

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

ROLF BRANDL

LIBERO VERARDI

Finite groups with few conjugacy classes of subgroups

Rendiconti del Seminario Matematico della Università di Padova,
tome 87 (1992), p. 267-280

[<http://www.numdam.org/item?id=RSMUP_1992__87__267_0>](http://www.numdam.org/item?id=RSMUP_1992__87__267_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1992, 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/>

Finite Groups with Few Conjugacy Classes of Subgroups.

ROLF BRANDL - LIBERO VERARDI(*)

Introduction.

Let $(X, \leq)$ be a finite partially ordered set (poset). A subset A of X is called an *antichain* if no two distinct elements of A are comparable with respect to the order of X . Thus if $x, y \in A$ and $x \leq y$ then $x = y$. Such a subset intersects every chain of X in one element at most. The Dilworth number $D(X)$ is a nonnegative integer defined to be the maximum taken over all cardinalities of antichains in X . As we will consider finite posets, $D(X)$ is a positive integer.

In this note we consider the poset $C(G)$ of all conjugacy classes of subgroups of a finite group G . If H is a subgroup of G , the set $\{H^g \mid g \in G\}$ will be denoted by $[H]$. Thus $C(G) = \{[H] \mid H \leq G\}$. The ordering in $C(G)$ is defined by setting $[H] \leq [K]$ if H is contained in some conjugate of K . It is clear that $C(G)$ is a poset; however, in general, $C(G)$ need not be a lattice.

DEFINITION. The Dilworth number $D(C(G))$ of the poset $C(G)$ will be denoted by $w_{C(G)}(G)$. If it is clear which poset is meant, we shall write $w_C(G)$.

It is easy to see that $w_C(G) = 1$ implies that G is a cyclic p -group for some prime p , and, in general, groups G with $w_C(G) \leq n$ for a fixed n , seem to have a rather restricted structure. For example, in [1] it was shown that although all 2-groups G of maximal class satisfy $w_C(G) = 3$, for every $n \geq 4$ there are only finitely many p -groups G with $w_C(G) =$

(*) Indirizzo degli AA.: R. BRANDL: Mathematisches Institut, Am Hubland 12, D-8700 Würzburg; L. VERARDI, Dipartimento di Matematica, Piazza di Porta San Donato 5, 40127 Bologna, Italy.

Research supported by GNSAGA-CNR and MURST of Italy.

$= n$. This may be compared with a similar result of Landau (see [6]) on groups with a given number of conjugacy classes of elements.

Here, we are interested in arbitrary finite groups G . Clearly, the set of conjugacy classes of Sylow subgroups for all primes forms an antichain in $C(G)$, and hence we have $w_C(G) \geq |\Pi(G)|$, where $\Pi(G)$ denotes the set of all primes dividing the order of G . In this paper we give a characterization of groups for which the aforementioned inequality becomes an equality.

During the proofs, we frequently need to consider the poset of the conjugacy classes of subgroups of G contained in a fixed subgroup H of G . The corresponding Dilworth number will be denoted by $w_{C(G)}(H)$. Thus $w_{C(G)}(G) = w_C(G)$. The case when H is a Sylow p -subgroup is crucial and we determine the possibilities when $w_{C(G)}(H) = 1$ (see Theorem 3). This may be of interest in the theory of defect groups in modular representation theory.

Results.

First we give some simple upper bounds for $w_C(G)$. Let $\mathfrak{A}$ be any antichain in $C(G)$, let $\nu(\mathfrak{A})$ be the maximal number of subgroups of G such that no one of them is isomorphic to a subgroup of any other and whose conjugacy classes are belonging to $\mathfrak{A}$. Let then $\nu(G) = \max\{\nu(\mathfrak{A}) \mid \mathfrak{A} \text{ antichain of } C(G)\}$. The following is obvious:

LEMMA 1. Let G be a finite group. We have:

- a) $w_C(G) \geq |\Pi(G)|$.
- b) If $H \triangleleft G$ then $w_C(G) \geq w_{C(G/H)}(G/H)$.
- c) If H is a nontrivial complemented normal subgroup of G , then $w_C(G) \geq w_{C(G/H)}(G/H) + w_{C(G)}(H)$.
- d) For every subgroup M and for every quotient G/H of G we have $w_C(G) \geq \nu(M)$ and $w_C(G) \geq \nu(G/H)$.

COROLLARY 2. Let G be a finite soluble group and let $f(G)$ be the Fitting length of G . Then $f(G) \leq w_C(G)$.

PROOF. By induction on $f(G)$. The result is true if G is nilpotent. Since $F(G)/\Phi(G)$ is complemented in $G/\Phi(G)$, we have:

$$\begin{aligned} w_C(G) &\geq w_{C(G/\Phi(G))}(G/\Phi(G)) \geq \\ &\geq w_{C(G/F(G))}(G/F(G)) + w_{C(G/\Phi(G))}(F(G)/\Phi(G)) \geq f(G/F(G)) + 1 = f(G). \end{aligned}$$

Our aim is now the classification of groups G such that $w_G(G) = |\Pi(G)|$. Before answering this question, we examine the case of a group G containing a Sylow subgroup P such that $w_{C(G)}(P) = 1$, by classifying these subgroups P and showing their existence by examples.

THEOREM 3. Let G be a finite group and P a Sylow p -subgroup of G such that $w_{C(G)}(P) = 1$. Then one of the following holds:

- 1) P is cyclic.
- 2) P is a quaternion group of order 8.
- 3) P is elementary abelian of order $p^2, p^3, 2^5$.
- 4) G is not p -soluble and P is extraspecial of order p^3 and exponent p .

PROOF. Certainly the subgroups of P of the same order must be isomorphic. If $\exp P \geq p^2$ then the subgroups of order p^2 are cyclic, therefore by [5], p. 311, we have that P is cyclic or generalized quaternion. But in the last case, if $|P| > 8$ then P would have two nonisomorphic subgroups of order 8, the first one being cyclic and the other one isomorphic to Q_8 , so $|P| = 8$.

If $\exp P = p$ and if P is elementary abelian of order p^n , then two subgroups of P are conjugate in G if and only if they are conjugate in $N_G(P)$ ([5], pag. 418, Lemma 2.5 (a theorem of Burnside)), so we may assume that P is normal in G . Then for every k , our group G acts transitively on the subgroups of order p^k of P . Therefore if $n > 3$, a theorem of Cameron & Kantor (see [2]) yields that, if p is odd, G/P contains $SL(n, p)$ and, if $p = 2$, then $|P| = 2^4$ and G/P is isomorphic to A_7 , or $|P| = 2^5$ and G/P is isomorphic to $\Gamma L(1, 2^5)$. But p divides $|SL(n, p)|$ and 2 divides $|A_7|$, so that in these two cases, P is not a Sylow p -subgroup of G . Thus $|P| = p^2, p^3$ or 2^5 .

Finally, if P is nonabelian of exponent p , then P contains a subgroup, which is extraspecial of order p^3 (to see this, let $x \in Z_2(P) \setminus Z(P)$ and $y \in P$ such that $[x, y] \neq 1$. Then $\langle x, y \rangle$ has the property, since $[[x, y], x] = [[x, y], y] = x^p = y^p = [x, y]^p = 1$). It follows that the maximal order of an abelian normal subgroup of P is p^2 . Let A be one of them. Then $|\text{Aut}(A)| = p(p-1)^2(p+1)$ and $A = C_P(A)$ and hence it follows that P/A has order p at most, therefore $|P| = p^3$. But in this case there cannot exist a normal subgroup H in G whose Sylow p -subgroup is nontrivial and has order $< p^3$, because otherwise P would contain at least two conjugacy classes of subgroups of order p . Thus G is not p -soluble.

EXAMPLES. In Case 2) we have for example $G = SL(2, 3)$.

In Case 3), when $|P| = p^k$, $k = 2, 3$, we can choose the semi-direct product of the additive group by the multiplicative group of the field $GF(p^k)$; if $|P| = 2^5$ we can take the relative holomorph of P by $\Gamma L(1, 2^5)$.

Finally, in Case 4), for $p = 5$, there is the Thompson simple group G , whose Sylow 5-subgroups are of the required type (see [7]). Moreover, we show that all subgroups of order 5 (respectively 25) are conjugate. Using the notation of [7], let z be an involution of G , $H = C_G(z)$, $b \in H$, $|b| = 5$, $B = \langle b \rangle$. Then by [7], (5.2), $P = O_5(C_G(b))$ is a Sylow 5-subgroup of G , $B = Z(P)$, and P is normal in $N_G(B)$. Moreover, G contains one class of elements of order 5 and an element $b_1 \in P \setminus B$ has 120 conjugates in P under the action of $N_G(B)$. Thus all subgroups of order 5 and 25 of P are conjugate in G and we have $w_{C(G)}(P) = 1$.

Returning to our classification, we observe that if $w_C(G) = |\Pi(G)|$, $p \in \Pi(G)$ and P is a Sylow p -subgroup of G then $w_{C(G)}(P) = 1$, so P is as in Theorem 3. Moreover, we have:

LEMMA 4. If G is a finite group such that $w_C(G) = |\Pi(G)|$ then:

- a) if $M \leq G$ then $\nu(M) \leq |\Pi(M)|$.
- b) If H is a proper normal soluble subgroup of G , then $w_{C(G/H)}(G/H) = |\Pi(G/H)|$.
- c) If $1 \neq H \triangleleft G$ and p is a prime divisor of both $|H|$ and $[G:H]$, then the Sylow p -subgroups of G are cyclic or quaternion groups.

PROOF. a) If $\nu(M) > |\Pi(M)|$, then

$$w_C(G) \geq \nu(M) + |\Pi(G) \setminus \Pi(M)| > |\Pi(G)|.$$

b) Let $H \triangleleft G$. First assume that H has a complement M in G : if $\mathcal{A}$ is any antichain of G/H with $m = w_{C(G/H)}(G/H)$ elements and $K_1, \dots, K_m$ are subgroups of M such that $[HK_i/H] \in \mathcal{A}$, then these subgroups are not conjugate in G . Let Π' be the set of all prime divisors of $|G|$ that are not divisors of $|G/H|$ and let $n = |\Pi'|$. For every $p_i \in \Pi'$ we consider a Sylow p_i -subgroup S_i of G . Then the set $\{[K_1], \dots, [K_m], [S_1], \dots, [S_n]\}$ is an antichain of $C(G)$, therefore in this case the assertion follows from:

$$w_C(G) \geq m + n = w_{C(G/H)}(G/H) + n \geq |\Pi(G/H)| + n = |\Pi(G)| = w_C(G).$$

Now assume that H is contained in $\Phi(G)$. Then:

$$|\Pi(G)| = |\Pi(G/H)| \leq w_{C(G/H)}(G/H) \leq w_C(G) = |\Pi(G)|,$$

and the assertion follows also in this case. Finally, let H be soluble and let P be a minimal normal subgroup of G contained in H . Then $P \leq \Phi(G)$ or P has a complement in G , therefore in every case $w_{C(G/P)} = |\Pi(G/P)|$. So the assertion follows by induction.

c) Let P be a Sylow p -subgroup of G . From $w_{C(G)}(P) = 1$ it follows that $P \cap H$ is the only subgroup of P of its order. Thus P is cyclic or a quaternion group.

Now we distinguish two subcases: G soluble and G non-soluble. Let $O(G)$ and $O'(G)$ be respectively the maximal normal subgroup of odd order and the minimal normal subgroup with odd quotient. For the non-soluble case, we need the following:

LEMMA 5. Let G be a finite group such that $w_C(G) = |\Pi(G)|$. Then:

a) If $G/O(G)$ is isomorphic to $PSL(2, 5)$ or to $SL(2, 5)$ then $O(G) = 1$.

b) If G contains a normal subgroup K isomorphic to $PSL(2, 5)$ then $K = G$.

PROOF. a) Let $G/O(G) \cong PSL(2, 5)$. As $O(G)$ is soluble, it has a subgroup H normal in G whose index in $O(G)$ is a power of an odd prime p . First let $p = 3$ or $p = 5$. The Sylow p -subgroups of G/H are cyclic, by Lemma 4c) so $C_{G/H}(O(G)/H)$ contains the Sylow p -subgroups of G/H , therefore it is equal to G/H . Thus $O(G)/H$ is in the center of G/H , but then for $p = 3$ and $p = 5$ respectively, G/H contains subgroups of order 4, 9, 5 and 6 and of order 4, 3, 25, 10, against Lemma 4. If $p > 5$ then p does not divide $|PSL(2, 5)|$. So $O(G)/H$ is the Sylow p -subgroup of G/H , and it must have order p , p^2 or p^3 . Trivially we do not have $PSL(2, 5)H/H \triangleleft G/H$, because otherwise G would contain subgroups of order $2p$, $3p$, $5p$, 4, 10, 6; a contradiction. It is well known that, in characteristic $p > 5$, $PSL(2, 5)$ has no faithful representations of degree < 3 , therefore $|O(G)/H| = p^3$. Then there are $p^2 + p + 1$ subgroups of order p , so if $x \in G/H$, $x^2 = 1$, then x must fix at least one of them. Thus in G/H there is also a subgroup of order $2p$, so $w_{C(G/H)}(G/H) \geq 5$, while $|\Pi(G/H)| = 4$, against Lemma 4. Thus $O(G) = 1$. We can use the same argument if $G/O(G)$ is isomorphic to $SL(2, 5)$.

b) Recall that $\text{Aut}(PSL(2, 5)) \cong \text{Aut}(A_5) \cong S_5$. Let p be a prime divisor of $|G/K|$. If $p = 2$ then G would contain the dihedral group of

order 8, against Lemma 2, or there would be an involution out of K , so in every case $w_C(G) \geq |\Pi(G)| + 1$. If p were odd, let $M \leq G$ such that $|M/K| = p$. If $p = 3$ then M would contain subgroups of order 4, 6, 10, 9, so in every case $v(M) > 3 = |\Pi(M)|$, against Lemma 4a). The same argument works if $p = 5$. Finally, if $p > 5$, we would have $M = PSL(2, 5) \times P$, with $|P| = p$ and $v(M) = 6 > 4 = |\Pi(M)|$, against Lemma 4a) again. Thus $K = G$.

THEOREM 6. Let G be a non-soluble group. Then $w_C(G) = |\Pi(G)|$ if and only if G is isomorphic to $PSL(2, 5)$ or to $SL(2, 5)$.

PROOF. If G is isomorphic to $PSL(2, 5)$ or $SL(2, 5)$, the direct examination of the poset of conjugacy classes of subgroups shows that $w_C(G) = 3 = |\Pi(G)|$. We prove that these two groups are the only non-soluble groups with this property. So let G be a non-soluble group such that $w_C(G) = |\Pi(G)|$. Then $|G|$ is even, so let P be a Sylow 2-subgroup of G . We know that $w_{C(G)}(P) = 1$. As P is not cyclic, we have the following two cases:

I) P is elementary abelian. Here Walter's theorem (see [8]) tell us that the group $R = O'(G/O(G))$ is isomorphic to the direct product $A \times S_1 \times \dots \times S_t$, where A is abelian and the S_i are isomorphic to the first Janko group J_1 , or to a group $PSL(2, 2^k)$, or to $PSL(2, q)$, q an odd prime, or to a Ree group. But the Sylow 3-subgroups of the Ree groups are nilpotent of class three (see [9]), against Theorem 3. Moreover, there are 7 isomorphism classes of maximal subgroups in J_1 ([3], p. 36), so $w_C(J_1) \geq 7 > 6 = |\Pi(J_1)|$ eliminates J_1 . Since the involutions of G must be all conjugate, $A \triangleleft G/O(G)$ implies $A = 1$. The direct product $K = S_1 \times \dots \times S_t$ contains t classes of involutions that are not conjugate because their centralizers form a chain: let $x_i \in S_i$, $o(x_i) = 2$ and let $e_i = x_1 x_2 \dots x_i$; if $C_i = C_{S_i}(x_i)$, we have $C_K(e_i) = C_1 \times C_2 \times \dots \times C_i \times S_{i+1} \times \dots \times S_t$. Thus if $t > 1$ the subgroups $\langle e_1 \rangle, \dots, \langle e_t \rangle$ cannot be conjugate in $G/O(G)$, so $t = 1$ and therefore R is isomorphic to $PSL(2, 2^k)$ or to $PSL(2, q)$, where q is an odd prime. In the first case, we have $|P| = 2^k$, then $|N_G(P)/C_G(P)| = 2^k - 1$ (see [5], p. 191). Now, P is elementary abelian of order 2^k , so it has $((2^k - 1)(2^k - 2))/6$ subgroups of order 2^2 , that must be conjugate in G , so in $N_G(P)$. This implies $((2^k - 1)(2^k - 2))/6 \leq 2^k - 1$, i.e. $k \leq 3$. Then R is isomorphic to $PSL(2, 4)$ ($\cong PSL(2, 5)$) or to $PSL(2, 8)$. The last group however contains subgroups of order 9, 4, 6, 7, so $v(PSL(2, 8)) > |\Pi(PSL(2, 8))|$, against Lemma 4. Now let R be isomorphic to $PSL(2, q)$. Then it contains cyclic subgroups of order $(q + 1)/2$ and $(q - 1)/2$, dihedral subgroups of order $2r$ for every odd prime $r \in \Pi(R)$ and the Sylow 2-subgroups, which contain elementary abelian subgroups of order 4. Thus $v(R) > |\Pi(R)|$ un-

less one of the numbers $(q+1)/2$ and $(q-1)/2$ is odd and the other one is 2. This is possible only for $q=3$ or $q=5$, but $PSL(2,3)$ is soluble, so $R \cong PSL(2,5)$. By Lemma 5 we have $G \cong PSL(2,5)$.

II) $P \cong Q_8$. In this case, Glauberman's Z^* -theorem (see [4]) implies that the centre of the group $G/O(G)$ has even order. Let $T \leq G$ be such that $Z(G/O(G)) = T/O(G)$. Then $w_{C(G/T)}(G/T) = |\Pi(G/T)|$, by Lemma 4. As the Sylow 2-subgroup of G/T is elementary abelian, by I) we have $O'((G/T)/O(G/T)) \cong PSL(2,5)$. By Lemma 5, we have $G/T \cong PSL(2,5)$, and then $G/O(G) \cong SL(2,5)$. Again by Lemma 5 we must have $O(G) = 1$. This concludes the proof.

Now we examine the case when G is soluble. Certainly, we have $m = w_C(G) = |\Pi(G)| \leq 3$, because the conjugacy classes of Hall subgroups whose order is a multiple of two distinct prime powers form an antichain of $\binom{m}{2}$ elements.

The case $m=1$ is trivially that of cyclic p -groups. We examine now the case $m=2$. Let G be a soluble group such that $w_C(G) = 2$. Then G is not a p -group, since a non-cyclic p -group has three maximal normal subgroups at least. Therefore $|G| = p^a q^b$ and G is soluble, $f(G) \leq 2$ by Lemma 2 and its Sylow subgroups must be as in Theorem 3, (except for the case 4). Moreover, we have:

LEMMA 7. Let $w_C(G) = 2$. Then:

- a) If G is nilpotent then it is cyclic of order $p^a q$.
- b) $G/F(G)$ is cyclic.

PROOF. a) In this case the maximal subgroups of a Sylow subgroup P of G are normal in G , therefore P must contain just one maximal subgroup and hence it is cyclic. Thus G is cyclic too. If $|G| = p^a q^b$ with $a, b > 1$ then G would have subgroups of order p^2 , q^2 and pq , therefore $w_C(G) \geq 3$. Now b) follows from a) and Corollary 2.

The Fitting subgroup of G can be a p -group or not. We first examine the case when $F(G)$ is not a p -group. We have:

PROPOSITION 8. Let $w_C(G) = 2$, and assume that G is non-nilpotent and $F(G)$ is not a p -group. Then $|G| = p^n q$ where $q \equiv 1 \pmod{p}$ and the Sylow p -subgroups are cyclic. Moreover $|G'| = q$ and G has the following presentation:

$$G = \langle a, b \mid a^q = b^{p^n} = 1, \quad b^{-1}ab = a^r, \quad 1 < r < q, \quad r^{p^k} \equiv 1 \pmod{q} \rangle$$

for some k .

If h is the minimal integer such that $r^{p^h} \equiv 1 \pmod{q}$ then $Z(G) = \Phi(G)$ is a p -subgroup of order p^{n-h} . Also, $F(G) = \Phi(G) \times G'$.

PROOF. Since $F(G)$ is not a p -group, we have $F(G) = P \times Q$, where P and Q are normal in G . One of them must have prime order, because otherwise G would have subgroups of order p^2, q^2, pq and then $w_c(G) \geq 3$. Let us assume that $|Q| = q$. The same argument shows that G must have order $p^n q$, Q is the Sylow q -subgroup and is normal in G . Thus Q is not contained in $\Phi(G)$. Therefore $\Phi(G) \leq P$. Let S be a Sylow p -subgroup of G . Since G is non-nilpotent then $P \neq S$; being $P < G$, P is unique in its order in G and being $G/F(G)$ cyclic, then S/P is cyclic and S is cyclic too, by Theorem 3. This implies that G is supersoluble. Clearly, G is noncyclic, and so we must have $q > p$ and $q \equiv 1 \pmod{p}$. Certainly $P = Z(G) = \Phi(G)$ and moreover $G' = Q$. This concludes the proof.

When $F(G)$ is a p -group there are some more cases. We have in fact:

PROPOSITION 9. Let $w_c(G) = 2$ and assume that G is non-nilpotent and $F(G)$ is a p -subgroup. Then $F(G)$ is the Sylow p -subgroup of G . Moreover:

a) If $F(G)$ is a quaternion group, then G is isomorphic to $SL(2, 3)$.

b) If $F(G)$ is cyclic then $|G| = p^a q$ with $p \equiv 1 \pmod{q}$ or $|G| = pq^b$, where q^b is a divisor of $p - 1$.

c) If $F(G)$ is elementary abelian, its order must be 4 (and then G is isomorphic to A_4) or p^3 and in this case $|G| = p^3 q^b$, with $q^b = p^2 + p + 1$.

PROOF. Since $F(G)$ is a normal p -subgroup and $G/F(G)$ is cyclic, we have $G' \leq F(G)$, so the Sylow p -subgroup of G is normal in G and therefore coincides with $F(G)$. Let Q be a Sylow q -subgroup of G . Then Q is isomorphic to $G/F(G)$, it is cyclic and it acts transitively on the subgroups of the same order in $F(G)$. So:

a) If $F(G)$ is a quaternion group, $\text{Aut } F(G) \cong S_4$ implies that we must have $q = 3$ and $|Q| = 3$, therefore G is isomorphic to $SL(2, 3)$.

b) If $F(G)$ is cyclic and $|F(G)| = p^a$ with $a > 1$ then $|Q| = q$, because otherwise G would have subgroups of order p^2, pq, q^2 . If $|F(G)| = p$ then q^b must divide $p - 1$, since no q -element can centralize $F(G)$.

c) Let $F(G)$ be elementary abelian. First of all $|F(G)| \neq 2^5$, since in this case the order of $G/F(G)$ would be a multiple of $31 \cdot 5$, as $G/F(G)$ must act transitively on subgroups of order 2 and 4 respectively. If $|G| = p^2$ then $F(G)$ contains $p + 1$ subgroups of order p , on which Q must act transitively. Then $p + 1 = q^n$. If $p > 2$, we must have $q = 2$, so $n \geq 2$ but since every element of order 2 of $GL(2, p)$ fixes at least one subgroup of order p , G contains one subgroup of order p^2 , one of order 4 and a dihedral one of order $2p$, a contradiction. Thus $p = 2$ and then G is isomorphic to A_4 . Instead if $|F(G)| = p^3$ then Q must have order q^b and must act transitively on $p^2 + p + 1$ subgroups of order p . Thus $q^b = p^2 + p + 1$. This is possible for example, for $b = 1$, if $p = 2$ and $q = 7$, or $p = 3$ and $q = 13$.

Concerning the last case of the previous proposition, we have:

PROPOSITION 10. Let $G = [V]C$, with $|V| = p^3$, $|C| = q^n$, V elementary abelian, C cyclic, and $1 + p + p^2 = q^n$. If $Z(G) = 1$ then $w_C(G) = 2$.

PROOF. Let us consider the equation $1 + p + p^2 = q^n$, with p, q primes. If $n = 1$, as known, there are some solutions: $(p, q) = (2, 7), (3, 13), (5, 31), \dots$. We have:

a) n is odd. In fact the equation $x^2 + x + (1 - q^n) = 0$ has discriminant $4q^n - 3$ and it must be a square d^2 in $\mathbb{Z}$, therefore if $n = 2m$ then $(2q^m)^2 - d^2 = 3$, so $d = 1$ and $q = 1$, a contradiction.

b) $q \neq 3$. In fact if $q = 3$ then $p^2 + p + 1 \equiv 0 \pmod{3}$, so $p \equiv 1 \pmod{3}$, i.e. $p = 3r + 1$. But then $9r^2 + 6r + 1 + 3r + 1 + 1 = 3(3r^2 + 3r + 1) = 3^{2m+1}$ and 3 would divide $3r^2 + 3r + 1$.

c) If an element y of order q fixes a subgroup P of order p of V then $Z(G) \neq 1$. In fact let's suppose first that y does not centralize P . Then q divides $p - 1$, so q divides also $3p = 1 + p + p^2 - (p - 1)^2$. Thus $q = 3$, a contradiction by b). Therefore y centralizes P . Moreover by Maschke's theorem there is a complement W in V which is fixed by y . Since W contains $p + 1$ subgroups of order p , the same argument shows that W is centralized by y . Then $[y, V] = 1$ and $y \in Z(G)$.

d) If G is as before and $Z(G) = 1$ then $w_C(G) = 2$. In fact an element u of order q^n must permute cyclically the subgroups of order p of V : otherwise $N_G(P)$, where $|P| = p$, would be greater than V , so at least one element y of order q would fix P and belong to $Z(G)$. Likewise u permutes cyclically the subgroups of order p^2 . So we have that in $C(G)$ there are only two maximal chains: $[G], [\langle u \rangle], [\langle u^q \rangle], \dots, [1]$ and $[G], [V, \langle u^q \rangle], \dots, [V], [W], [P], [1]$, where $|W| = p^2$; thus $w_C(G) = 2$.

REMARK. If $n > 1$ then $q \equiv 1 \pmod{3}$ and $p \equiv 2 \pmod{3}$. In fact from $4q^{2m+1} - 3 = d^2$ it follows $q^{2m+1} \equiv 1 \pmod{3}$, as $q \neq 3$, so $q \equiv 1 \pmod{3}$. Next, from $1 + p + p^2 = q^{2m+1}$ it follows $p(p+1) \equiv 0 \pmod{3}$, thus if $p = 3$ then $q = 13$ and $n = 1$: otherwise $p \equiv 3 \pmod{3}$.

Now let $w_C(G) = |\Pi(G)| = 3$, let G be soluble and $|G| = p^a q^b r^c$. We distinguish three cases depending on $|\Pi(F(G))|$. First of all, we need the following lemma:

LEMMA 11. Let $w_C(G) = |\Pi(G)| = 3$ and let G be soluble. Then:

- a) G contains no proper subgroup H such that $|\Pi(H)| = 3$.
- b) All the minimal normal subgroups of G are Sylow subgroups, and just one of them can have order not a prime.
- c) If the Sylow p -subgroup is normal in G , $a > 1$ and there is a subgroup of order pq then there is none of order $p^h r$, $0 < h < a$.

PROOF. a) Let $0 < h < a$ and let $|H| = p^h q^k r^m$: then G contains subgroups of order p^a , $p^h q^k$, $p^h r^m$, $q^k r^m$, a contradiction.

b) If P is a minimal normal subgroup, $|P| = p^h$ with $0 < h < a$, then G would contain subgroups of order p^a , $p^h q$, $p^h r$, $q^b r^c$, a contradiction. If the Sylow q -subgroup Q also is normal in G and $a, b > 1$ then G would contain subgroups of order $p^a q$, $p^a r$, $q^b r$, pq^b , another contradiction. Likewise we can prove the last assertion.

COROLLARY 12. Let G be soluble. Then $w_C(G) = |\Pi(G)| = 3$ and $|\Pi(F(G))| = 3$ if and only if $|G| = pqr$ and G is cyclic.

PROPOSITION 13. Let G be soluble. Then $w_C(G) = |\Pi(G)| = 3$ and $|\Pi(F(G))| = 2$ if and only if G is one of the following types:

- a) $G = [\mathbb{Z}_p \times \mathbb{Z}_q] \mathbb{Z}_r$.
- b) $G = [(\mathbb{Z}_2)^2 \times \mathbb{Z}_q] \mathbb{Z}_3$ and the 2-Sylow subgroup is a minimal normal subgroup of G . (Thus G has a subgroup isomorphic to A_4).
- c) $G = [(\mathbb{Z}_p)^3 \times \mathbb{Z}_q] \mathbb{Z}_r$ and the Sylow p -subgroup is a minimal normal subgroup. (Thus $p^2 + p + 1 = r$ and G has no subgroups of order pr or $p^2 r$).

PROOF. Let $w_C(G) = |\Pi(G)| = 3$ and let $|F(G)| = p^h q^k$, where $h, k > 0$. By Lemma 11 we have $h = a$, $k = b = c = 1$, the Sylow p -subgroup P of G is a minimal normal subgroup of G and hence elementary abelian. If $a = 1$ we are in Case a). If $a = 2$ then the subgroups of order p must be all conjugate. Therefore $p + 1 = r$, which implies $p = 2$,

$r = 3$, and we are in Case b). Notice that there are no subgroups of order 6, therefore G contains a subgroup isomorphic to A_4 . If $a = 3$, we are in Case c). Also we must have $p^2 + p + 1 = r$ and there are no subgroups of order pr or p^2r . It is impossible that $p^a = 2^5$ because, as observed in Theorem 3, in this case $|G| = 32 \cdot 31 \cdot 5$, but $|F(G)| = 32$.

Conversely, a straightforward inspection of the poset $C(G)$ shows that if G is as in a), b), c) then $w_C(G) = |\Pi(G)| = 3$. Case a) is obvious. In Case b), since the Sylow 2-subgroup is a minimal normal subgroup, G cannot have subgroups of order 6. It has subgroups of orders 1, 2, 3, 4, 12, q , $2q$, $4q$, $3q$, $12q$, and for each of these orders the subgroups are conjugate in both cases of $A_4 \times \mathbb{Z}_q$ and when the q -Sylow subgroup is not central. In Case c), likewise, G cannot have subgroups of order pr or p^2r . It has subgroups of orders 1, p , p^2 , p^3 , q , pq , p^2q , p^3q , r , p^3r , qr ; subgroups of the same order are conjugate. Indeed, as G does not contain subgroups of order pr , an element of order r permutes cyclically the $r = p^2 + p + 1$ subgroups of order p and p^2 respectively, so it also acts transitively on the set of the (abelian) subgroups of order pq and p^2q respectively. The remaining subgroups are Hall subgroups.

We say that a group A acts fixed point freely (f.p.f.) on a vector space V if for every $1 \neq a \in A$ and $0 \neq v \in V$ we have $v^a \neq v$.

PROPOSITION 14. Let G be soluble. If $w_C(G) = |\Pi(G)| = 3$ and $|\Pi(F(G))| = 1$ then:

i) $F(G)$ is the Sylow p -subgroup of G and it is a minimal normal subgroup.

ii) $G/F(G)$ is cyclic and it acts f.p.f. on $F(G)$.

iii) $|G| = p^a qr$, with $a = 1$ or $a = 3$.

iv) If $a = 3$ then $p^2 + p + 1 = qr$, $(qr, 6) = 1$, or $p^2 + p + 1 = q$, $r|p - 1$, $r \neq 1$, and an element of order r induces a power automorphism on $F(G)$.

PROOF. Let $|G| = p^a q^b r^c$ and let Q be a Hall subgroup of order $q^b r^c$ of G .

i) Lemma 11 implies that $F(G)$ is a minimal normal subgroup of G , so it is elementary abelian, and $|F(G)| = p^a$.

ii) Since $F(G)$ is abelian, we have $C_G(F(G)) = F(G)$. We show that Q acts f.p.f. on $F(G)$. Let $x \in Q$ be of order q . If x would centralize an element y of order p then $a > 1$ (because otherwise $x \in F(G)$) and $C = C_{F(G)}(\langle x \rangle)$ is a proper subgroup of $F(G)$ and the subgroup $M\langle x \rangle$ would have no elements of order pq . Therefore G would have sub-

groups of order p^a , pq (cyclic), $|M|q$, $q^b r^c$, a contradiction. Likewise if x has order r or pq . Thus, Q acts f.p.f. on $F(G)$.

iii) First we show that $|Q| = qr$ and Q is cyclic. By [5], p. 502 and Theorem 3, for each odd prime dividing $|Q|$ the Sylow subgroup must be cyclic, while the Sylow 2-subgroup must be also cyclic or quaternion. In the first case Q is supersoluble and, if $q > r$, all of its q -subgroups are normal in Q . If $b > 1$ then G would have subgroups of order $p^a q$, $p^a r$, q^b , qr , a contradiction. Thus $b = 1$. A similar argument shows that $c = 1$. Therefore $|Q| = qr$ and by [5], p. 502, Q is cyclic. When $q = 2$ the same argument shows that the Sylow 2-subgroup of Q cannot be isomorphic to the quaternion group Q_8 .

Next, we cannot have $p^a = 2^5$, otherwise $|G| = 2^5 \cdot 31 \cdot 5$ and $F(G)$ would have 31 elements of order 2, so G would have an element of order 10.

By Theorem 3, $|F(G)| \leq p^3$. The subgroups of order p must form just one conjugacy class of G , so $G/F(G)$ must act transitively on them. Let $2 \leq a \leq 3$ and let g be of order qr , $x = g^q$ and $y = g^r$. First of all we need to consider the case when x fixes a nontrivial subgroup of $F(G)$. Then x fixes a subgroup of order p and has an eigenvalue $k \neq 0$ in $GF(p)$. Being $xy = yx$, the eigenspace P of k is also fixed by y . Therefore $P^y = P$, and because $P \triangleleft F(G)$, we have $P \triangleleft G$, so i) implies $P = F(G)$ and x must act as a power automorphism on $F(G)$. In this case the number of subgroups of order p must be q .

If $a = 2$, p must be odd (otherwise $\text{Aut}(F(G))$ would be noncyclic); then $p + 1$ is even, so we can assume $r = 2$ and $p + 1 = 2q$. But since an element of order 2 has always eigenvalues, by the previous argument we would also have $p + 1 = q$, a contradiction. Thus $a \neq 2$.

iv) If $a = 3$ then either $p^2 + p + 1 = qr$ or $p^2 + p + 1 = q$ and r divides $p - 1$. In the first case we have $r \neq 2, 3$. In fact, if $r = 3$ and $x = g^q$, as a basis of $F(G)$ one could choose three vectors u, v, w such that $u^x = v$, $v^x = w$, $w^x = u$, but then $(uvw)^x = (uvw)$, a contradiction, because x cannot fix any subgroup of order p . Similar arguments can be used for $r = 2$. So $(qr, 6) = 1$. In the second case, when $p^2 + p + 1 = q$ and r divides $p - 1$, we must have $r \neq 3$; in fact if $r = 3$ then $p = 3t + 1$, so $9t^2 + 9t + 3 = q$ and $3|q$, a contradiction.

PROPOSITION 15. Let G be a soluble group. Then $w_c(G) = 3 = |\Pi(G)|$ and $F(G)$ is a p -group if and only if:

- i) $|G| = p^a qr$, with $a = 1$ or $a = 3$;
- ii) $|F(G)| = p^a$ and $F(G)$ is elementary abelian;

iii) in the case $a = 3$ we have:

iiia) $p^2 + p + 1 = qr$, $(qr, 6) = 1$, $G/F(G)$ cyclic, or

iiib) $p^2 + p + 1 = q$, $r \mid p - 1$, and an element of order r acts on $F(G)$ as a power automorphism.

PROOF. The necessity follows by Proposition 14. If G satisfies i), ii), iii), the case $a = 1$ is obvious. Let $a = 3$, let x be of order q and let y be of order r . If $p^2 + p + 1 = q$, no p -subgroup P or order p can be fixed by x . In fact otherwise, since q does not divide $p - 1$, we would have $[P, x] = 1$, and on the other hand x would fix a complement W of P in $F(G)$ and permute its $p + 1$ onedimensional subspaces. But q neither divides $p + 1$ nor p , therefore x must fix at least two of them, so it would fix them pointwise. Therefore $[x, F(G)] = 1$, a contradiction. Thus $F(G)$ is a minimal normal subgroup, the subgroups of order p are all conjugate and also those of order p^2 . Moreover there are no subgroups of order $p^h q$, with $0 < h < a$. Since y induces a power automorphism on $F(G)$, then $xy = yx$, so $G/F(G)$ is cyclic. Thus the subgroups of order pr are all conjugate and also these of order $p^2 r$. Then $w_C(G) = 3$. In the case $p^2 + p + 1 = qr$, let g be of order qr and let $x = g^r$ and $y = g^q$. If x should fix some subgroup P of order p , then q would divide $p - 1$, so $q = 3$, a contradiction, or $[x, P] = 1$, so $[x, F(G)] = 1$ as before, another contradiction. Likewise, y fixes no subgroup of order p . Thus there are no subgroups of order $p^h q$ or $p^h r$, with $0 < h < 3$, $F(G)$ is a minimal normal subgroup, the subgroups of order p are all conjugate and also those of order p^2 . This implies $w_C(G) = 3$.

EXAMPLES. Let $p = 41$, let V be the elementary abelian p -group of order p^3 and let x and y be the automorphisms of V whose matrices are

$$\begin{bmatrix} 10 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 10 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

respectively. They commute and we have $x^5 = 1$, $y^{1723} = 1$. If G is the split extension of V with respect to $\langle xy \rangle$, it satisfies i), ii), iiib) of Proposition 15 and we have $w_C(G) = 3$.

One can construct a similar example, of even order, if $p = 3$, $q = 13$, $r = 2$.

We have an example of the other type, that satisfies iiia) of Proposition 15, if $p = 11$, $q = 29$, $r = 7$.

Acknowledgement. The first named author thanks the Dipartimento di Matematica dell'Università di Bologna for its warm and excellent hospitality during the time of writing this paper.

REFERENCES

- [1] R. BRANDL, *Conjugacy classes of subgroups in p -groups*, J. Austral. Math. Soc., to appear.
- [2] P. CAMERON - W. KANTOR, *2-transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra, **60** (1979), pp. 380-422.
- [3] J. H. CONWAY *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford (1985).
- [4] G. GLAUBERMAN, *Central elements of core-free groups*, J. Algebra, **4** (1966), pp. 403-420.
- [5] B. HUPPERT, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York (1967).
- [6] E. LANDAU, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante*, Math. Ann., **56** (1903), pp. 671-676.
- [7] D. PARROT, *On Thompson's simple group*, J. Algebra, **46** (1977), pp. 389-404.
- [8] J. WALTER, *The characterization of finite groups with abelian Sylow 2-subgroups*, Ann. Math., **89** (1969), pp. 405-514.
- [9] H. N. WARD, *On Ree's series of simple groups*, Trans. Amer. Math. Soc., **121** (1966), pp. 62-89.

Manoscritto pervenuto in redazione il 4 ottobre 1990 e, in forma revisionata, il 13 marzo 1991.