GALOIS COHOMOLOGY OF LINEAR ALGEBRAIC GROUPS

Contents

[This chapter needs a lot of work. For now, we only summarize the results needed in other sections.]

Let G be a linear algebraic group over a field k and k^s be a separable closure of k. There is a natural action of $Gal(k^s/k)$ on the k^s-points of G, and we can define the Galois cohomology group $H^1(k,G)$. In this chapter, we discuss this cohomology group for k is finite, local, or number field. A good reference for this chapter is Chapter 6 of [PR94].

1. Galois cohomology over a finite field

In this section, k is a finite field. The absolute Galois group $Gal(k^s/k) \cong \hat{\mathbb{Z}}$ is a procyclic group. Let φ be the arithmetic Frobenius in $Gal(k^s/k)$. Then φ is a topological generator of $Gal(k^s/k)$ and it induces a k-scheme endomorphism $\varphi_G := id_G \times \varphi$ of G_{k^s}.

Theorem 1.1 (Lang's theorem)**.** *If G is a connected algebraic group over k, then $H^1(k,G) = 1$.*

Proof. We define a k-scheme morphism $f : G \to G$ by

$$f(g) = g^{-1}\varphi(g).$$

To prove Lang's theorem, it suffices to prove that f is surjective.

Considering the action of G on itself by $g.a = g^{-1}a\varphi(g)$. If we fix a, this define a k-scheme endomorphism of G denoted by f_a. In particular, $f_e = f$. We claim that the map f_a is separable and its image is open and closed for any a. Then f is surjective since G is connected. This would complete the proof of Lang's theorem.

Let me prove the claim. We have

$$d_e f_a(X) = -Xa + d_e\varphi_G(X) = -Xa$$

for $X \in T_e(G)$. So the differential map $d_e f_a : T_e(G) \to T_a(G)$ is an isomorphism of the tangent spaces. As a consequence, f_a is dominant and separable. In particular, the orbit $f_a(G)$ contains a nonempty open subset of G, hence is open by homogeneity. Since this holds for any a, $f_a(G)$ are also closed. We are done. □

Lang's theorem has several important corollaries.

Proposition 1.2. *If G is a connected reductive group over k, then G is quasisplit.*

Proof. Let B be a Borel subgroup of G_{k^s}, and let B^φ be the Borel subgroup obtained by applying φ. Then $aB^\varphi a^{-1} = B$ for some a in $G(k^s)$. By the proof of Theorem 1.1, $a = g^{-1}\varphi(g)$ for some g in $G(k^s)$. Now, we consider the Borel subgroup $H = gBg^{-1}$. We can check that H is defined over k by the following computation.

$$H^\varphi = \varphi(g)B^\varphi\varphi(g)^{-1} = gaB^\varphi a^{-1}g^{-1} = H.$$

This completes the proof of this proposition. □

Proposition 1.3 (Lang's isogeny theorem)**.** *If G and H are connected k-groups and $f : G \to H$ is a k-isogeny, then $|G(k)| = |H(k)|$.*

Proof. Let F be the kernel of f. We have a short exact sequence

$$1 \to F(k^s) \to G(k^s) \to H(k^s) \to 1$$

of groups. This exact sequence is compatible with the natural Galois action. Then we obtain an exact sequence

$$\{*\} \to F(k) \to G(k) \to H(k) \to H^1(k, F) \to H^1(k, G)$$

of pointed set. By Theorem 1.1, we have

$$\frac{|H(k)|}{|G(k)|} = \frac{|H^1(k, F)|}{|F(k)|}.$$

So it suffices to show that $|H^1(k, F)| = |F(k)|$. Note that

$$|H^1(k, F)| = \varinjlim H^1(Gal(k_n/k), F(k_n))$$

where k_n is the degree n extension of k. So it is enough to prove that, for each n, $|H^1(Gal(k_n/k), F(k_n))| = |F(k)|$. This is a property of Herbrand quotient (see [AW67, Proposition 11]). This completes the proof. □

Remark 1.4. Lang's theorem can also be used to classify connected reductive groups over a finite field. Let G be a split connected reductive group over k. We fix a based root system Ψ^+ of G. By Theorem 1.1, we have $H^1(k, Aut(G_{k^s})) \cong H^1(k, Aut(\Psi^+))$. So the k-forms of G are classified by the elements of $H^1(k, Aut(\Psi^+))$. We have the following conclusions.

(1) Any k-group of type B_n, C_n, E_7, E_8, F_4 or G_2 is split.
(2) There are exactly two nonisomorphic k-groups of type A_n (where $n > 1$) and D_n (where $n > 4$). The nonsplit one is split over a quadratic extension of k.
(3) There are exactly three nonisomorphic k-groups. The two non-split ones become split over a quadratic and a cubic extension of k respectively.

Theorem 1.5. *If G is a connected algebraic group over a number field K, then G_{K_v} is quasisplit for almost all finite places v of K.*

Proof. See [PR94, Theorem 6.7]. □

Using Lang's theorem we can also deduce a result on Galois cohomology of groups over the ring of integers of a local field. Let K be a local field with ring of integers $\mathcal{O}_K$. Let $G_{\mathcal{O}_K}$ be an algebraic group defined over $\mathcal{O}_K$ and let L be a finite Galois extension of K. The Galois group $Gal(L/K)$ acts naturally on the $\mathcal{O}_L$-point of $G_{\mathcal{O}_K}$. We can define the Galois cohomology group $H^1(L/K, G_{\mathcal{O}_K})$.

Theorem 1.6. *If a connected group $G_{\mathcal{O}_K}$ has a connected smooth reduction $\underline{G_{\mathcal{O}_K}}$ and the extension L/K is unramified, then $H^1(L/K, G_{\mathcal{O}_K}) = 1$.*

Proof. See [PR94, Theorem 6.8]. □

Remark 1.7. Let L be a finite extension of a number field K. By the above theorem, if G is a connected algebraic group over K, then for almost all finite places v of K and any w a place of L above v, we have $H^1(L_w/K_v, G_{\mathcal{O}_{K_v}}) = 1$.

2. Tate–Nakayama duality for tori

3. Cohomology of reductive groups over local fields

Lemma 3.1. *If G is an algebraic group over a local field F, then $H^1(F, G)$ is finite.*

Proof. □

Theorem 3.2. *If G is a (connected) simply connected, semisimple group over a non-Archimedean field F, then $H^1(F, G)$ is trivial. For an arbitrary connected reductive group over a local field F, there is a canonical surjective map [Kottwitz], which in the non-Archimedean case is a bijection.*

Proof. □

4. Cohomology of reductive groups over global fields; the Hasse principle

Definition 4.1. Let G be an algebraic group over a global field k. The kernel of the natural map $H^1(k, G) \to \prod_v H^1(k_v, G)$ is the *Tate–Shafarevich group* of G, denoted Sha(G). We say that G satisfies the *Hasse principle* if Sha$(G) = 1$.

Theorem 4.2. *If G is an algebraic group over a number field, then Sha(G) is finite.*

Proof. □

The following is the Hasse principle for algebraic groups, due to Kneser, Harder (who proved it for groups without E_8 factors) and Chernousov (who completed the E_8 case) over number fields, and to Harder over function fields.

Theorem 4.3. *If G is (connected and) simply connected or adjoint over a global field, then Sha$(G) = 1$.*

Proof. See [PR94, Theorems 6.6] for the number field case, and [PR94, Theorems 6.22] for the reduction of the adjoint case to the simply connected case. The proof for number fields involves a difficult case-to-case analysis. For function fields, there is a general proof due to Harder, [Har75]. □

Proposition 4.4. *If G is a connected algebraic group over a global field k, then $H^1(k, G) \to \prod_{v|\infty} H^1(k_v, G)$ is surjective.*

Proof. See [PR94, Proposition 6.17]. □

5. Other chapters

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR 0219512

[Har75] G. Harder, *Über die Galoiskohomologie halbeinfacher algebraischer Gruppen. III*, J. Reine Angew. Math. **274(275)** (1975), 125–138. MR 382469

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen. MR 1278263