Lecture 11: Galois Cohomology

William Stein

Feb 5, 2010

1 Galois Cohomology

In this course we have developed a foundation for group cohomology. The goal for the rest of the course (about 15 lectures), is to see some applications of group cohomology to Galois theory and algebraic number theory that are important to understanding contemporary research in number theory. For the rest of the course, our group will always be the Galois G of an extension of fields, and our module A will "arise in nature", equipped with a *natural* action of G. The main topics are Galois cohomology of abelian varieties, the Brauer group of a field, local and global duality, and étale (and other) cohomology which generalizes the idea of Galois cohomology to bases other than fields. This part of the course requires more background in number theory.

Excellent references include the many articles with the title *Galois Cohomology*, such as Tate's, Washington's, etc.

1.1 The Definition

Let K be a field, e.g., a number field such as $\mathbb{Q}(\sqrt[3]{2})$, a finite field such as $\mathbb{F}_9$, a p-adic field such as $\mathbb{Q}_{11}$, or a function such as $\mathbb{F}_7(t)$ or $\mathbb{C}(u,v)$. Let L/K be a *finite* separable Galois extension of K with Galois group $G = \mathrm{Gal}(L/K)$. For any G-module A, let

$$\mathrm{H}^q(L/K, A) = \mathrm{H}^q(\mathrm{Gal}(L/K), A), \qquad \text{for } q \geq 0$$

and

$$\hat{\mathrm{H}}^q(L/K, A) = \hat{\mathrm{H}}^q(\mathrm{Gal}(L/K), A), \qquad \text{for all } q \in \mathbb{Z}.$$

We call A a *Galois module.*

1.2 Infinite Galois extensions

John Tate pioneered the study of $\mathrm{H}^q(L/K, A)$ when L/K is *infinite.* When L is infinite, let

$$\mathrm{H}^q(L/K, A) = \varinjlim_{M} \mathrm{H}^q\left(M/K,\ A^{\mathrm{Gal}(L/M)}\right),$$

where the injective limit is over all finite Galois extensions M of K contained in L, and the maps are the inflation maps. We will often write

$$A(M) = A^{\mathrm{Gal}(L/M)},$$

motivated by similar notation for the group of rational points on an elliptic curve.

When $K \subset M \subset M'$, we have a morphism of pairs

$$(\mathrm{Gal}(M/K),\ A(M)) \to (\mathrm{Gal}(M'/K),\ A(M')),$$

given by the natural map $\mathrm{Gal}(M'/K) \to \mathrm{Gal}(M/K)$ and the inclusion $A(M) \hookrightarrow A(M')$, which defines

$$\mathrm{H}^q(M/K, A(M)) \xrightarrow{\mathrm{inf}} \mathrm{H}^q(M'/K, A(M')).$$

When $q = 1$, the inf-res sequence is exact, so all of the maps used to define the above injective limit are injections, and we can think of $\mathrm{H}^1(L/K, A)$ as simply being the "union" of the groups $\mathrm{H}^1(M/K, A(M))$, over all finite Galois M. When $q > 1$, (presumably) the above inflation maps need not be injective.

Finally, we let

$$\mathrm{H}^q(K, A) = \mathrm{H}^q(K^{\mathrm{sep}}/K, A).$$

With this notation, the inf-res sequence is

$$0 \to \mathrm{H}^1(M/K, A(M)) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(K, A) \xrightarrow{\mathrm{res}} \mathrm{H}^1(M, A).$$

The correct topology on the group $\mathrm{Gal}(L/K)$ is the one for which the open subgroups are the subgroups $\mathrm{Gal}(L/M)$ for M any finite Galois extension of K.

Exercise 1.1. Use the axiom of choice to show that there exists a finite index normal subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that is not open. [Hint: Consider the compositum of infinitely many distinct quadratic extensions of $\mathbb{Q}$. Their Galois group is $\prod \mathbb{F}_2$. The ideal $\oplus\mathbb{F}_2$ in $\prod \mathbb{F}_2$ contains a maximal ideal I. Consider the inverse image of I in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.]

We always equip A with the discrete topology.

Proposition 1.2. *Fix topologies on* $\mathrm{Gal}(L/K)$ *and* A *as above. Then* $\mathrm{H}^q(L/K, A)$ *is the group of* continuous *cocycles modulo coboundaries.*

Proof. We first show that if $[f] \in \mathrm{H}^q(L/K, A)$ then f is continuous. By definition we have $[f] \in \mathrm{H}^q(M/K, A(M))$ for some finite Galois extension M/K. Since the natural restriction map $\mathrm{Gal}(L/K)^q \to \mathrm{Gal}(M/K)^q$ is continuous and both $\mathrm{Gal}(M/K)$ and $A(M)$ are discrete, we conclude that the composite map f is continuous.

Next suppose $f : \mathrm{Gal}(L/K)^q \to A$ is a continuous cocycle. Because A has the discrete topology, the inverse image of $0 \in A$ is an open set. From the cocycle condition, the inverse image of 0 is a subgroup as well. Thus f factors through some finite Galois extension M, $\mathrm{Gal}(L/K)^q \to \mathrm{Gal}(M/K)^q$, hence $[f]$ is defined by an element of $\mathrm{H}^q(M/K, A(M))$. □

1.3 Some Galois Modules

The following are all examples of $G = \mathrm{Gal}(L/K)$-modules:

1. The groups $A = \mathbb{Z}$ and $A = \mathbb{Q}/\mathbb{Z}$ with the trivial action.

2. The additive group $A = (L, +)$ of L.

3. The multiplicative group $A = L^*$ of L.

4. When $n \geq 2$, the non-commutatative G-modules $A = \mathrm{GL}_n(L)$ and $\mathrm{SL}_n(L)$.

5. When L is a number field, the ring of integers $\mathcal{O}_L$, the units $\mathcal{O}_L^*$, and the class group $\mathrm{Cl}(\mathcal{O}_L)$ are all G-modules.

6. For E an elliptic curve defined over K, the group $A = E(L)$ of L-rational points.

7. The group $B(L)$, where B ia an abelian variety over K.

8. If S is any (commutative) group scheme over K, then $A = S(L)$ is a (commutative) G-module.

9. For any integer n and any (commutative) A elsewhere in this list, the group $A[n]$ of elements of order dividing n is a G-module.

10. The p-adic Tate module $\mathrm{Tate}_p(A) = \varprojlim A[p^n]$ associated to an abelian variety A.

1.4 The Additive and Multiplicative Groups of a Field

We recall some basic facts from Galois theory. Suppose L/K is a finite Galois extension of fields, which means that $\#\operatorname{Aut}(L/K) = [L : K]$, or equivalently, L is the splitting field of a single irreducible separable polynomial $f \in K[x]$. We write $\operatorname{Gal}(L/K) = \operatorname{Aut}(L/K)$.

Proposition 1.3. *Let L/K be any Galois extension of fields. Then for all $q \in \mathbb{Z}$,*

$$\hat{\mathrm{H}}^q(L/K, L) = 0.$$

Proof. Without loss, we may assume that L is a finite extension of K, since otherwise, we use the result on each finite subextension and take the limit. Since L/K is finite separable, by the normal basis theorem from Galois theory, there exists $\alpha \in L$ such that, letting $K\beta$ denote the 1-dimensional K-vector space spanned by β, we have

$$L = \bigoplus_{\sigma \in \operatorname{Gal}(L/K)} K\sigma(\alpha) \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[\operatorname{Gal}(L/K)]. \tag{1.1}$$

But then L is induced, from which the conclusion follows. □

Proposition 1.4. *Let L/K be any Galois extension of fields. Then*

$$\mathrm{H}^1(L/K, L^*) = 0.$$

Proof. As above, we may assume that L/K is a finite extension. Suppose $f : \operatorname{Gal}(L/K) \to L^*$ is a 1-cocycle. For any $c \in L$, consider the sum

$$b = \sum_{\sigma \in \operatorname{Gal}(L/K)} f(\sigma)\sigma(c).$$

If $b = 0$ for all c, then the elements of $\operatorname{Gal}(L/K)$ are linearly dependent. But in view of Equation (1.1), this would imply that the conjugates of a normal basis element α would generate a field of degree $< [L : K]$, a contradiction. Thus there exists $c \in L$ with $b \neq 0$. Then for any $\sigma \in \operatorname{Gal}(L/K)$, we have

$$0 \neq \sigma(b) = \sum_{\tau} \sigma(f(\tau))\sigma\tau(c) = \sum_{\sigma\tau} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(c) = f(\sigma)^{-1} b,$$

so $f(\sigma) = b\sigma(b)^{-1}$, hence f is a coboundary. □

Theorem 1.5 (Hilbert's Theorem 90)**.** *Suppose* $\operatorname{Gal}(L/K)$ *is finite cyclic, with generator σ. If $\alpha \in L^*$ has norm 1, then there exists $\beta \in L^*$ such that $\alpha = \beta/\sigma(\beta)$.*

Proof. Recall that when G is a finite cyclic group and A is a G-module, then

$$\mathrm{H}^1(G, A) \cong \ker(N_A)/I_G(A).$$

By Proposition 1.4, we have $\mathrm{H}^1(L/K, L^*) = 0$, so the kernel of norm on L^* equals the image of $1 - \sigma \in \mathbb{Z}[\operatorname{Gal}(L/K)]$. Thus α, which is in the kernel of the norm, is of the form $(1 - \sigma)\beta = \beta/\sigma(\beta)$ for some β. (Note that the group ring is written additively, which is why minus changes to inverse.) □

Remark 1.6. Here is an amusing consequence of Theorem 1.5. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Then $\alpha = a + bi \in \mathbb{Q}(i)$ has norm 1 if and only if $a^2 + b^2 = 1$, i.e., (a, b) is a rational point on the unit circle. Theorem 1.5 asserts that there is $\beta = c + di$ such that

$$a + bi = \frac{\beta}{\sigma(\beta)} = \frac{c + di}{c - di} = \frac{(c + di)^2}{c^2 + d^2} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i.$$

This recovers the standard parameterization of rational points on the unit circle.

Later we will study the *Brauer group* of a field K

$$\mathrm{Br}(K) = \mathrm{H}^2(K, (K^{\mathrm{sep}})^*),$$

which can be very large and subtle.

1.5 Upcoming Topics

Kummer theory; the Brauer group; abelian varieties; Lang's theorem; Tate local duality; Global duality; Étale cohomology