Trends in Commutative Algebra
MSRI Publications
Volume **51**, 2004

Commutative Algebra in the Cohomology of Groups

DAVE BENSON

Abstract. Commutative algebra is used extensively in the cohomology of groups. In this series of lectures, I concentrate on finite groups, but I also discuss the cohomology of finite group schemes, compact Lie groups, p-compact groups, infinite discrete groups and profinite groups. I describe the role of various concepts from commutative algebra, including finite generation, Krull dimension, depth, associated primes, the Cohen–Macaulay and Gorenstein conditions, local cohomology, Grothendieck's local duality, and Castelnuovo–Mumford regularity.

Contents

The author is partly supported by NSF grant DMS-9988110.

1. Introduction

The purpose of these lectures is to explain how commutative algebra is used in the cohomology of groups. My interpretation of the word "group" is catholic: the kinds of groups in which I shall be interested include finite groups, finite group schemes, compact Lie groups, p-compact groups, infinite discrete groups, and profinite groups, although later in the lectures I shall concentrate more on the case of finite groups, where representation theoretic methods are most effective. In each case, there are finite generation theorems which state that under suitable conditions, the cohomology ring is a graded commutative Noetherian ring; over a field k, this means that it is a finitely generated graded commutative k-algebra.

Although graded commutative is not quite the same as commutative, the usual concepts from commutative algebra apply. These include the maximal/prime ideal spectrum, Krull dimension, depth, associated primes, the Cohen–Macaulay and Gorenstein conditions, local cohomology, Grothendieck's local duality, and so on. One of the themes of these lectures is that the rings appearing in group cohomology theory are quite special. Most finitely generated graded commutative k-algebras are not candidates for the cohomology ring of a finite (or compact Lie, or virtual duality, or p-adic Lie, or ...) group. The most powerful restrictions come from local cohomology spectral sequences such as the Greenlees spectral sequence $H^{s,t}_{\mathfrak{m}} H^*(G,k) \Longrightarrow H_{-s-t}(G,k)$, which can be viewed as a sort of duality theorem. We describe how to construct such spectral sequences and obtain information from them.

The companion article to this one, [Iyengar 2004], explains some of the background material that may not be familiar to commutative algebraists. A number of references are made to that article, and for distinctiveness, I write [Sri].

2. Some Examples

For motivation, let us begin with some examples. We defer until the next section the definition of group cohomology

$$H^*(G,k) = \mathrm{Ext}^*_{kG}(k,k)$$

(or see § 6 of [Sri]). All the examples in this section are for finite groups G over a field of coefficients k.

(2.1) The first comment is that in the case where k is a field of characteristic zero or characteristic not dividing the order of G, Maschke's theorem in representation theory shows that all kG-modules are projective (see Theorem 3.1 of [Sri]). So for any kG-modules M and N, and all $i > 0$, we have $\mathrm{Ext}^i_{kG}(M,N) = 0$. In particular, $H^*(G,k)$ is just k, situated in degree zero. Given this fact, it makes sense to look at examples where k has characteristic p dividing $|G|$.

(2.2) Next, we discuss finite abelian groups. See also § 7.4 of [Sri]. The Künneth theorem implies that

(2.2.1) $$H^*(G_1 \times G_2, k) \cong H^*(G_1, k) \otimes_k H^*(G_2, k).$$

So we decompose our finite abelian group as a direct product of cyclic groups of prime power order. The factors of order coprime to the characteristic may be thrown away, using (2.1). For a cyclic p-group in characteristic p, there are two possibilities (Proposition 7.3 of [Sri]). If $p = 2$ and $|G| = 2$, then $H^*(G, k) = k[x]$ where x has degree one. In all other cases (i.e., p odd, or $p = 2$ and $|G| \geq 4$), we have $H^*(G, k) = k[x, y]/(x^2)$ where x has degree one and y has degree two. It follows that if G is any finite abelian group then $H^*(G, k)$ is a tensor product of a polynomial ring and a (possibly trivial) exterior algebra.

(2.2.2) In particular, if G is a finite elementary abelian p-group of rank r (i.e., a product of r copies of $\mathbb{Z}/p$) and k is a field of characteristic p, then the cohomology ring is as follows. For $p = 2$, we have

$$H^*((\mathbb{Z}/2)^r, k) = k[x_1, \dots, x_r]$$

with $|x_i| = 1$, while for p odd, we have

$$H^*((\mathbb{Z}/p)^r, k) = \Lambda(x_1, \dots, x_r) \otimes k[y_1, \dots, y_r]$$

with $|x_i| = 1$ and $|y_i| = 2$. In the latter case, the nil radical is generated by $x_1, \dots, x_r$, and in both cases the quotient by the nil radical is a polynomial ring in r generators.

(2.3) The next comment is that if S is a Sylow p-subgroup of G then a transfer argument shows that the restriction map from $H^*(G, k)$ to $H^*(S, k)$ is injective. What's more, the stable element method of Cartan and Eilenberg [1956] identifies the image of this restriction map. For example, if $S \trianglelefteq G$ then $H^*(G, k) = H^*(S, k)^{G/S}$, the invariants of G/S acting on the cohomology of S (see § 7.6 of [Sri]). It follows that really important case is where G is a p-group and k has characteristic p. Abelian p-groups are discussed in (2.2), so let's look at some nonabelian p-groups.

(2.4) Consider the quaternion group of order eight,

(2.4.1) $$Q_8 = \langle g, h \mid gh = h^{-1}g = hg^{-1} \rangle.$$

There is an embedding

$$g \mapsto i, \quad h \mapsto j, \quad gh \mapsto k, \quad g^2 = h^2 = (gh)^2 \mapsto -1$$

of Q_8 into the unit quaternions (i.e., SU(2)), which form a three dimensional sphere S^3. So left multiplication gives a free action of Q_8 on S^3; in other words, each nonidentity element of the group has no fixed points on the sphere. The quotient S^3/Q_8 is an orientable three dimensional manifold, whose cohomology therefore satisfies Poincaré duality. The freeness of the action implies that we can choose a CW decomposition of S^3 into cells permuted freely by Q_8. Taking cellular chains with coefficients in $\mathbb{F}_2$, we obtain a complex of free $\mathbb{F}_2Q_8$-modules of length four, whose homology consists of one copy of $\mathbb{F}_2$ at the beginning and another copy at the end. Making suitable choices for the cells, this looks as follows.

$$0 \to \mathbb{F}_2Q_8 \xrightarrow{\left(\begin{smallmatrix} g-1 \\ h-1 \end{smallmatrix}\right)} (\mathbb{F}_2Q_8)^2 \xrightarrow{\left(\begin{smallmatrix} h-1 & hg+1 \\ gh+1 & g-1 \end{smallmatrix}\right)} (\mathbb{F}_2Q_8)^2 \xrightarrow{(g-1\ \ h-1)} \mathbb{F}_2Q_8 \to 0$$

So we can form a Yoneda splice of an infinite number of copies of this sequence to obtain a free resolution of $\mathbb{F}_2$ as an $\mathbb{F}_2Q_8$-module. The upshot of this is that we obtain a decomposition for the cohomology ring

$$\begin{aligned} H^*(Q_8, \mathbb{F}_2) &= \mathbb{F}_2[z] \otimes_{\mathbb{F}_2} H^*(S^3/Q_8; \mathbb{F}_2) \\ &= \mathbb{F}_2[x, y, z]/(x^2 + xy + y^2, x^2y + xy^2), \end{aligned} \tag{2.4.2}$$

where z is a polynomial generator of degree four and x and y have degree one. This structure is reflected in the Poincaré series

$$\sum_{i=0}^{\infty} t^i \dim H^i(Q_8, \mathbb{F}_2) = (1 + 2t + 2t^2 + t^3)/(1 - t^4).$$

The decomposition (2.4.2) into a polynomial piece and a finite Poincaré duality piece can be expressed as follows (cf. § 11):

$$\boxed{H^*(Q_8, \mathbb{F}_2) \text{ IS A GORENSTEIN RING.}}$$

(2.5) We recall that the meanings of Cohen–Macaulay and Gorenstein in this context are as follows. Let R be a finitely generated graded commutative k-algebra with $R_0 = k$ and $R_i = 0$ for $i < 0$. Then Noether's normalization lemma guarantees the existence of a homogeneous polynomial subring $k[x_1, \dots, x_r]$ over which R is finitely generated as a module.

PROPOSITION 2.5.1. *If R is of the type described in the previous paragraph, then the following are equivalent.*

(a) *There exists a homogeneous polynomial subring $k[x_1, \dots, x_r] \subseteq R$ such that R is finitely generated and free as a module over $k[x_1, \dots, x_r]$.*

(b) *If $k[x_1, \dots, x_r] \subseteq R$ is a homogeneous polynomial subring such that R is finitely generated as a $k[x_1, \dots, x_r]$-module then R a free $k[x_1, \dots, x_r]$-module.*

(c) *There exist homogeneous elements of positive degree $x_1, \dots, x_r$ forming a regular sequence, and $R/(x_1, \dots, x_r)$ has finite rank as a k-vector space.*

We say that R is *Cohen–Macaulay* of dimension r if the equivalent conditions of the above proposition hold.

(2.6) If R is Cohen–Macaulay, and the quotient ring $R/(x_1, \dots, x_r)$ has a simple socle, then we say that R is *Gorenstein.* Whether this condition holds is independent of the choice of the polynomial subring. Another way to phrase the condition is that $R/(x_1, \dots, x_r)$ is injective as a module over itself. This quotient satisfies Poincaré duality, in the sense that if the socle lies in degree d (d is called the *dualizing degree*) and we write

$$p(t) = \sum_{i=0}^{\infty} t^i \dim_k (R/(x_1, \dots, x_r))_i$$

then

$$t^d p(1/t) = p(t). \tag{2.6.1}$$

Setting

$$P(t) = \sum_{i=0}^{\infty} t^i \dim_k R_i,$$

the freeness of R over $k[x_1, \dots, x_r]$ implies that $P(t)$ is the power series expansion of the rational function $p(t)/\prod_{i=1}^r (1 - t^{|x_i|})$. So plugging in equation (2.6.1), we obtain the functional equation

$$P(1/t) = (-t)^r t^{-a} P(t), \tag{2.6.2}$$

where $a = d - \sum_{i=1}^r (|x_i| - 1)$. We say that R is Gorenstein with a-invariant a.

Another way of expressing the Gorenstein condition is as follows. If R (as above) is Cohen–Macaulay, then the local cohomology $H^{s,t}_{\mathfrak{m}} R$ is only nonzero for $s = r$. The graded dual of $H^{r,*}_{\mathfrak{m}} R$ is called the *canonical module*, and written Ω_R. To say that R is Gorenstein with a-invariant a is the same as saying that Ω_R is a copy of R shifted so that the identity element lies in degree $r - a$.

In the case of $H^*(Q_8, \mathbb{F}_2)$, we can choose the polynomial subring to be $k[z]$. The ring $H^*(Q_8, \mathbb{F}_2)$ is a free module over $k[z]$ on six generators, corresponding to a basis for the graded vector space $H^*(S^3/Q_8; \mathbb{F}_2) \cong H^*(Q_8, \mathbb{F}_2)/(z)$, which satisfies Poincaré duality with $d = 3$. So in this case the a-invariant is $3-(4-1) = 0$. We have $p(t) = 1 + 2t + 2t^2 + t^3$ and $P(t) = p(t)/(1 - t^4)$.

(2.7) A similar pattern to the one seen above for Q_8 holds for other groups. Take for example the group $\mathrm{GL}(3, 2)$ of 3×3 invertible matrices over $\mathbb{F}_2$. This is a finite simple group of order 168. Its cohomology is given by

$$H^*(\mathrm{GL}(3, 2), \mathbb{F}_2) = \mathbb{F}_2[x, y, z]/(x^3 + yz)$$

where $\deg x = 2$, $\deg y = \deg z = 3$. A homogeneous system of parameters for this ring is given by y and z, and these elements form a regular sequence. Modulo the ideal generated by y and z, we get $\mathbb{F}_2(x)/(x^3)$. This is a finite Poincaré duality ring whose dualizing degree is 4. Again, this means that the cohomology is a Gorenstein ring with a-invariant $4-(3-1)-(3-1) = 0$, but it does not decompose as a tensor product the way it did for the quaternion group (2.4.2).

(2.8) It is not true that the cohomology ring of a finite group is always Gorenstein. For example, the semidihedral group of order 2^n ($n \geq 4$),

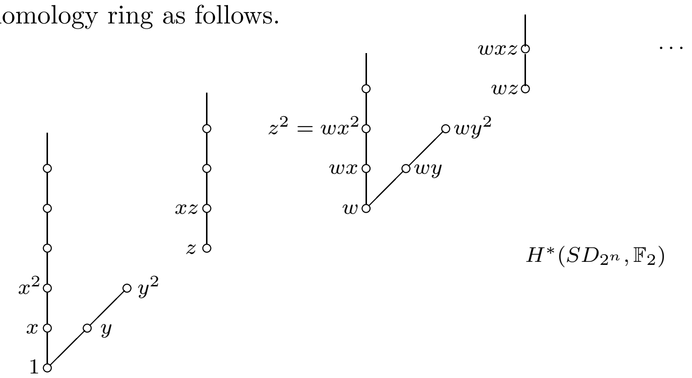
$$G = SD_{2^n} = \langle g, h \mid g^{2^{n-1}} = 1,\ h^2 = 1,\ h^{-1}gh = g^{2^{n-2}-1} \rangle \tag{2.8.1}$$

has cohomology ring

$$H^*(SD_{2^n}, \mathbb{F}_2) = \mathbb{F}_2[x, y, z, w]/(xy, y^3, yz, z^2 + x^2w)$$

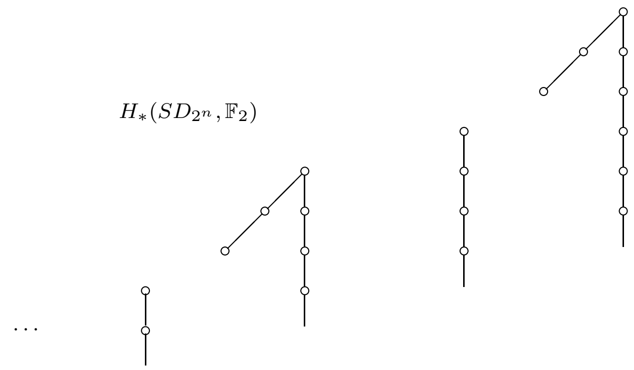
with $\deg x = \deg y = 1$, $\deg z = 3$ and $\deg w = 4$. This ring is not even Cohen–Macaulay. But what is true is that whenever the ring is Cohen–Macaulay, it is Gorenstein with a-invariant zero. See § 11 for further details.

Even if the cohomology ring is not Cohen–Macaulay, there is still a certain kind of duality, but it is expressed in terms of a spectral sequence of Greenlees, $H^{s,t}_{\mathfrak{m}} H^*(G, k) \implies H_{-s-t}(G, k)$. Let us see in the case above of the semidihedral group, what this spectral sequence looks like. And let's do it in pictures. We'll draw the cohomology ring as follows.



The vertical coordinate indicates cohomological degree, and the horizontal coordinate is just for separating elements of the same degree. To visualize the homology, just turn this picture upside down by rotating the page, as follows.

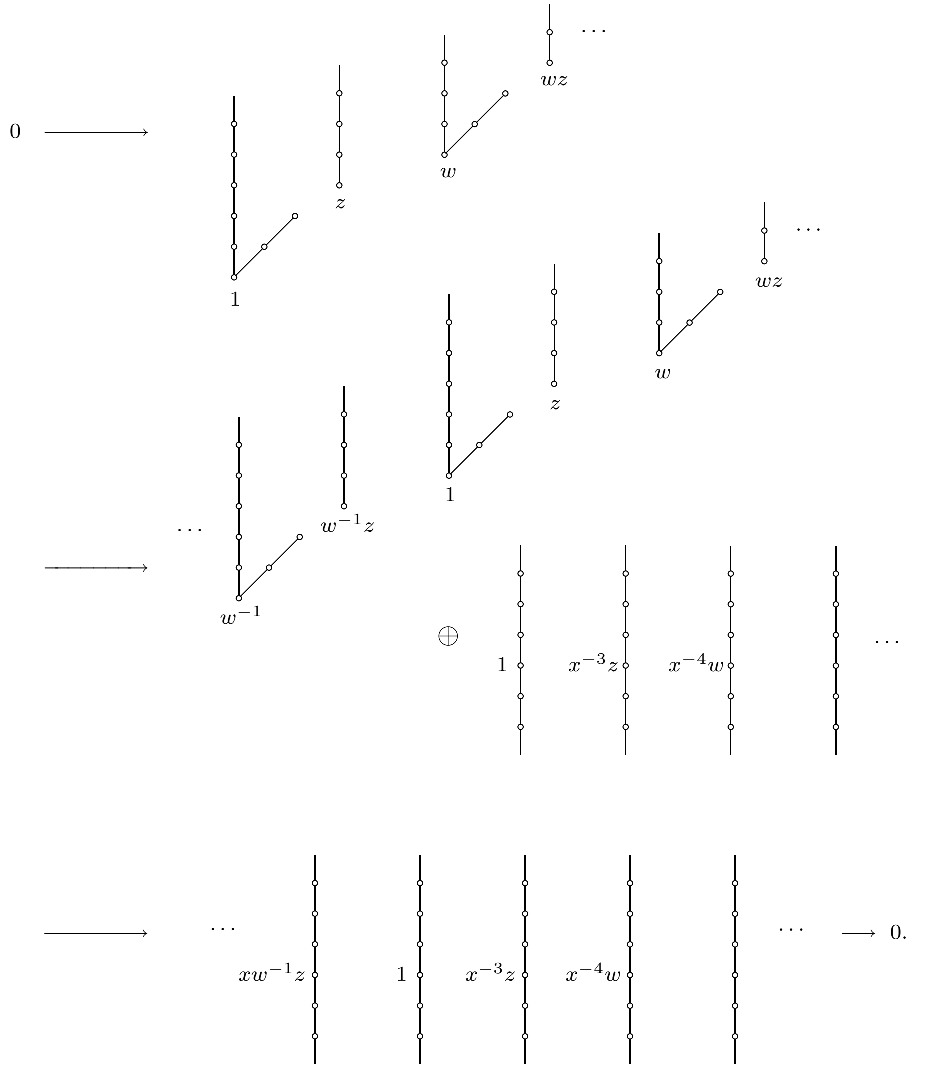
(2.8.2)



We compute local cohomology using the stable Koszul complex for the homogeneous system of parameters w, x,

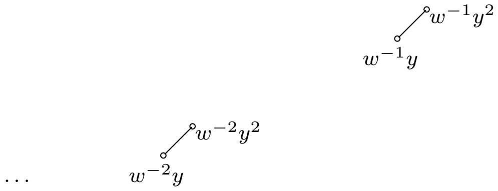
$$0 \to H^*(G, \mathbb{F}_2) \to H^*(G, \mathbb{F}_2)[w^{-1}] \oplus H^*(G, \mathbb{F}_2)[x^{-1}] \to H^*(G, \mathbb{F}_2)[w^{-1}x^{-1}] \to 0$$

where the subscripts denote localization by inverting the named element. A picture of this stable Koszul complex is as follows.



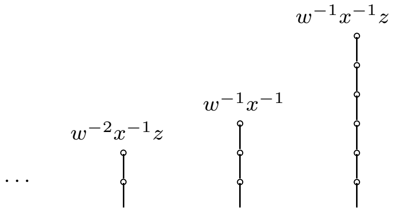
The local cohomology of $H^*(G, k)$ is just the cohomology of this complex. In degree zero there is no cohomology. In degree one there is some cohomology, namely the hooks that got introduced when w was inverted,

$$H^1_{\mathfrak{m}} H^*(SD_{2^n}, \mathbb{F}_2) =$$



In degree two, we get the part of the plane not hit by either of the two degree one pieces,

$$H^2_{\mathfrak{m}} H^*(SD_{2^n}, \mathbb{F}_2) =$$



Now the differential d_2 in this spectral sequence increases local cohomological degree by two and decreases internal degree by one, and the higher differentials are only longer. So there is no room in this example for nonzero differentials. It follows that the spectral sequence takes the form of a short exact sequence

$$0 \to H^{1,t-1}_{\mathfrak{m}} H^*(SD_{2^n}, \mathbb{F}_2) \to H_{-t}(SD_{2^n}, \mathbb{F}_2) \to H^{2,t-2}_{\mathfrak{m}} H^*(SD_{2^n}, \mathbb{F}_2) \to 0.$$

This works fine, because $H_*(SD_{2^n}, \mathbb{F}_2)$ is the graded dual of $H^*(SD_{2^n}, \mathbb{F}_2)$, as shown in (2.8.2). So the short exact sequence places the hooks of $H^1_{\mathfrak{m}}$ underneath every second nonzero column in $H^2_{\mathfrak{m}}$ to build $H_*(SD_{2^n}, \mathbb{F}_2)$. Notice that the hooks appear inverted, so that there is a separate Poincaré duality for a hook.

The same happens as in this case whenever the depth and the Krull dimension differ by one. The kernel of multiplication by the last parameter, modulo the previous parameters, satisfies Poincaré duality with dualizing degree determined by the degrees of the parameters; in particular, the top degree of this kernel is determined. In the language of commutative algebra, this can be viewed in terms of the Castelnuovo–Mumford regularity of the cohomology ring. See § 14 for more details.

The reader who wishes to understand these examples better can skip directly to § 14, and refer back to previous sections as necessary to catch up on definitions. Conjecture 14.6.1 says that for a finite group G, $\mathsf{Reg}\, H^*(G, k)$ is always zero. This conjecture is true when the depth and the Krull dimension differ by at most one, as in the above example. It is even true when the difference is two, by a more subtle transfer argument sketched in § 14 and described in detail in [Benson 2004].

3. Group Cohomology

For general background material on cohomology of groups, the textbooks I recommend are [Adem and Milgram 1994; Benson 1991b; Brown 1982; Cartan and Eilenberg 1956; Evens 1991]. The commutative algebra texts most relevant to these lectures are [Bruns and Herzog 1993; Eisenbud 1995; Grothendieck 1965; 1967; Matsumura 1989].

(3.1) For a *discrete group*, the easiest way to think of group cohomology is as the Ext ring (see § 5 of [Sri]). If G is a group and k is a commutative ring of coefficients, we define group cohomology via

$$H^*(G,k) = \operatorname{Ext}^*_{\mathbb{Z}G}(\mathbb{Z},k) \cong \operatorname{Ext}^*_{kG}(k,k).$$

Here, the group ring kG consists of formal linear combinations $\sum \lambda_i g_i$ of elements of the group G with coefficients in k. The cup product in cohomology comes from the fact that kG is a Hopf algebra (see § 1.8 of [Sri]), with comultiplication $\Delta(g) = g \otimes g$. Another part of the Hopf structure on kG is the augmentation map $kG \to k$, $\sum \lambda_i g_i \mapsto \sum \lambda_i$, which is what allows us to regard k as a kG-module.

Cup product and Yoneda product define the same multiplicative structure, and this makes cohomology into a *graded commutative* ring, in the sense that

$$ab = (-1)^{|a||b|} ba,$$

where $|a|$ denotes the degree of an element a (see Prop. 5.5 of [Sri]). In contrast, the Ext ring of a commutative local ring is seldom graded commutative; this happens only for a restricted class of complete intersections. The group ring of an abelian group is an example of a complete intersection (see § 1.4 of [Sri]).

More generally, if M is a left kG-module then

$$H^*(G,M) = \operatorname{Ext}^*_{\mathbb{Z}G}(\mathbb{Z},M) \cong \operatorname{Ext}^*_{kG}(k,M)$$

is a graded *right* $H^*(G,k)$-module.

It is a nuisance that most texts on commutative algebra are written for *strictly* commutative graded rings, where $ab = ba$ with no sign. I do not know of an instance where the signs make a theorem from commutative algebra fail. It is worth pointing out that if a is an element of odd degree in a graded commutative ring then $2a^2 = 0$. So $2a$ is nilpotent, and it follows that modulo the nil radical the ring is strictly commutative. On the other hand, it is *more than a nuisance* that commutative algebraists often assume that their graded rings are generated by elements of degree one, because this is not at all true for cohomology rings. Nor, for that matter, is it true for rings of invariants.

(3.2) A homomorphism of groups $\rho\colon H \to G$ gives rise to a map the other way

$$\rho^*\colon H^*(G,M) \to H^*(H,M)$$

for any kG-module M. If $\rho\colon H \to G$ is an inclusion, this is called the *restriction map*, and denoted $\operatorname{res}_{G,H}$. If G is a quotient group of H and $\rho\colon H \to G$ is the quotient map, then it is called the *inflation map*, and denoted $\inf_{G,H}$.

(3.3) For a *topological group* (this includes compact Lie groups as well as discrete groups), a theorem of Milnor [1956] says that the infinite join

$$EG = G \star G \star \cdots$$

is weakly contractible, G acts freely on it, and the quotient $BG = EG/G$ together with the principal G-bundle $p\colon EG \to BG$ forms a classifying space for principal G-bundles over a paracompact base. A topologist refers to $H^*(BG;k)$ as the classifying space cohomology of G. Again, it is a graded commutative ring. For example, for the compact unitary group $\mathrm{U}(n)$, the cohomology ring

$$H^*(B\mathrm{U}(n);k) \cong k[c_1,\dots,c_n] \tag{3.3.1}$$

is a polynomial ring over k on n generators $c_1,\dots,c_n$ with $|c_i| = 2i$, called the *Chern classes*. Similarly, for the orthogonal group $\mathrm{O}(2n)$, if k is a field of characteristic not equal to two, then we have

$$H^*(B\mathrm{O}(2n);k) \cong k[p_1,\dots,p_n] \tag{3.3.2}$$

is a polynomial ring over k on n generators $p_1,\dots,p_n$ with $|p_i| = 4i$, called the *Pontrjagin classes*. For $\mathrm{SO}(2n)$ we have

$$H^*(B\mathrm{SO}(2n);k) \cong k[p_1,\dots,p_{n-1},e]. \tag{3.3.3}$$

where $e \in H^{2n}(B\mathrm{SO}(2n);k)$ is called the *Euler class*, and satisfies $e^2 = p_n$. We shall discuss these examples further in § 12.

If G is a discrete group then BG is an *Eilenberg–Mac Lane space* for G; in other words, $\pi_1(BG) \cong G$ and $\pi_i(BG) = 0$ for $i > 1$. The relationship between group cohomology and classifying space cohomology for G discrete is that the singular chains $C_*(EG)$ form a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module. Then there are isomorphisms

$$H^*(BG;k) = H^*\operatorname{Hom}_{\mathbb{Z}}(C_*(BG),k) \cong H^*\operatorname{Hom}_{\mathbb{Z}G}(C_*(EG),k) \cong H^*(G,k),$$

and the topologically defined product on the left agrees with the algebraically defined product on the right.

(3.4) Another case of interest is *profinite groups*. A profinite group is defined to be an inverse limit of a system of finite groups, which makes it a compact, Hausdorff, totally disconnected topological group. For example, writing $\hat{\mathbb{Z}}_p$ for the ring of p-adic integers, $\mathrm{SL}_n(\hat{\mathbb{Z}}_p)$ is a profinite group. The open subgroups of a profinite group are the subgroups of finite index.

Classifying space cohomology turns out to be the wrong concept for a profinite group. A better concept is continuous cohomology, which is defined as follows [Serre 1965a]. Let $G = \varprojlim_{U \in \mathscr{U}} G/U$ be a profinite group, where $\mathscr{U}$ is a system of