

**Proceedings Trim Size: 9in x 6in**  
**Text Area: 7.35in (include runningheads) x 4.5in**  
**Main Text is 10/13pt**

For Half-Title Page (prepared by publisher)

Publishers' page — (Blank page)

For Full Title Page (prepared by publisher)

For Copyright Page (prepared by publisher)

## A primer on computational group homology and cohomology using GAP and Sage

D. Joyner

*Department of Mathematics,  
United States Naval Academy,  
Annapolis, MD 21402  
wdj@usna.edu*

*Dedicated to my friend and colleague Tony Gaglione on the occasion of his sixtieth birthday.*

These are expanded lecture notes of a series of expository talks surveying basic aspects of group cohomology and homology. They were written for someone who has had a first course in graduate algebra but no background in cohomology. You should know the definition of a (left) module over a (non-commutative) ring, what  $\mathbb{Z}[G]$  is (where  $G$  is a group written multiplicatively and  $\mathbb{Z}$  denotes the integers), and some ring theory and group theory. However, an attempt has been made to (a) keep the presentation as simple as possible, (b) either provide an explicit reference or proof of everything.

Several computer algebra packages are used to illustrate the computations, though for various reasons we have focused on the free, open source packages, such as GAP [10] and Sage [20] (which includes GAP). In particular, Graham Ellis generously allowed extensive use of his HAP [7] documentation (which is sometimes copied almost verbatim) in the presentation below. Some interesting work not included in this (incomplete) survey is (for example) that of Marcus Bishop [2], Jon Carlson [4] (in MAGMA), David Green [12] (in C), Pierre Guillot [13] (in GAP, C++, and Sage), and Marc Röder [16].

Though Graham Ellis' HAP package (and Marc Röder's add-on HAPcryst [16]) can compute cohomology and homology of some infinite groups, the computational examples given below are for finite groups only.

2 *D. Joyner*

## 1. Introduction

First, some words of motivation.

Let  $G$  be a group and  $A$  a  $G$ -module\*.

Let  $A^G$  denote the largest submodule of  $A$  on which  $G$  acts trivially.

Let us begin by asking ourselves the following natural question.

**Question:** Suppose  $A$  is a submodule of a  $G$ -module  $B$  and  $x$  is an arbitrary  $G$ -fixed element of  $B/A$ . Is there an element  $b$  in  $B^G$  (fixed by  $G$ ) which maps onto  $x$  under the quotient map?

The answer to this question can be formulated in terms of group cohomology. (“Yes”, if  $H^1(G, A) = 0$ .) The details, given below, will help motivate the introduction of group cohomology.

Let  $A_G$  is the largest quotient module of  $A$  on which  $G$  acts trivially. Next, we ask ourselves the following analogous question.

**Question:** Suppose  $A$  is a submodule of a  $G$ -module  $B$  and  $b$  is an arbitrary element of  $B_G$  which maps to 0 under the natural map  $B_G \rightarrow (B/A)_G$ . Is there an element  $a$  in  $A_G$  which maps onto  $b$  under the inclusion map?

The answer to this question can be formulated in terms of group homology. (“Yes”, if  $H_1(G, A) = 0$ .) The details, given below, will help motivate the introduction of group homology.

Group cohomology arises as the right higher derived functor for  $A \mapsto A^G$ . The **cohomology groups of  $G$  with coefficients in  $A$**  are defined by

$$H^n(G, A) = \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A).$$

(See §4 below for more details.) These groups were first introduced in 1943 by S. Eilenberg and S. MacLane [6]. The functor  $A \mapsto A^G$  on the category of left  $G$ -modules is additive and left exact. This implies that if

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is an exact sequence of  $G$ -modules then we have a **long exact sequence of cohomology**

$$\begin{aligned} 0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow \\ H^1(G, B) \rightarrow H^1(G, C) \rightarrow H^2(G, A) \rightarrow \dots \end{aligned} \quad (1)$$

\*We call an abelian group  $A$  (written additively) which is a left  $\mathbb{Z}[G]$ -module a  **$G$ -module**.

*A primer on computational group homology and cohomology using GAP and Sage* 3

Similarly, group homology arises as the left higher derived functor for  $A \mapsto A_G$ . The **homology groups of  $G$  with coefficients in  $A$**  are defined by

$$H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

(See §5 below for more details.) The functor  $A \mapsto A_G$  on the category of left  $G$ -modules is additive and right exact. This implies that if

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is an exact sequence of  $G$ -modules then we have a **long exact sequence of homology**

$$\begin{aligned} \cdots \rightarrow H_2(G, C) \rightarrow H_1(G, A) \rightarrow H_1(G, B) \rightarrow \\ H_1(G, C) \rightarrow A_G \rightarrow B_G \rightarrow C_G \rightarrow 0. \end{aligned} \quad (2)$$

Here we will define both cohomology  $H^n(G, A)$  and homology  $H_n(G, A)$  using projective resolutions and the higher derived functors  $\mathrm{Ext}^n$  and  $\mathrm{Tor}_n$ . We “compute” these when  $G$  is a finite cyclic group. We also give various functorial properties, such as corestriction, inflation, restriction, and transfer. Since some of these cohomology groups can be computed with the help of computer algebra systems, we also include some discussion of how to use computers to compute them. We include several applications to group theory.

One can also define  $H^1(G, A)$ ,  $H^2(G, A)$ ,  $\dots$ , by explicitly constructing cocycles and coboundaries. Similarly, one can also define  $H_1(G, A)$ ,  $H_2(G, A)$ ,  $\dots$ , by explicitly constructing cycles and boundaries. For the proof that these constructions yield the same groups, see Rotman [17, chapter 10].

For the general outline, we follow §7 in chapter 10 of [17] on homology. For some details, we follow Brown [3], Serre [18] or Weiss [21].

For a recent expository account of this topic, see for example Adem [1]. Another good reference is Brown [3].

## 2. Differential groups

In this section cohomology and homology are viewed in the same framework. This “differential groups” idea was introduced by Cartan and Eilenberg [5, chapter IV], and developed in R. Godement [11, chapitre 1, §2]. However, we shall follow Weiss [21, chapter 1].

4 *D. Joyner*

### 2.1. Definitions

A **differential group** is a pair  $(L, d)$ ,  $L$  an abelian group and  $d : L \rightarrow L$  a homomorphism such that  $d^2 = 0$ . We call  $d$  a **differential operator**. The group

$$H(L) = \text{Kernel}(d)/\text{Image}(d)$$

is the **derived group** of  $(L, d)$ . If

$$L = \bigoplus_{n=-\infty}^{\infty} L_n$$

then we call  $L$  **graded**. Suppose  $d$  (more precisely,  $d|_{L_n}$ ) satisfies, in addition, for some fixed  $r \neq 0$ ,

$$d : L_n \rightarrow L_{n+r}, \quad n \in \mathbb{Z}.$$

We say  $d$  is **compatible** with the grading provided  $r = \pm 1$ . In this case, we call  $(L, d, r)$  a **graded differential group**. As we shall see, the case  $r = 1$  corresponds to cohomology and the the case  $r = -1$  corresponds to homology. Indeed, if  $r = 1$  then we call  $(L, d, r)$  a (differential) **group of cohomology type** and if  $r = -1$  then we call  $(L, d, r)$  a **group of homology type**. Note that if  $L = \bigoplus_{n=-\infty}^{\infty} L_n$  is a group of cohomology type then  $L' = \bigoplus_{n=-\infty}^{\infty} L'_n$  is a group of homology type, where  $L'_n = L_{-n}$ , for all  $n \in \mathbb{Z}$ .

**For the impatient:** For *cohomology*, we shall eventually take

$$L = \bigoplus_n \text{Hom}_G(X_n, A),$$

where the  $X_n$  form a chain complex (with +1 grading) determined by a certain type of resolution. The group  $H(L)$  is an abbreviation for  $\bigoplus_n \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A)$ . For *homology*, we shall eventually take  $L = \bigoplus_n \mathbb{Z} \otimes_{\mathbb{Z}[G]} X_n$ , where the  $X_n$  form a chain complex (with -1 grading) determined by a certain type of resolution. The group  $H(L)$  is an abbreviation for  $\bigoplus_n \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$ .

Let  $(L, d) = (L, d_L)$  and  $(M, d) = (M, d_M)$  be differential groups (to be more precise, we should use different symbols for the differential operators of  $L$  and  $M$  but, for notational simplicity, we use the same symbol and hope the context removes any ambiguity). A homomorphism  $f : L \rightarrow M$  satisfying  $d \circ f = f \circ d$  will be called **admissible**. For any  $n \in \mathbb{Z}$ , we define  $nf : L \rightarrow M$  by  $(nf)(x) = n \cdot f(x) = f(x) + \dots + f(x)$  ( $n$  times). If  $f$  is admissible then so is  $nf$ , for any  $n \in \mathbb{Z}$ . An admissible map  $f$  gives rise to a map of derived groups: define the map  $f_* : H(L) \rightarrow H(M)$ , by  $f_*(x + dL) = f(x) + dM$ , for all  $x \in L$ .

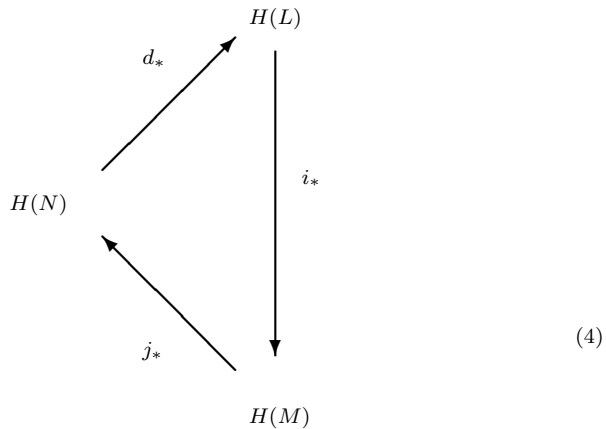
**2.2. Properties**

Let  $f$  be an admissible map as above.

- (1) The map  $f_* : H(L) \rightarrow H(M)$  is a homomorphism.
- (2) If  $f : L \rightarrow M$  and  $g : L \rightarrow M$  are admissible, then so is  $f + g$  and we have  $(f + g)_* = f_* + g_*$ .
- (3) If  $f : L \rightarrow M$  and  $g : M \rightarrow N$  are admissible then so is  $g \circ f : L \rightarrow N$  and we have  $(g \circ f)_* = g_* \circ f_*$ .
- (4) If

$$0 \rightarrow L \xrightarrow{i} M \xrightarrow{j} N \rightarrow 0 \tag{3}$$

is an exact sequence of differential groups with admissible maps  $i, j$  then there is a homomorphism  $d_* : H(N) \rightarrow H(L)$  for which the following triangle is exact:



6 *D. Joyner*

This diagram<sup>†</sup> encodes both the long exact sequence of cohomology (1) and the long exact sequence of homology (2).

Here is the construction of  $d_*$ :

Recall  $H(N) = \text{Kernel}(d)/\text{Image}(d)$ , so any  $x \in H(N)$  is represented by an  $n \in N$  with  $dn = 0$ . Since  $j$  is surjective, there is an  $m \in M$  such that  $j(m) = n$ . Since  $j$  is admissible and the sequence is exact,  $j(dm) = d(j(m)) = dn = 0$ , so  $dm \in \text{Kernel}(j) = \text{Image}(i)$ . Therefore, there is an  $\ell \in L$  such that  $dm = i(\ell)$ . Define  $d_*(x)$  to be the class of  $\ell$  in  $H(L)$ , i.e.,  $d_*(x) = \ell + dL$ .

Here's the verification that  $d_*$  is well-defined:

We must show that if we defined instead  $d_*(x) = \ell' + dL$ , some  $\ell' \in L$ , then  $\ell' - \ell \in dL$ . Pull back the above  $n \in N$  with  $dn = 0$  to an  $m \in M$  such that  $j(m) = n$ . As above, there is an  $\ell \in L$  such that  $dm = i(\ell)$ . Represent  $x \in H(N)$  by an  $n' \in N$ , so  $x = n' + dN$  and  $dn' = 0$ . Pull back this  $n'$  to an  $m' \in M$  such that  $j(m') = n'$ . As above, there is an  $\ell' \in L$  such that  $dm' = i(\ell')$ . We know  $n' - n \in dN$ , so  $n' - n = dn''$ , some  $n'' \in N$ . Let  $j(m'') = n''$ , some  $m'' \in M$ , so  $j(m' - m - dm'') = n' = n - j(dm'') = n' - n - dj(m'') = n' - n - dn'' = 0$ . Since the sequence  $L - M - N$  is exact, this implies there is an  $\ell_0 \in L$  such that  $i(\ell_0) = m' - m - dm''$ . But  $di(\ell_0) = i(d\ell_0) = dm' - dm = i(\ell') - i(\ell) = i(\ell' - \ell)$ , so  $\ell' - \ell \in dL$ .

(5) If  $M = L \oplus N$  then  $H(M) = H(L) \oplus H(N)$ .

**proof:** To avoid ambiguity, for the moment, let  $d_X$  denote the differential operator on  $X$ , where  $X \in \{L, M, N\}$ . In the notation of (3),  $j$  is projection and  $i$  is inclusion. Since both are admissible, we know that  $d_M|_L = d_L$  and  $d_M|_N = d_N$ . Note that  $H(X) \subset X$ , for any differential group  $X$ , so  $H(M) = H(M) \cap L \oplus H(M) \cap N \subset H(L) \oplus H(N)$ . It follows from this that  $d_* = 0$ . From the exactness of the triangle (4), it therefore follows that this inclusion is an equality.

□

(6) Let  $L, L', M, M', N, N'$  be differential groups. If

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & L & \xrightarrow{i} & M & \xrightarrow{j} & N & \longrightarrow & 0 \\
 & & f \downarrow & & g \downarrow & & h \downarrow & & \\
 0 & \longrightarrow & L' & \xrightarrow{i'} & M' & \xrightarrow{j'} & N' & \longrightarrow & 0
 \end{array} \tag{5}$$

<sup>†</sup>This is a special case of Théorème 2.1.1 in [11].

*A primer on computational group homology and cohomology using GAP and Sage* 7

is a commutative diagram of exact sequences with  $i, i', j, j', f, g, h$  all admissible then

$$\begin{array}{ccc} H(L) & \xrightarrow{i_*} & H(M) \\ f_* \downarrow & & g_* \downarrow \\ H(L') & \xrightarrow{i'_*} & H(M') \end{array}$$

commutes,

$$\begin{array}{ccc} H(M) & \xrightarrow{j_*} & H(N) \\ g_* \downarrow & & h_* \downarrow \\ H(M') & \xrightarrow{i'_*} & H(N') \end{array}$$

commutes, and

$$\begin{array}{ccc} H(N) & \xrightarrow{d_*} & H(L) \\ h_* \downarrow & & f_* \downarrow \\ H(N') & \xrightarrow{d_*} & H(L') \end{array}$$

commutes.

This is a case of Theorem 1.1.3 in [21] and of Théorème 2.1.1 in [11]. The proofs that the first two squares commute are similar, so we only verify one and leave the other to the reader. By assumption, (5) commutes and all the maps are admissible. Representing  $x \in H(M)$  by  $x = m + dM$ , we have

$$\begin{aligned} h_* j_*(x) &= h_*(j(m) + dN) = hj(m) + dN' = gi'(m) + dN' \\ &= g_*(i'(m) + dM') = g_* i'_*(m + dM) = g_* i'_*(x), \end{aligned}$$

as desired.

The proof that the last square commutes is a little different than this, so we prove this too. Represent  $x \in H(N)$  by  $x = n + dN$  with  $dn = 0$  and recall that  $d_*(x) = \ell + dL$ , where  $dm = i(\ell)$ ,  $\ell \in L$ , where  $j(m) = n$ , for  $m \in M$ . We have

$$f_* d_*(x) = f_*(\ell + dL) = f(\ell) + dL'.$$

8 *D. Joyner*

On the other hand,

$$d_* h_*(x) = d_*(h(n) + dN') = \ell' + dL',$$

for some  $\ell' \in L'$ . Since  $h(n) \in N'$ , by the commutativity of (5) and the definition of  $d_*$ ,  $\ell' \in L'$  is an element such that  $i'(\ell') = gi(\ell)$ . Since  $i'$  is injective, this condition on  $\ell'$  determines it uniquely mod  $dL'$ . By the commutativity of (5), we may take  $\ell' = f(\ell)$ .

- (7) Let  $L, L', M, M', N, N'$  be differential graded groups with grading +1 (i.e., of “cohomology type”). Suppose that we have a commutative diagram, with all maps admissible and all rows exact as in (5). Then the following diagram is commutative and has exact rows:

$$\begin{array}{cccccccccccc} \dots & \longrightarrow & H_{n-1}(N) & \xrightarrow{d_*} & H_n(L) & \xrightarrow{i_*} & H_n(M) & \xrightarrow{j_*} & H_n(N) & \xrightarrow{d_*} & H_{n+1}(L) & \longrightarrow & \dots \\ & & h_* \downarrow & & f_* \downarrow & & g_* \downarrow & & h_* \downarrow & & f_* \downarrow & & \\ \dots & \longrightarrow & H_{n-1}(N') & \xrightarrow{d_*} & H_n(L') & \xrightarrow{i'_*} & H_n(M') & \xrightarrow{j'_*} & H_n(N') & \xrightarrow{d_*} & H_{n+1}(L') & \longrightarrow & \dots \end{array}$$

This is Proposition 1.1.4 in [21]. As pointed out there, it is an immediate consequence of the properties, 1-6 above.

Compare this with Proposition 10.69 in [17].

- (8) Let  $L, L', M, M', N, N'$  be differential graded groups with grading  $-1$  (i.e., of “homology type”). Suppose that we have a commutative diagram, with all maps admissible and all rows exact, as in (5). Then the following diagram is commutative and has exact rows:

$$\begin{array}{cccccccccccc} \dots & \longrightarrow & H_{n+1}(N) & \xrightarrow{d_*} & H_n(L) & \xrightarrow{i_*} & H_n(M) & \xrightarrow{j_*} & H_n(N) & \xrightarrow{d_*} & H_{n-1}(L) & \longrightarrow & \dots \\ & & h_* \downarrow & & f_* \downarrow & & g_* \downarrow & & h_* \downarrow & & f_* \downarrow & & \\ \dots & \longrightarrow & H_{n+1}(N') & \xrightarrow{d_*} & H_n(L') & \xrightarrow{i'_*} & H_n(M') & \xrightarrow{j'_*} & H_n(N') & \xrightarrow{d_*} & H_{n-1}(L') & \longrightarrow & \dots \end{array}$$

This is the analog of the previous property and is proven similarly.

Compare this with Proposition 10.58 in [17].

- (9) Let  $(L, d)$  be a differential graded group with grading  $r$ . If  $d_n = d|_{L_n}$  then  $d_{n+r} \circ d_n = 0$  and

$$\dots \rightarrow L_{n-r} \xrightarrow{d_{n-r}} L_n \xrightarrow{d_n} L_{n+r} \xrightarrow{d_n} L_{n+2r} \rightarrow \dots \quad (6)$$

is exact.

- (10) If  $\{L_n \mid n \in \mathbb{Z}\}$  is a sequence of abelian groups with homomorphisms  $d_n$  satisfying (6) then  $(L, d)$  is a differential group, where  $L = \bigoplus_n L_n$  and  $d = \bigoplus_n d_n$ .

**2.3. Homology and cohomology**

When  $r = 1$ , we call  $L_n$  the **group of  $n$ -cochains**,  $Z_n = L_n \cap \text{Kernel}(d_n)$  the group of  **$n$ -cocycles**, and  $B_n = L_n \cap d_{n-1}(L_{n-1})$  the group of  **$n$ -coboundaries**. We call  $H_n(L) = Z_n/B_n$  the  $n^{\text{th}}$  **cohomology group**. When  $r = -1$ , we call  $L_n$  the **group of  $n$ -chains**,  $Z_n = L_n \cap \text{Kernel}(d_n)$  the group of  **$n$ -cycles**, and  $B_n = L_n \cap d_{n+1}(L_{n+1})$  the group of  **$n$ -boundaries**. We call  $H_n(L) = Z_n/B_n$  the  $n^{\text{th}}$  **homology group**.

**3. Complexes**

We introduce complexes in order to define explicit differential groups which will then be used to construct group (co)homology.

**3.1. Definitions**

Let  $R$  be a non-commutative ring, for example  $R = \mathbb{Z}[G]$ .

We shall define a “finite free, acyclic, augmented chain complex” of left  $R$ -modules.

A **complex** (or chain complex or  $R$ -complex with a negative grading) is a sequence of maps

$$\dots \rightarrow X_{n+1} \xrightarrow{\partial_{n+1}} X_n \xrightarrow{\partial_n} X_{n-1} \xrightarrow{\partial_{n-1}} X_{n-2} \rightarrow \dots \tag{7}$$

for which  $\partial_n \partial_{n+1} = 0$ , for all  $n$ . If each  $X_n$  is a free  $R$ -module with a finite basis over  $R$  (so is  $\cong R^k$ , for some  $k$ ) then the complex is called **finite free**. If this sequence is exact then it is called an **acyclic complex**. The complex is **augmented** if there is a surjective  $R$ -module homomorphism  $\epsilon : X_0 \rightarrow \mathbb{Z}$  and an injective  $R$ -module homomorphism  $\mu : \mathbb{Z} \rightarrow X_{-1}$  such that  $\partial_0 = \mu \circ \epsilon$ , where (as usual)  $\mathbb{Z}$  is regarded as a trivial  $R$ -module.

The **standard diagram** for such an  $R$ -complex is

$$\begin{array}{ccccccccccc} \dots & \longrightarrow & X_2 & \xrightarrow{\partial_2} & X_1 & \xrightarrow{\partial_1} & X_0 & \xrightarrow{\partial_0} & X_{-1} & \xrightarrow{\partial_{-1}} & X_{-2} & \longrightarrow & \dots \\ & & & & & & \epsilon \downarrow & & \uparrow \mu & & & & \\ & & & & & & \mathbb{Z} & \xlongequal{\quad} & \mathbb{Z} & & & & \\ & & & & & & \downarrow & & \uparrow & & & & \\ & & & & & & 0 & & 0 & & & & \end{array}$$

Such an acyclic augmented complex can be broken up into the **positive part**

10 *D. Joyner*

$$\cdots \rightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

and the **negative part**

$$0 \rightarrow \mathbb{Z} \xrightarrow{\mu} X_{-1} \xrightarrow{\partial_{-1}} X_{-2} \xrightarrow{\partial_{-2}} X_{-3} \rightarrow \cdots .$$

Conversely, given a positive part and a negative part, they can be combined into a standard diagram by taking  $\partial_0 = \mu \circ \epsilon$ .

If  $X$  is any left  $R$ -module, let  $X^* = \text{Hom}_R(X, \mathbb{Z})$  be the dual  $R$ -module, where  $\mathbb{Z}$  is regarded as a trivial  $R$ -module. Associated to any  $f \in \text{Hom}_R(X, Y)$  is the pull-back  $f^* \in \text{Hom}_R(Y^*, X^*)$ . (If  $y^* \in Y^*$  then define  $f^*(y^*)$  to be  $y^* \circ f : X \rightarrow \mathbb{Z}$ .) Since “dualizing” reverses the direction of the maps, if you dualize the entire complex with a  $-1$  grading, you will get a complex with a  $+1$  grading. This is the **dual complex**.

When  $R = \mathbb{Z}[G]$  then we call a finite free, acyclic, augmented chain complex of left  $R$ -modules, a  **$G$ -resolution**. The maps  $\partial_i : X_i \rightarrow X_{i-1}$  are sometimes called **boundary maps**.

**Remark 3.1.** Using the command `BoundaryMap` in the `GAPCRIME` package of Marcus Bishop, one can easily compute the boundary maps of a cohomology object associated to a  $G$ -module. However,  $G$  must be a  $p$ -group.

**Example 3.1.** We use the package `HAP` [7] to illustrate some of these concepts more concretely. Let  $G$  be a finite group, whose elements we have ordered in some way:  $G = \{g_1, \dots, g_n\}$ .

Since a  $G$ -resolution  $X_*$  determines a sequence of finitely generated free  $\mathbb{Z}[G]$ -modules, to concretely describe  $X_*$  we must be able to concretely describe a finite free  $\mathbb{Z}[G]$ -module. In order to represent a word  $w$  in a free  $\mathbb{Z}[G]$ -module  $M$  of rank  $n$ , we use a list of integer pairs  $w = [[i_1, e_1], [i_2, e_2], \dots, [i_k, e_k]]$ . The integers  $i_j$  lie in the range  $\{-n, \dots, n\}$  and correspond to the free  $\mathbb{Z}[G]$ -generators of  $M$  and their additive inverses. The integers  $e_j$  are positive (but not necessarily distinct) and correspond to the group element  $g_{e_j}$ .

Let’s begin with a `HAP` computation.

GAP

```
gap> LoadPackage("hap");
true
gap> G:=Group([(1,2,3),(1,2)]);;
gap> R:=ResolutionFiniteGroup(G, 4);;
```

This computes the first 5 terms of a  $G$ -resolution ( $G = S_3$ )

$$X_4 \xrightarrow{\delta_4} X_3 \xrightarrow{\delta_3} X_2 \xrightarrow{\delta_2} X_1 \xrightarrow{\delta_1} X_0 \rightarrow \mathbb{Z} \rightarrow 0.$$

The boundary maps  $\delta_i$  are determined from the **boundary** component of the GAP record  $R$ . This record has (among others) the following components:

- $R!.dimension(k)$  – the  $\mathbb{Z}[G]$ -rank of the module  $X_k$ ,
- $R!.boundary(k, j)$  – the image in  $X_{k-1}$  of the  $j$ -th free generator of  $X_k$ ,
- $R!.elts$  – the elements in  $G$ ,
- $R!.group$  is the group in question.

Here is an illustration:

```

                                GAP
gap> R!.group;
      Group([ (1,2), (1,2,3) ])
gap> R!.elts;
      [ (), (2,3), (1,2), (1,2,3), (1,3,2), (1,3) ]
gap> R!.dimension(3);
      4
gap> R!.boundary(3,1);
      [ [ 1, 2 ], [ -1, 1 ] ]
gap> R!.boundary(3,2);
      [ [ 2, 2 ], [ -2, 4 ] ]
gap> R!.boundary(3,3);
      [ [ 3, 4 ], [ 1, 3 ], [ -3, 1 ], [ -1, 1 ] ]
gap> R!.boundary(3,4);
      [ [ 2, 5 ], [ -3, 3 ], [ 2, 4 ], [ -1, 4 ], [ 2, 1 ], [ -3, 1 ] ]

```

In other words,  $X_3$  is rank 4 as a  $G$ -module, with generators  $\{f_1, f_2, f_3, f_4\}$  say, and

$$\delta_3(f_1) = f_1g_2 - f_1g_1,$$

$$\delta_3(f_2) = f_2g_2 - f_2g_4,$$

$$\delta_3(f_3) = f_3g_4 - f_3g_1 + f_1g_3 - f_1g_1,$$

$$\delta_3(f_4) = f_2(g_1 + g_3 + g_5) - f_3g_3 + f_1g_4 - f_3g_1.$$

Now, let us create another resolution and compute the equivariant chain map between them. Below is the complete GAP session:

```

                                GAP
gap> G1:=Group([(1,2,3),(1,2)]);
Group([ (1,2,3), (1,2) ])
gap> G2:=Group([(1,2,3),(2,3)]);
Group([ (1,2,3), (2,3) ])
gap> phi:=GroupHomomorphismByImages(G1,G2,[(1,2,3),(1,2)],[(1,2,3),(2,3)]);
[ (1,2,3), (1,2) ] -> [ (1,2,3), (2,3) ]
gap> R1:=ResolutionFiniteGroup(G1, 4);
Resolution of length 4 in characteristic 0 for Group([ (1,2), (1,2,3) ]) .

gap> R2:=ResolutionFiniteGroup(G2, 4);
Resolution of length 4 in characteristic 0 for Group([ (2,3), (1,2,3) ]) .

gap> ZP_map:=EquivariantChainMap(R1, R2, phi);
Equivariant Chain Map between resolutions of length 4 .

gap> map := TensorWithIntegers( ZP_map);
Chain Map between complexes of length 4 .

gap> Hphi := Homology( map, 3);
[ f1, f2, f3 ] -> [ f2, f2*f3, f1*f2^2 ]
gap> AbelianInvariants(Image(Hphi));
[ 2, 3 ]
gap>
gap> GroupHomology(G1,3);
[ 6 ]
gap> GroupHomology(G2,3);
[ 6 ]

```

In other words,  $H(\phi)$  is an isomorphism (as it should be, since the homology is independent of the resolution chosen).

### 3.2. Constructions

Let  $R = \mathbb{Z}[G]$ .

#### 3.2.1. Bar resolution

This section follows §1.3 in [21].

Define a symbol  $[\cdot]$  and call it the **empty cell**. Let  $X_0 = R[\cdot]$ , so  $X_0$  is a finite free (left)  $R$ -module whose basis has only 1 element. For  $n > 0$ , let  $g_1, \dots, g_n \in G$  and define an  $n$ -**cell** to be the symbol  $[g_1, \dots, g_n]$ . Let

$$X_n = \bigoplus_{(g_1, \dots, g_n) \in G^n} R[g_1, \dots, g_n],$$

where the sum runs over all ordered  $n$ -tuples in  $G^n$ .

Define the differential operators  $d_n$  and the augmentation  $\epsilon$ , as  $G$ -module maps, by

$$\begin{aligned}
\epsilon(g[\cdot]) &= 1, & g \in G \\
d_1([g]) &= g[\cdot] - [\cdot], \\
d_2([g_1, g_2]) &= g_1[g_2] - [g_1g_2] + [g_1], \\
&\vdots \\
d_n([g_1, \dots, g_n]) &= g_1[g_2, \dots, g_n] + \sum_{i=1}^{n-1} (-1)^i [g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n] \\
&\quad + (-1)^n [g_1, \dots, g_{n-1}],
\end{aligned}$$

for  $n \geq 1$ . Note that the condition  $\epsilon(g[\cdot]) = 1$  for all  $g \in G$  is equivalent to saying  $\epsilon([\cdot]) = 1$ . This is because  $\epsilon$  is a  $G$ -module homomorphism and  $\mathbb{Z}$  is a trivial  $G$ -module, so  $\epsilon(g[\cdot]) = g\epsilon([\cdot]) = g \cdot 1 = 1$ , where the (trivial)  $G$ -action on  $\mathbb{Z}$  is denoted by a  $\cdot$ .

The  $X_n$  are finite free  $G$ -modules, with the set of all  $n$ -cells serving as a basis.

**Proposition 3.1.** *With these definitions, the sequence*

$$\dots \rightarrow X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

*is a free  $G$ -resolution.*

Sometimes this resolution is called the **bar resolution**<sup>‡</sup>. There are two other resolutions we shall consider. One is the closely related “homogeneous resolution” and the other is the “normalized bar resolution”.

This simple-looking proposition is not so simple to prove. First, we shall show it is a complex, i.e.,  $d^2 = 0$ . Then, and this is the most non-trivial part of the proof, we show that the sequence is exact.

First, we need some definitions and a lemma.

Let  $f : L \rightarrow M$  and  $g : L \rightarrow M$  be  $+1$ -graded admissible maps. We say  $f$  is **homotopic** to  $g$  if there is a homomorphism  $D : L \rightarrow M$ , called a **homotopy**, such that

- $D_n = D|_{L_n} : L_n \rightarrow M_{n+1}$ ,
- $f - g = Dd + dD$ .

<sup>‡</sup>This resolution is not the same as the resolution computed by HAP in Example 3.1. For details on the resolution used by HAP, please see Ellis [8].

14 *D. Joyner*

If  $L = M$  and the identity map  $1 : L \rightarrow L$  is homotopic to the zero map  $0 : L \rightarrow L$  then the homotopy is called a **contracting homotopy for  $L$** .

**Lemma 3.1.** *If  $L$  has a contracting homotopy then  $H(L) = 0$ .*

**proof:** Represent  $x \in H(L)$  by  $\ell \in L$  with  $d\ell = 0$ . But  $\ell = 1(\ell) - 0(\ell) = dD(\ell) + Dd(\ell) = dD(\ell)$ . Since  $D : L \rightarrow L$ , this shows  $\ell \in dL$ , so  $x = 0$  in  $H(L)$ .  $\square$

Next, we construct a contracting homotopy for the complex  $X_*$  in Proposition 3.1 with differential operator  $d$ . Actually, we shall *temporarily* let  $X_{-1} = \mathbb{Z}$ ,  $X_{-n} = 0$  and  $d_{-n} = 0$  for  $n > 1$ , so that that the complex is infinite in both directions. We must define  $D : X \rightarrow X$  such that

- $D_{-1} = D|_{\mathbb{Z}} : \mathbb{Z} \rightarrow X_0$ ,
- $D_n = D|_{X_n} : X_n \rightarrow X_{n+1}$ ,
- $\epsilon D_{-1} = 1$  on  $\mathbb{Z}$ ,
- $d_1 D_0 + D_{-1} \epsilon = 1$  on  $X_0$ ,
- $d_{n+1} D_n + D_{n-1} d_n = 1$  in  $X_n$ , for  $n \geq 1$ .

Define

$$\begin{aligned} D_{-n} &= 0, & n > 1, \\ D_{-1}(1) &= [\cdot], \\ D_0(g[\cdot]) &= [g], \\ D_n(g[g_1, \dots, g_n]) &= [g, g_1, \dots, g_n], & n > 0, \end{aligned}$$

and extend to a  $\mathbb{Z}$ -basis linearly.

Now we must verify the desired properties.

By definition, for  $m \in \mathbb{Z}$ ,  $\epsilon D_{-1}(m) = \epsilon(m[\cdot]) = m\epsilon([\cdot]) = m$ . Therefore,  $\epsilon D_{-1}$  is the identity map on  $\mathbb{Z}$ .

Similarly,

$$\begin{aligned} (d_1 D_0 + D_{-1} \epsilon)(g[\cdot]) &= d_1([g]) + D_{-1}(1) \\ &= g[\cdot] - [\cdot] + D_{-1}(1) = g[\cdot] - [\cdot] + [\cdot] = g[\cdot]. \end{aligned}$$

For the last property, we compute

$$\begin{aligned}
d_{n+1}D_n(g[g_1, \dots, g_n]) &= d_{n+1}([g, g_1, \dots, g_n]) \\
&= g[g_1, \dots, g_n] - [gg_1, \dots, g_n] \\
&\quad + \sum_{i=1}^{n-1} (-1)^{i-1} [g, g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n] \\
&\quad + (-1)^{n+1} [g, g_1, \dots, g_{n-1}],
\end{aligned}$$

and

$$\begin{aligned}
D_{n-1}d_n(g[g_1, \dots, g_n]) &= D_{n-1}(gd_n([g_1, \dots, g_n])) \\
&= D_{n-1}(gg_1[g_2, \dots, g_n]) \\
&\quad + \sum_{i=1}^{n-1} (-1)^i g[g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n] \\
&\quad + (-1)^n g[g_1, \dots, g_{n-1}] \\
&= [gg_1, g_2, \dots, g_n] \\
&\quad + \sum_{i=1}^{n-1} (-1)^i [g, g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_n] \\
&\quad + (-1)^n [g, g_1, \dots, g_{n-1}].
\end{aligned}$$

All the terms but one cancels, verifying that  $d_{n+1}D_n + D_{n-1}d_n = 1$  in  $X_n$ , for  $n \geq 1$ .

Now we show  $d^2 = 0$ . One verifies  $d_1d_2 = 0$  directly (which is left to the reader). Multiply  $d_kD_{k-1} + D_{k-2}d_{k-1} = 1$  on the right by  $d_k$  and  $d_{k+1}D_k + D_{k-1}d_k = 1$  on the left by  $d_k$ :

$$d_kD_{k-1}d_k + D_{k-2}d_{k-1}d_k = d_k = d_kd_{k+1}D_k + d_kD_{k-1}d_k.$$

Cancelling like terms, the induction hypothesis  $d_{k-1}d_k = 0$  implies  $d_kd_{k+1} = 0$ . This shows  $d^2 = 0$  and hence that the sequence in Proposition 3.1 is exact. This completes the proof of Proposition 3.1.  $\square$

The above complex can be “dualized” in the sense of §3.1. This dualized complex is of the form

$$0 \rightarrow \mathbb{Z} \xrightarrow{\mu} X_{-1} \xrightarrow{d_{-1}} X_{-2} \xrightarrow{d_{-2}} X_{-3} \rightarrow \dots$$

The **standard  $G$ -resolution** is obtained by splicing these together.

16 *D. Joyner*

### 3.2.2. Normalized bar resolution

Define the **normalized cells** by

$$[g_1, \dots, g_n]^* = \begin{cases} [g_1, \dots, g_n], & \text{if all } g_i \neq 1, \\ 0, & \text{if some } g_i = 1. \end{cases}$$

Let  $X_0 = R[\cdot]$  and

$$X_n = \bigoplus_{(g_1, \dots, g_n) \in G^n} R[g_1, \dots, g_n]^*, \quad n \geq 1,$$

where the sum runs over all ordered  $n$ -tuples in  $G^n$ . Define the differential operators  $d_n$  and the augmentation map exactly as for the bar resolution.

**Proposition 3.2.** *With these definitions, the sequence*

$$\dots \rightarrow X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

*is a free  $G$ -resolution.*

Sometimes this resolution is called the **normalized bar resolution**.

**proof:** See Theorem 10.117 in [17].  $\square$

### 3.2.3. Homogeneous resolution

Let  $X_0 = R$ , so  $X_0$  is a finite free (left)  $R$ -module whose basis has only 1 element. For  $n > 0$ , let  $X_n$  denote the  $\mathbb{Z}$ -module generated by all  $(n+1)$ -tuples  $(g_0, \dots, g_n)$ . Make  $X_i$  into a  $G$ -module by defining the action by  $g : X_n \rightarrow X_n$  by

$$g : (g_0, \dots, g_n) \mapsto (gg_0, \dots, gg_n), \quad g \in G.$$

Define the differential operators  $\partial_n$  and the augmentation  $\epsilon$ , as  $G$ -module maps, by

$$\begin{aligned} \epsilon(g) &= 1, \\ \partial_n(g_0, \dots, g_n) &= \sum_{i=0}^{n-1} (-1)^i (g_0, \dots, g_{i-1}, \hat{g}_i, g_{i+1}, \dots, g_n), \end{aligned}$$

for  $n \geq 1$ .

**Proposition 3.3.** *With these definitions, the sequence*

$$\cdots \rightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

is a  $G$ -resolution.

Sometimes this resolution is called the **homogeneous resolution**.

Of the three resolutions presented here, this one is the most straightforward to deal with.

**proof:** See Lemma 10.114, Proposition 10.115, and Proposition 10.116 in [17].  $\square$

#### 4. Definition of $H^n(G, A)$

For convenience, we briefly recall the definition of  $\text{Ext}^n$ . Let  $A$  be a left  $R$ -module, where  $R = \mathbb{Z}[G]$ , and let  $(X_i)$  be a  $G$ -resolution of  $\mathbb{Z}$ . We define

$$\text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A) = \text{Kernel}(d_{n+1}^*) / \text{Image}(d_n^*),$$

where

$$d_n^* : \text{Hom}(X_{n-1}, A) \rightarrow \text{Hom}(X_n, A),$$

is defined by sending  $f : X_{n-1} \rightarrow A$  to  $fd_n : X_n \rightarrow A$ . It is known that this is, up to isomorphism, independent of the resolution chosen. Recall  $\text{Ext}_{\mathbb{Z}[G]}^*(\mathbb{Z}, A)$  is the right-derived functors of the right-exact functor  $A \mapsto A^G = \text{Hom}_G(\mathbb{Z}, A)$  from the category of  $G$ -modules to the category of abelian groups. We define

$$H^n(G, A) = \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A), \quad (8)$$

When we wish to emphasize the dependence on the resolution chosen, we write  $H^n(G, A, X_*)$ .

For example, let  $X_*$  denote the bar resolution in §3.2.1 above. Call  $C^n = C^n(G, A) = \text{Hom}_G(X_n, A)$  the **group of  $n$ -cochains of  $G$  in  $A$** ,  $Z^n = Z^n(G, A) = C^n \cap \text{Kernel}(\partial)$  the group of  **$n$ -cocycles**, and  $B^n = B^n(G, A) = \partial(C^{n-1})$  the group of  **$n$ -coboundaries**. We call  $H^n(G, A) = Z^n/B^n$  the  $n^{\text{th}}$  **cohomology group of  $G$  in  $A$** . This is an abelian group.

We call also define the cohomology group using some other resolution, the normalized bar resolution or the homogeneous resolution for example. If we wish to express the dependence on the resolution  $X_*$  used, we write

18 *D. Joyner*

$H^n(G, A, X_*)$ . Later we shall see that, up to isomorphism, this abelian group is independent of the resolution.

The group  $H_2(G, \mathbb{Z})$  (which is isomorphic to the algebraic dual group of  $H^2(G, \mathbb{C}^\times)$ ) is sometimes called the **Schur multiplier** of  $G$ . Here  $\mathbb{C}$  denotes the field of complex numbers.

We say that the group  $G$  has **cohomological dimension**  $n$ , written  $cd(G) = n$ , if  $H^{n+1}(H, A) = 0$  for all  $G$ -modules  $A$  and all subgroups  $H$  of  $G$ , but  $H^n(H, A) \neq 0$  for some such  $A$  and  $H$ .

**Remark 4.1.**

- If  $cd(G) < \infty$  then  $G$  is torsion-free<sup>§</sup>.
- If  $G$  is a free abelian group of finite rank then  $cd(G) = rank(G)$ .
- If  $cd(G) = 1$  then  $G$  is free. This is a result of Stallings and Swan (see for example [17, page 885]).

**4.1. Computations**

We briefly discuss computer programs which compute cohomology and some examples of known computations.

4.1.1. *Computer computations of cohomology*

GAP [10] can compute some cohomology groups<sup>¶</sup>.

All the Sage commands which compute group homology or cohomology require that the package HAP be loaded. You can do this on the command line from the main Sage directory by typing<sup>||</sup>

```
sage -i gap_packages-4.4.10_3.spkg
```

**Example 4.1.** This example uses Sage, which wraps several of the HAP functions.

Sage

```
sage: G = AlternatingGroup(5)
```

<sup>§</sup>This follows from the fact that if  $G$  is a cyclic group then  $H^n(G, \mathbb{Z}) \neq 0$ , discussed below.

<sup>¶</sup>See §37.22 of the GAP manual, M. Bishop's package CRIME for cohomology of  $p$ -groups, G. Ellis' package HAP for group homology and cohomology of finite or (certain) infinite groups, and M. Röder's HAPCryst package (an add-on to the HAP package). Sage [20] computes cohomology via its GAP interface.

<sup>||</sup>This is the current package name - change 4.4.10.3 to whatever the latest version is on <http://www.sagemath.org/packages/optional/> at the time you read this. Also, this command assumes you are using Sage on a machine with an internet connection.

```
sage: G.cohomology(1,7)
Trivial Abelian Group
sage: G.cohomology(2,7)
Trivial Abelian Group
```

This implies  $H^1(A_5, GF(7)) = H^2(A_5, GF(7)) = 0$ .

#### 4.1.2. Examples

Some example computations of a more theoretical nature.

- (1)  $H^0(G, A) = A^G$ .  
This is by definition.
- (2) Let  $L/K$  denote a Galois extension with finite Galois group  $G$ . We have  $H^1(G, L^\times) = 1$ . This is often called Hilbert's Theorem 90. See Theorem 1.5.4 in [21] or Proposition 2 in §X.1 of [18].
- (3) Let  $G$  be a finite cyclic group and  $A$  a trivial torsion-free  $G$ -module. Then  $H^1(G, A) = 0$ .  
This is a consequence of properties given in the next section.
- (4) If  $G$  is a finite cyclic group of order  $m$  and  $A$  is a trivial  $G$ -module then

$$H^2(G, A) = A/mA$$

This is a consequence of properties given below.

For example,  $H^2(GF(q)^\times, \mathbb{C}) = 0$ .

- (5) If  $|G| = m$ ,  $rA = 0$  and  $\gcd(r, m) = 1$ , then  $H^n(G, A) = 0$ , for all  $n \geq 1$ .  
This is Corollary 3.1.7 in [21].  
For example,  $H^1(A_5, \mathbb{Z}/7\mathbb{Z}) = 0$ .

### 5. Definition of $H_n(G, A)$

We say  $A$  is **projective** if the functor  $B \mapsto \text{Hom}_G(A, B)$  (from the category of  $G$ -modules to the category of abelian groups) is exact. Recall, if

$$P_{\mathbb{Z}} = \cdots \rightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0 \quad (9)$$

is a projective resolution of  $\mathbb{Z}$  then

$$\text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A) = \text{Kernel}(d_n \otimes 1_A) / \text{Image}(d_{n+1} \otimes 1_A).$$

20 *D. Joyner*

It is known that this is, up to isomorphism, independent of the resolution chosen. Recall  $\text{Tor}_*^{\mathbb{Z}[G]}(\mathbb{Z}, A)$  are the right-derived functors of the right-exact functor  $A \mapsto A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$  from the category of  $G$ -modules to the category of abelian groups. We define

$$H_n(G, A) = \text{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A), \quad (10)$$

When we wish to emphasize the dependence on the resolution, we write  $H_n(G, A, P_{\mathbb{Z}})$ .

**Remark 5.1.** If  $G$  is a  $p$ -group, then using the command `ProjectiveResolution` in GAP's `CRIME` package, one can easily compute the minimal projective resolution of a  $G$ -module, which can be either trivial or given as a `MeatAxe**` module.

Since we can identify the functor  $A \mapsto A_G$  with  $A \mapsto A \otimes_{\mathbb{Z}[G]} \mathbb{Z}$  (where  $\mathbb{Z}$  is considered as a trivial  $\mathbb{Z}[G]$ -module), the following is another way to formulate this definition.

If  $\mathbb{Z}$  is considered as a trivial  $\mathbb{Z}[G]$ -module, then a free  $\mathbb{Z}[G]$ -resolution of  $\mathbb{Z}$  is a sequence of  $\mathbb{Z}[G]$ -module homomorphisms

$$\dots \rightarrow M_n \rightarrow M_{n-1} \rightarrow \dots \rightarrow M_1 \rightarrow M_0$$

satisfying:

- (Freeness) Each  $M_n$  is a free  $\mathbb{Z}[G]$ -module.
- (Exactness) The image of  $M_{n+1} \rightarrow M_n$  equals the kernel of  $M_n \rightarrow M_{n-1}$  for all  $n > 0$ .
- (Augmentation) The cokernel of  $M_1 \rightarrow M_0$  is isomorphic to the trivial  $\mathbb{Z}[G]$ -module  $\mathbb{Z}$ .

The maps  $M_n \rightarrow M_{n-1}$  are the boundary homomorphisms of the resolution. Setting  $TM_n$  equal to the abelian group  $M_n/G$  obtained from  $M_n$  by killing the  $G$ -action, we get an induced sequence of abelian group homomorphisms

$$\dots \rightarrow TM_n \rightarrow TM_{n-1} \rightarrow \dots \rightarrow TM_1 \rightarrow TM_0$$

This sequence will generally not satisfy the above exactness condition, and one defines the integral homology of  $G$  to be

---

\*\*See for example <http://www.math.rwth-aachen.de/~MTX/>.

$$H_n(G, \mathbb{Z}) = \text{Kernel}(TM_n \rightarrow TM_{n-1}) / \text{Image}(TM_{n+1} \rightarrow TM_n)$$

for all  $n > 0$ .

### 5.1. Computations

We briefly discuss computer programs which compute homology and some examples of known computations.

#### 5.1.1. Computer computations of homology

**Example 5.1.** GAP will compute the Schur multiplier  $H_2(G, \mathbb{Z})$  using the `AbelianInvariantsMultiplier` command. To find  $H_2(A_5, \mathbb{Z})$ , where  $A_5$  is the alternating group on 5 letters, type

```

GAP
gap> A5:=AlternatingGroup(5);
Alt( [ 1 .. 5 ] )
gap> AbelianInvariantsMultiplier(A5);
[ 2 ]
```

So,  $H_2(A_5, \mathbb{C}) \cong \mathbb{Z}/2\mathbb{Z}$ .

Here is the same computation in Sage:

```

Sage
sage: G = AlternatingGroup(5)
sage: G.homology(2)
Multiplicative Abelian Group isomorphic to C2
```

**Example 5.2.** The Sage command `poincare_series` returns the Poincare series of  $G$  (mod  $p$ ) ( $p$  must be a prime). In other words, if you input a (finite) permutation group  $G$ , a prime  $p$ , and a positive integer  $n$ , `poincare_series(G,p,n)` returns a quotient of polynomials  $f(x) = P(x)/Q(x)$  whose coefficient of  $x^k$  equals the rank of the vector space  $H_k(G, \mathbb{Z}\mathbb{Z}/p\mathbb{Z}\mathbb{Z})$ , for all  $k$  in the range  $1 \leq k \leq n$ .

```

Sage
sage: G = SymmetricGroup(5)
sage: G.poincare_series(2,10)
(x^2 + 1)/(x^4 - x^3 - x + 1)
sage: G = SymmetricGroup(3)
sage: G.poincare_series(2,10)
```

22 *D. Joyner*

$$1/(-x + 1)$$

This last one implies

$$\dim_{GF(2)} H_k(S_2, \mathbb{Z}/2\mathbb{Z}) = 1,$$

for  $1 \leq k \leq 10$ .

**Example 5.3.** Here are some more examples using Sage's interface to HAP:

```

Sage
-----
sage: G = SymmetricGroup(5)
sage: G.homology(1)
Multiplicative Abelian Group isomorphic to C2
sage: G.homology(2)
Multiplicative Abelian Group isomorphic to C2
sage: G.homology(3)
Multiplicative Abelian Group isomorphic to C2 x C4 x C3
sage: G.homology(4)
Multiplicative Abelian Group isomorphic to C2
sage: G.homology(5)
Multiplicative Abelian Group isomorphic to C2 x C2 x C2
sage: G.homology(6)
Multiplicative Abelian Group isomorphic to C2 x C2
sage: G.homology(7)
Multiplicative Abelian Group isomorphic to C2 x C2 x C4 x C3 x C5

```

The last one means that

$$H_7(S_5, \mathbb{Z}) = (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}).$$

```

Sage
-----
sage: G = AlternatingGroup(5)
sage: G.homology(1)
Trivial Abelian Group
sage: G.homology(1,7)
Trivial Abelian Group
sage: G.homology(2,7)
Trivial Abelian Group

```

This implies  $H_1(A_5, \mathbb{Z}) = H_1(A_5, GF(7)) = H_2(A_5, GF(7)) = 0$ .

### 5.1.2. Examples

Some example computations of a more theoretical nature.

- (1) If  $A$  is a  $G$ -module then  $\mathrm{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, A) = H_0(G, A) = A_G \cong A/DA$ .

**proof:** We need some lemmas.

Let  $\epsilon : \mathbb{Z}[G] \rightarrow \mathbb{Z}$  be the augmentation map. This is a ring homomorphism (but not a  $G$ -module homomorphism). Let  $D = \mathrm{Kernel}(\epsilon)$  denote its kernel, the **augmentation ideal**. This is a  $G$ -module.

**Lemma 5.1.** *As an abelian group,  $D$  is free abelian generated by  $G - 1 = \{g - 1 \mid g \in G\}$ .*

We write this as  $D = \mathbb{Z}\langle G - 1 \rangle$ .

**proof of lemma:** If  $d \in D$  then  $d = \sum_{g \in G} m_g g$ , where  $m_g \in \mathbb{Z}$  and  $\sum_{g \in G} m_g = 0$ . Thus,  $d = \sum_{g \in G} m_g (g - 1)$ , so  $D \subset \mathbb{Z}\langle G - 1 \rangle$ . To show  $D$  is free: If  $\sum_{g \in G} m_g (g - 1) = 0$  then  $\sum_{g \in G} m_g g - \sum_{g \in G} m_g = 0$  in  $\mathbb{Z}[G]$ . But  $\mathbb{Z}[G]$  is a free abelian group with basis  $G$ , so  $m_g = 0$  for all  $g \in G$ .  $\square$

**Lemma 5.2.**  $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A = A/DA$ , where  $DA$  is generated by elements of the form  $ga - a$ ,  $g \in G$  and  $a \in A$ .

Recall  $A_G$  denotes the largest quotient of  $A$  on which  $G$  acts trivially<sup>††</sup>.

**proof of lemma:** Consider the  $G$ -module map,  $A \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ , given by  $a \mapsto 1 \otimes a$ . Since  $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A$  is a trivial  $G$ -module, it must factor through  $A_G$ . The previous lemma implies  $A_G \cong A/DA$ . (In fact, the quotient map  $q : A \rightarrow A_G$  satisfies  $q(ga - a) = 0$  for all  $g \in G$  and  $a \in A$ , so  $DA \subset \mathrm{Kernel}(q)$ . By maximality of  $A_G$ ,  $DA = \mathrm{Kernel}(q)$ . QED) So, we have maps  $A \rightarrow A_G \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ . By the definition of tensor products, the map  $\mathbb{Z} \times A \rightarrow A_G$ ,  $1 \times a \mapsto 1 \cdot aDA$ , corresponds to a map  $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \rightarrow A_G$  for which the composition  $A_G \rightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \rightarrow A_G$  is the identity. This forces  $A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ .  $\square$

See also # 11 in §6.

- (2) If  $G$  is a finite group then  $H_0(G, \mathbb{Z}) = \mathbb{Z}$ .  
This is a special case of the example above (taking  $A = \mathbb{Z}$ , as a trivial  $G$ -module).
- (3)  $H_1(G, \mathbb{Z}) \cong G/[G, G]$ , where  $[G, G]$  is the commutator subgroup of  $G$ .  
This is Proposition 10.110 in [17, §10.7].  
**proof:** First, we **claim:**  $D/D^2 \cong G/[G, G]$ , where  $D$  is as in Lemma 5.1. To prove this, define  $\theta : G \rightarrow D/D^2$  by  $g \mapsto (g-1)+D^2$ . Since  $gh-1-(g-1)-(h-1) = (g-1)(h-1)$ , it follows that  $\theta(gh) = \theta(g)\theta(h)$ , so  $\theta$  is

<sup>††</sup>Implicit in the words “largest quotient” is a universal property which we leave to the reader for formulate precisely.

24 *D. Joyner*

a homomorphism. Since  $D/D^2$  is abelian and  $G/[G, G]$  is the maximal abelian quotient of  $G$ , we must have  $\text{Kernel}(\theta) \subset [G, G]$ . Therefore,  $\theta$  factors through  $\theta' : G/[G, G] \rightarrow D/D^2$ ,  $g[G, G] \mapsto (g-1) + D^2$ . Now, we construct an inverse. Define  $\tau : D \rightarrow G/[G, G]$  by  $g-1 \mapsto g[G, G]$ . Since  $\tau(g-1+h-1) = g[G, G] \cdot h[G, G] = gh[G, G]$ , it is not hard to see that this is a homomorphism. We would be essentially done (with the construction of the inverse of  $\theta'$ , hence the proof of the claim) if we knew  $D^2 \subset \text{Kernel}(\tau)$ . (The inverse would be the composition of the quotient  $D/D^2 \rightarrow D/\text{Kernel}(\tau)$  with the map induced from  $\tau$ ,  $D/\text{Kernel}(\tau) \rightarrow G/[G, G]$ .) This follows from the fact that any  $x \in D^2$  can be written as  $x = (\sum_g m_g(g-1))(\sum_h m'_h(h-1)) = (\sum_{g,h} m_g m'_h (g-1)(h-1))$ , so  $\tau(x) = \prod_{g,h} (ghg^{-1}h^{-1})^{m_g m'_h} [G, G] = [G, G]$ . QED (claim)

Next, we show  $H_1(G, \mathbb{Z}) \cong D/D^2$ . From the short exact sequence

$$0 \rightarrow D \rightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

we obtain the long exact sequence of homology

$$\begin{aligned} \cdots \rightarrow H_1(G, D) \rightarrow H_1(G, \mathbb{Z}[G]) \rightarrow \\ H_1(G, \mathbb{Z}) \xrightarrow{\partial} H_0(G, D) \xrightarrow{f} H_0(G, \mathbb{Z}[G]) \xrightarrow{\epsilon_*} H_0(G, \mathbb{Z}) \rightarrow 0. \end{aligned} \quad (11)$$

Since  $\mathbb{Z}[G]$  is a free  $\mathbb{Z}[G]$ -module,  $H_1(G, \mathbb{Z}[G]) = 0$ . Therefore  $\partial$  is injective. By item # 1 above (i.e.,  $H_0(G, A) \cong A/DA \cong A_G$ , we have  $H_0(G, \mathbb{Z}) \cong \mathbb{Z}_G = \mathbb{Z}$  and  $H_0(G, \mathbb{Z}[G]) \cong \mathbb{Z}[G]/D \cong \mathbb{Z}$ . By (11),  $\epsilon_*$  is surjective. Combining the last two statements, we find  $\mathbb{Z}/\text{Kernel}(\epsilon_*) \cong \mathbb{Z}$ . This forces  $\epsilon_*$  to be injective. This, and (11), together imply  $f$  must be 0. Since this forces  $\partial$  to be an isomorphism, we are done.  $\square$

- (4) Let  $G = F/R$  be a presentation of  $G$ , where  $F$  is a free group and  $R$  is a normal subgroup of relations. **Hopf's formula** states:  $H_2(G, \mathbb{Z}) \cong (F \cap R)/[F, R]$ , where  $[F, R]$  is the commutator subgroup of  $G$ . See [17, §10.7].

The group  $H_2(G, \mathbb{Z})$  is sometimes called the **Schur multiplier** of  $G$ .

## 6. Basic properties of $H^n(G, A)$ , $H_n(G, A)$

Let  $R$  be a (possibly non-commutative) ring and  $A$  be an  $R$ -module. We say  $A$  is **injective** if the functor  $B \mapsto \text{Hom}_R(B, A)$  (from the category of  $R$ -modules to the category of abelian groups) is exact. (Recall  $A$  is projective if the functor  $B \mapsto \text{Hom}_R(A, B)$  is exact.) We say  $A$  is **co-induced** if it has the form  $\text{Hom}_{\mathbb{Z}}(R, B)$  for some abelian group  $B$ . We say  $A$  is **relatively**

**injective** if it is a direct factor of a co-induced  $R$ -module. We say  $A$  is **relatively projective** if

$$\begin{aligned} \pi : \mathbb{Z}[G] \otimes_{\mathbb{Z}} A &\rightarrow A, \\ x \otimes a &\mapsto xa, \end{aligned}$$

maps a direct factor of  $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$  isomorphically onto  $A$ . These are the  $G$ -modules  $A$  which are isomorphic to a direct factor of the induced module  $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ . When  $G$  is finite, the notions of relatively injective and relatively projective coincide<sup>‡‡</sup>.

- (1) The definition of  $H^n(G, A)$  does not depend on the  $G$ -resolution  $X_*$  of  $\mathbb{Z}$  used.
- (2) If  $A$  is an projective  $\mathbb{Z}[G]$ -module then  $H^n(G, A) = 0$ , for all  $n \geq 1$ .  
This follows immediately from the definitions.
- (3) If  $A$  is an injective  $\mathbb{Z}[G]$ -module then  $H_n(G, A) = 0$ , for all  $n \geq 1$ .  
See also [18, §VII.2].
- (4) If  $A$  is a relatively injective  $\mathbb{Z}[G]$ -module then  $H^n(G, A) = 0$ , for all  $n \geq 1$ .  
This is Proposition 1 in [18, §VII.2].
- (5) If  $A$  is a relatively projective  $\mathbb{Z}[G]$ -module then  $H^n(G, A) = 0$ , for all  $n \geq 1$ .  
This is Proposition 2 in [18, §VII.4].
- (6) If  $A = A' \oplus A''$  then  $H^n(G, A) = H^n(G, A') \oplus H^n(G, A'')$ , for all  $n \geq 0$ . More generally, if  $I$  is any indexing family and  $A = \bigoplus_{i \in I} A_i$  then  $H^n(G, A) = \bigoplus_{i \in I} H^n(G, A_i)$ , for all  $n \geq 0$ .  
This follows from Proposition 10.81 in §10.6 of Rotman [17].
- (7) If

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is an exact sequence of  $G$ -modules then we have a long exact sequence of cohomology (1). See [18, §VII.2], and properties of the Ext functor [17, §10.6].

- (8)  $A \mapsto H^n(G, A)$  is the higher right derived functor associated to  $A \mapsto A^G = \text{Hom}_G(A, \mathbb{Z})$  from the category of  $G$ -modules to the category of abelian groups.  
This is by definition. See [18, §VII.2], or [17, §10.7].

<sup>‡‡</sup>These notions were introduced by Hochschild [14].

26 *D. Joyner*

(9) If

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is an exact sequence of  $G$ -modules then we have a long exact sequence of homology (2). In the case of a finite group, see [18, §VIII.1]. In general, see [18, §VII.4], and properties of the Tor functor in [17, §10.6].

(10)  $A \mapsto H_n(G, A)$  is the higher left derived functor associated to  $A \mapsto A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$  on the category of  $G$ -modules.

This is by definition. See [18, §VII.4], or [17, §10.7].

(11) If  $G$  is a finite cyclic group then

$$\begin{aligned} H_0(G, A) &= A_G, \\ H_{2n-1}(G, A) &= A^G/NA, \\ H_{2n}(G, A) &= \text{Kernel}(N)/DA, \end{aligned}$$

for all  $n \geq 1$ .

To prove this, we need a lemma.

**Lemma 6.1.** *Let  $G = \langle g \rangle$  be acyclic group of order  $k$ . Let  $M = g - 1$  and  $N = 1 + g + g^2 + \dots + g^{k-1}$ . Then*

$$\dots \rightarrow \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{M} \mathbb{Z}[G] \rightarrow \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{M} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0,$$

*is a free  $G$ -resolution.*

**proof of lemma:** It is clearly free. Since  $MN = NM = (g - 1)(1 + g + g^2 + \dots + g^{k-1}) = g^k - 1 = 0$ , it is a complex. It remains to prove exactness. Since  $\text{Kernel}(\epsilon) = D = \text{Image}(M)$ , by Lemma 5.1, this stage is exact.

To show  $\text{Kernel}(M) = \text{Image}(N)$ , let  $x = \sum_{j=0}^{k-1} m_j g^j \in \text{Kernel}(M)$ . Since  $(g - 1)x = 0$ , we must have  $m_0 = m_1 = \dots = m_{k-1}$ . This forces  $x = m_0 N \in \text{Image}(N)$ . Thus  $\text{Kernel}(M) \subset \text{Image}(N)$ . Clearly  $MN = 0$  implies  $\text{Image}(N) \subset \text{Kernel}(M)$ , so  $\text{Kernel}(M) = \text{Image}(N)$ . To show  $\text{Kernel}(N) = \text{Image}(M)$ , let  $x = \sum_{j=0}^{k-1} m_j g^j \in \text{Kernel}(N)$ . Since  $Nx = 0$ , we have  $0 = \epsilon(Nx) = \epsilon(N)\epsilon(x) = k\epsilon(x)$ , so  $\sum_{j=0}^{k-1} m_j = 0$ . Observe that

$$\begin{aligned}
x &= m_0 \cdot 1 + m_1 g + m_2 g^2 + \dots + m_{k-1} g^{k-1} \\
&= (m_0 - m_0 g) + (m_0 + m_1)g + m_2 g^2 + \dots + m_{k-1} g^{k-1} \\
&= (m_0 - m_0 g) + (m_0 + m_1)g - (m_0 + m_1)g^2 \\
&\quad + (m_0 + m_1 + m_2)g^2 - (m_0 + m_1 + m_2)g^3 + \dots \\
&\quad + (m_0 + \dots + m_{k-1})g^{k-1} - (m_0 + \dots + m_{k-1})g^k.
\end{aligned}$$

where the last two terms are actually 0. This implies  $x = -M(m_0 + (m_0 + m_1)g + (m_0 + m_1 + m_2)g^2 + \dots + (m_0 + \dots + m_{k-1})g^{k-1}) \in \text{Image}(M)$ . Thus  $\text{Kernel}(N) \subset \text{Image}(M)$ . Clearly  $NM = 0$  implies  $\text{Image}(M) \subset \text{Kernel}(N)$ , so  $\text{Kernel}(N) = \text{Image}(M)$ .

This proves exactness at every stage.  $\square$

Now we can prove the claimed property. By property 1 in §5.1.2, it suffices to assume  $n > 0$ . Tensor the complex in Lemma 6.1 on the right with  $A$ :

$$\begin{aligned}
\dots \rightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{N_*} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{M_*} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{N_*} \\
\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{M_*} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{\epsilon} \mathbb{Z} \otimes \mathbb{Z}[G]A \rightarrow 0,
\end{aligned}$$

where the new maps are distinguished from the old maps by adding an asterisk. By definition,  $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \cong A$ , and by property 1 in §5.1.2,  $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong A/DA$ . The above sequence becomes

$$\dots \rightarrow A \xrightarrow{N_*} A \xrightarrow{M_*} A \xrightarrow{N_*} A \xrightarrow{M_*} A \xrightarrow{\epsilon} A/DA \rightarrow 0.$$

This implies, by definition of Tor ,

$$\text{Tor}_{2n-1}^{\mathbb{Z}[G]}(\mathbb{Z}, A) = \text{Kernel}(M_*)/\text{Image}(N_*) = A^G/NA,$$

and

$$\text{Tor}_{2n}^{\mathbb{Z}[G]}(\mathbb{Z}, A) = \text{Kernel}(N_*)/\text{Image}(M_*) = A[N]/DA.$$

See also [18], §VIII.4.1 and the Corollary in §VIII.4.

- (12) The group  $H^2(G, A)$  classifies group extensions of  $A$  by  $G$ . This is Theorem 5.1.2 in [21]. See also §10.2 in [17].
- (13) If  $G$  is a finite group of order  $m = |G|$  then  $mH^n(G, A) = 0$ , for all  $n \geq 1$ . This is Proposition 10.119 in [17].
- (14) If  $G$  is a finite group and  $A$  is a finitely-generated  $G$ -module then  $H^n(G, A)$  is finite, for all  $n \geq 1$ . This is Proposition 3.1.9 in [21] and Corollary 10.120 in [17].

28 *D. Joyner*

- (15) The group  $H^1(G, A)$  constructed using resolutions is the same as the group constructed using 1-cocycles. The group  $H^2(G, A)$  constructed using resolutions is the same as the group constructed using 2-cocycles. This is Corollary 10.118 in [17].
- (16) If  $G$  is a finite cyclic group then

$$\begin{aligned} H^0(G, A) &= A^G, \\ H^{2n-1}(G, A) &= \text{Kernel } N/DA, \\ H^{2n}(G, A) &= A^G/NA, \end{aligned}$$

for all  $n \geq 1$ . Here  $N : A \rightarrow A$  is the norm map  $Na = \sum_{g \in G} ga$  and  $DA$  is the augmentation ideal defined above (generated by elements of the form  $ga - a$ ).

**proof:** The case  $n = 0$ : By definition,  $H^0(G, A) = \text{Ext}_{\mathbb{Z}[G]}^0(\mathbb{Z}, A) = \text{Hom}_G(\mathbb{Z}, A)$ . Define  $\tau : \text{Hom}_G(\mathbb{Z}, A) \rightarrow A^G$  by sending  $f \mapsto f(1)$ . It is easy to see that this is well-defined and, in fact, injective. For each  $a \in A^G$ , define  $f = f_a \in \text{Hom}_G(\mathbb{Z}, A)$  by  $f(m) = ma$ . This shows  $\tau$  is surjective as well, so case  $n = 0$  is proven.

Case  $n > 0$ : Applying the functor  $\text{Hom}_G(*, A)$  to the  $G$ -resolution in Lemma 6.1 to get

$$\cdots \leftarrow \text{Hom}_G(\mathbb{Z}[G], A) \xleftarrow{N_*} \text{Hom}_G(\mathbb{Z}[G], A) \xleftarrow{M_*} \text{Hom}_G(\mathbb{Z}[G], A) \xleftarrow{\epsilon_*} \text{Hom}_G(\mathbb{Z}, A) \leftarrow 0.$$

It is known that  $\text{Hom}_G(\mathbb{Z}[G], A) \cong A$  (see Proposition 8.85 on page 583 of [17]). It follows that

$$\cdots \leftarrow A \xleftarrow{N_*} A \xleftarrow{M_*} A \xleftarrow{\epsilon_*} A^G \leftarrow 0.$$

By definition of  $\text{Ext}$ , for  $n > 0$  we have

$$\text{Ext}_{\mathbb{Z}[G]}^{2n}(\mathbb{Z}, A) = \text{Kernel}(M_*)/\text{Image}(N_*) = A^G/NA,$$

and

$$\text{Ext}_{\mathbb{Z}[G]}^{2n-1}(\mathbb{Z}, A) = \text{Kernel}(N_*)/\text{Image}(M_*) = \text{Kernel}(N)/(g-1)A,$$

where  $g$  is a generator of  $G$  as in Lemma 6.1.  $\square$

See also [18], §VIII.4.1 and the Corollary in §VIII.4.

(17) If  $G$  is a finite cyclic group of order  $m$  and  $A$  is a *trivial*  $G$ -module then

$$\begin{aligned} H^0(G, A) &= A^G, \\ H^{2n-1}(G, A) &\cong A[m], \\ H^{2n}(G, A) &\cong A/mA, \end{aligned}$$

for all  $n \geq 1$ .

This is a consequence of the previous property.

## 7. Functorial properties

In this section, we investigate some of the ways in which  $H^n(G, A)$  depends on  $G$ .

One way to construct all these in a common framework is to introduce the notion of a “homomorphism of pairs”. Let  $G, H$  be groups. Let  $A$  be a  $G$ -module and  $B$  an  $H$ -module. If  $\alpha : H \rightarrow G$  is a homomorphism of groups and  $\beta : A \rightarrow B$  is a homomorphism of  $H$ -modules (using  $\alpha$  to regard  $B$  as an  $H$ -module) then we call  $(\alpha, \beta)$  a **homomorphism of pairs**, written

$$(\alpha, \beta) : (G, A) \rightarrow (H, B).$$

Let  $G \subset H$  be groups and  $A$  an  $H$ -module (so, by restriction, a  $G$ -module). We say a map

$$f_{G,H} : H^n(G, A) \rightarrow H^n(H, A),$$

is **transitive** if  $f_{G_2, G_3} f_{G_1, G_2} = f_{G_1, G_3}$ , for all subgroups  $G_1 \subset G_2 \subset G_3$ .

Let  $X_*$  be a  $G$ -resolution and  $X'_*$  a  $H$ -resolution, each with a  $-1$  grading. Associated to a homomorphism of groups  $\alpha : H \rightarrow G$  is a sequence of  $H$ -homomorphisms

$$A_n : X'_n \rightarrow X_n, \tag{12}$$

$n \geq 0$ , such that  $d_{n+1} A_{n+1} = A_n d'_{n+1}$  and  $\epsilon A_0 = \epsilon'$ .

### Theorem 7.1.

(1) If  $(\alpha, \beta) : (G, A) \rightarrow (G', A')$  and  $(\alpha', \beta') : (G', A') \rightarrow (G'', A'')$  are homomorphisms of pairs then so is  $(\alpha' \circ \alpha, \beta' \circ \beta) : (G, A) \rightarrow (G'', A'')$ .

30 *D. Joyner*

(2) Suppose  $(\alpha, \beta) : (G, A) \rightarrow (G', A')$  is homomorphism of pairs,  $X_*$  is a  $G$ -resolution, and  $X'_*$  is a  $G'$ -resolution (each infinite in both directions, with a  $-1$  grading). Let  $H^n(G, A, X_*)$  denote the derived groups associated to the differential groups  $\text{Hom}_G(X_*, A)$  with  $+1$  grading. There is a homomorphism

$$(\alpha, \beta)_{X_*, X'_*} : H^n(G, A, X_*) \rightarrow H^n(G', A', X'_*)$$

satisfying the following properties.

- (a) If  $G = G'$ ,  $A = A'$ ,  $X = X'$ ,  $\alpha = 1$  and  $\beta = 1$  then  $(1, 1)_{X_*, X'_*} = 1$ .  
 (b) If  $(\alpha', \beta') : (G', A') \rightarrow (G'', A'')$  is homomorphism of pairs,  $X''_*$  is a  $G''$ -resolution then

$$(\alpha' \circ \alpha, \beta' \circ \beta)_{X_*, X''_*} = (\alpha', \beta')_{X'_*, X''_*} \circ (\alpha, \beta)_{X_*, X'_*}.$$

- (c) If  $(\alpha, \gamma) : (G, A) \rightarrow (G', A')$  is homomorphism of pairs then

$$(\alpha, \beta + \gamma)_{X_*, X'_*} = (\alpha, \beta)_{X_*, X'_*} + (\alpha, \gamma)_{X_*, X'_*}.$$

**Remark 7.1.** For an analogous result for homology, see §§III.8 in Brown [3].

**proof:** We sketch the proof, following Weiss, [21, Theorem 2.1.8, pp 52-53].

(1): This is “obvious”.

(2): Let  $(\alpha, \beta) : (G, A) \rightarrow (G', A')$  be a homomorphism of pairs. Using (12), we have an associated chain map

$$\alpha^* : \text{Hom}_G(X_*, A) \rightarrow \text{Hom}_{G'}(X'_*, A')$$

of differential groups (Brown §III.8 in [3]). The homomorphism of cohomology groups induced by  $\alpha^*$  is denoted

$$\alpha^*_{n, X_*, X'_*} : H^n(G, A, X_*) \rightarrow H^n(G', A', X'_*).$$

Properties (a)-(c) follow from §2.2 and the corresponding properties of  $\alpha^*$ .  
 $\square$

As the cohomology groups are independent of the resolution used, the map  $(\alpha, \beta)_{X_*, X'_*} : H^n(G, A, X_*) \rightarrow H^n(G', A', X'_*)$  is sometimes simply denoted by

$$(\alpha, \beta)_* : H^n(G, A) \rightarrow H^n(G', A'). \quad (13)$$

### 7.1. Restriction

Let  $X_* = X_*(G)$  denote the bar resolution.

If  $H$  is a subgroup of  $G$  then the cycles on  $G$ ,  $C^n(G, A) = \text{Hom}_G(X_n(G), A)$ , can be restricted to  $H$ :  $C^n(H, A) = \text{Hom}_H(X_n(H), A)$ . The restriction map  $C^n(G, A) \rightarrow C^n(H, A)$  leads to a map of cohomology classes:

$$\text{Res} : H^n(G, A) \rightarrow H^n(H, A).$$

In this case, the homomorphism of pairs is given by the inclusion map  $\alpha : H \rightarrow G$  and the identity map  $\beta : A \rightarrow A$ . The map  $\text{Res}$  is the induced map defined by (13). By the properties of this induced map, we see that  $\text{Res}_{H,G}$  is transitive: if  $G \subset G' \subset G''$  then

$$\text{Res}_{G',G} \circ \text{Res}_{G'',G'} = \text{Res}_{G'',G}.$$

(There is an analog of the restriction for homology which also satisfies this transitive property – see Proposition 9.5 in Brown [3].)

A particularly nice feature of the restriction map is the following fact.

**Theorem 7.2.** *If  $G$  is a finite group and  $G_p$  is a  $p$ -Sylow subgroup and if  $H^n(G, A)_p$  is the  $p$ -primary component of  $H^n(G, A)$  then*

- (a) *there is a canonical isomorphism  $H^n(G, A) \cong \bigoplus_p H^n(G, A)_p$ , and*
- (b)  *$\text{Res} : H^n(G, A) \rightarrow H^n(G_p, A)$  restricted to  $H^n(G, A)_p$  (identified with a subgroup of  $H^n(G, A)$  via (a)) is injective.*

**proof:** See Weiss, [21, Theorem 3.1.15].  $\square$

**Example 7.1.** Homology is a functor. That is, for any  $n > 0$  and group homomorphism  $f : G \rightarrow G'$  there is an induced homomorphism  $H_n(f) : H_n(G, \mathbb{Z}) \rightarrow H_n(G', \mathbb{Z})$  satisfying

- $H_n(gf) = H_n(g)H_n(f)$  for group homomorphisms  $f : G \rightarrow G'$   $g : G' \rightarrow G''$ ,
- $H_n(f)$  is the identity homomorphism if  $f$  is the identity.

The following commands compute  $H_3(f) : H_3(P, \mathbb{Z}) \rightarrow H_3(S_5, \mathbb{Z})$  for the inclusion  $f : P \hookrightarrow S_5$  into the symmetric group  $S_5$  of its Sylow 2-subgroup. They also show that the image of the induced homomorphism  $H_3(f)$  is precisely the Sylow 2-subgroup of  $H_3(S_5, \mathbb{Z})$ .

GAP

```
gap> S_5:=SymmetricGroup(5);; P:=SylowSubgroup(S_5,2);;
gap> f:=GroupHomomorphismByFunction(P,S_5, x->x);;
```

32 *D. Joyner*

```

gap> R:=ResolutionFiniteGroup(P,4);
gap> S:=ResolutionFiniteGroup(S_5,4);
gap> ZP_map:=EquivariantChainMap(R,S,f);
gap> map:=TensorWithIntegers(ZP_map);
gap> Hf:=Homology(map,3);
gap> AbelianInvariants(Image(Hf));
[2,4]
gap> GroupHomology(S_5,3);
[2,4,3]

```

If  $H$  is a subgroup of finite index in  $G$  then there is an analogous restriction map in group homology (see for example Brown [3, §III.9]).

## 7.2. Inflation

Let  $X_*$  denote the bar resolution of  $G$ . Recall

$$X_n = \bigoplus_{(g_1, \dots, g_n) \in G^n} R[g_1, \dots, g_n],$$

where the sum runs over all ordered  $n$ -tuples in  $G^n$ . If  $H$  is a subgroup of  $G$ , let  $X_*^H$  denote the complex defined by

$$X_n^H = \bigoplus_{(g_1 H, \dots, g_n H) \in (G/H)^n} R[g_1 H, \dots, g_n H].$$

This is a resolution, and we have a chain map defined on  $n$ -cells by  $[g_1, \dots, g_n] \mapsto [g_1 H, \dots, g_n H]$ .

Suppose that  $H$  is a normal subgroup of  $G$  and  $A$  is a  $G$ -module. We may view  $A^H$  as a  $G/H$ -module. In this case, the homomorphism of pairs is given by the quotient map  $\alpha : G \rightarrow G/H$  and the inclusion map  $\beta : A^H \rightarrow A$ . The **inflation** map  $\text{Inf}$  is the induced map defined by (13), denoted

$$\text{Inf} : H^n(G/H, A^H) \rightarrow H^n(G, A).$$

The **inflation-restriction sequence in dimension  $n$**  is

$$0 \rightarrow H^n(G/H, A^H) \xrightarrow{\text{Inf}} H^n(G, A) \xrightarrow{\text{Res}} H^n(H, A).$$

For a proof, see Weiss, [21, §3.4].

There an analog of this inflation-restriction sequence for homology.

We omit any discussion of transfer and Shapiro's lemma, due to space limitations.

*Acknowledgements:* I thank G. Ellis, M. Mazur and J. Feldvoss, P. Guillot for correspondence which improved the content of these notes.

## References

1. A. Adem, “Recent developments in the cohomology of finite groups,” Notices AMS, vol 44(1997)806-812. Available online at <http://www.ams.org/notices/199707/199707-toc.html>.
2. M. Bishop, The GAP package CRIME, available from <http://www.gap-system.org/Packages/crime.html>
3. K. Brown, **Cohomology of groups**, Springer-Verlag, 1982.
4. J. Carlson’s page: <http://www.math.uga.edu/~lvalero/cohointro.html>.
5. E. Cartan and S. Eilenberg, **Homological algebra**, Princeton Univ. Press, 1956.
6. S. Eilenberg, S. MacLane, “Relations between homology and homotopy groups,” Proc. Nat. Acad. Sci. U. S. A. 29 (1943). 155–158.
7. G. Ellis, The GAP package HAP 1.8.4, available from <http://www.gap-system.org/Packages/hap.html>.
8. —, “Computing group resolutions”, J. Symbolic Computation, 28 (2004), 1077-1118. available from <http://hamilton.nuigalway.ie/preprints.html>.
9. L. Evens, **The cohomology of groups**, Oxford Univ. Press, 1991.
10. The GAP Group, **GAP– Groups, Algorithms, and Programming, Version 4.3**, 2000 <http://www.gap-system.org/>.
11. R. Godement, **Topologie algébrique et théorie des faisceaux**, Hermann, 1958.
12. D. Green’s page: [http://www.math.uni-wuppertal.de/~green/Coho\\_v2/](http://www.math.uni-wuppertal.de/~green/Coho_v2/).
13. P. Guillot’s page: [http://www-irma.u-strasbg.fr/~guillot/research/cohomology\\_of\\_groups/index.html](http://www-irma.u-strasbg.fr/~guillot/research/cohomology_of_groups/index.html)
14. G. Hochschild, “Relative homological algebra,” Trans. Amer. Math. Soc. 82 (1956), 246–269.
15. G. Karpilovsky, **The Schur multiplier**, Oxford Univ. Press, 1987.
16. M. Röder, The GAP package HAPcryst, available from <http://www.gap-system.org/Packages/undep.html>.
17. J. Rotman, **Advanced modern algebra**, Prentice Hall, 2002.
18. J.-P. Serre, **Local fields**, Springer-Verlag, 1979.
19. S. Shatz, **Profinite groups, arithmetic, and geometry**, Princeton Univ. Press, 1972.
20. William Stein, *SAGE Mathematics Software (Version 2.9)*, The SAGE Group, 2007, <http://www.sagemath.org>.
21. E. Weiss, **Cohomology of groups**, Academic Press, 1969.

## Groups Universally Equivalent to Free Burnside Groups of Prime Exponent and a Question of Philip Hall

A. Gaglione

*Department of Mathematics  
U.S. Naval Academy  
Annapolis, MD 21402*

S. Lipschutz

*Department of Mathematics  
Temple University  
Philadelphia, PA 19122*

D. Spellman

*Department of Mathematics  
Temple University  
Philadelphia, PA 19122*

This paper proposes the Tarski Problem for free groups in a Burnside variety,  $\mathbf{B}_n$ , where  $n$  is a sufficiently large odd integer so that Adian's results hold. We note that just as in the case of absolutely free groups it is easy to show that the nonabelian free groups in  $\mathbf{B}_n$  for  $n$  as above are all universally equivalent.

### 1. Introduction

We bear in mind two problems which resisted solution for decades and succumbed only to the fresh attacks of supremely talented mathematicians. For our purposes we shall dub the questions (1) and (2) below as *The Tarski Problem* and *The Burnside Problem* respectively.

- (1) Are the nonabelian free groups elementarily equivalent?
- (2) Must the finitely generated nonabelian free Burnside groups of fixed finite exponent be finite?

Of course the answers to (1) and (2) are now known to be (1) yes and (2) no respectively. (1) was solved independently by Kharlampovich

and Myasnikov on the one hand and by Sela on the other. Kharlampovich and Myasnikov applied *algebraic geometry over groups* invented by G. Baumslag, Myasnikov and Remeslennikov while Sela invented *Diophantine geometry in groups* to solve the Tarski problem.

Let's focus on algebraic geometry over groups. By way of analogy let us consider a Noetherian integral domain  $R$ . The closed subsets in the *Zariski topology* on affine  $n$ -space over  $R$  are precisely the affine algebraic subsets. In order for the analog of this scenario to go through in groups the proper notions of domain and Noetherian had to be defined. One consequence of the correct definition of domain is that every nonabelian CSA group (See Section 3) is a domain. Since free groups are CSA, nonabelian free groups are domains. The correct notion of Noetherian is *equationally Noetherian* (See Section 6). Happily free groups are also equationally Noetherian. One felicitous consequence of this confluence of facts is the existence and uniqueness (in the usual sense) of the decomposition of a closed set into a finite union of irreducible affine algebraic subsets. (We need to reserve the word *variety* for an equational class in this paper.) While the groups free in the variety of all groups are elementarily equivalent (provided their rank exceeds 1) it is easy to see that the corresponding result is false for groups free in many other varieties. For example, one can distinguish the free nilpotent groups (of fixed class) of different finite ranks by first order sentences. Perhaps the variety of all groups is unique in this regard? Or is it!

We now turn our attention to Question (2). A negative answer was first provided by Adian who showed that, for all sufficiently large odd  $n$ , the nonabelian free groups in the variety  $\mathbf{B}_n$  determined by the law  $x^n = 1$  were all infinite. Soon afterward Sirvanjan proved that, just as in the variety of all groups, the free group of countably infinite rank in the variety  $\mathbf{B}_n$  embeds in its group free of rank 2 for all sufficiently large odd  $n$ . From this it easily follows that the nonabelian free groups in the varieties  $\mathbf{B}_n$ , for all sufficiently large fixed odd  $n$ , have the same universal theory in the sense of first order logic. For our purposes we can say the most when  $n = p$  is a sufficiently large prime. In any event, if  $n$  is a sufficiently large odd integer, the free groups in  $\mathbf{B}_n$  are CSA; hence, the nonabelian free groups in such varieties are domains. We do not know whether or not they are equationally Noetherian. The Tarski problem relativized to such  $\mathbf{B}_n$  will require new techniques for its solution. This paper provides some halting first steps and should be viewed as an invitation to our colleagues to ponder possible approaches.

## 2. Preliminaries

We let  $\omega$  be the first limit ordinal, which we identify with the first infinite cardinal  $\aleph_0$ . If  $H$  and  $G$  are groups we say that  $G$  is *H-inclusive* provided it contains a subgroup isomorphic to  $H$ ;  $G$  is *H-exclusive* provided it is not *H-inclusive*. For each positive integer  $n$ ,  $C_n$  shall be a group cyclic of order  $n$ . If  $G$  is a group and  $\mathbf{H}$  is a nonempty class of groups, then we say that  $\mathbf{H}$  *separates*  $G$  provided for every  $g \in G \setminus \{1\}$  there is a group  $H_g \in \mathbf{H}$  and a homomorphism  $\varphi_g : G \rightarrow H_g$  such that  $\varphi_g(g) \neq 1$ ; we say that  $\mathbf{H}$  *discriminates*  $G$  provided for every finite nonempty subset  $S \subseteq G \setminus \{1\}$  there is a group  $H_S \in \mathbf{H}$  and a homomorphism  $\varphi_S : G \rightarrow H_S$  such that  $\varphi_S(g) \neq 1$  for all  $g \in S$ . In the case  $\mathbf{H} = \{H\}$  is a singleton we say that  $H$  *separates* (discriminates)  $G$  for  $\mathbf{H}$  *separates* (discriminates)  $G$ . In the case that  $\mathbf{H}$  *separates* (discriminates)  $G$  by epimorphisms the language  $G$  is *residually* (*fully residually*)  $\mathbf{H}$  is sometimes used.

Let  $L_0$  be the first order language with equality containing a binary operation symbol  $\bullet$ , a unary operation symbol  $^{-1}$  and a constant symbol  $1$ . We remark that being first order means that the variables are interpreted as varying over individual elements of the domain of discourse - never over subsets nor functions. Thus an  $L_0$ -*structure* is a set  $G$  provided with a distinguished constant  $1 \in G$ , a unary operation  $G \rightarrow G$ ,  $g \mapsto g^{-1}$  and a binary operation  $G^2 \rightarrow G$ ,  $(g, h) \mapsto gh$ . A *universal sentence* of  $L_0$  is one of the form  $\forall \mathbf{x} \varphi(\mathbf{x})$  where  $\mathbf{x}$  is a tuple of distinct variables and  $\varphi(\mathbf{x})$  is a formula of  $L_0$  containing no quantifiers and containing free at most the variables in  $\mathbf{x}$ . A *law* in  $L_0$  is a universal sentence of the form  $\forall \mathbf{x}(s(\mathbf{x}) = t(\mathbf{x}))$  where  $\mathbf{x}$  is a tuple of distinct variables and  $s(\mathbf{x})$  and  $t(\mathbf{x})$  are terms of  $L_0$  containing at most the variables in  $\mathbf{x}$ . The model class of a set of laws of  $L_0$  is a *variety* of  $L_0$ -structures. The following three sentences are laws.

$$\begin{array}{ll} \gamma_1: \forall x_1, x_2, x_3((x_1 \bullet x_2) \bullet x_3 = x_1 \bullet (x_2 \bullet x_3)) & \text{Associative Law} \\ \gamma_2: \forall x(x \bullet 1 = x) & \text{Identity Law} \\ \gamma_3: \forall x(x \bullet x^{-1} = 1) & \text{Inverse Law} \end{array}$$

We shall refer to the set  $\{\gamma_1, \gamma_2, \gamma_3\}$  as *the group axioms*. The model class  $\mathbf{O}$  of the group axioms is *the variety of all groups*. Every variety under consideration in this paper shall be a subvariety of  $\mathbf{O}$ . If  $\gamma$  is the conjunction  $\gamma_1 \wedge \gamma_2 \wedge \gamma_3$  of the group axioms and  $\sigma$  and  $\tau$  are sentences of  $L_0$  then we shall say that  $\sigma$  and  $\tau$  are *equivalent modulo the group axioms* provided the sentence  $\gamma \rightarrow (\sigma \leftrightarrow \tau)$  is true. Every law in  $L_0$  is equivalent modulo the group axioms to one of the form  $\forall \mathbf{x}(w(\mathbf{x}) = 1)$  where  $\mathbf{x}$  is a tuple of distinct variables and  $w(\mathbf{x})$  is a word in at most the variables in  $\mathbf{x}$ . Henceforth we shall omit the universal quantifiers and abbreviate the law

$\forall \mathbf{x}(w(\mathbf{x}) = 1)$  as simply  $w(\mathbf{x}) = 1$ . From this point on we tacitly assume the group axioms. The *trivial variety*  $\mathbf{E}$ , determined by the law  $x = 1$ , is the isomorphism class of the one element group. All other varieties of groups are *nontrivial*. Every nontrivial variety  $\mathbf{V}$  of groups admits, for each cardinal  $r$ , groups free of rank  $r$  relative to  $\mathbf{V}$ . We adopt the notation  $F_r(\mathbf{V})$  for a fixed, but arbitrary, group free of rank  $r$  relative to  $\mathbf{V}$ . Any two such groups (for fixed  $\mathbf{V}$  and  $r$ ) are isomorphic.

**Convention:** If  $\mathbf{E}$  is the trivial variety and  $r$  is any cardinal, then  $F_r(\mathbf{E})$  is the trivial group 1.

If  $G$  and  $H$  are groups then we say that  $G$  *universally covers*  $H$  provided every universal sentence of  $L_0$  true in  $G$  is also true in  $H$ . Note that  $H \leq G$  is a sufficient condition for  $G$  to universally cover  $H$ . We say that  $G$  and  $H$  are *universally equivalent* or *have the same universal theory* and write  $G \equiv_{\forall} H$  provided  $G$  universally covers  $H$  and  $H$  universally covers  $G$ . An *existential sentence* of  $L_0$  is one of the form  $\exists \mathbf{x} \varphi(\mathbf{x})$  where  $\mathbf{x}$  is a tuple of distinct variables and  $\varphi(\mathbf{x})$  is a formula of  $L_0$  containing no quantifiers and containing free at most the variables in  $\mathbf{x}$ . A *primitive sentence* of  $L_0$  is an existential sentence of  $L_0$  equivalent modulo the group axioms to one of the form  $\exists \mathbf{x}(\wedge_j (u_j(\mathbf{x}) = 1) \wedge \wedge_k (v_k(\mathbf{x}) \neq 1))$  where  $\mathbf{x}$  is a tuple of distinct variables and the  $u_j(\mathbf{x})$  and  $v_k(\mathbf{x})$  are words in at most the variables in  $\mathbf{x}$ . Since the negation of a universal sentence of  $L_0$  is equivalent to an existential sentence of  $L_0$  and vice-versa  $G \equiv_{\forall} H$  may be paraphrased as asserting that every universal sentence and every existential sentence of  $L_0$  true in  $G$  is also true in  $H$  (and vice-versa). It is easy to see that if  $G_1 \equiv_{\forall} G \equiv_{\forall} G_2$ , then  $G_1 \leq H \leq G_2$  is a sufficient condition for  $G \equiv_{\forall} H$ . A somewhat more sophisticated sufficient condition is the following.  $H \leq G$  and every finite system

$$\begin{aligned} u_j(\mathbf{x}) &= 1, 1 \leq j \leq J \\ v_k(\mathbf{x}) &\neq 1, 1 \leq k \leq K \end{aligned}$$

of equations and inequations ( in finitely many variables  $\mathbf{x} = (x_1, \dots, x_n)$ ) which has a solution in  $G$  must also have a solution in  $H$ . To see that this is so observe that  $G$  universally covers  $H$ ; so, it will suffice to show that every existential sentence of  $L_0$  true in  $G$  must also be true in  $H$ . Now we may assume that the *matrix*  $\varphi(\mathbf{x})$  of the existential sentence  $\exists \mathbf{x} \varphi(\mathbf{x})$  is written in *disjunctive normal form* modulo the group axioms  $\vee_i (\wedge_j (u_{i,j}(\mathbf{x}) = 1) \wedge \wedge_k (v_{i,k}(\mathbf{x}) \neq 1))$ . The sentence is then equivalent to the disjunction  $\vee_i \exists \mathbf{x} (\wedge_j (u_{i,j}(\mathbf{x}) = 1) \wedge \wedge_k (v_{i,k}(\mathbf{x}) \neq 1))$  of primitive sentences. Since a disjunction is true provided at least one of the disjuncts is,

38 *A. Gaglione, S. Lipschutz, D. Spellman*

it suffices to prove that every primitive sentence of  $L_0$  true in  $G$  is also true in  $H$ ; hence, the sufficiency of the above criterion is established.

We say that two groups  $G$  and  $H$  are *elementarily equivalent* and write  $G \equiv H$  provided  $G$  and  $H$  satisfy the same sentences of  $L_0$ . A theorem of Vaught (Theorem 4 of Chapter 6, Section 38 in [G]) asserts that, if  $\mathbf{V}$  is any variety and  $r$  and  $s$  are infinite cardinals, then  $F_r(\mathbf{V}) \equiv F_s(\mathbf{V})$ . In particular,  $F_r(\mathbf{V}) \equiv_{\forall} F_s(\mathbf{V})$  when  $r$  and  $s$  are infinite.

Let  $n$  be a positive integer. The *Burnside variety*  $\mathbf{B}_n$  of exponent  $n$  is the variety of groups determined by the law  $x^n = 1$ . Adian proved that, for all sufficiently large odd  $n$ ,

(B1)  $F_r(\mathbf{B}_n)$  is infinite for all  $r \geq 2$ ; moreover, every finite subgroup of  $F_r(\mathbf{B}_n)$  is cyclic.

and

(B2) The centralizer of every nontrivial element in  $F_r(\mathbf{B}_n)$  is cyclic for all  $r \geq 2$ .

Sirvanjan proved that, for all sufficiently large odd  $n$ ,

(B3)  $F_\omega(\mathbf{B}_n)$  embeds in  $F_2(\mathbf{B}_n)$ .

We shall call an integer  $n > 0$  an *Adian-Sirvanjan integer* provided (B1), (B2) and (B3) hold for  $\mathbf{B}_n$ . A prime Adian-Sirvanjan integer  $p$  shall be an *Adian-Sirvanjan prime*.

Every member  $G$  of a variety  $\mathbf{V}$  of groups is a homomorphic image of a group  $F_r(\mathbf{V})$  free in  $\mathbf{V}$ . If there is an epimorphism  $\psi : F_r(\mathbf{V}) \rightarrow G$  such that  $r$  is finite and  $\text{Ker}(\psi)$  is the normal closure in  $F_r(\mathbf{V})$  of finitely many elements of  $F_r(\mathbf{V})$ , then  $G$  is *finitely presented relative to*  $\mathbf{V}$ .

### 3. Varieties and Discrimination

We begin by remarking that, although we chose to live in the world of groups, the results of this section go through in the context of universal algebra.

Let  $\mathbf{V}$  be a nontrivial variety of groups. Let  $F_\omega(\mathbf{V})$  be a group free of countably infinite rank relative to  $\mathbf{V}$ . Suppose  $\{a_1, a_2, \dots\} = \{a_{n+1} : n < \omega\}$  freely generates  $F_\omega(\mathbf{V})$  relative to  $\mathbf{V}$ .

**Definition 3.1.** [N] A group  $G \in \mathbf{V}$  **discriminates**  $\mathbf{V}$  provided  $G$  discriminates  $F_\omega(\mathbf{V})$ .

Now  $G \in \mathbf{V}$  discriminates  $\mathbf{V}$  just in case, given finitely many elements

$$w_k(a_1, \dots, a_n) \neq 1$$

in  $F_\omega(\mathbf{V})$ , there is a homomorphism  $\psi : F_\omega(\mathbf{V}) \rightarrow G$  such that  $\psi(w_k(a_1, \dots, a_n)) \neq 1$  for all  $k$ . This is equivalent to the following. Given finitely many words  $w_k(x_1, \dots, x_n)$  such that none of the equations

$$w_k(x_1, \dots, x_n) = 1$$

is a law in  $\mathbf{V}$ , there is a tuple  $(g_1, \dots, g_n) \in G^n$  such that  $w_k(g_1, \dots, g_n) \neq 1$  for all  $k$ .

**Convention:** *The trivial group 1 discriminates the trivial variety  $E$ .*

**Definition 3.2.** Let  $\mathbf{V}$  be a variety of groups.  $\mathbf{V}$  is **finitely discriminable** provided there is a finitely generated group  $G \in \mathbf{V}$  such that  $G$  discriminates  $\mathbf{V}$ .

**Lemma 3.1.**  *$\mathbf{V}$  is finitely discriminable if and only if there is a positive integer  $r$  such that  $F_r(\mathbf{V})$  discriminates  $\mathbf{V}$ .*

*Proof:* If  $G = F_r(\mathbf{V})$  discriminates  $\mathbf{V}$  for some integer  $r > 0$ , then  $\mathbf{V}$  is discriminated by an  $r$ -generator member; hence, it is finitely discriminable. Suppose  $\mathbf{V}$  is finitely discriminable. Suppose  $r$  is a positive integer and  $G = \langle b_1, \dots, b_r \rangle \in \mathbf{V}$  discriminates  $\mathbf{V}$ . Let  $F_r(\mathbf{V})$  be freely generated relative to  $\mathbf{V}$  by  $a_1, \dots, a_r$ . Then we get an epimorphism  $\psi : F_r(\mathbf{V}) \rightarrow G$ ,  $a_i \mapsto b_i$ ,  $1 \leq i \leq r$ .

Suppose that  $w_k(x_1, \dots, x_n)$  are finitely many words such that none of the equations  $w_k(x_1, \dots, x_n) = 1$  is a law in  $\mathbf{V}$ . Then there are elements  $g_i = u_i(b_1, \dots, b_r)$ ,  $1 \leq i \leq n$  in  $G$  such that  $w_k(u_1(b_1, \dots, b_r), \dots, u_n(b_1, \dots, b_r)) \neq 1$  for all  $k$ . It follows that  $w_k(u_1(a_1, \dots, a_r), \dots, u_n(a_1, \dots, a_r)) \neq 1$  in  $F_r(\mathbf{V})$  for all  $k$ . Hence,  $F_r(\mathbf{V})$  discriminates  $\mathbf{V}$ . ■

**Definition 3.3.** Let  $\mathbf{V}$  be a finitely discriminable variety of groups. Then  $\min\{1 \leq r < \omega : F_r(\mathbf{V}) \text{ discriminates } \mathbf{V}\}$  is the **index of discrimination** of  $\mathbf{V}$ . If  $m$  is the index of discrimination of  $\mathbf{V}$ , then

$$D(\mathbf{V}) = \{F_r(\mathbf{V}) : m \leq r < \omega\}.$$

**Theorem 3.1.** *[GS] Let  $\mathbf{V}$  be a finitely discriminable variety of groups. Let  $r \geq 1$  be a cardinal. Then  $F_r(\mathbf{V}) \equiv_{\mathbf{V}} F_s(\mathbf{V})$  for all cardinals  $s \geq r$  if and only if  $F_r(\mathbf{V})$  discriminates  $\mathbf{V}$ . In particular, if  $m$  is the index of discrimination of  $\mathbf{V}$ , then  $F_m(\mathbf{V}) \equiv_{\mathbf{V}} F_s(\mathbf{V})$  for all  $m \leq s \leq \omega$ .*

40 *A. Gaglione, S. Lipschutz, D. Spellman*

**Theorem 3.2.** *Let  $\mathbf{V}$  be a finitely discriminable variety of groups with index of discrimination  $m$ . Let  $G \in \mathbf{V}$  be  $F_m(\mathbf{V})$  inclusive. If  $D(\mathbf{V})$  discriminates  $G$ , then  $G \equiv_{\mathbf{V}} F_m(\mathbf{V})$ .*

*Proof:* Assume  $D(\mathbf{V})$  discriminates  $G$ . It will suffice to show that, if

$$\begin{aligned} u_j(x_1, \dots, x_n) &= 1 & 1 \leq j \leq J \\ v_k(x_1, \dots, x_n) &\neq 1 & 1 \leq k \leq K \end{aligned}$$

has a solution  $(g_1, \dots, g_n) \in G^n$ , then it has a solution over  $F_m(\mathbf{V})$ . Since  $D(\mathbf{V})$  discriminates  $G$  there is an integer  $r \geq m$  and a homomorphism  $\psi : G \rightarrow F_r(\mathbf{V})$  such that  $\psi(v_k(g_1, \dots, g_n)) \neq 1$  for all  $1 \leq k \leq K$ . It follows that the primitive sentence

$$\exists x_1, \dots, x_n (\wedge_j (u_j(x_1, \dots, x_n) = 1) \wedge \wedge_k (v_k(x_1, \dots, x_n) \neq 1))$$

is true in  $F_r(\mathbf{V})$ . But since  $F_r(\mathbf{V}) \equiv_{\mathbf{V}} F_m(\mathbf{V})$  the above primitive sentence must also be true in  $F_m(\mathbf{V})$ . Hence, the system has a solution over  $F_m(\mathbf{V})$ . ■

**Corollary 3.1.** *Let  $\mathbf{V}$  be a finitely discriminable variety of groups with index of discrimination  $m$ . Let  $G \in \mathbf{V}$  be finitely presented relative to  $\mathbf{V}$  and suppose that  $G$  is  $F_m(\mathbf{V})$  inclusive. Then  $G \equiv_{\mathbf{V}} F_m(\mathbf{V})$  if and only if  $D(\mathbf{V})$  discriminates  $G$ .*

*Proof:* One direction follows immediately from the theorem. Suppose  $G \in \mathbf{V}$  is finitely presented relative to  $\mathbf{V}$ , is  $F_m(\mathbf{V})$  inclusive and  $G \equiv_{\mathbf{V}} F_m(\mathbf{V})$ . Suppose  $\langle a_1, \dots, a_n; R_1, \dots, R_J \rangle_{\mathbf{V}}$  is a finite presentation of  $G$  relative to  $\mathbf{V}$ . Let  $w_k(a_1, \dots, a_n)$ ,  $1 \leq k \leq K$  be finitely many nontrivial elements of  $G$ . Then the primitive sentence

$$\exists x_1, \dots, x_n (\wedge_j (R_j(x_1, \dots, x_n) = 1) \wedge \wedge_k (w_k(x_1, \dots, x_n) \neq 1))$$

holds in  $G$ ; hence, it holds in  $F_m(\mathbf{V})$  and there is  $(b_1, \dots, b_n) \in F_m(\mathbf{V})^n$  such that

$$\begin{aligned} R_j(b_1, \dots, b_n) &= 1 & 1 \leq j \leq J \\ w_k(b_1, \dots, b_n) &\neq 1 & 1 \leq k \leq K. \end{aligned}$$

It follows that the assignment  $a_i \mapsto b_i$ ,  $1 \leq i \leq n$  extends to a homomorphism  $\psi : G \rightarrow F_m(\mathbf{V})$  such that  $\psi(w_k(a_1, \dots, a_n)) \neq 1$ ,  $1 \leq k \leq K$ . ■

#### 4. The Variety $\mathbf{O}$ of All Groups

In this section we merely review known results about universally free groups (see Definition 4.1). These results will be contrasted later with results for the groups  $G \equiv_{\forall} F_2(\mathbf{B}_p)$  where  $p$  is an Adian-Sirvanjan prime. If  $\mathbf{O}$  is the variety of all groups and  $r \geq 1$  is a cardinal, then we write  $F_r$  for  $F_r(\mathbf{O})$ .  $F_\omega$  embeds in  $F_2$ . For example, the commutator subgroup  $[F_2, F_2]$  of  $F_2$  is free of countably infinite rank. Now let  $2 \leq r \leq \omega$ . Then  $F_\omega \cong [F_2, F_2] \leq F_r \leq F_\omega$  from which it follows that  $F_r \equiv_{\forall} F_s$  for all cardinals  $2 \leq r < s$ . Thus 2 is the index of discrimination of  $\mathbf{O}$ . The universal equivalence of the nonabelian free groups suggests the possibility of their elementary equivalence. Of course their universal equivalence is a far cry from their elementary equivalence.

Suppose  $R$  is a commutative ring with 1. Within the category of unital  $R$ -modules an object  $P$  is *projective* just in case every short exact sequence

$$0 \rightarrow N \rightarrow M \rightarrow P \rightarrow 0$$

splits. This is easily seen to be equivalent to  $P$  being a direct summand in a free  $R$ -module. Now suppose  $\mathbf{V}$  is a variety of groups. We define a group  $P \in \mathbf{V}$  to be *projective* relative to  $\mathbf{V}$  provided every short exact sequence of groups in  $\mathbf{V}$ ,

$$1 \rightarrow K \rightarrow G \rightarrow P \rightarrow 1,$$

splits. Essentially the same proof shows that this is equivalent to  $P$  being a retract of a group free in  $\mathbf{V}$ . By the Nielsen-Schreier subgroup theorem, a group  $P$  is projective relative to the variety of all groups if and only if it is free. The Nielsen-Schreier subgroup theorem also implies that a group is freely separated (discriminated) if and only if it is residually (fully residually) free. Suppose  $G$  is a nonabelian residually free group. Suppose  $gh \neq hg$  in  $G$ . Then their commutator  $[g, h] = g^{-1}h^{-1}gh$  is nontrivial. Thus, there is a free group  $F_r$  and an epimorphism  $\psi : G \rightarrow F_r$  such that  $[\psi(g), \psi(h)] = \psi([g, h]) \neq 1$ . Hence,  $F_r$  is nonabelian and  $r \geq 2$ . Since  $F_r$  is projective it is a retract in  $G$  and  $F_2 \leq F_r \leq G$ ; so,  $G$  is  $F_2$ -inclusive. Nonabelian free groups, of course, satisfy the existential sentence  $\exists x, y(xy \neq yx)$ . Other properties of nonabelian free groups are that they are CT and even CSA. Here a group is *CT* or *commutative transitive* provided the centralizers of nontrivial elements coincide with the maximal abelian subgroups. That is rendered by the universal sentence

$$\forall x, y, z((y \neq 1) \wedge (xy = yx) \wedge (yz = zy)) \rightarrow (xz = zx).$$

42 A. Gaglione, S. Lipschutz, D. Spellman

Moreover, a group is *CSA* or *conjugately separated abelian* provided maximal abelian subgroups are malnormal. That is equivalent to being CT and satisfying the universal sentence

$$\forall x, y, z(((x \neq 1) \wedge (xy = yx) \wedge (z^{-1}yzx = xz^{-1}yz)) \rightarrow (xz = zx)).$$

Free groups are CSA.

**Lemma 4.1.** [B] *A CT residually free group is CSA.*

*Proof:* Suppose  $G$  is CT and residually free. Let  $a \in G \setminus \{1\}$  and suppose  $b, g^{-1}bg \in C_G(a) = \{x \in G : ax = xa\}$ . Suppose to deduce a contradiction that  $g \notin C_G(a)$ . Then  $[g, a] \neq 1$ . Thus there is a free group  $F$  and an epimorphism  $\psi : G \rightarrow F$  such that  $[\psi(g), \psi(a)] = \psi([g, a]) \neq 1$ . But this is impossible. From  $[\psi(g), \psi(a)] \neq 1$  we have  $\psi(a) \neq 1$ . Moreover  $\psi(b), \psi(g)^{-1}\psi(b)\psi(g) \in C_F(\psi(a))$  and  $F$  is CSA. Hence,  $\psi(g)$  commutes with  $\psi(a)$  - a contradiction. Hence  $g \in C_G(a)$  and  $G$  is CSA. ■

**Theorem 4.1.** [B] *Let  $G$  be a nonabelian residually free group. The following three conditions are equivalent in pairs.*

- (1)  $G$  is fully residually free.
- (2)  $G$  is CT.
- (3)  $G$  is CSA.

*Proof:* Lemma 4.1 has already established the equivalence of (2) and (3). It will suffice to show that (1) and (2) are equivalent.

Suppose  $G$  is fully residually free. Let  $b \in G \setminus \{1\}$  and suppose  $a, c \in C_G(b)$ . Assume to deduce a contradiction that  $ac \neq ca$ . Then  $[a, c] \neq 1$ . Thus there is a free group  $F$  and an epimorphism  $\psi : G \rightarrow F$  such that  $\psi(b) \neq 1$  and  $[\psi(a), \psi(c)] = \psi([a, c]) \neq 1$ . But this is impossible.  $\psi(a)\psi(b) = \psi(b)\psi(a)$ ,  $\psi(b)\psi(c) = \psi(c)\psi(b)$  and  $F$  is CT; hence,  $\psi(a)\psi(c) = \psi(c)\psi(a)$  - a contradiction. Therefore  $ac = ca$  and  $G$  is CT.

Now suppose  $G$  is CT. The proof will proceed by induction on the cardinality  $n$  of  $S = \{g_1, \dots, g_n\} \subseteq G \setminus \{1\}$  no element of which is annihilated in a free homomorphic image. The result is true when  $n = 1$  since  $G$  is residually free. Now suppose  $n > 1$  and the result is true for all  $1 \leq k < n$ . Suppose first that  $S$  is not contained in an abelian subgroup of  $G$ . Then some pair of elements of  $S$ , which we may take to be  $g_{n-1}$  and  $g_n$ , does not commute. Thus  $T = \{g_1, \dots, g_{n-2}, [g_{n-1}, g_n]\}$  is contained in  $G \setminus \{1\}$  and, by inductive hypothesis, there is a free group  $F$  and an epimorphism

$\psi : G \rightarrow F$  such that  $\psi$  does not annihilate any element of  $T$ . But then  $\psi$  cannot annihilate any element of  $S$  either. It remains to treat the case where the  $g_i$  commute in pairs, which hypothesis we now assume. Since  $G$  is a residually free CT group it is CSA by Lemma 4.1. We claim that there is some  $g \in G$  such that  $g^{-1}g_n g$  does not commute with  $g_{n-1}$ . Otherwise, since  $G$  is CSA,  $g_{n-1}$  would be central in  $G$ . But a nonabelian CT group must be centerless; so, we have arrived at a contradiction. The claim is established. Pick one such  $g$ . Hence  $U = \{g_1, \dots, g_{n-2}, [g_{n-1}, g^{-1}g_n g]\}$  is contained in  $G \setminus \{1\}$ . By inductive hypothesis there is a free group  $F$  and an epimorphism  $\psi : G \rightarrow F$  such that  $\psi$  does not annihilate any element of  $U$ . But then  $\psi$  cannot annihilate any element of  $S$  either. That completes the induction. ■

**Definition 4.1.** A group  $G \equiv_{\forall} F_2$  is **universally free**.

**Theorem 4.2.** [R] *A finitely generated group is universally free if and only if it is nonabelian and fully residually free.*

**Theorem 4.3.** [KM1] *A finitely generated fully residually free group is finitely presented.*

**Definition 4.2.** Let  $G$  be a CT group and let  $a \in G \setminus \{1\}$ . Let  $M = C_G(a)$ . Then the HNN-extension

$$\langle G, t; \text{rel}(G), t^{-1}mt = m, \forall m \in M \rangle$$

is a **free rank 1 centralizer extension of  $G$** .

The above construction preserves fully residually freeness. In particular, we have

**Theorem 4.4.** *If  $G_0$  is fully residually free then so is every free rank 1 centralizer extension of  $G_0$ .*

44 *A. Gaglione, S. Lipschutz, D. Spellman*

*Proof:* By Definition 4.2, we take  $b \in G_0 \setminus \{1\}$  and let  $M = C_{G_0}(b)$ . So that our free rank 1 centralizer extension of  $G_0$  is the group  $G$ ,

$$G = \langle G_0, t; \text{rel}(G_0), t^{-1}zt = z \ \forall z \in M \rangle.$$

Start off by viewing  $G$  as the amalgamated free product

$$G = G_0 *_M (M \times \langle t; \rangle).$$

We need to show that  $G$  is fully residually free. For that purpose let  $g_1, \dots, g_k$  be finitely many nontrivial elements of  $G$ . Using the normal form for free products with amalgamation (see [MKS]), we may write for each  $j = 1, \dots, k$

$$g_j = b_{0,j} t^{m_{1,j}} b_{1,j} \dots b_{N(j)-1,j} t^{m_{N(j),j}} z_j$$

where  $N(j) \geq 0$ ,  $b_{i,j} \in G_0 \setminus M$ ,  $m_{i,j} \in \mathbb{Z} \setminus \{0\}$ , and  $z_j \in M$ . Note that  $b_{i,j} \in G_0 \setminus M$  is equivalent to  $[b_{i,j}, b] \neq 1$ . Now since  $G_0$  is fully residually free, there is a free group  $F$  and an epimorphism  $\varphi : G_0 \rightarrow F$  such that  $[\varphi(b_{i,j}), \varphi(b)] = \varphi([b_{i,j}, b]) \neq 1$  for all  $i, j$ . This forces  $\varphi(b_{i,j}) \neq 1$  and  $\varphi(b) \neq 1$ .

Let  $C_F(\varphi(b)) = \langle u \rangle$ . Suppose that  $\varphi(z_j) = u^{e_j}$  for all  $j$ ,  $1 \leq j \leq k$ . Now for each positive integer  $n \in \mathbb{N}$ , we may define an extension  $\psi_n : G \rightarrow F$  of  $\varphi$  by  $\psi_n|_{G_0} = \varphi$ ,  $\psi_n(t) = u^n$ .

Now fix a  $j$ ,  $1 \leq j \leq k$ . Could we have  $\psi_n(g_j) = 1$  for infinitely many  $n \in \mathbb{N}$ ? Suppose to deduce a contradiction that there were infinitely many  $n \in \mathbb{N}$  such that  $\psi_n(g_j) = 1$ . Then

$$\varphi(b_{0,j}) u^{m_{1,j}n} \varphi(b_{1,j}) \dots \varphi(b_{N(j)-1,j}) u^{m_{N(j),j}n + e_j} = 1$$

for infinitely many values of  $n$ . But then by G. Baumslag's "Big Powers Lemma" (see Proposition 1 [GB]), we then conclude that

$$\varphi(b_{i,j}) u = u \varphi(b_{i,j})$$

for some  $i$ , with  $0 \leq i \leq N(j) - 1$ . Thus for that  $\varphi(b_{i,j})$  we must have that  $\varphi(b_{i,j}) \in C_F(u) = C_F(\varphi(b))$  and so  $[\varphi(b_{i,j}), \varphi(b)] = 1$ . This contradicts our choice of  $\varphi$ .

The above contradiction shows that the set

$$S_j = \{n \in \mathbb{N} : \psi_n(g_j) \neq 1\}$$

is a cofinite subset of  $\mathbb{N}$  (i.e., its complement  $S'_j = \mathbb{N} \setminus S_j$  is finite). Since this is so for all  $j$ ,  $1 \leq j \leq k$ , we must have the finite intersection

$$S_1 \cap \dots \cap S_k \neq \emptyset.$$

(Note if  $S_1 \cap \dots \cap S_k$  were empty, then  $(S_1 \cap \dots \cap S_k)' = S_1' \cup \dots \cup S_k' = \mathbb{N}$  - which is impossible since  $S_1' \cup \dots \cup S_k'$  is a finite union of finite sets.)

Choose  $n \in S_1 \cap \dots \cap S_k$ . Then  $\psi_n(g_j) \neq 1$  for all  $j$  with  $1 \leq j \leq k$ . Hence  $G$  is fully residually free. ■

**Theorem 4.5.** [KM1] *A finitely generated group  $G$  is fully residually free if and only if there is a finite rank free group  $G_0$  and a finite sequence  $G_0 \leq G_1 \leq \dots \leq G_n$  of free rank 1 centralizer extensions such that  $G$  is isomorphic to a finitely generated subgroup of  $G_n$ .*

## 5. The Burnside Varieties

Let  $n$  be an Adian-Sirvanjan integer. Then  $F_\omega(\mathbf{B}_n)$  embeds in  $F_2(\mathbf{B}_n)$ . So, if  $2 \leq r \leq \omega$ , then  $F_2(\mathbf{B}_n)$  embeds in  $F_r(\mathbf{B}_n)$  which, in turn, embeds in  $F_2(\mathbf{B}_n)$ . It follows that  $F_r(\mathbf{B}_n) \equiv_{\forall} F_2(\mathbf{B}_n)$  for all  $2 \leq r \leq \omega$ . Thus 2 is the index of discrimination of  $\mathbf{B}_n$ . Moreover, since the centralizer of every nontrivial element in  $F_r(\mathbf{B}_n)$  is cyclic, the relatively free groups  $F_r(\mathbf{B}_n)$  are CT. Now suppose that  $p$  is an Adian-Sirvanjan prime.

**Lemma 5.1.** *Suppose  $G \in \mathbf{B}_p$  and  $G$  is  $C_p \times C_p$  exclusive. If  $G$  is CT, then  $G$  is CSA.*

*Proof:* Suppose  $G \in \mathbf{B}_p$ ,  $G$  is  $C_p \times C_p$  exclusive and  $G$  is CT. Let  $a \in G \setminus \{1\}$ . Then  $C_G(a) = \langle a \rangle \cong C_p$ . Suppose  $g^{-1}bg \in \langle a \rangle$  for some  $1 \neq b \in \langle a \rangle$ . Since  $\langle a \rangle = \langle b \rangle$  we may assume  $b = a$ . Then  $g^{-1}ag = a^m$  and  $a = g^{-p}ag^p = a^{m^p}$ . But we may compute exponents modulo  $p$  and, by Fermat's Little Theorem,  $a^{m^p} = a^m$ . Therefore,  $a^m = a$  and  $g^{-1}ag = a$ . So  $g \in C_G(a) = \langle a \rangle$ . Hence,  $G$  is CSA. ■

**Corollary 5.1.** *The relatively free groups  $F_r(\mathbf{B}_p)$  are CSA.*

*Proof:* Since the centralizer of every nontrivial element is isomorphic to  $C_p$ , one has that  $F_r(\mathbf{B}_p)$  is CT and  $C_p \times C_p$  exclusive. ■

More generally, if  $n$  is any Adian-Sirvanjan integer, then the free groups  $F_r(\mathbf{B}_n)$  are CSA. To see that let  $G = F_r(\mathbf{B}_n)$  where  $r \geq 2$ . Let  $a \in G \setminus \{1\}$ . Let  $C_G(a) = \langle b \rangle$ . Suppose  $g^{-1}\langle b \rangle g$  intersects  $\langle b \rangle$  nontrivially. Since  $G$  is CT we must have, in that event,  $g^{-1}\langle b \rangle g = \langle b \rangle$ . Consider the subgroup  $H = \langle g, b \rangle \leq G$ . Observe  $\langle b \rangle$  is normal in  $H$  and the quotient  $H/\langle b \rangle$  is generated by the image of  $g$  - an element of finite order. Then  $|H| = |\langle b \rangle|[H : \langle b \rangle] < \infty$ .

46 A. Gaglione, S. Lipschutz, D. Spellman

Then  $H$  must be cyclic. But  $C_G(a) = \langle b \rangle \leq H$  is maximal cyclic. Hence,  $H = \langle b \rangle$  and  $g \in \langle b \rangle = C_G(a)$ . It follows that  $C_G(a)$  is malnormal in  $G$ . Hence,  $G$  is CSA.

**Theorem 5.1.** *Suppose  $G \in \mathbf{B}_p$  is CT and  $C_p \times C_p$  exclusive. If  $G$  is separated by  $D(\mathbf{B}_p)$ , then  $G$  is discriminated by  $D(\mathbf{B}_p)$ .*

*Proof:* The proof will be by induction on the cardinality  $n$  of  $S = \{g_1, \dots, g_n\} \subseteq G \setminus \{1\}$  no element of which is annihilated by a homomorphism into a group free in  $\mathbf{B}_p$ . We have the result for  $n = 1$  since  $G$  is separated by  $D(\mathbf{B}_p)$ . Now suppose  $n > 1$  and the result is true for all  $k$  with  $1 \leq k < n$ . Assume first that  $S$  is contained in an abelian subgroup of  $G$ . Then  $\langle g_1 \rangle = \dots = \langle g_n \rangle \cong C_p$  and so  $g_i = g_1^{m_i}$  where  $p$  does not divide  $m_i$  for  $2 \leq i \leq n$ . Now, since  $D(\mathbf{B}_p)$  separates  $G$ , there is  $r \geq 2$  and a homomorphism  $\psi : G \rightarrow F_r(\mathbf{B}_p)$  such that  $\psi(g_1) \neq 1$ . But then  $\psi(g_i) = \psi(g_1)^{m_i} \neq 1$  for all  $2 \leq i \leq n$ . Hence,  $\psi$  does not annihilate any element of  $S$ . Now suppose at least one pair of elements of  $S$  does not commute. We may assume that  $g_{n-1}$  and  $g_n$  do not commute. Then  $T = \{g_1, \dots, g_{n-2}, [g_{n-1}, g_n]\}$  is contained in  $G \setminus \{1\}$ . By inductive hypothesis there is  $r \geq 2$  and a homomorphism  $\psi : G \rightarrow F_r(\mathbf{B}_p)$  such that  $\psi$  does not annihilate any element of  $T$ . But then  $\psi$  does not annihilate any element of  $S$  either. That completes the induction. ■

Observe that, since  $F_2(\mathbf{B}_p)$  satisfies the universal sentence

$$\forall x, y(((x \neq 1) \wedge (xy = yx)) \rightarrow \bigvee_{k=0}^{p-1} (y = x^k)),$$

every group  $G \equiv_{\forall} F_2(\mathbf{B}_p)$  is  $C_p \times C_p$  exclusive. More generally, if  $n$  is any Adian-Sirvanjan integer and

$$G \equiv_{\forall} F_2(\mathbf{B}_n),$$

then, for every  $g \in G \setminus \{1\}$ , one has that  $C_G(g)$  is cyclic. To see that consider the universal sentences

$$\begin{aligned} \text{(u1)} \quad & \forall x_1, x_2((x_1 x_2 = x_2 x_1) \rightarrow \bigvee_{0 \leq k_1, k_2, m_1, m_2 < n} ((x_1 = (x_1^{m_1} x_2^{m_2})^{k_1}) \wedge \\ & (x_2 = (x_1^{m_1} x_2^{m_2})^{k_2})) \text{ and} \\ \text{(u2)} \quad & \forall x_1, \dots, x_{n+1}(\bigwedge_{i < j} (x_i x_j = x_j x_i) \rightarrow \bigvee_{i < j} (x_i = x_j)). \end{aligned}$$

Both hold in  $F_2(\mathbf{B}_n)$  since every abelian subgroup of  $F_2(\mathbf{B}_n)$  is cyclic of order at most  $n$ . Hence they both hold in  $G$ . (u1) asserts that every abelian

subgroup is locally cyclic and (u2) asserts that every abelian subgroup has at most  $n$  elements.

Suppose that  $n$  is a composite Adian-Sirvanjan integer. Let  $1 < d < n$  be a divisor of  $n$ . Let  $B$  be freely generated in  $\mathbf{B}_n$  by  $\{a_1, a_2, a_3\}$  and let  $A$  be the subgroup generated (necessarily freely) by  $\{a_1, a_2\}$ . Let  $G$  be the subgroup of  $B$  generated by  $\{a_1, a_2, a_3^{\frac{n}{d}}\}$ . Since  $F_2(\mathbf{B}_n) = A \leq G \leq B = F_3(\mathbf{B}_n) \equiv_{\forall} F_2(\mathbf{B}_n)$  we have  $G \equiv_{\forall} F_2(\mathbf{B}_n)$ . But the finitely generated group  $G$  cannot be free in  $\mathbf{B}_n$  since its abelianization, isomorphic to  $C_n \times C_n \times C_d$ , has order  $n^2d$  which is not a power of  $n$ . For an Adian-Sirvanjan prime  $p$  are there any finitely generated  $G \equiv_{\forall} F_2(\mathbf{B}_p)$  which are not free in  $\mathbf{B}_p$ ? We ponder that question in the next section.

We conclude this section with a proof that cyclicity of finite subgroups is inherited by models of the universal and existential theory of the free Burnside groups.

**Theorem 5.2.** *Let  $n$  be an Adian-Sirvanjan integer and assume*

$$G \equiv_{\forall} F_2(\mathbf{B}_n).$$

*Then every finite subgroup of  $G$  is cyclic.*

*Proof:* For each positive integer  $N$  the universal sentence

$$\forall x_1, \dots, x_N (\wedge_{i \leq j} \vee_k (x_i x_j = x_k) \rightarrow \wedge_{i < j} (x_i x_j = x_j x_i))$$

holds in  $F_2(\mathbf{B}_n)$  since every finite subgroup is abelian. Thus every finite subgroup of  $G$  is abelian. But we have already seen that every abelian subgroup of such  $G$  is cyclic. ■

## 6. A Possible Non-Free Model and a Question of Philip Hall

If  $G$  is a group and  $H \leq G$  let  $H^G$  be the normal closure of  $H$  in  $G$ . If  $H, K \leq G$  let  $[H, K]$  be the subgroup generated by  $\{[h, k] : (h, k) \in H \times K\}$ . If  $G_1$  and  $G_2$  are groups let  $G_1 * G_2$  be their free product. Let  $\mathbf{V}$  be a variety of groups and  $G$  be a group. Let  $V(G)$  be the intersection of the family of subgroups  $K$  normal in  $G$  such that  $G/K \in \mathbf{V}$ . Then  $V(G)$ , the *verbal subgroup* of  $G$  corresponding to  $\mathbf{V}$ , is fully invariant in  $G$  and is the least normal subgroup  $K$  in  $G$  such that  $G/K \in \mathbf{V}$ . We define (following Hanna Neumann [N] and Magnus, Karrass, Solitar [MKS]) the *verbal product*  $G_1 *_{\mathbf{V}} G_2$  as  $\Gamma / ([G_1, G_2]^{\Gamma} \cap V(\Gamma))$  where  $\Gamma = G_1 * G_2$ .

48 *A. Gaglione, S. Lipschutz, D. Spellman*

If  $G_1, G_2 \in \mathbf{V}$  then  $G_1 *_{\mathbf{V}} G_2 \in \mathbf{V}$  and each of  $G_1$  and  $G_2$  embeds in  $G_1 *_{\mathbf{V}} G_2$ . Moreover  $*_{\mathbf{V}}$  restricted to groups in  $\mathbf{V}$  is the coproduct in  $\mathbf{V}$ . That means essentially that if  $G_1, G_2, G \in \mathbf{V}$  then every pair of homomorphisms  $\psi_i : G_i \rightarrow G$ ,  $i = 1, 2$ , uniquely determines a homomorphism

$$\psi : G_1 *_{\mathbf{V}} G_2 \rightarrow G.$$

Among other results one has that  $F_r(\mathbf{V})$  is the verbal product relative to  $\mathbf{V}$  of  $r$  copies of  $F_1(\mathbf{V})$ . Moreover, if  $G_1, G_2 \in \mathbf{V}$ , then each of  $G_1$  and  $G_2$  is a retract of  $G_1 *_{\mathbf{V}} G_2$ . We observe  $G_1$  is a retract since if  $\psi : G_1 *_{\mathbf{V}} G_2 \rightarrow G_1$  is the homomorphism determined by  $\psi_1 : G_1 \rightarrow G_1$  and  $\psi_2 : G_2 \rightarrow G_1$  where  $\psi_1$  is the identity automorphism and  $\psi_2$  is the trivial map  $\psi_2(x) = 1$  for all  $x$ , then  $\psi$  is a retraction from  $G_1 *_{\mathbf{V}} G_2$  onto  $G_1$ . Similarly  $G_2$  is a retract of  $G_1 *_{\mathbf{V}} G_2$ . Furthermore,  $G_1 *_{\mathbf{V}} G_2$  is generated by the embedded images of  $G_1$  and  $G_2$  and, if  $H_i \leq G_i$ ,  $i = 1, 2$ , then the subgroup  $\langle H_1, H_2 \rangle$  of  $G_1 *_{\mathbf{V}} G_2$  has the verbal product decomposition  $H_1 *_{\mathbf{V}} H_2$ .

Now let  $p$  be an Adian-Sirvanjan prime. Let  $*_p$  denote the verbal product with respect to the variety  $\mathbf{B}_p$  and let  $\mathbf{K}_p$  be the Kostrikin variety of locally finite groups satisfying the law  $x^p = 1$ . Let  $\kappa_p$  be the verbal subgroup operator corresponding to  $\mathbf{K}_p$ . Suppose  $r \geq 2$  is finite. Then  $F_r(\mathbf{K}_p) = F_r(\mathbf{B}_p)/\kappa_p(F_r(\mathbf{B}_p))$  is a finite group. Since  $\kappa_p(F_r(\mathbf{B}_p))$  has finite index in the finitely generated group  $F_r(\mathbf{B}_p)$  it must itself be finitely generated. However,  $\kappa_p(F_r(\mathbf{B}_p))$  is perfect (i.e. it coincides with its commutator subgroup). Therefore it cannot be free in  $\mathbf{B}_p$ . This is so since the abelianization of  $F_d(\mathbf{B}_p)$  for any cardinal  $d \geq 1$  is a vector space of dimension  $d$  over the  $p$  element field. Now let  $F = F_4(\mathbf{B}_p)$  be freely generated relative to  $\mathbf{B}_p$  by  $a_1, a_2, a_3$  and  $a_4$ . Let  $A$  be the subgroup generated (necessarily freely) by  $a_3$  and  $a_4$  and let  $B$  be the subgroup generated (necessarily freely) by  $a_1$  and  $a_2$ . Let  $C = \kappa_p(A)$  so that  $C$  is finitely generated and perfect.  $F = B *_p A$ . Consider the subgroup  $G = \langle B, C \rangle = B *_p C$ . Now  $F_2(\mathbf{B}_p) = B \leq G \leq F = F_4(\mathbf{B}_p) \equiv_{\mathbf{V}} F_2(\mathbf{B}_p)$ . It follows that the finitely generated group  $G$  is universally equivalent to  $F_2(\mathbf{B}_p)$ . Observe that, if  $G$  were free in  $\mathbf{B}_p$ , then the retract  $C$  of  $G$  would be projective relative to  $\mathbf{B}_p$ .

Here we observe a connection with Problem 21 of [N], which problem is attributed to Philip Hall. The question posed is the following. Suppose  $\mathbf{V}$  is a variety of groups of exponent zero or prime power. If  $P \in \mathbf{V}$  is projective relative to  $\mathbf{V}$  must  $P$  be free in  $\mathbf{V}$ ? Note that a positive answer to Philip Hall's question in the case of exponent an Adian-Sirvanjan prime would imply that  $G$  is not free in  $\mathbf{B}_p$ .

Kovács and Newman [KN] report that Philip Hall's question has a negative answer in the case of exponent zero; however, to the best of our knowledge the question remains open for prime power exponent. Other conditions would also imply that  $G$  is not free in  $\mathbf{B}_p$ . Suppose we define the Rank of a group to be the minimum cardinality of a set of generators. A consequence of the Grushko-Neumann Theorem asserts that  $\text{Rank}(G_1 * G_2) = \text{Rank}(G_1) + \text{Rank}(G_2)$ . Now  $C = C' \leq G'$  so  $G/G' \cong C_p \times C_p$ . If  $G$  were free it would have rank 2 and, since it is nonabelian,  $\text{Rank}(G) = 2$  also under the assumption of freeness. But, if it were the case that  $\text{Rank}(G_1 *_p G_2) = \text{Rank}(G_1) + \text{Rank}(G_2)$  for all  $G_1, G_2 \in \mathbf{B}_p$ , we would have  $\text{Rank}(G) = \text{Rank}(B) + \text{Rank}(C) = 2 + \text{Rank}(C)$  and  $\text{Rank}(C) > 0$  since  $C \neq 1$ . Thus, if the analog of the Grushko-Neumann corollary holds for  $\mathbf{B}_p$ , then  $G$  cannot be free in  $\mathbf{B}_p$ . Suppose the finite rank free groups  $F_r(\mathbf{B}_p)$ ,  $2 \leq r < \omega$  are Hopfian. As just argued, if  $G$  were free in  $\mathbf{B}_p$ , then  $\text{rank}(G) = 2$ . Say  $G$  were freely generated by  $b_1$  and  $b_2$ . Now let  $\psi : G \rightarrow G$  be the endomorphism determined by  $\psi_1 : B \rightarrow G$ ,  $\psi_2 : C \rightarrow G$  where  $\psi_1$  is the homomorphism determined by  $a_i \mapsto b_i$ ,  $i = 1, 2$ , and  $\psi_2$  is the trivial map  $\psi_2(x) = 1$  for all  $x$ . Then  $\psi$  is an epi-endomorphism with  $1 \neq C \leq \text{Ker}(\psi)$ . That would contradict the Hopf property. Hence, if the free groups  $F_r(\mathbf{B}_p)$ ,  $2 \leq r < \omega$  are Hopfian, then  $G$  cannot be free in  $\mathbf{B}_p$ . As far as we know it also is an open question as to whether or not these free groups  $F_r(\mathbf{B}_p)$  are Hopfian.

## 7. Questions

Let  $G$  be a group and let  $n$  be a positive integer. Let  $\langle x_1, \dots, x_n; \rangle$  be free on the  $n$  distinct elements  $x_1, \dots, x_n$ . Let  $w \in G * \langle x_1, \dots, x_n; \rangle$ . View the formal expression  $w = 1$  as an equation over  $G$  in the variables  $x_1, \dots, x_n$ . Now every assignment  $x_i \mapsto g_i \in G$ ,  $i = 1, \dots, n$ , extends to a unique retraction  $\psi : G * \langle x_1, \dots, x_n; \rangle \rightarrow G$ . Call the tuple  $(g_1, \dots, g_n) \in G^n$  a *solution to  $w = 1$*  provided  $w \in \text{Ker}(\psi)$ . For each subset  $S \subseteq G * \langle x_1, \dots, x_n; \rangle$ , let  $V_G(S) \subseteq G^n$  be the solution set to the system  $w = 1$ ,  $w \in S$  of equations.  $G$  is *equationally Noetherian* provided for every positive integer  $n$  and every subset  $S \subseteq G * \langle x_1, \dots, x_n; \rangle$  there is a finite subset  $S_0 \subseteq S$  such that  $V_G(S) = V_G(S_0)$ .

**Question 1:** *If  $n$  is an Adian-Sirvanjan integer and  $r \geq 2$  is an integer must  $F_r(B_n)$  be equationally Noetherian?*

50 A. Gaglione, S. Lipschutz, D. Spellman

**Question 2**(Philip Hall): *If  $V$  is a variety of groups of prime power exponent and  $P \in V$  is projective relative to  $V$  must  $P$  be free in  $V$ ?*

**Question 3:** *Suppose we define the Rank of a group to be the minimum cardinality of a set of generators. Let  $p$  be an Adian-Sirvanjan prime and let  $*_p$  be the coproduct in  $B_p$ . If  $G_1, G_2 \in B_p$  must  $\text{Rank}(G_1 *_p G_2) = \text{Rank}(G_1) + \text{Rank}(G_2)$ ?*

**Question 4:** *If  $p$  is an Adian-Sirvanjan prime and  $r \geq 2$  is an integer must  $F_r(B_p)$  be Hopfian?*

**Question 5:** *If  $n$  is an Adian-Sirvanjan integer and  $H \in \mathbf{B}_n$  is finitely generated and universally equivalent to  $F_2(\mathbf{B}_n)$  must  $H$  be embeddable in some  $F_r(\mathbf{B}_n)$ ?*

**Question 6:** *If  $n$  is an Adian-Sirvanjan integer and  $2 \leq r < s \leq \omega$  must  $F_r(B_n) \cong F_s(B_n)$ ?*

## 8. References

- [A] S.I. Adian, "Classification of periodic words and their application in group theory," *Springer Lecture Notes in Mathematics 806, Burnside Groups*, J.L. Mennicke, Editor, Springer-Verlag, Berlin (1980), 1 -40.
- [B] B. Baumslag, "Residually free groups," *Proc. London Math. Soc. (3)* 17 (1967), 402 - 418.
- [GB] G. Baumslag, "On generalised free products," *Math. Z.* 78 (1962), 423-438.
- [BMR] G. Baumslag, A.G. Myasnikov and V.N. Remeslennikov, "Algebraic geometry over groups I. Algebraic sets and ideal theory," *J. Alg.* 219 (1999), 16 - 79.
- [G] G. Grätzer, *Universal Algebra*, Van Nostrand, Princeton (1968).
- [GS] A.M. Gaglione and D. Spellman, "The persistence of universal formulae in free algebras," *Bull. Austral. Math. Soc.* 36 (1987), 11 - 17.

- [K] A.I. Kostrikin, "The Burnside problem," *Izv. akad. Nauk. Ser. Mat.* 23 (1959), 3 - 34.
- [KM1] O. Kharlampovich and A.G. Myasnikov, "Irreducible affine varieties over a free group: II Systems in quasi-quadratic triangular form and description of residually free groups," *J. Alg.* 200 (1998), 517 - 570.
- [KM2] O. Kharlampovich and A.G. Myasnikov, "Tarski's problem about the elementary theory of free groups has a positive solution," *Electron. Res. Announc. Amer. Math. Soc.* 4 (December 1998), 101 - 108.
- [KN] L.G. Kovács and M.F. Newman, "Hanna Neumann's problems on varieties of groups," *Springer Lecture Notes in Mathematics 372, Proc. Internat. Conf. Theory of Groups, Canberra* (1973), 417 - 431.
- [MKS] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Dover, Mineola (2004).
- [N] H. Neumann, *Varieties of Groups*, Springer - Verlag, New York (1967).
- [Ne] P.M. Neumann, "Splitting groups and projectives in varieties of groups," *Q. J. Maths (Oxford)* 18 (1967), 325 - 352.
- [R] V.N. Remeslennikov, " $\exists$ -Free groups," *Siberian J. Math.* 30 (6) (1989), 153 - 157.
- [Se] Z. Sela, "Diophantine geometry over groups VI: The elementary theory of a free group," *GAF*, in press.
- [Si] V.L. Sirvanjan, "Imbedding of the group  $B(\infty, n)$  in the group  $B(2, n)$ ," *Math. USSR-Izv.* 4 (1977), 181 - 199.

## Matrix Completions over Principal Ideal Rings

William H. Gustafson

*Department of Mathematics  
Texas Tech University  
Lubbock, Texas*

Donald W. Robinson

*Department of Mathematics  
Brigham Young University  
Provo, Utah*

R. Bruce Richter

*Department of Mathematics  
University of Waterloo  
Waterloo, Ontario*

William P. Wardlaw

*Department of Mathematics  
U.S. Naval Academy  
Annapolis, MD 21402*

*Dedicated to Anthony M. Gaglione on his sixtieth birthday and to the memory of William H. Gustafson.*

We show that if  $A$  is a  $k \times n$  matrix over a principal ideal ring  $R$ , with  $k < n$ , and if  $d$  is any element of the ideal generated by the  $k \times k$  minors of  $A$ , then  $A$  forms the top  $k$  rows of an  $n \times n$  matrix of determinant  $d$ . This parallels a 1981 result of Gustafson, Moore, and Reiner, and continues a program initiated by Hermite in 1849. Then we use these results to obtain an extension of a 1997 result of Richter and Wardlaw for good matrices.

## 1. Introduction

If  $A$  is a  $k \times n$  matrix with  $k < n$ , the matrix completion problem initiated by Hermite asks if  $A$  can be completed to an  $n \times n$  matrix with prescribed determinant  $d$ . Gustafson, Moore, and Reiner, at the beginning of [5], give a brief summary of the history of the problem of completing a  $k \times n$  matrix with  $k < n$  over certain commutative rings to an  $n \times n$  matrix over the same ring with appropriate determinant. They also include references to some of the principal players in this program initiated by Hermite in 1849. In our contribution below, we show in Theorem 1 that principal ideal rings are among the rings over which this matrix completion is always possible. Theorem 2 states the relationships between six properties of a  $k \times n$  matrix over a commutative ring. It extends a similar theorem in [9] by giving a best possible exposition of these relationships. Finally we show in Theorem 3 that if such completions are always possible over each ring in a given collection of rings, then they are also always possible over the unrestricted direct product of the collection.

Throughout this paper,  $R$  will denote a commutative ring with identity. If  $A$  is a  $k \times n$  matrix over  $R$  with  $k \leq n$ , then  $D_k(A)$  denotes the ideal of  $R$  generated by the  $k \times k$  subdeterminants of  $A$ . We say that  $A$  has *left block form* if  $A$  is equivalent over  $R$  to a matrix  $E = [L \ 0]$ , where  $L$  is a  $k \times (k + 1)$  matrix over  $R$  and  $0$  is the  $k \times (n - k - 1)$  zero matrix over  $R$ . That is, there are matrices  $P \in GL(k, R)$  and  $Q \in GL(n, R)$  such that  $PAQ = [L \ 0]$ . Note that if  $k = n - 1$  or  $k = n$ , the  $0$  block is missing and  $E = L$ ; indeed, we can take  $A = E = L$ .

## 2. Results

The following lemma was proved but not explicitly stated in [5], and was used to prove their main result. For the sake of completeness, we include a proof here.

**Lemma.** *Let  $A$  be a  $k \times n$  matrix over the commutative ring  $R$  with identity, let  $k < n$ , and let  $d \in D_k(A)$ . If  $A$  has left block form over  $R$ , then  $A$  enlarges to an  $n \times n$  matrix  $A^*$  over  $R$  whose determinant is  $d$  and whose top  $k$  rows form the matrix  $A$ .*

*Proof.* Let  $P \in GL(k, R)$  and  $Q \in GL(n, R)$  be such that  $PAQ = E = [L \ 0]$ , where  $L$  is  $k \times (k + 1)$ . Clearly,  $D_k(A) = D_k(E) = D_k(L)$ . Let

54 *W. H. Gustafson, D. W. Robinson, R. B. Richter, W. P. Wardlaw*

$c_j = (-1)^{k+1+j} \det(L_j)$ , where  $L_j$  is the  $k \times k$  submatrix of  $L$  obtained by deleting the  $j$ th column of  $L$ . Thus we can write  $d \in D_k(A)$  as a linear combination  $d = \sum a_j c_j = \det(L^*)$ , where  $L^*$  is the  $(k+1) \times (k+1)$  matrix obtained from  $L$  by adding  $[a_1 \ a_2 \ \cdots \ a_{k+1}]$  as its last row. Let  $p = \det(P)$  and  $q = \det(Q)$ , and multiply the last row of  $L^*$  by the unit  $pq$  to obtain the matrix  $M^*$  with  $\det(M^*) = pdq$ . Now let  $E^*$  be the direct sum of  $M^*$  and the  $(n-k-1) \times (n-k-1)$  identity matrix  $I_{n-k-1}$ ; thus,

$$E^* = \begin{bmatrix} M^* & 0 \\ 0 & I_{n-k-1} \end{bmatrix} = \begin{bmatrix} E \\ F \end{bmatrix}$$

is an  $n \times n$  matrix over  $R$  with  $\det(E^*) = pdq$  whose first  $k$  rows form the matrix  $E = PAQ$ . It follows that the matrix

$$A^* = \begin{bmatrix} P^{-1} & 0 \\ 0 & I_{n-k-1} \end{bmatrix} E^* Q^{-1} = \begin{bmatrix} P^{-1} E Q^{-1} \\ F Q^{-1} \end{bmatrix} = \begin{bmatrix} A \\ A' \end{bmatrix}$$

has  $\det(A^*) = d$  and its first  $k$  rows form the matrix  $A$ .  $\square$

Our first main result is

**Theorem 1.** *Suppose that  $R$  is either a Dedekind domain or a principal ideal ring, and that  $A$  is a  $k \times n$  matrix over  $R$  with  $k < n$ . If  $d$  is any element of  $D_k(A)$ , then there is an  $n \times n$  matrix  $A^*$  over  $R$  with determinant  $\det(A^*) = d$  whose first  $k$  rows form the matrix  $A$ .*

*Proof.* In view of our lemma, we need only establish that  $A$  has a left block form over  $R$  for each of the two cases.

When  $R$  is a Dedekind domain, Theorem 1 is the main result of [5], where they proved a lemma that every  $k \times n$  matrix over a Dedekind domain  $R$  has a left block form over  $R$ . They comment that this lemma was established in a more general form by Levy [6] in 1972.

When  $R$  is a principal ideal ring, W. C. Brown shows in [2, Thm. 15.24, p. 194], that every matrix over  $R$  has a Smith normal form. When  $A$  is  $k \times n$  over  $R$  with  $k < n$ , its Smith normal form is a left block form for  $A$  over  $R$ .  $\square$

Since every principal ideal domain is also a Dedekind domain, Theorem 1 only extends the result of [5] when  $R$  is a principal ideal ring with nonzero divisors of zero.

We were especially interested in the connection between Theorem 1 and the 1997 result [9] regarding good matrices. In [9],  $R$  was a commutative

ring with identity and an  $r \times n$  matrix  $A$  over  $R$  was defined to be *left good* if, for every vector  $\mathbf{x}$  in  $R^{1 \times r}$ , the ideal  $(\mathbf{x}A)$  generated by the entries in the vector  $\mathbf{x}A$  is the same as the ideal  $(\mathbf{x})$  generated by the entries of the vector  $\mathbf{x}$ . Our lemma allows us to extend the Main Theorem of [9] to our second main result.

**Theorem 2.** *Consider the following statements about an  $r \times n$  matrix  $A$  over the commutative ring  $R$  with identity.*

- (1) *The rows of  $A$  extend to a basis of  $R^{1 \times n}$ .*
- (2)  *$A$  can be enlarged to a matrix  $A^* \in GL(n, R)$ .*
- (3)  *$A$  has a Smith normal form  $[I_r \ 0]$ .*
- (4)  *$A$  has a right inverse over  $R$ .*
- (5)  *$D_r(A) = R$ .*
- (6)  *$A$  is left good.*

*Then*

- (a) *The statements (1), (2), and (3) are equivalent over any commutative ring  $R$  with identity.*
- (b) *The statements (4), (5), and (6) are equivalent over any commutative ring  $R$  with identity.*
- (c) *The statement (3) implies the statement (4) but in general they are not equivalent.*
- (d) *If  $A$  has left block form then all six statements are equivalent.*

*Proof.* Theorem 2 (a), (b), and (c) was proved in [9], except for the implications  $(2) \Rightarrow (3)$  and  $(5) \Rightarrow (4)$ , and the fact that  $(4) \not\Rightarrow (3)$ .

The statement (2) means that there is an  $(n - r) \times n$  matrix  $A'$  over  $R$  and an  $n \times n$  matrix  $B^*$  over  $R$  such that

$$A^* = \begin{bmatrix} A \\ A' \end{bmatrix}$$

and  $A^*B^* = I$  is the  $n \times n$  identity matrix. But then it is clear that  $AB^* = [I_r \ 0]$  is a Smith normal form for  $A$ . That is,  $(2) \Rightarrow (3)$ .

The implication  $(5) \Rightarrow (4)$  is immediate from [8, Cor. I.28, p. 84]. However, for the sake of completeness we give the following elementary proof. If  $M$  is any  $m \times n$  matrix over  $R$  and  $\mathbf{v} = (c_1, \dots, c_r)$  a vector of column indices of  $M$ , so that  $1 \leq c_j \leq n$ , we let  $M(\mathbf{v})$  denote the  $m \times r$  submatrix of  $M$  whose  $j$ th column is the  $c_j$ th column of  $M$ . It is easy to see that if  $I_n$  is the  $n \times n$  identity matrix, then  $M(\mathbf{v}) = M I_n(\mathbf{v})$ . Now each

56 *W. H. Gustafson, D. W. Robinson, R. B. Richter, W. P. Wardlaw*

$r$ -subset  $\{c_1, \dots, c_r\}$  of  $\{1, 2, \dots, n\}$  with  $1 \leq c_1 < c_2 < \dots < c_r \leq n$  corresponds uniquely to a vector  $\mathbf{v} = (c_1, \dots, c_r)$ , and we can number these vectors (perhaps lexicographically)  $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_N$  with  $N = \binom{n}{r}$ . Let  $d_j = \det(A_j)$  with  $A_j = A(\mathbf{v}_j)$ . Then  $D_r(A) = R$  implies  $1 = \sum b_j d_j$  for scalars  $b_1, b_2, \dots, b_N$  in  $R$ . Now, for each  $j = 1, 2, \dots, N$ , let  $B_j$  be the  $n \times r$  matrix  $B_j = I_n(\mathbf{v}_j) \text{Adj}(A_j)$ , and let  $B$  be the  $n \times r$  matrix  $B = \sum b_j B_j$ . Then

$$\begin{aligned} AB &= \sum b_j AB_j = \sum b_j A I_n(\mathbf{v}_j) \text{Adj}(A_j) \\ &= \sum b_j A_j \text{Adj}(A_j) = \sum b_j d_j I_r = I_r \end{aligned}$$

and (4)  $A$  has a right inverse  $B$ . That is, (5)  $\Rightarrow$  (4).

The following example from [4], attributed to Kaplansky in [1, p. 7], shows that (4)  $\not\Rightarrow$  (3) in Theorem 2 (c), and hence the result of Theorem 2 (c) is the best possible. Let  $R$  be the ring of polynomials in  $x, y, z$  over the real numbers modulo the ideal generated by  $x^2 + y^2 + z^2 - 1$ . This is the ring of polynomial functions on the standard 2-sphere in 3-space. The  $1 \times 3$  matrix  $A = [x \ y \ z]$  has a right inverse  $A^T$ . If it had a Smith normal form  $[1 \ 0 \ 0]$ , then there would be a matrix  $Q \in GL(3, R)$  such that  $AQ = [1 \ 0 \ 0]$ . Assume such a  $Q$  exists with last column  $\mathbf{q} = [f \ g \ h]^T$ . Then  $A\mathbf{q} = xf + yg + zh = 0$  for all points on the 2-sphere. Thus  $\mathbf{q}$  provides a tangent vector field to the 2-sphere which, because of independence of the columns of  $Q$ , is never zero on the 2-sphere. But no such vector field exists, as is shown in [3, p. 70]. This contradiction shows (4)  $\not\Rightarrow$  (3). (In fact, the same argument shows directly that  $A$  does not have a left block form, since that would require an invertible  $Q$  with  $AQ = [u \ v \ 0]$ .) This completes the proof of Theorem 2 (a), (b), and (c).

To establish (d), we first observe that when  $r = n$ , the implication (4)  $\Rightarrow$  (2) is a tautology. Then we use our lemma to show that (5)  $\Rightarrow$  (2) when  $r < n$  and  $A$  has a left block form over  $R$ . It is clear from (5) that  $1 \in R = D_r(A)$ . By our lemma,  $A$  can be enlarged to a matrix  $A^*$  with determinant 1 when  $r < n$ . It is well known that a matrix over a commutative ring  $R$  with identity is invertible over  $R$  if and only if its determinant is a unit in  $R$ . (See [7, Thm. 50, p. 158].) Hence (5)  $\Rightarrow$  (2).  $\square$

We remark that if  $A$  is an  $(n-1) \times n$  matrix over  $R$ , then it is already in left block form, so statements (1) - (6) of Theorem 2 are equivalent. In particular, if  $A$  has a right inverse, then it extends to an  $n \times n$  matrix

which is invertible over  $R$ . (The latter was shown using an outer product argument in [9].)

Recall that in the proof of Theorem 1 we observed that if  $R$  was either a principal ideal ring or a Dedekind domain, then every  $r \times n$  matrix over  $R$  with  $r \leq n$  had a left block form. Thus we have the following corollary to Theorem 2.

**Corollary.** *If  $R$  is a principal ideal ring or a Dedekind domain, then statements (1) - (6) of Theorem 2 are equivalent.*

This corollary extends the Main Theorem of [9] from principal ideal rings to rings which are either principal ideal rings or are Dedekind domains. Our next theorem allows further extension of the class of rings for which certain properties mentioned above hold.

Let  $R$  be a commutative ring with identity. Then  $R$  has property **L** if every  $r \times n$  matrix  $A$  over  $R$  with  $r \leq n$  has a left block form over  $R$ .  $R$  has property **C** if every  $r \times n$  matrix  $A$  over  $R$  with  $r < n$  has, for each  $d \in D_r(A)$  an  $n \times n$  completion  $A^*$  with  $\det(A^*) = d$ .  $R$  has property **G** if statements (1) - (6) of Theorem 2 are equivalent for every  $r \times n$  matrix  $A$  over  $R$  with  $r \leq n$ . Note that **L**  $\Rightarrow$  **C**  $\Rightarrow$  **G**, by our Lemma and Theorem 2.

**Theorem 3.** *Let  $P$  be any one of the properties **L**, **C**, or **G**, and let  $R = \bigoplus_j R_j$  be the unrestricted direct sum of the commutative rings  $R_j$  ( $j \in J$ ), where each  $R_j$  has identity  $1_j$ . Then  $R$  has property  $P$  if and only if each  $R_j$  has property  $P$ .*

*Proof.* We consider  $R$  to be an internal direct sum, so each  $R_j$  is a subring and an ideal of  $R$ . For each  $a \in R$ ,  $a_j = a1_j$  denotes the projection of  $a$  into  $R_j$ ; we call  $a_j$  the  $j$ -component of  $a$ . Thus  $(a_j)_k = 0$  if  $j \neq k$  and  $(a_j)_j = a_j$  for all  $j, k \in J$ . If  $A$  is a matrix over  $R$ , then we let  $A_j = 1_j A$  be the matrix of the same size over  $R_j$  obtained by replacing each entry in  $A$  by its  $j$ -component. We write  $A'_j$  to denote a matrix chosen with entries in  $R_j$ , to distinguish it from the  $j$ -component  $A_j = 1_j A$  obtained from a matrix  $A$  already chosen with entries in  $R$ . In the proofs below, we will often define a matrix  $A$  over  $R$  by first specifying a matrix  $A'_j$  over  $R_j$  for each  $j \in J$ , and letting  $A$  be the matrix of the same size over  $R$  with  $j$ -component  $A_j = 1_j A = A'_j$ .

Now suppose that  $R$  has property **L** and that  $A'_j \in (R_j)^{r \times n}$  with  $r \leq n$ . Since  $A'_j \in R^{r \times n}$ , there are matrices  $P \in GL(r, R)$  and  $Q \in GL(n, R)$  such

58 *W. H. Gustafson, D. W. Robinson, R. B. Richter, W. P. Wardlaw*

that  $PA'_jQ = E = [L \ 0]$ , with  $L \in R^{r \times (r+1)}$ . But  $A'_j = 1_j A'$  implies that  $PA'_jQ = P(1_j A')Q = (1_j P)(A'_j)(1_j Q) = P_j A'_j Q_j = E = E_j = [L_j \ 0]$  with  $P_j \in GL(r, R_j)$  and  $Q_j \in GL(n, R_j)$ . Thus,  $R_j$  has property **L**.

On the other hand, suppose that for each  $j \in J$ ,  $R_j$  has property **L**, and that  $A \in R^{r \times n}$  with  $r \leq n$ . Then  $A_j \in (R_j)^{r \times n}$  for each  $j \in J$ , and so there are matrices  $P'_j \in GL(r, R_j)$  and  $Q'_j \in GL(n, R_j)$  such that  $P'_j A_j Q'_j = [L'_j \ 0]$  with  $L'_j \in (R_j)^{r \times (r+1)}$ . Let  $P \in R^{r \times r}$  be the matrix with  $j$ -component  $1_j P = P'_j$  and let  $Q \in R^{n \times n}$  be the matrix with  $j$ -component  $1_j Q = Q'_j$  for every  $j \in J$ . It is easy to see that  $P \in GL(r, R)$ ,  $Q \in GL(n, R)$ , and  $PAQ = [L \ 0]$  with  $L \in R^{r \times (r+1)}$  such that  $1_j L = L'_j$  for each  $j \in J$ . Thus,  $R$  has property **L**.

Now suppose that  $R$  has property **C** and that  $A'_j \in (R_j)^{r \times n}$  with  $r < n$  and  $d \in D_r(A'_j)$ . Since  $A'_j \in R^{r \times n}$ , there is an  $A^* \in R^{n \times n}$  whose first  $r$  rows form the matrix  $A'_j$  and with determinant  $\det(A^*) = d$ . But the first  $r$  rows of  $1_j A^* = (A^*)_j \in (R_j)^{n \times n}$  also form the matrix  $A'_j$  and  $\det((A^*)_j) = d = d_j$ . Thus,  $R_j$  has property **C**.

On the other hand, suppose that for each  $j \in J$ ,  $R_j$  has property **C**,  $A \in R^{r \times n}$  with  $r < n$ , and  $d \in D_r(A)$ . For each  $j \in J$ ,  $1_j A = A_j \in (R_j)^{r \times n}$  has  $1_j d = d_j \in D_r(A_j)$  and has an  $n \times n$  completion  $(A_j)^*$  over  $R_j$  with  $\det((A_j)^*) = d = d_j$ . Let  $A^*$  be the  $n \times n$  matrix over  $R$  with  $1_j A^* = (A^*)_j = (A_j)^*$  for each  $j \in J$ . Since  $\det((A^*)_j) = d_j$  for each  $j \in J$ , it follows that  $\det(A^*) = d$ . Since the first  $r$  rows of  $(A^*)_j$  form the matrix  $A_j$  for each  $j \in J$ , it follows that the first  $r$  rows of  $A^*$  form the matrix  $A$ . That is,  $A^*$  is the  $n \times n$  completion of  $A$  with determinant  $d$ . Hence,  $R$  has property **C**.

Suppose  $R$  has property **G** and that  $A'_j, (B'_j)^T \in (R_j)^{r \times n}$  satisfy  $A'_j B'_j = (I_r)_j$ , which is statement (4) of Theorem 3 for the ring  $R_j$ . Let  $E = [I_r \ 0] - [I_r \ 0]_j$ ,  $A = E + A'_j$ , and  $B = E^T + B'_j$ . Note that  $A_i = [I_r \ 0]_i$  if  $i \neq j$ ,  $A_j = A'_j$ , and similarly for  $B$ . Then  $AB = I_r$  shows that  $A$  satisfies (4) for the ring  $R$ . Since  $R$  has property **G**,  $A$  must also satisfy (2), so  $A$  has an invertible completion  $A^*$  over  $R$ . It follows that  $(A^*)_j \in GL(n, R_j)$  is the  $n \times n$  completion of  $A_j = A'_j$  over  $R_j$ . Thus, (4)  $\Rightarrow$  (2) in  $R_j$ , so  $R_j$  has property **G**.

Finally, suppose for each  $j \in J$  that  $R_j$  has property **G** and that  $A, B^T \in R^{r \times n}$  satisfy  $AB = I_r$ . Then  $A_j B_j = (I_r)_j$  for each  $j \in J$ , and so property **G** ensures that each  $A_j$  can be completed to an  $(A_j)^* \in GL(n, R_j)$ . Now let  $A^*$  be the  $n \times n$  matrix over  $R$  with  $j$ -component  $1_j A^* = (A^*)_j = (A_j)^*$ . Then  $A^* \in GL(n, R)$  and its first  $r$  rows form the matrix  $A$ . Thus (4)  $\Rightarrow$  (2) in  $R$ , so  $R$  has property **G**.  $\square$

**References**

1. H. Bass, *Introduction to some methods of algebraic K-theory*, CBMS 20, Amer. Math. Soc., Providence, RI, 1974.
2. W. C. Brown, *Matrices over Commutative Rings*, Dekker, New York, 1992.
3. M. J. Greenberg, *Lectures on Algebraic Topology*, W. A. Benjamin, New York, 1967.
4. W. H. Gustafson, P. R. Halmos, and J. M. Zelmanowitz, The Serre Conjecture, *Amer. Math. Monthly* **85** (1978), 357-359.
5. W. H. Gustafson, M. E. Moore, and I. Reiner, Matrix completions over Dedekind rings, *Linear and Multilinear Algebra* **10** (1981), 141-144.
6. L. S. Levy, Almost diagonal matrices over Dedekind domains, *Math. Z.* **124** (1972), 89-99.
7. N. H. McCoy, *Rings and Ideals*, Mathematical Association of America, Washington, 1965.
8. B. R. McDonald, *Linear Algebra over Commutative Rings*, Dekker, New York, 1984.
9. R. B. Richter and W. P. Wardlaw, Good matrices: matrices which preserve ideals, *Amer. Math. Monthly* **104** (1997), 932-938.