CLASSIFICATION OF GROUP EXTENSIONS AND H^2

RAPHAEL HO

Abstract. In this paper we will outline the foundations of homological algebra, starting with the theory of chain complexes which arose in algebraic topology. Building upon that we shall then introduce the derived functors Ext and Tor and their various properties. Finally, we will apply the theory built thus far to the case of group cohomology to classify equivalence classes of group extensions. Throughout this paper we will assume basic knowledge of module theory and familiarity with elementary categorical language.

Contents

1. Chain Complexes

Let R be a unital and assoctiative ring. Unless precised otherwise, R-modules shall refer to right R-modules.

Definition 1.1. A chain complex C_* of R-modules is a collection $\{C_n\}_{n\in\mathbb{Z}}$ together with R-module maps $d_n : C_n \to C_{n-1}$, called boundary operators or differentials, satisfying the relation $d_{n+1} \circ d_n = 0$. In particular, this implies that $\mathrm{im}(d_{n-1}) \subseteq \ker(d_n)$. If $\ker(d_n) = \mathrm{im}(d_{n-1})$, we then say the resulting sequence is exact. Denoting $\mathrm{im}(d_{n+1})$ by B_n and $\ker(d_n)$ by Z_n, we always have $0 \subseteq B_n \subseteq Z_n \subseteq C_n$. Elements in B_n are called n-boundaries, while elements in Z_n are called n-cycles. This geometric terminology comes from algebraic topology where chain complexes first arose. This leads us to consider the quotient Z_n/B_n, which we call the n-th homology module of C_* and write as $H_n(C_*)$. We often drop the subscript on C_* and simply write $H_n(C)$.

Example 1.2. Simplicial homology. Given a simplicial complex K of dimension n, we may look at the set K_k of k-dimensional simplices ($0 \leq k \leq n$). We form a chain complex by taking the free $\mathbb{Z}$-module on the set K_k. For $k > n$ we set

Date: DEADLINE AUGUST 26, 2011.

$C_k = 0$. The boundary homomorphisms $\partial_k : C_k \to C_{k-1}$ are given by sending a basis element $\sigma = \langle v_0, v_1, \ldots, v_k \rangle$ to $\partial_k(\sigma) = \sum_{i=0}^{k}(-1)^i \langle v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k \rangle$ These maps are obviously homomorphisms, and one can easily compute that the composite $\partial_{k-1}\partial_k$ is zero. The homology of this chain complex is called the simplicial homology of K with coefficients in $\mathbb{Z}$.

Definition 1.3. Let C_* be a chain complex of R-modules. We say a chain complex B_* is a subcomplex of C_* if for each n, $B_n \subseteq C_n$ and the differential on B_* is the restriction to B_n of the differential given by C_*.

Definition 1.4. A map $f : B_* \to C_*$ between chain complexes is a family of maps $f_n : B_n \to C_n$ such that the following diagram commutes:

$$\begin{tikzcd}
\cdots \arrow[r] & B_{n+1} \arrow[r, "d"] \arrow[d, "f_{n+1}"] & B_n \arrow[r, "d"] \arrow[d, "f_n"] & B_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & \cdots \\
\cdots \arrow[r] & C_{n+1} \arrow[r, "d"] & C_n \arrow[r, "d"] & C_{n-1} \arrow[r] & \cdots.
\end{tikzcd}$$

In other words, $d \circ f_{n+1} = f_n \circ d$ for all n. In particular, f sends cycles to cycles and boundaries to boundaries. Thus, f induces a well-defined map $f_* : H_n(B) \to H_n(C)$ for all n.

Considering chain complexes as objects and maps between complexes as morphisms, we may define a category Ch(Mod-R) of chain complexes. The argument above shows that for each n, H_n is a functor from Ch(Mod-R) to Mod-R.

Definition 1.5. Using the notational change $C_{-n} = C^n$, we can define the notion of a cochain complex in a similar fashion to chain complexes. A cochain complex C^* is a family of R-modules $\{C^n\}_{n\in\mathbb{Z}}$ with maps $d^n : C^n \to C^{n+1}$ such that $d^{n+1} \circ d^n = 0$. The kernel Z^n of d^n is the module of n-cocycles, while $B^n = \operatorname{im}(d^{n-1})$ is called the module of n-coboundaries. Once again, we may consider the quotient $H^n(C^*) = Z^n/B^n$, which we unsurprisingly dub the n-th cohomology module of C^*. Maps between cochain complexes are defined in a similar manner to maps of chain complexes.

Now that we have defined what a map of chain complex is, we can consider short exact sequences of chain (or cochain) complexes

$$0 \to A_* \xrightarrow{f} B_* \xrightarrow{g} C_* \to 0$$

i.e maps such that for all n,

$$0 \to A_n \xrightarrow{f} B_n \xrightarrow{g} C_n \to 0$$

is exact and the maps commute with the boundary operators.

Lemma 1.6. *(Snake lemma)*
Consider the following diagram of R-modules:

$$\begin{tikzcd}
 & A \arrow[r, "i"] \arrow[d, "f"'] & B \arrow[r, "j"] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & A' \arrow[r, "p"'] & B' \arrow[r, "q"'] & C' & .
\end{tikzcd}$$

If the top and bottom row are exact, then there exists an exact sequence

$$\ker(f) \to \ker(g) \to \ker(h) \xrightarrow{\delta} \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(h).$$

If, furthermore, the rows are short exact sequences, the above sequence can be extended to an exact sequence

$$0 \to \ker(f) \to \ker(g) \to \ker(h) \xrightarrow{\delta} \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(h) \to 0.$$

Proof. The maps between kernels are simply the restriction of the maps of the top row. Commutativity of the diagram ensures that they are well defined. The maps between cokernels are defined by taking a coset represented by one element to the coset represented by the image of that element under the corresponding bottom row map. To define the map $\delta : \ker(h) \to \operatorname{coker}(f)$, we must do a bit more diagram chasing. Let $\gamma \in \ker(h)$. We can lift γ to an element $b \in B$, and take its image $g(b)$ in B'. Now $h(\gamma) = hj(b) = qg(b) = 0$, so $g(b) \in \ker(q) = \operatorname{im}(p)$, thus we can lift $g(b)$ to $x \in A'$. Since p is injective, this element is unique. Our candidate for the map δ is now the composite $\delta(\gamma) = p^{-1}gj^{-1}(\gamma) + \operatorname{im}(f)$. The only ambiguity in this definition is the choice of lift $j^{-1}(\gamma)$. Suppose we chose $j(b_1) = j(b_2) = \gamma$. Then by the diagram chase above, there exists unique $x_1, x_2 \in A'$ such that $p(x_1) = g(b_1)$ and $p(x_2) = g(b_2)$. Now j is a homomorphism, so $b_1 - b_2 \in \ker(j) = \operatorname{im}(i)$, hence there exists $a \in A$ such that $i(a) = b_1 - b_2$, hence $j(f(a)) = g(i(a)) = j(x_1 - x_2)$. Injectivity now gives us that $f(a) = x_1 - x_2$, hence $x_1 + \operatorname{im}(f) = x_2 + \operatorname{im}(f)$, i.e δ is well defined.

The proof that the sequence we obtain by pasting these maps together is exact at each term is a straightforward (if somewhat lengthy) diagram chase. Furthermore, if i is injective and q is surjective, the corresponding maps $\ker(f) \to \ker(g)$ and $\operatorname{coker}(g) \to \operatorname{coker}(h)$ are also injective and surjective respectively from the way they are defined, giving us the augmented sequence. □

Theorem 1.7. *Given a short exact sequence of chain complexes*

$$0 \to L_* \xrightarrow{f} M_* \xrightarrow{g} N_* \to 0,$$

there exists a long exact sequence

$$\cdots \xrightarrow{g_*} H_{n+1}(N) \xrightarrow{\partial} H_n(L) \xrightarrow{f_*} H_n(M) \xrightarrow{g_*} H_n(N) \xrightarrow{\partial} H_{n-1}(L) \xrightarrow{f_*} \cdots .$$

The maps $\partial : H_{n+1}(N) \to H_n(L)$ are called the connecting homomorphisms.

Dually, if $0 \to L^* \xrightarrow{f} M^* \xrightarrow{g} N^* \to 0$ is a short exact sequence of cochain complexes, there exist connecting homomorphisms $\partial : H^{n-1}(N) \to H^n(L)$ such that the following sequence is exact:

$$\cdots \xrightarrow{g_*} H^{n-1}(N) \xrightarrow{\partial} H^n(L) \xrightarrow{f_*} H^n(M) \xrightarrow{g_*} H^n(N) \xrightarrow{\partial} H^{n+1}(L) \xrightarrow{f_*} \cdots .$$

Proof. We supply the proof for the case of chain complexes. The proof follows exactly the same way for cochain complexes.

Consider the short exact sequence at the $(n+1)$-th term.

$$\begin{tikzcd}
0 \arrow[r] & L_{n+1} \arrow[r, "f"] \arrow[d, "d^L"] & M_{n+1} \arrow[r, "g"] \arrow[d, "d^M"] & N_{n+1} \arrow[r] \arrow[d, "d^N"] & 0 \\
0 \arrow[r] & L_n \arrow[r, "f"] & M_n \arrow[r, "g"] & N_n \arrow[r] & 0
\end{tikzcd}$$

Given any R-module homomorphism $A \xrightarrow{f} B$, we may form the exact sequence

$$0 \to \ker(f) \to A \xrightarrow{f} B \to \operatorname{coker}(f) \to 0.$$

Applying this construction to the columns of the given diagram then applying the snake lemma gives us the following commutating diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & Z_{n+1}(L) \arrow[r] \arrow[d] & Z_{n+1}(M) \arrow[r] \arrow[d] & Z_{n+1}(N) \arrow[d] & \\
0 \arrow[r] & L_{n+1} \arrow[r, "f"] \arrow[d, "d^L_{n+1}"] & M_{n+1} \arrow[r, "g"] \arrow[d, "d^M_{n+1}"] & N_{n+1} \arrow[r] \arrow[d, "d^N_{n+1}"] & 0 \\
0 \arrow[r] & L_n \arrow[r, "f"] \arrow[d] & M_n \arrow[r, "g"] \arrow[d] & N_n \arrow[r] \arrow[d] & 0 \\
 & L_n/B_n(L) \arrow[r] \arrow[d] & M_n/B_n(M) \arrow[r] \arrow[d] & N_n/B_n(N) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 & .
\end{tikzcd}$$

By definition of the boundary operators, the maps $d^X_n : X_n \to X_{n-1}$ factor through $X_{n+1}/B_{n+1}(X) \to Z_n(X)$, thus the above diagram gives the following diagram, in which the rows are exact:

$$\begin{tikzcd}
 & L_{n+1}/B_{n+1}(L) \arrow[r] \arrow[d, "d^L_{n+1}"] & M_{n+1}/B_{n+1}(M) \arrow[r] \arrow[d, "d^M_{n+1}"] & N_{n+1}/B_{n+1}(N) \arrow[r] \arrow[d, "d^N_{n+1}"] & 0 \\
0 \arrow[r] & Z_n(L) \arrow[r] & Z_n(M) \arrow[r] & Z_n(N) & .
\end{tikzcd}$$

Note that the kernel of the vertical maps are precisely the $(n+1)$-th homology module of that complex, while the cokernels are the n-th homology. Thus, applying the snake lemma to the above sequence gives us an exact sequence

$$H_{n+1}(L) \to H_{n+1}(M) \to H_{n+1}(N) \to H_n(L) \to H_n(M) \to H_n(N).$$

By pasting these sequences together, we obtain the desired long exact sequence.

□

Definition 1.8. A map $f : C_* \to D_*$ of chain complexes is said to be null-homotopic if there exists maps $s_n : C_n \to D_{n+1}$ such that $f_n = d_{n+1}s_n + s_{n-1}d_n$ We say f is homotopic to g if their difference $f - g$ is null-homotopic.
For convenience, we often drop the subscripts and simply write $f = ds + sd$.

Proposition 1.9. *Let $f, g : C_* \to D_*$ be chain maps. If f and g are chain homotopic, then they induce the same map on the homology modules $H_n(C) \to H_n(D)$*

Proof. It suffices to prove that if f is null-homotopic, then the induced map on homology is the zero map. Suppose $f = ds + sd$. Let x be an n-cycle representing an element in $H_n(C)$. Then $f(x) = ds(x) + sd(x) = ds(x)$ since $x \in \ker(d)$. Thus $f(x)$ is an n-boundary in D_n, hence is trivial in the module $H_n(D)$. □

2. Ext and Tor

2.1. **Projective Resolutions and Tor.** Let R be a fixed ring.

Definition 2.1. An R-module (left or right) P is projective if given a surjective map $g : M \to N$ of R-modules and a map $f : P \to N$, there exists a map $\bar{f} : P \to M$ such that $f = g \circ \bar{f}$. Pictorially, we have the following diagram:

$$\begin{tikzcd}
& P \arrow[dl, dotted, "\exists \bar{f}"'] \arrow[d, "f"] & \\
M \arrow[r, "g"] & N \arrow[r] & 0.
\end{tikzcd}$$

Lemma 2.2. *Free R-modules are projective.*

Proof. Since g is surjective, for any $n \in \text{im}(f)$, there exists an element $m \in M$ such that $g(m) = n$. Let A be a set of generators for the free R-module P, and define a set map $\phi : f(A) \subseteq N \to M$ that takes $f(p) \in N$ to an element m_p in its pre-image under g. By the universal property of free objects there exists an R-module homomorphism $\bar{f} : P \to M$ such that $\bar{f}(p) = m_p$. In other words $(g \circ \bar{f})(p) = f(p)$. □

Proposition 2.3. *An R-module P is projective if and only if it is a direct summand of a free module.*

Proof. Let Q be an R-module such that $P \oplus Q = F$ is free. If $\pi : F \to P$ is the projection map, $\pi \circ f$ gives a map $F \to M$. By the previous lemma, F is projective, thus composing $F \to M$ with the inclusion $P \hookrightarrow F$ gives us the desired map $\bar{f} : P \to M$ such that $f = g \circ \bar{f}$.
Conversely, if P is projective, let $F(P)$ be the free R-module on the underlying set of P and choose (as we always can) a surjection $\pi : F(P) \to P$. Taking the identity map on P and using the definition of a projective module gives us a map $i : P \to F(P)$ such that $\pi \circ i = \text{id}$, i.e P is a direct summand of $F(P)$. □

Definition 2.4. Let L and M be right R-modules, and let $0 \to L \xrightarrow{\psi} M$ be exact. A right R-module A is flat if the sequence $0 \longrightarrow A \otimes L \xrightarrow{1 \otimes \psi} A \otimes M$ is exact.
We have a symmetrical definition for flat left R-modules.

Corollary 2.5. *Projective modules are flat.*

Proof. This follows from the fact that free modules and more generally direct summand of free modules are flat (cf D&F, chap. 10.5, Cor. 42) [2]. □

Definition 2.6. A left resolution of an R-module M is a chain complex P_* such that $P_i = 0$ for $i < 0$, together with a map $\epsilon : P_0 \to M$ such that the augmented complex

$$\cdots \xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{\epsilon} M \to 0$$

is exact. If each P_i is a projective module, we say it is a projective resolution. It is often convenient to view M as a chain complex concentrated in its last term and consider $P_* \xrightarrow{\epsilon} M$ as a map of chain complexes.

Lemma 2.7. *Every R-module has a projective resolution.*

Proof. Starting with an R-module M, choose a free (hence projective) module P_0 such that M is a quotient of P_0. The natural projection $\epsilon : P_0 \to M$ is a surjection. We may now choose a free module P_1 such that the module $\ker(\epsilon)$ is a quotient of P_1 and define the map $d : P_1 \to P_0$ to be the composite of the natural projection $P_1 \to \ker(\epsilon)$ with the inclusion $\ker(\epsilon) \hookrightarrow P_0$. Since any R-module is always the quotient of a free module, we may proceed inductively and form surjections $P_{i+1} \to \ker(d_i)$ with P_{i+1} free. Pictorially we have the following diagram:

$$\begin{tikzcd}
0 \arrow[dr] & & 0 & & & & \\
& \ker(d_1) \arrow[ur] \arrow[dr] & & & & & \\
\cdots \arrow[ur] \arrow[rr, "d_2"] & & P_1 \arrow[rr, "d_1"] \arrow[dr] & & P_0 \arrow[r, "\epsilon"] & M \arrow[r] & 0 \\
& & & \ker(\epsilon) \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & & .
\end{tikzcd}$$

□

Theorem 2.8. *(Comparison Theorem)*
Let M, N be R-modules, and suppose $f : M \to N$ is a map of R-modules. Given a map of chain complexes $P_* \xrightarrow{\epsilon} M$ such that each P_i is projective and an arbitrary left resolution $Q_* \xrightarrow{\eta} N$, there exists a map of chain complexes $\tilde{f} : P_* \to Q_*$ lifting f in the sense that $\eta \circ \tilde{f} = f \circ \epsilon$. This map is unique up to chain homotopy.

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r] \arrow[d, dotted, "\tilde{f}"] & P_1 \arrow[r] \arrow[d, dotted, "\tilde{f}"] & P_0 \arrow[r, "\epsilon"] \arrow[d, dotted, "\tilde{f}"] & M \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r] & Q_2 \arrow[r] & Q_1 \arrow[r] & Q_0 \arrow[r, "\eta"] & N \arrow[r] & 0
\end{tikzcd}$$

Proof. Since P_0 is projective and η is a surjection, we can lift η to a map $\tilde{f}_0 : P_0 \to Q_0$ such that $\eta\tilde{f}_0 = f\epsilon$. Inductively, if we have a map $\tilde{f}_{i-1}$ such that $d_{i-1}\tilde{f}_{i-1} = \tilde{f}_{i-2}d_{i-1}$ (thinking of f as f_{-1} and d_0 as η or ϵ), then $d_{i-1}\tilde{f}_{i-1}d_i = 0$, hence $\tilde{f}_{i-1}d_i$ maps P_i to $\ker(d_{i-1})$, which is equal to $\mathrm{im}(d_i)$ by exactness. Thus by projectivity of P_i we get a map $\tilde{f}_i$ such that $d_i\tilde{f}_i = \tilde{f}_{i-1}d_i$.
Now suppose we have another map $\tilde{f'} : P_* \to Q_*$. Then $\eta(\tilde{f'}_0 - \tilde{f}_0) = 0$ hence $\tilde{f'}_0 - \tilde{f}_0$ sends P_0 to $\ker(\eta) = \mathrm{im}(d_1)$. Since P_0 is surjective, we get a map $s_0 : P_0 \to Q_1$ so

that $(\widetilde{f'}_0 - \tilde{f}_0) = ds_0 = ds_0 + s_{-1}d$, where s_{-1} is the zero map. Inductively, if we have s_{i-1} such that $(\widetilde{f'}_{i-1} - \tilde{f}_{i-1}) = d_i s_{i-1} + s_{i-2}d_{i-1}$, then $d_i(\widetilde{f'}_i - \tilde{f}_i - s_{i-1}d_i) = 0$, so again by projectivity of P_i there exists a map $s_i : P_i \to Q_{i+1}$ such that $d_{i+1}s_i = \widetilde{f'}_i - \tilde{f}_i - s_{i-1}d_i$. □

Lemma 2.9. *(Horseshoe Lemma)*
Suppose we have a short exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *of* R*-modules. Let* P'_*, P''_* *be projective resolutions of* M' *and* M'' *respectively. Then there exists a projective resolution* P_* *of* M *such that* $0 \to P'_* \xrightarrow{i} P_* \xrightarrow{\pi} P''_* \to 0$ *is a (split) short exact sequence of chain complexes.*

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
\cdots P'_2 \arrow[r] & P'_1 \arrow[r] & P'_0 \arrow[r, "\epsilon'"] & M' \arrow[r] \arrow[d, "f"] & 0 \\
 & & & M \arrow[d, "g"] & \\
\cdots P''_2 \arrow[r] & P''_1 \arrow[r] & P''_0 \arrow[r, "\epsilon''"] & M'' \arrow[r] \arrow[d] & 0 \\
 & & & 0 & .
\end{tikzcd}$$

Proof. The proof of this lemma will be omitted due to space constraints. Readers searching for completion may find it filled out in detail in Weibel [1]. The idea however, is to define P_n to be the direct sum $P'_n \oplus P''_n$ and then use projectivity to build the required maps. □

Since $\otimes_R$ preserves exactness of the sequence on the right but not on the left, we say it is a right exact functor. We now introduce the torsion product, which measures how by how much $\otimes_R$ fails to be exact (i.e both left and right exact).

Definition 2.10. Let M be a right R-module and N be a left R-module. Choose a projective resolution $P_* \xrightarrow{\epsilon} M$. Define $\mathrm{Tor}_n^R(M, N) = H_n(P \otimes_R N)$. This means that for all n, $\mathrm{Tor}_n^R(M, N)$ is a functor from Mod-R × R-Mod to Ab.

The first thing we need to check is that $\mathrm{Tor}_n^R(M, N)$ does not depend on the choice of resolution of M.

Lemma 2.11. *If* $Q_* \xrightarrow{\eta} M$ *is another projective resolution, then we have an isomorphism* $H_n(Q \otimes_R N) \cong H_n(P \otimes_R N)$*, hence* $\mathrm{Tor}_n^R(M, N)$ *does not depend on the choice of resolution for* M*.*

Proof. Consider the identity map $\mathrm{id}_M : M \to M$. Using the comparison theorem, we get a map of chain complexes $\tilde{f} : P_* \to Q_*$ commuting with the boundary maps on P_* and Q_*. We thus get maps f_* on the homology modules $H_n(P_*) \xrightarrow{f_*} H_n(Q_*)$. As we've seen in the proof of the theorem, this map is unique up to homotopy. Now Q_* is also projective, so similarly we get a map $g_* : H_n(Q_*) \to H_n(P_*)$. The maps

gf and id_P are both chain maps $P \to P$ lifting id_M, thus $g_* f_* = (gf)_* = (\mathrm{id}_P)_* = \mathrm{id}_{H_n(P)}$. Similarly, fg and id_Q both lift id_M, so $f_* g_*$ is the identity on $H_n(Q_*)$, hence f_* and g_* are isomorphisms. □

We may now list a few useful properties about Tor.

Proposition 2.12. $\mathrm{Tor}_0^R(M,N)$ *is naturally isomorphic to* $M \otimes_R N$. *Furthermore, if either* M *or* N *is projective, then* $\mathrm{Tor}_n^R(M,N) = 0$ *for* $n \geq 1$

Proof. Since $\otimes_R$ is right exact, the sequence

$$P_1 \otimes_R N \to P_0 \otimes_R N \to M \otimes_R N \to 0$$

is exact, thus $\mathrm{Tor}_0^R(M,N) = H_0(P_0 \otimes_R N) = M \otimes_R N$.
If M is projective, the identity map $M \to M$ can be seen as a projective resolution. Since projective modules are flat, the the tensor functor is exact, thus the homology group of the chain is trivial for $i > 0$. □

Theorem 2.13. *For every short exact sequence of right* R*-modules* $0 \to M' \to M \to M'' \to 0$*, if* N *is a fixed left* R*-module then there exists a long exact sequence*

$$\cdots \to \mathrm{Tor}_n^R(M',N) \to \mathrm{Tor}_n^R(M,N) \to \mathrm{Tor}_n^R(M'',N) \xrightarrow{\partial} \mathrm{Tor}_{n-1}^R(M',N) \to \cdots$$

Proof. Given

$$0 \to M' \to M \to M'' \to 0$$

choose projective resolutions $P' \to M'$ and $P'' \to M''$. Using the Horseshoe Lemma, there exists a projective resolution $P \to M$ such that the each

$$0 \to P'_n \to P_n \to P''_n \to 0$$

is split exact. Since $\otimes_R$ is an additive functor, $P_n \otimes_R N = (P'_n \oplus P''_n) \otimes_R N = (P'_n \otimes_R N) \oplus (P''_n \otimes_R N)$, hence the sequence

$$0 \to P'_n \otimes_R N \to P_n \otimes_R N \to P''_n \otimes_R N \to 0$$

is also split exact. This means that $0 \to (P' \otimes_R N)_* \to (P_n \otimes_R N)_* \to (P''_n \otimes_R N)_* \to 0$ is a short exact sequence of chain complexes. The corresponding long exact sequence on the homology of these chain complexes is sequence promised in the statement of the theorem. □

Tor is an example of a left derived functor, namely the left derived functor of the tensor product. More generally, one can define the left derived functor of a right exact functor between two abelian categories, provided the domain category has enough projectives. What we mean by this is that for each object A in the category there exists a surjection $P \to A$ with P satisfying the same universal property as layed out in the definition of a projective module. The 'left' part of the terminology comes from the fact that after applying our right exact functor to a short exact sequence, we wish to prolong this to a long exact sequence on the left. Axiomatizing the properties we've seen above for Tor, with a little work it can be shown that the left derived functor is universal with respect to extending short exact sequences to long exact sequences on the left. In particular, this means that we could reverse the roles of M and N above and choose a projective resolution of N instead and still obtain the same functor.

2.2. **Injective Resolutions and Ext.** There is a dual notion to projectivity in an abelian category which is called injectivity. Although the Ext functor which we shall introduce in this section can be defined using only projective modules, we shall include some basic facts about injective modules for completion.

Definition 2.14. Let R, S be rings. An (R, S)-bimodule M is simultaneously a left R-module and a right S-module such that $(rm)s = r(ms)$.

Proposition 2.15. *Let L be a right R-module, M an (R, S)-bimodule and N a left S-module. We can impose a right R-module structure on $\mathrm{Hom}_S(M, N)$ by the rule $(fr)(m) = f(rm)$. The functors $\mathrm{Hom}_S(M, -)$ from Mod-S to Mod-R and $-\otimes_R M$ from Mod-R to Ab form an adjunction, meaning that for every right R-module L and left S-module N there is a natural isomorphism*

$$\mathrm{Hom}_S(L \otimes_R M, N) \cong \mathrm{Hom}_R(L, \mathrm{Hom}_S(M, N))$$

Proof. Starting with a map $f : L \otimes_R M \to N$, define $\tau : \mathrm{Hom}_S(L \otimes_R M, N) \to \mathrm{Hom}_R(L, \mathrm{Hom}_S(M, N))$ by letting $(\tau f)(l)$ be the map $m \mapsto f(l \otimes_R m)$ for each $l \in L$. Conversely, if we have a map $g : L \to \mathrm{Hom}_S(M, N)$, let $\tau^{-1}(g)$ be the bilinear form $l \otimes_R m \mapsto g(l)(m)$.
The map $m \mapsto f(l \otimes_R m)$ is an S-module map since

$$ms+m's' \mapsto f(l\otimes(ms+m's')) = f(s(l\otimes m)+s'(l\otimes m')) = (fs)(l\otimes m)+(fs')(l\otimes m')$$

We also have that f is an R-module map since $(\tau f)(rl+r'l')$ is the map $m \mapsto f((rl+r'l')\otimes m) = rf(l\otimes m)+r'f(l\otimes m)$, which is the same as taking $\tau(rf)(m)+\tau(r'f)(m')$. Furthermore, $\tau^{-1}(g)(r(l \otimes m) + r'(l' \otimes m)) = g(rl + r'l')(m) = (g(rl) + g(r'l'))(m)$ so $\tau^{-1}(g)$ is also an R-module map. The maps τ and τ^{-1} are clearly inverse of each other, thus τ is an isomorphism. The proof that this isomorphism is natural is left to the reader. □

Taking $S = \mathbb{Z}$ and $M = R$ as a $(\mathbb{Z}, R)$-bimodule in the above proposition gives us the following specialized version.

Corollary 2.16. *Let L be a left R-module and N be an abelian group. We then have a natural isomorphism of abelian groups*

$$Hom_{\mathbb{Z}}(L, N) \cong Hom_R(L, Hom_{\mathbb{Z}}(R, N))$$

Proof. This follows immediately from the fact that $L \otimes_R R \cong L$ and the above proposition. □

Definition 2.17. An R-module I is said to be injective if for any injection $e : M \to N$ of modules and each map $f : M \to I$, there exists a map $\tilde{f} : M \to I$ making the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "e"] \arrow[d, "f"] & N. \arrow[dl, dotted, "\exists \tilde{f}"] \\
& I &
\end{tikzcd}$$

Proposition 2.18. *(Baer's Criterion)*
A right module I is injective if and only if for every right ideal J of R, every map $J \to I$ can be extended to a map $R \to I$.

Proof. Since right ideals are R-modules, the 'only if' direction is clear from the definition of injectivity.
Conversely suppose every homomorphism $g : J \to I$ can be lifted to a map $G : R \to I$. Let $e : M \to N$ be injective, so that $e(M)$ is a submodule of N. Given a map $f : M \to I$, we can look at the set $\mathcal{S}$ of all extensions $f' : A' \to I$ of f to an intermediate submodule $e(M) \subseteq A' \subseteq N$. We can define a partial order on this set by letting $(f', A') \leq (f'', A'')$ if $L' \subseteq L''$ and $f'' = f'$ on L'. By Zorn's Lemma, there exists a maximal extension $f' : A' \to I$ in $\mathcal{S}$. Suppose there exists some $n \in N$ not in A'. We can then look at the right ideal $J = \{r \in R | mr \in A'\}$. We thus have a map $J \xrightarrow{m} A' \xrightarrow{f'} I$, hence by assumption it extends to a map $G : R \to I$. Define $A'' \subseteq M$ to be the submodule $A' + mR$ and let $f'' : A'' \to I$ by $f''(a + mr) = f'(a) + G(r)$. If $mr \in A' \cup mR$, $f'(mr) = G(r)$ so this map is well defined, and f'' extends f', contradicting the maximality of f'. We thus have that $A' = N$, thus completing the proof. □

Corollary 2.19. *If R is a PID, an R-module I is injective if and only if it is divisible, meaning that for every non-zero $r \in R$ and every $x \in I$, $x = yr$ for some $y \in I$.*

Proof. If R is a PID, then every ideal is of the form $J = (r)$ for some $r \in R$, hence any R-module homomorphisms $g : J \to I$ is uniquely determined by $g(r) = i \in I$. We can extend this homomorphism to a map $G : R \to I$ if and only if there exists an element $i' \in I$ with $G(1) = i'$ such that $i = g(r) = G(r) = ri'$. Hence by Baer's criterion I is injective if and only if $rI = I$. □

Lemma 2.20. *Every R-module embeds as a submodule of an injective R-module.*

Proof. We prove this for $\mathbb{Z}$-modules first, then generalize to an arbitrary ring. Since abelian groups can be regarded as $\mathbb{Z}$-modules and $\mathbb{Z}$ is a PID, by the above corollary an abelian group A is injective if and only if A is divisible. If M is any $\mathbb{Z}$-module, let G be a set of generators for M. Let $\mathcal{F}$ be the free module on the set G. We can then identify $M = \mathcal{F}/\mathcal{K}$ where $\mathcal{K}$ is a $\mathbb{Z}$-module. Now take $\mathcal{Q}$ to be the free $mathbbQ$-module on G. $\mathcal{Q}$ is a direct sum of copies of $\mathbb{Q}$, hence divisible since $\mathbb{Q}$ is. Now $\mathcal{K} \subseteq \mathcal{F} \subseteq \mathcal{Q}$, thus $M = \mathcal{F}/\mathcal{K} \subseteq \mathcal{Q}/\mathcal{K}$. Since the quotient of divisible groups is again divisible, this show M is a submodule of an injective $\mathbb{Z}$-module.
Now let R be an arbitrary ring, and let N be a left R-module. Define a map $j : N \to \operatorname{Hom}_{\mathbb{Z}}(R, N)$ by $j(n)(r) = rn$. Clearly this is a homomorphism between abelian groups, however recall that $\operatorname{Hom}_{\mathbb{Z}}(R, N)$ has a left R-module structure given by $(rf)(n) = f(rn)$. Thus if $r, s \in R$ and $n \in N$, we have that

$$j(sn)(r) = r(sn) = (rs)n = j(n)(rs) = s(j(n))(r)$$

It follows that j is in fact a map of R-modules. Since $j(n)(1) = n$, $j = 0$ if and only if $n = 0$, hence j is a injection. Now take any injective abelian group map $i : N \to D$ where D is divisible and let $i_* : \operatorname{Hom}_{\mathbb{Z}}(R, N) \to \operatorname{Hom}_{\mathbb{Z}}(R, D)$ be the induced map. Then i_* is an injection, thus the composite $i_* \circ j : N \to \operatorname{Hom}_{\mathbb{Z}}(R, D)$ is an injection of R-modules. Since D is an injective $\mathbb{Z}$-module, applying $\operatorname{Hom}_{\mathbb{Z}}(-, D)$ to an exact sequence $0 \to M' \to N'$ gives rise to an exact sequence $\operatorname{Hom}_{\mathbb{Z}}(N', D) \to \operatorname{Hom}_{\mathbb{Z}}(M', D) \to 0$. Now using Corollary 2.16, this tells us that the sequence $\operatorname{Hom}_R(N', \operatorname{Hom}_{\mathbb{Z}}(R, D)) \to \operatorname{Hom}_R(M', \operatorname{Hom}_{\mathbb{Z}}(R, D)) \to 0$ is exact, thus proving that $\operatorname{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module. □

Definition 2.21. An injective resolution of an R-module N is a cochain complex I^* and a map $\eta :\to I^0$ such that

$$0 \to N \xrightarrow{\eta} I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \xrightarrow{d} \cdots$$

is exact and each I^i is injective.

The following three statements have analogues in the previous section. Their proof is identical up to replacing 'projective' with 'injective' and reversing the direction of the arrows, and thus will not be supplied.

Lemma 2.22. *Every R-module has an injective resolution.*

Theorem 2.23. *(Comparison Theorem)*
Let M, N be R-modules, and suppose $f : M \to N$ is a map of R-modules. Given $N \xrightarrow{\epsilon} I^*$ an injective resolution and $M \xrightarrow{\eta} J^*$ an arbitrary right resolution, there exists a of chain complexes $\tilde{f} : J^* \to I^*$ lifting f in the sense that $\tilde{f} \circ \eta = \epsilon \circ f$. This map is unique up to chain homotopy.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\eta"] \arrow[d, "f"] & J^0 \arrow[r] \arrow[d, dotted, "\tilde{f}"] & J^1 \arrow[r] \arrow[d, dotted, "\tilde{f}"] & J^2 \arrow[r] \arrow[d, dotted, "\tilde{f}"] & \cdots \\
0 \arrow[r] & N \arrow[r, "\epsilon"] & I^0 \arrow[r] & I^1 \arrow[r] & I^2 \arrow[r] & \cdots
\end{tikzcd}$$

Lemma 2.24. *(Horseshoe Lemma) Suppose we have a short exact sequence $0 \to N' \xrightarrow{f} N \xrightarrow{g} N'' \to 0$ of R-modules. Let $(I')^*, (I'')^*$ be injective resolutions of N' and N'' respectively. Then there exists an injective resolution I^* of N such that $0 \to I'^* \xrightarrow{i} I^* \xrightarrow{\pi} I'' * * \to 0$ is a short exact sequence of chain complexes.*

As we've seen above, the torsion product is right exact. Building upon this functor we then defined a new functor Tor which allowed us to continue the sequence on the left. We will now introduce a left exact functor and similarly define Ext to be the functor extending exactness to the right.
If we start with a short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$ and an R-module N, the functor $\mathrm{Hom}_R(-, N)$ is left exact, i.e we get an exact sequence

$$0 \to \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M'', N)$$

Similarly, one can start with a short exact sequence $0 \to N' \to N \to N'' \to 0$ and a module M, then apply left exact functor $\mathrm{Hom}_R(M, -)$.

Definition 2.25. Let M, N be right R-modules, and let $P^* \xrightarrow{\epsilon} M$ be a projective resolution. Define

$$\mathrm{Ext}^*_R(M, N) = H^*(\mathrm{Hom}_R(P^*, N))$$

Alternatively, one can instead choose an injective resolution $N \xrightarrow{\eta} I^*$ and apply the left exact functor $\mathrm{Hom}_R(M, -)$ then take the homology of that complex to define $\mathrm{Ext}^*_R(M, N)$. The proof that this in fact gives us the same group is rather technical and will be omitted due to space constraints.
Analogously to Tor, $\mathrm{Ext}^n_R(M, N)$ is a functor from $(\mathrm{Mod}{-}R)^{op} \times \mathrm{Mod}{-}R$ to Ab for each n.

The properties of Ext are quite similar to those of Tor and proved analogously by taking a projective resolution of the first variable, or by taking an injective resolution in the second variable. We will state them without proof to avoid unnecessary redundancy.

Proposition 2.26. $\operatorname{Ext}^0_R(M,N)$ *is naturally isomorphic to* $\operatorname{Hom}_R(M,N)$*. If* M *is projective, then* $\operatorname{Ext}^n_R(M,N) = 0$ *for* $n \geq 0$*.*

Theorem 2.27. *Let* $0 \to M' \to M \to M'' \to 0$ *be a short exact sequence of* R*-modules and* N *be an* R*-module. Then the following sequence is exact:*

$$\cdots \to \operatorname{Ext}^n_R(M'',N) \to \operatorname{Ext}^n_R(M,N) \to \operatorname{Ext}^n_R(M',N) \to \operatorname{Ext}^{n+1}_R(M'',N) \to \cdots$$

If we now have an exact sequence $0 \to N' \to N \to N'' \to 0$ *and a module* M*, we also have an exact sequence*

$$\cdots \to \operatorname{Ext}^n_R(M,N') \to \operatorname{Ext}^n_R(M,N) \to \operatorname{Ext}^n_R(M,N'') \to \operatorname{Ext}^{n+1}_R(M,N') \to \cdots$$

3. Group Extensions and Group Cohomology

3.1. Group extensions.

Definition 3.1. Let A an abelian group and G be any group. We say a third group E is an extension of G by A if there exists a short exact sequence

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

Note that A (more precisely, $i(A)$) is a normal subgroup of E and that the quotient E/A is isomorphic to G.

Lemma 3.2. *An extension* E *of* G *by* A *defines a* G*-action on* A*.*

Proof. For each $g \in G$, choose an element $e_g \in \pi^{-1}(g) \subset E$. This defines a map of sets $\sigma : G \to E$ called a section of π. Since A is abelian and i is injective, the subgroup $i(A) \subseteq E$ is also abelian, and the element e_g acts on an element $i(a) \in i(A)$ by conjugation. As we've said before, $E/i(A) \cong G$, thus any other element in E mapping to g under π is of the form $e_g i(a_1)$ for some $a_1 \in A$. Using that i is a homomorphism and A is abelian, we see that conjugation by $e_g i(a_1)$ is the same as conjugation by e_g, hence the action is independent of our choice of e_g. This means that our G action is well defined on $i(A)$, hence on A as well since i is injective. □

This action of G on A turns A into a G-module, meaning that G acts on A as automorphisms. We can now look at when two extensions are essentially the same.

Definition 3.3. We say two extensions are isomorphic if there is an isomorphism of short exact sequences

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\alpha"] & E \arrow[r, "\pi"] \arrow[d, "\beta"] & G \arrow[r] \arrow[d, "\gamma"] & 1 \\
1 \arrow[r] & A' \arrow[r, "i'"] & E' \arrow[r, "\pi'"] & G' \arrow[r] & 1.
\end{tikzcd}$$

In other words, this diagram commutes and the vertical maps are isomorphisms. If we require the stronger condition that the maps α and γ be the identity, we then say that E and E' are equivalent extensions.

Proposition 3.4. *Equivalent extensions define the same G-module structure on A.*

Proof. If E and E' are two equivalent extensions as in the definition, let e_g be a representative of π^{-1} in E, and let $e'_g = \beta(e_g)$. This gives two actions of g on a, one sending a to $i^{-1}(e_g i(a) e_g^{-1})$ and the other to $i'^{-1}(e'_g\ i'(a)\ e'^{-1}_g)$. Since i, i', β are injective, these two actions are equal if and only if $(\beta \circ i)(i^{-1}(e_g i(a) e_g^{-1})) = e'_g i'(a) e'^{-1}_g$, which is true by the definition of e'_g and the commutativity of the diagram. □

3.2. **Group Cohomology.** We will now use an alternative definition of a G-module.

Definition 3.5. Let G be a group. The integral group ring $\mathbb{Z}[G]$ is the free abelian group with basis the set G, on which we put a ring structure with addition defined formally on integer linear combinations of elements of G, and multiplication defined by the group operation in G, extended $\mathbb{Z}$-linearly to $\mathbb{Z}[G]$.
A G-module is now the same as a (left) $\mathbb{Z}[G]$-module.

A trivial G-module is an abelian group A on which G acts trivially, meaning that $ga = a$ for all $g \in G$ and for all $a \in A$. By convention we will always take $\mathbb{Z}$ to be a trivial G-module unless specified.

Definition 3.6. The augmentation map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is defined to be the map taking $\sum n_g g$ to $\sum n_g$, $n_g \in \mathbb{Z}$. The kernel of this map is called the augmentation ideal, which we denote by $\mathcal{I}$. Since $\mathbb{Z}[G]$ has basis $\{1\} \cup \{g - 1 | g \neq 1\}$ as a free $\mathbb{Z}$-module, it follows that $\mathcal{I}$ has basis $\{g - 1 | g \neq 1\}$.

We now introduce two canonical resolutions of the trivial G-module $\mathbb{Z}$ that are of great theoretical importance.

Definition 3.7. Let B^u_n be the free $\mathbb{Z}[G]$-module on the set of all symbols $[g_1 \otimes \cdots \otimes g_n]$ with $g_i \in G$. We let B^u_0 be the free $\mathbb{Z}[G]$-module on a single generator, which we shall denote by $[\cdot]$. Define maps $d : B^u_n \to B^u_{n-1}$ by

$$\begin{aligned} d([g_1 \otimes \cdots \otimes g_n]) =& g_1 . [g_2 \otimes \cdots \otimes g_n] \\ &+ \sum_{i=1}^{n-1} (-1)^i [g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \cdots \otimes g_n] \\ &+ (-1)^n [g_1 \otimes \cdots \otimes g_{n-1}] \end{aligned}$$

Theorem 3.8. *Given $\{B^u_n\}_{n\in\mathbb{N}}$ and maps d as defined above, the chain complex*

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} B^u_0 \xleftarrow{d_1} B^u_1 \xleftarrow{d_2} \cdots$$

is a projective resolution of the trivial G-module $\mathbb{Z}$, where ϵ is the map taking $[.]$ to 1. We call this resolution the unnormalized bar resolution.

Proof. The first thing we need to prove is that this is indeed a chain complex. Define maps

$$\begin{aligned} d_0([g_1 \otimes \cdots \otimes g_n]) &= g_1 . [g_2 \otimes \cdots g_n] \\ d_i([g_1 \otimes \cdots \otimes g_n]) &= [g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \cdots \otimes g_n], 1 \leq i \leq n-1 \\ d_n([g_1 \otimes \cdots \otimes g_n]) &= [g_1 \otimes \cdots g_{n-1}]. \end{aligned}$$

Then $d : B_n^u \to B_{n-1}^u$ can be written as $\sum_{i=0}^{n}(-1)^i d_i$. A direct computation shows that for $i \leq j-1$, $d_i d_j = d_{j-1} d_i$. When computing $d \circ d$, the terms $d_i d_j$ and $d_{j-1} d_i$ appear with opposite signs, hence everything cancels out pairwise, giving us that $d \circ d$ is indeed 0.

We shall now give the splitting maps $s : B_n^u \to B_{n+1}^u$ and check that the identity map on B_n^u is null-homotopic, and hence that the chain complex is (split) exact. Let $s_{-1} : \mathbb{Z} \to B_0^u$ and $s_n : B_n^u \to B_{n+1}^u$, $n \geq 0$ be maps defined respectively by

$$s_{-1}(1) = [.]$$
$$s_n(g[g_1 \otimes \cdots \otimes g_n]) = [g \otimes g_1 \otimes \cdots \otimes g_n].$$

Clearly we have that $\epsilon s_{-1} = 1$ and $ds_0 + s_{-1}d$ is the identity on B_0^u. For $n \geq 1$, we see that

$$\begin{aligned} ds_n(g[g_1 \otimes \cdots \otimes g_n]) =& d([g \otimes g_1 \otimes \cdots \otimes g_n]) \\ =& g[g_1 \otimes \cdots \otimes g_n] - [gg_1 \otimes \cdots \otimes g_n] \\ &+ \sum_{i=1}^{n-1} (-1)^{i-1} [g \otimes g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \cdots \otimes g_n] \\ &+ (-1)^{n+1} [g \otimes g_1 \otimes \cdots \otimes g_{n-1}]. \end{aligned}$$

On the other hand, we also have that

$$\begin{aligned} s_{n-1}d(g[g_1 \otimes \cdots \otimes g_n]) =& s_{n-1}(gg_1[g_2 \otimes \cdots \otimes g_n]) \\ &+ \sum_{i=1}^{n-1} (-1)^i g[g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \cdots \otimes g_n] \\ &+ (-1)^n g[g_1 \otimes \cdots \otimes g_{n-1}] \\ =& [gg_1 \otimes \cdots \otimes g_n] \\ &+ \sum_{i=1}^{n-1} (-1)^i [g \otimes g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes g_{i+2} \otimes \cdots \otimes g_n] \\ &+ (-1)^n [g \otimes g_1 \otimes \cdots \otimes g_{n-1}]. \end{aligned}$$

Thus we see that $ds_n + s_{n-1}d$ is the identity on B_n^u, hence that the complex is split exact. Since each B_n^u is free, it follows immediately that it is a projective resolution. □

There exists a normalized version of the bar resolution. We define B_n to be the free $\mathbb{Z}[G]$ module on the set of symbols $[g_1|\cdots|g_n]$, $1 \neq g \in G$. By convention, we set $[g_1|\cdots|g_n]$ to be equal to 0 if $g_i = 1$ for some i. For $n = 0$, we let $B_0 = \mathbb{Z}[G]$. The differential maps are defined in the same way as for the unnormalized version. It is sometimes advantageous to identify B_n as the quotient module of B_n^u by S_n, which is the submodule generated by elements of the form $[g_1 \otimes \cdots \otimes g_n]$ where $g_i = 1$ for some i.

Theorem 3.9. *The chain complex*

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} B_0 \xleftarrow{d_1} B_1 \xleftarrow{d_2} \cdots$$

is a projective resolution of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$.

Proof. The proof of this theorem is virtually identical to the previous one, and thus will be omitted. □

Application 3.10. (Group Cohomology)
Let A be a left G-module. The n-th cohomology group $H^n(G;A)$ is defined for all $n \geq 0$ to be the cohomology of $\mathrm{Hom}_G(B_n^u, A)$, i.e the group $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Elements in $\mathrm{Hom}_G(B_n^u, A)$ are called n-cochains, and are simply set maps $G^n \to A$. If ϕ is a n-cochain, the differential $d\phi$ is an $(n+1)$-cochain defined by

$$\begin{aligned} d\phi(g_0, \cdots, g_n) =& g_0\phi(g_1, \cdots, g_n) \\ &+ \sum_{i=1}^{n-1} (-1)^i \phi(\cdots, g_i g_{i+1}, \cdots) \\ &+ \phi(g_0, \cdots, g_{n-1}). \end{aligned}$$

If $d\phi = 0$, we say that ϕ is a n-cocycle. Elements $d\phi$ in $\mathrm{Hom}_G(B_n^u, A)$ are called n-coboundaries. The group of n-cocycles and of n-coboundaries are denoted by $Z^n(G;A)$ and $B^n(G;A)$ respectively. We thus recover the familiar formula $H^n(G;A) = Z^n(G;A)/B^n(G;A)$. One can also take the cohomology of $\mathrm{Hom}_G(B_*, A)$ instead and consider normalized cochains, meaning that $\phi(g_1, \cdots) = 0$ if any of the $g_i = 1$. For the rest of this paper we shall in fact take this latter approach, since it will make computations slightly easier.

Recall from the previous section that given an extension $1 \to A \to E \xrightarrow{\pi} G \to 1$, a section σ of π is a set-theoretic map $G \to E$ such that $\pi\sigma(g) = g$ for all $g \in G$. We shall restrict our choice of maps to based sections only, meaning sections such that $\sigma(1_G) = 1_E$. This choice is equivalent to taking the normalized bar resolution in our computation of $H^n(G;A)$, and while the following proposition can be proved using the unnormalized resolution, doing it this way simplifies the issue of the unit for the group operation in E.
Now for any $g, h \in G$, $\sigma(gh)$ and $\sigma(g)\sigma(h)$ both map to gh under π, hence their difference lies in A by exactness. We thus define

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

This defines a function $[\,] : G \times G \to A$ depending on E and σ called the factor set determined by E and σ.

Proposition 3.11. *Let A be a G-module. A map of sets $[\,] : G \times G \to A$ is a factor set if and only if it is a normalized 2-cocycle.*

Proof. A normalized 2-cycle is an element of $Z^2(G;A)$, meaning it is a set map $[\,] : G \times G \to A$ satisfying that for all $f, g, h \in G$

- [g,1] = [1,g] = 0
- f[g,h] - [fg,h] + [f,gh] - [f,g] = 0

Now suppose we have a factor set $[\,]$. This determines the group operation in E, which is given by

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

where $g \cdot b$ denotes the G-module action of g on b given by conjugation in E. Now we have that

$$\begin{aligned} (0,f) \cdot ((0,g) \cdot (0,h)) &= (f[g,h] + [f,gh], fgh) \\ ((0,f) \cdot (0,g)) \cdot (0,h) &= ([f,g] + [fg,h], fgh) \end{aligned}$$

By associativity of E, we recover exactly the second condition in the definition of a normalized 2-cocycle. The first condition is obvious since $\sigma(1) = 1$.

Now conversely, suppose we have a normalized 2-cocycle $[\,]$. Let E be the set $A\times G$, and define an operation on E exactly as the one in the first part of the proof. One easily checks $(0,1)$ is the identity for this product. Associativity holds because of the second condition of a normalized 2-cycle. Given $(a,g)\in E$, we have that

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

Thus E is a group. The subgroup $A\times 1$ is isomorphic to A and $E/A\times 1$ is G. We thus have that $1\to A\to E\to G\to 1$ is an extension, and the section $G\cong 0\times G\hookrightarrow E$ gives us a factor set $[\,]$ which is identical to our original 2-cocycle. □

Lemma 3.12. *Let E be an extension of G by A with based section σ, and let $[\,]$ be the factor set determined by σ. If E' is an equivalent extension, then there exists a based section σ' of E' such that the factor set determined by σ' is $[\,]$.*

Proof. Since E and E' are equivalent, there exists an isomorphism β between them. If σ is a based section of E, then clearly $\sigma'=\beta\circ\sigma$ is a based section of E'. By definition, $[g,h]=\sigma(g)\sigma(h)\sigma(gh)^{-1}$, so we have

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

However, β restricts to the identity on A, thus $\beta([g,h])=[g,h]$, thereby giving us the desired result. □

Lemma 3.13. *Given an extension $0\to A\to E\xrightarrow{\pi}G\to 0$, two different factor sets $[\,]$ and $[\,]'$, corresponding to choices σ and σ' of based sections respectively, differ by a 2-coboundary.*

Proof. Given two based section maps σ and σ', $\sigma'(g)$ lies in the same coset of A as $\sigma(g)$. That means that there exists an element $\alpha(g)\in A$ such that $\sigma'(g)=\alpha(g)\sigma(g)$. The corresponding factor set is

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

As we see, the difference $[g,h]'-[g,h]$ is precisely the coboundary $d\alpha(g,h)=\alpha(g)-\alpha(gh)+g\cdot\alpha(h)$. □

The above three lemmas show that there is a well-defined map Φ from the set of equivalence classes of extensions to $H^2(G;A)$.

Lemma 3.14. *Two extensions of G by A with section maps $\sigma_i:G\to E_i$ giving rise to the same factor set are equivalent.*

Proof. As sets, we already have that $E_1\cong E_2\cong A\times G$. Writing out the group operation of an extension E with factor set $[\,]$ under the bijection with $A\times G$, we see that the products $(a,1)\cdot(b,1)=(a+b,1)$, $(a,1)\cdot(0,g)=(a,g)$ and $(0,g)\cdot(a,1)=(ga,a)$ are fixed. The group structure is thus entirely determined by the product $(1,g)\cdot(1,h)=([g,h],gh)$. Thus if σ_1,σ_2 determine the same factor set, the bijections of E_1 and E_2 with $A\times G$ give a group isomorphism $E_1\cong E_2$ and thus an equivalence of extensions. □

In particular, if $[\,] = 0$, it means that the set map σ is a group homomorphism. In other words the extension is split, thus E is the familiar semi-direct product $A \rtimes G$ from group theory.

Lemma 3.15. *The map Φ is injective.*

Proof. Suppose $[\ \ ]$ and $[\ \ ]'$ are two factor sets corresponding to based sections $\sigma : G \to E$ and $\sigma' : G \to E'$ respectively, that represent the same cohomology class in $H^2(G; A)$. That means that $[g, h] - [g, h]' = \alpha(g) - \alpha(gh) + g\alpha(h)$, where α is a 2-coboundary. Let $\mu(g) = \alpha(g)^{-1}\sigma(g)$. Since $\alpha(g)$ lies in A, μ is also a based section of E'. Its corresponding factor set is

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

Thus $[g, h] - [g, h]'' = 0$, so by Lemma 3.14, E and E' lie in the same equivalence class. □

Theorem 3.16. *Equivalence classes of extensions are in 1-1 correspondence with the cohomology group $H^2(G; A)$.*

Proof. We've already shown that the map Φ was well-defined, and the previous lemma shows it is injective. By Lemma 3.11, every normalized 2-cocycle gives rise to a extension of G by A, thus Φ is also a surjection, thereby establishing the bijection. □

Acknowledgments. I would like to thank my mentors, Rolf Hoyer and Michael Smith, for the support and patience they showed during the writing of this paper.

References

[1] Weibel, C., *An introduction to homological algebra*, Cambridge University Press, 1994.

[2] Dummit, D. & Foote, R., *Abstract algebra*, John Wiley and Sons, Third Edition, 2004.

[3] May, J.P., *Notes on Tor and Ext*, http://www.math.uchicago.edu/m̃ay/MISC/TorExt.pdf