JOURNAL OF COMBINATORIAL THEORY, Series A **74**, 287–300 (1996)
ARTICLE NO. 0051

The Modular Homology of Inclusion Maps and Group Actions

VALERY MNUKHIN

Department of Mathematics, State University of Radio Engineering, Taganrog, 347 928 Russia

AND

JOHANNES SIEMONS*

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom

Communictated by the Managing Editors

Received April 18, 1994

Let Ω be a finite set of n elements, R a ring of characteristic $p>0$ and denote by M_k the R-module with k-element subsets of Ω as basis. The set inclusion map $\partial\colon M_k \to M_{k-1}$ is the homomorphism which associates to a k-element subset Δ the sum $\partial(\Delta)=\Gamma_1+\Gamma_2+\cdots+\Gamma_k$ of all its $(k-1)$-element subsets Γ_i. In this paper we study the chain

$$0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_k \leftarrow M_{k+1} \leftarrow M_{k+2} \cdots \qquad (*)$$

arising from ∂. We introduce the notion of p-exactness for a sequence and show that any interval of $(*)$ not including $M_{n/2}$ or $M_{n+1/2}$ respectively, is p-exact for any prime $p>0$. This result can be extended to various submodules and quotient modules, and we give general constructions for permutation groups on Ω of order not divisible by p. If an interval of $(*)$, or an equivalent sequence arising from a permutation group on Ω, does include the middle term then proper homologies can occur. In these cases we have determined all corresponding Betti numbers. A further application are p-rank formulae for orbit inclusion matrices. © 1996 Academic Press, Inc.

1. INTRODUCTION

Let Ω be a finite set and 2^{Ω} the collection of subsets of Ω. The *inclusion map* on 2^{Ω} is the linear map ∂ given by $\partial(\Delta)=\Gamma_1+\Gamma_2+\cdots+\Gamma_k$ when Δ is a k-element subset of Ω and when the Γ_i are the $(k-1)$-element subsets

[*] E-mail: J.Siemons@UEA.AC.UK.

0097-3165/96 $18.00

of Δ. To make sense of this definition we regard the collection of Ω-subsets as basis of a module over some ring. So if R is that ring we denote the module with 2^{Ω} as basis by $R2^{\Omega}$. In particular, we put $M_k := \{\sum r_{\Delta}\,\Delta \mid \Delta \subseteq \Omega,\ |\Delta| = k,\ r_{\Delta} \in R\}$. In this paper we study the sequence

$$0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_k \leftarrow M_{k+1} \leftarrow M_{k+2} \cdots \tag{I}$$

arising from ∂. It is of course fundamental in many investigations in combinatorics and the subject of numerous papers.

Our interest concerns the homological properties of the sequence (I) when the ring has prime characteristic $p \neq 0$. The first main result, Theorem 3.6, shows that all subsequences in (I) of the kind

$$\cdots \leftarrow M_{k-2p} \leftarrow M_{k-p-i} \leftarrow M_{k-p} \leftarrow M_{k-i} \leftarrow M_k \tag{II}$$

are exact for every $0 < i < p$ in the "lower part" of (I), that is when $2k \leqslant |\Omega|$. Any sequence (I) for which all subsequences (II) are exact will be called p-exact. This concept is interesting for several reasons. For one, it gives an immediate formula for the p-rank of $\partial^i\colon M_k \to M_{k-i}$ as an alternating sum of dimensions of the modules to the left of M_k. This in turn can be viewed as an inclusion-exclusion principle and we suggest that p-exactness is the natural interpretation for the p-rank formulae given in several papers, see [1, 2, 4, 16, 17].

The "upper part" of the sequence fails to be p-exact. Nevertheless, we can show that exactness holds everywhere except for some term near the middle of the sequence. The precise result is contained in theorem 5.3 which computes all Betti numbers.

These results are extended naturally to permutation groups on Ω: If G acts on Ω it also acts on 2^{Ω} and hence on each of the M_k. In Section 4 we consider the submodules of elements fixed by G and study their homological properties. The results in Sections 4 and 5 show that all the results mentioned above hold for groups of order co-prime to p. In particular, the Betti numbers of the fixed-modules give new invariants. In Section 6 we give explicit values for the Betti numbers for cyclic groups in the case of characteristic $p = 3$. Another interesting application is obtained by considering the case $p = 2$. Here let Ω have size $2m$ and suppose that the group G has odd order with n_k orbits on k-subsets. We show that $n_m = 2(n_{m-1} - n_{m-2} + n_{m-3} - n_{m-4} + \cdots)$.

We have also studied group actions on infinite sets and in particular the question of p-exactness in subsequences of the corresponding sequence (I). The techniques are somewhat different and so these results are contained in another paper [9].

2. Inclusion Maps

First we introduce the notation. Throughout this section let R be an associative ring with 1 and let Ω be a finite set of size n. Then 2^{Ω} denotes the collection of all subsets of Ω and $R2^{\Omega}$ denotes the R-module with 2^{Ω} as basis.

For a natural number k the collection of all k-element subsets of Ω is denoted by $\Omega^{\{k\}}$ and $R\Omega^{\{k\}} \subset R2^{\Omega}$ denotes the submodule with k-element subsets as basis. We will always abbreviate $R\Omega^{\{k\}}$ by M_k as the context will be clear. We refer to R also as the *coefficient ring* of M_k.

For $f = \sum r_\Delta \Delta \in R2^{\Omega}$ the *support* $\operatorname{supp}(f)$ is the union of all Δ for which $r_\Delta \neq 0$ and the *support size* is $\|f\| := |\operatorname{supp}(f)|$. Two elements f and g are *disjoint* if $\operatorname{supp}(f)$ and $\operatorname{supp}(g)$ are disjoint sets.

The Boolean operations on 2^{Ω} are easily extended to products on $R2^{\Omega}$. The most important is the $\bigcup$-product: if $f = \sum f_\Delta \Delta$ and $g = \sum g_\Gamma \Gamma$ we define $f \cup g := \sum \Gamma_\Delta g_\Gamma (\Delta \cup \Gamma)$. It is not difficult to see that this definition turns $R2^{\Omega}$ into an associative ring with the empty set as identity. In different guises this algebra has also been considered in [6, 11, 13].

The *inclusion map* $\partial \colon R2^{\Omega} \to R2^{\Omega}$ is defined by $\partial(\Delta) := \sum_{\alpha \in \Delta} (\Delta \backslash \alpha)$ and extended to a homomorphism on $R2^{\Omega}$ by $\partial(\sum f_\Delta \Delta) := \sum f_\Delta \partial(\Delta)$. Clearly, this map restricts to homomorphisms $\partial \colon M_k \to M_{k-1}$. Very important is the *product rule*:

If f and g are disjoint elements in $R2^{\Omega}$ then

$$\partial(f \cup g) = \partial(f) \cup g + f \cup \partial(g).$$

This can be verified easily. It shows that the inclusion map behaves very much like differentiation and we often use the natural notation $f' := \partial(f)$ and $f^{(s)} := [f^{(s-1)}]'$.

For the remainder Ω denotes a finite set of cardinality n unless explicitly stated otherwise.

Theorem 2.1. *For any associative coefficient ring with* 1 *the kernel of* $\partial \colon M_k \to M_{k-1}$ *is generated by elements of support size at most* $2k$.

Proof. It is easy to see that the result holds when $n := |\Omega| = 2$. So suppose that the theorem is true for all sets of size less than n. Clearly, when $2k \geqslant n$ there is nothing to prove. So suppose that $2k < n$ and let f be some element in the kernel of $\partial \colon M_k \to M_{k-1}$. If $\|f\| \leqslant 2k$ we include f in the generator set. So we can assume that $\|f\| > 2k$. For any element α in $\operatorname{supp}(f)$ we write f uniquely as $f = \alpha \cup f_\alpha + g$ in such a way that α does not belong to $\operatorname{supp}(g)$ nor to $\operatorname{supp}(f_\alpha)$. By the product rule, $0 = f' = \alpha \cup (f_\alpha)' + f_\alpha + g'$ and as only the first term involves α we have $(f_\alpha)' = 0 = f_\alpha + g'$. As $\|f_\alpha\| < n$

we may assume that f_α can be written as $f_\alpha = h_1 + \cdots + h_s$ where the h_i satisfy $(h_i)' = 0$ and $\|h_i\| \leqslant 2(k-1)$.

For each h_i we select a point $\beta_i \in \text{supp}(f)$ with $\alpha \neq \beta_i \notin \text{supp}(h_i)$. Note that this is possible since $\|f\| > 2k$, and $\|h_i\| + 2 \leqslant 2k$. Now consider the term $G = (\beta_1 \cup h_1) + \cdots + (\beta_s \cup h_s)$. Computing G' shows that $G' = f_\alpha$. As $0 = f_\alpha + g'$ we see that $(g+G)' = 0$, and as $g + G$ does not involve α, we have $\|g + G\| < \|f\| \leqslant n$. So we can write $g + G = w_1 + \cdots + w_t$ where the w_i are elements in the kernel with $\|w_i\| \leqslant 2k$.

Therefore $f = \alpha \cup f_\alpha + g = \alpha \cup (h_1 + \cdots + h_s) - G + (w_1 + \cdots + w_t) = \alpha \cup (h_1 + \cdots + h_s) - [(\beta_1 \cup h_1) + \cdots + (\beta_s \cup h_s)] + (w_1 + \cdots + w_t) = (\alpha - \beta_1) \cup h_1 + \cdots + (\alpha - \beta_s) \cup h_s + (w_1 + \cdots + w_t)$. As $[(\alpha - \beta_i) \cup h_i]' = (\alpha - \beta_i)' \cup h_i + (\alpha - \beta_i) \cup (h_i)' = 0$ and as each $(\alpha - \beta_i) \cup h_i$ has support size at most $2 + 2(k-1)$, we have expressed f by elements in the kernel with support size at most $2k$. ▌

Remark. When the coefficient ring is a field of characteristic zero the minimum support size of elements in the kernel is $2k$ exactly, and as generators one can choose *signed dual cubes* of dimension k. These are expressions of the form $(\alpha_1 - \beta_1) \cup (\alpha_2 - \beta_2) \cup \cdots \cup (\alpha_k - \beta_k)$. When $k = 3$, for instance, then $(\alpha_1 - \beta_1) \cup (\alpha_2 - \beta_2) \cup (\alpha_3 - \beta_3)$ represents the faces of an ordinary octahedron signed alternately $+1$ and -1, see [3, 14]. Further, in [14] it is shown that these are precisely the minimum weight terms in the kernel. Note also that signed dual cubes appear naturally in the proof above in arbitrary characteristic.

However, when the coeffcient ring has characteristic $\neq 0$, then there may be elements of shorter support. Already for $p = 2$ or 3 ordinary triangles and tetrahedra belong to the kernel of $\partial\colon M_k \to M_{k-1}$ when $k = 2$ or 3.

In a similar way we can determine the support size of generators of the kernels of higher powers of ∂. This is the next result.

THEOREM 2.2. *For any associative coefficient ring with* 1 *the kernel of* $\partial^m\colon M_k \to M_{k-m}$, *where* $1 \leqslant m \leqslant k$, *is generated by elements of the form* $h \cup \Delta$ *where* h *belongs to the kernel of* $\partial\colon M_{k-m-1} \to M_{k-m}$ *and where* Δ *is an* $(m-1)$-*element set disjoint from* h. *In particular, the kernel of* $\partial^m\colon M_k \to M_{k-m}$ *is generated by elements of support size at most* $2k - m + 1$.

Proof. Evidently, $(h \cup \Delta)^{(m)} = 0$ by the product rule. The result holds when $n := |\Omega| = 2$ and so suppose the same is true for all sets of size less than n.

Let f be some element in M_k with $f^{(m)} = 0$. As before, if α is in supp(f), we write $f = \alpha \cup f_\alpha + g$. By the product rule, $f^{(m)} = \alpha \cup (f_\alpha)^{(m)} + mf_\alpha^{(m-1)} + g^{(m)} = 0$ and so $(f_\alpha)^{(m)} = 0 = mf_\alpha^{(m-1)} + g^{(m)}$. As $\|f_\alpha\| < n$ we assume that f_α can be written as $f_\alpha = h_1 \cup \Gamma_1 + \cdots + h_s \cup \Gamma_s$ with $h_i' = 0$ and $(m-1)$-sets Γ_i disjoint from h_i. Then $(f_\alpha)^{(m-1)} = (m-1)!\ [h_1 + \cdots + h_s]$.

Now let $G = h_1 \cup \Gamma_1 \cup \beta_1 + \cdots + h_s \cup \Gamma_s \cup \beta_s$ where $\beta_i \neq \alpha$ are points disjoint from h_i and Γ_i. Note that $G^{(m)} = m!\ (h_1 + \cdots + h_s) = m(f_\alpha)^{(m-1)}$ so that $(g + G)^{(m)} = 0$. As $\operatorname{supp}(g + G) \subseteq \operatorname{supp}(f) \backslash \{\alpha\}$ we employ induction to write $g + G = w_1 \cup \Delta_1 + \cdots + w_t \cup \Delta_t$ with $(w_i)' = 0$ and $(m-1)$-sets Δ_i disjoint from w_i. This gives $f = \alpha \cup f_\alpha + g = \alpha \cup f_\alpha - G + [w_1 \cup \Delta_1 + \cdots + w_t \cup \Delta_t] = (\alpha \cup h_1 \cup \Gamma_1 - \beta_1 \cup h_1 \cup \Gamma_1) + \cdots + (\alpha \cup h_s \cup \Gamma_s - \beta_s \cup h_s \cup \Gamma_s) + [w_1 \cup \Delta_1 + \cdots + w_t \cup \Delta_t] = (\alpha - \beta_1) \cup h_1 \cup \Gamma_1 + \cdots + (\alpha - \beta_s) \cup h_s \cup \Gamma_s + [w_1 \cup \Delta_1 + \cdots + w_t \cup \Delta_t]$. Clearly, $[(\alpha - \beta_s) \cup h_s \cup \Gamma_s]^{(m)} = 0$ and $((\alpha - \beta_s) \cup h_s)' = 0$ so that the main part is proved.

By theorem 2.1 the kernel of $\partial\colon M_k \to M_{k-1}$ is generated by elements of support size at most $2k$ and so the kernel of $\partial^m\colon M_k \to M_{k-m}$ is generated by elements of support size at most $2k - m + 1$. ▮

Corollary 2.3 (The Integration Lemma). *Let $2k < m \leqslant |\Omega|$. If $(m-2k)!$ has an inverse in R and if $f \in M_k$ satisfies $f' = 0$, then there is some F in M_{m-k} with $F^{(m-2k)} = f$.*

Proof. By theorem 2.1 we write f as a combination $f = w_1 + \cdots + w_t$ where $w_i' = 0$ and $\|w_i\| \leqslant 2k$. For each w_i select a set Δ_i of $m - 2k$ points disjoint from $\operatorname{supp}(w_i)$. Now consider $F = ((m-2k)!)^{-1} [\Delta_1 \cup w_1 + \cdots + \Delta_t \cup w_t]$. ▮

Lemma 2.4. *Let R be an associative ring with 1 of prime characteristic $p \neq 0$ and suppose that $0 \leqslant k \leqslant m \leqslant n$ (where $n = |\Omega|$) are integers with $m < p$. Then $\partial^{m-k}\colon M_m \to M_k$ is injective if and only if $m + k \geqslant n$; it is surjective if and only if $m + k \leqslant n$.*

Proof. See Corollary 2.5 in [13].

For convenience we abbreviate $\operatorname{Ker} \partial^i \cap M_j$ by K_j^i and $\partial^i(M_{i+j}) = \operatorname{Im} \partial^i \cap M_j$ by I_{i+j}^i where M_j as before stands for $R\Omega^{\{j\}}$.

Lemma 2.5. *Let R be an associative ring with 1 of prime characteristic $p \neq 0$ and suppose that i, j are integers with $2 \leqslant i < p$ and $2j \leqslant n + 1$. Then $\partial(K_j^i) = K_{j-1}^{i-1}$.*

Proof. Evidently $\partial(K_j^i) \subseteq K_{j-1}^{i-1}$. So let $f \in K_{j-1}^{i-1}$; we must find some $F \in K_j^i$ for which $F' = f$. By Theorem 2.2 we can write f as $f = h_1 \cup \Delta_1 + \cdots + h_t \cup \Delta_t$ where h_s in M_{j-i+1} with $h_s' = 0$ and where Δ_s is disjoint from h_s and has size $i - 2$ for $1 \leqslant s \leqslant t$, in terms of elements of short support $\|h_s\| \leqslant 2(j - i + 1)$. Abbreviate $\Omega \backslash \operatorname{supp}(h_s)$ by Ω_s. Then $|\Omega_s| = n - \|h_s\| \geqslant n - 2(j - i + 1) = (n - 2j) + 2(i-1) > 0$. Now consider the map $\partial\colon R\Omega_s^{\{i-1\}} \to R\Omega_s^{\{i-2\}}$; as $(i-1) + (i-2) = 2i - 3 \leqslant 2(i-1) + (n - 2j) \leqslant |\Omega_s|$ by lemma 2.4 the map is surjective and there is some

$g_s \in R\Omega_s^{\{i-1\}}$ for which $\partial(g_s) = \Delta_s$. Hence let $F := h_1 \cup g_1 + \cdots + h_t \cup g_t$ and verify that $F' = f$ so that also $F^{(i)} = 0$. ▮

3. Homological Sequences

Throughout this chapter R is an associative ring with 1 which has prime characteristic $p \neq 0$. In particular, R is an algebra over $GF(p)$. As $p \neq 0$, the crucial observation is that $\partial^p \colon R2^\Omega \to R2^\Omega$ is the zero map. To see this let Δ be any set of size $d \geqslant p$. Then $\partial^p(\Delta) = c \sum \Gamma$ where the summation runs over all $(d-p)$-element subsets of Δ and where c counts the number of chains with $\Gamma = \Gamma_0 \subset \Gamma_1 \subset \cdots \subset \Gamma_p = \Delta$. So c is $p! = 0$.

The results in Chapter 2 lead us to investigate homology. We recall the usual definitions: if $\chi \colon A \to B$ and $\psi \colon B \to C$ are homomorphisms then the sequence $A \to B \to C$ is *homological* at B if $\mathrm{Ker}(\psi) \supseteq \chi(A)$, and *exact*, if $\mathrm{Ker}(\psi) = \chi(A)$. A longer sequence, $\cdots \leftarrow A_k \leftarrow A_{k+1} \leftarrow A_{k+2} \leftarrow A_{k+3} \leftarrow \cdots$ is *homological* (*exact*) if it has that property at every A_i.

Our main objective is to study the sequence

$$0 \leftarrow 0 \leftarrow \cdots \leftarrow 0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_k \leftarrow M_{k+1} \leftarrow M_{k+2} \cdots \qquad (1)$$

where as before M_j stands for $R\Omega^{\{i\}}$. Clearly, when R has characteristic 2, then this sequence is homological. In fact:

Theorem 3.1. *Let R be a ring of characteristic 2 and Ω a set of arbitrary cardinality. Then $0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots \leftarrow M_{m-1} \leftarrow M_m$ is exact for all $m \leqslant |\Omega|$.*

Proof. It remains to show that $\mathrm{Ker}(\partial) \cap M_m \subseteq \partial(M_{m+1})$. So let f be in $\mathrm{Ker}(\partial) \cap M_m$. For any point α in $\mathrm{supp}(f)$ write f uniquely as $f = \alpha \cup f_\alpha + g$ where f_α and g are disjoint from α. Then $0 = f'$ so that $f_\alpha + g' = 0$. Now consider $F = \alpha \cup g$ and verify that $F' = \alpha \cup f_\alpha + g$. ▮

For characteristic $p > 2$ we require a more general notion.

Definition 3.2. If $2 \leqslant p$ is some integer, then the sequence $A_0 \leftarrow A_1 \leftarrow A_2 \cdots A_{m-2} \leftarrow A_{m-1} \leftarrow A_m$ is *p-exact* (*p-homological*) if $A_k \leftarrow A_{k+i} \leftarrow A_{k+p}$ is exact (homological) for every $0 \leqslant k \leqslant m-p$ and every i, $1 \leqslant i < p$. (The arrows in $A_k \leftarrow A_{k+i} \leftarrow A_{k+p}$ are the natural compositions of arrows in the original sequence.)

So 2-exactness is exactness in the usual meaning and $A_0 \leftarrow A_1 \leftarrow A_2 \cdots A_k \leftarrow A_{k+1} \leftarrow A_{k+2} \cdots$ is 3-exact if and only if both $A_0 \leftarrow A_1 \leftarrow A_3 \leftarrow A_4 \leftarrow A_6 \leftarrow \cdots \leftarrow A_{3s-3} \leftarrow A_{3s-2} \leftarrow A_{3s} \leftarrow \cdots$ and $A_0 \leftarrow A_2 \leftarrow A_3 \leftarrow A_5 \leftarrow A_6 \leftarrow \cdots \leftarrow A_{3s-3} \leftarrow A_{3s-1} \leftarrow A_{3s} \leftarrow \cdots$ are exact.

We return to the sequence (1) above. To clarify the situation consider the first members in $0 \leftarrow \cdots \leftarrow 0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_k \leftarrow M_{k+1} \leftarrow M_{k+2} \cdots$. The module M_0 consists of all R-multiples of the empty set in Ω and $0 \leftarrow M_0$ is the zero map. Further, if $2(p-1) \leqslant n$ and $j \leqslant p-1$, then $\partial^{j-i}\colon M_j \to M_i$ is surjective by Lemma 2.4 and so we have

LEMMA 3.3. *Let R have prime characteristic $p \neq 0$ and $0 < 2p \leqslant |\Omega|$. Then $0 \leftarrow 0 \leftarrow \cdots \leftarrow 0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \cdots \leftarrow M_{p-1}$ is p-exact.*

Our aim will be to show that the lemma remains true for even longer initial segments. For this reason we begin to consider the homology modules. Let as before $K_j^i := \operatorname{Ker} \partial^i \cap M_j$ and $I_{i+j}^i := \operatorname{Im} \partial^i \cap M_j$ and put $H_{jk} := K_j^{j-k+p}/I_k^{k-j}$.

LEMMA 3.4. *Let R have prime characteristic $p \neq 0$ and $2j \leqslant |\Omega| + 1$. Then $H_{jk} \cong K_j^{j-k+p}/(I_k^{k-j} + K_j^1)$.*

Proof. It follows from Lemma 2.5 that $K_j^{j-k+p} = \partial^{-1}(K_{j-1}^{j-k+p-1})$, so that $K_{j-1}^{j-k+p-1} \cong K_j^{j-k+p}/K_j^1$. Similarly, $I_k^{k-j} = \partial^{-1}(I_k^{k-j+1})$ and so $I_k^{k-j+1} \cong I_k^{k-j}/(K_j^1 \cap I_k^{k-j}) \cong (K_j^1 + I_k^{k-j})/K_j^1$ by the isomorphism theorem. Putting the expressions together we get $H_{j-1,k} = K_{j-1}^{j-k+p-1}/I_k^{k-j+1} \cong (K_j^{j-k+p}/K_j^1)/((K_j^1 + I_k^{k-j})/K_j^1) \cong K_j^{j-k+p}/(I_k^{k-j} + K_j^1)$. ∎

THEOREM 3.5. *Let R be an associative ring with 1 of prime characteristic $p \neq 0$ and let $k-p < j < k$ be integers with $k+j \leqslant |\Omega|$. Then $H_{ik} = 0$ for all i with $k-p+1 \leqslant i \leqslant j$.*

Proof. As $2i < |\Omega|$ the condition of Lemma 3.4 holds for H_{ik}. Further, we have $|\Omega| - 2i \geqslant k-i$ and so the Integration Lemma implies that $K_i^1 \subseteq I_k^{k-i}$ and $I_k^{k-i} + K_i^1 = I_k^{k-i}$. Therefore $H_{jk} \cong H_{j-1,k} \cong \cdots \cong H_{k-p+1,k}$. But $H_{k-p+1,k} = K_{k-p+1}^1/I_k^{p-1}$ and since $k+j \leqslant |\Omega|$ we have $|\Omega| - 2(k-p+1) \geqslant p-1$, it follows from the Integration Lemma that $K_{k-p+1}^1 = I_k^{p-1}$. So $H_{k-p+1,k} = 0$. ∎

An immediate consequence now is

THEOREM 3.6. *Let R be an associative ring with 1 of prime characteristic $p \neq 0$. If $2k \leqslant |\Omega|$, then $0 \leftarrow \cdots \leftarrow 0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_{k-2} \leftarrow M_{k-1} \leftarrow M_k$ is p-exact.*

At this point the only result about the "upper part" of the sequence (1) is Theorem 3.1 for the case $p = 2$. If $p \neq 2$ the sequence certainly remains p-homological but examples show that it may fail to be exact. Therefore the question about homology modules arises. We will deal with this in the next section.

4. Group Actions on Ω

Let g be a permutation of Ω. Then g acts on 2^{Ω} by $\Delta \to \Delta^{g} := \{\delta^{g} \mid \delta \in \Delta\}$ which can be extended linearly to all of $R2^{\Omega}$ by $g(\sum r_{\Delta} \Delta) = \sum r_{\Delta} \Delta^{g}$. It is not difficult to see that g commutes with ∂ and so

$$0 \leftarrow 0 \leftarrow \cdots \leftarrow 0 \leftarrow M_0 \leftarrow M_1 \leftarrow M_2 \cdots M_k \leftarrow M_{k+1} \leftarrow M_{k+2} \cdots \qquad (1)$$

is invariant under any set of permutations.

As before let R be an associative ring with 1 of prime characteristic $p \neq 0$. Then the *orbit module* in M_k is $\mathbb{O}_k^G := \{f \mid f \in M_k \text{ and } gf = f \text{ for all } g \in G\}$. We will omit the superscript as it will be clear which group it refers to. The natural basis for $\mathbb{O}_k$ are the "orbits sums" $\underline{\Delta} = \sum_{\Delta^* \in \Delta^G} \Delta^*$ where Δ^G as usual denotes $\{\Delta^g \mid g \in G\}$.

Now define two linear maps $\gamma\colon M_k \to \mathbb{O}_k$ through

$$\gamma_1(\Delta) = \underline{\Delta} \text{ and, when } p \text{ does not divide } |G|,$$

$$\gamma_2(\Delta) = |G|^{-1} \sum_{g \in G} \Delta^g.$$

Note that $\gamma_1(\underline{\Delta}) = |\Delta^G|\, \gamma_2(\underline{\Delta})$ and that γ_2 restricted to $\mathbb{O}_k \subseteq M_k$ is the identity map. Consider therefore the diagram

$$\begin{tikzcd}
{} & M_{k-1} \arrow[l, "\partial"'] \arrow[d, "\gamma"'] & M_k \arrow[l, "\partial"'] \arrow[d, "\gamma"'] & M_{k+1} \arrow[l, "\partial"'] \arrow[d, "\gamma"'] & {} \arrow[l, "\partial"'] \\
{} & \mathbb{O}_{k-1} \arrow[l] & \mathbb{O}_k \arrow[l] & \mathbb{O}_{k+1} \arrow[l] & {} \arrow[l]
\end{tikzcd} \qquad (2)$$

which can be completed at the bottom: As $\Delta_1, \Delta_2 \in \Delta^G$ implies $\gamma_1(\partial \Delta_1) = \gamma_1(\partial \Delta_2)$ we put $\partial_1(\underline{\Delta}) := \gamma_1[\partial(\Delta_1)]$. Similarly, if p does not divide $|G|$ then ∂_2 is given by $\partial_2(\underline{\Delta}) = \gamma_2[\partial(\underline{\Delta})]$.

Denote the number of G-orbits on $\Omega^{\{k\}}$ by $n_k(G)$. It is well-know [5] that for $t \leqslant k \leqslant |\Omega|/2$ we have $n_t(G) \leqslant n_k(G)$. Define the orbit inclusion matrix $W_{tk}(G, \Omega)$ as the matrix whose columns are indexed by G-orbits on $\Omega^{\{k\}}$, its rows by G-orbits on $\Omega^{\{t\}}$ and with (i, j)-entry, for a fixed k-set Γ in the jth orbit, counting the number of t-subset $\Delta \subseteq \Gamma$ belonging to the ith orbit.

It is easy to see that the matrix of ∂_1 (for the natural bases) is $W_{k-1,k}(G)$ viewed as a matrix over R. If the matrix of ∂_2 is $W^*_{k-1,k}(G)$ and n the cardinality of Ω one shows easily that for any $s < t$

$$W^*_{s,t}(G) = [W_{n-t,n-s}(G)]^T. \qquad (3)$$

In general, if D_s is the diagonal matrix $(|\Delta_1^G|, |\Delta_2^G|, ...)$ and D_t the diagonal matrix $(|\Gamma_1^G|, |\Gamma_2^G|, ...)$ where the Δ_i and Γ_j run through systems of s-orbits and t-orbits of G respectively, then the relation between $W_{st}(G)$ and $W_{st}^*(G)$ is

$$W_{st}^*(G) = D_s\, W_{st}(G)\, D_t^{-1}. \tag{4}$$

For the remainder we will deal only with the case when p does not divide the group order. This is an essential restriction as some examples will show later.

In view of (4) it is not surprising that the theory for ∂_1 and ∂_2 essentially is the same:

THEOREM 4.1. *Let R be an associative ring with* 1 *which has prime characteristic $p \neq 0$. Suppose that G is a permutation group on Ω with order co-prime to p. For $p > 2$ and $2m \leqslant |\Omega|$ the sequence*

$$0 \leftarrow 0 \leftarrow \cdots \leftarrow 0 \leftarrow \mathbb{O}_0 \leftarrow \mathbb{O}_1 \leftarrow \cdots \leftarrow \mathbb{O}_{m-1} \leftarrow \mathbb{O}_m \tag{5}$$

is p-exact for both ∂_1 and ∂_2. If $p = 2$, then the same is true for all $m \leqslant |\Omega|$.

Proof. In both cases γ is surjective and so the sequence is p-homological. First we deal with ∂_2. Note that ∂_2 is just the restriction of ∂ to the subspace $\mathbb{O}_{k+j} \subseteq M_{k+j}$. So, if $x \in \mathbb{O}_{k+j}$ satisfies $(\partial_2)^j\, x = 0$ then $x^{(j)} = 0$. Hence, by theorems 3.1 and 3.6 we find some X in M_{m+p} with $X^{(p-j)} = x$ and so $\gamma_2(X) \in \mathbb{O}_{m+p}$ satisfies $[\gamma_2(X)]^{(p-j)} = \gamma_2(x) = x$.

Regarding ∂_1 we know already that $\mathrm{Ker}(\partial_1^j) \cap \mathbb{O}_{m+j} \supseteq \partial_1^{(p-j)}(\mathbb{O}_{m+p})$. From (4) we conclude that the powers of ∂_1 and ∂_2 have the same rank and the same nullity. Therefore $\dim(\mathrm{Ker}(\partial_1^j) \cap \mathbb{O}_{m+j}) = \dim(\mathrm{Ker}(\partial_2^j) \cap \mathbb{O}_{m+j})$ and $\dim(\partial_1^{(p-j)}(\mathbb{O}_{m+p})) = \dim(\partial_2^{(p-j)}(\mathbb{O}_{m+p}))$. As $\partial_2^{(p-j)}(\mathbb{O}_{m+p}) = \mathrm{Ker}(\partial_2^j) \cap \mathbb{O}_{m+j}$ by the first part, $\mathrm{Ker}(\partial_1^j) \cap \mathbb{O}_{m+j}$ and $\partial_1^{(p-j)}(\mathbb{O}_{m+p})$ have the same dimension and so are equal. ▮

As an application we determine the p-rank of the inclusion matrices $W_{st}(G)$. Let $n_k(G)$ as before denote the number of G-orbits on $\Omega^{\{k\}}$.

THEOREM 4.2. *Let G act on the finite set Ω. If p is a prime not dividing the order of G let $s < t$ be be integers such that $t - s < p$ and $t + s \leqslant |\Omega|$. Then the p-rank of $W_{st}(G)$ is $\sum_{0 \leqslant i < t/p} n_{s-ip}(G) - n_{t-(i+1)p}(G)$.*

Proof. By theorem 4.1 the sequence $0 \leftarrow \cdots \leftarrow \mathbb{O}_{t-2p}^G \leftarrow \mathbb{O}_{s-p}^G \leftarrow \mathbb{O}_{t-p}^G \leftarrow \mathbb{O}_s^G \leftarrow \mathbb{O}_t G$ is exact. ▮

Remarks. (1) In the special case when G is the identity group we have a formula for the p-rank of the incidence matrix W_{st} of s-subsets in t-subsets of Ω. It agrees with the results of Linial and Rothschild [4], Frankl

[1], Frumkin and Yakir [2] and the theorem of Wilson in [16]. The formulae given there were obtained in rather different ways, and the implicit inclusion-exclusion principle appears mostly without proper explanation. Here this principle appears as an entirely natural consequence of p-exactness. So we contend that the notion of p-homology and p-exactness is indeed the natural way to study these phenomena.

(2) So far the rank formula above is restricted to the case when $t-s<p$. It may be possible, however, to obtain corresponding results for general $s \leqslant t$ by extending the arguments of p-homology.

5. The Upper Part of the Sequence: Betti Numbers

We now concern ourselves with the upper part of the orbit module sequence (2) when

$$\cdots \leftarrow \mathbb{O}_{m-1} \leftarrow \mathbb{O}_m \leftarrow \mathbb{O}_{m+1} \leftarrow \cdots \leftarrow \mathbb{O}_{|\Omega|-1} \leftarrow \mathbb{O}_{|\Omega|} \tag{6}$$

is p-homological but not necessarily p-exact. For the remainder let R be a field of characteristic p and G a permutation group on Ω of order co-prime to p.

We define the *Betti numbers* of the sequence (6). When $j<k$ and $k-j<p$ put

$$\beta^G_{jk} := \dim[\operatorname{Ker}(\partial_2^{p-(k-j)}) \cap \mathbb{O}_j] - \dim \partial_2^{k-j}(\mathbb{O}_k). \tag{7}$$

By (4) the powers of ∂_1 and ∂_2 have the same rank and nullity, so that the Betti numbers for ∂_1 and ∂_2 are the same.

We begin to evaluate these invariants. Theorems 3.1 implies directly

Lemma 5.1. *If G has odd order and if $p=2$, then $\beta^G_{jk}=0$.*

Further, theorems 3.6 and 4.1 give

Lemma 5.2. (The Balance Condition). *Let $j<k$ and $k-j<p$. If $j+k \leqslant |\Omega|$ then $\beta^G_{jk}=0$.*

If $0<r<q \leqslant p$, we say that the subsequence

$$\cdots \leftarrow \mathbb{O}_{q-p} \leftarrow \mathbb{O}_r \leftarrow \mathbb{O}_q \leftarrow \mathbb{O}_{r+p} \leftarrow \mathbb{O}_{q+p} \leftarrow \mathbb{O}_{r+2p} \leftarrow \cdots \tag{8}$$

of (6) has *type* (r, q) or is an (r, q)-*sequence*. Here for indeces $j<0$ we have put $\mathbb{O}_j=0$ and arrows are appropriate powers of ∂. As before $n_j(G)$ is the number of G-orbits on j-element subsets for $0 \leqslant j \leqslant |\Omega|$, and for convenience we put $n_j(G)=0$ for all other values of j.

For such a sequence let $r^* < q^*$ be the least indeces for which $r^* + q^* > |\Omega|$. So $\mathbb{O}_{r^*} \leftarrow \mathbb{O}_{q^*}$ is the first arrow in (8) for which the Balance Condition fails. The next result determines all Betti numbers.

THEOREM 5.3. *If the order of G is not divisible by the prime p, then the sequence* (8) *of type* (r, q) *is exact everywhere except* (*possibly*) *at* $\mathbb{O}_{q^*-p} \leftarrow \mathbb{O}_{r^*} \leftarrow \mathbb{O}_{q^*}$ *when*

$$\beta_{r^*q^*} = \sum_{k \in \mathbb{Z}} n_{r^*+kp}(G) - n_{q^*+kp}(G)$$

$$= \left| \sum_{k \in \mathbb{Z}} n_{r+kp}(G) - n_{q+kp}(G) \right|.$$

Proof. It will be useful to put $B_{ij} := \sum_{k \in \mathbb{Z}} n_{i+kp}(G) - n_{j+kp}(G)$. Let ψ and ζ be the occurances of ∂_2 in

$$\begin{tikzcd} \mathbb{O}_{q^*-p} & \mathbb{O}_{r^*} \arrow[l] & \mathbb{O}_{q^*} \arrow[l, "\psi"'] \end{tikzcd} \tag{9}$$

and

$$\begin{tikzcd} \mathbb{O}_{n-r^*} \arrow[r, "\zeta"] & \mathbb{O}_{n-q^*} \arrow[r] & \mathbb{O}_{n-r^*-p} \end{tikzcd} \tag{10}$$

Clearly, the Balance Condition implies that (10) is exact. Further, (9) is exact except (possibly) at $\mathbb{O}_{r^*}$. According to (3) and (4) the maps ζ and ψ have the same rank. Therefore

$$\operatorname{rank} \psi = [n_{r^*}(G) - n_{q^*-p}(G) + n_{r^*-p}(G) - \cdots] - \beta_{r^*q^*}$$

$$= \operatorname{rank} \zeta = [n_{n-q^*}(G) - n_{n-r^*-p}(G) + n_{n-q^*-p}(G) - \cdots]$$

So $\beta_{r^*q^*} = [n_{r^*}(G) - n_{q^*-p}(G) + n_{r^*-p}(G) - \cdots] - [n_{n-q^*}(G) - n_{n-r^*-p}(G) + n_{n-q^*-p}(G) - \cdots]$ and using $n_j(G) = n_{n-j}(G)$ we see that $\beta_{r^*q^*} = B_{rq}$.

Next we show that the first Betti number "to the right" of β_{r^*, q^*} is 0. So consider the maps ψ and ζ in

$$\begin{tikzcd} \mathbb{O}_{r^*} & \mathbb{O}_{q^*} \arrow[l] & \mathbb{O}_{r^*+p} \arrow[l, "\psi"'] \end{tikzcd}$$

and

$$\begin{tikzcd} \mathbb{O}_{n-q^*} \arrow[r, "\zeta"] & \mathbb{O}_{n-r^*-p} \arrow[r] & \mathbb{O}_{n-q^*-p} \end{tikzcd}$$

As ψ and ζ have the same rank by (3) and (4) we get

$$\operatorname{rank} \psi = [n_{q^*}(G) - n_{r^*}(G) + n_{q^*-p}(G) - \cdots] - [\beta_{q^*, r^*+p} - \beta_{r^*, q^*}]$$

$$= \operatorname{rank} \zeta = [n_{n-r^*-p}(G) - n_{n-q^*-p}(G) + n_{n-r^*-2p}(G) - \cdots].$$

Note that in the expression for rank(ζ) no Betti numbers appear since $2n-(r^*+q^*)-p<|\Omega|$ so that the Balance Condition applies again. Therefore, $\beta_{q^*,r^*+p}-\beta_{r^*q^*}=B_{q,r+p}$ and from above we get $\beta_{q^*,r^*+p}=B_{q,r+p}+B_{rq}$. But a simple calculation shows that the latter expression is 0. The same arguments apply to the remaining Betti numbers. ▮

Thus Betti numbers are determined entirely by the type of the relevant subsequence of (5). There is at most one non-zero Betti number in a sequence of type (r, q), this is denoted by $\beta_{(r,q)}(G, p)$. So we have the

Corollary 5.4. *Let G be a group acting on Ω and $p\geqslant 2$ a prime not dividing the order of G. If $0<r<q\leqslant p$, then $0\leqslant\beta_{(r,q)}(G,p)\leqslant n_{r^*}(G)$.*

Remark. If $p>|\Omega|$ then $\beta_{(r,q)}(G,p)=n_{r^*}(G)-n_{q^*}(G)$ and so for $p>|G|$ the inequality $0\leqslant\beta_{(r,q)}(G,p)$ implies the theorem of Livingstone & Wagner [5].

6. Some Examples for Small Characteristic

Theorem 5.3 yields already interesting consequences for small primes. Here we investigate only the case when $p=2$ or 3.

6.1. *When $p=2$ and G Has Odd Order*

The only type for a sequence is $r=1$, $q=2$, and instead of $\beta_{(1,2)}(G,2)$ we simply write $\beta(G,2)$. From the formula in Theorem 5.4 we see that $\beta(G,2)=|\sum_{k\in\mathbb{Z}}n_{1+2k}(G)-n_{2+2k}(G)|=|-n_0(G)+n_1(G)-n_2(G)+n_3(G)-\cdots|$. When $|\Omega|=n$ is odd, using the fact that $n_k(G)=n_{n-k}(G)$, we see of course that $\beta(G,2)=0$.

However, by Lemma 5.1, we known that $\beta(G,2)$ is zero in any case. So, when $n=2m$, then $\beta(G,2)=|-n_0(G)+n_1(G)-n_2(G)+n_3(G)-\cdots|$ can be arranged as $0=\beta(G,2)=n_m(G)-2[(n_{m-1}(G)-n_{m-2}(G))+(n_{m-3}(G)-n_{m-4}(G))+\cdots]$. Therefore we have

Theorem 6.1. *If G is a group of odd order acting on a set of size $2m$, then $n_m(G)=2[(n_{m-1}(G)-n_{m-2}(G))+(n_{m-3}(G)-n_{m-4}(G))+\cdots]$.*

The condition that G has odd order is indeed indispensable: Already $G=C_6$ acting naturally has $n_3(G)=4\neq 2[(n_2(G)-n_1(G))+n_0(G)]=6$.

6.2. *The Case $p=3$ and G has order prime to 3*

Here the only types for sequences are $(r,q)=(1,2)$, $(1,3)$ and (2,3). Writing down the various values of n modulo 6 we first work out the possibilities for r^* and q^*. Then, using the formula in Theorem 5.3 we observe that in each case two of the Betti numbers are equal, while the other is zero. So we denote the only relevant Betti number by $\beta(G, 3)$. For $n = 2m$ theorem 5.3 yields

$$\begin{aligned}\beta(G, 3) = n_m(G) - n_{m-1}(G) - n_{m-2}(G) + 2n_{m-3}(G)\\ - n_{m-4}(G) - n_{m-5}(G) + 2n_{m-6}(G)\\ - n_{m-7}(G) - n_{m-8}(G) + 2n_{m-9}(G) \cdots. \qquad (11)\end{aligned}$$

And when $n = 2m + 1$ we get

$$\begin{aligned}\beta(G, 3) = n_m(G) - 2n_{m-1}(G) + n_{m-2}(G) + n_{m+3}(G)\\ - 2n_{m-4}(G) + n_{m-5}(G) + n_{m-6}(G)\\ - 2n_{m-7}(G) + n_{m-8}(G) + n_{m-9}(G) \cdots. \qquad (12)\end{aligned}$$

In contrast to the case of characteristic $p = 2$, we have no independent information about $\beta(G, 3)$ apart from the inequalities of Corollary 5.4. Evaluating these give

THEOREM 6.2. *Let G be a group of order co-prime to* 3 *acting on the set Ω of size n and let $N := \sum_{0 \leqslant k} n_k(G)$.*

(i) *If $n = 2m$ then $(N - 3n_m(G))/6 \leqslant \sum_{1 \leqslant k} n_{m-3k}(G) \leqslant (N - n_m(G))/6$, and*

(ii) *if $n = 2m + 1$ then $(N - 2n_m(G))/6 \leqslant \sum_{1 \leqslant k} n_{m-1-3k}(G) \leqslant N/6$.*

Remark. Returning to the formulae (11) and (12): It would of course be quite interesting to determine those groups for which $\beta(G, 3)$ vanishes. We have done further computations and would like to mention some of our observations. If G is either the identity group or the cyclic group C_q of prime order $q \neq 3$ then one of the Betti numbers is 0 while the other two are $\beta(G, 3) = 1$. (To do this, first write down the number of G-orbits on k-element subset and then make use of Problem 8, page 161 in [12]). We are led to conjecture that $\beta(C_{2m}, 3) = 0$ for m not divisible by 3. In support of this we have verified that $\beta(C_{10}, 3) = \beta(C_{14}, 3) = \beta(C_{16}, 3) = \beta(C_{20}, 3) = \beta(C_{22}, 3) = 0$. More generally: Characterize the groups with $\beta(G, p) = 0$.

REFERENCES

1. P. FRANKL, Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Theory Ser. A* **54** (1990), 85–94.
2. A. FRUMKIN AND A. YAKIR, Rank of inclusion matrices and modular representation theory, *Israel J. Math.* **71**, No. 3 (1990), 309–320.

3. R. L. Graham, S. Y. R. Li, and W. C. Li, On the structure of t-designs, *SIAM J. Algebraic Discrete Metholds* **1** (1980), 8–14.
4. N. Linial and B. L. Rothschild, Incidence matrices of subsets—a rank formula, *SIAM J. Algebraic Discrete Methods* **2** (1981), 330–340.
5. D. Livingstone and A. Wagner, Transitivity of finite permutation groups on unordered sets, *Math. Z.* **90** (1965), 393–403.
6. V. B. Mnukhin, The k-orbit reconstruction and the orbit algebra, *Acta Appl. Math.* **29** (1992), 83–117.
7. V. B. Mnukhin, The k-orbit reconstruction for Abelian and Hamiltonian groups, to appear.
8. V. B. Mnukhin, On the relationship between the lenghts of k-orbits and $(k+1)$-orbits, *Arch. Math.*, in press.
9. V. B. Mnukhin and I. J. Siemons, On modular homology in the Boolean algebra, *J. Algebra* **179** (1996), 191–199.
10. R. E. Peile, Inclusion transformations: (n, m)-graphs and their classification, *Discrete Math.* **96** (1991), 111–129.
11. W. Plesken, Counting with groups and rings, *J. Reine Angew. Math.* **334** (1982), 40–68.
12. J. Riordan, "Combinatorial Identities," Wiley, New York, 1968.
13. J. Siemons, On partitions and permutation groups on unordered sets, *Arch. Math.* **38** (1982), 391–403.
14. J. Siemons, Decompositions of modules associated to finite partially ordered sets, *Europ. J. Combin.* **15** (1994), 53–56.
15. R. Stanley, Some aspects of groups acting on finite posets, *J. Combin. Theory Ser. A* **32**, No. 2 (1982), 132–161.
16. R. M. Wilson, A diagonal form for the incidence matrix of t-subsets versus k-subsets, *Europ. J. Combin.* **11** (1990), 609–615.
17. A. Yakir, Inclusion matrix of k versus l affine subspaces and a permutation module of the general affine group, *J. Combin. Theory Ser. A* **63** (1993), 301–317.