# GROUP AND GALOIS COHOMOLOGY

Romyar Sharifi

# Contents


Chapter 1. Group cohomology 5
1.1. Group rings 5
1.2. Group cohomology via cochains 6
1.3. Group cohomology via projective resolutions 11
1.4. Homology of groups 14
1.5. Induced modules 16
1.6. Tate cohomology 18
1.7. Dimension shifting 23
1.8. Comparing cohomology groups 24
1.9. Cup products 34
1.10. Tate cohomology of cyclic groups 41
1.11. Cohomological triviality 44
1.12. Tate's theorem 48

Chapter 2. Galois cohomology 53
2.1. Profinite groups 53
2.2. Cohomology of profinite groups 60
2.3. Galois theory of infinite extensions 64
2.4. Galois cohomology 67
2.5. Kummer theory 69

CHAPTER 1

# Group cohomology

## 1.1. Group rings

Let $G$ be a group.

DEFINITION 1.1.1. The *group ring* (or, more specifically, $\mathbb{Z}$-group ring) $\mathbb{Z}[G]$ of a group $G$ consists of the set of finite formal sums of group elements with coefficients in $\mathbb{Z}$

$$\left\{ \sum_{g\in G} a_g g \mid a_g \in \mathbb{Z} \text{ for all } g \in G, \text{ almost all } a_g = 0 \right\}.$$

with addition given by addition of coefficients and multiplication induced by the group law on $G$ and $\mathbb{Z}$-linearity. (Here, "almost all" means all but finitely many.)

In other words, the operations are

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$

and

$$\left( \sum_{g\in G} a_g g \right) \left( \sum_{g\in G} b_g g \right) = \sum_{g\in G} (\sum_{k\in G} a_k b_{k^{-1}g}) g.$$

REMARK 1.1.2. In the above, we may replace $\mathbb{Z}$ by any ring $R$, resulting in the $R$-group ring $R[G]$ of $G$. However, we shall need here only the case that $R = \mathbb{Z}$.

DEFINITION 1.1.3.

i. The *augmentation map* is the homomorphism $\varepsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\varepsilon \left( \sum_{g\in G} a_g g \right) = \sum_{g\in G} a_g.$$

ii. The *augmentation ideal* $I_G$ is the kernel of the augmentation map $\varepsilon$.

LEMMA 1.1.4. *The augmentation ideal $I_G$ is equal to the ideal of $\mathbb{Z}[G]$ generated by the set $\{g-1 \mid g \in G\}$.*

PROOF. Clearly $g - 1 \in \ker \varepsilon$ for all $g \in G$. On the other hand, if $\sum_{g\in G} a_g = 0$, then

$$\sum_{g\in G} a_g g = \sum_{g\in G} a_g (g-1).$$

□

DEFINITION 1.1.5. If $G$ is a finite group, we then define the *norm element* of $\mathbb{Z}[G]$ by $N_G = \sum_{g\in G} g$.

REMARK 1.1.6.

a. We may speak, of course, of modules over the group ring $\mathbb{Z}[G]$. We will refer here to such $\mathbb{Z}[G]$-modules more simply as *$G$-modules*. To give a $G$-module is equivalent to giving an abelian group $A$ together with a $G$-action on $A$ that is compatible with the structure of $A$ as an abelian group, i.e., a map

$$G \times A \to A, \qquad (g,a) \mapsto g \cdot a$$

satisfying the following properties:

(i) $1 \cdot a = a$ for all $a \in A$,

(ii) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $a \in A$ and $g_1, g_2 \in G$, and

(iii) $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2$ for all $a_1, a_2 \in A$ and $g \in G$.

b. A homomorphism $\kappa\colon A \to B$ of $G$-modules is just a homomorphism of abelian groups that satisfies $\kappa(ga) = g\kappa(a)$ for all $a \in A$ and $g \in G$. The group of such homomorphisms is denoted by $\mathrm{Hom}_{\mathbb{Z}[G]}(A,B)$.

DEFINITION 1.1.7. We say that a $G$-module $A$ is a *trivial* if $g \cdot a = a$ for all $g \in G$ and $a \in A$.

DEFINITION 1.1.8. Let $A$ be a $G$-module.

i. The group of *$G$-invariants* $A^G$ of $A$ is given by

$$A^G = \{a \in A \mid g \cdot a = a \text{ for all } g \in G, a \in A\},$$

which is to say the largest submodule of $A$ fixed by $G$.

ii. The group of *$G$-coinvariants* $A_G$ of $A$ is given by

$$A_G = A/I_G A,$$

which is to say (noting Lemma 1.1.4) the largest quotient of $A$ fixed by $G$.

EXAMPLE 1.1.9.

a. If $A$ is a trivial $G$-module, then $A^G = A$ and $A_G \cong A$.

b. One has $\mathbb{Z}[G]_G \cong \mathbb{Z}$. We have $\mathbb{Z}[G]^G = (N_G)$ if $G$ is finite and $\mathbb{Z}[G]^G = (0)$ otherwise.

## 1.2. Group cohomology via cochains

The simplest way to define the $i$th cohomology group $H^i(G,A)$ of a group $G$ with coefficients in a $G$-module $A$ would be to let $H^i(G,A)$ be the $i$th derived functor on $A$ of the functor of $G$-invariants. However, not wishing to assume homological algebra at this point, we take a different tack.

DEFINITION 1.2.1. Let $A$ be a $G$-module, and let $i \geq 0$.

i. The group of *$i$-cochains* of $G$ with coefficients in $A$ is the set of functions from $G^i$ to $A$:

$$C^i(G,A) = \{f\colon G^i \to A\}.$$

ii. The $i$th *differential* $d^i = d^i_A\colon C^i(G,A) \to C^{i+1}(G,A)$ is the map

$$d^i(f)(g_0,g_1,\ldots,g_i) = g_0 \cdot f(g_1,\ldots g_i) + \sum_{j=1}^{i} (-1)^j f(g_0,\ldots,g_{j-2},g_{j-1}g_j,g_{j+1},\ldots,g_i) + (-1)^{i+1} f(g_0,\ldots,g_{i-1}).$$

We will continue to let $A$ denote a $G$-module throughout the section. We remark that $C^0(G,A)$ is taken simply to be $A$, as $G^0$ is a singleton set. The proof of the following is left to the reader.

LEMMA 1.2.2. *For any $i \geq 0$, one has $d^{i+1} \circ d^i = 0$.*

REMARK 1.2.3. Lemma 1.2.2 shows that $C^{\cdot}(G,A) = (C^i(G,A), d^i)$ is a cochain complex.

We consider the cohomology groups of $C^{\cdot}(G,A)$.

DEFINITION 1.2.4. Let $i \geq 0$.

i. We set $Z^i(G,A) = \ker d^i$, the group of *$i$-cocycles* of $G$ with coefficients in $A$.

ii. We set $B^0(G,A) = 0$ and $B^i(G,A) = \operatorname{im} d^{i-1}$ for $i \geq 1$. We refer to $B^i(G,A)$ as the group of *$i$-coboundaries* of $G$ with coefficients in $A$.

We remark that, since $d^i \circ d^{i-1} = 0$ for all $i \geq 1$, we have $B^i(G,A) \subseteq Z^i(G,A)$ for all $i \geq 0$. Hence, we may make the following definition.

DEFINITION 1.2.5. We define the *ith cohomology group* of $G$ with coefficients in $A$ to be

$$H^i(G,A) = Z^i(G,A)/B^i(G,A).$$

The cohomology groups measure how far the cochain complex $C^{\cdot}(G,A)$ is from being exact. We give some examples of cohomology groups in low degree.

LEMMA 1.2.6.

*a. The group $H^0(G,A)$ is equal to $A^G$, the group of $G$-invariants of $A$.*

*b. We have*

$$Z^1(G,A) = \{f\colon G \to A \mid f(gh) = gf(h) + f(g) \text{ for all } g,h \in G\}$$

*and $B^1(G,A)$ is the subgroup of $f\colon G \to A$ for which there exists $a \in A$ such that $f(g) = ga - a$ for all $g \in G$.*

*c. If $A$ is a trivial $G$-module, then $H^1(G,A) = \operatorname{Hom}(G,A)$.*

PROOF. Let $a \in A$. Then $d^0(a)(g) = ga - a$ for $g \in G$, so $\ker d^0 = A^G$. That proves part a, and part b is simply a rewriting of the definitions. Part c follows immediately, as the definition of $Z^1(G,A)$ reduces to $\mathrm{Hom}(G,A)$, and $B^1(G,A)$ is clearly $(0)$, in this case. □

We remark that, as $A$ is abelian, we have $\mathrm{Hom}(G,A) = \mathrm{Hom}(G^{\mathrm{ab}},A)$, where $G^{\mathrm{ab}}$ is the maximal abelian quotient of $G$ (i.e., its abelianization). We turn briefly to an even more interesting example.

DEFINITION 1.2.7. A *group extension* of $G$ by a $G$-module $A$ is a short exact sequence of groups

$$0 \to A \xrightarrow{\iota} \mathscr{E} \xrightarrow{\pi} G \to 1$$

such that, choosing any section $s\colon G \to \mathscr{E}$ of $\pi$, one has

$$s(g)as(g)^{-1} = g \cdot a$$

for all $g \in G$, $a \in A$. Two such extensions $\mathscr{E} \to \mathscr{E}'$ are said to be equivalent if there is an isomorphism $\theta\colon \mathscr{E} \xrightarrow{\sim} \mathscr{E}'$ fitting into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathscr{E} & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle\theta} & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathscr{E}' & \longrightarrow & G & \longrightarrow & 0, \end{array}$$

We denote the set of equivalence classes of such extensions by $\mathscr{E}(G,A)$.

We omit the proof of the following result, as it is not used in the remainder of these notes. We also leave it as an exercise to the reader to define the structure of an abelian group on $\mathscr{E}(G,A)$ which makes the following identification an isomorphism of groups.

THEOREM 1.2.8. *The group $H^2(G,A)$ is in canonical bijection with $\mathscr{E}(G,A)$ via the map induced by that taking a 2-cocycle $f\colon G^2 \to A$ to the extension $\mathscr{E}_f = A \times G$ with multiplication given by*

$$(a,g)\cdot(b,h) = (a + gb + f(g,h), gh)$$

*This identification takes the identity to the semi-direct product $A \ltimes G$ determined by the action of $G$ on $A$.*

One of the most important uses of cohomology is that it converts short exact sequences of $G$-modules to long exact sequences of abelian groups. For this, in homological language, we need the fact that $C^i(G,A)$ provides an exact functor in the module $A$.

LEMMA 1.2.9. *If $\alpha\colon A \to B$ is a $G$-module homomorphism, then for each $i \geq 0$, there is an induced homomorphism of groups*

$$\alpha^i\colon C^i(G,A) \to C^i(G,B)$$

*taking $f$ to $\alpha \circ f$ and compatible with the differentials in the sense that*

$$d_B^i \circ \alpha^i = \alpha^{i+1} \circ d_A^i.$$

PROOF. We need only check the compatibility. For this, note that

$$d^i(\alpha\circ f)(g_0,g_1,\dots,g_i) = g_0\alpha\circ f(g_1,\dots g_i) + \sum_{j=i}^{i}(-1)^j\alpha\circ f(g_0,\dots,g_{j-2},g_{j-1}g_j,g_{j+1},\dots,g_i)+(-1)^{i+1}\alpha\circ f(g_0,\dots,g_{i-1}) = \alpha(d^i(f)(g_0,g_1,\dots,g_i)),$$

as $\alpha$ is a $G$-module homomorphism (the fact of which we use only to deal with the first term). □

In other words, $\alpha$ induces a morphism of complexes $\alpha^{\cdot}: C^{\cdot}(G,A)\to C^{\cdot}(G,B)$. As a consequence, one sees easily the following

NOTATION 1.2.10. If not helpful for clarity, we will omit the superscripts from the notation in the morphisms of cochain complexes. Similarly, we will consistently omit them in the resulting maps on cohomology, described below.

COROLLARY 1.2.11. *A $G$-module homomorphism $\alpha: A\to B$ induces maps*

$$\alpha^*: H^i(G,A)\to H^i(G,B)$$

*on cohomology.*

The key fact that we need about the morphism on cochain complexes is the following.

LEMMA 1.2.12. *Suppose that*

$$0\to A\xrightarrow{\iota} B\xrightarrow{\pi} C\to 0$$

*is a short exact sequence of $G$-modules. Then the resulting sequence*

$$0\to C^i(G,A)\xrightarrow{\iota} C^i(G,B)\xrightarrow{\pi} C^i(G,C)\to 0$$

*is exact.*

PROOF. Let $f\in C^i(G,A)$, and suppose $\iota\circ f=0$. As $\iota$ is injective, this clearly implies that $f=0$, so the map $\iota^i$ is injective. As $\pi\circ\iota=0$, the same is true for the maps on cochains. Next, suppose that $f'\in C^i(G,B)$ is such that $\pi\circ f'=0$. Define $f\in C^i(G,A)$ by letting $f(g_1,\dots,g_i)\in A$ be the unique element such that

$$\iota(f(g_1,\dots,g_i)) = f'(g_1,\dots,g_i),$$

which we can do since $\operatorname{im}\iota=\ker\pi$. Thus, $\operatorname{im}\iota^i=\ker\pi^i$. Finally, let $f''\in C^i(G,C)$. As $\pi$ is surjective, we may define $f'\in C^i(G,B)$ by taking $f'(g_1,\dots,g_i)$ to be any element with

$$\pi(f'(g_1,\dots,g_i)) = f''(g_1,\dots,g_i).$$

We therefore have that $\pi^i$ is surjective. □

We now prove the main theorem of the section.

THEOREM 1.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

*is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups*

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

*Moreover, this construction is natural in the short exact sequence in the sense that any morphism*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\iota} & B & \xrightarrow{\pi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\iota'} & B' & \xrightarrow{\pi'} & C' & \longrightarrow & 0, \end{array}$$

*gives rise to a morphism of long exact sequences, and in particular, a commutative diagram*

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H^i(G,A) & \xrightarrow{\iota^*} & H^i(G,B) & \xrightarrow{\pi^*} & H^i(G,C) & \xrightarrow{\delta^i} & H^{i+1}(G,A) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \alpha^*} & & \downarrow{\scriptstyle \beta^*} & & \downarrow{\scriptstyle \gamma^*} & & \downarrow{\scriptstyle \alpha^*} & & \\ \cdots & \longrightarrow & H^i(G,A') & \xrightarrow{(\iota')^*} & H^i(G,B') & \xrightarrow{(\pi')^*} & H^i(G,C') & \xrightarrow{\delta^i} & H^{i+1}(G,A') & \longrightarrow & \cdots. \end{array}$$

PROOF. First consider the diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^j(G,A) & \xrightarrow{\iota} & C^j(G,B) & \xrightarrow{\pi} & C^j(G,C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^j} & & \downarrow{\scriptstyle d_B^j} & & \downarrow{\scriptstyle d_C^j} & & \\ 0 & \longrightarrow & C^{j+1}(G,A) & \xrightarrow{\iota} & C^{j+1}(G,B) & \xrightarrow{\pi} & C^{j+1}(G,C) & \longrightarrow & 0 \end{array}$$

for $j \geq 0$. Noting Lemma 1.2.12, the exact sequences of cokernels (for $j = i-1$) and kernels (for $j = i+1$) can be placed in a second diagram

$$\begin{array}{ccccccccc} & & \frac{C^i(G,A)}{B^i(G,A)} & \xrightarrow{\iota} & \frac{C^i(G,B)}{B^i(G,B)} & \xrightarrow{\pi} & \frac{C^i(G,C)}{B^i(G,C)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_A^i} & & \downarrow{\scriptstyle d_B^i} & & \downarrow{\scriptstyle d_C^i} & & \\ 0 & \longrightarrow & Z^{i+1}(G,A) & \xrightarrow{\iota} & Z^{i+1}(G,B) & \xrightarrow{\pi} & Z^{i+1}(G,C) & & \end{array}$$

(recalling that $B^0(G,A) = 0$ for the case $i = 0$), and the snake lemma now provides the exact sequence

$$H^i(G,A) \xrightarrow{\alpha^*} H^i(G,B) \xrightarrow{\beta^*} H^i(G,C) \xrightarrow{\delta^i} H^{i+1}(G,A) \xrightarrow{\alpha^*} H^{i+1}(G,B) \xrightarrow{\beta^*} H^{i+1}(G,C).$$

Splicing these together gives the long exact sequence in cohomology, exactness of

$$0 \to H^0(G,A) \to H^0(G,B)$$

being obvious. We leave naturality of the long exact sequence as an exercise. □

REMARK 1.2.14. The maps $\delta^i\colon H^i(G,C) \to H^{i+1}(G,A)$ defined in the proof of theorem 1.2.13 are known as *connecting homomorphisms*. Again, we will often omit superscripts and simply refer to $\delta$.

REMARK 1.2.15. A sequence of functors that take short exact sequences to long exact sequences (i.e., which also give rise to connecting homomorphisms) and is natural in the sense that every morphism of short exact sequences gives rise to a morphism of long exact sequences is known as a $\delta$-functor. Group cohomology forms a (cohomological) $\delta$-functor that is universal in a sense we omit a discussion of here.

## 1.3. Group cohomology via projective resolutions

In this section, we assume a bit of homological algebra, and redefine the $G$-cohomology of $A$ in terms of projective resolutions.

For $i \geq 0$, let $G^{i+1}$ denote the direct product of $i+1$ copies of $G$. We view $\mathbb{Z}[G^{i+1}]$ as a $G$-module via the left action

$$g \cdot (g_0, g_1, \ldots, g_i) = (gg_0, gg_1, \ldots, gg_i).$$

We first introduce the standard resolution.

DEFINITION 1.3.1. The *(augmented) standard resolution* of $\mathbb{Z}$ by $G$-modules is the sequence of $G$-module homomorphisms

$$\cdots \to \mathbb{Z}[G^{i+1}] \xrightarrow{d_i} \mathbb{Z}[G^i] \to \cdots \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z},$$

where

$$d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i)$$

for each $i \geq 1$, and $\varepsilon$ is the augmentation map.

At times, we may use $(g_0, \ldots, \widehat{g_j}, \ldots, g_i) \in G^i$ to denote the $i$-tuple excluding $g_j$. To see that this definition is actually reasonable, we need the following lemma.

PROPOSITION 1.3.2. *The augmented standard resolution is exact.*

PROOF. In this proof, take $d_0 = \varepsilon$. For each $i \geq 0$, compute

$$d_i \circ d_{i+1}(g_0, \ldots, g_{i+1}) = \sum_{j=0}^{i+1} \sum_{\substack{k=0 \\ k \neq j}}^{i+1} (-1)^{j+k-s(j,k)} (g_0, \ldots, \widehat{g_j}, \ldots, \widehat{g_k}, \ldots, g_{i+1}),$$

where $s(j,k)$ is 0 if $k < j$ and 1 if $k > j$. Each possible $(i-1)$-tuple appears twice in the sum, with opposite sign. Therefore, we have $d_i \circ d_{i+1} = 0$.

Next, define $\theta_i\colon \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}]$ by

$$\theta_i(g_1, \ldots, g_i) = (1, g_1, \ldots, g_i).$$

Then

$$\begin{aligned} d_i \circ \theta_i(g_0,\dots,g_i) &= (g_0,\dots,g_i) - \sum_{j=0}^{i} (-1)^j (1,g_0,\dots,\widehat{g_j},\dots,g_i) \\ &= (g_0,\dots,g_i) - \theta_{i-1} \circ d_{i-1}(g_0,\dots,g_i), \end{aligned}$$

which is to say that

$$d_i \circ \theta_i + \theta_{i-1} \circ d_{i-1} = \mathrm{id}_{\mathbb{Z}[G^i]}.$$

If $\alpha \in \ker d_{i-1}$ for $i \geq 1$, it then follows that $d_i(\theta_i(\alpha)) = \alpha$, so $\alpha \in \mathrm{im}\, d_i$. □

For a $G$-module $A$, we wish to consider the following complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \xrightarrow{D^i} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+2}],A) \to \cdots . \tag{1.3.1}$$

Here, we define $D^i = D^i_A$ by $D^i(\varphi) = \varphi \circ d_{i+1}$. We compare this with the complex of cochains for $G$.

THEOREM 1.3.3. *The maps*

$$\psi^i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \to C^i(G,A)$$

*defined by*

$$\psi^i(\varphi)(g_1,\dots,g_i) = \varphi(1,g_1,g_1g_2,\dots,g_1g_2\cdots g_i)$$

*are isomorphisms for all $i \geq 0$. This provides isomorphisms of complexes in the sense that $\psi^{i+1} \circ D^i = d^i \circ \psi^i$ for all $i \geq 0$. Moreover, these isomorphisms are natural in the $G$-module $A$.*

PROOF. If $\psi^i(\varphi) = 0$, then $\varphi(1,g_1,g_1g_2,\dots,g_1g_2\cdots g_i) = 0$ for all $g_1,\dots,g_i \in G$. Let $h_0,\dots,h_i \in G$, and define $g_j = h_{j-1}^{-1}h_j$ for all $1 \leq j \leq i$. We then have

$$\varphi(h_0,h_1,\dots,h_i) = h_0\varphi(1,h_0^{-1}h_1,\dots,h_0^{-1}h_i) = h_0\varphi(1,g_1,\dots,g_1\cdots g_i) = 0.$$

Therefore, $\psi^i$ is injective. On the other hand, if $f \in C^i(G,A)$, then defining

$$\varphi(h_0,h_1,\dots,h_i) = h_0 f(h_0^{-1}h_1,\dots,h_{i-1}^{-1}h_i),$$

we have

$$\varphi(gh_0,gh_1,\dots,gh_i) = gh_0 f((gh_0)^{-1}gh_1,\dots,(gh_{i-1})^{-1}gh_i) = g\varphi(h_0,h_1,\dots,h_i)$$

and $\psi^i(\varphi) = f$. Therefore, $\psi^i$ is an isomorphism of groups.

That $\psi^{\cdot}$ forms a map of complexes is shown in the following computation:

$$\begin{aligned} \psi^{i+1}(D^i(\varphi))(g_1,\dots,g_{i+1}) &= D^i(\varphi)(1,g_1,\dots,g_1\cdots g_{i+1}) \\ &= \varphi \circ d_{i+1}(1,g_1,\dots,g_1\cdots g_{i+1}) \\ &= \sum_{j=0}^{i+1} (-1)^j \varphi(1,g_1,\dots,\widehat{g_1\cdots g_j},\dots,g_1\cdots g_{i+1}). \end{aligned}$$

The latter term equals

$$g_1\psi^i(\varphi)(g_2,\dots,g_{i+1})+\sum_{j=1}^{i}(-1)^j\psi^i(\varphi)(g_1,\dots,g_{j-1},g_jg_{j+1},g_{j+2},\dots,g_{i+1})$$
$$+(-1)^{i+1}\psi^i(\varphi)(g_1,\dots,g_i),$$

which is $d^i(\psi^i(\varphi))$.

Finally, suppose that $\alpha\colon A\to B$ is a $G$-module homomorphism. We then have

$$\alpha\circ\psi^i(\varphi)(g_1,\dots,g_i)=\alpha\circ\varphi(1,g_1,\dots,g_1\cdots g_i)=\psi^i(\alpha\circ\varphi)(g_1,\dots,g_i),$$

hence the desired naturality. □

COROLLARY 1.3.4. *The ith cohomology group of the complex* $(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A),D_A^i)$ *is naturally isomorphic to* $H^i(G,A)$.

In fact, the standard resolution is a projective resolution of $\mathbb{Z}$, as is a consequence of the following lemma and the fact that every free module is projective.

LEMMA 1.3.5. *The G-module* $\mathbb{Z}[G^{i+1}]$ *is free.*

PROOF. In fact, we have

$$\mathbb{Z}[G^{i+1}]\cong\bigoplus_{(g_1,\dots,g_i)\in G^i}\mathbb{Z}[G](1,g_1,\dots,g_i),$$

and the submodule generated by $(1,g_1,\dots,g_i)$ is clearly free. □

REMARKS 1.3.6.

a. Lemma 1.3.5 implies that the standard resolution provides a projective resolution of $\mathbb{Z}$. It follows that

$$H^i(G,A)\cong\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$$

for any $G$-module $A$. Moreover, if $P_\cdot\to\mathbb{Z}\to 0$ is any projective resolution of $\mathbb{Z}$ by $G$-modules, we have that $H^i(G,A)$ is the $i$th cohomology group of the complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\cdot,A)$.

b. By definition, $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$ is the $i$th right derived functor of the functor that takes the value $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)$ on $A$. Note that $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},A)\cong A^G$, the module of $G$-invariants. Therefore, if $0\to A\to I^\cdot$ is any injective $\mathbb{Z}[G]$-resolution of $A$, then $H^i(G,A)$ is the $i$th cohomology group in the sequence

$$0\to(I^0)^G\to(I^1)^G\to(I^2)^G\to\cdots.$$

## 1.4. Homology of groups

In this section, we consider a close relative of group cohomology, known as group homology. Note first that $\mathbb{Z}[G^{i+1}]$ is also a right module over $\mathbb{Z}[G]$ by the diagonal right multiplication by an element of $G$. Up to isomorphism of $G$-modules, this is the same as taking the diagonal left multiplication of $\mathbb{Z}[G^{i+1}]$ by the inverse of an element of $G$.

DEFINITION 1.4.1. The $i$th *homology group* $H_i(G,A)$ of a group $G$ with coefficients in a $G$-module $A$ is defined to be the $i$th homology group $H_i(G,A) = \ker d_i / \operatorname{im} d_{i+1}$ in the complex

$$\cdots \to \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_2} \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1} \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_0} 0$$

induced by the standard resolution.

We note that if $f : A \to B$ is a $G$-module homomorphism, then there are induced maps $f_* : H_i(G,A) \to H_i(G,B)$ for each $i \geq 0$.

REMARK 1.4.2. It follows from Definition 1.4.1 that $H_i(G,A) \cong \operatorname{Tor}^i_{\mathbb{Z}[G]}(\mathbb{Z},A)$ for every $i \geq 0$, and that $H_i(G,A)$ may be calculated by taking the homology of $P_\cdot \otimes_{\mathbb{Z}[G]} A$, where $P_\cdot$ is any projective $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Here, we view $P_i$ as a right $G$-module via the action $x \cdot g = g^{-1}x$ for $g \in G$ and $x \in X$.

As a first example, we have

LEMMA 1.4.3. *We have natural isomorphisms $H_0(G,A) \cong A_G$ for every $G$-module $A$.*

PROOF. Note first that $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \cong A$, and the map $d_1$ under this identification is given by

$$d_1((g_0,g_1) \otimes a) = (g_0 - g_1)a.$$

Hence, the image of $d_1$ is $I_G A$, and the result follows. □

As $A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$, we have in particular that $H_i(G,A)$ is the $i$th left derived functor of $A_G$. As with cohomology, we therefore have in particular that homology carries short exact sequences to long exact sequences, as we now spell out.

THEOREM 1.4.4. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

*is a short exact sequence of $G$-modules. Then there are connecting homomorphisms $\delta_* : H_i(G,C) \to H_{i-1}(G,A)$ and a long exact sequence of abelian groups*

$$\cdots \to H_1(G,C) \xrightarrow{\delta} H_0(G,A) \xrightarrow{\iota_*} H_0(G,B) \xrightarrow{\pi_*} H_0(G,C) \to 0.$$

*Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.*

The following result computes the homology group $H_1(G,\mathbb{Z})$, where $\mathbb{Z}$ has the trivial $G$-action.

PROPOSITION 1.4.5. *There are canonical isomorphisms $H_1(G,\mathbb{Z}) \cong I_G/I_G^2 \cong G^{\mathrm{ab}}$, where $G^{\mathrm{ab}}$ denotes the abelianization of $G$, the latter taking the coset of $g-1$ to the coset of $g \in G$.*

PROOF. Since $\mathbb{Z}[G]$ is $\mathbb{Z}[G]$-projective, we have $H_1(G,\mathbb{Z}[G]) = 0$, and hence our long exact sequence in homology has the form

$$0 \to H_1(G,\mathbb{Z}) \to H_0(G,I_G) \to H_0(G,\mathbb{Z}[G]) \to H_0(G,\mathbb{Z}) \to 0.$$

Note that $H_0(G,I_G) \cong I_G/I_G^2$ and $H_0(G,\mathbb{Z}[G]) \cong \mathbb{Z}[G]/I_G \cong \mathbb{Z}$ via the augmentation map. Since $H_0(G,\mathbb{Z}) \cong \mathbb{Z}$ and any surjective map $\mathbb{Z} \to \mathbb{Z}$ (in this case the identity) is an isomorphism, we obtain the first isomorphism of the proposition.

For the second isomorphism, let us define maps $\phi\colon G^{\mathrm{ab}} \to I_G/I_G^2$ and $\psi\colon I_G/I_G^2 \to G^{\mathrm{ab}}$. For $g \in G$, we set

$$\phi(g[G,G]) = (g-1) + I_G^2,$$

where $[G,G]$ denotes the commutator subgroup of $G$. To see that this is a homomorphism on $G$, hence on $G^{\mathrm{ab}}$, note that

$$(gh-1) + I_G^2 = (g-1) + (h-1) + (g-1)(h-1) + I_G^2 = (g-1) + (h-1) + I_G^2$$

for $g,h \in G$.

Next, define $\psi$ on $\alpha = \sum_{g\in G} a_g g \in I_G$ by

$$\psi(\alpha + I_G^2) = \prod_{g\in G} g^{a_g}[G,G].$$

The order of the product doesn't matter as $G^{\mathrm{ab}}$ is abelian, and $\psi$ is then a homomorphism if well-defined. It suffices for the latter to check that the recipe defining $\psi$ takes the generators $(g-1)(h-1)$ of $I_G^2$ for $g,h \in G$ to the trivial coset, but this follows as $(g-1)(h-1) = gh - g - h + 1$, and for instance, we have

$$gh \cdot g^{-1} \cdot h^{-1} \in [G,G].$$

Finally, we check that the two homomorphisms are inverse to each other. We have

$$\phi(\psi(\alpha + I_G^2)) = \sum_{g\in G} a_g(g-1) + I_G^2 = \alpha + I_G^2$$

since $\alpha \in I_G$ implies $\sum_{g\in G} a_g = 0$, and

$$\psi(\phi(g[G,G])) = \phi((g-1) + I_G^2) = g[G,G].$$

□

## 1.5. Induced modules

DEFINITION 1.5.1. Let $H$ be a subgroup of $G$, and suppose that $B$ is a $\mathbb{Z}[H]$-module. We set

$$\mathrm{Ind}_H^G(B) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B \quad \text{and} \quad \mathrm{CoInd}_H^G(B) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B).$$

We give these $G$-actions by

$$g \cdot (\alpha \otimes b) = (g\alpha) \otimes b \quad \text{and} \quad (g \cdot \varphi)(\alpha) = \varphi(\alpha \cdot g).$$

We say that the resulting modules are *induced* and *coinduced*, respectively, from $H$ to $G$.

REMARK 1.5.2. What we refer to as a "coinduced" module is often actually referred to as an "induced" module.

We may use these modules to interpret $H$-cohomology groups as $G$-cohomology groups.

THEOREM 1.5.3 (Shapiro's Lemma). *For each $i \geq 0$, we have canonical isomorphisms*

$$H_i(G, \mathrm{Ind}_H^G(B)) \cong H_i(H, B) \quad \text{and} \quad H^i(G, \mathrm{CoInd}_H^G(B)) \cong H^i(H, B)$$

*that provide natural isomorphisms of $\delta$-functors.*

PROOF. Let $P_\cdot$ be the standard resolution of $\mathbb{Z}$ by $G$-modules. Define

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$. If $\theta \in \ker \psi_i$, then

$$\theta(x)(g) = (g \cdot \theta(x))(1) = \theta(gx)(1) = 0.$$

for all $x \in P_i$ and $g \in G$, so $\theta = 0$. Conversely, if $\varphi \in \mathrm{Hom}_{\mathbb{Z}[H]}(P_i, B)$, then define $\theta$ by $\theta(x)(g) = \varphi(gx)$, and we have $\psi_i(\theta) = \varphi$.

As for the induced case, note that associativity of tensor products yields

$$P_i \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B) \cong P_i \otimes_{\mathbb{Z}[H]} B,$$

and $P_i = \mathbb{Z}[G^{i+1}]$ is free as a left $H$-module, hence projective. (We leave it to the reader to check that usual $\otimes$-Hom adjunction can be similarly used to give a shorter proof of the result for cohomology.) □

In fact, if $H$ is of finite index in $G$, the notions of induced and coinduced from $H$ to $G$ coincide.

PROPOSITION 1.5.4. *Suppose that $H$ is a subgroup of finite index in $G$ and $B$ is a $H$-module. Then we have a canonical isomorphism of $G$-modules*

$$\chi \colon \mathrm{CoInd}_H^G(B) \xrightarrow{\sim} \mathrm{Ind}_H^G(B), \qquad \chi(\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(g),$$

*where for each $\bar{g} \in H\backslash G$, the element $g \in G$ is an arbitrary choice of representative of $\bar{g}$.*

PROOF. First, we note that $\chi$ is a well-defined map, as

$$(hg)^{-1} \otimes \varphi(hg) = g^{-1}h^{-1} \otimes h\varphi(g) = g \otimes \varphi(g)$$

for $\varphi \in \mathrm{CoInd}_H^G(B)$, $h \in H$, and $g \in G$. Next, we see that $\chi$ is a $G$-module homomorphism, as

$$\chi(g'\varphi) = \sum_{\bar{g} \in H\backslash G} g^{-1} \otimes \varphi(gg') = g' \sum_{\bar{g} \in H\backslash G} (gg')^{-1} \otimes \varphi(gg') = g'\chi(\varphi)$$

for $g' \in G$. As the coset representatives form a basis for $\mathbb{Z}[G]$ as a free $\mathbb{Z}[H]$-module, we may define an inverse to $\chi$ that maps

$$\sum_{\bar{g} \in H\backslash G} g^{-1} \otimes b_g \in \mathrm{Ind}_H^G(B)$$

to the unique $\mathbb{Z}[H]$-linear map $\varphi$ that takes the value $b_g$ on $g$ for the chosen representative of $\bar{g} \in H\backslash G$. □

In the special case of the trivial subgroup, we make the following definition.

DEFINITION 1.5.5. We say that $G$-modules of the form

$$\mathrm{Ind}^G(X) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X \quad \text{and} \quad \mathrm{CoInd}^G(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X),$$

where $X$ is an abelian group, are *induced* and *coinduced* $G$-modules, respectively.

REMARK 1.5.6. Note that Proposition 1.5.4 implies that the notions of induced and coinduced modules coincide for finite groups $G$. On the other hand, for infinite groups, $\mathrm{CoInd}^G(X)$ will never be finitely generated over $\mathbb{Z}[G]$ for nontrivial $X$, while $\mathrm{Ind}^G(X)$ will be for any finitely generated abelian group $X$.

THEOREM 1.5.7. *Suppose that $A$ is an induced (resp., coinduced) $G$-module. Then we have $H_i(G,A) = 0$ (resp., $H^i(G,A) = 0$) for all $i \geq 1$.*

PROOF. Let $X$ be an abelian group. By Shapiro's Lemma, we have

$$H_i(G, \mathrm{Ind}^G(X)) = H_i(\{1\}, X)$$

for $i \geq 1$. Since $\mathbb{Z}$ has a projective $\mathbb{Z}$-resolution by itself, the latter groups are 0. The proof for cohomology is essentially identical. □

DEFINITION 1.5.8. A $G$-module $A$ such that $H^i(G,A) = 0$ for all $i \geq 1$ is called *$G$-acyclic*.

We show that we may construct induced and coinduced $G$-modules starting from abelian groups that are already equipped with a $G$-action.

REMARK 1.5.9. Suppose that $A$ and $B$ are $G$-modules. We give $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ and $A \otimes_{\mathbb{Z}} B$ actions of $G$ by

$$(g \cdot \varphi)(a) = g\varphi(g^{-1}a) \quad \text{and} \quad g \cdot (a \otimes b) = ga \otimes gb,$$

respectively.

LEMMA 1.5.10. *Let $A$ be a $G$-module, and let $A^\circ$ be its underlying abelian group. Then*

$$\mathrm{Hom}_\mathbb{Z}(\mathbb{Z}[G],A) \cong \mathrm{CoInd}^G(A^\circ) \quad \text{and} \quad \mathbb{Z}[G]\otimes_\mathbb{Z} A \cong \mathrm{Ind}^G(A^\circ).$$

PROOF. We define

$$\kappa\colon \mathrm{Hom}_\mathbb{Z}(\mathbb{Z}[G],A) \to \mathrm{CoInd}^G(A^\circ), \qquad \kappa(\varphi)(g) = g\cdot\varphi(g^{-1}).$$

For $g,k\in G$, we then have

$$(k\cdot\kappa(\varphi))(g) = \kappa(\varphi)(gk) = gk\cdot\varphi(k^{-1}g^{-1}) = g\cdot(k\cdot\varphi)(g^{-1}) = \kappa(k\cdot\varphi)(g),$$

so $\kappa$ is a $G$-module homomorphism. Note that $\kappa$ is also self-inverse on the underlying set of both groups, so is an isomorphism. In the induced case, we define

$$\nu\colon \mathbb{Z}[G]\otimes_\mathbb{Z} A \to \mathrm{Ind}^G(A^\circ), \qquad \nu(g\otimes a) = g\otimes g^{-1}a.$$

For $g,k\in G$, we now have

$$k\cdot\nu(g\otimes a) = (kg)\otimes g^{-1}a = \nu(kg\otimes ka) = \nu(k\cdot(g\otimes a)),$$

so $\nu$ is a $G$-module isomorphism with inverse $\nu^{-1}(g\otimes a) = g\otimes ga$. □

REMARK 1.5.11. Noting the lemma, we will simply refer to $\mathrm{Hom}_\mathbb{Z}(\mathbb{Z}[G],A)$ as $\mathrm{CoInd}^G(A)$ and $\mathbb{Z}[G]\otimes_\mathbb{Z} A$ as $\mathrm{Ind}^G(A)$.

## 1.6. Tate cohomology

We suppose in this section that $G$ is a finite group. In this case, recall that we have the norm element $N_G\in\mathbb{Z}[G]$, which defines by left multiplication a map $N_G\colon A\to A$ on any $G$-module $A$. Its image $N_GA$ is the *group of $G$-norms* of $A$.

LEMMA 1.6.1. *The norm element induces a map $\bar{N}_G\colon A_G\to A^G$.*

PROOF. We have $N_G((g-1)a)=0$ for any $g\in G$ and $a\in A$, so the map factors through $A_G$, and clearly $\mathrm{im}N_G\subseteq A^G$. □

DEFINITION 1.6.2. We let $\hat{H}^0(G,A)$ (resp., $\hat{H}_0(G,A)$) denote the cokernel (resp., kernel) of the map in Lemma 1.6.1. In other words,

$$\hat{H}^0(G,A) = A^G/N_GA \quad \text{and} \quad \hat{H}_0(G,A) = {}_NA/I_GA,$$

where ${}_NA$ denotes the kernel of the left multiplication by $N_G$ on $A$.

EXAMPLE 1.6.3. Consider the case that $A=\mathbb{Z}$, where $\mathbb{Z}$ is endowed with a trivial action of $G$. Since $N_G\colon\mathbb{Z}\to\mathbb{Z}$ is just the multiplication by $|G|$ map, we have that $\hat{H}^0(G,\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ and $\hat{H}_0(G,\mathbb{Z}) = 0$.

REMARK 1.6.4. In general, when we take cohomology with coefficients in a group, like $\mathbb{Z}$ or $\mathbb{Q}$, with no specified action of the group $G$, the action is taken to be trivial.

The Tate cohomology groups are an amalgamation of the homology groups and cohomology groups of $G$, with the homology groups placed in negative degrees.

DEFINITION 1.6.5. Let $G$ be a finite group and $A$ a $G$-module. For any $i \in \mathbb{Z}$, we define the *ith Tate cohomology group* by

$$\hat{H}^i(G,A) = \begin{cases} H_{-i-1}(G,A) & \text{if } i \leq -2 \\ \hat{H}_0(G,A) & \text{if } i = -1 \\ \hat{H}^0(G,A) & \text{if } i = 0 \\ H^i(G,A) & \text{if } i \geq 1. \end{cases}$$

We have modified the zeroth homology and cohomology groups in defining Tate cohomology so that we obtain long exact sequences from short exact sequences as before, but extending infinitely in both directions, as we shall now see.

THEOREM 1.6.6 (Tate). *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

*is a short exact sequence of G-modules. Then there is a long exact sequence of abelian groups*

$$\cdots \to \hat{H}^i(G,A) \xrightarrow{\iota} \hat{H}^i(G,B) \xrightarrow{\pi} \hat{H}^i(G,C) \xrightarrow{\delta} \hat{H}^{i+1}(G,A) \to \cdots.$$

*Moreover, this construction is natural in the short exact sequence in the sense that any morphism of short exact sequences gives rise to a morphism of long exact sequences.*

PROOF. The first part follows immediately from applying the snake lemma to the following diagram, which in particular defines the map $\delta$ on $\hat{H}^{-1}(G,C)$:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & H_1(G,C) & \xrightarrow{\delta} & H_0(G,A) & \xrightarrow{\iota_*} & H_0(G,B) & \xrightarrow{\pi_*} & H_0(G,C) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \downarrow{\scriptstyle \bar{N}_G} & & \\ & & 0 & \longrightarrow & H^0(G,A) & \xrightarrow{\iota_*} & H^0(G,B) & \xrightarrow{\pi_*} & H^0(G,C) & \xrightarrow{\delta} & H^1(G,A) \longrightarrow \cdots, \end{array}$$

and the second part is easily checked. □

Tate cohomology groups have the interesting property that they vanish entirely on induced modules.

PROPOSITION 1.6.7. *Suppose that A is an induced G-module. Then $\hat{H}^i(G,A) = 0$ for all $i \in \mathbb{Z}$.*

PROOF. By Theorem 1.5.7 and Proposition 1.5.4, it suffices to check this for $i = -1$ and $i = 0$. Let $X$ be an abelian group. Since $\mathbb{Z}[G]^G = N_G\mathbb{Z}[G]$, we have

$$H^0(G, \mathrm{Ind}^G(X)) = N_G\mathbb{Z}[G] \otimes_{\mathbb{Z}} X,$$

so $\hat{H}^0(G, \mathrm{Ind}^G(X)) = 0$ by definition. We also have that

$$H_0(G, \mathrm{Ind}^G(X)) = (\mathbb{Z}[G] \otimes_{\mathbb{Z}} X)_G \cong \mathbb{Z} \otimes_{\mathbb{Z}} X \cong X. \tag{1.6.1}$$

Let $\alpha = \sum_{g\in G}(g \otimes x_g)$ be an element of $\mathrm{Ind}^G(X)$. Then

$$N_G\alpha = N_G \otimes \sum_{g\in G} x_g$$

is trivial if and only if $\sum_{g\in G} x_g = 0$, which by the identification in (1.6.1) is to say that $\alpha$ has trivial image in $H_0(G, \mathrm{Ind}^G(X))$. Hence $\hat{H}_0(G, \mathrm{Ind}^G(X)) = 0$ as well. □

The Tate cohomology groups can also be computed via a doubly infinite resolution of $G$-modules. The proof of this is rather involved and requires some preparation.

LEMMA 1.6.8. *Let $X$ be a $G$-module that is free of finite rank over $\mathbb{Z}$, and let $A$ be any $G$-module. Then the map*

$$\nu\colon X \otimes_{\mathbb{Z}} A \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), A), \qquad \nu(x \otimes a)(\varphi) = \varphi(x)a$$

*is an isomorphism of $G$-modules.*

PROOF. We note that

$$\nu(g \cdot (x \otimes a))(\varphi) = \varphi(gx)ga,$$

while

$$(g \cdot \nu(x \otimes a))(\varphi) = g\nu(x \otimes a)(g^{-1}\varphi) = (g^{-1}\varphi)(x)ga = \varphi(gx)ga,$$

so $\nu$ is a homomorphism of $G$-modules.

Let $x_1, \ldots, x_m$ be any $\mathbb{Z}$-basis of $X$, and let $x_1^*, \ldots, x_m^*$ be the dual basis of $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$ such that $x_i^*(x_j) = \delta_{ij}$ for $1 \le i, j \le m$. We define

$$\omega\colon \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), A) \to X \otimes_{\mathbb{Z}} A, \qquad \omega(\psi) = \sum_{i=1}^{m} x_i \otimes \psi(x_i^*).$$

Then

$$(\nu \circ \omega)(\psi)(\varphi) = \nu\left(\sum_{i=1}^{m} x_i \otimes \psi(x_i^*)\right)(\varphi) = \sum_{i=1}^{m} \varphi(x_i)\psi(x_i^*) = \psi\left(\sum_{i=1}^{m} \varphi(x_i)x_i^*\right) = \psi(\varphi).$$

On the other hand,

$$(\omega \circ \nu)(x \otimes a) = \sum_{i=1}^{m} x_i \otimes x_i^*(x)a = \sum_{i=1}^{m} x_i^*(x)x_i \otimes a = x \otimes a.$$

Hence, $\nu$ is an isomorphism. □

LEMMA 1.6.9. *Let $X$ and $A$ be $G$-modules, and endow $X$ with a right $G$-action by $x \cdot g = g^{-1}x$. Then we have a canonical isomorphism*

$$X \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (X \otimes_{\mathbb{Z}} A)_G$$

*induced by the identity on $X \otimes_{\mathbb{Z}} A$.*

PROOF. First, note that $X \otimes_{\mathbb{Z}[G]} A$ is a quotient of the $G$-module $X \otimes_{\mathbb{Z}} A$, which is endowed the diagonal left $G$-action. By definition of the tensor product over $\mathbb{Z}[G]$, we have

$$g^{-1}x \otimes a = x \cdot g \otimes a = x \otimes ga,$$

so $G$ acts trivially on $X \otimes_{\mathbb{Z}[G]} A$, and hence the latter group is a quotient of $(X \otimes_{\mathbb{Z}} A)_G$. On the other hand, the $\mathbb{Z}$-bilinear map

$$X \times A \to (X \otimes_{\mathbb{Z}} A)_G, \qquad (x,a) \mapsto x \otimes a$$

is $\mathbb{Z}[G]$-balanced, hence induces a map on the tensor product inverse to the above-described quotient map. □

We are now ready to prove the theorem.

THEOREM 1.6.10. *Let $P_\cdot \xrightarrow{\alpha} \mathbb{Z}$ be a projective resolution by $G$-modules of finite $\mathbb{Z}$-rank, and consider the $\mathbb{Z}$-dual $\mathbb{Z} \xrightarrow{\hat{\alpha}} P_*^\cdot$, where $P_*^i = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$ for $i \geq 0$ and $G$ acts on $P_*^i$ by $(g \cdot \varphi)(x) = \psi(g^{-1}x)$. Let $Q_\cdot$ be the exact chain complex*

$$\cdots \to P_1 \to P_0 \xrightarrow{\hat{\alpha} \circ \alpha} P_*^0 \to P_*^1 \to \cdots,$$

*where $P_0$ occurs in degree 0. (That is, we set $Q_i = P_i$ for $i \geq 0$ and $Q_i = P_*^{-1-i}$ for $i < 0$.) For any $G$-module $A$, the Tate cohomology group $\hat{H}^i(G,A)$ is the $i$th cohomology group of the cochain complex $C^\cdot = \mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$.*

PROOF. As $P_i$ is projective over $\mathbb{Z}[G]$, it is in particular $\mathbb{Z}$-free, so the $\mathbb{Z}$-dual sequence $\mathbb{Z} \to P_*^\cdot$ is still exact. Let us denote the $i$th differential on $P_i$ by $d_i$ and its $\mathbb{Z}$-dual by $\hat{d}^i$. We check exactness at $Q_0$ and $Q_{-1}$. Let $\beta = \hat{\alpha} \circ \alpha$. By definition, $\mathrm{im}\, d_1 = \ker \alpha$, and as $\hat{\alpha}$ is injective, we have $\mathrm{im}\, d_1 = \ker \beta$. Similarly, we have $\ker \hat{d}^0 = \mathrm{im}\, \hat{\alpha}$, and as $\alpha$ is surjective, we have $\ker \hat{d}^0 = \mathrm{im}\, \beta$. Therefore, $Q_\cdot$ is exact.

That $\mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ computes the Tate cohomology groups $\hat{H}^i(G,A)$ follows immediately from the definition for $i \geq 1$. By Lemma 1.6.9, we have an isomorphism

$$P_i \otimes_{\mathbb{Z}[G]} A \xrightarrow{\sim} (P_i \otimes_{\mathbb{Z}} A)_G.$$

By Proposition 1.6.7 and Lemma 1.5.10, we have that

$$(P_i \otimes_{\mathbb{Z}} A)_G \xrightarrow{\bar{N}_G} (P_i \otimes_{\mathbb{Z}} A)^G$$

is an isomorphism as well, and following this by the restriction

$$(P_i \otimes_{\mathbb{Z}} A)^G \to \mathrm{Hom}_{\mathbb{Z}}(P^i_*, A)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(P^i_*, A)$$

of the map $\nu$ of Lemma 1.6.8, we obtain in summary an isomorphism

$$\chi_i \colon P_i \otimes_{\mathbb{Z}[G]} A \to \mathrm{Hom}_{\mathbb{Z}[G]}(P^i_*, A).$$

Next, we check that the maps $\nu$ of Lemma 1.6.8 commute with the differentials on the complexes $P_\cdot \otimes_{\mathbb{Z}} A$ and $\mathrm{Hom}_{\mathbb{Z}}(P_*^\cdot, A)$, the former of which are just the tensor products of the differentials $d_i$ on the $P_i$ with the identity (then also denoted $d_i$), and the latter of which are double duals $\tilde{d}_i$ of the $d_i$, i.e., which satisfy

$$\tilde{d}_i(\psi)(\varphi) = \psi(\varphi \circ d_i),$$

for $\psi \in \mathrm{Hom}_{\mathbb{Z}}(P^i_*, A)$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(P_{i-1}, \mathbb{Z})$. We have

$$(\nu \circ d_i)(x \otimes a)(\varphi) = \nu(d_i(x) \otimes a)(\varphi) = \varphi(d_i(x))a.$$

On the other hand, we have

$$(\tilde{d}_i \circ \nu)(x \otimes a)(\varphi) = \tilde{d}_i(\nu(x \otimes a))(\varphi) = \nu(x \otimes a)(\varphi \circ d_i) = \varphi(d_i(x))a,$$

as desired. Moreover, the $d_i$ commute with $\bar{N}_G$ on $(P_i \otimes_{\mathbb{Z}} A)_G$, being that they are $G$-module maps. Hence, the maps $\chi_i$ for all $i$ together provide an isomorphism of complexes. In particular, the $i$th cohomology group of $\mathrm{Hom}_{\mathbb{Z}[G]}(Q_\cdot, A)$ is $\hat{H}^i(G, A)$ for all $i \leq -2$, and we already knew this for all $i \geq 1$.

It remains to consider the cases $i = 0, -1$. We need to compute the cohomology of

$$P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \xrightarrow{\tau} \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \tag{1.6.2}$$

in the middle two degrees, and

$$\tau(x \otimes a)(y) = (\chi_0(x \otimes a) \circ \hat{\alpha} \circ \alpha)(y) = \sum_{g \in G} (\hat{\alpha} \circ \alpha)(y)(gx)ga = \sum_{g \in G} \alpha(y)\alpha(x)ga,$$

noting that $\alpha(gx) = \alpha(x)$ for every $g \in G$ and $\hat{\alpha}(n)(x) = n\alpha(x)$ for every $n \in \mathbb{Z}$. On the other hand, viewing $\alpha$ and $\hat{\alpha}$ as inducing maps

$$\lambda \colon P_0 \otimes_{\mathbb{Z}[G]} A \to A_G \quad \text{and} \quad \hat{\lambda} \colon A^G \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A),$$

respectively, we have

$$\begin{aligned}(\hat{\lambda} \circ \bar{N}_G \circ \lambda)(x \otimes a)(y) = \hat{\lambda}(\bar{N}_G(\alpha(x)a))(y) = \hat{\lambda}\Big(\sum_{g \in G} \alpha(x)ga\Big)(y) \\ = \sum_{g \in G} \hat{\alpha}(\alpha(x))(y)ga = \sum_{g \in G} \alpha(x)\alpha(y)ga.\end{aligned}$$

In other words, we have $\tau = \hat{\lambda} \circ \bar{N}_G \circ \lambda$. As the cokernel of the first map in (1.6.2) is $H_0(G, A) = A_G$ and the kernel of the last is $H^0(G, A) = A^G$, with these identifications given by the maps $\lambda$ and

$\hat{\lambda}$ respectively, we have that the complex given by $A_G \xrightarrow{\bar{N}_G} A^G$ in degrees $-1$ and $0$ computes the cohomology groups in question, as desired. □

As what is in essence a corollary, we have the following version of Shapiro's lemma.

THEOREM 1.6.11. *Let $G$ be a finite group, let $H$ be a subgroup, and let $B$ be an $H$-module. Then for every $i \in \mathbb{Z}$, we have canonical isomorphisms*

$$\hat{H}^i(G, \mathrm{CoInd}_H^G(B)) \cong \hat{H}^i(H, B)$$

*that together provide natural isomorphisms of $\delta$-functors.*

PROOF. The proof is nearly identical to that of Shapiro's lemma for cohomology groups. That is, we may simply use the isomorphisms induced by

$$\psi_i \colon \mathrm{Hom}_{\mathbb{Z}[G]}(Q_i, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(Q_i, B)$$

by $\psi_i(\theta)(x) = \theta(x)(1)$, for $Q_\cdot$ the doubly infinite resolution of $\mathbb{Z}$ for $G$ of Theorem 1.6.10. □

## 1.7. Dimension shifting

One useful technique in group cohomology is that of dimension shifting. The key idea here is to use the acyclicity of coinduced modules to obtain isomorphisms among cohomology groups.

To describe this technique, note that we have a short exact sequence

$$0 \to A \xrightarrow{\iota} \mathrm{CoInd}^G(A) \to A^* \to 0, \tag{1.7.1}$$

where $\iota$ is defined by $\iota(a)(g) = a$ for $a \in A$ and $g \in G$, and $A^*$ is defined to be the cokernel of $\iota$. We also have a short exact sequence

$$0 \to A_* \to \mathrm{Ind}^G(A) \xrightarrow{\pi} A \to 0, \tag{1.7.2}$$

where $\pi$ is defined by $\pi(g \otimes a) = a$ for $a \in A$ and $g \in G$, and $A_*$ is defined to be the kernel of $\pi$.

REMARK 1.7.1. If we view $A$ as $\mathbb{Z} \otimes_{\mathbb{Z}} A$, we see by the freeness of $\mathbb{Z}$ as a $\mathbb{Z}$-module and the definition of $\mathrm{Ind}^G(A)$ that $A_* \cong I_G \otimes_{\mathbb{Z}} A$ with a diagonal action of $G$. Moreover, viewing $A$ as $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$, we see that $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$.

PROPOSITION 1.7.2. *With the notation as above, we have*

$$H^{i+1}(G, A) \cong H^i(G, A^*) \quad \text{and} \quad H_{i+1}(G, A) \cong H_i(G, A_*)$$

*for all $i \geq 1$.*

PROOF. By Lemma 1.5.10, we know that $\mathrm{CoInd}^G(A)$ (resp., $\mathrm{Ind}^G(A)$) is coinduced (resp., induced). The result then follows easily by Theorem 1.5.7 and the long exact sequences of Theorems 1.2.13 and 1.4.4. □

For Tate cohomology groups, we have an even cleaner result.

THEOREM 1.7.3 (Dimension shifting). *Suppose that $G$ is finite. With the above notation, we have*

$$\hat{H}^{i+1}(G,A) \cong \hat{H}^i(G,A^*) \quad \text{and} \quad \hat{H}^{i-1}(G,A) \cong \hat{H}^i(G,A_*)$$

*for all $i \in \mathbb{Z}$.*

PROOF. Again noting Lemma 1.5.10, it follows from Theorem 1.5.4 and Proposition 1.6.7 that the long exact sequences associated by Theorem 1.6.6 to the short exact sequences in (1.7.1) and (1.7.2) reduce to the isomorphisms in question. □

This result allows us to transfer questions about cohomology groups in a certain degree to analogous questions regarding cohomology groups in other degrees. Let us give a first application.

PROPOSITION 1.7.4. *Suppose that $G$ is a finite group and $A$ is a $G$-module. Then the groups $\hat{H}^i(G,A)$ have exponent dividing $|G|$ for every $i \in \mathbb{Z}$.*

PROOF. By Theorem 1.7.3, the problem immediately reduces to proving the claim for $i = 0$ and every module $A$. But for any $a \in A^G$, we have $|G|a = N_G a$, so $\hat{H}^0(G,A)$ has exponent dividing $|G|$. □

This has the following important corollary.

COROLLARY 1.7.5. *Suppose that $G$ is a finite group and $A$ is a $G$-module that is finitely generated as an abelian group. Then $\hat{H}^i(G,A)$ is finite for every $i \in \mathbb{Z}$.*

PROOF. We know that $\hat{H}^i(G,A)$ is a subquotient of the finitely generated abelian group $Q_i \otimes_{\mathbb{Z}[G]} A$ of Theorem 1.6.10, hence is itself finitely generated. As it has finite exponent, it is therefore finite. □

We also have the following.

COROLLARY 1.7.6. *Suppose that $G$ is finite. Suppose that $A$ is a $G$-module on which multiplication by $|G|$ is an isomorphism. Then $\hat{H}^i(G,A) = 0$ for $i \in \mathbb{Z}$.*

PROOF. Multiplication by $|G|$ on $A$ induces multiplication by $|G|$ on Tate cohomology, which is then an isomorphism. Since by Proposition 1.7.4, multiplication by $|G|$ is also the zero map on Tate cohomology, the Tate cohomology groups must be 0. □

## 1.8. Comparing cohomology groups

DEFINITION 1.8.1. Let $G$ and $G'$ be groups, $A$ a $G$-module and $A'$ a $G'$-module. We say that a pair $(\rho, \lambda)$ with $\rho : G' \to G$ and $\lambda : A \to A'$ group homomorphisms is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a).$$

Compatible pairs are used to provide maps among cohomology groups.

PROPOSITION 1.8.2. *Suppose that $\rho\colon G' \to G$ and $\lambda\colon A \to A'$ form a compatible pair. Then the maps*

$$C^i(G,A) \to C^i(G',A'), \qquad f \mapsto \lambda \circ f \circ (\rho \times \cdots \times \rho)$$

*induce maps on cohomology $H^i(G,A) \to H^i(G',A')$ for all $i \geq 0$.*

PROOF. One need only check that this is compatible with differentials, but this is easily done using compatibility of the pair. That is, if $f'$ is the image of $f$, then to show that

$$d^i f'(g'_0,\ldots,g'_i) = \lambda(d^i f(\rho(g'_0),\ldots,\rho(g'_i))),$$

immediately reduces to showing that the first terms on both sides arising from the expression for the definition of the differential are equal. Since the pair is compatible, we have

$$g'_0 f'(g'_1,\ldots g'_i) = g'_0\lambda(f(\rho(g'_1),\ldots,\rho(g'_i))) = \lambda(\rho(g'_0)f(\rho(g'_1),\ldots,\rho(g'_i))),$$

as desired. □

REMARK 1.8.3. Using the standard resolution, we have a homomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}],A) \to \mathrm{Hom}_{\mathbb{Z}[G']}(\mathbb{Z}[(G')^{i+1}],A'), \qquad \psi \mapsto \lambda \circ \psi \circ (\rho \times \cdots \times \rho)$$

attached to a compatible pair $(\rho,\lambda)$ that is compatible with the map on cochains.

REMARK 1.8.4. Given a third group $G''$, a $G''$-module $A''$, and compatible pair $(\rho',\lambda')$ with $\rho'\colon G'' \to G'$ and $\lambda'\colon A' \to A''$, we may speak of the composition $(\rho\circ\rho',\lambda'\circ\lambda)$, which will be a compatible pair that induces the morphism on complexes that is the composition of the morphisms arising from the pairs $(\rho,\lambda)$ and $(\rho',\lambda')$.

EXAMPLE 1.8.5. In Shapiro's Lemma, the inclusion map $H \hookrightarrow G$ and the evaluation at 1 map $\mathrm{CoInd}_H^G(B) \to B$ form a compatible pair inducing the isomorphisms in its statement.

We consider two of the most important examples of compatible pairs, and the maps on cohomology arising from them.

DEFINITION 1.8.6. Let $H$ be a subgroup of $G$. Let $A$ be a $G$-module.

a. Let $e\colon H \hookrightarrow G$ be the natural inclusion map. Then the maps

$$\mathrm{Res}\colon H^i(G,A) \to H^i(H,A)$$

induced by the compatible pair $(e,\mathrm{id}_A)$ on cohomology are known as *restriction maps*.

b. Suppose that $H$ is normal in $G$. Let $q\colon G \to G/H$ be the quotient map, and let $\iota\colon A^H \to A$ be the inclusion map. Then the maps

$$\mathrm{Inf}\colon H^i(G/H,A^H) \to H^i(G,A)$$

induced by the compatible pair $(q,\iota)$ are known as *inflation maps*.

REMARK 1.8.7. Restriction of an $i$-cocycle is just simply that, it is the restriction of the map $f\colon G^i \to A$ to a map $\mathrm{Res}(f)\colon H^i \to A$ given by $\mathrm{Res}(f)(h) = f(h)$ for $h \in H^i$. Inflation of an $i$-cocycle is just as simple: $\mathrm{Inf}(f)(g) = f(\bar{g})$, for $g \in G^i$ and $\bar{g}$ its image in $(G/H)^i$.

EXAMPLE 1.8.8. In degree 0, the restriction map $\mathrm{Res}\colon A^G \to A^H$ is simply inclusion, and the inflation map $\mathrm{Inf}\colon (A^H)^{G/H} \to A^G$ is the identity.

REMARKS 1.8.9.

a. Restriction provides a morphism of $\delta$-functors. That is, it provides a sequence of natural transformations between the functors $H^i(G,\cdot)$ and $H^i(H,\cdot)$ on $G$-modules (which is to say that restriction commutes with $G$-module homomorphisms) such that for any short exact sequence of $G$-modules, the maps induced by the natural transformations commute with the connecting homomorphisms in the two resulting long exact sequences.

b. We could merely have defined restriction for $i = 0$ and used dimension shifting to define it for all $i \geq 1$, as follows from the previous remark.

THEOREM 1.8.10 (Inflation-Restriction Sequence). *Let $G$ be a group and $N$ a normal subgroup. Let $A$ be a $G$-module. Then the sequence*

$$0 \to H^1(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(N,A)$$

*is exact.*

PROOF. The injectivity of inflation on cocycles obvious from Remark 1.8.7. Let $f$ be a cocycle in $Z^1(G/N, A^N)$. If $f(\bar{g}) = (g-1)a$ for some $a \in A$ and all $g \in G$, then $a \in A^N$ as $f(\bar{1}) = 0$, so Inf is injective. Also, note that $\mathrm{Res} \circ \mathrm{Inf}(f)(n) = f(\bar{n}) = 0$ for all $n \in N$.

Let $f' \in Z^1(G,A)$ and suppose $\mathrm{Res}(f') = 0$. Then there exists $a \in A$ such that $f'(n) = (n-1)a$ for all $n \in N$. Define $k \in Z^1(G,A)$ by $k(g) = f'(g) - (g-1)a$. Then $k(n) = 0$ for all $n \in N$. We then have

$$k(gn) = gk(n) + k(g) = k(g)$$

for all $g \in G$ and $n \in N$, so $k$ factors through $G/N$. Also,

$$k(g) = k(g \cdot g^{-1}ng) = k(ng) = nk(g) + k(n) = nk(g),$$

so $k$ has image in $A^N$. Therefore, $k$ is the inflation of a cocycle in $Z^1(G/N, A^N)$, proving exactness. □

In fact, under certain conditions, we have an inflation-restriction sequence on the higher cohomology groups.

PROPOSITION 1.8.11. *Let $G$ be a group and $N$ a normal subgroup. Let $A$ be a $G$-module. Let $i \geq 1$, and suppose that $H^j(N,A) = 0$ for all $1 \leq j \leq i-1$. Then the sequence*

$$0 \to H^i(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^i(G,A) \xrightarrow{\mathrm{Res}} H^i(N,A)$$

*is exact.*

PROOF. Let $A^*$ be as in (1.7.1). By Theorem 1.8.10, we may assume that $i \geq 2$. Since $H^1(N,A) = 0$, we have an exact sequence

$$0 \to A^N \to \mathrm{CoInd}^G(A)^N \to (A^*)^N \to 0 \tag{1.8.1}$$

in $N$-cohomology. Moreover, noting Lemma 1.5.10, we have that

$$\mathrm{CoInd}^G(A)^N \cong \mathrm{Hom}_{\mathbb{Z}[N]}(\mathbb{Z}[G],A^\circ) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/N],A^\circ) \cong \mathrm{CoInd}^{G/N}(A),$$

where $A^\circ$ is the abelian group $A$ with a trivial $G$-action. Thus, the connecting homomorphism

$$\delta^{i-1}\colon H^{i-1}(G/N,(A^*)^N) \xrightarrow{\sim} H^i(G/N,A^N)$$

in the $G/N$-cohomology of (1.8.1) is an isomorphism for $i \geq 2$.

Consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{i-1}(G/N,(A^*)^N) & \xrightarrow{\mathrm{Inf}} & H^{i-1}(G,A^*) & \xrightarrow{\mathrm{Res}} & H^{i-1}(N,A^*) \\ & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} & & \downarrow{\scriptstyle \delta^{i-1}} \\ 0 & \longrightarrow & H^i(G/N,A^N) & \xrightarrow{\mathrm{Inf}} & H^i(G,A) & \xrightarrow{\mathrm{Res}} & H^i(N,A). \end{array} \tag{1.8.2}$$

We have already seen that the leftmost vertical map in (1.8.2) is an isomorphism, and since $\mathrm{CoInd}^G(A)$ is an coinduced $G$-module, the central vertical map in (1.8.2) is an isomorphism. Moreover, as a coinduced $G$-module, $\mathrm{CoInd}^G(A)$ is also coinduced as an $N$-module, and therefore the rightmost vertical map in (1.8.2) is also an isomorphism. Therefore, the lower row of (1.8.2) will be exact if the top row is. But the top row is exact by Theorem 1.8.10 if $i = 2$, and by induction if $i > 2$, noting that

$$H^{j-1}(N,A^*) \cong H^j(N,A) = 0$$

for all $j < i$. □

We consider one other sort of compatible pair, which is conjugation.

PROPOSITION 1.8.12. *Let $A$ be a $G$-module.*

*a. Let $H$ be a subgroup of $G$. Let $g \in G$, and define $\rho_g\colon gHg^{-1} \to H$ by $\rho_g(k) = g^{-1}kg$ for $k \in gHg^{-1}$. Define $\lambda_g\colon A \to A$ by $\lambda_g(a) = ga$. Then $(\rho_g,\lambda_g)$ forms a compatible pair, and we denote by $g^*$ the resulting map*

$$g^*\colon H^i(H,A) \to H^i(gHg^{-1},A).$$

*We have $g_1^* \circ g_2^* = (g_1 \circ g_2)^*$ for all $g_1, g_2 \in G$.*

*b. Suppose that $N$ is normal in $G$. Then $H^i(N,A)$ is a $G$-module, where $g \in G$ acts as $g^*$. We refer to the above action as the conjugation action of $G$. The conjugation action factors through the quotient $G/N$ and turns $N$-cohomology into a $\delta$-functor from the category of $G$-modules to the category of $(G/N)$-modules.*

*c. The action of conjugation commutes with restriction maps among subgroups of G, which is to say that if $K \leq H \leq G$ and $g \in G$, then the diagram*

$$\begin{array}{ccc} H^i(H,A) & \xrightarrow{\text{Res}} & H^i(K,A) \\ \downarrow{\scriptstyle g^*} & & \downarrow{\scriptstyle g^*} \\ H^i(gHg^{-1},A) & \xrightarrow{\text{Res}} & H^i(gKg^{-1},A) \end{array}$$

*commutes.*

PROOF.

a. First, we need check compatibility:

$$\lambda_g(\rho_g(h)a) = g \cdot g^{-1}hga = hga = h\lambda_g(a).$$

Next, we have

$$\lambda_{g_1g_2} = \lambda_{g_1} \circ \lambda_{g_2} \quad \text{and} \quad \rho_{g_1g_2} = \rho_{g_2} \circ \rho_{g_1},$$

so by Remark 1.8.4, composition is as stated.

b. Suppose that $\kappa\colon A \to B$ is a $G$-module homomorphism. If $\alpha \in H^i(N,A)$ is the class of $f \in Z^i(N,A)$, then $\kappa^* \circ g^*(\alpha)$ is the class of

$$(n_1,\ldots,n_i) \mapsto \kappa(gf(g^{-1}n_1g,\ldots,g^{-1}n_ig)) = g\kappa(f(g^{-1}n_1g,\ldots,g^{-1}n_ig)),$$

and so has class $g^* \circ \kappa^*(\alpha)$.

Moreover, if

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of $G$-modules, then let

$$\delta\colon H^i(N,C) \to H^{i+1}(N,A)$$

Let $\gamma \in H^i(N,C)$. We must show that $\delta \circ g^*(\gamma) = g^* \circ \delta(\gamma)$. Since $\iota$ and $\pi$ are $G$-module maps, by what we showed above, we need only show that the differential on $C^i(N,B)$ commutes with the map $g^{\cdot}$ induced by $g$ on cochains. Let $z \in C^i(N,B)$. Then

$$\begin{aligned} g^{\cdot} \circ d^i(z)(n_0,\ldots,n_i) &= gd^i(z)(g^{-1}n_0g,\ldots,g^{-1}n_ig) \\ &= n_0gz(g^{-1}n_0g,\ldots,g^{-1}n_ig) + \sum_{j=1}^{i}(-1)^j f(g^{-1}n_0g,\ldots,g^{-1}n_{j-1}n_jg,\ldots,g^{-1}n_ig) \\ &\qquad + (-1)^{i+1}f(g^{-1}n_0g,\ldots,g^{-1}n_{i-1}g) = d^i(g^*(z))(n_0,\ldots,n_i). \end{aligned}$$

It only remains to show that the restriction of the action of $G$ on Tate cohomology to $N$ is trivial. This is easily computed on $H^0$: for $a \in A^N$ and $n \in N$, we have $n^*(a) = na = a$. In general, let $A^*$ be as in (1.7.1) for the group $G$. The diagram

$$\begin{array}{ccc} H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A) \\ \downarrow{\scriptstyle n^*} & & \downarrow{\scriptstyle n^*} \\ H^i(N,A^*) & \xrightarrow{\delta} & H^{i+1}(N,A), \end{array}$$

which commutes what we have already shown. Assuming that $n^*$ is the identity on $H^i(N,B)$ for every $G$-module $B$ by induction (and in particular for $B = A^*$), we then have that $n^*$ is the identity on $H^{i+1}(N,A)$ as well.

c. Noting Remark 1.8.4, it suffices to check that the compositions of the compatible pairs in question are equal, which is immediate from the definitions.

□

We note the following corollary.

COROLLARY 1.8.13. *The conjugation action of $G$ on $H^i(G,A)$ is trivial for all $i$: that is,*

$$g^* \colon H^i(G,A) \to H^i(G,A)$$

*is just the identity for all $g \in G$ and $i \geq 0$.*

On homology, the analogous notion of a compatible pair is a pair $(\rho, \lambda)$ where $\rho \colon G \to G'$ and $\lambda : A \to A'$ are group homomorphisms satisfying

$$\lambda(ga) = \rho(g)\lambda(a) \tag{1.8.3}$$

for all $g \in G$ and $a \in A$. These then provide morphisms

$$\tilde{\rho} \otimes \lambda \colon \mathbb{Z}[G^{i+1}] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z}[(G')^{i+1}] \otimes_{\mathbb{Z}[G']} A',$$

where $\tilde{\rho}$ is the induced map $\mathbb{Z}[G^{i+1}] \to \mathbb{Z}[(G')^{i+1}]$. By the homological compatibility of (1.8.3), these are seen to be compatible with the differentials, providing maps

$$H_i(G,A) \to H_i(G',A')$$

for all $i \geq 0$. As a consequence, we may make the following definition.

DEFINITION 1.8.14. For $i \geq 0$ and a subgroup $H$ of $G$, the *corestriction maps*

$$\mathrm{Cor} \colon H_i(H,A) \to H_i(G,A)$$

are defined to be the maps induced by the compatible pair $(e, \mathrm{id}_A)$, where $e \colon H \to G$ is the natural inclusion map.

EXAMPLE 1.8.15. In degree 0, corestriction $\mathrm{Cor}\colon A_H \to A_G$ is just the quotient map.

DEFINITION 1.8.16. For $i \geq 0$ and a normal subgroup $H$ of $G$, the *coinflation maps*

$$\mathrm{CoInf}\colon H_i(G,A) \to H_i(G/H, A_H)$$

are defined to be the maps induces by the compatible pair $(q,\pi)$, where $q\colon G \to G/H$ and $\pi\colon A \to A_H$ are the quotient maps.

REMARK 1.8.17. For a $G$-module $A$ and any normal subgroup $H$ of $G$, the sequence

$$H_1(H,A) \xrightarrow{\mathrm{Cor}} H_1(G,A) \xrightarrow{\mathrm{CoInf}} H_1(G/H, A_H) \to 0.$$

is exact.

REMARK 1.8.18. For a subgroup $H$ of $G$, the pair $(\rho_g^{-1}, \lambda_g)$ is a compatible pair for $H$-homology, inducing conjugation maps

$$g_*\colon H_i(H,A) \to H_i(gHg^{-1}, A).$$

If $H$ is a normal subgroup, then these again provide a $(G/H)$-action on $H_i(H,A)$ and turn $H$-homology into a $\delta$-functor. Conjugation commutes with corestriction on subgroups of $G$.

If $H$ is of finite index in $G$, then we may define restriction maps on homology and corestriction maps on cohomology as well. If $G$ is finite, then we obtain restriction and corestriction maps on all Tate cohomology groups as well. Let us first explain this latter case, as it is a bit simpler. Take, for instance, restriction. We have

$$\mathrm{Res}\colon H^i(G,A) \to H^i(H,A)$$

for all $i \geq 0$, so maps on Tate cohomology groups for $i \geq 1$. By Proposition 1.7.3, we have

$$\hat{H}^{i-1}(G,A) \cong \hat{H}^i(G, A_*),$$

and the same holds for $H$-cohomology, as $\mathrm{Ind}^G(A)$ is also an induced $H$-module. We define

$$\mathrm{Res}\colon \hat{H}^{i-1}(G,A) \to \hat{H}^{i-1}(H,A)$$

to make the diagram

$$\begin{array}{ccc} \hat{H}^{i-1}(G,A) & \xrightarrow{\sim} & \hat{H}^i(G,A_*) \\ \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ \hat{H}^{i-1}(H,A) & \xrightarrow{\sim} & \hat{H}^i(H,A_*) \end{array}$$

commute.

If we wish to define restriction on homology groups when $G$ is not finite, we need to provide first a definition of restriction on $H_0(G,A)$, so that we can use dimension shifting to define it for $H_i(G,A)$ with $i \geq 1$. Similarly, we need a description of corestriction on $H^0(G,A)$.

DEFINITION 1.8.19. Suppose that $H$ is a finite index subgroup of a group $G$ and $A$ is a $G$-module.

i. Define

$$\mathrm{Res}\colon H_0(G,A) \to H_0(H,A), \qquad x \mapsto \sum_{\bar{g}\in H\backslash G} g\cdot\tilde{x},$$

where $x \in A_G$ and $\tilde{x} \in A_H$ is any lift of it, and where $g$ denotes any coset representative of $\bar{g} \in H\backslash G$.

ii. Define

$$\mathrm{Cor}\colon H^0(H,A) \to H^0(G,A), \qquad a \mapsto \sum_{\bar{g}\in G/H} g\cdot a$$

where $a \in A^H$ and $g$ is as above.

PROPOSITION 1.8.20. *Let $G$ be a group and $H$ a subgroup of finite index. Then there are maps*

$$\mathrm{Res}\colon H_i(G,A) \to H_i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon H^i(H,A) \to H^i(G,A)$$

*for all $i \geq 0$ that coincide with the maps of Definition 1.8.19 for $i = 0$ and that provide morphisms of $\delta$-functors.*

PROOF. Again, we consider the case of restriction, that of corestriction being analogous. We have a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H_1(G,A) & \longrightarrow & H_0(G,A_*) & \longrightarrow & H_0(G,\mathrm{Ind}^G(A)) \\
 & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
0 & \longrightarrow & H_1(H,A) & \longrightarrow & H_0(H,A_*) & \longrightarrow & H_0(H,\mathrm{Ind}^G(A)),
\end{array}$$

which allows us to define restriction as the induced maps on kernels. For any $i \geq 2$, we proceed as described above in the case of Tate cohomology to define restriction maps on the $i$th homology groups.

That Res gives of morphism of $\delta$-functors can be proven by induction using dimension shifting and a straightforward diagram chase and is left to the reader. □

REMARK 1.8.21. Corestriction commutes with conjugation on the cohomology groups of subgroups of $G$ with coefficients in $G$-modules. In the same vein, restriction commutes with conjugation on the homology of subgroups of $G$ with $G$-module coefficients.

COROLLARY 1.8.22. *Let $G$ be finite and $H$ a subgroup. The maps* Res *and* Cor *defined on both homology and cohomology above induce maps*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(H,A) \quad \textit{and} \quad \mathrm{Cor}\colon \hat{H}^i(H,A) \to \hat{H}^i(G,A)$$

*for all $i \in \mathbb{Z}$, and these provide morphisms of $\delta$-functors.*

PROOF. The reader may check that Res and Cor defined in homological and cohomological degree 0, respectively, induce morphisms on the corresponding Tate cohomology groups. We then have left only to check the commutativity of one diagram in each case.

Suppose that

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

is an exact sequence of $G$-modules. For restriction, we want to check that

$$\begin{array}{ccc} \hat{H}^{-1}(G,C) & \xrightarrow{\delta} & \hat{H}^0(G,A) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ \hat{H}^{-1}(H,C) & \xrightarrow{\delta} & \hat{H}^0(H,A) \end{array}$$

commutes. Let $c$ be in the kernel of $N_G$ on $C$, and denote its image in $\hat{H}^{-1}(G,C)$ by $\bar{c}$. Choose $b \in B$ with $\pi(b) = c$ and considering $N_G b \in B^G$, which is $\iota(a)$ for some $a \in A^G$. Then $\delta(c)$ is the image of $a$ in $\hat{H}^0(G,A)$. Then $\text{Res}(\delta(\bar{c}))$ is just the image of $a$ in $\hat{H}^0(H,A)$. On the other hand,

$$\text{Res}(\bar{c}) = \sum_{\bar{g} \in H\backslash G} g\tilde{c},$$

where $\tilde{c}$ is the image of $c$ in $\hat{H}^{-1}(H,C)$. We may lift the latter element to $\sum_{\bar{g}} gc$ in the kernel of $N_H$ on $C$ and then to $\sum_{\bar{g}} gb \in B$. Taking $N_H$ of this element gives us $N_G b$, which is $\iota(a)$, and so $\delta(\text{Res}(\bar{c}))$ is once again the image of $a$ in $\hat{H}^0(H,A)$.

The case of corestriction is very similar, and hence omitted. □

The following describes an important relationship between restriction and corestriction.

PROPOSITION 1.8.23. *Let $G$ be a group and $H$ a subgroup of finite index. Then the maps* $\text{Cor} \circ \text{Res}$ *on homology, cohomology, and, when $G$ is finite, Tate cohomology, are just the multiplication by* $[G:H]$ *maps.*

PROOF. It suffices to prove this on the zeroth homology and cohomology groups. The result then follows by dimension shifting. On cohomology we have the composite map

$$A^G \xrightarrow{\text{Res}} A^H \xrightarrow{\text{Cor}} A^G,$$

where Res is the natural inclusion and Cor the map of Definition 1.8.19. For $a \in A^G$, we have

$$\sum_{g \in G/H} ga = [G:H]a,$$

as desired.

On homology, we have maps

$$A_G \xrightarrow{\text{Res}} A_H \xrightarrow{\text{Cor}} A_G,$$

where Res is as in Definition 1.8.19 and Cor is the natural quotient map. For $x \in A_G$ and $\tilde{x} \in A_H$ lifting it, the element

$$\sum_{g \in H \backslash G} g\tilde{x}$$

has image $[G:H]x$ in $A_G$, again as desired. □

Here is a useful corollary.

COROLLARY 1.8.24. *Let $G_p$ be a Sylow $p$-subgroup of a finite group $G$, for a prime $p$. Then the kernel of*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

*has no elements of order $p$.*

PROOF. Let $\alpha \in \hat{H}^i(G,A)$ with $p^n\alpha = 0$ for some $n \geq 0$. Then $\mathrm{Cor}(\mathrm{Res}(\alpha)) = [G:G_p]\alpha$, but $[G:G_p]$ is prime to $p$, hence $\mathrm{Cor}(\mathrm{Res}(\alpha))$ is nonzero if $\alpha \neq 0$, and therefore $\mathrm{Res}(\alpha)$ cannot be 0 unless $\alpha = 0$. □

We then obtain the following.

COROLLARY 1.8.25. *Let $G$ be a finite group. For each prime $p$, fix a Sylow $p$-subgroup $G_p$ of $G$. Fix $i \in \mathbb{Z}$, and suppose that*

$$\mathrm{Res}\colon \hat{H}^i(G,A) \to \hat{H}^i(G_p,A)$$

*is trivial for all primes $p$. Then $\hat{H}^i(G,A) = 0$.*

PROOF. The intersection of the kernels of the restriction maps over all $p$ contains no elements of $p$-power order for any $p$ by Corollary 1.8.24. So, if all of the restriction maps are trivial, the group $\hat{H}^i(G,A)$ must be trivial. □

Finally, we remark that we have conjugation Tate cohomology, as in the cases of homology and cohomology.

REMARK 1.8.26. Suppose that $G$ is finite and $H$ is a subgroup of $G$. The conjugation maps on $H^0(H,A)$ and $H_0(H,A)$ induce maps on $\hat{H}^0(H,A)$ and $\hat{H}_0(H,A)$, respectively, and so we use the conjugation maps on homology and cohomology to define maps

$$g^*\colon \hat{H}^i(H,A) \to \hat{H}^i(gHg^{-1},A).$$

for all $i$. Again, these turn Tate cohomology for $H$ into a $\delta$-functor from $G$-modules to $(G/H)$-modules when $H$ is normal in $G$. Conjugation commutes with restriction and corestriction on subgroups of $G$.

## 1.9. Cup products

We consider the following maps on the standard complex $P_\cdot$:

$$\kappa_{i,j}\colon P_{i+j} \to P_i \otimes_{\mathbb{Z}} P_j, \qquad \kappa_{i,j}(g_0,\dots,g_{i+j}) = (g_0,\dots,g_i)\otimes(g_i,\dots,g_{i+j}).$$

That is, there is a natural map

$$\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B) \to \operatorname{Hom}_{\mathbb{Z}[G]}(P_i\otimes_{\mathbb{Z}} P_j, A\otimes_{\mathbb{Z}} B)$$

defined by

$$\varphi\otimes\varphi' \mapsto (\alpha\otimes\beta \mapsto \varphi(\alpha)\otimes\varphi'(\beta)).$$

Composing this with the map induced by precomposition with $\kappa_{i,j}$ gives rise to a map

$$\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B) \xrightarrow{\cup} \operatorname{Hom}_{\mathbb{Z}[G]}(P_{i+j},A\otimes_{\mathbb{Z}} B),$$

and we denote the image of $\varphi\otimes\varphi'$ under this map by $\varphi\cup\varphi'$. Let us summarize this.

DEFINITION 1.9.1. Let $\varphi\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)$ and $\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B)$. The *cup product* $\varphi\cup\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_{i+j},A\otimes_{\mathbb{Z}} B)$ is defined by

$$(\varphi\cup\varphi')(g_0,\dots,g_{i+j}) = \varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,g_{i+j}).$$

LEMMA 1.9.2. *Let* $\varphi\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_i,A)$ *and* $\varphi'\in\operatorname{Hom}_{\mathbb{Z}[G]}(P_j,B)$. *Then*

$$D^{i+j}_{A\otimes B}(\varphi\cup\varphi') = D^i_A(\varphi)\cup\varphi' + (-1)^i\varphi\cup D^j_B(\varphi'),$$

*where the differentials* $D^i$ *are as in* (1.3.1).

PROOF. We compute the terms. We have

$$D^{i+j}_{A\otimes B}(\varphi\cup\varphi')(g_0,\dots,g_{i+j+1}) = \sum_{k=0}^{i}(-1)^k\varphi(g_0,\dots,\widehat{g_k},\dots,g_{i+1})\otimes\varphi'(g_{i+1},\dots,g_{i+j+1}) + \sum_{k=i+1}^{i+j+1}(-1)^k\varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,\widehat{g_k},\dots,g_{i+j+1}),$$

while

$$(D^i_A(\varphi)\cup\varphi')(g_0,\dots,g_{i+j+1}) = \sum_{k=0}^{i+1}(-1)^k\varphi(g_0,\dots,\widehat{g_k},\dots,g_{i+1})\otimes\varphi'(g_{i+1},\dots,g_{i+j+1}) \tag{1.9.1}$$

and

$$(\varphi\cup D^j_B(\varphi'))(g_0,\dots,g_{i+j+1}) = \sum_{k=i}^{j+i+1}(-1)^{k-i}\varphi(g_0,\dots,g_i)\otimes\varphi'(g_i,\dots,\widehat{g_j},\dots,g_{i+j+1}). \tag{1.9.2}$$

As $(-1)^{i+1}+(-1)^i=0$, the last term in (1.9.1) cancels with the $(-1)^i$ times the first term in (1.9.2). The equality of the two sides follows. □

REMARK 1.9.3. On cochains, we can define cup products

$$C^i(G,A)\otimes_{\mathbb{Z}} C^j(G,B)\xrightarrow{\cup} C^{i+j}(G,A\otimes_{\mathbb{Z}} B)$$

of $f\in C^i(G,A)$ and $f'\in C^j(G,B)$ by

$$(f\cup f')(g_1,g_2,\dots g_{i+j}) = f(g_1,\dots,g_i)\otimes g_1g_2\dots g_if'(g_{i+1},\dots,g_{i+j}).$$

To see that these match up with the previous definition, note that if we define $\varphi$ and $\varphi'$ by

$$\varphi(1,g_1,\dots,g_1\cdots g_i) = f(g_1,\dots,g_i) \quad \text{and} \quad \varphi'(1,g_1,\dots,g_1\cdots g_j) = f'(g_1,\dots,g_j),$$

then

$$\begin{aligned}(f\cup f')(g_1,\dots,g_{i+j}) &= \varphi(1,g_1,\dots,g_1\cdots g_i)\cup g_1g_2\dots g_i\varphi(1,g_{i+1},\dots,g_{i+1}\cdots g_{i+j+1})\\ &= \varphi(1,g_1,\dots,g_1\cdots g_i)\cup \varphi(g_1\cdots g_i,g_1\cdots g_{i+1},\dots,g_1\cdots g_{i+j+1})\\ &= (\varphi\cup\varphi')(1,g_1,\dots,g_1\cdots g_{i+j+1}),\end{aligned}$$

so the definitions agree under the identifications of Theorem 1.3.3. As a consequence of Lemma 1.9.2, the cup products on cochains satisfy

$$d^{i+j}_{A\otimes B}(f\cup f') = d^i_A(f)\cup f' + (-1)^j f\cup d^i_B(f'). \tag{1.9.3}$$

LEMMA 1.9.4. *The sequences*

$$0\to A\otimes_{\mathbb{Z}} B\to \mathrm{CoInd}^G(A)\otimes_{\mathbb{Z}} B\to A^*\otimes_{\mathbb{Z}} B\to 0 \tag{1.9.4}$$

$$0\to A_*\otimes_{\mathbb{Z}} B\to \mathrm{Ind}^G(A)\otimes_{\mathbb{Z}} B\to A\otimes_{\mathbb{Z}} B\to 0 \tag{1.9.5}$$

*are exact for any G-modules A and B.*

PROOF. Since the augmentation map $\varepsilon$ is split over $\mathbb{Z}$, it follows using Remark 1.7.1 that the sequences (1.7.1) and (1.7.2) are split as well. It follows that the sequences in the lemma are exact. □

THEOREM 1.9.5. *The cup products of Definition 1.9.1 induce maps, also called cup products,*

$$H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B)\xrightarrow{\cup} H^{i+j}(G,A\otimes_{\mathbb{Z}} B)$$

*that are natural in A and B and satisfy the following properties:*

*(i) For $i=j=0$, one has that the cup product*

$$A^G\otimes_{\mathbb{Z}} B^G\to (A\otimes_{\mathbb{Z}} B)^G$$

*is induced by the identity on $A\otimes_{\mathbb{Z}} B$.*

*(ii) If*

$$0 \to A_1 \to A \to A_2 \to 0$$

*is an exact sequence of G-modules such that*

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

*is exact as well, then*

$$\delta(\alpha_2 \cup \beta) = (\delta\alpha_2) \cup \beta \in H^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

*for all $\alpha_2 \in H^i(G,A_2)$ and $\beta \in H^j(G,B)$. (In other words, cup product on the right with a cohomology class provides a morphism of $\delta$-functors.)*

*(iii) If*

$$0 \to B_1 \to B \to B_2 \to 0$$

*is an exact sequence of G-modules such that*

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

*is exact as well, then*

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta\beta_2) \in H^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

*for all $\alpha \in H^i(G,A)$ and $\beta_2 \in H^j(G,B_2)$.*

*Moreover, the cup products on cohomology are the unique collection of such maps natural in A and B and satisfying properties (i), (ii), and (iii).*

PROOF. Let $f \in C^i(G,A)$ and $f' \in C^j(G,B)$. By (1.9.3), it is easy to see that the cup product of two cocycles is a cocycle and that the cup product of a cocycle and a coboundary is a coboundary. Thus, the cup product on cochains induces cup products on cohomology. The naturality in $A$ and $B$ follows directly from the definition. Property (i) is immediate from the definition as well. Property (ii) can be seen by tracing through the definition of the connecting homomorphism. Let $f_2$ represent $\alpha_2$. Then $\delta(\alpha_2)$ is obtained by lifting $f_2$ to a cochain $f \in C^i(G,A)$, taking its boundary $df \in C^{i+1}(G,A)$, and then noting that $df$ is the image of some cocycle $z_1 \in Z^{i+1}(G,A_1)$. Let $f' \in Z^j(G,B)$ represent $\beta$. By (1.9.3), we have $df \cup f' = d(f \cup f')$. Note that $z_1 \cup f'$ has class $\delta(\alpha_2) \cup \beta$ and image $df \cup f'$ in $C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$. On the other hand, $d(f \cup f')$ is the image of a cocycle representing $\delta(\alpha_2 \cup \beta)$, as $f \cup f'$ is a cocycle lifting $f_2 \cup f'$. Since the map

$$C^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B) \to C^{i+j+1}(G, A \otimes_{\mathbb{Z}} B)$$

is injective, we have (ii). Property (iii) follows similarly, the sign appearing in the computation arising from (1.9.3).

The uniqueness of the maps with these properties follows from the fact that given a collection of such maps, property (i) specifies them uniquely for $i = j = 0$, while properties (ii) and (iii) specify

them uniquely for all other $i, j \geq 0$ by dimension shifting. For instance, by (ii) and Lemma 1.9.4, we have a commutative square

$$\begin{array}{ccc} H^i(G,A^*) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G,A^* \otimes_{\mathbb{Z}} B) \\ \downarrow\!\!\downarrow & & \downarrow \\ H^{i+1}(G,A) \otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^{i+j+1}(G,A \otimes_{\mathbb{Z}} B) \end{array}$$

in which the lefthand vertical arrow is a surjection for all $i$ (and an isomorphism for $i \geq 1$). Thus, the cup products in degrees $(i, j)$ for $i \geq 1$ and $j \geq 0$ specify by the cup products in degrees $(i+1, j)$. Similarly, using (iii), we see that the cup products in degrees $(i, j)$ specify the cup products in degrees $(i, j+1)$. □

REMARK 1.9.6. Associativity of tensor products and Lemma 1.5.10 tell us that

$$\mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B,$$

so in particular the latter modules is induced. This also implies that we have isomorphisms

$$(A \otimes_{\mathbb{Z}} B)_* \cong A_* \otimes_{\mathbb{Z}} B.$$

If $G$ is finite, Proposition 1.5.4 tells us that we have

$$\mathrm{CoInd}^G(A \otimes_{\mathbb{Z}} B) \cong \mathrm{CoInd}^G(A) \otimes_{\mathbb{Z}} B \quad \text{and} \quad (A \otimes_{\mathbb{Z}} B)^* \cong A^* \otimes_{\mathbb{Z}} B$$

as well.

COROLLARY 1.9.7. *Consider the natural isomorphism*

$$s_{AB} \colon A \otimes_{\mathbb{Z}} B \to B \otimes_{\mathbb{Z}} A$$

*given by $a \otimes b \mapsto b \otimes a$, and the maps that it induces on cohomology. For all $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has that*

$$s_{AB}^*(\alpha \cup \beta) = (-1)^{ij}(\beta \cup \alpha).$$

PROOF. We first verify the result in the case $i = j = 0$. For $a \in A^G$ and $b \in B^G$, we have

$$s_{AB}^*(a \cup b) = s_{AB}(a \otimes b) = b \otimes a = b \cup a.$$

Suppose that we know the result for a given pair $(i-1, j)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$. Recall that the maps $H^{i-1}(G,A^*) \to H^i(G,A)$ are surjective for all $i \geq 1$ (and isomorphisms for $i \geq 2$), and write $\alpha = \delta(\alpha^*)$ for some $\alpha^* \in H^{i-1}(G,A^*)$. Since (1.9.4) is exact, we have by Theorem 1.9.5 that

$$\begin{aligned} s_{AB}^*(\alpha \cup \beta) = s_{AB}^*(\delta(\alpha^*) \cup \beta) = s_{AB}^*(\delta(\alpha^* \cup \beta)) = \delta(s_{AB}^*(\alpha^* \cup \beta)) \\ = (-1)^{(i-1)j}\delta(\beta \cup \alpha^*) = (-1)^{(i-1)j}(-1)^j \beta \cup \delta(\alpha^*) = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

Suppose next that we know the result for a given pair $(i, j-1)$. Let $\alpha \in H^i(G,A)$ and $\beta \in H^{j-1}(G,B)$, and write $\beta = \delta(\beta^*)$ for some $\beta^* \in H^j(G,B^*)$. Since (1.9.4) is exact, we have by Theorem 1.9.5 that

$$\begin{aligned} s^*_{AB}(\alpha \cup \beta) = s^*_{AB}(\alpha \cup \delta(\beta^*)) = (-1)^i s^*_{AB}(\delta(\alpha \cup \beta^*)) = \delta(s^*_{AB}(\alpha \cup \beta^*)) \\ = (-1)^i(-1)^{i(j-1)}\delta(\beta^* \cup \alpha) = (-1)^{ij}\delta(\beta^*) \cup \alpha = (-1)^{ij}\beta \cup \alpha. \end{aligned}$$

The result now follows by induction on $i$ and $j$. □

Cup products also have an associative property, which can be checked directly on cochains.

PROPOSITION 1.9.8. *Let $A$, $B$, and $C$ be $G$-modules, and let $\alpha \in H^i(G,A)$, $\beta \in H^j(G,B)$, and $\gamma \in H^k(G,C)$. Then*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, A \otimes_{\mathbb{Z}} B \otimes_{\mathbb{Z}} C).$$

Often, when we speak of cup products, we apply an auxiliary map from the tensor product of $A$ and $B$ to a third module before taking the result. For instance, if $A = B = \mathbb{Z}$, then one will typically make the identification $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$. We codify this in the following definition.

DEFINITION 1.9.9. Suppose that $A$, $B$, and $C$ are $G$-modules and $\theta : A \otimes_{\mathbb{Z}} B \to C$ is a $G$-module homomorphism. Then the maps

$$H^i(G,A) \otimes_{\mathbb{Z}} H^j(G,B) \to H^{i+j}(G,C), \qquad \alpha \otimes \beta \mapsto \theta(\alpha \cup \beta)$$

are also referred to as cup products. When $\theta$ is understood, we denote $\theta(\alpha \cup \beta)$ more simply by $\alpha \cup \beta$.

Cup products behave nicely with respect to restriction, corestriction, and inflation.

PROPOSITION 1.9.10. *Let $A$ and $B$ be $G$-modules. We then have the following compatibilities.*

*a. Let $H$ be a subgroup of $G$. For $\alpha \in H^i(G,A)$ and $\beta \in H^j(G,B)$, one has*

$$\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta) \in H^{i+j}(H, A \otimes_{\mathbb{Z}} B),$$

*where* Res *denotes restriction from $G$ to $H$.*

*b. Let $N$ be a normal subgroup of $G$. For $\alpha \in H^i(G/N, A^N)$ and $\beta \in H^j(G/N, B^N)$, one has*

$$\mathrm{Inf}(\alpha \cup \beta) = \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

*where* Inf *denotes inflation from $G/N$ to $G$. (Here, we implicitly use the canonical map $A^N \otimes_{\mathbb{Z}} B^N \to (A \otimes_{\mathbb{Z}} B)^N$ prior to taking inflation on the left.)*

*c. Let $H$ be a subgroup of finite index in $G$. For $\alpha \in H^i(H,A)$ and $\beta \in H^j(G,B)$, one has*

$$\mathrm{Cor}(\alpha) \cup \beta = \mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B),$$

*where* Res *denotes restriction from $G$ to $H$ and* Cor *denotes corestriction from $H$ to $G$.*

PROOF. We can prove part a by direct computation on cocycles. That is, for $f \in Z^i(G,A)$, $f' \in Z^i(G,B)$, and $h_1,\dots,h_{i+j} \in H$, we have

$$\begin{aligned}\mathrm{Res}(f\cup f')(h_1,\dots,h_{i+j}) &= (f\cup f')(h_1,\dots,h_{i+j}) = f(h_1,\dots,h_i)\otimes h_1\cdots h_i f'(h_{i+1},\dots,h_{i+j})\\ &= \mathrm{Res}(f)(h_1\dots,h_i)\otimes h_1\cdots h_i\,\mathrm{Res}(f')(h_{i+1},\dots,h_{i+j}) = (\mathrm{Res}(f)\cup\mathrm{Res}(f'))(h_1,\dots,h_{i+j}).\end{aligned}$$

Part b is similarly computed.

We now prove part c. Consider the case that $i=j=0$. Then $a\in A^H$ and $b\in B^G$. By property (i) in Theorem 1.9.5 and the definition of corestriction on $H^0$, we have

$$\mathrm{Cor}(a)\cup b = \sum_{\bar g\in G/H}(ga)\otimes b = \sum_{\bar g\in G/H}(ga\otimes gb) = \sum_{\bar g\in G/H} g(a\otimes b) = \mathrm{Cor}(a\cup\mathrm{Res}(b)).$$

As corestriction and restriction commute with connecting homomorphisms, and as cup products behave well with respect to connecting homomorphisms on either side, we can use dimension shifting to prove the result for all $i$ and $j$. That is, suppose we know the result for a fixed pair $(i-1,j)$. We prove it for $(i,j)$. Letting $\delta$ the connecting homomorphism induced by (1.7.1) for $A$, and choose $\alpha^*\in H^{i-1}(G,A^*)$ such that $\delta(\alpha^*)=\alpha$. We then have

$$\begin{aligned}\mathrm{Cor}(\alpha)\cup\beta = \delta(\mathrm{Cor}(\alpha^*))\cup\beta &= \delta(\mathrm{Cor}(\alpha^*)\cup\beta)\\ &= \delta(\mathrm{Cor}(\alpha^*\cup\mathrm{Res}(\beta)) = \mathrm{Cor}(\delta(\alpha^*\cup\mathrm{Res}(\beta))) = \mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta)).\end{aligned}$$

Similarly, take $\delta$ for the sequence analogous to (1.7.1) for the module $B$ and assume the result for $(i,j-1)$. Choosing $\beta^*\in H^{j-1}(G,B^*)$ with $\delta(\beta^*)=\beta$, we have

$$\begin{aligned}\mathrm{Cor}(\alpha)\cup\beta = \mathrm{Cor}(\alpha)\cup\delta(\beta^*) = (-1)^i\delta(\mathrm{Cor}(\alpha)\cup\beta^*) &= (-1)^i\delta(\mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta^*)))\\ &= (-1)^i\mathrm{Cor}(\delta(\alpha\cup\mathrm{Res}(\beta^*))) = \mathrm{Cor}(\alpha\cup\delta(\mathrm{Res}(\beta^*))) = \mathrm{Cor}(\alpha\cup\mathrm{Res}(\beta)).\end{aligned}$$

□

NOTATION 1.9.11. We may express the statement of Proposition 1.9.10a as saying that the diagram

$$\begin{array}{ccc} H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G,A\otimes_{\mathbb{Z}} B)\\ \downarrow{\scriptstyle \mathrm{Res}} \quad \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}}\\ H^i(H,A)\otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H,A\otimes_{\mathbb{Z}} B)\end{array}$$

commutes (with a similar diagram for part b) and the statement of Proposition 1.9.10c as saying that the diagram

$$\begin{array}{ccc} H^i(G,A)\otimes_{\mathbb{Z}} H^j(G,B) & \xrightarrow{\cup} & H^i(G,A\otimes_{\mathbb{Z}} B)\\ \uparrow{\scriptstyle \mathrm{Cor}} \quad \downarrow{\scriptstyle \mathrm{Res}} & & \uparrow{\scriptstyle \mathrm{Cor}}\\ H^i(H,A)\otimes_{\mathbb{Z}} H^j(H,B) & \xrightarrow{\cup} & H^i(H,A\otimes_{\mathbb{Z}} B)\end{array}$$

commutes.

For finite groups, we have cup products on Tate cohomology as well.

THEOREM 1.9.12. *Let $G$ be finite. There exists a unique family of maps*

$$\hat{H}^i(G,A) \otimes_{\mathbb{Z}} \hat{H}^j(G,B) \xrightarrow{\cup} \hat{H}^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

*with $i, j \in \mathbb{Z}$ that are natural in the $G$-modules $A$ and $B$ and which satisfy the following properties:*

*(i) The diagram*

$$\begin{array}{ccc} H^0(G,A) \otimes_{\mathbb{Z}} H^0(G,B) & \xrightarrow{\cup} & H^0(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow & & \downarrow \\ \hat{H}^0(G,A) \otimes_{\mathbb{Z}} \hat{H}^0(G,B) & \xrightarrow{\cup} & \hat{H}^0(G, A \otimes_{\mathbb{Z}} B) \end{array}$$

*commutes.*

*(ii) If*

$$0 \to A_1 \to A \to A_2 \to 0$$

*is an exact sequence of $G$-modules such that*

$$0 \to A_1 \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to A_2 \otimes_{\mathbb{Z}} B \to 0$$

*is exact as well, then*

$$\delta(\alpha_2 \cup \beta) = (\delta \alpha_2) \cup \beta \in \hat{H}^{i+j+1}(G, A_1 \otimes_{\mathbb{Z}} B)$$

*for all $\alpha_2 \in \hat{H}^i(G,A_2)$ and $\beta \in \hat{H}^j(G,B)$.*

*(iii) If*

$$0 \to B_1 \to B \to B_2 \to 0$$

*is an exact sequence of $G$-modules such that*

$$0 \to A \otimes_{\mathbb{Z}} B_1 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B_2 \to 0$$

*is exact as well, then*

$$\delta(\alpha \cup \beta_2) = (-1)^i \alpha \cup (\delta \beta_2) \in \hat{H}^{i+j+1}(G, A \otimes_{\mathbb{Z}} B_1)$$

*for all $\alpha \in \hat{H}^i(G,A)$ and $\beta_2 \in \hat{H}^j(G,B_2)$.*

PROOF. Consider the complex $Q_\cdot$ of Theorem 1.6.10, obtained from the standard resolution $P_\cdot$. The proof goes through as in Theorem 1.9.5 once we define maps $Q_{i+j} \to Q_i \otimes_{\mathbb{Z}} Q_j$ satisfying the formula of Lemma 1.9.2. There are six cases to consider (the case $i, j \geq 0$ being as before), and these are omitted. □

REMARK 1.9.13. Corollary 1.9.7, Proposition 1.9.8, and Proposition 1.9.10 all hold for cup products on Tate cohomology as well. We can also compose cup products with $G$-module maps from the tensor product, and we again denote them using the same symbol, as in Definition 1.9.9.

## 1.10. Tate cohomology of cyclic groups

In this section, let $G$ be a cyclic group of finite order. We prove that the Tate cohomology groups with coefficients in a module $A$ are periodic in the degree of period 2, up to isomorphisms determined by a choice of generator $g$ of $G$.

The first thing that we will observe is that for such a group $G$, there is an even nicer projective resolution of $\mathbb{Z}$ than the standard one: i.e., consider the sequence

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0, \tag{1.10.1}$$

where the boundary maps are multiplication $N_G$ in even degree and by $g-1$ in odd degree. We can splice this together with its dual as in Theorem 1.6.10.

PROPOSITION 1.10.1. *The $G$-cohomology groups of $A$ are the cohomology groups of the complex*

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

*with a map $g-1$ following the term in degree* 0.

PROOF. Note first that for $i \in \{-1,0\}$, the group $\hat{H}^i(G,A)$ is by definition isomorphic to the $i$th cohomology group of the complex in question. Let $C_\cdot$ denote the projective resolution of $\mathbb{Z}$ given by (1.10.1). The complex $C_\cdot \otimes_{\mathbb{Z}[G]} A$ that ends

$$\cdots \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to 0$$

computes $H_i(G,A)$, yielding the result for $i \leq -2$.

Multiplication by $g$ induces the endomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A), \qquad \varphi \mapsto (x \mapsto \varphi(gx) = g\varphi(x)).$$

Via the isomorphism of $G$-modules $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],A) \xrightarrow{\sim} A$ given by evaluation at 1, the latter endomorphism is identified with multiplication by $g$ on $A$. The complex $\mathrm{Hom}_{\mathbb{Z}[G]}(C_\cdot,A)$ that computes $H^i(G,A)$ is therefore isomorphic to

$$0 \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to \cdots,$$

providing the result for $i \geq 1$. □

COROLLARY 1.10.2. *For any $i \in \mathbb{Z}$, we have*

$$\hat{H}^i(G,A) \cong \begin{cases} \hat{H}^0(G,A) & i \text{ even} \\ \hat{H}^{-1}(G,A) & i \text{ odd.} \end{cases}$$

We show that, in fact, these isomorphisms can be realized by means of a cup product. As usual, consider $\mathbb{Z}$ as having a trivial $G$-action. We remark that

$$\hat{H}^{-2}(G,\mathbb{Z}) \cong H_1(G,\mathbb{Z}) \cong G^{\mathrm{ab}} \cong G$$

by Proposition 1.4.5. Any choice of generator $g$ of $G$ is now a generator $u_g$ of this Tate cohomology group. Note that $\mathbb{Z}\otimes_{\mathbb{Z}} A \cong A$ for any $G$-module $A$ via multiplication. Here then is the result.

PROPOSITION 1.10.3. *Let $G$ be cyclic with generator $g$, and let $A$ be a $G$-module. Then the map*

$$\hat{H}^i(G,A) \to \hat{H}^{i-2}(G,A), \qquad c \mapsto u_g \cup c$$

*is an isomorphism for any $i \in \mathbb{Z}$.*

PROOF. Consider the two exact sequences of $G$-modules:

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \quad \text{and} \quad 0 \to \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} I_G \to 0.$$

As $\hat{H}^i(G,\mathbb{Z}[G]) = 0$ for all $i \in \mathbb{Z}$, we then have two isomorphisms

$$\hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\delta} \hat{H}^{-1}(G,I_G) \xrightarrow{\delta} \hat{H}^0(G,\mathbb{Z}).$$

(In fact, tracing it through, one sees that the image of $u_g$ under this composition is 1 modulo $|G|$. This is not needed for the proof.)

Since we have

$$\delta(\delta(u_g)) \cup c = \delta(\delta(u_g \cup c))$$

by property (ii) of Theorem 1.9.12, it suffices to show that cup product with the image of 1 in $\hat{H}^0(G,\mathbb{Z})$ is an isomorphism. For this, using property (iii) of Theorem 1.9.12 to dimension shift, the problem reduces to the case that $i = 0$. In this case, we know that the cup product is induced on $\hat{H}^0$ by the multiplication map on $H^0$'s:

$$\mathbb{Z}\otimes_{\mathbb{Z}} A^G \to A^G, \qquad m \otimes a \mapsto ma.$$

However, $1 \cdot a = a$, so the map $\hat{H}^0(G,A) \to \hat{H}^0(G,A)$ induced by taking cup product with the image of 1 is an isomorphism. □

Given the 2-periodicity of the Tate cohomology groups of a finite cyclic group, we can make the following definition.

DEFINITION 1.10.4. Let $G$ be a finite cyclic group and $A$ a $G$-module. Set $h_0(A) = |\hat{H}^0(G,A)|$ and $h_1(A) = |\hat{H}^1(G,A)|$, taking them to be infinite when the orders of the Tate cohomology groups are infinite. If both $h_0(A)$ and $h_1(A)$ are finite, we then define the *Herbrand quotient* $h(A)$ by

$$h(A) = \frac{h_0(A)}{h_1(A)}.$$

Clearly, if $A$ is finitely generated, then $h(A)$ will be defined. The following explains how Herbrand quotients behave with respect to modules in short exact sequences.

THEOREM 1.10.5. *Let*

$$0 \to A \to B \to C \to 0$$

*be an exact sequence of G-modules. Suppose that any two of $h(A)$, $h(B)$, and $h(C)$ are defined. Then the third is as well, and*

$$h(B) = h(A) \cdot h(C).$$

PROOF. It follows immediately from Proposition 1.10.3 that we have an exact hexagon

$$\begin{array}{ccccc} & & \hat{H}^0(G,A) & \longrightarrow & \hat{H}^0(G,B) & & \\ & \nearrow & & & & \searrow & \\ \hat{H}^1(G,C) & & & & & & \hat{H}^0(G,C) \\ & \nwarrow & & & & \swarrow & \\ & & \hat{H}^1(G,B) & \longleftarrow & \hat{H}^1(G,A) & & \end{array} .$$

Note that the order of any group in the hexagon is the product of the orders of the image of the map from the previous group and the order of the image of the map to the next group. Therefore, that any two of $h(A)$, $h(B)$, and $h(C)$ are finite implies the third is. When all three are finite, an Euler characteristic argument then tells us that

$$\frac{h_0(A) \cdot h_0(C) \cdot h_1(B)}{h_0(B) \cdot h_1(A) \cdot h_1(C)} = 1, \tag{1.10.2}$$

hence the result. More specifically, the order of each cohomology group is the product of the orders of the images of two adjacent maps in the hexagon, and the order of the image of each such map then appears once in each of the numerator and denominator of the left-hand side of (1.10.2). □

As an immediate consequence of Theorem 1.10.5, we have the following.

COROLLARY 1.10.6. *Suppose that*

$$0 \to A_1 \to A_2 \to \cdots \to A_n \to 0$$

*is an exact sequence of G-modules with $h(A_k)$ finite for at least one of each consecutive pair of subscripts k, including at least one of $A_n$ and $A_1$. Then all $h(A_k)$ are finite and*

$$\prod_{k=1}^{n} h(A_k)^{(-1)^k} = 1.$$

Next, we show that the Herbrand quotients of finite modules are trivial.

PROPOSITION 1.10.7. *Suppose that A is a finite G-module. Then $h(A) = 1$.*

PROOF. Let $g$ be a generator of $G$, and note that the sequence

$$0 \to A^G \to A \xrightarrow{g-1} A \to A_G \to 0$$

is exact. As $A$ is finite and any alternating product of orders of finite groups in exact sequences of finite length is 1, we therefore have $|A^G| = |A_G|$. On the other hand, we have the exact sequence

$$0 \to \hat{H}^{-1}(G,A) \to A_G \xrightarrow{\tilde{N}_G} A^G \to \hat{H}^0(G,A) \to 0$$

defining $\hat{H}^i(G,A)$ for $i = 0,-1$. As $h_1(A) = |\hat{H}^{-1}(G,A)|$, we therefore have $h(A) = 1$. □

We therefore have the following.

PROPOSITION 1.10.8. *Let $f\colon A \to B$ be a $G$-module homomorphism with finite kernel and cokernel. Then $h(A) = h(B)$ if either one is defined.*

PROOF. This follows immediately from the exact sequence

$$0 \to \ker f \to A \to B \to \operatorname{coker} f \to 0,$$

Corollary 1.10.6, and Proposition 1.10.7. □

## 1.11. Cohomological triviality

In this section, we suppose that $G$ is a finite group.

DEFINITION 1.11.1. A $G$-module $A$ is said to be *cohomologically trivial* if $\hat{H}^i(H,A) = 0$ for all subgroups $H$ of $G$ and all $i \in \mathbb{Z}$.

In this section, we will give conditions for a $G$-module to be cohomologically trivial.

REMARK 1.11.2. Every free $G$-module is also a free $H$-module for every subgroup $H$ of $G$ and any group $G$, not necessarily finite. In particular, $\mathbb{Z}[G]$ is free over $\mathbb{Z}[H]$ on any set of cosets representatives of $H\backslash G$.

We remark that it follows from this that induced $G$-modules are induced $H$-modules, as direct sums commute with tensor products. We then have the following examples of cohomologically trivial modules.

EXAMPLES 1.11.3.

a. Induced $G$-modules are cohomologically trivial by Proposition 1.6.7.

b. Projective $G$-modules are cohomologically trivial. To see this, suppose that $P$ and $Q$ are projective $G$-modules with $P \oplus Q$ free over $\mathbb{Z}[G]$, hence over $\mathbb{Z}[H]$. Then

$$\hat{H}^i(H,P) \hookrightarrow \hat{H}^i(H,P) \oplus \hat{H}^i(H,Q) \cong \hat{H}^i(H,P \oplus Q) = 0$$

for all $i \in \mathbb{Z}$.

We need some preliminary lemmas. Fix a prime $p$.

LEMMA 1.11.4. *Suppose that $G$ is a $p$-group and that $A$ is a $G$-module of exponent dividing $p$. Then $A = 0$ if and only if $A_G = 0$ and if and only if $A^G = 0$.*

PROOF. Suppose $A^G = 0$, and let $a \in A$. The submodule $B$ of $A$ generated by $a$ is finite, and $B^G = 0$. The latter fact implies that the $G$-orbits in $B$ are either $\{0\}$ or have order a multiple of $p$. Since $B$ has $p$-power order, this forces the order to be 1, so $B = 0$. Since $a$ was arbitrary, $A = 0$. On the other hand, if $A_G = 0$, then $X = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ satisfies $pX = 0$ and

$$X^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}[G]}(A_G, \mathbb{F}_p) = 0.$$

By the invariants case just proven, we know $X = 0$, so $A = 0$. □

LEMMA 1.11.5. *Suppose that $G$ is a $p$-group and that $A$ is a $G$-module of exponent dividing $p$. If $H_1(G,A) = 0$, then $A$ is free as an $\mathbb{F}_p[G]$-module.*

PROOF. Lift an $\mathbb{F}_p$-basis of $A_G$ to a subset $\Sigma$ of $A$. For the $G$-submodule $B$ of $A$ generated by $\Sigma$, the quotient $A/B$ has trivial $G$-coinvariant group, hence is trivial by Lemma 1.11.4. That is, $\Sigma$ generates $A$ as an $\mathbb{F}_p[G]$-module. Letting $F$ be the free $\mathbb{F}_p[G]$-module generated by $\Sigma$, we then have a canonical surjection $\pi\colon F \to A$, and we let $R$ be the kernel. Consider the exact sequence

$$0 \to R_G \to F_G \xrightarrow{\bar{\pi}} A_G \to 0$$

that exists since $H_1(G,A) = 0$. We have by definition that the map $\bar{\pi}$ induced by $\pi$ is an isomorphism, so we must have $R_G = 0$. As $pR = 0$, we have by Lemma 1.11.4 that $R = 0$, and so $\pi$ is an isomorphism. □

We are now ready to give a module-theoretic characterization of cohomologically trivial modules that are killed by $p$.

PROPOSITION 1.11.6. *Suppose that $G$ is a $p$-group and that $A$ is a $G$-module of exponent dividing $p$. The following are equivalent:*

*(i) $A$ is cohomologically trivial*

*(ii) $A$ is a free $\mathbb{F}_p[G]$-module.*

*(iii) There exists $i \in \mathbb{Z}$ such that $\hat{H}^i(G,A) = 0$.*

PROOF.

(i) $\Rightarrow$ (iii) Immediate.

(i) $\Rightarrow$ (ii) This is a special case of Lemma 1.11.5, since $H_1(G,A) \cong \hat{H}^{-2}(G,A)$.

(ii) $\Rightarrow$ (i) Suppose $A$ is free over $\mathbb{F}_p[G]$ on a generating set $I$. Then

$$A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \bigoplus_{i \in I} \mathbb{F}_p,$$

so $A$ is induced, hence cohomologically trivial.

(iii) $\Rightarrow$ (ii) We note that the modules $A_*$ and $A^*$ that we use to dimension shift, as in (1.7.2) and (1.7.1) are killed by $p$ since $A$ is. In particular, it follows by dimension shifting that there exists a $G$-module $B$ such that $pB = 0$ and

$$\hat{H}^{j-2}(G,B) \cong \hat{H}^{j+i}(G,A)$$

for all $j \in \mathbb{Z}$. In particular, $H_1(G,B) = \hat{H}^{-2}(G,B)$ is trivial. By Lemma 1.11.5, $B$ is $\mathbb{F}_p[G]$-free. However, we have just shown that this implies that $B$ is cohomologically trivial, and therefore so is $A$.

□

We next consider the case that $A$ has no elements of order $p$.

PROPOSITION 1.11.7. *Suppose that $G$ is a $p$-group and $A$ is a $G$-module with no elements of order $p$. The following are equivalent:*

*(i) $A$ is cohomologically trivial.*

*(ii) There exists $i \in \mathbb{Z}$ such that $\hat{H}^i(G,A) = \hat{H}^{i+1}(G,A) = 0$.*

*(iii) $A/pA$ is free over $\mathbb{F}_p[G]$.*

PROOF.

(i) $\Rightarrow$ (ii) Immediate.

(ii) $\Rightarrow$ (iii) Since $A$ has no $p$-torsion,

$$0 \to A \xrightarrow{p} A \to A/pA \to 0$$

is exact. By (ii) and the long exact sequence in Tate cohomology, we have $\hat{H}^i(G,A/pA) = 0$. By Proposition 1.11.6, we have therefore that $A/pA$ is free over $\mathbb{F}_p[G]$.

(iii) $\Rightarrow$ (i) By Proposition 1.11.6, we have that $A/pA$ is cohomologically trivial, and therefore multiplication by $p$ is an isomorphism on each $\hat{H}^i(H,A)$ for each subgroup $H$ of $G$ and every $i \in \mathbb{Z}$. However, the latter cohomology groups are annihilated by the order of $H$, so must be trivial since $H$ is a $p$-group.

□

We next wish to generalize to arbitrary finite groups.

PROPOSITION 1.11.8. *Let $G$ be a finite group and, for each $p$, choose a Sylow $p$-subgroup $G_p$ of $G$. Let $A$ be a $G$-module. Then $A$ is cohomologically trivial if and only if $A$ is cohomologically trivial as a $G_p$-module for each $p$.*

PROOF. Suppose that $A$ is cohomologically trivial for all $G_p$. Let $H$ be a subgroup of $G$. Any Sylow $p$-subgroup $H_p$ of $H$ is contained in a conjugate of $G_p$, say $gG_pg^{-1}$. By the cohomological triviality of $G_p$, we have that $\hat{H}^i(g^{-1}H_pg,A) = 0$. As $g^*$ is an isomorphism, we have that $\hat{H}^i(H_p,A) =$

0. Therefore, we see that the restriction map $\mathrm{Res}\colon \hat{H}^i(H,A) \to \hat{H}^i(H_p,A)$ is 0. Since this holds for each $p$, Corollary 1.8.25 implies that $\hat{H}^i(H,A) = 0$. □

In order to give a characterization of cohomologically trivial modules in terms of projective modules, we require the following lemma.

LEMMA 1.11.9. *Suppose that $G$ is a $p$-group and $A$ is a $G$-module that is free as an abelian group and cohomologically trivial. For any $G$-module $B$ which is $p$-torsion free, we have that* $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ *is cohomologically trivial.*

PROOF. Since $B$ has no $p$-torsion and $A$ is free over $\mathbb{Z}$, we have that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A,B) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A,B) \to \mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \to 0$$

is exact. In particular, $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ has no $p$-torsion, and

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A,B)/p\,\mathrm{Hom}_{\mathbb{Z}}(A,B).$$

Since $A/pA$ is free over $\mathbb{F}_p[G]$ with some indexing set that we shall call $I$, we have

$$\mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB) \cong \prod_{i\in I} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{F}_p[G],B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}\Big(\mathbb{Z}[G],\prod_{i\in I} B/pB\Big),$$

so $\mathrm{Hom}_{\mathbb{Z}}(A,B/pB)$ is coinduced, and therefore $\mathbb{F}_p[G]$-free. By Proposition 1.11.7, we have that $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ is cohomologically trivial. □

PROPOSITION 1.11.10. *Let $G$ be a finite group and $A$ a $G$-module that is free as an abelian group. Then $A$ is cohomologically trivial if and only if $A$ is a projective $G$-module.*

PROOF. We have already seen that projective implies cohomologically trivial. Suppose that $A$ is cohomologically trivial as a $G$-module. Since $A$ is $\mathbb{Z}$-free, it follows that $\mathrm{Ind}^G(A)$ is a free $G$-module, and the sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A,A_*) \to \mathrm{Hom}_{\mathbb{Z}}(A,\mathrm{Ind}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}}(A,A) \to 0 \tag{1.11.1}$$

is exact. Moreover, $A_*$ is rather clearly $\mathbb{Z}$-free since $A$ is, so it follows from Lemma 1.11.9 that the module $\mathrm{Hom}_{\mathbb{Z}}(A,A_*)$ is cohomologically trivial. In particular, by the long exact sequence in cohomology attached to (1.11.1), we see that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A,\mathrm{Ind}^G(A)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(A,A)$$

is surjective. In particular, the identity map lifts to a homomorphism $A \to \mathrm{Ind}^G(A)$, which is a splitting of the natural surjection $\mathrm{Ind}^G(A) \to A$. It follows that $A$ is projective as a $G$-module. □

Finally, we consider the general case.

THEOREM 1.11.11. *Let $G$ be a finite group and $A$ a $G$-module. The following are equivalent.*

*(i) $A$ is cohomologically trivial.*

*(ii) For each prime $p$, there exists some $i \in \mathbb{Z}$ such that $\hat{H}^i(G_p,A) = \hat{H}^{i+1}(G_p,A) = 0$.*

*(iii) There is an exact sequence of $G$-modules*

$$0 \to P_1 \to P_0 \to A \to 0$$

*in which $P_0$ and $P_1$ are projective.*

PROOF.

(i) $\Rightarrow$ (ii) This follows from the definition of cohomologically trivial.

(ii) $\Rightarrow$ (iii) Let $F$ be a free $G$-module that surjects onto $A$, and let $R$ be the kernel. As $F$ is cohomologically trivial, we have $\hat{H}^{j-1}(G_p,A) \cong \hat{H}^j(G_p,R)$ for every $j \in \mathbb{Z}$. It follows that $\hat{H}^j(G_p,R)$ vanishes for two consecutive values of $j$. Since $R$ is $\mathbb{Z}$-free, being a subgroup of $F$, we have by Propositions 1.11.7, 1.11.8, and 1.11.10 that $R$ is projective.

(iii) $\Rightarrow$ (i) This follows from the fact that projective modules are cohomologically trivial and the long exact sequence in Tate cohomology.

□

## 1.12. Tate's theorem

We continue to assume that $G$ is a finite group, and we choose a Sylow $p$-subgroup $G_p$ of $G$ for each prime $p$. We begin with a consequence of our characterization of cohomologically trivial modules to maps on cohomology.

PROPOSITION 1.12.1. *Let $\kappa\colon A \to B$ be a $G$-module homomorphism. Viewed as a $G_p$-module homomorphism, let us denote it by $\kappa_p$. Suppose that, for each prime $p$, there exists a $j \in \mathbb{Z}$ such that*

$$\kappa_p^*\colon \hat{H}^i(G_p,A) \to \hat{H}^i(G_p,B)$$

*is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. Then*

$$\kappa^*\colon \hat{H}^i(H,A) \to \hat{H}^i(H,B)$$

*is an isomorphism for all $i \in \mathbb{Z}$ and subgroups $H$ of $G$.*

PROOF. Consider the canonical injection of $G$-modules

$$\kappa \oplus \iota\colon A \to B \oplus \mathrm{CoInd}^G(A),$$

and let $C$ be its cokernel. As $\mathrm{CoInd}^G(A)$ is $H$-cohomologically trivial for all $H \leq G$, we have

$$\hat{H}^i(H, B \oplus \mathrm{CoInd}^G(A)) \cong \hat{H}^i(H,B)$$

for all $i \in \mathbb{Z}$. The long exact sequence in $G_p$-cohomology then reads

$$\cdots \to \hat{H}^i(G_p,A) \xrightarrow{\kappa_p^*} \hat{H}^i(G_p,B) \to \hat{H}^i(G_p,C) \xrightarrow{\delta} \hat{H}^{i+1}(G_p,A) \xrightarrow{\kappa_p^*} \hat{H}^{i+1}(G_p,B) \to \cdots.$$

Consider the case $i = j-1$. The map $\kappa_p^*$ being surjective on $\hat{H}^{j-1}$ and injective on $\hat{H}^j$ implies that $\hat{H}^{j-1}(G_p, C) = 0$. Similarly, for $i = j$, the map $\kappa_p^*$ being surjective on $\hat{H}^j$ and injective on $\hat{H}^{j+1}$ implies that $\hat{H}^j(G_p, C) = 0$. Therefore, $C$ is cohomologically trivial by Theorem 1.11.11, and so each map $\kappa^*\colon \hat{H}^i(H,A) \to \hat{H}^i(H,B)$ in question must be an isomorphism by the long exact sequence in Tate cohomology. □

We now prove the main theorem of Tate and Nakayama.

THEOREM 1.12.2. *Suppose that A, B, and C are G-modules and*

$$\theta\colon A \otimes_{\mathbb{Z}} B \to C$$

*is a G-module map. Let $k \in \mathbb{Z}$ and $\alpha \in \hat{H}^k(G,A)$. For each subgroup H of G, define*

$$\Theta^i_{H,\alpha}\colon \hat{H}^i(H,B) \to \hat{H}^{i+k}(H,C), \qquad \Theta^i_{H,\alpha}(\beta) = \theta^*(\mathrm{Res}(\alpha) \cup \beta).$$

*For each prime p, suppose that there exists $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. Then for every subgroup H of G and $i \in \mathbb{Z}$, one has that $\Theta^i_{H,\alpha}$ is an isomorphism.*

PROOF. First consider the case that $k = 0$. Then the map $\psi\colon B \to C$ given by $\psi(b) = \theta(a \otimes b)$, where $a \in A^G$ represents $\alpha$, is a map of $G$-modules, since

$$\psi(gb) = \theta(a \otimes gb) = \theta(ga \otimes gb) = g\theta(a \otimes b) = g\psi(b).$$

We claim that the induced maps on cohomology

$$\psi^*\colon \hat{H}^i(H,B) \to \hat{H}^i(H,C)$$

agree with the maps given by left cup product with $\mathrm{Res}(\alpha)$. Given this, we have by Proposition 1.12.1 that the latter maps are all isomorphisms in the case $k = 0$.

To see the claim, consider first the case that $i = 0$, in which the map $\psi^*$ is induced by $\psi\colon B^H \to C^H$. For $b \in B^H$, we have $\psi(b) = \theta(a \otimes b)$, and the class of the latter term is $\theta^*(\mathrm{Res}(a) \cup b)$ by (i) of Theorem 1.9.12. For the case of arbitrary $i$, we consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (A \otimes_{\mathbb{Z}} B)_* & \longrightarrow & \mathrm{Ind}^G(A \otimes_{\mathbb{Z}} B) & \longrightarrow & A \otimes_{\mathbb{Z}} B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\theta}} & & \downarrow{\scriptstyle \mathrm{Ind}^G(\theta)} & & \downarrow{\scriptstyle \theta} & & \\ 0 & \longrightarrow & C_* & \longrightarrow & \mathrm{Ind}^G(C) & \longrightarrow & C & \longrightarrow & 0, \end{array} \tag{1.12.1}$$

where $\mathrm{Ind}^G(\theta) = \mathrm{id}_{\mathbb{Z}[G]} \otimes \theta$, and where $\tilde{\theta}$ is both the map making the diagram commute and $\mathrm{id}_{I_G} \otimes \theta$, noting Remark 1.7.1. In fact, by Remark 1.9.6, we have an exact sequence isomorphic to the top row of (1.12.1), given by

$$0 \to A \otimes_{\mathbb{Z}} B_* \to A \otimes_{\mathbb{Z}} \mathrm{Ind}^G(B) \to A \otimes_{\mathbb{Z}} B \to 0$$

and then a map $\tilde{\psi}\colon B_* \to C_*$ given by $\tilde{\psi}(b') = \tilde{\theta}(a \otimes b')$ for $b' \in B_*$. We then have two commutative diagrams

$$\begin{array}{ccc} \hat{H}^{i-1}(H,B) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H,B_*) \\ \downarrow & & \downarrow \\ \hat{H}^{i-1}(H,C) & \xrightarrow[\sim]{\delta} & \hat{H}^i(H,C_*). \end{array}$$

In the first, the left vertical arrow is $\Theta^{i-1}_{H,\alpha}$ and the right vertical arrow is the map $\tilde{\Theta}^i_{H,\alpha}$ given on $\beta' \in \hat{H}^i(H,B_*)$ by

$$\tilde{\Theta}^i_{H,\alpha}(\beta') = \tilde{\theta}^*(\mathrm{Res}(\alpha) \cup \beta').$$

In the second, the left vertical arrow is $\psi^*$ and the right is $\tilde{\psi}^*$. Supposing our claim for $i$, we have $\tilde{\psi}^* = \tilde{\Theta}^i_{H,\alpha}$. As the connecting homomorphisms in the diagrams are isomorphisms, we then have that $\psi^* = \Theta^i_{H,\alpha}$. I.e., if the claim holds for $i$, it holds for $i-1$. The analogous argument using coinduced modules allows us to shift from $i$ to $i+1$, proving the claim for all $i \in \mathbb{Z}$, hence the theorem for $k = 0$.

For any $k \in \mathbb{Z}$, the result is again proven by dimension shifting, this time for $A$. Fix $\alpha \in \hat{H}^{k-1}(H,A)$, and let $\alpha' = \delta(\alpha) \in \hat{H}^k(H,A_*)$. We note that the top row of (1.12.1) is also isomorphic to

$$0 \to A_* \otimes_{\mathbb{Z}} B \to \mathrm{Ind}^G(A) \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B \to 0.$$

Much as before, define $\Theta^i_{H,\alpha'}\colon \hat{H}^i(H,B) \to \hat{H}^{i+k}(H,C_*)$ by $\Theta^i_{H,\alpha'}(\beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta)$, where $\tilde{\theta}\colon A_* \otimes_{\mathbb{Z}} B \to C_*$ is the map determined by $\theta$. The diagram

$$\begin{array}{ccc} \hat{H}^i(H,B) & = & \hat{H}^i(H,B) \\ \downarrow{\scriptstyle \Theta^i_{H,\alpha}} & & \downarrow{\scriptstyle \Theta^i_{H,\alpha'}} \\ \hat{H}^{i+k-1}(H,C) & \xrightarrow[\sim]{\delta} & \hat{H}^{i+k}(H,C_*) \end{array}$$

then commutes as

$$\delta \circ \Theta^i_{H,\alpha}(\beta) = \delta \circ \theta^*(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^* \delta(\mathrm{Res}(\alpha) \cup \beta) = \tilde{\theta}^*(\mathrm{Res}(\alpha') \cup \beta) = \Theta^i_{H,\alpha'}(\beta).$$

There exists by assumption $j \in \mathbb{Z}$ such that the map $\Theta^i_{G_p,\alpha}$ is surjective for $i = j-1$, an isomorphism for $i = j$, and injective for $i = j+1$. By the commutativity of the diagram, the same holds for $\Theta^i_{G_p,\alpha'}$. Assuming the theorem for $k$, we then have that all of the maps $\Theta^i_{H,\alpha'}$ are isomorphisms, and therefore again by commutativity that so are the maps $\Theta^i_{H,\alpha}$. Thus, the theorem for a given $k$ implies the theorem for $k-1$. By the analogous argument using coinduced modules, the theorem for $k$ implies the theorem for $k+1$ as well. □

The following special case was first due to Tate.

THEOREM 1.12.3 (Tate). *Let $A$ be a $G$-module, and let $\alpha \in H^2(G,A)$. Suppose that, for every $p$, the group $H^1(G_p,A)$ is trivial and $H^2(G_p,A)$ is a cyclic group of order $|G_p|$ generated by the restriction of $\alpha$. Then the maps*

$$\hat{H}^i(H,\mathbb{Z}) \to \hat{H}^{i+2}(H,A), \qquad \beta \mapsto \mathrm{Res}(\alpha) \cup \beta$$

*are isomorphisms for every $i \in \mathbb{Z}$ and subgroup $H$ of $G$.*

PROOF. For $H = G_p$, the maps in question are surjective for $i = -1$, as $H^1(G_p,A) = 0$, and injective for $i = 1$, as

$$H^1(G_p,\mathbb{Z}) = \mathrm{Hom}(G_p,\mathbb{Z}) = 0.$$

For $i = 0$, we have

$$\hat{H}^0(G_p,\mathbb{Z}) \cong \mathbb{Z}/|G_p|\mathbb{Z},$$

and the map takes the image of $n \in \mathbb{Z}$ to $n\mathrm{Res}(\alpha)$ (which is straightforward enough to see by dimension shifting, starting with the known case of cup products of degree zero classes), hence is an isomorphism by the assumption on $H^2(G_p,A)$. □

CHAPTER 2

# Galois cohomology

## 2.1. Profinite groups

DEFINITION 2.1.1. A *topological group* $G$ is a group endowed with a topology with respect to which both the multiplication map $G \times G \to G$ and the inversion map $G \to G$ that takes an element to its inverse are continuous.

EXAMPLES 2.1.2.

a. The groups $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ are continuous with respect to the topologies defined by their absolute values.

b. Any group can be made a topological group by endowing it with the discrete topology.

REMARK 2.1.3. We may consider the category of topological groups, in which the maps are continuous homomorphisms between topological groups.

DEFINITION 2.1.4. A homomorphism $\phi\colon G \to G'$ between topological groups $G$ and $G'$ is a *topological isomorphism* if it is both an isomorphism and a homeomorphism.

The following lemma is almost immediate, since elements of a group are invertible.

LEMMA 2.1.5. *Let $G$ be a topological group and $g \in G$. Then the map $m_g\colon G \to G$ with $m_g(a) = ga$ for all $a \in G$ is a homeomorphism.*

We also have the following.

LEMMA 2.1.6. *A group homomorphism $\phi\colon G \to G'$ between topological groups is continuous if and only if, for each open neighborhood $U$ of $1$ in $G'$ with $1 \in U$, the set $\phi^{-1}(U)$ contains an open neighborhood of $1$.*

PROOF. We consider the non-obvious direction. Let $V$ be an open set in $G'$, and suppose that $g \in G$ is such that $h = \phi(g) \in V$. Then $h^{-1}V$ is open in $G'$ as well, by Lemma 2.1.5. By assumption, there exists an open neighborhood $W$ of 1 in $G$ contained in $\phi^{-1}(h^{-1}V)$, and so $gW$ is an open neighborhood of $g$ in $G$ such that $\phi(gW) \subseteq V$. Hence, $\phi$ is continuous. □

LEMMA 2.1.7. *Let $G$ be a topological group.*

*a. Any open subgroup of $G$ is closed.*

*b. Any closed subgroup of finite index in G is open.*

PROOF. If $H$ is an open (resp., closed) subgroup of $G$, then its cosets are open (resp., closed) as well. Moreover, $G-H$ is the union of the nontrivial cosets of $H$. Therefore, $G-H$ is open if $G$ is open and closed if $G$ is closed of finite index, so that there are only finitely many cosets of $H$. □

LEMMA 2.1.8. *Every open subgroup of a compact group G is of finite index in G.*

PROOF. Let $H$ be a open subgroup of $G$. Note that $G$ is the union of its distinct $H$-cosets, which are open and disjoint. Since $G$ is compact, there can therefore only be finitely many cosets, which is to say that $H$ is of finite index in $G$. □

We leave it to the reader to verify the following.

LEMMA 2.1.9.

*a. A subgroup of a topological group is a topological group with respect to the subspace topology.*

*b. The quotient of a topological group G by a normal subgroup N is a topological group with respect to the quotient topology, and it is Hausdorff if N is closed.*

*c. A direct product of topological groups is a topological group with respect to the product topology.*

Recall the definitions of a directed set, inverse system, and the inverse limit.

DEFINITION 2.1.10. A *directed set* $I = (I, \geq)$ is a partially ordered set such that for every $i, j \in I$, there exists $k \in I$ with $k \geq i$ and $k \geq j$.

DEFINITION 2.1.11. Let $I$ be a directed set. An *inverse system* $(G_i, \phi_{i,j})$ of groups over the indexing set $I$ is a set

$$\{G_i \mid i \in I\}$$

of groups and a set

$$\{\phi_{i,j} \colon G_i \to G_j \mid i, j \in I, i \geq j\}$$

of group homomrphisms.

DEFINITION 2.1.12. An *inverse limit*

$$G = \varprojlim_i G_i$$

of an inverse system of groups $(G_i, \phi_{i,j})$ over a directed indexing set $I$ is a pair $G = (G, \{\pi_i \mid i \in I\})$ consisting of a group $G$ and homomorphisms $\pi_i \colon G \to G_i$ such that $\phi_{i,j} \circ \pi_i = \pi_j$ for all $i, j \in I$ with $i \geq j$ that satisfy the following universal property: Given a group $G'$ and maps $\pi'_i \colon G' \to G_i$ for $i \in I$ such that $\phi_{i,j} \circ \pi'_i = \pi'_j$ for all $i \geq j$, there exists a unique map $\psi \colon G' \to G$ such that $\pi'_i = \pi_i \circ \psi$ for all $i \in I$.

By the universal property, any two inverse limits of an inverse system of groups are canonically isomorphic (via compatible maps).

REMARK 2.1.13. We may make the latter definition more generally with any category $\mathscr{C}$ replacing the category of groups. The groups are replaced with objects in $\mathscr{C}$ and the group homomorphisms with morphisms in $\mathscr{C}$. Moreover, we may view the system of groups as a covariant functor to the category $\mathscr{C}$ from the category that has the elements of $I$ as its objects and morphisms $i \to j$ for each $i, j \in I$ with $i \geq j$.

We may give a direct construction of an inverse limit of an inverse system of groups as follows. The proof is left to the reader.

PROPOSITION 2.1.14. *Let $(G_i, \phi_{i,j})$ be an inverse system of groups over an indexing set $I$. Then the an inverse limit of the system is given explicitly by the group*

$$G = \left\{ (g_i)_i \in \prod_{i \in I} G_i \mid \phi_{i,j}(g_i) = g_j \right\}$$

*and the maps $\pi_i \colon G \to G_i$ for $i \in I$ that are the compositions of the $G \to \prod_{i \in I} G_i \to G_i$ of inclusion followed by projection.*

We may endow an inverse limit of groups with a topology as follows.

DEFINITION 2.1.15. Let $(G_i, \phi_{i,j})$ be an inverse system of topological groups over an indexing set $I$, with continuous maps. Then the *inverse limit topology* on the inverse limit $G$ of Proposition 2.1.14 is the subspace topology for the product topology on $\prod_{i \in I} G_i$.

LEMMA 2.1.16. *The inverse limit of an inverse system $(G_i, \phi_{i,j})$ of topological groups (over a directed indexing set $I$) is a topological group under the inverse limit topology.*

PROOF. The maps

$$\prod_{i \in I} G_i \times \prod_{i \in I} G_i \to \prod_{i \in I} G_i \quad \text{and} \quad \prod_{i \in I} G_i \to \prod_{i \in I} G_i$$

given by componentwise multiplication and inversion are clearly continuous, and this continuity is preserved under the subspace topology on the inverse limit. □

REMARK 2.1.17. In fact, the inverse limit of an inverse system of topological groups and continuous maps, when endowed with the product topology, is an inverse limit in the category of topological groups.

When we wish to view it as a topological group, we typically endow a finite group with the discrete topology.

DEFINITION 2.1.18. A *profinite group* is an inverse limit of a system of finite groups, endowed with the inverse limit topology for the discrete topology on the finite groups.

Recall the following definition.

DEFINITION 2.1.19. A topological space is *totally disconnected* if and only if every point is a connected component.

We leave the following as difficult exercises.

PROPOSITION 2.1.20. *A compact Hausdorff space is totally disconnected if and only if it has a basis of open neighborhoods that are also closed.*

PROPOSITION 2.1.21. *A compact Hausdorff group that is totally disconnected has a basis of neighborhoods of* 1 *consisting of open normal subgroups (of finite index).*

We may now give a topological characterization of profinite groups.

THEOREM 2.1.22. *A profinite topological group $G$ is compact, Hausdorff, and totally disconnected.*

PROOF. First, suppose that $G$ is profinite, equal to an inverse limit of a system $(G_i, \phi_{i,j})$ of finite groups over an indexing set $I$. The direct product $\prod_{i\in I} G_i$ of finite (discrete) groups $G_i$ is compact Hausdorff (compactness being Tychonoff's theorem). As a subset of the direct product, $G$ is Hausdorff, and to see it is compact, we show that $G$ is closed. Suppose that

$$(g_i)_i \in \prod_{i\in I} G_i$$

with $(g_i)_i \notin G$, and choose $i, j \in I$ with $i > j$ and $\phi_{i,j}(g_i) \neq g_j$. The open subset

$$\left\{ (h_k)_k \in \prod_{k\in I} G_k \mid h_i = g_i, h_j = g_j \right\}$$

of the direct product contains $(g_i)_i$ and has trivial intersection with $G$. In that the complement of $G$ is open, $G$ itself is closed. Finally, note that any open set $\prod_{i\in I} U_i$ with each $U_i$ open in $G_i$ (i.e., an arbitrary subset) and $U_i = G_i$ for all but finitely many $i$ is also closed. That is, its complement is the intersection

$$\bigcap_{j\in I} \left( (G_j - U_j) \times \prod_{i\in I-\{j\}} U_i \right)$$

of open sets, which is actually equal to the finite intersection over $j \in I$ with $U_i \neq G_i$. It is therefore open, and by Proposition 2.1.20, the group $G$ is totally disconnected. □

REMARK 2.1.23. We leave it to the reader to check that the converse to Theorem 2.1.22 also holds. They key is found in the proof of part a of the following proposition.

PROPOSITION 2.1.24. *Let $G$ be a profinite group, and let $\mathscr{U}$ be the set of all open normal subgroups of $G$. Then the following canonical homomorphisms are homeomorphisms:*

*a.* $G \to \varprojlim_{N\in\mathscr{U}} G/N$,

*b.* $H \to \varprojlim_{N\in\mathscr{U}} H/(H\cap N)$, *for $H$ a closed subgroup of $G$, and*

*c.* $G/K \to \varprojlim_{N\in\mathscr{U}} G/NK$, *for $K$ a closed normal subgroup of $G$.*

PROOF. We prove part *a*. The continuous map $\phi$ from $G$ to the inverse limit $Q$ of its quotients has closed image, and $\phi$ is injective since $\mathscr{U}$ is a basis of 1 in $G$ as in Proposition 2.1.21. Suppose that $(g_N N)_{N\in\mathscr{U}}$ is not in the image of $\phi$, which is exactly to say that the intersection of the closed sets $g_N N$ is empty. Since $G$ is compact this implies that some finite subset of the $\{g_N N \mid N \in \mathscr{U}\}$ is empty, and letting $M$ be the intersection of the $N$ in this subset, we see that $g_M M = \varnothing$, which is a contradiction. In other words, $\phi$ is surjective. □

The following is a consequence of Proposition 2.1.24a. We leave the proof to the reader.

COROLLARY 2.1.25. *Let $G$ be a profinite group and $\mathscr{V}$ a set of open normal subgroups of $G$ that forms a basis of open neighborhoods of* 1. *Then the homomorphism*

$$G \to \varprojlim_{N\in\mathscr{V}} G/N$$

*is a homeomorphism.*

The following lemma will be useful later.

LEMMA 2.1.26. *The closed subgroups of a profinite group are exactly those that may be written as intersections of open subgroups.*

PROOF. In a topological group, an open subgroup is also closed, an arbitrary intersection of closed sets is closed, and an arbitrary intersection of subgroups is a subgroup, so an intersection of open subgroups is a closed subgroup. Let $\mathscr{U}$ denote the set of open subgroups of a profinite group $G$. Let $H$ be a closed subgroup of $G$. It follows from Proposition 2.1.24b and the second isomorphism theorem that the set of subgroups of the form $NH$ with $N$ open normal in $G$ has intersection $H$. Note that each $NH$ is open as a union of open subgroups, so it is open. □

We may also speak of pro-$p$ groups.

DEFINITION 2.1.27. A *pro-$p$ group*, for a prime $p$, is an inverse limit of a system of finite $p$-groups.

We may also speak of profinite and pro-$p$ completions of groups.

DEFINITION 2.1.28. Let $G$ be a group.

a. The *profinite completion* $\hat{G}$ of $G$ is the inverse limit of its finite quotients $G/N$, for $N$ a normal subgroup of finite index in $G$, together with the natural quotient maps $G/N \to G/N'$ for $N \leq N'$.

b. The *pro-p completion* $G^{(p)}$ of $G$, for a prime $p$, is the inverse limit of the finite quotients of $G$ of $p$-power order, i.e., of the $G/N$ for $N \trianglelefteq G$ with $[G:N]$ a power of $p$, together with the natural quotient maps.

REMARK 2.1.29. A group $G$ is endowed with a canonical homomorphism to its profinite completion $\hat{G}$ by the universal property of the inverse limit.

REMARK 2.1.30. We may also speak of topological rings and fields, where multiplication, addition, and the additive inverse map are continuous, and in the case of a topological field, the multiplicative inverse map on the multiplicative group is continuous as well. We may speak of profinite rings as inverse limits by quotients by two-sided ideals of finite index (or for pro-$p$ rings, of $p$-power index).

The next proposition shows that $\mathbb{Z}_p$ is the pro-$p$ completion of $\mathbb{Z}$.

PROPOSITION 2.1.31. *Let $p$ be a prime. We have an isomorphism of rings*

$$\psi\colon \mathbb{Z}_p \xrightarrow{\sim} \varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}, \qquad \sum_{i=0}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{k-1} a_i p^i\right)_k,$$

*where the maps $\mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ in the system are the natural quotient maps. Moreover, $\psi$ is a homeomorphism.*

PROOF. The canonical quotient map $\psi_k\colon \mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ is the $k$th coordinate of $\psi$, which is then a ring homomorphism by the universal property of the inverse limit. The kernel $\psi$ is the intersection of the kernels of the maps $\psi_k$, which is exactly

$$\bigcap_k p^k\mathbb{Z}_p = 0.$$

Moreover, any sequence of partial sums modulo increasing powers of $p$ has a limit in $\mathbb{Z}_p$, which maps to the sequence under $\psi$. The open neighborhood $p^n\mathbb{Z}_p$ of 0 in the $p$-adic topology is sent to the intersection

$$\left(\prod_{k=1}^{n}\{0\} \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right),$$

which is open in the product topology. On the other hand, the inverse image of a basis open neighborhood

$$\left(\prod_{k=1}^{n} U_k \times \prod_{k=n+1}^{\infty} \mathbb{Z}_p/p^k\mathbb{Z}_p\right) \cap \left(\varprojlim_{k\geq 1} \mathbb{Z}/p^k\mathbb{Z}\right)$$

with $0 \in U_k$ for all $1 \leq k \leq n$ under $\psi$ clearly contains $p^n\mathbb{Z}_p$. It then follows from Lemma 2.1.6 that $\psi$ is a homeomorphism. □

DEFINITION 2.1.32. The *Prüfer ring* $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. That is, we have

$$\mathbb{Z} \cong \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$$

with respect to the quotient maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$.

Since $\mathbb{Z}/n\mathbb{Z}$ may be written as a direct product of the $\mathbb{Z}/p^k\mathbb{Z}$ for primes $p$ with $p^k$ exactly dividing $n$, we have the following.

LEMMA 2.1.33. *We have an isomorphism of topological rings*

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

EXAMPLE 2.1.34. The free profinite (or pro-$p$) group on a generating set $S$ is the profinite (resp., pro-$p$) completion of the free group on $S$.

REMARK 2.1.35. As with free groups, closed subgroups of free profinite (or pro-$p$) groups are free profinite (or pro-$p$) groups. Moreover, every profinite (resp., pro-$p$) group is a topological quotient of the free group on a set of its generators, so we may present such groups via generators and relations much as before.

DEFINITION 2.1.36. A subset $S$ of a topological group $G$ is said to be a *topological generating set* of $G$ if $G$ is the closure of the subgroup generated by $S$.

DEFINITION 2.1.37. We say that a topological group is *(topologically) finitely generated* if it has a finite set of topological generators.

REMARK 2.1.38. If $G$ is a free profinite (or pro-$p$) group on a set $S$, then it is topologically generated by $S$.

We leave a proof of the following to the reader.

LEMMA 2.1.39. *Let $G$ be a topological group, and let $H$ be a (normal) subgroup. Then the closure $\overline{H}$ of $H$ is also a (normal) subgroup of $G$.*

DEFINITION 2.1.40. The Frattini subgroup $\Phi(G)$ of a pro-$p$ group $G$, where $p$ is a prime, is smallest closed normal subgroup containing the commutator subgroup $[G,G]$ and the $p$th powers in $G$.

The following lemma is a consequence of the well-known case of finite $p$-groups.

LEMMA 2.1.41. *Let $G$ be a pro-$p$ group for a prime $p$. Then $\Phi(G)$ is normal in $G$, and a subset $S$ of $G$ generates $G$ if and only if its image in $G/\Phi(G)$ generates $G/\Phi(G)$.*

REMARK 2.1.42. In the case that $G$ is an abelian pro-$p$ group, the Frattini subgroup $\Phi(G)$ in Lemma 2.1.41 is $G^p$.

Finally, we state without proof the structure theorem for (topologically) finitely generated abelian pro-$p$ groups. In fact, this is an immediate consequence of the structure theorem for finitely generated modules over a PID.

THEOREM 2.1.43. *Let $A$ be a topologically finitely generated abelian pro-$p$ group. Then there exist $r,k \geq 0$ and $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$ such that we have an isomorphism*

$$A \cong \mathbb{Z}_p^r \oplus \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$$

*of topological groups.*

## 2.2. Cohomology of profinite groups

In this section, $G$ will denote a topological group.

DEFINITION 2.2.1. A *topological $G$-module $A$* is an abelian topological group such that the map $G \times A \to A$ defining the action of $G$ on $A$ is continuous.

DEFINITION 2.2.2. A $G$-module $A$ is *discrete* if it is a topological $G$-module for the discrete topology on $A$.

PROPOSITION 2.2.3. *Let $G$ be a profinite group, and let $A$ be a $G$-module. The following are equivalent:*

*i. $A$ is discrete,*

*ii. $A = \bigcup_{N \in \mathscr{U}} A^N$, where $\mathscr{U}$ is the set of open normal subgroups of $G$, and*

*iii. the stabilizer of each $a \in A$ is open in $G$.*

PROOF. Let $\pi\colon G \times A \to A$ be the map defining the $G$-action on $A$. For $a \in A$, let $G_a$ denote the stabilizer of $a$. If $A$ is discrete, then $\pi^{-1}(a) \cap (G \times \{a\})$ is open and equal to $G_a \times \{a\}$, so $G_a$ is open as well. Thus, (i) implies (iii). Conversely, suppose that (iii) holds. To see (i), it suffices to check that for any $a, b \in A$, then set $X_{a,b} = \{g \in G | ga = b\}$ is open. If $X_{a,b}$ is nonempty, then for any $g \in X_{a,b}$, we clearly have $X_{a,b} = G_b g$, which is open by the continuity of the multiplication on $G$. Thus, (iii) implies (i).

If $G_a$ is open for a given $a \in A$, then as $\mathscr{U}$ is a base of open neighborhoods of 1 in $G$, there exists $N \in \mathscr{U}$ with $N \subseteq G_a$. In other words, $a \in A^N$. Thus (iii) implies (ii). Conversely, suppose that (ii) holds. Take $a \in A$ and let $N \in \mathscr{U}$ be such that $a \in A^N$. Since $N$ has finite index in $G$, the stabilizer $G_a$ is a finite union of $N$-cosets, so $G_a$ is open as well. Thus (ii) implies (iii). □

REMARK 2.2.4. Note that our notion of a discrete $G$-module $A$ says only that the $G$-action on $A$ is continuous with respect to the discrete topology, so $A$ can be thought of as a topological module when endowed with said topology. It is possible that the discrete topology is not the unique topology that makes $A$ a topological $G$-module. For instance, $\mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{R}$ by $x \mapsto -x$, and this is continuous with respect to both the discrete and the usual topology on $\mathbb{R}$.

EXAMPLES 2.2.5.

a. Every trivial $G$-module is a discrete $G$-module.

b. If $G$ is finite (with the discrete topology), then every $G$-module is discrete.

c. If $G$ is profinite, then every finite $G$-module is necessarily discrete.

d. The action of $\mathbb{C}^\times$ on $\mathbb{C}$ by left multiplication gives $\mathbb{C}$ the structure of a $\mathbb{C}^\times$-module that is not discrete.

e. The action of $\hat{\mathbb{Z}}^\times$ on the group of roots of unity in $\mathbb{C}$ by $u\cdot\zeta=\zeta^u$, for $u\in\hat{\mathbb{Z}}^\times$ and $\zeta$ a root of unity, is discrete. Here, $\zeta^u$ is $\zeta$ raised to the power of any integer that is congruent to $u$ modulo the order of $\zeta$.

DEFINITION 2.2.6. We say that a topological $G$-module $A$ is *discrete* if its topology is the discrete topology.

DEFINITION 2.2.7. For a topological $G$-module $A$ and $i\in\mathbb{Z}$, the group of continuous $i$-cochains of $G$ with $A$-coefficients is

$$C^i_{\mathrm{cts}}(G,A)=\{f\colon G^i\to A \mid f \text{ continuous}\}.$$

LEMMA 2.2.8. *Let $A$ be a topological $G$-module. The usual differential $d^i_A$ on $C^i(G,A)$ restricts to a map $d^i_A\colon C^i_{\mathrm{cts}}(G,A)\to C^{i+1}_{\mathrm{cts}}(G,A)$. Thus, $(C^{\cdot}_{\mathrm{cts}}(G,A),d^{\cdot}_A)$ is a cochain complex.*

PROOF. Set $X=G^{i+1}$. Since $f\in C^i_{\mathrm{cts}}(G,A)$ and the multiplication maps $G\times G\to G$ and $G\times A\to A$ are continuous, so are the $i+2$ maps $X\to A$ taking $(g_1,\dots,g_{i+1})$ to $g_1f(g_2,\dots,g_{i+1})$, to $f(g_1,\dots,g_jg_{j+1},\dots,g_i)$ for some $1\le j\le i$, and to $f(g_1,\dots,g_i)$. The alternating sum defining $d^i_A(f)$ from these $i+2$ maps is the composition of the diagonal map $X\to X^{i+2}$, the direct product $X^{i+2}\to A^{i+2}$ of the maps in question, and the alternating sum map $A^{i+2}\to A$. Since all of these maps are continuous, so is $d^i_A(f)$. □

REMARK 2.2.9. In general, $C^{\cdot}(G,\ \cdot\ )$ is a left exact functor from the category of topological $G$-modules with continuous $G$-module homomorphisms to the category of abelian groups. However, it need not be exact.

PROPOSITION 2.2.10. *Let $G$ be a topological group. If*

$$0\to A\xrightarrow{\iota} B\xrightarrow{\pi} C\to 0$$

*is an exact sequence of discrete $G$-modules, then endowing $A$, $B$, and $C$ with the discrete topology, the sequence*

$$0\to C^i_{\mathrm{cts}}(G,A)\xrightarrow{\iota^i} C^i_{\mathrm{cts}}(G,B)\xrightarrow{\pi^i} C^i_{\mathrm{cts}}(G,C)\to 0$$

*is exact for each $i$.*

PROOF. We need only show right-exactness. Choose a set-theoretic splitting of $s\colon C \to B$ of $\pi$. In that $B$ and $C$ are discrete, $s$ is necessarily continuous. For any continuous $f\colon G^i \to C$, the map $s \circ f\colon G^i \to B$ is therefore continuous, and $\pi^i(s \circ f) = f$. □

DEFINITION 2.2.11. Let $G$ be a profinite group and $A$ a discrete $G$-module. The $i$th profinite cohomology group of $G$ with coefficients in $A$ is $H^i(G,A) = H^i(C^{\cdot}_{\mathrm{cts}}(G,A))$, where $A$ is endowed with the discrete topology.

NOTATION 2.2.12. If $f\colon A \to B$ is a $G$-module homomorphism between discrete $G$-modules $A$ and $B$, where $G$ is profinite, then the induced maps on cohomology are denoted $f^*\colon H^i(G,A) \to H^i(G,B)$.

As a corollary of Proposition 2.2.10, any short exact sequence of discrete $G$-modules gives rise to a long exact sequence of profinite cohomology groups.

THEOREM 2.2.13. *Suppose that*

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$$

*is a short exact sequence of discrete $G$-modules. Then there is a long exact sequence of abelian groups*

$$0 \to H^0(G,A) \xrightarrow{\iota^*} H^0(G,B) \xrightarrow{\pi^*} H^0(G,C) \xrightarrow{\delta^0} H^1(G,A) \to \cdots.$$

*Moreover, this construction is natural in the short exact sequence in the sense of Theorem 1.2.13.*

REMARK 2.2.14. If $G$ is a profinite group and $A$ is a discrete $G$-module, then $H^i(G,A)$ in the sense of Definition 2.2.11 need not be the same as $H^i(G,A)$ in the sense of (abstract) group cohomology. They do, however, agree in the case that $G$ is finite, since in that case $G$ is a discrete group, and every cochain $G^i \to A$ is continuous. Whenever $G$ is a profinite group and $A$ is discrete, we take $H^i(G,A)$ to be the profinite cohomology group.

EXAMPLE 2.2.15. For a pro-$p$ group $G$, the first cohomology group $H^1(G,\mathbb{F}_p)$ consists of the continuous homomorphisms from $G$ to $\mathbb{F}_p$. It is then canonically isomorphic to the $\mathbb{F}_p$-dual of $G/\Phi(G)$, with $\Phi(G)$ the Frattini subgroup. It follows from Lemma 2.1.41 that the $\mathbb{F}_p$-dimension of $H^1(G,\mathbb{F}_p)$ is equal to the order of the smallest (topological) generating set of $G$.

The following proposition shows that profinite cohomology groups are direct limits of usual cohomology groups of finite groups under inflation maps.

PROPOSITION 2.2.16. *Let $G$ be a profinite group, and let $\mathscr{U}$ be the set of open normal subgroups of $G$. For each discrete $G$-module $A$, we have an isomorphism*

$$H^i(G,A) \cong \varinjlim_{N \in \mathscr{U}} H^i(G/N, A^N),$$

*where the direct limit is taken with respect to inflation maps, and these isomorphisms are natural in $A$.*

PROOF. It suffices to check that we have natural isomorphisms

$$C^i_{\text{cts}}(G,A) \cong \varinjlim_{N\in\mathscr{U}} C^i(G/N,A^N)$$

commuting with connecting homomorphisms. We verify the isomorphism, which then clearly has the other properties. Let $f\colon G^i \to A$ be continuous. Since $G$ is compact and $A$ is discrete, the image of $f$ is finite. For each $a \in \operatorname{im} f$, let $M_a \in \mathscr{U}$ be such that $a \in A^{M_a}$. Then $M = \bigcap_{a\in\operatorname{im} f} M_a \in \mathscr{U}$, and $\operatorname{im} f \subset A^M$.

We next check that $f$ factors through $(G/H)^i$ for an open subgroup $H \in \mathscr{U}$. For this, note that the continuity of $f$ forces it to be constant on an open neighborhood of any $x \in G^i$, and inside such a neighborhood is a neighborhood of the form $x\prod_{j=1}^i H_j(x)$ with $H_j$ an open normal subgroup of $G$. Take $H(x) = \bigcap_{j=1}^i H_j(x)$, which again is an open normal subgroup, so $f$ is constant on $xH(x)^i$. Now $G^i$ is covered by the $xH(x)^i$ for $x \in G^i$. Compactness of $G^i$ tells us that is a finite subcover corresponding to some $x_1,\dots,x_n \in G^i$. The intersection $H = \bigcap_{k=1}^n H(x_k)$ is then such that $f$ factors through $(G/H)^i$, since for any $y \in G^i$, we have $y \in x_kH(x_k)^i$ for some $k$, and therefore $f$ is constant on $yH \subseteq x_iH(x_i)^i$. Thus $f$ factors through $(G/H)^i$.

We have shown that $f$ is the inflation of a map $(G/H)^i \to A^M$. If we take $N = H \cap M$, then $f$ factors through a map $(G/N)^i \to A^N$, proving the result. □

The notion of a compatible pair passes to profinite group cohomology if we merely suppose that our map of profinite groups is continuous.

DEFINITION 2.2.17. Let $G$ and $G'$ be profinite groups, $A$ a discrete $G$-module and $A'$ a $G'$-module. We say that a pair $(\rho,\lambda)$ with $\rho\colon G' \to G$ a continuous group homomorphism and $\lambda : A \to A'$ a group homomorphism is *compatible* if

$$\lambda(\rho(g')a) = g'\lambda(a)$$

for all $a \in A$ and $g' \in G'$.

Consequently, we have inflation, restriction, and conjugation maps as in Definition 1.8.6 and Proposition 1.8.12 so long as the subgroup is taken to be closed, which insures that it is a profinite group. By Proposition 2.2.16 and exactness of the direct limit, it is easy to see that these maps are just direct limits of the analogous maps for usual group cohomology under inflation, as holds for any map on profinite cohomology induced by a compatible pair. In fact, we also have corestriction, defined simply as the direct limit of corestriction maps at finite level. Moreover, the inflation-restriction sequence is still exact, and this works for any closed normal subgroup. We state the higher degree version of this result for later use.

PROPOSITION 2.2.18. *Let $G$ be a profinite group, let $N$ be a closed normal subgroup of $G$, and let $A$ be a discrete $G$-module. Let $i \geq 1$, and suppose that $H^j(N,A) = 0$ for all $j \leq i-1$. Then the sequence*

$$0 \to H^i(G/N,A^N) \xrightarrow{\text{Inf}} H^i(G,A) \xrightarrow{\text{Res}} H^i(N,A)$$

*is exact.*

## 2.3. Galois theory of infinite extensions

Recall that an algebraic extension of fields $L/K$ is Galois if it is normal, so that every polynomial in $K[x]$ that has a root in $L$ splits completely, and separable, so that no irreducible polynomial in $K[x]$ has a double root in $L$. The Galois group $\mathrm{Gal}(L/K)$ of such an extension is the group of automorphisms of $L$ that fix $K$.

In the setting of finite Galois extensions $L/K$, the subfields $E$ of $L$ containing $K$ are in one-to-one correspondence with the subgroups $H$ of $\mathrm{Gal}(L/K)$. In fact, the maps $E \mapsto \mathrm{Gal}(L/E)$ and $H \mapsto L^H$ give inverse bijections between these sets. This is not so in the setting of infinite Galois extensions, where there are rather more subgroups than there are subfields. To fix this issue, we place a topology on $\mathrm{Gal}(L/K)$ and consider only the closed subgroups under this topology. The above-described correspondences then work exactly as before.

PROPOSITION 2.3.1. *Let $L/K$ be a Galois extension of fields. Let $\mathscr{E}$ denote the set of finite Galois extensions of $K$ contained in $L$, ordered by inclusion. This is a directed set. Let $\rho$ be the map*

$$\rho\colon \mathrm{Gal}(L/K) \to \varprojlim_{E\in\mathscr{E}} \mathrm{Gal}(E/K)$$

*defined by the universal property of the inverse limit, with the maps $\mathrm{Gal}(E'/K) \to \mathrm{Gal}(E/K)$ for $E, E' \in \mathscr{E}$ with $E \subseteq E'$ and the maps $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ for $E \in \mathscr{E}$ being restriction maps. Then $\rho$ is an isomorphism.*

PROOF. Let $\sigma \in \mathrm{Gal}(L/K)$. If $\sigma|_E = 1$ for all $E \in \mathscr{E}$, then since

$$L = \bigcup_{E\in\mathscr{E}} E,$$

we have that $\sigma = 1$. On the other hand, if elements $\sigma_E \in \mathrm{Gal}(E/K)$ for each $E \in \mathscr{E}$ are compatible under restriction, then define $\sigma \in \mathrm{Gal}(L/K)$ by $\sigma(\alpha) = \sigma_E(\alpha)$ if $\alpha \in E$. Then, if $\alpha \in E'$ for some $E' \in \mathscr{E}$ as well, then

$$\sigma_{E'}(\alpha) = \sigma_{E\cap E'}(\alpha) = \sigma_E(\alpha),$$

noting that $E \cap E' \in \mathscr{E}$. Therefore, $\sigma$ is well-defined, and so $\rho$ is bijective. □

Proposition 2.3.1 gives us an obvious topology to place on the Galois group of a Galois extension.

DEFINITION 2.3.2. Let $L/K$ be a Galois extension of fields. The *Krull topology* on $\mathrm{Gal}(L/K)$ is the unique topology under which the set of $\mathrm{Gal}(L/E)$ for $E/K$ finite Galois with $E \subseteq L$ forms a basis of open neighborhoods of 1.

REMARK 2.3.3. The Krull topology agrees with the inverse limit topology induced by the isomorphism of Proposition 2.3.1, since

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) \to 1$$

is exact. Therefore, if $L/K$ is Galois, then $\mathrm{Gal}(L/K)$ is a topological group under the Krull topology.

LEMMA 2.3.4. *Let $L/K$ be a Galois extension of fields. The open subgroups in $\mathrm{Gal}(L/K)$ are exactly those subgroups of the form $\mathrm{Gal}(L/E)$ with $E$ an intermediate field in $L/K$ of finite degree over $K$.*

PROOF. First, let $E$ be an intermediate field in $L/K$ of finite degree. Let $E'$ be the Galois closure of $E$ in $L$, which is of finite degree over $K$. Then $\mathrm{Gal}(L/E')$ is an open normal subgroup under the Krull topology, contained in $\mathrm{Gal}(L/E)$. Since $\mathrm{Gal}(L/E)$ is then a union of left $\mathrm{Gal}(L/E')$-cosets, which are open, we have that $\mathrm{Gal}(L/E)$ is open.

Conversely, let $H$ be an open subgroup in $\mathrm{Gal}(L/K)$. Then $H$ contains $\mathrm{Gal}(L/E)$ for some finite Galois extension $E/K$ in $L$. Any $\alpha \in L^H$, where $L^H$ is the fixed field of $H$ in $L$, is contained in $M^{\mathrm{Gal}(L/E)}$, where $M$ is the Galois closure of $E(\alpha)$. Since the restriction map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(M/E)$ is surjective, we then have $\alpha \in M^{\mathrm{Gal}(M/E)}$. But $M/K$ is finite, so $M^{\mathrm{Gal}(M/E)} = E$ by the fundamental theorem of Galois theory. Thus $L^H \subseteq E$.

Let $\bar{H}$ be the image of $H$ under the restriction map $\pi\colon\ \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. As $\mathrm{Gal}(L/E) \leq H$, we have that $\pi^{-1}(\bar{H}) = H$. We remark that $\bar{H} = \mathrm{Gal}(E/L^H)$, since $\bar{H} = \mathrm{Gal}(E/E^{\bar{H}})$ by the fundamental theorem of Galois theory for finite extensions and $L^H = E^H = E^{\bar{H}}$. But $\pi^{-1}(\bar{H})$ is then $\mathrm{Gal}(L/L^H)$ as well. □

From this, we may derive the following.

LEMMA 2.3.5. *Let $L/K$ be a Galois extension of fields. The closed subgroups of $\mathrm{Gal}(L/K)$ are exactly those of the form $\mathrm{Gal}(L/E)$ for some intermediate field $E$ in the extension $L/K$.*

PROOF. Under the Krull topology on $\mathrm{Gal}(L/K)$, the open subgroups are those of the form $\mathrm{Gal}(L/E)$ with $E/K$ finite. By Lemma 2.1.26, we have therefore that the closed subgroups are those that are intersections of $\mathrm{Gal}(L/E)$ over a set $S$ of finite degree over $K$ intermediate fields $E$. Any such intersection necessarily fixes the compositum $E' = \prod_{E \in S} E$, while if an element of $\mathrm{Gal}(L/K)$ fixes $E'$, then it fixes every $E \in S$, so lies in the intersection. That is, any closed subgroup has the form

$$\mathrm{Gal}(L/E') = \bigcap_{E \in S} \mathrm{Gal}(L/E).$$

□

THEOREM 2.3.6 (Fundamental theorem of Galois theory). *Let $L/K$ be a Galois extension. Then there are inverse one-to-one, inclusion reversing correspondences*

$$\{\text{intermediate extensions in } L/K\} \underset{\theta}{\overset{\psi}{\rightleftarrows}} \{\text{closed subgroups of } \mathrm{Gal}(L/K)\}$$

*given by $\psi(E) = \mathrm{Gal}(L/E)$ for any intermediate extension $E$ in $L/K$ and $\theta(H) = L^H$ for any closed subgroup $H$ of $\mathrm{Gal}(L/K)$. These correspondences restrict to bijections between the normal extensions of $K$ in $L$ and the closed normal subgroups of $\mathrm{Gal}(L/K)$, as well as to bijections between the finite degree (normal) extensions of $K$ in $L$ and the open (normal) subgroups of $\mathrm{Gal}(L/K)$. Moreover, if $E$ is normal over $K$ (resp., $H \trianglelefteq \mathrm{Gal}(L/K)$ is closed), then restriction induces a topological isomorphism*

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \xrightarrow{\sim} \mathrm{Gal}(E/K)$$

(*resp.,* $\mathrm{Gal}(L/K)/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$).

PROOF. We will derive this from the fundamental theorem of Galois theory for finite Galois extensions. Let $E$ be an intermediate extension in $L/K$. Then $E \subseteq L^{\mathrm{Gal}(L/E)}$ by definition. Let $x \in L^{\mathrm{Gal}(L/E)}$. The Galois closure $M$ of $E(x)$ in $L$ is of finite degree over $E$. But every element of $\mathrm{Gal}(M/E)$ extends to an element of $\mathrm{Gal}(L/E)$, which fixes $x$. So $x \in M^{\mathrm{Gal}(M/E)}$, which equals $E$ by fundamental theorem of Galois theory for finite Galois extensions. Since $x$ was arbitrary, we have $E = L^{\mathrm{Gal}(L/E)}$. In other words, $\theta(\psi(E)) = E$.

Let $H$ be a closed subgroup of $\mathrm{Gal}(L/K)$. In Lemma 2.3.5, we saw that $H = \mathrm{Gal}(L/E)$ for some intermediate $E$ in $L/K$. Since $E = L^{\mathrm{Gal}(L/E)} = L^H$ from what we have shown, we have that $H = \mathrm{Gal}(L/L^H)$. Therefore, $\psi(\theta(H)) = H$. It follows that we have the desired inclusion-reserving one-to-one correspondences. The other claims are then easily checked and are left to the reader. □

DEFINITION 2.3.7. A *separable closure* of a field $L$ is any field that contains all roots of all separable polynomials in $L$.

NOTATION 2.3.8. We typically denote a separable closure of $L$ by $L^{\mathrm{sep}}$.

REMARK 2.3.9. If one fixes an algebraically closed field $\Omega$ containing $L$, then there is a unique separable closure of $L$ in $\Omega$, being the subfield generated by the roots of all separable polynomials in $L[x]$.

DEFINITION 2.3.10. The *absolute Galois group* of a field $K$ is the Galois group

$$G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K),$$

where $K^{\mathrm{sep}}$ is a separable closure of $K$.

REMARK 2.3.11. The absolute Galois group, despite the word "the", is not unique, but rather depends on the choice of separable closure. An isomorphism of separable closures gives rise to a canonical isomorphism of absolute Galois groups, however.

EXAMPLE 2.3.12. Let $q$ be a power of a prime number. Then there is a unique topological isomorphism $G_{\mathbb{F}_q} \xrightarrow{\sim} \hat{\mathbb{Z}}$ sending the Frobenius automorphism $\varphi_q\colon x \mapsto x^q$ to 1. To see this, note that $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathbb{Z}/n\mathbb{Z}$ given by sending $\varphi_q$ to 1 is an isomorphism, and these give rise to compatible isomorphisms in the inverse limit

$$G_{\mathbb{F}_q} \xrightarrow{\sim} \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \hat{\mathbb{Z}}.$$

EXAMPLE 2.3.13. Let $\mathbb{Q}(\mu_{p^\infty})$ denote the field given by adjoining all $p$-power roots of unity to $\mathbb{Q}$. Then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times$$

the middle isomorphisms arising from the $p^n$th cyclotomic characters.

TERMINOLOGY 2.3.14. The isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times$ of Example 2.3.13 called the *$p$-adic cyclotomic character*.

Since the compositum of two abelian extensions of a field inside a fixed algebraic closure is abelian, the following makes sense.

NOTATION 2.3.15. Let $K$ be a field. The *maximal abelian extension* of $K$ inside an algebraic closure of $K$ is denoted $K^{\mathrm{ab}}$.

REMARK 2.3.16. The abelianization $G_K^{\mathrm{ab}}$ of the absolute Galois group $G_K$ of a field $K$ canonically isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ via the map induced by restriction on $G_K$.

## 2.4. Galois cohomology

DEFINITION 2.4.1. Let $L/K$ be a Galois extension of fields, and let $A$ be a discrete $\mathrm{Gal}(L/K)$-module with respect to the Krull topology on $\mathrm{Gal}(L/K)$. For $i \geq 0$, the *$i$th Galois cohomology group* of $L/K$ with coefficients in $A$ is the profinite cohomology group $H^i(\mathrm{Gal}(L/K), A)$.

EXAMPLE 2.4.2. Let $L/K$ be a Galois extension with Galois group $G$. Then the additive and multiplicative groups of $L$ are discrete $G$-modules. That is, $L$ is the union of the finite Galois subextensions $E$ of $K$ in $L$, and $E = L^{\mathrm{Gal}(L/E)}$ by the fundamental theorem of infinite Galois theory.

Hilbert's Theorem 90 admits the following generalization to Galois cohomology.

THEOREM 2.4.3. *Let $L/K$ be a Galois extension of fields. Then $H^1(\mathrm{Gal}(L/K), L^\times) = 0$.*

PROOF. Let $\mathscr{E}$ denote the set of finite Galois extensions of $K$ in $L$. Then

$$H^1(\mathrm{Gal}(L/K), L^\times) = \varinjlim_{E \in \mathscr{E}} H^1(\mathrm{Gal}(E/K), E^\times),$$

which reduces us to the case that $L/K$ is finite Galois. Let $G = \mathrm{Gal}(L/K)$, and let $f\colon G \to L^\times$ be a 1-cocycle. We may view the elements $\sigma \in G$ as abelian characters $L^\times \to L^\times$. As distinct characters

of $L^\times$, these characters form a linearly independent set. The sum $\sum_{\sigma\in G} f(\sigma)\sigma$ is therefore a nonzero map $L^\times \to L$. Let $\alpha \in L^\times$ be such that $z = \sum_{\sigma\in G} f(\sigma)\sigma(\alpha) \neq 0$. For any $\tau \in G$, we have

$$\begin{aligned}\tau^{-1}(z) &= \sum_{\sigma\in G} \tau^{-1}(f(\sigma))\cdot\tau^{-1}\sigma(\alpha) = \sum_{\sigma\in G} \tau^{-1}(f(\tau\sigma))\sigma(\alpha)\\ &= \sum_{\sigma\in G} \tau^{-1}(f(\tau)\cdot\tau f(\sigma))\sigma(\alpha) = \tau^{-1}(f(\tau))\sum_{\sigma\in G} f(\sigma)\sigma(\alpha) = \tau^{-1}(f(\tau))z.\end{aligned}$$

Thus,

$$f(\tau) = \frac{z}{\tau(z)},$$

so $f$ is the 1-coboundary of $z^{-1}$. □

This has the usual statement of Hilbert's Theorem 90 as a corollary.

COROLLARY 2.4.4. *Let $L/K$ be a finite cyclic extension of fields, and let $N_{L/K}\colon L^\times \to K^\times$ be the norm map. Then*

$$\ker N_{L/K} = \left\{\alpha \in L^\times \mid \alpha = \tfrac{\sigma(\beta)}{\beta} \text{ for some } \beta \in L^\times\right\},$$

*where $\sigma$ is a generator of* $\mathrm{Gal}(L/K)$.

PROOF. Since $\sigma$ generates $G = \mathrm{Gal}(L/K)$, the element $\sigma - 1 \in \mathbb{Z}[G]$ generates $I_G$, and so the statement at hand is $\ker N_{L/K} = I_G L^\times$, which is to say $\hat{H}^{-1}(G, L^\times) = 0$. Since $G$ is cyclic, we have $\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times)$. Thus, the result follows from Theorem 2.4.3. □

For the additive group, we have the following much stronger generalization of the additive version of Hilbert's Theorem 90.

THEOREM 2.4.5. *Let $L/K$ be a Galois extension of fields. Then $H^i(\mathrm{Gal}(L/K), L) = 0$ for all $i \geq 1$.*

PROOF. As in the proof of Theorem 2.4.3, this reduces quickly to the case that $L/K$ is finite, which we therefore suppose. As a $K[G]$-module, $L$ is free on a single generator by the normal basis theorem, and therefore it is isomorphic to

$$Z[G] \otimes_{\mathbb{Z}} K \cong \mathrm{Ind}^G(K) \cong \mathrm{CoInd}^G(K).$$

So, the result follows from the acyclicity of coinduced modules. □

NOTATION 2.4.6. For a field $K$, we let $K^{\mathrm{sep}}$ denote a fixed separable closure and $G_K$ denote its absolute Galois group.

DEFINITION 2.4.7. The Brauer group $\mathrm{Br}(K)$ of a field $K$ is $H^2(G_K, (K^{\mathrm{sep}})^\times)$.

We have the following inflation-restriction theorem for Brauer groups.

PROPOSITION 2.4.8. *For any Galois extension $L/K$, there is an exact sequence*

$$0 \to H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L)$$

*of abelian groups.*

PROOF. Let $K^{\mathrm{sep}}$ be a separable closure of $K$ containing $L$. Note that $((K^{\mathrm{sep}})^\times)^{G_L} = L^\times$ by the fundamental theorem of Galois theory, and we have $H^1(G_L, (K^{\mathrm{sep}})^\times) = 0$ by Theorem 2.4.3. The sequence is then just the inflation-restriction sequence of Proposition 2.2.18 for $i = 2$, $G = G_K$, $N = G_L$, and $A = (K^{\mathrm{sep}})^\times$. □

EXAMPLE 2.4.9. Consider the finite field $\mathbb{F}_q$ for a prime power $q$. For $n \geq 1$, we know that $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of degree $n$, so we have an isomorphism

$$H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \hat{H}^0(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) \cong \mathbb{F}_q^\times / N_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{F}_{q^n}^\times.$$

Now, any the norm of a primitive $(q^n - 1)$th root of unity $\xi$ is

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\xi) = \prod_{i=0}^{n-1} \xi^{q^i} = \xi^{\frac{q^n-1}{q-1}},$$

which is a primitive $(q-1)$th root of unity. In other words, the norm map is surjective, so

$$\mathrm{Br}(\mathbb{F}_q) = \varinjlim_n H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = 0.$$

## 2.5. Kummer theory

NOTATION 2.5.1. For a field $K$ of characteristic not dividing $n \geq 1$, we use $\mu_n$ to denote the group of $n$th roots of unity in $K^{\mathrm{sep}}$.

NOTATION 2.5.2. For an abelian group $A$ and $n \geq 1$, let $A[n]$ denote the elements of exponent dividing $n$ in $A$.

EXAMPLE 2.5.3. We have $K^{\mathrm{sep}}[n] = \mu_n$ for any $n \geq 1$ not divisible by $\mathrm{char}(K)$.

PROPOSITION 2.5.4. *Let $K$ be a field of characteristic not dividing $n \geq 1$, and let $\mu_n$ be the group of roots of unity in a separable closure $K^{\mathrm{sep}}$ of $K$. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group. Then there are canonical isomorphisms*

$$K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n) \quad \text{and} \quad H^2(G_K, \mu_n) \xrightarrow{\sim} \mathrm{Br}_K[n].$$

PROOF. Since $K^{\mathrm{sep}}$ is separably closed, we have an exact sequence

$$1 \to \mu_n \to (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \to 1 \tag{2.5.1}$$

of discrete $G_K$-modules. By Hilbert's Theorem 90, the long exact sequence attached to (2.5.1) breaks into exact sequences

$$K^\times \xrightarrow{n} K^\times \to H^1(G_K, \mu_n) \to 0 \quad \text{and} \quad 0 \to H^2(G_K, \mu_n) \to \mathrm{Br}(K) \xrightarrow{n} \mathrm{Br}(K).$$

□

TERMINOLOGY 2.5.5. The sequence in (2.5.1) is often called a *Kummer sequence*.

DEFINITION 2.5.6. Let $K$ be a field of characteristic not dividing $n \geq 1$, let $a \in K^\times$, and choose an $n$th root $\alpha \in (K^{\mathrm{sep}})^\times$ of $a$. The *Kummer cocycle* $\chi_a \colon G_K \to \mu_n$ attached to $a$ (or more precisely, $\alpha$) is the 1-cocycle defined on $\sigma \in G_K$ by

$$\chi_a(\sigma) = \frac{\sigma(\alpha)}{\alpha}.$$

REMARKS 2.5.7. We maintain the notation of Definition 2.5.6.

a. If $\mu_n \subset K$, then $\chi_a$ is independent of the choice of $\alpha$ and is in fact a group homomorphism, since $G_K$ acts trivially on $\mu_n$. In this case, we refer to $\chi_a$ as the *Kummer character* attached to $a$.

b. The class of $\chi_a$ in $H^1(G_K, \mu_n)$ is independent of the choice of $\alpha$, as the difference between two such choices is the 1-coboundary of an $n$th root of unity.

LEMMA 2.5.8. *Let $K$ be a field of characteristic not dividing $n \geq 1$. Then the isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Proposition 2.5.4 takes the image of $a \in K^\times$ to $\chi_a$.*

PROOF. The connecting homomorphism yielding the map is the snake lemma map in the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mu_n & \longrightarrow & (K^{\mathrm{sep}})^\times & \xrightarrow{n} & (K^{\mathrm{sep}})^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \downarrow{\scriptstyle d^0} & & \\
0 & \longrightarrow & Z^1(G_K, \mu_n) & \longrightarrow & Z^1(G_K, (K^{\mathrm{sep}})^\times) & \xrightarrow{n} & Z^1(G_K, (K^{\mathrm{sep}})^\times) & \longrightarrow & 0,
\end{array}$$

so given on $a \in K^\times$ by picking $\alpha \in (K^{\mathrm{sep}})^\times$ with $\alpha^n = a$, taking $d^0(\alpha) \in Z^1(G_K, K^\times)$ and noting that it takes values in $\mu_n$. Since $d^0(\alpha) = \chi_a$ by definition, we are done. □

TERMINOLOGY 2.5.9. The isomorphism $K^\times/K^{\times n} \xrightarrow{\sim} H^1(G_K, \mu_n)$ of Lemma 2.5.8 is called the *Kummer isomorphism*.

PROPOSITION 2.5.10. *Let $L/K$ be a Galois extension of fields of characteristic not dividing $n \geq 1$, and suppose that $\mu_n$ is contained in $L$. Then the Kummer isomorphism restricts to an isomorphism*

$$(K^\times \cap L^{\times n})/K^{\times n} \xrightarrow{\sim} H^1(\mathrm{Gal}(L/K), \mu_n).$$

PROOF. This is a simple consequence of the inflation-restriction sequence combined with the Kummer isomorphisms for $K$ and $L$. These yield a left exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), \mu_n) \to K^\times/K^{\times n} \to L^\times/L^{\times n}$$

that provides the isomorphism. □

PROPOSITION 2.5.11. *Let $K$ be a field of characteristic not dividing $n \geq 1$, and suppose that $K$ contains the $n$th roots of unity. Let $L/K$ be a cyclic extension of degree $n$. Then $L = K(\sqrt[n]{a})$ for some $a \in K^\times$.*

PROOF. Let $\zeta$ be a primitive $n$th root of unity in $K$. Note that $N_{L/K}(\zeta) = \zeta^n = 1$, so Hilbert's Theorem 90 tells us that there exists $\alpha \in L$ and a generator $\sigma$ of $\mathrm{Gal}(L/K)$ with $\frac{\sigma(\alpha)}{\alpha} = \zeta$. Note that

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma^i \alpha = \prod_{i=1}^{n} \zeta^i \alpha = \zeta^{n(n-1)/2} \alpha^n = (-1)^{n-1} \alpha^n,$$

so setting $a = -N_{L/K}(-\alpha)$, we have $\alpha^n = a$. Since $\alpha$ has $n$ distinct conjugates in $L$, we have that $L = K(\alpha)$. □

NOTATION 2.5.12. Let $\Delta$ be a subset of a field $K$, and let $n \geq 1$ be such that $K$ contains the $n$th roots of unity in $\overline{K}$. Then the field $K(\sqrt[n]{\Delta})$ is the field given by adjoining an $n$th root of each element of $\Delta$ to $K$.

THEOREM 2.5.13 (Kummer duality). *Let $K$ be a field of characteristic not dividing $n \geq 1$, and suppose that $K$ contains the $n$th roots of unity. Let $L$ be an abelian extension of $K$ of exponent dividing $n$, and set $\Delta = L^{\times n} \cap K^\times$. Then $L = K(\sqrt[n]{\Delta})$, and there is a perfect bimultiplicative pairing*

$$\langle\ ,\ \rangle \colon \mathrm{Gal}(L/K) \times \Delta/K^{\times n} \to \mu_n$$

*given by $\langle \sigma, a \rangle = \chi_a(\sigma)$ for $\sigma \in \mathrm{Gal}(L/K)$ and $a \in \Delta$.*

PROOF. Since $\mu_n \subset K$, Proposition 2.5.10 tells us that the map taking $a \in \Delta$ to its Kummer cocycle $\chi_a$ yields

$$\Delta/K^{\times n} \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n).$$

This isomorphism gives rise to the bimultiplicative pairing $\langle\ ,\ \rangle$, and it implies that any $a \in \Delta/K^{\times n}$ of order $d$ dividing $n$ pairs with some element of $\mathrm{Gal}(L/K)$ to a $d$th root of unity. It remains to show that the pairing also induces an isomorphism

$$\mathrm{Hom}(\Delta/K^{\times n}, \mu_n) \cong \mathrm{Gal}(L/K).$$

Clearly, $K(\sqrt[n]{\Delta})$ is contained in $L$. On the other hand, $L/K$ is a compositum of cyclic extensions of exponent dividing $n$, we have by Proposition 2.5.11 that $L = K(\sqrt[n]{\Gamma})$ for some subset $\Gamma$ of $K^\times$, which then can be taken to be $\Delta$. So, let $\sigma \in \mathrm{Gal}(L/K)$ be of order $d$ dividing $n$. Since $L = K(\sqrt[n]{\Delta})$, we have that there exists $a \in \Delta$ such that $\sigma(\sqrt[n]{\alpha})/\sqrt[n]{\alpha}$ is a primitive $d$th root of unity times $\sqrt[n]{\alpha}$. Hence, the pairing is perfect. □

REMARK 2.5.14. One may replace $\Delta$ in Theorem 2.5.13 by any $\Gamma \subseteq \Delta$ with $\Delta = \Gamma K^{\times n}$. Then $\Delta/K^{\times n}$ should be replaced by the isomorphic $\Gamma/(\Gamma \cap K^{\times n})$.

REMARK 2.5.15. The pairing of Proposition 2.5.13 is perfect with respect to the Krull topology on $\mathrm{Gal}(L/K)$ and the discrete topology on $\Delta$.

TERMINOLOGY 2.5.16. We say that $\mathrm{Gal}(L/K)$ and $\Delta/K^{\times n}$ in Proposition 2.5.13 are *Kummer dual* to each other.

COROLLARY 2.5.17. *Let $K$ be a field of characteristic not dividing $n \geq 1$, and suppose that $K$ contains the $n$th roots of unity. The Galois group of the maximal abelian extension of $K$ of exponent $n$ is Kummer dual to $K^\times/K^{\times n}$.*

REMARK 2.5.18. Suppose that $K$ contains $\mu_n$, where $n$ is not divisible by the residue characteristic of $K$. Let $L/K$ be abelian of exponent $n$ and $G = \mathrm{Gal}(L/K)$. Write $L = K(\sqrt[n]{\Delta})$ for some $\Delta \leq K^\times$. Then $L_d = K(\sqrt[d]{\Delta})$ is the maximal subextension of exponent dividing $d$, and $G_d = \mathrm{Gal}(L_d/K) \cong G/G^d$. Moreover, we have a commutative diagram of pairings

$$\begin{array}{ccc} G \times \Delta/(\Delta \cap K^{\times n}) & \xrightarrow{\langle\ ,\ \rangle} & \mu_n \\ \downarrow & & \downarrow \\ G_d \times \Delta/(\Delta \cap K^{\times d}) & \xrightarrow{\langle\ ,\ \rangle_d} & \mu_d, \end{array}$$

where the left vertical map is the direct product of the restriction (or the quotient map) with the map induced by the identity and the map $\mu_n \to \mu_d$ is the $n/d$-power map. That is, we have

$$\langle \sigma, a \rangle_d = \frac{\sigma(\sqrt[d]{a})}{\sqrt[d]{a}} = \left( \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \right)^{n/d} = \langle \sigma, a \rangle^{n/d},$$

where $\sigma$ denotes both an element of $G$ and its image in $G_d$ and $a$ denotes the image of an element of $\Delta$. In particular, the composition

$$G \to \mathrm{Hom}(\Delta, \mu_n) \to \mathrm{Hom}(\Delta, \mu_d)$$

in which the first map is given by $\langle\ ,\ \rangle$ and the second by the $(n/d)$-power map agrees with the map $G \to \mathrm{Hom}(\Delta, \mu_d)$ given by $\langle\ ,\ \rangle_d$.

REMARK 2.5.19. By Kummer duality, if $K$ has characteristic 0 and contains all roots of unity, then

$$G_K^{\mathrm{ab}} \cong \varprojlim_n G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^n \cong \varprojlim_n \mathrm{Hom}(K^\times, \mu_n) \cong \varprojlim_n \mathrm{Hom}_{\mathrm{cts}}(\widehat{K^\times}, \mu_n) \cong \mathrm{Hom}_{\mathrm{cts}}\left(\widehat{K^\times}, \varprojlim_n \mu_n\right),$$

where $\widehat{K^\times}$ denotes the profinite completion of $K^\times$.

EXAMPLE 2.5.20. Let $K$ be a field of characteristic not $p$ containing the group $\mu_{p^\infty}$ of all $p$-power roots of unity, and let $a \in K^\times$ with $a \notin K^{\times p}$. Then the field $L = K(\sqrt[p^\infty]{a})$ given by adjoining all $p$-power roots of $a$ to $K$ is the union of the fields $L_n = K(\sqrt[p^n]{a})$, each of which has degree $p^n$ over $K$ by Theorem 2.5.13 since $a$ has order $p^n$ in $K^\times/K^{\times p^n}$. Let $\Delta = \langle a \rangle$. Then

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(L_n/K) \cong \varprojlim_n \mathrm{Hom}(\Delta, \mu_{p^n}) \cong \varprojlim_n \mu_{p^n} \cong \mathbb{Z}_p,$$

since a homomorphism from $\Delta$ is determined by where it sends $a$.

DEFINITION 2.5.21. Let $K$ be a field of characteristic $p$. The *Tate module* $\mathbb{Z}_p(1)$ is the topological $G_K$-module that is $\mathbb{Z}_p$ as a topological group together with the action of the $G_K$ given by

$$\sigma \cdot a = \chi(\sigma)a$$

for $a \in \mathbb{Z}_p$, where $\chi\colon G_K \to \mathbb{Z}_p^\times$ is the $p$-adic cyclotomic character.

REMARK 2.5.22. Let $K$ be a field of characteristic not $p$, set $G = \mathrm{Gal}(K(\mu_{p^\infty})/K)$. The group

$$T_p = \varprojlim_n \mu_{p^n}$$

is a Galois module also referred to as the Tate module, the action of $G$ given by multiplication by the $p$-adic cyclotomic character $\chi\colon G \to \mathbb{Z}_p^\times$ (which factors through $G$) in the sense that

$$\sigma((\xi_n)_n) = (\xi_n^{\chi(\sigma)})_n$$

for all $(\xi_n)_n \in T_p$. The group $T_p$ is noncanonically topologically isomorphic to the Tate module $\mathbb{Z}_p(1)$, with the isomorphism given by choice of a compatible sequence $(\zeta_{p^n})_n$ of primitive $p^n$th roots of unity, which is taken to 1.

EXAMPLE 2.5.23. Let $K$ be a field of characteristic not $p$ and $a \in K^\times - K^{\times p}$. Set $L = K(\mu_{p^\infty})$ and $M = L(\sqrt[p^\infty]{a})$. By Example 2.5.20, we know that $\mathrm{Gal}(M/L) \cong \mathbb{Z}_p$ as topological groups. But note that $M/K$ is Galois. In fact, take $\sigma \in \mathrm{Gal}(L/K)$ and lift it to an embedding $\delta$ of $M$ into a separable closure of $M$. Then

$$\tilde{\sigma}(\sqrt[p^n]{a})^{p^n} = a,$$

so $\tilde{\sigma}(\sqrt[p^n]{a}) = \xi \sqrt[p^n]{a}$ for some $p^n$th root of unity $\xi$, which is in $M$ by definition. To determine the Galois group, take $\tau \in \mathrm{Gal}(M/L)$, and let $\zeta$ be the $p^n$th root of unity such that $\tau(\sqrt[p^n]{a}) = \zeta \sqrt[p^n]{a}$. For $n \geq 1$, we then have

$$\tilde{\sigma}\tau\tilde{\sigma}^{-1}(\sqrt[p^n]{a}) = \tilde{\sigma}(\tau(\tilde{\sigma}^{-1}(\xi^{-1})\sqrt[p^n]{a})) = \tilde{\sigma}(\sigma^{-1}(\xi^{-1})\zeta\sqrt[p^n]{a}) = \sigma(\zeta)\sqrt[p^n]{a} = \zeta^{\chi(\sigma)}\sqrt[p^n]{a},$$

where $\chi$ is the $p$-adic cyclotomic character. In other words, we have

$$\mathrm{Gal}(M/L) \cong \mathrm{Gal}(M/L) \rtimes \mathrm{Gal}(L/K) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^\times,$$

where through the conjugation action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$, the latter module is isomorphic to the Tate module $\mathbb{Z}_p(1)$.