omega(G) \leq Z(G)$, then the number of generators of $G$ is bounded by the number of generators of $Z(G)$ (see [4], p. 342).

b) Let $G$ be a finite group, $N_p = \left| \{(a, b) \in G \mid a^p = b^p \} \right|$ and, for all $x \in G$, $\theta_p(x) = \left| \{ y \in G \mid y^p = x \} \right|$. Then $N_p = \sum_{x \in G} \theta_p(x^p)$.

As $\theta_p$ is a function class (constant on the conjugacy classes) for all irreducible character $\chi$ of $G$ there exists an algebraic integer $\nu_p(\chi)$ such that

$$\theta_p = \sum_{\chi \in \text{Irr}(G)} \nu_p(\chi) \chi.$$ 

Therefore

$$N_p = \sum_{x \in G} \sum_{\chi \in \text{Irr}(G)} \nu_p(\chi) \chi(x^p) = \sum_{\chi \in \text{Irr}(G)} \nu_p(\chi) \sum_{x \in G} \chi(x^p).$$
It is well-known (see [5], 4.4) that

\[ v_p(\chi) = \frac{1}{|G|} \sum_{x \in G} \chi(x^p) \]

so

\[ \sum_{x \in G} \chi(x^p) = |G|v_p(\chi). \]

It follows that

\[ N_p = |G| \sum_{\chi \in \text{Irr}(G)} (v_p(\chi))^2 \]

and, as \( v_p(\chi) \in \mathbb{Z} \), then \(|G|\) divides \( N_p \). Now if \( G \) is a \( p \)-group \( G \in \mathcal{C}_p \) for each couple \((a, b)\) it is \( a^p = b^p \) if and only if \( b \in a\Omega(G) \). So, if we fix \( a \), one gets \(|\Omega(G)|\) couples \((a, b)\) such that \( a^p = b^p \). It follows \( N_p = |G| \cdot |\Omega(G)| \) so

\[ |\Omega(G)| = \sum_{\chi \in \text{Irr}(G)} (v_p(\chi))^2 \]

(see [3] for the case \( p = 2 \)).

Now let us examine the case of a finite group \( G \) whose order is a multiple of the odd prime \( p \). First of all we observe that with the following lemma one reduces the problem to the comparison among \( p \)-elements.

**Lemma 5.** A group \( G \) belongs to \( \mathcal{C}_p \) if and only if for each \( x, y \in G \) such that \( x^p = y^p \), \( o(x) = o(y) = p^h m \), \( h > 0 \) and \((p, m) = 1\) it is \([x^m, y^m] = 1\).

**Proof.** Lemma 1 shows that to prove that \( G \in \mathcal{C}_p \) it is sufficient to examine those couples of elements \( x, y \) such that \( x^p = y^p \) and whose order is a multiple of \( p \) and it is the same for \( x \) and \( y \). Now if \( n = p^hm \), \( h \geq 1 \) is the common order, it is \( x = x'x'' \) and \( y = y'y'' \) with \( o(x') = o(y') = p^h \), \( o(x'') = o(y'') = m \). Being \( x^p = y^p \) it is \( x'' = x^{p^h} = y^{p^h} = y'' \). If follows \( xy = yx \) if and only if \( x'y' = y'x' \), that is if and only if their \( p \)-components permute.

**Theorem B.** Let \( G \) be a finite group and \( p \) an odd prime divisor of \(|G|\). Then \( G \in \mathcal{C}_p \) if and only if \( G \) possesses a normal Sylow \( p \)-subgroup \( P \in \mathcal{C}_p \).
**Proof.** Let $P$ be a Sylow $p$-subgroup of $G$ and suppose $P \triangleleft G$, $P \in \mathcal{S}_p$. Let $x, y \in G$ such that $x^p = y^p$ with $(o(x), o(y))$ multiple of $p$.

According to Lemma 5, let us consider their $p$-components $x'$ and $y'$: they belong to $P$ and they have the same $p$-power and, being $P \in \mathcal{S}_p$, they permute. It follows that $x$ and $y$ permute too and $G \in \mathcal{S}_p$.

Vice-versa let $G \in \mathcal{S}_p$ a minimal counterexample; this means that $P$ is not normal in $G$. Because of Lemma 1.c, $\Omega(G)$ is normal and abelian, so $\Omega(G) \leq P$ and therefore $\Omega(G) = \Omega(P)$ and Theorem A assures that it is included in $Z(P)$. Therefore $P$ is a Sylow $p$-subgroup of $C = C_G(\Omega(G))$.

If $C$ were a proper subgroup of $G$, then $P$ would be normal in it, better $P$ would be characteristic in $C$. But being $C$ normal in $G$ then $P$ would be normal in $G$, a contradiction. So $\Omega(G) \leq Z(G)$. If $\exp(P) = p$ then $P = \Omega(G) \triangleleft G$ again a contradiction. So $\exp(P) \geq p^2$. Besides for each $x \in G$ it is $\{y \in G \mid y^p = x^p\} = x\Omega(G)$.

Being $\Omega(G) \leq P$, if $x \in P$, from $x^p = y^p$ it follows $y \in P$. In particular if $u \in P$, $o(u) = p^2$, it is $u^p \in \Omega(G) \leq Z(G)$, which means that, for all $g \in G$, it holds $(u^g)^p = (u^p)^g = u^p$ and then $u^g \in u\Omega(G) \leq P$. In this case the elements of order $p^2$ belong to each Sylow $p$-subgroup of $G$. Besides $u \in Z_2(G)$ and $(ug)^p = u^p g^p \forall g \in G$.

Now let us suppose that for such an element $u$ of order $p^2$ the subgroup $\langle u \rangle$ is normal in $G$. If $K = \langle u^p \rangle$, with the same argument of Proposition 4.c), for each couple $xK$, $yK$ of $p$-elements of $G/K$ such that $(xK)^p = (yK)^p$ one gets either $x^p = y^p$ or $x^p = y^p c$, with $c \in K$, so one can suppose $c = u^p$ and $x^p = (yu)^p$. In the first case it follows $xy = xy$ in the second one $xyu = yux = yx[u, x] = yx[u, x]u$ so $xy = yx[u, x]$.

Being $\langle u \rangle \triangleleft G$ it is $\langle [u, x] \rangle \in \langle u \rangle$ and since $x \in P^g$, which is nilpotent, it follows $[x, u] \in \langle u^p \rangle = K$.

But then $xKyuK = yKxK$ and therefore $G/K \in \mathcal{S}_p$, because of Lemma 5. For the minimality of $G$ it follows $P/K \triangleleft G/K$ so $P \triangleleft G$, a contradiction. This means that $\langle u \rangle$ is non normal in $G$. Then $C_G(u) \leq N_G(\langle u \rangle) < G$ and, as $u \in Z_2(G)$ and $G' \leq C_G(u)$,(see [6] 5.1.11. (iii)), it is $G' < G$.

If $PG' < G$, then, again for the minimality of $G$, the group $P$ would be characteristic in $PG' \triangleleft G$, then $P \triangleleft G$, which forces $PG' = G$.

Besides, if $M$ is maximal in $P$ and contains $P \cap G'$, it follows $MG' < G$: consequently, being $M$ a Sylow $p$-subgroup of the proper normal subgroup $MG'$, it is $M \triangleleft G$ and so $M$ is the unique maximal subgroup of $P$ containing $P \cap G'$. Then $P/P \cap G'$ is cyclic and $G'/G'$ is cyclic too.

Let $t \in P$ such that $\langle tG' \rangle = G/G'$ and let $T = \langle t \rangle$. Then $G = TG'$ and $P = TM$. Let $u \in T$ of order $p^2$: then $t \in C_G(u)$ too and this means $G = TG' \leq C_G(u)$ and $u \in Z(G)$, a contradiction. Then $o(t) = p$ and
\( t \in Z(G), T \triangleleft G \) and \( P = T \times M \triangleleft G \), a final contradiction.

Therefore such a group \( G \) does not exist and the theorem is proved.

In [2] one proves that if \( G \in \mathcal{C}_2 \) then \( G \) is soluble. The same property does not hold if \( p > 2 \), as the following proposition shows:

**Proposition 6.**

(a) Let \( p \) be an odd prime. \( S \) a simple group whose order is prime to \( p \), and consider a faithful action of \( S \) on a set with \( n \) elements. Let \( G \) be the wreath product of \( Z_p \) by \( S \) through this action. Then \( G \in \mathcal{C}_p \).

(b) For each prime \( p > 2 \) there exists in \( \mathcal{C}_p \) a non-soluble group whose order is a multiple of \( p \).

**Proof.**

a) Let \( K \) be a normal subgroup of \( G \) isomorphic to \( (Z_p)^n \), on which \( S \) acts. As \( |S| \) is prime to \( p \), \( K \) is the Sylow \( p \)-subgroup of \( G \) and besides it is abelian. The assertion follows from Theorem A.

b) If \( p = 3 \), let \( S \cong S_3(8) \); if \( p = 5 \) let \( S \cong PSL(2, 7) \), if \( p > 7 \) let \( S \cong A_5 \). In all the 3 cases it is \( (p, |S|) = 1 \). So one can apply a) to get a non-soluble group \( G \in \mathcal{C}_p \) whose order is multiple of \( p \).

**Corollary 7.** Let \( G \) a finite group of odd order. For each \( p_i \) such that \( p_i \) divides the order of \( G \) it is \( G \in C_{p_i} \) if and only if:

a) \( G \) is nilpotent, and

b) if \( x \in G \) has prime order then \( x \in Z(G) \).

**Proof.** Let \( G \in C_{p_i}, \forall p_i \): then every Sylow \( p_i \)-subgroup \( S_i \) is normal in \( G \), so \( G \) is nilpotent. Then \( Z(G) = \prod_{p_i \mid |G|} Z(S_i) \geq \prod_{p_i \mid |G|} \Omega(S_i) \) and the thesis follows.

Vice-versa, let \( G \) be a nilpotent group such that all \( x \in G \) of prime order are central. Then \( \forall p_i \mid |G| \) it is \( \Omega(S_i) \leq Z(G) \cap S_i = Z(S_i) \), which implies \( S_i \in \mathcal{C}_p \) and besides being normal in \( G \), \( G \in C_{p_i} \) for all \( i \).

The class of finite \( p \)-groups such that \( \Omega(G) \leq Z(G) \) is very large and well-known. Several other properties of these \( p \)-groups can be found for example in [1] and [7].
REFERENCES


\textit{Mariagrazia Bianchi and Anna Gillio Berta Mauri,}
\textit{Dipartimento di Matematica “F. Enriques”,}
\textit{Università di Milano,}
\textit{Via C. Saldini 50,}
\textit{20133 Milano (ITALY)}

\textit{Libero Verardi,}
\textit{Dipartimento di Matematica,}
\textit{Università di Bologna,}
\textit{Piazza di Porta San Donato 5,}
\textit{40127 Bologna (ITALY)}