Galois cohomology in algebraic groups

Ed Belk

March 26, 2020

In this talk, we go over some of the essential aspects of (abelian and nonabelian) group cohomology, and how they arise in the study of algebraic groups.

1 Basics of cohomology

Let $\Gamma$ be a group acting on another group $A$; depending on the context, we will want certain further assumptions on these objects, for instance that $A$ is abelian, or that the action is a continuous action of topological groups. Essentially, group cohomology is a systematic way to collect information on certain maps $\Gamma \to A, \Gamma \times \Gamma \to A$, etc. (called respectively 1-cocycles, 2-cocycles, and so on), which naturally encode important information about the objects under consideration.

In this talk, we will restrict our attention to 1-cocycles (sometimes called crossed homomorphisms) alone.

1.1 Abelian cohomology

We begin with the most basic example. Let $\Gamma$ be a finite or profinite group acting on an abelian group $A$, and let $Z^1(\Gamma, A)$ be the set of all 1-cocycles; that is, the set of all functions $c : \Gamma \to A$ which satisfy

$$c(\sigma \tau) = c(\sigma) + \sigma.c(\tau) \text{ for all } \sigma, \tau \in \Gamma,$$

where $\sigma.a$ denotes the action of $\sigma \in \Gamma$ on $a \in A$. We can make $Z^1(\Gamma, A)$ into an abelian group by equipping it with the operation

$$(c_1 + c_2)(\sigma) = c_1(\sigma) + c_2(\sigma).$$
Inside \( Z^1(\Gamma, A) \) is the subgroup \( B^1(\Gamma, A) \) of \textbf{1-coboundaries}, which are those 1-cocycles \( c \) for which there exists \( a \in A \) such that
\[
c(\sigma) = \sigma.a - a \quad \text{for all } \sigma \in \Gamma.
\]
The \textbf{1-cohomology group} is defined to be the quotient of the 1-cocycles by the 1-coboundaries: that is,
\[
H^1(\Gamma, A) = Z^1(\Gamma, A)/B^1(\Gamma, A).
\]
Elements of \( H^1(\Gamma, A) \) are typically written \([c]\), with \( c \in Z^1(\Gamma, A) \). From the definition, it follows that \([c] = [d]\) if and only if there exists \( a \in A \) such that
\[
d(\sigma) = -a + c(\sigma) + \sigma.a \quad \text{for all } \sigma \in \Gamma.
\]
for all \( \sigma \in \Gamma \).

\textbf{Theorem 1.1.} Let \( \Gamma \) be a finite or profinite group and let
\[
1 \to A \to B \to C \to 1
\]
be a short exact sequence of \( \Gamma \)-modules; then there exists a long exact sequence of groups
\[
1 \to A^\Gamma \to B^\Gamma \to C^\Gamma \to H^1(\Gamma, A) \to H^1(\Gamma, B) \to H^1(\Gamma, C) \to H^2(\Gamma, A) \to \cdots
\]
where \( A^\Gamma \) is the subgroup of \( \Gamma \)-fixed elements and \( H^n(\Gamma, -) \) are the higher cohomology groups (whose definition we omit).

Abelian cohomology provides a framework for other cohomology theories, as we will soon see.

\section*{1.2 Nonabelian cohomology}

Now \( \Gamma \) will continue to be a finite or profinite group, but \( A \) will be allowed to be an arbitrary group equipped with an action of \( \Gamma \); we will write \( \sigma.a \) for this action as before. This time, the \textbf{set of 1-cocycles} is defined to be the set of all maps \( c : \Gamma \to A \) satisfying
\[
c(\sigma\tau) = c(\sigma)(\sigma.c(\tau)) \quad \text{for all } \sigma, \tau \in \Gamma;
\]
the analogy with the abelian case is clear. Unfortunately, pointwise multiplication of cocycles does not generally yield a cocycle, and so $Z^1(Γ, A)$ is not a group, merely a set.

On the set $Z^1(Γ, A)$ we place the equivalence relation $∼$, where $c ∼ d$ if and only if there exists $a ∈ A$ such that

$$d(σ) = a^{-1}c(σ)(σ.a) \quad (***)$$

for all $σ ∈ Γ$. We denote by $H^1(Γ, A)$ the pointed set of equivalence classes in $Z^1(Γ, A)$, called the 1-cohomology set. As a pointed set, it has a distinguished element $[1]$; namely, the class consisting of the cocycles $c$ satisfying

$$c(σ) = a^{-1}(σ.a) \text{ for some } a ∈ A.$$

The nonabelian case gives us familiar, but decidedly weaker results.

**Theorem 1.2.** Let $Γ$ be a finite or profinite group and let

$$1 → A → B → C → 1$$

be an exact sequence of groups equipped with a $Γ$-action; then the sequence of pointed sets

$$1 → A^Γ → B^Γ → C^Γ → H^1(Γ, A) → H^1(Γ, B)$$

is exact. Moreover, if $A$ is normal in $B$, then

$$1 → A^Γ → B^Γ → C^Γ → H^1(Γ, A) → H^1(Γ, B) → H^1(Γ, C)$$

is exact, and if $A$ lies in the centre of $B$, then

$$1 → A^Γ → B^Γ → C^Γ → H^1(Γ, A) → H^1(Γ, B) → H^1(Γ, C) → H^2(Γ, A)$$

is exact.

**Remark:** A sequence $A \overset{f}{→} B \overset{g}{→} C$ of pointed sets is called exact at $B$ if $g^{-1}([1]_C) = f(A)$, where $[1]_C$ is the distinguished element of $C$.

The parallels with the abelian case are clear. In practice, we will take $Γ$ to be the Galois group of an extension of local fields, and we may make further assumptions about the objects in question (for instance, we may want our groups to be topological and the action to be continuous).

Finally, we observe that, in all of these cohomology theories, an inclusion $A ↪ B$ of $Γ$ modules induces a map $H^1(Γ, A) → H^1(Γ, B)$ (which is not, in general, injective).
2 Tori

Until now we have considered algebraic groups defined over an algebraically closed field; now, we will allow the possibility that the group we are working with is defined over some other field (say, $\mathbb{Q}_p$ or $F_p((t))$). It will turn out that our cohomology groups/sets will help us categorize these groups.

Throughout this section, $F$ will be an arbitrary field, and $F_s \supset F$ will be a fixed separable closure.

2.1 Basic notions

In the case that $F$ is algebraically closed, we have defined a torus over $F$ to be an algebraic group defined over $F$ (more briefly, an $F$-group) which is isomorphic over $F$ to finitely many copies of $\mathbb{G}_m$. For general fields $F$, however, we will need a stronger definition.

**Definition 1:** An $F$-group $T$ is called an $F$-torus (or simply torus) if there exist an integer $r \geq 0$ and an isomorphism $T(F_s) \cong \mathbb{G}_m(F_s)^r$ defined over $F_s$. In this case, the integer $r$ is called the rank of the torus. The torus $T$ is said to be $F$-split (or simply split) if there exists an isomorphism $T(F) \cong \mathbb{G}_m(F)^r$ defined over $F$.

**Terminology:** If $G$ is an $F$-group which contains a maximal torus which is split, then $G$ is said to be a split group. In case $G$ admits a Borel subgroup defined over $F$, it is called quasi-split.

**Example 1:** Let $F$ be a nonarchimedean local field. Inside $\text{SL}_2(F)$ we have the split maximal torus $T$ consisting of the diagonal matrices, as we have seen. However, there are also many non-split maximal tori, of the form

$$T_\varepsilon(F) = \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} : x^2 - \varepsilon y^2 = 1 \right\},$$

where $\varepsilon \in F$ is a non-square. More precisely, we can write

$$T \cong \{(u, v) \in F^2 : uv - 1 = 0\} \text{ and } T_\varepsilon \cong \{(x, y) \in F^2 : x^2 - \varepsilon y^2 - 1 = 0\}.$$

To see that $T_\varepsilon$ is a torus, we pass to the extension field $E = F(\sqrt{\varepsilon})$; we then see that an isomorphism $T \cong T_\varepsilon$ is given by the mutually inverse change of variables

$$u = x + y\sqrt{\varepsilon}, \quad v = x - y\sqrt{\varepsilon} \quad \text{and} \quad x = \frac{u + v}{2}, \quad y = \frac{u - v}{2\sqrt{\varepsilon}}.$$
from which it follows immediately that $T(E) \cong T_\varepsilon(E) \cong G_m(E)$.

The same example, with $F = \mathbb{R}, E = \mathbb{C}$, and $\varepsilon = -1$ gives us the familiar example

$$T(\mathbb{R}) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} : (x, y) \in \mathbb{R}^2 \right\}$$

and

$$T^{-1}(\mathbb{R}) = \text{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : (a, b) \in \mathbb{R}^2, a^2 + b^2 = 1 \right\};$$

respectively, the split and compact forms of the one-dimensional real torus.

We might colloquially call the field $E$ from the previous example the splitting field of the torus $T_\varepsilon$.

### 2.2 Galois actions

By definition, all maximal $F$-tori of a given $F$-group $G$ are isomorphic over $F_s$; however, we might want to ask how many different $F$-isomorphism classes of tori there are. It turns out there is a very elegant answer to this question.

Let $T$ be an $F$-torus. The action of $\Gamma$ on $F_s$ induces an action on $T(F_s)$ by its natural action on the ring of functions $F[T]$; we will denote this action by $\sigma.t$ for $\sigma \in \Gamma, t \in T(F_s)$. This further induces an action of $\Gamma$ on the group of characters $X = X^*(T)$ of $T$ defined over $F_s$ via

$$(\sigma, \chi)(t) := \sigma.(\chi(\sigma^{-1}.t))$$

for $\chi \in X, \sigma \in \Gamma, t \in T(F_s)$, making the diagram

$$\begin{array}{ccc}
T(F_s) & \xrightarrow{\sigma.} & T(F_s) \\
\downarrow{\chi} & & \downarrow{\sigma, \chi} \\
G_m & \xrightarrow{\sigma.} & G_m
\end{array}$$

commute. Furthermore, considered topologically (where $\Gamma$ has the profinite topology, and $X$ and $T(F_s)$ the discrete topology), these actions are continuous.

Recalling that $X$ is a free abelian group of finite rank, we conclude that, to each $F$-torus $T$, we can associate a finitely-generated free abelian group $X$ equipped with a continuous action of $\Gamma$. It turns out that this association is bijective: we have
Theorem 2.1. Let \( \mathcal{T} \) be the category of algebraic tori defined over \( F \), and let \( \mathcal{X} \) be the category of finitely-generated free abelian groups equipped with a continuous action of \( \Gamma \). There is an anti-equivalence of categories \( \mathcal{T} \to \mathcal{X} \) given by the map \( T \mapsto X^*(T) \).

That is: to have an \( F \)-torus is to have a finitely-generated free abelian group with a continuous \( \Gamma \)-action.

We can say something about the torus if we know something about the group, or vice versa: for instance, if \( T \) is \( F \)-split (of rank \( r \), say), then there exists an \( F \)-isomorphism \( T(F) \cong \mathbb{G}_m(F)^r \), and so evidently all characters of \( T \) are defined over \( F \), and so are fixed by the action of \( \Gamma \). Conversely, if \( T \) is \textbf{anisotropic}, meaning it contains no nontrivial \( F \)-split torus, then \( T \) has no nontrivial characters which are defined over \( F \), and so only the trivial character is fixed by the \( \Gamma \)-action. That is:

Proposition 2.2. Let \( T \) be an \( F \)-torus and let \( X \) be its character lattice with the associated \( \Gamma \)-action. Then:

1. \( T \) is split if and only if \( \Gamma \) acts trivially on \( X \), and
2. \( T \) is anisotropic if and only if \( \Gamma \) has no nontrivial fixed point in \( X \).

3 Galois descent

Finally, it is also possible to answer questions about tori sitting inside a given algebraic group \( G \) using cohomology; we retain the notation from the previous section.

3.1 Stable and rational conjugacy

Let \( G \) be an \( F \)-group. We will say two maximal \( F \)-tori \( S, S' \) in \( G \) are \textbf{stably conjugate} if there exists \( g \in G(F_s) \) such that

\[ gS(F)g^{-1} = S'(F), \]

and we will say that they are \textbf{rationally conjugate} if there exists \( h \in G(F) \) such that

\[ hS(F)h^{-1} = S'(F); \]
these are clearly equivalence relations. Furthermore, as rational conjugacy implies stable conjugacy, we have the following

**Fact:** Let \( \mathfrak{T}(G) \) be the set of all maximal \( F \)-tori of \( G \); then \( \mathfrak{T}(G) \) is partitioned into stable conjugacy classes, which are in turn partitioned into rational conjugacy classes.

It turns out that Galois cohomology will allow us to classify both sets of equivalence classes.

**Theorem 3.1.** Let \( F \) be a local nonarchimedean field and let \( \Gamma \) be the absolute Galois group \( \text{Gal}(F_s/F) \). Let \( G \) be an \( F \)-group, \( T \subset G \) a maximal \( F \)-torus, and \( N \) the normalizer of \( T \) in \( G \). There is a one-to-one correspondence between the set of rational conjugacy classes of maximal tori of \( G \), and the kernel of the map

\[
H^1(\Gamma, N(F_s)) \rightarrow H^1(\Gamma, G(F_s)),
\]

which we shall call \( \ker(G, T) \).

**Proof.** We remark that the restriction of the action of \( \Gamma \) to any subgroup \( H \) of \( G \) yields a \( \Gamma \)-action on \( H \) (so in particular, \( H^\sigma = H \) for all \( \sigma \in \Gamma \)).

Let \( S \) be a maximal torus of \( G \), and let \( g \in G(F_s) \) satisfy

\[
S(F_s) = gT(F_s)g^{-1}.
\]

To lighten notation, we will temporarily write \( g^\sigma \) for \( \sigma g \) (and \( g^{-\sigma} \) for \( \sigma g^{-1} \)). By our previous remarks we know \( S(F_s)^\sigma = S(F_s) \); thus

\[
T(F_s) = g^{-1}S(F_s)g = g^{-1}S(F_s)^\sigma g = g^{-1}(gT(F_s)g^{-1})^\sigma g
\]
\[
= g^{-1}g^\sigma T(F_s)^\sigma g^{-\sigma}g = (g^{-1}g^\sigma)T(F_s)(g^{-1}g^\sigma)^{-1},
\]

from which we see \( g^{-1}g^\sigma \in N(F_s) \).

Furthermore, the map \( c_g : \Gamma \rightarrow N(F_s) \) defined by \( c_g(\sigma) = g^{-1}g^\sigma \) satisfies the 1-cocycle condition: we have

\[
c_g(\sigma\tau) = g^{-1}g^{\sigma\tau} = g^{-1}(g^{\tau})^\sigma = g^{-1}g^\sigma g^{-\sigma}(g^{\tau})^\sigma = g^{-1}g^\sigma(g^{-1}g^\tau)^\sigma,
\]

and so \( c_g \in Z^1(\Gamma, N(F_s)) \). Therefore, we can define a map \( \mathfrak{T}(G) \) to \( H^1(\Gamma, N(F_s)) \) by sending the torus \( S(F_s) = gT(F_s)g^{-1} \) to the cocycle \( \sigma \mapsto g^{-1}g^\sigma \). 

This map is invariant on rational conjugacy classes: if \( S, S' \) lie in the same conjugacy class, we can write \( S(F) = \gamma S'(F) \gamma^{-1} \) for some \( \Gamma \in G(F) \), and so if we write \( S = xT_{x^{-1}}, S' = yT_{y^{-1}} \) (for some \( x, y \in G(F_s) \)), then we have

\[
T(F_s) = x^{-1} S(F_s) x = x^{-1} \gamma S'(F_s) \gamma^{-1} x = x^{-1} \gamma y T(F_s) y^{-1} \gamma^{-1} x,
\]

and so \( n := x^{-1} \gamma y \in N(F_s) \). Using the fact that \( \gamma^\sigma = \gamma \) for all \( \sigma \in \Gamma \), we see that

\[
y^{-1} y^\sigma = (\gamma^{-1} x n)^{-1} (\gamma^{-1} x n)^\sigma = n^{-1} x^{-1} \gamma \gamma^{-1} x^\sigma n^\sigma = n^{-1} x^{-1} x^\sigma n^\sigma,
\]

and hence \([c_y] = [c_x] \) in \( H^1(\Gamma, N(F_s)) \).

Surjectivity of the map is clear, as \( \ker(G, T) \) is precisely the set of maps \( \sigma \mapsto g^{-1} g^\sigma \) as \( g \) varies over elements of \( G(F_s) \); it remains only to show injectivity. Therefore suppose \([c_x] = [c_y] \); we aim to show that the rational class of \( xT_{x^{-1}} \) is the same as that of \( yT_{y^{-1}} \). By assumption, we know there exists \( n \in N(F_s) \) such that

\[
x^{-1} x^\sigma = n^{-1} y^{-1} y^\sigma n^\sigma \text{ for all } \sigma \in \Gamma,
\]

or equivalently

\[
1 = y n x^{-1} x n^{-\sigma} y^{-\sigma} = (x n^{-1} y^{-1})^{-1} (x n^{-1} y^{-1})^\sigma \text{ for all } \sigma \in \Gamma,
\]

which implies that \( x n^{-1} y^{-1} \) is fixed by every \( \sigma \in \Gamma \), and therefore lies in \( G(F) \). It follows that the rational conjugacy class of \( y T_{y^{-1}} \) is the same as that of

\[
(x n^{-1} y^{-1}) y T_{y^{-1}} (x n^{-1} y^{-1})^{-1} = x T_{x^{-1}},
\]

and we are done.

\[\square\]

### 3.2 Isomorphism classes of \( F \)-tori

The previous subsection had the situation of a torus \( T \) sitting inside of an ambient group \( G \); if we want to answer questions about tori in the abstract, we should take the situation \( G = T \). This immediately yields

**Corollary 1:** Let \( r \geq 0 \) and let \( T \) be an \( F \)-torus of rank \( r \). There is a one-to-one correspondence between the set of rational \( F \)-tori of rank \( r \), and the group \( H^1(\Gamma, T(F_s)) \).

We also have the following result of Tate:
Theorem 3.2 (Local duality theorem). Let $F$ be a non-archimedean local field with separable closure $F_s$, and let $\mu$ be the subgroup of $F_s^\times$ consisting of the roots of unity. If $A$ is a $\Gamma$-module and let $A^\vee = \text{Hom}(A, \mu)$, then there is a perfect pairing

$$H^i(\Gamma, A) \times H^{2-i}(\Gamma, \mu(F_s)) \cong \mathbb{Q}/\mathbb{Z}$$

for $i = 0, 1, 2$. In particular, if $A = T(F_s)$ is an $F$-torus of rank $r$, then there is an isomorphism

$$H^1(\Gamma, T(F_s)) \cong H^1(\Gamma, \mathbb{Z}^r).$$

Combining this theorem with corollary 1 gives us

**Theorem 3.3.** Let $r \geq 0$. There is a one-to-one correspondence between the set of rational $F$-tori of rank $r$, and the group $H^1(\Gamma, \mathbb{Z}^r)$.

Finally, it is also possible to understand the weaker notion of stable conjugacy through cohomology groups: retaining notation from before, let us put $W = N(F_s)/T(F_s)$, and let us consider the short exact sequence

$$1 \to T \to N \to W \to 1$$

of $\Gamma$-modules; the action of $\Gamma$ on $W$ is induced by the action on $G$.

**Theorem 3.4.** Under the hypotheses of theorem 3.1: there is a one-to-one correspondence between the stable conjugacy classes in $\Sigma(G)$ and the 1-cohomology set $H^1(\Gamma, W)$.

We omit the proof.