MATHEMATICA, Tome 46 (69), N° 2, 2004, pp. 193–203

ON THE NUMBER OF CONJUGACY CLASSES OF FINITE p-GROUPS

CASIAN ALEXANDRU PANTEA

Abstract. Denote by $\mathrm{k}(G)$ the number of conjugacy classes of a group G. Some inequalities are deduced by arithmetic means for $\mathrm{k}(G)$, where G is a p-group. As an application, $\mathrm{k}(G)$ is calculated for special cases of p-groups. A method of estimating $\mathrm{k}(G)$ for some finite groups, others then p-groups is also presented.

MSC 2000. 20C15.

Key words. Conjugacy classes, characters, p-groups.

1. INTRODUCTION

Brauer was the first to estimate $\mathrm{k}(G)$ for a group G of order n. He has proved the inequality $\mathrm{k}(G) \geqslant \log\log n$. The result was later improved by L. Pyber [8] who emphasized an $\epsilon > 0$ such that $\mathrm{k}(G) \geqslant \epsilon\frac{\log n}{(\log\log n)^8}$. For smaller classes of finite groups stronger inequalities had been shown; P. Hall has proved, for instance, that $\mathrm{k}(G) \geqslant \log n$ for any nilpotent group G of order n; M. Cartwright has shown the existence of two positive constants a and b such that the inequality $\mathrm{k}(G) \geqslant a(\log n)^b$ holds for any solvable group G of order n. L. Héthely and B. Külshammer [3] have shown that $\mathrm{k}(G) \geqslant 2\sqrt{(p-1)}$, for any solvable group G and any prime p dividing the order of G. Moreover, they have conjectured that this estimation holds for any finite group G. They have also shown that there are no positive integers $a,\ b$ such that $\mathrm{k}(G) \geqslant ap + b$, for any group G and prime p, with $p^2||G|$.

In the case of p-groups, using mainly elementary notions and results we will deduce two main inequalities on $\mathrm{k}(G)$. The first one is studied together with its equality case, and some remarks are made concerning the strength of the second one. Two classes of p-groups are studied in detail, namely the p-groups having an abelian subgroup of index p and the groups G with $|Z(G)| = |G'| = p$. In the end, we develop a method of estimating $\mathrm{k}(G)$ for other classes of finite groups, other than p-groups.

2. PRELIMINARIES

If no other specifications are made, G will always denote a nonabelian group of order p^n, where p is a prime, $n \geqslant 2$, and the notations are the usual ones: G' for the derived subgroup of G, $Z(G)$ for the center of G, $C_G(x)$ for the centralizer of x in G, x^G for the conjugacy class of x in G.

Lemma 2.1. *With the above assumptions*

$$|x^G| \leqslant p^{n-2}.$$

Proof. It is enough to prove that

$$p^2 \leqslant |G : G'| \leqslant |C_G(x)|.$$

The second inequality is well known and easy to prove by putting it in the form $|G'| \geqslant |G : C_G(x)| = |x^G|$ and observing that if y is a conjugate of x, then $yx^{-1} \in G'$, so $y \rightarrowtail yx^{-1}$ is an injection from x^G in G'. For the first inequality, if we assume that $|G : G'| = p$, then G/G' would be cyclic and by the next more general result([2, Problem 6.31]) its lower central series would be stationary, impossible as G is nilpotent as a p-group. □

Proposition 2.2. *Let $G = G^{(0)} \leqslant G^{(1)} \leqslant \ldots$ the lower central series of a group (not necessarily p-group) G. If $G/G^{(1)}$ is cyclic, then $G^{(i)} = G^{(1)}$, for all $i \geqslant 1$.*

Proof. Consider the group $G/G^{(2)}$. Observe that $G^{(1)}/G^{(2)} \leqslant Z(G/G^2)$. We have $(G/G^{(2)})/(G^{(1)}/G^{(2)}) \simeq G/G^{(1)}$, thus cyclic. But then it follows that $G/G^{(2)}$ is abelian, and moreover, $G^{(2)} \geqslant G^{(1)}$, thus $G^{(2)} = G^{(1)}$. We can proceed now by induction. □

3. THE FIRST INEQUALITY

We shall denote by α_i, $i = 1, \ldots, n-2$ the number of conjugacy classes of G of size p^i. The class equation becomes

$$p^n = \sum_{i=0}^{n-2} \alpha_i p^i. \tag{1}$$

The number of conjugacy classes is then $\sum_{i=0}^{n-2} \alpha_i$ and $\alpha_0 = |Z(G)|$, so $p|\alpha_0$.

The main result of this section is obtained regarding the relation (1) as an equation in α_i and determining those α_i that minimize $\sum_{i=0}^{n-2} \alpha_i$. The next lemma solves the problem of determining this minimum.

Lemma 3.1. *Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-2}$ be positive integers that satisfy the equality* (1) *and $p|\alpha_0$. Then the minimum of the sum $\sum_{i=0}^{n-2} \alpha_i$ is obtained for $\alpha_0 = p$, $\alpha_1 = \alpha_2 = \ldots = \alpha_{n-3} = p-1$ and $\alpha_{n-2} = p^2 - 1$.*

Proof. Consider the set $\mathcal{S}$ of vectors $(\alpha_0, \alpha_1, \ldots, \alpha_{n-2}) \in \mathbb{N}^{n-1}$ which are solutions for (1), with $\alpha_0 \neq 0$ multiple of p, and let $(\beta_0, \beta_1, \ldots, \beta_{n-2}) \in \mathcal{S}$ which minimize the sum $\sum_{i=0}^{n-2} \alpha_i$. First we prove that $\beta_0 = p$. Indeed, suppose that $\beta_0 \neq p$. As $p|\beta_0$ we get $\beta_0 = \beta_0' + p$, where $p|\beta_0'$ and $\beta_0' \neq 0$. But then $(\beta_0', \beta_1 + 1, \beta_2, \ldots \beta_{n-2}) \in \mathcal{S}$, and

$$\beta_0' + (\beta_1 + 1) + \beta_2 + \ldots + \beta_{n-2} = \sum_{i=0}^{n-2} \beta_i + 1 - p < \sum_{i=0}^{n-2} \beta_i,$$

which contradicts the choice of $(\beta_0, \beta_1, \ldots, \beta_{n-2})$.

We similarly prove that $\beta_i \leqslant p-1$, for $i = 1, \ldots, n-3$. Suppose there is k in $\{1, \ldots, n-3\}$ such that $\beta_k \geqslant p$. Then $\beta_k = \beta'_k + p$, where $\beta'_k \in \mathbb{N}$. We get $(\beta_0, \ldots, \beta_{k-1}, \beta'_k, \beta_{k+1}+1, \beta_{k+2}, \ldots, \beta_{n-2}) \in \mathcal{S}$ and

$$\beta_0 + \ldots + \beta_{k-1} + \beta'_k + (\beta_{k+1}+1) + \ldots + \beta_{n-2} = \sum_{i=0}^{n-2} \beta_i + 1 - p < \sum_{i=0}^{n-2} \beta_i,$$

again contradiction. Further on, from (1) and $\alpha_0 > 0$ we get $\alpha_{n-2} \leqslant p^2 - 1$.

Taking into account that $(p, p-1, p-1, \ldots, p-1, p^2-1) \in \mathcal{S}$ and what proved above we conclude that the minimum of the sum $\sum_{i=1}^{n-2} \alpha_i$ is indeed reached for α_i chosen like in the lemma. □

This lemma immediately implies the next result.

PROPOSITION 3.2. *Let G be a group of order p^n. Then*

$$\mathrm{k}(G) \geqslant p^2 + (n-2)(p-1). \tag{2}$$

4. ANOTHER PROOF FOR THE INEQUALITY (2). THE EQUALITY CASE

A new proof of Proposition 3.2 allows us to treat the equality case. The method of the first proof will be used again in this paper since it provides some information on the structure of groups satisfying the equality in (2). The second proof uses the following lemma, which is true for any finite group.

LEMMA 4.1. *Let G be a finite group, $H \lhd G$ and j the number of conjugacy classes of G which are not included in H. Then*

$$\mathrm{k}(G) \geqslant k(G/H) + j - 1. \tag{3}$$

Proof. Define the mapping $\phi : \{x^G \mid x \notin H\} \to \{(xH)^{(G/H)} \mid x \notin H\}$, $\phi(x^G) = (xH)^{G/H}$ taking the set of the conjugacy classes of G not included in H into the set of nontrivial conjugacy classes of G/H. We show that ϕ is well defined. Let $y \in x^G$; there is $g \in G$ such that $y = g^{-1}xg$, thus $\phi(y^G) = (g^{-1}xgH)^{G/H}$. We need to prove that xH and $g^{-1}xgH$ are conjugate in G/H. But that is clearly true, since $g^{-1}xgH = (gH)^{-1}xHgH$.

Now, ϕ is obviously onto. Then $|\{x^G \mid x \notin H\}| \geqslant |\{(xH)^{G/H} \mid x \notin H\}|$, so $\mathrm{k}(G) - j \geqslant k(G/H) - 1$, and the conclusion follows. □

In what the equality in (3) is concerned, the next proposition emphasizes the subgroups H of G for which it is true.

PROPOSITION 4.2. *Maintaining the hypothesis of Lemma 4.1, the equality holds in* (3) *if and only if the subgroup H satisfies the condition*

$$\textit{for all } x, y \in G \setminus H, \quad xy^{-1} \in H, \quad \textit{implies} \quad x^G = y^G. \tag{4}$$

Proof. The equality in (3) is equivalent to the injectivity of ϕ, or, further, with the implication

$$(xH)^{G/H} = (yH)^{G/H} \quad \Longrightarrow \quad x^G = y^G,$$

for any $x, y \in G \setminus H$, which is equivalent to the implication

$$(\text{there is } g \in G : yH = (g^{-1}xg)H) \Longrightarrow x^G = y^G,$$

for $x, y \in G \setminus H$, or

$$(\text{there is } g \in G : g^{-1}xgy^{-1} \in H) \Longrightarrow x^G = y^G. \tag{5}$$

To finish, we prove that the implications (4) and (5) are equivalent. Let $x, y \in G \setminus H$ with $xy^{-1} \in H$. Then there is $1 \in G : 1^{-1}x1y^{-1} \in H$, so $x^G = y^G$ according to (5). We conclude that (5) implies (4).

Conversely, let $x, y \in G \setminus H$ and $g \in H : g^{-1}xgy^{-1} \in H$. According to (4), we have $(g^{-1}xg)^G = y^G$. But $(g^{-1}xg)^G = x^G$, and this proves that (4) implies (5). □

Remark 4.3. A subgroup H of G satisfies condition (4) if and only if the cosets xH, $x \notin H$ represent exactly the conjugacy classes of G not included in H.

A subgroup H of G is called *special* (see [2, page 6]) if, for any $x, y \in G$ with $x \notin H$, there is a unique $u \in G$ such that $y^{-1}xy = u^{-1}xu$. Note that any special subgroup H of G provides equality in (3).

Indeed, first we prove that $H \lhd G$. Let $v \in H, y \in G$ and $x = yvy^{-1}$. We need to show that $x \in H$. Suppose $x \notin H$. Then there exists $u \in H$ such that $v = y^{-1}xy = u^{-1}xu$. It follows that $uvu^{-1} = x \in H$, contradiction. Further on, in order to prove that (4) is fulfilled, let $x \in G - H$. Because H is special, the elements $u^{-1}xux^{-1}$ are pairwise distinct and form a set of cardinal $|H|$. But $u^{-1}(xux^{-1}) \in H$, so $H = \{u^{-1}xux^{-1} | u \in H\}$. Thus $Hx = \{u^{-1}xu | u \in H\} = \{y^{-1}xy | y \in G\}$.

Now we can give a proof of Proposition 3.2 using (3). Taking in 4.1 $H = Z(G)$, we obtain $\mathrm{k}(G) \geqslant k(G/Z(G)) + |Z(G)| - 1$. We use induction on n. For $n = 2$ we have equality. Suppose that $k(P) \geqslant p^2 + (\alpha - 2)(p - 1)$, for any group P with $|P| = p^\alpha, \alpha < n$. Let $|Z(G)| = p^{n-k}$. The inequality above and the hypothesis of induction applied to $G/Z(G)$ give $\mathrm{k}(G) \geqslant p^2 + (k-2)(p-1) + p^{n-k} - 1$, and the obvious inequality $p^{n-k} \geqslant (n-k)(p-1) + 1$ leads to the desired conclusion.

Observe the fact that the equality in (2) imposes equalities in each of the inequalities used above. By 4.3 it follows that the nontrivial conjugacy classes of G are exactly the cosets $xZ(G)$, where $x \notin Z(G)$, and they all have the same cardinal. On the other hand, we have saw that $n \geqslant 4$ implies the existence of $p^2 - 1$ conjugacy classes of size p^{n-2} and of $p - 1$ classes of size p^{n-3}. Consequently, n can only be 3, and in this case it is well known that $\mathrm{k}(G) = p^2 + p - 1$, so the equality in (2) holds.

The next proposition summarizes the above observations.

PROPOSITION 4.4. *The following statements are equivalent:*
(i) $\mathrm{k}(G) = p^2 + (n-2)(p-1)$*;*
(ii) G *has exactly* $p^2 - 1$ *conjugacy classes of size* p^{n-2}*, exactly* $p-1$ *conjugacy classes of size* p^i*,* $i = 1, \ldots, n-3$ *and* $|Z(G)| = p$*;*
(iii) $n = 3$.

5. THE SECOND INEQUALITY

Let p be a prime and $|G| = p^n$, where $n = 2m + e$, $m \geqslant 0$ and $e = 0, 1$. A result of P. Hall states that

$$\mathrm{k}(G) = p^{\mathrm{e}} + (p^2 - 1)(m + (p-1)k)$$

for some positive integer k. The original proof is rather complicated; simpler proofs use characters and can be found in [7] and [4, Theorem 26.5]. As an immediate consequence, one obtains

THEOREM 5.1. *With the above notations we have*

$$\mathrm{k}(G) \geqslant p^{\mathrm{e}} + (p^2 - 1)m.$$

Separating into two cases, we can write

$$\mathrm{k}(G) \geqslant m(p^2 - 1) + 1, \text{ if } |G| = 2m, \tag{6}$$

$$\mathrm{k}(G) \geqslant m(p^2 - 1) + p, \text{ if } |G| = 2m + 1. \tag{7}$$

The equality

$$\chi_1(1)^2 + \chi_2(1)^2 + \ldots + \chi_k(1)^2 = |G|,$$

where $\chi_1, \ldots, \chi_k$ are the complex irreducible characters of G, can be further written

$$p^{2m} = \sum_{i=0}^{m-1} \alpha_i p^{2i}, \tag{8}$$

if $n = 2m$ is even and

$$p^{2m+1} = \sum_{i=0}^{m} \alpha_i p^{2i} \tag{9}$$

if $n = 2m + 1$ is odd, where α_i denotes the number of irreducible characters of G of degree p^i.

A direct proof of inequalities (6) and (7) can be given by a simple mimic of the proof of Proposition 3.2 taking as starting relations (8) and (9) respectively. This idea of proving the two inequalities is not new; it turns out that G. Pazderski used it to prove the next result concerning their equality case, actually the correspondent of Proposition 4.4:

THEOREM 5.2. *With the above notations, suppose* $\mathrm{k}(G) = p^{\mathrm{e}} + (p^2 - 1)m$. *Then*

$$\begin{aligned} \alpha_0 &= p^2, \\ \alpha_i &= p^2 - 1, \ for\ i = \overline{1, n-1}, \\ \alpha_n &= p^e - 1. \end{aligned}$$

REMARK 5.3. a) For a group G of order p^p, (7) gives $\mathrm{k}(G) \geqslant \frac{1}{2}(p^3 - p^2 + p + 1)$. L.G. Kovács and C.R. Leedham-Green ([6]) have constructed, for every odd prime p a group of order p^p having exactly $\frac{1}{2}(p^3 - p^2 + p + 1)$ conjugacy classes. The estimation (7) is, therefore, smooth in this case.

b) Obviously, for nonabelian groups of order p^3 we have equality in (7). For groups of order p^4 the inequality (6) gives $\mathrm{k}(G) \geqslant 2p^2 - 1$. Let G a group of order p^4 with $|G'| = p^2$. From (8) it follows that G has only characters of degree 1 and p. (8) can be then written $\alpha_0 + \alpha_1 p^2 = p^4$, with $\alpha_0 = p^2$, thus $\alpha_1 = p^2 - 1$. It follows that $\mathrm{k}(G) = 2p^2 - 1$, so the estimation (6) is smooth in this case.

c) Let $K(r)$ be the minimum of the degrees of conjugacy classes for groups of order r and $k(r)$ the estimation from Theorem 5.1. Using the computer program GAP we can compare $K(r)$ and $k(r)$ for some powers of primes:

r	2^5	2^6	2^7	3^5	3^6	5^5
K(r)	11	13	14	19	41	53
k(r)	8	11	11	19	25	53

d) From the table above we see that, for the groups of order 3^5 and 5^5 the inequality (7) is smooth, reaching the equality. It's likely for this inequality to be exact for groups of order p^5, p odd prime.

e) Further descriptions of the equality case are due to G. Pazderski and can be found in [4, Theorem 26.5]; he has also proved that the bound is sharp for only finitely many exponents n.

6. FINITE P-GROUPS WITH AN ABELIAN SUBGROUP OF INDEX P

A well known result [5, Theorem 26.9] gives the characters of finite p-groups having an abelian subgroup of index p. We present this result in a slightly different way, in order to emphasize the number of conjugacy classes. Using then the inequalities (6) and (7) we will obtain very strong inequalities for such groups.

The following lemma turns out to be very useful:

LEMMA 6.1. *G be a nonabelian p-group having an abelian subgroup H of index p. Then there exists $K \lhd G$ such that $K \subseteq H \cap G' \cap Z(G)$ and $|K| = p$.*

Proof. We have $1 \neq G' \lhd G$ thus $G' \cap Z(G) \neq 1$. Let K be a subgroup of order p of $G' \cap Z(G)$. But then KH is an abelian subgroup of G; since H is maximal, it follows that $KH = H$, so $K \leqslant H$. $\square$

THEOREM 6.2. *Let G be a group of order p^n having an abelian subgroup H of index p. Let K be as in the lemma. Then*

$$\mathrm{k}(G) = \mathrm{k}(G/H) + p^{n-2} - p^{n-3}. \tag{10}$$

Proof. The irreducible characters of G/K lift to give exactly the characters of G that contain K in their kernel. The sum of the squares of their degrees is therefore $|G/K| = p^{n-1}$. We will construct another $p^{n-2} - p^{n-3}$ irreducible characters of G, each of degree p; we will have then constructed all the irreducible characters of G since

$$p^{n-1} + (p^{n-2} - p^{n-3})p^2 = p^n = |G|. \tag{11}$$

Let χ be a character of degree p of G. If χ is a sum of linear characters, then $G' \leqslant \operatorname{Ker}\chi$, thus $K \leqslant \operatorname{Ker}\chi$. Therefore if $\chi(1) = p$ and $K \nleqslant \operatorname{Ker}\chi$, then χ is irreducible. Now let Φ be the set of linear characters of H which do not have K in their kernel (that is, the lifts of the linear characters of G/K). Then $|\Phi| = p^{n-1} - p^{n-2}$. Let $\psi \in \Phi$. Since $K \leqslant Z(G)$ we have

$$(\psi \uparrow^G)(k) = p\psi(k), \quad \text{for all } k \in K.$$

We can conclude that $\psi \uparrow^G$ has degree p and can not contain K in its kernel, therefore is irreducible.

Suppose now that ψ_1 is a linear character of H such that $\psi \uparrow^G = \psi_1 \uparrow^G$. The Frobenius Reciprocity Theorem gives

$$1 = \langle \psi \uparrow^G, \psi_1 \uparrow^G \rangle_G = \langle (\psi \uparrow^G) \downarrow_H, \psi_1 \rangle_H.$$

Since $(\psi \uparrow^G) \downarrow_H$ has degree p, there are at most p elements ψ_1 of Φ such that $\psi_1 \uparrow^G = \psi \uparrow^G$. It follows that the set $\{\psi \uparrow^G \mid \psi \in \Phi\}$ gives at least $|\Phi|/p = p^{n-2} - p^{n-3}$ irreducible characters of G with degree p which do not have K in their kernel. But relation (11) assures us that this number is also the maximum, and the conclusion follows. □

Since in the above hypothesis G/K is a p-group, using the inequalities (6) and (7) we obtain the following estimations.

PROPOSITION 6.3. *Let G be a group of order p^n having an abelian subgroup of index p. Then*

a) $\mathrm{k}(G) \geqslant p^{n-2} - p^{n-3} + (m-1)(p^2-1) + p$, *if $n = 2m$;*

b) $\mathrm{k}(G) \geqslant p^{n-2} - p^{n-3} + m(p^2-1) + 1$, *if $n = 2m+1$.*

The equality (10) provides an upper bound for $\mathrm{k}(G)$.

PROPOSITION 6.4. *Let G be a group of order p^n having an abelian subgroup of index p. Then $\mathrm{k}(G) \leqslant p^{n-1} + p^{n-2} - p^{n-3}$, with equality if and only if $|G'| = p$.*

Proof. In view of (10), the maximum of $\mathrm{k}(G)$ is reached when G/K is abelian, or, equivalently, $G' \subseteq K$. But $K \subseteq G' \cap Z(G)$ and $|K| = p$, thus $G' \subseteq Z(G)$ and $|G'| = p$. But the last equality implies the first one, and the conclusion follows. □

Remark 6.5. a) The above inequalities are smooth (there is a group G for which the equality holds) if and only if the inequalities (6) and (7) used on G/K are smooth. We conclude, based on the remarks in the previous section, that the following estimations for groups G having abelian subgroups of index p are smooth:

$\mathrm{k}(G) \geqslant p^{p-1} - p^{p-2} + \frac{1}{2}(p^3 - p^2 + p + 1)$, for $|G| = p^{p+1}$;

$\mathrm{k}(G) \geqslant 3^4 - 3^3 + 19 = 73$ for $|G| = 3^6$;

$\mathrm{k}(G) \geqslant 5^4 - 5^3 + 53 = 553$ for $|G| = 5^6$.

b) The values of $\mathrm{k}(G)$ for groups of order p^3 and p^4 are known. We can also calculate them using the above inequalities. Clearly, a group of order p^3 contains an abelian subgroup of order p^2. Let G be a group of order p^4 and $|Z(G)| = p^2$. We can find a subgroup H of G of order p^3 such that $Z(G) \leqslant H$. But then, if H is not abelian, $H/Z(H)$ is cyclic of order p, a contradiction. If $|Z(G)| = p$, taking into account the class equation (1), there is an element x of G with $|x^G| = p$. Then $H = C_G(x)$ is of index p. Moreover, $Z(G)$ and $\langle x \rangle$ are distinct subgroups of H, thus $|Z(H)| \geqslant p^2$. As above, we conclude that H is abelian. Consequently, using Propositions 6.3 and 6.4 we obtain $\mathrm{k}(G) = p^2 + p - 1$ for $|G| = p^3$ and $2p^2 - 1 \leqslant \mathrm{k}(G) \leqslant p^3 + p^2 - p$ for $|G| = p^4$; in view of relation (10), these are the only values that $\mathrm{k}(G)$ can take in this case.

7. GROUPS G WITH $|Z(G)| = |G'| = P$

This class of groups is a generalization of extraspecial groups [1, page 108]. A group G is called extraspecial if $\Phi(G) = Z(G) = G'$ and they all are of order p. We go back to Lemma 4.1, and we will prove that under our hypothesis, the equality is reached in (3) by putting $H = Z(G)$. Moreover, we will be able to calculate the exact number of conjugacy classes for such groups.

Firstly, observe that $|G'| = |Z(G)| = p$ implies $G' = Z(G)$; using (3) we get $\mathrm{k}(G) \geqslant k(G/G') + |Z(G)| - 1 = p^{n-1} + p - 1$, since G/G' is abelian. On the other hand, G has p conjugacy classes of size 1 and another $p^n - p$ elements arranged in conjugacy classes of size greater or equal to p, thus at most another $(p^n - p)/p = p^{n-1} - 1$ conjugacy classes. Therefore, $\mathrm{k}(G) \leqslant p^{n-1} + p - 1$, thus G satisfies the equality in (3) with $H = Z(G)$.

In conclusion, we have the following result.

Proposition 7.1. *Let G be a group of order p^n with the property $|Z(G)| = |G'| = p$. The following statements are true:*

a) $\mathrm{k}(G) = p^{n-1} + p - 1$*;*

b) *the nontrivial conjugacy classes of G are exactly the cosets $xZ(G)$, $x \in G \setminus Z(G)$.*

Remark 7.2. We have proved that the special subgroups of a group G satisfy the equality in (3). Clearly, $Z(G)$ is not a special subgroup of G. It follows that the special subgroups of G do not cover, in general, the set of subgroups of G that give equality in (3).

We use now the results obtained in the previous section. If G contains an abelian subgroup of index p, then it follows from Propositions 6.4 and 7.1 that $\mathrm{k}(G) = p^{n-1} + p - 1 = p^{n-1} + p^{n-2} - p^{n-3}$, which implies $n = 3$. Therefore we obtain:

PROPOSITION 7.3. *Let G be a group of order p^n with the property $|G'| = |Z(G)| = p$. Then the following statements are equivalent:*
(i) *G contains an abelian subgroup of index p;*
(ii) $n = 3$.

8. AN APPLICATION: THE NUMBER OF COMMUTING PAIRS

One of our early motivations for this paper was a problem concerning the number of commuting pairs of elements of a group G.

We define the following two numbers associated to the finite group G.

$$N(G) = |\{(a,b) \in G \times G \mid ab = ba\}|,$$
$$N'(G) = |\{\{a,b\} \mid a,b \in G \setminus \{1\},\ a \neq b,\ ab = ba\}|.$$

The connection between these numbers and $\mathrm{k}(G)$ is given in the next proposition.

PROPOSITION 8.1. *For any finite group G we have:*
a) $N'(G) = \frac{N(G)-3|G|}{2} + 1$;
b) $N(G) = \mathrm{k}(G)|G|$.

Proof. a) We have

$$\{(a,b) \in G\times G \mid ab = ba\} = \{(a,b) \in G\times G \mid ab = ba,\ a \neq b\} \cup \{(a,a) \mid a \in G\},$$

hence

$$|\{\{a,b\} \in G \times G \mid ab = ba,\ a \neq b\}| = \frac{N(G) - |G|}{2}.$$

Further on, $\{\{a,b\} \in G\times G \mid ab = ba, a \neq b\} = \{\{1,a\} \mid a \in G\setminus\{1\}\} \cup \{\{a,b\} \mid a \neq b \neq 1 \neq a\}$, thus $N'(G) = |\{\{a,b\} \mid a \neq b \neq 1 \neq a\}| = \frac{N(G)-|G|}{2} - (|G| - 1) = \frac{N(G)-3|G|}{2} + 1$.

b) We have $\{(a,b) \in G \times G \mid ab = ba\} = \bigcup_{a\in G}\{(a,b) \mid ab = ba\}$, thus

$$N(G) = \sum_{a\in G} |\{b \mid ab = ba\}| = \sum_{a\in G} |C_G(a)|.$$

We group the elements of G in conjugacy classes to obtain

$$N(G) = \sum_{a\in\mathcal{R}} |a^G||C_G(a)| = \mathrm{k}(G)|G|,$$

where $\mathcal{R}$ is a complete set of representatives for the conjugacy classes of G. $\square$

9. OTHER CLASSES OF GROUPS

Any attempt to obtain estimations for $\mathrm{k}(G)$, where G is a finite group not necessarily p-group, based on the results obtained so far, implies the use of Sylow subgroups of G. In general though, going from a subgroup to the whole group does not imply the growth of the number of conjugacy classes. For instance, the group $\mathrm{PSL}(2,7)$ has order $168 = 24 \cdot 7$, 6 conjugacy classes and it obviously contains an abelian subgroup of order 7.

However, the previous section allows such a passing, based not on $\mathrm{k}(G)$, but on $\mathrm{k}(G)|G|$, which, in concordance with its meaning (the number of pairs which commute) grows from subgroup to group. By and large, the method is as follows. If P_p is a Sylow p-subgroup of G, then

$$\mathrm{k}(G)|G| \geqslant \sum_{p||G|} k(P_p)|P_p|,$$

and an inequality for $\mathrm{k}(G)$ follows. Observe that, in order for this inequality to be efficient, we need conditions on $|G|$, like, for instance, to have few prime factors in its decomposition or one of them to be greater then the product of the others. In what follows we illustrate the method for groups of order $p^n q$.

Proposition 9.1. *Let G be a group of order $p^n q$, p, q primes, $p > q$. Then*

$$\mathrm{k}(G) \geqslant \left[\frac{n}{2}\right](p+1) + q - 2.$$

Proof. As we saw in the previous section, $\mathrm{k}(G)|G| = \sum_{x\in G} |C_G(x)|$. Let P be a Sylow p-subgroup (actually, the only one) of G and Q a Sylow q-subgroup of G. Then

$$\begin{aligned}\mathrm{k}(G)|G| &= \sum_{x\in P} |C_G(x)| + \sum_{x\in Q} |C_G(x)| + \sum_{x\in G-(P\cup Q)} |C_G(x)| - p^n q\\ &\geqslant \sum_{x\in P} |C_P(x)| + \sum_{x\in Q} |C_Q(x)| + \sum_{x\in G-(P\cup Q)} |C_G(x)| - p^n q.\end{aligned}$$

Since $|C_G(x)| \geqslant q$, we get

$$\mathrm{k}(G)p^n q \geqslant k(P)|P| + k(Q)|Q| + (p^n q - p^n - q)q - p^n q$$

and further,

$$\mathrm{k}(G) \geqslant \frac{k(P)}{q} + \frac{q-q^2}{p^n} + q - 2.$$

Using the inequality (7) for P we obtain

$$k(P) \geqslant \left[\frac{n}{2}\right](p^2-1) + \frac{1}{q} + \frac{q-q^2}{p^n} + q - 2 \geqslant \left[\frac{n}{2}\right](p+1) + q - 2.$$

$\square$

REFERENCES

[1] Aschbacher, M., *Finite Groups Theory*, Cambridge University Press, 1994.
[2] Dixon, J.D., *Problems in Group Theory*, Dover Publications, 1973.
[3] Héthely, L. and Külshammer, B., *On the number of conjugacy classes of a finite solvable group*, Bull. London Math. Soc., **32** (2000), 668–672.
[4] Huppert, B., *Character Theory of Finite Groups*, De Gruyter, 1998.
[5] James, G. and Liebeck, M., *Representations and Characters of Groups*, Cambridge University Press, 1993.
[6] Kovács, L.G. and Leedham-Green, C.R., *Some normally monomial p-groups of maximal class and large derived length*, J. Math. Oxford, **37** (1986), 49–54.
[7] Mann, A., *Conjugacy classes in finite groups*, Israel Journal of Mathematics, **31** (1978), 78–84.
[8] Pyber, L., *Finite groups have many conjugacy classes*, J. London Math. Soc., **46** (1992), 239–249.
[9] Suzuki, M., *Group Theory II*, Springer-Verlag, 1986.

Received April 10, 2003

"Babeş-Bolyai" University
Faculty of Mathematics and Computer Science
Str. M. Kogălniceanu nr. 1
RO-400084 Cluj-Napoca, Romania
E-mail: casianpantea@hotmail.com