6

Group Homology and Cohomology

6.1 Definitions and First Properties

Let G be a group. A (left) *G-module* is an abelian group A on which G acts by additive maps on the left; if $g \in G$ and $a \in A$, we write ga for the action of g on a. Letting $\mathrm{Hom}_G(A, B)$ denote the G-set maps from A to B, we obtain a category G–**mod** of left G-modules. The category G–**mod** may be identified with the category $\mathbb{Z}G$–**mod** of left modules over the integral group ring $\mathbb{Z}G$. It may also be identified with the functor category $\mathbf{Ab}^G$ of functors from the category "G" (one object, G being its endomorphisms) to the category **Ab** of abelian groups.

A *trivial G-module* is an abelian group A on which G acts "trivially," that is, $ga = a$ for all $g \in G$ and $a \in A$. Considering an abelian group as a trivial G-module provides an exact functor from **Ab** to G–**mod**. Consider the following two functors from G–**mod** to **Ab**:

1. The *invariant subgroup* A^G of a G-module A,

$$A^G = \{a \in A : ga = a \text{ for all } g \in G \text{ and } a \in A\}.$$

2. The *coinvariants* A_G of a G-module A,

$$A_G = A/\text{submodule generated by } \{(ga - a) : g \in G, a \in A\}.$$

Exercise 6.1.1

1. Show that A^G is the maximal trivial submodule of A, and conclude that the invariant subgroup functor $-^G$ is right adjoint to the trivial module functor. Conclude that $-^G$ is a left exact functor.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

2. Show that A_G is the largest quotient module of A that is trivial, and conclude that the coinvariants functor $-_G$ is left adjoint to the trivial module functor. Conclude that $-_G$ is a right exact functor.

Lemma 6.1.1 *Let A be any G-module, and let $\mathbb{Z}$ be the trivial G-module. Then $A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}G} A$ and $A^G \cong \mathrm{Hom}_G(\mathbb{Z}, A)$.*

Proof Considering $\mathbb{Z}$ as a $\mathbb{Z}-\mathbb{Z}G$ bimodule, the "trivial module functor" from $\mathbb{Z}$–**mod** to $\mathbb{Z}G$–**mod** is the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$. We saw in 2.6.3 that $\mathbb{Z} \otimes_{\mathbb{Z}G} -$ is its left adjoint; this functor must agree with its other left adjoint $(-)_G$. For the second equation, we use adjointness: $A^G \cong \mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Z}, A^G) \cong \mathrm{Hom}_G(\mathbb{Z}, A)$. ◇

Definition 6.1.2 Let A be a G-module. We write $H_*(G; A)$ for the left derived functors $L_*(-_G)(A)$ and call them the *homology groups of G with coefficients in A*; by the lemma above, $H_*(G; A) \cong \mathrm{Tor}_*^{\mathbb{Z}G}(\mathbb{Z}, A)$. By definition, $H_0(G; A) = A_G$. Similarly, we write $H^*(G; A)$ for the right derived functors $R^*(-^G)(A)$ and call them the *cohomology groups of G with coefficients in A*; by the lemma above, $H^*(G; A) \cong \mathrm{Ext}^*_{\mathbb{Z}G}(\mathbb{Z}, A)$. By definition, $H^0(G; A) = A^G$.

Example 6.1.3 If $G = 1$ is the trivial group, $A_G = A^G = A$. Since the higher derived functors of an exact functor vanish, $H_*(1; A) = H^*(1; A) = 0$ for $* \neq 0$.

Example 6.1.4 Let G be the infinite cyclic group T with generator t. We may identify $\mathbb{Z}T$ with the Laurent polynomial ring $\mathbb{Z}[t, t^{-1}]$. Since the sequence

$$0 \to \mathbb{Z}T \xrightarrow{t-1} \mathbb{Z}T \to \mathbb{Z} \to 0$$

is exact,

$$H_n(T; A) = H^n(T; A) = 0 \text{ for } n \neq 0, 1, \text{ and}$$
$$H_1(T; A) \cong H^0(T; A) = A^T, H^1(T; A) \cong H_0(T; A) = A_T.$$

In particular, $H_1(T; \mathbb{Z}) = H^1(T; \mathbb{Z}) = \mathbb{Z}$. We will see in the next section that all free groups display similar behavior, because $pd_G(\mathbb{Z}) = 1$.

Exercise 6.1.2 (kG-modules) As a variation, we can replace $\mathbb{Z}$ by any commutative ring k and consider the category kG–**mod** of k-modules on which G acts k-linearly. The functors A_G and A^G from kG–**mod** to k–**mod** are left

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

(resp. right) exact and may be used to form the derived functors Tor_*^{kG} and Ext^*_{kG}. Prove that if A is a kG-module, then we have isomorphisms of abelian groups

$$H_*(G; A) \cong \mathrm{Tor}_*^{kG}(k, A) \quad \text{and} \quad H^*(G; A) \cong \mathrm{Ext}^*_{kG}(k, A).$$

This proves that $H_*(G; A)$ and $H^*(G; A)$ are k-modules whenever A is a kG-module. *Hint:* If $P \to \mathbb{Z}$ is a projective $\mathbb{Z}G$-resolution, consider $P \otimes_{\mathbb{Z}} k \to k$.

We now return our attention to H_0 and H^0.

Definition 6.1.5 The *augmentation ideal* of $\mathbb{Z}G$ is the kernel $\mathfrak{I}$ of the ring map $\mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z}$ which sends $\sum n_g g$ to $\sum n_g$. Because $\{1\} \cup \{g - 1 : g \in G, g \neq 1\}$ is a basis for $\mathbb{Z}G$ as a free $\mathbb{Z}$-module, it follows that $\mathfrak{I}$ is a free $\mathbb{Z}$-module with basis $\{g - 1 : g \in G, g \neq 1\}$.

Example 6.1.6 Since the trivial G-module $\mathbb{Z}$ is $\mathbb{Z}G/\mathfrak{I}$, $H_0(G; A) = A_G$ is isomorphic to $\mathbb{Z} \otimes_{\mathbb{Z}G} A = \mathbb{Z}G/\mathfrak{I} \otimes_{\mathbb{Z}G} A \cong A/\mathfrak{I}A$ for every G-module A. For example, $H_0(G; \mathbb{Z}) = \mathbb{Z}/\mathfrak{I}\mathbb{Z} = \mathbb{Z}$, $H_0(G; \mathbb{Z}G) = \mathbb{Z}G/\mathfrak{I} \cong \mathbb{Z}$, and $H_0(G; \mathfrak{I}) = \mathfrak{I}/\mathfrak{I}^2$.

Example 6.1.7 ($A = \mathbb{Z}G$) Because $\mathbb{Z}G$ is a projective object in $\mathbb{Z}G$–**mod**, $H_*(G; \mathbb{Z}G) = 0$ for $* \neq 0$ and $H_0(G; \mathbb{Z}G) = \mathbb{Z}$. When G is a finite group, Shapiro's Lemma (6.3.2 below) implies that $H^*(G; \mathbb{Z}G) = 0$ for $* \neq 0$. This fails when G is infinite; for example, we saw in 6.1.4 that $H^1(T; \mathbb{Z}T) \cong \mathbb{Z}$ for the infinite cyclic group T.

The following discussion clarifies the situation for $H^0(G; \mathbb{Z}G)$: If G is finite, then $H^0(G; \mathbb{Z}G) \cong \mathbb{Z}$, but $H^0(G; \mathbb{Z}G) = 0$ if G is infinite.

The Norm Element 6.1.8 Let G be a finite group. The *norm element* N of the group ring $\mathbb{Z}G$ is the sum $N = \sum_{g \in G} g$. The norm is a central element of $\mathbb{Z}G$ and belongs to $(\mathbb{Z}G)^G$, because for every $h \in G$ $hN = \sum_g hg = \sum_{g'} g' = N$, and $Nh = N$ similarly.

Lemma 6.1.9 *The subgroup $H^0(G; \mathbb{Z}G) = (\mathbb{Z}G)^G$ of $\mathbb{Z}G$ is the 2-sided ideal $\mathbb{Z} \cdot N$ of $\mathbb{Z}G$ (isomorphic to $\mathbb{Z}$) generated by N.*

Proof If $a = \sum n_g g$ is in $(\mathbb{Z}G)^G$, then $a = ga$ for all $g \in G$. Comparing coefficients of g shows that all the n_g are the same. Hence $a = nN$ for some $n \in \mathbb{Z}$. ◇

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.1.3

1. Show that if G is an infinite group, then $H^0(G; \mathbb{Z}G) = (\mathbb{Z}G)^G = 0$.
2. When G is a finite group, show that the natural map $\mathbb{Z} \cdot N = (\mathbb{Z}G)^G \to (\mathbb{Z}G)_G \cong \mathbb{Z}$ sends the norm N to the order $\#G$ of G. In particular, it is an injection.
3. Conclude that $\mathfrak{I}$ is $\ker(\mathbb{Z}G \xrightarrow{N} \mathbb{Z}G) = \{a \in \mathbb{Z}G : Na = 0\}$ when G is finite.

Proposition 6.1.10 *Let G be a finite group of order m, and N the norm. Then $e = N/m$ is a central idempotent element of $\mathbb{Q}G$ and of $\mathbb{Z}G[\frac{1}{m}]$. If A is a $\mathbb{Q}G$-module, or any G-module on which multiplication by m is an isomorphism,*

$$H_0(G; A) = H^0(G; A) = eA \quad \text{and} \quad H_*(G; A) = H^*(G; A) = 0 \text{ for } * \neq 0.$$

Proof $N^2 = (\sum g) \cdot N = m \cdot N$, so $e^2 = e$ in $R = \mathbb{Z}G[\frac{1}{m}]$. Note that $R \cong eR \times (1 - e)R$ as a ring, that $eR = \mathbb{Z}[\frac{1}{m}]$, and that the projection e from R-**mod** to (eR)-**mod** $\subseteq$ **Ab** is an exact functor. Let A be an R-module; we first show that $eA = A_G = A^G$. Clearly $N \cdot A \subseteq A^G$, and if $a \in A^G$, then $N \cdot a = m \cdot a$, that is, $a = e \cdot a$. Therefore $eA = A^G$. By exercise 6.1.3 (3), $\mathfrak{I}[\frac{1}{m}] = \ker(R \xrightarrow{e} R) = (1 - e)R$. Hence $(1 - e)A = (1 - e)R \otimes_R A$ equals $\mathfrak{I}[\frac{1}{m}] \otimes_R A = \mathfrak{I}A$; therefore $A_G = A/\mathfrak{I}A = A/(1 - e)A = eA$.

Because eR is projective over R, $\mathrm{Tor}_n^R(eR, A) = \mathrm{Ext}_R^n(eR, A) = 0$ if $n \neq 0$. Since R is flat over $\mathbb{Z}G$, flat base change for Tor (3.2.29) yields

$$H_n(G; A) = \mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A) = \mathrm{Tor}_n^R(\mathbb{Z} \otimes R, A) = \mathrm{Tor}_n^R(eR, A) = 0 \text{ if } n \neq 0.$$

For cohomology, we modify the argument used in 3.3.11 for localization of Ext. If $P \to \mathbb{Z}$ is a resolution of $\mathbb{Z}$ by projective $\mathbb{Z}G$-modules, then $P[\frac{1}{m}] \to \mathbb{Z}[\frac{1}{m}]$ is a resolution of $\mathbb{Z}[\frac{1}{m}] = eR$ by projective R-modules. Because A is an R-module, adjointness yields $\mathrm{Hom}_G(P, A) \cong \mathrm{Hom}_R(P[\frac{1}{m}], A)$. Thus for $n \neq 0$ we have

$$H^n(G; A) = H^n \mathrm{Hom}_G(P, A) \cong H^n \mathrm{Hom}_R(P[\frac{1}{m}], A) = \mathrm{Ext}_R^n(eR, A) = 0. \qquad \diamond$$

We now turn our attention to the first homology group H_1.

Exercise 6.1.4

1. Define $\theta: G \to \mathfrak{I}/\mathfrak{I}^2$ by $\theta(g) = g - 1$. Show that θ is a group homomorphism and that the commutator subgroup $[G, G]$ of G maps to zero.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

2. Define $\sigma: \mathfrak{I} \to G/[G,G]$ by $\sigma(g-1) = \bar{g}$, the (left) coset of g. Show that $\sigma(\mathfrak{I}^2) = 1$, and deduce that θ and σ induce an isomorphism $\mathfrak{I}/\mathfrak{I}^2 \cong G/[G,G]$.

Theorem 6.1.11 *For any group G, $H_1(G;\mathbb{Z}) \cong \mathfrak{I}/\mathfrak{I}^2 \cong G/[G,G]$.*

Proof The sequence $0 \to \mathfrak{I} \to \mathbb{Z}G \to \mathbb{Z} \to 0$ induces an exact sequence

$$H_1(G;\mathbb{Z}G) \to H_1(G;\mathbb{Z}) \to \mathfrak{I}_G \to (\mathbb{Z}G)_G \to \mathbb{Z} \to 0.$$

Since $\mathbb{Z}G$ is projective, $H_1(G;\mathbb{Z}G) = 0$. The right-hand map is the isomorphism $(\mathbb{Z}G)_G \cong \mathbb{Z}G/\mathfrak{I} \cong \mathbb{Z}$, so evidently $H_1(G;\mathbb{Z})$ is isomorphic to $\mathfrak{I}_G = \mathfrak{I}/\mathfrak{I}^2$. By the previous exercise, this is isomorphic to $G/[G,G]$. ◇

Theorem 6.1.12 *If A is any trivial G-module, $H_0(G;A) \cong A$, $H_1(G;A) \cong G/[G,G] \otimes_{\mathbb{Z}} A$, and for $n \geq 2$ there are (noncanonical) isomorphisms:*

$$H_n(G;A) \cong H_n(G;\mathbb{Z}) \otimes_{\mathbb{Z}} A \oplus \mathrm{Tor}_1^{\mathbb{Z}}(H_{n-1}(G;\mathbb{Z}), A).$$

Proof If $P \to \mathbb{Z}$ is a free right $\mathbb{Z}G$-module resolution, $H_*(G;A)$ is the homology of $P \otimes_{\mathbb{Z}G} A = (P \otimes_{\mathbb{Z}G} \mathbb{Z}) \otimes_{\mathbb{Z}} A$. Now use the Universal Coefficient Theorem. ◇

Exercises 6.1.5 Let A be a trivial G-module.

1. Show that $H^1(G;A)$ is isomorphic to the group $\mathrm{Hom}_{\mathbf{Groups}}(G,A) \cong \mathrm{Hom}_{\mathbf{Ab}}(G/[G,G],A)$ of all group homomorphisms from G to A.
2. Conclude that $H^1(G;\mathbb{Z}) = 0$ for every finite group.
3. Show that in general there is a split exact sequence

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(H_{n-1}(G;\mathbb{Z}),A) \to H^n(G;A) \to \mathrm{Hom}_{\mathbf{Ab}}(H_n(G;\mathbb{Z}),A) \to 0.$$

Exercise 6.1.6 If G is finite, show that $H^1(G;\mathbb{C}) = 0$ and that $H^2(G;\mathbb{Z})$ is isomorphic to the group $H^1(G,\mathbb{C}^*) \cong \mathrm{Hom}_{\mathbf{Groups}}(G,\mathbb{C}^*)$ of all 1-dimensional representations of G. Here G acts trivially on $\mathbb{Z}$, $\mathbb{C}$, and on the group $\mathbb{C}^*$ of complex units.

We now turn to the product $G \times H$ of two groups G and H. First note that $\mathbb{Z}[G \times H] \cong \mathbb{Z}G \otimes \mathbb{Z}H$. Indeed, the ring maps from $\mathbb{Z}G$ and $\mathbb{Z}H$ to $\mathbb{Z}[G \times H]$ induce a ring map from $\mathbb{Z}G \otimes \mathbb{Z}H$ to $\mathbb{Z}[G \times H]$. Both rings have the set $G \times H$ as a $\mathbb{Z}$-basis, so this map is an isomorphism. The Künneth formula gives the homology of $G \times H$:

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Proposition 6.1.13 (Products) *For every G and H there is a split exact sequence:*

$$0 \to \bigoplus_{\substack{p+q\\=n}} H_p(G;\mathbb{Z}) \otimes H_q(H;\mathbb{Z}) \to H_n(G\times H;\mathbb{Z}) \to \bigoplus_{\substack{p+q\\=n-1}} \mathrm{Tor}_1^{\mathbb{Z}}(H_p(G;\mathbb{Z}), H_q(H;\mathbb{Z})) \to 0.$$

Proof Let $P \to \mathbb{Z}$ be a free $\mathbb{Z}G$-resolution and $Q \to \mathbb{Z}$ a free $\mathbb{Z}H$-resolution, and write $P \otimes_{\mathbb{Z}} Q$ for the total tensor product chain complex (2.7.1), which is a complex of $\mathbb{Z}G \otimes \mathbb{Z}H$-modules. By the Künneth formula for complexes (3.6.3), the homology of $P \otimes_{\mathbb{Z}} Q$ is zero except for $H_0(P \otimes_{\mathbb{Z}} Q) = \mathbb{Z}$. Hence $P \otimes_{\mathbb{Z}} Q \to \mathbb{Z}$ is a free $\mathbb{Z}G \otimes \mathbb{Z}H$-module resolution of $\mathbb{Z}$, and $H_*(G\times H;\mathbb{Z})$ is the homology of

$$(P \otimes_{\mathbb{Z}} Q) \otimes_{\mathbb{Z}G\otimes\mathbb{Z}H} \mathbb{Z} \cong (P \otimes_{\mathbb{Z}G} \mathbb{Z}) \otimes_{\mathbb{Z}} (Q \otimes_{\mathbb{Z}H} \mathbb{Z}).$$

Moreover, $H_*(G;\mathbb{Z}) = H_*(P \otimes_{\mathbb{Z}G} \mathbb{Z})$ and $H_*(H;\mathbb{Z}) = (Q \otimes_{\mathbb{Z}H} \mathbb{Z})$. As each $P_n \otimes_{\mathbb{Z}G} \mathbb{Z}$ is a free $\mathbb{Z}$-module, the proposition follows from the Künneth formula for complexes. ◇

Exercise 6.1.7 (kG-**modules**) Let k be a field, considered as a trivial module. Modify the above proof to show that $H_n(G\times H;k) \cong \bigoplus H_p(G;k) \otimes_k H_{n-p}(H;k)$ for all n.

Cohomology Cross Product 6.1.14 Keeping the notation of the preceding proposition, there is a natural homomorphism of tensor product double complexes:

$$\mu\colon \mathrm{Hom}_G(P,\mathbb{Z}) \otimes \mathrm{Hom}_H(Q,\mathbb{Z}) \to \mathrm{Hom}_{G\times H}(P\otimes_{\mathbb{Z}} Q,\mathbb{Z}),$$

$$\mu(f\otimes f')(x\otimes y) = f(x)f'(y),\ x\in P_p,\ y\in Q_q.$$

The *cross product* $\times\colon H^p(G;\mathbb{Z}) \otimes H^q(H;\mathbb{Z}) \to H^{p+q}(G\times H;\mathbb{Z})$ is the composite obtained by taking the cohomology of the total complexes.

$$\begin{array}{ccc} H^p(G;\mathbb{Z}) \otimes H^q(H;\mathbb{Z}) & \longrightarrow & H^{p+q}[\mathrm{Hom}_G(P,\mathbb{Z}) \otimes \mathrm{Hom}_H(Q,\mathbb{Z})], \\ \times\downarrow & & \downarrow\mu \\ H^{p+q}(G\times H;\mathbb{Z}) & = & H^{p+q}[\mathrm{Hom}_{G\times H}(P\otimes Q,\mathbb{Z})] \end{array}$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.1.8 Suppose that each P_p is a finitely generated $\mathbb{Z}G$-module. (For example, this can be done when G is finite; see section 6.5 below.) Show in this case that μ is an *isomorphism.* Then deduce from the Künneth formula 3.6.3 that the cross product fits into a split short exact sequence:

$$0 \to \bigoplus_{\substack{p+q \\ =n}} H^p(G;\mathbb{Z}) \otimes H^q(H;\mathbb{Z}) \xrightarrow{\times} H^n(G \times H;\mathbb{Z})$$

$$\to \bigoplus_{\substack{p+q \\ =n+1}} \operatorname{Tor}_1^{\mathbb{Z}}(H^p(G;\mathbb{Z}), H^q(H;\mathbb{Z})) \to 0.$$

Exercises 6.1.9

1. Show that the cross product is independent of the choice of P and Q.
2. If $H = 1$, show that cross product with $1 \in H^0(1;\mathbb{Z})$ is the identity map.
3. Show that the cross product is associative in the sense that the two maps

$$H^p(G;\mathbb{Z}) \otimes H^q(H;\mathbb{Z}) \otimes H^r(I;\mathbb{Z}) \to H^{p+q+r}(G \times H \times I;\mathbb{Z})$$

given by the formulas $(x \times y) \times z$ and $x \times (y \times z)$ agree.

Exercise 6.1.10 Let k be a commutative ring.

1. Modify the above construction to obtain cross products $H^p(G;k) \otimes_k H^q(H;k) \to H^{p+q}(G \times H;k)$. Then verify that this cross product is independent of the choice of P and Q, that it is associative, and that the cross product with $1 \epsilon H^0(1;k) = k$ is the identity.
2. If k is a field, show that $H^n(G \times H;k) \cong \bigoplus H^p(G;k) \otimes_k H^{n-p}(H;k)$ for all n.

We will return to the cross product in section 6.7, when we introduce the restriction map $H^*(G \times G) \to H^*(G)$ and show that the cross product makes $H^*(G;\mathbb{Z})$ into a ring.

Hyperhomology 6.1.15 If A_* is a chain complex of G-modules, the hyper-derived functors $\mathbb{L}_i(-_G)(A_*)$ of 5.7.4 are written as $\mathbb{H}_i(G;A_*)$ and called the *hyperhomology* groups of G. Similarly, if A^* is a cochain complex of G-modules, the *hypercohomology* groups $\mathbb{H}^i(G;A^*)$ are just the hyper-derived functors $\mathbb{R}^i(-^G)(A^*)$. The generalities of Chapter 5, section 7 become the following facts in this case. The hyperhomology spectral sequences are

$${}^{II}E^2_{pq} = H_p(G;H_q(A_*)) \Rightarrow \mathbb{H}_{p+q}(G;A_*); \quad \text{and}$$

$${}^{I}E^2_{pq} = H_p(H_q(G;A_*)) \Rightarrow \mathbb{H}_{p+q}(G;A_*) \text{ when } A_* \text{ is bounded below,}$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

and the hypercohomology spectral sequences are

$$^{II}E_2^{pq} = H^p(G; H^q(A^*)) \Rightarrow \mathbb{H}^{p+q}(G; A^*), \text{ weakly convergent; and}$$

$$^{I}E_2^{pq} = H^p(H^q(G; A^*)) \Rightarrow \mathbb{H}^{p+q}(G; A^*) \text{ if } A \text{ is bounded below.}$$

In particular, suppose that A is bounded below. If each A_i is a flat $\mathbb{Z}G$-module, then $\mathbb{H}_i(G; A_*) = H_i((A_*)_G)$; if each A^i is a projective $\mathbb{Z}G$-module, then $\mathbb{H}^i(G; A^*) = H^i((A^*)^G)$.

Exercise 6.1.11 Let T be the infinite cyclic group. Show that there are short exact sequences

$$0 \to H_q(A_*)_T \to \mathbb{H}_q(T; A_*) \to H_{q-1}(A_*)^T \to 0;$$

$$0 \to H^{q-1}(A^*)_T \to \mathbb{H}^q(T; A^*) \to H^q(A^*)^T \to 0.$$

Exercise 6.1.12 Let k be a commutative ring and G a group such that all the k-modules $H_*(G; k)$ are flat. (For example, this is true for $G = T$.) Use the hypertor spectral sequence (5.7.8) to show that $H_n(G \times H; k) \cong \bigoplus H_p(G; k) \otimes_k H_{n-p}(H; k)$ for all n and H.

6.2 Cyclic and Free Groups

Cyclic and free groups are two classes of groups for which explicit calculations are easy to make. We first consider cyclic groups.

Calculation 6.2.1 (Cyclic groups) Let C_m denote the cyclic group of order m on generator σ. The norm in $\mathbb{Z}C_m$ is the element $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{m-1}$, so $0 = \sigma^m - 1 = (\sigma - 1)N$ in $\mathbb{Z}C_m$. I claim that the trivial C_m-module $\mathbb{Z}$ has the periodic free resolution

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}C_m \xleftarrow{\sigma-1} \mathbb{Z}C_m \xleftarrow{N} \mathbb{Z}C_m \xleftarrow{\sigma-1} \mathbb{Z}C_m \xleftarrow{N} \cdots.$$

Indeed, since $\mathbb{Z} \cdot N = (\mathbb{Z}G)^G$ and $\mathfrak{I} = \{a \in \mathbb{Z}G : Na = 0\}$ by exercise 6.1.3, there are exact sequences

$$0 \leftarrow \mathbb{Z} \cdot N \xleftarrow{N} \mathbb{Z}G \leftarrow \mathfrak{I} \leftarrow 0 \quad \text{and} \quad 0 \leftarrow \mathfrak{I} \xleftarrow{\sigma-1} \mathbb{Z}C_m \leftarrow \mathbb{Z} \cdot N \leftarrow 0.$$

The periodic free resolution is obtained by splicing these sequences together. Applying $\otimes_{\mathbb{Z}G} A$ and $\mathrm{Hom}_G(-, A)$ and taking homology, we find the following result:

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Theorem 6.2.2 *If A is a module for the cyclic group $G = C_m$, then*

$$H_n(C_m; A) = \left\{ \begin{array}{ll} A/(\sigma - 1)A & \text{if } n = 0 \\ A^G/NA & \text{if } n = 1, 3, 5, 7, \ldots \\ \{a \in A : Na = 0\}/(\sigma - 1)A & \text{if } n = 2, 4, 6, 8, \ldots \end{array} \right\};$$

$$H^n(C_m; A) = \left\{ \begin{array}{ll} A^G & \text{if } n = 0 \\ \{a \in A : Na = 0\}/(\sigma - 1)A & \text{if } n = 1, 3, 5, 7, \ldots \\ A^G/NA & \text{if } n = 2, 4, 6, 8, \ldots \end{array} \right\}.$$

Exercise 6.2.1 Show for $G = C_m$ that when $H^1(G; A) = 0$ there is an exact sequence

$$0 \to A^G \to A \xrightarrow{\sigma - 1} A \xrightarrow{N} A^G \to H^2(G; A) \to 0.$$

Example 6.2.3 Taking $A = \mathbb{Z}$ we find that

$$H_n(C_m; \mathbb{Z}) = \left\{ \begin{array}{ll} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}/m & \text{if } n = 1, 3, 5, 7, \ldots \\ 0 & \text{if } n = 2, 4, 6, 8, \ldots \end{array} \right\};$$

$$H^n(C_m; \mathbb{Z}) = \left\{ \begin{array}{ll} \mathbb{Z} & \text{if } n = 0 \\ 0 & \text{if } n = 1, 3, 5, 7, \ldots \\ \mathbb{Z}/m & \text{if } n = 2, 4, 6, 8, \ldots \end{array} \right\}.$$

Exercise 6.2.2 Calculate $H_*(C_m \times C_n; \mathbb{Z})$ and $H^*(C_m \times C_n; \mathbb{Z})$.

Definition 6.2.4 (Tate cohomology) Taking full advantage of this periodicity, we set

$$\widehat{H}^n(C_m; A) = \left\{ \begin{array}{ll} A^G/NA & \text{if } n \in \mathbb{Z} \text{ is even} \\ \{a \in A : NA = 0\}/(\sigma - 1)A & \text{if } n \in \mathbb{Z} \text{ is odd} \end{array} \right\}.$$

More generally, if G is a finite group and A is a G-module, we define the *Tate cohomology groups* of G to be the groups

$$\widehat{H}^n(G; A) = \left\{ \begin{array}{ll} H^n(G; A) & \text{if } n \geq 1 \\ A^G/NA & \text{if } n = 0 \\ \{a \in A : Na = 0\}/\mathcal{I}A & \text{if } n = -1 \\ H_{1-n}(G; A) & \text{if } n \leq -2 \end{array} \right\}.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.2.3 If G is a finite group and $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, show that there is a long exact sequence

$$\cdots \widehat{H}^{n-1}(G; C) \to \widehat{H}^n(G; A) \to \widehat{H}^n(G; B) \to \widehat{H}^n(G; C) \to \widehat{H}^{n+1}(G; A) \cdots.$$

Application 6.2.5 (Dimension-shifting) Given a G-module A, choose a short exact sequence $0 \to K \to P \to A \to 0$ with P projective. Shapiro's Lemma (6.3.2 below) implies that $\widehat{H}^*(G, P) = 0$ for all $* \in \mathbb{Z}$. Therefore $\widehat{H}^n(G; A) \cong \widehat{H}^{n+1}(G; K)$. This shows that every Tate cohomology group $\widehat{H}^n(G; A)$ determines the entire theory.

Proposition 6.2.6 *Let G be the free group on the set X, and consider the augmentation ideal $\mathfrak{I}$ of $\mathbb{Z}G$. Then $\mathfrak{I}$ is a free $\mathbb{Z}G$-module with basis the set $X - 1 = \{x - 1 : x \in X\}$.*

Proof We have seen that $\mathfrak{I}$ is a free abelian group with $\mathbb{Z}$-basis $\{g - 1 : g \in G, g \neq 1\}$. We claim that another $\mathbb{Z}$-basis is $\{g(x - 1) : g \in G, x \in X\}$. Every $g \in G$ may be written uniquely as a reduced word in the symbols $\{x, x^{-1} : x \in X\}$; write $G(x)$ (resp. $G(x^{-1})$) for the subset of all $g \in G$ ending in the symbol x (resp. in x^{-1}) so that $G - \{1\}$ is the disjoint union (over all $x \in X$) of the sets $G(x)$ and $G(x^{-1})$. The formulas

$$(gx - 1) = g(x - 1) + (g - 1) \quad \text{if } gx \in G(x)$$
$$(gx^{-1} - 1) = -(gx^{-1})(x - 1) + (g - 1) \quad \text{if } gx^{-1} \in G(x^{-1})$$

and induction on word length allow us to uniquely rewrite the basis $\{g - 1 : g \neq 1\}$ in terms of the set $\{g(x - 1)\}$, and vice versa. Therefore $\{g(x - 1) : g \in G, x \in X\}$ is a $\mathbb{Z}$-basis of $\mathfrak{I}$, and $X - 1 = \{x - 1 : x \in X\}$ is a $\mathbb{Z}G$-basis. ◇

Corollary 6.2.7 *If G is a free group on X, then $\mathbb{Z}$ has the free resolution*

$$0 \to \mathfrak{I} \to \mathbb{Z}G \to \mathbb{Z} \to 0.$$

Consequently, $pd_G(\mathbb{Z}) = 1$, that is, $H_n(G; A) = H^n(G; A) = 0$ for $n \neq 0, 1$. Moreover, $H_0(G; \mathbb{Z}) \cong H^0(G; \mathbb{Z}) \cong \mathbb{Z}$, while

$$H_1(G; \mathbb{Z}) \cong \bigoplus_{x \in X} \mathbb{Z} \quad \text{and} \quad H^1(G; \mathbb{Z}) \cong \prod_{x \in X} \mathbb{Z}.$$

Proof $H_*(G; A)$ is the homology of $0 \to \mathfrak{I} \otimes_{\mathbb{Z}G} A \to A \to 0$, and $H^*(G; A)$ is the cohomology of $0 \to A \to \mathrm{Hom}_G(\mathfrak{I}, A) \to 0$. For $A = \mathbb{Z}$, the differentials are zero. ◇

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Remark Conversely, Stallings [St] and Swan [SwCd1] proved that if $H^n(G,A)$ vanishes for all $n \neq 0, 1$ and all G-modules A, then G is a free group.

Exercise 6.2.4 Let G be the free group on $\{s,t\}$, and let $T \subseteq G$ be the free group on $\{t\}$. Let $\mathbb{Z}'$ denote the abelian group $\mathbb{Z}$, made into a G-module (and a T-module) by the formulas $s \cdot a = t \cdot a = -a$.

1. Show that $H_0(G, \mathbb{Z}') = H_0(T, \mathbb{Z}') = \mathbb{Z}/2$.
2. Show that $H_1(T, \mathbb{Z}') = 0$ but $H_1(G, \mathbb{Z}') \cong \mathbb{Z}$.

Free Products 6.2.8 Let $G*H$ denote the free product (or coproduct) of the groups G and H. By [BAII, 2.9], every element of $G*H$ except 1 has a unique expression as a "reduced" word, either of the form $g_1h_1g_2h_2g_3\cdots$ or of the form $h_1g_1h_2g_2h_3\cdots$ with all $g_i \in G$ and all $h_i \in H$ (and all $g_i, h_i \neq 1$).

Proposition 6.2.9 *Let $\mathfrak{I}_G$, $\mathfrak{I}_H$, and $\mathfrak{I}_{G*H}$ denote the augmentation ideals of $\mathbb{Z}G$, $\mathbb{Z}H$, and $\Lambda = \mathbb{Z}(G*H)$, respectively. Then*

$$\mathfrak{I}_{G*H} \cong (\mathfrak{I}_G \otimes_{\mathbb{Z}G} \Lambda) \oplus (\mathfrak{I}_H \otimes_{\mathbb{Z}H} \Lambda).$$

Proof As a left $\mathbb{Z}G$-module, $\Lambda = \mathbb{Z}(G*H)$ has a basis consisting of $\{1\}$ and the set of all reduced words beginning with an element of H. Therefore $\mathfrak{I}_G \otimes_{\mathbb{Z}G} \Lambda$ has a $\mathbb{Z}$-basis $\mathcal{B}_1$ consisting of the basis $\{g-1 | g \in G,\ g \neq 1\}$ of $\mathfrak{I}_G$ and the set of all terms

$$(g-1)(h_1g_1h_2\cdots) = (gh_1g_1h_2\cdots) - (h_1g_1h_2\cdots).$$

Similarly, $\mathfrak{I}_H \otimes_{\mathbb{Z}H} \Lambda$ has a $\mathbb{Z}$-basis $\mathcal{B}_2$ consisting of $\{h-1\}$ and the set of all terms

$$(h-1)(g_1h_1g_2\cdots) = (hg_1h_1g_2\cdots) - (g_1h_1g_2\cdots).$$

By induction on the length of a reduced word w in $G*H$, we see that $w-1$ can be written as a sum of terms in $\mathcal{B}_1$ and $\mathcal{B}_2$. This proves that $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ generates $\mathfrak{I}_{G*H}$. In any nontrivial sum of elements of $\mathcal{B}$, the coefficients of the longest words must be nonzero, so $\mathcal{B}$ is linearly independent. This proves that $\mathcal{B}$ forms a $\mathbb{Z}$-basis for $\mathfrak{I}_{G*H}$, and hence that $\mathfrak{I}_{G*H}$ has the decomposition we described. ◇

Corollary 6.2.10 *For every left $(G*H)$-module A, and $n \geq 2$:*

$$H_n(G*H; A) \cong H_n(G; A) \oplus H_n(H; A);$$
$$H^n(G*H; A) \cong H^n(G; A) \oplus H^n(H; A).$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Remark When $n = 0$, the conclusion fails even for $A = \mathbb{Z}$. We gave an example above of a $(T*T)$-module $\mathbb{Z}'$ for which the conclusion fails when $n = 1$.

Proof We give the proof of the homology assertion, the cohomology part being entirely analogous. Write Λ for $\mathbb{Z}(G*H)$. Because $\mathrm{Tor}_n^{\Lambda}(\Lambda, A) = 0$ for $n \geq 1$, we see that $\mathrm{Tor}_n^{\Lambda}(\mathbb{Z}, A) \cong \mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_{G*H}, A)$ for $n \geq 2$. Hence in this range

$$H_n(G*H; A) = \mathrm{Tor}_n^{\Lambda}(\mathbb{Z}, A) \cong \mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_{G*H}, A)$$
$$\cong \mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_G \otimes_{\mathbb{Z}G} \Lambda, A) \oplus \mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_H \otimes_{\mathbb{Z}H} \Lambda, A).$$

Since Λ is free over $\mathbb{Z}G$ and $\mathbb{Z}H$, base-change for Tor (3.2.9 or 5.6.6) implies that

$$\mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_G \otimes_{\mathbb{Z}G} \Lambda, A) \cong \mathrm{Tor}_{n-1}^{\mathbb{Z}G}(\mathfrak{I}_G, A) \cong \mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A) = H_n(G; A).$$

By symmetry, $\mathrm{Tor}_{n-1}^{\Lambda}(\mathfrak{I}_H \otimes_{\mathbb{Z}H} \Lambda, A) \cong H_n(H; A)$. ◇

Exercise 6.2.5 Show that if A is a trivial $G*H$-module, then for $n = 1$ we also have

$$H_1(G*H; A) \cong H_1(G; A) \oplus H_1(H; A);$$
$$H^1(G*H; A) \equiv H^1(G; A) \oplus H^1(H; A).$$

6.3 Shapiro's Lemma

For actually performing calculations, Shapiro's Lemma is a fundamental tool. Suppose that H is a subgroup of G and A is a left $\mathbb{Z}H$-module. We know (2.6.2) that $\mathbb{Z}G \otimes_{\mathbb{Z}H} A$ and $\mathrm{Hom}_H(\mathbb{Z}G, A)$ are left $\mathbb{Z}G$-modules. Here are their names:

Definition 6.3.1 $\mathbb{Z}G \otimes_{\mathbb{Z}H} A$ is called the *induced G-module* and is written $\mathrm{Ind}_H^G(A)$. Similarly, $\mathrm{Hom}_H(\mathbb{Z}G, A)$ is called the *coinduced G-module* and is written $\mathrm{Coind}_H^G(A)$.

Shapiro's Lemma 6.3.2 Let H be a subgroup of G and A an H-module. Then

$$H_*(G; \mathrm{Ind}_H^G(A)) \cong H_*(H; A); \text{ and } H^*(G; \mathrm{Coind}_H^G(A)) \cong H^*(H; A).$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Proof Note that $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module (any set of coset representatives will form a basis). Hence any projective right $\mathbb{Z}G$-module resolution $P \to \mathbb{Z}$ is also a projective $\mathbb{Z}H$-module resolution. Therefore the homology of the chain complex

$$P \otimes_{\mathbb{Z}G} (\mathbb{Z}G \otimes_{\mathbb{Z}H} A) \cong P \otimes_{\mathbb{Z}H} A$$

is both

$$\mathrm{Tor}_*^{\mathbb{Z}G}(\mathbb{Z}, \mathbb{Z}G \otimes_{\mathbb{Z}H} A) \cong H_*(G; \mathrm{Ind}_H^G(A))$$

and $\mathrm{Tor}_*^{\mathbb{Z}H}(\mathbb{Z}, A) \cong H_*(H; A)$. Similarly, if $P \to \mathbb{Z}$ is a projective left $\mathbb{Z}G$-module resolution, then there is an adjunction isomorphism of cochain complexes:

$$\mathrm{Hom}_G(P, \mathrm{Hom}_H(\mathbb{Z}G, A)) \cong \mathrm{Hom}_H(P, A).$$

The cohomology of this complex is both

$$\mathrm{Ext}^*_{\mathbb{Z}G}(\mathbb{Z}, \mathrm{Hom}_H(\mathbb{Z}G, A)) \cong H^*(G; \mathrm{Coind}_H^G(A))$$
$$\text{and} \quad \mathrm{Ext}^*_{\mathbb{Z}H}(\mathbb{Z}, A) \cong H^*(H; A). \qquad \diamond$$

Corollary 6.3.3 (Shapiro's Lemma for $H = 1$) *If A is an abelian group, then*

$$H_*(G; \mathbb{Z}G \otimes_{\mathbb{Z}} A) = H^*(G; \mathrm{Hom}_{\mathbf{Ab}}(\mathbb{Z}G, A)) = \left\{ \begin{matrix} A & \text{if } * = 0 \\ 0 & \text{if } * \neq 0 \end{matrix} \right\}.$$

Lemma 6.3.4 *If the index $[G : H]$ is finite,* $\mathrm{Ind}_H^G(A) \cong \mathrm{Coind}_H^G(A)$.

Proof Let X be a set of left coset representatives for G/H, so that X forms a basis for the right H-module $\mathbb{Z}G$. $\mathrm{Ind}_H^G(A)$ is the sum over X of copies $x \otimes A$ of A, with $g(x \otimes a) = y \otimes ha$ if $gx = yh$ in G. Now $X^{-1} = \{x^{-1} : x \in X\}$ is a basis of $\mathbb{Z}G$ as a left H-module, so $\mathrm{Coind}_H^G(A)$ is the product over X of copies $\pi_x A$ of A, where $\pi_x a$ represents the H-map from $\mathbb{Z}G$ to A sending x^{-1} to $a \in A$ and z^{-1} to 0 for all $z \neq x$ in X. Therefore if $gx = yh$, that is, $y^{-1}g = hx^{-1}$, the map $g(\pi_x a)$ sends y^{-1} to

$$(\pi_x a)(y^{-1}g) = (\pi_x a)(hx^{-1}) = h \cdot (\pi_x a)(x^{-1}) = ha$$

and z^{-1} to 0 if $z \neq y$ in X. That is, $g(\pi_x a) = \pi_y(ha)$. Since $X \cong [G : H]$ is finite, the map $\mathrm{Ind}_H^G(A) \to \mathrm{Coind}_H^G(A)$ sending $x \otimes a$ to $\pi_x a$ is an H-module isomorphism. $\diamond$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Corollary 6.3.5 *If G is a finite group, then $H^*(G; \mathbb{Z}G \otimes_{\mathbb{Z}} A) = 0$ for $* \neq 0$ and all A.*

Corollary 6.3.6 (Tate cohomology) *If G is finite and P is a projective G-module,*

$$\widehat{H}^*(G; P) = 0 \quad \textit{for all } *.$$

Proof It is enough to prove the result for free G-modules, that is, for modules of the form $P = \mathbb{Z}G \otimes_{\mathbb{Z}} F$, where F is free abelian. Shapiro's Lemma gives vanishing for $* \neq 0, -1$. Since $P^G = (\mathbb{Z}G)^G \otimes F = N \cdot P$, we get $\widehat{H}^0(G; P) = 0$. Finally, $\widehat{H}^{-1}(G; P) = 0$ follows from the fact that $N = \#G$ on the free abelian group $P_G = P/\mathfrak{I}P \cong F$. ◇

Hilbert's Theorem 90 6.3.7 (Additive version) Let $K \subset L$ be a finite Galois extension of fields, with Galois group G. Then L is a G-module, $L^G \cong L_G \cong K$, and

$$H^*(G; L) = H_*(G; L) = 0 \text{ for } * \neq 0.$$

Proof The Normal Basis Theorem [BAI, p. 283] asserts that there is an $x \in L$ such that the set $\{g(x) : g \in G\}$ of its conjugates forms a basis of the K-vector space L. Hence $L \cong \mathbb{Z}G \otimes_{\mathbb{Z}} K$ as a G-module. We now cite Shapiro's Lemma. ◇

Example 6.3.8 (Cyclic Galois extensions) Suppose that G is cyclic of order m, generated by σ. The *trace* $tr(x)$ of an element $x \in L$ is the element $x + \sigma x + \cdots + \sigma^{m-1}x$ of K. In this case, Hilbert's Theorem 90 states that there is an exact sequence

$$0 \to K \to L \xrightarrow{\sigma - 1} L \xrightarrow{tr} K \to 0.$$

Indeed, we saw in the last section that for $* \neq 0$ every group $H_*(G; L)$ and $H^*(G; L)$ is either $K/tr(L)$ or $\ker(tr)/(\sigma - 1)K$.

As an application, suppose that $\mathrm{char}(K) = p$ and that $[L : K] = p$. Since $tr(1) = p \cdot 1 = 0$, there is an $x \in L$ such that $(\sigma - 1)x = 1$, that is, $\sigma x = x + 1$. Hence $L = K(x)$ and $x^p - x \in K$ because

$$\sigma(x^p - x) = (x + 1)^p - (x + 1) = x^p - x.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Remark If G is not cyclic, we will see in the next section that the vanishing of $H^1(G; L)$ is equivalent to Noether's Theorem [BAI, p. 287] that if $D: G \to L$ is a map satisfying $D(gh) = D(g) + g \cdot D(h)$, then there is an $x \in L$ such that $D(g) = g \cdot x - x$.

Application 6.3.9 (Transfer) Let H be a subgroup of finite index in G. Considering a G-module A as an H-module, we obtain a canonical map from A to $\mathrm{Hom}_H(\mathbb{Z}G, A) = \mathrm{Coind}_H^G(A) \cong \mathrm{Ind}_H^G(A)$ and from $\mathrm{Coind}_H^G(A) \cong \mathbb{Z}G \otimes_{\mathbb{Z}H} A$ to A. Applying Shapiro's Lemma, we obtain *transfer maps* $H_*(G; A) \to H_*(H; A)$ and $H^*(H; A) \to H^*(G; A)$. We will return to these maps in exercise 6.7.7 when we discuss restriction.

6.4 Crossed Homomorphisms and H^1

If A is a bimodule over any ring R, a *derivation* of R in A is an abelian group homomorphism $D: R \to A$ satisfying the *Leibnitz rule:* $D(rs) = rD(s) + D(r)s$. When $R = \mathbb{Z}G$ and A is a *left* $\mathbb{Z}G$-module, made into a bimodule by giving it a trivial right G-module structure, this definition simplifies as follows:

Definition 6.4.1 A *derivation* (or *crossed homomorphism*) of G in a left G-module A is a set map $D: G \to A$ satisfying $D(gh) = gD(h) + D(g)$. The family $\mathrm{Der}(G, A)$ of all derivations is an abelian group in an obvious way: $(D + D')(g) = D(g) + D'(g)$.

Example 6.4.2 (Principal derivations) If $a \in A$, define $D_a(g) = ga - a$; D_a is a derivation because

$$D_a(gh) = (gha - ga) + (ga - a) = gD_a(h) + D_a(g).$$

The D_a are called the *principal derivations* of G in A. Since $D_a + D_b = D_{(a+b)}$, the set $\mathrm{PDer}(G, A)$ of principal derivations forms a subgroup of $\mathrm{Der}(G, A)$.

Exercise 6.4.1 Show that $\mathrm{PDer}(G, A) \cong A/A^G$.

Example 6.4.3 If $\varphi: \mathfrak{I} \to A$ is a G-map, let $D_\varphi: G \to A$ be defined by $D_\varphi(g) = \varphi(g - 1)$. This is a derivation, since

$$D_\varphi(gh) = \varphi(gh - 1) = \varphi(gh - g) + \varphi(g - 1) = gD_\varphi(h) + D_\varphi(g).$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Lemma 6.4.4 *The map $\varphi \mapsto D_\varphi$ is a natural isomorphism of abelian groups*

$$\mathrm{Hom}_G(\mathfrak{I}, A) \cong \mathrm{Der}(G, A).$$

Proof The formula defines a natural homomorphism from $\mathrm{Hom}_G(\mathfrak{I}, A)$ to $\mathrm{Der}(G, A)$, so it suffices to show that this map is an isomorphism. Since $\{g - 1 : g \neq 1\}$ forms a basis for the abelian group $\mathfrak{I}$, if $D_\varphi(g) = 0$ for all g, then $\varphi = 0$. Therefore the map in question is an injection. If D is a derivation, define $\varphi(g - 1) = D(g) \in A$. Since $\{g - 1 : g \neq 1\}$ forms a basis of $\mathfrak{I}$, φ extends to an abelian group map $\varphi: \mathfrak{I} \to A$. Since

$$\begin{aligned}\varphi(g(h - 1)) &= \varphi(gh - 1) - \varphi(g - 1)\\ &= D(gh) - D(g) = gD(h)\\ &= g\varphi(h - 1),\end{aligned}$$

φ is a $G-$map. As $D_\varphi = D$, the map in question is also a surjection. ◇

Theorem 6.4.5 $H^1(G; A) \cong \mathrm{Der}(G, A)/\mathrm{PDer}(G, A)$.

Proof The sequence $0 \to \mathfrak{I} \to \mathbb{Z}G \to \mathbb{Z} \to 0$ induces an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}, A) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}G, A) & \longrightarrow & \mathrm{Hom}_G(\mathfrak{I}, A) & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}G}(\mathbb{Z}, A) \longrightarrow 0. \\ & & \| & & \| & & \| & & \| \\ & & A^G & \hookrightarrow & A & \longrightarrow & \mathrm{Der}(G, A) & \longrightarrow & H^1(G; A) \end{array}$$

Now $A \to \mathrm{Hom}_G(\mathfrak{I}, A)$ sends $a \in A$ to the map φ sending $(g - 1)$ to $(g - 1)a$. Under the identification of $\mathrm{Hom}_G(\mathfrak{I}, A)$ with $\mathrm{Der}(G, A)$, φ corresponds to the principal derivation $D_\varphi = D_a$. Hence the image of A in $\mathrm{Der}(G, A)$ is $\mathrm{PDer}(G, A)$, as claimed. ◇

Corollary 6.4.6 *If A is a trivial G-module,*

$$H^1(G; A) \cong \mathrm{Der}(G, A) \cong \mathrm{Hom}_{\mathbf{Groups}}(G, A).$$

Proof $\mathrm{PDer}(G, A) \cong A/A^G = 0$ and a derivation is a group homomorphism. ◇

Hilbert's Theorem 90 6.4.7 (Multiplicative version) *Let $K \subset L$ be a finite Galois extension of fields, with Galois group G. Let L^* denote the group of units in L. Then L^* is a G-module, and $H^1(G; L^*) = 0$.*

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Proof Using multiplicative notation, a derivation is a map $\theta: G \to L^*$ such that $\theta(gh)/\theta(g) = g \cdot \theta(h)$. These are "Noether's equations"; the usual Theorem 90 [BAI, p. 286] states that if θ satisfies Noether's equations then $\theta(g) = (g \cdot x)/x$ for some $x \in L^*$, that is, θ is a principal derivation. ◇

Example 6.4.8 (Cyclic Galois extensions) Hilbert originally proved his Theorem 90 for cyclic field extensions in his 1897 report, *Theorie der Algebraische Zahlkörper*. Let $K \subset L$ be a cyclic Galois extension of fields, with Galois group C_m. The *norm* Nx of an element $x \in L$ is the product $\Pi g(x)$; as $H^1(C_m; L^*) = \{x : Nx = 1\}/(\sigma - 1)L^*$ (see 6.2.2), we may rephrase Hilbert's Theorem 90 as stating that whenever $Nx = 1$, there is a $y \in L$ such that $x = (\sigma y)/y$. Since $H^2(C_m; L^*) = L^{*G}/\{Nx : x \in L^*\} = K^*/NL^*$,

$$1 \to K^* \to L^* \xrightarrow{\sigma - 1} L^* \xrightarrow{N} K^* \to H^2(C_m; L^*) \to 1$$

is exact. (See exercise 6.2.1.) For the cyclic extension $\mathbb{R} \subset \mathbb{C}$ it is easy to calculate that $H^2(C_2; \mathbb{C}^*) \cong \mathbb{Z}/2$, so the higher analogue of the additive version of Theorem 90 fails for $H^*(G; L^*)$.

Remark The group $H^2(G; L^*)$ is usually nonzero. We will return to this topic in 6.6.11, identifying $H^2(G; L^*)$ with the *relative Brauer group* $Br(L/K)$ of all simple algebras Λ with center K and $\dim_K \Lambda = n^2$, $n = [L : K]$, such that $\Lambda \otimes_K L$ is the matrix ring $M_n(L)$. The nonzero element of $Br(\mathbb{C}/\mathbb{R}) \cong H^2(C_2; \mathbb{C}^*) \cong \mathbb{Z}/2$ corresponds to the 4-dimensional quaternion algebra $\mathbb{H}$, which has center $\mathbb{R}$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$.

In order to indicate the historical origins of the terminology "crossed homomorphism," we introduce the *semidirect product* $A \rtimes G$ of a group G with a G-module A. $A \rtimes G$ is a group whose underlying set is the product $A \times G$, and whose multiplication is given by the formula

$$(a, g) \cdot (b, h) = (a + gb, gh).$$

The semidirect product contains $A = A \times 1$ as a normal subgroup. It also contains the subgroup $0 \times G$, which maps isomorphically onto the quotient $G = (A \rtimes G)/A$.

Definition 6.4.9 If σ is an automorphism of $A \rtimes G$, we say that σ *stabilizes* A *and* G if $\sigma(a) = a$ for $a \in A$ and the induced automorphism on $G \cong (A \rtimes G)/A$ is the identity.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.4.2 If D is a derivation of G in A, show that σ_D, defined by

$$\sigma_D(a, g) = (a + D(g), g),$$

is an automorphism of $A \rtimes G$ stabilizing A and G, and that $\mathrm{Der}(G, A)$ is isomorphic to the subgroup of $\mathrm{Aut}(A \rtimes G)$ consisting of automorphisms stabilizing A and G. Show that $\mathrm{PDer}(G, A)$ corresponds to the inner automorphisms of $A \rtimes G$ obtained by conjugating by elements of A, with the principal derivation D_a given by $D_a(g) = a^{-1}ga$. Conclude that $H^1(G; A)$ is the group of outer automorphisms stabilizing A and G.

Example 6.4.10 (Dihedral groups) Let C_2 act on the cyclic group $\mathbb{Z}/m = C_m$ by $\sigma(a) = -a$. The semidirect product $C_m \rtimes C_2$ is the *dihedral group* D_m of symmetries of the regular m–gon. Our calculations in section 6.2 show that $H^1(C_2; C_m) \cong C_m/2C_m$. If m is even, D_m has an outer (= *not* inner) automorphism with $\varphi(0, \sigma) = (1, \sigma)$. If m is odd, every automorphism of D_m is inner.

6.5 The Bar Resolution

There are two canonical resolutions B_* and B_*^u of the trivial G-module $\mathbb{Z}$ by free left $\mathbb{Z}G$-modules, called the *normalized* and *unnormalized bar resolutions*, respectively. We shall now describe these resolutions.

$$(*) \qquad 0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} B_0 \xleftarrow{d} B_1 \xleftarrow{d} B_2 \xleftarrow{d} \cdots.$$

$$(**) \qquad 0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} B_0^u \xleftarrow{d} B_1^u \xleftarrow{d} B_2^u \xleftarrow{d} \cdots.$$

B_0 and B_0^u are $\mathbb{Z}G$. Letting the symbol [ ] denote $1 \in \mathbb{Z}G$, the map $\epsilon\colon B_0 \to \mathbb{Z}$ sends [ ] to 1. For $n \geq 1$, B_n^u is the free $\mathbb{Z}G$-module on the set of all symbols $[g_1 \otimes \cdots \otimes g_n]$ with $g_i \in G$, while B_n is the free $\mathbb{Z}G$-module on the (smaller) set of all symbols $[g_1 | \cdots | g_n]$ with the $g_i \in G - \{1\}$. We shall frequently identify B_n with the quotient of B_n^u by the submodule S_n generated by the set of all symbols $[g_1 \otimes \cdots \otimes g_n]$ with some g_i equal to 1.

Definition 6.5.1 For $n \geq 1$, define the differential $d\colon B_n^u \to B_{n-1}^u$ to be $d = \sum_{i=0}^{n}(-1)^i d_i$, where:

$$d_0([g_1 \otimes \cdots \otimes g_n]) = g_1[g_2 \otimes \cdots \otimes g_n];$$

$$d_i([g_1 \otimes \cdots \otimes g_n]) = [g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes \cdots \otimes g_n] \quad \text{for } i = 1, \ldots, n-1;$$

$$d_n([g_1 \otimes \cdots \otimes g_n]) = [g_1 \otimes \cdots \otimes g_{n-1}].$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

The differential for B_* is given by formulas similar for those on B^u_*, except that for $i = 1, \ldots, n-1$

$$d_i([g_1|\cdots|g_n]) = \begin{cases} [g_1|\cdots|g_ig_{i+1}|\cdots|g_n] & \text{when } g_ig_{i+1} \neq 1 \\ 0 & \text{when } g_ig_{i+1} = 1. \end{cases}$$

To avoid the clumsy case when $g_ig_{i+1} = 1$, we make the convention that $[g_1|\cdots|g_n] = 0$ if any $g_i = 1$. *Warning:* With this convention, the above formula for $d_i([g_1|\cdots])$ does not hold when g_i or $g_{i+1} = 1$; the formula for the alternating sum d does hold because the d_i and d_{i-1} terms cancel.

Examples 6.5.2

1. The image of the map $d: B_1 \to B_0$ is the augmentation ideal $\mathfrak{I}$ because $d([g]) = g[\,] - [\,] = (g-1)[\,]$. Therefore $(*)$ and $(**)$ are exact at B_0.
2. $d([g|h]) = g[h] - [gh] + [g]$.
3. $d([f|g|h]) = f[g|h] - [fg|h] + [f|gh] - [f|g]$.
4. If $G = C_2$, then $B_n = \mathbb{Z}G$ for all n on $[\sigma|\cdots|\sigma]$ and $(*)$ is familiar from 6.2.1:

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \xleftarrow{\sigma-1} \mathbb{Z}G \xleftarrow{\sigma+1} \mathbb{Z}G \xleftarrow{\sigma-1} \cdots.$$

Exercises 6.5.1

1. Show that $d \circ d = 0$, so that B^u_* is a chain complex. *Hint:* If $i \leq j-1$, show that $d_id_j = d_{j-1}d_i$.
2. Show that $d(S_n)$ lies in S_{n-1}, so that S_* is a subcomplex of B^u_*.
3. Conclude that B_* is a quotient chain complex of B^u_*.

Theorem 6.5.3 *The sequences $(*)$ and $(**)$ are exact. Thus both B_* and B^u_* are resolutions of $\mathbb{Z}$ by free left $\mathbb{Z}G$-modules.*

Proof It is enough to prove that $(*)$ and $(**)$ are split exact as chain complexes of abelian groups. As the proofs are the same, we give the proof in the B_* case. Consider the abelian group maps s_n determined by

$$s_{-1}: \mathbb{Z} \to B_0, \qquad s_{-1}(1) = [\,];$$
$$s_n: B_n \to B_{n+1}, \quad s_n(g_0[g_1|\cdots|g_n]) = [g_0|g_1|\cdots|g_n].$$

Visibly, $\epsilon s_{-1} = 1$ and $ds_0 + s_{-1}\epsilon$ is the identity map on B_0. If $n \geq 1$, the first term of $ds_n(g_0[g_1|\cdots|g_n])$ is $g_0[g_1|\cdots|g_n]$, and the remaining terms are exactly the terms of $s_{n-1}d(g_0[g_1|\cdots|g_n])$ with a sign change. This yields

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

the final identity $ds_n + s_{n-1}d = 1$ needed to show that $\{s_n\}$ forms a chain contraction of $(*)$. $\diamond$

Application 6.5.4 (Homology) For every right G-module A, $H_*(G; A)$ is the homology of the chain complex $A \otimes B_*$. (If A is a left G-module, we must take the homology of $B'_* \otimes A$, where B'_* is the mirror image bar resolution.) In particular, we see that $H_1(G; \mathbb{Z})$ is the quotient of the free abelian group on the symbols $[g]$, $g \in G$, by the relations that $[1] = 0$ and $[f] + [g] = [fg]$ for all $f, g \in G$. This recovers the calculation in 6.1.11 that

$$H_1(G; \mathbb{Z}) = G/[G, G].$$

Application 6.5.5 (Cohomology) If A is a left G-module, $H^*(G; A)$ is the cohomology of either $\mathrm{Hom}_G(B^u_*, A)$ or $\mathrm{Hom}_G(B_*, A)$. An *n-cochain* is a set map φ from $G^n = G \times \cdots \times G$ to A; elements of $\mathrm{Hom}_G(B^u_n, A)$ are just n-cochains. A cochain φ is *normalized* if $\varphi(g_1, \cdots)$ vanishes whenever some $g_i = 1$; these are the elements of $\mathrm{Hom}_G(B_n, A)$. The differential $d\varphi$ of an n-cochain is the $(n+1)$-cochain

$$(d\varphi)(g_0, \cdots, g_n) = g_0\varphi(g_1, \cdots, g_n) + \sum (-1)^i \varphi(\cdots, g_i g_{i+1}, \cdots) + \varphi(g_0, \cdots, g_{n-1}).$$

The n-cochains such that $d\varphi = 0$ are *n-cocycles*, and the n-cochains $d\varphi$ are called *n-coboundaries*. We write $Z^n(G; A)$ and $B^n(G; A)$ for the groups of all n-cocycles and n-coboundaries, respectively. Thus $H^n(G; A) = Z^n(G; A)/B^n(G; A)$.

Example 6.5.6 A 0-cochain is a map $1 \to A$, that is, an element of A. If $a \in A$, then da is the map $G \to A$ sending g to $ga - a$. Thus a is a 0-cocycle iff $a \in A^G$, and the set $B^1(G; A)$ of 1-coboundaries is the set $\mathrm{PDer}(G, A)$ of principal derivations.

The set $Z^1(G; A)$ of 1-cocyles is $\mathrm{Der}(G, A)$, because a 1-cocyle is a function D with $D(1) = 0$ and $gD(h) - D(gh) + D(g) = D(d[g|h]) = 0$. Therefore, the bar resolution provides a direct proof of the isomorphism $H^1(G; A) \cong \mathrm{Der}(G, A)/\mathrm{PDer}(G, A)$ of 6.4.5.

Example 6.5.7 $B^2(G; A)$ is the set of all $\psi: G \times G \to A$ such that $\psi(1, g) = \psi(g, 1)$ and

$$\psi(f, g) = \beta(d[f|g]) = f \cdot \beta(g) - \beta(fg) + \beta(f) \quad \text{for some } \beta: G \to A.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

$Z^2(G; A)$ is the set of all 2-cochains $\psi: G \times G \to A$ such that $\psi(1, g) = \psi(g, 1)$ and

$$f \cdot \psi(g, h) - \psi(fg, h) + \psi(f, gh) - \psi(f, g) = 0 \quad \text{for every } f, g, h \in G.$$

Theorem 6.5.8 *Let G be a finite group with m elements. Then for $n \neq 0$ and every G-module A, both $H_n(G; A)$ and $H^n(G; A)$ are annihilated by m, that is, they are $\mathbb{Z}/m$-modules.*

Proof Let η denote the endomorphism of B_*, which is multiplication by $(m - N)$ on B_0 and multiplication by m on B_n, $n \neq 0$. We claim that η is null homotopic. Applying $A\otimes$ or $\mathrm{Hom}(-, A)$, will then yield a null homotopic map, which must become zero upon taking homology, proving the theorem.

Define $\nu_n: B_n \to B_{n+1}$ by the formula

$$\nu_n([g_1|\cdots|g_n]) = (-1)^{n+1} \sum_{g \in G} [g_1|\cdots|g_n|g].$$

Setting $\omega = [g_1|\cdots|g_n]$ and $\epsilon = (-1)^{n+1}$, we compute for $n \neq 0$

$$d\nu_n(\omega) = \epsilon \sum \{g_1[\cdots|g] + \sum (-1)^i [\cdots|g_i g_{i+1}|\cdots|g] - \epsilon[\cdots|g_{n-1}|g_n g] + \epsilon\omega\}$$

$$\nu_{n-1} d(\omega) = -\epsilon \sum \{g_1[\cdots|g] + \sum (-1)^i [\cdots|g_i g_{i+1}|\cdots|g] - \epsilon[\cdots|g_{n-1}|g]\}.$$

As the sums over all $g \in G$ of $[\cdots|g_n g]$ and $[\cdots|g]$ agree, we see that $(d\nu + \nu d)(\omega)$ is $\epsilon^2 \sum \omega = m\omega$. Now $d\nu_0([\,]) = d(-\sum [g]) = (m - N)[\,]$, where $N = \sum g$ is the norm. Thus $\{\nu_n\}$ provides the chain contraction needed to make η null homotopic. ◇

Corollary 6.5.9 *Let G be a finite group of order m, and A a G-module. If A is a vector space over $\mathbb{Q}$, or a $\mathbb{Z}[\frac{1}{m}]$-module, then $H_n(G; A) = H^n(G; A) = 0$ for $n \neq 0$. (We had already proven this result in 6.1.10 using a more abstract approach.)*

Corollary 6.5.10 *If G is a finite group and A is a finitely generated G-module, then $H_n(G; A)$ and $H^n(G; A)$ are* finite abelian *groups for all $n \neq 0$.*

Proof Each $A \otimes_{\mathbb{Z}G} B_n$ and $\mathrm{Hom}_G(B_n, A)$ is a finitely generated abelian group. Hence $H_n(G; A)$ and $H^n(G; A)$ are finitely generated $\mathbb{Z}/m$-modules when $n \neq 0$. ◇

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Shuffle Product 6.5.11 When G is an abelian group, the normalized bar complex B_* is actually a graded-commutative differential graded algebra (or DG-algebra; see 4.5.2) under a product called the *shuffle product*. If $p \geq 0$ and $q \geq 0$ are integers, a (p,q)-*shuffle* is a permutation σ of the set $\{1, \cdots, p+q\}$ of integers in such a way that $\sigma(1) < \sigma(2) < \cdots < \sigma(p)$ and $\sigma(p+1) < \cdots < \sigma(p+q)$. The name comes from the fact that the (p,q)-shuffles describe all possible ways of shuffling a deck of $p+q$ cards, after first cutting the deck between the p and $(p+1)^{st}$ cards.

If G is any group, we define the *shuffle product* $*$: $B_p \otimes_{\mathbb{Z}} B_q \to B_{p+q}$ by

$$a[g_1|\cdots|g_p] * b[g_{p+1}|\cdots|g_{p+q}] = \sum_{\sigma} (-1)^{\sigma} ab[g_{\sigma^{-1}1}|g_{\sigma^{-1}2}|\cdots|g_{\sigma^{-1}(p+q)}],$$

where the summation is over all (p,q)-shuffles σ. The shuffle product is clearly bilinear, and $[\,] * [g_1|\cdots|g_q] = [g_1|\cdots|g_q]$, so B_* is a graded ring with unit $[\,]$, and the inclusion of $\mathbb{Z}G = B_0$ in B_* is a ring map.

Examples 6.5.12 $[g] * [h] = [g|h] - [h|g]$, and

$$[f] * [g|h] = [f|g|h] - [g|f|h] + [g|h|f].$$

Exercise 6.5.2

1. Show that the shuffle product is associative. Conclude that B_* and $\mathbb{Z} \otimes_{\mathbb{Z}G} B_*$ are associative rings with unit.
2. Recall (from 4.5.2) that a graded ring R_* is called *graded-commutative* if $x * y = (-1)^{pq} y * x$ for all $x \in R_p$ and $y \in R_q$. Show that B_* is graded-commutative if G is an abelian group.

Theorem 6.5.13 *If G is an abelian group, then B_* is a differential graded algebra.*

Proof We have already seen in exercise 6.5.2 that B_* is an associative graded-commutative algebra, so all that remains is to verify that the Leibnitz identity 4.5.2 holds, that is, that

$$d(x * y) = (dx) * y + (-1)^p x * dy,$$

where x and y denote $a[g_1|\cdots|g_p]$ and $b[g_{p+1}|\cdots|g_{p+q}]$, respectively. Contained in the expansion of $x*y$, we find the expansions for $(dx)*y$ and $(-1)^p x*dy$. The remaining terms are paired for each $i \leq p < j$, and each (p,q)-shuffle σ which puts i immediately just before j, as

$$(-1)^{\sigma} ab[\cdots|g_i g_j|\cdots] \text{ and } (-1)^{\sigma+1} ab[\cdots|g_j g_i|\cdots].$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

(The terms with j just before i arise from the composition of σ with a transposition.) As G is abelian, these terms cancel. ◇

Corollary 6.5.14 *For every abelian group G and commutative $\mathbb{Z}G$-algebra R, $H_*(G; R)$ is a graded-commutative ring.*

Proof $B_* \otimes_{\mathbb{Z}G} R$ is a graded-commutative DG-algebra (check this!); we saw in exercise 4.5.1 that the homology of such a DG-algebra is a graded-commutative ring. ◇

6.6 Factor Sets and H^2

The origins of the theory of group cohomology go back—at least in nascent form—to the landmark 1904 paper [Schur]. For any field k, the *projective linear group* $PGL_n(k)$ is the quotient of the *general linear group* $GL_n(k)$ by the diagonal copy of the units k^* of k. If G is any group, a group map $\rho: G \to PGL_n(k)$ is called a *projective representation* of G. The pullback

$$E = \{(\alpha, g) \in GL_n(k) \times G : \bar{\alpha} = \rho(g)\}$$

is a group, containing $k^* \cong k^* \times 1$, and there is a diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^* & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \rho'} & & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & k^* & \longrightarrow & GL_n(k) & \longrightarrow & PGL_n(k) & \longrightarrow & 1. \end{array}$$

Schur's observation was that the projective representation ρ of G may be replaced by an ordinary representation ρ' if we are willing to replace G by the larger group E, and it raises the issue of when E is a semidirect product, so that there is a representation $G \hookrightarrow E \to GL_n(k)$ lifting the projective representation. (See exercise 6.6.5.)

Definition 6.6.1 A *group extension* (of G by A) is a short exact sequence

$$0 \to A \to E \xrightarrow{\pi} G \to 1$$

of groups in which A is an abelian group; it is convenient to write the group law in A as addition, whence the term "0" on the left. The extension *splits* if $\pi: E \to G$ has a section $\sigma: G \to E$.

Given a group extension of G by A, the group G acts on A by conjugation in E; to avoid notational confusion, we shall write ${}^g a$ for the conjugate gag^{-1} of a in E. This induced action makes A into a G-module.

Exercise 6.6.1 Show that an extension $0 \to A \to E \to G \to 1$ splits if and only if E is isomorphic to the semidirect product $A \rtimes G$ (6.4.9).

Exercise 6.6.2 Let $G = \mathbb{Z}/2$ and $A = \mathbb{Z}/3$. Show that there are two extensions of G by A, the (split) product $\mathbb{Z}/6 = A \times G$ and the dihedral group D_3. These extensions correspond to the two possible G-module structures on A.

Exercise 6.6.3 (Semidirect product) Let A be a G-module and form the split extension

$$0 \to A \to A \rtimes G \to G \to 1.$$

Show that the induced action of G on A agrees with the G-module structure.

Extension Problem 6.6.2 Given a G-module A, we would like to determine how many extensions of G by A exist in which the induced action of G on A agrees with the given G-module structure, that is, in which ${}^g a = g \cdot a$.

In order to avoid duplication and set-theoretic difficulties, we say that two extensions $0 \to A \to E_i \to G \to 1$ are *equivalent* if there is an isomorphism $\varphi : E_1 \cong E_2$ so

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \varphi\downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

commutes, and we ask for the set of equivalence classes of extensions. Here is the main result of this section:

Classification Theorem 6.6.3 *The equivalence classes of extensions are in 1–1 correspondence with the cohomology group $H^2(G; A)$.*

Here is the canonical approach to classifying extensions. Suppose given an extension $0 \to A \to E \xrightarrow{\pi} G \to 1$; choose a set map $\sigma : G \to E$ such that $\sigma(1)$ is the identity element of E and $\pi\sigma(g) = g$ for all $g \in G$. Both $\sigma(gh)$ and $\sigma(g)\sigma(h)$ are elements of E mapping to $gh \in G$, so their difference lies in A. We define

$$[g, h] = \sigma(g)\sigma(h)\sigma(gh)^{-1}.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Note that $[g, h]$ is an element of A that depends on our choice of E and σ.

Definition 6.6.4 The set function $[\,]: G \times G \to A$ defined above is called the *factor set* determined by E and σ.

Lemma 6.6.5 *If two extensions* $0 \to A \to E_i \to G \to 1$ *with maps* $\sigma_i: G \to E_i$ *yield the same factor set, then the extensions are equivalent.*

Proof The maps σ_i give a concrete set-theoretic identification $E_1 \cong A \times G \cong E_2$; we claim that it is a group homomorphism. Transporting the group structure from E_1 to $A \times G$, we see that the products $(a, 1) \cdot (b, 1) = (a + b, 1)$, $(a, 1) \cdot (0, g) = (a, g)$, and $(0, g) \cdot (a, 1) = (ga, g)$ are fixed. Therefore the group structure on $A \times G$ is completely determined by the products $(1, g) \cdot (1, h)$, which by construction is $([g, h], gh)$. By symmetry, this is also the group structure induced from E_2, whence the claim. ◇

Corollary 6.6.6 *If E were a semidirect product and σ were a group homomorphism, then the factor set would have $[g, h] = 0$ for all $g, h \in G$. Hence if an extension has $[\,] = 0$ as a factor set, the extension must be split.*

Recall (6.5.7) that a *(normalized) 2-cocycle* is a function $[\,] : G \times G \to A$ such that

1. $[g, 1] = [1, g] = 0$ for all $g \in G$.
2. $f[g, h] - [fg, h] + [f, gh] - [f, g] = 0$ for all $f, g, h \in G$.

Theorem 6.6.7 *Let A be a G-module. A set function $[\ ] : G \times G \to A$ is a factor set iff it is a normalized 2-cocycle, that is, an element of $Z^2(G, A)$.*

Remark Equations (1) and (2) are often given as the definition of factor set.

Proof If $[\,]$ is a factor set, formulas (1) and (2) hold because $\sigma(1) = 1$ and multiplication in E is associative (check this!).

Conversely, suppose given a normalized 2-cocycle, that is, a function $[\,]$ satisfying (1) and (2). Let E be the set $A \times G$ with composition defined by

$$(a, g) \cdot (b, h) = (a + (g \cdot b) + [g, h], gh).$$

This product has (0,1) as identity element, and is associative by (2). Since

$$(a, g) \cdot (-g^{-1} \cdot a - g^{-1} \cdot [g, g^{-1}], g^{-1}) = (0, 1),$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

E is a group. Evidently $A \times 1$ is a subgroup isomorphic to A and $E/A \times 1$ is G. Thus $0 \to A \to E \to G \to 1$ is an extension, and the factor set arising from $G \cong 0 \times G \hookrightarrow E$ is our original function [ ]. (Check this!) ◇

Change of Based Section 6.6.8 Fix an extension $0 \to A \to E \xrightarrow{\pi} G \to 1$. A *based section* of π is a map $\sigma: G \to E$ such that $\sigma(1) = 1$ and $\pi\sigma(g) = g$ for all g. Let σ' be another based section of π. Since $\sigma'(g)$ is in the same coset of A as $\sigma(g)$, there is an element $\beta(g) \in A$ so that $\sigma'(g) = \beta(g)\sigma(g)$. The factor set corresponding to σ' is

$$\begin{aligned}[g, h]' &= \beta(g)\sigma(g)\beta(h)\sigma(h)\sigma(gh)^{-1}\beta(gh)^{-1} \\ &= \beta(g) + \sigma(g)\beta(h)\sigma(g)^{-1} + \sigma(g)\sigma(h)\sigma(gh)^{-1} - \beta(gh) \\ &= [g, h] + \beta(g) - \beta(gh) + g \cdot \beta(h).\end{aligned}$$

The difference $[g, h]' - [g, h]$ is the coboundary $d\beta(g, h) = \beta(g) - \beta(gh) + g \cdot \beta(h)$. Therefore, although the 2-cocyle [ ] is not unique, its class in $H^2(G; A) = Z^2(G, A)/B^2(G, A)$ is independent of the choice of based section. Therefore the factor set of an extension yields a well-defined set map Ψ from the set of equivalence classes of extensions to the set $H^2(G; A)$.

Proof of Classification Theorem Analyzing the above construction, we see that the formula $\sigma'(g) = \beta(g)\sigma(g)$ gives a 1–1 correspondence between the set of all possible based sections σ' and the set of all maps $\beta: G \to A$ with $\beta(1)$. If two extensions have the same cohomology class, then an appropriate choice of based sections will yield the same factor sets, and we have seen that in this case the extensions are equivalent. Therefore Ψ is an injection. We have also seen that every 2-cocycle [ ] is a factor set; therefore Ψ is onto. ◇

Exercise 6.6.4 Let $\rho: G \to H$ be a group homomorphism and A an H-module. Show that there is a natural map $Z^2\rho$ on 2-cocycles from $Z^2(H, A)$ to $Z^2(G, A)$ and that $Z^2\rho$ induces a map $\rho^*: H^2(H; A) \to H^2(G; A)$. Now let $0 \to A \to E \xrightarrow{\pi} H \to 1$ be an extension and let E' denote the pullback $E \times_H G = \{(e, g) \in E \times G : \pi(e) = \rho(g)\}$. Show that ρ^* takes the class of the extension E to the class of the extension E'.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow\rho & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & H & \longrightarrow & 1 \end{array}$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.6.5 (Schur) For any field k and any n, let γ denote the class in $H^2(PGL_n(k); k^*)$ corresponding to the extension $1 \to k^* \to GL_n(k) \to PGL_n(k) \to 1$. If $\rho: G \to PGL_n(k)$ is a projective representation, show that ρ lifts to a linear representation $G \to GL_n(k)$ if and only if $\rho^*(\gamma) = 0$ in $H^2(G; k^*)$.

Exercise 6.6.6 If k is an algebraically closed field, and μ_m denotes the subgroup of k^* consisting of all m^{th} roots of unity in k, show that $H^2(G; \mu_m) \cong H^2(G; k^*)$ for every finite group G of automorphisms of k order m. *Hint:* Consider the "Kummer" sequence $0 \to \mu_m \to k^* \xrightarrow{m} k^* \to 1$.

Theorem 6.6.9 (Schur-Zassenhaus) *If m and n are relatively prime, any extension $0 \to A \to E \to G \to 1$ of a group G of order m by a group A of order n is split.*

Proof If A is abelian, the extensions are classified by the groups $H^2(G; A)$, one group for every G-module structure on A. These are zero as A is a $\mathbb{Z}[\frac{1}{m}]$-module (6.1.10).

In the general case, we induct on n. It suffices to prove that E contains a subgroup of order m, as such a subgroup must be isomorphic to G under $E \to G$. Choose a prime p dividing n and let S be a p-Sylow subgroup of A, hence of E. Let Z be the center of S; $Z \neq 1$ [BAI, p. 75]. A counting argument shows that m divides the order of the normalizer N of Z in E. Hence there is an extension $0 \to (A \cap N) \to N \to G \to 1$. If $N \neq E$, this extension splits by induction, so there is a subgroup of N (hence of E) isomorphic to G. If $N = E$, then $Z \lhd E$ and the extension $0 \to A/Z \to E/Z \to G \to 1$ is split by induction. Let E' denote the set of all $x \in E$ mapping onto the subgroup G' of E/Z isomorphic to G. Then E' is a subgroup of E, and $0 \to Z \to E' \to G' \to 1$ is an extension. As Z is abelian, there is a subgroup of E', hence of E, isomorphic to G'. ◇

Application 6.6.10 (Crossed product algebras) Let L/K be a finite Galois field extension with $G = Gal(L/K)$. Given a factor set $[\ ]$ of G in L^*, we can form a new associative K-algebra Λ on the left L-module $L[G]$ using the "crossed" product:

$$(\sum_{g \in G} a_g g) \times (\sum_{h \in G} b_h g) = \sum_{g,h} [g, h] a_g (g \cdot b_h)(gh), \quad (a_g, b_h \in L).$$

It is a straightforward matter to verify that the factor set condition is equivalent to the associativity of the product $\times$ on Λ. Λ is called the *crossed product*

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

algebra of L and G over K with respect to [ ]. Note that L is a subring of Λ and that $\dim_K \Lambda = n^2$, where $n = [L : K]$. As we choose to not become sidetracked, we refer the reader to [BAII, 8.4] for the following facts:

1. Λ is a simple ring with center K and $\Lambda \otimes_K L \cong M_n(L)$. By Wedderburn's Theorem there is a division algebra Δ with center K such that $\Lambda \cong M_d(\Delta)$.
2. Every simple ring Λ with center K and $\Lambda \otimes_K L \cong M_n(L)$ is isomorphic to a crossed product algebra of L and G over K for some factor set [ ].
3. Two factor sets yield isomorphic crossed product algebras if and only if they differ by a coboundary.
4. The factor set [ ] = 1 yields the matrix ring $M_n(K)$, where $n = [L : K]$.
5. If Λ and Λ' correspond to factor sets [ ] and [ ]$'$, then $\Lambda \otimes_K \Lambda' \cong M_n(\Lambda'')$, where Λ'' corresponds to the factor set [ ] + [ ]$'$.

Definition 6.6.11 The *relative Brauer group* $Br(L/K)$ is the set of all simple algebras Λ with center K such that $\Lambda \otimes_K L \cong M_n(L)$, $n = [L : K]$. By Wedderburn's Theorem it is also the set of division algebras Δ with center K and $\Delta \otimes_K L \cong M_r(L)$, $r^2 = \dim_K \Delta$. By (1)–(3), the crossed product algebra construction induces an isomorphism

$$H^2(Gal(L/K); L^*) \xrightarrow{\cong} Br(L/K).$$

The induced group structure $[\Lambda][\Lambda'] = [\Lambda'']$ on $Br(L/K)$ is given by (4) and (5).

Crossed Modules and H^3 6.6.12 Here is an elementary interpretation of the cohomology group $H^3(G; A)$. Consider a 4-term exact sequence with A central in N

$$(*) \qquad 0 \to A \to N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1,$$

and choose a based section $\sigma: G \to E$ of π; as in the theory of factor sets, the map [ ]: $G \times G \to \ker(\pi)$ defined by $[g, h] = \sigma(g)\sigma(h)\sigma(gh)^{-1}$ satisfies a nonabelian cocycle condition

$$[f, g][fg, h] = {}^{\sigma(f)}[g, h] \quad [f, gh],$$

where ${}^{\sigma(f)}[g, h]$ denotes the conjugate $\sigma(f)[g, h]\sigma(f)^{-1}$. Since $\ker(\pi) = \alpha(N)$, we can lift each $[f, g]$ to an element $[[f, g]]$ of N and ask if an analogue of the cocycle condition holds—for some interpretation of ${}^{\sigma(f)}[[g, h]]$. This leads to the notion of crossed module.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

A *crossed module* is a group homomorphism $\alpha: N \to E$ together with an action of E on N (written $(e, n) \mapsto {}^e n$) satisfying the following two conditions:

1. For all $m, n \in N$, ${}^{\alpha(m)}n = mnm^{-1}$.
2. For all $e \in E, n \in N$, $\alpha({}^e n) = e\alpha(n)e^{-1}$.

For example, the canonical map $N \to \mathrm{Aut}(N)$ is a crossed module for any group N. Crossed modules also arise naturally in topology: given a Serre fibration $F \to E \to B$, the map $\pi_1(F) \to \pi_1(E)$ is a crossed module. (This was the first application of crossed modules and was discovered in 1949 by J. H. C. Whitehead.)

Given a crossed module $N \xrightarrow{\alpha} E$, we set $A = \ker(\alpha)$ and $G = \mathrm{coker}(\alpha)$; G is a group because $\alpha(N)$ is normal in E by (2). Note that A is in the center of N and G acts on A, so that A is a G-module, and we have a sequence $(*)$.

Returning to our original situation, but now assuming that $N \to E$ is a crossed module, the failure of $[[f, g]]$ to satisfy the cocycle condition is given by the function $c: G^3 \to A$ defined by the equation

$$c(f, g, h)[[f, g]]\,[[fg, h]] = {}^{\sigma(f)}[[g, h]] \quad [[f, gh]].$$

The reader may check that c is a 3-cocyle, whose class in $H^3(G; A)$ is independent of the choices of σ and $[[f, g]]$. As with Yoneda extensions (3.4.6), we say that $(*)$ is *elementarily equivalent* to the crossed module

$$0 \to A \to N' \to E' \to G \to 1$$

if there is a morphism of crossed modules between them, that is, a commutative diagram compatible with the actions of E and E' on N and N'

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & N & \xrightarrow{\alpha} & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & N' & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1. \end{array}$$

Since our choices of σ and $[[f, g]]$ for $(*)$ dictate choices for $N' \to E'$, these choices clearly determine the same 3-cocycle c. This proves half of the following theorem; the other half may be proven by modifying the proof of the corresponding Yoneda Ext Theorem in [BX, section 7.5].

Crossed Module Classification Theorem 6.6.13 *Two crossed modules with kernel A and cokernel G determine the same class in $H^3(G; A)$ if and only if*

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

they are equivalent (under the equivalence relation generated by elementary equivalence). In fact, there is a 1–1 correspondence for each G and A:

$$\left\{\begin{array}{c}\text{equivalence classes of crossed modules} \\ 0 \to A \to N \xrightarrow{\alpha} E \to G \to 1\end{array}\right\} \longleftrightarrow \text{elements of } H^3(G; A).$$

6.7 Restriction, Corestriction, Inflation, and Transfer

If G is fixed, $H_*(G; A)$ and $H^*(G; A)$ are covariant functors of the G-module A. We now consider them as functors of the group G.

Definition 6.7.1 If $\rho: H \to G$ is a group map, the forgetful functor $\rho^\#$ from G–**mod** to H–**mod** is exact. For every G-module A, there is a natural surjection $(\rho^\# A)_H \to A_G$ and a natural injection $A^G \to (\rho^\# A)^H$. These two maps extend uniquely to the two morphisms $\rho_* = \mathrm{cor}_H^G$ (called *corestriction*) and $\rho^* = \mathrm{res}_H^G$ (called *restriction*) of δ-functors:

$$\mathrm{cor}_H^G: H_*(H; \rho^\# A) \to H_*(G; A) \quad \text{and} \quad \mathrm{res}_H^G: H^*(G; A) \to H^*(H; \rho^\# A)$$

from the category G–**mod** to **Ab** (2.1.4). This is an immediate consequence of the theorem that $H_*(G; A)$ and $H^*(G; A)$ are universal δ-functors, once we notice that $T_*(A) = H_*(H; \rho^\# A)$ and $T^*(A) = H^*(H; \rho^\# A)$ are δ-functors.

Subgroups 6.7.2 The terms *restriction* and *corestriction* are normally used only when H is a subgroup of G. In this case $\mathbb{Z}G$ is actually a free $\mathbb{Z}H$-module, a basis being given by any set of coset representatives. Therefore every projective G-module is also a projective H-module, and we may use any projective G-module resolution $P \to \mathbb{Z}$ to compute the homology and cohomology of H. If A is a G-module, we may calculate cor_H^G as the homology $H_*(\alpha)$ of the chain map $\alpha: P \otimes_H A \to P \otimes_G A$; similarly, we may calculate res_H^G as the cohomology $H^*(\beta)$ of the map $\beta: \mathrm{Hom}_G(P, A) \to \mathrm{Hom}_H(P, A)$.

Exercise 6.7.1 Let H be the cyclic subgroup C_m of the cyclic group C_{mn}. Show that the map $\mathrm{cor}_H^G: H_*(C_m; \mathbb{Z}) \to H_*(C_{mn}; \mathbb{Z})$ is the natural inclusion $\mathbb{Z}/m \hookrightarrow \mathbb{Z}/mn$ for $*$ odd, while $\mathrm{res}_H^G: H^*(C_{mn}; \mathbb{Z}) \to H^*(C_m; \mathbb{Z})$ is the natural projection $\mathbb{Z}/mn \to \mathbb{Z}/m$ for $*$ even. (See 6.2.3.)

Inflation 6.7.3 Let H be a normal subgroup of G and A a G-module. The composites

$$\mathrm{inf}: H^*(G/H; A^H) \xrightarrow{\mathrm{res}} H^*(G; A^H) \to H^*(G; A) \quad \text{and}$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

$$\text{coinf: } H_*(G; A) \to H_*(G; A_H) \xrightarrow{\text{cor}} H_*(G/H; A_H)$$

are called the *inflation* and *coinflation* maps, respectively. Note that on H^0 we have inf: $(A^H)^{G/H} \cong A^G$ and on H_0 we have coinf: $A_G \cong (A_H)_{G/H}$.

Example 6.7.4 If A is trivial as an H-module, inflation = restriction and coinflation = corestriction. Thus by the last exercise we see that (for $*$ odd) the map coinf: $H_*(C_m; \mathbb{Z}) \to H_*(C_{mn}; \mathbb{Z})$ is the natural inclusion $\mathbb{Z}/m \hookrightarrow \mathbb{Z}/mn$, while (for $*$ even) inf: $H^*(C_{mn}; \mathbb{Z}) \to H^*(C_m; \mathbb{Z})$ is the natural projection $\mathbb{Z}/mn \to \mathbb{Z}/m$.

Exercise 6.7.2 Show that the following compositions are zero for $i \neq 0$:

$$H^*(G/H; A^H) \xrightarrow{\text{inf}} H^*(G; A) \xrightarrow{\text{res}} H^*(H; A);$$

$$H_*(H; A) \xrightarrow{\text{cor}} H_*(G; A) \xrightarrow{\text{coinf}} H_*(G/H; A_H).$$

In general, these sequences are not exact, but rather they fit into a spectral sequence, which is the topic of the next section. (See 6.8.3.)

Functoriality of H_* and Corestriction 6.7.5 Let $\mathcal{C}$ be the category of pairs (G, A), where G is a group and A is a G-module. A morphism in $\mathcal{C}$ from (H, B) to (G, A) is a pair $(\rho: H \to G, \varphi: B \to \rho^{\#}A)$, where ρ is a group homomorphism and φ is an H-module map. Such a pair (ρ, φ) induces a map $\text{cor}_H^G \circ \varphi: H_*(H; B) \to H_*(G; A)$. It follows (and we leave the verification as an exercise for the reader) that H_* is a covariant functor from $\mathcal{C}$ to **Ab**.

We have already seen some examples of the naturality of H_*. Corestriction is H_* for $(\rho, B = \rho^{\#}A)$ and coinflation is H_* for $(G \to G/H, A \to A_H)$.

Functoriality of H^* and Restriction 6.7.6 Let $\mathcal{D}$ be the category with the same objects as $\mathcal{C}$, except that a morphism in $\mathcal{D}$ from (H, B) to (G, A) is a pair $(\rho: H \to G \ \varphi: \rho^{\#}A \to B)$. (Note the reverse direction of φ!) Such a pair (ρ, φ) induces a map $\varphi \circ \text{res}_H^G: H^*(G; A) \to H^*(H; B)$. It follows (again as an exercise) that H^* is a contravariant functor from $\mathcal{D}$ to **Ab**.

We have already seen some examples of the naturality of H^*. Restriction is H^* for $(\rho, \rho^{\#}A = B)$ and inflation is H^* for $(G \to G/H, A^H \to A)$. Conjugation provides another example:

Example 6.7.7 (Conjugation) Suppose that H is a subgroup of G, so that each $g \in G$ induces an isomorphism ρ between H and its conjugate gHg^{-1}. If A is a G-module, the abelian group map $\mu_g: A \to A$ $(a \mapsto ga)$ is actually

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

an H-module map from A to $\rho^{\#}A$ because $\mu_g(ha) = gha = (ghg^{-1})ga = \rho(h)\mu_g a$ for all $h \in H$ and $a \in A$. In the category $\mathcal{C}$ of 6.7.5, (ρ, μ_g) is an isomorphism $(H, A) \cong (gHg^{-1}, A)$. Similarly, (ρ, μ_g^{-1}) is an isomorphism $(H, A) \cong (gHg^{-1}, A)$ in $\mathcal{D}$. Therefore we have maps $H_*(H; A) \to H_*(gHg^{-1}; A)$ and $H^*(gHg^{-1}; A) \to H^*(H; A)$.

One way to compute these maps on the chain level is to choose a projective $\mathbb{Z}G$-module resolution $P \to \mathbb{Z}$. Since the P_i are also projective as $\mathbb{Z}H$-modules and as $\mathbb{Z}[gHg^{-1}]$-modules, we may compute our homology and cohomology groups using P. The maps $\mu_g\colon P_i \to P_i$ $(p \mapsto gp)$ form an H-module chain map from P to $\rho^{\#}P$ over the identity map on $\mathbb{Z}$. Hence the map $H_*(H; A) \to H_*(gHg^{-1}; A)$ is induced from

$$P \otimes_H A \to P \otimes_{gHg^{-1}} A, \quad x \otimes a \mapsto gx \otimes ga.$$

Similarly, the map $H^*(gHg^{-1}; A) \to H^*(H; A)$ is induced from

$$\mathrm{Hom}_H(P, A) \to \mathrm{Hom}_{gHg^{-1}}(P, A), \quad \varphi \mapsto (p \mapsto g\varphi(g^{-1}p)).$$

Theorem 6.7.8 *Conjugation by an element $g \in G$ induces the identity automorphism on $H_*(G; \mathbb{Z})$ and $H^*(G; \mathbb{Z})$.*

Proof The maps $P \otimes \mathbb{Z} \to P \otimes \mathbb{Z}$ and $\mathrm{Hom}_G(P, \mathbb{Z}) \to \mathrm{Hom}_G(P, \mathbb{Z})$ are the identity. ◇

Corollary 6.7.9 *If H is a normal subgroup of G, then the conjugation action of G on $\mathbb{Z}$ induces an action of G/H on $H_*(G; \mathbb{Z})$ and $H^*(G; \mathbb{Z})$.*

Example 6.7.10 (Dihedral groups) The cyclic group C_m is a normal subgroup of the dihedral group D_m (6.4.10), and $D_m/C_m \cong C_2$. To determine the action of C_2 on the homology of C_m, note that there is an element g of D_m such that $g\sigma g^{-1} = \sigma^{-1}$. Let $\rho\colon C_m \to C_m$ be conjugation by g. If P denotes the $(\sigma - 1, N)$ complexof 6.2.1, consider the following map from P to $\rho^{\#}P$:

$$\begin{array}{ccccccccccccccc}
0 & \longleftarrow & \mathbb{Z} & \longleftarrow & \mathbb{Z}G & \xleftarrow{1-\sigma} & \mathbb{Z}G & \xleftarrow{N} & \mathbb{Z}G & \xleftarrow{1-\sigma} & \mathbb{Z}G & \xleftarrow{N} & \mathbb{Z}G & \xleftarrow{1-\sigma} & \mathbb{Z}G \cdots \\
 & & \| & & \| & & -\sigma\downarrow & & -\sigma\downarrow & & \sigma^2\downarrow & & \sigma^2\downarrow & & (-\sigma)^3\downarrow \\
0 & \longleftarrow & \mathbb{Z} & \longleftarrow & \mathbb{Z}G & \xleftarrow{1-\sigma^{-1}} & \mathbb{Z}G & \xleftarrow{N} & \mathbb{Z}G & \xleftarrow{1-\sigma^{-1}} & \mathbb{Z}G & \xleftarrow{N} & \mathbb{Z}G & \xleftarrow{1-\sigma^{-1}} & \mathbb{Z}G \cdots
\end{array}$$

An easy calculation (exercise!) shows that the map induced from conjugation by g is multiplication by $(-1)^i$ on $H_{2i-1}(C_m; \mathbb{Z})$ and $H^{2i}(C_m; \mathbb{Z})$.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

6.7.1 Cup Product

As another application of the naturality of H^*, we show that $H^*(G;\mathbb{Z})$ is an associative graded-commutative ring, a fact that is familiar to topologists.

In 6.1.14 we constructed a cross product map $\times$ from $H^*(G;\mathbb{Z})\otimes H^*(H;\mathbb{Z})$ to $H^*(G\times H;\mathbb{Z})$. When $G=H$, composition with the restriction $\Delta^* = \mathrm{res}_G^{G\times G}$ along the diagonal map $\Delta: G\to G\times G$ gives a graded bilinear product on $H^*(G;\mathbb{Z})$, called the *cup product*. If $x, y\in H^*(G;\mathbb{Z})$, the cup product $x\cup y$ is just $\Delta^*(x\times y)$.

Exercise 6.7.3 (Naturality of the cross and cup product) Show that the cross product is natural in G and H in the sense that $(\rho^* x)\times(\sigma^* y) = (\rho\times\sigma)^*(x\times y)$ in $H^{p+q}(G'\times H';\mathbb{Z})$ for every $\rho: G'\to G$ and $\sigma: H'\to H$, $x\in H^p(G;\mathbb{Z})$, and $y\in H^q(H;\mathbb{Z})$. Conclude that the cup product is natural in G, that is, that $(\rho^* x_1)\cup(\rho^* x_2) = \rho^*(x_1\cup x_2)$.

Theorem 6.7.11 (Cohomology ring) *The cup product makes $H^*(G;\mathbb{Z})$ into an associative, graded-commutative ring with unit. The ring structure is natural in the group G.*

Proof Since the composites of Δ with the maps $\Delta\times 1$, $1\times\Delta: G\times G\to G\times G\times G$ are the same, and the cross product is associative (by exercise 6.1.9),

$$\begin{aligned} x\cup(y\cup z) &= x\cup\Delta^*(y\times z) = \Delta^*(x\times\Delta^*(y\times z)) \\ &= \Delta^*(1\times\Delta)^*(x\times y\times z) = \Delta^*(\Delta\times 1)^*(x\times y\times z) \\ &= \Delta^*(\Delta^*(x\times y)\times z) = \Delta^*(x\times y)\cup z = (x\cup y)\cup z. \end{aligned}$$

If $\pi: G\to 1$ is the projection, the compositions $(1\times\pi)\Delta$ and $(\pi\times 1)\Delta$ are the identity on $H^*(G;\mathbb{Z})$, and the restriction π^* sends $1\in H^0(1;\mathbb{Z})$ to $1\in H^0(G;\mathbb{Z})\cong\mathbb{Z}$. Since we saw in exercise 6.1.9 that the cross product with $1\in H^0(G;\mathbb{Z})$ is the identity map,

$$x\cup 1 = \Delta^*(x\times\pi^*(1)) = \Delta^*(1\times\pi)^*(x\times 1) = x\times 1 = x,$$

and $1\cup x = x$ similarly. Hence the cup product is associative with unit 1.

To see that the cup product is graded-commutative, it suffices to show that the cross product (with $G=H$) is graded-commutative, that is, that $y\times x = (-1)^{ij}x\times y$ for $x\in H^i(G;\mathbb{Z})$ and $y\in H^j(G;\mathbb{Z})$. This is a consequence of the following lemma, since if τ is the involution $\tau(g,h)=(h,g)$ on $G\times G$, we have $y\cup x = \Delta^*(y\times x) = \Delta^*\tau^*(x\times y)$. ◇

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Lemma 6.7.12 *Let $\tau: G \times H \to H \times G$ be the isomorphism $\tau(g, h) = (h, g)$ and write τ^* for the associated restriction map $H^*(H \times G, \mathbb{Z}) \to H^*(G \times H, \mathbb{Z})$. Then for $x \in H^p(G; \mathbb{Z})$ and $y \in H^q(H; \mathbb{Z})$, we have $\tau^*(y \times x) = (-1)^{pq}(x \times y)$.*

Proof Let $P \to \mathbb{Z}$ be a free $\mathbb{Z}G$-resolution and $Q \to \mathbb{Z}$ a free $\mathbb{Z}H$-resolution. Because of the sign trick 1.2.5 used in taking total complexes, the maps $a \otimes b \mapsto (-1)^{pq} b \otimes a$ from $P_p \otimes Q_q$ to $Q_q \otimes P_p$ assemble to give a chain map τ': Tot$(P \otimes Q) \to$ Tot$(Q \otimes P)$ over τ. (Check this!) This gives the required factor of $(-1)^{pq}$, because τ^* is obtained by applying Hom$(-, \mathbb{Z})$ and taking cohomology. ◇

Exercise 6.7.4 Let $\beta \in H^2(C_m; \mathbb{Z}) \cong \mathbb{Z}/m$ be a generator. Show that the ring $H^*(C_m; \mathbb{Z})$ is the polynomial ring $\mathbb{Z}[\beta]$, modulo the obvious relation that $m\beta = 0$.

Exercise 6.7.5 This exercise uses exercise 6.1.10.

1. Show that there is a cup product on $H^*(G; k)$ for any commutative ring k, making H^* into an associative, graded-commutative k-algebra, natural in G.
2. Suppose that $k = \mathbb{Z}/m$ and $G = C_m$, with m odd. Show that the graded algebra $H^*(C_m; \mathbb{Z}/m)$ is isomorphic to the ring $\mathbb{Z}/m[\sigma, \beta]/(\sigma^2 = \beta\sigma = 0)$, with $\sigma \in H^1$ and $\beta \in H^2$.

Coalgebra Structure 6.7.13 Dual to the notion of a k-algebra is the notion of a coalgebra over a commutative ring k. We call a k-module H a *coalgebra* if there are module homomorphisms $\Delta: H \to H \otimes_k H$ (the *coproduct*) and $\varepsilon: H \to k$ (the *counit*) such that both composites $(\varepsilon \otimes 1)\Delta$ and $(1 \otimes \varepsilon)\Delta$ (mapping $H \to H \otimes H \to H$) are the identity on H. We say that the coalgebra is *coassociative* if in addition $(\Delta \otimes 1)\Delta = (1 \otimes \Delta)\Delta$ as maps $H \to H \otimes H \to H \otimes H \otimes H$. For example, $H = kG$ is a cocommutative coalgebra; the coproduct is the diagonal map from kG to $k(G \times G) \cong kG \otimes kG$ and satisfies $\Delta(g) = g \otimes g$, while the counit is the usual augmentation $\varepsilon(g) = 1$. More examples are given below in (9.10.8).

Lemma 6.7.14 *Suppose that k is a field, or more generally that $H_*(G; k)$ is flat as a k-module. Then $H_*(G; k)$ is a cocommutative coalgebra.*

Proof Recall from exercises 6.1.7 and 6.1.12 that $H_*(G \times G; k)$ is isomorphic to $H_*(G; k) \otimes_k H_*(G; k)$, so the diagonal map $\Delta: G \to G \times G$ induces

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

a map $\Delta_*: H_*(G;k) \to H_*(G;k) \otimes_k H_*(G;k)$. The projection $\varepsilon: G \to 1$ induces a map ε_* from $H_*(G;k)$ to $H_*(1;k) = k$. Since $(\varepsilon \times 1)\Delta = (1 \times \varepsilon)\Delta$ as maps $G \to G \times G \to G$ and $(\Delta \times 1)\Delta = (1 \times \Delta)\Delta$ as maps $G \to G \times G \to G \times G \times G$, we have the required identities $(\varepsilon_* \otimes 1)\Delta_* = (1 \otimes \varepsilon_*)\Delta_*$ and $(\Delta_* \otimes 1)\Delta_* = (1 \otimes \Delta_*)\Delta_*$. ◇

Definition 6.7.15 (Hopf algebras) A *bialgebra* is an algebra H, together with algebra homomorphisms Δ and ε making H into a cocommutative coalgebra. We call H a *Hopf algebra* if in addition there is a k-module homomorphism $s: H \to H$ (called the *antipode*) such that both maps $\times(s \otimes 1)\Delta$ and $\times(1 \otimes s)\Delta$ (from $H \to H \otimes H \to H \otimes H \to H$) equal the the projection $H \xrightarrow{\varepsilon} k \hookrightarrow H$.

For example, the involution $s(g) = g^{-1}$ makes kG into a Hopf algebra, because $(s \otimes 1)\Delta(g) = g^{-1} \otimes g$ and $(1 \otimes s)\Delta(g) = g \otimes g^{-1}$. We will see another example in exercise 7.3.7.

Exercise 6.7.6 Suppose that G is an abelian group, so that the product $\mu: G \times G \to G$ is a group homomorphism and that k is a field. Show that $H_*(G;k)$ and $H^*(G;k)$ are both Hopf algebras.

Transfer Maps 6.7.16 Let H be a normal subgroup of finite index in G, and let A be a G-module. The sum $\sum ga$ over the right cosets $\{Hg\}$ of H yields a well-defined map from A to A_H. This map sends $(ga - a)$ to zero, so it induces a well-defined map $tr: A_G \to A_H$. Since $H_*(G;A)$ is a universal δ-functor, tr extends to a unique map of δ-functors, called the *transfer map:*

$$tr : H_*(G;A) \to H_*(H;A).$$

Similarly, the sum $\sum ga$ over the left cosets $\{gH\}$ of H yields a well-defined map from A^H to A. The image is G-invariant, so it induces a well-defined map $tr: A^H \to A^G$. This induces a map of δ-functors, also called *the transfer map:*

$$tr : H^*(H;A) \to H^*(G;A).$$

Lemma 6.7.17 *The composite* $\mathrm{cor}_H^G \circ tr$ *is multiplication by the index* $[G:H]$ *on* $H_*(G;A)$. *Similarly, the composite* $tr \circ \mathrm{res}_H^G$ *is multiplication by* $[G:H]$ *on* $H^*(G;A)$.

Proof In A_G and A^G, the sums over the cosets are just $\sum ga = (\sum g) \cdot a =$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

$[G : H] \cdot a$. The corresponding maps between the δ-functors are determined by their behavior on A_G and A^H, so they must also be multiplication by $[G : H]$. ◇

Exercise 6.7.7 Show that the transfer map defined here agrees with the transfer map defined in 6.3.9 using Shapiro's Lemma. *Hint:* By universality, it suffices to check what happens on H_0 and H^0.

Exercise 6.7.8 Use the transfer maps to give another proof of 6.5.8, that when G is a finite group of order $m = [G : 1]$ multiplication by m is the zero map on $H_n(G; A)$ and $H^n(G; A)$ for $n \neq 0$.

6.8 The Spectral Sequence

The inflation and restriction maps fit into a filtration of $H^*(G; A)$ first studied in 1946 by Lyndon. The spectral sequence codifying this relationship was found in 1953 by Hochschild and Serre. We shall derive it as a special case of the Grothendieck spectral sequence 5.8.3, using the following lemma.

Lemma 6.8.1 *If H is a normal subgroup of G, and A is a G-module, then both A_H and A^H are G/H-modules. Moreover, the forgetful functor $\rho^\#$ from G/H–**mod** to G–**mod** has $-_H$ as left adjoint and $-^H$ as right adjoint.*

Proof A G/H-module is the same thing as a G-module on which H acts trivially. Therefore A_H and A^H are G/H-modules by construction. The universal properties of $A^H \to A$ and $A \to A_H$ translate into the natural isomorphisms

$$\mathrm{Hom}_G(A, \rho^\# B) \cong \mathrm{Hom}_{G/H}(A_H, B) \text{ and}$$

$$\mathrm{Hom}_G(\rho^\# B, A) \cong \mathrm{Hom}_{G/H}(B, A^H),$$

which provide the required adjunctions. ◇

Lyndon/Hochschild-Serre Spectral Sequence 6.8.2 *For every normal subgroup H of a group G, there are two convergent first quadrant spectral sequences:*

$$E^2_{pq} = H_p(G/H; H_q(H; A)) \Rightarrow H_{p+q}(G; A);$$

$$E_2^{pq} = H^p(G/H; H^q(H; A)) \Rightarrow H^{p+q}(G; A).$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

The edge maps $H_*(G; A) \to H_*(G/H; A_H)$ and $H_*(H; A)_{G/H} \to H_*(G; A)$ in the first spectral sequence are induced from the coinflation and corestriction maps. The edge maps $H^*(G/H; A^H) \to H^*(G; A)$ and $H^*(G; A) \to H^*(H; A)^{G/H}$ in the second spectral sequence are induced from the inflation and restriction maps.

Proof We claim that the functors $-_G$ and $-^G$ factor through G/H–**mod** as follows:

$$\begin{array}{ccc} G\text{–}\mathbf{mod} & \xrightarrow{{}^{-}H} & G/H\text{–}\mathbf{mod} \\ {}^{-}G \searrow & & \swarrow {}^{-}G/H \\ & \mathbf{Ab} & \end{array} \qquad \begin{array}{ccc} G\text{–}\mathbf{mod} & \xrightarrow{{}_{-}H} & G/H\text{–}\mathbf{mod} \\ {}_{-}G \searrow & & \swarrow {}_{-}G/H \\ & \mathbf{Ab} & \end{array}$$

To see this, let A be a G-module; we saw in the last lemma that A_H and A^H are G/H-modules. The abelian group $(A_H)_{G/H}$ is obtained from A by first modding out by the relations $ha - a$ with $h \in H$, and then modding out by the relations $\bar{g}a - a$ for $\bar{g} \in G/H$. If $\bar{g}$ is the image of $g \in G$ then $\bar{g}a - a \equiv ga - a$, so we see that $(A_H)_{G/H}$ is $A/\mathfrak{I}A = A_G$.

Similarly, $(A^H)^{G/H}$ is obtained from A by first restricting to the subgroup of all $a \in A$ with $ha = a$, and then further restricting to the subgroup of all a with $\bar{g}a = a$ for $\bar{g} \in G/H$. If $\bar{g}$ is the image of $g \in G$, $\bar{g}a = ga$. Thus $(A^H)^{G/H} = A^G$.

Finally, we proved in Lemma 6.8.1 that $-_H$ is left adjoint to an exact functor, and that $-^H$ is right adjoint to an exact functor. We saw in 2.3.10 that this implies that $-_H$ preserves projectives and that $-^H$ preserves injectives, so that the Grothendieck spectral sequence exists. The description of the edge maps is just a translation of the description given in 5.8.3. ◇

Low Degree Terms 6.8.3 The exact sequences of low degree terms in the Lyndon-Hochschild-Serre spectral sequence are

$$H_2(G; A) \xrightarrow{\text{coinf}} H_2(G/H; A_H) \xrightarrow{d} H_1(H; A)_{G/H} \xrightarrow{\text{cor}} H_1(G; A) \xrightarrow{\text{coinf}} H_1(G/H; A_H) \to 0;$$

$$0 \to H^1(G/H; A^H) \xrightarrow{\text{inf}} H^1(G; A) \xrightarrow{\text{res}} H^1(H; A)^{G/H} \xrightarrow{d} H^2(G/H; A^H) \xrightarrow{\text{inf}} H^2(G; A).$$

Example 6.8.4 If H is in the center of G, G/H acts trivially on $H_*(H; A)$ and $H^*(H; A)$, so we may compute the E^2 terms from $H_*(H; \mathbb{Z})$ and Universal Coefficient theorems. For example, let G be the cyclic group C_{2m} and $H = C_m$ for m odd. Then $H_p(C_2; H_q(C_m; \mathbb{Z}))$ vanishes unless $p = 0$ or $q = 0$.

The groups $\mathbb{Z}/2$ lie along the x-axis, and the groups $\mathbb{Z}/m$ lie along the y-axis. The spectral sequence collapses at E^2 to yield the formula for $H_*(C_{2m};\mathbb{Z})$ that we derived in 6.2.3.

$G = C_{2m}$

0				
$\mathbb{Z}/m$	0			
0	0	0		
$\mathbb{Z}/m$	0	0	0	
$\mathbb{Z}$	$\mathbb{Z}/2$	0	$\mathbb{Z}/2$	0

$G = D_{2m}$

0				
$\mathbb{Z}/m$	0			
0	0	0		
0	0	0	0	
$\mathbb{Z}$	$\mathbb{Z}/2$	0	$\mathbb{Z}/2$	0

Example 6.8.5 (Dihedral groups) Let G be the dihedral group $D_{2m} = C_m \rtimes C_2$ and set $H = C_m$. If m is odd, then once again $H_p(C_2; H_q(C_m))$ vanishes unless $p = 0$ or $q = 0$. As before, the groups $\mathbb{Z}/2$ lie along the x-axis, but along the y-axis we now have $H_q(C_m)_{C_2}$. From our calculation 6.7.10 of the action of C_2 on $H_*(C_m)$ we see that $H_q(C_m)_{C_2}$ is zero unless $q = 0$, when it is $\mathbb{Z}$, or $q \equiv 3 \pmod 4$, when it is $\mathbb{Z}/m$. Summarizing, we have computed that

$$H_n(D_{2m};\mathbb{Z}) = \left\{ \begin{array}{ll} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}/2 & \text{if } n \equiv 1 \pmod 4 \\ \mathbb{Z}/2m & \text{if } n \equiv 3 \pmod 4 \\ 0 & \text{otherwise} \end{array} \right\}.$$

Example 6.8.6 (Gysin sequence) A central element t of infinite order in G generates an infinite cyclic subgroup T. As in 5.3.7 the spectral sequence collapses to the long exact "Gysin" sequence for every trivial G-module k:

$$\cdots H_n(G;k) \xrightarrow{\text{coinf}} H_n(G/T;k) \xrightarrow{S} H_{n-2}(G/T;k) \to H_{n-1}(G;k) \cdots$$

Exercise 6.8.1 The *infinite dihedral group* D_∞ is the semidirect product $T \rtimes C_2$, where $\sigma \in C_2$ acts as multiplication by -1 on the infinite cyclic group T ($\sigma t \sigma^{-1} = t^{-1}$). Show that σ acts as multiplication by -1 on $H_1(T;\mathbb{Z})$, and deduce that

$$H_n(D_\infty;\mathbb{Z}) \cong \left\{ \begin{array}{ll} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}/2 \oplus \mathbb{Z}/2 & \text{if } n \equiv 1, 3, 5, 7, \ldots \\ 0 & \text{if } n \equiv 2, 4, 6, 8, \ldots \end{array} \right\}.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Hint: By naturality, $H_*(C_2)$ is a summand of $H_*(D_\infty)$.

Presentations 6.8.7 A presentation of a group by generators and relations amounts to the same thing as a short exact sequence of groups $1 \to R \to F \to G \to 1$, where F is the free group on the generators of G and R is the normal subgroup of F generated by the relations of G. Note that R is also a free group, being a subgroup of the free group F. The spectral sequence of this extension has $E^2_{pq} = 0$ for $q \neq 0, 1$ and $H_n(F; \mathbb{Z}) = 0$ for $n \neq 0, 1$. Therefore the differentials $H_{n+2}(G; \mathbb{Z}) \to H_n(G; H_1(R))$ must be isomorphisms for $n \geq 1$, and we have the low degree sequence

$$0 \to H_2(G; \mathbb{Z}) \to \left[\frac{R}{R, R}\right]_G \to \frac{F}{[F, F]} \to \frac{G}{[G, G]} \to 0.$$

The action of G on $R/[R/R]$ is given by $g \cdot r = frf^{-1}$, where $f \in F$ lifts $g \in G$ and $r \in R$. The following calculation shows that $(R/[R/R])_G = R/[F, R]$:

$$(g - 1) \cdot r = frf^{-1} - r \equiv frf^{-1}r^{-1} = [f, r].$$

By inspection of the low degree sequence, we see that we have proven the following result, which was first established in [Hopf].

Hopf's Theorem 6.8.8 *If $G = F/R$ with F free, then $H_2(G; \mathbb{Z}) \cong \frac{R \cap [F,F]}{[F,R]}$.*

6.9 Universal Central Extensions

A *central extension* of G is an extension $0 \to A \to X \xrightarrow{\pi} G \to 1$ such that A is in the center of X. (If π and A are clear from the context, we will just say that X is a central extension of G.) A homomorphism over G from X to another central extension $0 \to B \to Y \xrightarrow{\tau} G \to 1$ of G is a map $f: X \to Y$ such that $\pi = \tau f$. X is called a *universal central extension* of G if for every central extension $0 \to B \to Y \xrightarrow{\tau} G \to 1$ of G there exists a unique homomorphism f from X to Y over G.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & X & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \exists!} & & \| & & \\ 0 & \longrightarrow & B & \longrightarrow & Y & \xrightarrow{\tau} & G & \longrightarrow & 1 \end{array}$$

Clearly, a universal central extension is unique up to isomorphism over G, provided that it exists. We will show that a necessary and sufficient condition

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

for a universal central extension to exist is that G is perfect; recall that a group G is *perfect* if it equals its commutator subgroup $[G, G]$.

Example 6.9.1 The smallest perfect group is A_5. The universal central extension of A_5 describes A_5 as the quotient $PSL_2(\mathbb{F}_5)$ of the binary icosahedral group $X = SL_2(\mathbb{F}_5)$ by the center of order 2, $A = \pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ [Suz, 2.9].

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)} SL_2(\mathbb{F}_5) \longrightarrow PSL_2(\mathbb{F}_5) \longrightarrow 1.$$

Lemma 6.9.2 *If G has a universal central extension X, then both G and X are perfect.*

Proof If X is perfect, then so is G. If X is not perfect, then $B = X/[X, X]$ is a nonzero abelian group, $0 \to B \to B \times G \to G \to 1$ is a central extension, and there are two homomorphisms $X \to B \times G$ over G : $(0, \pi)$ and (pr, π). ◇

Exercises 6.9.1

1. If $0 \to A \to X \to G \to 1$ is any central extension in which G and X are perfect groups, show that $H_1(X; \mathbb{Z}) = 0$ and that there is an exact sequence

$$H_2(X; \mathbb{Z}) \xrightarrow{\text{cor}} H_2(G; \mathbb{Z}) \to A \to 0.$$

2. Show that if G is perfect then central extensions $0 \to A \to X \to G \to 1$ are classified by $\text{Hom}(H_2(G; \mathbb{Z}), A)$. (Use exercise 6.1.5.)

Remark The above exercises suggest that $H_2(G; \mathbb{Z})$ has something to do with universal central extensions. Indeed, we shall see that the universal central extension $0 \to A \to X \to G \to 1$ has $A \cong H_2(G; \mathbb{Z})$. The group $H_2(G; \mathbb{Z})$ is called the *Schur multiplier* of G in honor of Schur, who first investigated the notion of a universal central extension of a finite group G in [Schur].

As indicated in section 6.6, Schur was concerned with central extensions with $A = \mathbb{C}^*$, and these are classified by the group $H^2(G; \mathbb{C}^*) = \text{Hom}(H_2(G; \mathbb{Z}), \mathbb{C}^*)$. Since G is finite, $H^2(G; \mathbb{C}^*)$ is the Pontrjagin dual (3.2.3) of the finite group $H_2(G; \mathbb{Z})$. Hence the groups $H^2(G; \mathbb{C}^*)$ and $H_2(G; \mathbb{Z})$ are noncanonically isomorphic.

Construction of a Universal Central Extension 6.9.3 Choose a free group F mapping onto G and let $R \subset F$ denote the kernel. Then $[R, F]$ is a normal

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

subgroup of F, and the short exact sequence $1 \to R \to F \to G \to 1$ induces a central extension

$$0 \to R/[R, F] \to F/[R, F] \to G \to 1.$$

Now suppose that G is perfect. Since $[F, F]$ maps onto G, there is a surjection from $[F, F]/[R, F]$ to G; its kernel is the subgroup $(R \cap [F, F])/[R, F]$, which Hopf's Theorem 6.8.8 states is the Schur multiplier $H_2(G; \mathbb{Z})$. We shall prove that

$$0 \to (R \cap [F, F])/[R, F] \to [F, F]/[R, F] \to G \to 1$$

is a universal central extension of G.

Lemma 6.9.4 *$[F, F]/[R, F]$ is a perfect group.*

Proof Since $[F, F]$ and F both map onto G, any $x \in F$ may be written as $x = x'r$ with $x' \in [F, F]$ and $r \in R$. Writing $y \in F$ as $y's$ with $y' \in [F, F]$ and $s \in R$, we find that in $F/[R, F]$

$$[x, y] = (x'r)(y's)(x'r)^{-1}(y's)^{-1} \equiv [x', y'].$$

Thus every generator $[x, y]$ of $[F, F]/[R, F]$ is a commutator of elements x' and y' of $[F, F]/[R, F]$. ◇

Theorem 6.9.5 *A group G has a universal central extension if and only if G is perfect. In this case, the universal central extension is*

$$(*) \qquad 0 \to H_2(G; \mathbb{Z}) \to \frac{[F, F]}{[R, F]} \xrightarrow{\pi} G \to 1.$$

Here $1 \to R \to F \to G \to 1$ is any presentation of G.

Proof If G has a universal central extension, then G must be perfect by 6.9.2. Now suppose that G is perfect; we have just seen that $(*)$ is a central extension and that $[F, F]/[R, F]$ is perfect. In order to show that $(*)$ is universal, let $0 \to B \to Y \xrightarrow{\tau} G \to 1$ be another central extension. Since F is a free group, the map $F \to G$ lifts to a map $h: F \to Y$. Since $\tau h(R) = 1$, $h(R)$ is in the central subgroup B of Y. This implies that $h([R, F]) = 1$. Therefore h induces a map

$$\eta: [F, F]/[R, F] \hookrightarrow F/[R, F] \xrightarrow{h} Y$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

such that $\tau\eta = \pi$, that is, such that η is a homomorphism over G. The following lemma shows that η is unique and finishes the proof that $(*)$ is universal. ◇

Lemma 6.9.6 *If* $0 \to A \to X \xrightarrow{\pi} G \to 1$ *and* $0 \to B \to Y \to G \to 1$ *are central extensions, and* X *is perfect, there is at most one homomorphism* f *from* X *to* Y *over* G.

Proof If f_1 and f_2 are two such homomorphisms, define a set map $\varphi: X \to B$ by the formula $f_1(x) = f_2(x)\varphi(x)$. Since B is central,

$$f_1(xx') = f_2(x)\varphi(x)f_2(x')\varphi(x') = f_2(xx')\varphi(x)\varphi(x').$$

Hence $\varphi(xx') = \varphi(x)\varphi(x')$, that is, φ is a group homomorphism. Since B is an abelian group, φ must factor through $X/[X, X] = 1$. Hence $\varphi(x) = 1$ for all x, that is, $f = f'$. ◇

Exercise 6.9.2 (Composition) If $0 \to B \to Y \xrightarrow{\rho} X \to 1$ and $0 \to A \to X \xrightarrow{\pi} G \to 1$ are central extensions, show that the "composition" $0 \to \ker(\pi\rho) \to Y \xrightarrow{\pi\rho} G \to 1$ is a central extension of G. If X is a universal central extension of G, conclude that every central extension $0 \to B \to Y \to X \to 1$ splits.

Recognition Criterion 6.9.7 A central extension $0 \to A \to X \xrightarrow{\pi} G \to 1$ is universal if and only if X is perfect and every central extension of X splits as a direct product of X with an abelian group.

Proof The 'only if' direction follows from the preceding exercise. Now suppose that X is perfect and that every central extension of X splits. Given a central extension $0 \to B \to Y \xrightarrow{\tau} G \to 1$ of G, we can construct a homomorphism from X to Y over G as follows. Let P be the pullback group $\{(x, y) \in X \times Y : \pi(x) = \tau(y)\}$. Then in the diagram

$$\begin{array}{ccccccccc} & & & & & \overset{\exists\sigma}{\longleftarrow} & & & \\ 0 & \longrightarrow & B & \longrightarrow & P & \longrightarrow & X & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow\pi & & \\ 0 & \longrightarrow & B & \longrightarrow & Y & \xrightarrow{\tau} & G & \longrightarrow & 1 \end{array}$$

the top row is a central extension of X, so it is split by a map $\sigma: X \to P$. The composite $f: X \to P \to Y$ is the homomorphism over G we wanted to

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

construct. Since X is perfect, f is unique (6.9.6); this proves that X is a universal central extension of G. ◇

Corollary 6.9.8 *If* $0 \to A \to X \to G \to 1$ *is a universal central extension, then*

$$H_1(X; \mathbb{Z}) = H_2(X; \mathbb{Z}) = 0.$$

Corollary 6.9.9 *If* G *is a perfect group and* $H_2(G; \mathbb{Z}) = 0$, *then every central extension of* G *is a direct product of* G *with an abelian group.*

$$0 \to A \to A \times G \to G \to 1$$

Proof Evidently $0 \to 0 \to G = G \to 1$ is the universal central extension of G. ◇

Example 6.9.10 (Alternating groups) It is well known that the alternating groups A_n are perfect if $n \geq 5$. From [Suz, 3.2] we see that

$$H_2(A_n; \mathbb{Z}) \cong \left\{ \begin{array}{ll} \mathbb{Z}/6 & \text{if } n = 6, 7 \\ \mathbb{Z}/2 & \text{if } n = 4, 5 \text{ or } n \geq 8 \\ 0 & \text{if } n = 1, 2, 3 \end{array} \right\}$$

We have already mentioned (6.9.1) the universal central extension of A_5. In general, the regular representation $A_n \to SO_{n-1}$ gives rise to a central extension

$$0 \to \mathbb{Z}/2 \to \tilde{A}_n \to A_n \to 1$$

by restricting the central extension

$$0 \to \mathbb{Z}/2 \to \mathrm{Spin}_{n-1}(\mathbb{R}) \to SO_{n-1} \to 1.$$

If $n \neq 6, 7$, $\tilde{A}_n$ must be the universal central extension of A_n.

Example 6.9.11 It is known [Suz, 1.9] that if F is a field, then the special linear group $SL_n(F)$ is perfect, with the exception of $SL_2(\mathbb{F}_2) \cong D_6$ and $SL_2(\mathbb{F}_3)$, which is a group of order 24. The center of $SL_n(F)$ is the group $\mu_n(F)$ of n^{th} roots of unity in F (times the identity matrix I), and the quotient of $SL_n(F)$ by $\mu_n(F)$ is the *projective special linear group* $PSL_n(F)$.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

When $F = \mathbb{F}_q$ is a finite field, we know that $H_2(SL_n(\mathbb{F}_q); \mathbb{Z}) = 0$ [Suz, 2.9]. It follows, again with two exceptions, that

$$0 \to \mu_n(\mathbb{F}_q) \xrightarrow{I} SL_n(\mathbb{F}_q) \to PSL_n(\mathbb{F}_q) \to 1$$

is the universal central extension of the finite group $PSL_n(\mathbb{F}_q)$.

Example 6.9.12 The *elementary matrix* e_{ij}^{λ} in $GL_n(R)$ is the matrix that coincides with the identity matrix except for the single nonzero entry λ in the (i, j) spot. The subgroup $E_n(R)$ of $GL_n(R)$ generated by the elementary matrices is a perfect group when $n \geq 3$ because $[e_{ij}^{\lambda}, e_{jk}^{\mu}] = e_{ik}^{\lambda\mu}$ for $i \neq k$. We now describe the universal central extension of $E_n(R)$.

Definition 6.9.13 Let R be any ring. For $n \geq 3$ the *Steinberg group* $St_n(R)$ is the group that is presented as having generators x_{ij}^{λ} $(\lambda \in R, 1 \leq i, j \leq n)$ and relations

1. $x_{ij}^{\lambda} x_{ij}^{\mu} = x_{ij}^{\lambda+\mu}$;
2. $[x_{ij}^{\lambda}, x_{jk}^{\mu}] = x_{ik}^{\lambda\mu}$ for $i \neq k$; and
3. $[x_{ij}^{\lambda}, x_{k\ell}^{\mu}] = 1$ for $j \neq k$ and $i \neq \ell$.

There is a homomorphism $St_n(R) \to E_n(R)$ sending x_{ij}^{λ} to e_{ij}^{λ} because these relations are also satisfied by the elementary matrices. It is known [Milnor] [Swan, p. 208] that $St_n(R)$ is actually the universal central extension of $E_n(R)$ for $n \geq 5$. The kernel of $St_n(R) \to E_n(R)$ is denoted $K_2(n, R)$ and may be identified with the Schur multiplier. The direct limit $K_2(R)$ of the groups $K_2(n, R)$ is an important part of algebraic K-theory. See [Milnor] for more details and computations.

6.10 Covering Spaces in Topology

Let G be a group that acts on a topological space X. We shall assume that each translation $X \to X$ arising from multiplication by an element $g \in G$ is a continuous map and that the action is *proper* in the sense that every point of X is contained in a small open subset U such that every translate gU is disjoint from U. Under these hypotheses, the quotient topology on the orbit space X/G is such that the projection $p: X \to X/G$ makes X into a covering space of X/G. Indeed, every small open set U is mapped homeomorphically onto its image in X/G.

Example 6.10.1 Let Y be a connected, locally simply connected space, so that its universal covering space $\tilde{Y} \to Y$ exists. The group $G = \pi_1(Y)$ acts properly on $X = \tilde{Y}$, and $\tilde{Y}/G = Y$.

Lemma 6.10.2 *If G acts properly on X, the singular complex $S_*(X)$ of X is a chain complex of free $\mathbb{Z}G$-modules, and $S_*(X)_G$ is the singular complex of X/G.*

Proof Let $\mathcal{B}_n$ denote the set of continuous maps $\sigma\colon \Delta_n \to X$. G acts on $\mathcal{B}_n$, with $g\sigma$ being the composition of σ with translation by $g \in G$. Since $S_n(X)$ is the free $\mathbb{Z}$-module with basis $\mathcal{B}$, $S_n(X)$ is a G-module. Since translation by g sends the faces of σ to the faces of $g\sigma$, the boundary map $d\colon S_n(X) \to S_{n-1}(X)$ is a G-map, so $S_n(X)$ is a G-module complex.

Let $\mathcal{B}'_n$ denote the set of continuous maps $\sigma'\colon \Delta_n \to X/G$. The unique path lifting property of a covering space implies that any $\sigma'\colon \Delta_n \to X/G$ may be lifted to a map $\sigma\colon \Delta_n \to X$ and that every other lift is $g\sigma$ for some $g \in G$. As the $g\sigma$ are distinct, this proves that $\mathcal{B} \cong G \times \mathcal{B}'$ as a G-set. Choosing one lift for each σ' gives a map $\mathcal{B}' \to \mathcal{B}$, hence a basis for $S_n(X)$ as a free $\mathbb{Z}G$-module. This proves that the natural map from $S_n(X)$ to $S_n(X/G)$ induces an isomorphism $S_n(X)_G \cong S_n(X/G)$. ◇

Corollary 6.10.3 *If G acts properly on X, $H_*(X, \mathbb{Z})$ and $H^*(X, \mathbb{Z})$ are G-modules.*

Definition 6.10.4 (Classifying space) A CW complex with fundamental group G and contractible universal covering space is called a *classifying space* for G, or a *model for* BG; by abuse of notation, we will call such a space BG, and write EG for its universal covering space. From the Serre fibration $G \to EG \to BG$ we see that

$$\pi_i(BG) = \begin{Bmatrix} G & \text{if } i = 1 \\ 0 & \text{otherwise} \end{Bmatrix}.$$

It is well known that any two classifying spaces for G are homotopy equivalent. One way to find a model for BG is to find a contractible CW complex X on which G acts properly (and cellularly) and take $BG = X/G$.

Theorem 6.10.5 $H_*(BG; \mathbb{Z}) \cong H_*(G; \mathbb{Z})$ *and* $H^*(BG; \mathbb{Z}) \cong H^*(G; \mathbb{Z})$.

Proof Since $H_*(EG) \cong H_*(\text{point})$ is 0 for $* \neq 0$ and $\mathbb{Z}$ for $* = 0$, the chain complex $S_*(EG)$ is a free $\mathbb{Z}G$-module resolution of $\mathbb{Z}$. Hence $H_*(G; \mathbb{Z}) =$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

$H_*(S_*(EG) \otimes_{\mathbb{Z}G} \mathbb{Z}) = H_*(S_*(EG)_G) = H_*(S_*(BG)) = H_*(BG; \mathbb{Z})$. Similarly, $H^*(G; \mathbb{Z})$ is the cohomology of

$$\mathrm{Hom}_G(S_*(EG), \mathbb{Z}) = \mathrm{Hom}_{\mathbf{Ab}}(S_*(EG)_G, \mathbb{Z}) = \mathrm{Hom}_{\mathbf{Ab}}(S_*(BG), \mathbb{Z}),$$

the chain complex whose cohomology is $H^*(BG; \mathbb{Z})$. ◇

Remark The relationship between the homology (resp. cohomology) of G and BG was worked out during World War II by Hopf and Freudenthal (resp. by Eilenberg and MacLane). MacLane asserts in [MacH] that this interplay "was the starting point of homological algebra." Here are some useful models of classifying spaces.

Example 6.10.6 The circle S^1 and the complex units $\mathbb{C}^*$ are two models for $B\mathbb{Z}$; the extensions $0 \to \mathbb{Z} \to \mathbb{R} \to S^1 \to 1$ and $0 \to \mathbb{Z} \xrightarrow{2\pi i} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^* \to 1$ expressing $\mathbb{R}$ (resp. $\mathbb{C}$) as the universal cover of S^1 (resp. $\mathbb{C}^*$) are well known.

Example 6.10.7 The infinite sphere S^∞ is contractible, and $G = C_2$ acts properly in such a way that $S^\infty/G = \mathbb{RP}^\infty$. Hence we may take $\mathbb{RP}^\infty$ as our model for BC_2.

Example 6.10.8 Let S be a Riemann surface of genus $g \neq 0$. The fundamental group $G = \pi_1(S)$ has generators $a_1, \cdots, a_g, b_1, \cdots, b_g$ and the single defining relation $[a_1, b_1][a_2, b_2] \cdots [a_g, b_g] = 1$. One knows that the universal cover X of S is the hyperbolic plane, which is contractible. Thus S is the classifying space BG.

Example 6.10.9 Any connected Lie group L has a maximal compact subgroup K, and the homogeneous space $X = L/K$ is diffeomorphic to $\mathbb{R}^d$, where $d = \dim(L) - \dim(K)$. If Γ is a discrete torsionfree subgroup of L, then $\Gamma \cap K = \{1\}$, so Γ acts properly on X. Consequently, the double coset space $\Gamma\backslash X = \Gamma\backslash L/K$ is a model for the classifying space $B\Gamma$.

For example, the special linear group $SL_n(\mathbb{R})$ has $SO_n(\mathbb{R})$ as maximal compact, so $X = SO_n(\mathbb{R}) \setminus SL_n(\mathbb{R}) \cong \mathbb{R}^d$ where $d = \frac{n(n+2)}{2} - 1$. $SL_n(\mathbb{Z})$ is a discrete but not torsionfree subgroup of $SL_n(\mathbb{R})$. For $N \geq 3$, the *principal congruence subgroup* $\Gamma(N)$ *of level* N is the subgroup of all matrices in $SL_n(\mathbb{Z})$ congruent to the identity matrix modulo N. One knows that $\Gamma(N)$ is torsionfree, so $X/\Gamma(N)$ is a model for $B\Gamma(N)$.

Theorem 6.10.10 *Let G act properly on a space X with $\pi_0(X) = 0$. Then for every abelian group A there are spectral sequences*

$$^{I}E^2_{pq} = H_p(G; H_q(X, A)) \Rightarrow H_{p+q}(X/G, A);$$
$$^{II}E_2^{pq} = H^p(G; H^q(X, A)) \Rightarrow H^{p+q}(X/G, A).$$

Proof Let us write $\mathbb{H}_*(G; -)$ for the hyperhomology functors $\mathbb{L}_*(-_G)$ defined in 6.1.15 (or 5.7.4). Since $C = S_*(X) \otimes_{\mathbb{Z}} A$ is a chain complex of G-modules, there are two spectral sequences converging to the group hyperhomology $\mathbb{H}_*(G; C)$. Shapiro's Lemma 6.3.2 tells us that $H_q(S_n(X) \otimes_{\mathbb{Z}} A)$ is 0 for $q \neq 0$ and $S_n(X/G) \otimes_{\mathbb{Z}} A$ for $q = 0$ (6.10.2). Hence the first spectral sequence collapses to yield

$$\mathbb{H}_p(G; C) = H_p(S_*(X/G) \otimes A) = H_p(X/G, A).$$

The second spectral sequence has the desired E^2 term

$$^{II}E^2_{pq} = H_p(G; H_q C) = H_p(G; H_q(X, A)).$$

Similarly, if we write $\mathbb{H}^*(G; -)$ for the group hypercohomology $\mathbb{R}^*(-^G)$ and D for $\mathrm{Hom}_{\mathbf{Ab}}(S(X), A)$, there are two spectral sequences (6.1.15) converging to $\mathbb{H}^*(G; D)$. Since

$$D_n = \mathrm{Hom}(\mathbb{Z}G \otimes S_n(X/G), A) = \mathrm{Hom}(\mathbb{Z}G, \mathrm{Hom}(S_n(X/G), A)),$$

Shapiro's Lemma tells us that the first spectral sequence collapses to yield $\mathbb{H}^*(G; D) \cong H^*(X/G, A)$, and the second spectral sequence has the desired E_2 term

$$^{II}E_2^{pq} = H^p(G; H^q(D)) = H^p(G; H^q(A)). \qquad \diamond$$

Remark There is a map from X/G to BG such that $X \to X/G \to BG$ has the homotopy type of a Serre fibration. The spectral sequences (6.10.10) may then be viewed as special cases of the Serre spectral sequence 5.3.2.

6.11 Galois Cohomology and Profinite Groups

The notion of profinite group encodes many of the important properties of the Galois group $\mathrm{Gal}(L/K)$ of a *Galois field extension* (i.e., an algebraic extension

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

that is separable and normal but not necessarily finite). The largest Galois extension of any field K is the *separable closure* K_s of K; K_s is the subfield of the algebraic closure $\bar{K}$ consisting of all elements separable over K, and $K_s = \bar{K}$ if $\text{char}(K) = 0$.

K_s is also the union $\cup L_i$ of the partially ordered set $\{L_i : i \in I\}$ of all finite Galois field extensions of K. If $K \subset L_i \subset L_j$, the Fundamental Theorem of finite Galois theory [BAI, 4.5] states that there is a natural surjection from $\text{Gal}(L_j/K)$ to $\text{Gal}(L_i/K)$ with kernel $\text{Gal}(L_j/L_i)$. In other words, there is a contravariant functor $\text{Gal}(-/K)$ from the filtered poset I to the category of finite groups.

Krull's Theorem 6.11.1 *The Galois group* $\text{Gal}(K_s/K)$ *of all field automorphisms of* $\bar{K}$ *fixing* K *is isomorphic to the inverse limit* $\varprojlim \text{Gal}(L_i/K)$ *of finite groups.*

Proof Since the L_i are splitting fields over K, any automorphism α of K_s over K restricts to an automorphism α_i of L_i. The resulting restriction maps $\text{Gal}(K_s/K) \to \text{Gal}(L_i/K)$ are compatible and yield a group homomorphism ϕ from $\text{Gal}(K_s/K)$ to the set $\varprojlim \text{Gal}(L_i/K)$ of all compatible families $(\alpha_i) \in \prod \text{Gal}(L_i/K)$. If $\alpha \neq 1$, then $\alpha(x) \neq x$ for some $x \in K_s = \cup L_i$; if $x \in L_i$, then $\alpha_i(x) = \alpha(x) \neq x$. Therefore $\phi(\alpha) \neq 1$, that is, ϕ is injective. Conversely, if we are given (α_i) in $\varprojlim \text{Gal}(L_i/K)$, define $\alpha \in \text{Gal}(K_s/K)$ as follows. If $x \in K_s$, choose L_i containing x and set $\alpha(x) = \alpha_i(x)$; compatibility of the α_i's implies that $\alpha(x)$ is independent of the choice of i. Since any $x, y \in K_s$ lie in some L_i, α is a field automorphism of K_s, that is, an element of $\text{Gal}(K_s/K)$. By construction, $\phi(\alpha) = (\alpha_i)$. Hence ϕ is surjective and so an isomorphism. ◇

Example 6.11.2 If $\mathbb{F}_q$ is a finite field, its separable and algebraic closures coincide. The poset of finite extensions $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ is the poset of natural numbers, partially ordered by divisibility, and $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is $\varprojlim(\mathbb{Z}/n\mathbb{Z}) = \widehat{\mathbb{Z}} \cong \prod_p \widehat{\mathbb{Z}}_p$. For every prime p, let K be the union of all the $\mathbb{F}_{q^n}$ with $(p, n) = 1$; then $\text{Gal}(\bar{\mathbb{F}}_q/K)$ is $\widehat{\mathbb{Z}}_p$.

There is a topology on $\text{Gal}(K_s/K) = \varprojlim \text{Gal}(L_i/K)$ that makes it into a compact Hausdorff group: the profinite topology. To define it, recall that the *discrete topology* on a set X is the topology in which every subset of X is both open and closed. If we are given an inverse system $\{X_i\}$ of topological spaces, we give the inverse limit $\varprojlim X_i$ the topology it inherits as a subspace of the

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

product ΠX_i. If the X_i are all finite discrete sets, the resulting topology on $X = \varprojlim X_i$ is called the *profinite topology* on X. Since each $\mathrm{Gal}(L_i/K)$ is a finite discrete set, this defines the profinite topology on $\mathrm{Gal}(K_s/K)$. To show that this is a compact Hausdorff group, we introduce the concepts of profinite set and profinite group.

Profinite Sets 6.11.3 A *profinite set* is a set X that is the inverse limit $\varprojlim X_i$ of some system $\{X_i\}$ of finite sets, made into a topological space using the profinite topology described above. The choice of the inverse system is not part of the data; we will see below that the profinite structure is independent of this choice.

The Cantor set is an interesting example of a profinite set; the subspace $\{0, 1, \frac{1}{2}, \ldots, \frac{1}{n}, \ldots\}$ of $\mathbb{R}$ is another. Profinite groups like $\widehat{\mathbb{Z}}_p$ and $\mathrm{Gal}(K_s/K)$ form another important class of profinite sets.

Some elementary topological remarks are in order. Any discrete space is Hausdorff; as a subspace of ΠX_i, $\varprojlim X_i$ is Hausdorff. A discrete space is compact iff it is finite. A topological space X is called *totally disconnected* if every point of X is a connected component, and discrete spaces are totally disconnected.

Exercise 6.11.1 Suppose that $\{X_i\}$ is an inverse system of compact Hausdorff spaces. Show that $\varprojlim X_i$ is also compact Hausdorff. Then show that if each of the X_i is totally disconnected, $\varprojlim X_i$ is also totally disconnected. This proves one direction of the following theorem; the converse is proven in [Magid].

Theorem 6.11.4 *Profinite spaces are the same thing as totally disconnected, compact Hausdorff topological spaces. In particular, the profinite structure of* $X \cong \varprojlim X_i$ *depends only upon the topology and not upon the choice of inverse system* $\{X_i\}$.

Exercise 6.11.2 Let X be a profinite set.

1. Show that there is a canonical choice of the inverse system $\{X_i\}$ making X profinite, namely the system of its finite topological quotient spaces.
2. Show that every closed subspace of X is profinite.
3. If X is infinite, show that X has an open subspace U that is not profinite.

Definition 6.11.5 A *profinite group* is a group G that is an inverse limit of finite groups, made into a topological space using the profinite topology. Clearly

G is a profinite set that is also a compact Hausdorff topological group. In fact, the converse is true: Every totally disconnected compact Hausdorff group is a profinite group. A proof of this fact may be found in [Shatz], which we recommend as a good general reference for profinite groups and their cohomology.

Examples 6.11.6 (Profinite groups)

1. Any finite group is trivially profinite.
2. The p-adic integers $\widehat{\mathbb{Z}}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ are profinite by birthright.
3. Krull's Theorem 6.11.1 states that $\mathrm{Gal}(K_s/K)$ is a profinite group.
4. (Profinite completion) Let G be any (discrete) group. The *profinite completion* $\widehat{G}$ of G is the inverse limit of the system of all finite quotient groups G/H of G. For example, the profinite completion of $G = \mathbb{Z}$ is $\widehat{\mathbb{Z}} = \varprojlim(\mathbb{Z}/n\mathbb{Z})$, but the profinite completion of $G = \mathbb{Q}/\mathbb{Z}$ is 0. The kernel of the natural map $G \to \widehat{G}$ is the intersection of all subgroups of finite index in G.

Exercise 6.11.3 Show that the category of profinite abelian groups is dual to the category of torsion abelian groups. *Hint:* Show that A is a torsion abelian group iff its Pontrjagin dual $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ is a profinite group.

Exercise 6.11.4 Let G be a profinite group, and let H be a subgroup of G.

1. If H is closed in G, show that H is also a profinite group.
2. If H is closed and normal, show that G/H is a profinite group.
3. If H is open in G, show that the index $[G : H]$ is finite, that H is closed in G, and therefore that H is profinite.

It is useful to have a canonical way of writing a profinite group G as the inverse limit of finite groups, and this is provided by the next result.

Lemma 6.11.7 *If G is a profinite group, let $\mathcal{U}$ be the poset of all open normal subgroups U of G. Then $\mathcal{U}$ forms a fundamental system of neighborhoods of 1, each G/U is a finite group, and $G \cong \varprojlim G/U$.*

Proof If $G = \varprojlim G_i$, then the $U_i = \ker(G \to G_i)$ are open normal subgroups of G and the natural map $G \to \varprojlim G_i$ factors through $\varprojlim G/U_i$. Since $\varprojlim$ is left exact, this yields $G \cong \varprojlim G/U_i$ and shows that $\{U_i\}$ (hence $\mathcal{U}$) forms a fundamental system of neighborhoods of 1. Hence every open subgroup U of G contains some U_i, and this suffices to show that $G \cong \varprojlim\{G/U : U \in \mathcal{U}\}$. (Check this!) ◇

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Exercise 6.11.5 (Fundamental Theorem of Galois theory) Prove that the usual correspondence of Galois theory induces a bijection between the set of topologically closed subgroups H of $G = \mathrm{Gal}(K_s/K)$ and the set of intermediate fields $K \subset L \subset K_s$. (Here $L = (K_s)^H$ and $H = \{g | gx = x \text{ for all } x \in L\}$.) Show that the closed normal subgroups of G correspond to the Galois extensions L of K. Conclude that if L/K is any Galois field extension, then $\mathrm{Gal}(L/K)$ is a profinite group: $\mathrm{Gal}(L/K) = G/H$.

To connect this result to more familiar Galois theory, show that the open subgroups H of $\mathrm{Gal}(K_s/K)$ correspond to the finite field extensions of K, and that the open normal subgroups of $\mathrm{Gal}(K_s/K)$ correspond to the finite Galois extensions of K.

In order to discuss the cohomology of profinite groups, we need to introduce an appropriate notion of G-module.

Definition 6.11.8 Let G be a profinite group. A *discrete G-module* is a G-module A such that, when A is given the discrete topology, the multiplication map $G \times A \to A$ is continuous. The next exercise provides a more elementary description of this.

Exercise 6.11.6

1. If A is a discrete G-module, show that for every $a \in A$ the stabilizer $U = \{g \in G : ga = a\}$ is an open subgroup of G, and $a \in A^U$, the submodule fixed by U.
2. If A is any G-module, let $\cup A^U$ denote the union of all subgroups A^U as U runs over the set of open subgroups of G. Show that A is a discrete G-module $\Longleftrightarrow \cup A^U = A$.

Examples 6.11.9 The field K_s is a discrete $\mathrm{Gal}(K_s/K)$-module for every K. If G is a finite group, every G-module is discrete, because $G \times A$ has the discrete topology.

A map of discrete G-modules is defined to be just a G-module map, so that the category $\mathbf{C}_G$ of discrete G-modules is a full additive subcategory of G–**mod**. The following exercise shows that in fact $\mathbf{C}_G$ is an abelian subcategory of G–**mod**.

Exercise 6.11.7 Let $f: A \to B$ be a map of discrete G-modules. Show that the G-modules $\ker(f) = \{a \in A : f(a) = 0\}$, $f(A)$, and $\mathrm{coker}(f) = B/f(A)$ are discrete G-modules. Conclude that $\mathbf{C}_G$ is an abelian category and that the

inclusion $\mathbf{C}_G \subset G$–**mod** is an exact functor. Then show that for all discrete G-modules A and all G-modules B,

$$\mathrm{Hom}_G(A, B) = \mathrm{Hom}_G(A, \cup B^U).$$

Conclude that the inclusion $\mathbf{C}_G \subset G$–**mod** has the functor $\cup(\cdot)^U$ as right adjoint.

Lemma 6.11.10 *The abelian category* $\mathbf{C}_G$ *has enough injectives.*

Proof We may embed any discrete G-module A in an injective G-module I. By the above exercise, $A \subseteq \cup I^U \subseteq I$. Since $\cup(-)^U$ is right adjoint to the exact functor $\mathbf{C}_G \subset G$–**mod**, it preserves injectives (2.3.10). Consequently $\cup I^U$ is an injective object in $\mathbf{C}_G$. ◇

Remark $\mathbf{C}_G$ does *not* have enough projectives.

Profinite Cohomology 6.11.11 The cohomology groups $H^*(G; A)$ of a profinite group G with coefficients in a discrete G-module A are defined to be the right derived functors of the functor $\mathbf{C}_G \to \mathbf{Ab}$ sending A to A^G, applied to A.

From this definition, we see that $H^0(G; A) = A^G$ and that when G is a finite group, $H^*(G; A)$ agrees with the usual group cohomology.

In fact, many of the results for the cohomology of finite groups carry over to profinite groups. For example, there is a category of profinite groups, a morphism being a continuous group homomorphism, and $H^*(G; A)$ is contravariant in G via the restriction maps. Indeed, the entire discussion of the functoriality of H^* in sections 6.3 and 6.7 carries through verbatim to our context. Of course, the inflation maps $\mathrm{inf}: H^*(G/H; A^H) \to H^*(G; A)$ are only defined when H is a closed normal subgroup of G, because the map $G \to G/H$ is only continuous when H is a closed normal subgroup of G. Similarly, whenever H is a closed normal subgroup of G, we can construct a Lyndon/Hochschild-Serre spectral sequence (6.8.2):

$$E_2^{pq} = H^p(G/H; H^q(H; A)) \Rightarrow H^{p+q}(G; A).$$

Since $\mathbf{C}_G$ doesn't have enough projectives, we need to modify the discussion in section 6.5 about the bar construction in order to talk about cocycles.

Cochains and cocycles 6.11.12 If A is a discrete G-module, let $C^n(G, A)$ denote the set of continuous maps from G^n to A. (When $n = 0$, $C^0(G, A) = A$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

because $G^0 = \{1\}$.) Under pointwise addition, $C^n(G, A)$ becomes an abelian group, a subgroup of the group of n-cochains $\mathrm{Hom}_G(B_n^u, A)$ described in 6.5.4. The explicit formula for d shows that $C^*(G, A)$ is a subcomplex of the cochain complex $\mathrm{Hom}_G(B_*^u, A)$.

Exercise 6.11.8 Show that a map $\varphi: G^n \to A$ is continuous iff φ is locally constant, that is, iff each point of G^n has a neighborhood on which φ is constant.

Exercise 6.11.9 Show that $C^n(G, -)$ is an exact functor from $\mathbf{C}_G$ to **Ab**. *Hint:* If $g: B \to C$ is onto, use the fact that every continuous $\varphi: G^n \to C$ is locally constant to lift φ to $C^n(G, B)$.

Exercise 6.11.10 Show that $C^n(G, A) = \varinjlim C^n(G/U, A^U)$, where U runs through all open normal subgroups of G.

Theorem 6.11.13 *Let G be a profinite group and A a discrete G-module. Then*

$$\begin{aligned} H^*(G; A) &\cong H^*(C^*(G, A)) \\ &\cong \varinjlim H^*(G/U; A^U), \end{aligned}$$

where U runs through all open normal subgroups of G.

Proof For simplicity, set $T^n(A) = H^n(C^*(G, A))$. We first calculate that

$$\begin{aligned} T^0(A) &= \ker(A \xrightarrow{d} C^1(G, A)) \\ &= \{a \in A : (\forall g \in G) \quad 0 = (da)(g) = ga - a\} \\ &= A^G. \end{aligned}$$

Since $C^*(G, A) = \varinjlim C^*(G/U; A^U)$, and $\varinjlim$ commutes with cohomology (2.6.15), we see that $T^n(A) = \varinjlim H^n(C^*(G/U, A^U)) = \varinjlim H^n(G/U; A^U)$.

It now suffices to show that the $\{T^n\}$ form a universal cohomological δ-functor in the sense of 2.1.4, for this will imply that $T^n(A) \cong H^n(G; A)$. To see that they form a δ-functor, let $0 \to A \to B \to C \to 0$ be a short exact sequence of discrete G-modules. By exercise 6.11.9, each sequence

$$0 \to C^n(G, A) \to C^n(G, B) \to C^n(G, C) \to 0$$

is naturally exact, so we get a short exact sequence of cochain complexes. The associated long exact cohomology sequence with its natural coboundary $\delta^n: T^n(C) \to T^{n+1}(A)$ makes $\{T^n\}$ into a cohomological δ-functor.

To see that $\{T^n\}$ is universal, it suffices to show that each T^n (except T^0) vanishes on injective objects, for then T^n will be effaceable in the sense of exercise 2.4.5. If I is an injective object in $\mathbf{C}_G$ and U is an open normal subgroup of G, then I^U is an injective object in $C_{G/U} = G/U$–**mod** because (as in 6.8.1) $-^U$ is right adjoint to the forgetful functor. Hence if $n \neq 0$, then

$$T^n(I) = \varinjlim H^n(G/U; I^U) = 0. \qquad \diamond$$

Corollary 6.11.14 *For $n \geq 1$, the $H^n(G; A)$ are torsion abelian groups.*

Proof Each G/U is a finite group, so $H^n(G/U, A^U)$ is a torsion group. $\diamond$

Exercise 6.11.11 Let G be the profinite group $\widehat{\mathbb{Z}}_p$. Show that

$$H^i(G; \mathbb{Z}) = \begin{cases} \widehat{\mathbb{Z}}_p & i \text{ even} \\ 0 & i \text{ odd} \end{cases}.$$

Low Dimensions 6.11.15 We have already seen that $H^0(G; A) = A^G$. A calculation using the complex $C^*(G, A)$ shows that $H^1(G; A)$ is the group of continuous derivations of G in A, modulo the (ctn.) principal derivations, and that $H^1(G; \mathbb{Z})$ is the group of continuous maps from G to $\mathbb{Z}$. Similarly, $H^2(G; A)$ is the group of classes of continuous factor sets of G in A. If A is *finite*, $H^2(G; A)$ classifies the profinite extensions of G by A. (The discrete group A is only profinite when it is finite.)

Hilbert's Theorem 90 6.11.16 *Let K be a field and set $G = \mathrm{Gal}(K_s/K)$. Then K_s and its units K_s^* are discrete G-modules with $(K_s)^G = K$ and $(K_s^*)^G = K^*$. Moreover*

1. *$H^n(G; K_s) = 0$ for all $n \neq 0$.*
2. *$H^1(G; K_s^*) = 0$.*

Proof Let U be an open normal subgroup of G and $L = K_s^U$ the corresponding Galois extension of K, so that $G/U = \mathrm{Gal}(L/K)$ and $(K_s^*)^U = L^*$. By Hilbert's Theorem 90 for L/K (6.3.7, 6.4.7), we see that

$$H^n(G/U; L) = 0 \text{ for } n \neq 0,$$
$$H^1(G/U; L^*) = 0.$$

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

Now take the limit over all U to get the result. ◇

Brauer group 6.11.17 The classical *Brauer group* of K is the set of all equivalence classes of central simple K-algebras Λ (with equivalence relation $M_i(\Lambda) \approx M_j(\Lambda')$). It is also isomorphic to the set of all finite-dimensional division K-algebras Δ with center K. The relative Brauer groups $Br(L/K)$ of 6.6.11 were constructed so that $Br(K)$ is the union of the relative groups $Br(L/K)$. On the other hand, since $Br(L/K) = H^2(\mathrm{Gal}(L/K), L^*)$ by 6.6.11, $H^2(G; K_s^*)$ is also the direct limit of the $Br(L/K)$, because if U is an open normal subgroup and $L = (K_s)^U$, then $G/U = \mathrm{Gal}(L/K)$ and $(K_s^*)^U = L^*$. Therefore $Br(K)$ is naturally isomorphic to the profinite cohomology group $H^2(G; K_s^*)$. The following result provides a cohomological proof of the fact that each $Br(L/K)$ is a subgroup of $Br(K)$.

Proposition 6.11.18 *If $K \subset L$ is a Galois field extension with Galois group $G = \mathrm{Gal}(L/K)$, there is an exact sequence*

$$0 \to Br(L/K) \xrightarrow{\inf} Br(K) \xrightarrow{\mathrm{res}} Br(L)^G \to H^3(G; L^*) \to H^3(K, K_s^*).$$

In particular, $Br(L/K)$ is the kernel of $Br(K) \to Br(L)$.

Proof Let $H \subset \mathrm{Gal}(K_s/K)$ be the closed normal subgroup corresponding to L, so that $G = \mathrm{Gal}(K_s/K)/H$. The Hochschild-Serre spectral sequence 6.11.11 is

$$E_2^{pq} = H^p(G; H^q(H; K_s^*)) \Rightarrow H^*(\mathrm{Gal}(K_s/K); K_s^*).$$

Along the x-axis we find $H^p(G; L^*)$. By Hilbert's Theorem 90 for L, the row $q = 1$ vanishes. The exact sequence of low degree terms is the sequence in question. ◇

Exercise 6.11.12 Let $\mathbb{F}_q$ be a finite field. Show that $Br(L/\mathbb{F}_q) = 0$ for every finite extension L of $\mathbb{F}_q$ and conclude that $Br(\mathbb{F}_q) = 0$. *Hint*: $\mathrm{Gal}(L/\mathbb{F}_q)$ is cyclic of order $n = [L : \mathbb{F}_q]$ and the norm map $N: L^* \to K^*$ is onto (6.4.8).

Vista 6.11.19 Many deep results about the Brauer group can be established more easily using cohomological machinery. We list a few here, referring the reader to [Shatz] for more details.

- If $\mathrm{char}(K) = p \neq 0$, $Br(K)$ is divisible by p.
- (Tsen's Theorem) If K is a function field in one variable over an algebraically closed field, then $Br(K) = 0$.

https://doi.org/10.1017/CBO9781139644136.007 Published online by Cambridge University Press

- $Br(\mathbb{R}) = \mathbb{Z}/2$, the quaternion algebra $\mathbb{H}$ being nontrivial. (See 6.4.8.)
- (Hasse) If K is a local field, that is, the p-adic rationals $\widehat{\mathbb{Q}}_p$, or a finite extension of $\widehat{\mathbb{Q}}_p$, then there is a canonical isomorphism $Br(K) \cong \mathbb{Q}/\mathbb{Z}$. The element of $\mathbb{Q}/\mathbb{Z}$ corresponding to a central simple K-algebra Λ is called the *Hasse invariant* of Λ.
- The Brauer group of $\mathbb{Q}$ injects into $Br(\mathbb{R}) \cong \mathbb{Z}/2$ plus the direct sum over all primes p of the groups $Br(\widehat{\mathbb{Q}}_p) \cong \mathbb{Q}/\mathbb{Z}$, with cokernel $\mathbb{Q}/\mathbb{Z}$. Thus the Hasse invariants uniquely determine $Br(\mathbb{Q})$, and the sum of the Hasse invariants is zero.