RENDICONTI
*del*
SEMINARIO MATEMATICO
*della*
UNIVERSITÀ DI PADOVA

ANDREA LUCCHINI

# Generating wreath products and their augmentation ideals

*Rendiconti del Seminario Matematico della Università di Padova*, tome 98 (1997), p. 67-87

<http://www.numdam.org/item?id=RSMUP_1997__98__67_0>

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

# Generating Wreath Products and their Augmentation Ideals.

ANDREA LUCCHINI (*)

*To Giovanni Zacher, in occasion of his 70th birthday*

## Introduction.

For a group $G$, let $d(G)$ denote the minimum of the cardinalities of the generating sets of $G$. In this paper we will study $d(W)$ for the wreath product $W = H \wr G$ of a finite group $H$ and a finite permutation group $G$.

In [3] and [4] this problem is discussed when $H$ and $G$ are nilpotent and with respect to the regular permutation representation of the group $G$.

In [13] we have considered the case of soluble groups, using a formula, due to Gaschütz, that allows us to express the minimum number of generators of a finite soluble group $G$ as a function of some integers coming from the study of the chief factors of the group $G$. Gaschütz's result has been generalized to arbitrary finite groups by Cossey, Gruenberg and Kovács: if $I_G$ is the augmentation ideal of $\mathbb{Z}G$ then $d(I_G)$, its minimum number of generators as a $G$-module, can be computed from the knowledge of the structure of the irreducible $G$-modules. Applying this result we will prove:

PROPOSITION 1. *If $H$ is a finite group and $G$ is a transitive permutation group of degree $n$, then*

$$d(I_{H \wr G}) = \max\left(d(I_{H/H' \wr G}), \left[\frac{d(I_H) - 2}{n}\right] + 2\right).$$

(*) Indirizzo dell'A.: Dipartimento di Elettronica per l'Automazione, Università degli Studi di Brescia, Via Branze, 25123 Brescia, Italy.

The connection between $d(G)$ and $d(I_G)$ is: $d(G) = d(I_G) + \mathrm{pr}(G)$ where $\mathrm{pr}(G)$ is a non negative integer, called the presentation rank. The class of groups with zero presentation rank is known to be large and contains all soluble groups. Therefore this proposition can be considered as a generalization of a similar result ([13] Theorem 1) proved for the minimum number of generators of the wreath product of soluble groups.

From Proposition 1 we will deduce:

THEOREM 2. *If $H$ is a finite soluble group and $G$ is a transitive permutation group of degree $n$, then*

$$d(H \wr G) = \max\left(d\left(\frac{H}{H'} \wr G\right), \left[\frac{d(H)-2}{n}\right] + 2\right).$$

A similar result is proved in [13], but assuming that $G$ is soluble and only with respect to the regular permutation representation of $G$.

In Theorem 2 we assume that $H$ is soluble; this hypothesis is necessary. In section 3 we will describe an example with $H$ perfect for which our result does not hold.

Proposition 1 and Theorem 2 restrict the problem to the particular case $H$ abelian. We will study this problem in two particular situations.

In section 4 we will consider $W = A \wr G$ with $A$ abelian and $G$ an arbitrary finite group with respect to its regular permutation representation. The same problem is discussed in [13] (Theorem 2) but with the hypothesis that $G$ is soluble. We will prove that a similar result holds in the general case; precisely for every non trivial irreducible $G$-module $M$ define

$$h_G(M) = \left[\frac{\dim_{\mathrm{End}_G(M)} H^1(G, M) - 1}{\dim_{\mathrm{End}_G(M)} M}\right] + 2,$$

denote with $d_p(A)$ the minimum number of generators of the Sylow $p$-subgroup of $A$ and define

$$\varrho_p = \max_M h_G(M) + d_p(A)$$

where $M$ ranges over the set of non trivial irreducible $\mathbb{F}_p G$-modules, with $\varrho_p = 0$ if every irreducible $\mathbb{F}_p G$-module is trivial. Then we have:

PROPOSITION 3. *If $A$ is a finite abelian group then*

$$d(I_{A \wr G}) = \max_{p \mid |A|} (d(I_{A \times G}), \varrho_p).$$

THEOREM 4. *If $A$ is a finite abelian group then*

$$d(A \wr G) = \max_{p \mid |A|} (d(A \times G), \varrho_p).$$

Theorem 4 has the following consequence:

COROLLARY 5. *Let $A$ be an abelian finite group, let $G$ be a finite group and suppose that for every prime $p$ dividing $|A|$ and every non trivial irreducible $\mathrm{F}_p G$-module $M$, $M$ is not isomorphic as a $G$-module to a complemented chief factor of $G$; then*

$$d(A \wr G) = \max_{q} (d(A \times G), d(A) + 1, d_q(A) + 2)$$

where $q$ *ranges over the set of the prime numbers dividing* $|A|$ *and such that* $G$ *is not* $q$*-soluble.*

In particular:

COROLLARY 6. *If $A$ is abelian and $A$ and $G$ have coprime orders then*

$$d(A \wr G) = \max (d(A) + 1, d(G)).$$

COROLLARY 7. *If $p$ is a prime and $S$ is a finite non abelian simple group then*

(i) $d(\mathbb{Z}_p \wr S) = 2$ *if $p$ does not divide* $|S|$;

(ii) $d(\mathbb{Z}_p \wr S) = 3$ *if $p$ divides* $|S|$.

In section 5 we consider the wreath product $W = A \wr \mathrm{Sym}(n)$ of an abelian group $A$ with the symmetric group of degree $n$, proving:

THEOREM 8. *If $A$ is a non trivial abelian group, then*

(i) $d(A \wr \mathrm{Sym}(2)) = d(A) + 1$;

(ii) *if* $n \geqslant 3$ *then* $d(A \wr \mathrm{Sym}(n)) = \max_{p \mid |A|} (2, d_p(A), d_2(A) + 1)$.

In [20] Gruenberg and Roggenkamp use a similar elaboration of Gaschütz's methods to study the minimal number of generators of semidirect products $A \rtimes G$, where $A$ is a semisimple $G$-module. The wreath

product $W = A \wr G = A^n \rtimes G$ is a particular case of this situation ($A^n$ is not in general a semisimple $G$-module but one may consider the quotient over the radical). So Theorem 4 and Theorem 8, but not the corresponding results for the augmentation ideal, could be deduced from Proposition 4 of [20].

The results proved in this paper will be applied in section 6 to compute the minimum number of generators of $\mathrm{Aut}(S^n)$, the automorphism group of the direct product of $n$ copies of a finite non abelian simple group $S$. We will obtain:

PROPOSITION 9. *Suppose that $S$ is a finite non abelian simple group and let $\mathrm{Out}S = \mathrm{Aut}S/S$ be the outer automorphism group of $S$. If $n \neq 1$ then*

$$d(\mathrm{Aut}(S^n)) = \max\left(2, d_2\left(\frac{\mathrm{Out}S}{(\mathrm{Out}S)'}\right) + 1\right).$$

1. – Given a finite group $G$ we will denote with $I_G$ the augmentation ideal of $ZG$ and with $d(I_G)$ the minimum number of generators of $I_G$ as a $ZG$-module. A formula, proved by Cossey, Gruenberg and Kovács ([5] Theorem 3) allows us to express $d(I_G)$ as a function of some integers coming from the study of the structure of the irreducible $G$-modules.

In this section we describe this formula and introduce some related remarks.

Let $M$ be an irreducible $G$-module; we define the integer numbers $r_G(M)$, $s_G(M)$ and $h_G(M)$ by setting:

$$r_G(M) = \dim_{\mathrm{End}_G(M)} M\,, \qquad s_G(M) = \dim_{\mathrm{End}_G(M)} H^1(G, M)\,,$$

$$h_G(M) = \left[\frac{s_G(M) - 1}{r_G(M)}\right] + 2\,.$$

Cossey, Gruenberg and Kovács proved:

1.1. $d(I_G) = \max_M (d(G/G'), h_G(M))$ *where $M$ ranges over the set of non isomorphic non trivial irreducible $G$-modules.*

To compute $h_G(M)$ it is useful to remark (see [2] 2.10 and Theorem A):

1.2. $s_G(M) = \delta_G(M) + \dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M)$ *where* $\delta_G(M)$

*denotes the number of chief factors G-isomorphic to M and complemented in an arbitrary chief series of G and $C_G(M)$ is the centralizer in G of M.*

1.3. $\dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M) < r_G(M)$.

From 1.2 and 1.3 it can be easily deduced ([12] Lemma 1.5):

1.4. $h_G(M) \leqslant \max(2, \delta_G(M) + 1)$.

A consequence of this is:

1.5. *Let N be a normal subgroup of G with $N \leqslant G'$, then*

$$d(I_G) \leqslant \max_M (2, d(I_{G/N}), h_G(M))$$

*where M ranges over the set of non isomorphic non trivial irreducible G-modules such that $\delta_{G/N}(M) < \delta_G(M)$.*

PROOF. Suppose $d(I_G) > \max(2, d(I_{G/N}))$. By (1.1) there exists a non trivial irreducible $G$-module $M$ such that $d(I_G) = h_G(M)$. We have to prove $\delta_{G/N}(M) < \delta_G(M)$. First notice that $\delta_G(M) \neq 0$, otherwise (1.4) would imply $d(I_G) = h_G(M) \leqslant 2$. Now suppose, by contradiction, $\delta_G(M) = \delta_{G/N}(M) > 0$; then there exist two normal subgroups of $G$, say $K_1$ and $K_2$, such that $N \leqslant K_1 < K_2$ and $K_2/K_1$ is $G$-isomorphic to $M$; in particular this implies $N \leqslant C_G(M)$ but then $\mathrm{End}_G(M) \cong \mathrm{End}_{G/N}(M)$ and, by (1.2), $\dim_{\mathrm{End}_G(M)} H^1(G, M) = \dim_{\mathrm{End}_{G/N}(M)} H^1(G/N, M)$ so $d(I_G) = h_G(M) = h_{G/N}(M) \leqslant d(I_{G/N})$, a contradiction. ∎

On the other hand (see [18] p. 189-190):

1.6. $d(I_G) = 1$ *if and only if G is a cyclic group.*

So from (1.5) and (1.6) we can conclude:

1.7. *If G is not a cyclic group and N is a normal subgroup of G with $N \leqslant G'$, then*

$$d(I_G) = \max_M (2, d(I_{G/N}), h_G(M))$$

*where M ranges over the set of non isomorphic non trivial irreducible G-modules such that $\delta_{G/N}(M) < \delta_G(M)$.*

REMARK 1.8. Consider an arbitrary chief series of $G$

$$(*) \qquad 1 = A_t \trianglelefteq A_{t-1} \trianglelefteq \dots \trianglelefteq A_s = N \trianglelefteq \dots \trianglelefteq A_1 \trianglelefteq A_0 = G$$

passing through $N$. The assertion «$\delta_{G/N}(M) < \delta_G(M)$» means that in $(*)$ there exists an abelian complemented chief factor $A_i/A_{i+1}$ with $A_i \leq N$ such that $A_i/A_{i+1}$ is $G$-isomorphic to $M$. Since $M$ is a non trivial $G$-module, $G$ does not centralize $A_i/A_{i+1}$.

Another useful consequence of (1.1) and (1.4) is

1.9. *If $N$ is a normal subgroup of a finite group $G$ and $N \leq \mathrm{Frat}\, G$ then $d(I_{G/N}) = d(I_G)$.*

PROOF. It suffices to remark that the abelian chief factors of $G$ contained in $N$ are not complemented in $G$. ∎

The connection between $d(G)$ and $d(I_G)$ is given by a theorem of Roggenkamp ([17]) which states that

1.10. $d(G) = d(I_G) + \mathrm{pr}(G)$.

Here the non negative integer $\mathrm{pr}(G)$ is an invariant of the finite group $G$ called its presentation rank, whose definition comes from the study of relation modules ([9]). It is known that $\mathrm{pr}(G) = 0$ for many groups $G$, in particular we will use ([7] p. 263-264 and [8]):

1.11. *If $d(G) \leq 2$ then* $\mathrm{pr}(G) = 0$.

1.12. *If $G$ is a soluble group then* $\mathrm{pr}(G) = 0$.

We will need also the following result ([10] p.218):

1.13. *If $N$ is a soluble normal subgroup of $G$ and* $\mathrm{pr}(G) > 0$ *then* $d(G) = d(G/N)$.

2. – Let $H$ be a non trivial finite group and let $G$ be a transitive permutation group of degree $n$; $G$ acts on $B = H^n$ by the rule: $(h_1, \dots, h_n)^g = (h_{1g^{-1}}, \dots, h_{ng^{-1}})$ for every $(h_1, \dots, h_n) \in B$ and $g \in G$. This action of $G$ on $B$ leads to a semidirect product $W = B \rtimes G$, which is called the wreath product of $H$ and $G$ and it is denoted with the symbol $H \wr G$; the subgroup $B$ is called the base subgroup of the wreath product $W$.

In this section we will prove that the problem to compute $d(I_W)$ can be reduced to the case $H$ abelian.

Consider the derived subgroup $B'$ of $B$: $B' = (H')^n$ is a normal subgroup of $W$ with $W/B' \cong (H/H') \wr G$, so, by (1.7):

2.1. $d(I_W) = \max_M (2, d(I_{H/H' \wr G}), h_W(M))$ *where* $M$ *ranges over the set of non isomorphic non trivial irreducible* $G$*-modules such that* $\delta_{W/B'}(M) < \delta_W(M)$.

But if $A$ is an $H$-module then $A^n$ can be viewed as a $W$-module if we define $(a_1, \ldots, a_n)^{(h_1, \ldots, h_n)g} = (a_1^{h_1 g^{-1}}, \ldots, a_n^{h_n g^{-1}})$ and ([13] Propositon 1.3) the map $A \mapsto A^n$ gives a bijection between the set of non-central complemented chief factors of $H$ and the set of non isomorphic non trivial irreducible $G$-modules such that $\delta_{W/B'}(M) < \delta_W(M)$. So we have:

2.2. $d(I_W) = \max_A (2, d(I_{H/H \wr G}), h_W(A^n))$ *where* $A$ *ranges over the set of non isomorphic complemented chief factors of* $H$ *that are not centralized by* $H$.

We want to compare $h_H(A)$ with $h_W(A^n)$.

2.3. $r_W(A^n) = n r_H(A)$.

PROOF. It suffices to remark that $\mathrm{End}_W(A^n) \cong \mathrm{End}_H(A)$ (see [13] Lemma 1.6). ■

2.4. $s_W(A^n) = s_H(A)$.

PROOF. We have to prove $H^1(H, A) \cong H^1(W, A^n)$. Consider the cohomology sequence determined by the group extension

$$1 \to B \to W \to W/B \to 1$$

and denote, as usual, the $B$-fixed points in $A^n$ by $(A^n)^B$. Then we have the exact sequence:

$$(*) \quad 0 \to H^1(W/B, (A^n)^B) \xrightarrow{\inf} H^1(W, A^n) \xrightarrow{\mathrm{res}} \xrightarrow{\mathrm{res}} H^1(B, A^n)^W \xrightarrow{\tau} H^2(W/B, (A^n)^B),$$

where $\tau$ is the transgression ([15] p. 354). Since $A$ is a non trivial irreducible $H$-module $(A^n)^B = C_{A^n}(H^n) = (C_A(H))^n = 0$, so $H^1(W/B, (A^n)^B) = H^2(W/B, (A^n)^B) = 0$ and we obtain

$$(**) \qquad 0 \to H^1(W, A^n) \to H^1(B, A^n)^W \to 0.$$

To conclude the proof we have to show that $H^1(B, A^n)^W \cong H^1(H, A)$. Recall that $H^1(B, A^n) = \mathrm{Der}(B, A^n)/\mathrm{Inn}(B, A^n)$ where $\mathrm{Der}(B, A^n)$ is the set of all derivations from $B$ to $A^n$ and $\mathrm{Inn}(B, A^n)$ is the set of inner derivations; if $\delta \in \mathrm{Der}(B, A^n)$ and $w \in W$ then $b(\delta^w) = ((b^{w^{-1}})\delta)^w$ for every $b \in B$. Let $\delta + \mathrm{Inn}(B, A^n) \in H^1(B, A^n)^W$; for every $w \in W$ there exists $\alpha_w = (\alpha_1, \ldots, \alpha_n) \in A^n$ such that

$$(***) \qquad ((b^{w^{-1}})\delta)^w - b\delta = [b, \alpha_w] \text{ for all } b \in B.$$

Let $A_i = \{(a_1, \ldots, a_n) | a_j = 0 \text{ for } 1 \leqslant j \leqslant n, j \neq i\}$, $H_i = \{(h_1, \ldots, h_n) | h_j = 1 \text{ for } 1 \leqslant j \leqslant n, j \neq i\}$: $A^n = A_1 \times \ldots \times A_n$ and $B^n = H_1 \times \ldots \times H_n$. We claim that $H_i\delta \leqslant A_i$ for every $1 \leqslant i \leqslant n$. We prove this when $i = 1$, but the same argument holds for every $1 \leqslant i \leqslant n$. Let $\underline{h} = (h, 1 \ldots, 1) \in H_1$ and $w = (1, h_2, \ldots, h_n) \in H^n \leqslant W$; suppose $\underline{h}\delta = (a_1, a_2, \ldots, a_n) \in A^n$; by $(***)$

$$(a_1, a_2, \ldots, a_n)^{(1, h_2, \ldots, h_n)} - (a_1, a_2, \ldots, a_n) =$$

$$= (\underline{h}^{w^{-1}}\delta)^w - \underline{h}\delta = [\underline{h}, \alpha_w] = ([h, \alpha_1], 0, \ldots, 0)$$

which implies $a_i^{h_i} = a_i$ for every $2 \leqslant i \leqslant n$ and every choice of $h_i \in H$; since $C_A(H) = 0$ we conclude $a_2 = \ldots = a_n = 0$ so that $\underline{h}\delta = (a_1, 0, \ldots, 0) \in A_1$. But then we may assume $\delta = (\delta_1, \ldots, \delta_n) \in \mathrm{Der}(H_1, A_1) \times \ldots \times \mathrm{Der}(H_n, A_n) \cong \mathrm{Der}(H, A)^n$. Since $G$ is transitive on $\{1, \ldots, n\}$, for every $i \neq 1$ there exists $g_i \in G$ such that $1 = ig_i$. Apply $(***)$ with $b = (h, \ldots, h)$, $h \in H$ and $w = g_i$; we deduce that, for every $h \in H_i$

$$((h, \ldots, h)^{g_i^{-1}}\delta)^{g_i} - (h, \ldots, h)\delta = (h\delta_1, \ldots, h\delta_n)^{g_i} - (h\delta_1, \ldots, h\delta_n) =$$

$$= (h\delta_i, \ldots, h\delta_{ng_i^{-1}}) - (h\delta_1, \ldots, h\delta_n) = [\alpha_w, (h, \ldots, h)] =$$

$$= ([\alpha_1, h], \ldots, [\alpha_n, h]).$$

but then $h\delta_i - h\delta_1 = [\alpha_1, h]$ for all $h \in H$, hence $\delta_i \equiv \delta_1 \bmod \mathrm{Inn}(H, A)$. Conversely if $(\delta_1, \ldots, \delta_n) \in \mathrm{Der}(H, A)^n$ and $\delta_i \equiv \delta_1 \bmod \mathrm{Inn}(H, A)$ for every $1 \leqslant i \leqslant n$ then the map $\delta: H^n \to A^n$ defined by $(h_1, \ldots, h_n)\delta = (h_1\delta_1, \ldots, h_n\delta_n)$ satisfies the condition $\delta + \mathrm{Inn}(B, A^n) \in H^1(B, A^n)^W$. So we conclude $H^1(B, A^n)^W \cong H^1(H, A)$. ■

2.5. $$h_w(A^n) = \left[\frac{h_H(A) - 2}{n}\right] + 2.$$

PROOF. $$h_w(A^n) = \left[\frac{s_W(A^n) - 1}{r_W(A^n)}\right] + 2 = \left[\frac{s_H(A) - 1}{nr_H(A)}\right] + 2 =$$

$$= \left[\frac{[s_H(A) - 1/r_H(A)] + 2 - 2}{n}\right] + 2 = \left[\frac{h_H(A) - 2}{n}\right] + 2. \quad \blacksquare$$

Now we can prove the main result ot this section:

THEOREM 2.6. $$d(I_W) = \max\left(d(I_{H/H' \wr G}), \left[\frac{d(I_H) - 2}{n}\right] + 2\right).$$

PROOF. If $H$ is cyclic then there is nothing to prove: indeed $H' = 1$ so $d(I_{H/H' \wr G}) = d(I_W)$ and, by 1.6, $[(d(I_H) - 2)/n] + 2 = [(1 - 2)/n] + 2 = 1$. So we may assume that $H$ is not a cyclic group, which in particular implies $[(d(I_H) - 2)/n] + 2 \geqslant 2$. By 2.2 and 2.5

$$d(I_W) = \max_A\left(2, d(I_{H/H' \wr G}), \left[\frac{h_H(A) - 2}{n}\right] + 2\right) =$$

$$= \max\left(2, d(I_{H/H' \wr G}), \left[\frac{\max_A (h_H(A)) - 2}{n}\right] + 2\right).$$

On the other hand, by (1.1) and (1.4),

$$d(I_H) = \max_A (2, d(H/H'), h_H(A)).$$

Now consider the different cases. If $d(I_H) = \max_A (h_H(A))$ then

$$d(I_W) = \max_A\left(2, d(I_{H/H' \wr G}), \left[\frac{d(I_H) - 2}{n}\right] + 2\right) =$$

$$= \max_A\left(d(I_{H/H' \wr G}), \left[\frac{d(I_H) - 2}{n}\right] + 2\right).$$

If $d(I_H) = d(H/H')$ then

$$\left[\frac{\max_A (h_H(A)) - 2}{n}\right] + 2 \leqslant \left[\frac{d(I_H) - 2}{n}\right] + 2 \leqslant$$

$$\leqslant d(I_H) = d(H/H') \leqslant d(I_{H/H' \wr G})$$

where the last inequality depends on the fact that $H/H'$ is a homomor-

phic image of $H/H' \wr G$ (see, for example, Lemma 3.1 in [16]), and

$$d(I_W) = \max\left(2, d(I_{H/H' \wr G}), \left\lceil \frac{\max_A (h_H(A)) - 2}{n} \right\rceil + 2\right) = d(I_{H/H' \wr G}).$$

Finally if $d(I_H) = 2$ then

$$\left\lceil \frac{\max_A (h_H(A)) - 2}{n} \right\rceil + 2 \leqslant \left\lceil \frac{d(I_H) - 2}{n} \right\rceil + 2 = 2$$

and

$$d(I_W) = \max\left(d(I_{H/H' \wr G}), \left\lceil \frac{d(I_H) - 2}{n} \right\rceil + 2\right). \quad \blacksquare$$

COROLLARY 2.7. *If $H$ is a soluble group then*

$$d(W) = \max\left(d\left(\frac{H}{H'} \wr G\right), \left\lceil \frac{d(H) - 2}{n} \right\rceil + 2\right).$$

PROOF. By (1.10) and (1.12) $d(H) = d(I_H)$ so

$$d(W) \geqslant d(I_W) \geqslant \left\lceil \frac{d(I_H) - 2}{n} \right\rceil + 2 = \left\lceil \frac{d(H) - 2}{n} \right\rceil + 2.$$

Furthermore, since $H/H' \wr G \cong W/B'$, $d(W) \geqslant d(H/H' \wr G)$, so we have

$$d(W) \geqslant \max\left(d\left(\frac{H}{H'} \wr G\right), \left\lceil \frac{d(H) - 2}{n} \right\rceil + 2\right).$$

To prove that

$$d(W) \leqslant \max\left(d\left(\frac{H}{H'} \wr G\right), \left\lceil \frac{d(H) - 2}{n} \right\rceil + 2\right)$$

we distinguish two cases. If $\mathrm{pr}(G) = 0$ then

$$d(W) = d(I_W) = \max\left(d\big(I_{H/H' \wr G}\big), \left[\frac{d(I_H) - 2}{n}\right] + 2\right) \leqslant$$

$$\leqslant \max\left(d\left(\frac{H}{H'} \wr G\right), \left[\frac{d(H) - 2}{n}\right] + 2\right).$$

If $\mathrm{pr}(G) \neq 0$ then, by (1.13), $d(W) = d(W/B') = d(W/B) = d(G)$ and therefore

$$d(W) = d\left(\frac{H}{H'} \wr G\right) > d(I_W) = \max\left(d\big(I_{H/H' \wr G}\big), \left[\frac{d(H) - 2}{n}\right] + 2\right). \quad \blacksquare$$

3. – In this section we want to show that the equality

$$d(W) = \max\left(d\left(\frac{H}{H'} \wr G\right), \left[\frac{d(H) - 2}{n}\right] + 2\right)$$

given by Corollary 2.7 does not in general hold if $H$ is not assumed to be soluble.

To do that we consider the particular case $H = S^m$, the direct product of $m$ copies of a finite non abelian simple group $S$ and $G = Z_2$, the cyclic group of order 2. If $m = 1$ then $W = S \wr Z_2$ can be generated with 2 elements [14]. We ask for which integers $m$ the statement $d(S^m \wr Z_2) = 2$ remains true. Let $B = \{(a_1, \ldots, a_m, b_1, \ldots, b_m) \mid a_i, b_j \in S\} \cong S^m \times S^m \cong S^{2m}$ be the base subgroup of $W$ and, for every $1 \leqslant i \leqslant m$, define $B_i = \{(a_1, \ldots, a_m, b_1, \ldots, b_m) \mid a_j = b_j = 1$ for every $1 \leqslant j \leqslant m, j \neq i\}$; $B_i \cong S^2$ is a normal subgroup of $W$ and $W_i = B_i Z_2 \cong S \wr Z_2$. Let $Z_2 = \langle \varepsilon \rangle$; $d(W) = 2$ if and only if there exist $x_1, y_1 \in B_1, \ldots, x_m, y_m \in B_m$ such that $\langle x_1 x_2 \ldots x_m \varepsilon, y_1 y_2 \ldots y_m \rangle = W$ and it is not difficult to see that this holds if and only if:

*a*) $\langle x_i \varepsilon, y_i \rangle = W_i \cong S \wr Z_2$ for every $1 \leqslant i \leqslant m$;

*b*) for every $1 \leqslant i < j \leqslant m$ and $\phi \in \mathrm{Aut}(S^2)$ the subgroup $\langle x_i x_j \varepsilon, y_i y_j \rangle$ of $W$ does not normalize the diagonal subgroup $\Delta_\phi = \{(x, x^\phi) \mid x \in S^2\} \leqslant B_i \times B_j$.

Define $\Omega = \{(x, y) \in S^2 \times S^2 \mid \langle x\varepsilon, y \rangle = S \wr Z_2\}$ and $\Gamma = \{\phi \in \mathrm{Aut}(S) \wr Z_2 \cong \mathrm{Aut}(S^2) \mid \varepsilon^\phi \varepsilon \in S^2\} \cong N_{\mathrm{Aut}(S^2)}(S \wr Z_2)$. If $(x, y) \in \Omega$ and $\phi \in \Gamma$ then $\langle x\varepsilon, y \rangle = S \wr Z_2$ implies $\langle x^\phi \varepsilon^\phi, y^\phi \rangle = \langle x^\phi \varepsilon^\phi \varepsilon\varepsilon, y^\phi \rangle = S \wr Z_2$ and so $(x^\phi \varepsilon^\phi \varepsilon, y^\phi) \in \Omega$. It can be verified that $(x, y)^\phi = (x^\phi \varepsilon^\phi \varepsilon, y^\phi)$

defines a group action of $\Gamma$ on the set $\Omega$. Notice that this action is regular: in fact if $(x, y)^\phi = (x^\phi \varepsilon^\phi \varepsilon, y^\phi) = (x, y)$ then $(x\varepsilon)^\phi = x\varepsilon$ and $y^\phi = y$; but $x\varepsilon$, $y$ generate $S \wr Z_2$ so we must have $\phi = 1$. Now the condition $(a)$ holds if and only if $(x_i, y_i) \in \Omega$ for every $1 \leqslant i \leqslant m$. Furthermore $\langle x_i x_j \varepsilon, y_i y_j \rangle$ normalizes the diagonal subgroup $\Delta_\phi$ if and only if, for every $x \in S^2$

$$(x, x^\phi)^{x_i x_j \varepsilon} = (x^{x_i \varepsilon}, x^{\phi x_j \varepsilon}) \in \Delta_\phi \quad \text{and} \quad (x, x^\phi)^{y_i y_j} = (x^{y_i}, x^{\phi y_j}) \in \Delta_\phi$$

and this occurs if and only if $x_j = x_i^\phi \varepsilon^\phi \varepsilon$ and $y_j = y_i^\phi$, that is $\phi \in \Gamma$ and $(x_i, y_i)^\phi = (x_j, y_j)$. But then $x_1, \ldots, x_m, y_1, \ldots, y_m$ satisfying $(a)$ and $(b)$ can be found if and only if there are at least $m$ different orbits for the action of $\Gamma$ on $\Omega$. Since this action is regular we deduce:

3.1. *$d(S^m \wr Z_2) = 2$ if and only if $m \leqslant \dfrac{|\Omega|}{|\Gamma|}$.*

Now define $\tilde{\Omega} = \{(z_1, z_2, z_3, z_4) \in S^4 \mid \langle z_1, z_2, z_3, z_4 \rangle = S\}$.

3.2. $|\Omega| \leqslant |\tilde{\Omega}|$.

PROOF. Suppose $(x, y) \in \Omega$ with $x = (x_1, x_2)$ and $y = (y_1, y_2)$. If $(x_1, x_2, y_1, y_2) \notin \tilde{\Omega}$ then $\langle x_1, x_2, y_1, y_2 \rangle = M$ is a proper subgroup of $S$ and $\langle x\varepsilon, y \rangle \leqslant M \wr Z_2$, a contradiction. ■

Using a method developed by P. Hall ([11]) the number $|\tilde{\Omega}|$ can be calculated in terms of the Moebius function $\mu$ of the lattice of subgroups of $S$, namely:

3.3. $|\tilde{\Omega}| = \sum_{K \leqslant S} \mu(K) |K|^4$.

Furthermore observe that:

3.4. $|\Gamma| = 2|S||\mathrm{Aut}\, S|$.

PROOF. Since $\Gamma \leqslant \mathrm{Aut}(S^2) = \mathrm{Aut}\, S \wr Z_2$, every $\phi \in \Gamma$ can be written in the form $\phi = (x_1, x_2)\varepsilon^i$, with $x_1, x_2 \in \mathrm{Aut}\, S$ and $0 \leqslant i \leqslant 1$; $\phi \in \Gamma$ if and only if $\varepsilon^\phi \varepsilon \in S^2$ and this holds if and only if $x_1 \equiv x_2 \bmod S$. ■

In particular from 3.1, 3.2 and 3.4 we deduce:

3.5 *If $m > \tilde{\Omega}/(2|S|\,|\mathrm{Aut}\, S|)$ then $d(S^m \wr Z_2) > 2$.*

Now let $S = \mathrm{Alt}(5)$, the alternating group of degree 5; by 3.3, $|\tilde{\Omega}| = 12785880$, while $|\Gamma| = 2|S|\,|\mathrm{Aut}\, S| = 14400$; by 3.5 we obtain:

3.6. $d(\mathrm{Alt}(5)^m \wr \mathbb{Z}_2) \geqslant 3$ *if* $m \geqslant 888$.

In particular consider $H = \mathrm{Alt}(5)^{888}$; $d(H) = 3$ (namely $d(\mathrm{Alt}(5)^m) = 3$ for $20 \leqslant m \leqslant 1668$), but

$$\max\left(d\left(\frac{H}{H'} \wr \mathbb{Z}_2\right), \left[\frac{d(H) - 2}{n}\right] + 2\right) =$$

$$= \max\left(d(\mathbb{Z}_2), \left[\frac{3-2}{n}\right] + 2\right) = 2 < 3 \leqslant d(H \wr \mathbb{Z}_2)$$

so in this case the statement of Corollary 2.7 does not hold.

4. – The theorem proved in section 1 reduces the study of $d(I_G)$ for a wreath product $W = H \wr G$ to the case $H$ abelian. We will study this problem in two cases. In the next section we will discuss the case $G = \mathrm{Sym}(n)$. In this section we consider any arbitrary finite group $G$ with respect to its regular representation. So let $A$ be a finite abelian group, $G$ an arbitrary finite group and let $W = A \wr G$ be the wreath product of $A$ and $G$ with respect to the regular permutation representation of $G$.

For every prime $p$ dividing $|A|$, denote by $d_p(A)$ the minimum number of generators of a Sylow $p$-subgroup of $A$ and define

$$\varrho_p = \max_M h_G(M) + d_p(A)$$

where $M$ ranges over the set of non trivial irreducible $\mathbb{F}_p G$-modules, with $\varrho_p = 0$ if every irreducible $\mathbb{F}_p G$-module is trivial (here $\mathbb{F}_p$ denotes the field with $p$-elements). As is well known, $O_p(G) = \bigcap_M C_G(M)$ where $M$ runs through the irreducible $\mathbb{F}_p G$-modules, so $\varrho_p = 0$ if and only if $G = O_p(G)$ is a $p$-group.

LEMMA 4.1. $$d(I_W) = \max_{p \mid |A|} (d(I_{A \times G}), \varrho_p).$$

PROOF. The statement is obvious if $A$ is trivial. So from now on we may assume that $A$ is a non trivial abelian group. Let $n = |G|$ and consider $B = A^n$ the base subgroup of $W$. $\mathrm{Frat}\, B = \mathrm{Frat}\, A^n = (\mathrm{Frat}\, A)^n \leqslant \mathrm{Frat}\, W$ so, if we consider $\overline{W} = W/\mathrm{Frat}\, B = W/(\mathrm{Frat}\, A)^n \cong A/\mathrm{Frat}\, A \wr G$, by (1.9), $d(I_W) = d(I_{\overline{W}})$. Let $\mathbb{F}_p G$ be the group algebra of $G$ over the field $\mathbb{F}_p$ and let $\overline{B} = \prod_{p \mid |A|} (\mathbb{F}_p G)^{d_p(A)}$; $G$ acts on $\overline{B}$ by rigth multiplication and $\overline{W} \cong \overline{B} \rtimes G$ ([13] pp. 485-486). Now $[\overline{B}, G]$ is a normal subgroup of $\overline{W}$ with $\overline{W}/[\overline{B}, G] \cong \overline{A} \times G$ (here $\overline{A}$ denotes the factor group $A/\mathrm{Frat}\, A$),

so, by (1.7)

$$d(I_W) = d(I_{\overline{W}}) = \max_M (2, d(I_{\overline{A}\times G}), h_{\overline{W}}(M)) = \max_M (2, d(I_{A\times G}), h_W(M))$$

where $M$ ranges over the set of the non trivial irreducible $W$-modules which are isomorphic to some complemented chief factor of $\overline{W}$ contained in $\overline{B}$. But ([13] Lemma 2.1) for every prime $p$ dividing $|A|$, every non trivial irreducible $\mathbb{F}_pG$-module $M$ is isomorphic to a complemented chief factor of $\overline{W}$ contained in $\overline{B}$ and

$$\delta_W(M) = d_p(A)r_G(M) + \delta_G(M).$$

Since $B$ centralizes $M$, $\mathrm{End}_G(M) \cong \mathrm{End}_W(M)$, so $r_W(M) = r_G(M)$. Furthermore, by (1.2),

$$s_W(M) = \delta_W(M) + \dim_{\mathrm{End}_W(M)} H^1(W/C_W(M), M) =$$

$$= \delta_W(M) + \dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M) = d_p(A)r_G(M) +$$

$$+ \delta_G(M) + \dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M) = d_p(A)r_G(M) + s_G(M).$$

But then

$$h_W(M) = \left[\frac{s_W(M)-1}{r_W(M)}\right] + 2 = \left[\frac{s_G(M) - 1 + d_p(A)r_G(M)}{r_G(M)}\right] + 2 =$$

$$= \left[\frac{s_G(M)-1}{r_G(M)}\right] + 2 + d_p(A) = h_G(M) + d_p(A).$$

So $\max_M h_W(M) = \max_{p\,||A|} \varrho_p$ and $d(I_W) = \max_{p\,||A|} (2, d(I_{A\times G}), \varrho_p)$. To conclude the proof it remains to see that $2 \leq \max_{p\,||A|} (d(I_{A\times G}), \varrho_p)$. If $A \times G$ is not cyclic, then $d(I_{A\times G}) \geq 2$. Suppose that $A \times G$ is cyclic: a prime $p$ dividing $|A|$ does not divide $|G|$ so there exists at least one non-trivial irreducible $\mathbb{F}_pG$-module, say $M$. But then $\varrho_p \geq h_G(M) + d_p(A) \geq 2$. ∎

COROLLARY 4.2. $d(A \wr G) = \max_{p\,||A|} (d(A \times G), \varrho_p)$.

PROOF. Since $A \times G$ is an epimorphic image of $W = A \wr G$, $d(W) \geq d(A \times G)$. Furthermore $d(W) \geq d(I_W) \geq \max_{p\,||A|} \varrho_p$, so $d(A \wr G) \geq$ $\geq \max_{p\,||A|} (d(A \times G), \varrho_p)$. To prove $d(A \wr G) \leq \max_{p\,||A|} (d(A \times G), \varrho_p)$ we distinguish two cases. If $\mathrm{pr}(W) = 0$ then $d(W) = d(I_W) =$

$= \max_{p \mid |A|} (d(I_{A \times G}), \varrho_p) \leqslant \max_{p \mid |A|} (d(A \times G), \varrho_p)$. If $\mathrm{pr}(W) \neq 0$ then, by (1.13), $d(W) = d(G) = d(A \times G)$ and $d(W) > d(I_W) \geqslant \max_{p \mid |A|} \varrho_p$. ■

We consider now a particular case; suppose

(*) *For every prime $p$ dividing $|A|$ and every non trivial irreducible $\mathbb{F}_p G$-module $M$, $\delta_G(M) = 0$, that is $M$ is not isomorphic as a $G$-module to a complemented chief factor of $G$.*

Notice that (*) holds in particular if $G$ is nilpotent, if $G$ is simple or if $A$ and $G$ have coprime orders.

LEMMA 4.3. *Suppose that $G$ is not a $p$-group and that $G$ satisfies* (*):

(i) $\varrho_p = 1 + d_p(A)$ *if $G$ is $p$-soluble;*

(ii) $\varrho_p = 2 + d_p(A)$ *if $G$ is not $p$-soluble.*

PROOF. Suppose that $G$ is not a $p$-group and let $M$ be a non trivial irreducible $\mathbb{F}_p G$-module. Since $\delta_G(M) = 0$, by (1.2), $s_G(M) = \dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M)$ so

$$h_G(M) = \left[ \frac{\dim_{\mathrm{End}_G(M)} H^1(G/C_G(M), M) - 1}{r_W(M)} \right] + 2 .$$

By (1.3) $h_G(M) \leqslant 2$ and $h_G(M) = 1$ if and only if $H^1(G/C_G(M), M) = 0$. The conclusion follows from the following theorem proved by Stammbach ([19]): a finite group $G$ is $p$-soluble if and only if $H^1(G/C_G(M), M) = 0$ for every irreducible $\mathbb{F}_p G$-module. ■

COROLLARY 4.4. *If* (*) *holds then*

$$d(A \wr G) = \max_q (d(A \times G), d(A) + 1, d_q(A) + 2)$$

*where $q$ ranges over the set of the prime numbers dividing $|A|$ and such that $G$ is not $q$-soluble.*

In particular:

COROLLARY 4.5. *If $A$ is abelian and $A$ and $G$ have coprime orders then*

$$d(A \wr G) = \max (d(A) + 1, d(G)) .$$

PROOF. If $(|A|, |G|) = 1$ then $d(A \times G) = \max(d(A), d(G))$ and, for every prime $p$ dividing $|A|$, since $p$ does not divide $|G|$, $G$ is $p$-soluble. ∎

Using the fact that every non abelian finite simple group can be generated with 2 elements [2], we deduce:

COROLLARY 4.6. *If $p$ is a prime and $S$ is a finite non abelian simple group then*

(i) $d(\mathbb{Z}_p \wr S) = 2$ *if $p$ does not divide $|S|$;*

(ii) $d(\mathbb{Z}_p \wr S) = 3$ *if $p$ divides $|S|$.*

5. – In this next section we compute the minimum number of generators for $W = A \wr \mathrm{Sym}(n)$, the wreath product of a non trivial abelian group $A$ with the symmetric group of degree $n$.

LEMMA 5.1. $\mathrm{pr}(W) = 0$.

PROOF. Suppose, by contradiction, $\mathrm{pr}(W) \neq 0$; by (1.13) $d(W) = d(A^n \rtimes \mathrm{Sym}(n)) = d(\mathrm{Sym}(n)) \leq 2$, hence, by (1.11), $\mathrm{pr}(W) = 0$, a contradiction. ∎

In the same way we can also prove:

LEMMA 5.2. $\mathrm{pr}(A \times \mathrm{Sym}(n)) = 0$.

Now $\mathrm{Frat}\, B = (\mathrm{Frat}\, A)^n \leq \mathrm{Frat}\, W$ so, by (1.9), $d(I_W) = d(I_{W/\mathrm{Frat}\, B})$. Let $B_p$ be the base subgroup of the wreath product $\mathbb{Z}_p \wr \mathrm{Sym}(n)$; $B_p$ can be viewed as a $\mathrm{Sym}(n)$-module and $W/\mathrm{Frat}\, B = W/(\mathrm{Frat}\, A)^n \cong A/\mathrm{Frat}\, A \wr \mathrm{Sym}(n) \cong \prod_{p \mid |A|} B_p^{d_p(A)} \rtimes \mathrm{Sym}(n)$. Let $\overline{B} = \prod_{p \mid |A|} B_p^{d_p(A)}$ and $\overline{W} = \overline{B} \rtimes \mathrm{Sym}(n)$; $[\overline{B}, \mathrm{Sym}(n)] \trianglelefteq \overline{W}$ with $\overline{W}/[\overline{B}, \mathrm{Sym}(n)] \cong \cong A/\mathrm{Frat}\, A \times \mathrm{Sym}(n)$, so, by (5.1), (5.2) and (1.7) we have

$$5.3.\quad d(I_W) = d(W) = d(\overline{W}) = \max_M (2, d(I_{\overline{A} \times \mathrm{Sym}(n)}), h_{\overline{W}}(M)) =$$

$$= \max_M (d(\overline{A} \times \mathrm{Sym}(n)), h_{\overline{W}}(M)) = \max_M (d(A \times \mathrm{Sym}(n)), h_W(M))$$

where $M$ ranges over the set of the non trivial irreducible $W$-modules which are isomorphic to some complemented chief factor of $\overline{W}$ contained in $\overline{B}$.

To apply these result we need some information about the structure of $B_p$ as a $\mathrm{Sym}(n)$-module. Define $I_p = \{(x_1, \ldots, x_n) \in B_p \mid \sum_{1 \leq i \leq n} x_i = 0\}$

and, for every $1 \leqslant i < j \leqslant n$, let $e_{i,j} = (x_1, \ldots, x_n)$ with $x_i = 1$, $x_j = -1$, $x_k = 0$ if $k \neq i, j$. It is easy to verify that $I_p$ is a submodule of $B_p$ and that, for every $i \neq j$, $e_{i,j}$ generates $I_p$ as a $\mathrm{Sym}(n)$-module. Furthermore it can be easily seen that

5.4. *$B_p/I_p \cong \mathbb{Z}_p$, the trivial $\mathrm{Sym}(n)$-module and*

(i) *if $p$ divides $n$ then $I_p$ is the unique maximal submodule of $B_p$;*

(ii) *if $p$ does not divide $n$ then $B_p \cong I_p \oplus \mathbb{Z}_p$ and $I_p$ is an irreducible $\mathrm{Sym}(n)$-module.*

Let $\mathrm{rad}(\overline{B})$ be the intersection of the maximal $\mathrm{Sym}(n)$-submodules of $\overline{B}$; no chief factor of $\overline{B}$ contained in $\mathrm{rad}(\overline{B})$ is complemented, so we have only to consider the chief factors of $B/\mathrm{rad}(\overline{B})$ which are not centralized by $\mathrm{Sym}(n)$. By (5.4)

$$\frac{\overline{B}}{\mathrm{rad}(\overline{B})} \cong \prod_{p \mid |A|} \mathbb{Z}_p^{d_p(A)} \prod_{p \mid |A|,\, p \nmid n} I_p^{d_p(A)},$$

and, from (5.3), we deduce

$$5.5 \qquad d(W) = \max_{p \mid |A|,\, p \nmid n} (d(A \times \mathrm{Sym}(n)), h_W(I_p)).$$

We have to compute $h_W(I_p) = [(s_W(I_p) - 1)/r_W(I_p)] + 2$.

5.6 *If $p$ does not divide $n$, then $\mathrm{End}_W(I_p) = \mathrm{End}_{\mathrm{Sym}(n)}(I_p) \cong \mathrm{F}_p$.*

Proof. Since $I_p = \langle e_{1,2} \rangle_{\mathrm{Sym}(n)}$, $\phi \in \mathrm{End}_{\mathrm{Sym}(n)}(I_p)$ is uniquely determined by the knowledge of $e_{1,2}^{\phi} = (x_1, \ldots, x_n)$. Let $\sigma = (1, 2) \in \mathrm{Sym}(n)$:

$$(x_2, x_1, x_3, \ldots, x_n) = (e_{1,2}^{\phi})^{\sigma} = (e_{1,2}^{\sigma})^{\phi} = (-e_{1,2})^{\phi} = -(x_1, x_2, x_3, \ldots, x_n);$$

if $p \neq 2$ then $x_k = -x_k = 0$ for $3 \leqslant k \leqslant n$, $x_1 = -x_2 = x \in \mathbb{Z}_p$ and $e_{1,2}^{\phi} = xe_{1,2}$. If $p = 2$ then we can conclude only $x_1 = x_2 = x$. But consider now $\sigma \in \mathrm{Stab}_{\mathrm{Sym}(n)}(1, 2) = \{\sigma \in \mathrm{Sym}(n) \mid 1\sigma = 1, 2\sigma = 2\}$:

$$(x_1, \ldots, x_n)^{\sigma} = (e_{1,2}^{\phi})^{\sigma} = (e_{1,2}^{\sigma})^{\phi} = e_{1,2}^{\phi} = (x_1, \ldots, x_n);$$

since this holds for every $\sigma \in \mathrm{Stab}_{\mathrm{Sym}(n)}(1, 2)$, it must be $x_3 = \ldots = x_n = y$ and $e_{1,2}^{\phi} = (x, x, y \ldots, y)$. But $e_{1,2}^{\phi} \in I_p$ implies $2x + (n-2)y = ny = 0$; since, by hypothesis, 2 does not divide $n$, we deduce $y = 0$ and again the conclusion is $e_{1,2}^{\phi} = xe_{1,2}$. ∎

5.7. *If $p$ does not divide $n$, then $r_W(I_p) = n - 1$.*

PROOF. $r_W(I_p) = \dim_{\mathrm{End}_W(I_p)}(I_p) = \dim_{\mathrm{F}_p}(I_p) = n - 1$. ∎

5.8. *If $p$ does not divide $n$, then $H^1(\mathrm{Sym}(n), I_p) = 0$.*

PROOF. Recall that

$$H^1(\mathrm{Sym}(n), I_p) = \mathrm{Der}(\mathrm{Sym}(n), I_p)/\mathrm{Inn}(\mathrm{Sym}(n), I_p).$$

Since $p$ does not divide $n$, $C_{I_p}(\mathrm{Sym}(n)) = 0$ and $|\mathrm{Inn}(\mathrm{Sym}(n), I_p)| = |I_p| = p^{n-1}$. To conclude it suffices to prove that $|\mathrm{Der}(\mathrm{Sym}(n), I_p)| \leqslant p^{n-1}$. Consider the transpositions $\sigma_2 = (1, 2), \ldots, \sigma_n = (1, n)$. Since $\mathrm{Sym}(n) = \langle \sigma_2 \ldots, \sigma_n \rangle$, $\delta \in \mathrm{Der}(\mathrm{Sym}(n), I_p)$ is uniquely determined by the knowledge of $\sigma_i\delta$, for $2 \leqslant i \leqslant n$. We claim

$$(*) \qquad \sigma_i\delta = \lambda_i e_{1,i}, \qquad \lambda_i \in \mathrm{F}_p .$$

This will imply that $\sigma_i\delta$ can be chosen in at most $p$ different ways, so there are at most $p^{n-1}$ different possibilities for $\delta$.

We prove our claim for $i = 2$, but the same argument can be repeated for every $2 \leqslant i \leqslant n$. Let $\sigma_2\delta = (x_1, \ldots, x_n)$:

$$0 = (\sigma_2^2)\delta = (\sigma_2\delta)^{\sigma_2} + \sigma_2\delta = (x_1 + x_2, x_1 + x_2, 2x_3, \ldots, 2x_n).$$

If $p \neq 2$ then $x_1 = -x_2 = x$ and $x_k = 0$ for every $k \geqslant 3$ so $\sigma_2\delta = xe_{1,2}$. If $p = 2$ we can only deduce $x_1 = x_2 = x$; but let $\sigma \in \mathrm{Stab}_{\mathrm{Sym}(n)}(1, 2)$ and suppose $\sigma\delta = (y_1, \ldots, y_n)$:

$$(y_1, \ldots, y_n) = \sigma\delta = (\sigma_2\sigma\sigma_2)\delta = (\sigma_2\delta)^{\sigma\sigma_2} + (\sigma\delta)^{\sigma_2} + \sigma_2\delta =$$

$$= (x, x, x_3, \ldots, x_n)^{\sigma} + (y_2, y_1, y_3, \ldots, y_n) + (x, x, x_3, \ldots, x_n);$$

this implies $(x, x, x_3, \ldots, x_n)^{\sigma} = (x, x, x_3, \ldots, x_n)$ for every $\sigma \in \mathrm{Stab}_{\mathrm{Sym}(n)}(1, 2)$ and, of consequence, $x_3 = \ldots = x_n = y$. But, as at the end of the proof of 5.6, $\sigma_2\delta = (x, x, y, \ldots, y) \in I_p$ implies $y = 0$ and $\sigma_2\delta = xe_{1,2}$. ∎

5.9. *If $p$ does not divide $n$, then $s_W(I_p) = d_p(A)$.*

PROOF. By (1.2) $s_W(I_p) = \delta_W(I_p) + \dim_{\mathrm{End}_W}(H^1(W/C_W(I_p), I_p))$. But

$$H^1(W/C_W(I_p), I_p) \cong H^1(\mathrm{Sym}(n), I_p) = 0,$$

while, since $I_p$ cannot be a factor of $\mathrm{Sym}(n)$, $\delta_W(I_p)$ is the number of chief factors isomorphic to $I_p$ in $\overline{B}/\mathrm{rad}(\overline{B})$, and this is equal to $d_p(A)$. ∎

By (5.7) and (5.9) we have

5.10. *If $p$ does not divide $n$, then* $h_W(I_p) = [d_p(A) - 1/n - 1] + 2$.

From this it can be easily deduced:

5.11. *If $p$ does not divide $n$, then*

(i) $h_W(I_p) = d_p(A) + 1$ *if* $n = 2$;

(ii) $h_W(I_p) \leqslant \max(2, d_p(A))$ *if* $n \neq 2$.

Now we can conclude:

THEOREM 5.12. *If $A$ is a non trivial abelian group, then*

(i) $d(A \wr \mathrm{Sym}(2)) = d(A) + 1$;

(ii) If $n \geqslant 3$ *then* $d(A \wr \mathrm{Sym}(n)) = \max_{p \mid |A|}(2, d_p(A), d_2(A) + 1)$.

PROOF. By (5.5) $d(A \wr \mathrm{Sym}(n)) = \max_{p \mid |A|,\, p \nmid n}(d(A \times \mathrm{Sym}(n)), h_W(I_p))$. On the other hand it can be easily seen that $\max(2, d(A \times \mathrm{Sym}(n)) = \max_{p \mid |A|}(2, d_p(A), d_2(A) + 1)$ and the conclusion follows immediately from (5.11). ■

6. – In [6] it is proved that if $S$ is a finite non abelian simple group then $d(\mathrm{Aut}\, S) = \max(2, d(\mathrm{Out}\, S) = \max(2, d_2(\mathrm{Out}\, S/(\mathrm{Out}\, S)'))$ where $\mathrm{Out}\, S = \mathrm{Aut}\, S/S$ is the outer automorphism group of $S$. We may use the results discussed in the previous sections to compute $d(\mathrm{Aut}(S^n))$.

THEOREM 6.1. *Suppose that $S$ is a finite non abelian simple group. If $n \neq 1$ then*

$$d(\mathrm{Aut}(S^n)) = \max\left(2, d_2\left(\frac{\mathrm{Out}\, S}{(\mathrm{Out}\, S)'}\right) + 1\right).$$

PROOF. It is well known that $W = \mathrm{Aut}(S^n) \cong \mathrm{Aut}\, S \wr \mathrm{Sym}(n)$; the socle of $W$ is $S^n$ and it is the unique minimal normal subgroup of $W$; in [14] it is proved that if $N$ is the unique minimal normal subgroup of a finite group $G$ and is not abelian then $d(G) = \max(2, d(G/N))$. In our case, since $W/S^n \cong \mathrm{Aut}\, S/S \wr \mathrm{Sym}(n)$ we obtain

$$d(W) = \max\left(2, d\left(\frac{\mathrm{Aut}\, S}{S} \wr \mathrm{Sym}(n)\right)\right).$$

The outer automorphism group $\mathrm{Out}S$ of a finite non abelian simple group $S$ is a soluble group whose structure is well known; in particular $d(\mathrm{Out}S) \leqslant 3$ and $d(\mathrm{Out}S) = 3$ if and only if $Z_2 \times Z_2 \times Z_2$ is an epimorphic image of $\mathrm{Out}(S)$ (this occurs, for example, if $S = PSL(m, p^h)$ with $p$ odd, $h$ and $m$ even). Since $\mathrm{Out}S$ is solvable and $d(\mathrm{Out}S) \leqslant 3$, by (2.7)

$$d(W) = \max\left(2, d(\mathrm{Out}S \wr \mathrm{Sym}(n))\right) =$$

$$= \max\left(2, d\left(\frac{\mathrm{Out}S}{(\mathrm{Out}S)'} \wr \mathrm{Sym}(n)\right), \left[\frac{d(\mathrm{Out}S) - 2}{n}\right] + 2\right) =$$

$$= \max\left(2, d\left(\frac{\mathrm{Out}S}{(\mathrm{Out}S)'} \wr \mathrm{Sym}(n)\right)\right).$$

On the other hand it is not difficult to see $d_p(\mathrm{Out}S/(\mathrm{Out}S)') \leqslant 1$ for every odd prime; but then, applying Theorem 5.12, we conclude

$$d(\mathrm{Aut}(S^n)) = \max\left(2, d_2\left(\frac{\mathrm{Out}S}{(\mathrm{Out}S)'}\right) + 1\right). \qquad \blacksquare$$

## REFERENCES


[1] J. H. Conway, - S. P. Norton - R. P. Parker - R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford (1985).

[2] M. Aschbacher - R. Guralnick, *Some applications of the first cohomology Group*, J. Algebra, **90** (1984), pp. 446-460.

[3] K. Buzási - L. G. Kovács, *The minimal number of generators of wreath products of nilpotent groups*, Contemporary Mathematics, **93** (1989), pp. 115-121.

[4] Yeo Kok Chye, *Minimal generating sets for some wreath products of groups*, Bull. Austral. Math. Soc., **9** (1973), pp. 127-136.

[5] J. Cossey - K. W. Gruenberg - L. G. Kovács, *The presentation rank of a direct product of finite groups*, J. Algebra, **28** (1974), pp. 597-603.

[6] F. Dalla Volta - A. Lucchini, *Generation of almost simple groups*, J. Algebra, **178** (1995), pp. 194-223.

[7] K. W. Gruenberg, *Cohomological Topics in Group Theory*, Lectures Notes Math. no. **143**, Springer (1970).

[8] K. W. Gruenberg, *Über die Relationen moduln einer endlichen Gruppe*, Math. Z., **118** (1970).

[9] K. W. Gruenberg, *Relation modules of finite groups*, CBMS Monograph 25, Amer. Math. Soc., Providence (1976), pp. 408-421.

[10] K. W. GRUENBERG, *Groups of non zero presentation rank*, Symposia Math., **17** (1976), pp. 215-224.
[11] P. HALL, *The Eulerian functions of a group*, Quart. J. Math., **7** (1936), pp. 134-151.
[12] A. LUCCHINI, *Some questions on the number of generators of a finite group*, Rend. Sem. Mat. Univ. Padova, **83** (1990), pp. 201-222.
[13] A. LUCCHINI, *Generating wreath products*, Arch. Math., **62** (1994), pp. 481-490.
[14] A. LUCCHINI - F. MENEGAZZO, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova, to appear.
[15] S. MAC LANE, *Homology*, Springer (1963).
[16] L. RIBES - K. WONG, *On the minimal number of generators of certain groups*, Groups St Andrews 1989, London Math. Soc. Lecture Note Series, **160**, pp. 408-421.
[17] K. W. ROGGENKAMP, *Relation modules of finite groups and related topics*, Algebra i Logika, **12** (1973), pp. 351-369.
[18] K. W. ROGGENKAMP, *Integral representation and presentations of finite groups*, Lectures Notes Math. no. **744**, Springer (1979).
[19] U. STAMMBACH, *Cohomological characterizations of finite solvable and nilpotent groups*, J. Pure Appl. Algebra, **11** (1977), pp. 293-301.
[20] K. W. GRUENBERG - K. W. ROGGENKAMP, *Decomposition of the relation modules of a finite group*, J. London Math. Soc., **12** (1976), pp. 262-266.

Manoscritto pervenuto in redazione il 6 luglio 1995
e, in forma revisionata, il 16 gennaio 1996.