Canad. Math. Bull. Vol. **29** (2), 1986

THE NILPOTENCY CLASS OF THE p-SYLOW SUBGROUPS OF $GL(n, q)$ WHERE $(p, q) = 1$

BY
ARIE BIALOSTOCKI

ABSTRACT. Formulae for the nilpotency class of the p-sylow subgroups of $GL(n, q)$ where $(p, q) = 1$ are derived. These formulae are used in author's following paper: "On the other $p^\alpha q^\beta$ theorem of Burnside".

A. **Introduction**. In [7] A. Weir described, for an odd prime p, the structure of the p-Sylow subgroups of $GL(n, q)$ where $(p, q) = 1$, and in [2] R. Carter and P. Fong described the structure of the 2-Sylow subgroups of $GL(n, q)$ where $(2, q) = 1$. In a forthcoming paper [1] we need formulae for the nilpotency class of the above subgroups and the aim of this paper is to derive these formulae.

Most of our notation is standard, in particular $S_p(G)$ denotes the p-Sylow subgroup of G. We denote by C_{p^s} and S_{2^s} the cyclic group of order p^s and the semidihedral group of order 2^{s+1}, respectively. Moreover, exp (G), class (G) and $A \wr B$ denote the exponent of G, the nilpotent class of G and the wreath product of A and B, respectively.

In Section B we provide some preliminary Propositions and in Section C we use them in order to prove two main Lemmas which imply our formulae, stated in Theorem C.3.

B. **Preliminary propositions**

PROPOSITION B.1. (a) *If P_1 and P_2 are p-groups, then*

$$\exp (P_1 \times P_2) = \max \{\exp (P_1), \exp (P_2)\}.$$

(b) *If P is a p-group, then*

$$\exp (P \wr C_p) = p \cdot \exp (P).$$

PROOF. The proof of (a) is trivial and for (b) see Lemma 2.4 of [3].

As the groups $S_p(\mathrm{Sym}(n))$ and $S_p(GL(n, q))$, where $(p, q) = 1$, are constructed from familiar groups using wreath products and direct products the following Proposition B.2 is an immediate consequence of Proposition B.1.

Received by the editors November 8, 1984, and, in revised form, February 14, 1985.

The author wishes to acknowledge help from Canadian N.S.E.R.C. Research Grants which supported this work.

AMS Subject Classification (1980): 20G40, 20D15.

PROPOSITION B.2. *Let n be a positive integer, and let p be a prime. If q is a power of a prime such that $(p, q) = 1$ and $p|q - 1$, then the following holds:*

(a) *If $q \neq 3 \pmod 4$ whenever $p = 2$ and if $p^s \| q - 1$, then* $\exp(S_p(\mathrm{GL}(n, q))) = p^{s+[\log_p n]}$ *and in particular* $\exp(S_p(\mathrm{GL}(p^\alpha, q))) = p^{s+\alpha}$ *for* $\alpha \geq 0$.

(b) If $p = 2$, $q = 3 \pmod 4$ and if $2^s \| q^2 - 1$, then $\exp(S_2(\mathrm{GL}(1, q))) = 2$ *and for* $n \geq 2$ $\exp(S_2(\mathrm{GL}(n, q))) = 2^{s+[\log_2[n/2]]}$. *In particular,* $\exp(S_2(\mathrm{GL}(2^\alpha, q))) = 2^{s+\alpha-1}$ for $\alpha \geq 1$.

PROPOSITION B.3. *Let G be a p-group, $G = BC$, where $B \lhd G$ and B is a direct product of p isomorphic copies P_i of P, $1 \leq i \leq p$. Moreover, suppose that $|G:B| = p$ and C is cyclic group which is generated by y. Assume that y permutes by the conjugation the P_i's in a p-cycle, but not necessarily $y^p = 1$ (or, equivalently, not necessarliy $G = P_1 \wr C_p$). Then the following hold:*

(a) *If* $\mathrm{class}(P) \geq n$, *then* $\mathrm{class}(G) \geq pn$,

(b) *If $P = C_{p^s}$, then* $\mathrm{class}(G) \geq (p - 1)s + 1$. *Equality holds if $G = P_l \int C_p$.*

PROOF. (a) We consider two cases:

I. $p > 2$

Since $\mathrm{class}(G) \geq n$, there are $x_1, x_2, \ldots, x_n \in P_1$ such that $[x_1, x_2, \ldots, x_n] \neq 1$. Defining the commutator u as:

$$u = [x_1, (p - 1)y, x_2, (p - 1)y, \ldots, x_n, (p - 1)y],$$

where $(p - 1)y$ denotes a successive block of y's of length $p - 1$, it follows that the projection of u on P_1 equals $[x_1, x_2, \ldots, x_n] \neq 1$ and the Proposition is proved in case I.

II. $p = 2$

Since $\mathrm{class}(P) \geq n$, there are $x_1, x_2, \ldots, x_n \in P_1$ such that $[x_n, [x_{n-1}, \ldots [x_2, x_1^{-1}] \ldots]] \neq 1$, see [5, 9.1]. Defining the commutator u as

$$[x_1, (p - 1)y, x_2, (p - 1)y, \ldots, x_n, (p - 1)y]$$

it follows that the projection of u on P_1 equals

$$[\ldots[[x_1^{-1}, x_2]^{-1}, x_3]^{-1}, \ldots, x_n]^{-1} = [x_n, [x_{n-1} \ldots [x_2, x_1^{-1}] \ldots]] \neq 1$$

and the Proposition is proved in case II as well.

(b) Follows from [6].

PROPOSITION B.4. *If $G = AB$ where $A \lhd G$, then elements of the lower central series $\{L_i(G)\}$, can be expressed in the form: $L_i(G) = A_i L_i(B)$, where $\{L_i(B)\}$ is the lower central series of the subgroup B and the A_i's are defined inductively:*

$$A_1 = A \qquad A_{i+1} = [G, A_i] \qquad i = 2, 3, \ldots$$

PROOF. See [4, p. 378].

https://doi.org/10.4153/CMB-1986-035-4 Published online by Cambridge University Press

C. **The main result**.

LEMMA C.1. *If* $G = C_{p^s} \wr S_p(\mathrm{Sym}(p^\alpha))$ *for* $\alpha \geq 1$, *then* class$(G) = m$, *where* $m = ((p-1)s+1)p^{\alpha-1}$.

PROOF. By Proposition B.3(b) it follows that class $(C_{p^s} \wr C_p) = (p-1)s+1$ and thus our Lemma holds for $\alpha = 1$ and every s. Since $C_p \wr S_p(\mathrm{Sym}(p^\alpha)) \cong S_p(\mathrm{Sym}(p^{\alpha+1}))$, [4, II, 15.3] implies that class $(C_p \wr S_p(\mathrm{Sym}(p^\alpha))) = p^\alpha$, hence the Lemma holds for $s = 1$ and every α. Using Proposition B.3 we get:

$$\text{Class } (C_{p^s} \wr S_p(\mathrm{Sym}(p^\alpha))) \geq ((p-1)s+1)p^{\alpha-1}$$

for every prime p and every positive integers s and α. Hence it is left to prove the opposite inequality. We use the following notation: Let $C_{p^s} \wr S_p(\mathrm{Sym}(p^\alpha)) = B \cdot S_p(\mathrm{Sym}(p^\alpha))$, where the base group $B = B_1 \times B_2 \times \ldots \times B_{p^\alpha}$ is a direct product of p^α copies of C_{p^s}, and let

$$D_i = B_{(i-1)p^{\alpha-1}+1} \times \ldots \times B_{ip^{\alpha-1}} \text{ for } 1 \leq i \leq p.$$

Thus, $B = D_1 \times D_2 \times \ldots \times D_p$. By [4, II, 15.3], Proposition B.4 and by the commutativity of B it suffices to prove that every commutator of the form $[y, u_1, u_2, \ldots, u_m]$ equals 1, where:

$$m = ((p-1)s+1)p^{\alpha-1}, \; y \in B \text{ and } u_j \in S_p(\mathrm{Sym}(p^\alpha)) \text{ for } 1 \leq j \leq m.$$

In fact we may assume that the u_j's belong to $\{g_1, \ldots, g_\alpha\}$, a set of generators of $S_p(\mathrm{Sym}(p^\alpha))$, see [4, p. 379], which are defined as follows:

Let $G = S_p(\mathrm{Sym}(p^\alpha))$, act on the set $\{1, 2, \ldots, p^\alpha\}$. If $1 \leq t \leq \alpha$ and $1 \leq i \leq p^\alpha$, then

$$g_t(i) = \begin{cases} i + p^{t-1} (\mathrm{mod}\ p^t) & 1 \leq i \leq p^t \\ i & p^t + 1 \leq i \leq p^\alpha \end{cases}$$

Consider the following facts which will be used in the sequel:

(a) Since B is an abelian normal subgroup of G, it follows that the mapping $y \to [y, u]$, where $y \in B$ and $u \in S_p(\mathrm{Sym}(p^\alpha))$, is an endomorphism of B.

(b) If d_i is an element of D_i for $1 \leq i \leq p$, then the mapping $d_i \to [d_i, pg_\alpha]$ maps d_i into $e_1 \cdot e_2 \cdot \ldots \cdot e_p$ where $e_j \in D_j$ for $1 \leq j \leq p$ and e_j is given by the following formula:

If $p \neq 2$ then:

$$e_j = \begin{cases} 1 & \text{if } j = i \\ (g_\alpha^{-k} d_i g_\alpha^k)^{x_j} \text{ where } x_j = \binom{p}{k}(-1)^{k+1}, & \\ \text{with } 1 \leq k \leq p-1 \text{ such that } j = i + k \ (\mathrm{mod}\ p) & \text{if } j \neq i \end{cases}$$

https://doi.org/10.4153/CMB-1986-035-4 Published online by Cambridge University Press

If $p = 2$ then

$$e_j = \begin{cases} d_i^{\alpha} & \text{if } j = i \\ (g_\alpha^{-1} d_i g_\alpha)^{-2} & \text{if } j \neq i \end{cases}$$

It follows that for every prime p, $[d_i, pg_\alpha]$ is contained in the subgroup of B generated by the elements $[g_\alpha^{-k} d_i g_\alpha^k]^p$ where $0 \leq k \leq p - 1$.

(c) By (b) it follows that the mapping $y \rightarrow [y, pg_\alpha]$ where $y \in B$, maps B into its subgroup $B^p = \{y^p | y \in B\}$.

(d) If $d_1 \in D_1$ and $1 \leq r \leq p - 1$, then the projection of $[d_1, rg_\alpha]$ on D_1 equals $d_1^{(-1)^r}$.

Assume that the Lemma does not hold for a certain prime p and fixing that prime consider a counter example such that $s + \alpha$ is minimal. It follows that there exists a $y \in B$ and a finite sequence $u_1, \ldots, u_\ell$ of elements of the set $\{g_1, \ldots, g_\alpha\}$ such that $[y, u_1, \ldots, u_\ell] \neq 1$ and $\ell \geq m = ((p - 1)s + 1)p^{\alpha-1}$. We may assume that among all choices of y and $u_1, \ldots, u_\ell$ which satisfy the conditions above, we have chosen one for which ℓ is maximal. Thus (d) yields that $u_1 = u_2 = \ldots = u_{p-1} = g_\alpha$. Now we consider two cases:

Case (a):

Assume that among the u_j's in the commutator $[y, u_1, \ldots, u_\ell]$ there exists a consecutive block of g_α's of length p, and let $u_t, u_{t+1}, \ldots, u_{t+p-1}$ be the first such block, that is either $t = 1$ or $u_{t-1} \neq g_\alpha$. If $t = 1$ then $u_1 = u_2 = \ldots = u_p = g_\alpha$ and by (c) it follows that

$$[y, u_1, \ldots, u_\ell] = [\tilde{y}, u_{p+1}, \ldots, u_\ell]$$

where $\tilde{y} \in B^p$. Now s is reduced by 1, hence the minimality of $s + \alpha$ and the fact that $\ell - p \geq m - p = ((p - 1)s + 1)p^{\alpha-1} - p \geq ((p - 1)(s - 1) + 1)p^{\alpha-1}$ for $\alpha > 1$ imply that $[y, u_1, \ldots, u_\ell] = 1$ in this subcase. If $t > 1$, then

$$[y, u_1, \ldots, u_\ell] = [y, u_1, \ldots, u_t, \ldots, u_{t+p-1}, \ldots, u_\ell]$$

where $u_{t-1} \neq g_\alpha$. It is clear that the projection of $z = [y, u_1, \ldots, u_{t-1}]$ on D_i for $2 \leq i \leq p$ equals 1. Hence by (a) it follows that

$$[y, u_1, \ldots, u_t, \ldots, u_{t+p-1}] = [z, pg_\alpha] \in \langle (g_\alpha^{-k} z g_\alpha^k)^p | 0 \leq k \leq p - 1 \rangle \equiv T.$$

Thus $[T, u_{t+p}, \ldots, u_\ell] \neq 1$ which implies that there exists a certain k, $0 \leq k \leq p - 1$, for which $[(g_\alpha^{-k} z g_\alpha^k)^p, u_{t+p}, \ldots, u_\ell] \neq 1$ or equivalently

$$\begin{aligned} [g_\alpha^{-k} z^p g_\alpha^k, u_{t+p}, \ldots, u_\ell] &= \\ &= [g_\alpha^{-k} [y, u_1, \ldots, u_{t-1}]^p g_\alpha^k, u_{t+p}, \ldots, u_\ell] = \\ &= [g_\alpha^{-k} [y^p, u_1, \ldots, u_{t-1}] g_\alpha^k, u_{t+p}, \ldots, u_\ell] \neq 1. \end{aligned}$$

Now it follows that:

$$w \equiv [y^p, u_1, \ldots, u_{t-1}, g_\alpha^k u_{t+p} g_\alpha^{-k}, \ldots, g_\alpha^k u_\ell g_\alpha^{-k}] \neq 1.$$

Again s is reduced by 1, hence by the minimality of $s + \alpha$ and the fact that $\ell - p \geq m - p = ((p-1)s + 1)p^{\alpha-1} - p \geq ((p-1)(s-1) + 1)p^{\alpha-1}$ for $\alpha > 1$, it follows that $w = 1$ and this contradiction settles case (a).

Case (b):

Assume that among the u_j's in the commutator $[y, u_1, u_2, \ldots, u_\ell]$, the length of the maximal consecutive block of g_α's does not exceed $p - 1$. In this case if we omit all the g_α's in the commutator $[y, u_1, u_2, \ldots, u_\ell]$ then by (d) we get that $[y, u_1, u_2, \ldots, u_\ell] = [\ldots[y^{\pm 1}, v_1]^{\pm 1}, \ldots, v_t]^{\pm 1}$, where the v_j's are the u_i's in the same order after the omission of the g_α's. The sign $+1$ or -1 depends on whether the corresponding omitted block was of even or odd length. We have reduced α by 1, hence the minimality of $s + \alpha$ and the fact that $t \geq m/p = ((p-1)s + 1)p^{\alpha-2}$ imply that $[y_1, u_1, u_2, \ldots, u_\ell] = 1$, a contradiction. Lemma C1 is proved.

LEMMA C2. *If S_{2^s} denotes the semidihedral group of order 2^{s+1} and $G = S_{2^s} \wr S_2(\mathrm{Sym}(2^\alpha))$, then* $\mathrm{class}(G) = s2^\alpha$.

PROOF. Since class $(S_{2^s}) = s$, Proposition B.3(a) implies that class $(G) \geq s2^\alpha$. Hence it suffices to prove the opposite inequality. Let $G = B \cdot S_2(\mathrm{Sym}(2^\alpha))$, where the base group B is a direct product of 2^α copies of S_{2^s}, $B = B_1 \times B_2 \times \ldots \times B_{2^\alpha}$. Moreover, let x_i, $1 \leq i \leq 2^\alpha$, be the generator of the cyclic subgroup of B_i of order 2^s. Denote by C_i, $1 \leq i \leq 2^\alpha$, the cyclic subgroup of B_i generated by x_i^4. Clearly $|B_i : C_i| = 8$ and it is easy to verify that B_i/C_i is the dihedral group of order 8. Finally consider C, the subgroup of B which is the direct product of the C_i's, $1 \leq i \leq 2^\alpha$. It follows that $G/C \cong (B_1/C_1) \wr S_2(\mathrm{Sym}2^\alpha)$ and since $B_1/C_1 \cong S_2(\mathrm{Sym}(4))$, we obtain that $G/C \cong S_2(\mathrm{Sym}(2^{\alpha+2}))$. If $\{L_i(G)\}$ denotes the lower central series of G, then Proposition B.4 and the fact that $\mathrm{class}(S_2(\mathrm{Sym}(2^{\alpha+2}))) = 2^{\alpha+1}$ imply that $L_{2^{\alpha+1}}(G) \subset C$. Now, since $|C| = 2^{(s-2)2^\alpha}$ it follows that $L_m(G) = 1$ where $m = 2^{\alpha+1} + (s-2)2^\alpha = s2^\alpha$, and Lemma C.2 is proved.

The structure of $S_p(\mathrm{GL}(n, q))$ where $(p, q) = 1$, Lemma C.1, Lemma C.2 and the fact that

$$\mathrm{class}(A \times B) = \max\{\mathrm{class}(A), \mathrm{class}(B)\},$$

imply our main Theorem.

THEOREM C.3. *Let n be a positive integer, p a prime and q a power of a prime such that $p|q-1$. Then the following hold:*

(a) *If* $q \not\equiv 3 \pmod 4$ *whenever $p = 2$ and if $p^s \| q - 1$, then* $\mathrm{class}(S_p(\mathrm{GL}(n, q))) = ((p-1)s + 1)p^{[\log_p n] - 1}$ *and in particular* $\mathrm{class}(S_p(\mathrm{GL}(p^\alpha, q))) = ((p-1)s + 1)p^{\alpha-1}$, for $\alpha \geq 1$.

(b) *If* $p = 2$, $q = 3 \pmod 4)$ *and if* $2^s \| q^2 - 1$, *then class* $(S_2(GL(1,q))) = 1$ *and for* $n \geq 2$, *class* $(S_2(GL(n,q))) = s2^{[\log_2[n/2]]}$. *In particular class* $(S_2(GL(2^\alpha, q))) = s2^{\alpha-1}$ for $\alpha \geq 1$.

ACKNOWLEDGMENT: This work is partially based on author's doctoral research at Tel-Aviv University and it was completed at the University of Calgary. I am grateful to my thesis advisor Prof. M. Herzog for his guidance and to the University of Calgary for their kind hospitality.

REFERENCES

1. A. Bialostocki, *On the other* $p^\alpha q^\beta$ *theorem of Burnside (Submitted)*.

2. R. Carter and P. Fong, *The Sylow 2-Subgroups of the Finite Classicial Groups*, J. Algebra **1**, (1964), pp. 139–151.

3. M. Herzog and C. E. Praeger, *On the order of linear groups of fixed finite exponent*, Journal of Algebra Vol. 43, No.1 (1976), pp. 216–220.

4. B. Huppert, *Endliche Gruppen I*, Springer Verlag, Berlin Heidelberg, New York, 1967.

5. R. Kochendörffer, *Group Theory*, McGraw-Hill, London, 1970.

6. H. Liebeck, *Concerning Nilpotent Wreath Products*, Proc. Cambridge Philos. Soc. **58** (1962), pp. 443–451.

7. A. Weir, *Sylow p-Subgroups of the Classical Groups Over Finite Fields with Characteristic Prime to p*, Proc. Amer. Math. Soc. **6** (1955), pp. 529–533.

UNIVERSITY OF CALGARY
CALGARY, ALBERTA