KERNEL SYSTEMS ON FINITE GROUPS

PAUL LESCOT

Abstract. We introduce a notion of kernel systems on finite groups: roughly speaking, a kernel system on the finite group $G$ consists in the data of a pseudo-Frobenius kernel in each maximal solvable subgroup of $G$, subject to certain natural conditions. In particular, each finite CA-group can be equipped with a canonical kernel system. We succeed in determining all finite groups with kernel system that also possess a Hall $p'$-subgroup for some prime factor $p$ of their order; this generalizes a previous result of ours (Communications in Algebra 18(3), 1990, pp. 833–838). Remarkable is the fact that we make no a priori abelianness hypothesis on the Sylow subgroups.

§0. Introduction

In this paper, we shall define a new class of finite groups, that contains the class of CA-groups, and shall derive (§1) its basic properties. Then, $CN^*$-groups will be defined via an extra hypothesis, and studied(§2). In the case (§3) that there also exists a solvable $p'$-Hall subgroup of the $CN^*$-group $G$ (for some prime $p \in \pi(G)$), we shall obtain a generalization of the main Theorem of [4].

This work was inspired by the conditions stated in p. ix of [1]. I am also much indebted to John Thompson for many enlightening comments on [4], in particular those contained in [6].

The notations are mostly standard; for $G$ a group and $A \subseteq G$, we denote

$$A^2 = A \cap (G \setminus \{1\});$$

for $(x, y) \in G \times G$

$$y^x = x^{-1}yx;$$

and, for $A \subseteq G$ and $x \in G$:

$$A^x = \{y^x | y \in A\}.$$
\( \mathcal{MS}(G) \) denotes the set of maximal solvable subgroups of \( G \). A finite group \( G \) will be termed \( CA \) (resp. \( CN \), \( CS \)) if, for each \( x \in G^a \), the centralizer \( C_G(x) \) is abelian (resp. nilpotent, solvable).

§1. Definition and first properties of kernel systems

Definition 1.1. By a kernel system on the finite group \( G \) we shall mean an application

\[ \mathcal{F} : M \mapsto M_0 = \mathcal{F}(M) \]

from \( \mathcal{MS}(G) \) to \( \mathcal{P}(G) \) such that, for each \( M \in \mathcal{MS}(G) \):

1. \( M_0 \) is a normal subgroup of \( M \),
2. \( \forall a \in M \setminus M_0 \quad C_{M_0}(a) = \{1\} \), and
3. \( \forall g \in G \setminus M \quad M_0 \cap M_0^g = \{1\} \).

On every finite group can be defined a trivial kernel system by:

\[ \forall M \in \mathcal{MS}(G) \quad M_0 = \{1\} \, . \]

More interesting is:

Lemma 1.2. If \( G \) is a \( CA \)-group, then \( G \) possesses a canonical kernel system.

Proof. Let \( G \) be a \( CA \)-group; if \( G \) is solvable then \( \mathcal{MS}(G) = \{G\} \), and (see for example Theorem 1.3 of [4]) \( G \) is either abelian or a Frobenius group with an abelian kernel (let it be \( A \)) that is also a maximal abelian subgroup of \( G \), and a cyclic complement. In the first case, \( G_0 = G \) is suitable; in the second case, \( G_0 = A \) works, thanks to Lemma 1.2 of [4].

We may therefore assume that \( G \) is not solvable; hence it is (non-abelian) simple by the result of [7], p.416. It now follows from Theorem 1.4 of [4] that the elements of \( \mathcal{MS}(G) \) are exactly the \( N_G(A) \), for \( A \) a maximal abelian subgroup of \( G \); setting \( (N_G(A))_0 = A \) for all such \( A \) yields the result, again thanks to Lemma 1.2 of [4].

By a \( KS \)-group we shall mean a pair \( (G, \mathcal{F}) \), with \( G \) a finite group and \( \mathcal{F} \) a kernel system on \( G \). If \( \mathcal{F} \) is clear from (or fixed in) the context, we shall term \( G \) itself a \( KS \)-group. In particular, if \( G \) is a \( CA \)-group, it will be considered as a \( KS \)-group via the canonical kernel system defined in the proof of Lemma 1.2.

In the following three lemmas, let \( G \) be a \( KS \)-group.
Lemma 1.3. Let $M \in \mathcal{MS}(G)$, and let $x \in M_0^\ast$; then $C_G(x) \subseteq M_0$.

Proof. If $a \in C_G(x)$, then $1 \neq x = x^a \in M_0 \cap M_0^a$, whence $a \in M$ by (3). If $a$ would belong to $M \setminus M_0$, then (2) would yield $x \in C_{M_0}(a) = \{1\}$, a contradiction. Therefore $a \in M_0$.

Corollary 1.4. For each $M \in \mathcal{MS}(G)$, $M_0$ is a Hall subgroup of $G$ (and hence of $M$).

Proof. This follows immediately from Lemma 1.3 by using Lemma 1.1 of [4].

Proposition 1.5. ([1], p.x) If $M \in \mathcal{MS}(G)$ and $M_0 \neq M$, then $M_0$ is nilpotent.

Proof. Assume $M_0 \neq M$, and let $q \in \pi(M/M_0)$; then Corollary 1.4 yields that $M_0$ is a $q'$-group. Let $x \in M$ have order $q$; then $x \notin M_0$, whence $C_{M_0}(x) = \{1\}$ by (2). Therefore $M_0$ has a fixed-point-free automorphism of order 1 or $q$ (induced by conjugation by $x$), hence is nilpotent by [5], 12.6.13, p.354 (we do not need Thompson’s Theorem here because we already know that $M_0 \subseteq M$ is solvable).

§2. $CN^*$-groups

Definition 2.1. A $KS$-group will be termed a $CN^*$-group if it satisfies:

(4) $G = \bigcup_{M \in \mathcal{MS}(G)} M_0$, and:

(5) For all $M \in \mathcal{MS}(G)$, $\frac{M}{M_0}$ is a nonidentity cyclic group.

Proposition 2.2. ([1], p.x) Let $G$ be a $KS$-group such that (5) holds and either:

(i) (4) holds (i.e. $G$ is a $CN^*$-group)
or
(ii) $G$ is a $CS$-group.

Then $G$ is a $CN$-group.
Proof. Let \( x \in G^2 \).

In case (i) \( x \) belongs to \( M_0^2 \) for some \( M \in \mathcal{M}(G) \), by (4). By Lemma 1.3, \( C_G(x) \subseteq M_0 \). But \( M_0 \) is nilpotent according to Proposition 1.5 and (5), hence so is \( C_G(x) \).

In case (ii), \( C_G(x) \) is solvable, hence \( C_G(x) \subseteq M \) for some \( M \in \mathcal{M}(G) \). Clearly \( x \in M^2 \); if \( x \in M_0^2 \), then \( C_G(x) \subseteq M_0 \) is nilpotent, as above. If \( x \in M \setminus M_0 \) then

\[
C_G(x) \cap M_0 = C_{M_0}(x) = \{1\}
\]

because of (2), thus \( C_G(x) \) is isomorphic to a subgroup of \( \frac{M}{M_0} \), hence is cyclic and a fortiori nilpotent. \( \square \)

**Lemma 2.3.** Let \( G \) be a \( CN^* \)-group, let \( q \in \pi(G) \), and let \( Q \in Syl_q(G) \); then \( N_G(Q) \in \mathcal{M}(G) \) and \( Q \) is the unique Sylow \( q \)-subgroup of \( N_G(Q)_0 \).

**Proof.** \( Q \neq \{1\} \), therefore by (4) one can find \( M \in \mathcal{M}(G) \) such that

\[
Q \cap M_0 \neq \{1\} ;
\]

let \( x \in Q \cap M_0 \), \( x \neq 1 \). Then, for any \( y \in Z(Q) \), one has \( 1 \neq x = x^y \in M_0 \cap M_0^y \), whence \( y \in M \) by (3), that is \( Z(Q) \subseteq Q \cap M \). Let then \( u \in Z(Q) \), \( u \neq 1 \) be fixed; if \( u \in M \setminus M_0 \), then \( x \in Q \cap M_0 \subseteq C_{M_0}(u) = \{1\} \), a contradiction. Therefore \( u \in M_0^2 \), whence \( Q \subseteq C_G(u) \subseteq M_0 \) by Lemma 1.3. Hence \( Q \) is a Sylow \( q \)-subgroup of \( M_0 \); according to Proposition 1.5, \( Q = O_q(M_0) \triangleleft M \), whence \( M \leq N_G(Q) \).

Let now \( y \in N_G(Q) \); then \( 1 \neq Q \cap M_0 \cap M_0^y \), whence \( y \in M \) by (3). Therefore \( N_G(Q) \subseteq M \), and \( N_G(Q) = M \in \mathcal{M}(G) \). The last part of the statement has already been proved. \( \square \)

**Proposition 2.4.** Let \( G \) be a \( CN^* \)-group, and let \( M \) and \( N \) be two nonconjugate maximal solvable subgroups of \( G \); then \( (|M_0|, |N_0|) = 1 \).

**Proof.** If not, let \( q \in \pi(G) \) divide both \( |M_0| \) and \( |N_0| \), and let \( Q_1 \) and \( Q_2 \) be Sylow \( q \)-subgroups of, respectively, \( M_0 \) and \( N_0 \). \( Q_1 \) is contained in a Sylow \( q \)-subgroup \( Q \) of \( G \), and \( Q_2 \) in a conjugate \( Q^x \) of \( Q \); obviously:

\[
\{1\} \neq Q_1 = Q \cap M_0, \quad \text{and} \quad \{1\} \neq Q_2 = Q^x \cap N_0.
\]

By the reasoning in the proof of Lemma 2.3, \( M = N_G(Q) \) and \( N = N_G(Q^x) \), whence \( N = M^x \). \( \square \)
Lemma 2.5. Let $G$ be a $CN^*$-group, and let $M \in MS(G)$ with $M_0 \neq 1$; then:

(i) $M = N_G(M_0)$, and:

(ii) For each $x \in G$ with $(M^x)_0 \neq \{1\}$, one has:

$$(M^x)_0 = M^x_0.$$ 

Proof.

(i) By (1), $M \subseteq N_G(M_0)$; let $g \in N_G(M_0)$. Then

$$\{1\} \neq M_0 = M^g_0 = M_0 \cap M^g_0$$

whence $g \in M$ by (3) and $N_G(M_0) \subseteq M$; we have shown that $M = N_G(M_0)$.

(ii) Let $Q$ be a Sylow $q$-subgroup of $M^x_0$, $Q \neq 1$; then, according to Lemma 2.3 and its proof,

(*)

$$M = N_G(Q^{x^{-1}}) = (N_G(Q))^{x^{-1}}.$$ 

If $Q \nsubseteq (M^x)_0$, let $u \in Q \setminus (M^x)_0$; then:

$$Z(Q) \cap (Q \cap (M^x)_0) = Z(Q) \cap (M^x)_0 \subseteq C_{(M^x)_0}(u) = \{1\}$$

by (2). But $Q \cap (M^x)_0 \triangleleft Q \cap M^x = Q$, hence $Q \cap (M^x)_0 = \{1\}$. Therefore $Q$ and $(M^x)_0$ are both, according to (*), normal subgroups of $M^x$, thus they centralize one another; let $1 \neq y \in Q$. Then

$$(M^x)_0 = C_{(M^x)_0}(y) = \{1\}$$

by (2), a contradiction. Therefore $Q \subseteq (M^x)_0$; it follows that $M^x_0 \subseteq (M^x)_0$. Applying the same reasoning to $M^x$ and $x^{-1}$ in place of $M$ and $x$ yields $((M^x)_0)^{x^{-1}} \subseteq ((M^x)^{x^{-1}})_0 = M_0$, i.e. $(M^x)_0 \subseteq M^x_0$ and $(M^x)_0 = M^x_0$.

Important is:

Proposition 2.6. Let $G$ be a nonsolvable $CA$-group; then $G$ is a $CN^*$-group.

Proof. This follows, again, from Theorem 1.4 in [4].
§3. The factorizability hypothesis and the main theorem

In this paragraph, we shall assume the following hypothesis:

(\mathcal{H}). \quad G is a nonsolvable CN*-group, p \in \pi(G), and H is a solvable Hall p'-subgroup of G.

Let P be a Sylow p-subgroup of G, and let \( p^n = |P| \).

**Lemma 3.1.** \( C_G(P) = Z(P) \)

**Proof.** By a well-known consequence of Burnside’s \( p \)-nilpotence criterion,

\[ C_G(P) = Z(P) \times D \]

where \( D \) is a \( p' \)-group. Therefore

\[ PC_G(P) = PZ(P)D = PD = P \times D \]

(because \( D \subseteq C_G(P) \)), and

\[ P \times D = (P \times D) \cap G \]
\[ = (P \times D) \cap PH \]
\[ = P[(P \times D) \cap H] \]
\[ = P(D \cap H) \quad (\text{because } H \text{ is a } p' \text{-group}) \]
\[ = P \times (D \cap H) \]

whence \( D = D \cap H : \)

\[ D \subseteq H. \]

The same reasoning applies to each \( P^x (x \in G) \), \( D \) being replaced by \( D^x \); therefore

\[ N = < D^x | x \in G > \subseteq H. \]

Let us assume \( D \neq \{1\} \); then \( N \) is a nonidentity solvable normal \( p' \)-subgroup of \( G \). Let \( N_1 \) be a minimal normal subgroup of \( G \) contained in \( N \); then \( N_1 \) is an elementary abelian \( q \)-group for some prime \( q \neq p \). Let \( Q \) be a Sylow \( q \)-subgroup of \( G \) that contains \( N_1 \); then \( Q \subseteq M_0 \) for some \( M \in \mathcal{M}(G) \), by Lemma 2.3 (in fact \( M = N_G(Q) \)). It follows that, for each \( x \in G \):

\[ \{1\} \neq N_1 = N_1^x \subseteq Q \cap Q^x \subseteq M_0 \cap M_0^x \]

whence \( x \in M \). Therefore \( G = M \) is solvable, a contradiction. Thus \( D = \{1\} \) and \( C_G(P) = Z(P) \times D = Z(P) \).
Corollary 3.2. $N_G(P) \in \mathcal{MS}(G)$ and $P = N_G(P)_0$.

Proof. By Lemma 2.3, $N_G(P) \in \mathcal{MS}(G)$ and $P$ is the unique Sylow $p$-subgroup of the nilpotent group $(N_G(P))_0$; therefore $P \subseteq N_G(P)_0 \subseteq PC_G(P) = P$, whence $P = (N_G(P))_0$.

Lemma 3.3. $H$ is not nilpotent and $H_0 \neq \{1\}$.

Proof. If $H$ were nilpotent, $G = PH$ would be the product of two finite nilpotent groups, hence solvable by a result of Kegel ([3], Satz 2), which is not the case. Therefore $H$ is not nilpotent; but $\frac{H}{H_0}$ is cyclic, hence nilpotent. Thus $H$ and $\frac{H}{H_0}$ are not isomorphic, hence $H_0 \neq \{1\}$.

Proposition 3.4. $H \in \mathcal{MS}(G)$; $H$ and $N_G(P)$ are not conjugate in $G$.

Proof. Let $M \in \mathcal{MS}(G)$ contain $H$; if $p$ would divide $|M_0|$, then for some $x \in G$ one would have $P^x \cap M_0 \neq \{1\}$, whence $M = N_G(P^x)$ by the proof of Lemma 2.3. But then $M$ would contain $P^x H = G$, contradicting the nonsolvability of $G$. Therefore $M_0$ is a $p'$-group. Let $x \in M$ be such that $xM_0$ generate $\frac{M}{M_0}$; if $p$ would divide the order of $x$, then some power $x^k \neq 1$ of $x$ would be a $p$-element, hence belong to some conjugate $P^y$ of $P$, and one would have:

$$x \in C_G(x^k) \subseteq N_G(P^y)_0 = P^y$$

by Lemma 1.3 applied to $x^k$ and $N_G(P^y)$, and Corollary 3.2 applied to $P^y$. Therefore $x$ would be a $p$-element and $\frac{M}{M_0}$ a $p$-group. But

$$\frac{HM_0}{M_0} \simeq \frac{H}{H \cap M_0}$$

is a $p'$-subgroup of $\frac{M}{M_0}$, therefore it would be trivial and $H \subseteq M_0$ would be nilpotent, in contradiction with Lemma 3.3. We have shown that $x$ is a $p'$-element, hence that $\frac{M}{M_0}$ is a $p'$-group; therefore so is $M$, whence $|M|$ divides $|G|_{p'} = |H|$ and

$$H = M \in \mathcal{MS}(G).$$
The second assertion is obvious (and has, in fact, been incidentally proved above).

Remark. This reasoning is adapted from the proof of Step 4 of [4] in an unpublished preliminary version of that paper.

Proposition 3.4 and (5) yield that $\frac{H}{H_0}$ is cyclic; let $h \in H$ be such that $hH_0$ generate $\frac{H}{H_0}$. By (5), $h \neq 1$; (4) implies the existence of $N \in \mathcal{MS}(G)$ such that $h \in N_0^\sharp$.

LEMMA 3.5. $N$ is not conjugate to either $H$ or $N_G(P)$.

Proof. If $N = N_G(P)^x = N_G(P^x)$, then $N_0 = P^x$ by Corollary 3.2 applied to $P^x$, whence $1 \neq h \in P^x \cap H$, a patent contradiction. If $N = H^x$, then $H_0 \neq \{1\}$ by Lemma 3.3 and $(H^x)_0 = N_0 \ni h \neq 1$, and Lemma 2.5 yields $H_0^x = (H^x)_0 = N_0$, whence $1 \neq h \in H_0^x$, i.e. $h^{x^{-1}} \in H_0$. Therefore $\omega(h) = \omega(h^{x^{-1}}) \mid |H_0|$, and

$$\frac{|H}{H_0}| = \omega(hH_0) \mid (\frac{H}{H_0}, |H_0|)$$

which is 1 by Corollary 1.4, thus $\frac{H}{H_0} = \{1\}$, again contradicting Lemma 3.3.

PROPOSITION 3.6. Let $M \in \mathcal{MS}(G)$ with $M_0 \neq \{1\}$; then $M$ is conjugate to $N$, $H$ or $N_G(P)$.

Proof. Let $q$ be a prime divisor of $|M_0|$; if $q = p$, then, for some $y \in G$, $P^y \cap M_0 \neq \{1\}$, and it appears from the proof of Lemma 2.3 that $M = N_G(P^y) = (N_G(P))^y$. If $q \neq p$, then

$$q \mid |G|_{p'} = |H| = \frac{|H}{H_0}| \mid |H_0|.$$  

If now $q \mid |H_0|$, then $(|H_0|, |M_0|) \neq 1$, therefore $M$ is conjugate to $H$ by Proposition 2.4. We are left with the case $q \mid \frac{|H}{H_0}|$, that is $q \mid \omega(hH_0)$; but then $q \mid \omega(h) \mid |N_0|$, whence $(|N_0|, |M_0|) \neq 1$, and now $M$ is conjugate to $N$.  


Corollary 3.7.

$$|G| \leq 1 + |G : N_G(P)||(|P| - 1) + |G : H||(|H_0| - 1) + |G : N||(|N_0| - 1).$$

Proof. By (4), one has

$$G^g = \bigcup_{M \in \mathcal{MS}(G)} M^g^g;$$

if $M \in \mathcal{MS}(G)$ is such that $M_0^g \neq \emptyset$, then, by Proposition 3.6, $M = A^x$ for some $x \in G$ and some $A \in \{N_G(P), H, N\}$. Thus $A_0 \neq \{1\}$ and $M_0 \neq \{1\}$; Lemma 2.5 now shows that $M_0 = A_0^x$, whence $|M_0^g| = |A_0| - 1$. But the total number of conjugates of $A_0$ is $|G : N_G(A_0)| = |G : A|$, also by Lemma 2.5.

From now on, we shall follow very closely the reasoning of [4], pages 836–837.

Lemma 3.8. $|G : N_G(P)| = 1 + \lambda p^n$, for some $\lambda \geq 1$.

Proof. Let $Q = P^y \neq P$ be a conjugate of $P$, and let $M = N_G(P) (\in \mathcal{MS}(G))$. If $P \cap Q \neq \{1\}$ then

$$\{1\} \neq P \cap P^y \subseteq M_0 \cap M_0^y$$

whence, by (3), $y \in M = N_G(P)$ and $Q = P^y = P$, a contradiction. Therefore $P \cap Q = \{1\}$ for any Sylow $p$-subgroup $Q$ of $G$ distinct from $P$.

The congruence

$$|G : N_G(P)| \equiv 1[p^n]$$

now follows by a well-known refinement of Sylow’s Theorem (see [5], 6.5.3, p.147). If $\lambda$ were equal to 0, then $G$ would equal $N_G(P)$ and hence be solvable, an absurdity.

Lemma 3.9. $|N_0| = |H : H_0|$.

Proof. $|N_0|$ divides

$$|G| = |P||H|$$

$$= |P||H_0||H : H_0|$$

$$= |(N_G(P))_0||H_0||H : H_0|.$$

Downloaded from https://www.cambridge.org/core. Réseau National des Bibliothèques de Mathématiques - RNBM, on 18 Jan 2020 at 18:19:58, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/S0027763000007911
By Proposition 2.4 and Lemma 3.5, $|N_0|$ is prime to $|(NG(P))_0|$ and to $|H_0|$, therefore it divides $|H : H_0|$. Conversely $|H : H_0| = \omega(hH_0)$ divides $\omega(h) = |<h>|$, that divides $|N_0|$; thus $|H : H_0| = |N_0|$.

Let us write $k = |H_0|$, $a = |N_0| = |\frac{H}{H_0}| = \omega(hH_0)$, $\delta = |NG(P) : P| = |N_H(P)|$, $\alpha = |N : N_0|$; by (5), $\alpha \geq 2$ and $\delta \geq 2$. Corollary 3.7 gives us:

\[
p^nka \leq 1 + (1 + \lambda p^n)(p^n - 1) + p^n(k - 1) + \frac{p^n k}{\alpha}(a - 1)
\]
\[
= p^n(1 + \lambda(p^n - 1) + k - 1 + \frac{k}{\alpha}(a - 1)),
\]

i.e.:

\[
ka(1 - \frac{1}{\alpha}) \leq k + \lambda(p^n - 1) - \frac{k}{\alpha},
\]

whence:

\[
k(a - 1)(1 - \frac{1}{\alpha}) \leq \lambda(p^n - 1).
\]

But

\[
1 + \lambda p^n = |G : N_G(P)| = \frac{p^nka}{p^n\delta} = \frac{ka}{\delta},
\]

thus:

\[
(**) \quad \frac{ka}{\delta} - k(a - 1)(1 - \frac{1}{\alpha}) \geq 1 + \lambda p^n - \lambda(p^n - 1) = 1 + \lambda \geq 2.
\]

Lemma 3.10. $\delta = 2$.

**Proof.** If $\delta \geq 3$ then $(**)$ yields:

\[
\frac{ka}{3} - k(a - 1)(1 - \frac{1}{\alpha}) \geq 2,
\]

whence:

\[
\frac{ka}{3} - k(\frac{a - 1}{2}) \geq 2, \text{ i.e. :}
\]

\[
\frac{k}{6}(3 - a) \geq 2,
\]
whence $a < 3$. But then $a = 2$ and $|N_0| = 2$. Let $N_0 = \{1, y\}$; it follows from Lemma 1.3 that:

$$N = N_G(N_0) \subseteq C_G(y) \subseteq N_0,$$

whence $N = N_0$, contradicting (5).

**Lemma 3.11.** $\alpha = 2$. 

**Proof.** If $\alpha \geq 3$, then:

$$\frac{ka}{2} = \frac{ka}{\delta} \geq 2 + k(a - 1)(1 - \frac{1}{\alpha}) \geq 2 + k(a - 1)(1 - \frac{1}{3}) \geq \frac{2}{3} k(a - 1),$$

whence:

$$4(a - 1) < 3a,$$

i.e.:

$$a < 4,$$

that is:

$$a \in \{1, 2, 3\}.$$ 

But then $|N_0| \leq 3$; let $N_0 = \langle y \rangle$. Again $C_G(N_0) = C_G(y) \subseteq N_0$, and:

$$\alpha = |N : N_0| \leq |N_G(N_0) : C_G(N_0)| \leq |Aut(N_0)| \leq 2,$$

a contradiction. Therefore $\alpha = 2$. 

**Proposition 3.12.** If $(M, M') \in MS(G)^2$ and $M_0^{\ast} \cap M_0^{\prime \ast} \neq \emptyset$, then $M = M'$. 

**Proof.** From $M_0 \cap M'_0 \neq \{1\}$ follows $(|M_0|, |M'_0|) \neq 1$, therefore Proposition 2.4 implies that $M$ and $M'$ are conjugate. Let $M' = M^x$; as $M_0^{\ast} \neq \emptyset$ and $M_0^{\prime \ast} \neq \emptyset$, $M_0' = M_0^x$ by Lemma 2.5. Then

$$M_0 \cap M_0^{x} = M_0 \cap M_0' \neq \{1\}$$

whence $x \in M$ by (3) and $M' = M^x = M$. 

\[\square\]
Lemma 3.13.

\[ |G| = 1 + |G : N_G(P)||(|P| - 1) + |G : H||(|H_0| - 1) + |G : N||(|N_0| - 1). \]

Proof. One applies the same reasoning as for Corollary 3.7, using Proposition 3.12 and (4).

Proposition 3.14. \( \frac{k}{2} = 1 + \lambda, \) \( p \) is odd and \( p^n - a \) divides \( p^n - 1. \)

Proof. By Lemma 3.10, \( \delta = 2, \) whence

\[ 1 + \lambda p^n = \frac{ka}{\delta} = \frac{ka}{2}. \]

Lemma 3.13 now gives, by using the equality \( \alpha = 2 \) (Lemma 3.11):

\[ p^nka = 1 + \frac{ka}{2}(p^n - 1) + p^n(k - 1) + \frac{1}{2}p^nk(a - 1) \]

i.e.

\[ 0 = 1 - \frac{ka}{2} + p^n(k - 1) - \frac{1}{2}p^nk \]

or

\[ \frac{k}{2}(p^n - a) = p^n - 1. \]

Thus:

\[ \frac{k}{2}p^n - \frac{ka}{2} = p^n - 1. \]

As

\[ 1 + \lambda p^n = \frac{ka}{2}, \]

one has:

\[ (1 + \lambda)p^n = p^n - 1 + 1 + \lambda p^n \]

\[ = \frac{k}{2}p^n - \frac{ka}{2} + \frac{ka}{2} \]

\[ = \frac{k}{2}p^n, \]

i.e.

\[ \frac{k}{2} = 1 + \lambda; \]

in particular, \( k \) is even, therefore \( p \neq 2 \) because \( p \nmid k. \) \(* * * *) \) now becomes:

\[ p^n - 1 = (1 + \lambda)(p^n - a), \]

whence \( p^n - a | p^n - 1. \)
Corollary 3.15. \( a = p^n - 2 \) and \( k = p^n - 1 \).

Proof. \( N \) acts on the set \( \Omega \) of the conjugates of \( N_0 \). If \( N_0^x \in \Omega \) and \( N_0 \cap N_G(N_0^x) \neq \{1\} \), then (cf. Lemma 2.5) \( N_0 \cap N^x \neq \{1\} \). But \( N_0 \) is a Hall subgroup of \( N \) (Corollary 1.4), whence \( N_0 \cap N_0^x \neq \{1\} \); therefore (by (3)) \( x \in N \) and \( N_0^x = N_0 \).

Any orbit of \( N_0 \) on \( \Omega \), other than \( \{N_0\} \), has therefore length \( |N_0| \), whence

\[
|\Omega| = 1[|N_0|],
\]

that is:

\[
|G : N| = 1[|N_0|]
\]

(we have used the fact that

\[
|\Omega| = |G : N_G(N_0)| = |G : N|.
\]

Thus:

\[
a | \frac{p^n k}{\alpha} - 1 = \frac{p^n k}{2} - 1 = p^n(1 + \lambda) - 1.
\]

But \( p^n - 1 = (1 + \lambda)(p^n - a) \) (see the proof of Proposition 3.14), therefore \( a \) divides \( 1 + \lambda p^n \), hence \( a \) divides \( p^n - 2 \). If \( a \neq p^n - 2 \), then \( a \leq \frac{1}{2}(p^n - 2) \), that is \( p^n - a \geq \frac{1}{2}(p^n + 2) > \frac{1}{2}(p^n - 1) \) and Proposition 3.14 gives \( p^n - a = p^n - 1 \), i.e. \( a = 1 \), a contradiction. Thus \( a = p^n - 2 \); but now:

\[
\frac{k}{2}(p^n - 2) = \frac{ka}{2} = 1 + \lambda p^n = 1 + (\frac{k}{2} - 1)p^n
\]

whence \( k = p^n - 1 \).

Theorem 3.16. Under hypothesis \((H)\), one of the following holds:

(i) \( p \) is a Fermat prime \((p = 2^{2m} + 1)\) for some \( m \geq 1 \), and \( G \simeq SL_2(\mathbb{F}_{2^m}) \)

(ii) \( p = 3 \) and \( G \simeq SL_2(\mathbb{F}_8) \).

In both cases, \( H \) is the normalizer of a Sylow 2-subgroup of \( G \).

Proof. \( |H_0| = k \) is even (Proposition 3.14), therefore \( H_0 \) contains an element \( t \) of order 2; by Lemma 1.3, \( C_G(t) \subseteq H_0 \), therefore the number of conjugates of \( t \) under \( H \) is:

\[
|H : C_H(t)| = |H : C_G(t)| \geq |H : H_0| = a = p^n - 2 = k - 1 = |H_0| - 1.
\]
Therefore \( H_0 = \{1\} \cup \{t^x | x \in H\} \) only has elements of order 1 or 2, \textit{i.e.} is a nontrivial elementary abelian 2-group; by Lemma 1.3 it is the centralizer of each of its nonidentity elements, and by Corollary 1.4 it is a Sylow 2-subgroup of \( G \). It follows readily that every element of \( G \) has order 2 or an odd number; as in [4], p.837, one finishes the proof using [2] and the fact that \( G \) is not solvable (the case of the Brauer-Suzuki-Wall that we use should actually be called \textit{Burnside’s Theorem}, a fact of which I was unfortunately unaware while writing [4]). The last assertion follows from Lemma 2.5: \( H = N_G(H_0) \).

\section{Corollaries and remarks}

\textbf{Corollary 4.1.} Let \( G \) be a (non-abelian) simple CA-group containing a solvable Hall \( p' \)-subgroup for some prime \( p \) dividing its order; then either \( p = 3 \) and \( G \) is isomorphic to \( SL_2(F_8) \), or \( p \) is a Fermat prime other than 3 and \( G \) is isomorphic to \( SL_2(F_{p-1}) \).

\textit{Remark.} This is the main Theorem of [4].

\textit{Proof.} By Proposition 2.6, \( G \) satisfies hypothesis (\( H \)), and one may therefore apply Theorem 3.16.

The original motivation for this paper was:

\textbf{Corollary 4.2.} If \( G \) is a minimal counterexample to the Feit-Thompson Theorem that satisfies the conditions listed on p.ix of [1], then there is no prime \( p \in \pi(G) \) such that \( G \) possess a \( p' \)-Hall subgroup.

\textit{Proof.} Our conditions (1) to (5) clearly follow from the conditions listed on p.ix of [1]; if \( G \) would have a Hall \( p' \)-subgroup \( H \), then \( H \) would be solvable(by the minimality of \( G \)), and hypothesis (\( H \)) would be satisfied: Theorem 3.16 would apply. But all the groups that appear in the conclusion of this Theorem have even order.

\textbf{References}


**INSSET, Université de Picardie**
48 Rue Raspail
02100 Saint-Quentin
France
paul.lescot@insset.u-picardie.fr