An Intuitive Development of Galois Cohomology

Noah Parker

April 2025

1 Introduction

Class field theory is one of the crowning achievements of 20-th century number theory. However, its original formulation dealt only with abelian extensions. Eventually, number theorists developed the tools of group cohomology to study non-abelian extensions in a similar manner.

We will study the generalities of group cohomology, along with an introduction to general homological algebra, before using our newfound tools to study the special case from which the general emerged: Galois cohomology. We will primarily concern ourselves with the cohomology of finite groups when discussing general group cohomology, before turning to profinite groups for the sake of studying the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$.

Some familiarity with the basic notions of category theory and infinite Galois theory will be assumed, but most topics will be at least defined before use. We attempt to present the ideas in as intuitive of a flow as possible, with logical gaps left to be filled by outside reading primarily when they are too excessive of a detour. Whenever such gaps are necessary, an appropriate source is provided.

2 G-modules

Before defining our cohomology, we must tend to some preliminary notions. Henceforth, G is a finite group, and A is an abelian group. Recall that the *group algebra of G over $\mathbb{Z}$* is the set of formal sums

$$\mathbb{Z}[G] := \Big\{ \sum_{g \in G} n_g g \ : \ n_g \in \mathbb{Z} \ \forall g \in G \Big\},$$

equipped with the obvious addition and convolutional multiplication. We will often refer to $\mathbb{Z}[G]$ simply as the group ring of G.

Definition 2.1. A *G-module* is a left $\mathbb{Z}[G]$-module.

This definition, however, is not very enlightening. Thus, we give an equivalent definition.

Definition 2.2. A *G-module* is an abelian group A equipped with a (left) action

$$\begin{aligned} \rho : G \times A &\to A \\ (g, a) &\mapsto g \cdot a, \end{aligned}$$

such that

$$\begin{aligned} g \cdot (g' \cdot a) &= (gg') \cdot a, \\ g \cdot (a + a') &= g \cdot a + g \cdot a', \\ 1 \cdot a &= a \end{aligned}$$

for all $g, g' \in G$ and $a, a' \in A$.

Example 2.3. Let L/K be a finite extension of fields. Then both K and K^* can be equipped with a $\mathrm{Aut}(L/K)$-module structure in a natural manner.

As you'd expect, we can also define a notion of G-module homomorphism.

Definition 2.4. A G-module homomorphism is a morphism $f : A \to A'$ of abelian groups such that A and A' are G-modules, and

$$g \cdot f(a) = f(g \cdot a)$$

for all $g \in G$ and $a \in A$.

Once again, we note that this is equivalent to being a $\mathbb{Z}[G]$-module homomorphism. Now that we have objects and maps, we can define a category.[1] Let Mod_G be the category of G-modules, with G-modules homorphisms as morphisms. Additionally, we denote by *Grp* the category of groups, and $\mathfrak{Ab}$ the category of abelian groups.

Now, given groups $H \leqslant G$ and an H-module A, the natural question is whether we can construct a G-module from A. Fortunately, we can.

Definition 2.5. Let $H \leqslant G$ be groups, and A an H-module. Then

$$\mathrm{Ind}_G^H(A) := \{f \in \mathrm{Hom}_{\mathrm{Grp}}(G, A) \; : \; \forall g \in G \; \forall h \in H, \;\; h \cdot f(g) = f(hg)\}$$

is a G-module under the structure

$$\begin{aligned}(f + f')(g) &= f(g) + f'(g),\\ (g \cdot f)(g') &= f(g'g)\end{aligned}$$

for all $g, g' \in G$ and $f, f' \in \mathrm{Ind}_G^H(A)$. We say that $I_G^H(A)$ is the *induced module* from H to G of the H-module A.

The first thing to consider now that we have induction is the induced module $\mathrm{Ind}_G^{\{1\}}(A)$. Since there is no ambiguity, we shorten it to the induced G-module of A and denote it $\mathrm{Ind}_G(A)$. The condition that $h \cdot f(g) = f(hg)$ is now trivial, so $\mathrm{Ind}_G(A)$ is just $\mathrm{Hom}(G, A)$ equipped with the action $(g \cdot f)(g') = f(g'g)$ of G. What can we do with these induced modules, though?

Proposition 2.6. *Let G be a finite group, and H a subgroup of G. Take A to be an H-module and $I_G^H(A)$ the induced module from H to G. Then, for any G-module B, we can identify $Hom_H(B, A)$ with $Hom_G(B, I_G^H(A))$.*

Proof. Let $\psi \in \mathrm{Hom}_H(B, A)$. We construct a G-compatible map $\varphi : B \to I_G^H(A)$ associated with ψ as follows. For each $b \in B$, $\varphi(b)$ is the map $g \mapsto \psi(gb)$. Since ψ is an H-morphism, we have that

$$h \cdot \varphi(b)(g) = h \cdot \psi(gb) = \psi((hg)b) = \varphi(b)(hg)$$

satisfies the property of $\mathrm{Ind}_G^H(A)$. Additionally, for any $g, g' \in G$ and $b \in B$, we have that

$$\varphi(g \cdot b)(g') = \psi(g'gb) = \varphi(b)(g'g) = (g \cdot \varphi(b))(g'),$$

which shows that φ is indeed a G-morphism $B \to I_G^H(A)$.

We define the map $u : \mathrm{Hom}_H(B, A) \to \mathrm{Hom}_G(B, I_G^H(A))$ by $\psi \mapsto \varphi$, as constructed above. We wish to show that u is an isomorphism of abelian groups. It suffices now to show that u is bijective. Injectivity follows easily, as $\varphi(b) \equiv 0$ for all b implies $\psi(b) = \varphi(b)(1) = 0$ for all b, i.e. $\psi \equiv 0$ is the zero map.

Now, we consider surjectivity. Take $\theta \in \mathrm{Hom}_G(B, I_G^H(A))$. By definition, we have

$$\theta(gb)(g') = (g \cdot \theta(b))(g') = \theta(b)(g'g)$$

for all $g, g' \in G$ and $b \in B$. Let $\psi \in \mathrm{Hom}_H(B, A)$ be defined by $\psi(b) = \theta(b)(1)$. For any $h \in H$ and $b \in B$, we have

$$\psi(hb) = \theta(hb)(1) = \theta(b)(h) = h \cdot (\theta(b)(1))$$

[1] Unfortunately, we must delve into the realm of category theory. Those unfamiliar are encouraged to keep a copy of [4] on hand for reference.

since $\theta(b) \in I_G^H(b)$, giving us that $\psi \in \mathrm{Hom}_H(B, A)$. Finally,

$$u(\psi)(b)(g) = \psi(gb) = \theta(gb)(1) = \theta(b)(g)$$

for all $b \in B$ and $g \in G$ gives us that $u(\psi) = \theta$. We conclude that u is surjective as well, so that u is an isomorphism. Hence,

$$\mathrm{Hom}_H(B, A) \cong \mathrm{Hom}_G(B, I_G^H(A)).$$

□

Now that we have an action of G on A, it's natural to consider its fixed points. We define

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

Clearly A^G is an abelian group. Further, we can think of A^G as the image of A under a map from the category of G-modules, Mod_G, to the category of abelian groups, $\mathfrak{Ab}$. It turns out this map behaves rather well.

Definition 2.7. For any group G, the map

$$\begin{aligned}(-)^G : \mathrm{Mod}_G &\to \mathfrak{Ab} \\ A &\mapsto A^G\end{aligned}$$

is a covariant functor.

Proving functoriality of the map is quite simple, but those unfamiliar with category theory are encouraged to do so as an exercise.

Now, as any good homological algebraist would, let's consider some exact sequences.

Proposition 2.8. *Let G be a finite group, and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{h} C \longrightarrow 0$$

an exact sequence of G-modules. Then the sequence

$$0 \longrightarrow A^G \xrightarrow{f} B^G \xrightarrow{h} C^G$$

is exact at A^G and B^G. That is, $(-)^G$ is left exact.

Proof. Exactness at A^G follows from exactness of the original sequence at A, since f only has its domain restricted. $\mathrm{im}\, f \subset \ker h$ follows similarly from exactness of the original sequence.

Now, let $b \in \ker h$. Exactness of the original sequence supplies us with $a \in A \cap f^{-1}(b)$. It suffices, then, to show that $s \cdot a = a$ for all $s \in G$. Let $s \in G$. Then

$$f(s \cdot a) = s \cdot f(a) = s \cdot b = b = f(a)$$

gives us $s \cdot a = a$, since f is injective. Thus, $a \in A^G$, so $\ker h \subset \mathrm{im}\, f$. We conclude that $\mathrm{im}\, f = \ker h$, so the sequence is exact at B^G. This completes the proof. □

Now that we have part of an exact sequence, we might naturally want to consider how to continue it. To do so, we will have to talk a little bit more about homological algebra.

3 Abelian Categories and Derived Functors

Definition 3.1. An *additive category* $\mathcal{C}$ is a category such that

1. For any objects A, B of $\mathcal{C}$, the set $\mathrm{Hom}(A,B)$ is an abelian group, and the composition morphisms is distributive with respect to addition. That is, for any objects A, B, C, D of $\mathcal{C}$ and morphisms $f : A \to B$, $g, g' : B \to C$, $h : C \to D$, we have
$$f(g+g')h = fgh + fg'h.$$
2. $\mathcal{C}$ has a zero object 0. That is, there are unique morphisms $A \to 0$ and $0 \to A$ for each object A of $\mathcal{C}$.
3. If A and B are objects of $\mathcal{C}$, the product $A \times B$ exists.[2]

The obvious examples are that of modules and abelian groups. In fact, we will specialize further.

Definition 3.2. An additive category $\mathcal{C}$ is called an *abelian category*, if

1. Every morphism in $\mathcal{C}$ has a kernel and cokernel,
2. Every monomorphism is the kernel of its cokernel,
3. Every epimorphism is the cokernel of its kernel.

We won't have to work much with kernels or cokernels, so their exact definitions are unimportant. What the reader should know is that the above definition is exactly what we need to discuss injections, surjections, and exact sequences of objects in a category. Those who are interested in digging deeper are encouraged to read a book on homological algebra, such as [5].

Remark 3.3. Mod_G is an abelian category.

This fact is the key to defining group cohomology. However, we need to specialize a little more what types of abelian categories we care about.

Definition 3.4. We say an object I in $\mathcal{C}$ is injective if the contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-,I)$ is exact. That is, applying $\mathrm{Hom}_{\mathcal{C}}(-,I)$ preserves short exact sequences.

In Mod_G, this is equivalent to every morphism of a submodule extending to a morphism of the full module.[3] In $\mathfrak{Ab}$, this is just another name for an abelian group being divisible. Recall that an abelian group G is divisible if $nG = G$ for all positive integers n. The rationals are the canonical example.

Definition 3.5. We say that an abelian category $\mathcal{C}$ *has enough injectives* if every object A can be embedded into an injective object, $M \hookrightarrow I$.

These two definitions build up to the following result.

Theorem 3.6. *Let $\mathcal{C}$ be an abelian category which has enough injectives. Then, for any object A of $\mathcal{C}$, there exists a chain complex*
$$(I^\bullet, d^\bullet) = 0 \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$
of injective objects, such that
$$0 \longrightarrow A \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$
is exact. The chain complex $I^\bullet$ is called an injective resolution of A, *and is unique up to chain homotopy.*

If $F : \mathcal{C} \to \mathcal{D}$ is a left exact functor and A, $(I^\bullet, d^\bullet)$ are as above, we can define the right derived functors $R^qF : \mathcal{C} \to \mathcal{D}$ *for $q > 0$ on A by*
$$R^qF(A) := \frac{\ker F(d^q)}{\operatorname{im} F(d^{q-1})}.$$

[2] See [4] for categorical definition of product.

[3] See [7].

The right derived functors are well-defined, and if $0 \to A \to B \to C \to 0$ *is an exact sequence in* $\mathcal{C}$*, then the sequence*

$$0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \xrightarrow{\delta^0} R^1F(A) \longrightarrow \cdots$$

$$\cdots \xrightarrow{\delta^{q-1}} R^qF(A) \longrightarrow R^qF(B) \longrightarrow R^qF(C) \xrightarrow{\delta^q} R^{q+1}F(A) \longrightarrow \cdots$$

is exact.

Proof. See [5], corollary 6.5 and section 6.2.3. □

Finally, we've answered the question we posed at the start of 2.1 — so long as Mod_G has enough injectives. Fortunately for us, this is not very difficult to verify.

Proposition 3.7. *G-module has enough injectives.*

Proof. Let A be a G-module, and take A_0 to be A regarded simply as an abelian group. We claim that A_0 can be embedded in a divisible, i.e. injective, group I.

Let i be the inclusion $\mathbb{Z} \to \mathbb{Q}$. Noting that direct sums and quotients of divisible groups are divisible, we have

$$A_0 = \frac{\oplus_j \mathbb{Z}}{R} \hookrightarrow \frac{\oplus_j \mathbb{Q}}{i(R)} =: I$$

for I a divisible group.

Now that we have the embedding $A_0 \hookrightarrow I$, we apply the functor Ind_G to receive $\mathrm{Ind}_G(A_0) \hookrightarrow \mathrm{Ind}_G(I)$. Composing this with the inclusion $A \hookrightarrow \mathrm{Ind}_G(A_0)$ mapping a to the function $g \mapsto ga$, we receive an inclusion $A \hookrightarrow \mathrm{Ind}_G(I)$. By Proposition 2.6, we can identify $\mathrm{Hom}_G(M, \mathrm{Ind}_G(I))$ with $\mathrm{Hom}_{\mathbb{Z}}(M, I)$ for each G-module M as before, so $\mathrm{Hom}(-, \mathrm{Ind}_G(I))$ is exact. □

Now, we've finally developed the tools to define group cohomology!

Definition 3.8. Let G be a group. We take $H^0(G, -) = (-)^G$, and let $H^q(G, -) : \mathrm{Mod}_G \to \mathfrak{Ab}$ for $q > 0$ be the right derived functors of $(-)^G$. That is, for any G-module A, we take an injective resolution $(I^\bullet, d^\bullet)$ of A, apply $(-)^G$ to receive the complex $(I^{\bullet G}, d^{\bullet G}) := ((I^\bullet)^G, (d^\bullet)^G)$, and define

$$H^q(G, A) := \frac{\ker d^{qG}}{\operatorname{im} d^{(q-1)G}}.$$

4 Group Cohomology

Although we've verified the existence of our homology groups, we know almost nothing about their structures for $q > 0$. Our flurry of exact sequences is meaningless if we hardly know anything about the groups involved. Thus, we get to work computing $H^q(G, A)$.

Fix a group G, $q \geqslant 0$, and consider the free $\mathbb{Z}$-module P_q generated by the set G^{q+1}, embued with the group action

$$g(g_0, \ldots, g_q) = (gg_0, \ldots, gg_q).$$

Additionally, note that P_q is a free $\mathbb{Z}[G]$ module generated by elements of the form $(1, g_1, \ldots, g_q)$ under the same action. Now, for any $q \geqslant 1$, we can define a boundary map $\partial_q : P_q \to P_{q-1}$ by

$$\partial(g_0, \ldots, g_q) = \sum_{i=0}^{q} (-1)^i (g_0, \ldots, \widehat{g_i}, \ldots, g_q),$$

where $\widehat{\cdot}$ in a list denotes omitting the element $\cdot$ from the list. Just as in simplicial homology, this analogous boundary map has the property that $\partial_{q-1} \circ \partial_q = 0$. Thus, $(P_\bullet, \partial_\bullet)$ is a chain complex.

Proposition 4.1. *Let G be a group and M be a G-module. Then*

$$H^q(G,M) \cong \frac{\ker{(\partial_q)}^*}{\operatorname{im}{(\partial_{q-1})}^*},$$

where $(\partial_q)^* : Hom_G(P_q, M) \to Hom_G(P_{q+1}, M)$ is precomposition by the boundary map.

There is a brief proof of this fact as chapter 2, proposition 1.16 in [3], relying on the notion of *projective resolutions*. This notion is dual to that of injective objects we discussed earlier, and plays an equivalent role in the study of homology.

Now, to each element of $\mathrm{Hom}_{\mathbb{Z}}(P_q, M)$ we can naturally assign an map $\varphi : G^{q+1} \to A$. Since a map from the free group is determined by its values on its generators, this is a bijection. However, we want to restrict to G-module homomorphisms.

Doing so, we can identify $\mathrm{Hom}(P_q, M)$ with its image of G-module homomorphisms under the above map. We call this image the set of *homogeneous q-cochains of G with values in M*, and denote it

$$\tilde{C}^q(G,A) := \{(\varphi : G^{q+1} \to A) \ : \ \varphi(gg_0, \ldots, gg_q) = g(\varphi(g_0, \ldots, g_q))\}.$$

Taking $\tilde{\delta}^q : \tilde{C}^q(G,A) \to \tilde{C}^{q+1}(G,A)$ to be the map induced by $(\partial_q)^*$, proposition 2.17 gives us

$$H^q(G,A) \cong \frac{\ker \tilde{\delta}^q}{\operatorname{im} \tilde{\delta}^{q-1}}.$$

Since we have the set of homeogenous q-chains, it is natural to wonder what q-cochains are. Fortunately, one need not wonder for long.

Definition 4.2. Let G be a group, and M a G-module. We define the sequence $(C^\bullet(G,A), \delta^\bullet)$ of *q-cochains of G with values in M* by

$$C^q(G,A) := \{\varphi : G^q \to A\},$$

and $\delta^q : C^q(G,A) \to C^{q+1}(G,A)$ by

$$(\delta^q\varphi)(g_1, \ldots, g_{q+1}) := g_1\varphi(g_2, \ldots, g_{q+1}) + \sum_{i=1}^{q}(-1)^i\varphi(g_1, \ldots, g_ig_{i+1}, \ldots, g_{q+1}) + (-1)^{q+1}\varphi(g_1, \ldots, g_q).$$

Further, we define the group

$$Z^q(G,A) := \ker \delta^q$$

of *q-cocyles*, and the group

$$B^q(G,A) := \operatorname{im} \delta^{q-1}$$

of *q-coboundaries.*

Proposition 4.3. *The sequence $(C^\bullet(G,A), \delta^\bullet)$ is a chain complex, and*

$$H^q(G,A) \cong \frac{Z^q(G,A)}{B^q(G,A)}.$$

Proof. We define maps $f_q : C^q(G,A) \to \tilde{C}^q(G,A)$ and $h_q : \tilde{C}^q(G,A) \to C^q(G,A)$ for each $q \geqslant 0$ as follows.

For any $\varphi \in C^q(G,A)$, let

$$f_q\varphi(g_0, \ldots, g_q) := g_0\varphi(g_0^{-1}g_1, g_1^{-1}g_2, \ldots, g_{q-1}^{-1} \cdots g_q).$$

Then

$$\begin{aligned} f_q\varphi(gg_0, \ldots, gg_q) &= gg_0\varphi((gg_0)^{-1}gg_1, \ldots, (gg_{q-1})^{-1}gg_q) \\ &= g(f_q\varphi(g_0, \ldots, g_q)) \end{aligned}$$

give us that $f_q\varphi \in \tilde{C}^q(G, A)$. We define h_q to be the inverse map

$$h_q\psi(g_1, \dots, g_q) := \psi(1, g_1, g_1g_2, \dots, g_1 \cdots g_q).$$

Thus, f_q is a bijection $C^q(G, A) \leftrightarrow \tilde{C}^q(G, A)$. Further, a computation shows that $\delta^q = g_{q+1} \circ \tilde{\delta}^q \circ f_q$. This gives us justification for the unwieldy definition of δ^q. More importantly, it shows that

$$\delta^q \circ \delta^{q-1} = (g_{q+1} \circ \tilde{\delta}^q \circ f_q) \circ (g_q \circ \tilde{\delta}^{q-1} \circ f_{q-1}) = g_{q+1} \circ \tilde{\delta}^q \circ \tilde{\delta}^{q-1} \circ f_{q-1} = 0,$$

and

$$\frac{\ker \tilde{\delta}^q}{\operatorname{im} \tilde{\delta}^{q-1}} \cong \frac{\ker \delta^q}{\operatorname{im} \delta^{q-1}},$$

from which our result follows. □

This definition is far more workable, so we will henceforth take it to be our definition of $H^q(G, A)$. That is,

Example 4.4. Fix a G-module M. δ^{q-1} is taken to be the zero map. $G^0 = \{*\}$ is singleton, so functions $\varphi : G^0 \to A$ are in correspondence with elements of a. If $\varphi(*) = a$, then

$$\delta^0\varphi(g) = ga - a.$$

We call such maps *principle crossed homomorphisms*, and, as in the general case, denote their $B^1(G, A)$. Thus, $H^0(G, A) = \ker \delta^0 = A^G$ is the elements fixed by G, as we constructed.

If $\varphi : G \to A$, then

$$\delta^1\varphi(g, g') = g\varphi(g') - \varphi(gg') + \varphi(g).$$

Then $\ker \delta^1$ is the set of maps φ such that

$$\varphi(gg') = \varphi(g) + g\varphi(g')$$

for all $g, g' \in G$. We call such maps *crossed homorphisms*, and denote the group of crossed homomorphisms $G \to A$ by $Z^1(G, A)$. This allows us to characterize $H^1(G, A)$ as the group of crossed homomorphisms modulo principle crossed homomorphisms.

5 Galois Cohomology

Now that we've sufficiently developed the theory of group cohomology, we can finally consider some concrete examples. One of the most important classes of explicit examples, as well as the main focus of this paper, is the special case of G being a Galois group.

Definition 5.1. Let L/k be a finite seperable Galois extension with Galois group $G = \mathrm{Gal}(L/k)$. For any G-module A, we denote the *Galois cohomology of L/k with coefficients in A*,

$$H^q(L/k, A) := H^q(G, A),\ q \geqslant 0.$$

We call A a *Galois module.*

Example 5.2. In the following examples, L/k is a finite seperable Galois extension of fields with Galois group $G = \mathrm{Gal}(L/k)$.

1. Let $\mathfrak{p} \subset k$ be an unramified prime in L, and take $\mathfrak{q} \subset L$ lying over $\mathfrak{p}$. Let $\ell := \mathcal{O}_L/\mathfrak{q}$, $\kappa := \mathcal{O}_k/\mathfrak{p}$. $\mathfrak{p}$ unramified implies that $D_{\mathfrak{q}/\mathfrak{p}} \cong \mathrm{Gal}(\ell/\kappa)$ is cyclic with generator $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$, and thus abelian. We can consider the cohomology groups $H^q(L/k, D_{\mathfrak{q}/\mathfrak{p}}) \cong H^q(L/k, \mathrm{Gal}(\ell/k))$.

2. The ring of integers $\mathcal{O}_L$ and its unit group $\mathcal{O}_L^*$ are Galois modules, with

$$H^0(L/k, \mathcal{O}_L) = \mathcal{O}_k,$$
$$H^0(L/k, \mathcal{O}_L^*) = \mathcal{O}_k^*.$$

   The action of G on $\mathcal{O}_L$ induces an action on its ideals, which in turn induces an action of G on $\mathrm{Cl}(\mathcal{O}_L)$. Thus, we can consider the cohomology of $\mathrm{Cl}(\mathcal{O}_L)$ as a Galois module. It turns out this is quite a rich subject in and of itself.

3. $(L, +)$ and $(L^*, \cdot)$ are naturally Galois modules, equipped with the action $\sigma \cdot \alpha = \sigma(\alpha)$. Additionally, we have

$$H^0(L/k, L) = k,$$
$$H^0(L/k, L^*) = k^*.$$

It turns out that $H^q(L/k, L)$ and $H^1(L/k, L^*)$ are quite nice as well. The exact statement of the latter fact is a cohomological formulation of a result known as Hilbert Theorem 90. This cohomological interpretation, which is often simply referred to as Hilbert 90, is the basis for many further results in Galois cohomology.

Theorem 5.3 (Hilbert 90)**.** *Let L/k be a finite seperable extension of fields. Then*

$$H^1(L/k, L^*) = 0.$$

Proof. Let $\sigma \mapsto \alpha_\sigma$ be a crossed homomorphism $G \to L^*$. That is, $\alpha_{\sigma\tau} = \alpha_\sigma \sigma(\alpha_\tau)$. For any $\gamma \in L$, consider the sum

$$\beta = \sum_{\tau \in G} \alpha_\tau \tau(\gamma).$$

By linear independence of automorphisms ([1], Section 14.2, Corollary 8), we can fix $\gamma \in L$ such that $\beta \neq 0$. Then for any $\sigma \in G$,

$$\sigma(\beta) = \sum_{\tau \in G} \alpha_\sigma^{-1} \alpha_{\sigma\tau} \sigma\tau(\gamma) = \alpha_\sigma^{-1}\beta.$$

This gives us $\alpha_\sigma = \beta/\sigma(\beta)$, which is the 1-coboundary condition for $a = \beta^{-1}$. We conclude that $\sigma \to \alpha_\sigma$ is in the image of δ^0, so that $H^1(L/k, L^*) = 0$. □

This result ends up being interesting in its own right when considering cyclic extensions. However, we will mostly consider it as a tool for studying other homology groups. Before moving forward, we must take a brief detour to define Galois cohomology of infinite Galois extensions.

Proposition 5.4. *Let H be a normal subgroup of G, and A a G-module. The inclusion $A^H \hookrightarrow A$ and projection $G \twoheadrightarrow G/H$ induce a map $H^q(G/H, A^H) \to H^q(G, A)$. We call this map the inflation map.*

Readers unfamiliar with the map are encouraged to construct it explicitly, and try to define the related notion of a *restriction map.*

Definition 5.5. Let L/k be an infinite Galois extension with Galois group $G = \mathrm{Gal}(L/k)$. For any G-module A, we define

$$H^q(L/k, A) = \varinjlim_{M} H^q(M/k, A^{\mathrm{Gal}(M/k)}),$$

where the limit is over all finite galois extensions M/k contained in L, and the maps are the inflation maps. We will sometimes write $A(M) = A^{\mathrm{Gal}(M/k)}$ as shorthand.[4]

Those who wish to brush up on limits are referred to Chapter 3 of [4]. We'll primarily concern ourselves with one special case.

[4] This is actually a proposition following from the general definition of cohomology of profinite groups. However, that is outside the scope of this paper. A brilliant coverage of the general case is present in chapter 4 of [2].

Definition 5.6. Let $\overline{k}$ be a seperable algebraic closure of k. We call $\Gamma_k = \text{Gal}(\overline{k}/k)$ the absolute Galois group of k. We often use the shorthand $H^q(k, A) = H^q(\Gamma_k, A)$.

Our shorthand is actually quite ambiguous, as one could imagine two seperable algebraic closures of k giving different cohomology groups. Fortunately, it's proven in Section 6.1 of [2] that any two closures give the same cohomology groups.[5]

As always, it's difficult to compute the cohomology of Γ_k in general. Fortunately for us, however, we've essentially computed one of its cohomology groups already.

Corollary 5.7.

$$H^1(k, \overline{k}^*) = 0.$$

Proof. This follows immediately from Hilbert 90. □

Now that we have an interesting group Γ_k to study, and an explicit computation to use, it's time to put our long exact sequences to use!

Theorem 5.8 (”Kummer Theory”)**.** *Let n be an integer such that k contains its n-th roots of unity, and take $\mu_n \subset \overline{k}^*$ to be the n-th roots of unity in $\overline{k}$. Then*

$$H^1(k, \mu_n) \cong k^*/k^{*n}.$$

Proof. Let $G = \Gamma_k$. Note that $\mu_n \subset k$ by supposition, so $\mu_n^G = \mu_n$. Since $\overline{k}$ is algebraically closed, we have that the map $-^n : \alpha \mapsto \alpha^n$ is surjective. μ_n is exactly the $\ker(-^n)$, so the sequence

$$\begin{tikzcd} 1 \arrow[r] & \mu_n \arrow[r] & \overline{k}^* \arrow[r, "-^n"] & \overline{k}^* \arrow[r] & 1 \end{tikzcd}$$

Is exact. We can finally make use of our original motivation for defining group cohomology, as we have the long exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mu_n^G \arrow[r] & (\overline{k}^*)^G \arrow[r, "-^n"] & (\overline{k}^*)^G \arrow[r] & H_1(k, \mu_n) \arrow[r] & H_1(k, \overline{k}^*) \arrow[r] & \cdots \end{tikzcd}$$

Some simple Galois theory and an application of Hilbert 90 gives us

$$\begin{tikzcd} 1 \arrow[r] & \mu_n \arrow[r] & k^* \arrow[r, "-^n"] & k^* \arrow[r] & H_1(k, \mu_n) \arrow[r] & 0 \end{tikzcd}$$

is exact. From this, we see that

$$H_1(k, \mu_n) \cong \frac{k^*}{k^{*n}}.$$

□

6 The Brauer Group

One homology group that comes up quite often in number theory is $H^2(k, \overline{k}^*)$. It comes up so often, that it gets its own special name![6] However, we haven't done much to characterize the second homology group, so we'll have to get a little more creative.

It turns out we can characterize $H^2(G, A)$ in general in relation to group extensions,[7] but this form isn't much easier to compute. We can at least do one computation with our current tools, though.

[5] This comes from the inclusions $i : k \to K$, $j : \overline{k} \to \overline{K}$ for an extension K/k and choice of closures $\overline{k}, \overline{K}$, as well as somewhat elementary facts which we've omitted for space.

[6] This is also because of its alternative characterization as the group of central simple algebras modulo certain relation, which are generalized quaternion algebras. [3] spends the entire fourth chapter discussing the Brauer group, including its central simple algebra interpretation.

[7] See [3], section 2.1 for details.

Proposition 6.1. *Let n be an integer such that k contains all n-th roots of unity. Then*

$$H^2(k, \mu_n) \cong (Br\ k)[n].$$

Proof. This proof is near identical to that of Kummer Theory. We once again have the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \overline{k}^* \xrightarrow{-^n} \overline{k}^* \longrightarrow 1,$$

to which we can associate a long exact sequence

$$\cdots \longrightarrow H^1(k, \overline{k}^*) \longrightarrow H^2(k, \mu_n) \longrightarrow H^2(k, \overline{k}^*) \xrightarrow{-^n} H^2(k, \overline{k}^*) \longrightarrow \cdots$$

Since $H^1(k, \overline{k}^*) = 0$, we have that

$$H^2(k, \mu_n) \cong \ker(-^n) \subset H^2(k, \overline{k}^*).$$

This is exactly the n-torsion in $H^2(k, \overline{k}^*) \cong \text{Br } k$, so we have

$$H^2(k, \mu_n) \cong (\text{Br } k)[n].$$

□

This result tells us that its at least tractable to find the n-torsion of Br k for some values of n. However, we still aren't much closer to understanding anything about the Brauer group in general. The reader will be disappointed to know it really isn't possible to understand much more about the Brauer group in general given our current tools.

However, we encourage the reader to study the computations and applications of the Brauer group further. A more thorough dive into the basics of the Brauer group (in both cohomological and classical definitions) can be found in IV of [3], while VII.7 and VII.8 of [3] give examples of much more advanced computations and applications respectively. Chapter 19 of [7] is another reference for basics, while Chapter 8 of [2] studies and computes the Brauer group exclusively in the context of a local field.

7 Conclusion

Unfortunately, it is simply impossible to cover group cohomology or its applications in the depth that it deserves, with such little space. The reader is encouraged to spend considerable time working with general group cohomology, like in part I of [2], before moving forward with many of the advanced topics mentioned. The theory is rich, and fluency will allow quick traversal through even richer applications. Those with extensive experience in algebra may prefer a terse text like [6] for this purpose. Personally, [3] had our favorite exposition.

References

[1] D.S. Dummit and R.M. Foote. *Abstract Algebra 2nd Ed.* Wiley India Pvt. Limited, 2008. ISBN: 978-8-126-51776-3.

[2] D. Harari. *Galois Cohomology and Class Field Theory.* Universitext. Springer-Verlag, 2017. ISBN: 978-3-030-43900-2.

[3] J.S. Milne. *Class Field Theory.* `https://https://jmilne.org/math/CourseNotes/cft.html`. [Online; accessed version 4.03 16-April-2025]. 2020.

[4] E. Riehl. *Category Thoery in Context.* Modern Math Originals. Dover, 2016. ISBN: 978-0-486-80903-8.

[5] J. Rotman. *An Introduction to Homological Algebra.* Universitext. Springer-Verlag, 2008. ISBN: 978-0-387-68324-9.

[6] J.P. Serre. *Galois Cohomology.* Monographs in Mathematics. Springer-Verlag, 2002. ISBN: 978-3-540-61990-1.

[7] W. Stein. *A Short Course on Galois Cohomology.* `https://wstein.org/edu/2010/582e/lectures/all/galois_cohomology.pdf`. [Online; accessed 16-April-2025]. 2010.