Certain Applications of the Burnside Rings and Ghost Rings in the Representation theory of finite Groups (I)

K. K. Nwabueze

1 Introduction

Let G be a finite group of order n and $U_1, \ . \ . , U_q$; a maximal non-conjugating set of cyclic subgroups of G. If $\psi_1, \ . \ . \ . , \psi_q$; are the characters of G induced from the trivial representations of $U_1, \ . \ . \ . , U_q$; respectively, then for any rational character χ of G, there exist integers $a_1, \ . \ . \ . , a_q$; such that

$$n\chi \quad = \quad \sum_{i=1}^{q} a_i\psi_i \qquad\qquad (*)$$

This is the statement of the well known Artin induction theorem. It is already known that in most cases smaller multiples of χ satisfy (*). So to make this induction theorem more precise, the smallest natural number k such that the equation $k\chi = \sum_{i=1}^{q} a_i\psi_i$ is solvable — for integral unknowns a_i — for any given rational character χ of G is called an Artin exponent for G (see [5]). All Artin exponents form an ideal in the integers and clearly $|G|$ is in this ideal. The unique positive generator for this ideal is called the Artin exponent of G. Now let $\mathcal{G}(QG)$ denote the Grothendieck ring of all rational representations of G and $\mathcal{G}_C(QG)$ the ideal in $\mathcal{G}(QG)$ generated by rational representations of G induced from cyclic subgroups. The Artin exponent of G has been computed by finding the characteristic of the quotient ring $\mathcal{G}(QG)/\mathcal{G}_C(QG)$ (see [5]). The purpose of this paper is to compute the same invariant (the Artin

Received by the editors January 1995 – in revised form December 1996.
Communicated by J. Van Geel.

exponent) using the Burnside ring theoretic approach. This arises in the following context:

Let $\mathcal{U}$ be a family of cyclic subgroups of a finite group G, closed with respect to conjugation. Let $B(G)$ and $\tilde{B}(G)$ denote the Burnside ring and Ghost ring (see section 2) of G respectively. For $U \leq G$, define $e_U \in \tilde{B}(G)$ by

$$e_U := \begin{cases} 1 & \text{if } U \in \mathcal{U} \\ 0 & \text{otherwise} \end{cases}$$

The integer $A(G) := min(n \in N \mid n \cdot e_U \in B(G))$ is called the Artin exponent of G (see section 3). For a finite p-group G of order p^α,— a power of a prime,— one has that $A(G) = 1$ if and only if G is cyclic; $A(G) = p^{\alpha-1}$ when G is noncyclic ($p \neq 2$). This statement remains valid for 2-groups except in the case where G is one of the special class of groups considered in 5.1.

As was pointed out in [5], the above results seem to suggest that the invariant $A(G)$ is a blunt measure of the deviation of G from being a cyclic group.

There are various reasons why such invariants are studied. Apart from the fact that these ideas are natural generalizations of number theoretic notions, — which in themselves have aesthetic values, — there are applications in other branches of mathematics. For example, a full knowledge of these invariants may sometimes yield nontrivial information about the induction theorems for various functors K on the category of finite groups (see [8]). Finally and above all the procedure used here for the computation of the Artin exponent affirms the utility of the Burnside ring in the representation theory of finite groups.

The structure of this paper is as follows. In section 2 we recollect some of the well known facts about the Burnside ring, — most of which are due to A. Dress (see [1], [3], [2]); in section 3 we reformulate the definition of the Artin exponent in terms of the Burnside ring; in section 4, we collect some necessary useful results about p-groups and finally in section 5 we compute the Artin exponent for finite p-groups.

For the reader's convenience we list here some of the notation used in this paper. For a finite group G we denote by;
Z: the ring of integers,
S: a G-set,
$G_s := \{g \in G \mid gs = s\}$ for an element $s \in S$,
$\{1_G\}$: the trivial subgroup of G,
p : a prime number,
$|G|$: the order of G,
$Z(G)$: the centre of G,
$C_G(N) := \{g \in G \mid gn = ng, \forall n \in N\}$ — the centralizer of N in G,
$< T >$: subgroup of G generated by T,
$< T >_N$: the normal subgroup of G generated by T,
$[g\ ,\ h] := g^{-1}h^{-1}gh$ – commutator of g and h,
$[S\ ,\ T] := < [s\ ,\ t] \mid s \in S,\ t \in T >$.

2 The Burnside ring and its ghost ring

Consider $\mathcal{U}$, sets of cyclic subgroups of a finite group G which is closed with respect to conjugation. We define a $(G\ ,\ \mathcal{U})$-set to be a finite left G-set S such that $G_s \in \mathcal{U}$ for all s in S. Our conditions on $\mathcal{U}$ imply that for any $U \in \mathcal{U}$ the set $G/U = \{gU \mid g \in G\}$ of left cosets of U in G is a $(G\ ,\ \mathcal{U})$-set, the G-action on G/U is defined by left multiplication $G \times G/U \longrightarrow G/U\ :\ (h\ ,\ gU) \longrightarrow hgU$, and that for any two $(G\ ,\ \mathcal{U})$-sets S_1 and S_2 the G-sets $S_1 \times S_2$ and $S_1 \cup S_2$ are $(G\ ,\ \mathcal{U})$-sets. We observe that the isomorphism classes of $(G\ ,\ \mathcal{U})$-sets form a commutative semiring $B^+(G\ ,\ \mathcal{U})$. Furthermore $1 \in B^+(G\ ,\ \mathcal{U})$ exists, namely G/G. Thus a map from the set $B^+(G\ ,\ \mathcal{U})$ of isomorphism classes of $(G\ ,\ \mathcal{U})$-sets into a ring R which commutes with sums and products and sends $1 \in B^+(G\ ,\ \mathcal{U})$ onto 1_R is nothing other than a homomorphism from the semiring $B^+(G\ ,\ \mathcal{U})$ into R and this factors uniquely through the universal ring associated to $B^+(G\ ,\ \mathcal{U})$, *the Burnside rings* $B(G\ ,\ \mathcal{U})$ *of* G *with respect to* $\mathcal{U}$. We note that if we assume $\mathcal{U}$ to be the set $\mathcal{S}(G)$ of all subgroups of G then $B(G\ ,\ \mathcal{U})$ coincides with the usual Burnside ring $B(G)$ of G, constructed from the semiring $B^+(G)$ of isomorphism classes of all finite G-sets. The following facts are more or less obvious:

Theorem 2.1. *(a)* $B(G\ ,\ \mathcal{U})$ *is generated freely as an additive group by the isomorphism classes of transitive* $(G\ ,\ \mathcal{U})$*-sets, i.e. of* G*-sets of the form* G/U *with* $U \in \mathcal{U}$*: so its rank equals the number* $k = k_{\mathcal{U}}$ *of* G*-conjugacy classes of subgroups in* $\mathcal{U}$*.*
(b) For any subgroup $V \leq G$ *of* G*, whether in* $\mathcal{U}$ *or not, the mapping*

$$\chi_V : S \longmapsto \#\{s \in S \mid V \leq G_s\}$$

which associates with any $(G\ ,\ \mathcal{U})$*-set* S *the number of elements in*

$$S^V := \{s \in S \mid V \leq G_s\},$$

the set of V*-invariant elements in* S *– induces a homomorphism also denoted by* χ_V *or more precisely* $\chi_V^{\mathcal{U}}$ *– from* $B(G\ ,\ \mathcal{U})$ *into* Z*.*
(c) Any homomorphism from $B(G\ ,\ \mathcal{U})$ *into* Z *takes the form given in (b).*

We shall briefly observe and show the following not so obvious facts.

Theorem 2.2. *For* $V,\ W \leq G$ *one has* $\chi_V^{\mathcal{U}} = \chi_W^{\mathcal{U}}$ *if and only if* $\overline{V} := \bigcap_{V \leq U \in \mathcal{U}} U$ *is conjugate to* $\overline{W} := \bigcap_{W \leq U \in \mathcal{U}} U$*. So, in view of the fact that* $\overline{V} \in \mathcal{U}$ *for all* $V \in \mathcal{S}(G)$ *and* $V \in \mathcal{U}$ *if and only if* $V = \overline{V}$*, one has* $k = k_{\mathcal{U}}$ *different homomorphisms from* $B(G\ ,\ \mathcal{U})$ *into* Z *which – after choosing a system* $\mathcal{U}' = \{U_1,\ U_2,\ \ldots, U_k\}$ *of representatives of conjugacy classes of subgroups of* $\mathcal{U}$ *with* $|U_1| \geq |U_2| \geq \ldots \geq |U_k|$ *– may be denoted by* $\chi_1 = \chi_{U_1},\ \chi_2 = \chi_{U_2},\ \ldots, \chi_k = \chi_{U_k}$*.*

Proof : Note first of all that $\chi_V^{\mathcal{U}} = \chi_{\overline{V}}^{\mathcal{U}}$ for all $V \in \mathcal{S}(G)$ because for any $(G\ ,\ \mathcal{U})$-set S one has

$$\chi_V^{\mathcal{U}}(S) = \chi_V(S) = \#\{s \in S \mid V \leq G_s\} = \#\{s \in S \mid \overline{V} \leq G_s\} = \chi_{\overline{V}}(S) = \chi_{\overline{V}}^{\mathcal{U}}(S),$$

since for $V \in \mathcal{S}(G)$ and $U \in \mathcal{U}$ one has $V \leq U$ if and only if $\overline{V} \leq U$.

Now suppose that $\chi_V^{\mathcal{U}} = \chi_W^{\mathcal{U}}$. Then $V \leq \overline{V} \in \mathcal{U}$ implies

$$0 \neq \chi_{\overline{V}}(G/\overline{V}) = \chi_V^{\mathcal{U}}(G/\overline{V}) = \chi_W^{\mathcal{U}}(G/\overline{V}) = \chi_{\overline{W}}(G/\overline{V})$$

and hence $\overline{W} \preceq \overline{V}$ (where the symbol "$\overline{W} \preceq \overline{V}$" denotes that $\overline{W}$ is subconjugate to $\overline{V}$ in G that is, there exists $g \in G$ with $g\overline{W}g^{-1} \subseteq \overline{V}$). By symmetry we have $\overline{V} \preceq \overline{W}$. So $\overline{V} \sim \overline{W}$.

Conversely assume that $\overline{V} \sim \overline{W}$. Then $\chi_{\overline{V}} = \chi_{\overline{W}}$ and therefore $\chi_V^{\mathcal{U}} = \chi_{\overline{V}}^{\mathcal{U}} = \chi_{\overline{W}}^{\mathcal{U}} = \chi_W^{\mathcal{U}}$. ■

Definition 2.3. *Let k be the number of G-conjugacy classes of subgroups in $\mathcal{U}$. The product $\prod_{i=1}^{k} Z$ (some copies of the integer ring), is called the Ghost ring of G.*

Theorem 2.4. *The product map $\chi := \prod_{i=1}^{k} \chi_i : B(G, \mathcal{U}) \longrightarrow \prod_{i=1}^{k} Z$ of k different homomorphisms from $B(G, \mathcal{U})$ into Z is injective and maps $B(G, \mathcal{U})$ onto a subring of finite index $\prod_{i=1}^{k}(N_G(U_i) : U_i)$ of $\prod_{i=1}^{k} Z$ – this way identifying $\prod_{i=1}^{k} Z$ with the integral closure $\tilde{B}(G, \mathcal{U})$ of $B(G, \mathcal{U})$ in its total quotient ring*

$$\tilde{B}(G, \mathcal{U}) \cong Q \otimes_Z B(G, \mathcal{U}) \cong \prod_{i=1}^{k} Q([3][chapter5]).$$

Proof : For the proof we need the following:

Lemma 2.5. *For S, S' $(G, \mathcal{U})$-sets, we have $S \cong S'$ if and only if $\chi_U(S) = \chi_U(S')$ for all $U \in \mathcal{U}$.*

Proof : Let $S = \sum_{U \in \mathcal{U}'} n_U \cdot G/U$ and $S' = \sum_{U \in \mathcal{U}'} n'_U \cdot G/U$ for nonnegative integers n_U, n'_U. Then it suffices to show that $n_U = n'_U$ for all $U \in \mathcal{U}' \iff \chi_U(S) = \chi_U(S')$ for all $U \in \mathcal{U}'$.

The direction "$\Longrightarrow$" is trivial.

Now assume $\chi_U(S) = \chi_U(S')$ but $n_U \neq n'_U$ for some $U \in \mathcal{U}'$. Then

$$\begin{aligned} 0 &= \chi_U(S) - \chi_U(S') \\ &= \sum_{U \in \mathcal{U}'} n_U \chi_U(G/U) - \sum_{U \in \mathcal{U}'} n'_U \chi_U(G/U) \\ &= \sum_{U \in \mathcal{U}'} (n_U - n'_U)\chi_U(G/U). \end{aligned}$$

Now consider a maximal subgroup $U' \in \mathcal{U}'$ with $n_{U'} \neq n'_{U'}$. Because of the maximality of $U' \in \mathcal{U}$ we have $\chi_{U'}(G/U) = 0$ for all $U \in \mathcal{U}'$ with $n_U \neq n'_U$ and $U \neq U'$. But this implies

$$\sum_{U \in \mathcal{U}'} (n_U - n'_U) \cdot \chi_{U'}(G/U) = (n_{U'} - n'_{U'})\chi_{U'}(G/U') \neq 0,$$

a contradiction.

Proof of 2.4: We observe that any $x \in B(G, \mathcal{U})$ can be written in the form $x = [S] - [S']$ with S and S' $(G, \mathcal{U})$-sets. If $\chi_i(x) = 0$ for all $i = 1, \ldots, k$ then

$\chi_i(S) = \chi_i(S')$ for all $i = 1, \ldots, k$; hence from the lemma $S \cong S'$. It follows that $x = [S] - [S'] = 0$, which shows injectivity. It remains to show that the map χ maps $B(G, \mathcal{U})$ onto a subring of finite index $\Pi_{i=1}^{k}(N_G(U_i) : U_i)$ of $\prod_{i=1}^{k} Z$. For this we invoke the following.

Lemma 2.6. *The automorphism group $N_G(U)/U$ of G/U acts freely on G/U and also on the set $(G/U)^V$ of V-invariant elements in G/U for any $V \leq G$. In particular $|N_G(U)/U| = |(G/U)^U|$ divides $|(G/U)^V|$ for any $V \leq G$.*

Proof : (see [3] [chapter 2]) ∎

We note from above that for $B(G, \mathcal{U}) = B(G)$ and for every subgroup U of G there exists a canonical homomorphism $\chi_U : B(G) \longrightarrow Z$, which maps every finite G-set S onto the cardinality $\chi_U(S) := \#S^U$ of its subset

$$S^U = \{s \in S \mid us = s \text{ for all } u \in U\}$$

of U invariant elements – in particular $\chi_1(S) = \#S$ if $1 = \{1_G\}$ denotes the trivial subgroup of G. One also has that $\chi_U = \chi_V$ if and only if $U \overset{G}{\sim} V$ for $U,\ V \leq G$ (where $U \overset{G}{\sim} V$ denotes that U and V are conjugate in G) and $\chi_U(x) = \chi_U(x')$ for all $U \leq G$ if and only if $x = x'$ for $x,\ x' \in B(G)$. So identifying each $x \in B(G)$ with the associated map $U \rightarrow \chi_U(x)$ from the set $\mathcal{S}(G)$ of all subgroups of G into Z also denoted by x, we can consider $B(G)$ in a canonical way as a subring of the ghost ring $\tilde{B}(G) = \prod_{U \leq G}{}' Z$ of G, consisting of all maps from $\mathcal{S}(G)$ into Z which are constant on each conjugacy class of subgroups. Now consider the isomorphism classes of the transitive G-sets of the form $G/U := \{gU \mid g \in G\}$. These isomorphism classes form a Z basis of $B(G)$ and for $U, V \leq G$ we have $G/U \cong G/V$ if and only if $U \overset{G}{\sim} V$. This then implies that every $x \in B(G)$ can be expressed uniquely in the form $x = \sum_{U \leq G}' \mu_U(x) \cdot G/U$ where " $\sum'$" indicates that the sum extends over just one subgroup out of every G-conjugacy class of subgroups. That is, every $x \in B(G)$ can be expressed as a linear combination of the isomorphism classes of transitive G-sets of type G/U with uniquely determined integral coefficients $\mu_U(x) \in Z$ subject to the relation $\mu_U(x) = \mu_V(x)$ if $U \overset{G}{\sim} V$. Now recall that for $U, V \leq G$ one has $chi_V(G/U) \neq 0$ if and only if $V \preceq U$ in which case one has

$$\begin{aligned}
\chi_V(G/U) &= \#\{gU \in G/U \mid VgU = gU\} \\
&= \frac{1}{|U|} . \#\{g \in G \mid VgU = gU\} \\
&= \frac{1}{|U|} \cdot \#\{g \in G \mid V \leq gUg^{-1}\} \\
&= (N_G(U) : U) \cdot \#\{U' \leq G \mid V \leq U' \overset{G}{\sim} U\},
\end{aligned}$$

where as usual

$$\begin{aligned}
N_G(U) &= \{g \in G \mid g^{-1}Ug = U\} \\
&= \{g \in G \mid UgU = gU\} \\
&= \{g \in G \mid gU \in (G/U)^U\}
\end{aligned}$$

is the normalizer of U in G. We note that given any $x \in B(G)$, a subgroup $U \leq G$ is a maximal subgroup (relative to "$\preceq$") with $\mu_U(x) \neq 0$ if and only if it is a maximal subgroup with $\chi_U(x) \neq 0$ because if $U \leq G$ is maximal with $\mu_V(x) \neq 0$ then

$$\chi_U(x) \quad = \quad {\sum_{U \preceq V \subseteq G}}' \mu_V(x)\chi_U(G/V) \quad = \quad \mu_U(x)\chi_U(G/U).$$

By assumption $\mu_U(x) \neq 0$ and we know that $\chi_U(G/U) \neq 0$. Therefore $\chi_U(x) \neq 0$. In addition, for any $U' \in \mathcal{S}(G)$ with $U \preceq U'$ but $U \not\sim U'$ we have $\chi_{U'}(x) = 0$ because $\mu_V(x).\chi_{U'}(G/V) = 0$ for all $V \leq G$ in view of the fact that $\chi_{U'}(G/V) \neq 0$ implies $U' \preceq V$ and therefore $\mu_V(x) = 0$.

The converse is proved by reversing the argument.

Note that in the foregone case one has

$$\chi_U(x) = \mu_U(x).\chi_U(G/U) = \mu_U(x) \cdot (N_G(U) : U).$$

Because as observed earlier, every $x \in B(G)$ can be expressed uniquely in the form

$$x = {\sum_{U \leq G}}' \mu_U(x) \cdot (G/U),$$

it follows that in the case where G is a p-group one has

$$\chi_1(x) \quad = \quad \sum_{U \leq G} \mu_U(x) \cdot (G : U) \quad \equiv \quad \mu_G(x) \quad = \quad \chi_G(x)(modp).$$

Hence, if V is a p-subgroup of an arbitrary finite group G and if U is a subgroup of G with its index $(G : U)$ prime to p then

$$\chi_V(G/U) \; \equiv \; \chi_1(G/U) \; = \; (G : U) \; \not\equiv \; 0(mod\ p),$$

and therefore $V \preceq U$.

Lemma 2.7. *For every $x \in B(G)$ one has*

$$\sum_{g \in G} \chi_{<g>}(x) \; \equiv \; 0(mod\ |G|)$$

where $< g >$ denotes the cyclic group generated by g. (This relation is sometimes called the Cauchy-Frobenius- Burnside relation).

Proof : It is enough to check this only for $x = G/U$ in which case one easily gets

$$\begin{aligned} \sum_{g \in G} \chi_{<g>}(G/U) \quad &= \quad \sum_{g \in G} \#\{hU \in G/U \mid ghU = hU\} \\ &= \quad \sum_{hU \in G/U} \#\{g \in G \mid ghU = hU\} \\ &= \quad \sum_{hU \in G/U} |hUh^{-1}| \; = \; (G : U)|U| \\ &= \quad |G| \; \equiv \; 0(\mathrm{mod}\ |G|). \end{aligned}$$

■

Note that if $U \trianglelefteq V \leq G$ and if S is a G-set, then the above lemma applied with respect to the V/U-set S^U implies $\sum_{vU \in V/U} \chi_{<v,U>}(S) \equiv 0(mod\ (V:U))$, where $< v\ ,\ U >$ denotes the subgroup generated by v and U. As a consequence one has:

Corollary 2.8. *Let $x \in \tilde{B}(G)$. Then $x \in B(G)$ if and only if for every $U \trianglelefteq V \leq G$ with $(V:U)$ a power of a prime one has $\sum_{vU \in V/U} x(< v\ ,\ U >) \equiv 0(mod\ (V:U))$.*

For more details on the Burnside ring (see [3], [9]).

3 The Artin exponent

We shall now give a definition of the Artin exponent in terms of the Burnside ring. Elaborating on what has been explained so far, one can actually characterize the elements in $\tilde{B}(G)$ which are in $B(G)$ as follows.

Definition 3.1. *For $\mathcal{U}$ a family of subgroups of G closed with respect to conjugation, define $e_{\mathcal{U}} \in \tilde{B}(G)$ by*

$$e_U := \begin{cases} 1 & \text{if } U \in \mathcal{U} \\ 0 & \text{if } U \notin \mathcal{U}. \end{cases}$$

Then for any $\mathcal{U}$ one has that

$$|G| \cdot e_U \in B(G) \qquad (**)$$

Furthermore define $A(G\ ,\ \mathcal{U}) := min(n \in N \mid n \cdot e_U \in B(G))$. The integer $A(G\ ,\ \mathcal{U})$ is said to be an exponent for G.

Theorem 3.2. *One has that (**) implies that $|G| \geq A(G\ ,\ \mathcal{U})$ – more precisely it implies that $A(G\ ,\ \mathcal{U})$ divides $|G|$.*

Proof : Put $a := A(G\ ,\ \mathcal{U})$ and write $|G| = qa + r$ with $0 \leq r < a$. Now

$$r \cdot e_U = (|G| - qa) \cdot e_U = |G| \cdot e_U - (qa) \cdot e_U \in B(G).$$

Hence $r = 0$ in view of the minimality of a. ∎

Observe from 2.8, that $n \cdot e_U \in B(G)$ if and only if for every $U \trianglelefteq V \leq G$ with $(V:U)$ a prime power one has $\sum_{vU \in V/U} n \cdot e_U(< v\ ,\ U >) \equiv 0(\text{mod}(V:U))$ where

$$e_U(< v\ ,\ U >) := \#\{vU \in V/U \mid < v\ ,\ U > \in \mathcal{U}\}.$$

In the case where $\mathcal{U}$ denotes the set of all cyclic subgroups of G, the quantity – which we shall henceforth denote by $A(G)$ – is called the Artin exponent of G. Compare Lam [5]. So in order to compute the Artin exponent, we shall be interested in the number
$\mathbf{c}(U\ ,\ V) := \#\{vU \in V/U \mid < v\ ,\ U > \text{ is cyclic }\}$. But this number is always equal to 0 unless U is cyclic. So assume U is cyclic.

Now for $U \trianglelefteq V \leq G$, assume that U is cyclic and $(V:U) = p^\alpha$ for some prime p. Consider the decomposition $U = U_p \times U_{p'}$ where $|U_p| = p^\beta$, a power of p and $|U_{p'}|$ is prime to p. Let V_p denote a Sylow p-subgroup of V. We have the following;

Proposition 3.3. *(a)* $(V : U) = p^\alpha$ *implies that* $V = V_p \propto U_{p'}$ *and* $V = V_p \times U_{p'}$ *if and only if* $U \leq Z(V)$*, the center of* V*. (Here* $\propto$*, resp.* $\times$ *denotes the semidirect product, resp. direct product with* $U_{p'} \trianglelefteq V$ *in the semidirect product).*

(b) $(V : U) = (V_p : U_p)$.

(c) If $\mathbf{c}(U\ ,\ V) := \#\{vU \in V/U \ \ | \ \ < v\ ,\ U > \ \textit{is cyclic}\ \}$ *and*

$\mathbf{c}(U_p\ ,\ V_p) := \#\{vU_p \in V_p/U_p \ \ | \ \ < v\ ,\ U_p > \ \textit{is cyclic}\ \}$ *then*

$\mathbf{c}(U\ ,\ V) \ = \ \mathbf{c}(U_p\ ,\ V_p)$ *if* $V = V_p \otimes U_{p'}$*, that is* $U \leq Z(V)$.

Proof : Since V_p is p-Sylow subgroup of V then $U_p \leq V_p$ and $(|U_{p'}|\ ,\ p) = 1 \ \Rightarrow$ $V_p \cap U_{p'} \ = \ \{1\}$. Because $(V\ :\ U) = p^\alpha$, the factor of $|U|$ relatively prime to p coincides with the factor of $|V|$ relatively prime to p and so $|V| = |V_p|.|U_{p'}|$. We therefore conclude that $V = V_p \propto U_{p'}$. Now if $V = V_p \times U_p$, then for $v,\ v^{'} \in V_p$ and $u,\ u^{'} \in U_{p'}$, one has $(v\ ,\ u)(v^{'}\ ,\ u^{'}) = (v \cdot v^{'}\ ,\ u^{v^{'}} \cdot u^{'})$ and $u^{v^{'}} := v^{'-1}uv^{'} = u \iff$ $uv^{'} = v^{'}u,\ i.e. \iff U \leq Z(V)$.

(b) From (a) one has, $(V : U) \ = \ ((V_p.U_{p'}) : (U_p.U_{p'})) \ = \ (V_p : U_p)$.

(c) Define a map $f : V_p/U_p \rightarrow V/U$ by $f(vU_p) = vU,\ (v \in V_p)$, and observe that $U_p \cap U = U_p =$ ker f. The rest follows from the isomorphism theorem. ∎

Let $C_V(U) \ := \ \{w \in V \mid wu = uw \text{ for all } u \in U\}$ denote the centralizer of U in V. Observe that for $vU \in V/U$ the group $< v\ ,\ U >$ is cyclic only if $v \in C_V(U)$.

Hence $\mathbf{c}(U\ ,\ V) \ = \ \mathbf{c}(U\ ,\ C_V(U))$. But since $\mathbf{c}(U\ ,\ C_V(U)) \leq (C_V(U) : U)$, we have that the number "n" must always be divisible by $(V\ :\ C_V(U))$ to have that $(V : U)$ divides $n \cdot \mathbf{c}(U\ ,\ V)$. We thus have the following strategy for computing the Artin exponent. For each p - subgroup V of G, consider the set of all cyclic normal subgroups U of V with U contained in the centre of V and compute the minimum of those positive integers n for which $(V\ :\ U)$ divides $n \cdot \mathbf{c}(U\ ,\ V)$. Finally, it is easy to see that if $U \leq Z(V)$ for a p-group V such that U is cyclic one has that $\mathbf{c}(U\ ,\ V) = \mathbf{c}(U/U^p\ ,\ V/U^p)$, where U^p denotes the unique subgroup of U of index p. So we can restrict ourselves to the case where $|U| = p$. In the next section we include some results concerning p-groups.

4 Some useful facts concerning p-groups

Recall (see [4][chapter 1]) that for elements $g,\ g_1,\ g_2,\ h,\ h_1,\ h_2,\ \ldots\ldots,$ a finite group G that the following remarks hold.

Remark 4.1. *(1)* $[g\ ,\ h]^{-1} \ = \ [h\ ,\ g] \ = \ g_{[g^{-1},h]}$.

(2) $[g_1g_2\ ,\ h] \ = \ g_1[g_2\ ,\ h]g_1^{-1} \cdot [g_1\ ,\ h] \ = \ g_{1[g_2,h]} \cdot [g_1, h]$.

(3) $(gh)^2 \ = \ g_{[h,g]} \cdot g^2 \cdot h^2$

(4) $(gh)^n \ = \ g_{[h,g]} \cdot {g^2}_{[h^2,g]} \cdot \ \cdot \ \cdot {g^{n-1}}_{[h^{n-1},g]} \cdot g^n \cdot h^n$.

(5) $[g\ ,\ G] \ = \ \{1\} \iff g \ \in \ Z(G) \ := \ \{g \in G \mid gh = hg \textit{ for all } h \in G\}$

(6) $U \leq G \Longrightarrow (U \trianglelefteq G \Longleftrightarrow [U\ ,\ G] \subseteq U)$.

(7) In particular if $[G\ ,\ G] \subseteq Z(G)$ *then* $[g_1g_2\ ,\ h] = [g_1\ ,\ h].[g_2\ ,\ h]$ *and* $(gh)^n = [h\ ,\ g]^{\binom{n}{2}} g^n h^n$ *for all* $g,\ g_1,\ g_2,\ h \in G$, *and if in addition* $[g,h]^k = 1$ *for s ome* $k \in N$ *and all* $g,h \in G$, *then* $g^k \in Z(G)$ *for all* $g \in G$ *and with*

$$N := < \{[g\ ,\ h]^{\binom{k}{2}} \mid g,h \in G\} > \quad \begin{cases} = 1 & \text{if } k \equiv 1(2) \\ \subseteq < \{z \in Z(G) \mid z^2 = 1\} >, & \text{if } k \equiv 0(2) \end{cases}$$

the map $G \longrightarrow Z(G)/N :\ g \to g^k \cdot N$ *is a group homomorphism.*
Other consequences of the above commutator formulae are as follows;

(8) If $T \subseteq G$ *then* $[< T >\ ,\ < T >] \subseteq < \{g_{[h_1,h_2]} \mid g \in < T >,\ h_1,h_2 \in T\} > \subseteq < [T\ ,\ T] >_N$.

(9) If $T \subseteq G$ *then* $< T > \trianglelefteq G$, *that is* $< T >_N = < T >$ *if and only if* $[T\ ,\ G] \subseteq < T >$; *more generally, for* $S,T \subseteq G$ *and* $T \subseteq U \leq G$ *we have*

$$[< T >\ ,\ S] \subseteq U \Leftrightarrow [T\ ,\ S] \subseteq U.$$

We also state the following results (see [4][chapter 3]).

Proposition 4.2. *(a) If* $N \trianglelefteq G$ *is a maximal abelian normal subgroup of* G, *so that in particular*

$$N \subseteq C_G(N) := \{g \in G \mid [g\ ,\ N] = 1\},$$

then

$$C_G(N) \cap \{g \in G \mid [g\ ,\ G]\ \subseteq < N \cup \{g\} >\} = N.$$

In particular if G/N *is nilpotent then* $C_G(N) = N$ *and therefore*

$$ker(G \longrightarrow Aut(N) : g \to (N \to N : x \to g_x)) = N.$$

So we may consider G/N *as a subgroup of* $Aut(N)$, *the full automorphism group of* N.

(b) For a finite p-group G *and an element* $g \in G$ *we have* $< g >\ \trianglelefteq G \Longleftrightarrow [g\ ,\ G]\ \subseteq < g^p >$.

(c) Let G *be a noncyclic finite p-group. If for some* $h \in G$ *the cyclic subgroup* $H := < h >$ *is a maximal abelian normal subgroup of* G *then* $|H| \geq p^2$ *and either* $p = 2$ *and* $(G : H) = 2$ *or there exists some* $g \in G - H$ *such that* $< H \cup \{g\} >\ \trianglelefteq G$ *and* $[g\ ,\ H]\ \subseteq\ \{y \in H \mid y^p = 1\}$.

Some Notation:
Let G be a finite p-group and let U and H be subgroups of G such that U is a cyclic normal subgroup with $U \subseteq H$.
Let $\mathcal{C}(H)$ denote the set of all cyclic subgroups V of H with $U\ \leq\ V$ and $(V\ :\ U)\ =\ p$, and let $\mathcal{C}'(H) = \mathcal{C}'_U(H)$ denote the subset of $\mathcal{C}(H)$, consisting of those $V \in \mathcal{C}(H)$ which are normal in H. One has the following lemmata.

Lemma 4.3. *(a.)* $|\mathcal{C}(H)| \equiv |\mathcal{C}'(H)|$ *(mod p).*

(b.) $H^{'} = H^{'}_U := \{h \in H \mid [h\ ,\ H] \subseteq U\}$ *is a normal subgroup of H.*

(c.) $\mathcal{C}^{'}(H) = \mathcal{C}(H^{'})$.

(d.) If $G^{'} \subseteq H \trianglelefteq G$, *then* $|\mathcal{C}(H)| = |\mathcal{C}(G^{'})|(mod\ p)$.

Lemma 4.4. *If* $|U| = p \neq 2$ *and* $[G\ ,\ G] \subseteq U$, *then the following are equivalent:*
(i) $|\mathcal{C}(G)| = 1$
(ii) $|\mathcal{C}(G)| \not\equiv 0(mod\ \ p)$
(iii) G is cyclic.

Proof : (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) is trivial.
(ii) $\Rightarrow$ (iii): Obviously, if $U =< u >$ then, $p \cdot |Z(G)| = |\{v \in G \mid v^p = u\}|$, and $\{z \in Z(G) \mid z^p = 1\}$ acts freely on $\{v \in G \mid v^p = u\}$ via multiplication. Hence (ii) implies that $Z(G)$ must be cyclic. Now $U \subseteq Z(G)$, hence for $g, h \in U$, one has by (4.1) remark 7 that $[g^p\ ,\ h] = [g\ ,\ h]^p = 1$ and $(g_1g_2)^p = [g_1\ ,\ g_2]^{\binom{p}{2}} g_1^p g_2^p = g_1^p g_2^p$, the map $G \to Z(G) : g \to g^p$ is a group homomorphism from G into $Z(G)$ (by (4.1) remark 7 again). So we have $|\{v \in G \mid v^p = u\}|$ is either 0 in contradiction to our assu mption or coincides with the order of the kernel of this homomorphism. So this kernel, containing U, must have order p, so it must coincide with U. Since one now has $U \subseteq Z(G)$, $G/U \hookrightarrow Z(G)$ and $Z(G)$ is cycli c, this implies that $G = Z(G)$, so G must be cyclic.

■

Lemma 4.5. *If G is abelian, then the following are equivalent:*
(i) $|\mathcal{C}(G)| = 1$
(ii) $|\mathcal{C}(G)| \not\equiv 0(mod\ \ p)$
(iii) G is cyclic.

Proof : (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) is again trivial. And (ii) $\Rightarrow$ (iii) follows from (4.4) by noting that here $Z(G) = G$. ■

Lemma 4.6. *If* $|U| = p \neq 2$, *then the following are equivalent;*
(i) $|\mathcal{C}_U(G)| = 1$
(ii) $|\mathcal{C}_U(G)| \not\equiv 0(mod\ \ p)$
(iii) G is cyclic.

Proof : Again (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii) is obvious.
So we assume (ii) and consider $G^{'} = \{\ g \in G \mid [g\ ,\ U] \subseteq U\} \trianglelefteq G$.
Since, $|\mathcal{C}(G')| \equiv |\mathcal{C}(G)| \not\equiv 0(\text{mod}\ \ p)$ by (4.4) and $[G^{'}\ ,\ G^{'}] \subseteq U$, G' must be cyclic. Now let $H \trianglelefteq G$ denote a maximal abelian normal subgroup of G, containing G'. Since $|\mathcal{C}(H)| \equiv |\mathcal{C}(G)| \not\equiv 0(\text{mod}\ \ p)$, H must be cyclic. For any $g \in G - H$ with $g^p \in H$ we therefo re have, $[g\ ,\ H] \subseteq U$ and $H_1 :=< g\ ,\ H > \trianglelefteq G$. Hence by (4.4) again $[H_1\ ,\ H_1] \subseteq U$ and $|\mathcal{C}(H_1)| \equiv |\mathcal{C}(G)| \not\equiv 0(\text{mod}\ \ p)$, so H_1 must be cyclic, a contradiction. ■

Next we collect the following results (see [4][chapter 3]).

Lemma 4.7. *(a) If G is a 2-group, one has that $|\mathcal{C}(H)| \equiv 1(mod\ 2) \Longrightarrow Z(G)$ is cyclic.*

(b) Let G be a finite 2-group. If $[G\ ,\ G] \subseteq U$ and $|\mathcal{C}(H)|$ is odd, then G is cyclic or nonabelian of order 8.

(c) Let G denote a finite 2-group. If $H \leq G$ with $[H\ ,\ H] \subseteq U \subseteq H$ and $|\{V \in \mathcal{C}(H) \mid V \subseteq H\}| \equiv 1(mod\ 2)$ then H is cyclic or nonabelian of order 8.

(d) If $|\mathcal{C}(H)| \equiv 1(mod\ 2)$ then either H' is cyclic or G is nonabelian of order 8.

(e) If $|\mathcal{C}(H)| \equiv 1(mod\ 2)$ then G contains a cyclic normal subgroup of index 2.

Proposition 4.8. *Let G be a noncyclic p-group $(p \neq 2)$ and $U \trianglelefteq G$, $|U| = p$. Then there exists a normal subgroup $V \trianglelefteq G$ of G of order p^2, containing U and isomorphic to $Z_p \times Z_p$.*

Proof : (see [4][satz 14.9]).

5 Applications

Here, using our setup, we give the proofs of the existing results concerning the Artin exponent of finite p-groups (see [5]). The global calculation will be discussed in a separate publication (see [7]). We first recall;

Lemma 5.1. *Let G be a p-group of order p^n, If there exists a $g \in G$ of order p^{n-1} then G has one of the following presentations for some h in G.*

(A) *If G abelian:*

(i) $n \geq 1$, Z_{p^n}: $h^{p^n} = 1$, or

(ii) $n \geq 2$, $g^{p^{n-1}} = 1$, $h^p = 1$, $gh = hg$.

(B) *If G is non-abelian and p odd, $n \geq 3$:*

(iii) $g^{p^{n-1}} = 1$, $h^p = 1$, $hgh^{-1} = g^{1+p^{n-2}}$.

(C) *If G nonabelian and $p = 2$, $n \geq 3$:*

(iv) $g^{2^{n-1}} = 1$, $h^2 = g^{2^{n-2}}$, $hgh^{-1} = g^{-1}$, i.e. the generalized quaternion group: **(Q)**,

(v) $g^{2^{n-1}} = 1$, $h^2 = 1$, $hgh^{-1} = g^{-1}$, i.e. the dihedral group: **(D)**.

(D) *If G is non-abelian and $p = 2$, $n \geq 4$:*

(vi) $g^{2^{n-1}} = 1$, $h^2 = 1$, $hgh^{-1} = g^{1+2^{n-2}}$,

(vii) $g^{2^{n-1}} = 1$, $h^2 = 1$, $hgh^{-1} = g^{-1+2^{n-2}}$, i.e. the semi- dihedral group: **(SD)**.

Proof : easy.

Proposition 5.2. *Let G be a p-group of order p^α and choose $\mathcal{U}$ to be the family of all cyclic subgroups of G. For $n \in N$ and a subgroup $U \leq G$, let $x_n \in \tilde{B}(G)$ be defined by*

$$x_n = \begin{cases} n & \textit{if } U \textit{ is cyclic} \\ 0 & \textit{otherwise} \end{cases}$$

Then $A(G) := min\{n \mid x_n \in B(G)\} = 1$ if and only if G is cyclic.

Proof : Assume $U \trianglelefteq V \leq G$, U cyclic, $|V| = p^\alpha$ (p a prime). Then $x_n \in B(G)$ implies

$$\begin{aligned} \sum_{vU \in V/U} x(< v\ ,\ U >) &= n \cdot \#\{\ vU \in V/U \mid < v\ ,\ U > \text{ cyclic }\} \\ &\equiv 0(mod\ (V : U)). \end{aligned}$$

Since G is not assumed cyclic and n is arbitrary, we get our $A(G)$ by making the following assumptions. Assume $|U| = p$, $V = G$, that is $|G| = p^\alpha$. Then if $n = 1$, then one has that $\#\{gU \in G/U \mid < g\ ,\ U > \text{ cyclic }\} \equiv 0(mod\ (G : U))$. That is $(G : U) \mid \#\{gU \in G/U \mid < g\ ,\ U > \text{ is cyclic }\}$. This implies that $|G| \mid \#\{g \in G \mid < g\ ,\ U > \text{ is cyclic }\}$. So for all $g \in G$, $< g\ ,\ U >$ is cyclic. This means that G is cyclic since if G is not cyclic then from (4.8) there exists a normal subgroup $V \trianglelefteq G$ such that V contains U and $V \cong Z_p \times Z_p \cong U \times Z_p = U \times < g >$ for some $g \in G$. That is $< g\ ,\ U > = V$ for some $g \in G$.
The converse is clear. ∎

Proposition 5.3. *Keeping the assumptions of (5.2), one has that if G is a noncyclic p-group of order p^α and $p \neq 2$ then $A(G) = p^{\alpha-1}$.*

Proof : Because G is noncyclic, $|G|$ does not divide $x(< g\ ,\ U >) = \#\{gU \in G/U \mid < g\ ,\ U > \text{ cyclic }\}$. But

$$\begin{aligned} x(< g\ ,\ U >) &= \#\{gU \in G/U \mid < g\ ,\ U > \text{ is cyclic }\} \\ &= \#\{gU \in G/U \mid < g\ ,\ U > \text{ is cyclic of order } p\} \\ &\quad + \sum_{\beta \geq 2} \#\{gU \in G/U \mid < g\ ,\ U > \text{ is cyclic of order } p^\beta\} \\ &= 1 + \sum_{\beta \geq 2} (p^{\beta-1} - p^{\beta-2}) \cdot \#\{C \leq G | C \text{ is cyclic of order } p^\beta, C \supseteq U\} \\ &= = 1 + (p-1) \cdot \#\{C \leq G \mid C \text{ is cyclic of order } p^2,\ C \supseteq U\} \\ &+ \sum_{\beta \geq 3} (p^{\beta-1} - p^{\beta-2}) \cdot \#\{C \leq G | \ C \text{ is cyclic of order } p^\beta, C \supseteq U\}. \end{aligned}$$

It suffices to look at the number $\#\{C \leq G \mid C \text{ is cyclic of order } p^2,\ C \supseteq U\}$. But since G is noncyclic one has from (4.5) that this number is divisible by p. This means $A(G) = (G : U) = p^{\alpha-1}$.

∎

Proposition 5.4. *With the assumptions of (5.2) one has that if G is noncyclic 2-group of order 2^α then $A(G) = 2^{\alpha-1}$, unless* $\mathbf{G} = \mathbf{Q}$, $\mathbf{D}$ *or* $\mathbf{SD}$ *(as defined in Lemma 5.1), in which cases we have $A(G) = 2$.*

Proof : Following (5.3) one has that if

$$\#\{C \ \leq \ G \ \mid \ C \text{ is cyclic of order } 4, \ C \supseteq U\} \equiv 0(mod\ 2),$$

then $A(G) = 2^{\alpha-1}$. On the other hand if

$$\#\{C \ \leq \ G \ \mid \ C \text{ is cyclic of order } 4, \ C \ \supseteq \ U\} \not\equiv 0(mod\ 2)\}$$

then by (4.7) G is cyclic or nonabelian group of order 8. Since G is noncyclic it must be nonabelian of order 8 and so must correspond to one the groups $\mathbf{Q}, \mathbf{D}$ and $\mathbf{SD}$ as presented in (5.1) and it is easy to see by direct computation that in any of these cases that $A(G) \ = \ 2.$ ■

References

[1] A. Dress; A Characterization of Solvable Groups, *Math. Z. 110, pp. 213- 217, (1969).*

[2] A. Dress; Congruence Relations characterizing the Representation Ring of the Symmetric Group *J. Algebra 2, pp. 350-363, (1986).*

[3] A. Dress; Notes on the Theory of Representations of Finite Groups, *Lecture Note, Bielefeld, (1971).*

[4] B. Huppert; Endliche Gruppen 1, *Springer Verlag, NewYork, (1968).*

[5] T.Y. Lam; Artin exponent for finite groups, *J. Algebra 9, pp. 94-119, (1963).*

[6] K.K. Nwabueze; A Burnside ring theoretic proof of T.Y. Lam's results concerning the Artin exponent of finite groups *Maths. report, The Royal Society of Canada, pp. 17-21, Feb., (1996).*

[7] K.K. Nwabueze & F. Van Oystaeyen; Certain applications of the Burnside rings and Ghost rings in the Representation theory of finite groups (II), (*to appear*).

[8] R. Swan; Induced Representation and Projective Modules, *Ann. Math. 71, (1960).*

[9] T. Tom - Dieck; Transformation groups and representation theory, *Lecture Notes in Maths 766, Springer, (1979).*

Dept of Mathematics & Computer Science,
University of Antwerpen (U.I.A),
2610 Wilrijk,
BELGIUM.

Current Address:
Mathematical Sciences Research Institute,
1000 Centennial Drive,
University of California,
Berkeley, Calif. 94720,
U.S.A.