17.2 THE COHOMOLOGY OF GROUPS

In this section we consider the application of the general techniques of the previous section in an important special case.

Let G be a group.

Definition. An abelian group A on which G acts (on the left) as automorphisms is called a *G-module*.

Note that a G-module is the same as an abelian group A and a homomorphism $\varphi : G \to \text{Aut}(A)$ of G into the group of automorphisms of A. Since an abelian group is the same as a module over $\mathbb{Z}$, it is also easy to see that a G-module A is the same as a module over the integral group ring, $\mathbb{Z}G$, of G with coefficients in $\mathbb{Z}$. When G is an infinite group the ring $\mathbb{Z}G$ consists of all the finite formal sums of elements of G with coefficients in $\mathbb{Z}$.

As usual we shall often use multiplicative notation and write ga in place of $g \cdot a$ for the action of the element $g \in G$ on the element $a \in A$.

Definition. If A is a G-module, let $A^G = \{a \in A \mid ga = a \text{ for all } g \in G\}$ be the elements of A fixed by all the elements of G.

Examples
(1) If $ga = a$ for all $a \in A$ and $g \in G$ then G is said to act *trivially* on A. In this case $A^G = A$. The abelian group $\mathbb{Z}$ will always be assumed to have trivial G-action for any group G unless otherwise stated.
(2) For any G-module A the fixed points A^G of A under the action of G is clearly a $\mathbb{Z}G$-submodule of A on which G acts trivially.
(3) If V is a vector space over the field F of dimension n and $G = GL_n(F)$ then V is naturally a G-module. In this case $V^G = \{0\}$ since any nonzero element in V can be taken to any other nonzero element in V by some linear transformation.
(4) A semidirect product $E = A \rtimes G$ as in Section 5.5 in the case where A is an abelian normal subgroup gives a G-module A where the action of G is given by the homomorphism $\varphi : G \to \text{Aut}(A)$. The subgroup A^G consists of the elements of A lying in the center of E. More generally, if A is any abelian normal subgroup of a group E, then E acts on A by conjugation and this makes A into a E-module and also an E/A-module. In this case $A^E = A^{E/A}$ also consists of the elements of A lying in the center of E.
(5) If K/F is an extension of fields that is Galois with Galois group G then the additive group K is naturally a G-module, with $K^G = F$. Similarly, the multiplicative group $K^\times$ of nonzero elements in K is a G-module, with fixed points $(K^\times)^G = F^\times$.

The fixed point subgroups in this last example played a central role in Galois Theory in Chapter 14. In general, it is easy to see that a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of G-modules induces an exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \tag{17.15}$$

that in general cannot be extended to a short exact sequence (in general a coset in the quotient C that is fixed by G need not be represented by an *element* in B fixed by G). One way to see that (15) is exact is to observe that A^G can be related to a Hom group:

Lemma 19. Suppose A is a G-module and $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ is the group of all $\mathbb{Z}G$-module homomorphisms from $\mathbb{Z}$ (with trivial G-action) to A. Then $A^G \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof: Any G-module homomorphism α from $\mathbb{Z}$ to A is uniquely determined by its value on 1. Let α_a denote the G-module homomorphism with $\alpha(1) = a$. Since α_a is a G-module homomorphism, $a = \alpha_a(1) = \alpha_a(g \cdot 1) = g \cdot \alpha_a(1) = g \cdot a$ for all $g \in G$, so that a must lie in A^G. Likewise, for any $a \in A^G$ it is easy to check that the map $\alpha_a \mapsto a$ gives an isomorphism from $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ to A^G.

Combined with the results of the previous section, the lemma not only shows that the sequence (15) is exact, it shows that any projective resolution of $\mathbb{Z}$ considered as a $\mathbb{Z}G$-module will give a long exact sequence extending (15). One such projective resolution is the *standard resolution* or *bar resolution* of $\mathbb{Z}$:

$$\cdots \longrightarrow F_n \xrightarrow{d_n} F_{n-1} \to \cdots \xrightarrow{d_1} F_0 \xrightarrow{\mathrm{aug}} \mathbb{Z} \longrightarrow 0. \qquad (17.16)$$

Here $F_n = \mathbb{Z}G \otimes_\mathbb{Z} \mathbb{Z}G \otimes_\mathbb{Z} \cdots \otimes_\mathbb{Z} \mathbb{Z}G$ (where there are $n + 1$ factors) for $n \geq 0$, which is a G-module under the action defined on simple tensors by $g \cdot (g_0 \otimes g_1 \otimes \cdots \otimes g_n) = (gg_0) \otimes g_1 \otimes \cdots \otimes g_n$. It is not difficult to see that F_n is a free $\mathbb{Z}G$-module of rank $|G|^n$ with $\mathbb{Z}G$ basis given by the elements $1 \otimes g_1 \otimes g_2 \otimes \cdots \otimes g_n$, where $g_i \in G$. The map $\mathrm{aug} : F_0 \to \mathbb{Z}$ is the *augmentation map* $\mathrm{aug}(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g$, and the map d_1 is given by $d_1(1 \otimes g) = g - 1$. The maps d_n for $n \geq 2$ are more complicated and their definition, together with a proof that (16) is a projective (in fact, free) resolution can be found in Exercises 1–3.

Applying ($\mathbb{Z}G$-module) homomorphisms from the terms in (16) to the G-module A (replacing the first term by 0) as in the previous section, we obtain the cochain complex

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(F_0, A) \xrightarrow{d_1} \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{d_2} \mathrm{Hom}_{\mathbb{Z}G}(F_2, A) \xrightarrow{d_3} \cdots, \qquad (17.17)$$

the cohomology groups of which are, by definition, the groups $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$. Then, as in Theorem 8, the short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ of G-modules gives rise to a long exact sequence whose first terms are given by (15) and whose higher terms are the cohomology groups $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$.

To make this more explicit, we can reinterpret the terms in this cochain complex without explicit reference to the standard resolution of $\mathbb{Z}$, as follows. The elements of $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$ are uniquely determined by their values on the $\mathbb{Z}G$ basis elements of F_n, which may be identified with the n-tuples $(g_1, g_2, \ldots, g_n)$ of elements g_i of G. It follows for $n \geq 1$ that the group $\mathrm{Hom}_{\mathbb{Z}G}(F_n, A)$ may be identified with the set of functions from $G \times \cdots \times G$ (n copies) to A. For $n = 0$ we identify $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A)$ with A.

Definition. If G is a finite group and A is a G-module, define $C^0(G, A) = A$ and for $n \geq 1$ define $C^n(G, A)$ to be the collection of all maps from $G^n = G \times \cdots \times G$ (n copies) to A. The elements of $C^n(G, A)$ are called n-*cochains (of G with values in A)*.

Each $C^n(G, A)$ is an additive abelian group: for $C^0(G, A) = A$ given by the group structure on A; for $n \geq 1$ given by the usual pointwise addition of functions: $(f_1 + f_2)(g_1, g_2, \ldots, g_n) = f_1(g_1, g_2, \ldots, g_n) + f_2(g_1, g_2, \ldots, g_n)$. Under the identification of $\text{Hom}_{\mathbb{Z}G}(F_n, A)$ with $C^n(G, A)$ the cochain maps d_n in (17) can be given very explicitly (cf. also Exercise 3 and the following comment):

Definition. For $n \geq 0$, define the nth *coboundary* homomorphism from $C^n(G, A)$ to $C^{n+1}(G, A)$ by

$$d_n(f)(g_1, \ldots, g_{n+1}) = g_1 \cdot f(g_2, \ldots, g_{n+1})$$
$$+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1})$$
$$+ (-1)^{n+1} f(g_1, \ldots, g_n) \tag{17.18}$$

where the product $g_i g_{i+1}$ occupying the ith position of f is taken in the group G.

It is immediate from the definition that the maps d_n are group homomorphisms. It follows from the fact that (17) is a projective resolution that $d_n \circ d_{n-1} = 0$ for $n \geq 1$ (a self contained direct proof just from the definition of d_n above can also be given, but is tedious).

Definition.
 (1) Let $Z^n(G, A) = \ker d_n$ for $n \geq 0$. The elements of $Z^n(G, A)$ are called n-*cocycles*.
 (2) Let $B^n(G, A) = \text{image } d_{n-1}$ for $n \geq 1$ and let $B^0(G, A) = 1$. The elements of $B^n(G, A)$ are called n-*coboundaries*.

Since $d_n \circ d_{n-1} = 0$ for $n \geq 1$ we have image $d_{n-1} \subseteq \ker d_n$, so that $B^n(G, A)$ is always a subgroup of $Z^n(G, A)$.

Definition. For any G-module A the quotient group $Z^n(G, A)/B^n(G, A)$ is called the nth *cohomology group of G with coefficients in A* and is denoted by $H^n(G, A), n \geq 0$.

The definition of the cohomology group $H^n(G, A)$ in terms of cochains will be particularly useful in the following two sections when we examine the low dimensional groups $H^1(G, A)$ and $H^2(G, A)$ and their application in a variety of settings. It should be remembered, however, that $H^n(G, A) \cong \text{Ext}^n(\mathbb{Z}, A)$ for all $n \geq 0$. In particular, these groups can be computed using *any* projective resolution of $\mathbb{Z}$.

Examples
 (1) For $f = a \in C^0(G, A)$ we have $d_0(f)(g) = g \cdot a - a$ and so $\ker d_0$ is the set $\{a \in A \mid g \cdot a = a$ for all $g \in G\}$, i.e., $Z^0(G, A) = A^G$ and so
$$H^0(G, A) = A^G,$$
for any group G and G-module A.

(2) Suppose $G = 1$ is the trivial group. Then $G^n = \{(1, 1, \ldots, 1)\}$ is also the trivial group, so $f \in C^n(G, A)$ is completely determined by $f(1, 1, \ldots, 1) = a \in A$. Identifying $f = a$ we obtain $C^n(G, A) = A$ for all $n \geq 0$. Then, if $f = a \in A$,

$$d_n(f)(1, 1, \ldots, 1) = a + \sum_{i=1}^{n}(-1)^i a + (-1)^{n+1}a = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases},$$

so $d_n = 0$ if n is even and $d_n = 1$ is the identity if n is odd. Hence

$$H^0(1, A) = A^G = A$$
$$H^n(1, A) = 0 \text{ for all } n \geq 1.$$

Example: (Cohomology of a Finite Cyclic Group)

Suppose G is cyclic of order m with generator σ. Let $N = 1 + \sigma + \sigma^2 + \cdots + \sigma^{m-1} \in \mathbb{Z}G$. Then $N(\sigma - 1) = (\sigma - 1)N = \sigma^m - 1 = 0$, and so we have a particularly simple free resolution

$$\cdots \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \cdots \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\text{aug}} \mathbb{Z} \longrightarrow 0$$

where aug denotes the augmentation map (cf. Exercise 8). Taking $\mathbb{Z}G$-module homomorphisms from the terms of this resolution to A (replacing the first term by 0) and using the identification $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) = A$ gives the chain complex

$$0 \longrightarrow A \xrightarrow{\sigma-1} A \xrightarrow{N} A \xrightarrow{\sigma-1} A \xrightarrow{N} \cdots$$

whose cohomology computes the groups $H^n(G, A)$:

$$H^0(G, A) = A^G, \text{ and } H^n(G, A) = \begin{cases} A^G/NA & \text{if } n \text{ is even, } n \geq 2 \\ {}_NA/(\sigma - 1)A & \text{if } n \text{ is odd, } n \geq 1 \end{cases}$$

where ${}_NA = \{a \in A \mid Na = 0\}$ is the subgroup of A annihilated by N, since the kernel of multiplication by $\sigma - 1$ is A^G.

If in particular $G = \langle \sigma \rangle$ acts trivially on A, then $N \cdot a = ma$, so that in this case $H^0(G, A) = A$, with $H^n(G, A) = A/mA$ for even $n \geq 2$, and $H^n(G, A) = {}_mA$, the elements of A of order dividing m, for odd $n \geq 1$. Specializing even further to $m = 1$ gives Example 2 previously.

Proposition 20. Suppose $mA = 0$ for some integer $m \geq 1$ (i.e., the G-module A has exponent dividing m as an abelian group). Then

$$mZ^n(G, A) = mB^n(G, A) = mH^n(G, A) = 0 \quad \text{for all } n \geq 0.$$

In particular, if A has exponent p for some prime p then the abelian groups $Z^n(G, A)$, $B^n(G, A)$ and $H^n(G, A)$ have exponent dividing p and so these groups are all vector spaces over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proof: If $f \in C^n(G, A)$ is an n-cochain then $f \in A$ (if $n = 0$), in which case $mf = 0$, or f is a function from G^n to A (if $n \geq 1$), in which case mf is a function from G^n to $mA = 0$, so again $mf = 0$. Hence $mZ^n(G, A) = mB^n(G, A) = 0$ since these are subgroups of $C^n(G, A)$. Then $mH^n(G, A) = 0$ since $mZ^n(G, A) = 0$, and the remaining statements in the proposition are immediate.

By Example 1, the long exact sequence in Theorem 10 written in terms of the cohomology groups $H^n(G, A)$ becomes