UNIVERSITY OF CALGARY

The Galois Cohomology Funtime Hour

Using Galois Theory and Homological Algebra for Fun and Profit

Geoff Vooys

April 27, 2015

Definitions

Defintion

Let G be a group and let A be an Abelian group. We say that A is a left G-module if the following hold for all $g, h \in G$ and all $a, b \in A$:

1. $(gh)a = g(ha)$.
2. $g(a + b) = ga + gb$.
3. $1_G(a) = a$.
4. $g(0_A) = 0_A$.

Hi! I'm the Group Ring!

UNIVERSITY OF

Group Rings

Let R be a ring (possibly without identity and possibly noncommutative) and let G be a group (not necessarily finite). Then define x to be the formal sum

$$x := \sum_{g \in G} r_g g, r_g \in R$$

in which at most a finite number of the $r_g \neq 0$. Call $R[G]$ the collection of all such x. Then we define addition on $R[G]$ by the rule

$$\sum_{g \in G} r_g g + \sum_{g \in G} s_g g = \sum_{g \in G} (r_g + s_g) g$$

and multiplication based on the rule

$$(r_g g)(s_h h) := r_g s_h (gh).$$

We call $R[G]$ the Group Ring of R and G. When $R = \mathbb{Z}$, $\mathbb{Z}[G]$ is called the Integral Group Ring.

Group Ring Facts and $\mathbb{Z}[G]$-modules

UNIVERSITY OF CALGARY

Quick Group Ring Factoids

While the only group ring we will really care about is $\mathbb{Z}[G]$, there are two immediate properties of group rings that are illuminating. To see them, let R be a ring and let G be a group. Then the following hold:

1. $R[G]$ is unital if and only if R is unital.
2. $R[G]$ is commutative if and only if R is commutative and G is Abelian.

Fixing the G-module Terminology Problem

Let A be an Abelian group. Then A is a left G-module if and only if A is a left $\mathbb{Z}[G]$-module.

The proof is easy: either extend through linearity in each action of $g \in G$ on A or retract from $\mathbb{Z}[G]$ to G by applying the functor $\mathrm{Unit} : \mathbf{Ring} \to \mathbf{Grp}$. The group of units of $\mathbb{Z}[G]$ is exactly G, and so there is an induced action carried through the Unit functor (note that we should prove that the pair $(\mathbb{Z}[-], \mathrm{Unit}(-))$ is an adjoint pair of functors to really nail this down).

Two Important Rings

Remark/Definition

When we see the group ring $\mathbb{Z}[G]$, it is natural to try and find a map $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$. If we assert that ε is a morphism of unital rings, then the image of the map will be completely determined by considering the forms $1g$ for each $g \in G$. We must then send $g \mapsto 1$ for each $g \in G$. The map $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is thus the unique map that sends $g \to 1$ for all $g \in G$ and is called the Augmentation Map of $\mathbb{Z}[G]$.

Definition

The kernel of ε is called the Augmentation Ideal of $\mathbb{Z}[G]$ and is written as $I[G]$. This produces the short exact sequence of rings

$$0 \to I[G] \xrightarrow{\iota} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \xrightarrow{\pi} 0.$$

Digression, Part One: Abelian Categories

Definition

A category $\mathfrak{A}$ is said to be Abelian if the following hold:

1. $\mathfrak{A}$ has a zero object.
2. For any two objects $A, B \in \mathrm{ob}(\mathfrak{A})$, $\mathrm{Hom}_{\mathfrak{A}}(A, B)$ is an Abelian group.
3. $\mathfrak{A}$ has all kernels and cokernels.
4. Every monomorphism is the kernel of its cokernel and every epimorphism is the cokernel to its kernel (i.e. every monomorphism is normal and every epimorphism is conormal).

Example

Let R be a ring (possibly without identity, possibly without commutativity). Then the category of all left R-modules A with morphisms R-linear maps is an Abelian category.

Topological G Modules

Theorem

Let G be a profinite group and let $\mathfrak{D}_G$ denote the class of discrete G-modules A for which G acts on A continuously. Then $\mathfrak{D}_G$ is an Abelian category.

An Alternate Characterization

Saying that a G-module $A \in \mathrm{ob}\left(\mathfrak{D}_G\right)$ amounts to saying that the stabilizer of each $a \in A$ is again open in G. Equivalently, we have that for all $U \subseteq G$ open subgroups and for $A^U := \{a \in A | ua = a, \forall u \in U\}$,

$$A = \varinjlim A^U = \bigcup A^U.$$

Proof of $\mathfrak{D}_G$ as an Abelian Category

Proof

Observe that if we can show that $\mathfrak{D}_G$ is a full subcategory of **G-Mod**, where **G-Mod** is the category of left G-modules, we will be done. As such, note that there is certainly a faithful embedding $\iota : \mathfrak{D}_G \to \mathbf{G\text{-}Mod}$ of categories given by $\iota(A) = A$ and $\iota(\varphi) = \varphi$ for every object A and every morphism φ of $\mathfrak{D}_G$. This allows us to treat $\mathfrak{D}_G$ as a subcategory of **G-Mod**; to see that it is a full subcategory of **G-Mod**, we will show that any map $\varphi : A \to B$ satisfies $\varphi \in \mathrm{Hom}_{\mathfrak{D}_G}(A, B)$. To do this consider that $A = \varinjlim A^H$ and $B = \varinjlim B^H$. Thusly we may consider the commutative diagram

$$\begin{tikzcd}
A^{H_1} \arrow[rrr, dashed, "res_\varphi(A^{H_1})"] \arrow[dd] \arrow[dr] & & & B^{H_1} \arrow[dl] \arrow[dd] \\
& \varinjlim A^H \arrow[r, "\varphi"] & \varinjlim B^H & \\
A^{H_2} \arrow[rrr, dashed, "res_\varphi(A^{H_2})"'] \arrow[ur] & & & B^{H_2} \arrow[ul]
\end{tikzcd}$$

Digression, Part Two: Chain Complexes

UNIVERSITY OF CALGARY

Definition

Let $\mathfrak{A}$ be an Abelian category and let $A_\bullet = (A_n, \partial_n)$ be a collection of objects A_n of $\mathfrak{A}$ such that each ∂_n is a morphism $\partial_n : A_n \to A_{n+1}$. We say that $A_\bullet$ is a cochain complex in $\mathfrak{A}$ if $\partial_n \partial_{n+1} = 0$ for all $n \in \mathbb{Z}$. Chain complexes are defined analogously.

Definition

A map $(\varphi_n) =: \varphi_\bullet : A_\bullet \to B_\bullet$ is said to be a homomorphism of cochain complexes if for every $n \in \mathbb{Z}$ the square

$$\begin{tikzcd} A_n \arrow[r, "\partial_n"'] \arrow[d, "\varphi_n"] & A_{n+1} \arrow[d, "\varphi_{n+1}"] \\ B_n \arrow[r, "\delta_n"'] & B_{n+1} \end{tikzcd}$$

commutes in $\mathfrak{A}$. Homomorphisms of chain complexes are defined similarly.

Digression, Part Three: (Short) Exact Sequences

Definition

Let $\mathfrak{C}$ be a category and let $A_\bullet := (A_n, \partial_n : A_n \to A_{n-1})$ a sequence of objects in $\mathfrak{C}$ (note that this says that $\partial_n \partial_{n+1} = 0$ for every $n \in \mathbb{Z}$). Then we say that the sequence

$$\cdots \longrightarrow A_{n+1} \xrightarrow[\partial_{n+1}]{} A_n \xrightarrow[\partial_n]{} A_{n-1} \longrightarrow \cdots$$

is exact at n if $\ker \partial_n = \operatorname{im} \partial_{n+1}$. If $A_\bullet$ is exact at every $n \in \mathbb{Z}$ then we say that $A_\bullet$ is an exact sequence in $\mathfrak{C}$. If $\mathfrak{C}$ is a category with a zero object 0 and only a finite number of objects in $A_\bullet$ are nonzero, then $A_\bullet$ is a short exact sequence.

Digression, Part Four: (Co)Homology

Definition

Let $\mathfrak{A}$ be an Abelian category, let $A_\bullet = (A_n, \partial_n)$ be a chain complex in $\mathfrak{A}$, and let $C^\bullet = (C^n, \delta_n)$ be a cochain complex in $\mathfrak{A}$. Then the n-th homology group of $A_\bullet$ is defined as the group

$$H_n(A_\bullet) := \frac{\ker \partial_n}{\operatorname{im} \partial_{n+1}};$$

similarly the n-th cohomology group of $C^\bullet$ is defined as the group

$$H^n(C^\bullet) := \frac{\ker \delta_n}{\operatorname{im} \delta_{n-1}}.$$

Definition

Let $A_\bullet = (A_n, \partial_n)$ be a chain complex over any small Abelian category $\mathfrak{A}$. Then any element $\sigma \in \ker \partial_n$ is called an n-cycle, and $\ker \partial_n = Z_n(A_\bullet)$; similarly, any element $\tau \in \operatorname{im} \partial_{n+1}$ is called an n-boundary and $\operatorname{im} \partial_{n+1} =: B_n(A_\bullet)$. In the case that $C^\bullet = (C^n, \delta_n)$ is a cochain complex in $\mathfrak{A}$, then we write $\ker \delta_n = Z^n(C^\bullet)$ and $\operatorname{im} \delta_{n-1} = B^n(C^\bullet)$. Each $\sigma \in Z^n$ is an n-cocycle in $C^\bullet$ while $\tau \in B^n$ is called an n-coboundary in $C^\bullet$.

Examples of (Co)Homology

Example

Let $\mathfrak{A} = \mathbf{Ab}$ be the category of Abelian groups and let $A_\bullet = 0 \to m\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$ be a short exact sequence in $\mathbf{Ab}$. Then we each homology group of $A_\bullet$ is trivial by the exactness of the sequence.

Example

Consider the sequence $A_\bullet$ of Abelian groups

$$0 \xrightarrow[\partial_3]{} \mathbb{Z} \xrightarrow[\partial_2]{4} \mathbb{Z} \xrightarrow[\partial_1]{} \frac{\mathbb{Z}}{2\mathbb{Z}} \xrightarrow[\partial_0]{} 0.$$

Then $H_3(A_\bullet) = 0$, $H_2(A_\bullet) = \ker \partial_2 / \operatorname{im} \partial_3 = 0$, $H_1(A_\bullet) = \ker \partial_1 / \operatorname{im} \partial_0 = 2\mathbb{Z}/4\mathbb{Z}$, $H_0(A_\bullet) = 0$. This shows that $H_n(A_\bullet)$ is not always trivial.

Example

Let $A_\bullet$ be the sequence defined above and define $C^\bullet = (C^n, \delta_n)$ by setting $C^n := A_{-n}$ and $\delta_n := \partial_{-n}$. Then the cohmology $H^*(C^\bullet)$ is nontrivial by the above example.

The Long Exact Cohomology Sequence

Theroem

Let $\mathfrak{A}$ be an Abelian category and let $A^\bullet$, $B^\bullet$, and $C^\bullet$ be cochain complexes in $\mathfrak{A}$ such the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_n \arrow[r, "\varphi_n"] \arrow[d, "\alpha_n"'] & B_n \arrow[r, "\psi_n"] \arrow[d, "\beta_n"'] & C_n \arrow[r] \arrow[d, "\gamma_n"'] & 0 \\
0 \arrow[r] & A_{n+1} \arrow[r, "\varphi_{n+1}"] & B_{n+1} \arrow[r, "\psi_{n+1}"] & C_{n+1} \arrow[r] & 0
\end{tikzcd}$$

commutes in $\mathfrak{A}$ for each $n \in \mathbb{N}$ with each row exact. Then there is a long exact sequence in $\mathfrak{A}$ given by

$$\begin{tikzcd}
0 \arrow[r] & H^0(A^\bullet) \arrow[r] & H^0(B^\bullet) \arrow[r] & H^0(C^\bullet) \arrow[r, "\delta_0"] & H^1(C^\bullet) \arrow[dllll] & \\
\cdots \arrow[r] & H^n(A^\bullet) \arrow[r] & H^n(B^\bullet) \arrow[r] & H^n(C^\bullet) \arrow[r, "\delta_n"] & \cdots &
\end{tikzcd}$$

with each δ_k given by the Snake Lemma.

A New Fix Functor

Definition

Let G be a profinite group and A a discrete G-module. Then define the functor

$$\mathrm{Fix}(A) : \mathfrak{D}_G \to \mathfrak{D}_G$$

by sending $A \mapsto A^G := \{a \in A \mid ga = a, \forall\, g \in G\}$ and adapting the maps $\varphi : A \to B$ apporopriately. Then $\mathrm{Fix}(-)$ is a covariant endofunctor.

Example

Let K be a field with L/K a Galois extension of fields. Then L and $\mathrm{Unit}(L)$ are continuous $\mathrm{Gal}(L/K)$-modules. Furthermore

$$\mathrm{Fix}(L) = L^{\mathrm{Gal}(L/K)} = K$$

and

$$\mathrm{Fix}(\mathrm{Unit}(L)) = \mathrm{Unit}(L)^{\mathrm{Gal}(L/K)} = \mathrm{Unit}(K).$$

Digression, Part Six: Cochains Over $\mathrm{Gal}(L/K)$

UNIVERSITY OF CALGARY

Definition

Let $G = \mathrm{Gal}(L/K)$ and let A be a discrete G-module. Then define $C^n(G, A) := \{\varphi : G^n \to A \mid \varphi \text{ continuous}\}$ (by A discrete and G profinite, continuous simply means locally constant) and define the coboundary map

$$\partial_n : C^n(G, A) \to C^{n+1}(G, A)$$

by

$$\begin{aligned}(\partial_n(f))(\sigma_1, \cdots, \sigma_{n+1}) := \quad & \sigma_1 f(\sigma_2, \cdots, \sigma_{n+1}) + (-1)^{n+1} f(\sigma_1, \cdots, \sigma_n) \\ & + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \cdots, \sigma_i \sigma_{i+1}, \cdots, \sigma_{n+1}).\end{aligned}$$

A Question of Fix and Cohomology

Question

Does the Fix : **G-Mod** $\to$ **G-Mod** functor take exact sequences to exact sequences, i.e., is Fix both left and right exact? To answer this question we need one quick digression to Hilbert 90.

Notation/Definition

Let A be a $\mathrm{Gal}(L/K)$-module for L/K a Galois extension of fields. Then we define the n-th cohomology group of $\mathrm{Gal}(L/K)$ witt coefficients in A to be

$$H^n(G,A) := \frac{Z^n(C^n(G,A))}{B^n(C^n(G,A))}.$$

This definition is equivalent to the derived functorial interpretation with $H^n(G,A) := \mathrm{Ext}^n_G(A) = \mathrm{Ext}^n(\mathbb{Z}[G],A)$. We likely will not have time to properly go into the Ext functor, and so it is deferred as an optional topic, but it is the correct way to see what we are doing and is consistent with our Z^n/B^n definition. Note that

$$\mathrm{Fix}(A) = A^G = \mathrm{Hom}_{\mathbf{G\text{-}Mod}}(\mathbb{Z},A) = H^0(G,A).$$

Hilbert 90 (Modern Cohomological Perspective)

UNIVERSITY OF CALGARY

Theorem (Hilbert 90)

Let K be a field. Then $H^1(\mathrm{Gal}(L/K), \mathrm{Unit}(L)) = 0$ for any Galois L/K.

Remarks

Our strategy towards proving the theorem will be to show that every 1-cocycle (derivation) f of $\mathrm{Gal}(L/K)$ into $\mathrm{Unit}(L)$, which looks like (in additive notation)

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau); \sigma, \tau \in \mathrm{Gal}(L/K)$$

actually is a 1-coboundary (an inner derivation) and hence takes the form, for some $\ell \in \mathrm{Unit}(L)$,

$$f(\sigma) = \sigma(\ell) - \ell; \sigma \in \mathrm{Gal}(L/K).$$

Proof of Hilbert 90

Proof

We prove the theorem by first proving it for Galf extensions of K. Begin by letting N/K be a Galf extension with $G_N := \mathrm{Gal}(N/K)$. Then let $\varphi \in Z_1(G_N, \mathrm{Unit}(N))$ so that $\varphi(\sigma\tau) = \varphi(\sigma)\sigma(\varphi(\tau))$. Now define the linear map $T : N \to N$ given by

$$u \mapsto \sum_{\sigma \in G_N} \varphi(\sigma)\sigma(u).$$

T is evidently nonzero by the Normal Basis Theorem, and so for any nonzero $b \in \operatorname{im} T$ we have that there is a $u \in \mathrm{Unit}(N)$ such that

$$b = \sum_{\sigma \in G_n} \varphi(\sigma)\sigma(u),$$

which tells us that taking τ of both sides of the equation, for some $\tau \in G_N$, gives

$$\tau(b) = \sum_{\sigma \in G_N} \tau\left(\varphi(\sigma)\sigma(u)\right) = \sum_{\sigma \in G_N} \frac{\varphi(\tau\sigma)}{\varphi(\tau)}\tau\sigma(u).$$

Proof of Hilbert 90, Cont.

Because $\tau(b) = \sum_{\sigma \in G_N} \varphi(\tau\sigma)\tau\sigma(u)/\varphi(\tau)$, it follows from multiplication in $\mathrm{Unit}(N)$ that

$$\tau(b)\varphi(\tau) = \sum_{\sigma \in G_N} \varphi(\tau\sigma)\tau\sigma(u) = b \implies \varphi(\tau) = \frac{b}{\tau(b)} = \frac{\tau(b^{-1})}{b^{-1}}.$$

Thusly $Z_1(G_N, \mathrm{Unit}(N)) = B_1(G_N, \mathrm{Unit}(N))$ and hence $H^1(G_N, \mathrm{Unit}(N)) = 0$. Taking the direct limit now yields that

$$H^1(\mathrm{Gal}(L/K), \mathrm{Unit}(L)) = \varinjlim H^1(\mathrm{Gal}(N/K), \mathrm{Unit}(N)) = \varinjlim 0 = 0,$$

and so we are done. We will prove the validity of taking the direct limit later on. $\square$

Answering the Question on Exactness of Fix

Proposition

The endofunctor $\mathrm{Fix} : \mathfrak{D}_G \to \mathfrak{D}_G$ is not right exact. In particular, if n is an integer prime to the characteristic of the base field K, then
$H^1(\mathrm{Gal}(K_s/K), \mu_n) = \mathrm{Unit}(K)/\,\mathrm{Unit}(K)^n$, where μ_n is the group of n-th roots of unity in K_s and K_s is the separable closure of K.

Proof

Let K be a field and let $n : \mathrm{Unit}(K) \to \mathrm{Unit}(K)$ be the endomorphism $x \mapsto x^n$. Then there is a short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \mathrm{Unit}(K_s) \xrightarrow{n} \mathrm{Unit}(K_s) \longrightarrow 1$$

of $\mathrm{Gal}(K_s/K)$ modules. Now, taking cohomology gives the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Fix}(\mu_n) \arrow[r] & \mathrm{Unit}(K) \arrow[r, "H^1(n)"] & \mathrm{Unit}(K) \arrow[dl] \\ & & H^1(\mathrm{Gal}(K_s, K), \mu_n) \arrow[r] & H^1(\mathrm{Gal}(K_s/K), \mathrm{Unit}(K_s)) \end{tikzcd}$$

Proof, Cont

The cohomology exact sequence (the right derived functor of Fix exact sequence) is then equivalent to the short exact sequence

$$0 \longrightarrow \mu_n \longrightarrow \mathrm{Unit}(K) \overset{n}{\twoheadrightarrow} \mathrm{Unit}(K)^n \longrightarrow H^1(\mathrm{Gal}(K_s/K), \mu_n) \longrightarrow 0$$

in **Ab**. Thusly $H^1(\mathrm{Gal}(K_s/K), \mu_n)$ is the cokernel to the map n, and hence an application of the first isomorphism theorem completes the proof. $\square$

An Introduction to Derived Functors, Part One

Definition

Let $\mathfrak{A}$ and $\mathfrak{B}$ be Abelian categories with a covariant functor $F : \mathfrak{A} \to \mathfrak{B}$. Then we say that T is an additive functor if either of the equivalent conditions hold:

1. F takes zero objects to zero objects.
2. The map $\mathrm{Hom}_{\mathfrak{A}}(A, B) \to \mathrm{Hom}_{\mathfrak{B}}(F(A), F(B))$ is a homomorphism of Abelian groups.

Definition

Let $\mathfrak{A}$ be an Abelian category and let $T : \mathfrak{A} \to \mathbf{Ab}$ be an additive functor. Let A be an object of $\mathfrak{A}$ and let $I_\bullet$ be an injective resolution of A such that the sequence

$$A \to I_0 \to I_1 \to \cdots \to I_n \to \cdots$$

forms a cochain complex in $\mathfrak{A}$ with $H^0(I_0) = T(A)$. Then the Right Derived Functors of T are defined by taking the cohomology cocomplex $H^*(T(I_\bullet))$ and defining the n-th Right Derived Functor of T as

$$R^nT := H^n(T(I_\bullet)).$$

An Introduction to Derived Functors, Part Two

UNIVERSITY OF CALGARY

Definition

Let $T : \mathbf{A} \to \mathbf{Ab}$ be an additive covariant functor and let $0 \to A \to B \to C \to 0$ be a short exact sequence. Then T is said to be left exact if the sequence

$$0 \to T(A) \to T(B) \to T(C)$$

is exact in $\mathbf{Ab}$.

Example

The functor $\mathrm{Fix} : \mathfrak{D}_G \to \mathfrak{D}_G$ is a left exact functor.

A Functorial Interpretation of Galois Cohomology and a Gap-Filling Theorem

UNIVERSITY OF CALGARY

Remark

Let K be a field and let L/K be a Galois extension with $G := \mathrm{Gal}(L/K)$. Then the Galois cohomology groups $A \mapsto H^n(G, A)$ are the right derived functors of the additive functor $\mathrm{Fix}(-)$.

Theorem

Let (G_i) be a projective (inverse) system of profinite groups and let (A_i) be a directed system of (discrete) G_i-modules such that the homomorphisms $A_i \to A_j$ are compatible with the maps $G_i \to G_j$. Set $A = \varinjlim A_j$ and $G = \varprojlim G_i$. Then we have for every $m \in \mathbb{N}$

$$H^m(G, A) = \varinjlim H^m(G_i, A_i).$$

Proof of the Gap-Filling Theorem

Proof

Let (G_i), (A_i), A, and G be given as in the statement of the theorem and consider for each $n \in \mathbb{N}$ the commutative square

$$\begin{tikzcd} C^n(G,A) \arrow[r, "\partial_n"] & C^{n+1}(G,A) \\ \varinjlim C^n(G_i,A_i) \arrow[u, "\varphi_n"'] \arrow[r, "\partial_{n,i}"'] & \varinjlim C^{n+1}(G_i,A_i) \arrow[u, "\varphi_{n+1}"] \end{tikzcd}$$

where the $\varphi_n : \varinjlim C^n(G_i, A_i) \to C^n(G, A)$ are the canonical homomorphisms given by the universal property of the direct limit. We note that through $G = \varprojlim G_i$ and $A = \varinjlim A_i$ it follows that the maps φ_n must each have $\ker \varphi_n = 0 = \operatorname{coker} \varphi_n$, showing that in $\mathfrak{D}_G$ there is an isomorphism of cochain complexes $C^\bullet(G, A) \cong \varinjlim C^\bullet(G_i, A_i)$. From here passing through the cohomology functor completes the proof of the theorem.

Right Derived Functors and Ext: Part One

Motivation and Definitions

Let R be a ring of unity and let A and B be left R-modules. We are interested in finding all left R-modules M such that B is a submodule of M with $A \cong M/B$, inducing a short exact sequence

$$0 \longrightarrow B \longrightarrow M \longrightarrow A \longrightarrow 0$$

in **R-Mod**. Such a sequence is called an extension of A by B. We say that two extensions $B \to M \to A$ and $B \to N \to A$ are equivalent if there is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & B \arrow[r] \arrow[d, equal] & M \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & B \arrow[r] & N \arrow[r] & A \arrow[r] & 0 \end{tikzcd}$$

in **R-Mod**. Note that the Five Lemma says that the map $M \to N$ is an isomorphism of R-modules.

Right Derived Functors and Ext: Part Two

UNIVERSITY OF

Definition

Let $E(A,B)$ denote the set of equivalence classes of extensions of A by B (it is nonempty always because $A \oplus B$ does the job).

Definition: Ext

Let R be a unital ring and let $0 \to C \xrightarrow{\iota} P \xrightarrow{\pi} A \to 0$ be a projective presentation of A in $\mathbf{R}\text{-}\mathbf{Mod}$ with A, P, C all left R-modules and P projective. Then there is, for any right R-module B, a short exact sequence of the form

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathbf{R}\text{-}\mathbf{Mod}}(A,B) \arrow[r, "\pi^*"] & \mathrm{Hom}_{\mathbf{R}\text{-}\mathbf{Mod}}(P,B) \arrow[d, "\iota^*"] & \\ & & \mathrm{Hom}_{\mathbf{R}\text{-}\mathbf{Mod}}(C,B) \arrow[r] & 0 \end{tikzcd}$$

in $\mathbf{R}\text{-}\mathbf{Mod}$. Then we define $\mathrm{Ext}_R^{\pi}(A,B)$ as

$$\mathrm{Ext}_R^{\pi}(A,B) := \mathrm{coker}\left(\iota^* : \mathrm{Hom}_{\mathbf{R}\text{-}\mathbf{Mod}}(P,B) \to \mathrm{Hom}_{\mathbf{R}\text{-}\mathbf{Mod}}(C,B)\right).$$

Ext: A Description of Elements and A Problem with π

Elements in $\mathrm{Ext}^{\pi}_{R}(A, B)$

An element of $\mathrm{Ext}^{\pi}_{R}(A, B)$ may be represented by a homomorphism $\varphi : C \to B$, which we will write as $[\varphi] \in \mathrm{Ext}^{\pi}_{R}(A, B)$. Two elements satisfy the equality $[\varphi_1] = [\varphi_2]$ if and only if the map $\varphi_1 - \varphi_2$ may be extended to P.

A Natural Question

Let $0 \to C_1 \xrightarrow{\iota_1} P_1 \xrightarrow{\pi_1} A_1 \to 0$ and $0 \to C_2 \xrightarrow{\iota_2} P_2 \xrightarrow{\pi_2} A_2 \to 0$ be projective resolutions of A_1 and A_2, respectively. Then if there is a $\varphi \in \mathrm{Hom}_{\mathbf{R\text{-}Mod}}(A_2, A_1)$, there is a map $\pi : P_2 \to P_1$, by the projectivity of P_2, inducing a map $\gamma : C_2 \to C_1$ such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & C_2 \arrow[r, "\iota_2"] \arrow[d, "\gamma"'] & P_2 \arrow[r, "\pi_2"] \arrow[d, "\pi"'] & A_2 \arrow[r] \arrow[d, "\varphi"'] & 0 \\
0 \arrow[r] & C_1 \arrow[r, "\iota_1"'] & P_1 \arrow[r, "\pi_1"'] & A_1 \arrow[r] & 0
\end{tikzcd}$$

commutes in **R-Mod**. Now, the map π, together with γ, induces a natural transformation of the functors $\mathrm{Ext}^{\pi_1}_{R}(A_1, -) \to \mathrm{Ext}^{\pi_2}_{R}(A_2, -)$.

Answering A Natural Question

Proposition

The natural transformation $\pi^* : \mathrm{Ext}_R^{\pi_1}(A_1, -) \to \mathrm{Ext}_R^{\pi_2}(A_2, -)$ depends only on the homomorphism $\varphi : A_2 \to A_1$.

Proof

Let $\pi_i, \pi_j : P_2 \to P_1$ be two homomorphisms inducing maps $\gamma_i, \gamma_j : C_2 \to C_1$ such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & C_2 \arrow[r, "\iota_2"] \arrow[d, "\gamma_i"'] & P_2 \arrow[r, "\pi_2"] \arrow[d, "\pi_i"'] & A_2 \arrow[r] \arrow[d, "\varphi"'] & 0 \\
0 \arrow[r] & C_1 \arrow[r, "\iota_1"'] & P_1 \arrow[r, "\pi_1"'] & A_1 \arrow[r] & 0
\end{tikzcd}$$

commutes in **R-Mod** for i and j. Consider now the function $\pi_i - \pi_j$. Because both π_i and π_j lift the same φ, it follows that $\pi_i - \pi_j$ factors through a map $\alpha : P_2 \to C_1$ such that $\pi_i - \pi_j = \iota_1 \alpha$ and $\gamma_i - \gamma_j = \alpha \iota_2$.

Finishing the Proof

So, setting $\beta : C_1 \to B$ as a representative for $[\beta] \in \mathrm{Ext}_R^{\pi_1}(A_1, B)$ we find that

$$\pi_i^*[\beta] = [\beta\gamma_i] = [\beta\gamma_j + \beta\alpha\iota_2] = [\beta\gamma_j] = \pi_j^*[\beta].$$

This proves the proposition. $\square$

Ext as a Functor, Explicitly

By the above proposition, it follows that $\mathrm{Ext}_R^{\pi}(A, -) \cong \mathrm{Ext}_R^{\theta}(A, -)$ for any lifts π and θ; as such, we simply write $\mathrm{Ext}_R(A, -)$ from here on out. In order to make $\mathrm{Ext}_R(-, B) : \mathbf{R\text{-}Mod} \to \mathbf{Ab}$ into a (contravariant) functor, we define the induced map of a homomorphism $\varphi : A \to C$ by choosing projecting presentaitons and setting φ^* to be the natural transformation between the resulting Ext groups. This allows us to turn Ext into a bifunctor from the product category $\mathbf{R\text{-}Mod} \prod \mathbf{R\text{-}Mod} \to \mathbf{Ab}$, contravariant in the first variable and covariant in the second.

Ext and Derived Functors: Part Three

Remarks and a Definition

The contravariant functor $\mathrm{Hom}_{\mathbf{R\text{-}Mod}}(-, B)$ is a left exact additive functor. As such we can define the right derived functors of $\mathrm{Hom}_{\mathbf{R\text{-}Mod}}(-, B)$ for any fixed R-module$B$. In fact, this is how we will arrive at the Ext_R^n functors. Explicitly, we define Ext_R^n as

$$\mathrm{Ext}_R^n(-, B) := R^n\left(\mathrm{Hom}_{\mathbf{R\text{-}Mod}}(-, B)\right).$$

Lemma

Let $K_n \xrightarrow{\mu} P_{n-1} \to \cdots \to P_0 \to A$ be an exact sequence with μ monic and the map to A epic in $\mathbf{R}$-$\mathbf{Mod}$ and each P_i projective. Then if T is a left exact contravariant functor $T : \mathbf{R}\text{-}\mathbf{Mod} \to \mathbf{Ab}$ the sequence

$$T(P_n) \xrightarrow{\mu^*} T(K_n) \longrightarrow R^nT(A) \longrightarrow 0$$

is exact.

Proof of Lemma

Proof of Lemma

Define the complex $P := (P_{n+k}, \delta_{n+k})_{k\in\mathbb{N}}$ such that the sequence $\cdots \to P_{n+1} \to P_n \to K_n \to 0$ is exact with each P_{n+k} projective over R. Then we induce the complex

$$\begin{tikzcd}
\cdots \arrow[r] & P_{n+1} \arrow[r, "\partial_{n+1}"] & P_n \arrow[rr, "\partial_n"] \arrow[dr] & & P_{n-1} \arrow[r] & \cdots \arrow[r] & P_0 \arrow[r] & 0 \\
& & & K_n \arrow[ur, "\mu"'] & & & &
\end{tikzcd}$$

as a projective resolution of A. Because T is left exact, we deduce the diagram, with top row exact,

$$\begin{tikzcd}
& T(P_{n-1}) \arrow[r, "\mu^*"] \arrow[d] & T(K_n) \arrow[r] \arrow[d] & T(P_n) \arrow[r] \arrow[d, "T(\partial_{n+1})"] & 0 \\
0 \arrow[r] & 0 \arrow[r] & T(P_{n+1}) \arrow[r, "\simeq"] & T(P_{n+1}) &
\end{tikzcd}$$

The End of Lemma and a Proposition on Ext

Through the diagram

$$\begin{tikzcd}
 & T(P_{n-1}) \arrow[r, "\mu^*"] \arrow[d] & T(K_n) \arrow[r] \arrow[d] & T(P_n) \arrow[r] \arrow[d, "T(\partial_{n+1})"] & 0 \\
0 \arrow[r] & 0 \arrow[r] & T(P_{n+1}) \arrow[r, "\simeq"] & T(P_{n+1}) &
\end{tikzcd}$$

and the top row being exact, it then follows that

$$\operatorname{coker}(\mu^*) = \ker T(\partial_{n+1}) / \operatorname{im} T(\partial_n) = R^n T(A),$$

whence the lemma. $\square$

Proposition

$$\operatorname{Ext}^1_R(A, B) \cong \operatorname{Ext}_R(A, B)$$

Proof of Proposition

UNIVERSITY OF CALGARY

Proof

Let $0 \to C_1 \xrightarrow{\mu} P_0 \xrightarrow{\pi} A \to 0$ be a projective presentation of A. Then by the lemma we obtain the exact sequence

$$\mathrm{Hom}_{\mathbf{R\text{-}Mod}}(P_0, B) \longrightarrow \mathrm{Hom}_{\mathbf{R\text{-}Mod}}(C_1, B) \longrightarrow \mathrm{Ext}^1_R(A, B) \longrightarrow 0.$$

It then follows by definition of $\mathrm{Ext}_R(A, B)$ that $\mathrm{Ext}^1_R(A, B) \cong \mathrm{Ext}_R(A, B)$. $\square$

Leading up to Understanding $H^2(\mathrm{Gal}(K_s/K), K_s)$

UNIVERSITY OF CALGARY

Interpreting H^2

Let L/K be a Galois extension of fields and let A be an object in $\mathfrak{D}_{\mathrm{Gal}(L/K)}$. Then we can think of $H^2(\mathrm{Gal}(L/K), A)$ as the group of classes of continuous factor systems of G to A.

Group Extensions

Let $A \xrightarrow{\iota} E \xrightarrow{\pi} G$ be an exact sequence of groups with A an Abelian group. Then define a a function (a section) $s : G \to E$ that assigns each $g \in G$ a representative $s(g)$ of g such that $s\pi = 1_G$. We then make $\iota(A)$ into a G-module via the action

$$g \circ (\iota(a)) = s(g)\iota(a)s(g^{-1}).$$

We define an extension of G by the G-module A as an exact sequence $A \xrightarrow{\mu} E \xrightarrow{\pi} G$ such that the the G-module structure on A as defined above is the given G-structure.

Equivalent Extensions and the Set of Extensions

Definition

We say that an extension $A \to E_1 \to G$ is equivalent to $A \to E_2 \to G$ if there is a homomorphism $\varphi : E_1 \to E_2$ of groups such that the diagram

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] \arrow[d, equal] & E_1 \arrow[r] \arrow[d, "\varphi"'] & G \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & A \arrow[r] & E_2 \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

commutes in **Grp**. By the Five-Lemma, φ is an isomorphism of groups. We then denote the set of equivalence classes of extensions of G by A as the set

$$M(G, A).$$

We associate the extension $A \to E \to G$ in $M(G, A)$ as the element $[E] \in M(G, A)$.

An Equivalence on $M(G, A)$

UNIVERSITY OF CALGARY

Theorem

Given an extension $A \to E \to G$, we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Der}(G,A) \arrow[r] & \mathrm{Der}(G,E) \arrow[d] & & \\ & & \mathrm{Hom}_{\mathbf{G\text{-}Mod}}(A,A) \arrow[r, "\theta"] & H^2(G,A) \arrow[r] & H^2(E,A). \end{tikzcd}$$

Now define a map $\Delta : M(G, A) \to H^2(G, A)$ by the association

$$\Delta\left([E]\right) = \theta(1_A) \in H^2(G, A).$$

Theorem

Δ is an isomorphism in $\mathbf{Set}$. In particular, there is a one-to-one correspondence between $H^2(G, A)$ and the set $M(G, A)$. Thusly the set $M(G, A)$ has a natural Abelian group structure and the map $M(G, -) : \mathbf{R\text{-}Mod} \to \mathbf{Ab}$ is a covariant functor.

What About Galois Groups?

UNIVERSITY OF CALGARY

Remarks

Let K be a field and let K_s be its separable closure. We now care about the structure of $H^2(G, \mathrm{Unit}(K_s))$ when $G = \mathrm{Gal}(K_s/K)$. Then, because $\mathrm{Unit}(K_s)$ is an object in $\mathfrak{D}_G$, we can think of $H^2(G, \mathrm{Unit}(K_s))$ as the group of continuous factor systems of G by $\mathrm{Unit}(K_s)$; in particular, the extensions that would appear in $M(G, \mathrm{Unit}(K_s))$ would all be continuous extensions.

Proposition

Let N/K and L/K be Galois extensions of fields such that N/L is a Galois extension. Then there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H^2(\mathrm{Gal}(L/K), \mathrm{Unit}(L)) \arrow[r] & H^2(\mathrm{Gal}(N/K), \mathrm{Unit}(N)) \arrow[d] \\ & & H^2(\mathrm{Gal}(N/L), \mathrm{Unit}(N)). \end{tikzcd}$$

Proof of Proposition

Proof

Begin by recalling the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r, tail] & \mathrm{Gal}(N/K) \arrow[r, two heads] & \mathrm{Gal}(N/L) \arrow[r] & 1 \end{tikzcd}$$

of continuous group homomorphisms. Now, $\mathrm{Unit}(L)$ is a $\mathrm{Gal}(L/K)$-module with continuous action, $\mathrm{Unit}(N)$ is a $\mathrm{Gal}(N/K)$-module with continuous action, and $\mathrm{Unit}(N)/\mathrm{Unit}(L)$ is a $\mathrm{Gal}(N/L)$-module with a continuous action. Then consider the diagram

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(L/K) \arrow[r, tail] \arrow[d, dashed] & \mathrm{Gal}(N/K) \arrow[r, two heads] \arrow[d, dashed] & \mathrm{Gal}(N/L) \arrow[r] \arrow[d, dashed] & 1 \\ 0 \arrow[r] & \mathrm{Unit}(L) \arrow[r, tail] & \mathrm{Unit}(N) \arrow[r, two heads] & \frac{\mathrm{Unit}(N)}{\mathrm{Unit}(L)} \arrow[r] & 0 \end{tikzcd}$$

with each dotted arrow denoting the action of the Galois group on the module. Through the injection of $\mathrm{Gal}(L/K) \to \mathrm{Gal}(N/K)$, we can $\mathrm{Unit}(L)$ into a $\mathrm{Gal}(N/K)$-module with continuous action by restricting scalars.

Proof, Cont.

The restriction of scalars that makes $\mathrm{Unit}(L)$ into a $\mathrm{Gal}(N/K)$-module is a continuous map. Thusly we can apply the cohomology functor and restrict scalars appropriately in the image of the functor in order to derive the long exact cohomology sequence. We can safely ignore the H^0 terms, for they will produce simply the sequence $0 \to \mathrm{Unit}(K) \to \mathrm{Unit}(K) \to 0$, which is silly. So, start at the 0 term, write $U(F) = \mathrm{Unit}(F)$ for any field, and give the sequence

$$\begin{tikzcd}
H^1(\mathrm{Gal}(L/K), U(L)) \arrow[r] & H^1(\mathrm{Gal}(N/K), U(N)) \arrow[r] & H^1(\mathrm{Gal}(N/L), U(N)) \arrow[d] \\
H^2(\mathrm{Gal}(N/L), U(N)) & H^2(\mathrm{Gal}(N/K), U(N)) \arrow[l] & H^2(\mathrm{Gal}(L/K), U(L)) \arrow[l]
\end{tikzcd}$$

Now, because L/K, N/K, and N/L are all Galois extensions, it follows that each H^1 term is zero. As such we have the exact sequence

$$0 \to H^2(\mathrm{Gal}(L/K), U(L)) \to H^2(\mathrm{Gal}(N/K), U(N)) \to H^2(\mathrm{Gal}(N/L), U(N)).$$

This completes the proof. $\square$

The Brauer Group

UNIVERSITY OF CALGARY

Definition

Let K be a field and let K_s be the separable closure of K. Then we define the Brauer Group of K, denoted $\mathrm{Br}(K)$, as the group

$$H^2(\mathrm{Gal}(K_s/K), \mathrm{Unit}(K_s)) =: \mathrm{Br}(K).$$

Proposition/Corollary

There is an exact sequence, for L/K a Galois extension of fields,

$$0 \to H^2(\mathrm{Gal}(L/K), \mathrm{Unit}(L)) \to \mathrm{Br}(K) \to \mathrm{Br}(L).$$

An Alternate Perspective on $\mathrm{Br}(K)$, Part One: Central Simple Algebras

UNIVERSITY OF CALGARY

Definition

Let K be a field. An algebra R over K is said to be central simple if R has no nontrivial two-sided ideals and $Z(R) = K$.

Theorem

Let R be a central simple K-algebra of finite K dimension. Then R is isomorphic as a K-algebra to the algebra

$$R \cong \mathrm{Mat}_n(D),$$

where D is a division ring of finite K-dimension and $n \in \mathbb{N}^\times$.

Definition

Two central simple K-algebras R and S are said to be equivalent if when we write $R \cong \mathrm{Mat}_n(D)$ and $S \cong \mathrm{Mat}_m(E)$ there is a K-algebra isomorphism between the division algebras $D \cong E$.

An Alternate Perspective on $\mathrm{Br}(K)$, Part Two: $\mathrm{Br}(K)$

UNIVERSITY OF CALGARY

Observation/Proposition

Let $B(K)$ denote the set of equivalence classes of all finite-dimensional central simple K-algebras. Then the tensor product of K-algebras is an Abelian binary map $\otimes : B(K) \prod B(K) \to B(K)$. Furthermore $[R] \otimes [R^{op}] = [K]$.

Definition

The set $B(K)$, equipped with the tensor product operation, defines the Brauer Group $\mathrm{Br}(K)$.

Theorem (cf. [Serre95] and [Farb])

The two notions of $\mathrm{Br}(K)$ are equivalent. The proofs suggested take two different perspectives: Serre's takes the point of view of Galois descent, while Farb/Dennis' takes the point of view of crossed products and factor systems.

A Short Exact Sequence of Brauer Groups

Example

Let V denote the set of nontrivial places of $\mathbb{Q}$. Then there is a short exact sequence of Brauer groups

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}) \longrightarrow \bigoplus_{v \in V} \mathrm{Br}(\mathbb{Q}_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Note the usage of the direct product (coproduct) of Abelian groups in the middle term (as opposed to the direct product).

Central References

Main References

Farb, Benson, and R. Keith Dennis. *Noncommutative Algebra.* 1st Ed. New York NY: Springer-Verlag. 1993. Print. GTM 144.

Hilton, P.J., and U. Stammbach. *A Course in Homological Algebra.* 2nd Ed. New York NY: Springer-Verlag. 1997. Print. GTM 4.

Serre, Jean-Pierre. *Galois Cohomology.* 2nd Ed. Trans. Patrick Ion. New York NY: Springer-Verlag. 2002. Print. SMM.

—. *Local Fields.* 2nd Ed, Corrected. Trans Marvin Jay Greenberg. New York NY: Springer-Verlag. 1995. Print. GTM 67.

Thanks

UNIVERSITY OF CALGARY

Thanks

Thank you everyone for listening to this
introduction to Galois cohomology, derived functors, and general group cohomology!