Rendiconti
del
Seminario Matematico
della
Università di Padova

Andrea Lucchini
Federico Menegazzo

# Generators for finite groups with a unique minimal normal subgroup

*Rendiconti del Seminario Matematico della Università di Padova*, tome 98 (1997), p. 173-191
<http://www.numdam.org/item?id=RSMUP_1997__98__173_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 98 (1997)

# Generators for Finite Groups with a Unique Minimal Normal Subgroup.

ANDREA LUCCHINI (*) - FEDERICO MENEGAZZO (**)

*A Giovanni Zacher nel suo 70° compleanno, con gratitudine*

## Introduction.

Among the many questions involving the minimum number $d(X)$ of generators of a finite group $X$, a very natural one asks for the deduction of $d(G)$ from $d(G/N)$, where $N$ is a minimal normal subgroup of $G$ and some structural information on $G$ is available.

The first relevant information is

$$d(G/N) \leqslant d(G) \leqslant d(G/N) + 1 \tag{1}$$

where the left inequality is trivial, and the right one is the content of [6].

In case $N$ is abelian a complete answer is known; namely $d(G) = d(G/N) + 1$ if and only if $N$ is complemented in $G$ and the number of complements is $|N|^{d(G/N)}$ (see [5]; the above statement can be reformulated in cohomological terms).

If $N$ is non abelian and $G/N$ is cyclic, it follows from (1) that $d(G) = 2$. So the interesting case is when $N$ is non abelian and $d(G/N) \geqslant 2$. An easy way to produce examples of this kind where $d(G) = d(G/N) + 1$ is the following. Fix $d \geqslant 2$; let $S$ be a (non abelian) finite simple group. Choose $m$ such that $S^m$ is $d$-generated, while $S^{m+1}$ is not, and put $G = S^{m+1}$. Then $d(G) = d + 1 > d(G/N) = d$ for every minimal normal subgroup $N$ of $G$ (e.g.: $d = 2$, $S = \mathrm{Alt}(5)$, $m = 19$).

(*) Indirizzo degll'A.: Dipartimento di Elettronica per l'Automazione, Università di Brescia, via Branze, I-25133 Brescia, Italy.

(**) Indirizzo degll'A.: Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova, via Belzoni 7, I-35131 Padova, Italy.

This may be considered an extreme situation. The object of our study is, in some sense, the other extreme; namely, when $G$ has a unique minimal normal subgroup. We prove the following:

THEOREM. *If $G$ is a non cyclic finite group with a unique minimal normal subgroup $N$, then $d(G) = \max(2, d(G/N))$.*

The proof of this theorem uses the classification of finite simple groups. When $N$ is abelian, we use a result of Aschbacher and Guralnick [1] (and we thank the referee for his suggestions). When $N$ is non abelian, our argument depends on the following result, concerning the automorphisms of a simple group:

LEMMA. *Let $S$ be a finite non abelian simple group. There exists a prime $r$ which divides $|S|$ and has the property: for every $y \in \mathrm{Aut}\, S$ there exists an element $x \in S$ such that $|y|_r \neq |yx|_r$.*

(We are using the standard notation: $|g|$ denotes the order of $g$, and if $m$ is a positive integer and $m = r^a k$ with $(r, k) = 1$ then we define $m_r = r^a$).

## 1. - The main theorem.

THEOREM 1.1. *If $G$ is a non cyclic finite group with a unique minimal normal subgroup $N$, then $d(G) = \max(2, d(G/N))$.*

To prove the theorem we need two results concerning the automorphism groups of finite simple groups.

RESULT 1. *Let $S$ be a finite non abelian simple group and identify $S$ with the normal subgroup $\mathrm{Inn}\, S$ of $\mathrm{Aut}\, S$: for every pair $y_1, y_2$ of elements of $\mathrm{Aut}\, S$ there exist $x_1, x_2 \in S$ such that $\langle y_1, y_2, S\rangle = \langle y_1 x_1, y_2 x_2\rangle$.*

RESULT 2. *Let $S$ be a finite non abelian simple group. There exists a prime $r$ which divides $|S|$ and has the property: for every $y \in \mathrm{Aut}\, S$ there exists an element $x \in S$ such that $xy \neq 1$ and, for every integer $m$, coprime with $r$, $y^m$ and $(xy)^m$ are not conjugate in $\mathrm{Aut}\, S$.*

Both these facts can be proved using the classification of the finite simple groups. The proof of the first is in [4], the second is an immediate corollary of the lemma proved in the next section.

PROOF OF THE THEOREM. Suppose that $N$ is abelian. If $N$ lies in the Frattini subgroup, then $d(G) = d(G/N)$. Otherwise $N$ has a complement, $K$ say. The kernel of the action of $K$ on $N$ is a normal subgroup of $G$, so by the uniqueness of $N$ that kernel must be trivial, the action must be faithful. Corollary 1 of [1] now implies that either $d(G) = d(G/N)$ or $d(G/N) \leq 1$; in the latter case $d(G) = 2$.

We now assume that $N$ is a non abelian minimal normal subgroup of $G$, so $N = S^n$, where $S$ is a non abelian simple group; furthermore, the hypothesis that $N$ is the unique minimal normal subgroup of $G$ implies that $G \leq \mathrm{Aut}\, S^n = \mathrm{Aut}\, S \wr \mathrm{Sym}(n)$ (the wreath product of $\mathrm{Aut}\, S$ with the symmetric group of degree $n$). So the elements of $G$ are of the kind $g = (h_1, \ldots, h_n)\sigma$, with $h_i \in \mathrm{Aut}\, S$ and $\sigma \in \mathrm{Sym}(n)$. The map $\pi$: $G \to \mathrm{Sym}(n)$ which sends $g = (h_1, \ldots, h_n)\sigma$ to $\sigma$ is a homomorphism; since $N$ is a minimal normal subgroup of $G$, $G\pi$ is a transitive subgroup of $\mathrm{Sym}(n)$.

To prove the theorem it is useful to define a quasi-ordering relation on the set of the cyclic permutations which belong to the group $\mathrm{Sym}(n)$: let $r$ be the prime number which appears in the statement of Result 2 ($r$ depends on the simple group $S$) and let $\sigma_1, \sigma_2 \in \mathrm{Sym}(n)$ be two cyclic permutations (including cycles of length 1); we define $\sigma_1 \leq \sigma_2$ if either $|\sigma_1|_r \lneqq |\sigma_2|_r$ or $|\sigma_1|_r = |\sigma_2|_r$ and $|\sigma_1| \leq |\sigma_2|$.

Let $d = \max(2, d(G/N))$; there exist $g_1, \ldots, g_d \in G$ such that $G = \langle g_1, \ldots, g_d, N\rangle$. Consider in particular $g_1 = (\alpha_1, \ldots, \alpha_n)\varrho$, $g_2 = (\beta_1, \ldots, \beta_n)\sigma$, with $\alpha_i, \beta_j \in \mathrm{Aut}\, S$ and $\varrho, \sigma \in \mathrm{Sym}(n)$.

We may suppose that $\varrho$ is not a cycle of length $n$. If $\varrho$ is a cycle of length $n$, but $\sigma$ is not, we exchange $g_1$ and $g_2$; if both $\varrho$ and $\sigma$ are cycles of length $n$, there exists $1 \leq i \leq n$ with $1\varrho = 1\sigma^i$ and we substitute $g_1$ by $g_1 g_2^{-i}$. Furthermore if $\varrho$ has no fixed point, but there exist $\bar{g}_1, \ldots, \bar{g}_d \in G$ such that $G = \langle \bar{g}_1, \ldots, \bar{g}_d, N\rangle$ and $\bar{g}_1\pi$ has a fixed point, we change $g_1, \ldots, g_d$ with $\bar{g}_1, \ldots, \bar{g}_d$.

We can write $\varrho = \varrho_1 \ldots \varrho_{s(\varrho)}$ as product of disjoint cycles (including possible cycles of length 1), with $\varrho_1 \leq \varrho_2 \leq \ldots \leq \varrho_{s(\varrho)}$. By our choice of $g_1, \ldots, g_d$, $s(\varrho) \neq 1$ and $|\varrho_1| \neq 1$ if and only if $g\pi$ is fixed-point-free for every $g$ which is contained in a set of $d$ elements which, together with $N$, generate $G$.

Moreover, we write $\sigma = \sigma_1 \ldots \sigma_q \ldots \sigma_{s(\sigma)}$ as product of disjoint cycles in such a way that:

*a)* $\mathrm{supp}(\sigma_i) \cap \mathrm{supp}(\varrho_1) \neq \emptyset$ if and only if $i \leq q$;

*b)* $\sigma_1 \leq \sigma_2 \leq \ldots \leq \sigma_q$.

The strategy of our proof is to find $u, v \in N$ such that $\langle ug_1, vg_2, g_3, \ldots, g_d\rangle = G$; so we will change the automorphisms $\alpha_i$, $\beta_j$

with elements in the same cosets modulo $S$, until we will be able to conclude $\langle g_1, \ldots, g_d \rangle = G$. In the following we will denote with $H$ the subgroup $\langle g_1, \ldots, g_d \rangle$ of $G$.

Let $\varrho_1 = (m_1, \ldots, m_k)$, $\sigma_1 = (n_1, \ldots, n_l)$ with $n_1 = m_1 = m$ and consider $a_1 = \alpha_{m_1} \ldots \alpha_{m_k}$, $b_1 = \beta_{n_1} \ldots \beta_{n_l}$. By Result 1, there exist $x, y \in S$ such that $S \leqslant \langle xa_1, yb_1 \rangle$. If we substitute $\alpha_{m_1}$ with $x\alpha_{m_1}$ and $\beta_{n_1}$ with $y\beta_{n_1}$ we obtain:

$$(1) \qquad S \leqslant \langle a_1, b_1 \rangle .$$

Now, for $j > 1$, let $\varrho_j = (m_{j,1}, \ldots, m_{j,k_j})$ and define $a_j = \alpha_{m_{j,1}} \ldots \alpha_{m_{j,k_j}}$. Since $\varrho_i \leqslant \varrho_j$ if $i \leqslant j$, $|\varrho_1 \ldots \varrho_j| / |\varrho_j|$ is coprime with $r$, but then, by Result 2, there exists $x \in S$ such that $(xa_j)^{|\varrho_1 \cdots \varrho_j|/|\varrho_j|}$ is not conjugate to $a_1^{|\varrho_1 \cdots \varrho_j|/|\varrho_1|}$ in $\mathrm{Aut}\, S$. We substitute $\alpha_{m_{j,1}}$ with $x\alpha_{m_{j,1}}$ and we obtain

(2) for every $2 \leqslant j \leqslant s(\varrho)$,

$$a_j^{|\varrho_1 \cdots \varrho_j|/|\varrho_j|} \text{ and } a_1^{|\varrho_1 \cdots \varrho_j|/|\varrho_1|} \text{ are not conjugate in } \mathrm{Aut}\, S.$$

For any $1 \leqslant i \leqslant n$ denote with $S_i$ the subset of $S^n = N$ consisting of the elements $x = (x_1, \ldots, x_n)$ with $x_j = 1$ for each $j \neq i$. Recall that $G$ is a subgroup of $\mathrm{Aut}\, S^n = \mathrm{Aut}\, S \wr \mathrm{Sym}\,(n)$, a wreath product with base group $B = (\mathrm{Aut}\, S)^n$ and let $\pi_i \colon B \to \mathrm{Aut}\, S$ be the projection on the $i$-th factor. Notice that $g_1^{|\varrho|} \in (\mathrm{Aut}\, S)^n$ with $(g_1^{|\varrho|})\pi_{m_1} = a_1^{|\varrho|/|\varrho_1|}$ and $(g_1^{|\varrho|})\pi_{m_{s(\varrho),1}} = a_{s(\varrho)}^{|\varrho|/|\varrho_{s(\varrho)}|}$. By (2) $a_1^{|\varrho|/|\varrho_1|}$ and $a_{s(\varrho)}^{|\varrho|/|\varrho_{s(\varrho)}|}$ are not conjugate in $\mathrm{Aut}\, S$; in particular this excludes $(g_1^{|\varrho|})\pi_{m_1} = (g_1^{|\varrho|})\pi_{m_{s(\varrho),1}} = 1$ so $g_1^{|\varrho|} \neq 1$. It is also useful to observe that: $g_1^{|\varrho_1|} = (\lambda_1, \ldots, \lambda_n)\varrho^{|\varrho_1|}$ with $\lambda_m = a_1$ and $g_2^{|\sigma_1|} = (\mu_1, \ldots, \mu_n)\sigma^{|\sigma_1|}$ with $\mu_m = b_1$; since $m\varrho^{|\varrho_1|} = m\sigma^{|\sigma_1|} = m$, we deduce that $g_1^{|\varrho_1|}$ and $g_2^{|\sigma_1|}$ normalize $S_m \cong S$ and induce by conjugation the automorphisms $a_1$ and $b_1$.

We have seen that $1 \neq g_1^{|\varrho|} \in H \cap (\mathrm{Aut}\, S)^n$; this implies that $(H \cap (\mathrm{Aut}\, S)^n)\pi_i \neq 1$ for at least one $i$, $1 \leqslant i \leqslant n$; but, since $H\pi = G\pi$ is a transitive subgroup of $\mathrm{Sym}\,(n)$, we conclude: $(H \cap (\mathrm{Aut}\, S)^n)\pi_i \neq 1$ for every $1 \leqslant i \leqslant n$. In particular $(H \cap (\mathrm{Aut}\, S)^n)\pi_m \neq 1$. Now $(H \cap (\mathrm{Aut}\, S)^n)\pi_m$ is a subgroup of $\mathrm{Aut}\, S$ which is normalized by the automorphisms of $S$ induced by conjugation with elements of $N_H(S_m)$: in particular $(H \cap (\mathrm{Aut}\, S)^n)\pi_m$ is a non trivial subgroup of $\mathrm{Aut}\, S$ normalized by $\langle a_1, b_1 \rangle$. Since, by construction, $S \leqslant \langle a_1, b_1 \rangle$, we deduce: $S_m \leqslant (H \cap (\mathrm{Aut}\, S)^n)\pi_m$. Since $\mathrm{Aut}\, S/S$ is solvable, this implies $S_m \leqslant (H \cap S^n)\pi_m$. But then, using again that $H$ acts transitively on $\{S_1, \ldots, S_n\}$, we conclude $(H \cap S^n)\pi_i = S_i$ for every $1 \leqslant i \leqslant n$.

This implies that there exists a partition $\Phi$ of $\{1, \ldots, n\}$ invariant for the action of $G\pi$ such that $H \cap S^n = \prod_{B \in \Phi} D_B$, where, for every block $B \in \Phi$, $D_B$ is a full diagonal subgroup of $\prod_{j \in B} S_j$ (that is, if $B = \{j_1, \ldots, j_t\}$, there exist $\phi_2, \ldots, \phi_t \in \mathrm{Aut}\, S$ such that $D_B = \{(x, x^{\phi_2}, \ldots, x^{\phi_t}) \mid x \in S\} \leq S_{j_1} \times \ldots \times S_{j_t}$). The subgroup $H \cap S^n$ must be normal in $H$; but we will prove that the automorphisms $\alpha_i, \beta_j$ can be chosen so that $\langle g_1, \ldots, g_d \rangle = H$ normalizes $H \cap S^n = \prod_{B \in \Phi} D_B$ only if $|B| = 1$ for all $B \in \Phi$; in other words $\alpha_i, \beta_j$ can be chosen so that $H \cap S^n = S^n$, which implies $H = HS^n = G$. Up to this point, we fixed all the $\alpha_i$'s, and the $\beta_j$'s for $j \in \mathrm{supp}(\sigma_1)$; we can still choose the remaining $\beta_j$'s in their cosets modulo $S$.

Let $B$ be the block of $\Phi$ which contains $m$; the first thing we can prove is:

$$(*) \qquad B \subseteq \mathrm{supp}(\varrho_1).$$

To prove that, suppose, by contradiction, that $h \in B \backslash \mathrm{supp}(\varrho_1)$; let $h = m_{j,t} \in \mathrm{supp}(\varrho_j)$, $j > 1$. We may assume

$$D_B = \{(x, x^{\phi_h}, \ldots) \mid x \in S\} \leq S_m \times S_h \times \ldots$$

Now consider the element $g_1^{|\varrho_1 \cdots \varrho_j|}$; since $(g_1^{|\varrho_1 \cdots \varrho_j|})\pi = \varrho^{|\varrho_1 \cdots \varrho_j|}$ fixes $m$ and $h$, $g_1^{|\varrho_1 \cdots \varrho_j|}$ normalizes $D_B$. But

$$(x, x^{\phi_h}, \ldots)^{g_1^{|\varrho_1 \cdots \varrho_j|}} = (x^{\lambda_m}, x^{\phi_h \lambda_h}, \ldots)$$

with

$$\lambda_m = \alpha_1^{|\varrho_1 \cdots \varrho_j| / |\varrho_1|}$$

and

$$\lambda_h = (\alpha_{m_{j,t}} \cdots \alpha_{m_{j,k_j}} \alpha_{m_{j,1}} \cdots \alpha_{m_{j,t-1}})^{|\varrho_1 \cdots \varrho_j| / |\varrho_j|} =$$

$$= (\alpha_{m_{j,1}} \cdots \alpha_{m_{j,t-1}})^{-1} \alpha_j^{|\varrho_1 \cdots \varrho_j| / |\varrho_j|} (\alpha_{m_{j,1}} \cdots \alpha_{m_{j,t-1}});$$

so if $g_1^{|\varrho_1 \cdots \varrho_j|}$ normalizes $D_B$ then $\lambda_m \phi_h = \phi_h \lambda_h$ which implies

$$\phi_h^{-1} \alpha_1^{|\varrho_1 \cdots \varrho_j| / |\varrho_1|} \phi_h = (\alpha_{m_{j,1}} \cdots \alpha_{m_{j,t-1}})^{-1} \alpha_j^{|\varrho_1 \cdots \varrho_j| / |\varrho_j|} (\alpha_{m_{j,1}} \cdots \alpha_{m_{j,t-1}})$$

in contradiction with (2).

If $\mathrm{supp}(\varrho_1) = 1$, since $B \subseteq \mathrm{supp}(\varrho_1)$, we can conclude $|B| = 1$ and $H \cap N = N$. So, from now on, we may suppose $|\varrho_1| \neq 1$, hence that there does not exist a set $\bar{g}_1, \dots, \bar{g}_d$ of generators for $G$ modulo $N$ such that $\bar{g}_i$ has a fixed point for at least one $1 \leqslant i \leqslant d$.

Let now $\sigma_i = (n_{i,1}, \dots, n_{i,l_i})$, for $2 \leqslant i \leqslant q$, and define $b_i = \beta_{n_{i,1}} \dots \beta_{n_{i,l_i}}$.

Since $\sigma_1 \leqslant \dots \leqslant \sigma_q$, for every $2 \leqslant j \leqslant q$, $|\sigma_1 \dots \sigma_j| / |\sigma_j|$ is coprime with $r$. But then, applying Result 2, we can find $x \in S$ such that $xb_j \neq 1$ and $(xb_j)^{|\sigma_1 \dots \sigma_j| / |\sigma_j|}$ is not conjugate to $b_1^{|\sigma_1 \dots \sigma_j| / |\sigma_1|}$ in $\mathrm{Aut}\, S$. We substitute $\beta_{n_{j,1}}$ with $x\beta_{n_{j,1}}$ and we have:

(3) for every $2 \leqslant j \leqslant q$,

$$\cdot\, b_j^{|\sigma_1 \dots \sigma_j| / |\sigma_j|} \text{ and } b_1^{|\sigma_1 \dots \sigma_j| / |\sigma_1|} \text{ are not conjugate in } \mathrm{Aut}\, S.$$

This enables us to prove:

$$(**) \qquad B \subseteq \mathrm{supp}(\sigma_1).$$

The proof of $(**)$ is similar to that of $(*)$: $B \subseteq \mathrm{supp}(\varrho_1) \subseteq \mathrm{supp}(\sigma_1) \cup \dots \cup \mathrm{supp}(\sigma_q)$. Suppose, by contradiction, that $h \in B \setminus \mathrm{supp}(\sigma_1)$; $h = n_{j,t} \in \mathrm{supp}(\sigma_j)$ with $2 \leqslant j \leqslant q$ and we may assume

$$D_B = \{(x, x^{\phi_h}, \dots) | x \in S\} \leqslant S_m \times S_h \times \dots .$$

Since $g_2^{|\sigma_1 \dots \sigma_j|}$ normalizes $D_B$, we deduce that $b_1^{|\sigma_1 \dots \sigma_j| / |\sigma_1|}$ and $b_j^{|\sigma_1 \dots \sigma_j| / |\sigma_j|}$ must be conjugate in $\mathrm{Aut}\, S$, in contradiction with (3).

A consequence of $(**)$ is

$$(***) \qquad B\varrho \cap \mathrm{supp}(\sigma_1) = \emptyset .$$

In fact, suppose $h \in B\varrho \cap \mathrm{supp}(\sigma_1)$: $h = j\varrho$ for $j \in B \subseteq \mathrm{supp}(\sigma_1)$, so that there exists $i \in \mathbb{Z}$ such that $h = j\sigma_1^i = j\sigma^i$, but then $\varrho\sigma^{-i} = (g_1 g_2^{-i})\pi$ fixes $j$ and $\langle g_1 g_2^{-i}, g_2, \dots, g_d, N \rangle = G$; a contradiction, since we have seen before that an element $g \in G$ cannot be contained in a set of $d$ elements generating $G$ modulo $N$, if $g\pi$ has a fixed point.

Notice that $(**)$ and $(***)$ imply $B \cap B\varrho = \emptyset$.

By $(*)$, $|B| = c$ where $c$ is a divisor of $k = |\varrho_1|$ and $B = \{m_1, m_{k/c+1}, \dots, m_{k(c-1)/c+1}\}$ is the orbit of $m = m_1$ under the action of $\varrho_1^{k/c}$; we will write:

$$D_B = \{(x, x^{\phi_2}, \dots, x^{\phi_c}) | x \in S\} \leqslant S_m \times \dots \times S_{m_{k(c-1)/c+1}} .$$

For every $1 \leqslant i \leqslant c$, let $t_i = k(i-1)/c + 1$; $m_{t_i} \in B \subseteq \mathrm{supp}(\varrho_1) \cap$

$\cap \operatorname{supp}(\sigma_1)$, hence $m_{t_i} = n_{u_i}$ for some $1 \leq u_i \leq l = |\sigma_1|$. Define :

$$\lambda_i = \prod_{t_i \leq j \leq k} \alpha_{m_j} \prod_{1 \leq j \leq t_i - 1} \alpha_{m_j}, \qquad \mu_i = \prod_{u_i \leq j \leq l} \beta_{n_j} \prod_{1 \leq j \leq u_i - 1} \beta_{n_j}.$$

Notice that $g_1^{|\varrho_1|}$ and $g_2^{|\sigma_1|}$ normalize $D_B$; more precisely, for every $(x, x^{\phi_2}, \ldots, x^{\phi_c}) \in D_B$ we have:

$$(x, x^{\phi_2}, \ldots, x^{\phi_c})^{g_1^{|\varrho_1|}} = (x^{\lambda_1}, x^{\phi_2 \lambda_2}, \ldots, x^{\phi_c \lambda_c}),$$

$$(x, x^{\phi_2}, \ldots, x^{\phi_c})^{g_2^{|\sigma_1|}} = (x^{\mu_1}, x^{\phi_2 \mu_2}, \ldots, x^{\phi_c \mu_c}),$$

but then, for every $2 \leq i \leq c$,

$$\lambda_i = \phi_i^{-1} \lambda_1 \phi_i = \phi_i^{-1} a_1 \phi_i, \qquad \mu_i = \phi_i^{-1} \mu_1 \phi_i = \phi_i^{-1} b_1 \phi_i.$$

Since $S \leq \langle a_1, b_1 \rangle$, $C_{\operatorname{Aut} S}(a_1) \cap C_{\operatorname{Aut} S}(b_1) = 1$; so there exists at most a unique $\phi_i \in \operatorname{Aut} S$ satisfying $a_1^{\phi_i} = \lambda_i$ and $b_1^{\phi_i} = \mu_i$. This means that, for every $B \subseteq \operatorname{supp}(\varrho_1) \cap \operatorname{supp}(\sigma_1)$, there is at most a unique possibility for the diagonal $D_B$ to consider. The automorphisms $\phi_2, \ldots, \phi_c$ that describe $D_B$ can be uniquely determined only from the knowledge of $\alpha_i, \beta_j$ for $i \in \operatorname{supp}(\varrho_1)$ and $j \in \operatorname{supp}(\sigma_1)$. For the remaining part of our proof we will not change these automorphisms any more, only we will perhaps modify $\beta_i$ for $i \notin \operatorname{supp}(\sigma_1)$. So for every block $B$ we will consider, there will be at most a unique and completely determined diagonal $D_B$ normalized by $\langle g_1^{|\varrho_1|}, g_2^{|\sigma_1|} \rangle \leq H$.

For a given block $B = \{m, m_{k/c+1}, \ldots, m_{k(c-1)/c+1}\}$ with $|B| = c$ consider now $B\varrho = \{m_2, m_{k/c+2}, \ldots, m_{j_c}\}$, where $j_c = k(c-1)/c + 2$; since $B \neq B\varrho$, $H \cap N = D_B \times D_{B\varrho} \times \ldots$ We have just remarked that $D_B$ is uniquely determined; now we will show that the same holds for $D_{B\varrho}$. We can write

$$D_{B\varrho} = \{(y, y^{\phi_2^*}, \ldots, y^{\phi_c^*}) \mid y \in S\} \leq S_{m_2} \times \ldots \times S_{m_{j_c}}.$$

It must be

$$D_{B\varrho} = (D_B)^{g_1} = \{(x^{\alpha_m}, x^{\phi_2 \alpha_{m_{k/c+1}}}, \ldots, x^{\phi_c \alpha_{m_{k(c-1)/c+1}}}) \mid x \in S\}$$

so $\alpha_m \phi_i^* = \phi_i \alpha_{m_{k(i-1)/c+1}}$ for every $2 \leq i \leq c$. But then also the automorphisms $\phi_i^*$, $2 \leq i \leq c$ and, of consequence, the diagonal $D_{B\varrho}$, will be uniquely determined in the remaining part of our proof.

In the last part of our proof we will modify again the elements $\beta_i$, for $i \notin \operatorname{supp}(\sigma_1)$ in such a way that the stabilizer in $H$ of the block $B\varrho$ could not normalize the corresponding diagonal $D_{B\varrho}$ for any choice of $B \subseteq \operatorname{supp}(\varrho_1) \cap \operatorname{supp}(\sigma_1)$.

For $2 \leq h \leq q$, let $\sigma_h = (n_{h,1}, \ldots, n_{h,l_h})$ and define, for $1 \leq s \leq l_h$,

$$b_{h,s} = \beta_{n_{h,s}} \cdots \beta_{n_{h,l_h}} \beta_{n_{h,1}} \cdots \beta_{n_{h,s-1}}$$

(in particular $b_{h,1} = b_h$).

Let $\sigma_i$ be the cyclic factor of $\sigma$ with $m_2 \in \operatorname{supp}(\sigma_i)$. Consider first the choices for $c$ such that $B = B_c = \{m_2, \ldots, m_{j_c}\}$ with $m_j = m_{j_c} \in \operatorname{supp}(\sigma_i)$; suppose $m_2 = n_{i,p}$, $m_j = n_{i,q}$. The element $g_2^{|\sigma_i|}$ normalizes the diagonal $D_{B\varrho}$ and fixes the coordinates $m_2$ and $m_j$:

$$\{(x, \ldots, x^{\phi_c^*}) \mid x \in S\} = D_{B\varrho} = (D_{B\varrho})^{g_2^{|\sigma_i|}} = \{(x^{b_{i,p}}, \ldots, x^{\phi_c^* b_{i,q}}) \mid x \in S\}$$

but then $b_{i,p}\phi_c^* = \phi_c^* b_{i,q}$, hence $(\phi_c^*)^{-1} b_{i,p} \phi_c^* = b_{i,q}$. Now $b_{i,q}$ is conjugate to $b_i$ and, since $i \neq 1$, by our original choice, $b_i \neq 1$: so $b_{i,q} \neq 1$ and there exists $z \in S$ such that $z^{-1} b_{i,q} z \neq (\phi_c^*)^{-1} b_{i,p} \phi_c^*$; we substitute $\beta_{n_{i,q}}$ with $z^{-1}\beta_{n_{i,q}}$ and $\beta_{n_{i,q-1}}$ with $\beta_{n_{i,q-1}} z$ (where by $n_{i,0}$ we mean $n_{i,l_i}$, $l_i$ being the length of $\sigma_i$). By (***) $n_{i,q-1}, n_{i,q} \notin \operatorname{supp}(\sigma_1)$ so we are not changing $\phi_2, \ldots, \phi_c$ and $\phi_2^*, \ldots, \phi_c^*$ and the diagonals $D_B$, $D_{B\varrho}$ remain determined in the same way; with these modifications we change $b_{i,q}$ with $z^{-1} b_{i,q} z$ but $b_{i,s}$ remains unchanged for every $s \neq q$, so we ensure that $(\phi_c^*)^{-1} b_{i,p} \phi_c^* \neq b_{i,q}$ and that $g_2^{|\sigma_i|}$ cannot normalize $D_{B\varrho}$ (notice also that with these modifications we may substitute $b_i$ with a conjugate but in this way, of course, the property (3) continues to hold).

The arguments above can be repeated for every choice of the divisor $c$ of $k = |\varrho_1|$ for which $m_{j_c} = n_{i,q_c} \in \operatorname{supp}(\sigma_i)$. The crucial remark is that the modifications of the automorphisms $\beta_h$ we introduce in the discussion of one case do not influence the discussion of the other cases: really each time we modify the value of $b_{i,s}$ only for $s = q_c$ and different choices for $c$ produce different values of $j_c$ and $q_c$. Notice also that in this part of our proof the values of $\alpha_t$, $\beta_s$ are relevant only for $t \in \operatorname{supp}(\varrho_1)$ and $s \in \operatorname{supp}(\sigma_1) \cup \operatorname{supp}(\sigma_i)$. In the last part of our proof we will change no more these elements but we can still modify our choices for $\beta_s$ if $s \notin \operatorname{supp}(\sigma_1) \cup \operatorname{supp}(\sigma_i)$.

To conclude the proof it remains to consider the case $B = B_c$, where $c$ is chosen so that $m_{j_c} \notin \operatorname{supp}(\sigma_i)$. So let $c$ be a divisor of $k$ and suppose $m_{j_c} = n_{h,q} \in \operatorname{supp}(\sigma_h)$ with $h \neq i$. It is also $h \neq 1$, since $m_{j_c} \in B\varrho$ and $B\varrho \cap \operatorname{supp}(\sigma_1) = \emptyset$. In this case consider the element $g_2^{|\sigma_h|}$: it fixes $m_j \in B\varrho$, so normalizes $D_{B\varrho}$. But then

$$\{(x, \ldots, x^{\phi_c^*}) \mid x \in S\} = D_{B\varrho} = (D_{B\varrho})^{g_2^{|\sigma_h|}} = \{(x^{\gamma}, \ldots, x^{\phi_c^* b_{h,q}}) \mid x \in S\}$$

where $\gamma$ is uniquely determined and depends only on $\phi_2^*, \ldots, \phi_c^*$ and $\beta_s$ for $s \in \operatorname{supp}(\sigma_i)$ so it is fixed and completely determined at this point of our proof (more precisely: let $m_2 = n^* \sigma_i^{|\sigma_h|}$: $n^* \in B_Q \cap \mathrm{supp}(\sigma_i)$ hence $n^* = m_{kt/c+2}$ for some $0 \leq t \leq c-1$. Consider $g_2^{|\sigma_h|} = (\gamma_1, \ldots, \gamma_n)\sigma^{|\sigma_h|}$ with $\gamma_1, \ldots, \gamma_n \in \mathrm{Aut}\, S$; since $n^* \in \mathrm{supp}(\sigma_i)$ $\gamma_{n^*}$ is a product of the automorphisms $\beta_s$ for $s \in \mathrm{supp}(\sigma_i)$: it results $\gamma = \phi^* \gamma_{n^*}$ where $\phi^* = 1$ if $n^* = m_2$, $\phi^* = \phi^*_{t+1}$ if $n^* = m_{kt/c+2}$ and $t \geq 1$). In particular it must be $b_{h,q} = (\phi_c^*)^{-1} \gamma \phi_c^*$. But $b_{h,q}$ is conjugate to $b_h$ and $b_h \neq 1$ so there exists $z \in S$ such that $z^{-1} b_{h,q} z \neq (\phi_c^*)^{-1} \gamma \phi_c^*$. We substitute $\beta_{n_{h,q}}$ with $z^{-1}\beta_{n_{h,q}}$ and $\beta_{n_{h,q-1}}$ with $\beta_{n_{h,q-1}} z$ (where by $n_{h,0}$ we mean $n_{h,l_h}$, $l_h$ being the length of $\sigma_h$). In this way we change $b_{h,q}$ with $z^{-1} b_{h,q} z$ but the values $b_{t,s}$ remain the same if $(t, s) \neq (h, q)$. This ensures that $g_2^{|\sigma_h|}$ cannot normalize $D_{B_Q}$.

We can repeat this argument for all the divisors $c$ of $k$ for which $m_{j_c} \notin \mathrm{supp}(\sigma_i)$. At each step we modify only some $\beta_s$ for $s \notin \mathrm{supp}(\sigma_1) \cup \cup \mathrm{supp}(\sigma_i)$, so all that we have proved before remains true. Furthermore also in this case the discussion about one possibility for $c$ is independent with the modifications we may introduce discussing the other possibilities: indeed, given a $c$, our modification will change only $b_{h,q}$ for $n_{h,q} = = m_{j_c}$ and to different choices for $c$ correspond different values for $m_{j_c}$ and, of consequence, for $n_{h,q}$.

At this point of the proof we have constructed a set $g_1, \ldots, g_d$ of elements of $G$ such that $H = \langle g_1, \ldots, g_d \rangle$ satisfies:

1) $G = HN$;

2) $H \cap S^n = \prod_{B \in \Phi} D_B$;

3) $H$ normalizes $\prod_{B \in \Phi} D_B$ if and only if $\prod_{B \in \Phi} D_B = N$.

This implies that $H \cap N = N$, hence $G = H$ and $d(G) = d$. ■

## 2. – An auxiliary lemma.

Let $m$ be a positive integer and $r$ a prime number. We define $m_r = r^a$ if $m = r^a k$ with $(r, k) = 1$.

LEMMA. *Let $S$ be a finite non abelian simple group. There exists a prime $r$ dividing $|S|$ with the property: for every $y \in \mathrm{Aut}\, S$ there exists an element $x \in S$ such that $|y|_r \neq |yx|_r$.*

(We note that this lemma immediately implies that every $y \in \mathrm{Aut}\, S$ has fixed points; in fact, if $y$ were fixed-point-free, then all the elements in the coset $yS$ would be conjugate to $y$).

We will prove that the prime $r$ can be chosen in the following way:

1) $r = 2$ if $S$ is an alternating group.
2) $r = 2$ if $S$ is a sporadic simple group.
3) $r = p$ if $S = {}^nL(p^h)$, a group of Lie type over a field of characteristic $p$, with the exception $r = 2$ if $S = A_1(q)$ and $q$ is odd.

In all cases $r$ divides the order of $S$.

We will divide our proof in several steps. Of course it suffices to prove that there exist $x_1, x_2 \in S$ with $|yx_1|_r \neq |yx_2|_r$, in other words we may substitute $y$ with an arbitrary element in the coset $yS$.

2.1. *If $y \in S$ is an inner automorphism then there exists $x \in S$ such that $|y|_r \neq |yx|_r$.*

PROOF. We may assume $y = 1$; since $r$ divides $|S|$ there exists an element $x$ in $S$ with order $r$: $|y|_r = 1$ while $|yx|_r = r$. ■

If $n \neq 6$ then $\mathrm{Aut}(\mathrm{Alt}(n)) = \mathrm{Sym}(n)$ and we have:

2.2. *Let $S = \mathrm{Alt}(n)$, $n \geq 5$ and $n \neq 6$, and $y \in \mathrm{Aut}\, S \setminus S$. There exists $x \in S$ such that $|y|_2 \neq |yx|_2$.*

PROOF. We may assume $y = (1, 2)$. Let $x = (1, 3, 4)$: $|y|_2 = 2$ while $|yx|_2 = |(1, 2, 3, 4)|_2 = 4$. ■

The group $\mathrm{Alt}(6)$ is isomorphic to $A_1(9)$, so it will be considered among the groups of Lie type.

2.3. *Let $S$ be a sporadic simple group and let $y \in \mathrm{Aut}\, S \setminus \mathrm{Inn}\, S$. There exists $x \in S$ such that $|y|_2 \neq |yx|_2$.*

PROOF. Recall that $|\mathrm{Aut}\, S : S| \leq 2$ with $|\mathrm{Aut}\, S : S| = 2$ only in the following cases: $M_{12}, M_{22}, J_2, J_3, HS, Suz, McL, He, O'N, F_{22}, F'_{24}, HN$. In all these cases, consider an element $y \in \mathrm{Aut}\, S \setminus S$; from the character table of these groups (see [2]) it can be easily seen that the coset $yS$ contains both elements of order 2 and elements of order divisible by 4. ■

Before considering the case of groups of Lie type let us recall some properties of these groups.

Let $\Phi$ be a root system corresponding to a simple Lie algebra $L$ over the complex field $\mathbb{C}$, and let us consider a fundamental system $\Pi =$

$= \{a_1, \ldots, a_n\}$ in $\Phi$. A labelling of $\Pi$ can be chosen in such a way that $(a, a) = 2$ and $(a, b) = 0$ for each pair of roots in $\Pi$, with the following exceptions:

$A_n : (a_i, a_{i+1}) = -1$ for $1 \leq i \leq n-1$;

$B_n : (a_1, a_1) = 1, \quad (a_i, a_{i+1}) = -1$ for $1 \leq i \leq n-1$;

$C_n : (a_i, a_i) = 1, \quad (a_i, a_{i+1}) = -\frac{1}{2}$ for $1 \leq i \leq n-2$,

$$(a_{n-1}, a_{n-1}) = -(a_{n-1}, a_n) = 1;$$

$D_n : (a_1, a_3) = (a_i, a_{i+1}) = -1$ for $2 \leq i \leq n-1$;

$E_n : (a_i, a_{i+1}) = (a_{n-3}, a_n) = -1$ for $1 \leq i \leq n-2$;

$F_4 : (a_1, a_1) = (a_2, a_2) = 1, \ (a_1, a_2) = -\frac{1}{2}, \ (a_2, a_3) = (a_3, a_4) = -1$;

$G_2 : (a_1, a_1) = \frac{2}{3}, \quad (a_1, a_2) = -1$.

A Chevalley group $L(q)$, viewed as a group of automorphisms of a Lie algebra $L_K$ over the field $K = \mathrm{F}_q$, obtained from a simple Lie algebra $L$ over the complex field $\mathbb{C}$, is the group generated by certain automorphisms $x_r(t)$, where $t$ runs over $\mathrm{F}_q$ and $r$ runs over the root system $\Phi$ associated to $L$. For each $r \in \Phi$, $X_r = \{x_r(t), t \in \mathrm{F}_q\}$ is a subgroup of $L(q)$ isomorphic to the additive group of the field. $X_r$ is called a root-subgroup.

Let $P = \mathbb{Z}\Phi$ be the additive group generated by the roots in $\Phi$; a homomorphism from $P$ into the multiplicative group $\mathrm{F}_q^*$ will be called an $\mathrm{F}_q$-character of $P$. From each $\mathrm{F}_q$-character $\chi$ of $P$ arises an automorphism $h(\chi)$ of $L(q)$ which maps $x_r(t)$ to $x_r(\chi(r)t)$ and which is called a diagonal automorphism (see [3], p. 98). The diagonal automorphisms form a subgroup $\widehat{H}$ of $\mathrm{Aut}(L(q))$. In the following, to semplify our notation, the same symbol will denote either the character $\chi$ or the element $h(\chi)$ of $\widehat{H}$.

Any automorphism $\sigma$ of the field $\mathrm{F}_q$ induces a field automorphism (still denoted by $\sigma$) of $L(q)$, which is defined in the following way: $(x_r(t))^\sigma = x_r(t^\sigma)$. The set of the field automorphisms of $L(q)$ is a cyclic group $F \simeq \mathrm{Aut}(\mathrm{F}_q)$.

We recall that a symmetry of the Dynkin diagram of $L(q)$ is a permutation $\varrho$ of the nodes of the diagram, such that the number of bonds joining nodes $i$, $j$ is the same as the number of bonds joining nodes $\varrho(i)$, $\varrho(j)$ for any $i \neq j$. A non trivial symmetry $\varrho$ of the Dynkin diagram can be extended to a map of the space $\langle \Phi \rangle$ into itself, we still denote by $\varrho$. This map yields an outer automorphism $\varepsilon$ of $L(q)$; $\varepsilon$ is said to be a graph automorphism of $L(q)$ and maps the root subgroup $X_r$ to $X_{\varrho(r)}$ (see [3] pp. 199-210 for the complete description).

The main result on the automorphism group of a finite non abelian simple group is the following ([3] Th.12.5.1): for each automorphism $\theta \in \in \mathrm{Aut}(L(q))$, there exist an inner automorphism $x$, a diagonal automorphism $h$, a field automorphism $\sigma$ and a graph automorphism $\varepsilon$, such that $\theta = \varepsilon\sigma h x$; moreover, we have the following normal sequence:

$$L(q) \trianglelefteq \langle L(q), \widehat{H} \rangle \trianglelefteq \langle L(q), \widehat{H}, F \rangle \trianglelefteq \mathrm{Aut}\,(L(q))\,.$$

2.4. *Let $S = L(q)$ be a Chevalley group over a field $\mathrm{F}_q$ of characteristic $p$ and suppose $L \neq A_1$. If $y = \sigma h \in \mathrm{Aut}\,S$, with $\sigma \in F$ and $h \in \widehat{H}$, then there exists $x \in S$ with $|yx|_p \neq |y|_p$.*

PROOF. The element $h$ can be modified modulo $H = \widehat{H} \cap S$, in such a way to have $[h, X_a] = 1$ for at least one root $a \in \Phi$. Let $|\sigma| = m$: $\sigma$ normalizes $X_a$ and $\widehat{H}$, so $(\sigma h)^m \in C_{\widehat{H}}(X_a)$; in particular $|(\sigma h)^m|$ divides $q-1$ and is coprime with $p$, so $|\sigma h|_p = m_p$. Now choose $t$ in $\mathrm{F}_q$ such that $u = = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$ (this is always possible) and consider $x = x_a(t)$; $(\sigma h x_a(t))^m = (\sigma h)^m x_a(u)$ has order divisible by $p$ since $p = |x_a(u)|$ and $(\sigma h)^m$ centralizes $x_a(u)$, but then $|\sigma h x|_p = m_p p$. ■

2.5. *Let $S = A_1(q)$ with $\mathrm{F}_q$ a field of characteristic $p$ and let $y \in \in \mathrm{Aut}\,S \backslash S$. Then there exists $x \in S$ such that $|y|_2 \neq |yx|_2$.*

PROOF. In this case $\Pi = \{a\}$ contains only one root and an element $h \in \widehat{H}$ is uniquely determined by the knowledge of $h(a)$: we denote by $h_\xi$ the element of $\widehat{H}$ such that $h(a) = \xi$. It is well known that $h_\xi \in \widehat{H} \cap S$ if and only if $\xi \in (\mathrm{F}_q^*)^2$.

If $p = 2$ then $\widehat{H} \leqslant S$ and we may assume $y = \sigma \in \mathrm{F}_q$. Let $|\sigma| = m$ and choose $t$ in $\mathrm{F}_q$ such that $u = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$. Now consider $x = = x_a(t)$: $(\sigma x)^m = x_a(u)$ so $|\sigma x|_2 = 2|\sigma|_2$.

Suppose $p \neq 2$; since $A_1(q)$ does not possess graph automorphims, we may assume $y = \sigma h$ with $\sigma \in \mathrm{F}_q$ and $h \in \widehat{H}$. Let $m = |\sigma|$ and consider the set $\mathbb{K} = \{x \in \mathrm{F}_q \mid x^{\sigma} = x\}$; $\mathbb{K}$ is a field and $\langle \sigma \rangle$ is the Galois group of $\mathrm{F}_q$ over $\mathbb{K}$; in particular, if we set $|\mathbb{K}| = s$, we have $q = s^m$ and, for every $x \in \mathrm{F}_q$, $x^{\sigma} = x^{s^i}$ with $(i, m) = 1$. We distinguish the different possibilities:

*a)* $m$ is odd.

If $h \in H$, we may assume $h = 1$ and $y = \sigma$. Observe that $X = = \langle x_a(t_1), x_{-a}(t_2) \mid t_1, t_2 \in \mathbb{K} \rangle \cong PSL(2, \mathbb{K})$ is a subgroup of $S$ centralized by $\sigma$. In particular $X$ contains an involution $x$ which is centralized by $\sigma$, so $|yx|_2 = 2$. Suppose $h \notin H$; let $\mathrm{F}_q^* = \langle t \rangle$ and consider $u = t^{(q-1)/(s-1)}$: since $(q-1)/(s-1)$ is an odd integer, $u \notin (\mathrm{F}_q^*)^2$ so we may assume $h = h_u$. Furthermore $(h_u)^\sigma = h_{u^\sigma} = h_u$ so $\sigma$ centralizes $\langle h_u, X \rangle \cong PGL(2, q)$ and the coset $h_u X$ contains an element $h_1$ of order $q-1$ and an element $h_2$ of order $q+1$. But then $|\sigma h_1|_2 = (q-1)_2 \neq (q+1)_2 = |\sigma h_2|_2$.

*b*) $m$ is even.

Let $n = x_r(1)x_{-r}(-1)x_r(1) \in S$. Since $(h_\xi)^\sigma = h_{\xi^\sigma}$, $n^\sigma = n$, $(h_\xi)^n = h_{1/\xi}$ we have: $(\sigma h_\xi)^m = h_\theta$ with $\theta = \xi^{q-1/s-1}$, $(\sigma h_\xi n)^m = h_\eta$ with $\eta = \xi^{(q-1)(s^i-1)/(s^2-1)}$. Let $\mathrm{F}_q^* = \langle t \rangle$. We may assume $y = \sigma h_\xi$ with $\xi = t$ if $h \notin S$, $\xi = t^2$ if $h \in S$. In the first case: $|y|_2 = |\sigma h_t|_2 = m_2(s-1)_2 \neq |yn|_2 = m_2(s+1)_2$. In the second case: $|y|_2 = |\sigma h_{t^2}|_2 = m_2((s-1)/2)_2 \neq |yn|_2 = m_2((s+1)/2)_2$. ■

Now we have to discuss the cases when $y$ involves a graph automorphism $\varepsilon$; if $L = A_n$, $E_6$ or $D_n$ and $\varepsilon$ corresponds to a symmetry $\varrho$ of the Dynkin diagram, we may assume $(x_r(t))^\varepsilon = x_{\varrho(r)}(t)$ for every $r \in \Pi$ ([3] Prop. 12.2.3).

2.6. *Let $S$ be a group of type $A_n$, $n \geq 4$, or $E_6$ over a field $\mathrm{F}_q$ of characteristic $p$ and let $y = \varepsilon\sigma h \in \mathrm{Aut}\, S$ with $\varepsilon$ a graph automorphism, $\sigma \in F$, $h \in \widehat{H}$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

Proof. Let $h_\xi \in \widehat{H}$ where $h_\xi(a_1) = \xi$, $h_\xi(a_i) = 1$ if $i \neq 1$. We may assume $h = h_\xi$ for a suitable $\xi \in \mathrm{F}_q^*$. Let $a = a_2$, $b = a_{n-1}$ and consider the subgroup $X = \langle X_a, X_b \rangle$; if $S \neq A_4(q)$ then $X = X_a \times X_b$, if $S = A_4(q)$ then $X' = X_{a+b}$, $X/X' \cong X_a \times X_b$ and every element of $X$ can be written uniquely in the form $x_a(t_1)x_b(t_2)x_{a+b}(t_3)$ with $t_1, t_2, t_3 \in \mathrm{F}_q$. Let $|\sigma| = m$; take $x = x_a(t)$, with $t$ chosen in such a way that:

*a*) if $m$ is odd, $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$,

*b*) if $m$ is even, $u = t + t^{\sigma^2} + \ldots + t^{\sigma^{2(m/2-1)}} \neq 0$.

Notice that $(\varepsilon\sigma h_\xi x_a(t))^2 = \sigma^2 \widetilde{h}\, x_b(t^\sigma))\, x_a(t)$ where $\widetilde{h}(a_1) = \xi$, $\widetilde{h}(a_n) = \xi^\sigma$, $\widetilde{h}(a_i) = 1$, if $i \notin \{1, n\}$; in particular $\widetilde{h}$ centralizes the subgroup $X$. Consider first the case $m$ odd; $y = \varepsilon\sigma h_\xi$ has order $2m\nu$, where $\nu$ divides $q-1$; but

$$(yx)^{2m} = (\varepsilon\sigma h_\xi x_a(t))^{2m} = (\sigma^2 \widetilde{h}\, x_b(t^\sigma)\, x_a(t))^m =$$

$$= (\sigma^2 \widetilde{h})^m x_b(t^{\sigma^{2m-1}})\, x_a(t^{\sigma^{2(m-1)}}) \ldots x_b(t^{\sigma^3})\, x_a(t^{\sigma^2})\, x_b(t^\sigma)\, x_a(t) =$$

$$= (\sigma^2 \widetilde{h})^m x_a(u)\, x_b(u^\sigma)\, z\,,$$

with $z = 1$ if $S \neq A_4(q)$, $z = x_{a+b}(v)$, $v \in \mathrm{F}_q$, if $S = A_4(q)$; $(\sigma^2 \tilde{h})^m$ centralizes $X$ and $x_a(u) x_b(u^\sigma) z$ is a non trivial element of the $p$-group $X$, so $p$ divides $|(yx)^{2m}|$, hence $|yx|_p \geq |y|_p p$.

Now suppose that $m$ is even; $y = \varepsilon\sigma h_\xi$ has order $m\nu$, where $\nu$ divides $q-1$; $(yx)^m = (\varepsilon\sigma h_\xi x_a(t))^m = (\sigma^2 \tilde{h})^m x_a(u) x_b(u^\sigma) z$, with $z \in X_{a+b}$; again, since $(\sigma^2 \tilde{h})^m$ centralizes $X$ and $x_a(u) x_b(u^\sigma) z \neq 1$, we deduce $|yx|_p \geq |y|_p p$. ■

2.7. *Let $S$ be a group of type $A_3$ over a field $\mathrm{F}_q$ of characteristic $p$ and let $y = \varepsilon\sigma h \in \mathrm{Aut}\, S$ with $\varepsilon$ a graph automorphism, $\sigma \in F$, $h \in \hat{H}$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

PROOF. Distinguish two cases. If $p = 2$ then $\hat{H} \leq S$. So we may assume $h = 1$ and $y = \varepsilon\sigma$. We repeat the argument used for the case $S = A_n$, $n \geq 5$, with $a = a_1$ and $b = a_3$.

Suppose $p \neq 2$. We may assume $h = h_\xi$. Let $|\sigma| = m$ and take $x = x_{a_2}(t)$ with $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$; the order of $y^m = (\varepsilon\sigma h)^m$ divides $2(q-1)$, hence is coprime with $p$, while $(yx)^m = y^m x_{a_2}(u)$ has order divisible by $p$, since $y^m$ centralizes $x_{a_2}(u)$. ■

2.8. *Let $S$ be a group of type $A_2$ over a field $\mathrm{F}_q$ of characteristic $p$ and let $y = \varepsilon\sigma h \in \mathrm{Aut}\, S$ with $\varepsilon$ a graph automorphism, $\sigma \in F$, $h \in \hat{H}$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

PROOF. If 3 does not divide $q-1$, then $\hat{H} \leq S$, so we may assume $y = \varepsilon\sigma$ and repeat the argument used in the case $S = A_4$, with $a = a_1$ and $b = a_2$.

Suppose that 3 divides $q-1$. We will use the symbol $h_{t_1, t_2}$ to denote the element $h \in \hat{H}$ such that $h(a_1) = t_1$, $h(a_2) = t_2$; $h_{t_1, t_2} \in S$ if and only if $t_1 t_2^{-1} \in (\mathrm{F}_q^*)^3$. But then, since in particular $h_{\xi, \xi^{-1}} \in S$ if and only if $\xi \in (\mathrm{F}_q^*)^3$, it is not restrictive to assume $h = h_{\xi, \xi^{-1}}$.

If $|\sigma| = m$ is odd, it can be easily seen that $y = \varepsilon\sigma h_{\xi, \xi^{-1}}$ has order $2m$. Consider $x = x_{a_1}(t)$ and let $\lambda = \xi/\xi^\sigma$: $(\varepsilon\sigma h x_{a_1}(t))^{2m} = (\sigma^2 h_{\lambda, \lambda^{-1}} x_{a_2}(\xi^{-1} t^\sigma) x_{a_1}(t))^m = x_{a_1}(u) x_{a_2}(u_2) x_{a_1+a_2}(u_3)$ with $u = t + \lambda t^{\sigma^2} + \ldots + \lambda\lambda^{\sigma^2} \ldots \lambda^{\sigma^{2(m-2)}} t^{\sigma^{2(m-1)}}$. We may choose $t$ so that $u \neq 0$; in this way $|yx|_p \geq |y|_p p$.

Now suppose that $|\sigma| = m$ is even: choose $t$ such that $u = t - t^\sigma + \ldots + t^{\sigma^{m-2}} - t^{\sigma^{m-1}} \neq 0$ and consider $x = x_{a_1+a_2}(t)$; notice that $h$ centralizes $X_{a_1+a_2}$ and that $x^\varepsilon = x^{-1} = x_{a_1+a_2}(-t)$. This implies that $(\varepsilon\sigma h)^m = \tilde{h} \in C_{\hat{H}}(X_{a_1+a_2})$ and has order coprime with $p$ while $(\varepsilon\sigma h x)^m = \tilde{h} x_{a_1+a_2}(u)$ has order divisible by $p$. ■

2.9. *Let $S$ be a group of type $D_n$ over a field $\mathrm{F}_q$ of characteristic $p$*

*and let* $y = \varepsilon\sigma h \in \operatorname{Aut} S$, *where* $\sigma \in F$, $h \in \widehat{H}$ *and* $\varepsilon$ *is the graph automorphism of order 2 which exchanges* $X_{a_1}$ *and* $X_{a_2}$ *and fixes* $X_{a_i}$ *if* $i \geq 3$. *There exists* $x \in S$ *such that* $|y|_p \neq |yx|_p$.

PROOF. First consider the case $p \neq 2$. Let $|\sigma| = m$ and take $x = x_{a_3}(t)$ with $u = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$; $y = \varepsilon\sigma h$ has order $m\nu$, where $\nu$, dividing $2(q-1)$, is coprime with $p$. Since $\varepsilon$ and $h$ centralize $X_{a_3}$, we obtain $(\varepsilon\sigma hx)^m = \tilde{y}\, x_{a_3}(u)$, with $\tilde{y} \in C_{\operatorname{Aut} S}(X_{a_3})$; but then $p$ divides $|(yx)^m|$ and $|yx|_p \geq m_p p$. Now suppose $p = 2$. In this case $\widehat{H} \leq S$, so we may assume $h = 1$ and $y = \varepsilon\sigma$. If $|\sigma| = m$ is even then $|y| = m$; take $x = x_{a_3}(t)$ with $u = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$; $(yx)^m = x_{a_3}(u)$, hence $|yx| = mp$. If $|\sigma| = m$ is odd then $|y| = 2m$; take $x = x_{a_1}(t)$ with $u = t + t^{\sigma^2} + \ldots + t^{\sigma^{2(m-1)}} \neq 0$; $(yx)^{2m} = (\varepsilon\sigma x_{a_1}(t))^{2m} = (\sigma^2 x_{a_1}(t)\, x_{a_2}(t^{\sigma}))^m = x_{a_1}(u)\, x_{a_2}(u^{\sigma})$ has order $p$, so $|yx| = 2mp$. ∎

2.10. *Let* $S$ *be a group of type* $D_4$ *over a field* $\mathbb{F}_q$ *of characteristic* $p$ *and let* $y = \varepsilon\sigma h \in \operatorname{Aut} S$ *with* $\varepsilon$ *a graph automorphism,* $\sigma \in F$, $h \in \widehat{H}$. *There exists* $x \in S$ *such that* $|y|_p \neq |yx|_p$.

PROOF. Every permutation $\varrho$ on the subset $\{a_1, a_2, a_4\}$ is a symmetry of the Dynkin diagram of $D_4(q)$ and produces a graph automorphism of $S$. We have already discussed the case when $\varrho$ exchanges two roots $a_i$ and $a_j$ and fixes the other. It remains to discuss the case $\varrho = (a_1, a_2, a_4)$. First of all notice that, modifying $h$ modulo $H = \widehat{H} \cap S$, we may assume that one of the following occours:

1) $h(a_1) = 1$ and $h(a_2)^{\sigma} h(a_4) = 1$;
2) $h(a_2) = 1$ and $h(a_4)^{\sigma} h(a_1) = 1$;
3) $h(a_4) = 1$ and $h(a_1)^{\sigma} h(a_2) = 1$.

Choose $a = a_1$ in the first case, $a = a_2$ in the second, $a = a_4$ in the third. Recall ([3] p. 104 and 114) that $U = \langle X_s \mid s \in \phi^+ \rangle$ is a $p$-Sylow subgroup of $S$, $U_1 = \langle X_s \mid s \in \phi^+, s \neq a \rangle$ is a normal subgroup of $U$ with $U = X_a U_1$. Let $|\sigma| = m$; $y$ has order $m^* \nu$, where $\nu$ is a divisor of $q-1$ and $m^* = m$ if 3 divides $m$, $m^* = 3m$ otherwise. Choose $t$ such that $u = t + t^{\sigma^3} + \ldots + t^{\sigma^{3(m^*/3-1)}} \neq 0$ and take $x = x_a(t)$; $(\varepsilon\sigma h x_a(t))^3 = (\varepsilon\sigma h)^3 x_a(t) z = \sigma^3 \tilde{h}\, x_a(t) z$ with $z \in U_1$, $\tilde{h} \in \widehat{H}$ and $\tilde{h}(a) = 1$; $\sigma^3 \tilde{h}$ normalizes $U$ and $U_1$ and $(x_a(t))^{\sigma^3 \tilde{h}} = x_a(t^{\sigma^3})$ so we obtain: $(yx)^{m^*} = (\varepsilon\sigma h x_a(t))^{m^*} = (\sigma^3 \tilde{h}\, x_a(t)\, z)^{m^*/3} = h^* x_a(u) z^*$ with $h^* \in N_{\widehat{H}}(U_1) \cap C_{\widehat{H}}(X_a)$ and $z^* \in U_1$; $x_a(u)$ has order $p$ modulo $U_1$ so we conclude $|yx|_p \geq |y|_p p$. ∎

2.11. *Let* $S$ *be a group of type* $B_2$, $F_4$ *or* $G_2$ *over a field* $\mathbb{F}_q$ *of charac-*

*teristic $p$ with $p = 2$ in the first two cases, $p = 3$ in the third. Let $y \in \operatorname{Aut} S \setminus \langle F, \widehat{H}, S\rangle$; there exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

PROOF. These groups admit a graph automorphism $\varepsilon$ such that $\langle \varepsilon^2 \rangle = F$. Moreover in these cases $\widehat{H} \leq S$, so $\operatorname{Aut} S = \langle \varepsilon, S \rangle$. Therefore we may assume $y \in \langle \varepsilon \rangle$. Since, by hypothesis, $y \notin F = \langle \varepsilon^2 \rangle$, $y$ has even order, say $2m$; $\varepsilon^2 = \sigma$ is a Frobenius automorphism of $S$. Choose $t \in \mathrm{F}_q$ such that $u = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$ and take $x = x_{a_1}(t)$; $(\varepsilon x_{a_1}(t))^2 = \sigma x_{a_1}(t) z$ with $z \in U_1 = \langle X_s \mid s \in \phi^+, s \neq a_1 \rangle$. $X_{a_1}$ normalizes $U_1$, $X_{a_1} \cap U_1 = 1$ and $U = X_{a_1} U_1$ is a $p$-Sylow subgroup of $S$. Since $\sigma$ normalizes $U_1$ we obtain: $(\varepsilon x_{a_1}(t))^{2m} = (\sigma x_{a_1}(t) z)^m = x_{a_1}(u) z^*$ with $z^* \in U_1$, a non trivial element of $U$. ■

To conclude the proof of our lemma it remains to discuss the case of the twisted groups of Lie type. Let us begin with a short description of these groups.

Let $G = L(q)$ be a group of Lie type whose Dynkin diagram has a non trivial symmetry $\varrho$.

If $g$ is the graph automorphism corresponding to $\varrho$, let us suppose that $L(q)$ admits a field automorphism $f$ such that the automorphism $\sigma = gf$ satisfies $\sigma^m = 1$, where $m$ is the order of $\varrho$. If such $\sigma$ does exist, the twisted groups are defined as the subgroup ${}^mL(q)$ of the group $L(q)$ which are fixed elementwise by $\sigma$ [3].

The structure of ${}^mL(q)$ is very similar to that of a Chevalley group: if $\Phi$ is the root-system fixed in $L(q)$, the automorphism $\sigma$ determines a partition of $\Phi = \cup S_i$, [3]. If $R$ is one element of the partition, we denote by $X_R$ the subgroup $\langle X_a, a \in R \rangle$ of $L(q)$, by $X_R^1$ the subgroup $\{x \in X_R, x^{\sigma} = x\}$ of ${}^mL(q)$. The group ${}^mL(q)$ is generated by the groups $X_{R_i}^1$, $\Phi = \cup R_i$; really, the subgroups $X_R^1$ play the role of the root-subgroups. An element $R$ of the partition which contains a simple root is said to be a *simple-set* . We have: $\operatorname{Aut}({}^mL(q)) = \langle {}^mL(q), \widehat{H}^1, F \rangle$, where $F$ is the group of the field automorphisms of $L(q)$ and $\widehat{H}^1 = N_{\widehat{H}}({}^mL(q))$. We observe that in the twisted case, the groups $X_R^1$ are not abelian in general; nevertheless their structure is quite simple and well known (see for example [3] Prop. 13.6.3).

2.12. *Let $S$ be a twisted group of type ${}^2A_n$, $n \geq 3$, or of type ${}^2E_6$ over a field $\mathrm{F} = \mathrm{F}_{q^2}$ of characteristic $p$ and let $y = \sigma h \in \operatorname{Aut} S$ with $\sigma \in F$, $h \in \widehat{H}^1$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

PROOF. First suppose $S = {}^2E_6(q^2)$ or $S = {}^2A_n(q^2)$ with $n \geq 5$ and let $a = a_2$, $b = a_{n-1}$; $R = \{a, b\}$ is a simple set; if we define $x_R(\lambda) = x_a(\lambda) x_b(\lambda^q)$ we have (see [3] p. 233-235) $X_R^1 = \{x_R(\lambda) \mid \lambda \in \mathrm{F}\} \cong (\mathrm{F}, +)$.

Changing $h$ with a suitable element in the coset $h(\widehat{H}^1 \cap S)$, we may assume that $h$ centralizes $X_R^1$ so $(x_R(\lambda))^y = x_R(\lambda^\sigma)$ for every $\lambda \in \mathrm{F}$. Let $|\sigma| = m$; $y = \sigma h$ has order $m\nu$, with $\nu$ coprime with $p$. Take $x = x_R(t)$ with $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$; $(yx)^m = (\sigma h)^m x_R(u)$ has order divisible by $p$ since $|x_R(u)| = p$ and $(\sigma h)^m \in C_{\widehat{H}^1}(X_R)$, hence $|yx|_p \geq |y|_p p$.

Now suppose $n = 4$. Let $a = a_2$, $b = a_3$ and consider the simple set $R = \{a, b, a+b\}$; $X_R^1$ is the set of elements $x_R(\lambda, \mu) = x_a(\lambda) x_b(\lambda^q) x_{a+b}(\mu)$ with $\lambda \in \mathrm{F}$ and $\mu + \mu^q = \lambda\lambda^q$. As in the previuos case it is not restrictive to assume that $h$ centralizes $X_R^1$. If $|\sigma| = m$ then $|y|_p = m_p$; choose $t$ such that $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$ and consider $x = x_R(\lambda, \mu)$ with $\lambda = t$: $(yx)^m = y^m x_R(\lambda^*, \mu^*)$ with $\lambda^* = u$. Since $x_R(\lambda^*, \mu^*)$ is a non trivial element of order a power of $p$ and $y^m$ centralizes $X_R^1$ we conclude $|yx|_p \geq m_p p = |y|_p p$.

Finally suppose $n = 3$. If $q$ is even, then $\widehat{H}^1 \leq S$ and we may assume $y = \sigma$; we can argue as in the case $n \geq 5$, considering the simple set $R = \{a_1, a_3\}$. Suppose $q$ odd. Let $a = a_2$: $R = \{a\}$ is a simple set with $X_R^1 = \{x_a(\lambda^{q+1}) \mid \lambda \in \mathrm{F}_{q^2}\} = \{x_a(\mu) \mid \mu \in \mathrm{F}_q\}$. We may assume that $h$ centralizes $X_R^1$. Now $\sigma \in \mathrm{Aut}(\mathrm{F}_{q^2})$ induces an automorphism $\sigma^*$ of the subfield $\mathrm{F}_q$ of $\mathrm{F}_{q^2}$. Let $|\sigma| = m$ and $|\sigma^*| = m^*$: either $m^* = m$ or $m = 2m^*$. In both cases, since $p$ is odd, $|y|_p = m_p = m_p^*$. But choose $t \in \mathrm{F}_q$ such that $u = t + t^{\sigma^*} + \ldots + t^{\sigma^{*(m^*-1)}} \neq 0$ and take $x = x_a(t)$: $(yx)^{m^*} = (\sigma h x_a(t))^{m^*} = (\sigma h)^{m^*} x_a(u)$ has order divisible by $p$, since $(\sigma h)^{m^*}$ centralizes $x_a(u)$. ■

2.13. *Let $S$ be a twisted group of type ${}^2A_2$ over a field $\mathrm{F} = \mathrm{F}_{q^2}$ of characteristic $p$ and let $y = \sigma h \in \mathrm{Aut}\, S$ with $\sigma \in F$, $h \in \widehat{H}^1$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

PROOF. $R = \{a_1, a_2, a_1 + a_2\}$ is a simple set whose elements have the form $x_R(\lambda, \mu) = x_{a_1}(\lambda) x_{a_2}(\lambda^q) x_{a_1+a_2}(\mu)$ with $\mu + \mu^q = \lambda\lambda^q$. We will use the symbol $h_\xi$ to denote the element of $\widehat{H}^1$ such that $h_\xi(a_1) = \xi$, $h_\xi(a_2) = \xi^q$. For every $h \in \widehat{H}^1$ there exists $\xi \in \mathrm{F}_{q^2}^*$ such that $h = h_\xi$ and $h_\xi \in S$ if and only if $\xi^{q-1} \in (\mathrm{F}_{q^2}^*)^3$.

If 3 does not divide $q + 1$, then $\widehat{H}^1 \leq S$ and we may assume $y = \sigma$. We repeat the same argument as in the case ${}^2A_4(q^2)$ with $a = a_1$, $b = a_2$.

Suppose that 3 divides $q + 1$; since 3 cannot divide $q - 1$, we may assume $h = h_\xi$ with $\xi \in (\mathrm{F}_{q^2}^*)^{q-1}$. Let $|\sigma| = m$: $y = \sigma h$ has order $m\nu$ with $\nu$ coprime with $p$. If $m$ is odd then it is not difficult to see that there exists $t \in \mathrm{F}_{q^2}$ such that $t + t^q = 0$ and $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$. Consider $x = x_R(0, t) = x_{a_1+a_2}(t)$. For every $\mu$, $x_R(0, \mu)^h = x_R(0, \xi^{q+1}\mu) =$

$= x_R(0, \mu)$, so we deduce $(yx)^m = y^m x_R(0, u)$, with $[y^m, x_R(0, u)] = 1$ but then $|yx|_p = |y|_p p$. Suppose that $m$ is even and let $s = |\{x \in \mathbb{F}_{q^2} \,|\, x^\sigma = x\}|$; since $q^2 = s^m$ and $q = -1 \bmod 3$, 3 cannot divide $s - 1$. We may assume $h = h_\xi$ with $|\xi| = 3^j, j \in \mathbb{Z}$. But then $y^m = (\sigma h)^m = hh^\sigma \ldots h^{\sigma^{m-1}} = h_\theta = 1$ since $\theta = \xi\xi^\sigma \ldots \xi^{\sigma^{m-1}} = \xi^{(q^2-1)/(s-1)}$. Now choose $t \in \mathbb{F}^*$ such that $u = t + \xi t^\sigma + \ldots + \xi\xi^\sigma \ldots \xi^{\sigma^{m-2}} t^{\sigma^{m-1}} \neq 0$ and consider $x = x_R(\lambda, \mu)$ with $\lambda = t$. Since $(\sigma h x_R(\lambda, \mu))^m = x_R(\lambda^*, \mu^*)$ with $\lambda^* = u$, we conclude $|yx|_p \geq pm_p = p|y|_p$. ■

2.14. *Let $S$ be a twisted group of type ${}^2D_n$ over a field $\mathbb{F} = \mathbb{F}_{q^2}$ of characteristic $p$ and let $y = \sigma h \in \operatorname{Aut} S$ with $\sigma \in F$, $h \in \widehat{H}^1$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

Proof. If $q$ is even then $\widehat{H}^1 \leq S$ so we may assume $y = \sigma$; $R = \{a_1, a_2\}$ is a simple set and the elements of $X_R^1$ have the form $x_R(\lambda) = x_{a_1}(\lambda)x_{a_2}(\lambda^q)$, $\lambda \in \mathbb{F}_{q^2}$. Let $|\sigma| = m$ and consider $t \in \mathbb{F}_{q^2}$ such that $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$ and take $x = x_R(t)$. Since $(\sigma x_R(t))^m = x_R(u)$, we can conclude as in the other cases. If $q$ is odd, consider the root $a = a_3$: $R = \{a\}$ is a simple set with $X_R^1 = \{x_a(\lambda^{q+1}) \,|\, \lambda \in \mathbb{F}_{q^2}\}$. We may assume that $h$ centralizes $X_R^1$ and use the same arguments as in the case ${}^2A_3(q^2)$, $q$ odd. ■

2.15. *Let $S$ be a twisted group of type ${}^3D_4$ over a field $\mathbb{F} = \mathbb{F}_{q^3}$ of characteristic $p$ and let $y \in \operatorname{Aut} S \backslash S$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

Proof. In these cases $\widehat{H}^1 \leq S$, so we may assume $y = \sigma$. Consider the simple set $R = \{a_1, a_2, a_3\}$; the elements of $X_R^1$ have the form $x_R(\lambda) = x_{a_1}(\lambda)x_{a_2}(\lambda^q)x_{a_3}(\lambda^{q^2})$, $\lambda \in \mathbb{F}$. If $|\sigma| = m$ take $x = x_R(t)$ with $u = t + t^\sigma + \ldots + t^{\sigma^{m-1}} \neq 0$. Since $(\sigma x_R(t))^m = x_R(u)$, we conclude $|yx|_p \geq p|y|_p$. ■

2.16. *Let $S$ be a twisted group of type ${}^2F_4, {}^2B_2, {}^2G_2$ over a field $\mathbb{F} = \mathbb{F}_q$ of characteristic $p$ and let $y \in \operatorname{Aut} S \backslash S$. There exists $x \in S$ such that $|y|_p \neq |yx|_p$.*

Proof. In these cases $\widehat{H}^1 \leq S$, so we may assume $y = \sigma$. Let $R = \{a_1, a_2, a_1 + a_2, 2a_1 + a_2\}$ if $S = {}^2B_2(q)$, $R = \{a_2, a_3, a_2 + a_3, 2a_2 + a_3\}$ if $S = {}^2F_4(q)$, $R = \{a_1, a_2, a_1 + a_2, 2a_1 + a_2, 3a_1 + a_2, 3a_1 + 2a_2\}$ if $S = {}^2G_2(q)$. $R$ is a simple set and the structure of $X_R^1$ is described in [3], Proposition 13.6.3 and 13.6.4; using the same terminology as in [3], the elements of $X_R^1$ can be represented in the form $x_R(t, u)$, with $t, u \in \mathbb{F}$, in the first two cases, in the form $x_R(t, u, v)$, with $t, u, v \in \mathbb{F}$, in the third case. In all these cases there exists an epimorphism $\gamma\colon X_R^1 \to$ $\to (\mathbb{F}, +)$ which maps $x_R(t, u)$, or respectively $x_R(t, u, v)$, to $t$. Choose $t$ such that $u = t + t^{\sigma} + \ldots + t^{\sigma^{m-1}} \neq 0$ and take $x \in X_R^1$ with $\gamma(x) = t$: $(\sigma x)^m = \tilde{x}$ with $\gamma(\tilde{x}) = u$; so $p$ divides $|(\sigma x)^m|$ and $|yx|_p \geq pm_p =$ $= p|y|_p$. ∎

This was the last step, and the Lemma is proved. We shall need the following

COROLLARY. *Let $S$ be a finite non abelian simple group. There exists a prime $r$ which divides $|S|$ and has the property: for every $y \in$ $\in \mathrm{Aut}\, S$ there exists an element $x \in S$ such that $xy \neq 1$ and, for every integer $m$, coprime with $r$, $y^m$ and $(xy)^m$ are not conjugate in* $\mathrm{Aut}\, S$.

PROOF. If $y \notin S$, by the lemma there exists $x \in S$ with $|xy|_r \neq |y|_r$; in particular, for every integer $m$, coprime with $r$, $|(xy)^m|_r \neq |y^m|_r$, so $(xy)^m$ and $y^m$ cannot be conjugate in $\mathrm{Aut}\, S$. Furthermore $xy \neq 1$, otherwise we would deduce $y \in S$. Now let $y \in S$: it suffices to prove that there exists $z \in S$ such that $z \neq 1$ and $z^m$ is not conjugate with $y^m$ in $\mathrm{Aut}\, S$ for every integer $m$ with $(m, r) = 1$. It is enough to consider a non trivial $z \in S$ such that: $|z|_r = 1$ if $|y|_r \neq 1$, $|z|_r \neq 1$ if $|y|_r = 1$. ∎

## REFERENCES


[1] M. ASCHBACHER - R. GURALNICK, *Some applications of the first cohomology group*, J. Algebra, **90** (1984), pp. 446-460

[2] J. H. CONWAY - S. P. NORTON - R. P. PARKER - R. A. WILSON, *Atlas of Finite Groups*, Clarendon Press, Oxford (1985).

[3] R. W. CARTER, *Simple Groups of Lie Type*, J. Wiley and Sons, New York (1972).

[4] F. DALLA VOLTA - A. LUCCHINI, *Generation of almost simple groups*, J. Algebra, **178** (1995), pp. 194-233.

[5] W. GASCHÜTZ, *Die Eulersche Funktion Endlicher Ausflösbarer Gruppen*, Illinois J. Math., 3 (1959), pp. 469-476.

[6] A. LUCCHINI, *Generators and minimal normal subgroups*, Arch. Math., **64** (1995), pp. 273-276.


Manoscritto pervenuto in redazione il 21 novembre 1995
e, in forma revisionata, il 2 aprile 1996.