# Cohomology, Computations, and Commutative Algebra

*Jon F. Carlson*

Group cohomology has roots that go back to the early part of the last century. The topic has played a significant role in several mathematical areas such as number theory, algebraic topology, and representation theory. Yet only in the last decade, with the aid of modern computers, have many examples been calculated. The results of the calculations have provided insight into theoretical developments, and they have stimulated interest in a whole new collection of issues involving the structure of cohomology rings.

The cohomology ring $\mathrm{H}^*(G,k)$ of a finite group $G$ is a finitely generated algebra over its coefficients. We usually write it using generators and relations, as in

$$\mathrm{H}^*(G,k) \cong k[z,y,x]/(zy).$$

This example is the cohomology ring of a dihedral 2-group in the case that the coefficient ring $k$ is a field of characteristic 2. It is the quotient of the polynomial ring $k[z.y.x]$ by the ideal generated by $zy$. Hence it looks like the coordinate ring of the union of two planes (the $z$-$x$ plane and the $y$-$x$ plane) that intersect in a line.

Another example is the cohomology ring of a semidihedral 2-group. The semidihedral group of order 16 has the form

$$G = \langle g,h \,|\, g^8 = h^2 = 1, hgh = g^3\rangle.$$

Again, if $k$ is a field of characteristic 2, then its cohomology ring has the form

$$\mathrm{H}^*(G,k) = k[z,y,x,w]/(z^3,\ zy,\ zx,\ x^2 + y^2w).$$

It is interesting to notice in this case that the structure of the cohomology ring is independent of the order of the group. All semidihedral 2-groups have isomorphic mod 2 cohomology rings.

Other examples are more complicated. There is a group of order 128 whose cohomology ring (with coefficients in a field of characteristic 2) has the form

$$\mathrm{H}^*(G,k) = k[z,y,x,w,v,u,t,s]/\mathcal{I}$$

where $\mathcal{I}$ is the ideal generated by the polynomials

$$zy,\ \ y^2,\ \ z^3 + yx,\ \ zx + yx,\ \ yw,\ \ z^2v + zt,$$

$$x^2,\ \ yu,\ \ yt,\ \ z^2u + z^2t + xt,\ \ xu,$$

$$z^2w^2 + zvt + t^2,\ \ xw^2 + zvu + zvt + ut + t^2,$$

and

$$zwu + zvu + zvt + z^2s + u^2 + ut + t^2.$$

You have probably guessed that this last example is a computer calculation. The wonders of modern technology have permitted us to generate data on a scale that we could only have dreamed about thirty years ago. The output of other computer-generated examples can be found in the the book

*Jon F. Carlson is professor of mathematics at the University of Georgia, Athens. His email address is* jfc@math.uga.edu.

*This research was supported in part by a grant from the NSF.*

*The author thanks Lisa Townsley for suggestions on this paper.*

[10] or on the web page `http://www.math.uga.edu/~lvalero/cohointro.html`. Experimental evidence has aided the development of the subject, and it has also provoked some new problems. In this paper we discuss a few of the problems, show why they are important in a more general mathematical setting, and explore the connections to other areas of algebra and mathematics. In particular, the cohomology rings seem to have some very special properties which illustrate some basic concepts of commutative algebra.

The motivation for considering the cohomology rings of finite groups comes from two very different directions. To someone in algebraic topology, the cohomology ring $\mathrm{H}^*(G,k)$ is an example of the cohomology ring of a space. Specifically, it is the cohomology ring of the classifying space $BG$ of the group $G$. The classifying spaces of groups occupy an important place in modern homotopy theory. For example, Lannes [18] has shown that the mod $p$ cohomology rings for elementary abelian $p$-groups are injective modules over the Steenrod algebra of reduced power operations. Another direction is the study of modular representation theory of finite groups. It is a fact that the geometry associated to the cohomology ring controls and expresses much of the homological algebra of $kG$-modules.

There are several equivalent ways to define group cohomology. For one thing, it is the topological cohomology of the classifying space mentioned above. For an algebraist, the usual classical definition is stated in terms of projective resolutions and homomorphisms. This is also the definition that we have used in the computer experiments [9, 15]. That is, the algorithms for the computation follow the definition almost exactly.

In this exposition we delay the actual definition of the cohomology ring until the discussion of the computations in the section on Computing Group Cohomology. Instead, we concentrate on the properties of the cohomology rings and how these properties reflect the properties of the group. The discussion ends up being something of a primer in certain aspects of modern commutative algebra. Both the problems that we encounter and the questions that we want to answer are expressed in the language of commutative algebra and algebraic geometry. In addition, some of the tools we employ to analyze the experimental data are developments of modern commutative and noncommutative algebra.

Throughout the paper, $G$ denotes a finite group and $k$ a field. By a “cohomology ring” we mean a mod $p$ cohomology ring in which the field $k$ has finite characteristic $p$. Moreover, if $G$ is a $p$-group for some prime $p$, then it should be assumed that the field $k$ has characteristic $p$.

## Properties of Cohomology Rings

To begin, we outline some of the basic structure of cohomology rings. This structure is measured with notions such as dimension, depth, and prime ideal spectra. We review some of these ideas in the discussion.

### Graded Commutativity and Elementary Abelian Groups

A cohomology ring $\mathrm{H}^*(G,k)$ is a $k$-algebra and is graded in the sense that it is a direct sum

$$\mathrm{H}^*(G,k) \quad = \quad \sum_{n\geq 0} \mathrm{H}^n(G,k)$$

of vector spaces over the field $k$. The product respects degrees in that

$$\mathrm{H}^r(G,K)\cdot \mathrm{H}^s(G,k) \quad \subseteq \quad \mathrm{H}^{r+s}(G,k).$$

We say the ring is graded commutative because the elements of odd degree anticommute. That is, if $x$ is in degree $m$ and $y$ is in degree $n$, then $yx = (-1)^{mn}xy$. In particular, if the degree of $x$ is odd and the characteristic of the field $k$ is not 2, then $x^2 = 0$. An element is homogeneous provided it has a homogeneous degree, i.e., it is contained in $\mathrm{H}^r(G,K)$ for some $r$.

An important example to consider is the cohomology ring of an elementary abelian group of order $p^n$, $G \cong (\mathbb{Z}/p\mathbb{Z})^n$. This is an abelian group in which every nonidentity element has order $p$. The cohomology rings of these groups are as close as possible to actual polynomial rings. If $p = 2$, then $-1 = 1$ and $\mathrm{H}^*(G,k)$ is genuinely commutative. So we have that

$$\mathrm{H}^*(G,k) \quad \cong \quad k[z_1,\dots,z_n]$$

is actually a polynomial ring generated by elements in degree 1. If the characteristic of $k$ is $p > 2$, then the graded commutativity requires that the polynomial generators be in degree 2. Hence, $\mathrm{H}^*(G,k)$ has the form

$$\mathrm{H}^*(G,k) \quad \cong \quad k[y_1,\dots,y_n] \;\otimes\; \Lambda(z_1,\dots,z_n)$$

where $\Lambda$ is an exterior algebra. The generators $z_i$ are in degree 1, while the $y_i$ occur in degree 2. The elements $z_i$ are in every prime or maximal ideal of $\mathrm{H}^*(G,k)$, and therefore, they are contained in the Jacobson radical $\operatorname{Rad}\mathrm{H}^*(G,k)$ which is the intersection of all maximal ideals. It follows that $\mathrm{H}^*(G,k)/\operatorname{Rad}\mathrm{H}^*(G,k) \cong k[y_1,\dots,y_n]$ is a polynomial ring even in the case where $p$ is odd.

### Functorial Properties

Group cohomology is a functor. This is a complicated way of saying that homomorphisms of groups induce homomorphisms of group cohomology. In particular, suppose that $H \subseteq G$ is a subgroup. Then there is a homomorphism induced from the inclusion called the restriction,

$$\mathrm{res}_{G,H} : \mathrm{H}^*(G,k) \longrightarrow \mathrm{H}^*(H,k).$$

Moreover, if $H$ is a normal subgroup of $G$, then the quotient map $G \longrightarrow G/H$ induces a homomorphism called the inflation,

$$\mathrm{inf}_{G/H}^{G}:\ \mathrm{H}^*(G/H,k) \longrightarrow \mathrm{H}^*(G,k).$$

These maps have many nice features. For one, each is transitive. That is, for example, if $H \subseteq K \subseteq G$, then $\mathrm{res}_{K,H} \circ \mathrm{res}_{G,K} = \mathrm{res}_{G,H}$. In addition, both the restriction and inflation maps are homomorphisms of graded commutative $k$-algebras. That is, they are linear in $k$ and preserve both the gradings and product structures.

In general, the inflation map can have a large kernel and may be very far from being surjective. Likewise, a restriction map may have a large kernel. However, restriction maps must be nearly surjective. The way we say this is that $\mathrm{H}^*(H,k)$ must be finitely generated as a module over the image $\mathrm{res}_{G,H}(\mathrm{H}^*(G,k))$.

### Varieties and Quillen's Theorem

For the purposes of this section we assume that $k$ is algebraically closed. A very important theorem in group cohomology says that the cohomology rings are finitely generated. The theorem was proved independently by Evens [14] and Venkov [21] more than forty years ago. The theorem tells us in the case $p = 2$ that $\mathrm{H}^*(G,k) \cong P/\mathcal{I}$ where $P$ is a polynomial ring in a finite number of variables and $\mathcal{I}$ is an ideal in $P$. When $p$ is odd, the theorem implies that $\mathrm{H}^*(G,k)/\operatorname{Rad}\mathrm{H}^*(G,k)$ (which is a commutative ring) can be written as $P/\mathcal{I}$. This means that cohomology rings are noetherian and the maximal ideals can be classified by varieties. If $P$ is a polynomial ring in $n$ generators, then the variety of $P/\mathcal{I}$ is simply the set of simultaneous zeros of the polynomials that generated $\mathcal{I}$. In the case that $G$ is an elementary abelian subgroup of order $p^n$ as above, the variety of $\mathrm{H}^*(G,k)$ is the affine space $k^n$. We denote the variety of $\mathrm{H}^*(G,k)$ by $V_G(k)$. This is the maximal ideal spectrum of the ring. The points are the maximal ideals in $\mathrm{H}^*(G,k)$ and a subset of $V_G(k)$ is closed if it is the set of all maximal ideals that contain a particular ideal.

The functoriality of the preceding section extends naturally to the varieties. For example, if $H$ is a subgroup of $G$, then the restriction homomorphism induces a map on varieties

$$\mathrm{res}_{G,H}^*:\ V_H(k) \longrightarrow\ V_G(k).$$

The point is that if $\underline{\mathrm{m}}$ is a maximal ideal in $\mathrm{H}^*(H,k)$, then its inverse image $\{u \in \mathrm{H}^*(G,k) \mid \mathrm{res}_{G,H}(u) \in \underline{\mathrm{m}}\}$ is a maximal ideal in $\mathrm{H}^*(G,k)$. It should be noted that because $\mathrm{H}^*(H,k)$ is finitely generated over the image $\mathrm{res}_{G,H}(\mathrm{H}^*(G,k))$, the map $\mathrm{res}_{G,H}^*$ on varieties is finite-to-one. Now consider the dihedral group, mentioned at the beginning of the paper. The dihedral group of order 8 has a presentation in the form $G = \langle g,h \mid g^2 = h^2 = 1 = (gh)^4\rangle$. The group has a cyclic center generated by the element $e = (gh)^2$ and two maximal elementary abelian subgroups, $E = \langle g,e\rangle$ and $F = \langle h,e\rangle$. The cohomology rings of these two groups can be given as

$$\mathrm{H}^*(E,k)\ \cong\ k[u,v]\ \cong\ \mathrm{H}^*(F,k).$$

The restriction maps have the following form (with suitable choice of the variables). The restriction $\mathrm{res}_{G,E}$ sends $z,y,x$ to $0,u,v(u+v)$, respectively, while $\mathrm{res}_{G,F}$ sends $z,y,x$ to $u,0,v(u+v)$. The intersection of the kernels of the restrictions is thus the ideal $(zy) = \mathcal{I} \subseteq P = k[z,y,x]$. Hence there is no element in $\mathrm{H}^*(G,k) \cong P/\mathcal{I}$ that is in the kernel of both of these restrictions. The variety of $\mathrm{H}^*(G,k)$ is union of the $z$-$x$ and $y$-$x$ planes in $k^3$. The maps on varieties have the form

$$\mathrm{res}_{G,E}^*(a,b) = (0,a,b(a+b)),$$
$$\mathrm{res}_{G,F}^*(a,b) = (a,0,b(a+b)),$$

and hence we can calculate that $V_G(k)$ is the union of the images

$$V_G(k) = \mathrm{res}_{G,E}^*(V_E(k)) \cup \mathrm{res}_{G,F}^*(V_F(k)).$$

In fact, this is the situation in general. The following theorem was proved by Quillen more than thirty years ago.

***Theorem.*** *Let G be any finite group. Then*

$$V_G(k) = \bigcup_{E\in\mathcal{MEA}} \mathrm{res}_{G,E}^*(V_E(k))$$

*where the union is over the set $\mathcal{MEA}$ of all maximal elementary abelian $p$-subgroups of $G$.*

### Dimension

In general, the dimension of a ring or a variety is a fairly complicated notion. However, with Quillen's theorem in view, calculating the dimension of a cohomology ring is an easy exercise. Perhaps it is naive, but still it seems obvious that $k^n$ should have dimension $n$. Thus it would seem that dimension, called "Krull dimension", of the polynomial ring $k[x_1,\dots,x_n]$ should be $n$. All of this is correct, and moreover, Quillen's Theorem implies that the Krull dimension of $\mathrm{H}^*(G,k)$ is the largest integer $r$ such that $G$ has an elementary abelian subgroup of order $p^r$. This number is called the $p$-rank of $G$.

Usually the Krull dimension of a commutative ring $R$ is defined as the length $\ell$ of the longest strictly increasing chain

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_\ell \subset R$$

of proper prime ideals in $R$. Under the circumstances that we encounter, the Krull dimension is also the length of the longest sequence of algebraically independent elements in $R$. Such sequences are of particular concern to us in later sections.

## Depth and Detection

We saw in the last section that the Krull dimension of the cohomology ring $\mathrm{H}^*(G,k)$ is the $p$-rank of $G$. This is one of the consequences of Quillen's Theorem. In this section we consider another ring-theoretic invariant that seems to be only partly discernible from the group structure. We are speaking here of the depth of the cohomology ring. To define the depth of a ring, we first need the notion of a regular sequence.

### Depth and Regular Sequences

Suppose that $R$ is a finitely generated graded commutative $k$-algebra such as $\mathrm{H}^*(G,k)$. A regular sequence for $R$ is a sequence $u_1, u_2, \dots, u_r$ of homogeneous elements of positive degree having the following properties. First, $u_1$ should be a regular element, meaning that multiplication by $u_1$ is an injective map or that the annihilator of $u_1$ in $R$ is $\{0\}$. Then for each $2 \leq i \leq r$, we must have that $u_i$ is a regular element on the quotient ring $R/(u_1, \dots, u_{i-1})$. That is, multiplication by $u_i$ on the quotient ring is an injective homomorphism of $R$-modules. The definition of depth is the following.

**Definition.** The depth of a finitely generated graded commutative $k$-algebra $R$ is the length $r$ of the longest regular sequence of elements in $R$.

In fact, a sequence $u_1, \dots, u_r$ is regular if and only if the ring $R$ is a free module over the polynomial subring $k[u_1, \dots, u_r] \subseteq R$. Thus, if a sequence of elements in $R$ is regular, then any permutation of the elements in the sequence is also regular. Moreover, it can be proved that if $u_1, \dots, u_s$ is a regular sequence, then it can be extended to a regular sequence of maximal length.

For a ring such as a graded polynomial ring, the depth is again equal to the Krull dimension. That is, for the ring $k[z,y,x]$ the sequence $z,y,x$ is a regular sequence. Such rings are said to be Cohen-Macaulay. Certainly, the depth of any ring is never greater than the Krull dimension. However, the depth can be less than the Krull dimension, and this can happen for several reasons. An example to consider is the cohomology ring of the semidihedral group over a field of characteristic 2 as in the introduction. It has the form $\mathrm{H}^*(G,k) \cong k[z,y,x,w]/\mathcal{I}$ where $\mathcal{I}$ is the ideal generated by $z^3$, $zy$, $zx$ and $x^2 + y^2w$. Note that the generators $z,y,x,w$ are in degrees 1, 1, 3, and 4, so that the relation $x^2 + y^2w$ is homogeneous in degree 6. In this case, $\mathrm{H}^*(G,k)$ has depth 1 while its Krull dimension is 2. The point is that the annihilator of the element $z^2$ is the ideal $\mathfrak{A} = (z,y,x)$. Prime ideals that are the annihilators of elements in a ring are called associated primes for the ring. In this case an element of positive degree in $\mathrm{H}^*(G,k)$ is regular if and only if it is not contained in $\mathfrak{A}$. So no matter what regular element $u_1$ may be chosen for the first element in a regular sequence, the class of $z^2$ in $\mathrm{H}^*(G,k)/(u_1)$ will be annihilated by all elements of positive degree. Consequently, there is no regular sequence of length 2.

It is not difficult to prove that this situation happens in general. The depth of a commutative graded ring $R$ is never larger than the Krull dimension of $R/\mathfrak{p}$ where $\mathfrak{p}$ is any associated prime ideal.

On the other hand, the depth of a ring need not be controlled by the existence of associated primes. As an example, consider the subring $R$ of the polynomial ring $k[z,y]$ that is generated by the monomials $y, z^2, z^3, zy$. That is, $R$ is the subring of $k[z,y]$ consisting of all polynomials in which the coefficient on $z$ is zero. This time $R$ is an integral domain, because $k[z,y]$ is an integral domain. Hence, every element in $R$ is regular. But it is not possible to choose a regular sequence of length 2. For example, if we choose $y$ as the first element of the regular sequence, then the element $zy$ (which is *not* in the ideal $(y) \subseteq R$) is annihilated by every element of positive degree in $R/(y)$.

The depth is one of the ways in which the mod $p$ cohomology rings of finite groups are special. It is never the case that $\mathrm{H}^*(G,k)$ has depth 0. In fact, there is a theorem by Duflot [12] which says that the depth of a cohomology ring is at least as large as the $p$-rank of the center. Indeed, it can be shown that if $u_1, \dots, u_r$ is a sequence of homogeneous elements whose restriction to the center of a Sylow $p$-subgroup of $G$ is a regular sequence, then $u_1, \dots, u_r$ is a regular sequence.

In addition, for all the known computations of cohomology rings of finite groups, there is no example of a cohomology ring where the depth is not determined by the existence of an associated prime. In every case that we know of, there is a nonzero element $u$ in $\mathrm{H}^*(G,k)$ such that the annihilator $\mathfrak{p}$ of $u$ is a prime ideal with $\mathrm{H}^*(G,k)/\mathfrak{p}$ having Krull dimension equal to the depth of $\mathrm{H}^*(G,k)$. So we can ask if this is always the case.

**Question.** Does every cohomology ring $\mathrm{H}^*(G,k)$ have an associated prime $\mathfrak{p}$ such that the depth of $\mathrm{H}^*(G,k)/\mathfrak{p}$ coincides with the Krull dimension of $\mathrm{H}^*(G,k)$?

There are a few partial results. The answer is affirmative if the $p$-rank of $G$ is one [8]. The same happens if the depth is equal to the $p$-rank of the center of a Sylow $p$-subgroup of $G$ [16]. Beyond that, not much is known. Indeed, there does not seem to be much known about the class of rings with this property.

### Detecting Cohomology

The question raised above is not an idle one. It is intimately involved with at least one study that is central to many of the efforts to compute group cohomology. This is the question of detection of cohomology. We say that a collection $S$ of subgroups of $G$ detects the cohomology of $G$, provided the intersections of the kernels of the restriction maps to the subgroups in $S$ is zero:

$$\bigcap_{H\in S} \textbf{Kernel}(\mathrm{res}_{G,H} : \mathrm{H}^*(G,k) \longrightarrow \mathrm{H}^*(H,k)) = \{0\}.$$

We should point out that if $S$ is a Sylow $p$-subgroup of $G$, then the restriction map $\mathrm{res}_{G,S}$ is always injective. Consequently, any collection of subgroups that contains a Sylow subgroup or any subgroup that contains a Sylow subgroup is a detecting family.

We saw above that for $G$ a dihedral 2-group, the two elementary abelian subgroups detect the cohomology of $G$. On the other hand, for some $p$-groups there is no family of detecting subgroups of $G$ that does not include $G$ itself. An example is the quaternion group of order 8, which can be presented as

$$G = \langle g, h \mid g^2 = h^2, g^4 = 1, hgh^{-1} = g^{-1}\rangle .$$

Its cohomology ring has the form

$$\mathrm{H}^*(G,k) \cong k[z,y,x]/(z^2 + zy + y^2,\ z^2y + zy^2)$$

where the generators $z, y, x$ have degrees 1, 1, and 4. All of the subgroups of order 4 in $G$ are cyclic and the restriction of any element in degree 2 or any element in degree 3 in $\mathrm{H}^*(G,k)$ to any one of these subgroups is zero.

The existence of detecting families has certainly played a role in several complicated cohomology calculations (see, for example, [1]). The point is that if a detecting family is known, then the ideal of relations among the cohomology generators can be found by simply taking the intersection of the kernels of the restrictions to the members of the detecting family. It reduces the computational problem to finding the generators of cohomology and computing their restriction to the elements in the detecting family. This is often a big improvement over trying to compute the relations among the generators directly.

The connection between depth and detection comes from the following theorem [7].

***Theorem.*** *Suppose that the cohomology ring $\mathrm{H}^*(G,k)$ has depth $d$. Then the cohomology is detected on the centralizers of the elementary abelian $p$-subgroups of rank $d$.*

The question that often arises is the converse.

**Question.** Suppose that the cohomology of $G$ is detected on the centralizers of the elementary abelian $p$-subgroups of rank $r$. Is it necessary that the depth of $\mathrm{H}^*(G,k)$ be at least $r$?

Adem and Karagueuzian [2] have shown this to be true in the case that the rank of the center of a Sylow $p$-subgroup of $G$ coincides with the $p$-rank of $G$. The answer to the question is yes for all of the cohomology rings that we have computed.

## Computing Group Cohomology

In this section, we describe the computer calculations for cohomology. Embedded in the algorithms is the definition of group cohomology and the product structure. At the present time, there are at least two different implementations of the algorithms. The older implementation [8, 10] by the author and his collaborators relies almost entirely on linear algebra methods in the early stages of the computation. The newer implementation by David Green [15] uses noncommutative Gröbner bases. Green's programs run somewhat faster and (more importantly) are less extravagant with memory usage. The basic algorithms are the same for both systems. The first system is built into the computer algebra system MAGMA [6], while Greens's system is a stand-alone package.

The computer programs are designed to compute the cohomology rings only of $p$-groups. This is arguably the hardest problem, since the first step of most cohomology calculations is to compute the cohomology of the Sylow $p$-subgroup of the group. The main reasons for considering $p$-groups have more to do with the reality of computer capabilities. On the one hand, while the cohomology of $p$-groups is important, the groups are also small, and the projective modules are also small and easily constructible. The Mathieu group $M_{12}$ has 95,040 elements, but its Sylow subgroup has order 64 [3].

The other reason that makes the calculation of the cohomology of $p$-groups seem practical is that the group rings are local rings. If $G$ is a $p$-group and $k$ is a field of characteristic $p$, then in $kG$ we have that $(x-1)^{p^n} = x^{p^n} - 1 = 0$ for any element $x$ of order $p^n$ in $G$. So the augmentation ideal, which is the ideal spanned by all $x - 1$ for $x \in G$ is a nilpotent ideal of codimension 1 in $kG$. It is the radical of $kG$, and $kG/\operatorname{Rad}(kG) \cong k$. It follows from this fact that every projective $kG$-module is free and is isomorphic to a direct sum of copies of $kG$. Consequently, the projective modules are easy to construct on the computer.

For the rest of this section we assume that $G$ is a $p$-group and that $k$ is the prime field $k = \mathbb{F}_p$. Since only the characteristic of the field really matters, for computational purposes we use the smallest field possible.

### Projective Resolutions

The first step in the cohomology computation is the construction of a projective resolution for the trivial $kG$-module $k \cong kG/\operatorname{Rad}(kG)$. The projective resolution is an exact sequence of the form

$$\cdots \longrightarrow P_3 \xrightarrow{\partial_3} P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} k \longrightarrow 0$$

where each $P_i$ is a projective $kG$-module. In practice, we take a minimal resolution of $k$, meaning that $P_0 \cong kG$ and that for every $i$, $\partial(P_i) \subseteq \mathrm{Rad}(P_{i-1})$. This insures that in the induced complex

$$0 \longrightarrow \mathrm{Hom}_{kG}(P_0, k) \xrightarrow{\partial^*} \mathrm{Hom}_{kG}(P_1, k)$$
$$\xrightarrow{\partial^*} \mathrm{Hom}_{kG}(P_2, k) \xrightarrow{\partial^*} \dots$$

all of the maps are zero maps. The definition of the group cohomology is precisely the cohomology of this complex. That is, $\mathrm{H}^n(G, k) = \mathrm{H}^n(\mathrm{Hom}_{kG}(P_*, k))$, the $n^{\text{th}}$ cohomology group of this complex. Because we have used a minimal resolution, we have that $\mathrm{H}^n(G, k) = \mathrm{Hom}_{kG}(P_n, k) \cong (P_n / \mathrm{Rad}(kG)P_n)^*$, where the $(\ )^*$ indicates the $k$-dual.

The calculation of a typical map $P_n \xrightarrow{\partial_n} P_{n-1}$ in the projective resolution proceeds by reasonably easy steps. First, in order that the sequence be exact, the image of $\partial_n$ should be the kernel of $\partial_{n-1}$. So we compute the kernel $K_n$ of $\partial_{n-1}$. If we have represented $\partial_{n-1}$ as a matrix, then we are only computing a null space. Next, we find a basis for $\mathrm{Rad}(kG)K_n = \sum_{x \in G}(x-1)K_n$. Of course, in practice we need only to let the sum range over a set of generators for $G$. Third, we find a complementary basis $u_1, \dots, u_{t_n}$ for $\mathrm{Rad}(kG)K_n$ in $K_n$. Finally, we let $P_n$ be the direct sum of $t_n$ copies of $kG$ and construct $\partial_n$ as the map which takes the identity element 1 in the $i^{\text{th}}$ copy of $kG$ to the element $u_i \in K_n \subseteq P_{n-1}$.

Various time- and space-saving tricks are built into the program. For example, the spaces $K_n$ and $P_n$ are never constructed as actual $kG$-modules but rather are just $k$-vector spaces on which the action of an element $x \in G$ is determined by the multiplication of $x$ on $kG$.

### Products and Relations

There are several equivalent ways of defining the cup product structure on group cohomology. One method uses the Hopf algebra structure on $kG$ to construct a chain map $P_* \longrightarrow P_* \otimes_k P_*$. This method is not practical in the computational setting, because the tensor product resolution becomes too big too fast. Instead, we compute products by compositions of chain maps. The fact is that every homomorphism $\zeta \in \mathrm{Hom}_{kG}(P_n, k) = \mathrm{H}^n(G, k)$ lifts to a chain map $\{\zeta_*\} : P_* \longrightarrow P_*$ of degree $-n$ as in the commuting diagram

$$\begin{tikzcd}
\cdots \arrow[r] & P_{n+2} \arrow[r] \arrow[d, "\zeta_2"] & P_{n+1} \arrow[r] \arrow[d, "\zeta_1"] & P_n \arrow[r] \arrow[d, "\zeta_0"] \arrow[dr, "\zeta"] & P_{n-1} \arrow[r] & \cdots \\
\cdots \arrow[r] & P_2 \arrow[r] & P_1 \arrow[r] & P_0 \arrow[r] & k \arrow[r] & 0
\end{tikzcd}$$

Likewise, any chain map determines a cohomology class. Then the definition of the product of two elements can be taken to be the composition of their chain maps.

The next step in the calculation is the construction of a chain map for the generators of cohomology. This is primarily a matter of solving linear equations to obtain each $\zeta_i$ in succession. In each degree $n$, the matrices of the monomials of degree $n$ in all previously calculated generators are computed so as to avoid computing chain maps for elements that are not generators for the cohomology.

Once we have computed the chain maps for the generators of cohomology, we want the relations. So suppose the generators are elements of the set $\{z, y, x, \dots\}$. Then for each $n$ we compute the induced maps $P_n / \mathrm{Rad}(kG)P_n \longrightarrow k$ for all monomials of degree $n$ in the generators. Each such map is a $(1 \times n)$-matrix since the null space of the matrix with these matrices (vectors) as rows is the set of all relations among the monomials of degree $n$.

Of course, we obtain far too many relations from the computation. For practical reasons, some analysis is required.

### Gröbner Bases

At this point we are given a polynomial ring and a huge collection of polynomials that generate the ideal of relations. The programs described in [8] generate many relations in each degree. For example, if $x^2 - zy$ is a relation in degree 2, then in degree 3 the system would generate the relation $zx^2 - z^2y$ as well as $yx^2 - zy^2$ and $x^3 - zyx$. We would like to have a minimal set of generators for the ideal of relations, so we need some technique for analyzing the data. In addition we need to calculate ring-theoretic properties such as depth, regular sequences, and associated primes. The method that does all of this is Gröbner bases.

The algorithm for obtaining a minimal set of relations is very simple. Suppose that $S = \{s_i | i = 1, \dots, t\}$ are the relations that have been computed. First we order the set by degree, so that $\mathrm{Degree}(s_i) \leq \mathrm{Degree}(s_j)$ whenever $i < j$. Note that we are assuming that all of our relations are homogeneous polynomials. Let $S_1 = \{s_1\}$. Then define $S_i$ inductively by the following rule: for each $i$, if $s_i$ is in the ideal generated by $S_{i-1}$, then let $S_i = S_{i-1}$. Otherwise, $S_i = S_{i-1} \cup \{s_i\}$. Then a minimal set of generators for the ideal of relations is the set $S_t$.

Computationally, the hard part in the algorithm is the line "if $s_i$ is in the ideal …". For this we need the membership test for an ideal that is provided by Gröbner bases. Suppose that $P = k[x_1, \dots, x_n]$ is a polynomial ring and let $\mathcal{I}$ be an ideal in $P$. To define a Gröbner basis for $\mathcal{I}$, we first choose an ordering on the monomials in $P$. Such an ordering might be lexicographic where the monomials are ordered as words in a dictionary. Or it might be graded lexicographic, where the longer words are higher in the ordering and ties are broken by a lexicographic test. In any case, the ordering should have the property that if $u, v$, and $w$ are monomials and $u \leq v$, then $uw \leq vw$. With the ordering, any polynomial $f$ in $P$ has a leading term, which is the term whose monomial has the largest order. A

Gröbner basis for an ideal $\mathcal{I}$ is a collection $S = S_{\mathcal{I}}$ of polynomials that generate $\mathcal{I}$ and also has the property that the leading term of any $f$ in $\mathcal{I}$ is divisible by the leading term of some element of $S$. It is a theorem that every ideal has a Gröbner basis [11].

The membership test goes as follows. Let $f$ be any element of $P$. If the leading term of $f$ is not divisible by the leading term of any element of $S$, then we are done. Otherwise, there exists an element $s \in S_{\mathcal{I}}$ and a monomial $\alpha \in P$ such that the leading term of $f - \alpha s$ is lower in the ordering than that of $f$. So now replace $f$ by $f - \alpha s$ and repeat until either $f = 0$ or it is shown that $f$ is not in $\mathcal{I}$.

Computing a Gröbner basis for an ideal can be difficult and time consuming. For one thing, the Gröbner basis depends heavily on the chosen order on the monomials. Consider the example of the ideal $\mathcal{I} = \langle x^2, z^2 + yx\rangle \subseteq k[z, y, x]$. Suppose that the ordering is chosen as graded lexicographic and that $z > y > x$. Then it can be seen that the Gröbner basis for $\mathcal{I}$ consists of the two generators $x^2$ and $z^2 + yx$ which have leading terms $x^2$ and $z^2$. On the other hand, if the ordering is chosen so that $z < y < x$, then the leading term of $z^2 + yx$ is $yx$. Hence the element $z^2x = (z^2 + yx)x - y(x^2)$ is in $\mathcal{I}$, but its leading term is not divisible by that of either $x^2$ or $z^2 + yx$. So in this case the Gröbner basis for $\mathcal{I}$ consists of $x^2, z^2 + yx$ and $z^2x$.

In the computation [10] of the cohomology rings of the groups of order 64, some of the Gröbner basis calculations took hours, or days. Most of the problems occurred in the actual computation of the Gröbner basis for an ideal. The Buchburger algorithm that computes the Gröbner basis can be as bad as doubly exponential in the number of variables. In practice, the algorithm usually works much faster. However, choices such as the ordering of the variables can be critical in very unpredictable ways. In the computation [10] of the cohomology ring of group number 187, the first few attempts to construct the Gröbner basis for the ideal of relations failed after several days of computing time on each attempt. The particular cohomology ring has twenty-six generators, and there was some question as to whether we would ever succeed. However, the problem was solved with a simple change in the ordering of the variables.

### Restrictions, Inflations, and Other Calculations

The computer programs continue by calculating the restriction maps to maximal subgroups. The algorithms are similar to those above. If $H$ is a subgroup of $G$, then to compute the restriction map $\mathrm{H}^*(G, k) \longrightarrow \mathrm{H}^*(H, k)$, we first construct a $kH$-chain map from the minimal projective $kH$-resolution of $k$ to the minimal projective $kG$-resolution. This is the chain map that lifts the identity on $k$. Then the restriction map is the composition with this chain map. The inflation map from a quotient group of $G$ is constructed similarly.

Other properties of cohomology rings, such as the depth or the associated primes can be computed using the Gröbner basis machinery. Some of these calculations can be very time consuming when the rings are complicated.

### Are We Almost There Yet?

The reader must have noticed by this point that we are computing the cohomology degree by degree. The problem with this approach should be obvious. If we only compute to degree 7, then any generator or any relation in degree 8 will be completely lost, ignored. On the other hand, the number of steps that we can compute is finite. Not only do the projective resolutions grow to absorb all available memory, but computing time also becomes a factor. A typical calculation of the cohomology ring of one of the groups of order 64 (assuming the group has rank 3 or more) would use a hundred or more megabytes of RAM after fifteen to twenty steps. In general, the time to compute each step would exceed the sum of all the time to compute the previous steps. The memory requirements also increase dramatically with each step.

As a result, a critical question arises. When are we done? When have we calculated far enough to get all of the generators and relations? There are at least two tests for completion available. Both depend on ring-theoretic properties of the cohomology ring. We present an outline of some of these results in the next section.

## Regularity and Tests for Completion

For the calculations in the appendix of [10], we used a rather complicated test to show that the computer program had produced the entire cohomology ring. Essentially, the same test was used by Green in [15]. More recently, Benson [4] has developed a new test which seems to be more direct and simple. All of these tests involve notions of systems of parameters and regularity in commutative algebra. In this section we present some of these ideas and show how they apply to the computations of cohomology rings. We state the definitions for cohomology rings, although in general they apply to finitely generated graded commutative $k$-algebras.

### Homogeneous Parameters

A homogeneous system of parameters for a cohomology ring $\mathrm{H}^*(G, k)$ is a sequence of homogeneous elements $x_1, x_2, \dots, x_n$ such that

1. $n$ is the Krull dimension of $\mathrm{H}^*(G, k)$, and
2. $\mathrm{H}^*(G, k)$ is finitely generated as a module over the subalgebra generated by $x_1, \dots, x_n$.

Note that because of condition (1), it must be that $k[x_1, \dots, x_n]$ is a polynomial subalgebra of $\mathrm{H}^*(G, k)$. Condition (2) is equivalent to the statement that the only maximal ideal which contains all of the elements $x_1, \dots, x_n$ is the ideal of all elements of positive degree in $\mathrm{H}^*(G,k)$. It is always possible to choose a homogeneous set of parameters with the property that the first $d$ elements in the sequence is a regular sequence of length equal to the depth $d$ of $\mathrm{H}^*(G,k)$.

The basic idea behind most of the tests for completion can be illustrated with the following example. Here we present only a sketch. More details can be found in Theorem 14.5.2 of [10].

### A Sample Test for Completion

Suppose that the cohomology ring of $G$ has Krull dimension 2. Then we can choose a homogeneous set of parameters $z, y$ such that the element $z$ is a regular element. Let $m, n$ be the degrees of $z$ and $y$, respectively. Now choose a minimal projective resolution $(P_*, \varepsilon)$ of the trivial module $k$ as above. Then the cohomology element $z$ is represented by a cocycle $f_z : P_m \longrightarrow k$. The statement that $f_z$ is a cocycle means that the composition

$$P_{m+1} \xrightarrow{\partial} P_m \xrightarrow{f_z} k$$

is the zero map. Hence, $f_z$ induces a homomorphism $f' : P_m/\partial(P_{m+1}) \longrightarrow k$ whose kernel we denote as $L_z$. So we have an exact sequence

$$0 \longrightarrow L_z \longrightarrow P_m/\partial(P_{m+1}) \xrightarrow{f_z'} k \longrightarrow 0,$$

and there is a corresponding long exact sequence

$$\begin{aligned} \dots \xrightarrow{\delta} \mathrm{Ext}^r_{kG}(k,k) &\xrightarrow{(f_z')^*} \mathrm{Ext}^r_{kG}(\Omega^m(k),k) \\ &\longrightarrow \mathrm{Ext}^r_{kG}(L_z,k) \xrightarrow{\delta} \mathrm{Ext}^{r-1}_{kG}(k,k) \longrightarrow \dots . \end{aligned}$$

Now $\mathrm{Ext}^r_{kG}(k,k) \cong \mathrm{H}^r(G,k)$ and by degree shifting $\mathrm{Ext}^r_{kG}(\Omega^m(k),k) \cong \mathrm{H}^{m+r}(G,k)$. Moreover the map $(f_z')^*$ is given by multiplication by $z$. Because $z$ is a regular element, $(f_z')^*$ is injective, and the connecting homomorphisms $\delta$ are all zero maps. Hence we have an exact sequences

$$0 \longrightarrow \mathrm{H}^r(G,k) \xrightarrow{(f_z')^*} \mathrm{H}^{r+m}(G,k) \longrightarrow \mathrm{Ext}^r_{kG}(L_z,k) \longrightarrow 0.$$

Consequently, the cokernel of multiplication by $z$ in degrees at least $m$ is the cohomology $\mathrm{Ext}^*_{kG}(L_z,k)$. Now here is the key. The module $L_z$ must be a periodic module, that is, a module whose cohomology repeats regularly after some fixed number of stages. The reason basically is that there is only one parameter left after factoring out $z$ (Proposition 9.7.3 of [10]). Moreover, because $y$ is the only parameter left, multiplication by $y$ must induce an isomorphism on the cohomology of $L_z$. So we have that

$$\begin{aligned} f_y^* : \mathrm{H}^{r+m}&(G,k)/z\,\mathrm{H}^r(G,k) \\ &\longrightarrow \mathrm{H}^{r+m+n}(G,k)/z\,\mathrm{H}^{r+n}(G,k) \end{aligned}$$

is an isomorphism for all $r \geq 0$, where $f_y^*$ is multiplication by $y$. The result is that every element of $\mathrm{H}^{r+m+n}(G,k)$ can be written in the form $z\alpha + y\beta$ for some $\alpha \in \mathrm{H}^{r+n}(G,k)$ and some $\beta \in \mathrm{H}^{r+m}(G,k)$. It follows that all of the generators of $\mathrm{H}^*(G,k)$ as both a ring and as a module over the polynomial subring $k[z,y]$ are in degrees less than $m+n$. Likewise, it can be shown that the ideal of relations among the generators is generated in degrees at most $2(m+n)$.

### Quasiregular Sequences and Regularity

What the sample test shows is that, while we can not expect a cohomology ring to have a regular sequence which is as long as its Krull dimension, we might always be able to find a quasiregular sequence. The notion of a quasiregular sequence was introduced by the author and Benson in [5]. The definition follows.

**Definition.** Suppose that H is a graded commutative, finitely generated $k$-algebra. We say that a sequence of homogeneous elements $x_1, \dots, x_n$ in degrees $n_1, \dots, n_n$ is a quasiregular sequence, provided that for each $i$ we have that the map

$$\hat{x_i} : (\mathrm{H}/(x_1, \dots, x_{i-1}))^j \longrightarrow (\mathrm{H}/(x_1, \dots, x_{i-1}))^{j+n_i}$$

of multiplication by $x_i$ is injective for all degrees

$$(*) \qquad j \geq n_1 + \cdots + n_{i-1}.$$

If the cohomology ring has a quasiregular sequence of length equal to its Krull dimension, then there is a straightforward formula for how far one has to compute in order to obtain a complete set of generators and relations for the ring. So we must ask the following question.

**Question.** Does every mod $p$ cohomology ring of a finite group have a quasiregular sequence?

In the event that the depth $\mathrm{H}^*(G,k)$ is one less than the Krull dimension, then a quasiregular sequence always exists. This is proved by an argument which is very similar to that in the example. Benson [4] has recently shown that the answer is affirmative in the case where the depth is no more than two less than the Krull dimension. A partial result in the codepth 2 case had also been proved by Okuyama and Sasaki [19]. However, Benson's work goes much further and involves the notion of regularity.

In [4], Benson considers cohomology rings in the context of some construction from local cohomology. In particular, he considers the Castelnuovo-Mumford regularity of the rings. The definition of this form of regularity is rather complicated, and we refer to Benson's paper or to [13] for a detailed explanation. All we will say here is that it is related to the cohomology of a certain Koszul complex associated to a homogeneous set of parameters. Such complexes are doubly graded and the regularity is the maximum value of the internal degrees such that the cohomology is nonzero. Benson has conjectured an affirmative answer to the following question.

**Question.** Is the regularity of $\mathrm{H}^*(G,k)$ equal to zero?

Benson shows that if the answer is yes, then the cohomology ring has a quasiregular sequence. Moreover, he shows that it has what he calls a strongly quasiregular sequence—a quasiregular sequence as in the definition above except that the condition (∗) is replaced by $j \geq \sum_{t=1}^{i-1}(n_t - 1)$. Moreover, he shows there is an explicit formula in terms of the regularity of the computed cohomology ring that determines whether the computation is complete. That is, if $R_n$ is the computation of $\mathrm{H}^*(G, k)$ calculated to degree $n$, and if $R_n$ satisfies Benson's formula, then it must be the case that $R_n \cong \mathrm{H}^*(G, k)$.

## So What Is True?

The investigations of the questions about depth, detection, and regularity share one curious property. The theoretical developments seem to be right at the edge of the experimental evidence. That is to say, we can prove most of what we can see. Moreover, seeing the evidence and proving the theorems seem to go hand in hand.

A case in point is the study of the quasiregular sequences and regularity. We can prove the results we want as long as the codepth of the cohomology ring is at most 2. This is also approximately what we have computed. There are almost no computed examples of groups $G$ such that $\mathrm{H}^*(G, k)$ has codepth more than 2. Green recently reported that he computed the mod 2 cohomology of codepth 3 of a group of order 128 [17]. In this case he got an affirmative answer to Benson's question (the regularity of $\mathrm{H}^*(G, k)$ equal to zero), but one example is hardly strong evidence.

The questions on depth and associated primes were developed partly by looking at experimental evidence. The computations have also aided in eliminating some of the earlier speculations. For example, it has now been shown that Question 3.3 of [7] has a negative answer. Counterexamples (if they exist) to any of conjectures will likely lie in large and complicated groups, and the computations become more expensive in terms of time and memory. At the same time both the equipment and the software are improving and perhaps will some day provide us with the insights to answer some of the questions.

## References

[1] A. Adem, J. F. Carlson, D. Karagueuzian, and R. J. Milgram, The cohomology of the Sylow 2-subgroup of Higman-Sims, *J. Pure Appl. Algebra* **164** (2001), 275–305.

[2] A. Adem and D. Karagueuzian, Essential cohomology of finite groups, *Comment. Math. Helv.* **72** (1997), 101–109.

[3] A. Adem, J. Maginnis, and R. J. Milgram, The geometry and cohomology of $M_{12}$, *J. Algebra* **139** (1991), 90–133.

[4] D. J. Benson, Dickson invariants and regularity in group cohomology, preprint.

[5] D. J. Benson and J. F. Carlson, Projective resolutions and Poincaré duality complexes, *Trans. Amer. Math. Soc.* **132** (1994), 447–488.

[6] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Magma Computer Algebra, Sydney, 2002.

[7] J. F. Carlson, Depth and transfer maps in the cohomology of groups, *Math. Z.* **218** (1995), 461–468.

[8] ____ , Problems in the computation of group cohomology, *Progr. Math.* **173** (1999), 107–120.

[9] ____ , Calculating group cohomology: Tests for completion, *J. Symbolic Comput.* **31** (2001), 229–242.

[10] J. Carlson, L. Townsley, L. Valero-Elizondo, and M. Zhang, *Cohomology Rings of Finte Groups*, Kluwer, Dordrecht, 2003.

[11] D. A. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York, 1997.

[12] J. Duflot, Depth and equivariant cohomology, *Comment. Math. Helv.* **56** (1981), 627–637.

[13] D. Eisenbud and S. Goto, Linear free resolutions and minimal multiplicities, *J. Algebra* **88** (1984), 89–133.

[14] L. Evens, The cohomology ring of a finite group, *Trans. Amer. Math. Soc.* **101** (1961), 224–239.

[15] D. J. Green, *Gröbner Bases and the Computation of Group Cohomology*, Lecture Notes in Math., vol. 1828, Springer-Verlag, Berlin, 2003.

[16] ____ , On Carlson's conjecture in group cohomology, *Math. Z.* **244** (2003), 711-723.

[17] ____ , private communication, 2004.

[18] J. Lannes, Sur les espaces fonctionnels dont la source est le classificant d'un $p$-groupe abélien élémentaire, *Publ. Math. Inst. Hautes Études Sci.* **75** (1992), 135–244.

[19] T. Okuyama and H. Sasaki, private communication.

[20] D. Quillen, The spectrum of an equivariant cohomology ring, I, II, *Ann. of Math.* **94** (1971), 549–602.

[21] B. B. Venkov, Cohomology algebras of some arbitrary classifying spaces, *Dokl. Akad. Nauk SSSR* **127** (1959), 943–944. (Russian)