Hilbert's theorem 90 and generalizations

Abhishek Parab
Purdue University
aparab@math.purdue.edu

September 24, 2013

Abstract

These notes are based on the Number Theory seminar I gave at Purdue University on September 19, 2013 titled "Hilbert's theorem 90 and generalization". The proof of Hilbert's 90 is taken from an answer I found on MathOverflow at http://mathoverflow.net/a/21117. In the seminar, Professor Goins asked an interesting question about the isomorphism classes of rank one tori which I have blogged here.

1 Non-abelian cohomology

General abstract nonsense says, in an abelian category a half-exact functor $\mathcal{F}$ gives rise to a long exact sequence of (co)homology. In other words, whenever

$$0 \to A \to B \to C \to 0$$

is an exact sequence, giving rise to the exact sequence

$$0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C);$$

then we have

$$0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to H^1(A) \to \cdots .$$

Group cohomology

Let Γ be a group and A, a Γ-module. (So A is an abelian group on which Γ acts.) Denote by A^Γ the set of fixed points of A under the action of Γ. The functor $A \mapsto A^\Gamma$ is left-exact but not right exact, giving rise to the following long-exact sequence of cohomology groups

$$0 \to A^\Gamma \to B^\Gamma \to C^\Gamma \to H^1(\Gamma, A) \to \cdots$$

for an exact sequence $0 \to A \to B \to C \to 0$ of Γ-modules.

We plan to consider a Galois extension L/K with Galois group Γ and $A = G(L)$ for some linear algebraic group G under the obvious (coordinate-wise) action of Γ on $G(L)$. The problem however is when G is not commutative for in this case, cohomology sets aren't defined. We overcome this by using non-abelian cohomology groups $H^0(\Gamma, \circ)$ and $H^1(\Gamma, \circ)$.

Non-abelian cohomology

Let A be a Γ-set, that is, a possibly noncommutative group with an action of Γ. We define

$$H^0(\Gamma, A) = \{a \in A : \gamma.a = a \qquad \forall \gamma \in \Gamma\}$$

A 1-*cocycle* is a map $\sigma \mapsto a_\sigma : \Gamma \to A$ satisfying the condition $a_{\sigma\tau} = a_\sigma.\sigma(a_\tau)$. A 1-*coboundary* is defined for every $x \in A$ by the map $\sigma \mapsto x^{-1}.\sigma(x)$. It is a routine verification that it is a cocycle; so we can define $H^1(\Gamma, A)$ to be the equivalence class of cocycles modulo coboundaries.

One observes that although H^0 is a group (in fact, a subgroup of A), H^1 does not necessarily have the structure of a group. It is however a pointed set so it makes sense to talk of exact sequences of H^1's in the obvious manner.

The general idea in using Galois cohomology is the following.

Fix a finite Galois extension L/K and let Γ be it's Galois group. (We'll talk about L being an infinite extension of K and Γ a profinite group later). For an exact sequence

$$1 \to \mathbf{H} \to \mathbf{G} \to \mathbf{G/H} \to 1$$

of algebraic groups (see Appendix below), we have an exact sequence of pointed sets

$$1 \to \mathbf{H}^\Gamma \to \mathbf{G}^\Gamma \to (\mathbf{G/H})^\Gamma \to H^1(\Gamma, \mathbf{H}) \to H^1(\Gamma, \mathbf{G}) \to H^1(\Gamma, \mathbf{G/H})$$

Appendix: Linear algebraic groups

A *linear algebraic group* over a field K can be thought of as a closed subgroup of $\mathbf{GL}_n(K)$. More generally, it is an affine variety with a group structure so that the group operation maps are actually morphisms of varieties.

An algebraic group can also be thought of as a functor from the category of fields to groups; when considered so it is usually denoted as an *affine group scheme*. The functor $\mathbf{SL}_n$ for example maps a field K into the group of $n \times n$ matrices over K with determinant one.

Two examples of algebraic groups that arise in Hilbert's 90 theorem are $\mathbf{G_a}(K) = K$ and $\mathbf{G_m}(K) = K^*$. An example of an exact sequence of algebraic groups as

mentioned above may be given by

$$1 \longrightarrow \mathbf{SL}_n \longrightarrow \mathbf{GL}_n \xrightarrow{\det} \mathbf{G}_m \longrightarrow 1.$$

2 Proof of Hilbert's 90

Theorem 2.1 (Cohomological version) *L/K is a finite Galois extension of fields and Γ is the Galois group. Then $H^1(\Gamma, L^*) = 0$.*

Theorem 2.2 (Hilbert's Hilbert 90) *Let L/K be a cyclic extension of degree n generated by $\sigma \in \Gamma$. For $y \in L$ of norm 1, there is an $x \in L$ so that*

$$y = \frac{x}{\sigma(x)}.$$

Proof.

First let us see how the cohomological version implies the classical statement. The map $\sigma \mapsto y$ is a cocycle. Since $H^1(\Gamma, L^*) = 0$, it is a coboundary. So this map also is $\sigma \mapsto x^{-1}.\sigma(x)$ for some $x \in L$. Now $x^{-1}.\sigma(x) = y$ so y is of the said form.

A proof of the cohomological statement can be found in Serre's *Galois Cohomology* and below, we give another interesting proof of Hilbert's cyclic version that generalizes to Grothendieck's theory of faithfully flat descent (cf. Emerton's answer on MathOverflow at `http://mathoverflow.net/a/21117`).

To show the existence of $x \in L$ with $y = \dfrac{x}{\sigma(x)}$ is equivalent to showing that the K-linear endomorphism T of L given by $T(x) = y.\sigma(x)$ has a fixed point. This is equivalent to T having an eigenvalue 1. Since eigenvalues don't change on extension of scalars, we can consider T as an endomorphism of the L-vector space L. We show that the tensor product below is an isomorphism and compute the action of T on it.

Claim, $L \otimes_K L \cong \bigoplus_{i=1}^n L$.

By primitive element theorem, $L \cong K[\alpha]$ with α having minimal polynomial $f(x) \in K[x]$. Now

$$L \otimes_K L \cong \frac{K[x]}{f(x)} \otimes_K L \cong \frac{L[x]}{f(x)} \cong \frac{L[x]}{\prod(x - \alpha_i)|} \cong \bigoplus_{i=1}^{n} L.$$

The action of T is given by

$$(x_1, x_2, \cdots, x_n) \mapsto (yx_n, \sigma(y)x_1, \sigma^2(y)x_2, \cdots, \sigma^{n-1}(y)x_{n-1}),$$

which has the fixed point

$$(1,\ y,\ \sigma(y).y, \cdots, \sigma^{n-1}(y)\sigma^{n-2}(y)\cdots\sigma(y)y). \qquad \square$$

A note on infinte Galois extensions

The theorem generalizes to possibly infinite extension L of K wherein the Galois group Γ is profinite. A profinite group is an inverse limit of finite groups. When each group is endowed with the discrete topology, the limit is a compact Hausdorff totally-disconnected group. Also, open normal subgroups form a neighbourhood basis around the identity. (Exercise: Prove that an open subgroup is of finite index in Γ hence closed). (Each of these two properties characterizes profinite groups completely; cf. Theorem 1.1.12 of Ribes & Zalesskii's *Profinite Groups*.)

In our case, Γ is a limit of $\mathrm{Gal}(E/K)$ as E ranges over finite Galois extensions of K inside L. Having proved the statement for finite extensions, the infinite case readily follows since

$$H^1(\Gamma, L^*) \cong \varprojlim H^1(\mathrm{Gal}(E/K), E^*) = 0.$$

In general if Γ is a profinite group, we let A be a Γ-set if the action of Γ is continuous with the discrete topology on A. (This is equivalent to saying that the union of fixed points of A under open subgroups of Γ covers A.) If so we have,

$$H^1(\Gamma, A) \cong \varprojlim_U H^1(\Gamma/U, A^U)$$

with the inverse limit taken over open normal subgroups U of A.

3 Applications

3.1 Pythagorean triplets

Consider the quadratic extension $\mathbb{Q}(i)$ over $\mathbb{Q}$ that has Galois group $\Gamma = \{1, \sigma\}$. Take $y = a + ib$ of norm 1, i.e., $a^2 + b^2 = 1$. By Hilbert's 90, there is a $z \in L$ so that $y = \dfrac{z}{\overline{z}}$. Writing z as $s + it$ with s, t integers gives

$$a + ib = \frac{s + it}{s - it}.$$

Rationalizing the denominator gives all integer solutions to $a^2 + b^2 = 1, \quad a, b \in \mathbb{Q}$ to be

$$a = \frac{s^2 - t^2}{s^2 + t^2}, \quad b = \frac{2st}{s^2 + t^2}; \qquad s, t \in \mathbb{Z}.$$

The above generalizes to finding solution to Brahmagupta-Bhaskaracharya-Pell's equation $a^2 + Db^2 = 1$ when one considers the extension $\mathbb{Q}(\sqrt{-D})$. The solutions are given by

$$a = \frac{s^2 - Dt^2}{s^2 + Dt^2}, \quad b = \frac{2st}{s^2 + DT^2}; \qquad s, t \in \mathbb{Z}.$$

3.2 Kummer theory

$$H^1(\Gamma_{\overline{K}/K}, \mu_n) \cong \frac{K^*}{(K^*)^n} \qquad \text{with } \mu_n \subseteq K^*.$$

Proof. Denote by Γ the absolute Galois group of K. Apply the functor $A \mapsto A^\Gamma$ to the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow L^* \xrightarrow{n} L^* \longrightarrow 1,$$

where the last map is $x \mapsto x^n$. We have the long exact sequence

$$1 \to \mu_n^\Gamma \to (L^*)^\Gamma \to (L^*)^\Gamma \to H^1(\Gamma, \mu_n) \to H^1(\Gamma, L^*) \to \cdots .$$

By Hilbert's 90, the map $(L^*)^\Gamma \to H^1(\Gamma, \mu_n)$ is surjective, q.e.d.

Kummer theory characterizes abelian extensions of K inside $\overline{K}$ of exponent dividing n (i.e., whose Galois group is annihilated by n). Such extensions are classified by $H^1(\Gamma, \mu_n)$ and are in bijection with subgroups of K^* containing $(K^*)^n$.

4 Generalizations to algebraic groups

Let $\mathbf{G}$ be a linear algebraic group (see Appendix to Section 1). We look at $H^1(\Gamma, \mathbf{G})$.

Recollect that (cf. Section 11.3 of Springer's *Linear Algebraic Groups*) two algebraic groups $\mathbf{G}$ and $\mathbf{H}$ defined over K are L/K-forms of each other if they are isomorphic over L.

One application of considering $H^1(\Gamma, \mathbf{G})$ is, that the L/K-forms of $\mathbf{G}$ are classified by $H^1(\Gamma, \mathrm{Aut}(G))$. As an example, we have the correspondence

$$\{\text{Forms of } \mathbf{SL}_n\} \leftrightarrow H^1(\Gamma, \mathrm{Aut}(\mathbf{SL}_n)) \cong H^1(\Gamma, \mathbf{PSL}_n).$$

The additive and multiplicative statement of Hilbert's 90 can be rewritten in terms of algebraic groups as the vanishing of $H^1(\Gamma, \mathbf{G_a}(L))$ and $H^1(\Gamma, \mathbf{G_m}(L))$ respectively. The following theorem generalizes this statement since $\mathbf{GL}_1 = \mathbf{G_m}$.

Theorem 4.1 $H^1(\Gamma, \mathbf{GL}_n(L)) = 1$.

For a proof when K is infinte see III §1.1 of Serre's *Galois Cohomology*.

Using this result, we prove that $H^1(\Gamma, \mathbf{SL}_n(L) = 1$. Consider the exact sequence

$$1 \longrightarrow \mathbf{SL}_n \longrightarrow \mathbf{GL}_n \xrightarrow{\det} \mathbf{G}_m \longrightarrow 1.$$

This gives the exact sequence

$$1 \longrightarrow \mathbf{SL}_n(K) \longrightarrow \mathbf{GL}_n(K) \xrightarrow{\det} \mathbf{G}_m(K) \longrightarrow H^1(\Gamma, \mathbf{SL}_n(L)) \longrightarrow H^1(\Gamma, \mathbf{GL}_n(L) \longrightarrow \cdots .$$

Since $H^1(\Gamma, \mathbf{GL}_n(L))$ vanishes and the determinant map is surjective, it follows that $H^1(\Gamma, \mathbf{SL}_n(L)) = 1$.

Remark

Let L/K be a Galois extension with Galois group Γ. Then $H^1(\Gamma, \mathbf{SP_{2n}}) = 0$. Also, $H^1(\Gamma, \mathbf{O_{2n}})$ is in bijective correspondence with the set of quadratic forms defined over K equivalent over L to x.

The proofs of these statements are obtained from a general principle called 'Galois descent'. See Chapter III §1 of Serre's *Galois Cohomology* for details.