Group Cohomology of Finite Cyclic Groups and the Herbrand Quotient

Alejandro De Las Peñas Castaño

14/December/2021

Group Cohomology of Finite Cyclic Groups and the Herbrand Quotient

1 The group ring $\mathbb{Z}G$

In this paper, we fix the following notation:

- G is a group.
- $\mathbb{Z}G$ is the integral group ring of G; it is the free abelian group generated by the elements of G with the following ring multiplication law:

$$\left(\sum_{g\in G} n_g g\right)\left(\sum_{h\in G} m_h h\right) = \sum_{h\in G}\left(\sum_{g\in G} n_g m_{g^{-1}h}\right) h.$$

- ${}_G\mathbf{Mod}$ is the category of G-modules which we can identify with the category of left $\mathbb{Z}G$-modules.
- $\mathbf{Ab}$ is the category of abelian groups.
- A is an abelian group and a G-module.
- $\mathbb{Z}$ is considered throughout as a trivial G-module.
- $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ is the augmentation map defined to be the surjective G-module map *and* ring homomorphism,

$$\varepsilon\left(\sum_{g\in G} n_g g\right) := \sum_{g\in G} n_g,$$

  and the kernel $I_G := \ker\varepsilon$ is the augmentation ideal; it is a two-sided ideal of $\mathbb{Z}G$.

Proposition 1.1. *We have the following short exact sequence of G-modules (with G-module maps):*

$$0 \longrightarrow I_G \hookrightarrow \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Proof. Clear from the definitions. □

Proposition 1.2. *The additive group $(I_G, +)$ of the augmentation ideal is the free abelian group generated by the set $\{g - 1 \mid g \in G \setminus \{1\}\}$.*

Proof. Let $z = \sum n_g g \in \mathbb{Z}G$, then $z \in I_G$ if and only if $\sum n_g = 0$. Thus, if $z \in I_G$, we have:

$$z = z - 0 \cdot 1 = \Big(\sum_{g \in G} n_g g\Big) - \Big(\sum_{g \in G} n_g\Big) \cdot 1 = \underbrace{(n_g - n_g) \cdot 1}_{=0} + \sum_{g \in G \setminus \{1\}} n_g(g-1)$$

and thus z is in the additive group generated by $\{g - 1 \mid g \in G \setminus \{1\}\}$. Clearly, every $g - 1 \in I_G$ since $\varepsilon(g-1) = 1 - 1 = 0$. Thus $(I_G, +) = \langle g - 1 \mid g \neq 1\rangle$ as required.

□

2 Right Derived Functors and the Cohomology of Groups

We start with an additive covariant functor $\mathscr{F} : {}_G\mathbf{Mod} \to \mathbf{Ab}$, an object $A \in {}_G\mathbf{Mod}$ and an injective resolution:

$$\mathbf{I} \;:= \quad 0 \longrightarrow A \xrightarrow{\eta} I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \longrightarrow \cdots$$

of A. If we delete A from the cochain complex above, and apply $\mathscr{F}$, we obtain the cochain:

$$\mathscr{F}\mathbf{I} \;= \quad 0 \longrightarrow \mathscr{F}(I^0) \xrightarrow{\mathscr{F}d^0} \mathscr{F}(I^1) \xrightarrow{\mathscr{F}d^1} \mathscr{F}(I^2) \longrightarrow \cdots$$

We can thus compute the cohomology groups of $\mathscr{F}\mathbf{I}$. Furthermore, if $f : A \to A'$ is a G-module homomorphism, and $\mathbf{I}'$ is an injective resolution for A', f extends to a cochain map $\check{f} : \mathbf{I} \to \mathbf{I}'$ which is unique up to homotopy (this is the Comparison Theorem); since $\mathscr{F}$ is additive, then $\mathscr{F}\check{f}$ is also unique up to homotopy and thus descends to a well-defined map $H^n(\mathscr{F}\check{f}) : H^n(\mathscr{F}\mathbf{I}) \to H^n(\mathscr{F}\mathbf{I}')$. This means we can define the following sequence of functors:

Definition 2.1. With the notation as above, define the nth (covariant) *right derived functor* of $\mathscr{F}$ is the functor

$$R^n\mathscr{F} : {}_G\mathbf{Mod} \longrightarrow \mathbf{Ab}$$

defined on objects as

$$(R^n\mathscr{F})(A) = H^n(\mathscr{F}\mathbf{I})$$

and defined on morphisms as

$$(R^n\mathscr{F})(f) = H^n(\mathscr{F}\check{f})$$

Example 2.2. A fundamental example of this construction is the right derived functors of the covariant hom functor. More precisely, if $B \in {}_G\mathbf{Mod}$ and $\mathscr{F} := \mathrm{Hom}_G(B, -)$, then the nth derived functor of $\mathscr{F}$ is denoted by

$$\mathrm{Ext}^n_{\mathbb{Z}G}(B, -) := R^n\mathscr{F}.$$

A special and fundamental case is when B is the trivial G-module $\mathbb{Z}$. In fact, this example gives rise to group cohomology:

Definition 2.3. The nth cohomology group of G with coefficients in A is defined as

$$H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$$

where $\mathbb{Z}$ is viewed as a trivial G-module.

Remark 2.4. Since the covariant Hom functor $\mathrm{Hom}_G(\mathbb{Z}, -)$ is naturally isomorphic to the fixed-point functor $A \mapsto A^G = \{a \in A \mid g.a = a,\ \forall g \in G\}$, then we can also define $H^n(G, A)$ to be the nth right derived functor of the fixed-point functor.

The major problem of the definition of $H^n(G, A)$ is that calculating injective resolutions for an arbitrary G-module A is hard. Fortunately, we can swap the roles of A and $\mathbb{Z}$ in order to use projective resolutions which are much easier to calculate. We make this statement more precise:

Let $\mathscr{G} : {}_G\mathbf{Mod} \to \mathbf{Ab}$ be a *contravariant* additive functor, let $B \in {}_G\mathbf{Mod}$ and fix a projective resolution

$$\mathbf{P} \;:=\quad \cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} B \longrightarrow 0.$$

After deleting B from the chain complex, we apply $\mathscr{G}$, which is contravariant, to obtain the cochain complex

$$\mathscr{G}\mathbf{P} \;=\quad 0 \longrightarrow \mathscr{G}(P_0) \xrightarrow{\mathscr{G}d_0} \mathscr{G}(P_1) \xrightarrow{\mathscr{G}d_1} \mathscr{G}(P_2) \longrightarrow \cdots$$

Similarly as above, a G-module homomorphism $f : B' \to B$ extends to a chain map $\check{f} : \mathbf{P} \to \mathbf{P}'$ which is unique up to homotopy. Since $\mathscr{G}$ is additive and contravariant, then $\mathscr{G}\check{f} : \mathscr{G}\mathbf{P}' \to \mathscr{G}\mathbf{P}$ is also unique up to homotopy and thus descends to a well-defined map $H^n(\mathscr{G}\check{f}) : H^n(\mathscr{G}\mathbf{P}') \to H^n(\mathscr{G}\check{f})$ on cohomology. We can thus define the contravariant right derived functors in exactly the same way as the covariant right derived functors:

Definition 2.5. With the notation as above, the nth (contravariant) *right derived functor* of $\mathscr{G}$ is the contravariant functor

$$R^n\mathscr{G} : {}_G\mathbf{Mod} \longrightarrow \mathbf{Ab}$$

defined on objects as

$$(R^n\mathscr{G})(B) = H^n(\mathscr{G}\mathbf{P})$$

and defined on morphisms as

$$(R^n\mathscr{F})(f) = H^n(\mathscr{G}\check{f})$$

Example 2.6. If $A \in {}_G\mathbf{Mod}$ and $\mathscr{G} := \mathrm{Hom}_G(-, A)$ is the contravariant hom functor, then the nth derived functor of $\mathscr{G}$ is denoted by

$$\mathrm{ext}^n_{\mathbb{Z}G}(-, A) := R^n\mathscr{G}.$$

The relationship between Ext and ext is given by the following important theorem:

Theorem 2.7. *Let A and B be G-modules, let $\mathbf{I}$ be an injective resolution of A and $\mathbf{P}$ be a projective resolution of B. Then for all n, we have*

$$\mathrm{Ext}^n_{\mathbb{Z}G}(B, A) = H^n(\mathrm{Hom}_G(B, \mathbf{I})) \cong H^n(\mathrm{Hom}_G(\mathbf{P}, A)) = \mathrm{ext}^n_{\mathbb{Z}G}(B, A).$$

The above theorem gives us a method to calculate the cohomology groups of G with coefficients in A without having to calculate injective resolutions for A:

1. Calculate a projective G-module resolution for the trivial G-module $\mathbb{Z}$.

2. Apply the contravariant hom functor $\mathrm{Hom}_G(-, A)$ to the projective resolution.

3. Compute the cohomology groups of the resulting projective resolution.

3 The Cohomology of Finite Cyclic Groups

For the rest of the paper, assume that:

G is a finite cyclic group of order k generated by $x \in G$.

In this section we compute $H^n(G, A)$ for finite cyclic G. In view of Theorem 2.7, there are three steps to be made which we separate into different subsections.

3.1 A Projective G-module Resolution of $\mathbb{Z}$

The projective G-module resolution for $\mathbb{Z}$ will in fact be a free 2-periodic projective resolution. The alternating differentials will simply be multiplication by special elements of $\mathbb{Z}G$, namely:

Definition 3.1. Define elements $N, D \in \mathbb{Z}G$ as

$$N = 1 + x + \cdots + x^{k-1}, \qquad D = x - 1,$$

and define the multiplication maps

$$\mu_N : \mathbb{Z}G \longrightarrow \mathbb{Z}G, \quad \mu_N(z) = Nz \quad \text{and} \quad \mu_D : \mathbb{Z}G \longrightarrow \mathbb{Z}G, \quad \mu_D(z) = Dz.$$

Lemma 3.2. *The maps μ_N and μ_D are G-module maps and $\mu_N\mu_D = \mu_D\mu_N = \varepsilon\mu_D = 0$.*

Proof. Observe that since $\mathbb{Z}$ and G are commutative, then $\mathbb{Z}G$ is commutative. Thus

$$\mu_N(zw) = N(zw) = z(Nw) = z\mu_N(w) \qquad \forall z, w \in \mathbb{Z}G$$

so that μ_N (and equivalently μ_D) are G-module homomorphisms. Again by commutativity we trivially have $\mu_D\mu_N = \mu_N\mu_D$.

Now, since x has order k,

$$ND = (1 + x + \cdots + x^{k-1})(x-1) = x^k - 1 = 1 - 1 = 0.$$

Therefore

$$\mu_N\mu_D(z) = N\big(\mu_D(z)\big) = N(Dz) = (ND)z = 0z = 0.$$

We have shown that $\mu_N\mu_D = \mu_D\mu_N = 0$. Finally, if $z \in \mathbb{Z}G$, then since ε is a ring homomorphism:

$$\varepsilon\mu_D(z) = \varepsilon(Dz) = \varepsilon\big((x-1)z\big) = \varepsilon(x-1)\varepsilon(z) = (1-1)\varepsilon(z) = 0.$$

Thus $\varepsilon\mu_D = 0$ as required. □

Proposition 3.3. *$\mathbb{Z}$ admits the following projective (indeed free) G-module resolution:*

$$\cdots \longrightarrow \mathbb{Z}G \xrightarrow{\mu_N} \mathbb{Z}G \xrightarrow{\mu_D} \mathbb{Z}G \xrightarrow{\mu_N} \mathbb{Z}G \xrightarrow{\mu_D} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \qquad (1)$$

Proof. By Lemma 3.2, we have that (1) is a chain complex. So we only need to show that the sequence is exact. First we label the terms of the sequence:

$$\cdots \longrightarrow \underbrace{\mathbb{Z}G}_{n=4} \xrightarrow{\mu_N} \underbrace{\mathbb{Z}G}_{n=3} \xrightarrow{\mu_D} \underbrace{\mathbb{Z}G}_{n=2} \xrightarrow{\mu_N} \underbrace{\mathbb{Z}G}_{n=1} \xrightarrow{\mu_D} \underbrace{\mathbb{Z}}_{n=0}G \xrightarrow{\varepsilon} \underbrace{\mathbb{Z}}_{n=-1} \longrightarrow 0.$$

Notice that the resolution is 2-periodic after the $n = 0$ term. So exactness at any odd (resp. even) n is identical to exactness at $n = 1$ (resp. $n = 2$). Thus we only need to prove exactness at $n = -1, 0, 1$ and 2:

$(n = -1)$ ε is surjective.

$(n = 0)$ By lemma 3.2, we already have that $\varepsilon\mu_D = 0$ so that $\mathrm{im}\mu_D \subseteq \ker\varepsilon = I_G$. To prove the other containment, we only need to observe that proposition 1.2 tells us that

$$\begin{aligned} I_G &= \langle g - 1 \mid g \in G \setminus \{1\}\rangle \\ &= \big\langle x^\ell - 1 \mid 0 < \ell < k\big\rangle \\ &= \big\langle D(x^\ell + \cdots + x + 1) \mid 0 < \ell < k\big\rangle \\ &\subseteq \mathrm{im}(\mu_D). \end{aligned}$$

$(n = 1)$ By lemma 3.2, we already have that $\mu_D\mu_N = 0$ so that $\mathrm{im}\mu_N \subseteq \ker\mu_D$. To prove the other containment, let $z \in \ker\mu_D$ and write it as:

$$z = \sum_{\ell=0}^{k-1} n_\ell x^\ell.$$

Then

$$0 = Dz = (x-1)\Big(\sum_{\ell=0}^{k-1} n_\ell x^\ell\Big) = (n_{k-1}-n_0) + (n_0-n_1)x + \cdots + (n_{k-2}-n_{k-1})x^{k-1}.$$

Since $\mathbb{Z}G$ is a free abelian group with basis $G = \{1, x, \ldots, x^{k-1}\}$, the above relation forces

$$n_0 = n_1 = \cdots = n_{k-1};$$

call $n \in \mathbb{Z}$ the common value. This implies:

$$z = \sum_{\ell=0}^{k-1} n x^\ell = \Big(\sum_{\ell=0}^{k-1} x^\ell\Big) n = Nn = \mu_N(n) \in \mathrm{im}(\mu_N)$$

as required.

$(n = 2)$ By definition of the product in $\mathbb{Z}G$ we have

$$Nz = \Big(\sum_{\ell=0}^{k-1} x^\ell\Big)\Big(\sum_{i=0}^{k-1} n_i x^i\Big) = \sum_{\ell=0}^{k-1}\Big(\sum_{i=0}^{k-1} n_i\Big)x^\ell = \sum_{\ell=0}^{k-1} \varepsilon(z)x^\ell = \varepsilon(z)N.$$

Thus, since $\{1, x, \ldots, x^{k-1}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}G$ then

$$z \in \ker \mu_N \quad\iff\quad 0 = Nz = \sum_{\ell=0}^{k-1} \varepsilon(z)x^\ell \quad\iff\quad \varepsilon(z) = 0 \quad\iff\quad z \in I_G.$$

In step $n = 0$, we already showed that $I_G = \mathrm{im}(\mu_D)$ so we conclude that $\ker \mu_N = \mathrm{im}\mu_D$ as required.

□

3.2 The Cochain Complex $0 \to \mathrm{Hom}_G(\mathbb{Z}G, A) \to \mathrm{Hom}_G(\mathbb{Z}G, A) \to \cdots$

The next step in computing $H^n(G, A)$ is to apply the contravariant hom functor $\mathrm{Hom}_G(-, A)$ to the *deleted* projective resolution

$$\mathbf{P} \;:=\; \cdots \longrightarrow \mathbb{Z}G \xrightarrow{\mu_N} \mathbb{Z}G \xrightarrow{\mu_D} \mathbb{Z}G \xrightarrow{\mu_N} \mathbb{Z}G \xrightarrow{\mu_D} \mathbb{Z}G \longrightarrow 0$$

of Corollary 3.3 to get the cochain:

$$\mathrm{Hom}_G(\mathbf{P}, A) \;=\; 0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}G, A) \xrightarrow{\mu_D^*} \mathrm{Hom}_G(\mathbb{Z}G, A) \xrightarrow{\mu_N^*} \mathrm{Hom}_G(\mathbb{Z}G, A) \longrightarrow \cdots$$

where μ_N^* and μ_D^* are the *pullbacks* of μ_N and μ_D respectively; for example $\mu_N^*(f) = f\mu_N$. However, this cochain can be safely changed to a simpler one:

Proposition 3.4. *The cochain* $\operatorname{Hom}_G(\mathbf{P}, A)$ *is isomorphic to the cochain*

$$\mathbf{Q} \ := \qquad 0 \longrightarrow A \xrightarrow{\mu_D} A \xrightarrow{\mu_N} A \xrightarrow{\mu_D} A \xrightarrow{\mu_N} A \longrightarrow \cdots$$

where $\mu_N(a) = N.a$ *and* $\mu_D(a) = D.a$. *In particular we have that*

$$H^n(\operatorname{Hom}_G(\mathbf{P}, A)) \cong H^n(\mathbf{Q}) \qquad \forall n \geq 0. \tag{2}$$

Proof. Observe that the covariant hom functor $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, -) : {}_G\mathbf{Mod} \to \mathbf{Ab}$ can actually be viewed as a functor with codomain ${}_G\mathbf{Mod}$. Indeed, since $\mathbb{Z}G$ is commutative, then $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A)$ has a natural G-module structure. Under this convention, $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, -)$ is naturally equivalent to the identity functor on ${}_G\mathbf{Mod}$ under the natural equivalence $\tau : \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, -) \to \operatorname{id}_{G\mathbf{Mod}}$ defined by:

$$\tau_A : \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \longrightarrow A \quad \text{with} \quad f \mapsto f(1).$$

We write the inverse of τ_A as $f_a := \tau_A^{-1}(a)$ where $f_a(z) = za$.

Thus if we apply this functor to the cochain complex $\operatorname{Hom}_G(\mathbf{P}, A)$, we get a cochain complex

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_G(\mathbb{Z}G, A) \arrow[r, "\mu_D^*"] \arrow[d, "\tau_A"] & \operatorname{Hom}_G(\mathbb{Z}G, A) \arrow[r, "\mu_N^*"] \arrow[d, "\tau_A"] & \operatorname{Hom}_G(\mathbb{Z}G, A) \arrow[r] \arrow[d, "\tau_A"] & \cdots \\
0 \arrow[r] & A \arrow[r, "d^0"] & A \arrow[r, "d^1"] & A \arrow[r] & \cdots
\end{tikzcd} \tag{3}$$

whose differentials are defined as (for example)

$$d^1(a) = \tau_A \mu_N^* \tau_A^{-1}(a) = \tau_A \mu_N^*(f_a) = \tau_A(f_A \mu_N) = f_a \mu_N(1) = f_a(N) = Na = \mu_N(a).$$

Thus the bottom row of (3) is exactly $\mathbf{Q}$ and $\operatorname{Hom}_G(\mathbf{P}, A) \cong \mathbf{Q}$ as required. □

Remark 3.5. We know that $\mathbf{P}$ is 2-periodic after the 0th term (this is clear from the definition) and thus $\mathbf{Q}$ is also 2-periodic. This means that the cohomology groups after the 0th cohomology group only depend on the parity of the term. More precisely:

$$H^1(\mathbf{Q}) = H^3(\mathbf{Q}) = H^5(\mathbf{Q}) = \cdots = H^{2n+1}(\mathbf{Q}) = \cdots$$
$$H^2(\mathbf{Q}) = H^4(\mathbf{Q}) = H^6(\mathbf{Q}) = \cdots = H^{2n}(\mathbf{Q}) = \cdots$$

Remark 3.6. If instead of applying $\operatorname{Hom}_G(-, A)$ to the deleted chain complex $\mathbf{P}$ we apply the *covariant* functor $- \otimes_{\mathbb{Z}G} A$ we obtain the chain complex:

$$\mathbf{P} \otimes \mathbb{Z}G \ = \qquad \cdots \longrightarrow \mathbb{Z}G \otimes_{\mathbb{Z}G} A \xrightarrow{\mu_N \otimes \operatorname{id}_A} \mathbb{Z}G \otimes_{\mathbb{Z}G} A \xrightarrow{\mu_D \otimes \operatorname{id}_A} \mathbb{Z}G \otimes_{\mathbb{Z}G} A \longrightarrow 0.$$

Taking the nth homology of this chain complex yields the nth *left derived functor* of $- \otimes_{\mathbb{Z}G} A$ which is by definition $\operatorname{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, A)$ which in turn is the definition of the nth cohomology group of G with coefficients in A.

Furthermore, we can follow the same proof of Proposition 3.4 using the natural equivalence

$$\operatorname{id}_{G\mathbf{Mod}} \cong (\mathbb{Z}G \otimes_{\mathbb{Z}G} -)$$

to obtain a chain complex

$$\mathbf{Q}' \;:= \qquad \cdots \longrightarrow A \xrightarrow{\mu_D} A \xrightarrow{\mu_N} A \xrightarrow{\mu_D} A \longrightarrow 0$$

whose homology is easier to compute. See remark 3.9.

Remark 3.7. If $G = \mathrm{Gal}(L/K)$ is the Galois group of a cyclic abelian extension (e.g. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}$ or a finite extension of finite fields), generated by σ and we write $A := L^\times$ multiplicatively, then for $\alpha \in L^\times$ we have

$$\mu_N(\alpha) = \Big(\sum_{\ell=0}^{k-1} \sigma^\ell\Big).\alpha := \prod_{\ell=0}^{k} \sigma^\ell(\alpha) = N_{L/K}(\alpha)$$

where $N_{L/K} : L^\times \to K^\times$ is the usual field norm map. This explains the choice of the letter N.

3.3 Computation of $H^n(G, A)$

In view of Theorem 2.7, we have that $H^n(G, A) \cong H^n(\mathbf{Q})$. To write the computations cleanly, we introduce the following notation:

(i) ${}_NA := \ker(\mu_N) = \{a \in A \mid Na = 0\}$,

(ii) $NA := \mathrm{im}(\mu_N) = \{Na \in A \mid a \in A\}$,

(iii) $DA := \mathrm{im}(\mu_D) = \{Da \in A \mid a \in A\}$,

Observe that

$$\ker(\mu_D) = \{a \in A \mid D.a = 0\} = \{a \in A \mid (x-1)a = x.a - a = 0\} = \{a \in A \mid x.a = a\}.$$

If $a \in A^G$, then clearly $a \in \ker(\mu_D)$. Conversely, if $a \in \ker(\mu_D)$, then $x.a = a$ and thus $x^\ell.a = a$ by induction and thus $a \in A^G$ since $G = \{1, \dots, x^{k-1}\}$. Therefore:

$$\ker \mu_D = A^G. \tag{4}$$

We can now state and prove the following:

Theorem 3.8. *The nth cohomology group of G with coefficients in A is given by:*

$$H^n(G, A) \cong \begin{cases} A^G & \text{if } n = 0, \\ {}_NA/DA & \text{if } n \text{ is odd}, \\ A^G/NA & \text{if } n \text{ is even.} \end{cases}$$

Proof. By remark 3.5 and $H^n(G, A) \cong H^n(\mathbf{Q})$ we only need to calculate $H^0(G, A), H^1(G, A)$ and $H^2(G, A)$. We recall the cochain $\mathbf{Q}$ and label its terms:

$$\mathbf{Q} \;:= \qquad 0 \longrightarrow \underbrace{A}_{n=0} \xrightarrow{\mu_D} \underbrace{A}_{n=1} \xrightarrow{\mu_N} \underbrace{A}_{n=2} \xrightarrow{\mu_D} \underbrace{A}_{n=3} \xrightarrow{\mu_N} \underbrace{A}_{n=4} \longrightarrow \cdots$$

For $n = 0$, (4) implies

$$H^0(G, A) \cong H^0(\mathbf{Q}) = \ker \mu_D/0 \cong \ker \mu_D = A^G.$$

For $n = 1$,

$$H^1(G, A) \cong H^1(\mathbf{Q}) = \frac{\ker(\mu_N)}{\mathrm{im}(\mu_D)} = \frac{{}_NA}{DA}$$

and for $n = 2$,

$$H^2(G, A) \cong H^2(\mathbf{Q}) = \frac{\ker(\mu_D)}{\mathrm{im}(\mu_N)} = \frac{A^G}{NA}.$$

□

Remark 3.9. In view of Remark 3.6, the homology groups of G with coefficients in n can be computed analogously:

$$H_n(G, A) \cong \begin{cases} A_G & \text{if } n = 0, \\ A^G/NA & \text{if } n \text{ is odd,} \\ {}_NA/I_GA & \text{if } n \text{ is even.} \end{cases} \qquad (A_G := A/I_GA).$$

Example 3.10. Suppose $G = 1$, then for all A we have $H^0(1, A) \cong A$ and $H^n(1, A) = 0$ for all $n > 0$, because $N = 1$ and $D = 0$ so that ${}_NA = 0$ and $NA = A = A^G$.

Corollary 3.11. *If A is a trivial G-module, then the nth cohomology group of G with coefficients in A is given by:*

$$H^n(G, A) \cong \begin{cases} A & \textit{if } n = 0, \\ A[k] = \{a \in A \mid ka = 0\} & \textit{if } n \textit{ is odd,} \\ A/kA & \textit{if } n \textit{ is even, .} \end{cases}$$

Proof. Observe that if A is a trivial G-module, then

$$Na = \Big(\sum_{\ell=0}^{k} x^\ell\Big)a := \sum_{\ell=0}^{k-1} x^\ell.a = \sum_{\ell=0}^{k-1} a = ka$$

and

$$Da = (x - 1)a = x.a - 1.a = a - a = 0.$$

Thus:

(*i*) $A^G = A$,

(*ii*) ${}_NA = \{a \in A \mid 0 = Na = ka\} = A[k]$,

(*iii*) $NA = \mathrm{im}(\mu_N) = \{Na \in A \mid a \in A\} = kA$,

(*iv*) $DA := \mathrm{im}(\mu_D) = \{Da = 0 \in A \mid a \in A\} = 0$, and the corollary follows. □

Example 3.12. If $A = \mathbb{Z}$ as a trivial G-module, then

$$H^n(G, \mathbb{Z}) \cong \begin{cases} \mathbb{Z} & \text{if } n = 0, \\ 0 & \text{if } 2 \nmid n, \\ \mathbb{Z}/k\mathbb{Z} & \text{if } 2 \mid n. \end{cases}$$

4 The Herbrand Quotient

Definition 4.1. Let A be a *finite* G-module. Then the *Herbrand quotient* of A as a G-module is defined as

$$h(A) = \frac{|H^2(G, A)|}{|H^1(G, A)|}.$$

Remark 4.2. Observe that $h(A)$ is well-defined since $H^2(G, A) \cong A^G/NA$, by Theorem 3.8, which is finite since A itself is finite.

Theorem 4.3. *(Herbrand) If A is a finite G-module, then $h(A) = 1$. That is*

$$|H^2(G, A)| = |H^1(G, A)|.$$

Proof. We compute $|A|$ in two different ways:

$$|NA| = |\mathrm{im}(\mu_N)| = [A : \ker \mu_N] = \frac{|A|}{|{}_NA|} \quad \Longrightarrow \quad |NA| \cdot |{}_NA| = |A|$$

and

$$|DA| = |\mathrm{im}(\mu_D)| = [A : \ker \mu_D] = \frac{|A|}{|\ker \mu_D|} \overset{(4)}{=} \frac{|A|}{|A^G|} \quad \Longrightarrow \quad |DA| \cdot |A^G| = |A|.$$

Equating both gives us

$$|NA| \cdot |{}_NA| = |DA| \cdot |A^G| \quad \Longrightarrow \quad \frac{|{}_NA|}{|DA|} = \frac{|A^G|}{|NA|}. \tag{5}$$

Thus by Theorem 3.8 we have

$$|H^2(G, A)| = |A^G/NA| = \frac{|A^G|}{|NA|} \overset{(5)}{=} \frac{|{}_NA|}{DA} = |H^1(G, A)|$$

as required. □

Remark 4.4. In view of Theorem 3.8, Herbrand's Theorem says that *all* the cohomology groups of a finite G-module A have the same cardinality.

Remark 4.5. Theorem 4.3 is a key lemma in the proof of Tate's Theorem in Class Field Theory, namely if A is a G-module such that for every subgroup $H \leq G$ we have

(i) $H^1(H, A) = 0$,

(ii) $H^2(H, A)$ is cyclic of order $|H|$,

then there is an isomorphism

$$H^r(G, \mathbb{Z}) \cong H^{r+2}(G, A).$$

The statement used in Class Field theory is more precise as it explicitly gives the isomorphism. This result is used to construct the Artin Map that realizes the Galois group of a finite abelian extension of number fields as the quotient of the idéle class group of the extension.