

Group cohomology

and a few things you can do with it

Siggy Moore

Advisor: Y. S. Tai

Helpful feedback: Josh Sabloff

May 1, 2009

Contents

0	Introduction	2
1	Algebra background	3
1.1	The group ring	3
1.2	Exact sequences	3
1.3	Free and projective modules	6
1.4	The functor Hom	7
1.5	Semidirect products	8
1.6	Some results in field theory	9
1.7	Limits	10
2	Cohomology	11
2.1	Cohomology of complexes	11
2.1.1	Induced maps on homology and cohomology	12
2.2	Cohomology of groups	14
2.2.1	Induced homomorphisms on group cohomology	16
2.3	Cohomology of cyclic groups	18
2.4	The bar resolution	20
3	Applications of group cohomology	22
3.1	Group extensions	22
3.1.1	Classifying splittings	23
3.1.2	Classifying extensions with abelian kernel	23
3.2	Galois cohomology	25
3.2.1	The Galois cohomology groups	26
3.2.2	Classification of cyclic extensions	28
4	Glossary	31
	References	33

0 Introduction

The study of homology began in topology. Originally, it was conceived as a process to count the n -dimensional “holes” in a topological space. Cohomology developed some time afterwards. It is the category theoretic dual to singular homology—the most general topological homology theory. But the machinery of cohomology can also be applied in a fairly natural way to generalized group representations known as G -modules. Properties of both the group and the representation can be deduced by studying the results obtained in this way.

More concretely, cohomology and homology both are families of functors which yield abelian groups. They are indexed by integers (usually nonnegative) and often have a second argument which is a ring or module to be used as coefficients. Therefore, one speaks of “the n th homology group of X with coefficients in A ”, written $H_n(X, A)$. Cohomology groups are written with an upper index: $H^n(X, A)$. If the coefficient ring or module is omitted it is generally assumed to be \mathbb{Z} .

Even before cohomology was adapted to study groups, essentially equivalent tools were used to solve problems including that of group extensions: if we have groups A and G the problem is to find a group E containing A as a normal subgroup and such that the quotient E/A is isomorphic to G . The “derivations” and “factor sets” that were invented in the solution to this problem are in fact elements of the first and second cohomology groups $H^1(G, A)$ and $H^2(G, A)$.

The cohomology of a Galois group is of particular interest. Being groups of automorphisms, Galois groups have natural representations that can be viewed as G -modules. The calculation of the cohomology of these representations is a more sophisticated way of accomplishing classifications of field extensions such as Kummer theory and Artin-Schreier theory. One of the earliest achievements in the field of Galois cohomology, Hilbert’s Theorem 90, is crucial in proving a fundamental result in Galois theory.

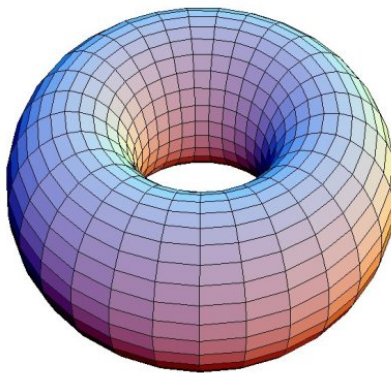


Figure 1: A torus has two one-dimensional holes and one two-dimensional hole. Its first and second homology groups are thus $\mathbb{Z} \times \mathbb{Z}$ and \mathbb{Z} , respectively.

1 Algebra background

The following is some algebra that will be necessary for the material in later sections. We will assume that the reader is familiar with the theory of groups, rings, fields, modules and finite Galois extensions. Basic familiarity with category theory also will be assumed.

1.1 The group ring

Let G be a group. The multiplication in G induces a product on the free abelian group on elements of G defined by

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{hk=g} a_h b_k \right) g.$$

This makes the free group into a ring called the **integral group ring** and denoted $\mathbb{Z}G$ or $\mathbb{Z}[G]$. The group ring of the infinite cyclic group, for example, is $\mathbb{Z}[\mathbb{Z}] = \Lambda$, the ring of Laurent polynomials.

The group ring is characterized by the following universal mapping property:

Theorem 1.1.1 ([7]). *For any ring R with unit, ring homomorphisms $\rho : \mathbb{Z}G \rightarrow R$ are in bijective correspondence with group homomorphisms $\mu : G \rightarrow U(R)$ of G into the group of units of R .*

Proof. The group of units of $\mathbb{Z}G$ contains G as a subgroup; as a set it is $\{1g : g \in G\}$. Any $\rho : \mathbb{Z}G \rightarrow R$ will therefore restrict to a group homomorphism of G into the multiplicative monoid of R . The image of G must be a group, so it is contained in $U(R)$. If we start with $\mu : G \rightarrow U(R)$, simply define $\rho(\sum a_g g) = \sum a_g \mu(g)$, which is easily verified to be a ring homomorphism. \square

An abelian group A is given a **G-module** structure by a homomorphism $\phi : G \rightarrow \text{Aut}(A)$. Because of the theorem, this is equivalent to a $\mathbb{Z}G$ -module structure on A . This means that we can treat them as we would modules over any other ring. A G -module is actually a generalization of a linear representation of G . To see this, consider a representation $\alpha : G \rightarrow \text{GL}_n(\mathbb{R})$. Since every invertible $n \times n$ matrix represents an invertible linear transformation of \mathbb{R}^n into itself, each element of $\text{GL}_n(\mathbb{R})$ is an automorphism of the additive group \mathbb{R}^n . Thus, α defines a G -module structure on \mathbb{R}^n .

Any abelian group can be considered a **trivial G-module** by the homomorphism $\phi = 0$, that is, by defining $ga = a$ for all $g \in G$.

1.2 Exact sequences

Exact sequences occur in a variety of different categories. There are exact sequences of modules, groups, and even chain complexes (cf. Section 2.1.1). In the greatest generality, if \mathcal{C} is any category with kernels and images, a sequence

$\cdots \rightarrow A_{n-1} \xrightarrow{\alpha} A_n \xrightarrow{\beta} A_{n+1} \rightarrow \cdots$ of objects and morphisms in \mathcal{C} is **exact at** A_n if $\ker \beta = \text{im } \alpha$.

A **short exact sequence** is a sequence of the form $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ exact at A , B and C . The morphisms $\alpha : A \rightarrow B$ and $\beta : B \rightarrow C$ fit in a short exact sequence if and only if α is monic, β is epic and $\ker \beta = \text{im } \alpha$. In most categories (at least in the categories mentioned above) this means that α is injective and β is surjective. Another formulation in the category of groups is that A , B and C fit in a short exact sequence if and only if $A \triangleleft B$ and $C \cong B/A$. The morphisms in this case are the inclusion of A in B and then the projection onto the quotient.

A short exact sequence with morphisms α and β is **split** if there is a morphism s that is a right inverse for β . For example, the sequence $0 \rightarrow A \rightarrow A \oplus B \rightarrow B \rightarrow 0$ is exact and is split by the canonical injection $B \rightarrow A \oplus B$. The exact sequence $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$, where the second map is multiplication by n and the third is the projection onto the quotient, is not a split exact sequence. This is evident from the observation that $\mathbb{Z}/n\mathbb{Z}$ admits only the zero homomorphism into \mathbb{Z} . In the category of groups, split exact sequences correspond to semidirect products (cf. Section 1.5).

A longer sequence may be called exact if it is exact at every intermediate object. If M is an R -module then a **resolution** of M over R is an exact sequence of R -modules of the form $0 \leftarrow M \leftarrow A_0 \leftarrow A_1 \leftarrow A_2 \leftarrow \cdots$. If, for example, $R = \mathbb{Z}[x]$, the additive group \mathbb{Z} is made an R -module by setting $(\sum a_i x^i) n = (\sum a_i) n$. Then a resolution of \mathbb{Z} over R is $0 \leftarrow \mathbb{Z} \leftarrow R \leftarrow R \leftarrow 0$, where the second map is induced by $x \mapsto 1$ and the third is multiplication by $x - 1$. For a more complicated example, let $R = \mathbb{Z}[x]/(x^2 - 1)$. The above module structure on \mathbb{Z} still works here. In this case, a resolution of \mathbb{Z} over R is $0 \leftarrow \mathbb{Z} \leftarrow R \leftarrow R \leftarrow R \leftarrow \cdots$, where the second map again is induced by $x \mapsto 1$ and the subsequent maps alternate between multiplication by $x - 1$ and multiplication by $x + 1$.

Exact sequences are one of the primary objects of study in homological algebra, so here are some useful lemmas concerning them. The snake lemma is a fairly general result in so-called ‘‘abelian categories’’ [8]. This proof works in the category of modules.

Lemma 1.2.1 (Snake lemma). *Given a commutative diagram*

$$\begin{array}{ccccccc}
 A & \xrightarrow{\sigma} & B & \xrightarrow{\tau} & C & \longrightarrow & 0 \\
 \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
 0 & \longrightarrow & A' & \xrightarrow{\sigma'} & B' & \xrightarrow{\tau'} & C'
 \end{array}$$

with exact rows, there is a morphism $\partial : \ker \gamma \rightarrow \text{cok } \alpha$ fitting in the exact sequence

$$\ker \alpha \xrightarrow{\sigma} \ker \beta \xrightarrow{\tau} \ker \gamma \xrightarrow{\partial} \text{cok } \alpha \xrightarrow{\sigma'} \text{cok } \beta \xrightarrow{\tau'} \text{cok } \gamma.$$

The maps labeled σ , τ , σ' and τ' are induced by the maps with the same name in the diagram. In the case of the maps between kernels, the restriction of e.g. σ

to $\ker \alpha$ has its image inside $\ker \beta$ because $\beta\sigma = \sigma'\alpha$ and similarly for τ . As for σ' and τ' , if π is the projection of A' onto $\text{cok } \alpha$ and ρ that of B' onto $\text{cok } \beta$, we would like to factor $\rho\sigma'$ over π . This is possible because $\rho\sigma'\alpha = \rho\beta\sigma = 0$. Thus, $\rho\sigma'$ descends to a homomorphism $\text{cok } \alpha \rightarrow \text{cok } \beta$, which we will also call σ' . The morphism $\tau' : \text{cok } \beta \rightarrow \text{cok } \gamma$ is constructed in the same way. The exact sequence that the lemma gives is sometimes called the **kernel-cokernel sequence**.

Proof. First, we construct ∂ . Take any $c \in \ker \gamma$. As τ is surjective, there is a $b \in B$ such that $\tau b = c$. Notice that $\tau'\beta b = \gamma\tau b = 0$, i.e. $\beta b \in \ker \tau'$. Since the bottom row is exact there is an $a \in A'$ such that $\sigma'a = \beta b$. We define ∂c to be the equivalence class of a in $\text{cok } \alpha$.

We must show that ∂ is well-defined with respect to the choice of b . (Once we obtain b there is only one possible choice for a since σ' is injective.) Suppose $b' \in B$ and $\tau b' = c$. Then $\tau(b' - b) = 0$, so there is an $a'' \in A$ such that $\sigma a'' = b' - b$. As per the construction of ∂ , we choose $a' \in A'$ such that $\sigma'a' = \beta b'$. Now $\sigma'\alpha a'' = \beta\sigma a'' = \beta b' - \beta b = \sigma'a' - \sigma'a$, so $a' - a = \alpha a''$ since σ' is injective. We have now shown that a and a' represent the same equivalence class in $\text{cok } \alpha$.

With ∂ well-defined, we are left with showing exactness of the kernel-cokernel sequence. Exactness at $\ker \beta$ and $\text{cok } \beta$ is quite straightforward, so we will demonstrate the four containments:

im $\tau \subseteq \ker \partial$ Let $b \in \ker \beta$. We would like to show that $\partial\tau b = 0$. In applying ∂ to τb , we may use the b we already have as a preimage of τb under τ . By construction, then, $\partial\tau b$ is a preimage of βb under σ' . But $\beta b = 0$, so we choose $a = 0$.

ker $\partial \subseteq \text{im } \tau$ Suppose $c \in \ker \gamma$ and $\partial c = 0$. This is the zero equivalence class in $\text{cok } \alpha$, so the a we choose in constructing ∂c is $\alpha a'$ for some $a' \in A$. We know $\beta\sigma a' = \beta b$, so $b - \sigma a' \in \ker \beta$. Furthermore, $\tau(b - \sigma a') = \tau b = c$, that is, $b - \sigma a'$ is the desired preimage of c .

im $\partial \subseteq \ker \sigma'$ Let $c \in \ker \gamma$. We would like to show that $\sigma'\partial c = 0$. As per the construction of ∂ , ∂c is the class of a where $\sigma'a = \beta b$ and $\tau b = c$. Then by definition, $\sigma'\partial c$ is the class of $\sigma'a = \beta b$ in $\text{cok } \beta$. This is the zero class, again by definition.

ker $\sigma' \subseteq \text{im } \partial$ Suppose a is a representative of an equivalence class in $\text{cok } \alpha$ whose image under σ' is the zero class, that is, $\sigma'a = \beta b$ for some $b \in B$. Inspection of the construction of ∂ reveals that applying ∂ to τb yields the chosen a , as desired. \square

Lemma 1.2.2 (Short five lemma). *Given a commutative diagram*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\sigma} & B & \xrightarrow{\tau} & C & \longrightarrow & 0 \\
& & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
0 & \longrightarrow & A' & \xrightarrow{\sigma'} & B' & \xrightarrow{\tau'} & C' & \longrightarrow & 0
\end{array}$$

with exact rows, if two of α , β and γ are isomorphisms then so is the third.

In abelian categories, such as the category of modules, the short five lemma is a consequence of the snake lemma [8]. The proof given here applies to short exact sequences of groups as well as of modules.

Proof. We have three cases:

α and β are isomorphisms First, we show that γ is injective. Suppose $c \in \ker \gamma$. As τ is surjective, there is a $b \in B$ such that $\tau b = c$. We know $\tau' \beta b = \gamma \tau b = 0$, so βb has a preimage in A' , which has a preimage $a \in A$ since α is surjective. Now $\beta(b - \sigma a) = \beta b - \sigma' \alpha a = 0$. Injectivity of β shows that, in fact, $b - \sigma a = 0$. Finally, we conclude that $c = \tau b = \tau \sigma a = 0$.

As for surjectivity of γ , let c' be any element of C' . Surjectivity of τ' and β gives a $b \in B$ such that $\tau' \beta b = c'$. Then $\gamma \tau b = \tau' \beta b = c'$, so τb is a preimage of c' under γ .

α and γ are isomorphisms To show that β is injective, let $b \in \ker \beta$. Since $\gamma \tau b = \tau' \beta b = 0$ and γ is injective, $\tau b = 0$. Thus, there is an $a \in A$ with $\sigma a = b$. We have $\sigma' \alpha a = \beta \sigma a = 0$ and $\sigma' \alpha$ is injective, so $a = 0$. Therefore, $b = \sigma a = 0$.

For surjectivity of β , given a $b' \in B'$, there is a $b \in B$ such that $\gamma \tau b = \tau' b$ because $\gamma \tau$ is surjective. Consider $b' - \beta b$. It is in the kernel of τ' because $\tau'(b' - \beta b) = \tau' b' - \gamma \tau b = 0$. Thus, there is an $a' \in A'$ such that $\sigma' a' = b' - \beta b$ and therefore also an $a \in A$ with $\sigma' \alpha a = \sigma' a' = b' - \beta b$. Finally, we find that $\beta(\sigma a + b) = \sigma' \alpha a + \beta b = b'$.

β and γ are isomorphisms Suppose $a \in \ker \alpha$ in order to show that α is injective. We have $\beta \sigma a = \sigma' \alpha a = 0$. Now $\beta \sigma$ is injective, so $a = 0$.

As for surjectivity, let a' be any element of A' . There is a $b \in B$ such that $\beta b = \sigma' a$ because β is surjective. We have $\gamma \tau b = \tau' \beta b = 0$, so $\tau b = 0$ since γ is injective. Thus, there is an $a \in A$ such that $\sigma a = b$. Now $\sigma' \alpha a = \beta \sigma a = \sigma' a$. Conclude that $\alpha a = a'$ because σ' is injective. \square

1.3 Free and projective modules

In this section, let R be a fixed ring with unit.

Recall that an R -module A is **free** if it has a basis, that is, if there is a collection $\{\lambda_i\}_{i \in I}$ of elements of A such that each element $a \in A$ is uniquely expressible as a finite linear combination $a = \sum_{i \in I} a_i \lambda_i$ with coefficients $a_i \in R$. An alternative definition is:

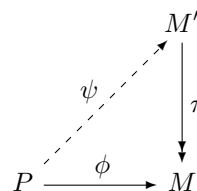
Proposition 1.3.1. *An R -module A is free if and only if $A \cong \bigoplus_{i \in I} R_i$ where each $R_i \cong R$.*

Proof. Let $\{\lambda_i\}_{i \in I}$ be a basis for A over R . Define the homomorphism $\phi : \bigoplus_{i \in I} R_i \rightarrow A$ by $(a_i) \mapsto \sum a_i \lambda_i$. This function is surjective because the basis spans A and injective because it is linearly independent.

On the other hand, if we have an isomorphism $\phi : \bigoplus R_i \rightarrow A$, let $\lambda_i = \phi(1_i)$ for each $i \in I$, where 1_i is the unit in R_i . Note that the collection $\{1_i\}$ is a basis for $\bigoplus R_i$, so $\{\lambda_i\}$ is a basis for A because ϕ is an isomorphism. \square

Another interesting fact about free modules is that every module is a quotient of a free module. A naïve proof is that if A is an R -module, it is a quotient of the free module generated by elements of A . More formally, we have the surjection $\bigoplus_{a \in A} R_a \rightarrow A$ given by sending 1_a to a . Of course, most modules are quotients of free modules generated by a set much smaller than the module itself.

A projective module is a generalization of a free module with a more abstract definition. A module P is **projective** if for every surjective module homomorphism $\pi : M' \rightarrow M$ and morphism $\phi : P \rightarrow M$, ϕ lifts to a morphism $\psi : P \rightarrow M'$ satisfying $\phi = \pi\psi$. It is indeed a generalization of a free module because of the following proposition.



Proposition 1.3.2. *Every free module is projective.*

Proof. Let F be a free module with basis $\{\lambda_i\}_{i \in I}$, $\pi : M' \rightarrow M$ any surjective R -homomorphism and $\phi : F \rightarrow M$ an R -homomorphism. For each $i \in I$, choose a $\lambda'_i \in M'$ so that $\pi(\lambda'_i) = \phi(\lambda_i)$. Now we define $\psi(\sum a_i \lambda_i) = \sum a_i \lambda'_i$. This map is clearly a homomorphism and it is well-defined because of the properties of a basis. It is now trivial to verify that $\phi = \pi\psi$. \square

Projective modules will prove very useful in the sections to come.

1.4 The functor Hom

In what follows, let R be a fixed ring.

If A and B are R -modules, $\mathbf{hom}_R(\mathbf{A}, \mathbf{B})$ is the set of R -module homomorphisms from A to B . The subscript is sometimes omitted if this will not cause confusion. With a capital h, $\mathbf{Hom}_R(\mathbf{A}, \mathbf{B})$ is the abelian group with underlying set $\mathbf{hom}_R(A, B)$ whose operation is addition of functions. Again, the subscript R may be omitted if it is obvious. If R happens to be a group ring $R = \mathbb{Z}G$, we generally write \mathbf{Hom}_G instead of $\mathbf{Hom}_{\mathbb{Z}G}$. Fixing the second argument, $\mathbf{Hom}(-, B)$ is actually a contravariant functor: if $f : A' \rightarrow A$ is a module homomorphism then $\mathbf{Hom}(f, B) : h \mapsto hf$ is a homomorphism from $\mathbf{Hom}(A, B)$ to $\mathbf{Hom}(A', B)$. We will sometimes write $f^\#$ for $\mathbf{Hom}(f, B)$ if B is clear from the context. If we instead fix the first argument we get a covariant functor: if $f : B \rightarrow B'$ then $\mathbf{Hom}(A, f) : h \mapsto fh$ is a homomorphism from $\mathbf{Hom}(A, B)$ to $\mathbf{Hom}(A, B')$. If A is clear, we may write $\mathbf{Hom}(A, f)$ as $f_\#$.

Theorem 1.4.1. *If P is a projective R -module, the functor $\mathbf{Hom}_R(P, -)$ is exact, i.e. it takes short exact sequences to short exact sequences.*

Proof. We are given an exact sequence

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

and we would like to show that

$$0 \rightarrow \text{Hom}(P, A) \xrightarrow{\alpha_{\#}} \text{Hom}(P, B) \xrightarrow{\beta_{\#}} \text{Hom}(P, C) \rightarrow 0$$

is exact. For exactness at $\text{Hom}(P, A)$, let $f \in \text{Hom}(P, A)$ with $\alpha_{\#}f = 0$, that is, $\alpha f = 0$. As α is injective, we may conclude that $f = 0$. Next we show exactness at $\text{Hom}(P, C)$. If $f \in \text{Hom}(P, C)$ then f may be lifted over the surjection $\beta : B \rightarrow C$ to $g : P \rightarrow B$ with $f = \beta g$, that is, $f = \beta_{\#}g$, because P is projective. Finally, the sequence is exact at $\text{Hom}(P, B)$ because if $f \in \text{Hom}(P, B)$ and $\beta_{\#}f = \beta f = 0$ then $f : P \rightarrow \ker \beta$. The morphism α is a surjection onto $\ker \beta$, so we can lift f to a $g : P \rightarrow A$ with $f = \alpha g = \alpha_{\#}g$. Conversely, if $f \in \text{Hom}(P, A)$ then $\beta_{\#}\alpha_{\#}f = \beta\alpha f = 0$. \square

1.5 Semidirect products

Let A and G be groups and $\phi : G \rightarrow \text{Aut}(A)$ a group homomorphism. The **semidirect product** $A \rtimes_{\phi} G$ of A and G with respect to ϕ is a group with underlying set $A \times G$ and multiplication defined by

$$(a, g)(b, h) = (a + \phi(g)(b), gh),$$

writing A additively (although it need not be abelian) and G multiplicatively. The direct product of two groups is equal to their semidirect product with respect to the trivial homomorphism from G to $\text{Aut}(A)$. Also, the dihedral group D_n is the semidirect product of $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ where the nonidentity element of the latter group acts as the automorphism $x \mapsto -x$ [9].

Theorem 1.5.1. *A group E is the semidirect product of A and G if and only if there is a split exact sequence $0 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$.¹*

Proof. First, suppose that $E = A \rtimes_{\phi} G$. Define homomorphisms $i : A \rightarrow E$ and $\pi : E \rightarrow G$ by $i(a) = (a, 1)$ and $\pi(a, g) = g$. Clearly i is injective, π is surjective and $\ker \pi = \text{im } i$, so they fit in an exact sequence. This sequence is split by $s : G \rightarrow E$ that sends g to $(0, g)$.

Conversely, given a split exact sequence as above, $i(A) \triangleleft E$ because it is the kernel of π . Thus, conjugation by any element in E is an automorphism of A . If we let $\theta : E \rightarrow \text{Aut}(A)$ be this action, then $\phi = \theta s$ is a homomorphism of G into $\text{Aut}(A)$. Now, define $\psi : A \rtimes_{\phi} G \rightarrow E$ by $\psi(a, g) = i(a)s(g)$. A little computation shows ψ to be a group homomorphism. That ψ is an isomorphism is now a consequence of the short five lemma. \square

¹Note the use of 1 for the identity in G and 0 for that in A . The reason for this is to be consistent with our notation for the operation in each group.

1.6 Some results in field theory

Let K be any field. We use K^\times to denote the multiplicative group of K . A **character** of a group G in K is a homomorphism $\chi : G \rightarrow K^\times$. A collection of characters χ_1, \dots, χ_n is called **independent** if whenever we have a collection $\{a_i \in K\}_{i=1}^n$ so that $\sum a_i \chi_i(x) = 0$ for every $x \in G$ then each $a_i = 0$. Being independent, it turns out, is generic behavior for characters for we have the following theorem due either to Artin [6] or to Dedekind [11]:

Theorem 1.6.1 (Independence of Characters). *Any set $\{\chi_1, \dots, \chi_n\}$ of pairwise distinct characters of G in K is independent.*

Proof. The proof is by induction. It is clear that a single character is independent. Now suppose that every set of fewer than n characters is independent and that we have a linear combination of characters $a_1\chi_1 + a_2\chi_2 + \dots + a_n\chi_n = 0$. As these characters are distinct, there is some $z \in G$ such that $\chi_1(z) \neq \chi_2(z)$. Then for every $x \in G$,

$$\begin{aligned} a_1\chi_1(zx) + a_2\chi_2(zx) + \dots + a_n\chi_n(zx) &= 0 \\ a_1\chi_1(z)\chi_1(x) + a_2\chi_2(z)\chi_2(x) + \dots + a_n\chi_n(z)\chi_n(x) &= 0 \\ a_1\chi_1(x) + a_2\frac{\chi_2(z)}{\chi_1(z)}\chi_2(x) + \dots + a_n\frac{\chi_n(z)}{\chi_1(z)}\chi_n(x) &= 0. \end{aligned}$$

Subtracting from this our original linear combination, the first terms cancel and we get

$$a_2\left(\frac{\chi_2(z)}{\chi_1(z)} - 1\right)\chi_2(x) + \dots + a_n\left(\frac{\chi_n(z)}{\chi_1(z)} - 1\right)\chi_n(x) = 0$$

where the first coefficient is nonzero because $\chi_2(z) \neq \chi_1(z)$. This contradicts the inductive hypothesis. \square

The Independence of Characters will be useful in its own right later on, but we will also use it to prove a small result about the trace. Recall that when K is a finite Galois extension of k with Galois group G , we define the trace as $\text{Tr}_K(\theta) = \sum_{\sigma \in G} \sigma(\theta)$ for all $\theta \in K$.

Proposition 1.6.2. *The trace is not identically zero.*

Proof. Observe that each of the elements of G is a character of K in itself. Thus, the function $\sum_{\sigma \in G} \sigma$ is not the zero function because the elements of G are independent. \square

Both this result and Independence of Characters will see applications in Section 3.2.

1.7 Limits

The following are two dual constructions² that allow us, when working with certain infinite groups, to derive properties of the group by considering its finite subgroups or finite quotients. We will see an application in Section 3.2.1.

First of all, a poset Λ is called **directed** if every $\alpha, \beta \in \Lambda$ have an upper bound $\gamma \geq \alpha$ and $\gamma \geq \beta$ (γ is not necessarily unique). A **directed inverse system of groups**, or simply an **inverse system**, is a contravariant functor from a directed poset Λ to the category of groups given by G_α and $\phi_{\alpha\beta} : G_\beta \rightarrow G_\alpha$ for all $\alpha, \beta \in \Lambda$ with $\alpha \leq \beta$. The **inverse limit** or **projective limit** $\varprojlim G_\alpha$ of an inverse system is the subgroup of the direct product $\prod_{\alpha \in \Lambda} G_\alpha$ consisting of the tuples $(g_\alpha)_{\alpha \in \Lambda}$ for which $\phi_{\alpha\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$ [5]. The inverse limit inherits projections $\pi_\alpha : \varprojlim G_\alpha \rightarrow G_\alpha$ for each $\alpha \in \Lambda$ from the direct product. If p is any prime number, we have the inverse system $G_n = \mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$ with $\phi_{n,m}$ the canonical projection when $m \geq n$. The projective limit of this system is the additive group of p -adic integers.

A **filtered direct system of abelian groups** or **direct system**, on the other hand, is a covariant functor B_α and $\psi_{\alpha\beta} : B_\alpha \rightarrow B_\beta$ from the directed poset Λ to the category of abelian groups. The **direct limit** or **injective limit** $\varinjlim B_\alpha$ of a direct system is the quotient of the direct sum $\bigoplus_{\alpha \in \Lambda} B_\alpha$ by the subgroup generated by elements of the form $b_\alpha - \psi_{\alpha\beta}(b_\alpha)$ for all $\alpha \leq \beta$ and all $b_\alpha \in B_\alpha$ [5]. Let's again take as an example a directed system whose objects are the groups $B_n = \mathbb{Z}/p^n\mathbb{Z}$ for p some prime and $n \in \mathbb{N}$. This time, however, the morphisms $\psi_{n,m} : \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^m\mathbb{Z}$ are given by multiplication by p^{m-n} when $n \leq m$. The direct limit of this system is isomorphic to the multiplicative group of p^k th roots of unity in \mathbb{C} .

²Although here we define them in two different categories.

2 Cohomology

In what follows, let R be a fixed ring.

2.1 Cohomology of complexes

Algebraically, homology measures the failure of certain sequences to be exact. In practice, the sequences to which we apply homology are derived from the objects of study.

Not just any sequence will do, however. The algebraic objects that have homology are called chain complexes. A sequence $C = \cdots \leftarrow C_{n-1} \xleftarrow{\partial_n} C_n \xleftarrow{\partial_{n+1}} C_{n+1} \leftarrow \cdots$ of R -modules is a **chain complex** if $\partial_i \partial_{i+1} = 0$ for all i , i.e. the following diagram commutes:

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \longleftarrow & & \\
 & & C_{n-1} & & & & C_{n+1} \\
 & \swarrow & & \nwarrow & & \swarrow & \nwarrow \\
 \dots & & \partial_{n-1} & & \partial_n & & \partial_{n+1} & & \partial_{n+2} & & \dots \\
 & & & & & & & & & & \\
 & & & & 0 & & & & 0 & & \\
 & & & & \longleftarrow & & \longleftarrow & & \longleftarrow & & \\
 & & C_{n-2} & & & & C_n & & & & C_{n+2}
 \end{array}$$

The sequence $0 \leftarrow \mathbb{Z} \xleftarrow{f} \mathbb{Z} \oplus \mathbb{Z} \xleftarrow{g} \mathbb{Z} \leftarrow 0$ where g is given by $n \mapsto (0, 2n)$ and f by $(m, n) \mapsto 3m$ is an example of a chain complex. The family of homomorphisms $\{\partial_i\}$ is called the **boundary operator**. (In this context, the symbol ∂ is pronounced “del.”) The condition required of the boundary operator is often abbreviated $\partial^2 = 0$, omitting the subscripts. It is equivalent to $\text{im } \partial_{i+1} \subseteq \ker \partial_i$. We can therefore define the **n th homology group of the chain complex C** to be

$$H_n(C) = \frac{\ker \partial_n}{\text{im } \partial_{n+1}}.$$

Notice that $H_n(C)$ is a quotient of abelian groups only; $\text{im } \partial_{n+1}$ may not be a submodule of $\ker \partial_n$.

Adding some terminology to make things easier later on, elements of $\ker \partial_n$ are called **n -cycles**, or simply cycles, and elements of $\text{im } \partial_{n+1}$ are **n -boundaries**, or just boundaries. Thus, the n th homology group is the quotient of n -cycles by n -boundaries. An element of the homology group, which is an equivalence class of cycles, is a **homology class** and cycles in the same homology class are said to be **homologous**. Equivalently, homologous cycles are those which differ by a boundary.

At this level, cohomology is nothing more than homology backwards. A sequence $C = \cdots \rightarrow C^{n-1} \rightarrow C^n \rightarrow C^{n+1} \rightarrow \cdots$ of R -modules is a **cochain complex** if C' is a complex when $C'_n = C^{-n}$. Like the cohomology groups themselves, the modules in the cochain complex and the morphisms of the boundary operator are written with upper indices instead of lower. Cochain complexes are also referred to as cocomplexes. The **cohomology of a cocomplex C** is the

homology of the complex C' as defined above, setting $H^n(C) = H_{-n}(C')$. An interesting example of a cocomplex is the sequence where C^n is the vector space of n -differential forms on some manifold and the coboundary operator is the exterior derivative. The cohomology of this cochain complex is known as deRham cohomology. It should go without saying that n -**cocycles** are elements of $\ker \partial^n$ and n -**coboundaries** are elements of $\text{im } \partial^{n-1}$, where the boundary operator is $\partial^n = \partial_{-n}$. As with homology, elements of a cohomology group are **cohomology classes** and cocycles in the same cohomology class are **cohomologous**.

The theory has until now been symmetric with respect to the prefix “co-”; here is where it diverges. The **cohomology of a chain complex C with coefficients in A** , written $H^n(C, A)$, is the cohomology of the image of C under the functor $\text{Hom}(-, A)$. In order for our definition of the cohomology of a complex to make sense we require the following:

Proposition 2.1.1. *If C is a chain complex then*

$$\cdots \rightarrow \text{Hom}(C_{n-1}, A) \xrightarrow{d^{n-1}} \text{Hom}(C_n, A) \xrightarrow{d^n} \text{Hom}(C_{n+1}, A) \rightarrow \cdots$$

*is a cochain complex, setting $d^n = \text{Hom}(\partial_{n+1}, A)$.*³

Proof. Let $h \in \text{Hom}(C_{n-1}, A)$. We apply the boundary operator twice to h in the hope of getting 0. By definition

$$d^{n-1}(h) = \text{Hom}(\partial_n, A)(h) = h\partial_n$$

and

$$d^n(h\partial_n) = \text{Hom}(\partial_{n+1}, A)(h\partial_n) = h\partial_n\partial_{n+1} = h \circ 0 = 0. \quad \square$$

2.1.1 Induced maps on homology and cohomology

A **chain homomorphism** between the chain complexes (C, ∂) and (C', ∂') is a family of morphisms $\{f_n : C_n \rightarrow C'_n\}$ such that $f_n\partial = \partial'f_{n+1}$ for all n , that is, a family of homomorphisms that commute with the boundary operator. Chain homomorphisms (also called **chain transformations**) will allow us to establish that homology, and therefore cohomology as well, is a functor. If $f : C \rightarrow C'$ is a chain transformation then it induces the map $f_* : H_n(C) \rightarrow H_n(C')$ sending a homology class represented by the cycle c to the class of $f(c)$. This is a well-defined homomorphism because if c and c' are homologous cycles then $\partial(c - c') = 0$, whence

$$0 = f\partial(c - c') = \partial'f(c - c') = \partial'(f(c) - f(c'))$$

shows that $f(c)$ and $f(c')$ are homologous. It is clear that the induced map of a composition of chain homomorphisms is the composition of the induced maps. Since we defined the cohomology of a cocomplex to be the homology

³Some authors define $d^n = (-1)^{n+1} \text{Hom}(\partial_{n+1}, A)$. The sign change yields the same cohomology groups so we will omit it here for simplicity.

of the complex with negative indices, this also demonstrates functoriality of cohomology. In addition, the cohomology of a complex is the composition of the Hom functor with the cohomology functor, so that is also a functor. Induced homomorphisms on cohomology are usually written with an upper star: f^* .

Homology and cohomology have an even more extraordinary property than functoriality. The special feature of these two functors (well, they're really the same functor) is the existence of the long exact sequence of homology or cohomology. We give the cohomological form here since cohomology is our specific focus.

Theorem 2.1.2. *Given a short exact sequence*

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

of cochain complexes, there is a family of homomorphisms $d^ : H^n(C) \rightarrow H^{n+1}(A)$ fitting in the long exact sequence*

$$H^0(A) \xrightarrow{\alpha^*} H^0(B) \xrightarrow{\beta^*} H^0(C) \xrightarrow{d^*} H^1(A) \xrightarrow{\alpha^*} H^1(B) \rightarrow \dots$$

in cohomology.

Proof. For each n , construct the diagram

$$\begin{array}{ccccccc} \text{cok } d_A^{n-1} & \longrightarrow & \text{cok } d_B^{n-1} & \longrightarrow & \text{cok } d_C^{n-1} & \longrightarrow & 0 \\ \tilde{d}_A \downarrow & & \tilde{d}_B \downarrow & & \tilde{d}_C \downarrow & & \\ 0 \longrightarrow & \text{ker } d_A^{n+1} & \longrightarrow & \text{ker } d_B^{n+1} & \longrightarrow & \text{ker } d_C^{n+1} & \end{array}$$

where d_A is the coboundary operator of the cochain complex A and similarly for d_B and d_C . The horizontal maps are induced by the morphisms in the exact sequence and the vertical maps by the respective coboundary operators. It is not hard to verify that the rows are exact.⁴ Inspection reveals that $\text{ker } \tilde{d}_A = H^n(A)$, $\text{cok } \tilde{d}_A = H^{n+1}(A)$ and similarly for \tilde{d}_B and \tilde{d}_C . Thus, the snake lemma (1.2.1) gives us a partial exact sequence

$$H^n(A) \rightarrow H^n(B) \rightarrow H^n(C) \rightarrow H^{n+1}(A) \rightarrow H^{n+1}(B) \rightarrow H^{n+1}(C).$$

We splice the partial sequences to get the entire long exact cohomology sequence. \square

The d^* in the theorem is known as the **connecting homomorphism**. The long exact homology sequence is essentially the same except that the connecting homomorphism goes from $H_n(C)$ to $H_{n-1}(A)$. In fact, the long exact sequence is one of the defining properties of a homology functor.

⁴Or we can use the more general fact that in abelian categories, taking kernels (cokernels) is a left (right) exact functor on the morphism category.

2.2 Cohomology of groups

Now that we can calculate the cohomology of a complex, where does such a complex come from? Recall the definition of a G -module from Section 1.1. Chain complexes of G -modules are what allow us to analyze groups using homological techniques. If A is a G -module, we define: the **cohomology of a group G with coefficients in A** , written $H^n(G, A)$, is $H^n(X, A)$, where X is a projective resolution of the trivial module \mathbb{Z} over $\mathbb{Z}G$. Being exact, such a resolution has trivial homology, so finding its cohomology really tells us how much $\text{Hom}(-, A)$ does not preserve exactness.

We need a couple of proofs for this definition to be perfectly ironclad. First of all, are we sure that such a resolution will always exist? This is not too hard to see, actually, by applying the knowledge that every module is a quotient of a free module. So \mathbb{Z} is the quotient of F_0 by R_0 , yielding the exact sequence $0 \rightarrow R_0 \rightarrow F_0 \rightarrow \mathbb{Z} \rightarrow 0$. Then, $R_0 = F_1/R_1$ and the composition of the projection of F_1 onto $F_1/R_1 = R_0$ followed by the inclusion of R_0 into F_0 extends our resolution to $0 \rightarrow R_1 \rightarrow F_1 \rightarrow F_0 \rightarrow \mathbb{Z} \rightarrow 0$. This process can be continued indefinitely, showing that a free resolution of \mathbb{Z} always exists, which is *a fortiori* projective. For example, suppose G is the free abelian group on two generators, so that $\mathbb{Z}G$ is the ring of Laurent polynomials in two variables. We map $\mathbb{Z}G$ onto \mathbb{Z} by “evaluation at $(1, 1)$,” that is, by sending both variables to 1. This map, which we will call ϵ , is clearly surjective, so we have the short exact sequence $0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \leftarrow \ker \epsilon \leftarrow 0$. The kernel of ϵ is contained in the ideal generated by $x - 1$ and $y - 1$, so we can extend our resolution by $\alpha : \mathbb{Z}G \oplus \mathbb{Z}G \rightarrow \mathbb{Z}G$ which takes the pair $(p(x, y), q(x, y))$ to $(x - 1)p(x, y) + (y - 1)q(x, y)$. Our partial resolution is now $0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \xleftarrow{\alpha} \mathbb{Z}G \oplus \mathbb{Z}G \leftarrow \ker \alpha \leftarrow 0$. The kernel of α is the principal ideal generated by $(y - 1, 1 - x)$, so our resolution is completed by $\beta : \mathbb{Z}G \rightarrow \mathbb{Z}G \oplus \mathbb{Z}G$ defined by $p(x, y) \mapsto ((y - 1)p(x, y), (1 - x)p(x, y))$. The complete resolution is, therefore,

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \xleftarrow{\alpha} \mathbb{Z}G \oplus \mathbb{Z}G \xleftarrow{\beta} \mathbb{Z}G \leftarrow 0.$$

The above process gives us at least one projective resolution, but we defined $H^n(G, A)$ using one particular resolution. Fortunately:

Theorem 2.2.1. *The cohomology of a group is well-defined with respect to choice of resolution.*

In order to prove this theorem we will introduce another new concept. A **chain homotopy** between chain homomorphisms $f, g : C \rightarrow C'$ is a family of homomorphisms $s_n : C_n \rightarrow C'_{n+1}$ such that $\partial' s_n + s_{n-1} \partial = f_n - g_n$.

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & C_{n+1} & \xrightarrow{\partial} & C_n & \xrightarrow{\partial} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} & & \\
 & & C'_{n+1} & \xrightarrow{\partial'} & C'_n & \xrightarrow{\partial'} & C'_{n-1} & \longrightarrow & \cdots \\
 & & \uparrow g_{n+1} & & \uparrow g_n & & \uparrow g_{n-1} & & \\
 & & \swarrow s_n & & \swarrow s_{n-1} & & & &
 \end{array}$$

If a chain homotopy exists between chain maps f and g then f and g are said to be **homotopic**. Chain homotopies are important because homotopic chain transformations induce the same map on homology.

Proposition 2.2.2. *If $f, g : C \rightarrow C'$ are two chain homomorphisms with a chain homotopy $\{s_n : C_n \rightarrow C_{n+1}\}$ from f to g then $f_* = g_*$.*

Proof. Suppose c is a representative of an element of $H_n(C)$. Being a cycle, $\partial(c) = 0$, so $f_n(c) - g_n(c) = \partial's_{n+1}(c)$. But this means that $f_n(c)$ and $g_n(c)$ differ only by a boundary, i.e. they represent the same element of $H_n(C')$. \square

Given this property of chain homotopic maps, we are obviously aiming to demonstrate chain homotopies between two projective resolutions. They are constructed in the following lemma, which is a major piece of the proof of Theorem 2.2.1.

Lemma 2.2.3 (Comparison Theorem [7]). *Let $\cdots \rightarrow X_1 \rightarrow X_0 \xrightarrow{\epsilon} C \rightarrow 0$ be a projective resolution and $\cdots \rightarrow X'_1 \rightarrow X'_0 \xrightarrow{\epsilon'} C' \rightarrow 0$ be a resolution. If $\gamma : C \rightarrow C'$ is a homomorphism then there is a chain homomorphism $f_n : X_n \rightarrow X'_n$ with $\gamma\epsilon = \epsilon'f_0$. Furthermore, any two such chain transformations are homotopic.*

Such a chain homomorphism is said to lift γ . Brown [3] calls a slightly different but equivalent theorem “the fundamental lemma of homological algebra.”

$$\begin{array}{ccccccccc}
 \cdots & \longrightarrow & X_2 & \xrightarrow{\partial} & X_1 & \xrightarrow{\partial} & X_0 & \xrightarrow{\epsilon} & C & \longrightarrow & 0 \\
 & & \downarrow f_2 & \nearrow s_1 & \downarrow f_1 & \nearrow s_0 & \downarrow f_0 & \nearrow t & \downarrow \gamma & & \\
 \cdots & \longrightarrow & X'_2 & \xrightarrow{\partial'} & X'_1 & \xrightarrow{\partial'} & X'_0 & \xrightarrow{\epsilon'} & C' & \longrightarrow & 0
 \end{array}$$

Proof. The proof proceeds by repeated application of a lifting property of projective modules that is a simple consequence of their definition. If P is projective then ϕ may be lifted to ψ in the commutative diagram at right given that the bottom row is exact [3]. The first application is with $P = X_0$, $\phi = \gamma\epsilon$ and bottom row $X'_0 \rightarrow C' \rightarrow 0$. The lift we get is $f_0 : X_0 \rightarrow X'_0$. Now we continue by moving the subdiagram to the left in the above diagram, for example, the next application is lifting $f_0\partial$ to f_1 and so on. This proves by induction the existence of the chain transformation.

$$\begin{array}{ccccc}
 & & P & & \\
 & \nearrow \psi & \downarrow \phi & \searrow 0 & \\
 M' & \xrightarrow{i} & M & \xrightarrow{j} & M''
 \end{array}$$

Showing the existence of a chain homotopy between two such chain homomorphisms, say f and f' , is also done by projective lifting. To start with, we need a $t : C \rightarrow X'_0$ such that $\epsilon't = \gamma - \gamma' = 0$. Clearly, $t = 0$ will do. Now we

can lift $f_0 - f'_0$ to $s_0 : X_0 \rightarrow X'_1$ because $e'(f_0 - f'_0) = \gamma\epsilon - \gamma\epsilon = 0$. The rest of the proof is done by lifting $f_n - f'_n - s_{n-1}\partial$ to s_n , which we can do since $\partial'(f_n - f'_n - s_{n-1}\partial)\partial'(f_n - f'_n) - \partial'(f_n - f'_n - \partial's_n) = 0$, guaranteeing that $\partial's_n + s_{n-1}\partial = f_n - f'_n$ at each step. \square

Notice that in the proof we never used the fact that the sequence $\cdots \rightarrow X_1 \rightarrow X_0 \xrightarrow{\epsilon} C \rightarrow 0$ is exact, only that the composition of two adjacent morphisms is zero, i.e. it is a complex, and that each X_i is projective. We require that X is a resolution only to avoid introducing new terminology. Every application of the lemma in this paper will indeed be to two resolutions.

We have come to the point where we are able to attempt a proof of Theorem 2.2.1. In this proof, we shall use the shorthand $f^\#$ to mean $\text{Hom}(f, A)$ as in Section 1.4.

Proof of Theorem 2.2.1. Let G be a group, A a G -module and $\cdots \rightarrow C_1 \rightarrow C_0 \rightarrow \mathbb{Z} \rightarrow 0$ and $\cdots \rightarrow C'_1 \rightarrow C'_0 \rightarrow \mathbb{Z} \rightarrow 0$ be projective resolutions. By the Comparison Theorem (2.2.3), we can lift the identity on \mathbb{Z} to chain transformations $f : C \rightarrow C'$ and $g : C' \rightarrow C$. Since the identity $1_C : C \rightarrow C$ and gf are both chain transformations lifting the identity on \mathbb{Z} , they are homotopic and similarly for fg and $1_{C'}$. The homomorphisms f and g induce maps $f^\#$ and $g^\#$ which are chain homomorphisms. Applying Hom to the homotopies from gf and fg to the appropriate identities yields chain homotopies between the two composites of the induced maps and the appropriate identities, respectively.⁵ As chain homotopic maps induce identical maps on homology, this shows that $f^*g^* : H^n(C, A) \rightarrow H^n(C, A)$ and $g^*f^* : H^n(C', A) \rightarrow H^n(C', A)$ are each the appropriate identity map. We conclude that f^* and g^* are isomorphisms. \square

2.2.1 Induced homomorphisms on group cohomology

Now that we can pick whichever projective resolution we like in calculating cohomology, we can more easily demonstrate functoriality of group cohomology. Let A and B be G -modules and $f : A \rightarrow B$ a G -homomorphism. For any G -module C , f induces a homomorphism $f_\# : \text{Hom}_G(C, A) \rightarrow \text{Hom}_G(C, B)$. Hence, if we take any projective resolution $0 \leftarrow \mathbb{Z} \leftarrow C_0 \leftarrow C_1 \leftarrow \cdots$ of \mathbb{Z} over $\mathbb{Z}G$ then f induces a homomorphism from the image of the resolution under $\text{Hom}(-, A)$ to its image under $\text{Hom}(-, B)$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}(C_0, A) & \xrightarrow{\partial^\#} & \text{Hom}(C_1, A) & \xrightarrow{\partial^\#} & \text{Hom}(C_2, A) \longrightarrow \cdots \\ & & \downarrow f_\# & & \downarrow f_\# & & \downarrow f_\# \\ 0 & \longrightarrow & \text{Hom}(C_0, B) & \xrightarrow{\partial^\#} & \text{Hom}(C_1, B) & \xrightarrow{\partial^\#} & \text{Hom}(C_2, B) \longrightarrow \cdots \end{array}$$

But is it a chain homomorphism? Observe that the horizontal maps $\partial^\#$ are given by $h \mapsto h\partial$ while the vertical maps are $h \mapsto fh$. Thus, the diagram

⁵Chain homotopies are preserved because Hom is an additive functor.

commutes by the associativity of function composition! This means that $f_{\#}$ is, in fact, a chain map. Hence, it induces the map $f_* : H^n(G, A) \rightarrow H^n(G, B)$ on cohomology.

Cohomology is a functor not only in the second argument but in the first as well. Let $f : G' \rightarrow G$ be a group homomorphism. Any G -module A may be considered a G' module by the homomorphism $\phi f : G' \rightarrow \text{Aut}(A)$, where $\phi : G \rightarrow \text{Aut}(A)$ is the action of G on A . This G' -module, written ${}_f A$ or sometimes just A , is called the **pullback of A along f** [7]. Notice that any G -homomorphism $h : A \rightarrow A'$ is also a G' -homomorphism of the pullbacks $h : {}_f A \rightarrow {}_f A'$; pullbacks are functorial in nature. This fact is what allows group homomorphisms to induce homomorphisms on cohomology.

If $f : G' \rightarrow G$ is a homomorphism of groups, construct f^* as follows: take projective resolutions C and C' of \mathbb{Z} over $\mathbb{Z}G$ and $\mathbb{Z}G'$, respectively. Since images and kernels are unaffected by the module structure, the pullback of C along f is still a resolution, although no longer necessarily projective. The identity on \mathbb{Z} is clearly a G' -morphism, so it may be lifted using the Comparison Theorem to a chain transformation $\tilde{f} : C' \rightarrow {}_f C$.⁶ The map induced by \tilde{f} on cohomology is what we define as f^* .

There is one particular induced homomorphism on cohomology that we will use later on. If G is a group and H a normal subgroup, let f be the projection onto the quotient G/H . Now if A is any G -module, we cannot pullback A along f ; pullbacks go the other way. Consider, however, the submodule $A^H = \{a \in A : ha = a \forall h \in H\}$ of elements fixed by H . Since the action of H on A^H is trivial, the G action on A^H descends to a G/H action. With A^H now a G/H module, we have an induced map on cohomology $f^* : H^n(G/H, A^H) \rightarrow H^n(G, A^H)$. We compose this homomorphism with the map induced by the inclusion of A^H in A to construct the **inflation** homomorphism $\text{Inf} : H^n(G/H, A^H) \rightarrow H^n(G, A)$.

Recall from the previous section the long exact sequence induced by a short exact sequence of cochain complexes. As morphisms between G -modules induce morphisms on cohomology we might hope that a short exact sequence of G -modules will give rise to a long exact cohomology sequence. This is indeed the case:

Theorem 2.2.4. *If*

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

is a short exact sequence of G -modules then there is a family of homomorphisms $d_ : H^n(G, C) \rightarrow H^{n+1}(G, A)$ fitting in the long exact cohomology sequence*

$$H^0(G, A) \xrightarrow{\alpha_*} H^0(G, B) \xrightarrow{\beta_*} H^0(G, C) \xrightarrow{d_*} H^1(G, A) \xrightarrow{\alpha_*} H^1(G, B) \rightarrow \dots$$

Proof. Because of Theorem 2.1.2, we need only show that the given short exact sequence induces a short exact sequence of chain complexes. Once we choose a

⁶It may not be lifted to a chain map $fC \rightarrow C'$ since ${}_f C$ may not be projective, as required by the Comparison Theorem.

projective resolution $0 \leftarrow \mathbb{Z} \leftarrow X_0 \leftarrow X_1 \leftarrow \cdots$, the induced chain maps form the diagram

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \text{Hom}(X_0, A) & \xrightarrow{d} & \text{Hom}(X_1, A) & \xrightarrow{d} & \text{Hom}(X_2, A) \longrightarrow \cdots \\
& & \downarrow \alpha_{\#} & & \downarrow \alpha_{\#} & & \downarrow \alpha_{\#} \\
0 & \longrightarrow & \text{Hom}(X_0, B) & \xrightarrow{d} & \text{Hom}(X_1, B) & \xrightarrow{d} & \text{Hom}(X_2, B) \longrightarrow \cdots \\
& & \downarrow \beta_{\#} & & \downarrow \beta_{\#} & & \downarrow \beta_{\#} \\
0 & \longrightarrow & \text{Hom}(X_0, C) & \xrightarrow{d} & \text{Hom}(X_1, C) & \xrightarrow{d} & \text{Hom}(X_2, C) \longrightarrow \cdots \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0.
\end{array}$$

The columns are exact sequences by Theorem 1.4.1 because each X_i is projective. This completes the proof since we have a short exact sequence of cochain complexes. \square

2.3 Cohomology of cyclic groups

For the calculations to follow, let's introduce the concepts of invariants and co-invariants. If the abelian group A is a G -module, the **invariants** form the subgroup of A defined by $A^G = \{a \in A : ga = a \text{ for all } g \in G\}$. **Co-invariants** A_G are the quotient of A by the additive subgroup generated by $\{ga - a : g \in G \text{ and } a \in A\}$. These are dual notions because A^G is the largest subgroup on which G acts trivially and A_G is the largest quotient with this property. If A is a trivial G -module, clearly $A^G = A_G = A$. As another example, if $G = \mathbb{Z}/2\mathbb{Z}$ and G acts on $A = \mathbb{Z}/n\mathbb{Z}$ by $1 : a \mapsto -a$ then $A^G = 0$ if n is odd or $A^G = \mathbb{Z}/2\mathbb{Z}$ if n is even. As for co-invariants, the kernel of the projection of A onto A_G is the set $\{2a : a \in A\}$, so again $A_G = 0$ if n is odd or $A_G = \mathbb{Z}/2\mathbb{Z}$ if n is even.

For the remainder of the section, let G be a cyclic group generated by t . In $\mathbb{Z}G$, assign $D = t - 1$. We will abuse some notation and also use D to refer to the endomorphism $a \mapsto Da$ of any G -module.

Proposition 2.3.1 ([3]). *If $G = \langle t \rangle$ has infinite order and A is any G -module then*

$$H^0(G, A) = A^G, \quad H^1(G, A) = A_G, \quad H^k(G, A) = 0 \text{ for } k > 1.$$

Proof. The following is a free resolution of \mathbb{Z} over $\mathbb{Z}G$:

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \xleftarrow{D} \mathbb{Z}G \leftarrow 0,$$

where $\epsilon(\sum a_i t^i) = \sum a_i$ is the augmentation. To prove this, we need to show that $\ker \epsilon = \text{im } D$. If $x = \sum_{i \in \mathbb{Z}} x_i t^i \in \mathbb{Z}G$ then $Dx = \sum (x_{i-1} - x_i) t^i$. Clearly,

then, $\epsilon D = 0$. Furthermore, if $\epsilon x = \sum x_i = 0$ then $x = -D \left(\sum_{i \in \mathbb{Z}} \sum_{j=-\infty}^{j=i} x_j t^i \right)$, that is, $x \in \text{im } D$. Once we realize that, for any G -module A , $\text{Hom}_G(\mathbb{Z}G, A) \cong A$ by the isomorphism $h \mapsto h(1)$, it is quite easy to apply Hom to the resolution to produce the cochain complex

$$0 \rightarrow A \xrightarrow{D} A \rightarrow 0.$$

Computing cohomology, we get $H^0(G, A) = \ker D$ and $H^1(G, A) = A/\text{im } D$. Notice that $(t-1)a = 0$ if and only if $ta = a$. As t generates G , then, $\ker D = A^G$. Thus, $H^0(G, A) = A^G$. As for H^1 , the kernel of the projection of A onto A_G turns out to be exactly $\text{im } D$. Thus, $H^1(G, A) = A_G$. \square

If A is a trivial G -module, then, the first and second cohomology turn out to be $H^0(G, A) = A = H^1(G, A)$ with higher cohomology groups zero. Suppose that $G = \mathbb{Z}$ and G acts on $A = \mathbb{Z}/n\mathbb{Z}$ by $k : a \mapsto (-1)^k a$. In this case, if n is odd then it has zero cohomology in all dimensions. If n is even, however, $H^0(G, A) = \mathbb{Z}/2\mathbb{Z} = H^1(G, A)$.

For any finite group G , the **norm** is the element of $\mathbb{Z}G$ defined by $N = \sum_{g \in G} g$. When $G = \langle t \mid t^n \rangle$, $N = \sum_{i=0}^{n-1} t^i$. As with D , we will write N both for the element of $\mathbb{Z}G$ and the morphism $a \mapsto Na$. Also, we write NA for the image of this endomorphism and define DA similarly. For a final bit of notation, let ${}_N A$ stand for the kernel of the endomorphism N .

Proposition 2.3.2 ([12]). *If G is cyclic of order n and A is any G -module then*

$$\begin{aligned} H^0(G, A) &= A^G, \\ H^k(G, A) &= {}_N A / DA \text{ for odd } k, \\ H^k(G, A) &= A^G / NA \text{ for even } k > 0. \end{aligned}$$

Proof [7]. We will demonstrate that the following is a free resolution of \mathbb{Z} over $\mathbb{Z}G$:

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} \mathbb{Z}G \xleftarrow{D} \mathbb{Z}G \xleftarrow{N} \mathbb{Z}G \xleftarrow{D} \mathbb{Z}G \xleftarrow{N} \mathbb{Z}G \leftarrow \dots$$

First, note that $ND = DN = 0$. This shows that $\text{im } D \subseteq \ker N$ and $\text{im } N \subseteq \ker D$. Observe that if $x = x_0 + x_1 t + \dots + x_{n-1} t^{n-1} \in \mathbb{Z}G$ then

$$Nx = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} x_j \right) t^i \quad \text{and} \quad Dx = (x_{n-1} - x_0) + \sum_{i=1}^{n-1} (x_{i-1} - x_i) t^i.$$

Now if $Dx = 0$ then $x_0 = x_1 = \dots = x_{n-1}$, so $x = Nx_0$. This gives us that $\ker D \subseteq \text{im } N$. If $Nx = 0$ then $\sum x_i = 0$ so $x = -D \sum_{i=0}^{n-1} \left(\sum_{j=0}^i x_j \right) t^i$, showing that $\ker N \subseteq \text{im } D$. Finally, we have $\epsilon Dx = (x_{n-1} - x_0) + \sum_{i=1}^{n-1} (x_{i-1} - x_i) = 0$ and we have already observed that if $\epsilon x = \sum x_i = 0$ then $x \in \text{im } D$. Hence, $\ker \epsilon = \text{im } D$. We have now shown that the above sequence is exact and

therefore a free resolution. Using the isomorphism $\text{Hom}_G(\mathbb{Z}G, A) \cong A$ as in the previous proof, we obtain the cochain complex

$$0 \rightarrow A \xrightarrow{D} A \xrightarrow{N} A \xrightarrow{D} A \xrightarrow{N} A \rightarrow \dots$$

From here we compute cohomology directly. Recall from the above proof that $\ker D = A^G$. Therefore, $H^0(G, A) = A^G$. The even terms in the cochain complex are in a similar situation. There we have $H^{2k}(G, A) = \ker D/NA = A^G/NA$. The odd terms in the cochain complex are the domain of N and the codomain of D . For odd indices, then, $H^{2k+1}(G, A) = {}_N A/DA$. \square

The case where A is a trivial G module is actually somewhat interesting in this case. When G acts trivially on A , the map D becomes the zero map since $(t-1)a = ta - a = a - a = 0$. The norm, on the other hand, becomes multiplication by $n = |G|$ because $Na = (t^{n-1} + \dots + t + 1)a = na$. The cohomology groups are, therefore, $H^0(G, A) = A$, $H^k(G, A) = \{a \in A : na = 0\}$ for odd k and $H^k(G, A) = A/nA$ for even $k > 0$.

2.4 The bar resolution

As we have shown that any resolution will do for calculating the cohomology of a group, we can construct a generic resolution that we may apply to any group. Let C_n be the free G -module generated by n -tuples of nonidentity elements of G , written $[g_1 | \dots | g_n]$, and let the boundary of such a tuple be

$$g_1[g_2 | \dots | g_n] + \sum_{i=1}^{n-1} (-1)^i [g_1 | \dots | g_i g_{i+1} | \dots | g_n] + (-1)^n [g_1 | \dots | g_{n-1}].$$

These modules and homomorphisms form a resolution

$$0 \leftarrow \mathbb{Z} \xleftarrow{\epsilon} C_0 \xleftarrow{\partial_1} C_1 \xleftarrow{\partial_2} C_2 \leftarrow \dots$$

called the **bar** or **standard resolution**. (The name comes from the bars written between the elements in the tuples above.) Some authors actually define the cohomology of a group as the cohomology of its bar resolution and then prove that any other resolution works as well. In particular, C_0 is the free G -module generated by a single, empty tuple and therefore isomorphic to $\mathbb{Z}G$. Also, we have the homomorphism $\epsilon : C_0 \rightarrow \mathbb{Z}$ called augmentation that maps $1g \mapsto 1$ for all $g \in G$ with $\ker \epsilon = \text{im } \partial_1$.

Since each C_n is free, we can represent elements of the cochain complex $\text{Hom}(C_n, A)$ as functions $f : G^n \rightarrow A$ with $f(g_1, \dots, g_n) = 0$ if any $g_i = 1$. In this form, cocycles are such functions where

$$\begin{aligned} g_0 f(g_1, \dots, g_n) - f(g_0 g_1, g_2, \dots, g_n) + \dots \\ + (-1)^n f(g_0, \dots, g_{n-1} g_n) + (-1)^{n+1} f(g_0, \dots, g_{n-1}) = 0 \end{aligned}$$

for all $g_0 \in G$ and coboundaries are functions of the form

$$f(g_1, \dots, g_n) = g_1 h(g_2, \dots, g_n) - h(g_1 g_2, g_3, \dots, g_n) + \dots \\ + (-1)^{n-1} h(g_1, \dots, g_{n-1} g_n) + (-1)^n h(g_1, \dots, g_{n-1})$$

for some $h : G^{n-1} \rightarrow A$.

In particular, 0-cocycles may be identified with elements $a \in A$ satisfying $ga - a = 0$. There are no 0-coboundaries. Recall that when calculating the cohomology of cyclic groups we found in both cases that $H^0(G, A) = A^G$. The bar resolution description of 0-cocycles allows us to generalize this to any group.

Proposition 2.4.1. $H^0(G, A) = A^G$.

Proof. Examination of the bar resolution shows that 0-cocycles are elements of $a \in A$ satisfying $ga - a = 0$ for all $g \in G$. These are exactly the elements of A^G . As 0-coboundaries are trivial, the proposition follows. \square

Continuing our analysis of low dimensions, 1-cocycles are functions $f : G \rightarrow A$ satisfying $gf(h) - f(gh) + f(g) = 0$ for all $g, h \in G$. Such functions were studied even before the invention of cohomology. There were called “crossed homomorphisms” because of the rearrangement $f(gh) = f(g) + gf(h)$. Another name for 1-cocycles is “derivations.” This comes from the fact that if we allow G to act trivially on A on the right in addition to the chosen left action then the cocycle condition becomes $f(gh) = f(g)h + gf(h)$, which resembles the product rule for derivatives. In dimension one, coboundaries are functions $f : G \rightarrow A$ of the form $f(g) = ga - a$ for some $a \in A$. These are known as “principal derivations.”

Dimension two cocycles are called “factor sets.” They are maps $f : G \times G \rightarrow A$ satisfying $gf(h, k) - f(gh, k) + f(g, hk) - f(g, h) = 0$, that is, $f(g, h) = gf(h, k) - f(gh, k) + f(g, hk)$ for all $g, h, k \in G$. Coboundaries in dimension two are functions that have the form $f(g, h) = gf'(h) - f'(gh) + f'(g)$ for some function $f' : G \rightarrow A$.

3 Applications of group cohomology

Now finally, finally at last, we have a good, well-defined definition of the cohomology of a group. What can we do with it?

3.1 Group extensions

The group extension problem is one that is very easily posed in the language of homological algebra: given groups G and A , can we find a group E such that the three groups fit into an exact sequence $1 \rightarrow A \rightarrow E \rightarrow G \rightarrow 1$? Such an E is called an **extension of G by A** . An equivalent formulation is finding a group E such that $A \triangleleft E$ and $E/A \cong G$. There is always at least one such extension: the direct product of A and G .

Group cohomology can be applied to the group extension question as well as a related one as long as the group A is abelian. The reason for this requirement is that when this is the case, an extension yields a G -module structure on A , which is something we can apply cohomology to. More precisely, if we have the exact sequence

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

and A is abelian then G acts on A by conjugation in E : as $i(A) \triangleleft E$ with i an isomorphism onto its image. Thus, E acts on A by conjugation, inducing the homomorphism $\psi : E \rightarrow \text{Aut}(A)$. When A is commutative, the action of A on itself is trivial. Thus, ψ factors over π , giving the group action $\phi : G \rightarrow \text{Aut}(A)$ with $\phi\pi = \psi$. Recall that such a ϕ makes A into a G -module. If a G -module structure for A is specified in advance then we are looking for an **extension of G by A with operators ϕ** . Even given a particular action on A , there is always at least one extension giving rise to it: the semidirect product $A \rtimes_{\phi} G$. Specifically, the G -module structure is given by

$$g \cdot a = i^{-1}(\tilde{g}i(a)\tilde{g}^{-1})$$

where $\pi(\tilde{g}) = g$. The above equation is often used as a commutation rule for A and G in the form

$$\tilde{g}i(a) = i(g \cdot a)\tilde{g}.$$

When $i(A)$ is contained in the center of E we call E a **central extension**. Equivalently, a central extension is an extension with trivial operators.

Extensions are classified only up to a certain equivalence relation: two extensions E and E' of G by A are equivalent if there is a group homomorphism $h : E \rightarrow E'$ making the following diagram commute:

$$\begin{array}{ccccccc}
 & & & & E & & \\
 & & & & \uparrow & \searrow & \\
 & & & & h & & \\
 & & & & \downarrow & \nearrow & \\
 & & & & E' & & \\
 1 & \longrightarrow & A & \begin{array}{l} \nearrow \\ \searrow \end{array} & & \longrightarrow & G & \longrightarrow & 1.
 \end{array}$$

The short five lemma guarantees that h is an isomorphism. If the projection π has a right inverse $s : G \rightarrow E$ that is also a homomorphism then, by Theorem 1.5.1, $E \cong A \rtimes G$. This isomorphism means that E is equivalent to the semidirect product extension. Such extensions are called split extensions.

3.1.1 Classifying splittings

If A is a given G -module and E a split extension then an interesting problem is to classify the splittings $s : G \rightarrow E$. This amounts to finding the different ways in which G can be embedded as a subgroup of E . As with many classification problems, splittings are classified up to equivalence. Two splittings s_1 and s_2 are **A -conjugate** if there is an $a \in A$ so that $s_1(g) = i(a)s_2(g)i(a)^{-1}$ for all $g \in G$. It turns out that the first cohomology group is exactly what we need to classify splittings in this way:

Theorem 3.1.1. *A -conjugacy classes of splittings $s : G \rightarrow E$ are in bijective correspondence with elements of the first cohomology group $H^1(G, A)$.*

Proof. We may take E to be the semidirect product $A \rtimes G$; it is the canonical split extension.

A splitting $s : G \rightarrow A \rtimes G$ must have the form $s(g) = (d(g), g)$ with d some function from G to A . In order for s to be a homomorphism, d must satisfy $d(gh) = gd(h) + d(g)$ for all $g, h \in G$. Inspection of the bar resolution reveals this to be exactly the form required for 1-cocycles.

If s_1 and s_2 are A -conjugate splittings as above with $s_1(g) = (d_1(g), g)$ and $s_2(g) = (d_2(g), g)$, a little calculation shows that $d_1 = a + d_2 - ga$ and thus $d_2 - d_1 = ga - a$. Functions mapping $g \mapsto ga - a$ for some $a \in A$ are coboundaries. This means that if s_1 and s_2 are A -conjugate then d_1 and d_2 are cohomologous cocycles. \square

As mentioned in Section 1.5, the dihedral group D_n is isomorphic to $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ where the nonidentity element of $\mathbb{Z}/2\mathbb{Z}$ acts as $x \mapsto -x$. Because of the above theorem, we can calculate splittings of the exact sequence $0 \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow D_n \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ by the first cohomology $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$. Proposition 2.3.2 tells us that the group we want is the quotient of the kernel of the norm by the image of D . In $\mathbb{Z}/2\mathbb{Z}$, the norm is $t + 1$. Since $tx = -x$, $(t + 1)x = -x + x = 0$ for all $x \in \mathbb{Z}/n\mathbb{Z}$. As for the image of D , if n is odd it is all of $\mathbb{Z}/n\mathbb{Z}$ or if n is even it is $2\mathbb{Z}/n\mathbb{Z}$. Thus, $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0$ if n is odd or it is $\mathbb{Z}/2\mathbb{Z}$ if n is even. The implication of this is that if n is odd, the only splitting is the usual one $s : \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ induced by $1 \mapsto (0, 1)$. If n is even, however, in addition to the usual splitting we also have the map induced by $1 \mapsto (\frac{n}{2}, 1)$.

3.1.2 Classifying extensions with abelian kernel

Leaving aside the split assumption, cohomology can be used to solve any extension problem in which A is abelian. It is necessary that A be abelian so that it can be given a G -module structure.

Theorem 3.1.2. *Let G be a group and A a G -module by $\phi : G \rightarrow \text{Aut}(A)$. Extensions of G by A with operators ϕ are in bijective correspondence with elements of $H^2(G, A)$.*

As G -module structures on A can be enumerated by $\text{hom}(G, \text{Aut}(A))$, this theorem lets us enumerate all extensions of G by A up to equivalence of extensions as long as A is abelian.

From extensions to cohomology. If E is any extension of G by A with operators ϕ , the homomorphism π must be surjective, so there is a function $s : G \rightarrow E$ with $\pi s = 1_G$ and for simplicity we shall set $s(1) = 1$.

We can measure how far s is from being a homomorphism by $f : G \times G \rightarrow A$ defined so that $s(g)s(h) = i(f(g, h))s(gh)$. The condition on s forces $f(g, 1) = 0 = f(1, g)$ for all $g \in G$. Some calculations based on associativity of the operation in E show that f satisfies $gf(h, k) - f(gh, k) + f(g, hk) - f(g, h) = 0$ for all $g, h, k \in G$. Therefore, f is a cocycle in the standard resolution.

If s' is another right inverse of π , it must be the case that $s'(g) = i(c(g))s(g)$ for some function $c : G \rightarrow A$ satisfying $c(1) = 0$. Furthermore, if we define f' for s' as we did f for s we find that $f'(g, h) = f(g, h) + gc(h) - c(gh) + c(g)$. Therefore, f and f' differ by a coboundary. \square

From cohomology to extensions. Let $f : G \times G \rightarrow A$ be a representative of a coset in $H^2(G, A)$ as above. We will construct the extension E_f equivalent to E .

The underlying set of E_f is $A \times G$. Define the product by $(a, g)(b, h) = (a + gb + f(g, h), gh)$. The group laws follow from the fact that f is a cocycle and $f(g, h) = 0$ if either of g or h are 1. In particular, E_f is an extension of G by A since we have the obvious homomorphisms $a \mapsto (a, 1)$ and $(a, g) \mapsto g$. Moreover, E_f is equivalent to E by the homomorphism $(a, g) \mapsto i(a)s(g)$.

Suppose we modify f by a coboundary, setting $f'(g, h) = f(g, h) + gc(h) - c(gh) + c(g)$ for some function $c : G \rightarrow A$ with $c(1) = 0$. The homomorphism $E_{f'} \rightarrow E_f$ defined by $(a, g) \mapsto (a + c(g), g)$ shows that $E_{f'}$ and E_f are equivalent extensions. \square

As an example, we show that the only central extensions of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$ for an odd natural number n is their direct product. By the theorem, we must calculate the second cohomology $H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. As we specify that the extension is central, we want trivial operators, i.e. we make $\mathbb{Z}/2\mathbb{Z}$ a trivial $\mathbb{Z}/n\mathbb{Z}$ -module. We have treated this case at the end of Section 2.3: the second cohomology is, as a set, $\{a \in A : na = 0\}$. As n is odd, the second cohomology is trivial, which means that the only extension is the split extension and, since the operators are trivial, this split extension is the direct product. If n is even, however, we get two central extensions: $\mathbb{Z}/2n\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ because we find that $H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

3.2 Galois cohomology

In this section we will assume the reader is familiar with the theory of finite Galois extensions. Let K be a finite Galois extension of the field k with Galois group $G = \text{Gal}_k K$. If K^\times denotes the multiplicative group of K then G acts on K^\times in the obvious way and we have:

Theorem 3.2.1 (Noether's equations [14]). $H^1(G, K^\times) = 0$.

Proof [6]. Let $h : G \rightarrow K^\times$ be a 1-cocycle. For any $c \in K$, we form the ‘‘Poincaré series’’ [12]

$$b = \sum_{\sigma \in G} h(\sigma)\sigma(c).$$

Notice that each element of G restricts to a character of K^\times in K . By the Independence of Characters (Theorem 1.6.1), then, the elements of G are linearly independent, i.e. we can choose c so that $b \neq 0$. Now if $\tau \in G$ we have

$$\begin{aligned} \tau(b) &= \sum_{\sigma} \tau(h(\sigma))\tau\sigma(c) \\ &= \sum_{\sigma} h(\tau)^{-1}h(\tau\sigma)\tau\sigma(c) \\ &= h(\tau)^{-1} \sum_{\sigma} h(\tau\sigma)\tau\sigma(c). \end{aligned}$$

The second line is a result of the cocycle condition, namely that for any $\tau, \sigma \in G$, $h(\tau\sigma) = h(\tau)\tau(h(\sigma))$. It is a consequence of Cayley's theorem that as σ traverses all of G , $\tau\sigma$ does so as well. Thus, the sum in the last line above is exactly b . The equation $\tau(b) = h(\tau)^{-1}b$ yields, after some manipulation, $h(\tau) = \tau(b^{-1})b$, which completes the proof as it shows that h is a coboundary. \square

This theorem is one of the key pieces in the proof that solvability of the Galois group implies solvability by radicals [11]. In this context it is applied by the following corollary. Recall the definition of the norm from algebraic number theory: if K is a Galois extension of k with Galois group G then the norm is $N_K(\theta) = \prod_{\sigma \in G} \sigma(\theta)$.

Corollary 3.2.2 (Hilbert Theorem 90 [6, 11, 12]). *If G is cyclic with generator σ then $N(\alpha) = 1$ iff there is some $\beta \in K^\times$ with $\alpha = \beta\sigma(\beta)^{-1}$.*

Proof. If $\alpha = \beta\sigma(\beta)^{-1}$ then we have

$$\begin{aligned} N(\alpha) &= N(\beta\sigma(\beta)^{-1}) = N(\beta)N(\sigma(\beta)^{-1}) \\ &= N(\beta)N(\sigma(\beta))^{-1} = N(\beta)N(\beta)^{-1} = 1. \quad [11] \end{aligned}$$

As for the converse, suppose that $N(\alpha) = 1$. The reader should note that the in this context—when the Galois group acts naturally on K^\times —the field theoretic norm coincides with the norm $N = \sum_{g \in G} g$ defined in Section 2.3. Our assumption, then, is that $\alpha \in {}_N K^\times$. By Proposition 2.3.2, $H^1(G, K^\times) =$

${}_N K^\times / DK^\times$. If $H^1(G, K^\times)$ is the trivial group then we must have ${}_N K^\times = DK^\times$. Thus, $\alpha \in DK^\times$, that is, $\alpha = (\sigma - 1)b$ for some $b \in K^\times$. There is a little notational confusion here because the multiplicative group of K is written multiplicatively (duh!) while the abelian group of a module is usually written additively. What we actually have is $\alpha = \sigma(b)b^{-1}$. If we now set $\beta = b^{-1}$ we end up with $\alpha = \beta\sigma(\beta^{-1}) = \beta\sigma(\beta)^{-1}$, as desired. \square

3.2.1 The Galois cohomology groups

Galois cohomology can be used to classify cyclic extensions of a field (extensions with cyclic Galois group). In order to treat the problem using homological algebra, however, we need to consider all of a field's cyclic extensions at once. If we are working in a fixed algebraic closure k_a of k , k has a **separable closure** k_s which is the smallest subfield of k_a containing all separable extensions of k [6]. Notice that k_s is a Galois extension of k : it is separable by definition and it is normal because if an irreducible polynomial has a root in k_s then it must be a separable polynomial. The Galois group of k_s over k , called the **absolute Galois group** of k , is an infinite group, but it's not too big. It is the absolute Galois group and its action on k_s that give us traction on classifying cyclic extensions.

By "not too big," we mean that the absolute Galois group is a **profinite group**, that is, a group that is the projective limit (cf. Section 1.7) of a system of finite groups. In particular, it is the limit of the Galois groups of its finite subextensions. With slightly more generality, let K be a Galois extension of k , possibly of infinite degree, and for any finite Galois subextension L of K , let $G_L = \text{Gal}_k L$. If $M \supseteq L$ are two finite intermediate Galois extensions, define $\phi_{L,M} : G_M \rightarrow G_L$ as the restriction map $\sigma \mapsto \sigma|_L$.

Theorem 3.2.3 ([1]). *The Galois group of K over k is isomorphic to the inverse limit of the directed system $(G_L, \phi_{L,M})$.*

Proof. We have the obvious homomorphism $\psi : \text{Gal}_k K \rightarrow \varprojlim G_L$ given by restriction to each intermediate extension L . If σ and τ are two elements of $\text{Gal}_k K$ and $\sigma(x) \neq \tau(x)$ for some $x \in K$ then x is contained in some finite subextension L (e.g. its splitting field) and so $\sigma|_L \neq \tau|_L$. This shows that ψ is injective. As for surjectivity, suppose we have a family $(\sigma_L) \in \varprojlim G_L$. Define $\sigma(x) = \sigma_L(x)$ for some subextension L containing x . This map is well defined because if L and M are two subextensions containing x then also $x \in LM$. Our definition of projective limit requires that the restrictions of σ_{LM} to L and M , respectively, are exactly σ_L and σ_M , so $\sigma_L(x) = \sigma_{LM}(x) = \sigma_M(x)$. Inspection shows σ to be an element of $\text{Gal}_k K$, giving an inverse for ψ . \square

The theorem allows us to conclude rigorously that the Galois group of any infinite Galois extension, and in particular of k_s , is a profinite group.

Profinite groups are endowed with a topology that reflects their profinite nature. If $G = \varprojlim G_\alpha$ is a profinite group, we construct this topology by giving each G_α the discrete topology, $\prod G_\alpha$ the product topology and $\varprojlim G_\alpha$ the

subspace topology [5]. This topology is generated by the collection of preimages of singleton sets under the standard projections $\pi_\alpha : G \rightarrow G_\alpha$, i.e. the set $\{\pi_\alpha^{-1}(\{g_\alpha\})\}$ where g_α ranges over all elements of all G_α s [1].

Now that we have a topology on G , we can require that any action of G on a discrete abelian group A be continuous, that is, the map $\pi : G \times A \rightarrow A$ given by $(g, a) \mapsto ga$ is continuous when $G \times A$ has the product topology. When this condition is met, A is called a **continuous G -module**. An equivalent criterion is that the stabilizer of each element of A is open in G [5]. One more reformulation is $A = \bigcup A^U$ where U ranges over all of the open subgroups of G [13]. This is not too burdensome a restriction; we shall prove that the natural action of the absolute Galois group, which is our main focus, is continuous.

Let $G = \text{Gal}_k k_s$ be the absolute Galois group of a field k with separable closure k_s . We know from Theorem 3.2.3 that $G = \varprojlim G_L$ where $G_L = \text{Gal}_k L$ for every finite Galois extension L of k . Both k_s and k_s^\times are natural G -modules, where k_s denotes the additive group of k_s and k_s^\times the multiplicative group.

Proposition 3.2.4. *The action of G on any submodule of k_s or k_s^\times is continuous.*

Proof. To prove the proposition, we show that $A = \bigcup A^U$ where U ranges over all open subgroups of G and A is any submodule of k_s or k_s^\times . Let α be any element of A and define L as its splitting field over k . Certainly $\alpha \in A^U$ where $U = \text{Gal}_L k_s$, so we will demonstrate that U is open in G . By definition, U is the largest subgroup of G that fixes L , so $U = \pi^{-1}(1_L)$ where π is the standard projection of G onto G_L . This completes the proof because π is continuous and G_L has the discrete topology, meaning that $\{1_L\}$ is an open set. \square

We can define a modified cohomology functor for profinite groups acting continuously on discrete abelian groups that will allow us to exploit properties of the group's finite quotients. If $G = \varprojlim G_\alpha$ is a profinite group and A a continuous G -module, we form a direct system indexed by the standard quotients of G : letting U_α be the kernel of the projection of G onto G_α , define $\phi_{\alpha\beta} : H^n(G_\alpha, A^{U_\alpha}) \rightarrow H^n(G_\beta, A^{U_\beta})$ as the inflation map (cf. Section 2.2.1) induced by the surjection $G_\beta \rightarrow G_\alpha$. We now set $H^n(G, A) = \varinjlim H^n(G_\alpha, A^{U_\alpha})$; these are the **continuous cohomology groups**. In the case where G is the absolute Galois group of a field k , $H^n(G, A)$ is called the n th **Galois cohomology group** and we instead write $H^n(k, A)$.

Continuous cohomology groups, and in particular Galois cohomology groups, have many of the same properties as the cohomology groups introduced in Section 2.2. If G is a finite group (and therefore profinite) then its continuous cohomology groups are equal to its normal cohomology groups because $H^n(G, A)$ will be a terminal object in the direct system constructed above. The low dimensional continuous cohomology groups have concrete descriptions similar to the normal ones: the first cohomology is the group of equivalence classes of *continuous* crossed homomorphism and the second cohomology is the group of equivalence classes of *continuous* factor sets [13]. Also, the 0th continuous cohomology group is still the group of G -invariants, as we have seen for the usual

cohomology groups. Finally, a short exact sequence of continuous G -modules induces a long exact sequence in their continuous cohomology. The proof of this fact is long and will not appear here.⁷

3.2.2 Classification of cyclic extensions

We can use the Galois cohomology groups to prove some results about cyclic field extensions. The first case we deal with is where the degree of the extension is prime to the characteristic of the field. We start with a base field k containing all of the m th roots of unity in some separable closure. If $\alpha \in k_s$ is a root of $x^m - a$ for some $a \in k$, then it should be clear that $k(\alpha)$ is a cyclic Galois extension of degree dividing m . It turns out that the converse of this statement is also true. The theorem here is a high level statement of the result. Its corollary, below, states the implication in terms of cyclic extensions.

If k is a field and m a positive integer prime to the characteristic of k , let μ_m be the group of m th roots of unity in k_s . The Galois group of k_s acts on μ_m in the obvious way. Proposition 3.2.4 guarantees that this action is continuous.

Theorem 3.2.5 (Kummer Theory [5, 12]).

$$H^1(k, \mu_m) \cong k^\times / (k^\times)^m.$$

Specifically, any 1-cocycle $f : G \rightarrow \mu_m$ is given by $f(\sigma) = \sigma(\alpha)\alpha^{-1}$ for some $\alpha \in k_s$ with $\alpha^m \in k$. The isomorphism then maps the cohomology class of f to the equivalence class of α^m .

For the proof of the theorem, we generalize Theorem 3.2.1 to infinite Galois extensions.

Lemma 3.2.6.

$$H^1(k, k_s^\times) = 0.$$

Proof. Let $K = k_s$. By our definition of continuous cohomology, $H^1(k, K^\times)$ is the projective limit of $H^1(G, L^\times)$ for all finite Galois subextensions L of K with Galois group G over k . Theorem 3.2.1 tells us that all of these groups are the zero group. Thus, their limit is zero. \square

The lemma justifies the claim that a 1-cocycle $f : G \rightarrow \mu_m$ is of the form $f(\sigma) = \sigma(\alpha)\alpha^{-1}$. Now for the proof of the theorem:

Proof of Theorem 3.2.5. Let G be the absolute Galois group of k . We have a sequence of G -modules

$$1 \rightarrow \mu_m \rightarrow k_s^\times \rightarrow k_s^\times \rightarrow 1,$$

where the morphism $k_s^\times \rightarrow k_s^\times$ is the m th power map. This homomorphism is surjective because for any $a \in k_s$, the polynomial $x^m - a$ is separable since m is

⁷Essentially, it is a consequence of taking direct limits being an exact functor on the category of direct systems of abelian groups.

prime to the characteristic of k . Thus, it has roots in k_s , any of which maps to a under the m th power map. The first morphism is simply the inclusion and is therefore clearly injective. As μ_m is by definition the kernel of the m th power map, we have now shown that the above sequence is exact. A piece of the long exact cohomology sequence it induces is

$$k^\times \rightarrow k^\times \rightarrow H^1(k, \mu_m) \rightarrow 0,$$

where the first map is the m th power map. We obtain this by noticing that $H^0(k, k_s^\times) = (k_s^\times)^G = k^\times$ and using the lemma for $H^1(k, k_s^\times) = 0$. The result now follows by the first isomorphism theorem. The description of the isomorphism may be seen by inspection of the construction of the connecting homomorphism. \square

Corollary 3.2.7 ([5]). *Under the conditions of the above theorem, suppose that k contains μ_m . Then a cyclic extension of degree m must be of the form $k(\alpha)$ where $\alpha \in k_s$ and $\alpha^m \in k$.*

Proof. Let G be the absolute Galois group of k . By supposing $\mu_m \subseteq k$, we require that the action of G on μ_m is trivial. Looking to the bar resolution, 1-cocycles are now homomorphisms from G to μ_m , which we identify with $\mathbb{Z}/m\mathbb{Z}$ by choosing a primitive m th root. Coboundaries, being such homomorphisms of the form $f(a) = g(a)a^{-1}$, are trivial because $g(a) = a$. Thus, $\text{Hom}(G, \mathbb{Z}/m\mathbb{Z}) \cong H^1(k, \mu_m)$. Suppose K is such an extension and let χ be the projection $G \rightarrow \text{Gal}_k K \cong \mathbb{Z}/m\mathbb{Z}$. By the isomorphism we have just derived, χ corresponds to a unique member of $H^1(k, \mu_m)$. Now the theorem tells us that χ is given by $\chi(\sigma) = \sigma(\alpha)\alpha^{-1}$ for some $\alpha \in k_s$ with $\alpha^m = a \in k$. If we pick a generator $\sigma \in \text{Gal}_k K$, we have $\sigma(\alpha)\alpha^{-1} = \chi(\sigma) = \zeta \in \mu_m$. Rearranging, this is $\sigma(\alpha) = \zeta\alpha$. Note that this means that $\alpha \in K$ because $\alpha = \sigma^m(\alpha) \in K$. Observe that $\sigma^i(\alpha) = \zeta^i\alpha$ are distinct elements of K for $i = 0, 1, \dots, m-1$, so α is not contained in any proper Galois subextension of K [4]. But $k(\alpha)$ is a Galois subextension since it is a splitting field of $x^m - a$. We must have, therefore, $K = k(\alpha)$. \square

The cyclic extensions that are not covered by Kummer theory are those of degree p^n , where p is the characteristic of k and $n > 0$. Here we treat the $n = 1$ case; when $n \geq 1$ we require the use of ‘‘Witt vectors’’ [6, 12]. If k is any field, the absolute Galois group of k acts continuously on the additive group of any Galois extension K in the obvious way. The following lemma is an additive analogue of Hilbert’s Theorem 90.

Lemma 3.2.8.

$$H^1(k, k_s) = 0.$$

Proof. We demonstrate trivial first cohomology for all finite extensions of k . The result follows by passing to the limit. Let K be a finite Galois extension of k with Galois group G . First, choose an element $\theta \in K$ with $\text{Tr}(\theta) \neq 0$.

This is possible because of Proposition 1.6.2. Given a 1-cocycle $h : G \rightarrow K$ in $H^1(G, K)$, let

$$b = \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} h(\tau)\tau(\theta).$$

We now find that if σ is any element of G ,

$$\begin{aligned} \sigma(b) &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} \sigma(h(\tau))\sigma\tau(\theta) \\ &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} (h(\sigma\tau)\sigma\tau(\theta) - h(\sigma)\sigma\tau(\theta)) \\ &= \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} h(\sigma\tau) - h(\sigma) \frac{1}{\mathrm{Tr}(\theta)} \sum_{\tau \in G} \sigma\tau(\theta). \end{aligned}$$

The second line is a result of the cocycle condition which, in the additive case, reads $h(\sigma\tau) = h(\sigma) - \sigma(h(\tau))$. Cayley's theorem tells us that the last line actually reads $\sigma(b) = b - h(\sigma)$. Rearranged, this is $h(\sigma) = b - \sigma(b)$. If we now let $\beta = -b$ then $h(\sigma) = \sigma(\beta) - \beta$ shows that h is a coboundary [6]. \square

In fact, it is true that $H^n(k, k_s) = 0$ for all $n > 0$ [5, 12]. The proof of this fact is most often done using the Normal Basis Theorem, which can be found in Lang [6] or Roman [10] or, at a much higher level, in Blessenohl [2].

Theorem 3.2.9 (Artin-Schreier Theory [5, 12]). *Let k be a field of positive characteristic p and \wp be the endomorphism mapping x to $x^p - x$. Then there is an isomorphism $k/\wp(k) \cong H^1(k, \mathbb{Z}/p\mathbb{Z})$ given by associating to each 1-cocycle $f : G \rightarrow \mathbb{Z}/p\mathbb{Z}$ the equivalence class of $a \in k$ such that $f(\sigma) = \sigma(a) - a$ where $a \in k_s$ and $\wp(a) = a$.*

Proof. Observe that $\wp : k_s \rightarrow k_s$ is a homomorphism of G -modules, where G is the absolute Galois group of k . Following the method in the proof of the previous theorem, we apply cohomology to the exact sequence associated to the surjection \wp :

$$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow k_s \xrightarrow{\wp} k_s \rightarrow 0.$$

Note that \wp is surjective because the polynomial $x^p - x$ is separable in characteristic p and that $\ker \wp \cong \mathbb{Z}/p\mathbb{Z}$ because we know that $x^p - x$ has at most p roots and Fermat's little theorem gives us p roots: $0, 1, \dots, p-1$. Thus, the sequence is indeed exact. The result now follows as in the proof of Kummer Theory, using Lemma 3.2.8 instead of 3.2.6. \square

We classify cyclic extensions in this case just like we did in Corollary 3.2.7: every cyclic extension of degree p is of the form $k(\alpha)$ where $\wp(\alpha) \in k$. The proof of this is analogous to that for the corollary above.

4 Glossary

Abelian categories These are a class of categories in which $\text{Hom}(A, B)$ forms an abelian group for all objects A and B .

Cokernel The cokernel of the homomorphism of modules $\sigma : X \rightarrow Y$, written $\text{cok } \sigma = Y/\sigma X$, is the quotient of the codomain by the image of σ together with the canonical projection onto this quotient.

Epimorphism (Epic morphism) In any category, a morphism ϵ is called epic or an epimorphism if for every σ and τ left composable with ϵ , $\sigma\epsilon = \tau\epsilon$ implies $\sigma = \tau$. In most familiar concrete categories, including those of modules and of groups, the epimorphisms are exactly the surjective morphisms.

Exact sequence If \mathcal{C} is any category with kernels and images, a sequence $\cdots \rightarrow A_{n-1} \xrightarrow{\alpha} A_n \xrightarrow{\beta} A_{n+1} \rightarrow \cdots$ of objects and morphisms in \mathcal{C} is exact at A_n if $\ker \beta = \text{im } \alpha$. An exact sequence is a sequence that is exact at every intermediate object.

Free module A module F is free on a subset $S \subseteq F$ if for any module M and set function $f : S \rightarrow M$, f lifts to a module homomorphism $\tilde{f} : F \rightarrow M$ such that $\tilde{f}|_S = f$. A module is called free if it is free on some subset. An R -module F is free if and only if $F \cong \bigoplus_I R$ for some index set I . (In fact, we can take $I = S$.)

Free resolution A resolution $0 \leftarrow M \leftarrow A_0 \leftarrow A_1 \leftarrow A_2 \leftarrow \cdots$ in which each A_i is a free module.

Group ring If G is a group, the group ring $\mathbb{Z}G$ is the ring of finite \mathbb{Z} -linear combinations of elements of G .

Laurent polynomials Sums of the form $\sum_{i \in \mathbb{Z}} a_i x^i$ with coefficients $a_i \in \mathbb{Z}$, all but finitely many equal to zero, in a formal variable x form a ring called the ring of Laurent polynomials. They are readily generalized to more than one variable.

Monomorphism (Monic morphism) In any category, a morphism μ is called monic or a monomorphism if for every σ and τ right composable with μ , $\mu\sigma = \mu\tau$ implies $\sigma = \tau$. In most familiar concrete categories, including those of modules and of groups, the monomorphisms are exactly the injective morphisms.

Norm If K is a finite Galois extension of a field k with Galois group $G = \text{Gal}_k K$, the norm is the endomorphism of the multiplicative group K^\times given by $N_K(\theta) = \prod_{\sigma \in G} \sigma(\theta)$.

Projective module A module P is projective if for every surjective module homomorphism $\pi : M' \rightarrow M$ and morphism $\phi : P \rightarrow M$, ϕ lifts to a

morphism $\psi : P \rightarrow M'$ satisfying $\phi = \pi\psi$. A module is projective if and only if it is a direct summand of a free module. Every free module is therefore projective.

Projective resolution A resolution $0 \leftarrow M \leftarrow A_0 \leftarrow A_1 \leftarrow A_2 \leftarrow \dots$ in which each A_i is a projective module.

Resolution If M is an R -module, a resolution of M over R is an exact sequence $0 \leftarrow M \leftarrow A_0 \leftarrow A_1 \leftarrow A_2 \leftarrow \dots$ of R -modules.

Short exact sequence An exact sequence of the form $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$.

Split exact sequence A short exact sequence with morphisms α and β is split if β has a right inverse that is a homomorphism.

Trace If K is a finite Galois extension of a field k with Galois group $G = \text{Gal}_k K$, the trace is the linear functional on the k -vector space K given by $\text{Tr}_K(\theta) = \sum_{\sigma \in G} \sigma(\theta)$.

References

- [1] George M. Bergman. Infinite Galois theory, Stone spaces, and profinite groups. <http://math.berkeley.edu/~gbergman/grad.hndts/infGal+profin.ps>, 1997.
- [2] Dieter Blessenohl. On the normal basis theorem. *Note di Matematica*, 27(1):5–10, 2007.
- [3] Kenneth S. Brown. *Cohomology of Groups*. Springer-Verlag, 1982.
- [4] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Wiley, third edition, 2004.
- [5] Phillippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge University Press, 2006.
- [6] Serge Lang. *Algebra*. Addison-Wesley, third edition, 1993.
- [7] Saunders MacLane. *Homology*. Springer-Verlag, 1963.
- [8] Saunders MacLane. *Categories for the Working Mathematician*. Springer-Verlag, 1971.
- [9] Saunders MacLane and Garrett Birkhoff. *Algebra*. The MacMillan Company, 1967.
- [10] Steven Roman. *Field Theory*. Springer-Verlag, 1995.
- [11] Joseph Rotman. *Galois Theory*. Springer-Verlag, second edition, 1998.
- [12] Jean-Pierre Serre. *Local Fields*. Springer-Verlag, 1979.
- [13] Jean-Pierre Serre. *Galois Cohomology*. Springer-Verlag, 1997.
- [14] Edwin Weiss. *Cohomology of Groups*. Academic Press, 1969.