

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>
<i>2</i>	<i>Preliminaries from algebraic number theory.</i>	<i>6</i>
<i>2.1</i>	<i>Number fields</i>	<i>6</i>
<i>2.2</i>	<i>Integrality in number fields</i>	<i>7</i>
<i>2.3</i>	<i>The arithmetic of algebraic integers</i>	<i>8</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 ζ_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: σ_1 acts trivially, σ_3 maps ζ_8 to ζ_8^3 , σ_5 acts by multiplication by -1 and σ_7 maps ζ_8 to ζ_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 σ . 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 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 δ (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.

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.

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.

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

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

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 .

2 Preliminaries from algebraic number theory.

2.1 Number fields

Lecture 2, 17.10.24

User: GRK, password: 2240.

Definition 2.1. An algebraic number field is a finite field extension k/\mathbb{Q} .

- This definition implies the following properties:
 - The field k has characteristic 0.
 - By the Primitive Element Theorem, $k = \mathbb{Q}(a)$ for some $a \in K$.
 - There exists a unique minimal polynomial $f \in \mathbb{Q}[X]$ for a , with $\deg(f) = d = [k : \mathbb{Q}]$.
- Let (a_1, \dots, a_d) be the roots of f in the algebraic closure of \mathbb{Q} within \mathbb{C} . These roots are called the **Galois conjugates** of a . Note that these roots do not lie in \mathbb{Q} .
- Properties of embeddings:
 - For each i , the map $a \mapsto a_i$ defines an isomorphism $\mathbb{Q}(a) \cong \mathbb{Q}(a_i)$.
 - Any embedding $k \rightarrow \mathbb{C}$ must send a to some a_i .
 - There are exactly d embeddings $k \rightarrow \mathbb{C}$, denoted $\sigma_1, \dots, \sigma_d$.
- Classification of embeddings:
 - Note that $(a_1, \dots, a_d) = \overline{(a_1, \dots, a_d)}$, so $\sigma_i(k) \subseteq \mathbb{R}$ if and only if $\bar{a}_i = a_i$.
 - We can thus classify the embeddings as:
 - * Real embeddings (real places of K): r_1
 - * Complex embeddings (complex places of K): $2r_2$ (counted in pairs due to complex conjugation)
 - This classification implies $d = r_1 + 2r_2$
- Examples:
 - For $k = \mathbb{Q}(\sqrt[3]{2})$: $r_1 = 1, r_2 = 1$
 - For $k = \mathbb{Q}(\exp(2\pi i/n))$, $n \geq 3$: $r_1 = 0, r_2 = \varphi(n)/2$ (odd n)

Definition 2.2. For any $\alpha \in K$, we define two rational numbers:

1. The norm: $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^d \sigma_i(\alpha)$
2. The trace: $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^d \sigma_i(\alpha)$

Note: $N_{K/\mathbb{Q}}(\alpha) = \det(\alpha : K \rightarrow K)$, and similarly for the trace.

- Basis criterion: Let $(\alpha_1, \dots, \alpha_d) \in k$ and $\lambda_1, \dots, \lambda_d \in \mathbb{Q}$. Then $\sum_{i=1}^d \lambda_i \alpha_i = 0 \iff \sum_{i=1}^d \lambda_i \sigma_j(\alpha_i) = 0$ for all j . Moreover, $\{\alpha_i\}_{i=1}^d$ is a basis of k if and only if $\det(\sigma_i(\alpha_j)) \neq 0$.

Definition 2.3. The **discriminant** of a basis $\{\alpha_1, \dots, \alpha_d\}$ of a number field k of degree d over \mathbb{Q} is defined as: $\text{discr}(\{\alpha_1, \dots, \alpha_d\}) = \det^2(\sigma_i(\alpha_j)) \in \mathbb{Q}$, where $\sigma_1, \dots, \sigma_d$ are the d distinct embeddings of k into \mathbb{C} .

Exercise 2.4. Prove that $\text{discr}(\alpha_i) = \det(\text{Tr}_{k/\mathbb{Q}}(\alpha_i \alpha_j))_{1 \leq i, j \leq d}$. Show that if $k = \mathbb{Q}(a)$ for some $a \in k$, then $\text{discr}(\{1, a, a^2, \dots, a^{d-1}\}) = \prod_{1 \leq i < j \leq d} (\sigma_i(a) - \sigma_j(a))^2$.

To introduce relative versions for an extension l/k , we define the relative discriminant $\text{discr}()_{l/k}$ using only those embeddings $\sigma_i : l \hookrightarrow \mathbb{C}$ which restrict to the identity on k .

2.2 Integrality in number fields

Let k be an algebraic number field for the following discussion.

Definition 2.5. The ring of integers in k is defined as:

$$\mathcal{O}_k = \{\alpha \in k : f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[X]\}.$$

- Example: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. It is often referred to as the ring of “rational integers”.

Proposition 2.6. For $(\alpha_1, \dots, \alpha_r) \in k$, the following are equivalent:

1. $(\alpha_1, \dots, \alpha_r) \in \mathcal{O}_k$
2. $\mathbb{Z}[\alpha_1, \dots, \alpha_r]$ is finitely generated as a \mathbb{Z} -module.

The corollary is that \mathcal{O}_k is a ring. (why?)

Lemma 2.7. For $\alpha \in k$, there exist $\beta \in \mathcal{O}_k, n \in \mathbb{Z}$ such that $\alpha = \frac{\beta}{n}$.

From now on we can assume that our algebraic number field is generated by a primitive element which is an algebraic integer.

Proposition 2.8. We can sandwich the ring \mathcal{O}_k between $\mathbb{Z}[a]$ and $\frac{1}{\text{discr}\{1, \dots, a^{d-1}\}} \mathbb{Z}[a]$. (This $1/\text{discr}$ is in \mathbb{Z} because it is in the intersection of algebraic integers in k and \mathbb{Q}). Because it lies between two free abelian groups of the same rank, it has to be free abelian of the same rank.

Corollary 2.9. \mathcal{O}_k has a \mathbb{Z} -basis of rank d . Any such is called an integral basis.

(\mathbb{Z} lattice in a \mathbb{Q} vector space and you exhaust it by multiplying with the integers? What? Minkowski geometry of numbers (covolumes?))

Corollary 2.10. \mathcal{O}_k is noetherian.

Algebraic number theory is not (algebraic) number theory but rather (algebraic number) theory.

Definition 2.11. The discriminant of k is given by $\text{discr}_k = d_k = \text{discr}\{\alpha_1, \dots, \alpha_d\}$ for an integral basis. Well-defined because $\det(T\alpha_i) = \pm 1$.

More generally, we can also define relative discriminants $\text{fancyd}_{l/k} = \text{discr}(\beta_i) \subseteq \mathcal{O}_k$. This d is an ideal because in general we might not be in a PID anymore.

Exercise 2.12. $k = \mathbb{Q}(\sqrt{D})$, D square-free integer. If $D \equiv 1(4)$ or $D \equiv 2,3(4)$ then the integral basis is ... and discriminant is D or $4D$.

2.3 The arithmetic of algebraic integers

For $k = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_k = \mathbb{Z}[\sqrt{5}]$. In \mathcal{O}_k , we have $21 = 3 \cdot 7 = (1 + 2\sqrt{5}) \cdot (1 - 2\sqrt{5})$ and these factors are irreducible. (something something norm of a number). So it is not a UFD. Kummer suggested: in an ideal world, there would be ideal numbers $p_1 \cdot p_2 = 3$ and $p_3 \cdot p_4 = 7$, with $p_1 \cdot p_3 = 1 + 2\sqrt{5}$ and $p_2 \cdot p_4 = 1 - 2\sqrt{5}$, hence $21 = p_1 p_2 p_3 p_4 = p_1 p_3 p_2 p_4$ so they would differ only by a permutation and factorization would be unique. Apparently: $p_1 \mid 3$ and $p_1 \mid 1 + 2\sqrt{5} \implies p_1 \mid \lambda 3 + \mu(1 + 2\sqrt{5})$ and p_1 should be determined by the set of all $\alpha \in \mathcal{O}_k$ that it divides. So set $p_1 = (3, 1 + 2\sqrt{5})$ and $p_2 = (3, 1 - 2\sqrt{5})$ and so on... So the idea is that one might get unique factorization in ideals instead.

Theorem 2.13. The ring \mathcal{O}_k is noetherian, integrally closed and of dimension 1.

The hard thing is to single out that these three properties are key to a ring being a Dedekind domain.

Definition 2.14. An integral domain satisfying these three properties is called a Dedekind domain.

Lecture 3, ...