

# *Galois Cohomology of Algebraic Groups*

*Ayushi Tsydendorzhiev*

*October 17, 2024*

## *Contents*

<i>1</i>	<i>Introduction</i>	<i>2</i>
<i>1.1</i>	<i>Galois group actions</i>	<i>2</i>
<i>1.2</i>	<i>The fixed point functor and exact sequences</i>	<i>3</i>

## 1 Introduction

### 1.1 Galois group actions

Lecture 1, 10.10.2024

Let  $L/K$  be a Galois extension and  $G = \text{Gal}(L/K)$  its Galois group. The Galois group  $G$  acts on  $L$  via field automorphisms:

- Action on the field extension  $L$ : For  $\mathbb{Q}(\sqrt{2})$  its Galois group  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  acts either by identity or by sending  $\sqrt{2}$  to  $-\sqrt{2}$ .
- Action on the dual of the field extension  $L^*$ : For  $\mathbb{Q}(\sqrt{2})^*$  its Galois group acts on  $f(x_1, x_2) = x_1 \cdot 1 + x_2 \cdot \sqrt{2}$  either by identity or by sending  $f$  to  $f' = x_1 \cdot 1 - x_2 \cdot \sqrt{2}$ .
- Action on the group of  $n$ th roots of unity  $\mu_n(L)$ :
  - In  $\mathbb{Q}(\sqrt{2})$ , the  $n$ th roots of unity consist of  $\{-1, 1\}$  if  $n$  is even and  $\{1\}$  if  $n$  is odd. Both automorphisms in  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  leave  $\mu_n(\mathbb{Q})$  fixed, so this tells us that they all belong to the base field (are rational, in this case).
  - A more interesting example is the  $n$ th cyclotomic field  $\mathbb{Q}(\zeta_n)$ . In this field  $\mu_n(\mathbb{Q}(\zeta_n)) = \langle \zeta_n \rangle$ , the cyclic group generated by  $\zeta_n$ . The Galois group  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  is isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^*$ . For  $n = 5$  (prime), the Galois group is cyclic and consists of  $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$ . The action of the Galois group then permutes the 5th roots of unity. For  $n = 8$ , the Galois group  $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$  is isomorphic to  $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$  and is cyclic of order 4. The basis of  $\mathbb{Q}(\zeta_8)$  over  $\mathbb{Q}$  is given by  $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$ . The actions is given as:  $\sigma_1$  acts trivially,  $\sigma_3$  maps  $\zeta_8$  to  $\zeta_8^3$ ,  $\sigma_5$  acts by multiplication by  $-1$  and  $\sigma_7$  maps  $\zeta_8$  to  $\zeta_8^7$ .
- Action on the cyclic group  $(\mathbb{Z}/n\mathbb{Z})^*$ : same as above.
- Action on a finite abelian group  $M$ : trivial action.
- Action on the general linear group  $\text{GL}_n(L)$  over a field  $L$  of characteristic 0:  $\text{GL}_n(L)$  consists of  $n \times n$  invertible matrices over  $L$ . We have a Galois extension  $L/K$ . The Galois group acts by applying the field automorphisms to the entries of the matrices, so  $\sigma(A) = \sigma(a_{ij}) \forall 1 \leq i, j \leq n$ . The fixed points contain  $\text{GL}_n(K)$ .
  - Backstory: The determinant of a  $n \times n$  matrix  $A$  is defined as

$$\det(A) = \sum_{\pi \in S_n} \left( \text{sgn}(\pi) \prod_{i=1}^n a_{i, \pi(i)} \right)$$

Consider  $\sigma(\det(A))$ , where  $\sigma \in \text{Gal}(L/K)$  is a field automorphism. It distributes over addition and multiplication:

$$\sigma(\det(A)) = \sum_{\pi \in S_n} \left( \text{sgn}(\pi) \prod_{i=1}^n \sigma(a_{i, \pi(i)}) \right)$$

$\text{sgn}(\pi)$  is either even or odd.  $+1$  if even and  $-1$  if odd.

The signum is either  $+1$  or  $-1$ , so it is always in the base field  $K$  and is fixed by  $\sigma$ . Thus  $\sigma(\det(A)) = \det(\sigma(A))$ . So the action of the Galois group preserves determinants.

### 1.2 The fixed point functor and exact sequences

All of these examples are special cases of a more general concept: a group  $G$  acting on an algebraic group  $\mathbf{G} \subseteq \mathrm{GL}_n$ .

When studying group actions, we're often interested in fixed points

$$A^G = \{a \in A \mid \forall \sigma \in G : \sigma a = a\}$$

Here,  $A^G$  represents the set of all elements in  $A$  that are fixed by every element of  $G$ . To study fixed points more systematically, we introduce the fixed point functor  $-^G$ . This functor takes a  $\mathbb{Z}G$ -module and returns its fixed points. We're particularly interested in how this functor behaves with respect to exact sequences.

An algebraic group is a matrix group defined by polynomial conditions, at least this is what "The theory of group schemes of finite type over a field." by Milne says. I guess this is the consequence of Chevalley theorem?

#### Note 1.1.

**Group action perspective:** A  $\mathbb{Z}G$ -module is an abelian group  $A$  endowed with a (left) action  $(\sigma, a) \mapsto \sigma a$  of  $G$  on  $A$  such that for all  $\sigma \in G$  the map  $\varphi_\sigma : a \mapsto \sigma a$  from  $A$  to  $A$  is a morphism of abelian groups. This implies that the action of  $G$  is distributive,  $\varphi_\sigma(ab) = \varphi_\sigma(a) + \varphi_\sigma(b)$ .

**Ring module perspective:** Equivalently, a  $\mathbb{Z}G$ -module is a module over the group ring  $\mathbb{Z}[G]$ , where elements consist of formal linear combinations of elements from group  $G$  with integer coefficients, so something like  $3g_1 + 4g_2 + 10g_3 \in \mathbb{Z}[G]$ . It contains both  $\mathbb{Z}$  and  $G$  as subrings. The  $\mathbb{Z}[G]$ -module structure encapsulates both the abelian group structure of  $A$  and the  $G$ -action on  $A$ , which leads to the key insight:

$$\{\text{module over } \mathbb{Z}[G]\} \leftrightarrow \{\text{abelian group } A \text{ with } G\text{-action}\}$$

**Lemma 1.2.** Consider an exact sequence of  $\mathbb{Z}G$ -modules:

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

Applying the fixed point functor  $-^G$  to this sequence yields:

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

This new sequence is exact in  $\mathrm{Ab}$  (the category of abelian groups). Thus the functor  $-^G$  is left-exact, meaning it preserves exactness at the left end of the sequence.

- A natural question arises: Is the fixed point functor also right-exact? If such a lifting always exists, then the fixed point functor preserves exactness at  $C$ ,

making it right-exact. If not, we've discovered an obstruction that tells us something about the Galois action and the structure of our groups.

- To investigate this, we need to check if  $\ker h^G = \operatorname{im} g^G$ , or equivalently, if  $\operatorname{im} g^G = C^G$ . Breaking this down:
  - Take any  $c \in C^G$ .
  - Since  $C^G \subseteq C$ , there exists a  $b \in B$  such that  $g(b) = c$ .
  - If  $b$  were fixed by  $G$ , we'd be done. But it might not be.
    - \* Consider  $\sigma b - b$  for any  $\sigma \in G$ . We have  $g(\sigma b - b) = g(\sigma b) - g(b) = \sigma g(b) - g(b) = \sigma c - c$ .
    - \* Since  $c \in C^G$ ,  $\sigma c - c = 0$  and  $(\sigma b - b) \in \ker g$ .
    - \* By exactness,  $\ker g = \operatorname{im} f$ , so  $\sigma b - b \in \operatorname{im} f$ .
    - \* We can view this as an element of  $A$  (considering  $f$  as an inclusion  $A \subseteq B$ ).

Why  $\sigma b = b$ ?

Also,  $C \cong B / \operatorname{im} f$ . Or consider presentations of groups.

So the question of right-exactness boils down to whether or not every  $G$ -invariant element of  $C$  can be lifted to a  $G$ -invariant element of  $B$  and the obstruction to it lives inside of  $A$ .

And if  $b$  were indeed in  $B^G$  then  $(\sigma b - b) = 0 \in A$ .

- This analysis leads us to define a map (for a given  $c \in C^G$ ):

$$\varphi : G \rightarrow A, \quad \sigma \mapsto \sigma b - b =: a_\sigma$$

This map is called a crossed homomorphism (also known as a derivation or 1-cocycle). It measures how far  $b$  is from being  $G$ -invariant. If  $b$  were  $G$ -invariant, this map would be identically 0! Note that this is independent of any  $b$  taken such that  $g(b) = c$ . Such cocycles are cohomologous.

**Proposition 1.3.** The map  $\sigma \mapsto a_\sigma$  satisfies:

$$a_{\sigma\tau} = a_\sigma + \sigma a_\tau$$

This property is what defines a crossed homomorphism.

- **In the abelian case**, we define
  - $Z^1(G, A) = \{a' : G \rightarrow A \mid a'_{\sigma\tau} = a'_\sigma + \sigma a'_\tau\}$ , the set of all crossed homomorphisms from  $G$  to  $A$ .
  - $B^1(G, A) = \{a : \sigma \in G \mid \exists a' \in A : a_\sigma = \sigma a' - a'\}$ .
  - The quotient  $H^1(G, A) = Z^1(G, A) / B^1(G, A)$  is called the **first cohomology group** of  $G$  with coefficients in  $A$ . It measures the obstruction to the right-exactness of the fixed point functor.

The functor  $A \mapsto H^1(G, A)$  is a derived functor of the  $A \mapsto A^G$  functor.

The obstructions for right-exactness: find  $\sigma b - b \in A$  such that it is 0 under projection in  $Z^1(G, A)/B^1(G, A)$ . It is given by  $\delta(c) = [a_\sigma] \in H^1(G, A) = Z^1(G, A)/B^1(G, A)$ . We can extend our original sequence to a longer exact sequence:

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \xrightarrow{\delta} H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow 0$$

This sequence is exact in Ab, and the map  $\delta$  (called the connecting homomorphism) measures the failure of right-exactness of the fixed point functor, since  $\ker \delta$  represents all elements of  $C^G$  which can be lifted to elements of  $B^G$ .

- The key idea of the 1-cocycle is to encode the failure of  $G$ -invariance in a way that's compatible with the group structures involved. It allows us to move from concrete elements ( $b$  and  $c$ ) to cohomological objects ( $[\varphi]$ ) that capture essential information about the Galois action and the relationship between our groups  $A$ ,  $B$ , and  $C$ . This approach transforms specific lifting problems into more general cohomological questions, allowing us to apply powerful theoretical tools and gain deeper insights into the structures we're studying.

**Exercise 1.4.** Show that  $H^1(G, -)$  is functorial and

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow 0$$

is exact. Find example with  $\delta \neq 0$ .

- **In the non-abelian case**, we define

- $H^0(G, A) = A^G$ , the fixed points as before.
- $H^1(G, A) = Z^1(G, A) / \sim$ , where  $\sim$  is an equivalence relation defined by:  
 $a_\sigma \sim b_\sigma \iff \exists a' \in A : b_\sigma = (a')^{-1} \cdot a_\sigma \cdot {}^\sigma a'$ .

In this case,  $H^1(G, A)$  doesn't have a group structure, but is a pointed set (a set with a distinguished element). We can still define a notion of exactness for sequences of pointed sets.

**Proposition 1.5.** For  $A \leq_G B$ , we obtain  $G \curvearrowright B/A$  and

$$1 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \rightarrow H^1(G, A) \rightarrow H^1(G, B)$$

is exact.

This is the **Galois cohomology**. Why do we care? In the non-commutative case  $H^1(G, A)$  classifies "K-objects". In our lecture we will use this to classify simple and simply connected linear algebraic  $k$ -groups  $G$ .

In field theory,  $H^1(G, A)$  can represent the obstruction to an element being a norm. In the theory of algebraic groups,  $H^1(G, A)$  can represent the obstruction to a torsor having a rational point.

We cannot expect  $B^1(G, A)$  to be a subgroup. Why?

${}^\sigma a$  denotes the action of  $\sigma$  on  $a$ .

Exactness in pointed sets  $(A, *)$  is defined as  $\text{im } f = \ker g = g^{-1}(*)$   
 $A \leq_G B$  is  $G$ -equivariant inclusion.