Element orders and Sylow structure of finite groups

by

Gunter Malle
FB Mathematik
Universität Kaiserslautern
Postfach 3049
D-67653 Kaiserslautern GERMANY
E-mail: malle@mathematik.uni-kl.de

Alexander Moretó and Gabriel Navarro
Departament d'Àlgebra
Universitat de València
46100 Burjassot. València SPAIN
E-mail: Alexander.Moreto@uv.es, gabriel@uv.es

The second and third authors were partially supported by the Spanish Ministerio de Educación y Ciencia, MTM2004-06067-C02-01 and MTM2004-04665, and the FEDER. The third author was also supported by the Programa Ramón y Cajal.

1 Introduction

N. Chigira, N. Iiyori and H. Yamaki proved in the Main Theorem of their Inventiones paper [4] that if a finite group of even order G does not have any elements of order $2p$, p a prime, then the Sylow p-subgroups of G are abelian. The main result of this paper is an attempt to extend that theorem to odd primes. Recall that given a set of primes π, $O_{\pi'}(G)$ is the largest normal π'-subgroup of G.

Theorem A. *Let G be a finite group and $p \neq q$ prime integers. If G does not have any elements of order pq, then one of the following holds:*

(i) *The Sylow p-subgroups or the Sylow q-subgroups of G are abelian.*

(ii) *$G/O_{\{p,q\}'}(G) = M$ and $\{p, q\} = \{5, 13\}$ or $\{7, 13\}$.*

The situation (ii) is a genuine exception because the sporadic simple monster group M does not have any elements of order 65 or 91, while it has nonabelian Sylow $5, 7$ and 13-subgroups. One could perhaps think that if $p > q$ then, except for in the situation (ii), the Sylow p-subgroup is abelian. This cannot be guaranteed however, since there are nonabelian groups that admit fixed point free automorphisms of prime order $q > 2$.

As one could expect from the statement, the proof of Theorem A relies on the classification of finite simple groups, but it does not depend on the results in [4] and seems simpler. We will see that it is easy to give a new proof of the theorem of Chigira, Iiyori and Yamaki using Theorem A.

In many cases, it turns out from the proof that we get a cyclic Sylow p-subgroup or q-subgroup. However, it is not possible to replace the word "abelian" by "cyclic" in the statement of the theorem. For instance, the Frobenius group of order 72 does not have elements of order 6 and it has noncyclic Sylow subgroups. There are also examples for odd primes apart from (ii) above: the sporadic group He does not have elements of order 35 and it has noncyclic Sylow 5 and 7-subgroups. In Section 4 we will present two infinite families of examples. However, it can be easily proved that if G is solvable without elements of order pq and p and q are odd primes then a Sylow p-subgroup or a Sylow q-subgroup of G is cyclic.

2 Almost simple groups

We begin with the proof of Theorem A for almost simple groups. First, we consider the sporadic groups.

Lemma 1. *Suppose that $S \leq G \leq \mathrm{Aut}(S)$, where S is a sporadic group and $p \neq q$ are prime integers. If G does not have any elements of order pq, then one of the following holds:*

(i) *The Sylow p-subgroups or the Sylow q-subgroups of G are abelian.*

(ii) *$G = M$ and $\{p, q\} = \{5, 13\}$ or $\{7, 13\}$.*

Proof. It suffices to check the Atlas [5]. □

Lemma 2. *Suppose that $S \leq G \leq \mathrm{Aut}(S)$, where S is an alternating group of degree $n \geq 5$. If G does not have any elements of order pq, then the Sylow p-subgroups or the Sylow q-subgroups of G are abelian.*

Proof. Assume first that $2 < p < q$. We may assume that $G = S$ (notice that $|\mathrm{Out}(S)| = 2$ or 4). If $n \geq p + q$, then we can find a p-cycle $x \in G$ and a q-cycle $y \in G$ with $xy = yx$ of order pq. We deduce that $n < p + q < 2q$. Therefore the Sylow q-subgroup of G has order q and, in particular, is abelian.

Hence, we may assume that $p = 2$ and we want to prove that a Sylow q-subgroup of G is abelian. Again, we may assume that $G = S$. If $n \geq 4 + q$, then we can find as before an element of order $2q$. We deduce that $n \leq 3 + q \leq 2q$ and the Sylow q-subgroups of G have order $\leq q^2$ so in particular they are abelian. □

Finally, we consider the groups of Lie type. Let S be a finite simple group of Lie type. Then there exists a simple algebraic group $\mathbf{G}$ of adjoint type over the algebraic closure $\bar{\mathbb{F}}_q$ of a finite field, defined over $\mathbb{F}_q$ with corresponding Frobenius endomorphism $F : \mathbf{G} \to \mathbf{G}$, such that S is the derived subgroup of the group of fixed points $G := \mathbf{G}^F$. Let W denote the Weyl group of $\mathbf{G}$ with respect to some F-stable maximal torus $\mathbf{T}$ of $\mathbf{G}$ and ϕ the automorphism of W induced by F. Since ϕ permutes the set of simple reflections of W, it also defines a symmetry of the Dynkin diagram of $\mathbf{G}$.

Lemma 3. *In the notation introduced above, assume that the Sylow p-subgroups of G are non-abelian for some divisor p of $|G|$. Then either $p|q$ and $\mathbf{G}$ is not of type A_1, or p divides the order of W.*

Proof. It is shown in [2, Cor. 3.13], for example, that necessarily p divides $q|W\langle\phi\rangle|$. But note that when $\mathbf{G}$ is simple, the order of ϕ always divides the order of W. □

In particular, if $S = G'$ has a non-abelian Sylow p-subgroup, then the same conclusion holds. We will need a more precise criterion for non-abelian Sylow subgroups. For this note that, by a result of Steinberg, in the above setup there exists a product of cyclotomic polynomials

$$o_{\mathbf{G}}(X) = X^N \prod_d \Phi_d(X)^{a(d)} \in \mathbb{Z}[X]$$

such that for any choice of Frobenius map $F' : \mathbf{G} \to \mathbf{G}$ defining an $\mathbb{F}_{q'}$-rational structure of $\mathbf{G}$ and with the same action on W, the order of the group $\mathbf{G}^{F'}$ is given by $|\mathbf{G}^{F'}| = o_{\mathbf{G}}(q') = {q'}^N \prod_d \Phi_d(q')^{a(d)}$ (see e.g. [2]). Then we have:

Lemma 4. *In the notation introduced above, assume that the Sylow p-subgroups of G are non-abelian for some divisor p of $|G|$. Then either $p|q$ and $\mathbf{G}$ is not of type A_1, or p divides at least two different factors $\Phi_d(q)$ with $a(d) > 0$.*

Proof. This is also shown in [2, Cor. 3.13]. □

We need the following well-known number theoretic result:

Lemma 5. *Let $q \geq 1$, p an odd prime not dividing q, and e the multiplicative order of q mod p. Then $p|\Phi_f(q)$ if and only if $f = ep^j$ for some $j \geq 0$.*

Proof. By assumption we have $q^e \equiv 1 \pmod{p}$. If $p|\Phi_f(q)$ then $q^f \equiv 1 \pmod{p}$, hence $e|f$ by the definition of e. Now note that $\Phi_{et}(X)$ divides $\Phi_t(X^e)$. Hence $p|\Phi_{et}(q)$ implies $p|\Phi_t(1)$, so p divides the norm of $1 - \zeta$ for some primitive tth root of unity ζ. This forces t to be a power of p (see [11, p.12]), proving one direction.

Conversely, if $q^e = 1 + cp^a$ with $p \not| c$, $a \geq 1$, then

$$q^{ep^j} = (1 + cp^a)^{p^j} \equiv 1 + cp^{a+j} \pmod{p^{a+j+1}}$$

for all $j \geq 1$ (since $p > 2$). Thus, if p^a is the precise power dividing $q^e - 1$, then p^{a+j} is the precise power dividing $q^{ep^j} - 1$. In particular, $(q^{ep^j} - 1)/(q^{ep^{j-1}} - 1)$ is divisible by p. By the first part the only cyclotomic factor of $(q^{ep^j} - 1)/(q^{ep^{j-1}} - 1)$ which can account for this divisibility is $\Phi_{ep^j}(q)$. Thus $\Phi_{ep^j}(q)$ is divisible by p, which completes the proof. □

Corollary 6. *If p is odd and $p|\Phi_{d_i}(q)$ for $i = 1, 2$ with $d_1 < d_2$, then $d_1 \leq d_2/p$. Moreover, d_1 and d_2 have the same parity.*

We will use this corollary in conjunction with the order formulae for classical groups of adjoint type (see e.g. [3, 1.19 and 2.9])

$$\begin{aligned}
|\mathrm{PGL}_n(q)| &= q^{n(n-1)/2}\prod_{k=2}^{n}(q^k-1),\\
|\mathrm{PGU}_n(q)| &= q^{n(n-1)/2}\prod_{k=2}^{n}(q^k-(-1)^k),\\
|\mathrm{PCSp}_{2n}(q)| = |\mathrm{SO}_{2n+1}(q)| &= q^{n^2}\prod_{k=1}^{n}(q^{2k}-1),\\
|\mathrm{PCO}^{\pm}_{2n}(q)^\circ| &= q^{n(n-1)}\prod_{k=1}^{n-1}(q^{2k}-1)(q^n\mp 1),
\end{aligned}$$

and the existence of certain natural subgroups of classical groups, namely

$$\begin{aligned}
&\mathrm{GL}_m(q)\times\mathrm{GL}_{n-m}(q)\le\mathrm{GL}_n(q), && m=\lfloor\frac{n+1}{2}\rfloor,\\
&\mathrm{GU}_m(q)\times\mathrm{GU}_{n-m}(q)\le\mathrm{GU}_n(q), && m=\lfloor\frac{n+1}{2}\rfloor,\\
&\mathrm{Sp}_{2m}(q)\times\mathrm{Sp}_{2(n-m)}(q)\le\mathrm{Sp}_{2n}(q), && m=\lfloor\frac{n}{2}\rfloor,\\
&\mathrm{SO}_{2m+1}(q)\times\mathrm{SO}^+_{2(n-m)}(q)\le\mathrm{SO}_{2n+1}(q), && m=\lfloor\frac{n}{2}\rfloor,\\
&\mathrm{SO}^{\pm}_{2m}(q)\times\mathrm{SO}^+_{2(n-m)}(q)\le\mathrm{SO}^{\pm}_{2n}(q), && m=\lfloor\frac{n}{2}\rfloor,
\end{aligned}$$

which can be exhibited as stabilizers of suitable orthogonal decompositions of the underlying space. The groups of adjoint type listed above contain central quotients of the classical groups, thus they contain some central quotient of the natural subgroups just described.

Lemma 7. *In the notation introduced above, assume that the Sylow p-subgroups of* $\mathrm{Aut}(S)$ *are non-abelian for some divisor p of* $|\mathrm{Aut}(S)|$. *Then one of the following holds:*

(a) $p|q$ is the defining characteristic, or

(b) p divides $|W|$, or

(c) p divides the order of some field automorphism of S.

Proof. According to [6, 1.15, Th. 2.5.12 and 2.5.14], for example, $\mathrm{Out}(S)$ is generated by the diagonal automorphisms, the field automorphisms and the graph automorphisms of S. The group of diagonal automorphisms is already contained inside G. The group of graph automorphisms is either

trivial, cyclic of order 2, or a symmetric group of degree 3 if $\mathbf{G}$ is of type D_4. But note that in all cases the order of graph automorphisms always divides the order of the Weyl group of $\mathbf{G}$. Thus the assertion follows from Lemma 3. □

Lemma 8. *In the notation introduced above, assume that H with $S \leq H \leq \mathrm{Aut}(S)$ has non-abelian Sylow p_i-subgroups for two different primes p_1, p_2, with p_1 not dividing $q|W|$. Then there exist elements of order p_1p_2 in H.*

Proof. By Lemma 7 the prime p_1 divides the order of some field automorphism of S, and by Lemma 3 the group H must contain a conjugate of a field automorphism σ of S of order p_1. The centralizer in S of σ is a group of the same type as S, in particular with the same Weyl group as S and over a field of the same characteristic. Thus its order is divisible by all prime divisors of $|G|$ for which the Sylow subgroups of G are non-abelian, by Lemma 3. On the other hand, if p_2 is the order of some other field automorphism of S, then the fact that the group of field automorphisms is cyclic allows to conclude. □

Theorem 9. *Let S be a simple group of Lie type and $S \leq H \leq \mathrm{Aut}(S)$. Assume that $p_1 \neq p_2$ are prime divisors of $|H|$ such that there is no element of order p_1p_2 in H. Then either the Sylow p_1-subgroup or the Sylow p_2-subgroup of H is abelian.*

Proof. We treat the various possibilities for S. If H is a counterexample to the assertion, then there exist two prime divisors p_1, p_2 of $|H|$ for both of which the Sylow subgroups are non-abelian, and there is no element of order p_1p_2 in H. Moreover, by Lemmas 3–8 we may assume that p_1, p_2 both divide $q|W|$. We'll rule out this possibility.

If S is a Suzuki-group or a Ree-group ${}^2G_2(q^2)$, then only the primes 2 and 3 divide $q|W|$. But the Suzuki-groups have order prime to 3, while the Sylow 2-subgroup of $\mathrm{Aut}({}^2G_2(q^2))$ is elementary abelian of order 8. Thus in both cases the Sylow subgroups are abelian for all but one prime.

For the Ree groups ${}^2F_4(q^2)$, only the primes 2 and 3 matter. But the Tits group ${}^2F_4(2)'$ is contained in ${}^2F_4(q^2)$ and contains elements of order 6.

For S of type G_2, ${}^3D_4$ or F_4, only the primes 2,3 and the defining characteristic p are candidates for p_1, p_2. But in groups of type G_2 over fields of odd order there exist involutions with centralizer of type $A_1 \circ A_1$, hence containing unipotent elements, and over fields of characteristic different from 3 there exist elements of order 3 with centralizer of type A_2 or ${}^2A_2$, both containing elements of order 2 and unipotent elements (of order p). This deals with $G_2(q)$. Now we have containments $G_2(q) \leq {}^3D_4(q) \leq F_4(q)$, thus the latter two groups contain elements of the required orders.

For S of type E_6, ${}^2E_6$ and E_7, the primes 2,3,5 and the defining characteristic p have to be considered. Since $F_4(q) \leq {}^{(2)}E_6(q) \leq E_7(q)$ only the prime 5 needs attention. By Lemma 5 and the order formula for $E_6(q)$ (see [3, 2.9]) the Sylow 5-subgroup of $G = E_6(q)$ is abelian unless $5|(q-1)$. But there exist elements of order $q-1$ with centralizer of type $D_5(q)$ in G. Similarly, the Sylow 5-subgroup of $G = {}^2E_6(q)$ is abelian unless $5|(q+1)$, and there exist elements of order $q+1$ with centralizer of type ${}^2D_5(q)$ in G. Finally, if the Sylow 5-subgroup of $E_7(q)$ is non-abelian, then $5|(q^2-1)$, and we are done by the previous two cases.

For S of type E_8, the primes 2,3,5,7 and the defining characteristic p have to be considered. Using $E_7(q) \leq E_8(q)$, we are left with the prime 5 when $5 \not| (q^2-1)$, and the prime 7. By Lemma 5 the Sylow 7-subgroups are abelian unless $7|(q^2-1)$. A subgroup of type $E_6 \circ A_2$ shows that in this case all orders of the form $7p_2$ with $p_2 \in \{2,3,5,p\}$ occur. A subgroup of type $A_4 \circ A_4$ shows that all orders of the form $5p_2$, $p_2 \in \{2,3,p\}$ occur.

This completes the investigation of groups of exceptional type. If S is of type A_1, only the Sylow 2-subgroups can be non-abelian. For the remaining classical groups of Lie type, we make use of the natural subgroups introduced above. For $G = \mathrm{PGL}_n(q)$, $n \geq 3$, assume that $2 \neq p \not| q$ is such that the Sylow p-subgroup of G is non-abelian. Thus, by Lemma 4, p divides at least two factors $(q^{k_i}-1)$, $k_1 < k_2 \leq n$, and by Corollary 6, $k_1 \leq k_2/3 \leq n/3$. In particular, p divides a factor $q^k - 1$ with $k \leq m := \lfloor (n+1)/2 \rfloor$. Hence any odd p different from the defining characteristic for which the Sylow p-subgroups of G are non-abelian divides the order of $\mathrm{GL}_m(q)$. Clearly, that order is also divisible by 2 and the defining prime. The central quotient of $\mathrm{GL}_m(q) \times \mathrm{GL}_{n-m}(q)$ in G thus contains elements of all required orders.

For $G = \mathrm{PGU}_n(q)$, $n \geq 3$, we may argue similarly, using that the exponents k_1, k_2 above have the same parity by Corollary 6.

The same argument applies if G is of symplectic or odd dimensional orthogonal type. Any prime with non-abelian Sylow subgroup already divides the order of $\mathrm{Sp}_{2m}(q)$, respectively $\mathrm{SO}_{2m+1}(q)$, and the natural subgroup produces all necessary product orders.

The case of even-dimensional orthogonal groups is again similar. □

3 Proof of Theorem A

Now we are ready to complete the proof of Theorem A, which we restate.

Theorem 10. *Let G be a finite group and $p \neq q$ prime integers. If G does not have any elements of order pq, then one of the following holds:*

(i) *The Sylow p-subgroups or the Sylow q-subgroups of G are abelian.*

(ii) $G/O_{\{p,q\}'}(G) = M$ *and* $\{p, q\} = \{5, 13\}$ *or* $\{7, 13\}$.

Proof. First, we notice that the hypothesis is inherited by quotients and subgroups. We argue by induction on $|G|$. Let N be a normal subgroup of G. Assume first that neither p nor q divides $|N|$. Hence $N \leq O_{\{p,q\}'}(G)$. By the inductive hypothesis either (i) holds for G/N, and hence for G, or

$$M \cong \frac{G/N}{O_{\{p,q\}'}(G/N)} \cong G/O_{\{p,q\}'}(G) \text{ and } \{p, q\} = \{5, 13\} \text{ or } \{7, 13\},$$

as desired.

Now we may assume that, for instance, p divides $|N|$. Assume that q does not divide $|N|$. Let Q be a Sylow q-subgroup of G. We have that Q acts coprimely on N and we deduce that N has a Q-invariant Sylow p-subgroup P. Thus QP is a subgroup of G. By our hypothesis, the action of Q on P is Frobenius. This implies, by 12.6.15 of [9], for instance, that Q is cyclic or generalized quaternion. In the first case we are done so we may assume that Q is generalized quaternion and $q = 2$. By the Brauer-Suzuki theorem (see Theorem 45.1 of [7]), $|Z(G/O_{2'}(G))| = 2$. It follows from our hypothesis that p does not divide $|G/O_{2'}(G)|$ so a Sylow p-subgroup of $O_{2'}(G)$ is a Sylow p-subgroup of G. Since Q acts coprimely on $O_{2'}(G)$, we deduce that there exists a Q-invariant Sylow p-subgroup R of $O_{2'}(G)$. Now, QR is a Frobenius group with kernel R. Since R admits a fixed point free automorphism of order 2, we have that R is abelian, as desired. This means that we may assume that pq divides the order of any non-trivial normal subgroup of G.

Suppose that N_1 and N_2 are two different minimal normal subgroups of G. We know that there exists $n_1 \in N_1$ of order p and $n_2 \in N_2$ of order q, so the order of $n_1 n_2$ is pq. This contradicts our hypothesis, so we conclude that G has a unique minimal normal subgroup N.

Since pq divides $|N|$, we deduce that N is a direct product of copies of a non-abelian simple group S. In particular, pq divides $|S|$ and, the argument in the previous paragraph shows that $N = S$. This implies that G is isomorphic to a subgroup of $\mathrm{Aut}(S)$ containing S and the result follows from Lemmas 1, 2 and Theorem 9. □

4 Applications and Examples

We begin this section giving our new proof of the Theorem of Chigira, Iiyori and Yamaki [4].

Corollary 11 (Chigira, Iiyori and Yamaki). *Every non-abelian Sylow subgroup of a finite group of even order contains a non-trivial element that commutes with an involution.*

Proof. If a Sylow p-subgroup of a finite group of even order does not have any elements that commute with an involution, then the group does not have elements of order $2p$ and $p > 2$. If we are taking a non-abelian Sylow p-subgroup then, by Theorem A, we have that the Sylow 2-subgroups of G are abelian. By Walter's characterization of groups with abelian Sylow 2-subgroups, we have that G has normal subgroups $N \leq M$ such that $N = O_{2'}(G)$, M/N is the direct product of an abelian 2-group and non-abelian simple groups with abelian Sylow 2-subgroups and G/M has odd order. Furthermore, the non-abelian simple groups with abelian Sylow 2-subgroups are $\mathrm{PSL}(2, 2^f)$, $\mathrm{PSL}(2, q)$ where $q \equiv 3 \pmod 8$ or $q \equiv 5 \pmod 8$, J_1 or a Ree group ${}^2G_2(q)$. (See [10] or Theorem XI.13.7 of [8] and [1]).

We want to see that the Sylow p-subgroups of G are abelian. This contradiction will complete the proof of the corollary. Assume first that p divides $|N|$. Let S a Sylow 2-subgroup of G. By coprime action, there exists an S-invariant Sylow p-subgroup R of N. Then SR is a subgroup of G without elements of order $2p$. This implies that the action of S on R is Frobenius. Hence, since we knew that S is abelian, we deduce from 12.6.15 of [9] that S is cyclic. But this implies that M/N is a cyclic 2-group. It is easy to see that this implies that $G = M$. Hence, R is a Sylow p-subgroup of G that admits a fixed point free automorphism of order 2. We conclude, as desired, that the Sylow p-subgroups of G are abelian.

Therefore we may assume that $N = 1$ and even that $F(G) = 1$. Also, we may assume that p divides the order of each of the non-abelian simple groups that appear as direct factors of M. Hence, we deduce (as in the proof of Theorem A) that M is a non-abelian simple group and $G \leq \mathrm{Aut}(M)$.

Now note that all Sylow subgroups of $J_1 = \mathrm{Aut}(J_1)$ are abelian. By Lemma 7 the groups $\mathrm{Aut}(\mathrm{PSL}_2(q))$ and $\mathrm{Aut}({}^2G_2(q))$ have abelian Sylow p-subgroups for $p > 2$ except possibly if p is the order of some field automorphism of $\mathrm{PSL}_2(q)$. But any field automorphism centralizes the group over the prime field, which is of even order.

For the Ree groups ${}^2G_2(q)$ it suffices to note that it has abelian Sylow p-subgroups for every $p \neq 3$ and that it has elements of order 6. □

Finally, we give two infinite families of counterexamples that show that we cannot replace the word "abelian" by "cyclic" in the statement of Theorem A. For the simple group $G = F_4(q)$, q any prime power, let p_1, p_2, p_3 be Zsigmondy-primes dividing $\Phi_3(q)$, $\Phi_4(q)$, $\Phi_6(q)$ respectively. Then the

Sylow p_i-subgroups of G are homocyclic of rank 2, and G doesn't contain elements of order p_ip_j for any $i \neq j$. Similarly, for $G = E_8(q)$ we may take Zsigmondy primes p_1, p_2 dividing $\Phi_5(q)$, $\Phi_8(q)$ respectively.

References

[1] E. Bombieri, Thompson's problem ($\sigma^2 = 3$)., Invent. Math. **58** (1980), 77–100.

[2] M. Broué and G. Malle, Théorèmes de Sylow génériques pour les groupes réductifs sur les corps finis. Math. Ann. **292** (1992), 241–262.

[3] R.W. Carter, *Finite groups of Lie type*. Wiley-Interscience, New York, 1985.

[4] N. Chigira, I. Iiyori and H. Yamaki, Non-abelian Sylow subgroups of finite groups of even order. Invent. Math. **139** (2000), 525–539.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[6] D. Gorenstein, R. Lyons and R. Solomon, *The classification of the finite simple groups, Number 3*. Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 1994.

[7] B. Huppert, *Character theory of finite groups*, de Gruyter Expositions in Mathematics **25**, de Gruyter, Berlin, 1998.

[8] B. Huppert and N. Blackburn, *Finite groups III*, Springer-Verlag, New York, 1982.

[9] W. R. Scott, *Group theory*, Dover, New York, 1987.

[10] J. Walter, The characterization of finite groups with abelian Sylow 2-subgroups. Ann. Math. **89** (1969), 405–514.

[11] L.C. Washington, *Introduction to cyclotomic fields*. 2nd ed. Graduate Texts in Math. 83, Springer, New York, 1997.