# Bollettino Unione Matematica Italiana



Renza Cortini


## On special $p$-groups


*Bollettino dell'Unione Matematica Italiana, Serie 8*, Vol. **1-B** (1998), n.3, p. 677–689.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1998_8_1B_3_677_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1998.

Bollettino U. M. I.
(8) **1**-B (1998), 677-689

# On Special $p$-Groups.

RENZA CORTINI

**Sunto.** – *In questo lavoro viene data una caratterizzazione di quei p-gruppi nilpotenti di classe due ed esponente p che sono speciali. Vengono inoltre studiate alcune costruzioni, automorfismi e sottogruppi abeliani di p-gruppi speciali.*

## 1. – Introduction.

Let $p$ be a prime. A finite $p$-group $G$ is called *special* if the center $\boldsymbol{Z}$(G), the commutator subgroup $G'$ and the Frattini subgroup $\Phi(G)$ coincide. In this case, one can immediately show that $G'$ and $G/G'$ are elementary abelian groups and so $\exp(G) = p$ or $p^2$.

Special $p$-groups are a relevant class of finite groups. First of all, in a paper of 1973 Heineken and Liebeck [6] have shown that, for every odd prime, there is an injective mapping from the class of finite groups to that of special $p$-groups of exponent $p^2$. A similar result, but concerning infinite groups, is given by U. H. M. Webb in [14]. Then, (see [12]), Verardi has constructed a mapping from the class of groups to that of special $p$-groups of exponent $p$. By these mappings the knowledge of the associated special $p$-group allows us to obtain specific informations about the structure of the initial group. Moreover several papers and books present the study of particular subclasses, namely extra-special $p$-groups (see [3], [7] and their references), semi-extraspecial $p$-groups (see [1], [2], [5], [10]) and so on. In these books and papers, properties of subgroups, automorphisms and centralizers are investigated and some classifications are given. In two papers by Visnevetskii ([13]) and Heineken ([5]), the case of $|G'| = p^2$ is investigated. In particular they have shown that a special $p$-group of this type is the product of two abelian subgroups, and a classification is given as well.

Since every special $p$-group is nilpotent of class 2, it is natural to ask in which case a group of nilpotency class 2 is special. Therefore in this paper, firstly, a characterization of special $p$-groups of exponent $p$ is given in terms of a family of skew-symmetric matrices associated to the commutators of a minimal generating set (see Proposition 2.1 and Theorem 2.3).

This characterization allows us to find a general construction of special $p$-groups of exponent $p$ and order $p^{m+s}$, where $p^2 = |G'| \leq p^{m(m-1)/2}$. Particular constructions are given in the cases of $m = s$ with $m \leqslant 3$ or $m = s + 1$. For some values of $m$ and $s$, these groups are not the product of two abelian subgroups (see Proposition 3.3). Moreover the maximum order of an abelian subgroup is investigated as well (see Proposition 4.1). In particular it is studied the case of the so-called *ordinary* special $p$-groups (see Remark 4.6 and Proposition 4.7).

A characterization of automorphisms of a special $p$-groups is given in Proposition 4.5.

Finally special $p$-groups are studied as quotients of the relatively free $p$-group of nilpotency class two and exponent $p$. Indeed, such a group $F$ is special, and every special $p$-group of exponent $p$, with the same number of generators, is its omomorphic image. Some conditions are given on normal subgroups of $F$, so that the quotient group turns out to be special (see Proposition 5.1).

## 2. – Some characterizations of special $p$-groups of exponent $p$ with odd $p$.

In this section we want to characterize special $p$-groups of exponent $p$ through some properties of a family of skew-symmetric matrices associated to the commutators of a minimal generating set. Firstly, we recall the presentation of a nilpotent group of class 2 and exponent $p$.

Let $p$ be an odd prime and $M_k = [m_{k_{ij}}]$, $\forall k = 1, \dots, s$ skew-symmetric matrices of order $m$; then:

$$G = \langle e_1, \dots, e_m, c_1, \dots, c_s / e_i^p = c_k^p = 1, [e_i, c_k] = [c_l, c_k] = 1\ ,$$

$$[e_i, e_j] = c_1^{m_{1ij}} c_2^{m_{2ij}} \dots c_s^{m_{sij}}, \quad i, j = 1, \dots, m; \quad k, l = 1, \dots, s\rangle$$

is a nilpotent group of class 2 and exponent $p$, with:

$$G' = \langle c_1, \dots, c_s \rangle \leqslant \boldsymbol{Z}(G)$$

Conversely, let $p > 2$ and $G$ be a $p$-group of nilpotency class 2 and exponent $p$; so $\Phi(G) = G'$ and then $G'$ and $G/G'$ are elementary abelian $p$-groups, namely vector spaces on the field $\boldsymbol{Z}/p\boldsymbol{Z}$. Accordingly we can write them additively and, hence, read the map

$$f\colon\ G/G' \times G/G' \to G'\ ,$$

$$[xG', yG'] \mapsto [x, y]\,,$$

as a bilinear alternating one between these vector spaces. Setting $\{e_1 G', \dots, e_m G'\}$ and $\{c_1, \dots, c_s\}$ as bases of these vector spaces, we can find $s$ skew-symmetric matrices $M_1, \dots, M_s$ so that, if $M_k = [m_{k_{ij}}]$, then

$[e_i, e_j] = \prod_{k=1}^{s} c_k^{m_{kij}}$. On the other hand $G' \leqslant \boldsymbol{Z}(G)$ implies $[e_i, c_k] = [c_l, c_k] = 1$; hence $G$ has the previous presentation.

Our aim is now to characterize special $p$-groups of exponent $p$ through properties of $M_1, \ldots, M_s$.

2.1. PROPOSITION. – *Let $G$ be a nilpotent group of class 2 and exponent $p$. Then $G$ is a special $p$-group if and only if the following conditions hold*:

*a*) $\bigcap_{k=1}^{s} \ker M_k = \{0\}$,

*b*) *$G$ has no direct abelian factors.*

PROOF. – Suppose that *a*) and *b*) hold. We already know that $G' \leqslant \langle c_1, \ldots, c_s \rangle \leqslant \boldsymbol{Z}(G)$; now our first aim is to prove that $\langle c_1, \ldots, c_s \rangle = \boldsymbol{Z}(G)$. Writing additively the elementary abelian groups $G'$ and $G/G'$ and setting $\{e_1 G', \ldots, e_m G'\}$ and $\{c_1, \ldots, c_s\}$ as bases of them, we can consider

$$X = \sum_{i=1}^{m} x_i e_i + \sum_{j=1}^{s} x_j c_j = X' + \sum_{j=1}^{s} x_j c_j .$$

Then $X \in \boldsymbol{Z}(G)$ if and only if

$$\forall Y = \sum_{i=1}^{m} y_i e_i + \sum_{j=1}^{s} y_j c_j = Y' + \sum_{j=1}^{s} y_j c_j$$

it results:

$$0 = [X, Y] = [X', Y'] = \sum_{k=1}^{s} (X'^t M_k Y') c_k$$

(recalling that we are writing the groups additively). That is $X \in \boldsymbol{Z}(G)$ if and only if:

$$\begin{pmatrix} X'^t M_1 \\ X'^t M_2 \\ \vdots \\ X'^t M_s \\ \end{pmatrix} = \mathbf{0}_{s \times m} .$$

Consequently $X' \in \bigcap_{k=1}^{s} \operatorname{Ker} M_k = \{0\}$, i. e. $X' = 0$ and therefore $\boldsymbol{Z}(G) = \langle c_1, \ldots, c_s \rangle$. To prove that $G$ is a special $p$-group we must still verify that $G' = \langle c_1, \ldots, c_s \rangle$. By way of contradiction, let us suppose $G' < \boldsymbol{Z}(G) = \langle c_1, \ldots, c_s \rangle$. Then there exists $i \in \{1, \ldots, s\}$ such that $c_i \notin G'$. Since $\exp G = p$ and $\Phi(G) = G'$, it follows $c_i \notin \Phi(G)$. Therefore there exists a maximal subgroup $M$ of $G$

such that $c_i \notin M$. Then $G = M \times \langle c_i \rangle$, that is a contradiction. Hence $G' = \boldsymbol{Z}(G)$ and the group under consideration is special.

Vice versa, suppose that $G$ is a special $p$-group of exponent $p$. First we will prove that $G$ cannot have any direct abelian factor. Suppose $G = P \times A$ , with $A$ abelian. Then $G' = P'$, but $\boldsymbol{Z}(G) \geq A$, and then $A = 1$.

Moreover, as already said, $G$ has a representation by matrices $M_1, \dots, M_s$ and, setting $X = x\boldsymbol{Z}(G) = \sum_{i=1}^{m} x_i e_i \boldsymbol{Z}(G)$, we have $x \in \boldsymbol{Z}(G)$ if and only if

$$X^t M_k = 0 , \quad \forall k = 1, \dots, s$$

that is $X \in \ker M_k \ \ \forall k = 1, \dots, s$. Since $\boldsymbol{Z}(G) = G' = \langle c_1, \dots, c_s \rangle$ we must have $X = 0$; hence $\bigcap_{k=1}^{s} \ker M_k = \{0\}$, q.e.d.

2.2. Remark. – A sufficient condition to $a$) is that $\exists \lambda_1, \dots, \lambda_s \in \boldsymbol{Z}/p\boldsymbol{Z}$ such that

$$\det\left( \sum_{k=1}^{s} \lambda_k M_k \right) \neq 0 .$$

We call such a special $p$-group an *ordinary* special $p$-group.

In fact, in this case, $X^t M_k = 0$, $\forall k = 1, \dots, s$ implies $X^t \left( \sum_{k=1}^{s} \lambda_k M_k \right) = \boldsymbol{0}_{1 \times m}$ and, since this linear combination is non-singular, we have $X = 0$ and consequently $\bigcap_{k=1}^{s} \ker M_k = \{0\}$.

The following theorem gives another characterization of those nilpotent $p$-groups of class 2 and exponent $p$ which are special.

2.3. Theorem. – *With the notations of Proposition* 2.1, *$G$ is a special $p$-group of exponent $p$ if and only if the following conditions hold*:

$a$) $\bigcap_{k=1}^{s} \ker M_k = \{0\}$,

$b$) *the vectors*

$$v_1 = (m_{1_{12}}, m_{2_{12}}, \dots, m_{s_{12}}), \qquad v_2 = (m_{1_{13}}, m_{2_{13}}, \dots, m_{s_{13}}), \dots,$$

$$v_{m-1} = (m_{1_{1m}}, m_{2_{1m}}, \dots, m_{s_{1m}}), \qquad v_m = (m_{1_{23}}, m_{2_{23}}, \dots, m_{s_{23}}), \dots ,$$

$$v_{2m-3} = (m_{1_{2m}}, m_{2_{2m}}, \dots, m_{s_{2m}}), \dots , \qquad v_{(m(m-1))/2} = (m_{1_{m-1,m}}, m_{2_{m-1,m}}, \dots, m_{s_{m-1,m}})$$

*consist in a system of generators for the vector space* $\underbrace{\boldsymbol{Z}/p\boldsymbol{Z} \times \dots \times \boldsymbol{Z}/p\boldsymbol{Z}}_{s}$.

Proof. – As already seen in Proposition 2.1, $\bigcap_{k=1}^{s} \operatorname{Ker} M_k = \{0\}$ if and only if $\langle c_1, \dots, c_s \rangle = \boldsymbol{Z}(G)$; therefore to prove that the nilpotent group $G$ is special it suffices to prove that $\langle c_1, \ldots, c_s \rangle = G'$, that is $c_1, \ldots, c_s \in G'$. Conversely $c_1, \ldots, c_s \in G'$ if and only if the following relation holds:

$$c_1, \ldots, c_s \in \langle [e_i, e_j], i, j = 1, \ldots, m \rangle = \left\langle \prod_{k=1}^{s} c_k^{m_{k_{ij}}}, i, j = 1, \ldots, m \right\rangle$$

and since

$$c_1 = c_1^1 c_2^0 \ldots c_s^0, \qquad c_2 = c_1^0 c_2^1 c_3^0 \ldots c_s^0, \ \ldots, \ c_s = c_1^0 c_2^0 \ldots c_{s-1}^0 c_s^1$$

then $\{(m_{1_{ij}}, m_{2_{ij}}, \ldots, m_{s_{ij}}), i < j\}$

must be a set of generators of $\underbrace{\boldsymbol{Z}/p\boldsymbol{Z} \times \ldots \times \boldsymbol{Z}/p\boldsymbol{Z}}_{s}$.

2.4. REMARK. – The previous theorem gives a restriction to the order of $G'$: a nilpotent group of class 2 and exponent $p \neq 2$, with $m$ generators and with the commutator subgroup of order $p^s$, can be special only if $s \leqslant m(m-1)/2$, as we want to stress.

## 3. – Some constructions of special $p$-groups of exponent $p$ with $m$ generators and commutator subgroup of order $p^s$, with $s \leqslant m(m-1)/2$.

Let $p$ be an odd prime, $m$ and $s$ integers with $s \leqslant m(m-1)/2$; firstly, in this section, we will show that it is always possible to construct, up to isomorphism, a special $p$-group of exponent $p$ with $m$ generators and commutator subgroup of order $p^s$. In fact, let $G$ be such a group, then $s$ matrices $M_1, \ldots, M_s$, with the conditions of Theorem 2.3, are associated to $G$; in fact:

$$[e_i, e_j] = z_1^{m_{1_{ij}}} z_2^{m_{2_{ij}}} \ldots z_s^{m_{s_{ij}}}$$

where $M_k = [M_{k_{ij}}]$, $\forall k = 1, \ldots, s$.

We construct a group $\widetilde{G}$ which results to be isomorphic to $G$.

Consider the product of $m+s$ copies of the field $\boldsymbol{Z}/p\boldsymbol{Z}$, i.e. $\underbrace{\boldsymbol{Z}/p\boldsymbol{Z} \times \ldots \times \boldsymbol{Z}/p\boldsymbol{Z}}_{m+s}$, with the following operation:

$$(x_1, \ldots, x_m, c_1, \ldots, c_s) * (y_1, \ldots, y_m, d_1, \ldots, d_s) =$$

$$\left( x_1 + y_1, \ldots, x_m + y_m, c_1 + d_1 + \sum_{\lambda=1}^{m-1} \sum_{k=\lambda+1}^{m} m_{1_{k\lambda}} x_k y_\lambda, \ldots, c_s + d_s + \sum_{\lambda=1}^{m-1} \sum_{k=\lambda+1}^{m} m_{s_{k\lambda}} x_k y_k \right).$$

3.1. PROPOSITION. – $(\widetilde{G}, *)$ *is a group isomorphic to* $G$.

PROOF. – It is easy to verify that $(\widetilde{G}, *)$ is a group. In order to show that it is isomorphic to $G$, define $\varphi\colon G \to \widetilde{G}$ by the rule:

$$x = \prod_{i=1}^{m} e_i^{x_i} z_1^{\alpha_1} \dots z_s^{\alpha_s} \mapsto (x_1, \dots, x_m, \alpha_1, \dots, \alpha_s)$$

$\forall x, y$ as before; we have:

$$xy = \prod_{i=1}^{m} e_i^{x_i + y_i} \prod_{l=1}^{s} z_l^{\sum_{\lambda=1}^{m-1} \sum_{k=\lambda+1}^{m} m_{l_{k\lambda}} x_k y_\lambda + \alpha_l + \beta_l} .$$

Then

$$\varphi(xy) = \left( x_1 + y_1, \dots, x_m + y_m, \alpha_1 + \beta_1 + \sum_{\lambda=1}^{m-1} \sum_{k=\lambda+1}^{m} m_{1_{k\lambda}} x_k y_\lambda, \dots, \alpha_s + \beta_s + \right.$$

$$\left. \sum_{\lambda=1}^{m-1} \sum_{k=\lambda+1}^{m} m_{s_{k\lambda}} x_k y_\lambda \right) = (x_1, \dots, x_m, \alpha_1, \dots, \alpha_s) * (y_1, \dots, y_m, \beta_1, \dots, \beta_s) =$$

$$\varphi(x) * \varphi(y) .$$

This mapping is an isomorphism; in fact it results:

$\ker \varphi = \{x \in G / \varphi(x) = (0, \dots, 0, 0, \dots, 0)\} =$

$$\left\{ x = \prod_{i=1}^{m} e_i^{x_i} z_1^{\alpha_1} \dots z_s^{\alpha_s} \in G / (x_1, \dots, x_m, \alpha_1, \dots, \alpha_s) = (0, \dots, 0, 0, \dots, 0) \right\} = 1 .$$

The inequality $s \leqslant m(m-1)/2$ is weak, as we will show from the last results.

3.2. Remark. – Let $G$ be a special $p$-group satisfying the conditions of Theorem 2.3. If $(m_{1_{ij}}, m_{2_{ij}}, \dots, m_{s_{ij}}) \neq 0$ for some particular $i$ and $j$ and $m_{1_{lt}}, m_{2_{lt}}, \dots, m_{s_{lt}}) = 0$, $\forall l \neq i$ and $\forall t \neq j$, then $G$ is the product of two abelian subgroups. In fact, consider:

$A = \langle \boldsymbol{Z}(G),$

$$(0,\dots,0,\underset{i}{1},0,\dots,0,\underset{j}{1},0,\dots,\underbrace{0,\dots,0}_{s}),(0,\dots,0,\underset{i}{-1},0,\dots,0,\underset{j}{-1},0,\dots,\underbrace{0,\dots,0}_{s})\rangle$$

and

$B = \langle \boldsymbol{Z}(G),(1,0,\dots,0),(0,1,\dots,0),\dots,(0,\dots,0,\underset{i-1}{1},0,\dots,0),(0,\dots,0,\underset{i+1}{1},0,\dots,0),\dots$

$$\dots,(0, \dots, 0, \underset{j-1}{1}, 0, \dots, 0),(0, \dots, 0, \underset{j+1}{1}, 0, \dots, 0)\rangle .$$

Then it is easy to prove that $|A| = p^{s+2}$, $|B| = p^{s+m-2}$ and $A$ and $B$ are abelian with $G = AB$.

In 1977 Bert Beisiegel [1] has constructed special $p$-groups of order $p^{3n}$, with commutator subgroup of order $p^n$, in the following way: let $G = F^3$, where $F = GF(p^n)$; consider $G$ with this multiplication law:

$$(a_1, a_2, a_3) * (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3 + f(b_1, a_2)).$$

It is possible to generalize such a construction in several ways. One of them is the following. Let $G = \boldsymbol{Z}/p\boldsymbol{Z} \times \ldots \times \boldsymbol{Z}/p\boldsymbol{Z}$ be the cartesian product of $2n+1$ copies of the ciclic group $\boldsymbol{Z}/p\boldsymbol{Z}$. Let then $f\colon \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z} \to \boldsymbol{Z}/p\boldsymbol{Z}$ be a bilinear mapping on $\boldsymbol{Z}/p\boldsymbol{Z}$, different from the zero one. Consider $G$ with the following operation:

$$(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n+1}) * (b_1, \ldots, b_n, b_{n+1}, \ldots, b_{2n+1}) =$$

$$(a_1 + b_1, \ldots, a_{n+1} + b_{n+1}, a_{n+2} + b_{n+2} + f(b_1, a_2), \ldots, a_{2n+1} + b_{2n+1} + f(b_1, a_{n+1})).$$

By easy but tedious calculation one can see that $(G, *)$ is a non-abelian group with $(0, \ldots, 0)$ as identity element and $(-a_1, \ldots, -a_{n+1}, -a_{n+2} + f(a_1, a_2), \ldots, -a_{2n+1} + f(a_1, a_{n+1}))$ as inverse of $(a_1, \ldots, a_{2n+1})$. Furthermore the following condition holds:

$$\Phi(G) = G' = \boldsymbol{Z}(G) = \{(0, \ldots, 0, x_{n+2}, \ldots, x_{2n+1}) \text{ with } x_{n+2}, \ldots, x_{2n+1} \in \boldsymbol{Z}/p\boldsymbol{Z}\}$$

so that $(G, *)$ is a special $p$-group of exponent $p$, for odd $p$, and of exponent 4 for $p = 2$.

Observe that by such a construction we can only have special $p$-groups which are product of two abelian subgroups: it will be sufficient to consider the subgroups:

$$A = \langle \boldsymbol{Z}(G), (1, 0, \ldots, 0)\rangle,$$

$$B = \langle \boldsymbol{Z}(G), (0, 1, 0, \ldots, 0), (0, 0, 1, \ldots, 0), \ldots, (0, 0, 0, \ldots, 0, \underset{n+1}{1}, 0, \ldots, 0)\rangle.$$

Now consider $G = \boldsymbol{Z}/p\boldsymbol{Z} \times \ldots \times \boldsymbol{Z}/p\boldsymbol{Z}$ the product of $2n$ copies of $\boldsymbol{Z}/p\boldsymbol{Z}$ with $n \geqslant 3$. Let again $f\colon \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z} \to \boldsymbol{Z}/p\boldsymbol{Z}$ be a bilinear mapping on $\boldsymbol{Z}/p\boldsymbol{Z}$, different from the zero one. Consider in this set the following operation:

$$(a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}) * (b_1, \ldots, b_n, b_{n+1}, \ldots, b_{2n}) =$$

$$(a_1 + b_1, \ldots, a_{n+1} + b_{n+1} + f(a_2, b_3), a_{n+2} + b_{n+2} + f(b_1, a_2), \ldots, a_{2n} + b_{2n} + f(b_1, a_n)).$$

Then $(G, *)$ is a non-abelian group with $(0, \ldots, 0)$ as identity element and $(-a_1, \ldots, -a_n, -a_{n+1} + f(a_2, a_3), -a_{n+2} + f(a_1, a_2), \ldots, -a_{2n} + f(a_1, a_n))$ as inverse of $(a_1, \ldots, a_{2n})$. In this case the following condition holds as well: $\Phi(G) = G' = \boldsymbol{Z}(G) = \{(0, \ldots, 0, x_{n+1}, \ldots, x_{2n}) \text{ with } x_{n+1}, \ldots, x_{2n} \in \boldsymbol{Z}/p\boldsymbol{Z}\}$, so that also this group is a special one. Moreover, $(G, *)$ has exponent $p$ for odd $p$, and exponent 4 for $p = 2$.

3.3. PROPOSITION. – *Not all these special p-groups are the product of abelian subgroups.*

PROOF. – Consider in the last construction the case $p=2$. We want to investigate the abelian subgroups of $G$. It is easy to verify that

$$H=\{(0,0,0,x_4,x_5,\dots,x_{2n}),\quad x_4,x_5,\dots,x_{2n}\in \boldsymbol{Z}/2\boldsymbol{Z}\}$$

and all its subgroups are abelian.

Then an abelian subgroup $K$ of $G$, $K/\subset H$, must contain an element $a=(x_1,x_2,,x_3,x_4,\dots,x_{2n})$ in wich at least one among $x_1,x_2,x_3$ is not zero.

We now proceed to rule out each possible case:

if

$$a=(1,0,0,a_4,a_5,\dots,a_{2n}),$$

then $C_G(a)=\langle \boldsymbol{Z}(G),a\rangle$ i.e. $|C_G(a)|=p^{n+1}$;

if

$$a=(0,1,0,a_4,a_5,\dots,a_{2n}),$$

then the only elements which commute with this one and commute with each other are of this type: $(0,x_2,0,x_4,x_5,\dots,x_{2n})$, then $|K|=p^{2n-2}$;

if

$$a=(0,0,1,a_4,a_5,\dots,a_{2n}),$$

then the only elements which commute with this one and commute with each other are of this type: $(0,0,x_3,x_4,x_5,\dots,x_{2n})$, then $|K|=p^{2n-2}$;

if

$$a=(1,1,0,a_4,a_5,\dots,a_{2n}),$$

then $C_G(a)=\langle \boldsymbol{Z}(G),a\rangle$ i.e. $|C_G(a)|=p^{n+1}$;

if

$$a=(0,1,1,a_4,a_5,\dots,a_{2n}),$$

then the only elements which commute with this one and commute with each other are of this type: $(0,x_2,x_3,x_4,x_5,\dots,x_{2n})$, then $|K|=p^{2n-2}$;

if

$$a=(1,0,1,a_4,a_5,\dots,a_{2n}),$$

then $C_G(a)=\langle \boldsymbol{Z}(G),a\rangle$ i.e. $|C_G(a)|=p^{n+1}$;

if

$$a = (1, 1, 1, a_4, a_5, \dots, a_{2n}),$$

then $C_G(a) = \langle \boldsymbol{Z}(G), a\rangle$ i.e. $|C_G(a)| = p^{n+1}$.

In all this cases $|A||B|/|A \cap B| < p^{2n}$, for all abelian subgroups $A$ and $B$ of $G$; so $G$ cannot be the product of two abelian subgroups, q.e.d.

## 4. – Abelian subgroups and automorphisms.

Let $G$ be a special $p$-group of exponent $p$ with $|G| = p^{m+s}$ and $|G'| = p^s$. What can we say about a natural number $r$ if $A$ is an abelian subgroup of $G$ of order $p^{s+r}$?

4.1. PROPOSITION. – *Let $G$ be a special $p$-group of exponent $p$ with $|G| = p^{m+s}$. If $A$ is an abelian subgroup of $G$ with $|A| = p^{s+r}$ then $r(r-1)/2 \leqslant m(m-1)/2 - s$.*

PROOF. – Let $\{e_1, \dots, e_m\}$ be a base of $G$ with $e_1, \dots, e_r \in A$, then the matrices associated to $G'$ are of this type:

$$M_j = \begin{bmatrix} \mathbf{0} & M_{1j} \\ -M_{1j} & M_{2j} \end{bmatrix}, \qquad \forall j = 1, \dots, s\,.$$

By Theorem 2.3, $\{(m_{1_{ij}}, m_{2_{ij}}, \dots, m_{s_{ij}}), i < j\}$ is a system of generators of $\underbrace{\boldsymbol{Z}/p\boldsymbol{Z} \times \dots \times \boldsymbol{Z}/p\boldsymbol{Z}}_{s}$; on the other hand we have: $(m_{1_{lt}}, m_{2_{lt}}, \dots, m_{s_{lt}}) = (0, \dots, 0)$ $\forall l, t = 1, \dots, r,\ \ l < t$. Consequently by Theorem 2.3: $m(m-1)/2 - r(r-1)/2 \geqslant s$, i.e. $r(r-1)/2 \leqslant m(m-1)/2 - s$.

4.2. PROPOSITION. – *Every special $p$-group of exponent $p$, $|G| = p^{m+s}$, with $s = m(m-1)/2$, has abelian subgroups of order at most $p^{s+1}$ and then, if it is not an extraspecial $p$-group of order $p^3$, it cannot be the product of two abelian subgroups containing the center.*

PROOF. – The proof is almost immediate. In fact, since $r(r-1)/2 \leqslant m(m-1)/2 - s = 0$, then $r = 1$ and $|A| = p^{s+1}$.

4.3. COROLLARY. – *Every vector space of dimension $m$ on $\boldsymbol{Z}/p\boldsymbol{Z}$, with $s$ bilinear alternating forms, $s = m(m-1)/2$, has isotropic subspaces of dimension at most* 1.

4.4. PROPOSITION. – *Let $G$ be a special $p$-group of exponent $p$ with $|G| = p^{m+s}$. If it is ordinary, then $m = 2n$ and every abelian subgroup of $G$ containing the center has order at most $p^{n+s}$.*

PROOF. – By our hypothesis on $G$ there exists a non singular matrix $M = \sum_{i=1}^{s} \lambda_i M_i$. Let $f$ be the bilinear form associated to $M$: then $(G/G', f)$ is a non-degenerate simplectic space on $\boldsymbol{Z}/p\boldsymbol{Z}$ and $\dim G/G' = m = 2n$ (see [7]). Let
$A \geq \boldsymbol{Z}(G) = G'$ be an abelian subgroup of $G$. Then $A/G'$ is an isotropic subspace of $G/G'$; hence $\dim A/G' \leq n$, i. e. $|A| \leq p^{s+n}$.

Let now $\sigma$ be an automorphism of $G$. Since $G'$ is characteristic, it holds $\sigma(G') = G'$ and then, since $G'$ is a $s$-dimensional vector space on $\boldsymbol{Z}/p\boldsymbol{Z}$, $\sigma$ induces an automorphism $\sigma'\colon G' \to G'$ which can be represented by a non singular matrix $T$ of order $s$ on $\boldsymbol{Z}/p\boldsymbol{Z}$, i. e. $T \in (\boldsymbol{Z}/p\boldsymbol{Z}, s \times s)$. Similarly $\sigma$ induces on $G/G'$ an automorphism of vector space which can be represented by a non singular matrix $N \in (\boldsymbol{Z}/p\boldsymbol{Z}, m \times m)$. Moreover, $T$ and $N$ satisfy the following conditions: $\forall x, y \in G$ it holds $[x^\sigma, y^\sigma] = [x, y]^\sigma$, then, if $X$ and $Y$ are the column matrices of coordinates of $xG'$ and $yG'$ with respect to a given base, we have:

$$[NX, NY] = T[x, y], \qquad \forall X, Y.$$

Consequently:

$$N^t M_j N = \sum_{k=1}^{s} t_{jk} M_k, \qquad \forall j = 1, \ldots, s. \tag{$*$}$$

Vice versa, let $T$ and $N$ be non singular matrices satisfying condition ( $*$ ). They give rise to $p^{sm}$ different automorphisms of $G$ by the following expressions:

$$\begin{cases} e_i^\sigma = e_1^{n_{1i}} e_2^{n_{2i}} \ldots e_m^{n_{mi}} y_i, & \text{with } y_i \in G', \\ c_k^\sigma = c_1^{t_{1k}} c_2^{t_{2k}} \ldots c_s^{t_{sk}}, & \end{cases}$$

where $N = (n_{ij})$, $T = (t_{ij})$. It follows:

4.5. PROPOSITION. – *Let $T$ and $N$ be two non singular matrices of order $m$ and $s$ respectively on the field $\boldsymbol{Z}/p\boldsymbol{Z}$. Then there exists $\sigma \in \mathrm{Aut}(G)$, such that $T$ and $N$ are its associated matrices, if and only if they satisfy ( $*$ ). In this case there are precisely $p^{sm}$ of such automorphisms.*

Now suppose that $G$ is the product of two abelian subgroups $A$ and $B$. In this case one can choose a base $\{e_1, \ldots, e_m\}$ of $G$ with $e_1, \ldots, e_r \in A$ and $e_{r+1}, \ldots, e_m \in B$, so that:

$$M_j = \begin{pmatrix} \mathbf{0} & M_{1j} \\ -M_{1j}^t & \mathbf{0} \end{pmatrix}, \qquad \forall j = 1, \ldots, s.$$

4.6. REMARK. – If $G$ is the product of two abelian subgroups and it is ordinary, then each $M_{1j}$ is a square matrix of order $n$. Indeed, in this case, $m = 2n$.

Suppose that $|A| = p^{s+r}$ with $r > n$, i. e. $M_{1j} \in (\boldsymbol{Z}/p\boldsymbol{Z},\, r \times 2n - r)$, $\forall j = 1, \ldots, s$. Then also $M = \sum_{k=1}^{s} \lambda_k M_k$ is of the following type:

$$M = \begin{pmatrix} \mathbf{0} & M_1 \\ -M_1^t & \mathbf{0} \end{pmatrix}$$

with $M_1 \in (\boldsymbol{Z}/p\boldsymbol{Z},\, r \times 2n - r)$. Since $r > n$, we have $r > 2n - r$ and $\operatorname{rank} M_1 < r$, that is $\operatorname{rank} M_1 < 2n$. Obviously this is an absurd, so $r = n$ and $M_1, M_{1i} \in (\boldsymbol{Z}/p\boldsymbol{Z},\, n \times n)$, $\forall j = 1, \ldots, s$.

4.7. PROPOSITION. – *If $G$ is an ordinary special $p$-group product of two abelian subgroups, then $G$ admits $p'$-automorphisms.*

Proof. – Consider $N = h\boldsymbol{I}_{2n}$ and $T = h^2 \boldsymbol{I}_s$, with $h \in (\boldsymbol{Z}/p\boldsymbol{Z})^*$, then the following is an automorphism of $G$:

$$\begin{cases} e_i^\sigma = e_i^h\,, & \forall i = 1, \ldots, 2n\,, \\ c_k^\sigma = c_k^{h^2}\,, & \forall k = 1, \ldots, s\,. \end{cases}$$

Since $h^p \equiv h (\operatorname{mod} p)$, then $\sigma^p = \sigma$ and so $\sigma^{p-1} = Id_G$, i.e. $|\sigma| \,\Big|\, (p-1)$.

4.8. COROLLARY. – *If $G$ is the product of two abelian subgroups, then $G$ has normal subgroups which are not characteristic.*

Proof. – Let $|A| = p^{s+r}$ and $|B| = p^{s+m-r}$, with $G = AB$. If $h, k \in (\boldsymbol{Z}/p\boldsymbol{Z})^*$, $h \neq k$, we consider:

$$N = \begin{pmatrix} h\boldsymbol{I}_r & \mathbf{0} \\ \mathbf{0} & k\boldsymbol{I}_{m-r} \end{pmatrix}, \qquad T = hk\boldsymbol{I}_s\,.$$

Since $T$ and $N$ satisfy ( $*$ ), then from Proposition 4.5 there exists an automorphism $\sigma$ of $G$ associated to them. Let then $x = e_1 e_{r+1}$. Consider $H = \langle x \rangle G'$: then $H$ is normal in $G$ and, since $h \neq k$, we have: $x^\sigma = e_1^h e_{r+1}^k \notin H$. Therefore $H$ is not characteristic in $G$.

4.9. REMARK. – There are some special $p$-groups such that each normal subgroup is characteristic (see [4], [11]).

## 5. – Relatively free special $p$-groups and their quotients.

In this section we discuss about relatively free special $p$-groups. Firstly we will show that every special group having $m$ generators is a quotient of the free group $F$ on $m$ generators. Let $p > 2$ be a prime, $K_3(F) = [F', F]$ and $F^p = \langle x^p / x \in F \rangle$. The quotient $G = F/F^p K_3(F)$ is the relatively free group in the class of nilpotent groups of class 2 and exponent $p$. It is well known that

$$G \cong \langle a_1, \ldots, a_m / a_i^p = [[a_r, a_s], a_i] = 1, \quad \forall i, r, s = 1, \ldots, m \rangle .$$

$G$ is a special group. In fact, by contradiction, if $x = a_1^{\alpha_1} \ldots a_m^{\alpha_m} \in \boldsymbol{Z}(G) - G'$ then $x a_i = a_i x$, $\forall i = 1, \ldots, m$, that is, $a_1^{\alpha_1} \ldots a_m^{\alpha_m} a_i = a_i a_1^{\alpha_1} \ldots a_m^{\alpha_m}$. These are relations different both from those of the presentation and any of their linear combinations. This fact violates the freedom of $F$ on generators. Moreover, $G' = \langle [a_r, a_s], \forall r, s = 1, \ldots, m \rangle$, so that it has order $p^{m(m-1)/2}$. Necessarily $G$ has a smaller order than $p^{m(m-1)/2}$. Otherwise the commutators $[a_i, a_j]$, $i < j$ would not be indipendent and then there would exist $\lambda_{ij}$ for some $i, j$ so that $\prod_{i<j} [a_i, a_j]^{\lambda_{ij}} = 1$, contrary to the assumption of the relative freedom of $G$.

If $H$ is a special $p$-group of exponent $p$, using Von Dyck's theorem (see [8]), $H$ is an omomorphic image of $G$, that is, there exists an epimorphism $\varphi \colon G \to H$ with $H \cong G/\ker(\varphi)$.

Now we want to characterize those quotients of $G$ which are special groups. Let then $H$ be special, with $H' = \boldsymbol{Z}(H) = \Phi(H)$ and $|H/H'| = p^m$. It holds

$$\ker(\varphi) \leqslant G' = \Phi(G) .$$

Conversely $\exists x \in \ker(\varphi) - \Phi(G)$, so that $x$ could be an element of a basis of $G$, $\{x_1, \ldots, x_m\}$. In this case $H \cong G/\ker(\varphi)$ would have less than $m$ generators, what is a contradiction. If $\ker(\varphi) = G' = \Phi(G)$ then $G/H$ is elementary abelian. If it is non abelian, then $\ker(\varphi) < G'$. It holds $\varphi(\boldsymbol{Z}(G)) \leqslant \boldsymbol{Z}(H)$. Moreover, since $[G \colon \boldsymbol{Z}(G)] = [H \colon \boldsymbol{Z}(H)] = p^m$, we have, $\varphi(\boldsymbol{Z}(G)) = \boldsymbol{Z}(H)$.

Finally in Proposition 5.1 we will show that not every subgroup of $\boldsymbol{Z}(G)$ can be the kernel of an epimorphism from $G$ into a non-abelian special group.

5.1. PROPOSITION. – *$K \leqslant \boldsymbol{Z}(G)$ is the kernel of the above morphism if and only if $K$ does not contain any of $[a_i, G] = \langle \{[a_i, g] / g \in G\} \rangle$, $\forall a_i \in G - \boldsymbol{Z}(G)$.*

Proof. – Since $K \leqslant G' = \Phi(G)$, we have

$$(G/K)' \cong G'/K ,$$

$$\Phi(G/K) = \Phi(G)/K .$$

In order to verify whether the quotient is special it is necessary to study the properties of $\boldsymbol{Z}(G)$. Surely

$$\boldsymbol{Z}(G)/K \leqslant \boldsymbol{Z}(G/K),$$

therefore we must investigate when this inclusion becomes an equality.

It holds $aK \in \boldsymbol{Z}(G/K)$ if and only if $abK = baK$, $\forall bK \in G/K$, in other words if and only if $a^{-1}b^{-1}ab \in K$, $\forall b \in G$. The last condition is equivalent to have either $[a, b] = 1$, $\forall b \in G$, namely $a \in \boldsymbol{Z}(G)$, either $[a, b] \in K$, $\forall b \in G$, that is $[a, G] \leqslant K$.

Then it results $\boldsymbol{Z}(G)/K = \boldsymbol{Z}(G/K)$ if and only if $[a, b] \notin K$, $\forall a \in G - \boldsymbol{Z}(G)$.

## REFERENCES


[1] B. BEISIEGEL, *Semi-Extraspezielle p-Gruppen*, Math. Z., **156** (1977), 247-254.

[2] G. CORSI TANI, *Automorphisms and ultraspecial groups*, J. Algebra, **56** (1979), 43-49.

[3] D. GORENSTEIN, *Finite Groups*, Harper's Series in Modern Mathematics, Harper & Row, New York (1968).

[4] H. HEINEKEN, *Nilpotente Gruppen deren Samtliche Normalteileer charakteristich sind*, Archiv der Mathematik, **33** (1979), 497-503.

[5] H. HEINEKEN, *Nilpotent Groups of class two that can appear as central quotient groups*, Rend. Sem. Mat. Univ. Padova, **84** (1990), 241-248.

[6] H. HEINEKEN - H. LIEBECK, *The occurrence of finite groups in the automorphism group of nilpotent groups of class two*, Arch. Math., **24** (1973), 8-16.

[7] B. HUPPERT, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen Band CXXXIV, Springer-Verlag, Berlin (1967).

[8] D. ROBINSON, *A Course in the Theory of Groups*, Springer-Verlag, New York (1982).

[9] R. SCHARLAU, *Paare alternierender Formen*, Math. Z., **147** (1976), 13-19.

[10] L. VERARDI, *Gruppi semiextraspeciali di esponente p*, Ann. Mat. Pura Appl., IV, **146** (1987), 131-171.

[11] L. VERARDI, *Una classe di gruppi finiti di esponente p in cui ogni sottogruppo normale é caratteristico*, Boll. Un. Mat. Ital. (6), **4-B** (1985), 307-317.

[12] L. VERARDI, *A class of special p-groups*, submitted.

[13] A. L. VISNEVETSKII, *Nilpotent groups of class two and exponent p with commutator subgroup of order* $p^2$, Dokl. Akad. Nauk Ucrain SSR, ser. A, n. 9 (1980), 9-11.

[14] U. H. M. WEBB, *The occurrence of groups as automorphisms of nilpotent p-groups*, Arch. Math., **37** (1981), 481-489.



Dipartimento di Matematica, Politecnico di Torino
Corso Duca degli Abruzzi, 24 - I-10129 Torino

e-mail: cortini@dm.unito.it



*Pervenuta in Redazione*
*il 3 agosto 1996 e, in forma rivista, il 9 luglio 1997.*