LE MATEMATICHE
Vol. LXIII (2008) – Fasc. II, pp. 3–18

NILPOTENT GROUPS OF SEMILINEAR TRANSFORMATIONS WHICH ARE MONOMIAL

ANDREA LUCCHINI - M. CHIARA TAMBURINI

Let H be a nilpotent subgroup of $\Gamma L_n(q) = \langle \varphi \rangle \mathrm{GL}_n(q)$, where φ denotes the field automorfism induced by the Frobenius map. We give a condition on the primes dividing $|H \cap \mathrm{GL}_n(q)|$ under which H is conjugate to a subgroup of the generalized monomial group $\langle \varphi \rangle \, \mathrm{Diag}_n(\mathbb{F}_q^*) \, \mathrm{Sym}(n)$. We show an application of this result to the determination of Carter subgroups of finite groups.

1. Introduction

Let $\mathbb{F}$ be a field. For a subgroup T of $\mathbb{F}^*$, we denote by $\mathrm{Diag}_n(T)$ the subgroup of $\mathrm{GL}_n(\mathbb{F})$ consisting of diagonal matrices with entries in T. The product of $\mathrm{Diag}_n(\mathbb{F}^*)$ with the group $\mathrm{Sym}(n)$ of permutation matrices is called the monomial subgroup of $\mathrm{GL}_n(\mathbb{F})$. It is well known that a finite nilpotent group H is an IM group, i.e. every representation of H over an algebraically closed field of characteristic 0 or prime to $|H|$, is monomial [2, Theorem 52.1, page 356]. In particular, if $\mathbb{F}$ is algebraically closed, a finite nilpotent subgroup of $\mathrm{GL}_n(\mathbb{F})$ of order prime to the characteristic (when positive), is conjugate to a subgroup of the monomial group. Clearly this property no longer holds over a finite field. For example a Sylow 2-subgroup of $\mathrm{GL}_2(3)$ has order 2^4, whereas the monomial subgroup has order 2^3. On the other hand, if q is any power of a prime

Entrato in redazione: 26 luglio 2007
AMS 2000 Subject Classification: 20D15, 20G40
Keywords: Nilpotent groups, Carter subgroups

r_0, and p is an odd prime such that $q \equiv 1 \pmod p$, the monomial subgroup of $\mathrm{GL}_n(q)$ contains a Sylow p-subgroup of $\mathrm{GL}_n(q)$. And the same holds for $p = 2$, provided that $q \equiv 1 \pmod 4$. A similar property is still valid in the group $\Gamma L_n(q)$ of semilinear transformations, with respect to a natural generalization of the monomial group. Let φ denote the field automorphism of $\mathrm{GL}_n(q)$ induced by the Frobenius map $\alpha \mapsto \alpha^{r_0}$. Thus $\Gamma L_n(q) = \langle\varphi\rangle \mathrm{GL}_n(q)$. As φ normalizes $\mathrm{Diag}_n(\mathbb{F}_q^*)\,\mathrm{Sym}(n)$, we may consider the product

$$M := \langle\varphi\rangle\,\mathrm{Diag}_n(\mathbb{F}_q^*)\,\mathrm{Sym}(n)$$

and call M the generalized monomial subgroup of $\Gamma L_n(q)$. Under the above hypothesis on p it is still true that M contains a Sylow p-subgroup of $\Gamma L_n(q)$. The main aim of this paper is to prove the following generalization of this fact.

Theorem 1.1. *Let H be a nilpotent subgroup of $\Gamma L_n(q)$ and assume*

$$H\,\mathrm{GL}_n(q) = \langle\psi\rangle\,\mathrm{GL}_n(q)$$

where $\psi \in \langle\varphi\rangle$ and $r = \left|C_{\mathbb{F}_q}(\psi)\right|$. Let $p_1, \ldots, p_t$ be the primes which divide $|H \cap \mathrm{GL}_n(q)|$ and for $j \leq t$ denote by $R_{p_j} = \left(\mathbb{F}_q^*\right)_{p_j}$ the Sylow p_j-subgroup of $\mathbb{F}_q^*$. Suppose that $r \equiv 1 \pmod{p_j}$ for all $j \leq t$, and if $|H \cap \mathrm{GL}_n(q)|$ is even, suppose further that $q \equiv 1 \pmod 4$. Then, for some $g \in \mathrm{GL}_n(q)$:

$$H^g \leq \langle\psi\rangle\,\mathrm{Diag}_n(R_{p_1} \cdots R_{p_t})\,\mathrm{Sym}(n) \leq M.$$

We recall that a Carter subgroup is a nilpotent, selfnormalizing subgroup. It was established long ago that any finite soluble group contains precisely one conjugacy class of such subgroups [1]. And it is reasonable to conjecture that a finite group G can contain at most one conjugacy class of Carter subgroups: for a positive answer we refer to a recent paper of E.P.Vdovin [14]. Our Theorem 1.1 was partly motivated by an application to the proof of this conjecture. Namely, assume by contradiction that the conjecture is false, and let X be a minimal counterexample. Then, by [4], X is an almost-simple group. If H is a Carter subgroup of X, it is easy to see that every subgroup of X containing H is selfnormalizing. Applying this observation to the centralizer of an element $z \in Z(H)$, one gets that no other conjugate of z, under X, can lie in $Z(H)$ [12, Lemma 3.1 (b)]. This argument allows to rule out many classes of almost simple groups from the possible list of minimal counterexamples to the conjugacy conjecture, as done in [12]. On the other hand, when the socle S of X is $\mathrm{PSL}_n(q)$ or $\mathrm{PSU}_n(q)$, for example, this argument breaks down. Our Theorem 1.1 provides an alternative approach, which essentially rules out the almost simple groups with socle $\mathrm{PSL}_n(q)$ from the list, and which can probably be exploited in wider generality. Namely we prove:

Corollary 1.2. *Let* $\mathrm{SL}_n(q) \leq A \leq \Gamma L_n(q)$, *with* $q \equiv 1 \pmod 4$. *Then the projective image of A cannot be a minimal counterexample to the conjugacy conjecture of Carter subgroups.*

If A is as in the statement of the previous Corollary, with q odd, and has a Carter subgroup H of order coprime to q, then H contains a Sylow 2-subgroup of A (see [14]). When $q \equiv 1 \pmod 4$, an inductive argument on n allows to deduce this fact from Theorem 1.1 and our concluding result.

Theorem 1.3. *Let H be a Carter subgroup of* $M_0 = D\langle\psi\rangle\,\mathrm{Sym}(n)$ *where* $D \leq \mathrm{Diag}_n(\mathbb{F}_q^*)$ *is normal in* M_0 *and* $\langle\psi\rangle \leq \langle\varphi\rangle$. *Then H contains a Sylow* 2*-subgroup of* M_0.

2. Notations and basic facts

Let p be a prime. For an integer $z > 1$ we write $z = z_p z_{p'}$ where z_p is a p-power and p does not divide $z_{p'}$. Similarly, for an element g of a group G, we write $g = g_p g_{p'}$ where $g_p \in \langle g\rangle$ has order a p-power and $g_{p'}$ has order prime to p. Finally G_p denotes a Sylow p-subgroup of G. For the reader's convenience we recall some well known facts. In particular, a proof of the following Lemma for p odd is given in [8, Lemma 8.1, page 503].

Lemma 2.1. *Let* $x \in \mathbb{N}$, *with* $x \equiv 1 \pmod p$. *Then, for each* $y \in \mathbb{N}$*:*

i) $(x^y - 1)_p = (x^{y_p} - 1)_p$;

ii) $(x^{y_p} - 1)_p = (x-1)_p\, y_p$ *provided that* $x \equiv 1 \pmod 4$ *if* $p = 2$.

Proof. $i)$ $x^y - 1 = (x^{y_p} - 1)\left(x^{y_p(y_{p'}-1)} + \cdots + x^{y_p} + 1\right)$. As $x \equiv 1 \pmod p$, the second factor is congruent to $y_{p'} \pmod p$. Thus it is not divisible by p.

$ii)$ We set $y_p = p^\alpha$. Our claim is clear when $\alpha = 0$. So let us assume $\alpha > 0$ and put $z = x^{p^{\alpha-1}}$. It follows:

$$x^{p^\alpha} - 1 \;=\; z^p - 1 = (z-1)\left(z^{p-1} + \cdots + 1\right).$$

By induction $(z-1)_p \;=\; (x-1)_p\, p^{\alpha-1}$. From $z \equiv 1 \pmod p$:

$$\left(z^{p-1} + \cdots + 1\right) \;=\; p + \frac{p(p-1)}{2}\,p + kp^2, \quad k \in \mathbb{Z}.$$

Thus, if $p > 2$, we have $\left(z^{p-1} + \cdots + 1\right) \equiv p \pmod{p^2}$. On the other hand, if $p = 2$, we are assuming $x \equiv 1 \pmod 4$. It follows that $z \equiv 1 \pmod 4$, hence $z + 1 \equiv 2 \pmod 4$. In both cases we conclude that $\left(z^{p-1} + \cdots + 1\right)_p = p$. □

As in the Introduction we assume that q is a power of the prime r_0 and that φ is the field automorphism of $\mathrm{GL}_n(q)$ induced by the map $\alpha \mapsto \alpha^{r_0}$.

For a partition $n = n_1 + \cdots + n_\ell$, we set $\Gamma L_{n_j}(q) = \langle\varphi\rangle \mathrm{GL}_{n_j}(q)$, $j \leq \ell$, and identify $(\Gamma L_{n_1}(q) \times \cdots \times \Gamma L_{n_\ell}(q)) \cap \Gamma L_n(q)$ with

$$\langle\varphi\rangle \left(\mathrm{GL}_{n_1}(q) \times \cdots \times \mathrm{GL}_{n_\ell}(q)\right) \tag{1}$$

where

$$\mathrm{GL}_{n_1}(q) \times \cdots \times \mathrm{GL}_{n_\ell}(q) := \left\{ \begin{pmatrix} A_1 & & \\ & \cdots & \\ & & A_\ell \end{pmatrix} \mid A_j \in \mathrm{GL}_{n_j}(q) \right\}. \tag{2}$$

Definition 2.2. We say that a subgroup of $\Gamma L_n(q)$ is indecomposable if it is not conjugate, under $\mathrm{GL}_n(q)$, to a subgroup of (1), for any partition of n with $\ell > 1$.

For each $j \leq \ell$, let us denote by π_j the projection from (1) onto $\Gamma L_{n_j}(q)$.

Lemma 2.3. *Suppose that K is a subgroup of $\Gamma L_n(q)$ contained in* (1) *and set $K\,\mathrm{GL}_n(q) = \langle\varphi^k\rangle \mathrm{GL}_n(q)$. Then, for each $j \leq \ell$:*

i) $\pi_j(K)\,\mathrm{GL}_{n_j}(q) = \langle\varphi^k\rangle \mathrm{GL}_{n_j}(q)$;

ii) $\pi_j(K) \cap \mathrm{GL}_{n_j}(q) \leq \pi_j\left(K \cap \mathrm{GL}_n(q)\right)$.

In particular the primes which divide the order of $\pi_j(K) \cap \mathrm{GL}_{n_j}(q)$ are a subset of those which divide the order of $K \cap \mathrm{GL}_n(q)$.

Proof. *i)* $K = \langle\varphi^k g\rangle \left(K \cap \mathrm{GL}_n(q)\right)$ for some $g \in \mathrm{GL}_n(q)$. As $\langle\varphi\rangle \cap \mathrm{GL}_n(q) = 1$, the assumption that K is contained in (1) implies that $g \in$ (2). Thus $\pi_j(\varphi^k g) = \varphi^k g_j$, for some $g_j \in \mathrm{GL}_{n_j}(q)$.

ii) Take $j = 1$, say, and let $x_1 \in \pi_1(K) \cap \mathrm{GL}_{n_1}(q)$. Choose $y \in K$ such that $y = (x_1, \cdots, x_\ell)$ with $x_j \in \Gamma L_{n_j}(q)$. From $x_1 \in \mathrm{GL}_{n_1}(q)$ it follows easily that $x_j \in \mathrm{GL}_{n_j}(q)$ for all $j \geq 2$. Thus $y \in K \cap \mathrm{GL}_n(q)$. We conclude that $x_1 \in \pi_1\left(K \cap \mathrm{GL}_{n_1}(q)\right)$. □

From now on we fix a factorization $|\varphi| = im$ and set

$$\psi = \varphi^i, \qquad r = \left|C_{\mathbb{F}_q}(\psi)\right|. \tag{3}$$

Thus

$$r = r_0^i, \quad m = |\psi|, \quad q = r^m, \quad \mathbb{F}_r^* = (\mathbb{F}_q^*)^{1+r+\cdots+r^{m-1}}. \tag{4}$$

Lemma 2.4. *Let p be a prime such that $r \equiv 1 \pmod{p}$ and, if $p = 2$ and $|\varphi|$ is odd, assume further that $r_0 \equiv 1 \pmod{4}$. Denote by R_p a Sylow p-subgroup of $\mathbb{F}_q^*$ and by Σ_p a Sylow p-subgroup of* $\mathrm{Sym}(n)$. *Then:*

1) $R_p \leq \mathbb{F}^*_{r^{m_p}}$*;*

2) $\Gamma_p := \langle \psi_p \rangle \operatorname{Diag}_n(R_p)\Sigma_p$ *is a Sylow p-subgroup of* $\langle \psi \rangle \operatorname{GL}_n(q)$*;*

3) $\Gamma_p \ \leq \ \langle \psi \rangle \operatorname{GL}_n(r^{m_p})$*;*

4) Γ_p *is (absolutely) irreducible if and only if n is a power of p.*

Proof. 1) $(q-1)_p = (r^m-1)_p = (r^{m_p}-1)_p$ by point *i*) of Lemma 2.1. 2) We must show that $|GL_n(q)|_p = ((q-1)_p)^n |\Sigma_p|$. In fact

$$|GL_n(q)| \ = \ q^{\frac{n(n+1)}{2}} \prod_{\ell=1}^{n} (q^\ell - 1)$$

and, by Lemma 2.1, $(q^\ell-1)_p = (q^{\ell_p}-1)_p = (q-1)_p \, \ell_p$ for each ℓ. 3) Is an immediate consequence of 1) and 2). 4) Σ_p is transitive on the canonical basis $\{e_1,\ldots,e_n\}$ of $\mathbb{F}_q^n$ only if n is a power of p. So this condition is necessary for the irreducibility of Γ_p. On the other hand, assume that n is a power of p and let $0 \neq W$ be a Γ_p-invariant subspace. Denote by $w = \alpha_1 e_1 + \cdots + \alpha_n e_n$ a non-zero vector in W and assume $\alpha_i \neq 0$. Then there exists a diagonal matrix $d = (\lambda_1,\ldots,\lambda_n) \in \Gamma_p$ with $\lambda_i \neq 1$ and $\lambda_j = 1$ for all $j \neq i$. From $w - dw \in W$, it follows that $e_i \in W$. By the transitivity of Σ_p the canonical basis is contained in W, hence $W = \mathbb{F}_q^n$. □

Definition 2.5. Considering the factorization into distinct primes

$$r-1 \ = \ p_1^{\alpha_1} \cdots \ p_k^{\alpha_k}, \quad \alpha_j > 0 \tag{5}$$

set $R = R_{p_1} \cdots R_{p_k}$ where R_{p_j} denotes the Sylow p_j-subgroup of $\mathbb{F}_q^*$.

Note that $\lambda \in \mathbb{F}_q^*$ and $\lambda^{r-1} \in R$ implies $\lambda \in R$. In fact the primes which divide the order of λ must belong to $\{p_1, \ \ldots, \ p_k\}$.

Lemma 2.6. *For every* $d \in \mathbb{F}_q^*$*, the group* $\langle \psi d \rangle R$ *is a Carter subgroup of* $\langle \psi \rangle \mathbb{F}_q^*$*. In particular* $\langle \psi d \rangle R$ *is conjugate to* $\langle \psi \rangle R$ *under* $\mathbb{F}_q^*$*. Moreover every nilpotent subgroup M of* $\langle \psi \rangle \mathbb{F}_q^*$*, such that* $\langle \psi \rangle \mathbb{F}_q^* = MF_q^*$*, is contained in a Carter subgroup of* $\langle \psi \rangle \mathbb{F}_q^*$*.*

Proof. We fix $p \in \{p_1,\ldots p_k\}$. For every $x \in R_p$ we have: $x^{\psi d} = x^\psi = x^r$. But $x^r \equiv x \pmod{x^p}$, by the assumption $r \equiv 1 \pmod{p}$. Thus ψd centralizes each composition factor of R_p. It follows that $(\psi d)_{p'}$ centralizes R_p. By the same argument, $(\psi d)_p$ centralizes $R_{p'}$. We conclude that $\langle \psi d \rangle R$ is nilpotent.

Now let $N = N_{\langle\psi\rangle\mathbb{F}_q^*}(\langle\psi d\rangle R) = \langle\psi d\rangle\left(N\cap\mathbb{F}_q^*\right)$ and choose $\lambda\in N\cap\mathbb{F}_q^*$. By the definition of N, there exist $\mu\in R$ and $\ell\in\mathbb{N}$ such that:

$$\lambda^{-1}(\psi d)\lambda = (\psi d)^{\ell}\mu.$$

On the other hand $\lambda^{-1}(\psi d)\lambda = (\psi d)\lambda^{1-r}$. Thus $\mu\lambda^{-1+r}\in\langle\psi d\rangle$. In particular $\mu\lambda^{-1+r}\in\mathbb{F}_r^*$ as it is centralized by ψd. Noting that $\mathbb{F}_r^*\leq R$, we have $\lambda^{-1+r}\in R$. Hence $\lambda\in R$, by the observation after Definition 2.5. We conclude that $\langle\psi d\rangle R$ is a Carter subgroup of $\langle\psi\rangle\mathbb{F}_q^*$.

Finally let M be as in the statement. Thus $M = \langle\psi d\rangle\left(M\cap\mathbb{F}_q^*\right)$ for some $d\in\mathbb{F}_q^*$. If p is a prime which divides $|M\cap\mathbb{F}_q^*|$, then $M_p\cap\mathbb{F}_q^*$ is a non-trivial normal subgroup of M_p which gives $Z(M_p)\cap\mathbb{F}_q^*\neq 1$. From $Z(M_p)\leq Z(M)$ centralized by ψd, we deduce that $Z(M_p)\cap\mathbb{F}_q^*$ is centralized by ψ. Thus $Z(M_p)\cap\mathbb{F}_q^*\leq\mathbb{F}_r^*$, whence p divides $r-1$. We conclude that $M\cap\mathbb{F}_q^*\leq R$, which gives $M\leq\langle\psi d\rangle R$. □

Lemma 2.7. *Let $z\in\mathrm{GL}_a(q)$ be a Singer cycle of order q^a-1. Then there exists $\nu\in\mathrm{GL}_a(q)$ such that $\psi\nu$ has order $|\psi|a = ma$ and*

$$N_{\langle\psi\rangle\,\mathrm{GL}_a(q)}(\langle z\rangle) = \langle\psi\nu\rangle\langle z\rangle \quad \textit{with} \quad \langle\psi\nu\rangle\cap\langle z\rangle = 1.$$

Proof. The subalgebra $\langle z\rangle\cup\{0\}$ of $\mathrm{Mat}_a(q)$ can be identified with $\mathbb{F}_{q^a}$. The normalizer in $\Gamma L_n(q)$ of this subalgebra induces a group of automorphisms of $\mathbb{F}_{q^a}$ and the kernel of this action is the centralizer of z. Considering z as a permutation of $\mathbb{F}_{q^a}^*$, it generates an abelian regular group. Thus $\langle z\rangle$ is selfcentralizing in $\mathrm{Sym}(q^a-1)$ and, a fortiori, in $\Gamma L_a(q)$. In particular $\mathbb{F}_q^* I_a\leq\langle z\rangle$. By definition, ψ acts as the identity on $\mathbb{F}_r I_a$. Clearly conjugation by elements of $\mathrm{GL}_a(q)$ induces the identity on $\mathbb{F}_r I_a$. Thus:

$$\frac{N_{\langle\psi\rangle\,\mathrm{GL}_a(q)}(\langle z\rangle)}{\langle z\rangle} \;\leq\; \mathrm{Gal}(\mathbb{F}_{q^a}:\mathbb{F}_r). \tag{6}$$

$\min(z)$ is irreducible over $\mathbb{F}_q$ of degree a. It follows that $\min(z) = \mathrm{char}(z)$. From $\min(z^{\psi}) = \min(z^r)$ we deduce that z^{ψ} is conjugate to z^r. So there exists $\mu\in\mathrm{GL}_a(q)$ such that $z^{\psi\mu} = z^r$, i.e. $\psi\mu$ normalizes $\mathbb{F}_{q^a}$ inducing the automorphism $z\mapsto z^r$. This automorphism generates $\mathrm{Gal}(\mathbb{F}_{q^a}:\mathbb{F}_r)$, which has order ma: thus ma divides $|\psi\mu|$ and in (6) we have an equality. It follows:

$$N_{\langle\psi\rangle\,\mathrm{GL}_a(q)}(\langle z\rangle) \;=\; \langle\psi\mu\rangle\,\langle z\rangle, \quad \left|N_{\langle\psi\rangle\,\mathrm{GL}_a(q)}(\langle z\rangle)\right| \;=\; |z|\,ma. \tag{7}$$

Set $(\psi\mu)^{ma} = z^k$ and note that $z^k\in\mathbb{F}_r I_a$ since it is centralized by $\psi\mu$. By (4), there exists $\ell\in\mathbb{N}$ such that $\left(z^{\ell}\right)^{1+r+\cdots+r^{ma-1}} = z^{-k}$. Thus

$$(\psi\mu\,z^{\ell})^{ma} \;=\; (\psi\mu)^{ma}(z^{\ell})^{1+r+\cdots+r^{ma-1}} \;= z^k z^{-k} \;=\; 1.$$

Setting $\nu = \mu z^{\ell}$, we have $(\psi\nu)^{ma} = 1$ and $\langle\psi\mu\rangle\langle z\rangle = \langle\psi\nu\rangle\langle z\rangle$. We conclude that $\psi\nu$ has order ma and that $\langle\psi\nu\rangle \cap \langle z\rangle = 1$ from (7). □

In particular this Lemma gives $N_{\Gamma L_a(q)}(\langle z\rangle) = \Gamma_1(q^a)$.

3. The main result

The aim of this Section is to prove Theorem 1.1. To this purpose, we fix $h \in H$ such that $\psi^{-1}h \in \mathrm{GL}_n(q)$. Thus:

$$H = \langle h\rangle\,(H \cap \mathrm{GL}_n(q)). \tag{8}$$

Lemma 3.1. *If $|h| = |\psi|$, there exists $x \in \mathrm{GL}_n(q)$ such that $h^x = \psi$.*

Proof. Let $\mathbb{F}$ be the algebraic closure of $\mathbb{F}_q$ and $\Psi : \mathrm{GL}_n(\mathbb{F}) \to \mathrm{GL}_n(\mathbb{F})$ the Frobenius map $\alpha \mapsto \alpha^r$. Thus ψ is the restriction of Ψ to $\mathrm{GL}_n(q)$. Consider the epimorphism $\pi : \langle\Psi\rangle\,\mathrm{GL}_n(q) \;\to\; \langle\psi\rangle\,\mathrm{GL}_n(q)$ defined by

$$\Psi^j y \mapsto \psi^j y, \quad y \in \mathrm{GL}_n(q),\ j \in \mathbb{Z}.$$

By a Theorem of Lang-Steinberg [10], there exists $x \in \mathrm{GL}_n(\mathbb{F})$ such that

$$\psi^{-1}h = g = \Psi^{-1}x\Psi x^{-1}. \tag{9}$$

Thus $x\Psi x^{-1} = \Psi g \mapsto \psi g = h$. Now $h^m = 1$ implies that $(x\Psi x^{-1})^m$ lies in $\mathrm{Ker}\ \pi = \langle\Psi^m\rangle$. It follows that $x\Psi^m x^{-1}\Psi^{-m} \in \mathrm{GL}_n(\mathbb{F}) \cap \langle\Psi\rangle = 1$. We conclude $x \in C_{\mathrm{GL}_n(\mathbb{F})}\Psi^m = \mathrm{GL}_n(q)$. Thus (9) becomes $g = \psi^{-1}x\psi x^{-1}$, whence $h^x = \psi$. □

Lemma 3.2. *In the proof of Theorem* 1.1 *we may assume that $H \cap \mathrm{GL}_n(q)$ is non-scalar.*

Proof. If $H \cap \mathrm{GL}_n(q)$ is scalar, we have:

$$H \cap \mathrm{GL}_n(q) \le (R_{p_1} \cdots R_{p_t})\,I_n.$$

From $h^m \in H \cap \mathrm{GL}_n(q)$ we deduce that $h^m = \lambda I_n$, for some $\lambda \in R_{p_1} \cdots R_{p_t}$. It follows that h^m is centralized by $\psi^{-1}h \in \mathrm{GL}_n(q)$, hence by ψ. This gives $\lambda \in \mathbb{F}_r^*$ and, by (4), there exists $\rho \in \mathbb{F}_q^*$ such that $\rho^{1+r+\cdots+r^{m-1}} = \lambda^{-1}$. Write $o(\rho) = p_1^{\gamma_1} \cdots p_t^{\gamma_t} c$ where $(p_1 \cdots p_t, c) = 1$. Setting $1 = cy_1 + o(\lambda)y_2$ we have

$$(\rho^{1+r+\cdots+r^{m-1}})^{cy_1} = (\lambda^{-1})^{cy_1} = \lambda^{-1}.$$

From $\mathrm{o}(\rho^c) = p_1^{\gamma_1} \cdots p_t^{\gamma_t}$ we deduce that $\mu := \rho^{cy_1} \in R_{p_1} \cdots R_{p_t}$. Moreover:

$$(h\mu)^m = h^m \mu^{1+r+\cdots+r^{m-1}} = \lambda\lambda^{-1} I_n = I_n.$$

By Lemma 3.1, there exists $g \in \mathrm{GL}_n(q)$ such that $(h\mu)^g = \psi$. From $H \leq \langle h, (R_{p_1} \cdots R_{p_t}) I_n \rangle = \langle h\mu, (R_{p_1} \cdots R_{p_t}) I_n \rangle$ we get $H^g \leq \langle \psi, (R_{p_1} \cdots R_{p_t}) I_n \rangle$. □

Lemma 3.3. *Assume that Theorem* 1.1 *is false and let n be the smallest degree for which there exists a counterexample H. Then:*

1) *H is indecomposable;*

2) *if H is chosen so that the number t of prime divisors of its order is minimum with respect to all counterexamples of degree n, every prime p which divides $|H|$ also divides $|H \cap \mathrm{GL}_n(q)|$.*

Proof. 1) If H is decomposable, we can apply Lemma 2.3 with $\ell > 1$ and $K = H^x$, for an appropriate $x \in \mathrm{GL}_n(q)$. By the minimality of n, for each $j \leq \ell$ there exists $g_j \in \mathrm{GL}_{n_j}(q)$ such that

$$(\pi_j(H^x))^{g_j} \leq \langle \psi \rangle \, \mathrm{Diag}_{n_j}(R_{p_1} \cdots R_{p_t}) \, \mathrm{Sym}(n_j).$$

Taking $g = (g_1, \cdots, g_\ell)$ we get $H^{xg} \leq \langle \psi \rangle \, \mathrm{Diag}_n(R_{p_1} \cdots R_{p_t}) \, \mathrm{Sym}(n)$.

2) If p does not divide $|H \cap \mathrm{GL}_n(q)|$, we have $H_p \cap \mathrm{GL}_n(q) = 1$, hence

$$|H_p| = |h_p| = |\psi_p|.$$

By Lemma 3.1, there exists $y \in \mathrm{GL}_n(q)$ such that $h_p^y = \psi_p$. Substituting H with H^y we have that $H_p = \langle \psi_p \rangle$. It follows:

$$H_{p'} \leq C_{\langle \psi \rangle \mathrm{GL}_n(q)}(\psi_p) = \langle \psi_p \rangle \times \langle \psi_{p'} \rangle \, \mathrm{GL}_n\left(C_{\mathbb{F}_q}(\psi_p)\right).$$

Hence $H_{p'} \leq \langle \psi_{p'} \rangle \, \mathrm{GL}_n\left(C_{\mathbb{F}_q}(\psi_p)\right)$. By the minimality of t, there exists $g \in \mathrm{GL}_n(C_{\mathbb{F}_q}(\psi_p))$ such that $H_{p'}^g \leq \langle \psi_{p'} \rangle \, \mathrm{Diag}_n(R_{p_1} \cdots R_{p_t})) \, \mathrm{Sym}(n)$. Noting that g centralizes ψ_p, we have that H satisfies Theorem 1.1. As this fact contradicts our assumptions, we conclude that p divides $|H \cap \mathrm{GL}_n(q)|$. □

Proof. (*Theorem* 1.1).

Assume that Theorem 1.1 is false and let n, H and t be such that points 1) and 2) of Lemma 3.3 hold. By Lemma 2.4, $t > 1$, and by Lemma 3.2, there exists a non-scalar Sylow p-subgroup P of $H \cap \mathrm{GL}_n(q)$. Say $p = p_1$, and set

$$C := C_{\mathrm{Mat}_n(q)}(P), \quad Z = Z(C). \tag{10}$$

Thus

$$H \leq N_{\langle\psi\rangle \mathrm{GL}_n(q)}(C), \quad H \leq N_{\langle\psi\rangle \mathrm{GL}_n(q)}(Z). \tag{11}$$

Case 1 P has a unique homogeneous component W, of dimension m, say. As P_W is an irreducible subgroup of $\mathrm{GL}_m(q)$, a Sylow p-subgroup of $\mathrm{GL}_m(q)$ must be irreducible. From $q \equiv 1 \pmod p$, we have that m is a power of p. Z is a field extension of $\mathbb{F}_q$ and we claim that it has order q^{p^α}, for some $\alpha \geq 0$. Indeed, up to conjugation, we may assume

$$Z^* = \langle \begin{pmatrix} z & & \\ & \dots & \\ & & z \end{pmatrix} \rangle \quad z \text{ irreducible.}$$

The characteristic polynomial $c(t)$ of each block z has degree which divides m. As $c(t)$ is also the minimum polynomial of z, our claim follows.

1.1 $\alpha > 0$. Let $\psi\nu\langle z\rangle = N_{\langle\psi\rangle \mathrm{GL}_{p^\alpha}(q)}(\langle z\rangle)$, with $\psi\nu$ defined as in Lemma 2.7, with $a = p^\alpha$. The kernel of the homomorphism

$$f : N_{\mathrm{GL}_{p^\alpha}(q)}(z) \to \mathrm{Gal}(\mathbb{F}_{q^{p^\alpha}} : \mathbb{F}_q)$$

induced by the conjugation action, coincides with $\langle z\rangle$. From $\langle\psi\nu\rangle \cap \langle z\rangle = 1$, we deduce that the restriction of f to $\langle\psi\nu\rangle \cap \mathrm{GL}_{p^\alpha}(q)$, is injective. Hence $\langle\psi\nu\rangle \cap \mathrm{GL}_{p^\alpha}(q)$ is a p-group. It follows that $\left|(\psi\nu)_{p'}\right| = \left|\psi_{p'}\right|$ and, by Lemma 3.1, up to conjugation under $\mathrm{GL}_{p^\alpha}(q)$, we may suppose that $(\psi\nu)_{p'} = \psi_{p'}$, i.e.

$$\langle\psi\nu\rangle = \langle(\psi\nu)_p\rangle \times \langle\psi_{p'}\rangle.$$

From $|z| = q^{p^a} - 1$ with $p = p_1$ and the assumption $r \equiv 1 \pmod{p_j}$, $j \leq k$, it follows that for $j \geq 2$ the Sylow p_j-subgroup of $\langle z\rangle$ coincides with R_{p_j}. Hence it is scalar. Let $\overline{R}_p$ be the Sylow p-subgroup of $\langle z\rangle$. By Lemma 2.6, with ψ and q replaced respectively by $\psi\nu$ and q^{p^α}, the group

$$\langle\psi\nu\rangle\overline{R}_p \,\mathrm{Diag}_{p^\alpha}(R_{p_2}\cdots R_{p_t}) \;=\; \langle(\psi\nu)_p\rangle\,\overline{R}_p\,\langle\psi_{p'}\rangle\,\mathrm{Diag}_{p^\alpha}(R_{p_2}\cdots R_{p_t})$$

is a Carter subgroup of $\langle\psi\nu\rangle\langle z\rangle$. In particular $\langle(\psi\nu)_p\rangle\overline{R}_p$ is centralized by $\psi_{p'}$, hence:

$$\langle(\psi\nu)_p\rangle\,\overline{R}_p \leq \langle\psi\rangle\,\mathrm{GL}_{p^\alpha}(r^{m_p}).$$

Note that, if $p = 2$ and im_p is odd, then $|\varphi| = im$ is odd and, in this case, we are assuming $r_0 \equiv 1 \pmod 4$. So, by Lemma (2.4), there exists $x \in \mathrm{GL}_{p^\alpha}(r^{m_p})$ such that $\left(\langle(\psi\nu)_p\rangle\overline{R}_p\right)^x$ lies in $\langle\psi\rangle\,\mathrm{Diag}_{p^\alpha}(R_p)\,\mathrm{Sym}(p^\alpha)$. Substituting z with z^x we may suppose:

$$\langle\psi\nu\rangle\overline{R}_p \;\leq\; \langle\psi\rangle\,\mathrm{Diag}_{p^\alpha}(R_p)\,\mathrm{Sym}(p^\alpha). \tag{12}$$

1.1.1 $n = p^\alpha$. In this case $Z^* = \langle z \rangle$, hence $H \leq \langle \psi\nu \rangle \langle z \rangle$. By Lemma 2.6, up to conjugation under $\langle z \rangle$, we may suppose $H \leq \langle \psi\nu \rangle \overline{R}_p\ (R_{p_2} \cdots R_{p_t})\, I_n$.

Hence H satisfies Theorem 1.1 in virtue of (12).

1.1.2 $n > p^\alpha$. From $\mathbb{F}_q^* I_n \leq \langle Z \rangle$ and $C_{\langle \psi \rangle \mathrm{GL}_n(q)}(\mathbb{F}_q^* I_n) = \mathrm{GL}_n(q)$:

$$C_{\langle \psi \rangle \mathrm{GL}_n(q)}(Z) \;=\; C_{\mathrm{GL}_n(q)}(Z) \;=\; \mathrm{GL}_{\frac{n}{p^\alpha}}\left(q^{p^\alpha}\right). \tag{13}$$

Thus, by (11), setting $\Psi = \psi(\nu, \cdots, \nu)$ with $\nu \in \mathrm{GL}_{p^\alpha}(q)$ as above:

$$H \;\leq\; N_{\langle \psi \rangle \mathrm{GL}_n(q)}(Z) \;=\; \langle \Psi \rangle\, \mathrm{GL}_{\frac{n}{p^\alpha}}\left(q^{p^\alpha}\right). \tag{14}$$

Note that $\langle \Psi \rangle$ intersects trivially $\mathrm{GL}_{\frac{n}{p^\alpha}}\left(q^{p^\alpha}\right)$ as the automorphism induced by Ψ on the center of $\mathrm{GL}_{\frac{n}{p^\alpha}}\left(q^{p^\alpha}\right)$ has order $mp^\alpha = |\Psi|$. From

$$H \cap \mathrm{GL}_{\frac{n}{p^\alpha}}(q^{p^\alpha}) \;\leq\; H \cap \mathrm{GL}_n(q)$$

and our assumptions on n, there exists $g \in \mathrm{GL}_{\frac{n}{p^\alpha}}\left(q^{p^\alpha}\right)$ such that

$$H^g \;\leq\; \langle \Psi \rangle\, \mathrm{Diag}_{\frac{n}{p^\alpha}}\left(\overline{R}_p\, (R_{p_2} \cdots R_{p_t})\right) \mathrm{Sym}\left(\frac{n}{p^\alpha}\right).$$

We have that H satisfies Theorem 1.1 in virtue of (12), recalling the definition of Ψ given just before (14).

1.2 $\alpha = 0$. In the notation of (2), up to conjugation under $\mathrm{GL}_n(q)$ we may suppose that $P \leq \mathrm{GL}_u(q) \times \cdots \times \mathrm{GL}_u(q) = (\mathrm{GL}_u(q))^\ell$ and, moreover, that:

$$P \;=\; \left\{ \begin{pmatrix} A & & \\ & \cdots & \\ & & A \end{pmatrix} \mid A \in \pi_1(P) \right\} \;=\; \pi_1(P) \otimes I_\ell$$

where $\pi_1(P)$ is an absolutely irreducible subgroup of $\mathrm{GL}_u(q)$. It follows:

$$C = C_{\mathrm{Mat}_n(q)}(P) \;=\; I_u \otimes \mathrm{Mat}_\ell(q) \tag{15}$$

$$C_{\mathrm{Mat}_n(q)}(C) \;=\; \mathrm{Mat}_u(q) \otimes I_\ell. \tag{16}$$

By a result of Skolem-Noether [3, Theorem 3.62, page 69], every automorphism of $\mathrm{Mat}_\ell(q)$ which induces the identity on the center is inner. Hence:

$$N = N_{\langle \psi \rangle GL_n(q)}(C) \;=\; \langle \psi \rangle\, \mathrm{GL}_u(q) \otimes \mathrm{GL}_\ell(q). \tag{17}$$

Let let h be as in (8). Recalling that $H \leq N$ we have $H_p = \langle h_p \rangle P$ with:

$$h_p = \psi_p\, a \otimes b, \quad a \in \mathrm{GL}_u(q),\ b \in \mathrm{GL}_\ell(q). \tag{18}$$

We claim that, up to conjugation under $\mathrm{GL}_\ell(q)$, we may suppose b scalar. Indeed, call e the order of ψ_p. Then:

$$h_p^e = a^{1+\psi+\dots\psi^{e-1}} \otimes b^{1+\psi+\dots\psi^{e-1}} \in P.$$

This forces $b^{1+\psi+\dots\psi^{e-1}}$ to be scalar, i.e. $(\psi_p b)^e = \rho I_\ell$. Clearly $\psi_p b$ centralizes ρI_ℓ, hence $\rho \in C_{\mathbb{F}_q}(\psi_p)$. It follows from (4) that $\rho = \lambda^{1+\psi+\dots\psi^{e-1}}$ for some $\lambda \in \mathbb{F}_q$. So $\psi_p b\lambda^{-1}$ has the same order e of ψ_p and our claim follows from Lemma 3.1. So in (18) we may assume b scalar, i.e.

$$H_p \leq \langle\psi_p\rangle\,\mathrm{GL}_u(q) \otimes I_\ell$$

and it makes sense to consider the projection $\pi_1 : H_p \to \langle\psi_p\rangle\,\mathrm{GL}_u(q)$.

In particular $C_{\mathrm{Mat}_n(q)}(\pi_1(P)) = \mathbb{F}_q I_n$. So, if we set $C_{\mathbb{F}_q}(\psi_p) = \mathbb{F}_{q_0}$, then:

$$C_{\mathrm{Mat}_u(q)}(\pi_1(H_p)) = \mathbb{F}_{q_0} I_u. \tag{19}$$

From (15) and (19) it follows:

$$C_{\mathrm{Mat}_n(q)}(H_p) = I_u \otimes \mathrm{Mat}_\ell(q_0). \tag{20}$$

Under our assumptions, there exists a Sylow p-subgroup $\Gamma_{u,p}$ of $\langle\psi\rangle\,\mathrm{GL}_u(q)$ which is monomial. Noting that ψ normalizes $\Gamma_{u,p}$, up to conjugation under $\mathrm{GL}_u(q)$ we may assume $\pi_1(H_p) \leq \Gamma_{u,p}$. So we have $H_p \leq \Gamma_p$ where Γ_p is defined as in Lemma 2.4. Clearly $H_{p'} \leq \langle\psi_{p'}\rangle\,\mathrm{GL}_n(q)$. By Lemma 2.6 $\psi_{p'}$ centralizes Γ_p and, a fortiori, H_p. Hence

$$H_{p'} \leq C_{\langle\psi_{p'}\rangle \mathrm{GL}_n(q)}(H_p) = \langle\psi_{p'}\rangle\left(I_u \otimes \mathrm{GL}_\ell(q_0)\right).$$

By the minimality of n, there exists $x \in I_u \otimes \mathrm{GL}_\ell(q_0)$ such that $H_{p'}^x$ is monomial. Since x centralizes H_p, this completes this case.

Case 2 The homogeneous components of P are more than one. They are permuted transitively by h, defined in (8), since H is indecomposable. Let M be a maximal subgroup of H containing the stabilizer of a component V_0 and call W the subspace generated by $\{m(V_0) \mid m \in M\}$. Then M is a normal subgroup of prime index s and

$$\mathbb{F}_q^n = W \oplus h(W) \oplus \dots \oplus h^{s-1}(W)$$

where each direct summand is stabilized by M. Thus, in the notation of (2), we may assume that H is a subgroup of

$$\langle\psi\rangle\left(\mathrm{GL}_{\frac{n}{s}}(q) \times \dots \times \mathrm{GL}_{\frac{n}{s}}(q)\right)\langle\sigma\rangle = \langle\psi\rangle\,\mathrm{GL}_{\frac{n}{s}}(q)^s\,\langle\sigma\rangle \tag{21}$$

where σ is a permutation matrix of order s, which permutes the direct factors of $\mathrm{GL}_{\frac{n}{s}}(q)^s$ and

$$H_{s'} \leq M \leq \langle\psi\rangle\, \mathrm{GL}_{\frac{n}{s}}(q)^s. \tag{22}$$

Let η be a preimage of σ in H_s. Thus:

$$\eta = \psi^\ell \sigma(y_1,\cdots,y_s) \tag{23}$$

where ψ^ℓ can be chosen to be an s-element and each $y_j \in \mathrm{GL}_{\frac{n}{s}}(q)$.

We will use the fact that, for each $g=(g_1,\cdots,g_s) \in \mathrm{GL}_{\frac{n}{s}}(q)^s$:

$$\eta^{(g_1,\cdots,g_s)} \;=\; \psi^\ell\sigma(\bar{y}_1,\cdots,\bar{y}_s), \quad \bar{y}_j \in \mathrm{GL}_{\frac{n}{s}}(q). \tag{24}$$

Since we are assuming that point 2) of Lemma 3.3 holds, we can say $s = p_t$. Recalling (22) and the minimality of n, after a first conjugation of H by some $g \in \mathrm{GL}_{\frac{n}{s}}(q)^s$, we can suppose that

$$H_{s'} \;\leq\; \langle\psi\rangle \left(\mathrm{Diag}_{\frac{n}{s}}(R_{p_1}\cdots R_{p_{t-1}})\,\mathrm{Sym}(\frac{n}{s})\right)^s.$$

Recalling (23) this conjugation takes η into an element of the same shape. Note that

$$R_{p_1}\cdots R_{p_{t-1}} \leq \mathbb{F}_{r^{mp_1\cdots mp_{t-1}}}$$

as a consequence of point 2) of Lemma 2.4. It follows that ψ^ℓ, whose order divides $m_s = m_{p_t}$, centralizes $H_{s'}$. Imposing that η centralizes $H_{s'}$ we see that, up to a new conjugation by some element in $\mathrm{GL}_{\frac{n}{s}}(q)^s$, we may assume that $H_{s'}$ consists of elements of shape:

$$\psi^\ell \begin{pmatrix} x & & \\ & \cdots & \\ & & x \end{pmatrix}, \quad x \in \mathrm{GL}_{\frac{n}{s}}(q).$$

Set $G := \langle\psi\rangle\ \mathrm{GL}_{\frac{n}{s}}(q)^s\langle\sigma\rangle$ and let S be a Sylow s-subgroup of $C_G(H_{s'})$ which contains H_s. Then $\widehat{H} := S \times H_{s'}$ is nilpotent and $H \leq \widehat{H}\ \leq G$. As σ centralizes $H_{s'}$, there exists $c \in C_G(H_{s'})$ such that $\sigma \in S^c$. Then

$$\widehat{H}^c \;=\; \langle\sigma\rangle\ \left(\widehat{H}^c \cap \langle\psi\rangle\,\mathrm{GL}_{\frac{n}{s}}(q)^s\right).$$

The conjugation action of σ on the second factor implies that, for each $j \leq s$, $\pi_j\left(\widehat{H}^c \cap \langle\psi\rangle\,\mathrm{GL}_{\frac{n}{s}}(q)^s\right) \;=\; \pi_1\left(\widehat{H}^c \cap \langle\psi\rangle\,\mathrm{GL}_{\frac{n}{s}}(q)^s\right)$ Moreover, by the minimality of n, there exists $g_0 \in \mathrm{GL}_{\frac{n}{s}}(q)$ such that

$$\left(\pi_1\left(\widehat{H}^c \cap \langle\psi\rangle\,\mathrm{GL}_{\frac{n}{s}}(q)^s\right)\right)^{g_0} \;\leq\; \langle\psi\rangle\ \mathrm{Diag}_{\frac{n}{s}}(R_{p_1}\cdots R_{p_t})\left(\frac{n}{s}\right).$$

Taking $g := (g_0,\ldots,g_0)$ we have that $\sigma^g = \sigma$, hence

$$H^g \;\leq\; \widehat{H}^g \;\leq \langle\psi\rangle\,\mathrm{Diag}\,(R_{p_1}\cdots R_{p_t})\,\mathrm{Sym}(n).$$

□

4. An application to Carter Subgroups

Denote by F_G the set of conjugacy classes of Carter subgroups of a finite group G. As an easy consequence of [1], it is shown in [11] the following.

Lemma 4.1. *Let N be a finite normal solvable subgroup of G. The canonical epimorphism $\pi : G \to G/N$ induces a bijection $\widehat{\pi} : F_G \to F_{G/N}$.*

So the conjugacy conjecture holds for G if and only if it holds for G/N.

Lemma 4.2. *For each $n \geq 2$:*

1) *Two semisimple elements of $\mathrm{GL}_n(q)$ are conjugate under $\mathrm{GL}_n(q)$ if and only if they are conjugate under $\mathrm{SL}_n(q)$;*

2) *the Jordan unipotent block J_n is conjugate to its inverse under $\mathrm{GL}_n(\mathbb{Z})$;*

3) *if $q \equiv 1 \pmod 4$, then every element z of order r_0 is conjugate to its inverse under $\mathrm{SL}_n(q)$.*

Proof. 1) A consequence of the fact that the centralizer of a semisimple element contains matrices of all possible determinants. Enough to see this fact for the companion matrix m of an irreducible polynomial. The algebra generated by m over F_q is a field, whose multiplicative group is generated by a Singer cycle c of order $q^n - 1$. As $\langle c \rangle \cap \mathrm{SL}_n(q)$ has index $q-1$ in $\langle c \rangle$ [7, Satz 7.3, page 187], the determinant of c generates $\mathbb{F}_q^*$.

2) Set $A_1 := \begin{pmatrix} -1 \end{pmatrix}$ and, for $s \geq 1$, $A_{s+1} := \begin{pmatrix} J_s A_s & \\ & (-1)^{s+1} \end{pmatrix}$.
Then $(A_{s+1})^2 = I$ and $A_{s+1} J_{s+1} A_{s+1} = J_{s+1}^{-1}$. In fact, by induction:

$$A_{s+1} J_{s+1} A_{s+1} \;=\; A_{s+1} \begin{pmatrix} J_s & \\ e_s & 1 \end{pmatrix} A_{s+1} \;=\; \begin{pmatrix} J_s^{-1} & \\ (-1)^{s+1} e_s J_s A_s & 1 \end{pmatrix}.$$

The conclusion follows noting that $(-1)^s e_s = e_s A_s$, hence

$$(-1)^{s+1} e_s J_s A_s \;=\; -(-1)^s e_s J_s A_s \;=\; -e_s A_s J_s A_s \;=\; -e_s J_s^{-1}.$$

3) By the previous result, modulo r_0, each block J_m of the Jordan form of z is conjugate to J_m^{-1}, via A_m. Our claim follows from the fact that A_m has determinant 1 if $m \equiv 0, 3 \pmod 4$ and has determinant -1 if $m \equiv 1, 2 \pmod 4$. But in the second case, the assumption $q \equiv 1 \pmod 4$ ensures that in $\mathrm{SL}_n(q)$ there are scalar matrices of determinant -1. □

A more general statement than point 3) of the previous Lemma can be found in [13, Theorem 1.4 (i), (ii)].

Proof. (*Corollary* 1.2)

Suppose, by contradiction, that the projective image of A is a minimal counterexample to the conjecture. We show that every Carter subgroup H of A is conjugate to a subgroup of $A \cap M$, where M is the generalized monomial subgroup, and this will easily lead to a contradiction. For a fixed H, we may choose our notation so that $H\,\mathrm{GL}_n(q) = \langle \psi \rangle\, \mathrm{GL}_n(q)$ for an appropriate power ψ of φ, as in Theorem 1.1, and set $r = \left|C_{\mathbb{F}_q}(\psi)\right|$. Now let p be a prime which divides $|H \cap \mathrm{GL}_n(q)|$. As $H \cap \mathrm{GL}_n(q)$ is normal in H, there exists $z \in Z(H) \cap \mathrm{GL}_n(q)$ of order p. If $p = r_0$, we have that z is conjugate to z^{-1} under A by point 3) of the previous Lemma. But, as explained in the Introduction, the projective image of z cannot be conjugate to its inverse [12, Lemma 3.1 (b)]. This forces $z = z^{-1}$. Hence $r_0 = 2$, which contradicts the assumption $q \equiv 1 \pmod 4$. Thus $p \neq r_0$. In the notation of (8), we have $z = z^h$ where $h \in H$ is such that $h\psi^{-1} \in \mathrm{GL}_n(q)$. Therefore, z is conjugate to z^ψ under $\mathrm{GL}_n(q)$. This gives that the Jordan canonical form J of z is conjugate to the Jordan canonical form J^ψ of z^ψ under $\mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F}$ denotes the algebraic closure of $\mathbb{F}_q$. But $J^\psi = J^r$ gives that z and z^r are conjugate under $\mathrm{GL}_n(q)$ [9, Corollary 2, page 397]. We conclude that z is conjugate to z^r under A, by point 1) of the previous Lemma. In particular, if z is scalar, we have $z = z^r$ whence $r \equiv 1 \pmod p$. So assume that z is non-scalar. Again by [12, Lemma 3.1 (b)] the projective images of z and z^r must be the same, i.e. $z^r = \rho z$ for some $\rho \in \mathbb{F}_q^*$. This gives that z^{r-1} is scalar and we conclude that $r \equiv 1 \pmod p$, otherwise z would belong to $\langle z^{r-1} \rangle$. By Theorem 1.1, there exists $g \in \mathrm{GL}_n(q)$ such that $H^g \le M = \langle \varphi \rangle\, \mathrm{Diag}_n(\mathbb{F}_q^*)\, \mathrm{Sym}(n)$. For an appropriate $d \in \mathrm{Diag}_n(\mathbb{F}_q^*)$ we have that $a = gd \in \mathrm{SL}_n(q) \le A$. Thus H is conjugate, under A, to a subgroup of $A \cap M$. To reach the desired contradiction note that, by the assumption $\mathrm{SL}_n(q) \le A$:

$$\frac{A \cap M}{A \cap \left(\langle \varphi \rangle\, \mathrm{Diag}_n(\mathbb{F}_q^*)\right)} \sim \mathrm{Sym}(n).$$

The Carter subgroups of $\mathrm{Sym}(n)$ are its Sylow 2-subgroups, by [5]. Thus, by Lemma 4.1, all Carter subgroups of $A \cap M$ are conjugate. We conclude that all Carter subgroups of A are conjugate, a contradiction. □

Proof. of Theorem 1.3.

HD/D is a Carter subgroup of $M_0/D = \langle \psi \rangle \times \mathrm{Sym}(n)$. Thus, by [5], HD/D coincides with $\langle \psi \rangle \Sigma_2$, where Σ_2 is a Sylow 2-subgroup of $\mathrm{Sym}(n)$. It follows that H is a Carter subgroup of

$$HD = \langle \psi \rangle \Sigma_2 D = \left(\langle \psi \rangle \Sigma_2 D_2\right) D_{2'}.$$

If $d \in D$, we have $d^{\psi} = d^{r}$. This means that ψ normalizes every subgroup of D. In particular $\langle \psi \rangle_{2'}$ stabilizes any composition series of D_2, inducing the identity on each composition factor. It follows that $\langle \psi \rangle_{2'}$ centralizes D_2 [6, Theorem 3.2, page 178]. Thus $\langle \psi \rangle \Sigma_2 D_2$ is a nilpotent group. Note that $D_{2'}$ is characteristic in D, hence normal in HD. Again $HD_{2'}/D_{2'}$ is a Carter subgroup of $HD/D_{2'} = \langle \psi \rangle \Sigma_2 D_2$. It follows that $HD_{2'} = HD$. As HD contains a Sylow 2-subgroup of M_0, the same is true for H. □

Acknowledgements

The proofs of Lemma 2.6 and of Theorem 1.3 use ideas of Clara Franchi. We are also grateful to Roger Bryant, for useful discussions at an early stage of the preparation of this paper, and to the Referee for careful reading and detecting a mistake in a previous version.

REFERENCES

[1] R. Carter, *Nilpotent selfnormalizing subgroups of soluble groups*, Math. Z. vol. 75 (1961), 136–139.

[2] C. W. Curtis - I. Reiner, *RepresentaNo. 2tion Theory of finite groups and associative algebras*, Second edition, John Wiley and Sons, New Yor, London, Sidney, 1966.

[3] C. W. Curtis, I. Reiner, *Methods of Representation Theory* John Wiley & Sons, Inc., New York, 1990.

[4] F. Dalla Volta - A. Lucchini - M. C. Tamburini, *On the conjugacy problem for Carter subgroups*, Comm. Algebra **26**(2) (1998), 395–399.

[5] L. Di Martino - M. C. Tamburini, *I sottogruppi nilpotenti autonormalizzanti di S_n e A_n*, Istit. Lombardo Accad. Sci. Lett. Rend. A **110** (1976), 235–241.

[6] D. Gorenstein, *Finite Groups*, Harper and Row, 1968.

[7] B. Huppert, *Endliche Gruppen I, Zweiter Nachdruck*, Springer-Verlag, Berlin Heidelberg New York, 1983.

[8] B. Huppert, N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin Heidelberg New York, 1982.

[9] S. Lang, *Algebra*, First printing 1969, Addison-Wesley.

[10] R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc. 80, 1968.

[11] M. C. Tamburini, *The conjugacy conjecture for Carter subgroups*, Milan J. Math. **75** (2007), 357–377.

[12] M. C. Tamburini - E. P. Vdovin, *Carter Subgroups in Finite Groups*, J. Algebra **255** no.1 (2002), 148–163.

[13] P. H. Thiep - A. E. Zalesskii, *Real conjugacy classes in algebraic groups and finite groups of Lie type*, J. Group Theory **8** (2005), 291–315.

[14] E. P. Vdovin, *Carter subgroups of finite almost simple groups*, Algebra y Logica, **46** No. 2 (2007), 90–119.

ANDREA LUCCHINI
Dipartimento di Matematica Pura ed Applicata
Università degli Studi di Padova
Via Trieste 63
35121 Padova, Italy
e-mail: `lucchini@math.unipd.it`

M. CHIARA TAMBURINI
Dipartimento di Matematica e Fisica
Università Cattolica del Sacro Cuore
Via Musei 41
25121 Brescia, Italy
e-mail: `c.tamburini@dmf.unicatt.it`