ADVANCES IN MATHEMATICS **91**, 27–44 (1992)

An Application of Burnside Rings in Elementary Finite Group Theory

ANDREAS W. M. DRESS* AND CHRISTIAN SIEBENEICHER*

Fakultät für Mathematik, Universität Bielefeld, Universitätstrasse, 4800 Bielefeld 1, Germany

AND

TOMOYUKI YOSHIDA*

Department of Mathematics, Hokkaido University, Kita 10 Nishi 8, Sapporo 060, Japan; and Fakultät für Mathematik, Universität Bielefeld Universitätstrasse, 4800 Bielefeld 1, Germany

A canonical map from the Burnside ring $\Omega(C)$ of a finite cyclic group C into the Burnside ring $\Omega(G)$ of any finite group G of the same order is exhibited and it is shown that many results from elementary finite group theory, in particular those claiming certain congruence relations, are simple consequences of the existence of this map. In addition, it is shown that this map defines an isomorphism from $\Omega(C)$ onto the subring $\Omega_0(G)$ of $\Omega(G)$, consisting of those virtual G-sets x which have the same number of invariants for every two subgroups U, V of G of the same order, if and only if G is nilpotent. Finally, a rather natural extension to profinite groups is indicated. © 1992 Academic Press, Inc.

1. INTRODUCTION

In this note we want to point out a simple fact concerning Burnside rings which can be viewed as a surprisingly compact and transparent structural reformulation in Burnside ring theoretic terms of the various ideas and tricks introduced by G. Frobenius [Fr1] and H. Wielandt [Wi] to prove the existence and further properties of Sylow p-subgroups and used later on by L. Solomon [So] (see also [Wa]) to establish further elementary results in finite group theory.

To be more precise, let G be a finite group of order $n := |G|$ and let $C := C_n$ denote the cyclic group of the same order n. The sole purpose of

* This work was supported by the SFB 7^3 "Diskrete Strukturen in der Mathematik," Universität Bielefeld.

0001-8708/92 $7.50

this note is to establish and to discuss some consequences of the following theorem[1]:

THEOREM 1. *There exists a ring homomorphism*

$$\alpha = \alpha^G = \alpha^G_{FW} : \Omega(C) \to \Omega(G)$$

which we call the Frobenius–Wielandt homomorphism *from the Burnside ring $\Omega(C)$ of the cyclic group C into the Burnside ring $\Omega(G)$ of G such that for every subgroup $U \leqslant G$ of G and every $x \in \Omega(C)$ the number $\varphi_U(\alpha(x))$ of U-invariant elements in the virtual G-set $\alpha(x)$ coincides with the corresponding number $\varphi_{C_{|U|}}(x)$ of $C_{|U|}$-invariant elements in x, where, of course, $C_{|U|}$ denotes the unique subgroup of order $|U|$ in C.*

Remark 1. This theorem gives a precise conceptual interpretation of the observation (cf. [Fr3, p. 395; Hu, p. 34; Wa]) that many elementary group-theoretic results can be derived from the fact that various invariants of an arbitrary group are closely related to the same invariant evaluated for the cyclic group C of the same order.

Remark 2. In the context of the theory of *Mackey* (and *Green*) *functors* developed in [Dr2–4] Theorem 1 has the surprising consequence that for any Mackey functor **M**, defined on the category $G^\wedge$ of finite G-sets, the value $\mathbf{M}(G/U)$ of **M** on the transitive G-set G/U can be considered in a canonical way as an $\Omega(C_{|U|})$-module and that for any (multiplicative) Green functor **G**, defined on $G^\wedge$, the ring $\mathbf{G}(G/U)$ can be viewed as an $\Omega(C_{|U|})$-algebra.

The outline of this note is as follows: in Section 2 we introduce notations and collect some well-known facts about G-sets and Burnside rings, in Section 3 we prove Theorem 1, in Section 4 we apply Theorem 1 to derive Sylow's and Frobenius' theorems, in Section 5 we discuss functorial properties of the Frobenius–Wielandt homomorphism, in Section 6 the kernel and the image of this homomorphism are studied, and in Section 7 we extend our results to profinite groups.

2. SOME FACTS ABOUT BURNSIDE RINGS

Before proving Theorem 1 let us recall shortly the basic concepts and notations from Burnside ring theory we have used in its formulation or will use in its proof or its applications.

[1] Notations will be explained in detail in Section 2.

For a finite group G we define its Burnside ring $\Omega(G)$ to be the Grothendieck ring of finite G-sets, which is generated as an algebra over $\mathbf{Z}$ by the (isomorphism classes of) finite (left) G-sets X, Y, ..., relative to the relations

$$X - Y = 0 \qquad \text{if} \quad X \cong Y,$$
$$X + Y - (X \cup Y) = 0,$$
$$X \cdot Y - (X \times Y) = 0.$$

In consequence, its elements are the *virtual G-sets*, i.e., the formal differences $X - Y$ of (isomorphism classes of) finite G-sets X, Y, and one has

$$X - Y = X' - Y' \Leftrightarrow Z \cup X \cup Y' \cong Z \cup Y \cup X'$$

for some finite G-set Z (which in turn is well known to be equivalent with $X \cup Y' \cong Y \cup X'$). For every subgroup U there exists a canonical homomorphism $\varphi_U : \Omega(G) \to \mathbf{Z}$ which maps every finite G-set X onto the cardinality $\varphi_U(X) := \# X^U$ of its subset

$$X^U := \{x \in X \mid u \cdot x = x \text{ for all } u \in U\}$$

of U-invariant elements, in particular $\varphi_1(X) = \# X$ if $1 = \{1_G\}$ denotes the trivial subgroup of G. For $U, V \leqslant G$ one has $\varphi_U = \varphi_V$ if and only if $U \sim^G V$ (that is, U and V are conjugate in G) and for $x, x' \in \Omega(G)$ one has $\varphi_U(x) = \varphi_U(x')$ for all $U \leqslant G$ if and only if $x = x'$. Hence, identifying each $x \in \Omega(G)$ with the associated map $U \mapsto \varphi_U(x)$ from the set $\mathrm{Sub}(G)$ of all subgroups of G into $\mathbf{Z}$, we can consider $\Omega(G)$ in a canonical way as a subring of the *ghost ring*

$$\tilde{\Omega}(G) := \mathbf{Z}^{\mathrm{Sub}(G)/\sim}$$

of G, consisting of all maps from $\mathrm{Sub}(G)$ into $\mathbf{Z}$ which are constant on each conjugacy class of subgroups.

Finally recall that the (isomorphism classes of the) transitive G-sets of the form $G/U := \{gU \mid g \in G\}$ (U a subgroup of G, the G-action on G/U is, of course, defined by left multiplication: $G \times G/U \to G/U$: $(h, gU) \mapsto hgU$) form a $\mathbf{Z}$-basis of $\Omega(G)$, while for $U, V \leqslant G$ we have $G/U \cong G/V$ if and only if $U \sim^G V$. Hence every $x \in \Omega(G)$ can be expressed as a linear combination in the form

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

with uniquely determined integral coefficients $\mu_U(x) \in \mathbf{Z}$, satisfying $\mu_U(x) = \mu_V(x)$ for $U \sim^G V$, and where the prime attached to the summation symbol $\sum'$ indicates that the sum does not actually extend over all subgroups of G, but only over a *system of G-representatives*, that is, one out of each conjugacy class of subgroups of G.

For $U, V \leqslant G$ one has $\varphi_V(G/U) \neq 0$ if and only if $V \lesssim_G U$ (that is, there exists $g \in G$ with $gVg^{-1} \subseteq U$) in which case one has

$$\begin{aligned}\varphi_V(G/U) &= \#\{gU \in G/U \mid VgU = gU\} \\ &= (N_G(U):U) \cdot \#\{U' \leqslant G \mid V \leqslant U' \sim^G U\},\end{aligned}$$

where, as usual,

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

denotes the *normalizer* of U in G. Hence, given $x \in \Omega(G)$, a subgroup $U \leqslant G$ is a *maximal* subgroup with $\mu_U(x) \neq 0$ if and only if it is a *maximal* subgroup with $\varphi_U(x) \neq 0$, in which case one has

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

From the fact that every $x \in \Omega(G)$ can be expressed uniquely in the form $x = \sum'_{U \leqslant G} \mu_U(x) \cdot G/U$ it follows, in particular, that for every p-group G we have

$$\begin{aligned}\varphi_1(x) &= \sum_{U \leqslant G}' \mu_U(x) \cdot (G:U) \\ &\equiv \mu_G(x) = \varphi_G(x) \qquad (\text{mod } p).\end{aligned}$$

Hence if V is a p-subgroup of an arbitrary finite group G and if U is a subgroup of G with an index $(G:U)$ which is prime to p, then $\varphi_V(G/U) \equiv \varphi_1(G/U) = (G:U) \not\equiv 0 \pmod p$ and therefore $V \lesssim_G U$. In particular, if Sylow p-subgroups exist in G, they all must be *conjugate* in G and every other p-group must be subconjugate in G to each of them.

3. Proof of Theorem 1

This is all (and actually quite a bit more than) we need to know to prove Theorem 1.

Let us observe first that the properties of α_{FW}^G described in Theorem 1 determine this map uniquely. Indeed, let γ_{FW}^G denote the map from $\text{Sub}(G)$ into $\text{Sub}(C)$ which associates to every subgroup U of G the unique subgroup $C_{|U|}$ of C which has the same order as U. Then clearly, γ^G_{FW} induces a ring homomorphism

$$\tilde{\alpha} = \tilde{\alpha}^G_{FW}: \tilde{\Omega}(C) \to \tilde{\Omega}(G): s \mapsto s \cdot \gamma^G_{FW}$$

on the level of ghost rings and Theorem 1 just claims that $\tilde{\alpha}$ maps the subring $\Omega(C)$ of $\tilde{\Omega}(C)$ into the subring $\Omega(G)$ of $\tilde{\Omega}(G)$.

To prove this claim we recall that for every finite G-set X and every natural number q the set $\binom{X}{q}$ of all subsets Y of X of cardinality q is also a finite G-set relative to the G-action

$$G \times \binom{X}{q} \to \binom{X}{q}: (g, Y) \mapsto g \cdot Y := \{g \cdot y \mid y \in Y\}.$$

Using these G-sets for $X := G/1$, the *regular* G-set, Theorem 1 follows immediately from the following two observations:

LEMMA 1. *$\tilde{\alpha}$ maps $\binom{C/1}{q} \in \Omega(C) \subseteq \tilde{\Omega}(C)$ onto $\binom{G/1}{q} \in \Omega(G) \subseteq \tilde{\Omega}(G)$.*

LEMMA 2. *If $\mathrm{Div}(n) := \{d \in \mathbf{N} \mid d \text{ divides } n\}$ denotes the set of divisors of n (and hence corresponds canonically in a one-to-one fashion with the set of subgroups of C via $d \leftrightarrow C_d$), then the family $\binom{C/1}{d}$ $(d \in \mathrm{Div}(n))$ of C-sets forms a $\mathbf{Z}$-basis of $\Omega(C)$.*

Lemma 1 in turn is an immediate consequence of the well-known fact that for every finite group G, every subgroup $U \leqslant G$ of G, and every $q \in \mathbf{N}$ the value of $\varphi_U(\binom{G/1}{q})$, that is, the number of U-invariant subsets of cardinality q in $G/1$, depends only on q and the orders of G and of U; that is, it follows from the following more explicit

LEMMA 1′. *For every finite group G, every subgroup $U \leqslant G$ of G, and every $q \in \mathbf{N}$ one has*

$$\varphi_U\left(\binom{G/1}{q}\right) = \begin{cases} 0 & \text{if } |U| \text{ does not divide } q, \\ \binom{(G:U)}{q/|U|} & \text{otherwise}; \end{cases}$$

in particular, if $|U| = q$, then $\varphi_U(\binom{G/1}{q}) = (G:U)$ and therefore

$$\mu_U\left(\binom{G/1}{q}\right) = \frac{(G:U)}{(N_G(U):U)} = (G:N_G(U)).$$

Proof. Indeed $Y \in \binom{G/1}{q}$ is U-invariant if and only if Y is the union of right cosets $Ug \subseteq G$ of U in G; hence such Y exist only if $|U|$ divides q in which case the set $\binom{G/1}{q}$ of U-invariant subsets Y in $\binom{G/1}{q}$ corresponds in a one-to-one fashion to the set $\binom{U\backslash G}{q/|U|}$ of subsets of $U\backslash G := \{Ug \mid g \in G\}$ of cardinality $q/|U|$. So its cardinality is of course $\binom{(G:U)}{q/|U|}$, as stated. ∎

The proof of Lemma 2 is equally simple: For every $d, d' \in \mathrm{Div}(n)$ we have integers

$$\mu_{d,d'} = \mu_{C_{d'}}\left(\binom{C/1}{d}\right) \in \mathbf{Z}$$

such that

$$\binom{C/1}{d} = \sum_{d' \in \mathrm{Div}(n)} \mu_{d,d'} \cdot C/C_{d'}$$

and we have to show that the determinant of the matrix

$$M := (\mu_{d,d'})_{d,d' \in \mathrm{Div}(n)}$$

is a unit in $\mathbf{Z}$. But in view of Lemma 1 we have $\varphi_{C_{d'}}(\binom{C/1}{d}) = 0$ unless d' divides d and, hence, we have also $\mu_{d,d'} = 0$ unless d' divides d, so M is *triangular* (relative to the obvious ordering of $\mathrm{Div}(n)$ according to which d comes before d' if d is smaller than d'). In addition, we have

$$\mu_{d,d} = \mu_{C_d}\left(\binom{C/1}{d}\right) = (C : N_C(C_d)) = 1,$$

so the main diagonal of M consists of ones, only, and hence its determinant is indeed 1. ∎

Remark. Rather than using *exterior powers* of G-sets, that is, the G-sets of the form $\binom{G/1}{q}$, introduced by H. Wielandt in this context, we could as well have used the *symmetric powers*, that is, the G-sets of the form

$$S^q(X) := \left\{ f : X \to \mathbf{N}_0 \;\middle|\; \sum_{x \in X} f(x) = q \right\},$$

where for a G-set X the group G acts on $S^q(X)$ via

$$G \times S^q(X) \to S^q(X) : (g, f) \mapsto (g \cdot f : X \to \mathbf{N}_0 : x \mapsto f(g^{-1} \cdot x)),$$

used by Wagner in this context [Wa] (see also [Fr1]). As before, the value of $\varphi_U(S^q(G/1))$ depends only on q, $|G|$, and $|U|$ and vanishes unless $|U|$ divides q, since $f \in S^q(G/1)$ is U-invariant if and only if it is constant on the U-cosets of the form Ug ($g \in G$); so $|U|$ must divide $q = \sum_{x \in G/1} f(x)$ if f is U-invariant, and in this case there are exactly as many U-invariant maps f in $S^q(G/1)$ as there are elements in $S^{q/|U|}(U\backslash G)$ (that is, there are precisely $\binom{(G:U)+q/|U|-1}{q/|U|}$ U-invariant maps in $S^q(G)$ if $|U|$ divides q, but we will not need this detailed information). So, as above, we have $\tilde{\alpha}(S^q(C/1)) = S^q(G/1)$. Moreover, if $|U|$ equals q, then there are exactly $(G:U)$ U-invariant elements in $S^q(G/1)$, that is, we have also

$$\mu_U(S^q(G/1)) = \frac{(G:U)}{(N_G(U):U)} = (G:N_G(U));$$

in particular we have $\mu_{C_d}(S^d(C/1)) = 1$ if d divides n, so the C-sets $S^d(C/1)$ $(d \in \mathrm{Div}(n))$ also form a $\mathbf{Z}$-basis of $\Omega(C)$. Hence the same arguments as above yield Theorem 1.

It is well known that both exterior powers as well as symmetric powers, provide a λ-ring structure on the Burnside ring (cf. [Si]) and the above discussion implies that $\alpha\colon \Omega(C) \to \Omega(G)$ is a λ-ring homomorphism for both of them.

4. Some Applications

Corollary 1. *For every divisor d of $|G|$ there exists an element $x_d \in \Omega(G)$ satisfying*

$$\varphi_U(x_d) = \begin{cases} d & \text{if } d \text{ divides } (G:U), \\ 0 & \text{otherwise;} \end{cases}$$

in particular, $\mu_U(x_d) = 0$ unless d divides $(G:U)$ and

$$\mu_U(x_d) = (G:N_G(U)) = \#\{gUg^{-1} \mid g \in G\}$$

if $(G:U) = d$.

Proof. Put $x_d := \alpha(C/C_{|G|/d})$. Then obviously

$$\varphi_U(x_d) = \varphi_{C_{|U|}}(C/C_{|G|/d}) = (C:C_{|G|/d}) = d$$

if $C_{|U|}$ is contained in $C_{|G|/d}$, that is, if the index d of $C_{|G|/d}$ in C divides the index $(C:C_{|U|}) = (G:U)$ of $C_{|U|}$ in C, and $\varphi_U(x_d) = 0$ otherwise and therefore also $\mu_U(x_d) = 0$ unless d divides $(G:U)$. Finally, if $(G:U) = d$, then U is a maximal subgroup of G with $\mu_U(x_d) \neq 0$ and therefore

$$\mu_U(x_d) = \frac{\varphi_U(x_d)}{(N_G(U):U)} = \frac{d}{(N_G(U):U)} = \frac{(G:U)}{(N_G(U):U)} = (G:N_G(U))$$

equals the number of subgroups in G which are conjugate to U in G. ∎

To derive the next three corollaries we follow essentially the ideas of B. Wagner, published in [Wa]:

COROLLARY 2 (Sylow). *Every divisor d of $|G|$ is the greatest common divisor of all indices $(G:U)$ of subgroups U in G which are divisible by d; that is, we have*

$$d = \text{g.c.d.}((G:U) \mid d \text{ divides } (G:U)).$$

In particular (or, as well, equivalently), if $|G| = d \cdot p^\alpha$ for some prime p, then there exist subgroups U of G of index d and hence of order p^α.

Proof. Write $x_d \in \Omega(G)$ in the form

$$x_d = \sum_{U \leqslant G}' \mu_U(x_d) \cdot G/U = \sum_{U \leqslant G, d \mid (G:U)}' \mu_U(x_d) \cdot G/U$$

and apply φ_1 to derive

$$d = \sum_{U \leqslant G, d \mid (G:U)}' \mu_U(x_d) \cdot (G:U) \in \sum_{U \leqslant G, d \mid (G:U)}' \mathbf{Z} \cdot (G:U). \quad \blacksquare$$

In case $|G|/d$ is a power of a prime p we can exploit this argument even further to derive:

COROLLARY 3 (Sylow [Sy], Frobenius [Fr1]). *If a power p^α of a prime p divides the order $|G|$ of a finite group G, then the number of subgroups V of order p^α must be congruent to 1 modulo p.*

Proof. Put $d := |G|/p^\alpha$ and divide the above equation

$$d = \sum_{U \leqslant G, d \mid (G:U)}' \mu_U(x_d) \cdot (G:U) = \sum_{U \leqslant G, |U| \in \mathrm{Div}(p^\alpha)}' \mu_U(x_d) \cdot (G:U)$$

by d to derive

$$\begin{aligned} 1 &= \sum_{U \leqslant G, d \mid (G:U)}' \mu_U(x_d) \cdot \frac{(G:U)}{d} \\ &= \sum_{U \leqslant G, |U| \in \mathrm{Div}(p^\alpha)}' \mu_U(x_d) \cdot \frac{p^\alpha}{|U|} \\ &\equiv \sum_{U \leqslant G, |U| = p^\alpha}' \mu_U(x_d) \\ &= \sum_{U \leqslant G, |U| = p^\alpha}' (G:N_G(U)) \\ &= \sum_{U \leqslant G, |U| = p^\alpha}' \#\{gUg^{-1} \mid g \in G\} \\ &= \#\{V \leqslant G \mid |V| = p^\alpha\} \qquad (\text{mod } p). \quad \blacksquare \end{aligned}$$

Remark. Note that more generally the condition $\mu_U(x) = (G:N_G(U))$ for $|U| = q$ and $\mu_U(x) = 0$ for $|U| \notin \mathrm{Div}(q)$, which holds for $x = \binom{G/1}{q}$ as well as for $x = S^q(G/1)$ and for $x = x_{|G|/q}$, implies

$$x \equiv \sum_{U \leqslant G, |U| = q} G/U \qquad \text{modulo } I_q,$$

where I_q denotes the ideal in $\Omega(G)$, generated by all G-sets of the form G/V with $|V| \in \mathrm{Div}(q) - \{q\}$.

To derive the next corollary let us recall that for every $x \in \Omega(G)$ one has the *Cauchy–Frobenius–Burnside* congruence relation

$$\sum_{g \in G} \varphi_{\langle g \rangle}(x) \equiv 0 \qquad (\mathrm{mod}\ |G|).$$

Indeed, by additivity it is enough to verify this just for $x = G/U$ $(U \leqslant G)$ in which case a standard computation yields

$$\begin{aligned}
\sum_{g \in G} \varphi_{\langle g \rangle}(G/U) &= \sum_{g \in G} \#\{hU \in G/U \mid ghU = hU\} \\
&= \sum_{g \in G, hU \in G/U} \delta_{hU}^{ghU} \\
&= \sum_{hU \in G/U} \#\{g \in G \mid ghU = hU\} \\
&= \sum_{hU \in G/U} |hUh^{-1}| \\
&= (G:U) \cdot |U| = |G| \equiv 0 \qquad (\mathrm{mod}\ |G|).
\end{aligned}$$

Hence together with this Cauchy–Frobenius–Burnside relation Corollary 1 yields

COROLLARY 4 (Frobenius [Fr2, Fr3]). *Every divisor m of the order $|G|$ of a finite group G also divides the number*

$$\#\{g \in G \mid g^m = 1\}$$

of elements g in G, whose order divides m.

Proof. Apply the Cauchy–Frobenius–Burnside congruence relation to x_d for $d := |G|/m$ to derive that $|G| = d \cdot m$ divides

$$\begin{aligned}\sum_{g\in G}\varphi_{\langle g\rangle}(x_d) &= \sum_{g\in G,\, d\mid (G:\langle g\rangle)} d\\ &= \sum_{g\in G,\, |g|\in \mathrm{Div}(m)} d\\ &= d\cdot \#\{g\in G \mid g^m=1\}\end{aligned}$$

and hence, dividing by d, that m divides $\#\{g\in G \mid g^m=1\}$. ▮

Next recall (cf. [Gl, Yo1, Ro]) that for each $x\in\tilde{\Omega}(G)$ and each $U\leqslant G$ we have

$$\mu_U(x)=\frac{1}{(N_G(U):U)}\sum_{V\leqslant G}\chi(U,V)\cdot\varphi_V(x),$$

where for $U\leqslant V\leqslant G$ we denote by $\chi(U,V)$ the *Euler characteristic* of the simplicial complex of all chains of subgroups between U and V modulo the subcomplex of all those chains which do not start with U or end with V, while otherwise, that is, in case $U\nleqslant V$, we put $\chi(U,V)=0$. So for $U\leqslant V\leqslant G$ and with $[U,V]:=\{W\leqslant G \mid U\leqslant W\leqslant V\}$ we have

$$\chi(U,V):=\sum_{\substack{U,V\in T\subseteq[U,V]\\ T\text{ a chain}}}(-1)^{1+\#T}.$$

Indeed, again by additivity, it is enough to check the above equation for $x=G/W$ for every $W\leqslant G$: in case $W=U$ both sides easily give 1 and in case $W\not\sim U$ the left-hand side equals zero by definition while the right-hand side, multiplied with $(N_G(U):U)$, also gives

$$\begin{aligned}&\sum_{V\leqslant G}\chi(U,V)\cdot\varphi_V(G/W)\\ &\quad=\sum_{V\leqslant G}\chi(U,V)\cdot(N_G(W):W)\cdot\#\{W'\leqslant G \mid V\leqslant W'\overset{G}{\sim}W\}\\ &\quad=(N_G(W):W)\cdot\sum_{W'\overset{G}{\sim}W}\;\sum_{V\leqslant W'}\chi(U,V)\\ &\quad=(N_G(W):W)\cdot\sum_{W'\overset{G}{\sim}W}\;\sum_{V\leqslant W'}\;\sum_{\substack{U,V\in T\subseteq[U,V]\\ T\text{ a chain}}}(-1)^{1+\#T}=0,\end{aligned}$$

since for each $W'\overset{G}{\sim}W$ one has

$$\sum_{V\leqslant W'}\;\sum_{\substack{U,V\in T\subseteq[U,V]\\ T\text{ a chain}}}(-1)^{\#T}=\sum_{\substack{U\in T\subseteq[U,W']\\ T\text{ a chain}}}(-1)^{\#T}=0$$

in view of the fact that there exists a one-to-one correspondence between those linear subsets T of $[U, W']$ with $U \in T$ not containing W' and those containing W', given by $T \leftrightarrow T \cup \{W'\}$ (here we use, of course, $U \not< W$ and therefore $U \neq W'$). Hence we have

COROLLARY 5 (Quillen [Qu], Brown [Br], Yoshida [Yo2]). *For each divisor d of $|G|$ and for every $U \leqslant G$ with $d \mid (G:U)$ one has*

$$\chi(\{V \leqslant G \mid U < V, d \mid (G:V)\}) \equiv 1 \qquad (\text{mod } d(U)),$$

where for a subset $\mathbf{S}$ *of* $\mathrm{Sub}(G)$ *we write* $\chi(\mathbf{S})$ *for the Euler characteristic of the simplicial set of all linearly ordered subsets or chains in* $\mathbf{S}$ *and where* $d(U)$ *is defined by*

$$d(U) := (N_G(U):U)/\text{g.c.d.}((N_G(U):U), d);$$

in particular for $U = 1$ *and, hence,* $d(1) = |G|/d =: m$ *we have*

$$\chi(\{V \leqslant G \mid 1 \neq |V| \in \mathrm{Div}(m)\}) \equiv 1 \qquad (\text{mod } m).$$

Proof. For $x = x_d$ we must have $\mu_U(x_d) \in \mathbf{Z}$ and therefore

$$\sum_{V \leqslant G} \varphi_V(x) \cdot \chi(U, V) \equiv 0 \qquad \text{mod}(N_G(U):U)),$$

that is,

$$\sum_{V \in \mathscr{V}_d} \chi(U, V) \equiv 0 \qquad (\text{mod } d(U)),$$

where

$$\mathscr{V}_d := \{V \leqslant G \mid d \text{ divides } (G:V)\}.$$

So it remains to observe that in case $d \mid (G:U)$ one has

$$\sum_{V \in \mathscr{V}_d} \chi(U, V) = \chi(U, U) + \sum_{U < V \in \mathscr{V}_d} \chi(U, V)$$

and that

$$\sum_{V \in \mathscr{V}_d - \{U\}} \chi(U, V) = \sum_{T \text{ a chain of } \mathscr{V}_d - \{U\}} (-1)^{\# T}$$
$$= -\chi(\{V \in \mathscr{V}_d \mid U < V\}). \quad \blacksquare$$

Remark. One can of course elaborate on all these results, e.g., by picking subsets $\mathbf{S} \subseteq \mathrm{Sub}(G)$ which are closed with respect to conjugation and for which one knows an integer $k = k_{\mathbf{S}}$ such that the element $y = y_{k,\mathbf{S}} \in \tilde{\Omega}(G)$, defined by

$$\varphi_U(y) = \begin{cases} k & \text{for} \quad U \in \mathbf{S} \\ 0 & \text{otherwise,} \end{cases}$$

is actually in $\Omega(G)$ and applying the above considerations to the product $y \cdot x_d$. Many such subsets $\mathbf{S}$ and integers k are known from the theory of *idempotents* in $\Omega(G)$ and, more generally, in $R \otimes \Omega(G)$ for R any subring of the field $\mathbf{Q}$ of rational numbers (cf. [Dr1, 2]), but we will not detail all the corresponding consequences here. Let us just mention without proof one particular consequence which is a variation (and also a consequence) of the Frobenius Theorem:

COROLLARY 4′. *For π a set of primes and $n := \prod_p p^{\alpha_p} \in \mathbf{N}$ put $n_\pi := \prod_{p \in \pi} p^{\alpha_p}$. Then for every $m \in \operatorname{Div}(|G|)$ and every cyclic subgroup U of G with $|U|_\pi = 1$ one has*

$$\#\{g \in G \mid g^m = 1, \langle g^{m_\pi} \rangle \sim^G U\} \equiv 0 \qquad (\operatorname{mod} m_\pi).$$

5. FUNCTORIAL PROPERTIES OF α

For the sake of completeness let us just list the functorial properties of α. If $V \trianglelefteq U \leqslant G$, then for every G-set X the set X^V can be considered as a U/V-set via

$$U/V \times X^V \to X^V\colon (uV, x) \mapsto ux$$

(which is well defined since $uvx = ux$ for $v \in V$ and $x \in X^V$ and since $v(ux) = u(u^{-1}vu)x = ux$ for $u \in U$, $v \in V$, and $x \in X^V$), giving rise to a ring homomorphism

$$\beta^G_{V,U}\colon \Omega(G) \to \Omega(U/V)\colon x \mapsto x^U.$$

One checks easily that for all $V \trianglelefteq U \leqslant G$ the diagram

$$\begin{array}{ccc} \Omega(C) & \xrightarrow{\alpha^G} & \Omega(G) \\ {\scriptstyle \beta^C_{C_{|V|}, C_{|U|}}} \big\downarrow & & \big\downarrow {\scriptstyle \beta^G_{V,U}} \\ \Omega(C_{(U:V)}) & \xrightarrow{\alpha^{U/V}} & \Omega(U/V) \end{array}$$

commutes, in particular α commutes with *restriction* (choose $V = 1$).

The situation is not quite as easy with respect to *induction*: if for $U \leqslant G$ we denote by ind_U^G the additive map from $\Omega(U)$ into $\Omega(G)$ which maps each basis element U/V in $\Omega(U)$ onto the basis element G/V, then the following, slightly twisted diagram commutes for each $U \leqslant G$:

$$\begin{array}{ccc} \Omega(C_{|U|}) & \xrightarrow{\alpha^U} & \Omega(U) \\ {\scriptstyle \operatorname{ind}_{C_{|U|}}^{C}} \downarrow & & \downarrow {\scriptstyle \alpha^G(C/C_{|U|}) \cdot \operatorname{ind}_U^G} \\ \Omega(C) & \xrightarrow{G/U \cdot \alpha^G} & \Omega(G) \end{array}$$

This can be checked in a straightforward fashion, e.g., by computing

$$\varphi_V(\alpha^G(C/C_{|U|}) \cdot \operatorname{ind}_U^G(\alpha^U(x)))$$

and

$$\varphi_V(G/U \cdot \alpha^G(\operatorname{ind}_{C_{|U|}}^C(x)))$$

for all $x \in \Omega(C_{|U|})$ and all $V \leqslant G$.

Finally assume $N \trianglelefteq G$ and consider the *inflation* map $\Omega(G/N) \to \Omega(G)$ which is defined by considering every G/N-set X as a G-set via the canonical epimorphism $G \twoheadrightarrow G/N$. Then one can show that the diagram

$$\begin{array}{ccc} \Omega(C_{(G:N)}) & \xrightarrow{\alpha^{G/N}} & \Omega(G/N) \\ {\scriptstyle \inf} \downarrow & & \downarrow {\scriptstyle \inf} \\ \Omega(C) & \xrightarrow{\alpha^G} & \Omega(G) \end{array}$$

commutes if and only if for every $U \leqslant G$ we have $|U \cap N| = \text{g.c.d.}(|U|, |N|)$, that is, if and only if for every prime $p \mid |G|$ either $|N|_p = |G|_p$ or $|N|_p = 1$ or the p-Sylow subgroups of G are cyclic or $p = 2$, $|N|_2 = 2$ and the 2-Sylow subgroups of G are (generalized) quaternion groups (the last "if and only if" statement is a simple exercise in elementary finite group theory and should be folklore).

6. Some Observations Concerning the Kernel and the Image of α^G

It is obvious that α^G is injective if and only if for every $m \in \operatorname{Div}(|G|)$ there exists a subgroup of order m in G. It is also obvious that the image of α^G is always contained in

$$\Omega_0(G) := \{x \in \Omega(G) \mid \varphi_U(x) = \varphi_V(x) \text{ for all } U, V \leqslant G \text{ with } |U| = |V|\}.$$

So one may ask for those groups G for which α^G defines an isomorphism between $\Omega(C)$ and $\Omega_0(G)$. This is answered by

THEOREM 2. *α^G defines an isomorphism between $\Omega(C)$ and $\Omega_0(G)$ if and only if G is nilpotent.*

Proof. Invoking a simple and very standard inductive argument it is easy to see that α^G defines an isomorphism between $\Omega(C)$ and $\Omega_0(G)$ if and only if α^G is injective—that is, for every $m \in \mathrm{Div}(|G|)$ there exists a subgroup $U \leqslant G$ with $|U| = m$—and for every $x \in \Omega_0(G)$ and every maximal subgroup U of G with $\varphi_U(x) \neq 0$ one has $\varphi_U(x) \equiv 0 \pmod{(G:U)}$.

Now if G is nilpotent, then for every $m \in \mathrm{Div}(|G|)$ there exists even a normal subgroup N of that order. Moreover, if for some $x \in \Omega_0(G)$ we have a maximal subgroup U of G with $\varphi_U(x) \neq 0$ and if $N \trianglelefteq G$ is a normal subgroup of the same order, then N is also such a maximal subgroup of G and so we have indeed

$$\begin{aligned}\varphi_U(x) = \varphi_N(x) &= (N_G(N):N) \cdot \mu_N(x) \\ &= (G:U) \cdot \mu_N(x) \\ &\equiv 0 \qquad (\mathrm{mod}(G:U)).\end{aligned}$$

Vice versa, if α^G defines an isomorphism between $\Omega(C)$ and $\Omega_0(G)$ and if P denotes a Sylow p-subgroup of G, then one knows (cf. [KT] or [DV]) that the element $x_P \in \tilde{\Omega}(G)$, defined by

$$\varphi_U(x_P) := \begin{cases} p \cdot (N_G(P):P) & \text{if } U \sim^G P \\ 0 & \text{otherwise,} \end{cases}$$

is actually contained in $\Omega(G)$ and so, since every group of order $|P|$ is conjugate to P, it is contained even in $\Omega_0(G)$. Hence, since by definition $P \leqslant G$ is a maximal subgroup of G with $\varphi_P(x_P) \neq 0$, we have necessarily

$$\varphi_P(x_P) = p \cdot (N_G(P):P) \equiv 0 \qquad (\mathrm{mod}(G:P))$$

and therefore $(G:P) \mid (N_G(P):P)$, that is $N_G(P) = G$. So every Sylow p-subgroup of G is normal in G, that is, G is nilpotent. ∎

Remark. Elaborating on this argument one can show that for a subset π of primes and with

$$\mathbf{Z}_\pi := \left\{ \frac{a}{b} \in \mathbf{Q} \;\middle|\; b_\pi = 1 \right\}$$

the induced map

$$\alpha_\pi^G : \mathbf{Z}_\pi \otimes \Omega(C) \to \mathbf{Z}_\pi \otimes \Omega_0(G)$$

is an isomorphism if and only if for every $m \in \mathrm{Div}(|G|)$ and every $p \in \pi$ there exists a subgroup $U \leqslant G$ of order m with $(G : N_G(U))_p = 1$. So in particular, G must have a normal solvable Hall π'-subgroup and a nilpotent Hall π-subgroup, but in general this condition is not enough to ensure that α_π^G is an isomorphism.

7. An Extension to Profinite Groups

Using the (completed) Burnside rings $\hat{\Omega}(G)$ which have been defined and studied for every *profinite group* G in [DS1, 2], one can phrase Theorem 1 in a still more elegant way. Recall that for every profinite group G the ring $\hat{\Omega}(G)$ is defined to be the Grothendieck ring of the (virtual) *almost finite* G-sets, that is, those G-sets X for which X^U is finite for every open subgroup U of G and G_x is an open subgroup of G for every $x \in X$, and that for an arbitrary group G we write $\hat{\Omega}(G)$ for $\hat{\Omega}(\hat{G})$, $\hat{G}$ denoting the *profinite completion* of G relative to all subgroups U of G of finite index. Then, with C now denoting the infinite cyclic group, we can state

THEOREM 1′. *For every profinite group G there exists a canonical ring homomorphism*

$$\hat{\alpha} = \hat{\alpha}^G = \hat{\alpha}^G_{FW} : \hat{\Omega}(C) \to \hat{\Omega}(G),$$

satisfying $\varphi_U(\hat{\alpha}(x)) = \varphi_{C^{(G:U)}}(x)$ for every $x \in \hat{\Omega}(C)$ and every open subgroup U of G, where now

$$C^{(G:U)} := \{ g^{(G:U)} \mid g \in C \}$$

denotes the unique subgroup of index $(G:U)$ in C.

Proof. One can prove Theorem 1′ by using the fact that

$$\hat{\Omega}(G) = \varprojlim_{N \trianglelefteq G,\, N \text{ open}} \Omega(G/N)$$

(where for two open normal subgroups $N_1, N_2 \trianglelefteq G$ with $N_1 \leqslant N_2$ the map $\Omega(G/N_1) \to \Omega(G/N_2)$ being used for the construction of the above projective limit is, of course, the map $\beta^{G/N_1}_{N_2/N_1, G/N_1} : X \mapsto X^{N_2}$) and applying Theorem 1 to all factors $\Omega(G/N)$, using the above established functorial properties of α. One can also adapt the proof of Theorem 1 to the profinite situation directly: choose the *Haar measure dg* on G with $\int_G 1 \, dg = 1$ and for every measurable subset Y of G define the index

$$(G:Y) := \left(\int_Y 1 \, dg \right)^{-1}.$$

Note that for every open subgroup U of G there exist precisely $\binom{(G:U)}{d}$ U-invariant subsets Y of G of index $(G:U)/d$ for every $d \in \mathbf{N}$ while there exists none such U-invariant subset of index $(G:U)/d$ if d is not an integer. Hence for every rational number $q \geqslant 1$ we have an almost finite G-set

$$\bigwedge^{q}(G) := \{Y \subseteq G \mid (G:Y) = q,\ G_Y \text{ is open}\},$$

$$G_Y := \{g \in G \mid gY = Y\}$$

which satisfies

$$\hat{\alpha}^G\left(\bigwedge^{q}(\hat{C})\right) = \bigwedge^{q}(G)$$

in view of

$$\varphi_U\left(\bigwedge^{q}(G)\right) = \begin{cases} \binom{(G:U)}{d} & \text{if } d := (G:U)/q \in \mathbf{N} \\ 0 & \text{otherwise.} \end{cases}$$

So Theorem 1′ follows as in the finite case from the additional observation that the $\hat{C}$-sets $\bigwedge^d(\hat{C})$ $(d \in \mathbf{N})$ form a (topological) $\mathbf{Z}$-basis of $\hat{\Omega}(\hat{C})$. ∎

Remark 1. Instead of the G-sets $\bigwedge^q(G)$ we could also have used (again as in the finite case) the almost finite G-sets

$$S^q(G) \qquad (q \in \mathbf{Q},\ q > 0)$$

consisting of all $f\colon G \to \mathbf{N}_0$ such that f is constant on the U-cosets for some open subgroup U and $\int_G f\,dg = q^{-1}$, noting that $\hat{\alpha}^G(S^q(\hat{C})) = S^q(G)$ and that the $S^q(\hat{C})$ $(q \in \mathbf{N})$ also form a topological basis of $\hat{\Omega}(C)$.

Remark 2. For a profinite group G define

$$\hat{C}^{|G|} := \bigcap_{U \leqslant G,\ U \text{ open}} \hat{C}^{(G:U)} \qquad \text{and} \qquad \hat{C}_{|G|} := \hat{C}/\hat{C}^{|G|}.$$

Then

$$\hat{\alpha}\colon \hat{\Omega}(\hat{C}) \to \hat{\Omega}(G)$$

factors through

$$\hat{\beta}^{\hat{C}}_{\hat{C}^{|G|},\hat{C}}\colon \hat{\Omega}(C) = \hat{\Omega}(\hat{C}) \to \hat{\Omega}(\hat{C}_{|G|})\colon x \mapsto x^{\hat{C}^{|G|}}.$$

As in the finite case, it induces an isomorphism

$$\hat{\Omega}(\hat{C}_{|G|}) \to \hat{\Omega}_0(G)$$

onto the subring $\hat{\Omega}_0(G)$ of $\hat{\Omega}(G)$ consisting of all $x \in \hat{\Omega}(G)$ satisfying $\varphi_U(x) = \varphi_V(x)$ for all open subgroups $U, V \leqslant G$ with $(G:U) = (G:V)$, if and only if G is *pro-nilpotent*. Note that $\hat{C}_{|G|}$ can be considered to represent the *order* of G, as defined in the theory of profinite groups (cf. [Se]).

Remark 3. We leave it to the reader to establish the functorial properties of $\hat{\alpha}^G$ which do not differ from those established in Section 5.

Remark 4. Note that $\hat{\Omega}(\hat{C})$ coincides with the *necklace algebra* $N(\mathbf{Z})$ as defined by Metropolis and Rota and therefore it coincides with the ring of *universal Witt vectors* $\mathbf{W}(\mathbf{Z})$ (cf. [MR, DS1, DS2]). So, after all, it turns out that for every finite or pro-finite group G and for every *Mackey functor* $\mathbf{M}$ or *Green functor* $\mathbf{G}$, defined on $G^\wedge$, the abelian group $\mathbf{M}(*_G)$ or ring $\mathbf{M}(*_G)$ is a $\mathbf{W}(\mathbf{Z})$-module or a $\mathbf{W}(\mathbf{Z})$-algebra, respectively, in a completely canonical way.

References

[Br] K. Brown, Euler characteristics of groups: The p-fractional part, *Invent. Math.* **29** (1975), 1–5.

[BT] K. Brown and J. Thévenaz, A generalization of Sylow's third theorem, *J. Algebra* **115** (1988), 414–430.

[Di] T. Dieck, "Transformation Groups and Representation Theory," Lecture Notes in Math., Vol. 766, Springer-Verlag, Berlin, 1979.

[Dr1] A. W. M. Dress, A characterization of solvable groups, *Math. Z.* **110** (1969), 213–219.

[Dr2] A. W. M. Dress, Notes on the theory of finite groups I: The Burnside ring of a finite group and some AGN applications, multicopied lecture notes, Bielefeld University, 1971.

[Dr3] A. W. M. Dress, Contributions to the theory of induced representations, *in* "Algebraic K-Theory II," Proc. Battle Inst. Conf. 1972, Lecture Notes in Math., Vol. 342, pp. 183–240, Springer-Verlag, Berlin/New York, 1973.

[Dr4] A. W. M. Dress, On relative Grothendieck rings, *in* "Representations of Algebras," Proc. International Conf. Ottawa, 1974, Lecture Notes in Math., Vol. 488, pp. 79–131, Springer-Verlag, Berlin/New York, 1975.

[DS1] A. W. M. Dress and C. Siebeneicher, The Burnside ring of profinite groups and the Witt vector construction, *Adv. Math.* **70** (1988), 87–132.

[DS2] A. W. M. Dress and C. Siebeneicher, The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings, and the universal ring of Witt vectors, *Adv. Math.* **78** (1989), 1–41.

[DV] A. W. M. Dress and E. Vallejo, A simple proof for a result by Kratzer and Thévenaz concerning the embedding of the Burnside ring into its ghost ring, Instituto de Matemáticas, Universidad Nacional Autónoma de Mexico, preprint 1990.

[Fr1] G. FROBENIUS, Verallgemeinerung des Sylowschen Satzes, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1895), 981–993, *in* "Gesammelte Abhandlungen," Bd. II, pp. 664–676, Springer-Verlag, Berlin/New York, 1968.

[Fr2] G. FROBENIUS, Über einen Fundamentalsatz der Gruppentheorie, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1903), 987–991, *in* "Gesammelte Abhandlungen," Bd. III, pp. 330–334, Springer-Verlag, Berlin/New York, 1968.

[Fr3] G. FROBENIUS, Über einen Fundamentalsatz der Gruppentheorie II, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1907), 428–437, *in* "Gesammelte Abhandlungen," Bd. III, pp. 428–437, Springer-Verlag, Berlin/New York, 1968.

[Gl] D. GLUCK, Idempotent formulae for the Burnside algebra with applications to the p-subgroup simplicial complexes, *Illinois J. Math.* **25** (1981), 63–67.

[Go] D. GORENSTEIN, "Finite Groups," Harper & Row, New York, 1968.

[Gr] J. GREEN, Axiomatic representation theory of finite groups, *J. Pure Appl. Algebra* **1** (1971), 41–77.

[Hu] B. HUPPERT, "Endliche Gruppen," Vol. I, Springer-Verlag, Berlin/Heidelberg/New York, 1967.

[KT] C. KRATZER AND J. THÉVENAZ, Fonction de Möbius d'un groupe fini et anneau de Burnside, *Comment. Math. Helv.* **59** (1984), 425–438.

[MR] N. METROPOLIS AND G.-C. ROTA, Witt vectors and the algebra of necklaces, *Adv. Math.* **50** (1983), 95–125.

[Qu] D. QUILEN, Homotopy properties of the poset of non-trivial p-subgroups of a group, *Adv. Math.* **28** (1978), 101 128.

[Ro] G.-C. ROTA, On the foundations of combinatorial theory. I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie verw. Gebiete* **2** (1964), 340–368.

[Se] J.-P. SERRE, "Cohomologie Galoisienne," Lecture Notes in Math., 4th ed., Vol. 5, Springer-Verlag, New York/Berlin, 1973.

[Si] C. SIEBENEICHER, λ-Ringstrukturen auf dem Burnside Ring der Permutationsdarstellungen einer endlichen Gruppe, *Math. Z.* **146** (1976), 223–238.

[So] L. SOLOMON, On Schur's index and the solutions of $G^n = 1$ in a finite group, *Math. Z.* **70** (1962), 122–125.

[St] R. P. STANLEY, "Enumerative Combinatorics," Vol. I, Wadsworth, Monterey, 1986.

[Sy] L. SYLOW, Théorèmes sur les groupes de substitutions, *Math. Ann.* **5** (1872), 584–594.

[Wa] B. WAGNER, A permutation representation theoretical version of a theorem of Frobenius, *Bayreuth. Math. Schr.* **6** (1980), 23–32.

[Wi] H. WIELANDT, Ein Beweis für die Existenz der Sylowgruppen, *Arch. Math.* **10** (1959), 401–402.

[Yo1] T. YOSHIDA, Idempotents of Burnside rings and Dress induction theorem, *J. Algebra* **80** (1983), 90–105.

[Yo2] T. YOSHIDA, On the unit groups of Burnside rings, *J. Math. Soc. Japan* **42** (1990), 31–64.