ISRAEL JOURNAL OF MATHEMATICS 122 (2001), 93–115

FINITE GROUPS IN WHICH p'-CLASSES HAVE q'-LENGTH

BY

SILVIO DOLFI*

Dipartimento di Matematica "U. Dini"
viale Morgagni 67/A, I-50134 Firenze, Italy
e-mail: dolfi@math.unifi.it

AND

MARIA SILVIA LUCIDO

Dipartimento di Matematica ed Informatica
Università di Udine, via delle Scienze 206, 33100 Udine, Italy
e-mail:lucido@dimi.uniud.it

ABSTRACT

If G is a finite group in which every element of p'–order centralizes a q-Sylow subgroup of G, where p and q are distinct primes, it is shown that $O^{q'}(G)$ is solvable, $l_q(G) \leq 1$ and $l_p(O^{q'}(G)) \leq 2$. Further, the structure of G is determined to some extent.

1. Introduction

Let p, q be prime numbers and G be a finite group. We call an element of G a **p'-element** if its order is not divisible by p and a conjugacy class of G a **p'-class** if it consists of p'-elements of G.

We say that G has the property $P(p,q)$ if every p'-element of G centralizes a q-Sylow subgroup of G. Equivalently, G has $P(p,q)$ if the prime q does not divide the length of any p'-class of G.

* Work partially supported by MURST research program "Teoria dei gruppi ed applicazioni".
Received March 14, 1999 and in revised form October 25, 1999

If $p = q$ the property $P(p,q)$ holds if and only if G has a q-Sylow subgroup as a direct factor [1, Lemma 1]. (Observe that, as one can easily prove, the prime q does not divide the length of *any* conjugacy class of G if and only if G has a central q-Sylow subgroup.)

In this paper we prove that, if $p \neq q$ and G has $P(p,q)$ then:

(a) $O^p(G)$ has a normal q-complement and abelian q-Sylow subgroups (Theorem 5). In particular, $l_q(G) \leq 1$.

(b) $O^{q'}(G)$ is solvable (Theorem 3: it uses, via Proposition 1, the Classification of Finite Simple Groups).

Write $\overline{G} = O^{q'}(G/O_p(G))$, then:

(c) $\overline{G}$ has abelian p-Sylow subgroups (Corollary 4). In particular, $l_p(O^{q'}(G)) \leq 2$.

(d) We determine the structure of $\overline{G}/\Phi(\overline{G})$: it is, up to factoring out central q-subgroups, either 1 or a subdirect product of suitable affine semilinear groups (Corollary 3 to Proposition 6). Further, we get some conditions on the primes p and q (Corollary 5).

Finally, Examples 1 and 2 show that it is not possible to control either the top section $G/O^{q'}(G)$ or the derived length of the Frattini subgroup $\Phi(G)$ in a group G that satisfies $P(p,q)$.

With a view to comparing conditions on lengths of conjugacy classes and character degrees (see [6, §§2,4]), we recall that a group G has the property $BP(p,q)$ if every irreducible p-Brauer character of G has q'-degree. It is proved in [12, Theorem 2.6] that if $BP(p,q)$ holds in G for $p \neq q$ and G is p-solvable, then:

(a) $l_q(G) \leq 2$ and the Sylow q-subgroups of G are metabelian;

(b) $O^{q'}(G)$ is solvable;

(c) $l_p(O^{q'}(G)) \leq 2$ if $(p,q) \neq (7,3)$ and $l_p(O^{q'}(G)) \leq 3$ in all cases.

We finally recall that $BP(p,p)$ holds in G if and only if G has a normal p-Sylow subgroup (see Theorem 2.33 of [15] for $p = 2$ and [14] for p odd).

2. Preliminaries

We denote by g^G the conjugacy class of the element g in G and by $|g^G|$ its length. We start with an easy remark:

LEMMA 1: *Let N be a normal subgroup of G. Then:*

(i) *if $g \in N$, $| g^N |$ divides $| g^G |$;*

(ii) *if $g \in G$, $| (Ng)^{G/N} |$ divides $| g^G |$.*

We collect some further observations in the following:

LEMMA 2:

(i) *$P(p,q)$ is inherited by normal subgroups, factor groups and hence by subnormal sections;*

(ii) *$P(p,q)$ holds in $G = G_1 \times G_2 \times \cdots \times G_n$ if and only if it holds in G_i for $i = 1, 2, \ldots, n$; in particular $P(p,q)$ is inherited by direct product with q'-groups, that is if G has $P(p,q)$ and N is a q'-group, then $G \times N$ has $P(p,q)$ as well.*

If we assume $p \neq q$, then we have:

(iii) *$P(p,q)$ is inherited by extensions by p-groups, that is if G has $P(p,q)$, N is a p-group and E is a group such that $N \trianglelefteq E$ and $E/N \simeq G$, then E has $P(p,q)$ as well;*

(iv) *if $O^p(G)$ satisfies $P(p,q)$, then also G does.*

Proof: (i) and (ii) follow immediately by Lemma 1. Consider now a p'-element x of E. By hypothesis, there exists a q-Sylow subgroup Q of E such that $QN/N \leq C_{E/N}(< xN >)$. Hence Q acts on $K =< x > N$ and $C_K(Q)N/N = C_{K/N}(Q) = K/N$. But K is p-solvable, thus $C_K(Q)$ contains a p'-Hall subgroup H of K and there exists $k \in K$ such that $H^k =< x >$. It follows that $Q^k \leq C_E(x)$ and (iii) is proved. To prove (iv), observe that a p'-element of G is in $O^p(G)$ and that G and $O^p(G)$ have the same q-Sylow subgroups. ∎

Let r be a prime, k a positive integer and $K = GF(r^k)$. We will use the following notation for subgroups of the semilinear group:

$$A\Gamma(r^k) = \left\{ \begin{pmatrix} x \\ ax^\sigma + b \end{pmatrix} : x, a, b \in K, a \neq 0, \sigma \in \mathrm{Gal}(K/GF(r)) \right\},$$

$$A\Gamma_0(r^k) = \left\{ \begin{pmatrix} x \\ ax + b \end{pmatrix} : x, a, b \in K, a \neq 0 \right\},$$

$$\Gamma(r^k) = \left\{ \begin{pmatrix} x \\ ax^\sigma \end{pmatrix} : x, a \in K, a \neq 0, \sigma \in \mathrm{Gal}(K/GF(r)) \right\},$$

$$\Gamma_0(r^k) = \left\{ \begin{pmatrix} x \\ ax \end{pmatrix} : x, a \in K, a \neq 0 \right\},$$

$$A(r^k) = \left\{ \begin{pmatrix} x \\ x + b \end{pmatrix} : x, b \in K \right\}.$$

Finally, in the following "group" will always mean "finite group".

3. Solubility of $O^{q'}(G)$

In this section we want to prove that if the group G satisfies $P(p,q)$, then $O^{q'}(G)$ is solvable. To do this, we first consider almost simple groups. G is an **almost simple** group if there exists a non-abelian simple group S such that $S \leq G \leq \mathrm{Aut}(S)$, where $\mathrm{Aut}(S)$ is the automorphism group of S. We prove that an almost simple group can satisfy $P(p,q)$ just in the trivial case $(q,|G|)=1$.

PROPOSITION 1: *If G is an almost simple group, G satisfies $P(p,q)$ if and only if $(q,|G|)=1$.*

We first prove the same property for finite simple non-abelian groups.

PROPOSITION 2: *Let G be a finite simple non-abelian group. Then G has $P(p,q)$ if and only if $(q,|G|)=1$.*

Observe that we can assume that p divides $|G|$, since for p'–groups $P(p,q)$ amounts to having a central q-Sylow subgroup (see for example [6, Theorem 5′]). We can also assume $p \neq q$, since otherwise G has a normal p-Sylow subgroup (Theorem 4).

We recall the definition of the **prime graph** $\Gamma(G)$ for a finite group G. The set of vertices of $\Gamma(G)$ is the set $\pi(G)$ of primes dividing the order of G and two vertices p, q are joined by an edge if there is an element in G of order pq.

We denote the set of all the connected components of the graph $\Gamma(G)$ by $\{\pi_i(G), \text{ for } i=1,2,\ldots,n(G)\}$ and, if the order of G is even, we denote by $\pi_1(G)$ the component containing 2.

We can now prove the following easy lemma:

LEMMA 3: *Let G be a group such that $n(G) \geq 3$; then G does not satisfy $P(p,q)$.*

Proof: Let $\pi_1(G)$, $\pi_2(G)$ and $\pi_3(G)$ be three distinct connected components of $\Gamma(G)$. Let p,q be two distinct primes in $\pi(G)$; then $p \in \pi_i(G)$, $q \in \pi_j(G)$, with $i,j \in \{1,2,3\}$ not necessarily distinct. By our hypothesis, there exists a prime $s \in \pi_k(G)$, with $i \neq k \neq j$. Let x be an s-element of G; then x is a p'-element and q does not divide $|C_G(x)|$. Therefore G does not satisfy $P(p,q)$. ∎

We use the Classification of Finite Simple Groups to prove Proposition 2.

SPORADIC GROUPS. We can apply Lemma 3 to the following sporadic groups: M_{11}, M_{22}, M_{23}, M_{24}, J_1, J_3, J_4, HS, Sz, $O'N$, Ly, CO_2, F_{23}, F_{24}', F, F_2, F_3. In fact, from [18], we know that for these groups G we have $n(G) \geq 3$.

For the remaining sporadic groups G, we have that $n(G)=2$, $\pi_2(G)=\{t\}$, $t \geq 7$ and a t-Sylow subgroup of G is cyclic of order t. If $p \neq t$ and $q \neq t$, then there exists a t-element (and therefore a p'-element) x such that q does not divide $|C_G(x)|$. If $p \neq t$ and $q = t$, we can choose any $\{p,q\}'$-element x and again q does not divide $|C_G(x)|$. If now $p = t$, then in all the groups we are considering there exists an element x of order 6 such that $C_G(x)$ does not contain a q-Sylow subgroup of G, for any prime q dividing $|G|$. Therefore if G is a sporadic group and q divides $|G|$, then G does not satisfy $P(p,q)$.

ALTERNATING GROUPS. To any element σ of the symmetric group S_n, there is associated a partition of the integer n:

$$\sigma \longmapsto (n_1, n_2, \dots, n_h), \quad \sum_{i=1}^{h} n_i = n.$$

Moreover, we can order the numbers n_i such that

$$n_1 = n_2 = \cdots = n_{h_1} > n_{h_1+1} = \cdots = n_{h_1+h_2} > \cdots n_h, \quad h = \sum_{i=1}^{t} h_i.$$

In this case we then have ([9, ex. 3, p. 78])

$$|C_{S_n}(\sigma)| = \prod_{i=1}^{t} h_i! \prod_{j=1}^{h} n_j.$$

Here are some examples that will be useful later.

$\sigma \mapsto (n) \Longrightarrow |C_{S_n}(\sigma)| = n$ and $|C_{A_n}(\sigma)| = n$, if $\sigma \in A_n$;
$\sigma \mapsto (1, n-1) \Longrightarrow |C_{S_n}(\sigma)| = n-1$ and $|C_{A_n}(\sigma)| = n-1$, if $\sigma \in A_n$;
$\sigma \mapsto (1,1,n-2) \Longrightarrow |C_{S_n}(\sigma)| = 2(n-2)$ and $|C_{A_n}(\sigma)| = n-2$, if $\sigma \in A_n$;
$\sigma \mapsto (2, n-2) \Longrightarrow |C_{S_n}(\sigma)| = 2(n-2)$ and $|C_{A_n}(\sigma)| = n-2$, if $\sigma \in A_n$.

We study now the groups A_n. By Lemma 3, we can suppose that $n \geq 8$. We denote by $|n|_q$ the maximal power of q dividing n. Let Q be a q-Sylow subgroup of A_n; then $|Q| = |n!/2|_q$.

First we suppose that n is odd. If $q = n$ and σ is an element of order q, then $|C_{A_n}(\sigma)| = q$. Therefore, since $|\pi(A_n)| \geq 3$, for any prime $p \in \pi(A_n)$, $p \neq q$, there exists a p'-element x such that q does not divide $|C_G(x)|$.

We can therefore suppose $q < n$. We suppose now that p does not divide n. Then, since $q < n$, we have $|n!|_q > |n|_q$ and, moreover, $|n!/2|_q > |n|_q$, since we are supposing $n \geq 8$.

Let x be the permutation $(1, 2, \dots, n)$, then x is a p'-element in A_n and $|C_{A_n}(x)| = n$. Since $|n|_q < |Q|$, a q-Sylow subgroup Q^g cannot be contained in $C_{A_n}(x)$.

We now suppose that p divides n. Then p is an odd prime not dividing $(n-2)$. If $q = n-2$ and σ is a q-element, then $|C_{A_n}(\sigma)| = n-2$, and we can conclude with an argument similar to the one used in the case $q = n$. Therefore we suppose that $q < (n-2)$. Since $n \geq 8$, $n-2 \geq 6$ and then again

$$(**) \qquad |n-2|_q < \left|\frac{(n-2)!}{2}\right|_q \leq \left|\frac{n!}{2}\right|_q = |Q|.$$

Let x be the permutation $(1, 2, \ldots, n-2)$; then x is a p'-element in A_n whose centralizer in A_n has order $n-2$. Then, by $(**)$, a q-Sylow subgroup Q^g cannot be contained in $C_{A_n}(x)$.

If n is even, we can conclude in a similar way.

FINITE GROUPS OF LIE TYPE. We can now suppose that G is a finite simple group of Lie type defined over a field GF(t) of order $t = r^k$, for some prime r. First we suppose $p \neq r$. If $q = r$, the unipotent subgroup U of G is a q-Sylow subgroup of G. Since $C_G(U) = Z(U)$, any $\{p, q\}'$-element cannot centralize a q-Sylow subgroup and therefore $P(p, q)$ does not hold in G in this case. We can therefore suppose $q \neq r$. We recall that x is a semisimple element if and only if x is an r'-element. By Proposition 5.1.7 of [2], G contains an unipotent regular element u, that is a regular r-(and therefore p')-element. Then, by Proposition 5.1.5 of [2], $C = C_G(u)$ does not contain semisimple elements. We can conclude that q does not divide $|C|$ for any $q \in \pi(G) \setminus \{r\}$.

We suppose now that $p = r$; then a p'-element is a semisimple element. If q and s are distinct primes, both different from p, and if y is a q-element that centralizes an s-element x, then xy is a $\{q, s\}$-element and therefore a semisimple element. Since every semisimple element is contained in a maximal torus, there exists a maximal torus containing xy. Then for any $q \neq p$, we are looking for a prime $s \neq p$ such that qs does not divide the order of any maximal torus of G. We have to do a case-by-case analysis. We recall that, for any $i \geq 2$, the connected component $\pi_i(G)$ is the set of primes that divide $|T_i|$, for some maximal torus T_i. If $n(G) \geq 3$, by Lemma 3, G does not satisfy $P(p, q)$. We now suppose that $n(G) = 2$; therefore $p \in \pi_1(G)$ and $|\pi_1(G)| \geq 2$ (see [18] and [10]). If $q \in \pi_2(G)$, we choose a prime s such that $p \neq s \in \pi_1(G)$. If $q \in \pi_1(G)$, we choose a prime s such that $p \neq s \in \pi_2(G)$. In both cases, it is now clear that for any element x of order s, the prime q does not divide $|C_G(x)|$. Therefore in any finite simple group of Lie type such that its prime graph is not connected and for any q dividing $|G|$, we can find a p'-element such that $C_G(x)$ does not contain a q-Sylow subgroup. The statement of Proposition 2 is therefore proved in these cases.

It is therefore sufficient to examine the groups S of Lie type such that the prime graph of S is connected. From [18] and [10], we know that these are some classical groups and the exceptional groups $E_7(t)$.

We now quote a technical lemma, due to Zsigmondy.

LEMMA 4 (Zsigmondy): (i) *Let r, k be two positive integers, with $k \geq 3$: then there exists a "primitive divisor" of $r^k - 1$, that is a prime s dividing $r^k - 1$ and not dividing $r^j - 1$, for any $j = 1, \ldots, k-1$, except in the cases $r = 2$ and $k = 6$.*

(ii) *Let r, k be two positive integers, $(r, k) \neq (2, 3)$; then there exists a "primitive divisor" of $r^k + 1$, that is a prime s dividing $r^k + 1$ and not dividing $r^{2j} - 1$, for any $j = 1, \ldots, k-1$.*

Proof: (i) This is exactly the Zsigmondy Theorem [19].

(ii) We apply (i) to $r^{2k} - 1$ and find a primitive divisor s. Since s cannot divide $r^k - 1$, then s must divide $r^k + 1$. ∎

Before beginning with a case-by-case analysis, we make some general remarks. The orders of the finite groups of Lie type can be found in [2]. The orders of the maximal tori of finite groups of Lie type are known: for the classical groups and for $E_7(t)$, they can be deduced from [3]. We denote by $|n|_\pi$ the π-part of the integer n, where π is a set of primes. If $T =< x >$ is a cyclic maximal torus, then $|C_G(x)|_{p'} = |T|$; otherwise there would be an element y of order $|x|m$, with $(m, p) = 1$. But $|x|m$ cannot divide the order of any maximal torus in the cases we consider.

$A_l(t) \cong \mathrm{PSL}_{l+1}(t)$. The orders of maximal tori are

$$\frac{\prod_{i=1}^{k}(t^{r_i} - 1)}{(t-1)(l+1, t-1)} \quad (r_1, \ldots, r_k) \in \mathrm{Par}(l+1).$$

Let x be a Singer cycle of G (see [7, Satz II.7.3]). Then

$$|x| = (t^{l+1} - 1)/(t-1)(l+1, t-1) \quad \text{and} \quad C = C_G(x) =< x > .$$

If C does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then q is coprime with $t-1$. In fact if q divides $t-1$, then

$$|Q| = |(t^{l+1} - 1)/(t-1)(l+1, t-1)|_q < |t^{l+1} - 1|_q < |G|_q,$$

against the hypothesis that Q is a q-Sylow subgroup of G. Therefore $(q, t^l - 1) = 1$, because $(t^{l+1} - 1, t^l - 1) = (t-1)$. Let s be a primitive divisor of $t^l - 1$. If qs

divides the order of a maximal torus T, then by our choice of s, t^l-1 should divide $|T|$. Therefore the only possibility for the order of T is $(t^l-1)/(l+1,t-1)$. But q is coprime with t^l-1, and therefore q cannot divide $|T|$.

If $G=A_6(2)$, $A_1(t)$ or $A_2(t)$, we cannot apply Lemma 4 in the preceding argument. But in these cases we have that $n(G)\geq 2$ (see [18] and [10]) and we conclude by the remark preceding Lemma 4.

$B_l(t)\cong P\Omega_{2l+1}(t)$. The order of a maximal torus T is of the type

$$\frac{\prod_{i=1}^k(t^{r_i}-1)\prod_{j=1}^m(t^{s_j}+1)}{(2,t-1)}\quad (r_1,\ldots,r_k,s_1,\ldots,s_m)\in \mathrm{Par}(l).$$

By [11], there is a cyclic torus $T=<x>$ of order $(t^l+1)/(2,t-1)$ such that $|C_G(x)|_{p'}=|T|$ (by the remark preceding the case-by-case analysis). If $C=C_G(x)$ does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then q is odd. Therefore $(q,t^l-1)=1$, because $(t^l+1,t^l-1)=(2,t-1)$. Let s be a primitive divisor of t^l-1. If qs divides the order of a maximal torus T_1, then by our choice of s, t^l-1 should divide $|T_1|$. Therefore the only possibility for the order of T_1 is $(t^l-1)/(2,t-1)$. But q is coprime with t^l-1, and therefore q cannot divide $|T_1|$.

If $l=2$ or $G=B_6(2)$, we cannot apply Lemma 4. But if $G=B_2(t)$, then $\Gamma(G)$ is not connected (see [18] and [10]). If $G=B_6(2)$ we can apply the preceding argument, except in the case in which the order of a q-Sylow subgroup divides $2^6+1=5\cdot 13$, that is $q=13$. In this case we choose $s=31=2^5-1$ and again qs cannot divide the order of any maximal torus of G.

$D_l(t)\cong P\Omega_{2l}(t)$. We can suppose that $G\neq D_4(2),D_6(2)$, because in these cases $\Gamma(G)$ is not connected (see [18] and [10]). The order of a maximal torus T is of the type

$$\frac{\prod_{i=1}^k(t^{r_i}-1)\prod_{j=1}^m(t^{s_j}+1)}{(4,t^l-1)}\quad (r_1,\ldots,r_k,s_1,\ldots,s_m)\in \mathrm{Par}(l),\ m \text{ even}.$$

By [11], there is an element x of order $(t^{l-1}+1)/d$. The maximal tori T containing this element must be of order $(t^{l-1}+1)(t+1)/d$ and therefore $|C_G(x)|_{p'}=|T|$. If $C=C_G(x)$ does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then q is coprime with t^2-1. In fact q is certainly odd and $(t^{l-1}+1,t^{l-1}-1)=(2,t-1)$ implies that if q divides t^2-1, then it divides $t+1$. But then

$$|Q|=|C|_q=|(t^{l-1}+1)(t+1)/d|_q<|G|_q$$

against the hypothesis that Q is a q-Sylow subgroup of G. Therefore $(q, t^l - 1) = 1$, because $(t^{l-1}+1, t^l-1) \leq (t^{2(l-1)}-1, t^l-1) = (t^{(2,l)}-1)$. Let s be a primitive divisor of $t^l - 1$. If qs divides the order of a maximal torus T_1, then by our choice of s, $t^l - 1$ should divide $|T_1|$. Therefore the only possibility for the order of T_1 is $(t^l-1)/d$. But q is coprime with $t^l - 1$, and therefore q cannot divide $|T_1|$.

$E_7(t)$. The order of the maximal tori of $E_7(t)$ can be found in [3]. In particular there exists a maximal torus of order t^7+1 (see Tables 3 and 10 of [3]). By [17] there exists an element x of order $(t^8-1)/(t-1)$, generating a maximal torus T and such that $|T| = |C_G(x)|_{p'}$. If $C = C_G(x)$ does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then q is coprime with $t^2 - 1$. In fact, if q divides $t^2 - 1$, then

$$|Q| = |C|_q = |(t^8-1)/(t-1)|_q < |G|_q$$

against the hypothesis that Q is a q-Sylow subgroup of G. Therefore $(q, t^7+1) = 1$, because $(t^8-1, t^7+1) \leq (t^2-1)$. Let s be a primitive divisor of t^7+1. If qs divides the order of a maximal torus T_1, then by our choice of s, t^7+1 should divide $|T_1|$. Therefore the only possibility for the order of T_1 is (t^7+1). But q is coprime with t^7+1, and therefore q cannot divide $|T_1|$.

${}^2A_l(t) \cong \mathrm{PSU}_{l+1}(t)$. We can suppose that $G \neq {}^2A_5(2)$, ${}^2A_6(2)$ and ${}^2A_2(t)$, because in these cases $n(G) \geq 2$ (see [18] and [10]). The orders of the maximal tori are

$$\frac{\prod_{i=1}^k (t^{r_i}-1)\prod_{j=1}^m (t^{s_j}+1)}{(t+1)(t+1,l+1)} (r_1,\ldots,r_k,s_1,\ldots,s_m) \in \mathrm{Par}(l+1),\ r_i \text{ even}, s_j \text{ odd}.$$

By [11], there is an element x of order $(t^{l+1}+1)/(l+1,t+1)(t+1)$ if l is even and of order $(t^l+1)/(l+1,t+1)(t+1)$ if l is odd. The order of a maximal torus containing x is respectively $|T| = |x|$ if l is even, $|T| = (t^l+1)/(l+1,t+1)$ if l is odd. In both cases, however, $|C_G(x)|_{p'} = |T|$ by the remark preceding the case-by-case analysis. If $C = C_G(x)$ does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then using an argument similar to the one used in the case $D_l(t)$ we can prove respectively that $(q, t^l-1) = 1$ if l is even and $(q, t^{l+1}-1) = 1$ if l is odd. Let s be a primitive divisor of $t^l - 1$ if l is even, and of $t^{l+1}-1$ if l is odd. If qs divides the order of a maximal torus T_1, then by our choice of s, $(t^l-1)/(l+1,t+1)(t+1)$ (resp. $(t^{l+1}-1)/(l+1,t+1)(t+1)$) should divide $|T_1|$. Therefore the only possibility for the order of T_1 is $(t^l-1)/(l+1,t+1)$ if l

is even and $(t^{l+1}-1)/(l+1,t+1)(t+1)$ if l is odd. But in both cases q cannot divide $|T_1|$.

${}^2D_l(t) \cong P\Omega_{2l}(t)$. We can suppose that $G \neq {}^2D_4(2)$, because in this case $n(G) \geq 2$ (see [10]). The orders of the maximal tori are

$$\frac{\prod_{i=1}^{k}(t^{r_i}-1)\prod_{j=1}^{m}(t^{s_j}+1)}{(4,t^l+1)} \quad (r_1,\ldots,r_k,s_1,\ldots,s_m) \in \mathrm{Par}(l),\ m \text{ odd}.$$

By [11], there is an element x of order $(t^l+1)/(2,t+1)$ such that $<x>=T$ for a maximal torus T and therefore $|C_G(x)|_{p'} = |T|$ by the remark preceding the case-by-case analysis. If $C = C_G(x)$ does not contain a q-Sylow subgroup, then x is the p'-element we are looking for. If a q-Sylow subgroup Q is contained in C, then q is coprime with t^2-1, and therefore with $(q,(t^{l-1}+1)(t-1)) = 1$ by the same argument used in the case $D_l(t)$. Let now s be a primitive divisor of $t^{l-1}+1$. If qs divides the order of a maximal torus T_1, then by our choice of s, $(t^{l-1}+1)$ should divide $|T_1|$. Therefore the only possibility for the order of T_1 is $(t^{l-1}+1)(t-1)/(2,t+1)$. But q cannot divide $|T_1|$.

We have thus proved the statement for all finite simple groups. ∎

We now extend this result to almost simple groups, proving Proposition 1.

Proof: Let S be a simple group such that $S \trianglelefteq G \leq \mathrm{Aut}(S)$. If q divides $|S|$, then, by Proposition 2, there exists a p'-element $x \in S$ whose centralizer does not contain any q-Sylow subgroup of S and therefore the statement is proved also for G. We can therefore suppose that q divides $|G/S|$, but not $|S|$. This implies that S is a simple group of Lie type, defined over the field $\mathrm{GF}(t^q)$, for some prime power t, and q is the order of a field automorphism of S. Let α be an element of $G \setminus S$, such that $|\alpha| = q$. If we find two different primes $r_1, r_2 \in \pi(S)$, such that neither r_1 nor r_2 divides $|C_S(\alpha)|$, then the theorem is proved. In fact, a q-Sylow subgroup Q of G is isomorphic to a cyclic subgroup of G/S, and therefore all the subgroups of order q of G are conjugate. This means that if β is any element of order q of G, then $|C_S(\beta)| = |C_S(<\beta>)| = |C_S(<\alpha>)|$. But then for any $p \in \pi(G)$, there exists a p'-element (namely either an r_1- or an r_2-element) x such that $x \notin C_S(\beta)$ for any element β of order q, and therefore q does not divide $|C_G(x)|$. This proves that G does not satisfy $P(p,q)$ and therefore the proposition is true.

Let ${}^dL_n(t^q)$ denote a group of Lie type L, of rank n, defined over the field with t^q elements, and $d=1$ means $L_n(t^q)$ untwisted, $d=2$ means ${}^2L_n(t^q)$ twisted, $d=3$ implies $L=D$, $n=4$, that is ${}^dL_n(t^q) = {}^3D_4(t^q)$. If α is a field automorphism of order q, then $C_S(\alpha) \cong {}^dL_n(t)$. We now prove that there exists two different primes r_1, r_2 in $\pi(S) \setminus \pi(C_S(\alpha))$. Let r_1 and r_2 be primitive divisors respectively of m and n, where m and n are as listed in the following list, where we put $s = t^q$.

Type	m	n
$A_l(s)$	$s^{l+1}-1$	s^l-1
${}^2A_l(s)$	$s^{l+1}-(-1)^{l+1}$	$s^l-(-1)^l$
$B_l(s)$	s^l-1	s^l+1
$D_l(s)$	s^l-1	$s^{l-1}-1$
${}^2D_l(s)$	s^l+1	$s^{l-1}-1$
${}^3D_4(s)$	s^6+1	s^6-1
$E_6(s)$	s^6+1	s^9-1
${}^2E_6(s)$	s^6+1	s^9+1
$E_7(s)$	s^7+1	s^8-1
$E_8(s)$	$s^{15}+1$	$s^{12}+1$
$F_4(s)$	s^6+1	s^6-1
${}^2F_4(s)$	s^6+1	s^4-1
$G_2(s)$	s^3-1	s^3+1
${}^2G_2(s)$	s^3+1	$s-1$
${}^2B_2(s)$	s^2+1	$s-1$

It is easy to prove that r_1 and r_2 are two different primes that divide $|S|$ but not $|C_S(\alpha)|$. It can be useful to notice that $q \geq 5$ for any exceptional group of Lie type $S = {}^dL_n(t)$, except for $S = {}^2B_2(t^q)$ when $q \geq 3$. Moreover, if $S = E_8(t^r)$ then $q \geq 7$. ∎

As a corollary, recalling Lemma 2(i) we immediately get the following:

COROLLARY 1: *If the group G verifies $P(p,q)$, then G is q-solvable.*

We can now prove the main theorem of this section.

THEOREM 3: *If the group G satisfies $P(p,q)$, then $O^{q'}(G)$ is solvable.*

Proof: We show, proceeding by induction on $|G|$, that if G has $P(p,q)$ and the soluble radical $\mathcal{R}(G)$ of G is trivial, then $(q,|G|)=1$.

Write $S = \mathrm{Soc}(G) = M_1 \times \cdots \times M_n$, where $M_i = (S_i)^{k_i}$ is the direct product of k_i isomorphic copies of the non-abelian simple group S_i and $S_i \not\cong S_j$ for $i \neq j$. Since we are assuming that $\mathcal{R}(G) = 1$, S coincides with the generalized Fitting subgroup of G and hence $C_G(S) = Z(S) = 1$. Thus, we can identify G with a subgroup of the group $\mathrm{Dir}_{i=1}^n(\mathrm{Aut}(S_i) \wr \mathrm{Sym}(k_i))$ ([16, 3.3.20]). Let B_i be the base group of the wreath product $\mathrm{Aut}(S_i) \wr \mathrm{Sym}(k_i)$ and let $B = G \cap \mathrm{Dir}_{i=1}^n B_i$. As $B \trianglelefteq G$, B satisfies $P(p,q)$. Then, the projections of B on the factors $\mathrm{Aut}(S_i)$ have $P(p,q)$ as well (by Lemma 2) and, since they are almost simple groups, by Proposition 1 they are q'-groups. Therefore B is a q'-group, too.

Let now $R \leq G$ such that $R/B = \mathcal{R}(G/B)$. By inductive hypothesis, G/R is a q'-group. It only remains to show that R/B is a q'-group. Observe that R/B is a solvable group that acts as a permutation group on the simple factors S_i of $\mathrm{Soc}(G)$ and hence on the set of indices $\Omega = \bigcup_{i=1}^n \Omega_i$, where $\Omega_i = \{i_1, \ldots, i_{k_i}\}$. Then, by [5, Corollary 4] there exist two disjoint subsets Γ and Δ of Ω such that all (distinct) prime divisors of $|R/B|$ divide also $|R/B : \mathrm{Stab}_{R/B}(\Gamma) \cap \mathrm{Stab}_{R/B}(\Delta)|$. We fix r_i, s_i primes dividing $|M_i|$ such that $r_i \neq s_i$ and $r_i, s_i \neq p$ for all $i = 1, \ldots, n$. We then choose $c_\omega, d_\omega \in S_\omega$ such that $|c_\omega| = r_i$, $|d_\omega| = s_i$, if $\omega \in \Omega_i$. Write $\Gamma_i = \Gamma \cap \Omega_i$, $\Delta_i = \Delta \cap \Omega_i$ and consider in S the element $x = (x_\omega)_{\omega \in \Omega}$, where $x_\omega = c_i$ if $\omega \in \Gamma_i$, $x_\omega = d_i$ if $\omega \in \Delta_i$ and $x_\omega = 1$ otherwise. By definition of x, $C_R(x)B/B \leq \mathrm{Stab}_{R/B}(\Gamma) \cap \mathrm{Stab}_{R/B}(\Delta)$ and hence it follows that all prime divisors of $|R/B|$ divide $|x^R|$. But x is a p'-element and $R \trianglelefteq G$ verifies $P(p,q)$. Hence $(q, |R/B|) = 1$. ∎

4. Structure theorems

The structure of the groups that satisfy $P(p,q)$ for $p = q$ is known:

THEOREM 4 (Camina [1]): *$P(p,p)$ holds in G for a prime p if and only if a p-Sylow subgroup of G is a direct factor of G.*

Proof: Let P be a p-Sylow subgroup of G and $Z = C_G(P)$. Let $x \in G$ and write $x = yz$ with y p-element, z p'-element and $[y,z] = 1$. By assumption there exists $u \in G$ such that $z \in C_G(P^{u^{-1}}) = Z^{u^{-1}}$, i.e. $z^u \in Z$. Now, y^u is a p-element and $y^u \in C_G(z^u)$. Since $P \leq C_G(z^u)$, there exists $v \in C_G(z^u)$ such that $y^{uv} \in P$. It follows that $x^{uv} = y^{uv} z^{uv} = y^{uv} z^u \in PZ$. Then PZ intersects non-trivially every conjugacy class of G and hence $PZ = G$ and P is a direct factor of G. ∎

When the primes p and q are different, the structure of the groups that satisfy $P(p,q)$ can be more complicated.

THEOREM 5: *If the group G satisfies $P(p,q)$, with $p \neq q$, then $O^p(G)$ is q-nilpotent and G has abelian q-Sylow subgroups. In particular, $l_q(G) \leq 1$.*

Proof: Write $H = G/O_{q'}(G)$ and let h be a p'–element of H. As $P(p,q)$ holds in H, $h \in C_H(O_q(H))$. By Corollary 1, we have that H is q-solvable and then

$C_H(O_q(H)) \leq O_q(H)$. Thus every p'-element in H belongs to $Z(O_q(H))$ and hence H has a normal abelian q-Sylow subgroup and every element in $H \setminus O_q(H)$ has order divisible by p. Then $H/O_q(H)$ must be a p-group. ∎

COROLLARY 2: *If, for $p \neq q$, $P(p,q)$ holds in the group G and $O^p(G) = G$, then $O_q(G) \leq Z(G)$.*

Proof: By Theorem 5, $[O_q(G), G] \leq O_{q'}(G) \cap O_q(G) = 1$. ∎

On the other hand, $P(p,q)$ is inherited by extension by central q-groups, provided the q-Sylow subgroups remain abelian. By the way, observe that Corollary 2 and Lemma 5 hold even if $p = q$.

LEMMA 5: *Let G be a group with abelian q-Sylow subgroups and let Z be a q-subgroup, $Z \leq Z(G)$. If G/Z satisfy $P(p,q)$ for $p \neq q$, then $P(p,q)$ holds also in G.*

Proof: Let g be a p'-element of G and write $g = xy$ with x q'-element, y q-element and $[x,y] = 1$. By assumption there exists a q-Sylow subgroup Q of G such that $[x,Q] \leq Z$. So x acts trivially on Z and Q/Z and hence $Q \leq C_G(x)$. As $y \in C_G(x)$ and y is a q-element, there exists $u \in C_G(x)$ such that $y \in Q^u$. Since Q^u is abelian, it follows that $Q^u \leq C_G(x) \cap C_G(y) = C_G(g)$. ∎

It is therefore meaningful to consider groups G such that $O_q(G) = 1$. Moreover, we observe that, by (iii) and (iv) in Lemma 2, when $p \neq q$, $P(p,q)$ can control only the section $O^p(G)/O_p(G)$. In what follows we may hence consider groups G such that $O_p(G) = 1$ and $O^p(G) = G$.

Consequently, we give the following definition:

Definition 1: We say that a group G is a $P(p,q)$-group if:

(i) G has $P(p,q)$ for distinct primes p, q;

(ii) q divides $|G|$;

(iii) $O_p(G) = O_q(G) = 1$, $O^{q'}(G) = G$.

Remark 1: Observe that, by Theorem 3, a $P(p,q)$-group is solvable.

We next give a characterisation of the semilinear groups that satisfy $P(p,q)$, since they will turn out to be the "basic bricks" by which the groups with $P(p,q)$ are built.

Definition 2: Let k, n, h be positive integers and r, p, q distinct primes. Assume that $k = q^n$ and $(r^{q^n} - 1)/(r^{q^{n-1}} - 1) = p^h$. Let H be the subgroup of $GF(r^k)^\times$ of order p^h. Define:

$$A\Gamma^*(r^k) = \left\{ \begin{pmatrix} x \\ ax^\sigma + b \end{pmatrix} : x, b \in \mathrm{GF}(r^k), a \in H, \sigma \in \mathrm{Gal}(GF(r^k)/GF(r^{k/q})) \right\},$$

$$A\Gamma_0^*(r^k) = \left\{ \begin{pmatrix} x \\ ax + b \end{pmatrix} : x, b \in \mathrm{GF}(r^k), a \in H \right\}.$$

(Observe that $|A\Gamma^*(r^k)| = r^k p^h q$ and $|A\Gamma_0^*(r^k)| = r^k p^h$.)

LEMMA 6: *Let r, p, q be pairwise different primes. Let G be a subgroup of the affine semilinear group $A\Gamma(r^k)$, for some positive integer k. Assume $A(r^k) \leq G$ and $(q, |G|) \neq 1$. Then G satisfies $P(p, q)$ if and only if:*

(i) *$k = q^n$, with n a positive integer and $q \neq 2$;*

(ii) *the q-Sylow subgroups of G have order q;*

(iii) *for a suitable integer h*

$$\frac{r^{q^n} - 1}{r^{q^{n-1}} - 1} = p^h;$$

(iv) *$A\Gamma^*(r^k) \leq G$.*

Proof: Assume that G satisfies $P(p, q)$ and define $V = A(r^k)$ and $\Gamma_0 = G \cap \Gamma_0(r^k)$. By assumption, $V \leq G$ and V is a p'-group. As Γ_0 acts fixed point freely on V, we have $(q, |\Gamma_0|) = 1$. It follows that $\Gamma_0 = [\Gamma_0, Q] \times C_{\Gamma_0}(Q)$, where by Q we denote a (fixed) q-Sylow subgroup of G such that $Q \leq G \cap \Gamma(r^k)$.

By $P(p, q)$, we have that for all $x \in V$, there exists $g \in G$ such that $Q^g \leq C_G(x)$. Since $G = C_G(Q)[\Gamma_0, Q]V$, we get

$$V = \bigcup_{g \in [\Gamma_0, Q]} C_V(Q)^g.$$

Suppose $x \in C_V(Q)^{g_1} \cap C_V(Q)^{g_2}$ with $g_i \in [\Gamma_0, Q], g_1 \neq g_2$. Then $< Q^{g_1}, Q^{g_2} > \leq C_G(x)$ and hence $C_G(x) \cap \Gamma_0 \neq 1$, so $x = 1$. It follows that

$$|V| - 1 = |[\Gamma_0, Q]|(|C_V(Q)| - 1),$$

that is

$$|[\Gamma_0, Q]| = \frac{|V| - 1}{|C_V(Q)| - 1} = \frac{r^k - 1}{r^m - 1}$$

with $m = k/|Q|$ (we observe that $(q, |V\Gamma_0|) = 1$ and hence $|Q|$ divides k).

By Lemma 2(i), $P(p,q)$ holds in the section $[\Gamma_0,Q]Q$ of G. Hence, as Q does not commute with any nonidentity element of $[\Gamma_0,Q]$, we get $(r^k-1)/(r^m-1)=p^h$ for a suitable positive integer h. Note that, if $q=2$, then $p^h=\sum_{i=0}^{|Q|-1}(r^m)^i$ is even and hence $p=q$, a contradiction. So, $q\neq 2$ and p is the (only) Zsigmondy prime divisor for r^k-1.

Write now $|Q|=q^v$, v positive integer, and $t=r^m$. We have

$$p^h=\frac{t^{q^v}-1}{t-1}=\frac{t^{q^{v-1}}-1}{t-1}w$$

with w a positive integer. It follows that $(t^{q^{v-1}}-1)/(t-1)=p^{h_0}$ with h_0 an integer. By the Zsigmondy condition, we get $h_0=0$ and then $|Q|=q$.

Let now z be the q'-part of k, that is $k=zq^n$ for a positive integer n and $(q,z)=1$. We have

$$p^h\frac{r^m-1}{r^{q^{n-1}}-1}=\frac{r^k-1}{r^{q^{n-1}}-1}=\frac{(r^{q^n})^z-1}{r^{q^{n-1}}-1}=\frac{r^{q^n}-1}{r^{q^{n-1}}-1}u$$

with u a positive integer. Observe now that $(r^m-1,r^{q^n}-1)=r^{(m,q^n)}-1=r^{q^{n-1}}-1$ and hence

$$\left(\frac{r^m-1}{r^{q^{n-1}}-1},\frac{r^{q^n}-1}{r^{q^{n-1}}-1}\right)=1.$$

Therefore, $(r^{q^n}-1)/(r^{q^{n-1}}-1)$ is a power of p and hence the Zsigmondy condition forces $k=q^n$. Observe finally that r^kp^hq divides $|G|$ and that $A\Gamma^*(r^k)$ is the only subgroup of order r^kp^hq in the semilinear group $A\Gamma(r^k)$. It follows that $A\Gamma^*(r^k)\leq G$ and one implication is now proved. The other is easily checked. ∎

Remark 2: In the notation of Lemma 6, the Zsigmondy condition implies that q^n divides $p-1$, as q^n is the multiplicative order of the rest class of r modulo p. Further, $(q,r^{q^{n-1}}-1)=1$. In fact, writing $t=r^{q^{n-1}}$, $p^h=1+t+t^2+\cdots+t^{q-1}$ and, if $t\equiv 1 \pmod q$, then $p^h\equiv 0 \pmod q$, a contradiction.

Remark 3: Observe that the exponent n in Lemma 6 can be greater than 1. For instance, $r^{q^n}-1/r^{q^{n-1}}-1$ is a prime number for $n=2$ and $(r,q)=(2,3)$ or $(11,3)$.

The next result is the main step for understanding the structure of the $P(p,q)$-groups.

PROPOSITION 6: *Let p, q be distinct primes and K be a solvable group such that $O^{q'}(K) = K$. Let W be a completely reducible and faithful K-module, $W = \bigoplus_{i=1}^n V_i$, with V_i irreducible K-modules, $|V_i| = r_i^{k_i}$ for suitable primes r_i and positive integers k_i. Then, $G = WK$ is a $P(p,q)$-group if and only if:*

(i) *$k_i = q^{n_i}$, $r_i \neq q \neq 2$ and $(r_i^{k_i} - 1)/(r_i^{k_i/q} - 1) = p^{h_i}$, for $i = 1, \dots, n$ and suitable nonnegative integers n_i, h_i;*

(ii) *up to isomorphisms,*

$$\mathrm{Dir}_{i=1}^n A\Gamma_0^*(r_i^{k_i}) \leq G \leq M = \mathrm{Dir}_{i=1}^n A\Gamma^*(r_i^{k_i})$$

and the projections of G on the factors of M are surjective.

Proof: We assume that $G = WK$ is a $P(p,q)$-group and proceed by induction on $|G|$.

Suppose W reducible and write $W = W_1 \bigoplus W_2$, where $W_1 = V_1$ and $W_2 = \bigoplus_{i=2}^n V_i$. Write $K_i = K/C_K(W_i)$, $G_i = W_iK_i$, $i = 1, 2$. By induction, we have (i) and

$$G_1 = A\Gamma^*(r_1^{k_1})$$

and

$$\mathrm{Dir}_{i=2}^n A\Gamma_0^*(r_i^{k_i}) \leq G_2 \leq \mathrm{Dir}_{i=2}^n A\Gamma^*(r_i^{k_i})$$

with surjective projections on the factors of the direct product.

As G is a subdirect product of G_1 and G_2, to prove (ii) it is enough to show that $|\mathrm{Dir}_{i=1}^n A\Gamma_0^*(r_i^{k_i})|$ divides $|G|$. Observe namely that $\mathrm{Dir}_{i=1}^n A\Gamma_0^*(r_i^{k_i})$ is the only subgroup of $\mathrm{Dir}_{i=1}^n A\Gamma^*(r_i^{k_i})$ of that order, since it is a normal q'-Hall subgroup of $\mathrm{Dir}_{i=1}^n A\Gamma^*(r_i^{k_i})$. Define $I = \{(v_1, v_2, \dots, v_n) | \; v_i \in V_i, v_i \neq 1, i = 1, \dots, n\}$ and let P and Q be resp. a p- and a q-Sylow subgroup of K. Hence, $K = PQ$ and $P \trianglelefteq K$. Observe that, writing $C_I(Q) = C_W(Q) \cap I$, by $P(p,q)$ we have

$$I = \bigcup_{g \in K} C_I(Q)^g = \bigcup_{g \in P} C_I(Q)^g$$

and the union is disjoint. Namely, if $v \in C_I(Q)^{g_1} \cap C_I(Q)^{g_2}$ with $g_1, g_2 \in P$, $g_1 \neq g_2$, then $C_K(v)$ contains $< Q^{g_1}, Q^{g_2} >$ and hence it would follow that $C_P(v) \neq 1$. But P is conjugate to a subgroup of $\mathrm{Dir}_{i=1}^n \Gamma_0(V_i)$, so every nonidentity element of P acts without fixed points on I, a contradiction.

Therefore,

$$|I| = \prod_{i=1}^n (r_i^{k_i} - 1) = |P||C_I(Q)| = |P| \prod_{i=1}^n (r_i^{k_i/q} - 1).$$

Hence,

$$|\operatorname*{Dir}_{i=1}^{n} A\Gamma_0^*(V_i)| = \prod_{i=1}^{n} r_i^{k_i} \frac{r_i^{k_i}-1}{r_i^{k_i/q}-1} = |W||P| \text{ divides } |G|.$$

We can hence assume that W is an irreducible and faithful K-module. We have two cases:

W primitive: if W is a primitive K-module, the claim follows by [13, Theorem 10.4] and by Lemma 6.

W imprimitive: we shall conclude the proof by showing that this case cannot occur. Let W be an imprimitive K-module and consider C maximal among the subgroups $N \trianglelefteq K$ such that W_N is non-homogeneous. By [13, 9.2] and the assumption $O_q(G) = 1$, we have $q \neq 2$ and then by [13, 9.3] we get

1. $q = 3$ and $p = 7$;
2. $W_C = V_1 \oplus V_2 \oplus \cdots \oplus V_8$, where the V_i are the homogeneous components of W_C and $K/C \simeq A\Gamma(2^3)$;
3. $C/C_C(V_i)$ is transitive on $V_i \setminus \{1\}$, $i = 1, \ldots, n$.

Write $|V_i| = r^m$. By [13, 6.8], it follows that $C/C_C(V_i)$ is isomorphic to a subgroup of the semilinear group $\Gamma(r^m)$, unless $r^m = 3^2, 3^4, 5^2, 7^2, 11^2, 23^2$. But if m is even then $q = 3$ divides $r^m - 1$ (as $O_q(G) = 1$, $r \neq 3$) and hence q is a divisor of $|v^C|$ and $|v^G|$ for any $v \in V_i$, $v \neq 1$, a contradiction.

Therefore, $C/C_C(V_i)$ is isomorphic to a subgroup of the semilinear group $\Gamma(r^m)$ and hence C, being isomorphic to a subgroup of a direct product of supersolvable groups, is supersolvable.

Define now $R = O_{\{p,q\}}(K) = O_{\{p,q\}}(C)$ and $N/R = \Phi(K/R)$. Observe that $NC/C \leq \Phi(K/C) = C/C$, that is $N \leq C$. Write $\overline{K} = K/N$. The Fitting subgroup $F(\overline{K})$ of $\overline{K}$ has a complement $\overline{T}$ in $\overline{K}$ and $F(\overline{K})$ is a completely reducible and faithful $\overline{T}$-module. Further, $(pq, |F(\overline{K})|) = 1$, $O^{q'}(\overline{T}) = \overline{T}$ and q divides $|\overline{T}|$. By induction, we have

$$\mathrm{Dir}_{j\in J}\, A\Gamma_0^*(r_j^{b_j}) \leq \overline{K} \leq \mathrm{Dir}_{j\in J}\, A\Gamma^*(r_j^{b_j})$$

for a suitable set of indices J and suitable positive integers $b_j \geq 3$ and primes r_j. Write now $\overline{C} = C/N$. Recalling that $\overline{K}/\overline{C} \simeq A\Gamma(2^3) = A\Gamma^*(2^3)$, there must exist a $\tilde{\jmath} \in J$ such that $r_{\tilde{\jmath}}^{b_{\tilde{\jmath}}} = 2^3$ and $\overline{C} \geq \mathrm{Dir}_{j\in J,\, j\neq\tilde{\jmath}}\, A\Gamma_0^*(r_j^{b_j})$. But $\overline{C}$ is supersolvable, while $A\Gamma_0^*(r_j^{b_j})$ is not ($b_j > 1$). It follows that $J = \{\tilde{\jmath}\}$, that is $C = N$ and then $|C| = 2^d p^e q^f$ for suitable integers d, e, f. On the other hand, C is transitive on $V_i \setminus \{1\}$, $i = 1, \ldots, 8$, and hence for every $1 \neq v \in V_i$ we have that $|C : C_C(V_i)| = r^m - 1$ divides $|v^G|$. Therefore, by $P(p, q)$, $(q, r^m - 1) = 1$ and then $r^m - 1 = 2^a p^b$, for suitable integers a, b. But, as m is odd, $r^m - 1$ has a Zsigmondy prime divisor and then such a prime has to be $p = 7$. Hence, m divides 6 and it follows that $m = 3$.

Therefore, $r^3 - 1 = 2^a 7^b$. We claim that this is possible only if $a = 0$. Namely, assume $a > 0$: then r is odd and from the factorization $r^3 - 1 = (r-1)(r^2+r+1)$ it follows that $r^2 + r + 1 = 7^b$ and $r - 1 = 2^a$. Hence r is a Fermat prime and $a = 2^\alpha$ with α a suitable nonnegative integer. If α is even, say $\alpha = 2\beta$, we have $a = 4^\beta \equiv 1 \pmod 3$ and then, for a suitable nonnegative integer γ, $r = 2^a + 1 = 2(2^3)^\gamma + 1 \equiv 2(1^\gamma) + 1 = 3 \pmod 7$. It follows that $7^b \equiv 9 + 3 + 1 \equiv -1 \pmod 7$, a contradiction. If α is odd, we have $a = 2(2)^{\alpha-1} \equiv 2 \pmod 3$ and hence, for a suitable γ, $r = 2^{3\gamma+2} + 1 = 2^2 2^{3\gamma} + 1 \equiv 5 \pmod 7$. We get $7^b = r^2 + r + 1 \equiv 3 \pmod 7$, a contradiction. Hence, we have proved $a = 0$.

Therefore, $r^m - 1 = p^b$ and by [13, Proposition 3.1] it follows that $r = 2$ and $m = 3$.

Hence, G is isomorphic (as a permutation group) to a subgroup of the wreath product $A\Gamma(2^3) \wr A\Gamma(2^3)$. To see that, consider the action of G on the set $\bigcup_{i=1}^8 V_i$ and identify the V_i with $\{(v, i): v \in V\}$, where V is an elementary abelian group of order 8 and $i = 1, \ldots, 8$. Let $H = \mathrm{Stab}_G(V_1)$ and let $\{t_1, t_2, \ldots, t_8\}$ be a right transversal of H in G. Observe that G operates on $\Omega = \{1, 2, \ldots, 8\}$ by the action on the right cosets of H in G and the kernel of this action is $H_G = C$. Recalling that $G/C \simeq A\Gamma(2^3)$, we denote by π: $G \to A\Gamma(2^3)$ the corresponding epimorphism. Recall also that $CC_G(V_1)/C_G(V_1) \simeq C/C_C(V_1)$ is isomorphic to a subgroup of $\Gamma(2^3)$ and it is transitive on $V_i \setminus \{1\}$, so $H/C_G(V_1)$ has a normal cyclic subgroup that acts irreducibly on V_1. Hence, by [13, Theorem 2.1], $\overline{H} = H/C_G(V_1)$ is isomorphic, as a permutation group, to a subgroup of $\Gamma(2^3)$ and then we can embed the semidirect product $V_1\overline{H}$ in $A\Gamma(2^3)$. Since $V_1\overline{H}$ is an epimorphic image of H, by composition we have a homomorphism ϕ: $H \to A\Gamma(2^3)$.

Define ψ: $G \to A\Gamma(2^3) \wr A\Gamma(2^3)$ by $\psi(g) = ((g_1, g_2, \ldots, g_8), \pi(g))$, where $g_i = \phi(t_i g t_{i\pi(g)}^{-1}) \in A\Gamma(2^3)$, $i = 1, \ldots, 8$, and where, by numbering the elements of $\mathrm{GF}(2^3)$, we see that $\pi(g) \in A\Gamma(2^3)$ as a permutation on $\Omega = \{1, 2, \ldots, 8\}$. It is easy to check that ψ is a homomorphism. Furthermore, ψ is injective, as $\ker \pi = C$ and C acts faithfully on $W = V_1 \oplus V_2 \oplus \cdots \oplus V_8$.

We can hence identify G with a subgroup of the group $G^* = A\Gamma(2^3) \wr A\Gamma(2^3)$. We finish the proof by showing that there exists a 2-element $g \in G$ such that $(3, |C_{G^*}(g)|) = 1$.

We can assume, up to conjugation in G^*, that G contains the subgroup $S = A(2^3) \wr A(2^3)$. Namely, S is a 2-Sylow subgroup of G^* and $|G|_2 = |G^*|_2$. Fix an element $u \in A(2^3)$, $u \neq 1$ (we are going to use multiplicative notation in $A(2^3)$). By suitable numbering of the elements in $GF(2^3)$, we can assume that $1,2,3,4$ are a system of representatives for the orbits of u on $\Omega = \{1,\ldots,8\}$. Consider the element $g = ((v_i)_{i=1}^8,\ u) \in S$ where $v_1 = v_2 = v$, for a fixed $v \in A(2^3)$, $v \neq 1$, and $v_j = 1$ for $j = 3,\ldots,8$.

Consider an element $h \in C_{G^*}(g)$ of order 3 and write $h = ((w_i z_i)_{i=1}^8,\ t)$, where $w_i \in A(2^3)$, $z_i \in \Gamma(2^3)$, $t \in A\Gamma(2^3)$. Hence, in particular, t is of order 3. From now on, we shall write for short $h = (w_i z_i,\ t)$, showing only the i-th component in the base group, and the same for the other elements in G^*. We have $hgh^{-1} = (w_i z_i v_{it} z_{iu}^{-1} w_{iu}^{-1},\ tut^{-1})$. Since $g = hgh^{-1}$, it follows that $[u,t] = 1$ and $v_i = w_i v_{it}^{z_i^{-1}} (w_{iu}^{-1})^{z_{iu} z_i^{-1}} z_i z_{iu}^{-1}$. Observing that $w_i v_{it}^{z_i^{-1}} (w_{iu}^{-1})^{z_{iu} z_i^{-1}} \in A(2^3)$ and $z_i z_{iu}^{-1} \in \Gamma(2^3)$, we get $z_i = z_{iu}$ and, recalling that $A(2^3)$ is an elementary abelian 2-group, $v_i = v_{it}^{z_i^{-1}} w_i w_{iu}$, for all $i \in \Omega$. Therefore, we have $v_i v_{it}^{z_i^{-1}} = w_i w_{iu}$ for all $i \in \Omega$ and, writing that relation for $j = iu$, we get also $v_{iu} v_{iut}^{z_{iu}^{-1}} = w_{iu} w_{iu^2} = w_i w_{iu}$. Hence, recalling that $z_i = z_{iu}$, we get the relation

$$\text{(R)} \qquad v_i v_{iu} = (v_{it} v_{itu})^{z_i^{-1}},$$

which holds for all $i \in \Omega$. Observe that, since t and u commute, t acts on the set $\{1^{<u>},\ldots,4^{<u>}\}$ of the $< u >$-orbits on Ω. Since $|t| = 3$, t fixes one of them and cyclically permutes the others. We can hence assume that $1^{<u>}$ is not stabilized by t. Writing (R) for $i = 1, 1t$, we get $v_1 v_{1u} = (v_{1t} v_{1tu})^{z_1^{-1}} = (v_{1t^2} v_{1t^2 u})^{z_{1t}^{-1} z_1^{-1}}$. Since the $< u >$-orbits $1^{<u>}, (1t)^{<u>}, (1t^2)^{<u>}$ are pairwise distinct, at least one among $(1t)^{<u>}$ and $(1t^2)^{<u>}$ is not $2^{<u>}$. Therefore, we get $v_{1t} v_{1tu} = 1$ or $v_{1t^2} v_{1t^2 u} = 1$ by the choice of the v_i. It then follows that $v_1 v_{1u} = v = 1$, a contradiction.

We have hence shown that the 2-element $g \in G$ is not centralized by any 3-element of G^* and then of G. Therefore, we have ruled out the case of imprimitive action of K on the module W and the proof of the necessity of conditions (i) and (ii) is complete.

Conversely, assuming (i) and (ii) we have $\overline{G} \trianglelefteq M$ and, observing that $r_i \neq p$ for all i, by Lemma 6 and Lemma 2, $\overline{G}$ is a $P(p,q)$-group. Further, q divides $|G|$, as the projections of G on the factors of $\overline{G}$ are surjective, and also $O^p(G) = O^{q'}(G) = G$. Hence, G is a $P(p,q)$-group. ∎

Before stating the consequences of Proposition 6, it is convenient to fix some notation:

Definition 3: A group G is said to be a group of type $(*)_{(p,q)}$, where p, q are distinct prime numbers, if there exist positive integers k_i, h_i and primes $r_i \neq p, q$ such that the conditions (i) and (ii) of Proposition 6 hold for $G/\Phi(G)$.

COROLLARY 3: *Let G be a group that satisfies $P(p,q)$ for $p \neq q$ and let $H = O^{q'}(G)$. Then $O_q(G) \leq Z(H)$ and $O_{\{p,q\}}(H)$ is q-nilpotent with abelian q-Sylow subgroups. Further, $H/O_{\{p,q\}}(H)$ is either a group of type $(*)_{(p,q)}$ or 1. In particular, if G is a $P(p,q)$-group then G is a group of type $(*)_{(p,q)}$.*

Proof: By Corollary 2, we have $O_q(G) = O_q(H) \leq Z(H)$. Using the same argument, we have that $O_q(H/O_p(H)) = O_{\{p,q\}}(H/O_p(H))$ so $O_{\{p,q\}}(H)$ is q-nilpotent with abelian q-Sylow subgroups. Suppose $G_0 = H/O_{\{p,q\}}(H) \neq 1$ and let $\overline{G} = G_0/\Phi(G_0)$. Then $F(\overline{G})$ has a complement $\overline{K}$ in $\overline{G}$ and $F(\overline{G})$ is a completely reducible and faithful $\overline{K}$-module. Since $F(\overline{G}) = F(G_0)/\Phi(G_0)$, we have $O_p(\overline{G}) = O_q(\overline{G}) = 1$. Clearly, $O^{q'}(\overline{G}) = \overline{G}$ and hence $\overline{G}$ is a $P(p,q)$-group. Thus, the assertion follows by Proposition 6. ∎

COROLLARY 4: *If, for $p \neq q$, $P(p,q)$ holds in G, then the p-Sylow subgroups of $O^{q'}(G/O_p(G))$ are abelian. In particular, $l_p(O^{q'}(G)) \leq 2$.*

Proof: Observe first that $O^{q'}(G/O_p(G))$ is isomorphic to a subgroup of $T = O^{q'}(G)/O_p(O^{q'}(G))$. By Corollary 3, $T/O_q(T)$ is either 1 or a group of type $(*)_{(p,q)}$ and hence T has abelian p-Sylow subgroups. In particular, if we denote by R the pre-image in G of $O^{q'}(G/O_p(G))$, we have $O^{q'}(G) \leq R$ and hence $l_p(O^{q'}(G)) \leq 2$. ∎

If $P(p,q)$ holds for $p \neq q$ in a non-trivial way in a group G, then the primes p and q have to satisfy some conditions:

COROLLARY 5: *If G has $P(p,q)$ for distinct primes p, q and $O^p(G/O_p(G))$ does not have a central q-Sylow subgroup, then:*

(i) *$q \neq 2$ and q divides $p-1$;*

(ii) *there exist positive integers r, n, h, with r a prime, such that*

$$p^h = (r^{q^n} - 1)/(r^{q^{n-1}} - 1).$$

Proof: Observe that q divides $|O^{q'}(G) : O_{\{p,q\}}(O^{q'}(G))|$. Otherwise since, by Corollary 3, $O_{\{p,q\}}(O^{q'}(G))$ is q-nilpotent, $G/O_p(G)$ has a normal q-Sylow subgroup and then, by Corollary 2, $O^p(G/O_p(G))$ has a central q-Sylow subgroup. Hence, $O^{q'}(G)/O_{\{p,q\}}(O^{q'}(G))$ is a $P(p,q)$-group and the claim follows by Corollary 3. ∎

We now give two examples to show that nothing can be said about the top section $G/O^{q'}(G)$ and the derived length of the Frattini subgroup $\Phi(G)$ of a $P(p,q)$-group G. In fact $G/O^{q'}(G)$ can be isomorphic to any q'-group, as we show in the following example.

Example 1: Let p, q, r be pairwise different primes such that there exists an affine semilinear group $A\Gamma^*(r^k)$ that satisfies $P(p,q)$, and let H be a q'-subgroup of $\mathrm{Sym}(n)$, with n a positive integer. Then there exists a group G such that G satisfies $P(p,q)$ and $G/O^{q'}(G) \cong H$.

Proof: Let $L = A\Gamma^*(r^k)$ and $N = A\Gamma_0^*(r^k)$, where $A\Gamma^*(r^k)$ satisfies $P(p,q)$ (see Lemma 6). Let L^n be the n-fold direct power of L and define the subgroup L_n by

$$L_n = \{(l_1, \dots, l_n) \in L^n \colon l_1 \equiv \cdots \equiv l_n \mod N\}.$$

Equivalently, set $\operatorname{diag} L^n = \{(l, \dots, l) \in L^n \colon l \in L\}$ and $L_n = N^n \operatorname{diag} L^n$. It is easy to see that the $\{p,r\}$-Hall subgroup of L_n is N^n and that $L_n/N^n \cong L/N$ has order q. By the definition of L_n, we know that L_n is $\mathrm{Sym}(n)$-invariant. Therefore we have an induced action of H on L_n, that is if $(x_1, x_2, \dots, x_n)$ is in L_n and σ is in H, then $(x_1, x_2, \dots, x_n)^\sigma = (x_{1\sigma}, x_{2\sigma}, \dots, x_{n\sigma})$ is in L_n. We define $G = L_n H$ and we prove that G satisfies $P(p,q)$. Let $g = (\bar{a}, \sigma)$ be a p'-element of G, where $\bar{a} = (a_1, a_1, \dots, a_n)$ is in L_n. Since a q-Sylow subgroup of G has order q, it is enough to find a q-element $(\bar{c}, 1) \neq 1$ of L_n that centralizes g and this happens if and only if $\bar{c}^{\sigma^{-1}} = \bar{c}^{\bar{a}}$. If q divides $|g|$, then the statement is proved. We can now suppose that g is a q'-element and therefore it belongs to a $\{p,q\}'$-Hall subgroup of $L_n < \sigma >$. We can therefore suppose that a_i is an r-element, for $i = 1, 2, \dots, n$. If $\sigma^{-1} = (m_1 m_2 \cdots m_{i_1})(m_{i_1+1} \cdots m_{i_2}) \cdots (m_{i_{s-1}+1} \cdots m_{i_s})$, we define

$$b_1 = a_{m_1} a_{m_2} \cdots a_{m_{i_1}}, \quad b_2 = a_{m_{i_1+1}} \cdots a_{m_{i_2}}, \quad \dots, \quad b_s = a_{m_{i_{s-1}+1}} \cdots a_{m_{i_s}}.$$

Since b_1 is an r-element of $A\Gamma^*(r^k)$, there exists a q-element c_{m_1} such that $c_{m_1}^{b_1} = c_{m_1}$. We define

$$c_{m_2} = c_{m_1}^{a_{m_1}}, \quad c_{m_3} = c_{m_2}^{a_{m_2}} = c_{m_1}^{a_{m_1} a_{m_2}}, \quad \dots, \quad c_{m_{i_1}} = c_{m_{i_1-1}}^{a_{m_{i_1-1}}} = c_{m_1}^{a_{m_1} a_{m_2} \cdots a_{m_{i_1-1}}}.$$

If we do the same with the other cycles composing σ^{-1}, we can define $\bar{c} = (c_1, \dots, c_n)$ and then $\bar{c}^{\sigma^{-1}} = \bar{c}^{\bar{a}}$ by construction.

Example 2: Let r, p, q be pairwise different primes and h a positive integer such that $(r^q - 1)/(r-1) = p^h$. Then, following the construction given by I. M. Isaacs in [8, Section 4], we can build a group G such that $G/\Phi(G) \simeq A\Gamma^*(r^q)$ and

$dl(F(G)) > \log_2(q-1)$. Further, each element in $F(G)$ is centralized by a q-Sylow subgroup of G (see proof of Theorem 4.9 in [8]; observe also that the condition $q > r$ is replaced here by our assumption $q \neq r$ and $(r^q-1)/(r-1) = p^h$). Hence G is a $P(p,q)$-group. Then, taking for example $(r,q,p,h) = (3,5,11,2)$, we get $dl(F(G)) = 3$ and choosing $(r,q,p,h) = (5,11,12207031,1)$, we get $dl(F(G)) = 4$.

Although we were not able to prove that there exist quadruples (r,q,p,h) for arbitrarily large q, there is some 'experimental' evidence to believe that this should be the case.

ACKNOWLEDGEMENT: We thank the referee for very useful remarks.

References

[1] A. R. Camina, *Arithmetical conditions on the conjugacy class numbers of a finite group*, Journal of the London Mathematical Society (2) **5** (1972), 127–132.

[2] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley, Chichester, 1985.

[3] R. W. Carter, *Conjugacy classes in the Weyl group*, Compositio Mathematica **25** (1972), 1–59.

[4] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[5] S. Dolfi, *Orbits of permutation groups on the power set*, Archiv der Mathematik **75** (2000), 321–327.

[6] B. Huppert, *Research in Representation Theory at Mainz* (1982–1990), Progress in Mathematics, Vol. 95, Birkhäuser Verlag, Basel, 1991, pp. 17–35.

[7] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[8] I. M. Isaacs, *Coprime group actions fixing all nonlinear irreducible characters*, Canadian Journal of Mathematics **41** (1989), 68–82.

[9] N. Jacobson, *Basic Algebra I*, Freeman, New York, 1985.

[10] A. S. Kondrat'ev, *Prime graph components of finite simple groups*, Matematicheskii Sbornik **180** (1989), 787–797 (translated in Mathematics of the USSR **67** (1990), 235–247).

[11] G. Malle, J. Saxl and T. Weigel, *Generation of classical groups*, Geometriae Dedicata **49** (1994), 85–116.

[12] O. Manz and T. Wolf, *Brauer characters of q'-degree in p-solvable groups*, Journal of Algebra **115** (1988), 75–81.

[13] O. Manz and T. Wolf, *Representations of solvable groups*, London Mathematical Society Lecture Notes Series **185**, Cambridge University Press, 1993.

[14] G. Micheler, *A finite simple group of Lie-type has p-blocks with different defects, $p \neq 2$,* Journal of Algebra **104** (1986), 220–230.

[15] G. Navarro, *Characters and blocks of finite groups,* London Mathematical Society Lecture Notes 250, Cambridge University Press, 1998.

[16] D. R. Robinson, *A Course on the Theory of Groups,* Springer-Verlag, Berlin–Heidelberg–New York, 1982.

[17] T. Weigel, *Generation of exceptional groups of Lie type,* Geometriae Dedicata **41** (1992), 63–87.

[18] J. S. Williams, *Prime graph components of finite groups,* Journal of Algebra **69** (1981), 487–513.

[19] K. Zsigmondy, *Zur Theorie der Potenzreste,* Monatshefte für Mathematik und Physik **3** (1892), 265–284.