GROUP COHOMOLOGY
MATH 250B

ADAM TOPAZ

Throughout this note G will denote a group (you can assume it's finite, if you want).

1. The Group Ring

We recall the definition of the group ring denoted by $\mathbb{Z}[G]$. As a set, we define

$$\mathbb{Z}[G] = \mathbb{Z}^{(G)} = \bigoplus_{g \in G} \mathbb{Z} \cdot [g]$$

i.e. elements of this ring are formal linear combinations of elements of G with coefficients in $\mathbb{Z}$. Multiplication is defined by the condition that $[g] \cdot [h] = [gh]$.

The group ring can be described via adjoint functors:

Proposition 1.1. *The assignment $G \mapsto \mathbb{Z}G$ is a functor from the category of groups to the category of rings. This functor is left adjoint to the forgetful functor from rings to the category of monoids with unity. In other words, if R is any ring and $f : G \to R$ is a function such that $f(gh) = f(g)f(h)$ and $f(1) = 1$, then f extends to a unique morphism of rings $\mathbb{Z}G \to R$, such that the composition*

$$G \xrightarrow{g \mapsto [g]} \mathbb{Z}G \to R$$

is f.

Proof. Exercise. □

A G-module is an abelian group A with an action of G. In fact, the following concepts all yield the same definition of a G-module:

1. An abelian group A with a group homomorphism $G \to \mathrm{Aut}(A)$.
2. An abelian group A with a ring homomorphism $\mathbb{Z}G \to \mathrm{End}(A)$.
3. A left $\mathbb{Z}G$-module A.

The equivalence of (1) and (2) comes from the fact that $G \subset (\mathbb{Z}G)^\times$ and $\mathrm{Aut}(A) = \mathrm{End}(A)^\times$. We will usually write the action of $g \in G$ on elements $a \in A$ as $g.a$ or just ga if no confusion is possible.

A morphism of G-modules is a map of abelian group $A \to B$ which is compatible with the action of G. We let *Gmod* denote the category of G-modules, equivalently, the category of $\mathbb{Z}G$-modules.

2. Definition of Group Cohomology

Let G be a group and let A be a G-module. We define A^G to be the submodule of invariants. I.e.

$$A^G = \{a \in A \ : \ g.a = a, \ \forall g \in G\}.$$

It is clear that A^G is a submodule of A, and that the assignment $A \mapsto A^G$ is a covariant functor from *Gmod* to *Gmod* (or just to *Ab*). We say that A is a trivial G-module if $A = A^G$, i.e. if the action of G on A is trivial.

Lemma 2.1. *The functor* $(\bullet)^G$ *is left exact.*

Proof. Easy. $\square$

It turns out that the functor $(\bullet)^G$ is *not* right exact in most situations. Here is an example that comes up in Galois theory. Let's consider the group $G = \mathbb{Z}/2$, and consider the Galois extension of $\mathbb{Q}$ defined by $\mathbb{Q}(\sqrt{2}) = K$. Then there is a natural action of G on K since $G = \mathrm{Gal}(K|\mathbb{Q})$. Now consider the map $K^\times \to K^\times$ defined by $x \mapsto x^2$, and note that 2 is contained in the image of this morphism. Let me call the image $A \subset K^\times$, so that we have a surjective map

$$K^\times \to A \to 0.$$

But now we take invariants, and note that the invariant submodule of $K^\times$ is precisely $\mathbb{Q}^\times$, while the invariant module of A contains 2. The map $(K^\times)^G \to A^G$ is the same as the map from before, i.e. it's just squaring, but 2 is not a square of any rational number, hence the map $(K^\times)^G \to A^G$ is not surjective, even though $K^\times \to A$ was surjective.

We are now prepared to define group chomology. For a group G, we define

$$\mathrm{H}^*(G, \bullet) = R^*(\bullet)^G$$

i.e. $\mathrm{H}^*(G, \bullet)$ is the $*$-th right derived functor of $(\bullet)^G$.

3. Changing the Group

We already know that $\mathrm{H}^*(G, \bullet)$ is a functor, so a morphism $A \to B$ of G-modules induces a morphism on $H^*(G, A) \to H^*(G, B)$. What about changing the group? Suppose that $f : H \to G$ is a group homomorphism, and that A is a G-module. Then we can consider A also as an H-module via the action $h.a := f(h).a$, for $h \in H$ and $a \in A$. We note that $A^G \subset A^H$, just by definition. Thus, we obtain a morphism of functors $(\bullet)^G \to (\bullet)^H$. Namely, we obtain a morphism on right-derived functors

$$\mathrm{H}^*(G, \bullet) \to \mathrm{H}^*(H, \bullet).$$

4. Computation of Cohomology Using Free Resolutions

In this section we show how one can compute the cohomology groups $\mathrm{H}^*(G, A)$ in a much more explicit way, by using a "standard" projective (actually a free) resolution. First of all, we prove the following key lemma:

Lemma 4.1. *One has an isomorphism* $\mathrm{H}^*(G, A) \cong \mathrm{Ext}^*_{\mathbb{Z}G}(\mathbb{Z}, A)$*, functorial in* A.

Proof. This follows from the fact that $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) = A^G$, functorially in A, and from the definition of Ext. $\square$

As an immediate corollary of this lemma, we see that to any short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, we obtain a long exact sequence on cohomology.

The idea which we use to compute cohomology $\mathrm{H}^*(G, A)$ is to find a "nice" projective resolution P_* of $\mathbb{Z}$ in the category of $\mathbb{Z}G$-modules. Then we compute the ext groups using this projective resolution.

5. The Standard Resolution of $\mathbb{Z}$ as a G-module

The idea is to find a standard projective (in fact, free) resolution of $\mathbb{Z}$ as an object of $\mathbb{Z}G$. We construct this resolutoin just like we do any other, by constructing each term in the resolution as a projective/free presentation of the kernel of the previous term.

The standard free resolution of $\mathbb{Z}$ is the free resolution P_* where

$$P_i := \mathbb{Z}[G^{i+1}]$$

and the G-action on P_i is defined by $g(g_0, \dots, g_i) = (gg_0, \dots, gg_i)$. We define the differential

$$d : P_n \to P_{n-1}$$

is defined by the condition

$$d(g_0, \dots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_n).$$

Proposition 5.1. *The sequence*

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_0 \to \mathbb{Z} \to 0$$

is exact, where the map $P_0 \to \mathbb{Z}$ is the augmentation map.

We just describe what happens in low degrees. Namely, the augmentation map $P_0 \to \mathbb{Z}$ is the map $P_0 = \mathbb{Z}G \to \mathbb{Z}$ defined by $g \mapsto 1 \in \mathbb{Z}$. Thus, the element $\sum_g a_g \cdot g$ of $\mathbb{Z}G$ gets mapped to $\sum_g a_g$. The kernel of the augmentation map is called the augmentation ideal I.

Fact 5.2. *I is the ideal generated by elements of the form $1 - g$ for $g \in G$.*

The map $\mathbb{Z}[G^2] \to \mathbb{Z}[G]$ is the map which sends (g_0, g_1) to $g_0 - g_1$ and this is easily seen to be an element of the augmentation ideal. On the other hand, the element $(1, g)$ gets mapped to $1 - g$, in the augmentation ideal, and thus the map $\mathbb{Z}[G^2] \to \mathbb{Z}[G]$ is surjective onto the augmentation ideal.

Fact 5.3. *P_n is a free $\mathbb{Z}G$-module for all i.*

Proof. A basis for this module is given by $(1, g_1, g_1g_2 \dots, g_1 \cdots g_n)$ for $g_1, \dots, g_i \in G$. Details are left as an exercise. □

To compute cohomology with this resolution, we apply the functor $\mathrm{Hom}(\bullet, A)$ to the complex P_* to obtain

$$C_h^*(G, A) := \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A).$$

Then $C_h^*(G, A)$ is called the **complex of homogeneous cocycles of G with values in A.**

Fact 5.4. *One can identify $C_h^n(G, A)$ with the module of functions $f : G^{n+1} \to A$ such that*

$$g(gg_0, \dots, gg_n) = g \cdot f(g_0, \dots, g_n).$$

Under this identification, the differential $f : C_h^{n-1} \to C_h^n$ is defined by

$$(df)(g_0, \dots, g_n) = \sum_{i=0}^{n} (-1)^i f(g_0, \dots, \hat{g}_i, \dots, g_n).$$

We can therefore calculate group cohomology $H^*(G, A)$ as follows. Define $Z_h^*(G, A) = \ker(d : C_h^*(G, A) \to C_h^{*+1}(G, A))$ and $B_h^*(G, A) = \mathrm{im}(d : C^{*-1} \to C^*)$. Then $H^*(G, A) = Z_h^*/B_h^*$.

6. Functoriality

The assignment $A \mapsto C_h^*(G, A)$ is functorial in A. Namely, if $f : A \to B$ is a morphism of G-modules, then one gets a corresponding morhpism of complexes

$$C_h^*(G, A) \to C_h^*(G, B)$$

which is defined on the level of homogeneous cocycles by $\sigma \mapsto f \circ \sigma$. One obtains a corresponding map on cohomology $H^*(G, A) \to H^*(G, B)$ defined by $\sigma \mapsto f \circ \sigma$.

7. Inhomogeneous cochains

In this section we develop a different way to compute group cohomology using so-called inhomogeneous cochains. Recall that a homogeneous cochain $f : G^{n+1} \to A$ is a function such that

$$f(gg_0, \ldots, gg_n) = gf(g_0, \ldots, g_n).$$

Exercise 7.1. A homogeneous cochain f is completely determined by the restriction of f to elements of the form

$$(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n).$$

Let $C^n(G, A)$ denote the group of functions $G^n \to A$. Now consider the map $C_h^n(G, A) \to C^n(G, A)$ defined by

$$f \mapsto (g_1, \ldots, g_n) \mapsto f(1, g_1, g_1g_2, \ldots, g_1 \cdots g_n).$$

Then this map is an isomorphism of G-modules.

The elements of $C^*(G, A)$ are called inhomogeneous cochains, or just cochains. The goal of this section is to be able to compute the cohomology groups $H^*(G, A)$ using inhomogeneous cochains as opposed to homogeneous cochains. In order to do this, we must define a differential $d : C^*(G, A) \to C^{*+1}(G, A)$ which corresponds to the differential of homogeneous cochains defined in the previous section.

For an n-cochain $f : G^n \to A$, we define the **Hochschild differential** df as follows:

$$df(g_1, \ldots, g_{n+1}) = g_1f(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^{i-1} f(g_1, \ldots, g_ig_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n).$$

Exercise 7.2. The isomorphism of the previous exercise induces an isomorphism of complexes

$$(C_h^*(G, A), d) \cong (C^*(G, A), d).$$

8. Examples in Low Degrees

Let's take a look at the differential of some low-degree terms in the inhomogeneous cochain complex.

(1) First, one has $C^0(G, A) = A$. For an element $a \in A = C^0(G, A)$, one has $(da)(g) = ga - a$.
(2) For a 1-cochain $f : G \to A$, the differential is given by

$$(df)(g, h) = gf(h) - f(gh) + f(g).$$

In particular, a 1-cochain is precisely a so-called **crossed homomorphism** i.e. a function $f : G \to A$ such that

$$f(gh) = f(g) + gf(h).$$

(3) Thus, if A is a *trivial G-module*, i.e. the action of G on A is trivial, then we have:

$$\mathbb{Z}^1(G, A) = \mathrm{Hom}(G, A), \quad B^1(G, A) = 0$$

so that $H^1(G, A) = \mathrm{Hom}(G, A)$ canonically.

(4) For a 2-cochain $f : G^2 \to A$, the differential df is defined as

$$(df)(x, y, z) = xf(y, z) - f(xy, z) + f(x, yz) - f(x, y).$$

This will come up in the next section when we discuss the connection between H^2 and group extensions.

9. Group Extensions

Let G, H be two groups. An **extension of G by H** is a short exact sequence of *groups* of the form

$$1 \to H \to M \to G \to 1.$$

I.e. it is group E which has H as a normal subgroup such that the quotient E/H is isomorphic to G. Two extensions E, E' of G by H are considered equivalent if there is a map between the groups in the middle making the obvious diagram commute.

Suppose now that E is an extension of G by H. Then we get an **outer-representation** of G on H, i.e. a homomorphism of groups:

$$\rho_E : G \to \mathrm{Out}(H)$$

where $\mathrm{Out}(H)$ is the group of *outer* morphisms. This map is defined as follows.

For $g \in G$, choose a lift $\tilde{g}$ of g in E. We next consider the automorphism of H induced by $\tilde{g}$, i.e. this is the automorphism of H given by

$$\phi_{\tilde{g}} : h \mapsto \tilde{g}h\tilde{g}^{-1}.$$

But the point is that the automorphism $\phi_{\tilde{g}}$ depends on the choice of $\tilde{g}$, and not just on g. However, if we replace $\tilde{g}$ by another lift of g, then this other lift will be of the form $\tilde{g} \cdot x$ for some $x \in H$. Therefore, the corresponding automorphism will be

$$\phi_{\tilde{g}x}(x) = \tilde{g}xhx^{-1}\tilde{g}^{-1}$$

which is in the same class as $\phi_{\tilde{g}}$ in $\mathrm{Out}(H)$, since it differs from $\phi_{\tilde{g}}$ by an inner automorphism of H.

Also, if $x, y \in G$ and $\tilde{x}$ resp. $\tilde{y}$ are lifts, then one has

$$\phi_{\tilde{x}\tilde{y}} = \phi_{\tilde{x}} \circ \phi_{\tilde{y}}.$$

Thus we see that the map

$$g \mapsto \phi_{\tilde{g}}$$

induces a well-defined homomorphism $G \to \mathrm{Out}(H)$.

Exercise 9.1. Let E, E' be two extensions of G by A. Prove that if E and E' are equivalent, then $\rho_E = \rho_{E'}$.

What we usually do in group theory, when we try to classify extensions of G by H, we first fix an outer representation $\rho : G \to \mathrm{Out}(H)$, then try to classify all group extensions of G by H which induce a given outer representation. In terms of group cohomology, this is what we will do in the case where H is abelian.

Namely, we note that when H is abelian, one has $\mathrm{Aut}(H) = \mathrm{Out}(H)$, so that an outer representation of H by G is nothing but a group action of G on H, so that H becomes a G-module in a canonical way.

In particular, if the kernel H of the extension $E \to G$ is *abelian*, then we get a *caonical* action of G on H. Henceforth, we will only consider extensions whose kernel is abelian. Also, if A is a G-module, then saying that E is an extension of G by A will implicitly mean that the G-action induced by E on A is the same as the given action.

10. Split Extensions

In this section we consider the situation of a split extension. First of all, recall that the *semi-diorect product* of G by A is the group

$$A \rtimes G = \{(a, g) \ : \ a \in A, \ g \in G\}$$

where the product is defined by

$$(a, g) \cdot (a', g') = (a + g.a', gg').$$

Recall that an extension

$$1 \to A \to E \to G \to 1$$

is split if the map $E \to G$ has a section *which is a group homomorphism.* (later on we will use a set-theoretic section, i.e. a section which doesnt' respoect the group structure, so this is an important distinction).

Proposition 10.1. *Let A be a G-module. Let E be an extension of G by A. The following are equivalent:*

(1) E is split.
(2) There exists a subgroup G' of E which maps isomorphically onto G, and such that $E = A \cdot G'$ and $A \cap G' = 1$.
(3) E has a subgroup G' such that every element of E is uniquely expressible in the form $a \cdot g'$ for some $a \in A$ and $g' \in G'$.
(4) E is equivalent (as an extension of G by A) to the semi-direct product $A \rtimes G$.

Proof. Clearly 1-3 are equivalent. We must show that these imply that E is equivalent to the semidirect product. Let $s : G \to E$ be the group-theoretic section. Then every element of E can be uniquely represeted as $a \cdot s(g)$ for some $a \in A$ and $g \in G$. We just have to calculate the product structure on E, and see that it looks like the semi-direct product. It is easy to calculate that (WHY?):

$$(a \cdot s(g)) \cdot (a' \cdot s(g')) = (a + g.a') \cdot (s(gg')).$$

Thus E is equivalent to the semi-direct product. $\square$

11. Classifying Group Extensions

Let A be a G-module. Let $E(G, A)$ denote the equivalence classes of extensions of G by A which induce the given action of G on A. Our goal will be to prove the following theorem:

Theorem 11.1. *There is a canonical bijection $E(G, A) \cong \mathrm{H}^2(G, A)$.*

The idea is motivated by the proposition concerning split extensinos. Namely, $E(G, A)$ is a *pointed set* whose distinguished point is the equivalence class represented by the semi-direct product. The idea is therefore to measure "how far" a given extension is from being split, and this should be captured by a cocycle.

Extensions yields Cohomology Classes. First we construct a map $E(G, A) \to \mathrm{H}^2(G, A)$. Let E be an extension of G by A, and let $s : G \to E$ be a *set-theoretical* section (this always exists by the axiom of choice...). We want to "measure" how far this section is from being a homomorphism. Indeed, if it is a homomorphism, then the extension would be split. This is completely captured as follows. For $\sigma, \tau \in G$, we see that $s(\sigma)s(\tau)$ and $s(\sigma\tau)$ map to the same element of G. Thus, there exists some element $x(\sigma, \tau) \in A$ such that

$$s(\sigma)s(\tau) = x(\sigma, \tau)s(\sigma\tau).$$

Note that two equivalent extneions endowed with *compatible* section will yield the same function x.

Note that $x(\sigma, \tau)$ satisfies $x(1, \sigma) = x(\sigma, 1) = 0$ for all σ. We claim that x is a 2-cocycle (inhomogeneous). The cocycle condition essentially follows from the associativity in the group E:

$$(s(i)s(j))s(k) = x(i, j)s(ij)s(k) = x(i, j)x(ij, k)s(ijk)$$

while

$$s(i)(s(j)s(k)) = s(i)x(j, k)s(jk) = (i.x(j, k))s(i)s(jk) = (i.x(j, k))x(s, jk)s(ijk).$$

Thus

$$x(i, j)x(ij, k) = (i.x(j, k))x(s, jk)$$

and this is exactly the condition for x to be a 2-cocycle. Thus we obtain a cohomology class $[x] \in \mathrm{H}^2(G, A)$.

At this point, we dont know whether this class depends on the choice of section s. Supose that s' is another section, and that it induces another 2-cocycle x'. But then there exists a function $y : G \to A$ such that

$$s'(\sigma) = y(\sigma) \cdot s(\sigma)$$

for all $\sigma \in G$. I will leave it as an exercise to check that $x' = x + dy$, where d is the Hochschild differential. In particular, we obtain a well-defined map $E(G, A) \to \mathrm{H}^2(G, A)$. □

Cohomology Classes Yields Extensions. We take a hint from the previous construction. Namely, if x is the 2-cocycle which is *defined* by the extension E as in the previous construction, then we can try to reconstruct E using the cocycle x as follows. First, consider the set $E_x := A \times G$ (as a set). We define a binary operation on E_x as follows:

$$(a, i) \cdot (b, j) = (a + i.b + x(i, j), ij).$$

This product structure comes about as follows. First of all, note that there is a bijection $A \times G = E$ defined by $(a, g) \mapsto a \cdot s(g)$. Now if we calculate the product

$$as(g)bs(h) = a(g.b)s(g)s(h) = (a(g.b))x(g,h)s(gh)$$

Therefore, the binary operation on E_x corresponds precisely to the product structure on E, via the bijection $A \times G = E$. In particular, E_x is an extension of G by A which is equivalent to E.

So we want to figure out a method for constructing an extension given just a cocycle x. And we will define the structure in the naive way: $E_x = A \times G$ with the product structure:

$$(a, g)(b, h) = (a + gh + x(g, h), gh).$$

When you try to prove that this is actually a group, you will run into a problem, which comes from the fact that $x(1, g)$ or $x(g, 1)$ might be non-zero for some g. But, you will see that if x is *normalized* i.e. that $x(1, g) = x(g, 1) = 0$ for all g, then the construction actually yields an extension of G by A. The associativity is essentially equivalent to the cocycle condition.

I claim that every cohomology class $c \in \mathrm{H}^2(G, A)$ has a representative cocycle x which is normalized. Indeed, if x is any cocycle representing c, then one has

$$x(ij, k) + x(i, j) = x(i, jk) + i.x(j, k).$$

This implies that

$$x(i, 1) = i.x(1, 1), \quad x(1, k) = x(1, 1).$$

We put $y(i) = x(1, 1)$ (constant), and consider the cocycle which is equivalent to x:

$$x' = x + dy$$

It isn't hard to check that x' is normalized, i.e. that $x'(1, i) = x'(i, 1) = 0$ for all i (exercise).

So any cohomology class c is represented by a normalized cocycle x. For such a normalized cocycle x, we then define $E_x = A \times G$ as sets with the product structure:

$$(a, i)(b, j) = (a + ib, ij).$$

The associativity condition is essentially equivalent to the condition that x is a cocycle (i.e. that $dx = 0$). The element $(0, 1)$ is the identity (this comes from the normalized condition!). The rest of the verification that E_x is a group is left as an exercise (some might be on the 4th homework). The map $a \mapsto (a, 1)$ and $(a, g) \mapsto G$ are group homomorphisms which show that E_x is an extension of G by A.

This extension E_x doesn't depend on the choice of normalized cocyucle x representing c. Indeed, if y is a 1-cochain such that $x = x' + dy$ then the map

$$E_x \to E_{x'}$$

defined by $(a, g) \mapsto (y(g) + a, g)$ will witness the equivalence between E_x and $E_{x'}$. In particular, we obtain a canonical map $H^2(G, A) \to E(G, A)$. From the construction, it is clear that $E(G, A) \to H^2(G, A)$ and $H^2(G, A) \to E(G, A)$ are mutually inverse to eachother. □

12. Some Examples of Group Extensions and their Corresponding Cocycles

We will look at two important examples.

12.1. **The Bockstein Morphism.** Let p be a prime and G a group. Consider $\mathbb{Z}/p$ as a trivial G-module. Then the **Bockstein morphism** is a morphism

$$\mathrm{H}^*(G,\mathbb{Z}/p) \to \mathrm{H}^{*+1}(G,\mathbb{Z}/p)$$

which is the connecting morphism associated to the short exact sequence

$$1 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 1.$$

Now let's consider the situation where $G = \mathbb{Z}/p$. Then one has

$$\beta : H^1(\mathbb{Z}/p,\mathbb{Z}/p) \to \mathrm{H}^2(\mathbb{Z}/p,\mathbb{Z}/p).$$

But recall that $\mathrm{H}^1(\mathbb{Z}/p,\mathbb{Z}/p) = \mathrm{Hom}(\mathbb{Z}/p,\mathbb{Z}/p)$ so it has a distinguished element $\mathbf{1}$ which is non-trivial.

Proposition 12.1. *The extension correpsonding to* $\beta(\mathbf{1})$ *is precisely*

$$1 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 1.$$

To see this, we need to calculate the cocycle associated to this extension, and the cocycle associated to the Bockstein, and prove that they are cohomologous (i.e. differ by a coboundary). This is left as an exercise.

We will see in the next section that $\mathrm{H}^2(\mathbb{Z}/p,\mathbb{Z}/p)$ is *generated* by this extension.

We can also generalize this a little bit. Indeed, let $f : G \to \mathbb{Z}/p$ be a homomorphism, which we consider as an element of $\mathrm{H}^1(G,\mathbb{Z}/p)$. Consider the pullback:

$$G \times_{\mathbb{Z}/p} \mathbb{Z}/p^2.$$

This is an extension of G by $\mathbb{Z}/p$, and this extension precisely correspnds to $\beta(f) \in \mathrm{H}^2(G,\mathbb{Z}/p)$.

12.2. **Heisenberg.** Now consider $G = \mathbb{Z}/p \times \mathbb{Z}/p$. Then the map $G \times G \to \mathbb{Z}/p$ defined by $(i,j),(i',j') \mapsto ij'$ is a 2-cocycle (why?). The extension represented by this cocycle is the **Heisenberg Group** with cofficients in $\mathbb{Z}/p$. To see this, we can calculate the cocycle assocaited to the Heinseberg group... etc...

12.3. **Pullbacks.** Let $f : G' \to G$ be a morphism of groups, and let E be an extension of G by A. Then the pull-back of E is defined as the fibered product:

$$f^*E := G' \times_G E = \{(g',e) \in G' \times E \ : \ \mathrm{im}(g') = \mathrm{im}(e) \in G\}.$$

Exercise 12.2. If $\alpha \in \mathrm{H}^2(G,A)$ corresponds to E, then $f^*\alpha \in \mathrm{H}^2(G',A)$ corresponds to f^*E.

12.4. **Pushouts.** Let E be an extension of G by A, and let $f : A \to B$ be a morphism of G-modules. Then the pushout of E is defined as the fibered coproduct:

$$f_*E := B \coprod_A E := \frac{B \rtimes E}{\langle (-f(a),a) \ : \ a \in A\rangle}.$$

Exercise 12.3. If $\alpha \in \mathrm{H}^2(G,A)$ corresponds to E, then $f_*\alpha \in \mathrm{H}^2(G,B)$ corresponds to f_*E.

12.5. **The Baer Sum.** Let E_1, E_2 be two extensions of G by A. Then $E_1 \times E_2$ is an extension of $G \times G$ by $A \times A$. Let $s : A \times A \to A$ be the summation map (this is a G-morphism), and let $\Delta : G \to G \times G$ be the diagonal map (this is a homomorphism of groups). The **Baer Sum** of E_1 and E_2, denoted by $E_1 \oplus_B E_2$, is defined as:

$$E_1 \oplus_B E_2 := s_* \Delta^*(E_1 \times E_2).$$

Exercise 12.4. Let $\alpha_1, \alpha_2 \in \mathrm{H}^2(G, A)$ corresponds to E_1 resp. E_2. Then $\alpha_1 + \alpha_2$ corresponds to $E_1 \oplus_B E_2$.

13. Cohomology of Cyclic Groups

A particularly important example is the cohomology of cyclic groups. This comes up in algebraic topology as the cohomology of Lens Spaces, and it also comes up in number theory as the Galois cohomology of a local field (which is essential for local class field theory).

This will also be a good opportunity to discuss a simple instance of the **cup product** which is a useful tool in studying group cohomology (and cohomology theories in general). We won't develop the full theory here, instead we just focus on a simple case.

13.1. **Cup products with elements of $H^*(G, \mathbb{Z})$.** Let A be a G-module, and recall that we can consider $\mathbb{Z}$ as a trivial G-module. For $\alpha \in H^i(G, \mathbb{Z})$ and $\beta \in H^j(G, A)$, the **cup product** is an element of $H^{i+j}(G, A)$ which is defined as follows. First suppose that α is a *homogeneous* i-cochain $G^{i+1} \to \mathbb{Z}$, and β is a *homogeneous* j-cochain $G^{j+1} \to A$. Then we define

$$\alpha \cup \beta(g_0, \ldots, g_i, h_1, \ldots, h_j) = \alpha(g_0, \ldots, g_i) \cdot \beta(g_i, h_1, \ldots h_j).$$

Lemma 13.1. *One has $d(\alpha \cup \beta) = d(\alpha) \cup \beta + (-1)^i \alpha \cup d(\beta)$.*

Proof. Calculation with the homogeneous differential. $\square$

In particular, it follows that if α and β are homogeneous cocycles, then $\alpha \cup \beta$ is also a homogeneous cocycle. Moreover, if either α or β is a homogeneous coboundary and both are homogeneous cocycles, then $\alpha \cup \beta$ is a homogeneous coboundary. In particular, $\cup$ induces a well-defined map

$$\cup : H^i(G, \mathbb{Z}) \times \mathrm{H}^j(G, A) \to H^j(G, A)$$

which is bilinear.

13.2. **Norms.** Now suppose that G is a finite cyclic group of order n and that $\langle g \rangle = G$. The **norm operator** is the element $N_g := 1 + g + \cdots + g^{n-1} \in \mathbb{Z}[G]$. (The reason this is called the norm comes from the norm map on fields.) Furthermore, we let $I_g := (1 - g) \in \mathbb{Z}[G]$.

Here are a few observations: Let A be a G-module.

(1) Let $N_G A$ denote the set $N_g \cdot A$. Then G acts trivially on $N_G \cdot A$.
(2) Let $I_G A$ denote the set $I_g \cdot A$. Then G acts trivially on $A / I_G A$.

We introduce the **modified cohomology groups** of (G, A), defined as:

$$\hat{\mathrm{H}}^*(G, A) = \begin{cases} A^G / N_G A & * = 0 \\ H^*(G, A) & * > 0 \end{cases}$$

(Note: this is a portion of a more general story called **Tate Cohomology Groups** which are cohomolgy groups $\hat{H}^*(G,A)$ which are defined for all $* \in \mathbb{Z}$). We also define ${}_{N_G}A = \{a \in A \ : \ N_g(a) = 0\}$ and put $\hat{H}^{-1}(G,A) = {}_{N_G}A/I_GA$.

Here is the main theorem concerning the cohomology of cyclic groups.

Theorem 13.2. *Let G be a cyclic group of order n, and let A be a G-module. Then $\mathrm{H}^2(G,\mathbb{Z})$ is cyclic of the same order as G. If $\chi \in \mathrm{H}^2(G,\mathbb{Z})$ is any generator, then*

$$\chi \cup \bullet : \hat{\mathrm{H}}^*(G,A) \to \hat{\mathrm{H}}^{*+2}(G,A)$$

is an isomorphism for all $* \geq 0$.

13.3. **Proof of the Theorem.** First we show that the cohomology is 2-periodic, i.e. that $\hat{H}^*(G,A) = \hat{H}^{*+2}(G,A)$. The point is that there is a nicer projective resolution of $\mathbb{Z}$ than the standard one. Namely, we can take

$$\cdots \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

So we get a projective resolution of $\mathbb{Z}$ which is very simple, having $\mathbb{Z}[G]$ as the i-th term for each i, with alternating maps N_G and $g-1$. Applying $\mathrm{Hom}_{\mathbb{Z}[G]}(\bullet, A)$, we get a complex which computes the cohomology of A:

$$0 \to A \xrightarrow{(g-1)} A \xrightarrow{N} A \xrightarrow{g-1} \cdots$$

In particular, we deduce that $H^i(G,A) \cong H^{i+2}(G,A)$ for all $i \geq 1$. And moreover, one has

$$\begin{cases} H^2(G,A) = {}_IA/NA = A^G/NA \\ H^1(G,A) = {}_NA/IA \end{cases}$$

Moreover, by the definition of $\hat{\mathrm{H}}^*$ for $* = -1, 0$, we can extend this to all $* \geq 0$.

Now let's look at the statements concerning computations using cup products. To see this, we first calculate $\mathrm{H}^2(G,\mathbb{Z})$. By the above, we have

$$\mathrm{H}^2(G,\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z}$$

where the norm $N = (1 + g + \cdots + g^{n-1})$, Namely, one has $\mathrm{H}^2(G,\mathbb{Z}) = \mathbb{Z}/n$ since G acts trivially on $\mathbb{Z}$. Let χ be a generator of this group which corresponds to $1 \in \mathbb{Z}/n$.

Now we consider two exact sequences of G-modules:

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

and

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{g-1} I \to 0.$$

Since $H^*(G,\mathbb{Z}[G]) = 0$ by the homework, we obtain isomorphisms:

$$H^*(G,\mathbb{Z}) \cong \mathrm{H}^{*+1}(G,I) \cong \mathrm{H}^{*+2}(G,\mathbb{Z})$$

the first isomorphism comes from the first exact sequence and the scond one comes from the second exact sequence.

Exercise 13.3. The isomorphism $H^*(G,\mathbb{Z}) \to \mathrm{H}^{*+2}(G,\mathbb{Z})$ is precisely $\chi \cup \bullet$. Now note that the isomorphism $\mathrm{H}^*(G,A) \cong \mathrm{H}^{*+2}(G,A)$ induced by the sequence above is precisely given in a similar way by tensoring these two exact sequences with A:

$$0 \to I \otimes_{\mathbb{Z}} A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to A \to 0$$

and

$$0 \to A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to I \otimes_{\mathbb{Z}} A \to 0.$$

The rest of the theorem is left as an exercise.

14. Herbrand Quotient

Let G be a cyclic group of order n, and let A be a G-module. The **Herbrand Quotient** is defined as

$$h(A) := h_0(A)/h_1(A), \quad h_0(A) := |\hat{\mathrm{H}}^0(G, A)|, \ h_1(A) = |\hat{\mathrm{H}}^1(G, A)|$$

(if this is finite, e.g. if A is finitely generated).

Theorem 14.1. *Suppose that $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, and that $h(\bullet)$ is defined for at least two of A, B, C. Then $h(\bullet)$ is defined for the third, and one has $h(A) \cdot h(B) = h(C)$.*

To deduce the theorem, we note that there is an exact *hexagon*:

$$\hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C) \to \hat{H}^1(G, A) \to \hat{H}^1(G, B) \to \hat{H}^1(G, C) \to \hat{H}^2(G, A) = \hat{\mathrm{H}}^0(G, A).$$

To see this, we note that we can complete the complex calculating $H^*(G, A)$ to a complex which computes $\hat{\mathrm{H}}^*(G, A)$:

$$\cdots A \to A \to A \to \cdots$$

and also for B and C. The short exact sequence induces a short exact sequence of such complexes, etc. Thus we get a long exact sequence on **Tate cohomology groups**, which yields the hexagon above.

Now to conclude the proof, we note that

$$\frac{h_0(A)h_1(B)h_0(C)}{h_1(A)h_0(B)h_1(C)} = 1$$

so the theorem follows. Some applications of this will be on the homework.