Rendiconti del Seminario Matematico della Università di Padova

Antonio Vera Lopez

The number of conjugacy classes in a finite nilpotent group

Rendiconti del Seminario Matematico della Università di Padova, tome 73 (1985), p. 209-216

<http://www.numdam.org/item?id=RSMUP_1985__73__209_0>

© Rendiconti del Seminario Matematico della Università di Padova, 1985, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (http://rendiconti.math.unipd.it/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

REND. SEM. MAT. UNIV. PADOVA, Vol. 73 (1985)

The Number of Conjugacy Classes in a Finite Nilpotent Group.

ANTONIO VERA LOPEZ (*)

SUMMARY - In this paper, we obtain the number of conjugacy classes $r(G)$ of a finite nilpotent group G as a function of the orders of the center of G and of any maximal abelian subgroup of G. Also, we prove that, if G is a p-group of order p^m and a_i is the number of conjugacy classes of G of size p^i, then $a_i \equiv 0$ (mod. $p-1$) for each i and

$$\sum_{1 \leqslant 2k-1 \leqslant m-2} a_{2k-1} \equiv 0 \pmod{p^2-1} .$$

Finally, we get two lower bounds for $r(G)$ and we consider several examples which improves the $\log_2|G|$ bound, the P. Hall's bound and one Sherman's lower bound.

In the following, G will denote a finite nilpotent group. Since the number of conjugacy classes in a direct product is the product of the number of conjugacy classes in each factor, we can suppose that G is a p-group, in the study of the number of conjugacy classes $r(G)$.

We use the standard notation: $[x, y] = x^{-1}y^{-1}xy$, $x^y = y^{-1}xy$, $\mathrm{Cl}_G(x) = \{x^g : g \in G\}$, $G' = \langle [x, y] : x, y \in G \rangle$ and $Z(G) = \{x \in G : g^x = g \ \forall g \in G\}$.

(*) Indirizzo dell'A.: Universidad del Pais Vasco, Facultad de Ciencias, Dpto de Matematicas, Apartado 644, Bilbao, España (Spain).

Throughout this paper, we will suppose that:

$$|G| = p^m = p^{2n+e} \text{ with } e = 0 \text{ or } 1 \text{ and } |Z(G)| = p^b .$$

1. The number $r(G)$.

LEMMA. Let N and M be two subgroups of G such that $Z(G) \leqslant N \lhd M \leqslant G$ and $M/N = \langle \bar{x} \rangle \simeq C_p$. Consider the isomorphism h: $N \mapsto N$ $y \mapsto y^x$ and suppose that h leaves exactly s conjugacy classes of N unchanged: $\mathrm{Cl}_N(y_1), \ldots, \mathrm{Cl}_N(y_s)$. Then there is an integer $k' \geqslant 0$, such that $s = p^b + k' \cdot (p-1)$.

PROOF. We define $T = \{y \in N \colon \mathrm{Cl}_N(y)^x = \mathrm{Cl}_N(y)\} = \mathrm{Cl}_N(y_1) \,\dot{\cup}\, \ldots \,\dot{\cup}\, \mathrm{Cl}_N(y_s)$. Arguing as in [9] pp. 83, there exists a natural number k such that k has exactly order $p-1$ module any divisor ($\neq 1$) of $|N|$. Now we consider the permutation

$$f\colon T \to T \text{ defined by } y \mapsto y^k$$

Clearly, we have $Z(G) \subseteq T$ and $f(T - Z(G)) = T - Z(G)$, because g.c.d. $(k, |Z(G)|) = 1$, hence $T - Z(G)$ is a union of some orbits of f. Moreover, the length of each orbit $\neq \{1\}$ of f is $p-1$, because $o(k) = p-1$ module $o(y)$ for each $y \in T - \{1\}$, hence $|T - Z(G)| \equiv 0 \pmod{p-1}$. Finally, $|\mathrm{Cl}_N(y_i)| \equiv 1 \pmod{p-1}$ for each i, implies

$$|Z(G)| + |T - Z(G)| = |T| = \sum_{i=1}^{s} |\mathrm{Cl}_N(y_i)| \equiv s \pmod{p-1} ,$$

and therefore, there is an integer $k' \geqslant 0$ such that $s = p^b + k' \cdot (p-1)$.

THEOREM 1. Let A be a maximal abelian subgroup of G of order p^a. Then there is an integer $k \geqslant 0$ such that

$$r(G) = (p^{2a}/p^m) + (p^b(p+1)(p^{m-a}-1)/p^{m-a}) + k \cdot (p^2-1)(p-1)/p^{m-a} .$$

PROOF. Clearly we have $Z(G) \leqslant A$ and we can consider a composition series of G: $1 = N_m < \ldots < N_u < \ldots < N_v < \ldots < N_1 < N_0 = G$ with $N_u = Z(G)$ and $N_v = A$. Let g_{i-1} be an element of $N_{i-1} - N_i$.

We know (cf. [15]) that

$$r(G) = \left(\sum_{i=1}^{m} s_i\,(p^2-1)/p^i\right) + 1/p^m \tag{1}$$

where s_i is the number of conjugacy classes of N_i unchanged by the automorphism $h_i\colon N_i \to N_i$, $z \mapsto g_{i-1}^{-1} z g_{i-1}$, $i = 1, \ldots, m$.

Since A is an abelian group, we have:

$$s_m = 1,\ s_{m-1} = p, \ldots, s_{v+1} = p^{a-1}\ \left(\text{and } s_v = |C_{N_v}(g_{v-1})|\right).$$

Moreover $Z(G) \leqslant A \leqslant N_l$ for each $l \leqslant v$, so, by lemma, there are number integers $k_l \geqslant 0$ such that $s_l = p^b + k_l \cdot (p-1)$ for each $l \leqslant v$.

Consequently, we have

$$\begin{aligned} r(G) &= (1/p^m) + \left(\sum_{i=1}^{m} s_i(p^2-1)/p^i\right) = \\ &= (p^2-1)(1 + p^2 + \ldots + p^{2(a-1)})p^{-m} + p^{-m} + \\ &\quad + (p^2-1)p^b(p^{-1}p^{-(m-a)} - p^{-1})(p^{-1}-1)^{-1} + \\ &\quad + (p^2-1)(p-1)(k_1 p^{-1} + k_2 p^{-2} + \ldots + k_{m-a} p^{-(m-a)}) = \\ &= p^{2a-m} + p^b(p+1)(p^{m-a}-1)p^{-(m-a)} + k\cdot(p^2-1)(p-1)p^{-(m-a)} \end{aligned}$$

for some integer $k \geqslant 0$.

REMARK. The relation (1) implies the congruence:

$$|G| \equiv r(G)\ (\operatorname{mod}\ (p^2-1)(p-1))\ \text{(cf. [15])}$$

Moreover

$$p^m = p^{2n+e} \equiv p^e + n(p^2-1) \quad (\operatorname{mod}\ (p^2-1)(p-1)) \tag{2}$$

and arguing as in ([6] V.15.2) or ([9] pp. 79) one obtain the following result of P. Hall: Let G be a group of order p^{2n+e}, $e = 0$ or 1, then for some non-negative integer k, we have $r(G) = p^e + (p^2-1)\left(n + k(p-1)\right)$.

EXAMPLES.

1) Let G be a non-abelian p-group of order p^m and suppose that, there exists A an abelian subgroup of G such that $|G/A| = p$. Then, we have $r(G) = p^{m-2} + p^{b-1}(p^2 - 1)$, with $p^b = |Z(G)|$. For example

a) If there is $\langle g \rangle \leqslant G$ such that $G/\langle g \rangle \simeq C_p$, then G is isomorphic to one of the following groups: D_{2m}, Q_{2m}, SD_{2m}, or M_{p^m}, and we have $r(D_{2m}) = r(Q_{2m}) = r(SD_{2m}) = 2^{m-2} + 3$, and $r(M_{p^m}) = p^{m-2} + p^{m-3}(p-1)(p+1)$.

b) If $|G| = p^m$ with $m = 3$ or 4, then, there exists $A \leqslant G$ such that $|G/A| = p$ and A is an abelian subgroup of G.

If $(m, a) = (3, 2)$, then $b = 1$ and $r(G) = p + p^2 - 1$.
If $(m, a) = (4, 3)$, then $b = 1$ or 2 and $r(G) = 2p^2 - 1$ or $p^2 + p(p^2 - 1)$.

2) Let G be a p-group of order p^m and suppose that A is a maximal abelian subgroup of G of order p^{m-2}. Then from Theorem 1, we have $r(G) = p^{m-4} + p^{b-2}(p+1)(p^2-1) + kp^{-2}(p^2-1)(p-1)$, for some integer $k \geqslant 0$. Moreover, if $|Z(G)| \geqslant p^2$, then p^2 divides k and $r(G) = p^{m-4} + p^{b-2}(p+1)(p^2-1) + k_1(p^2-1)(p-1)$, with $k_1 \geqslant 0$.

2. Two lower bounds for $r(G)$.

P. Hall (cf. [6] V.15.2) proves that $r(G) = p^e + n(p^2 - 1)$ if $|G| = p^{2n+e}$ with $e = 0$ or 1.

In general, if G is a finite group, Erdös and Turan (cf. [2]) proved $r(G) > \log_2 \log_2 |G|$. In [1] Bertram improves the $\log_2 \log_2 |G|$ bound, proving that $r(G) > (\log |G|)^c$ for « most » groups G, where c is any constant less than log 2. In 1978 Sherman (cf. [13]) proves that if G is a finite nilpotent group of nilpotency class t, then $r(G) \geqslant t \cdot |G|^{1/t} - t + 1$ and note that $r(G) \geqslant \log_2 |G|$.

In the following, we obtain two new lower bounds for $r(G)$ when G is a p-group of order p^m and we give some examples where one verifies that these bounds improve the know lower bounds.

COROLLARY 1. Let G be a group of order p^m and center of order p^b. If A is a maximal abelian subgroup of G of order p^a, then

$$r(G) \geqslant f(a, b) = (p^{2a}/p^m) + p^b(p+1)\left((p^{m-a}-1)/p^{m-a}\right).$$

Moreover $f(a, b)$ is a increasing function of each variable a and b.

PROOF. This follows directly from Theorem 1.

REMARK. If A is a maximal abelian normal subgroup of G of order p^a, then A is a maximal abelian subgroup, and $2m \leqslant a(a+1)$ forces $a \geqslant \big(-1+(1+8m)^{1/2}\big)/2$. Moreover, $1 \leqslant b < a < m$ if G is a non-abelian group (cf. [14] pp. 94).

For every prime number p, we define

$$d_i(p) = \min\{r(G)\colon |G| = p^i\}\,.$$

We have:

THEOREM 2. Let G be a group of order p^m. Then

$$r(G) \geqslant d_i(p) + (m-i)\cdot(p-1) \text{ for each } i \leqslant m\,.$$

PROOF. We consider $C_p \simeq H_1 \leqslant Z(G)$. Then

$$r(G) \geqslant r(G/H_1) + |H_1| - 1 = r(G/H_1) + p - 1\,.$$

Set $G_1 = G/H_1$ and consider $C_p \simeq H_2/H_1 \leqslant Z(G_1)$. Then $G/H_2 \simeq G_1/ /(H_2/H_1)$ and $r(G_1) \geqslant r(G/H_2) + |H_2/H_1| - 1 = r(G/H_2) + p - 1$, hence $r(G) \geqslant r(G/H_2) + 2\cdot(p-1)$. Repeating this reasoning, we obtain

$$r(G) \geqslant r(G/H_{m-i}) + (m-i)\cdot(p-1)$$

with $|G/H_{m-i}| = p^{m-(m-i)} = p^i$. Thus, $r(G) \geqslant d_i(p) + (m-i)(p-1)$ for each $i \leqslant m$.

EXAMPLE 1. If $|G| = p^4$, then $r(G) \in \{p^4,\ 2p^2-1,\ p^3+p^2-p\}$, hence $d_4(p) = 2p^2 - 1$. Consequently, if G is a group of order p^m with $m \geqslant 6$, then $r(G) \geqslant 2p^2 - 1 + (m-4)(p-1)$. Thus, we have $r(G) = = p^e + (p^2-1)\big(n + k(p-1)\big)$ with k an integer such that

$$k \geqslant \big(2p^2 - 1 + (m-4)(p-1) - p^e - n(p^2-1)\big)/\big((p^2-1)(p-1)\big)\,.$$

EXAMPLE 2. If $p = 2$, we have $d_1(2) = 2$, $d_2(2) = 4$, $d_3(2) = 5$, $d_4(2) = 7$, $d_5(2) = 11$, $d_6(2) = 13$, $d_7(2) = 14$ (cf. [4] and [12]). Suppose G of order 2^8. Then P. Hall's bound is $r(G) \geqslant 1 + 3\cdot 4 = 13$. On the other hand, Theorem 2 yields $r(G) \geqslant d_6(2) + (8-6)\cdot 1 = 13 + 2 = 15$, hence $r(G) = 13 + 3k \geqslant 15$, implies $r(G) \geqslant 16$. Finally the Sherman's bound yields $r(G) > 7 \cdot 2^{8/7} - 7 + 1 > \log_2 2^8 = 8$.

EXAMPLE 3. *Let* G be a group of order p^8 such that $|G/Z(G)| = p^4$. Then the nilpotency class of G is $t \leqslant 4$, and the Sherman's bound yields $r(G) \geqslant 4 \cdot p^{8/4} - 4 + 1 = 4p^2 - 3$. On the other hand, if A is a maximal abelian subgroup of G of order p^a, then $Z(G) < A$, hence $a \geqslant 5$ and the Corollary 1 implies

$$r(G) \geqslant p^2 + p^4(p+1)(p^3-1)p^{-3} = p^5 + p^4 - p > 4p^2 - 3 .$$

EXAMPLE 4. Let G be a group of order p^m such that $|G/Z(G)| = p^3$. If $g \in G$, then $Z(G)\langle g\rangle \leqslant C_G(g)$, hence $|\mathrm{Cl}_G(g)| \leqslant p^2$. By Vaughan-lee's Theorem (cf. [7] pp. 341) it follows $|G'| \leqslant p^3$; our Corollary yields also the above result. In effect, we have $r(G) = p^{m-2} + (p^2 - 1)$ $p^{-2} \cdot |G/G'| \geqslant p^{m-2} + p^{m-5}(p^2 - 1)$, hence $|G/G'| \geqslant p^{m-3}$.

PROPOSITION. If G is a p-group, then $r(G) > \log_2(|G|^{(p+1)/2})$.

PROOF. Set $|G| = p^m = p^{2n+e}$ with $e = 0$ or 1. By the Remark we have

$$r(G) \geqslant p^e + (p^2 - 1)(m - e) \cdot 2^{-1} . \tag{3}$$

The desired inequality now follows from (3) if we argue by induction on m to prove that

$$p^e + (p^2 - 1)(m - e) \cdot 2^{-1} \geqslant 2^{-1} \cdot (p + 1) m \cdot \log_2 p .$$

Let G be a group of order p^m. We define

$$a_i = \left|\{Cl_G(g) \colon |Cl_G(g)| = p^i\}\right| \, 1 \leqslant i \leqslant m - 2 ,$$

$$r_0 = \sum_{1 \leqslant 2k \leqslant m-2} a_{2k} \text{ and } r_1 = \sum_{1 \leqslant 2k-1 \leqslant m-2} a_{2k-1} .$$

Finally we obtain:

PROPOSITION. Let G be a p-group, then G satisfies the following relations:

1) $r(G) = |Z(G)| + r_0 + r_1$.

2) $|G| - |Z(G)| = r_0 + r_1 \cdot p + k'(p^2 - 1)(p - 1)$ for some number integer $k' \geqslant 0$.

3) $a_i \equiv 0 \pmod{p-1}$ for every i.

4) $r_1 \equiv 0 \pmod{p^2-1}$.

PROOF. We have $|G| = |Z(G)| = \sum_{i=1}^{m-2} a_i p^i$ and $r(G) = |Z(G)| + r_0 + r_1$. On he other hand,

$$a_{2k}p^{2k} \equiv a_{2k}\big(1 + k(p^2-1)\big) \ \big(\mathrm{mod}\ (p^2-1)(p-1)\big)$$

and

$$a_{2k-1}p^{2k-1} = a_{2(k-1)+1}p^{2(k-1)+1} \equiv a_{2k-1}\big(p + (k-1)(p^2-1)\big)$$

module $(p^2-1)(p-1)$. Hence there is a number integer $k'' \geqslant 0$ such that

$$(4) \qquad |G| = r(G) + \sum_{1 \leqslant k \leqslant (m/2)-1} \Big(a_{2k}k(p^2-1) + a_{2k-1}\big(p - 1 + (k-1)(p^2-1)\big)\Big) + k''(p^2-1)(p-1)\,.$$

Arguing as in the Lemma, we deduce that $a_i \equiv 0 \pmod{p-1}$ for each i (considering $T_i = \{g \in G\colon |\mathrm{Cl}_G(g)| = p^i\}$), we have $|T_i| \equiv 0 \pmod{p-1}$ and $|T_i| \equiv a_i \ \big(\mathrm{mod}\,(p-1)\big)$, and consequently we have $|G| = |Z(G)| + r_0 + r_1 p + k'(p^2-1)(p-1)$ for some number integer $k' \geqslant 0$. Finally (4) yields $r_1 \equiv 0 \pmod{p^2-1}$.

EXAMPLES.

1) If G is a non-abelian group of order p^2, then $\big(|Z(G)|, a_1\big) = (p, p^2 - 1)$.

2) Let G be a non-abelian group of order p^4. Then $\big(|Z(G)|, a_1, a_2\big) = \big(p^2, p(p^2-1), 0\big)$ or $\big(p, p^2-1, p(p-1)\big)$.

REFERENCES

[1] E. A. BERTRAM, *A density Theorem on the number of conjugacy classes in finite groups*, Pacific J. Math., **55** (1974), pp. 329-333.

[2] P. ERDÖS - P. TURAN, *On some problems of a statistical group-theory, IV*, Acta Math. Acad. Sci. Hung., **19** (1968), pp. 413-435.

[3] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly, **80** (1973), pp. 1031-1034.
[4] M. Hall - J. Senior, *The groups of order* 2^n, $n \leqslant 6$, MacMillan Co., New York, 1964.
[5] P. Hall, *The Eulerian functions of a group*, Quart. J. Math., **7** (1936), pp. 134-151.
[6] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.
[7] B. Huppert - N. Blackburn, *Finite groups II*, Springer-Verlag, Berlin, New York, 1982.
[8] N. Ito, *On finite groups with given conjugate types I*, Nagoya Math. J., **6** (1953), pp. 17-28.
[9] A. Mann, *Conjugacy classes in finite groups*, Israel J. Math., **31**, No. 1, (1978), pp. 78-84.
[10] J. Poland, *Two problems of finite groups with k conjugate classes*, J. Austral. Math. Soc., **8** (1968), pp. 49-55.
[11] J. Rebmann, *F-gruppen*, Arch. Math., **22** (1971), pp. 225-230.
[12] E. Rodemich, *The groups of order* 128, J. Algebra, **67** (1980), pp. 129-142.
[13] G. Sherman, *A lower bound for the number of conjugacy classes in a finite nilpotent group*, Pacific J. Math., **80**, No. 1 (1979), pp. 253-254.
[14] M. Suzuki, *Group Theory I*, Springer Verlag, Berlin, New York, 1982.
[15] A. Vera, *Conjugacy classes in finite solvable groups*, to appear in Israel J. Math.

Manoscritto pervenuto in redazione il 4 aprile 1984.