Group and Galois Cohomology: An introduction

Justin Scarfy

The University of British Columbia

October 05, 2015

Motivation

Introduction

Homological algebra originated from the nineteenth century in the works of Riemann (1857) and Betti (1857) on "homology numbers" in topology, went under rigorous developments by Poincaré, Noether, Leray, and was finally crystallized by the book of Cartan and Eilenberg to arbitrary algebraic systems. Group cohomology was classically studied long before the notation was formulated in 1943-45 in other guises, e.g., $H^0(G, A) = A^G, H_1(\pi, \mathbb{Z}) = G/[G, G]$, and Galois cohomology was coined by Hochschild for the group cohomology of the Galois group $G = \mathrm{Gal}(K/k)$ for a (possibly infinite) Galois extension K of k, where it is applied by Hochschild and Tate to class field theory.

Plan for this lecture

- Define group cohomology from two constructions: cochain complex and resolutions/functors, discuss change of the group.
- A first taste of Galois cohomology via Hilbert 90.

G-modules

Definition

Let G denote a multiplicatively written finite topological group with unit element 1_G, a G-**modules** A is an (additive written) abelian group A on which the group G acts in a way such that for all $\sigma, \tau \in G$, $a, b \in A$,

1. $1_G a = a$,
2. $\sigma(a + b) = \sigma a + \sigma b$,
3. $(\sigma\tau)a = \sigma(\tau(a))$.

The Group Ring

We can interpret G-modules as modules over the group ring

$$\mathbb{Z}[G] := \left\{ \sum\nolimits_{\sigma \in G} n_\sigma \sigma \mid n_\sigma \in \mathbb{Z} \right\},$$

containing the augmentation ideal and the ideal of norms of $\mathbb{Z}[G]$:

$$I_G := \left\{ \sum\nolimits_{\sigma \in G} n_\sigma \sigma \mid \sum\nolimits_{\sigma \in G} = 0 \right\}, \quad \mathbb{Z} \cdot N_G := \left\{ n \cdot \sum\nolimits_{\sigma \in G} \sigma \mid n \in \mathbb{Z} \right\}.$$

Group Cohomology via Cochain Complex (1/7)

The cohomology of a group G arises from the diagram

$$\cdots \rightrightarrows G \times G \times G \rightrightarrows G \times G \to G,$$

with the arrows being the projections

$$d_i : G^{n+1} \to G^n, \quad i = 0, 1, \ldots,$$
$$d_i(\sigma_0, \ldots, \sigma_n) = (\sigma_0, \ldots, \hat{\sigma}_i, \ldots, \sigma_n),$$

where $\hat{\sigma}_i$ indicates that the ith entry is omitted from the $(n+1)$-tuple, and G acts on G^n by left multiplication.

Assuming all G-modules A to be discrete from now on, we form the abelian group

$$X^n = X^n(G, A) = \mathrm{Map}(G^{n+1}, A)$$

of all continuous maps $x : G^{n+1} \to A$, i.e., of all continuous functions with values in A.

Group Cohomology via Cochain Complex (2/7)

G-homomorphims

X^n is in a natural way a G-module by

$$(\sigma x)(\sigma_0, \ldots, \sigma_n) = \sigma x(\sigma^{-1}\sigma_0, \ldots, \sigma^{-1}\sigma_n).$$

The maps $d_i : G^{n+1} \to G^n$ induce G-homomorphisms $d_i^* : X^{n-1} \to X^n$ and we form the alternating sum

$$\partial^n = \sum_{i=0}^{n} (-1) d_i^* : X^{n-1} \to X^n,$$

$$(\partial^n x)(\sigma_0, \ldots, \sigma_n) = \sum_{i=0}^{n} (-1)^i x(\sigma_0, \ldots, \hat{\sigma}_i, \ldots, \sigma_n).$$

Moreover, the G-homomorphism $\partial^0 : A \to X^0$, which associates each $a \in A$ the constant function $x(\sigma_0) = a$.

Group Cohomology via Cochain Complex (3/7)

Enters homological algebra

The sequence

$$0 \to A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \to \cdots \qquad (*)$$

is a cochain complex, i.e., $\partial^n \partial^{n-1} = 0$, and is exact as if we consider the homomorphisms of $\mathbb{Z}$-modules (NOT of G-modules):

$$D^{-1} : X^0 \to A, \qquad D^{-1}x = x(1_G)$$
$$D^n : X^{n+1} \to X^n, \quad (D^n x)(\sigma_0, \ldots, \sigma_n) = x(1_G, \sigma_0, \ldots, \sigma_n).$$

Calculation reveals that for $n \geq 0$,

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = \mathrm{id}\,. \qquad (**)$$

The exact sequence of G-modules $(*)$ called the **standard resolution** of A, and a family $(D^n)_{n \geq -1}$ with the property $(**)$ is called a **contracting homotopy** of it.

Group Cohomology via Cochain Complex (4/7)

Homogenous Cochain Complex

Now apply the functor "fixed module": for $n \geq 0$,

$$C^n(G, A) = X^n(G, A)^G,$$

i.e., $C^n(G, A)$ consists of the continuous functions $x : G^{n+1} \to A$ such that

$$x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)$$

for all $\sigma \in G$. These functions x are called the homogeneous n-**cochain** of G with coefficients in A. From the standard resolution $(*)$ we obtain a sequence

$$C^0(G, A) \xrightarrow{\partial^1} C^1(G, A) \xrightarrow{\partial^2} C^2(G, A) \to \cdots, \qquad (***)$$

which is in general NO LONGER exact, but nevertheless is still a complex, which is called the **homogeneous cochain complex** of G with coefficients in A.

Group Cohomology via Cochain Complex (5/7)

Homogeneous Cocycles, Coboundaries

We set

$$Z^n(G,A) := \ker(C^n(G,A) \xrightarrow{\partial^{n+1}} C^{n+1}(G,A)),$$
$$B^n(G,A) := \mathrm{im}(C^{n-1}(G,A) \xrightarrow{\partial^n} C^n(G,A),$$

and $B^0(G,A) := 0$. The elements of $Z^n(G,A)$ and $B^n(G,A)$ are called the **homogeneous n-cocycles** and n-**coboundaries**, where since $\partial^n \partial^{n-1} = 0$, we have $B^n(G,A) \subseteq Z^n(G,A)$ as subgroups.

The Cohomology Group

For $n \geq 0$, the factor group

$$H^n(G,A) := Z^n(G,A)/B^n(G,A)$$

is called the n-dimensional cohomology group of G with coefficients in A.

Group Cohomology via Cochain Complex (6/7)

For computational purposes and many applications, we modify definition of group cohomology by reducing the number of variables in the homogeneous cochains by one:

Inhomogeneous Cochains, Cocycles, Coboundaries

Let $\mathscr{C}^0(G,A) = A$ and for $n \geq 1$, $\mathscr{C}^n(G,A) := X^{n-1}(G,A)$ be the abelian group of all continuous functions $y : G^n \to A$; thus we have the isomorphism

$$C^0(G,A) \to \mathscr{C}^0(G,A), \quad x(\sigma) \mapsto x(1),$$

and for $n \geq 1$ the isomorphisms

$$C^n(G,A) \to \mathscr{G}^n(G,A),$$
$$x(\sigma_0,\ldots,\sigma_n) \mapsto y(\sigma_1,\ldots,x_n) = x(1,\sigma_1,\sigma_1\sigma_2,\ldots,\sigma_1\sigma_2\cdots\sigma_n),$$

whose inverses are given by

$$y(\sigma_1,\ldots,\sigma_n) \mapsto x(\sigma_0,\sigma_1,\ldots,\sigma_n) = \sigma_0 y(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2\ldots, y(\sigma_{n-1}^{-1}\sigma_n).$$

Group Cohomology via Cochain Complex (7/7)

With these isomorphisms the coboundary operators $\partial^{n+1} : C^n(G, A) \to C^{n+1}(G, A)$ are transformed into homomorphisms $\partial^{n+1} : \mathscr{C}^n(G, A) \to \mathscr{C}^{n+1}(G, A)$ given by (for $a \in \mathscr{C}^0(G, A), \mathscr{C}^1(G, A)$, and $\mathscr{C}^n(G, A)$, respectively):

$$
\begin{aligned}
(\partial^1 a)(\sigma) &= \sigma a - a, \\
(\partial^2 y)(\sigma, \tau) &= \sigma y(\tau) - y(\sigma\tau) + y(\sigma), \\
(\partial^{n+1} y)(\sigma_1, \ldots, \sigma_{n+1}) &= \sigma_1 y(\sigma_2, \ldots, \sigma_{n+1}) + \sum_{i=1}^{n} (-1)^i \times \\
&\quad \times y(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_2, \ldots, \sigma_{n+1}) + (-1)^{n+1} y(\sigma_1, \ldots, \sigma_n).
\end{aligned}
$$

Setting

$$
\begin{aligned}
\mathscr{Z}^n(G, A) &= \ker(\mathscr{C}^n(G, A) \xrightarrow{\partial^{n+1}} \mathscr{C}^{n+1}(G, A)) \\
\mathscr{B}^n(G, A) &= \operatorname{im}(\mathscr{C}^n(G, A) \xrightarrow{\partial^n} \mathscr{C}^n(G, A)),
\end{aligned}
$$

the isomorphism $C^n(G, A) \xrightarrow{\sim} \mathscr{C}^n(G, A)$ induces

$$H^n(G, A) \cong \mathscr{Z}^n(G, A)/\mathscr{B}^n(G, A).$$

Explicit Familiar (and Unfamiliar) Examples (1/3)

Having just defined group cohomology, we interpret $H^n(G, A)$ for $n = 0, 1, 2$ in (hopefully) familiar languages:

$H^0(G, A)$

We have a natural isomorphism $C^0(G, A) \to A$ given by $x \mapsto x(1_G)$. Thus, for $a \in A$, $(\partial^1 a)(\sigma_0, \sigma_1) = \sigma_0 a - \sigma_1 a$, so that

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

$H^1(G, A)$

A map $\varphi : G \to M$ is a **crossed homomorphism** if

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma), \quad \text{for all } \sigma, \tau \in G.$$

Thus, as $\varphi(1_G) = \varphi(1_G \cdot 1_G) = 1_G\varphi(1_G) + \varphi(1_G) = 2\varphi(1_G)$, we arrive at $\varphi(1_G) = 0$. For every $a \in A$, the map $\sigma \mapsto \sigma a - a$ is a crossed homomorphism, called a **principal crossed homomorphism**.

Explicit Familiar (and Unfamiliar) Examples (2/3)

[ctd] $H^1(G, A)$

By definition,

$$H^1(G, A) := \frac{\ker(\partial^{n+1})}{\mathrm{im}(\partial^n)} = \frac{\{\text{crossed homomorphisms } G \to A\}}{\{\text{principal crossed homomorphisms}\}}.$$

$H^2(G, A)$

The inhomogeneous 2-cocycles are the continuous functions $x : G \times G \to A$ such that $\partial^2 x = 0$, i.e.,

$$x(\sigma\tau, \rho) + x(\sigma, \tau) = x(\sigma, \tau\rho) + \sigma x(\tau, \rho),$$

and among those are the inhomogeneous 2-coboundaries

$$x(\sigma, \tau) = y(\sigma) - y(\sigma\tau) + \sigma y(\tau)$$

where y is an arbitrary 1-cochain $G \to A$.

Explicit Familiar (and Unfamiliar) Examples (3/3)

The 2-cocycles had been known long before the developments of group cohomology as **factor systems**, which occurred in connection with group extension: Assuming either A or G is finite, how many groups $\widehat{G}$ is there, which have the G-module A as a normal subgroup and G as the quotient group – consider all exact sequences

$$1 \to A \to \widehat{G} \to G \to 1$$

of topological groups (i.e., of profinite groups if A is finite, and of discrete groups if G is finite), such that the action of G on A is given by ${}^{\sigma}a = \widehat{\sigma} a \widehat{\sigma}^{-1}$, where $\widehat{\sigma} \in \widehat{G}$ is a pre-image of $\sigma \in G$. If there is another sequence with $\widehat{G}$ replaced by $\widehat{G}'$ in the above, such that there is a topological isomorphism $f : \widehat{G} \to \widehat{G}'$, we call these sequences equivalent, and denote the set of equivalence classes $[\widehat{G}']$ by $\mathrm{EXT}(G, A)$, which has a distinguished element given by the semi-direct product $\widehat{G} = A \rtimes G$.

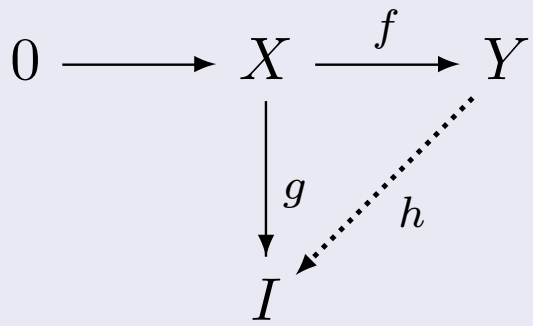
Theorem (Schereier) [NSW 1.2.4]

We have a canonical bijection of pointed sets $H^2(G, A) \cong \mathrm{EXT}(G, A)$.

Group Cohomology via Resolutions (1/3)

Injective G-modules

A G-module I is said to be **injective** if every G-homomorphism from a submodule of a G-module extends to the whole module, or, equivalently, if $\mathrm{Hom}_G(-, I)$ is an exact functor. Diagrammatically, if X and Y are G-modules and $f : X \to Y$ is a injective module homomorphism (hence X can be viewed as a submodule of Y) and $g : X \to I$ an arbitrary G-homomorphism, then there exists a G-homomorphism $h : Y \to I$ such that $hf = g$:



Fact: The category of G-modules, Mod_G has enough injectives, i.e., every G-module M can be embedded into an injective G-module, $M \hookrightarrow I$.

Group Cohomology via Resolutions (2/3)

For a G-module M, define

$$M^G := \{m \in M \mid gm \in m \text{ for all } g \in G\}.$$

The functor

$$\mathrm{Mod}_G \to \mathrm{Ab} \quad \text{given by} \quad M \mapsto M^G$$

is left exact, i.e., if

$$0 \to M' \to M \to M'' \to 0$$

is exact, then (the arrow coming into the sequence is preserved and hence)

$$0 \to M'^G \to M^G \to M''^G$$

is exact, and since Mod_G has enough injectives, we apply right derived functors and choose an injective resolution

Group Cohomology via Resolutions (3/3)

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} I^3 \to \cdots$$

of M. After applying the "fixed module" functor again, the complex

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} (I^3)^G \to \cdots$$

need no longer be exact.

We define the n-th cohomology group of G with coefficients in M to be

$$H^n(G, M) := \ker(d^r)/\mathrm{im}(d^{r-1}).$$

Note that we again recover $H^0(G, M) = M^G$, as

$$0 \to M^G \to (I^0)^G \xrightarrow{d^0} (I^1)^G$$

is exact, and $H^0(G, M) := \ker(d^0)/\mathrm{im}(d^{-1}) = \ker(d^0)$.

Group Homology (1/2)

For a G-module M, let M_G be the largest quotient of M on which G acts trivially: $M_G := M/\langle\{gm - m \,|\, g \in G, \quad m \in M\}\rangle$.

Projective Resolutions

Note that M_G is the dual notion to M^G, which is the largest subobject of M on which G acts trivially. The definition of the cohomology groups dualizes to give us homology groups: Let M be a G-module, and choose a projective resolution

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

of M. Applying the "largest quotient functor" to yield the complex

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0) \to 0$$

which no longer needs to be exact.

$$H_n(G, M) := \ker(d_n)/\operatorname{im}(d_{n+1}).$$

Group Homology (2/2)

$H_0(G, M)$

The zeroth homological group $H_0(G, M) = M_G$, as $(P_1)_G \to (P_0)_G \to M_G \to 0$ is exact.

$H_1(G, \mathbb{Z})$

Consider the exact augmentation sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

where $\mathbb{Z}[G]$ is a projective G module, i.e., $H_1(G, \mathbb{Z}[G]) = 0$, hence

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G \to \mathbb{Z} \to 0,$$

where the middle map is induced by the inclusion $I_G \hookrightarrow \mathbb{Z}[G]$, and so is zero. Thus the above sequence shows

$$H_1(G, \mathbb{Z}) \xrightarrow{\cong} I_G/I_G^2.$$

Combining this and the fact that there is an isomorphism $G^{\mathrm{ab}} := G/[G, G] \cong I_G/I_G^2$ yields the canonical isomorphism

$$H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}.$$

Change of the Group G (1/3)

Next we consider the question of what happens to the cohomology group $H^n(G, A)$ if we change the group G, and we only discuss three special cases of homomorphisms $H^n(G, A) \to H^n(G', A')$ with "compatible pairs" $G' \to G, A \to A'$, and an additional case:

Conjugation

Let $H \subseteq G$ be a *closed* subgroup, A a G-module, B an H-submodule of A. For $\sigma, \tau \in G$, we write $\tau^\sigma = \sigma^{-1}\tau\sigma$ and ${}^\sigma H = \sigma H \sigma^{-1}$, then the two compatible homomorphisms

$$ {}^\sigma H \to H, \tau \mapsto \tau^\sigma, \qquad B \to \sigma B, b \mapsto \sigma b $$

induce the **conjugation** homomorphisms

$$ \sigma_* : H^n(H, B) \to H^n({}^\sigma H, \sigma B), $$

and we have,

$$ 1_* = \mathrm{id} \quad \text{and} \quad (\sigma\tau)_* = \sigma_*\tau_*. $$

Change of the Group G (2/3)

Inflation and Restriction

Let $H \trianglelefteq G$ be a *normal closed* subgroup, then A^H is a G/H-module, and the projection and injection

$$G \to G/H, \qquad A^H \hookrightarrow A$$

form a compatible pair of homomorphisms, which induces the **inflation**

$$\inf_G^{G/H} : H^n(G/H, A^n) \to H^n(G, A).$$

homomorphism, which is transitive, i.e., for $H \subset F \trianglelefteq G$ normal closed,

$$\inf_G^{G/H} \circ \inf_{G/F}^{G/H} = \inf_G^{G/F}.$$

Let $H \subset G$ be a closed subgroup and A a G-module, consider the two homomorphisms

$$H \overset{\text{incl}}{\hookrightarrow} G, \qquad A \overset{\text{id}}{\longrightarrow} A.$$

We use cochains they induce the restriction maps to obtain the **restriction**

$$\text{res}_H^G : H^n(G, A) \to H^n(H, A)$$

homomorphisms, which is transitive, i.e., for $F \subset H \subset G$ closed,

$$\text{res}_F^H \circ \text{res}_H^G = \text{res}_F^G.$$

Change of the Group G (3/3)

Corestriction

If H is an *open* subgroups of G, then we have another map in the opposite direction of the restriction, it is a kind of norm map called the **corestriction**:

$$N_{G/H} : (X^n)^H \to (X^n)^G, \quad N_{G/H} :$$

Taking cohomology of these cochain complexes

$$\mathrm{cor}_G^H : H^n(H, A) \to H^n(G, A).$$

For $n = 0$, it is the usual **norm map**

$$N_{G/H} : A^H \to A^G, \qquad a \mapsto \sum_{g \in G/H} ga$$

For $F \subset H \leq G$ two open subgroups, the equation $N_{G/H} \circ N_{H/F} = N_{G/F}$ implies the transitivity

$$\mathrm{cor}_G^H \circ \mathrm{cor}_H^F = \mathrm{cor}_G^F .$$

Galois Cohomology (1/2)

Let L be a finite Galois extension of the field K, and let $G = \mathrm{Gal}(L/K)$, then both the additive and multiplicative groups of L are G-modules.

The additive group L^+ is cohomologically uninteresting, as

$$H^q(G, L^+) = 0 \quad \text{for all } q > 0.$$

Proof.

The above follows from the existence of a normal basis of L/K. If $c \in L$ is chosen in such a way that $\{\sigma c \,|\, \sigma \in G\}$ is a basis of L/K, then $L^+ = \bigoplus_{\sigma \in G} K^+ \cdot \sigma c = \bigoplus_{\sigma \in G} \sigma(K^+ \cdot c)$, which means that L^+ is a G-induced module, i.e., all of its cohomological groups are trivial. □

Generalization by Noether of Hilbert 90

$$H^1(G, L^\times) = 1.$$

Galois Cohomology (2/2)

Proof.

Let $a_0 \in L^\times$ be a 1-cocycle of the G-module $L^\times$. If $c \in L^\times$, consider $b = \sum_{\sigma \in G} a_\sigma \cdot \sigma c$. Since the automorphisms σ are linearly independent, there is an element $c \in L^\times$ such that $b \neq 0$. Therefore

$$\tau(b) = \sum_{\sigma \in G} \tau a_\sigma (\tau\sigma c) = \sum_{\sigma \in G} a_\tau^{-1} \cdot a_{\tau\sigma}(\tau\sigma c) = a_\tau^{-1} \cdot b,$$

i.e., $a_\tau = \tau(b^{-1})/b^{-1}$. Hence a_τ is a 1-coboundary. □

Corollary: Hilbert's 90

Let L/K be a cyclic extension, and let σ be a generator of G. If $x \in L^\times$ with $N_{L/K} x = 1$, then there is a $c \in L^\times$ such that

$$x = \frac{\sigma c}{c}.$$

Recap and Future topics

Review

Today we discussed

1. Definition of group cohomology via cochain complex.
2. Construction of group cohomology via resolutions.
3. H^0, H^1, H^2, H_0, H_1.
4. Conjugation, restriction, inflation, corestriction homomorphisms.
5. A first glimpse of Galois cohomology.

Future topics

1. Tate Cohomology and Tate's Theorem.
2. Local Class Field Theory.
3. Brauer Groups.
4. Global Class Field Theory.