Galois Cohomology of Algebraic Groups

Hang Chen

Dec 2023

Contents

1 Introduction

The goal of this article is to summarize some results related to the Galois cohomology of algebraic groups shown in [1].

Let G be an algebraic group over K and L/K be a finite Galois extension. The Galois group $\mathrm{Gal}(L/K)$ acts on $G(L)$, and then we obtain the group cohomology $H^i(\mathrm{Gal}(L/K), G(L))$, written as $H^i(L/K, G)$. When G is noncommutative, we only consider $H^1(\mathrm{Gal}(L/K), G(L))$, which is explained below. If $M \supset L$ is a larger Galois extension of K, then there is an inflation map $H^i(\mathrm{Gal}(L/K), G) \to H^i(\mathrm{Gal}(M/K), G)$ because $G(M)^{\mathrm{Gal}(M/L)} = G(L)$. Set $H^i(K, G) = \varinjlim H^i(L/K, G)$ where the direct system consists of all finite Galois extensions L/K and the morphisms are inflation maps. Basically, we want to know the information of the cohomology $H^i(K, G)$ for K a finite, local, or global field. Here is a remark for Group cohomology. When G is a group and A is an abelian group as a G-module, $H^i(G, A)$ can be defined as derived functors for each i and they have the structures of abelian groups. When A is a noncommutative group with a group homomorphism $G \to \mathrm{Aut}(A)$ from a discrete or

finite G, A is called a G-group. In this case, $H^1(G, A)$ can also be defined using cocycles. Given an exact sequence of G-groups $1 \to A \to B \to B/A \to 1$, we obtain an exact sequence of sets with a distinguished element

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \to H^1(G, A) \to H^1(G, B) \to H^1(G, B/A).$$

As we concern the Galois cohomology of $G(\bar{K})$ where G is an algebraic group, we shall take this non-abelian cohomology in the usual case of noncommutative G.

In the first section, we display some basic properties and computations of Galois cohomologies. We shall explain that only the Galois cohomology of reductive groups needs to be considered over a field of characteristic 0. Next, we prove Lang's theorem stating that for a connected algebraic group over K where K is finite, $H^1(K, G) = 0$, which has many intriguing corollaries. When we come back to the case of a field of characteristic 0, we work with semisimple groups and tori because every connected reductive group is the almost direct product of a semisimple group and a torus. In the tori case, the Nakayama-Tate theorem is introduced as a generalization of class field theory which connects the cohomology of a torus and the cohomology of its group of characters. In the semisimple case, we demonstrate some major results and the basic idea of calculating the cohomology of semisimple groups with some applications.

There are two topics that we shall pay special attention to. Firstly, the first Galois cohomology can be used to classify K-forms for a field K. To be specific, let L/K be a field extension, and first assume L/K is a finite extension. Let X be an object with an L-structure (a variety, a quadratic form, a central simple algebra, etc. over K). A K-object Y is said to be an L/K-form of X if there is an L-isomorphism $f : X \to Y$. The set of K-isomorphic classes of K-forms of X is denoted by $F(L/K, X)$. One can check $\sigma \mapsto f^{-1}f^{\sigma}$ defines a cocycle in $Z^1(\mathrm{Gal}(L/K), \mathrm{Aut}_L(X))$. Then we have a map $F(L/K, X) \to H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_L(X))$ which can be proven to be a bijection in many examples. By passing to the limit, we can also consider the case $L = \bar{K}$. For example, there is a one-one correspondence between isomorphism classes of central simple algebras over K of dimension n^2 and the elements of $H^1(K, \mathrm{PGL_n})$. Also, the equivalence classes of K-forms of a nondegenerate quadratic n-dimensional form f are classified by $H^1(K, \mathrm{O}_n(f))$.

The second focus is the Hasse principle. 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 called the Tate-Shafarevich group of G, denoted by $\mathrm{Sha}(G)$. An algebraic group G is said to satisfy the Hasse principle if $\mathrm{Sha}(G) = 1$. Since the K-forms of a nondegenerate quadratic n-dimensional form f are classified by $H^1(K, \mathrm{O}_n(f))$ and $\mathrm{SO}_n(f)$ is the identity component of $\mathrm{O}_n(f)$, the Hasse principle for $\mathrm{SO}_n(f)$ implies the weak Hasse principle for f which states that the equivalence

of two K-forms f and g over K can be deduced from the equivalence over all completions K_v.

2 Some Computations

We reformulate Hilbert's Theorem 90 in the language of algebraic groups and obtain $H^1(K, \mathbb{G}_m) = 1$. Moreover, the following lemma holds.

Lemma 2.1. $H^1(K, \mathrm{GL}_n) = 1$.

Proof. Adjust the proof of Hilbert's Thoerem 90 or consider the etale cohomology. □

Lemma 2.2. $H^1(K, \mathrm{SL}_n) = 1$.

Proof. Consider the exact sequence $0 \to \mathrm{SL}_n \to \mathrm{GL}_n \xrightarrow{det} \mathbb{G}_m$. It yields the long exact sequence $\mathrm{GL}_n(K) \xrightarrow{det} K^\times \to H^1(K, \mathrm{SL}_n) \to H^1(K, \mathrm{GL}_n)$. Since *det* is surjective, the statement follows from the above lemma. □

Lemma 2.3. $H^1(K, \mu_n) \simeq K^\times / K^{\times n}$, *and* $H^2(K, \mu_n) \simeq \mathrm{Br}(K)[n]$ *where* $\mathrm{Br}(K)[n] = \{a \in Br(K) \mid n \cdot a = 0\}$.

Proof. Consider the exact sequence $1 \to \mu_n \to \mathbb{G}_m \xrightarrow{\cdot n} \mathbb{G}_m \to 1$ and use Lemma 2.1. □

The next proposition follows from the additive form of Hilbert's Theorem 90.

Proposition 2.4. *Let K be a field of characteristic 0. Then for any unipotent goup U over K, $H^1(K, U) = 1$.*

Proof. The additive form of Hilbert's Theorem 90 asserts that $H^1(K, \mathbb{G}_a) = 1$. Since any unipotent K-group U splits over K, there exists a normal K-subgroup W of U which is isomorphic to $\mathbb{G}_a$. Then the statement follows from induction by dimension. Consider the long cohomological exact sequence associated with $0 \to W \to U \to U/W \to 0$. The statement will hold if it holds for W and U/W which are of lower dimension than U. □

Proposition 2.5. *Let G be a connected algebraic group over K where K is a field of characteristic 0, and let H be a maximal reductive K-subgroup of G. Then the natural map $H^1(K, H) \to H^1(K, G)$ is a bijection.*

Before the proof of the proposition, we first recall the Levi decomposition. The maximal connected unipotent normal subgroup of G is called the unipotent radical of G, denoted by $R_u(G)$.

Theorem 2.6. *Let K be a field of characteristic 0 and G be a connected algebraic group over K. Then there exists a reductive K-subgroup $H \subset G$ such that G is a semidirect product $HR_u(G)$. Moreover, any reductive subgroup H_1 of G is conjugate by an element of $R_u(G)(K)$ to a subgroup of H.*

The decomposition $G = HR_u(G)$ is called the Levi decomposition.

Proof of Proposition 2.5. Let $G = HU$ be the corresponding Levi decomposition. Consider $H \xrightarrow{\phi} G \xrightarrow{\pi} G/U \simeq H$ and the composition is identity. Then we have $H^1(K, H) \xrightarrow{\phi_*} H^1(K, G) \xrightarrow{\pi_*} H^1(K, H)$ and the composition is identity. To show ϕ_* is a bijection, it will suffice to show π_* is an injection. By the exactness of the cohomological sequence $H^1(K, U) \to H^1(K, G) \to H^1(K, H)$ and the fact $H^1(K, U) = 1$ (proven in Proposition 2.4), $\mathrm{Ker}\pi_* = 0$. In noncommutative cohomology, the injection of π_* can not be deduced directly from the triviality of $\mathrm{Ker}\pi_*$, thus a twisting trick is in turn needed. Let g and h be two elements of in $Z(K, G)$ such that $\pi_*(g) = \pi_*(h)$, and let ${}_gG$ be the group obtained from G by twisting g. Then there is a bijection $\tau_g : H^1(K, {}_gG) \to H^1(K, G)$ and $\tau_g^{-1}(h) \in \mathrm{Ker}_g\pi_*$ where ${}_g\pi$ is the projection ${}_g\pi :{}_g G \to {}_g G/{}_gU$. Since $\mathrm{Ker}_g\pi_* = 0$, g and h are in the same cohomological class. Therefore π_* is injective and ϕ_* is bijective. □

One more thing to be mentioned here is the cohomology of groups obtained by restriction of scalars. Let G be an algebraic group over a field L and let $G' = \mathrm{Res}_{L/K} G$ where L/K is a field extension. Then

$$G'(\bar{K}) \simeq G(L \otimes_K \bar{K}) = \prod_{K\text{-algbras morphism } \sigma: L \to \bar{K}} G(\bar{K})^\sigma.$$

Therefore, as a $\mathrm{Gal}(\bar{K}/K)$-module, $G'(\bar{K}) = \mathrm{Ind}_{\mathrm{Gal}(\bar{K}/L)}^{\mathrm{Gal}(\bar{K}/K)} G(\bar{K})$. By Shapiro's lemma, $H^i(K, G') = H^i(L, G)$.

Take $G = \mathbb{G}_m$. There exists a natural norm map $\mathrm{Res}_{L/K} G \to G$. Let $\mathrm{Res}^{(1)}_{L/K} \mathbb{G}_m$ be the kernel of $\mathrm{Res}_{L/K} \mathbb{G}_m \to \mathbb{G}_m$.

Lemma 2.7. $H^1(K, \mathrm{Res}^{(1)}_{L/K} \mathbb{G}_m) \simeq K^\times / N_{L/K}(L^\times)$.

Proof. Consider the exact sequence

$$1 \to \mathrm{Res}^{(1)}_{L/K} \mathbb{G}_m \to \mathrm{Res}_{L/K} \mathbb{G}_m \to \mathbb{G}_m \to 1.$$

The associated long exact sequence is

$$L^\times \xrightarrow{N_{L/K}} K^\times \to H^1(K, \mathrm{Res}^{(1)}_{L/K} \mathbb{G}_m) \to H^1(K, \mathrm{Res}_{L/K} \mathbb{G}_m) \to 1.$$

Because $H^1(K, \mathrm{Res}_{L/K} \mathbb{G}_m) = H^1(L, \mathbb{G}_m) = 1$, the desired formula follows. □

3 Cohomology of Algebraic Groups over a Finite Field

Theorem 3.1 (Lang)**.** *Let G be a connected algebraic group defined over a finite field K. Then $H^1(K, G) = 1$.*

Proof. It suffices to show $H^1(L/K, G) = 1$ for every finite Galois extension L/K. When L/K is a finite extension, $\mathrm{Gal}(L/K)$ has a generator σ, the Frobenius automorphism. Then a cocycle $g = \{g_{\sigma^i}\}$ is uniquely decided by g_σ because $g_{\sigma^i} = g_{\sigma^{i-1}}\sigma(g_\sigma)$. If one can find $x \in G(\bar{K})$ such that $g_\sigma = x^{-1}\sigma(x)$, then $g_{\sigma^i} = x^{-1}\sigma^i(x)$ by induction. Therefore, if we can further show $x \in G(L)$, g is proven trivial. Suppose $[L : K] = n$. Since $\sigma^n = id$, $1 = g_{\sigma^n} = x^{-1}\sigma^n(x)$, which shows that $\sigma^n(x) = x$. So $x \in G(L)$. Then the only thing left is to prove that for every $y \in G(\bar{K})$, there exists $x \in G(\bar{K})$ such that $y = x^{-1}\sigma(x)$, which is guaranteed by Lemma 3.2. □

Lemma 3.2. *If G is a connected K-group, then $g \mapsto g^{-1}f_q(g)$ is surjective, where $q = \#K$ and $f_q : g \mapsto g^{(q)}$ is the Frobenius automorphism.*

Proof. Actually we consider $s_a : g \mapsto g^{-1}af_q(g)$. A basic fact of the Frobenius automorphism is that the differential map $d_x f_q$ is equal to 0 for any x. Then $d_e s_a(X) = -Xa$ for $X \in T_e(G)$. Therefore, the differential map of s_a defines an isomorphism between $T_e(G)$ and $T_a(G)$, and thus s_a is a dominant morphism. So the image of s_a contains an open subset of G. Consider the G-action on G: $G \times G \to G, (g, h) \mapsto g^{-1}hf_q(g)$, then $s_a(G)$ is an orbit. Since all the orbits are open, $s_a(G)$ is also closed. Since G is connected, $s_e(G) = G$ and the statement follows. □

Lang's theorem has abundant corollaries. We discuss them in the rest of this section.

Corollary 3.3. *Let K be a finite field. Then there are no noncommutative finite-dimensional central division algebras over K.*

Proof. The isomorphism classes of central simple algebras over K of dimension n^2 are classified by $H^1(K, \mathrm{PGL_n})$. By Lang's theorem, $H^1(K, \mathrm{PGL_n})$ consists of only one element. Thus, the only central simple algebras over K of dimension n^2 is $M_n(K)$ and it can not be a division algebra when $n > 1$. □

Proposition 3.4. *Let G be a connected group over a finite field K, and let W be a nonempty K-variety with a transitive K-action of G. Then $W(K) \neq \emptyset$. Moreover, if the stabilizer $G(x)$ of a point $x \in W$ is connected, then $G(K)$ acts transitively on $W(K)$.*

Proof. Take $y \in W(\bar{K})$. By transitivity, there exists $g \in G(\bar{K})$ such that $gf_q(y) = y$. By Lemma 3.2, $g = h^{-1}f_q(h)$ for some $h \in G(\bar{K})$. Then $f_q(hy) = hy$, which means $hy \in W(K)$.

For the second assertion, we first consider the general long exact sequence

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

where $A \subset B$ are Γ-groups. Then one can deduce from this sequence that the orbits in $(B/A)^\Gamma$ under the action of B^Γ have a one-one correspondence to the elements in $\ker(H^1(\Gamma, A) \to H^1(\Gamma, B))$. In our case, take $\Gamma = \mathrm{Gal}(\bar{K}/K)$, $B = G(\bar{K})$ and $A = G(x)(\bar{K})$. Then $W(\bar{K}) = B/A$, $(B/A)^\Gamma = W(K)$, and $B^\Gamma = G(K)$. Because $G(x)$ is connected, Lang's theorem shows $H^1(\Gamma, A) = 1$. So $G(K)$ acts transitively on $W(K)$. □

Corollary 3.5. *Let G be a connected group over a finite field K. Then G is K-quasisplit, which means that G has a Borel K-subgroup. Moreover, any two Borel K-subgroups are conjugate by an element of $G(K)$.*

Proof. The corollary follows from taking $W = \mathcal{B}$ in the last proposition, where $\mathcal{B}$ is the variety of all Borel subgroups of G. □

Now we introduce some results about cohomology of algebraic groups over number fields and local fields which can be deduced from Lang's theorem. Let G be an algebraic group over a local field K. Let O be the valuation ring of K and $\mathfrak{B}$ be the maximal ideal of O. Fix a matrix representation $G \hookrightarrow \mathrm{GL}_n$. Define $G(O)$ to be $G(K) \cap \mathrm{GL}_n(O)$. The congruence subgroups are defined as $G(\mathfrak{B}^n) = G \cap (E_n + \mathfrak{B}^n M_n(O))$, and they constitute a base of the neighborhoods of the identity in $G(K)$. If G admits a smooth reduction $G^{(\mathfrak{B})}$ over $O/\mathfrak{B}$, then the Hensel's lemma states that the reduction map $G(O) \to G^{(\mathfrak{B})}(O/\mathfrak{B})$ is surjective.

Theorem 3.6. *Let G be a connected group over a local field K_v and assume that G has a connected smooth reduction $G^{(v)}$. If L_w/K_v is a finite unramified Galois extension, then $H^1(L_w/K_v, G(O_w)) = 1$.*

Proof. Let $\mathfrak{P}_v$ and $\mathfrak{B}_w$ be the maximal ideals of O_v and O_w respectively, and let k_v and l_w be the corresponding residue fields. Consider the exact sequence

$$1 \to G(\mathfrak{B}_w) \to G(O_w) \to G^{(v)}(l_w) \to 1. \tag{3.7}$$

Since L_w/K_v is an unramified extension, $\mathrm{Gal}(L_w/K_v) \simeq \mathrm{Gal}(l_w/k_v)$. Then the long exact sequence associated to (3.7) is

$$\cdots \to H^1(L_w/K_v, G(\mathfrak{B}_w)) \to H^1(L_w/K_v, G(O_w)) \to H^1(l_w/k_v, G^{(v)}(l_w)) \to \cdots. \tag{3.8}$$

We know from Lang's theorem that the last term is trivial. So we only need to establish the triviality of $H^1(L_w/K_v, G(\mathfrak{B}_w))$.

Take $\pi \in \mathfrak{B}_w$ a uniformizer of K. Then the map $\theta : G(\mathfrak{B}_w^n) \to M_n(l_w)$ sending $1 + \pi^n A$ to $\bar{A}$ yields an isomorphism $G(\mathfrak{B}_w^n)/G(\mathfrak{B}_w^{n+1}) \to \bar{\mathfrak{g}} = \overline{\mathfrak{g} \cap M_n(O_w)}$, where $\mathfrak{g}$ is the Lie algebra of G. Thus, $H^1(L_w/K_v, G(\mathfrak{B}_w^n)/G(\mathfrak{B}_w^{n+1})) \simeq H^1(l_w/k_v, \bar{\mathfrak{g}})$. The right-hand side is trivial because of Hilbert's Theorem 90. Using the exact sequence $1 \to G(\mathfrak{B}_w^n)/G(\mathfrak{B}_w^{n+1}) \to G(\mathfrak{B}_w)/G(\mathfrak{B}_w^{n+1}) \to G(\mathfrak{B}_w^n)/G(\mathfrak{B}_w^n) \to 1$, we see $H^1(L_w/K_v, G(\mathfrak{B}_w)/G(\mathfrak{B}_w^n)) = 1$ for any n by induction. Since $G(\mathfrak{B}_w) = \varprojlim G(\mathfrak{B}_w)/G(\mathfrak{B}_w^n)$, we finally have $H^1(L_w/K_v, G(\mathfrak{B}_w)) = 1$. Therefore, the left and right terms of (3.8) are both trivial and so is the middle term $H^1(L_w/K_v, G(O_w))$. □

We shall use Theorem 3.6 to discuss adic cohomology $H^i(L/K, G(\mathbb{A}_L))$. Let L and K be two number fields and $\mathbb{A}_K$, $\mathbb{A}_L$ be their adeles. Since $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$, $\mathrm{Gal}(L/K)$ acts on $\mathbb{A}_L$ via the second factor.

Proposition 3.9. *Let G be a connected group over a number field K and let L/K be a finite Galois extension. Then $H^1(L/K, G_{\mathbb{A}_L})$ can be identified with the subset X of the direct product $\prod_v H^1(L_w/K_v, G)$ consisting of those $x = (x_v)$ for which x_v is trivial for almost all v in V^K.*

Here V^K is the set of all places of K. The direct product $\prod_v H^1(L_w/K_v, G)$ is taken over all $v \in V^K$, and for each v we choose a single extension w in V^L.

Proof. If S is a subset of V^K, let $\bar{S}$ denote the subset of V^L consisting of all extensions to L of valuations in S. Then $G(\mathbb{A}_L) = \bigcup_S G(\mathbb{A}_L(\bar{S}))$, where the union is taken over all finite set S such that for any $v \notin S$, there exists a smooth reduction $G^{(v)}$ and any L_w/K_v is unramified. We have

$$H^1(L/K, G(\mathbb{A}_L(\bar{S}))) = \prod_{v \in S} H^1(L/K, \prod_{w|v} G(L_w)) \times \prod_{v \notin S} H^1(L/K, \prod_{w|v} G(O_w)).$$

Because $\prod_{w|v} G(L_w)$ (resp. $\prod_{w|v} G(O_w)$), as a $\mathrm{Gal}(L/K)$-module, is induced by the $\mathrm{Gal}(L_w/K_v)$-module $G(L_w)$ (resp. $G(O_w)$), we have $H^1(L/K, \prod_{w|v} G(L_w)) = H^1(L_w/K_v, G(L_w))$ (resp. $H^1(L/K, \prod_{w|v} G(O_w)) = H^1(L_w/K_v, G(O_w))$). Since $H^1(L_w/K_v, G(O_w)) = 1$ for $v \notin S$ by Theorem 3.6, we obtain

$$H^1(L/K, G(\mathbb{A}_L(\bar{S}))) = \prod_{v \in S} H^1(L_w/K_v, G) \times \{1\}.$$

As $G(\mathbb{A}_L) = \bigcup_S G(\mathbb{A}_L(\bar{S}))$, the statement follows. □

When G is a commutative group, $H^i(L/K, G)$ can be defined for every positive integer i. The above assertion remains true for any i, and we have $H^i(L/K, G_{\mathbb{A}_L}) \simeq \bigoplus_v H^i(L_w/K_v, G)$. Notice that we do not use the direct sum in the previous proposition because of the non-commutativity.

Proposition 3.10. *Let G be a commutative algebraic group over a number field K, and let L/K be a finite Galois extension. Then for any $i \geq 1$, $H^i(L/K, G_{\mathbb{A}_L}) \simeq \bigoplus_v H^i(L_w/K_v, G)$.*

Proof. We know from the proof of Proposition 3.9 that it will suffice to show that $H^i(L_w/K_v, G(O_v)) = 1$ for almost all v. We may assume that there exists a smooth reduction $G^{(v)}$ and any L_w/K_v is unramified. As L_w/K_v is cyclic, by the periodicity of the cohomology of cyclic groups, we have

$$\begin{aligned} H^i(L_w/K_v, G(O_v)) = H^1(L_w/K_v, G(O_v)) = 1, \quad & \text{for } i \text{ odd}, \\ \textit{and} \quad H^i(L_w/K_v, G(O_v)) = H^2(L_w/K_v, G(O_v)), \quad & \text{for } i \text{ even}. \end{aligned}$$

Thus, we only need to show $H^2(L_w/K_v, G(O_v)) = 1$ holds for almost all v. Consider $1 \to F \to H = \mathrm{Res}_{L/K}(G) \xrightarrow{\text{norm}} G \to 1$. There is an exact sequence

$$\cdots \to H^2(L_w/K_v, H(O_v)) \to H^2(L_w/K_v, G(O_v)) \to H^3(L_w/K_v, F(O_v)) \to \cdots$$

The last term is trivial for almost all v by periodicity and Theorem 3.6. The first term is trivial because $H(O_v)$ is induced. Therefore, $H^2(L_w/K_v, G(O_v)) = 1$ for almost all v. Thus one can argue the same way as in the proof of Proposition 3.9 to show the statement holds. □

4 Cohomology of Tori

Let G be an algebraic group over K. Let $\mathbf{X}(G)$ be the group of characters of G (that is, $\mathbf{X}(G) = \{\chi : G \to \mathbb{G}_m\}$), and $\mathbf{X}_*(G)$ be the group of cocharacters of G (that is, $\mathbf{X}_*(G) = \{\chi : \mathbb{G}_m \to G\}$). Then $\mathrm{Gal}(\bar{K}/K)$ acts on both $\mathbf{X}(G)$ and $\mathbf{X}_*(G)$, and the bilinear form $\mathbf{X}_*(G) \times \mathbf{X}(G)$ is compatible with the action. Let $\mathbf{X}(G)_K$ (resp. $\mathbf{X}(G)_{*K}$) be the group of characters (resp. cocharacters) over K. One fundamental property of algebraic tori is that $T \mapsto \mathbf{X}(T)$ is a contravariant category equivalence from the category of tori over K to the category of finite generated torsion-free $\mathbb{Z}$-modules with $\mathrm{Gal}(\bar{K}/K)$-actions. So one naturally wants to know the relationship between $H^i(K, T)$ and $H^i(K, \mathbf{X}(T))$. It is answered by one main result of this section when K is a local field. Note that if L is a splitting field for T, then

$$H^1(K, T) = H^1(L/K, T), \quad \text{and} \quad H^1(K, \mathbf{X}(T)) = H^1(L/K, \mathbf{X}(T)). \tag{4.1}$$

Theorem 4.2 (Takayama-Tate, local version)**.** *Let K be a local field. Then for every K-torus T with splitting field L and every $i \in \mathbb{Z}$, there is an isomorphism $\hat{H}^i(L/K, T) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T))$.*

The global version of the Takayama-Tate theorem, like the global class field theory, uses adele class group $C_L(T) = T(\mathbb{A}_L)/T(L)$ to substitute T.

Theorem 4.3 (Takayama-Tate, global version)**.** *Let K be a number field. Then for every K-torus T with splitting field L and every $i \in \mathbb{Z}$, there is an isomorphism $\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T))$.*

One remark is that the isomorphisms in the above two theorems are not natural or canonical, which will be seen in the proof.

We first introduce the Tate cohomology $\hat{H}^i(L/K, G)$. Let G be a finite group and let A be a G-module. Define the norm map $N : A \to A$ sending a to $\sum_{g \in G} ga$. Let A' be the submodule of A generated by elements of the form $ga - a$ for $g \in G, a \in A$. Then Tate cohomology groups $\hat{H}^i(G, A)$ $(i \in \mathbb{Z})$ are defined as follows:

$$\begin{aligned}
&\hat{H}^i(G, A) = H^i(G, A), \quad \text{if } i \geq 1,\\
&\hat{H}^i(G, A) = A^G/N(A),\\
&\hat{H}^i(G, A) = \mathrm{Ker}N/A',\\
&\hat{H}^i(G, A) = H_{-i}(G, A), \quad \text{if } i \leq -2.
\end{aligned}$$

We first show that the results in the cases $T = \mathbb{G}_m$ and $i = 0, 1, 2$ follow from the class field theory, and then prove the general case. The main theorem used in the proof is also the key ingredient in the proof of class field theory.

If $T = \mathbb{G}_m$, then $\mathbf{X}(T) = \mathbb{Z}$. We first discuss the case K is a local field. For $i = 0$, we have $\hat{H}^0(L/K, \mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$ and $H^2(L/K, L^\times) \simeq \mathrm{Br}(L/K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. The canonical isomorphism $\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is given by mapping a simple algebra to its invariant. The inverse image of $\frac{1}{n}$ is called the fundamental class of L/K, denoted by $u_{L/K}$. If F is an intermediate subfield, then $u_{L/F}$ is the image of $u_{L/K}$ under the restriction map $H^2(L/K, L^\times) \to H^2(L/F, L^\times)$.

For $i = 1$, $\hat{H}^1(L/K, L^\times)$ and $\hat{H}^1(L/K, \mathbb{Z})$ are both trivial.

For $i = 2$, $\hat{H}^2(L/K, \mathbb{Z}) \simeq \hat{H}^1(L/K, \mathbb{Q}/\mathbb{Z})$. (To show this, one can consider $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ and notice $H^i(G, \mathbb{Q}) = 0$ for a finite group G and $i > 0$.) We have $\hat{H}^1(L/K, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Gal}(L/K)^{\mathrm{ab}}$ by a direct calculation of Tate cohomology and $\hat{H}^0(L/K, L^\times) = K^\times/N_{L/K}(L^\times)$ by definition. The main result of local class field theory asserts that $K^\times/N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)^{\mathrm{ab}}$.

When K is a global field, the cases $T = \mathbb{G}_m$, $i = 0, 1, 2$ again follow directly from global class field theory. Here $L^\times$ is replaced by the idele class group $C_L = J_L/L^\times$. For $i = 0$, as in the local case, there is a canonical isomorphism $H^2(L/K, C_L) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and the inverse image of $\frac{1}{n}$ is the fundamental class of L/K, written as $u_{L/K}$. For $i = 1$, we have to establish that $H^1(L/K, C_L)$ is trivial. Consider $1 \to L^\times \to J_L \to C_L \to 1$. Then the triviality follows from Albert–Brauer–Hasse–Noether theorem, which states that $H^2(L/K, L^\times) = \mathrm{Br}(L/K) \to \sum \mathrm{Br}(L_w/K_v) = H^2(L/K, J_L)$ is injective. Case $i = 2$ follows from $\mathrm{Gal}(L/K)^{\mathrm{ab}} \simeq C_K/N_{L/K}(C_L)$.

To prove the general case, we exploit the following Tate's theorem.

Theorem 4.4 (Tate)**.** *Let G be a finite group, M be a G-module and u be an element of $H^2(G, M)$. Assume that for each prime number p and each Sylow p-subgroup of G, the following conditions are satisfied:*

(1) $H^1(G_p, M) = 1$,

(2) $H^2(G_p, M)$ *is a cyclic group of the same order as* G_p *with* $\mathrm{Res}^G_{G_p}(u)$ *being a generator, where* $\mathrm{Res}^G_{G_p} : H^2(G, M) \to H^2(G_p, M)$ *is the restriction morphism.*

Then for any torsion-free finitely generated G-module N and any subgroup H of G, the cup product with u induces an isomorphism $\hat{H}^i(H, N) \to \hat{H}^{i+2}(H, M \otimes N)$.

Proof of Theorem 4.2. In fact, we have a $\mathrm{Gal}(L/K)$-module isomorphism $\theta : \mathbf{X}_*(T) \otimes L^\times \to T(L)$. The morphism is defined in an obvious way: $\theta(\varphi \otimes x) = \varphi(x)$. Also, the isomorphism and the compatibility of $\mathrm{Gal}(L/K)$-actions on both sides are easy to check. Therefore, we take $M = L^\times$ and $u = u_{L/K} \in H^2(L/K, L^\times)$ in Tate's theorem, and obtain the isomorphisms

$$\hat{H}^i(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{i+2}(L/K, \mathbf{X}_*(T) \otimes L^\times) \simeq \hat{H}^{i+2}(L/K, T(L)). \tag{4.5}$$

Since there is a perfect pairing $\mathbf{X}_*(T) \times \mathbf{X}(T) \to \mathbb{Z}$, the duality theorem for cohomology implies $\hat{H}^i(L/K, \mathbf{X}_*(T))$ and $\hat{H}^{-i}(L/K, \mathbf{X}(T))$ are dual as finite abelian groups and are thus isomorphic. The statement then follows. □

As shown in the proof, isomorphism (4.5) involving the group of cocharacters is canonical. But as the construction of the isomorphism in Theorem 4.2 includes a duality, it is not canonical.

The proof of Theorem 4.3 is totally paralleled. One must take $M = C_L$ and $u = u_{L/K}$ in Tate's theorem. There is also an isomorphism $\mathbf{X}_*(T) \otimes C_L \simeq C_L(T)$.

The relationship between local and global Takayama-Tate theorems is described by the following commutative diagram:

$$\begin{array}{ccc} \hat{H}^i(L_w/K_v, T) & \xrightarrow{\tau} & \hat{H}^i(L/K, C_L(T)) \\ \uparrow & & \uparrow \\ \hat{H}^i(L_w/K_v, \mathbf{X}_*(T)) & \xrightarrow{\alpha} & \hat{H}^i(L/K, \mathbf{X}_*(T)) \end{array}$$

where α is the corestriction map $\mathrm{Cor}^{\mathrm{Gal}(L/K)}_{\mathrm{Gal}(L_w/K_v)}$, and τ is given by the composition $\hat{H}^i(L_w/K_v, T) \simeq \hat{H}^i(L/K, T(K_v \otimes_K L)) \to \hat{H}^i(L/K, C_L(T))$ in which the last morphism is induced by $T(K_v \otimes_K L) \to T(\mathbb{A}_K \otimes_K L) = T(\mathbb{A}_L) \to C_L(T)$.

Now we pass to discuss the Hasse principle. Let T be a torus defined over a number field K. As we established in Proposition 3.10, $\hat{H}^i(L/K, T(\mathbb{A}_L)) \simeq \bigoplus_v \hat{H}^i(L_w/K_v, T)$. It can be easily checked that the image of $H^i(L/K, T) \to \prod_v H^i(L_w/K_v, T)$ lies in $H^i(L/K, T(\mathbb{A}_L))$. Thus, the kernel $P^i(L/K, T) = \mathrm{Ker}(\hat{H}^i(L/K, T) \to \bigoplus_v \hat{H}^i(L_w/K_v, T))$ is equal to the kernel of $\hat{H}^i(L/K, T) \to \hat{H}^i(L/K, T(\mathbb{A}_L))$, and is therefore a quotient group of $\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{3-i}(L/K, \mathbf{X}(T))$. Because $\hat{H}^i(L/K, \mathbf{X}(T))$ is a finite generated abelian group killed by an integer, it is finite, and we have the following proposition.

Proposition 4.6. *Let T be an algebraic torus defined over K that splits over a finite Galois extension L of K. Then the following hold for every i:*

(1) $H^i(L/K, T)$ is finite when K is a local field.

(2) $P^i(L/K, T) = \mathrm{Ker}(\hat{H}^i(L/K, T) \to \bigoplus_v \hat{H}^i(L_w/K_v, T))$ is finite when K is a number field.

Considering (4.1), we have the following corollary.

Corollary 4.7. *Keep the assumptions in Proposition 4.6. Then*

(1) if K is local, $H^i(L/K, T)$ is finite;

(2) if K is a number field, the Tate-Shafarevich group $\mathrm{Sha}(T)$ is finite.

The finiteness theorems hold for arbitrary algebraic groups, and the results are quoted here.

Theorem 4.8. *Let G be an algebraic group over a field K. Then the following hold:*

(1) if K is local, $H^1(K, G)$ is finite;

(2) if K is a number field, the Tate-Shafarevich group $\mathrm{Sha}(G)$ is finite.

The following theorem shows how to compute $P^i(L/K,T)$ with the cohomology groups of $\mathbf{X}(T)$.

Theorem 4.9. *We have*

$$P^i(L/K,T) \simeq \mathrm{Ker}(\hat{H}^{3-i}(L/K,\mathbf{X}(T)) \to \prod_v \hat{H}^{3-i}(L_w/K_v,\mathbf{X}(T))).$$

Proof. Consider the long exact sequence associated to $1 \to T(L) \to T(\mathbb{A}_L) \to C_L(T) \to 1$:

$$\hat{H}^{i-1}(L/K,T(\mathbb{A}_L)) \xrightarrow{g} \hat{H}^{i-1}(L/K,C_L(T)) \to \hat{H}^i(L/K,T) \xrightarrow{f} \hat{H}^i(L/K,T(\mathbb{A}_L)).$$

Then $P^i(L/K,T) = \mathrm{Ker}f = \mathrm{Coker}g$. As

$$\hat{H}^{i-1}(L/K,T(\mathbb{A}_L)) = \bigoplus_v \hat{H}^{i-1}(L_w/K_v,T) \simeq \bigoplus_v \hat{H}^{i-3}(L_w/K_v,\mathbf{X}_*(T))$$

and $\hat{H}^{i-1}(L/K,C_L(T)) \simeq \hat{H}^{i-3}(L/K,\mathbf{X}_*(T))$, we obtain

$$P^i(L/K,T) \simeq \mathrm{Coker}(\bigoplus_v \hat{H}^{i-3}(L_w/K_v,\mathbf{X}_*(T)) \to \hat{H}^{i-3}(L/K,\mathbf{X}_*(T))).$$

We get the desired formula by dualizing it. □

Example 4.10 (Hasse Norm Principle)**.** Let P be a field extension of a number field K. Let $T = \mathrm{Res}^{(1)}_{P/K}(\mathbb{G}_m)$. We have calculated in Lemma 2.7 that $H^1(K,T) \simeq K^\times/N_{P/K}(P^*)$. Similarly, $H^1(K,T(\mathbb{A})) \simeq J_K/N_{P/K}(J_P)$. So $\mathrm{Sha}(T) \simeq (K^\times \cap N_{P/K}(J_P))/N_{P/K}(P^*)$. The Hasse norm principle is said to be satisfied by the extension P/K if $K^\times \cap N_{P/K}(J_P) = N_{P/K}(P^*)$, which is equivalent to $\mathrm{Sha}(T) = 0$.

From the definition of T, we have the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[\mathrm{Gal}(P/K)] \to \mathbf{X}(T) \to 0$. Passing to cohomology, we have $H^2(P/K,\mathbf{X}(T)) \simeq H^2(P/K,\mathbb{Z})$ because $H^i(P/K,\mathbb{Z}[\mathrm{Gal}(P/K)]) = 0$. So we now obtain the following formula:

$$\mathrm{Sha}(T) \simeq \mathrm{Ker}(H^3(P/K,\mathbb{Z}) \to \prod_v H^3(P_w/K_v,\mathbb{Z})).$$

Then we arrive at the Hasse norm theorem which states that the local-global norm principle holds for a cyclic extension P/K. This is because if P/K is cyclic, then $H^3(P/K,\mathbb{Z}) = 0$ and we can use the above formula.

5 Cohomology of Semisimple Groups

In this section, we just present some main results and discuss how they are applied to compute the cohomology and utilized in other applications.

Over the finite fields, Lang's theorem shows that the first cohomology always vanishes. When we try to compute the cohomology of semisimple groups over a (non-Archimedean) local field, while the cohomology does not vanish for a general semisimple group, it vanishes in the case of simply connected semisimple groups.

Theorem 5.1. *Let G be a simply connected semisimple group over a non-Archimedean local field K. Then $H^1(K, G) = 1$.*

Let us recall some facts related to semisimple groups. If G is a semisimple algebraic group over K, then it admits a universal K-covering $\tilde{G} \xrightarrow{\pi} G$ from a simply connected semisimple K-group $\tilde{G}$. The kernel of π is the fundamental group F lying in the centre of $\tilde{G}$. Passing to cohomology, we obtain the exact sequence $H^1(K, \tilde{G}) \to H^1(K, G) \xrightarrow{\delta} H^2(K, F)$. So it is natural to study δ and compute $H^2(K, F)$.

Theorem 5.2. *The map δ is bijective when K is a local field and surjective when K is a number field.*

Thus, in particular, when K is a non-Archimedean local field, it will suffice to compute $H^2(K, F)$. As the centres of simple groups can be totally classified and F is contained in the centre, we can complete the computation in this way.

As for the Hasse principle, it also holds for simply connected groups.

Theorem 5.3. *The map $H^1(K, G) \to \prod_v H^1(K_v, G)$ is bijective for every simply connected K-group G.*

Theorem 5.3 seems slightly different from our former focus on the injectivity of the map, but the next proposition shows that for connected groups, the surjectivity comes for free.

Proposition 5.4. *The map $H^1(K, G) \to \prod_v H^1(K_v, G)$ is surjective for every connected K-group G.*

It can be deduced from Theorem 5.3 and the exact sequence $1 \to F \to \tilde{G} \to G \to 1$ that the Hasse principle holds for G if

$$H^2(K, F) \to \prod_v H^2(K_v, F) \tag{5.5}$$

is injective. To show this, one can consider the exact cohomological sequence induced by $1 \to F \to \tilde{G} \to G \to 1$ and use the five lemma. We can base on this consideration to establish the Hasse principle for adjoint groups.

Theorem 5.6. *Let G be a semisimple adjoint group over a number field K. Then we have* $\mathrm{Sha}(G) = 1$.

This can also be used to show the weak Hasse principle for nondegenerate quadratic forms mentioned in the introduction.

Example 5.7 (Weak Hasse Principle for Quadratic Forms)**.** Let f be a nondegenerate n-dimensional quadratic form over a number field K. The equivalent classes of K-forms are classified by $H^1(K, \mathrm{O}_n(f))$. However, $\mathrm{O}_n(f)$ is not connected and its identity component is $\mathrm{SO}_n(f)$. Notice $1 \to \mathrm{SO}_n(f) \to \mathrm{O}_n(f) \xrightarrow{d} \mu_2 \to 1$. We have calculated $H^1(K, \mu_2) \simeq K^\times/K^{\times 2}$ in Lemma 2.3. It can be checked that if g is a K-form of f and is considered as an element of $H^1(\mathrm{O}_n(f))$, then its image under the map $H^1(\mathrm{O}_n(f)) \to H^1(K, \mu_2) \simeq K^\times/K^{\times 2}$ is just $d(g)/d(f)$, where d maps a form to its discriminant. If f and g are equivalent over all K_v, then $d = d(g)/d(f)$ is a square in every K_v. Thus d is a square in K. Consequently, the class of $H^1(K, \mathrm{O}_n(f))$ corresponding to g maps to zero in $H^1(K, \mu_2)$, and thus it lies in the image of $\mathrm{SO}_n(f)$. After a little diagram chasing, we know it suffices to prove that $H^1(K, \mathrm{SO}_n(f)) \to \prod_d H^1(K_v, \mathrm{SO}_n(f))$ is injective, which means the Hasse principle holds for $\mathrm{SO}_n(f)$. When $n \geq 3$, $\mathrm{SO}_n(f)$ is a semisimple group with fundamental group $F \simeq \mu_2$. When $F = \mu_2$, (5.5) is injective. Then the remark before Theorem 5.6 shows that Hasse principle holds for $\mathrm{SO}_n(f)$. Therefore, the weak Hasse principle holds if $n \geq 3$.

References

[1] V. Platonov, A. Rapinchuk, and R. Rowen. *Algebraic Groups and Number Theory.* Pure and Applied Mathematics. Elsevier Science, 1993.