MATH 776
GROUP COHOMOLOGY

ANDREW SNOWDEN

1. G-modules

Let G be a group. A **G-module** is an abelian group M equipped with a left action $G \times M \to M$ that is additive, i.e., $g \cdot (x+y) = (g \cdot x) + (g \cdot y)$ and $g \cdot 0 = 0$. A G-module is exactly the same thing as a left module over the group algebra $\mathbf{Z}[G]$. In particular, the category Mod_G of G-modules is a module category, and therefore has enough projectives and enough injectives.

We note that one can pass between left and right G-modules: if M is a right G-module then defining $gx = xg^{-1}$ gives M the structure of a left G-module. For this reason, we always work with left G-modules.

Suppose that M and N are two left G-modules. Then $M \otimes_{\mathbf{Z}} N$ has the structure of a G-module via $g(x \otimes y) = (gx) \otimes (gy)$. We also define a second tensor product, denoted $M \otimes_G N$, by regarding M as a right G-module and then forming the tensor product over $\mathbf{Z}[G]$. Explicitly, $M \otimes_G N$ is the quotient of $M \otimes_{\mathbf{Z}} N$ by the relations $g^{-1}x \otimes y = x \otimes gy$.

2. Group cohomology

Given a G-module M, we let M^G denote the set of invariant elements:

$$M^G = \{x \in M \mid gx = x \text{ for all } g \in G\}.$$

One easily verifies that $M \mapsto M^G$ is a left-exact functor of M. We define $\mathrm{H}^i(G, -)$ to be the ith right derived functor of this functor. These functors are called **group cohomology**. To be completely clear, group cohomology is computed as follows. Let $M \to I^\bullet$ be an injective resolution. Then $\mathrm{H}^i(G, M)$ is the ith cohomology group of the complex $(I^\bullet)^G$.

We regard $\mathbf{Z}$ as a G-module with trivial action. For a G-module M, one clearly has

$$M^G = \mathrm{Hom}_G(\mathbf{Z}, M).$$

Thus the invariants functor is just the Hom functor $\mathrm{Hom}_G(\mathbf{Z}, -)$. It follows that group cohomology is simply an Ext group:

$$\mathrm{H}^i(G, M) = \mathrm{Ext}^i_G(\mathbf{Z}, M).$$

Thus, by properties of Ext, we can compute group cohomology using a projective resolution of the trivial G-module $\mathbf{Z}$. This is a useful observation, since it means we can find just a single resolution (the projective resolution of $\mathbf{Z}$) and use it to compute the group cohomology of any module; we don't need to find injective resolutions of each module separately. Of course, this raises the problem of finding a projective resolution of $\mathbf{Z}$. Fortunately, there is a general construction that applies uniformly to all groups.

Date: February 19, 2019.

Let P_r be the free $\mathbf{Z}$-module with basis G^{r+1}; we write $[g_0, \ldots, g_r]$ for the element of P_r corresponding to $(g_0, \ldots, g_r) \in G^{r+1}$. We give P_r the structure of a G-module by defining $g[g_0, \ldots, g_r] = [gg_0, \ldots, gg_r]$. Define a differential $d \colon P_r \to P_{r-1}$ by

$$g[g_0, \ldots, g_r] = \sum_{i=0}^{r} (-1)^i [g_0, \ldots, \hat{g}_i, \ldots, g_r],$$

where the hat indicates omission. One readily verifies that $d^2 = 0$. Let $\epsilon \colon P_0 \to \mathbf{Z}$ be the augmentation map, i.e., the additive map defined by $\epsilon([g]) = 1$ for all $g \in G$.

Proposition 2.1. *$\epsilon \colon P_\bullet \to \mathbf{Z}$ is a projective resolution.*

Proof. It is clear that each P_r is a free $\mathbf{Z}[G]$-module, since G freely permutes a basis. It thus suffices to prove that the augmented complex is exact. Pick an arbitrary element $h \in G$, and define a map $s_r \colon P_r \to P_{r+1}$ by

$$s_r([g_0, \ldots, g_r]) = [h, g_0, \ldots, g_r].$$

Similarly, define $s_{-1} \colon \mathbf{Z} \to P_0$ by $1 \mapsto [h]$. We thus have the following diagram:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & \mathbf{Z} & \longrightarrow & 0 \\
 & \swarrow_{s_2} & & \swarrow_{s_1} & & \swarrow_{s_0} & & \swarrow_{s_{-1}} & & & \\
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & \mathbf{Z} & \longrightarrow & 0
\end{array}$$

One easily verifies that $ds_r + s_{r-1}d$ is the identity on P_r, and similarly, that ds_{-1} is the identity on $\mathbf{Z}$. We thus see that the identity map on the augmented complex is null-homotopic, and so the complex is acyclic. □

Remark 2.2. Note that the maps s_r in the above proof are not maps of G-modules. Thus we have not shown that the complex is null-homotopic in the category $\mathbf{Ch}(\mathrm{Mod}_G)$, and it typically is not (just think about trying to make s_{-1} a G-map). The proof does show that the complex is null-homotopic in $\mathbf{Ch}(\mathbf{Ab})$ though, and that's sufficient for checking it is exact. □

Corollary 2.3. *Let M be a G-module. Then $\mathrm{H}^i(G, M) = \mathrm{H}^i(\mathrm{Hom}_G(P_\bullet, M))$.*

Let's examine the above formula a bit more closely. An element of $\mathrm{Hom}_G(P_\bullet, M)$ can be identified with a function $\varphi \colon G^{r+1} \to M$ that is G-equivariant, i.e., that satisfies

$$\varphi(g[g_0, \ldots, g_r]) = g\varphi([g_0, \ldots, g_r]).$$

Such a function φ is called a **homogeneous r-cochain** of G with values in M. The group of such objects is denoted $\widetilde{C}^r(G, M)$. If φ is such an r-cochain then $d\varphi$ is the $(r+1)$-cochain given by

$$(d\varphi)([g_0, \ldots, g_{r+1}] = \sum_{i=0}^{r+1} (-1)^i \varphi([g_0, \ldots, \hat{g}_i, \ldots, g_{r+1}]).$$

We say that φ is a **homogeneous r-cocycle** if $d\varphi = 0$, and a **homogenous r-coboundary** if $\varphi = d\psi$ for some $(r-1)$-cochain ψ. The corollary identifies $\mathrm{H}^r(G, M)$ with the group of homogeneous r-cocycles modulo homogeneous r-coboundaries.

Define an **inhomogeneous r-cochain** to be any function $G^r \to M$, and let $C^r(G, M)$ be the group of them. We associated to a homogeneous r-cochain φ the inhomogeneous r-cochain given by

$$(g_1, \ldots, g_r) \mapsto \varphi([1, g_1, g_1g_2, \ldots, g_1 \cdots g_r]).$$

One easily verifies that this gives an isomorphism $\widetilde{C}^r(G, M) \to C^r(G, M)$. We can therefore transfer the differential on the latter to the former. The result is as follows: given an inhomogeneous r-cochain φ, the inhomogeneous $(r+1)$-cochain $d\varphi$ is

$$\begin{aligned}(d\varphi)(g_1, \ldots, g_{r+1}) = & g_1\varphi(g_2, \ldots, g_{r+1}) \\ & + \sum_{i=1}^{r} \left[(-1)^i \varphi(g_1, \ldots, g_i g_{i+1}, \ldots, g_{r+1})\right] \\ & + (-1)^{r+1}\varphi(g_1, \ldots, g_r).\end{aligned}$$

We thus have an isomorphism of complexes $C^\bullet(G, M) \cong \widetilde{C}^\bullet(G, M)$. Therefore, letting $Z^r(G, M)$ be the kernel of d (the group of **inhomogeneous r-cocycles**) and $B^r(G, M)$ denote the image of d (the group of **inhomogeneous r-coboundaries**), we find:

Proposition 2.4. $\mathrm{H}^r(G, M) = Z^r(G, M)/B^r(G, M)$.

Remark 2.5. Let us verify that the differentials on homogeneous and inhomogenous 1-chains agree. Let $\varphi \colon G \to M$ be an inhomogeneous 1-cochain. Then $d\varphi$ is given by

$$(d\varphi)(g_1, g_2) = g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1).$$

The corresponding homogeneous 1-cochain $\psi \colon G^2 \to M$ is given by $\psi([g_0, g_1]) = g_0\varphi(g_0^{-1}g_1)$. Thus

$$(d\psi)([g_0, g_1, g_2]) = \psi(g_1, g_2) - \psi(g_0, g_2) + \psi(g_0, g_1),$$

and so

$$(d\psi)([1, g_1, g_1g_2]) = \psi(g_1, g_1g_2) - \psi(1, g_2) + \psi(1, g_1) = g_1\varphi(g_2) - \varphi(g_2) - \varphi(g_1).$$

□

3. Group homology

Given a G-module M, let M_G be the group of coinvariants:

$$M_G = M/\{x - \sigma x \mid \sigma \in G, x \in M\}.$$

One easily verifies that $M \mapsto M_G$ is a right-exact functor of M. We define $\mathrm{H}_i(G, -)$ to be the ith left derived functor of this functor. These functors are called **group homology**. We quickly recall the definition: $\mathrm{H}_i(G, M)$ is the ith homology group of the complex $(P_\bullet)_G$ where $P_\bullet \to M$ is a projective resolution of M.

We have an identification

$$M_G = M \otimes_G \mathbf{Z}.$$

Indeed, recall that $M \otimes_G \mathbf{Z}$ is by definition the quotient of $M \otimes \mathbf{Z} = M$ by the relations $\sigma x \otimes 1 = x \otimes \sigma^{-1} = x \otimes 1$, which is exactly the definition of M_G. It follows that group homology can be viewed as Tor:

$$\mathrm{H}_i(G, M) = \mathrm{Tor}_i^G(G, \mathbf{Z}).$$

In particular, we can compute group homology using a projective resolution of $\mathbf{Z}$. Using the resolution from the previous section gives a description of group homology in terms of chains, cycles, and boundaries. We skip the details, but mention one important case:

Proposition 3.1. *If M is a trivial G-module then* $\mathrm{H}_1(G, M) = G^{\mathrm{ab}} \otimes_{\mathbf{Z}} M$. *In particular,* $\mathrm{H}_1(G, \mathbf{Z}) = G^{\mathrm{ab}}$.

4. Induced and coinduced modules

Let $H \subset G$ be groups and let M be an H-module. We define the **induction** of M to G by

$$\mathrm{Ind}_H^G(M) = \mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} M,$$

where the action of G comes from its (left) action on $\mathbf{Z}[G]$. Similarly, we define the **coinduction** of M to G by

$$\mathrm{CoInd}_H^G(M) = \mathrm{Hom}_H(G, M).$$

Thus $\mathrm{CoInd}_H^G(M)$ consists of all functions $f\colon G \to M$ satisfying $f(hg) = hf(g)$ for $g \in G$ and $h \in H$. The G-action is given by $(gf)(g') = f(g'g)$. We say that a G-module is **(co)induced** if it is (co)induced from the trivial subgroup.

Suppose that $G = \amalg_{i \in I} g_i H$ is the decomposition of G into cosets of H. Then $\mathbf{Z}[G]$ is free right $\mathbf{Z}[H]$-module with basis g_i, and so

$$\mathrm{Ind}_H^G(M) = \bigoplus_{i \in I} g_i \otimes M.$$

In particular, we see that $\mathrm{Ind}_H^G(M)$ is an exact functor of M. Similarly, if $G = \amalg_{i \in I} H g_i'$ then

$$\mathrm{CoInd}_H^G(M) \cong \prod_{i \in I} M, \qquad f \mapsto (f(g_i'))_{i \in I}.$$

In particular, $\mathrm{CoInd}_H^G(M)$ is an exact functor of M.

Proposition 4.1. *Suppose that H has finite index in G. Then we have a natural isomorphism of G-modules*

$$\mathrm{Ind}_H^G(M) \cong \mathrm{CoInd}_H^G(M).$$

Proof. Define a function

$$\Phi\colon \mathrm{CoInd}_H^G(M) \to \mathrm{Ind}_H^G(M), \qquad f \mapsto \sum_{g \in H \backslash G} g^{-1} \otimes f(g).$$

It is clear that Φ is well-defined and G-equivariant. By the above descriptions of induction and coinduction, it is an isomorphism. (We are essentially taking $g_i' = g_i^{-1}$ here.) □

Suppose that N is a G-module. Then we can obviously regard N as an H-module. We sometimes denote this H-module by $\mathrm{Res}_H^G(N)$, and refer to it as the **restriction** of N to H. It is clear that $\mathrm{Res}_H^G(N)$ is an exact functor of N.

Proposition 4.2 (Frobenius reciprocity)**.** *Let M be an H-module and let N be a G-module. We have natural isomorphisms*

$$\mathrm{Hom}_G(\mathrm{Ind}_H^G(M), N) = \mathrm{Hom}_H(M, \mathrm{Res}_H^G(N)),$$

$$\mathrm{Hom}_G(N, \mathrm{CoInd}_H^G(M)) = \mathrm{Hom}_H(\mathrm{Res}_H^G(N), M).$$

In other words, induction is left adjoint to restriction and co-induction is right adjoint. When H has finite index in G, induction and restriction are adjoint to each other on both sides.

Proof. Exercise. □

Corollary 4.3. *If M is an injective H-module then $\mathrm{CoInd}_H^G(M)$ is an injective G-module. Similarly, if M is a projective H-module then $\mathrm{Ind}_H^G(M)$ is a projective G-module.*

Proof. Suppose M is injective. Then

$$\mathrm{Hom}_G(-, \mathrm{CoInd}_H^G(M)) = \mathrm{Hom}_H(\mathrm{Res}_H^G(-), M)$$

is an exact functor, and so $\mathrm{CoInd}_H^G(M)$ is injective. □

Corollary 4.4. *We have natural isomorphisms $(\mathrm{CoInd}_H^G(M))^G \cong M^H$ and $(\mathrm{Ind}_H^G(M))_G \cong M_H$.*

Proof. For the first isomorphism, apply the proposition with $N = \mathbf{Z}$. For the second, note that

$$(\mathrm{Ind}_H^G(M))_G = \mathbf{Z} \otimes_{\mathbf{Z}[G]} (\mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} M) = \mathbf{Z} \otimes_{\mathbf{Z}[H]} M = M_H. \qquad \square$$

Proposition 4.5 (Shapiro's lemma)**.** *Let $H \subset G$ be groups and let M be an H-module. Then we have a canonical isomorphism*

$$\mathrm{H}^i(G, \mathrm{CoInd}_H^G(M)) \cong \mathrm{H}^i(H, M).$$

There is a similar statement for homology and induced modules.

Proof. Let $M \to I^\bullet$ be an injective resolution of M as an H-module. Since co-induction is exact and takes injectives to injectives, we see that $\mathrm{CoInd}_H^G(M) \to \mathrm{CoInd}_H^G(I^\bullet)$ is an injective resolution. Thus $\mathrm{H}^\bullet(G, \mathrm{CoInd}_H^G(M))$ is computed by the complex $(\mathrm{CoInd}_H^G(I^\bullet))^G$. But this is just $(I^\bullet)^H$, by the relationship between co-induction and invariants, which computes $\mathrm{H}^\bullet(H, M)$. □

Corollary 4.6. *Suppose that M is a co-induced G-module. Then $\mathrm{H}^i(G, M) = 0$ for $i > 0$. Similarly for induced modules and homology.*

5. Extended functoriality

Let (G, M) and (G', M') be pairs consisting of a group and a module over the group. A **morphism** $(G, M) \to (G', M')$ consists of a group homomorphism $\alpha \colon G' \to G$ and an additive map $\beta \colon M \to M'$ satisfying $\beta(\alpha(g)x) = g\beta(x)$ for all $g \in G'$ and $x \in M$. Given such a pair, one obtains a map of complexes

$$C^\bullet(G, M) \to C^\bullet(G', M'), \qquad \varphi \mapsto ((g_1, \ldots, g_r) \mapsto \beta(\varphi(\alpha(g_1), \ldots, \alpha(g_r))))$$

and thus a map on cohomology

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

Thus we can say that group cohomology is functorial in (G, M).

There are a number of important special cases of this general construction:

(a) Let $H \subset G$ be groups and let M be a G-module. We then have a morphism $(G, M) \to (H, \mathrm{Res}^G_H(M))$, where $\alpha\colon H \to G$ is the inclusion and $\beta\colon M \to \mathrm{Res}^G_H(M)$ is the identity. We thus obtain a map

$$\mathrm{res}\colon \mathrm{H}^i(G, M) \to \mathrm{H}^i(H, \mathrm{Res}^G_H(M))$$

called **restriction**. It simply restricts a cocycle on G to one on H.

(b) Let $H \subset G$ be a normal subgroup and let M be a G-module. We then have a morphism $(G/H, M^H) \to (G, M)$ where $\alpha\colon G \to G/H$ is the quotient map and $\beta\colon M^H \to M$ is the inclusion. We thus obtain a map

$$\mathrm{inf}\colon \mathrm{H}^i(G/H, M^H) \to \mathrm{H}^i(G, M)$$

called **inflation**.

(c) Again, let $H \subset G$ be a normal subgroup and let M be a G-module. For $g \in G$, let $\alpha_g\colon H \to H$ be the map $h \mapsto g^{-1}hg$ and let $\beta_g\colon M \to M$ be the map $\beta_g(x) = gx$. Then α_g and β_g define an endomorphism of $(H, \mathrm{Res}^G_H(M))$. In this way, we get an action of G on $\mathrm{H}^i(H, M)$. Exercise: show that the action of H on $\mathrm{H}^i(H, M)$ is trivial; thus the action of G can really be regarded as an action of G/H.

(d) Let $H \subset G$ be a subgroup and let M be an H-module. We then have a morphism $(G, \mathrm{CoInd}^G_H(M)) \to (H, M)$ where $\alpha\colon H \to G$ is the inclusion and $\beta\colon \mathrm{CoInd}^G_H(M) \to M$ is given by $\beta(f) = f(1)$. We thus get a map

$$\mathrm{H}^i(G, \mathrm{CoInd}^G_H(M)) \to \mathrm{H}^i(H, M).$$

Exercise: show that this is the isomorphism from Shapiro's lemma.

Proposition 5.1 (Inflation–restriction sequence)**.** *Let H be a normal subgroup of G and let M be a G-module. Let $r > 0$ be an integer, and suppose that $\mathrm{H}^i(H, \mathrm{Res}^G_H(M)) = 0$ for all $0 < i < r$. Then the sequence*

$$0 \to \mathrm{H}^r(G/H, M^H) \stackrel{\mathrm{inf}}{\to} \mathrm{H}^r(G, M) \stackrel{\mathrm{res}}{\to} \mathrm{H}^r(H, M)$$

is exact.

Proof. We first treat the $r = 1$ case, in which the vanishing hypothesis is vacuous. The first map is obviously injective, since it is simply pullback along $G \to G/H$. We must show that the image and kernel agree in the middle. Thus let $\varphi\colon G \to M$ be a crossed homomorphism that restricts to a principal crossed homomorphism of H. Let $x \in M$ be such that $\varphi(h) = hx - x$ for $h \in H$. Let $\varphi' = \varphi - dx$, i.e., $\varphi'(g) = \varphi(g) - (gx - x)$. Then φ' is a crossed homomorphism representing the same cohomology class as φ, and φ' restricts to 0 on H. We have $\varphi'(gh) = g\varphi'(h) + \varphi'(g) = \varphi'(g)$ and $\varphi'(hg) = h\varphi'(g) + \varphi'(h) = h\varphi'(g)$. We also have $h\varphi'(g) = \varphi'(hg) = \varphi'(g(g^{-1}hg)) = \varphi'(g)$. We thus see that φ' defines a function $G/H \to M^H$, which is easily seen to be a crossed homomorphism. This proves the proposition.

The general case now follows by dimension shifting. Precisely, we proceed by induction on r, having established the $r = 1$ case above. Consider a short exact sequence

$$0 \to M \to I \to N \to 0$$

with I injective. Then $\mathrm{H}^r(G, M) \cong \mathrm{H}^{r-1}(G, N)$; in particular, $\mathrm{H}^i(G, N) = 0$ for $0 < i < r-1$. Thus we have an inflation–restriction exact sequence for N in degree $r - 1$, and this gives one for M. (We leave the details as an exercise.) □

6. Corestriction

Let H be a subgroup of G and let M be a G-module. The adjunction between restriction and induction gives rise to the co-unit morphism

$$\mathrm{Ind}_H^G(\mathrm{Res}_H^G(M)) \to M, \qquad g \otimes x \mapsto gx,$$

which is a map of G-modules. Now suppose that H has finite index. We can then combine the above map with the isomorphism between induction and co-induction to get a natural map of G-modules

$$\mathrm{CoInd}_H^G(\mathrm{Res}_H^G(M)) \to M, \qquad f \mapsto \sum_{g \in H\backslash G} g^{-1} f(g).$$

Combining this with the Shapiro isomorphism, we thus get a map

$$\mathrm{cor}\colon \mathrm{H}^i(H, \mathrm{Res}_H^G(M)) \cong \mathrm{H}^i(G, \mathrm{CoInd}_H^G(\mathrm{Res}_G^H(M))) \to \mathrm{H}^i(G, M)$$

called **corestriction**.

Proposition 6.1. *The corestriction map on* H^0 *is given by*

$$\mathrm{cor}\colon M^H \to M^G, \qquad x \mapsto \sum_{g \in G/H} gx.$$

Proof. The isomorphism

$$M^H \cong (\mathrm{CoInd}_H^G(\mathrm{Res}_H^G(M)))^G$$

takes $x \in M^H$ to the function $f\colon G \to M$ given by $f(g) = x$ for all g; note that $f(hg) = x = hx = hf(g)$ since x is H-invariant. Under the map $\mathrm{CoInd}_H^G(\mathrm{Res}_H^G(M)) \to M$ defined above, the element f is sent to

$$\sum_{g \in H\backslash G} g^{-1} f(g) = \sum_{g \in H\backslash G} g^{-1} x = \sum_{g \in G/H} gx.$$

This completes the proof. □

Proposition 6.2. *The composition*

$$\mathrm{H}^i(G, M) \xrightarrow{\mathrm{res}} \mathrm{H}^i(H, \mathrm{Res}_H^G(M)) \xrightarrow{\mathrm{cor}} \mathrm{H}^i(G, M)$$

is multiplication by $[G : H]$.

Proof. First suppose $i = 0$. Let $x \in \mathrm{H}^0(G, M) = M^G$. Then

$$\mathrm{cor}(\mathrm{res}(x)) = \sum_{g \in G/H} gx = [G : H]x,$$

which proves the claim. Thus $\mathrm{cor} \circ \mathrm{res}$ and multiplication by $[G : H]$ define morphisms of $\mathrm{H}^\bullet(G, -)$ which agree at index 0, and so they are equal. □

Corollary 6.3. *Suppose that G is a finite group of order n. Then $n \cdot \mathrm{H}^i(G, M) = 0$ for any G-module M and any $i > 0$.*

Proof. Take H to be the trivial group. Then $\mathrm{H}^i(H, \mathrm{Res}_H^G(M)) = 0$, and so $\mathrm{res}(x) = 0$ for any $x \in \mathrm{H}^i(G, M)$. Thus $nx = \mathrm{cor}(\mathrm{res}(x)) = 0$. □

Corollary 6.4. *Let G be a finite group and let M be a finitely generated $\mathbf{Z}[G]$-module. Then $\mathrm{H}^i(G, M)$ is finite for $i > 0$.*

Proof. The group of cochains $C^i(G, M)$ is obviously a finitely generated abelian group, since M is finitely generated and G is finite. Since $\mathrm{H}^i(G, M)$ is a subquotient of $C^i(G, M)$, it too is finitely generated. Since it is also killed by $\#G$, it is thus finite. □

Corollary 6.5. *Let H be the p-Sylow subgroup of G and let M be a G-module. Then the restriction map*

$$\mathrm{res}\colon \mathrm{H}^i(G, M) \to \mathrm{H}^i(H, \mathrm{Res}^G_H(M))$$

is injective on the p-primary components of these groups.

Proof. Suppose $x \in \mathrm{H}^i(G, M)$ has order a power of p and $\mathrm{res}(x) = 0$. Then $0 = \mathrm{cor}(\mathrm{res}(x)) = [G : H]x$. But $[G : H]$ is prime to p and x has p-power order; thus $x = 0$. □

7. Cup products

Let G be a group and let M and N be G-modules. We define a map

$$\mathrm{H}^r(G, M) \times \mathrm{H}^s(G, N) \to \mathrm{H}^{r+s}(G, M \otimes N), \qquad (x, y) \mapsto x \cup y,$$

called the **cup product**, as follows. Let x be represented by the (homogeneous) r-cocycle φ and let y be represented by the s-cocycle ψ. Then $x \cup y$ is represented by the $(r + s)$-cocycle

$$(g_1, \ldots, g_{r+s}) \mapsto \varphi(g_1, \ldots, g_r) \otimes g_1 \cdots g_r \psi(g_{r+1}, \ldots, g_s).$$

We leave it as an exercise to verify that this is well-defined.

Proposition 7.1. *The cup product has the following properties:*

(a) It is bi-additive.
(b) It is functorial in M and N.
(c) In cohomological degree 0, it is the map

$$\cup\colon M^G \otimes N^G \to (M \otimes N)^G, \qquad x \cup y = x \otimes y.$$

(d) Suppose that

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is an exact sequence of G-modules, and N is a G-module such that the sequence

$$0 \to M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

is exact. Then for $x \in \mathrm{H}^r(G, M_3)$ and $y \in \mathrm{H}^s(G, N)$ we have $(\delta x) \cup y = \delta(x \cup y)$, where δ is the connecting homomorphism.

(e) Suppose that

$$0 \to N_1 \to N_2 \to N_3 \to 0$$

is an exact sequence of G-modules, and M is a G-module such that the sequence

$$0 \to M \otimes N_1 \to M \otimes N_2 \to M \otimes N_3 \to 0$$

is exact. Then for $x \in \mathrm{H}^r(G, M)$ and $y \in \mathrm{H}^s(G, N_3)$ we have $x \cup (\delta y) = (-1)^r \delta(x \cup y)$, where δ is the connecting homomorphism.

Moreover, these properties uniquely characterize cup product; that is, given another product rule on cohomology satisfying these axioms, it is equal to cup product.

Proof. Checking the properties is a simple exercise. Uniqueness is proved by dimension shifting. □

Proposition 7.2. *The cup product satisfies the following properties:*

(a) *For* $x \in \mathrm{H}^r(G, M)$, $y \in \mathrm{H}^s(G, N)$, *and* $z \in \mathrm{H}^t(G, K)$, *we have* $x \cup (y \cup z) = (x \cup y) \cup z$, *under the natural identification* $M \otimes (N \otimes K) = (M \otimes N) \otimes K$.
(b) *For* $x \in \mathrm{H}^r(G, M)$ *and* $y \in \mathrm{H}^s(G, N)$, *we have* $x \cup y = (-1)^{rs} y \cup x$ *under the natural identification* $M \otimes N = N \otimes M$.
(c) $\mathrm{res}(x \cup y) = \mathrm{res}(x) \cup \mathrm{res}(y)$ *when defined.*
(d) $\mathrm{cor}(x \cup \mathrm{res}(y)) = \mathrm{cor}(x) \cup y$ *when defined.*

Proof. Exercise. □

Suppose that $M \times N \to K$ is a G-equivariant pairing, that is, the map $M \otimes N \to K$ is a map of G-modules. We can then consider the composite

$$\mathrm{H}^r(G, M) \times \mathrm{H}^s(G, N) \xrightarrow{\cup} \mathrm{H}^{r+s}(G, M \otimes N) \to \mathrm{H}^{r+s}(G, K).$$

This will also be refereed to as the cup product.

As a corollary to the above proposition, we see that $\bigoplus_{i \geq 0} \mathrm{H}^i(G, \mathbf{Z})$ is a graded-commutative ring. That is, it is a graded, unital, and associative ring, and satisfies the modified commutativity rule $xy = (-1)^{rs} yx$ when x and y are homogeneous of degrees r and s. This ring is called the **cohomology ring** of G. Moreover, if M is a G-module then $\bigoplus_{i \geq 0} \mathrm{H}^i(G, M)$ is a module over the cohomology ring.

References

[K] K. Kedlaya. Notes on class field theory. http://www.math.mcgill.ca/darmon/courses/cft/refs/kedlaya.pdf

[K] J.S. Milne. Class field theory. https://www.jmilne.org/math/CourseNotes/cft.html