SOME REMARKS ON GALOIS COHOMOLOGY AND LINEAR ALGEBRAIC GROUPS

BY CONNOR HALLECK-DUBÉ

This expository note came from my attempts to reconcile some standard classical results in Galois cohomology, as in [Ser94], with modern geometric language and descent theory, as in [Ols16]. Isomorphism classes of fppf principal G-bundles, for example, can still be classified by the naive Galois cohomology set under mild assumptions. We will for the most part restrict to affine algebraic groups, with visions towards reductive groups over fields. By "fppf site" we always mean the large site, by "étale site" we always mean the small site. Most results we prove on the fppf site also hold on the fpqc site.

I. H^1 and Principal G-bundles

To summarize the results of this section, there are three closely related types of objects for G/k an algebraic group:

(1) Galois cohomology classes in $H^1(\mathrm{Gal}(k_s/k), G(k_s))$,
(2) principal G-bundles, and
(3) G-torsors.

There is a natural map from each to the next. The first two are in bijection if G is smooth (so that principal G-bundles split over k_s), and the latter two are in bijection if e.g. G is affine (so that we can descend each torsor to a principal G-bundle).

I.1. **Torsors and bundles.**

We recall the definitions of torsors and principal bundles on the fppf site.

Definition 1. Let G an fppf group scheme over X, and write $\mathcal{G}$ for its functor of points, an fppf-group sheaf. A *torsor* for G on X is an sheaf of sets $\mathcal{P}$ on X with a right action by $\mathcal{G}$ satisfying

(1) (local triviality) there exists an fppf cover $\{X_i \to X\}$ such that $\mathcal{P}(X_i) \neq \emptyset$ for all i, and
(2) (simple transitivity) the map of sheaves

$$\begin{aligned} \mathcal{P} \times \mathcal{G} &\longrightarrow \mathcal{P} \times \mathcal{P} \\ (p, g) &\longmapsto (p, pg) \end{aligned}$$

is an isomorphism. Note the second condition ensures that whenever $\mathcal{P}(S) \neq 0$, $\mathcal{G}(S)$-acts simply transitively on $\mathcal{P}(S)$.

More classically, a *principal G-bundle on X* is an fppf X-scheme $P \to X$ with a right G-action by morphisms of X-schemes such that the morphism $P \times_X G \to P \times_X P$ functorially given by $(p, g) \mapsto (p, pg)$ is an isomorphism. Morphisms of torsors and principal G-bundles are defined in the obvious ways.

Given a principal G-bundle $P \to X$, its functor of points $\mathcal{P}$ in the category of X-schemes is clearly a torsor: the action map passes to the functors of points, and since $P \to X$ is fppf, the sheaf is fppf-locally trivial (for example, $\mathcal{P}(P) \neq \emptyset$). The two simple transitivity conditions correspond. Indeed, since all we have done is apply the Yoneda embedding, we have a fully faithful functor

$$(G\text{-bundles on } X) \longrightarrow (\mathcal{G}\text{-torsors on } X).$$

In order for this to be an equivalence, we need something to let us descend local representability along a trivializing open cover, i.e. some hypothesis guaranteeing effective descent. For example, we have the following.

Proposition 2. *If $G \to X$ is (quasi-)affine, then the Yoneda map above is an equivalence of categories.*

Proof. It remains only to prove essential surjectivity, i.e. that every G-torsor $\mathcal{P}$ on X is representable. Choosing a trivializing open cover $\{X_i \to X\}$, the restrictions $\mathcal{P}|_{X_i}$ are representable by affine schemes $P_i = G|_{X_i} \to X_i$ (noncanonically – one has to choose a section over X_i). Since the $\mathcal{P}|_{X_i}$ glue to give a global sheaf, they give descent data for the P_i, which is effective by fppf descent for (quasi-)affine morphisms (see [Ols16, Thm. 4.4.9, 4.4.17]). □

If the group G is smooth, then studying principal bundles reduces to the étale site. We can define an *étale principal G-bundle* similarly to the above, replacing condition (1) with the existence of an étale trivializing cover. Note these are still sheaves for the full fppf (or even fpqc) site, only the local triviality condition has changed.

Lemma 3. *Every smooth morphism $f : Y \to X$ étale-locally has a section.*

Proof. Recall that every smooth morphism is locally "étale over affine," that is, for any $y \in Y$ there exists $f(y) \in U \subset X$ and $y \in V \subset f^{-1}(U)$ such that $f|_U$ factors as $V \xrightarrow{\pi} \mathbb{A}^n_U \to U$, with π étale [Sta22, Tag 039P]. Take an arbitrary section $U \to \mathbb{A}^n_U$, for example the zero section, and pull back π along it to obtain an étale map $V_{f(y)} := U \times_{\mathbb{A}^n_U} V \to U$ which also has a map to X. Doing this for each point in the image and taking the disjoint union gives an étale cover of X and a section of the pullback of f. □

Proposition 4. *Let $G \to X$ smooth. The natural inclusion defines an equivalence of categories between étale principal G-bundles and fppf principal G-bundles.*

Proof. Let $P \to X$ be an fppf G-bundle. Then the structure morphism is smooth: smoothness is an fppf-local property, so can be checked after the trivializing base change along $P \to X$ itself. By the lemma below, every smooth X-scheme has a section étale-locally on the base, so every fppf G-bundle is actually étale-locally trivial. This shows the natural inclusion (which is certainly fully faithful) is essentially surjective. □

Remark 5. The same reduction works for torsors when G is smooth but not affine (so torsors and bundles don't coincide). The argument uses a theorem of Artin that every fppf G-torsor for G smooth is representable by an algebraic space, then uses that smooth morphisms of algebraic spaces étale-locally have sections.

II. Galois Classification of Torsors

Now assume $X = \operatorname{Spec} k$ and G an algebraic group on X (that is, a finite type group scheme over k). We expect to be able to classify principal G-bundles in terms of some kind of cohomology, but since G is not abelian, the framework of cohomology on the fppf or étale site does not directly apply. Given that the topos-theoretic "points" of the flat site are difficult to work with (see [Sta22, 06VW] [Sch14] for some discussion), it is unclear what a generalization of Galois cohomology would look like and would likely be very difficult to compute with. For these reasons it is valuable to work with the naïve nonabelian Galois cohomology.

Recall the cochain definition of the noncommutative cohomology (pointed) set $H^1(\mathrm{Gal}(k_s/k), G(k_s))$: the cocycles are locally constant maps $\mathrm{Gal}(k_s/k) \to G(k_s)$ denoted $s \mapsto a_s$ with the property that $a_{st} = a_s s(a_t)$, and another such cocycle $s \mapsto a'_s$ is cohomologous if $a'_s = b^{-1} a_s s(b)$ for all s. We define H^1 as the quotient by this equivalence relation.

Proposition 6. *If G is a smooth affine algebraic group, there is a natural isomorphism between $H^1(\mathrm{Gal}(k_s/k), G(k_s))$ and the set $\mathrm{Bun}_G(k)$ of isomorphism classes of fppf principal G-bundles (= G-torsors) on $\operatorname{Spec} k$.*

Proof. The map $\mathrm{Bun}_G(k) \longrightarrow H^1(\mathrm{Gal}(k_s/k), G(k_s))$ sends a principal G-bundle $P \to \operatorname{Spec} k$ to a cocycle as follows: the base change P_{k_s} is isomorphic to G_{k_s}, hence has a k_s-point. Choosing $x_0 \in P(k_s)$ arbitrarily, $G(k_s)$ acts simply transitively on $P(k_s)$, so we obtain a cocycle by

$$s \longmapsto \text{ the unique } a_s \in G(k_s) \text{ such that } s(x_0) = x_0 a_s.$$

This is indeed a cocycle since

$$x_0 a_{st} = s(t(x_0)) = s(x_0 a_t) = x_0 a_s s(a_t).$$

Changing our choice of base-point x_0 would give a cohomologous cocycle, so we obtain a well-defined class in $H^1(\mathrm{Gal}(k_s/k), G(k_s))$.

Conversely, given a cocycle $s \mapsto a_s$, we will build a k-scheme by descending G_{k_s} along twisted descent data. First we reduce to finite level by noting that

$$H^1(\mathrm{Gal}(k_s/k), G(k_s)) = \varinjlim_{L/k \text{ finite Galois}} H^1(\mathrm{Gal}(L/k), G(L)) \tag{1}$$

where the maps in the directed system are, for $E/L/k$ all Galois, given by pre- and post-composition:

$$(a : \mathrm{Gal}(L/k) \to G(L)) \longmapsto \left(\mathrm{Gal}(E/k) \to \mathrm{Gal}(L/k) \xrightarrow{a} G(L) \to G(E)\right).$$

The equality (1) holds because a cocycle is by definition a continuous map from a compact group to a discrete group, hence has finite image and factors through a finite quotient, and $G(k_s)$ is a continuous (noncommutative) $\mathrm{Gal}(k_s/k)$-module, i.e. every point is contained in some $G(L)$ for L/k finite Galois. The principal G-bundle we build below will not depend upon our choice of L.[1]

Base change from k to L equips G_L with descent data, which we work to simplify from the general fibered descent formalism down to semilinear Galois automorphisms. This paragraph may be safely omitted if the reader is willing to take on faith that descent data for L/k is a collection of semi-L-linear automorphisms on G_L. Abstract descent data as defined in [Ols16, Ch. 4] is an isomorphism (which here exists by associativity of base change)

$$\sigma : G_L \times_{L,\pi_1} (L \otimes_k L) = G \times_k (L \otimes_k L) = G_L \times_{L,\pi_2} (L \otimes_k L),$$

This clearly satisfies the descent condition ("agreeing on triple overlaps") since all possible base changes to $L \otimes_k L \otimes_k L$ are the same:

$$\begin{array}{ccccc} \pi_{12}^\star \pi_1^\star G_L & \xrightarrow{\pi_{12}^\star \sigma} & \pi_{12}^\star \pi_2^\star G_L & = & \pi_{23}^\star \pi_1^\star G_L \\ \| & & & & \downarrow{\scriptstyle \pi_{23}^\star \sigma} \\ \pi_{13}^\star \pi_1^\star G_L & \xrightarrow{\pi_{13}^\star \sigma} & \pi_{13}^\star \pi_2^\star G_L & = & \pi_{23}^\star \pi_2^\star G_L \end{array}$$

In this diagram, pullback means base change, and the various π's represent the projections

$$\mathrm{Spec}(L \otimes_k L \otimes_k L) \to \mathrm{Spec}(L \otimes_k L) \quad \text{and} \quad \mathrm{Spec}(L \otimes_k L) \to \mathrm{Spec}\, L$$

onto the appropriate factors. Since L/k is finite Galois, fix a presentation $L = k[x]/(f(x))$ (that is, a primitive element l_0). Then the roots of f in L are exactly the $s(l_0)$ for $s \in \mathrm{Gal}(L/k)$. Expanding the right factor with respect to this power basis and applying the Chinese Remainder Theorem gives an isomorphism $L \otimes_k L \cong \prod_{s \in \mathrm{Gal}(L/k)} L$ as L-algebras (with the L-action on the left factor of the tensor and diagonal in the product), so $G_L \times_{L,\pi_1} (L \otimes_k L) \cong \bigsqcup_{s \in \mathrm{Gal}(L/k)} G_L$. The other pullback is less obvious: an element $1 \otimes l \in L \otimes L$ acts on the product along the CRT map

$$L[x]/(f(x)) = \prod_{s \in \mathrm{Gal}(L/k)} L[x]/(x - s(l_0)),$$

that is, it acts on the s-th factor by multiplication by its i-th conjugate. So we again have

$$G_L \times_{L,\pi_2} (L \otimes_k L) = \bigsqcup_{s \in \mathrm{Gal}(L/k)} G_L,$$

but the map between these two pullbacks is $\bigsqcup_s s$, that is, it acts on the s-factor by the morphism $s : G_L \to G_L$ given by naturality of base change. So the descent data for L/k indeed consists of the family of semilinear group automorphisms on G_L induced by the Galois group. The compatibility condition, translated into this language, just says that the map $\mathrm{Gal}(L/k) \to \mathrm{Aut}(G_L)$ is a group homomorphism.

Now we show that we can twist our descent data by the cocycle $s \mapsto a_s \in G(L)$ to obtain another descent data: define a new action ρ of $\mathrm{Gal}(L/k)$ on G_L by composing the old action with left-multiplication by a_s: that is, on R-points define $\rho(s)(g) = a_s s(g)$. Since the a_s are a cocycle, we have on R-points

$$\rho(st)(x) = a_{st} st(x) = a_s s(a_t t(x)) = \rho(s)\rho(t)(x)$$

so the $\rho(s)$ form a collection of semilinear automorphisms of G_L compatible with composition. Reversing the argument of the previous paragraph, this family translates into descent data for G_L. Since $\mathrm{Spec}\, L \to \mathrm{Spec}\, k$

[1] It is possible that one could directly apply fpqc descent to avoid some of these finiteness arguments, but interpreting the descent data for $k \to k_s$ is more difficult because $k_s \otimes_k k_s \neq \prod_{\mathrm{Gal}(k_s/k)} k_s$.

is fppf and G_L is affine, the descent data is automatically effective. So there is an affine scheme $P \to \operatorname{Spec} k$ whose base change to L gives G_L with this descent data.

To show that $P \to \operatorname{Spec} k$ is a principal G-bundle, we need to know that the right multiplication action $(P \times G)_L = P_L \times_L G_L \to P_L$ descends to $P \times_k G$. The necessary and sufficient condition for Galois descent of morphisms is that the morphism should be equivariant for the Galois actions on P_L and G_L.[2] We check the equivariance on R-points:

$$\rho(s)(xy) = a_s s(xy) = a_s s(x) \cdot s(y) = \rho(s)(x) \cdot s(y).$$

The base change morphism is also faithful, so we can check the axioms of a right action locally, and $P \to \operatorname{Spec} k$ is trivialized by $\operatorname{Spec} L \to \operatorname{Spec} k$, so indeed $P \to \operatorname{Spec} k$ is a principal G-bundle. The result is independent of our choice of L/k: had we chosen some other L'/k, full-faithfulness of the base change to $LL' \subseteq k_s$ ensures the two principal G-bundles are already isomorphic over k.

Finally, to check the two morphisms are inverses is straightforward using full-faithfulness of base change along L/k. Beginning with a cocycle, the original cocycle is recovered by the Galois action on k_s-points of $P \to \operatorname{Spec} k$, which are the same as the k_s-points of G_L. In the other direction, beginning with a principal G-bundle P and writing P' for the G-bundle obtained by descent from P_L, the isomorphism $P_L \cong P'_L$ is Galois-equivariant precisely because P_L and P'_L define the same cocycle, so by full faithfulness the isomorphism descends to $P \cong P'$. □

Remark 7. The hypothesis "affine" in the above result can be removed. First, any algebraic group scheme over a field is quasi-projective ([Sta22, Tag 0BF7]).

Then one can prove that Galois descent is effective for quasi-projective schemes X over a field ([Mil98a, Thm 16.25]): the essential idea of the proof is to note that the Galois orbit of each k_s-point is finite, hence contained in an affine subset. This implies X can be covered by Galois-stable affines; after descending each affine, they glue by uniqueness to give a scheme descending X. Note that this is essentially the proof of existence of fppf quotients of quasi-projective schemes.

Tracking the role of L in the above result, we deduce the following.

Corollary 8. *The cohomology group* $H^1(\operatorname{Gal}(L/k), G(L))$ *classifies isomorphism classes of principal G-bundles on* $\operatorname{Spec} k$ *which are trivialized by* $\operatorname{Spec} L \to \operatorname{Spec} k$. *Equivalently, the natural maps give an exact sequence of pointed sets*

$$0 \to H^1(\operatorname{Gal}(L/k), G(L)) \to H^1(\operatorname{Gal}(k_s/k), G(k_s)) \to H^1(\operatorname{Gal}(k_s/L), G(k_s)).$$

Remark 9. Were G abelian, this would be the start of the inflation-restriction exact sequence, the exact sequence of low-degree terms associated to the Hochschild-Serre spectral sequence. Asking for a nonabelian spectral sequence theory is pretty hopeless, but this small part still works.

Example 10. If G is not assumed smooth, the Galois cohomology cannot hope to capture all fppf-torsors. For example, let k an imperfect field of characteristic 2, and $L = k(\sqrt{a}) = k[x]/(x^2 - a)$ a purely inseparable quadratic extension of k. Then we claim that $\operatorname{Spec} L \to \operatorname{Spec} k$ is an fppf principal μ_2-bundle which is not trivialized by any separable extension.

Given R a k-algebra, we have $(\operatorname{Spec} L)(R) = \{r \in R : r^2 = a\}$, and $\mu_2(R) = \{s \in R : s^2 = 1\}$ acts on this set functorially by multiplication, so indeed $\operatorname{Spec} L$ has a right μ_2-action over k. For the local triviality condition, note $(\operatorname{Spec} L)(L) = \{\sqrt{a}\}$ and $\mu_2(L) = \{1\}$ acts simply transitively on it, so the cover splits itself, as expected. The action map $(\operatorname{Spec} L) \times \mu_2 \to (\operatorname{Spec} L)$ is on rings

$$\begin{aligned} k[x]/(x^2 - a) &\longrightarrow k[x]/(x^2 - a) \otimes_k k[y]/(y^2 - 1) \\ x &\longmapsto x \otimes y \end{aligned}$$

so the map $\operatorname{Spec} L \times \mu_2 \to \operatorname{Spec} L \times \operatorname{Spec} L$ which must be an isomorphism is the L-linear map

$$\begin{aligned} L \otimes_k k[x]/(x^2 - a) &\longrightarrow L \otimes_k k[y]/(y^2 - 1) \\ x &\longmapsto \sqrt{a} \otimes y. \end{aligned}$$

[2]This could be deduced from a similar unpacking of descent data as above.

This is an isomorphism (note both schemes are isomorphic to $L[\varepsilon]/(\varepsilon^2)$, and the map is $\varepsilon \mapsto \sqrt{a}\varepsilon$). In any separable extension, $x^2 - a$ remains irreducible, so the torsor cannot split (it becomes nonreduced upon splitting).

III. Forms of algebraic groups

Now let G a *smooth algebraic group* over k and L/k a Galois extension.

Definition 11. An *L/k-form* of G, or *twist*, is an algebraic group G' over k such that $G_L \cong G'_L$ as algebraic groups.

We would like to classify forms of G in terms of Galois cohomology. Classically, this argument goes by identifying L/k-forms of G with principal Aut_G-bundles, then identifying these with $H^1(\mathrm{Aut}_G)$. However, Aut_G as an algebraic group (representing $S \mapsto \mathrm{Aut}_{\mathrm{Gp}/S}(G_S)$) may not be smooth or affine, so the results of the previous section do not directly imply the classification. We will instead directly verify the correspondence.

Proposition 12. *Let G an algebraic group over k, L/k a Galois extension. The L/k-forms of G are in bijection with Galois cohomology classes $H^1(\mathrm{Gal}(L/k), \mathrm{Aut}_G(L))$, where $\mathrm{Aut}_G(L)$ is equipped with the left Galois action $\varphi \mapsto s\varphi s^{-1}$.*

Proof. First, observe we have indeed equipped $\mathrm{Aut}_G(L) = \mathrm{Aut}_L(G_L)$ with the structure of a left $\mathrm{Gal}(L/k)$-group: the action above is indeed a left action, and acts by group homomorphisms. We reduce to L/k finite similarly to before: if $G'_{k_s} \cong G_{k_s}$, then this isomorphism descends to some L/k finite since both G' and G are finite type over k.

As in the previous section, descent data for an L-scheme X along L/k reduces to a collection $s \mapsto \varphi_s$ of semilinear automorphisms for each $s \in \mathrm{Gal}(L/k)$, such that $\varphi_{st} = \varphi_s\varphi_t$. One can deduce similarly that "descent data" for a morphism of L-schemes simply demands that the morphism be Galois-equivariant. As in Remark 7, any such data is effective for quasiprojective schemes. From these remarks we immediately deduce the form and effectivity of descent data for *group schemes*: the descent data on an L-group scheme X should consist of a family of semilinear *group* automorphisms so that the multiplication map on X descends as well, and the group axioms are identities of morphisms which can be checked after base change back to L.

Now let $s \mapsto \varphi_s$ denote the standard descent data obtained by base change to G_L. Given a cocycle $s \mapsto a_s$ valued in $\mathrm{Aut}_G(L)$, we can twist the descent data by composition:

$$s \mapsto \psi_s := a_s \circ \varphi_s.$$

Since ψ_s is the composition of an s-semilinear group automorphism and an L-linear group automorphism, it is also an s-semilinear group automorphism. The collection is moreover still descent data:

$$\psi_{st} = a_{st}\varphi_{st} = a_s s(a_t)\varphi_{st} = a_s\varphi_s a_t \varphi_s^{-1}\varphi_s\varphi_t = \psi_s\psi_t.$$

So by effectivity of descent, $(G_L, \{\psi_s\}_s)$ descends to a k-group scheme which is an L/k form of G.

Conversely, given an L/k form G' of G, choose an isomorphism $\chi_0 : G'_L \to G_L$. It is clear that the abstract group $\mathrm{Aut}(G_L)$ acts simply transitively on the set $\mathrm{Isom}(G'_L, G_L)$, so we obtain a Galois cocycle by sending $s \in \mathrm{Gal}(L/k)$ to the unique element of $\mathrm{Aut}_L(G_L)$ sending χ_0 to $s(\chi_0) = \varphi_s\chi_0\varphi_s^{-1}$. This is a cocycle, and changing our basepoint χ_0 would give a cohomologous cocycle, so we obtain a well-defined class in H^1. The two constructions are inverses, so we are done. ∎

Remark 13. The above proposition does not need to assume smoothness of G because our twists are assumed to be split by a separable extension. We are "missing" those twists of G which are not split by a separable extension, as well as possibly those that are split by some fppf cover which is not a field extension.

IV. Principal G-bundles, associated bundles, and Tannakian stuff

Proposition 14. *On the Zariski, étale, or fppf site over a scheme X, the groupoid of principal $\mathrm{GL}_{n,X}$-bundles (= $\mathrm{GL}_{n,X}$-torsors) is equivalent to the groupoid of rank-n vector bundles (= quasi-coherent sheaves), which by descent for quasi-coherent sheaves is the same across these three sites.*

Proof. We mimic the usual topological construction of frame bundles. Given a rank-n vector bundle $\mathcal{E} \to X$, its frame bundle $F(\mathcal{E})$ is the open subscheme of the total space of $\mathcal{H}om(\mathcal{O}_X^n, \mathcal{E})$ (which is a rank-n^2 vector bundle) given by the nonvanishing of the determinant on each fiber. This is a principal GL_n-bundle (right action given by precomposition). The construction is functorial: given an isomorphism $\varphi : \mathcal{E} \xrightarrow{\sim} \mathcal{F}$ of vector bundles on X, we get a morphism $\mathcal{H}om(\mathcal{O}_X^n, \mathcal{E}) \to \mathcal{H}om(\mathcal{O}_X^n, \mathcal{F})$ which preserves the frame bundles as subschemes, and is clearly equivariant for the action. Note this functor cannot extend to all morphisms of vector bundles. We are forced to work with just the groupoids.

A pseudo-inverse is given by the associated bundle construction. Given an fppf principal GL_n-bundle $Y \to X$, consider the fiber product $P \times_X \mathbb{A}^n_X$. This has a functorial right GL_n-action given by $(p, v) \cdot g = (pg, g^{-1}v)$, where the left action on $\mathbb{A}^n$ is the standard one. Now we consider the *balanced product*, the quotient

$$P \times_X^{\mathrm{GL}_n} \mathbb{A}^n_X := (P \times_X \mathbb{A}^n_X)/\,\mathrm{GL}_n\,.$$

Here, the quotient should be taken as the categorical quotient for fppf-sheaves on X. This is obviously functorial in the bundle $P \to X$, and we wish to show the quotient is constructible.

Let $\{X_i \to X\}_i$ be a trivializing cover for $P \to X$. Since sheafification commutes with restriction to an open in any topos, the quotient sheaf is covered by trivial quotients, in which case the quotient presheaf is already a sheaf given by

$$(\mathrm{GL}_{n,X_i} \times_{X_i} \mathbb{A}^n_{X_i})/\,\mathrm{GL}_{n,X_i} \cong \mathbb{A}^n_{X_i},$$

hence obviously representable by an affine scheme over X_i, indeed, a vector bundle. This descends by effective descent to the same type of object on X.

We construct the natural isomorphisms between the compositions and the identity, given a vector bundle $\mathcal{E}$, we have a functorial evaluation isomorphism

$$(F(\mathcal{E}) \times_X \mathbb{A}^n_X)/\,\mathrm{GL}_n \to \mathcal{E}$$

constructed as follows: there is a natural map $F(\mathcal{E}) \times_X \mathbb{A}^n_X \to \mathcal{E}$ given by taking (for $f : S \to X$ a map) $(\varphi, v) \in \mathcal{H}om(\mathcal{O}_S^n, f^\star\mathcal{E}) \times \mathcal{O}_S^n \to \varphi(v) \in \Gamma(S, f^\star\mathcal{E})$. Using a trivializing cover, it can be checked to be locally functorially GL_n-equivariant and descend to an isomorphism. Hence we have a natural isomorphism of one composition with the identity.

In the other direction, given a principal G-bundle $P \to X$ we describe a natural isomorphism to the frame bundle of $\mathcal{E} := (P \times_X \mathbb{A}^n_X)/\,\mathrm{GL}_{n,X}$. Given a section $S \to P$ (i.e. an X-morphism), we get an isomorphism $P|_S \cong \mathrm{GL}_{n,S}$, hence a corresponding distinguished element of

$$\mathcal{H}om(\mathcal{O}_X^n, \mathcal{E})(S) = \mathrm{Hom}_S(\mathcal{O}_S^n, \mathcal{E}|_S) = \mathrm{Hom}_S(\mathcal{O}_S^n, \mathbb{A}^n_S) = \mathrm{Hom}_S(\mathcal{O}_S^n, \mathcal{O}_S^n),$$

(the one corresponding to the identity), which clearly vanishes nowhere on the base. This map is natural in S, so we get a sheaf morphism $P \to \mathcal{H}om(\mathcal{O}_X^n, \mathcal{E})$. It is natural in P, and can be checked to be an isomorphism over a trivializing cover onto the frame bundle, so this gives the desired natural isomorphism for the other composition, completing the (strict) equivalence of categories). □

The representability of associated bundles used above is quite general.

Proposition 15. *Let G be a group scheme over X (more generally, an fppf group sheaf) and $P \to X$ be a principal G-bundle. For each quasiprojective $Y \to X$ (or any other class of schemes for which descent is effective) equipped with a G-action, the associated bundle*

$$P \times_X^G Y := (P \times_X Y)/G$$

is representable by an X-scheme of the same type.

Applying this result with $Y \to X$ a G-representation is the starting point of the Tannakian formalism, reducing arbitrary G-bundles to vector bundles.

[TODO the associated vector bundle formalism for other G and connections to Tannakian stuff]

Proposition 16. *Let G a group scheme over k and X a k-scheme. Each principal G-bundle $P \to X$ determines an exact tensor functor $G - \mathrm{Rep} \to \mathrm{Vect}_X$, and conversely. This is an equivalence of groupoids, defined appropriately.*

V. Commutative Groups: Higher Étale and Galois Cohomology

Let k a field, k_s a separable closure (that is, a geometric point $\overline{x} : \operatorname{Spec} k_s \to \operatorname{Spec} k$), and $\mathcal{F}$ a sheaf of *abelian* groups on the small étale site of $\operatorname{Spec} k$. Commutativity ensures we can reduce all étale cohomology to Galois cohomology, not just H^1.

Proposition 17. *The étale sheaf cohomology and Galois cohomology coincide: we have a natural isomorphism for all r*

$$H^r_{\acute{e}t}(\operatorname{Spec} k, \mathcal{F}) \cong H^r(\operatorname{Gal}(k_s/k), \mathcal{F}_{\overline{x}}).$$

Sketch. See [Mil98b] and [Sta22, Tag 04JI] for more details. We have an equivalence of sites between the small étale site on $\operatorname{Spec} k$ and discrete G-sets, the maps given by

$$X = \bigsqcup_i \operatorname{Spec}(L_i) \longmapsto \operatorname{Mor}_{\operatorname{Spec} k}(\operatorname{Spec} k_s, X) = \bigsqcup_i \operatorname{Hom}_k(L_i, k_s),$$

conversely, given a discrete G-set with orbit decomposition $S = \bigsqcup_i S_i$, pick $s_i \in S_i$ with open stabilizer G_i and define

$$X = \bigsqcup_i \operatorname{Spec}(k_s^{G_i}).$$

These are quasi-inverses. So we have an induced morphism of topoi

$$(\text{abelian sheaves on ét}/k) \longleftrightarrow (\text{discrete } \operatorname{Gal}(k_s/k)\text{-modules}).$$

The map from left to right is given by taking the stalk at the geometric point $\overline{x}$, i.e.,

$$\mathcal{F}_{\overline{x}} = \varinjlim_{L/k \text{ finite}} \mathcal{F}(L) =: \mathcal{F}(k_s),$$

which is a discrete $\operatorname{Gal}(k_s/k)$-module by definition of the stalk. The map from left to right is given by $M \mapsto \left(L/k \mapsto \mathcal{F}(L) := M^{\operatorname{Gal}(k_s/L)}\right)$ (for an arbitrary étale cover, which is the disjoint union of these, take the corresponding direct sum of modules). This gives an étale sheaf: given E/L subextension of k_s and finite separable over k, we have

$$L \to E \rightrightarrows E \otimes_L E$$
$$M^{\operatorname{Gal}(k_s/L)} \to M^{\operatorname{Gal}(k_s/E)} \rightrightarrows M^{\operatorname{Gal}(k_s/E)}$$

Both are exact and they are certainly quasi-inverses, so indeed this is an equivalence of topoi.

Under this equivalence, the global sections functor corresponds to taking the $\operatorname{Gal}(k_s/k)$-invariants. So the equivalence induces natural isomorphisms of their derived functors, étale cohomology and (continuous) Galois cohomology. □

Corollary 18. *For G a commutative group scheme on $\operatorname{Spec} k$ (hence a commutative étale sheaf), the above becomes*

$$H^r_{\acute{e}t}(\operatorname{Spec} k, G) \cong H^r(\operatorname{Gal}(k_s/k), G(k_s)).$$

VI. Hilbert 90 and generalizations

The term “Hilbert’s Theorem 90” refers to a number of generalizations of the original result, due to Kummer. We begin with the classical version.

Theorem 19 (Dedekind)**.** *Let L/k a cyclic (finite Galois, degree d) field extension with Galois group generator s. If $x \in L$ has relative norm 1, then $x = y/s(y)$ for some $y \in L$.*

Proof. We give two proofs with slightly different insights. First, we use *linear independence of characters*, which states that for any abstract group G and any field k, distinct characters $G \to k^\star$ are k-linearly independent. This can be proved by a straightforward induction. In particular, we can apply it to the Galois automorphisms $s^i : L^\times \to L^\times$ by ignoring additivity. Consider the L-linear combination of automorphisms

$$\varphi := 1 + (x)s + (xs(x))s^2 + (xs(x)s^2(x))s^3 + \cdots + (x \cdots s^{d-2}(x))s^{d-1} \not\equiv 0.$$

So we can find some $z \in L^\star$ such that $y := \varphi(z) \neq 0$. Computing $s(y)$ we have

$$s(y) = 1 + s(x)s^2(z) + (s(x)s^2(x))s^3(z) + \cdots + (s(x) \cdots s^{d-1}(x))z = \frac{1}{x}y,$$

where we used $N(x) = 1$ to simplify the last term of $s(y)$ to z/x. Rearranging, $x = y/s(y)$. □

Corollary 20. *We have* $H^1_{ét}(\operatorname{Spec} k, \mathbb{G}_m) = H^1(\operatorname{Gal}(k_s/k), k_s^\star) = 0$.

On the opposite extreme of generality, the term is often applied to the following comparison result between cohomology on different sites, which immediately implies the previous corollary because $\operatorname{Spec} k$ has no interesting Zariski-bundles.

Theorem 21. *Let X a scheme, $n \geq 1$. We have canonical isomorphisms* $H^1_{fppf}(X, \mathrm{GL}_n) = H^1_{ét}(X, \mathrm{GL}_n) = H^1_{Zar}(X, \mathrm{GL}_n)$.

Proof. As in the section on associated bundles, there is an equivalence of categories between GL_n-torsors for any of these sites and locally free rank n quasicoherent sheaves on X; in particular the isomorphism classes coincide. □

VII. Fields of dimension ≤ 1.

Theorem 22. *If k is a field of dimension ≤ 1 and G is a connected reductive linear algebraic group, then* $H^1(\operatorname{Gal}(k_s/k), G) = 0$.

[TODO]

VIII. Rational and geometric orbits and conjugacy

VIII.1. **Orbits and Geometric Orbits.** Let G a smooth linear algebraic group over k acting on a finite type k-scheme X, and $x \in X(k)$ with orbit morphism $\alpha : G \to \mathcal{O}_x$.

Remark 23. Since the orbit morphism is surjective, it is surjective on $\overline{k}$-points. That is, $\mathcal{O}_x(\overline{k}) = G(\overline{k}) \cdot x$. This implies immediately from the universal property of a locally closed subscheme that

$$\mathcal{O}_x(k) = (G(\overline{k}) \cdot x) \cap X(k).$$

We call this the *geometric orbit* of x. We wish to investigate its relationship to the *rational orbit* $G(k) \cdot x$.

When the orbit morphism is smooth (tantamount to the stabilizer being smooth), the geometric orbit reduces to k_s-points.

Lemma 24. *If $X \to Y$ is a smooth surjective morphism of schemes over k, then it is surjective on k_s-points.*

Proof. Given a point $y \in Y(k_s)$ (i.e. $\kappa(y) \subseteq k_s$), the fiber over it is a smooth $\kappa(y)$-scheme. Replacing X with the fiber, we reduce to the case of $Y = \operatorname{Spec} \kappa(y) = \operatorname{Spec} k$ and X a smooth k-scheme. By the universal property of the separable closure, it now suffices to show that X contains a closed point with finite separable residue field over k.

Indeed we show such points are dense. For any $U \subseteq X$, since "smooth = locally étale over affine", we can shrink U so $X \to \operatorname{Spec} k$ factors as $U \xrightarrow{\pi} \mathbb{A}^n_k \to \operatorname{Spec} k$ with π étale. If we find a point in the (open) image of U in $\mathbb{A}^n_k$ with finite separable residue field over k, then its fiber under π is nonempty and consists of separable field extensions. So we reduce to showing such points are dense in $\mathbb{A}^n_k$, which is true: for any basic open $D(f) \subseteq \mathbb{A}^n_k$, we have

$$D(f)(k_s) = \{(a_1, \ldots, a_n) \in k_s^n : f(a_1, \ldots, a_n) \neq 0\} \neq \emptyset$$

because k_s is infinite. □

Proposition 25. *If the stabilizer $G_x \leq G$ is smooth, then $\mathcal{O}_x(k) = (G(k_s) \cdot x) \cap X(k)$. In particular, two k-points of X are conjugate by an element of k_s if and only if they are conjugate by an element of $\overline{k}$.*

Proof. Since the orbit map is finitely presented and faithfully flat with fibers over closed points isomorphic to the stabilizer (after passing to $\overline{k}$), the orbit morphism is smooth by [Sta22, Tag 01V8], so the above lemma implies it is surjective on k_s-points, i.e. $G(k_s) \cdot x = \mathcal{O}_x(k_s)$, which gives the result. □

VIII.2. **k_s-Orbits and Galois Cohomology.** We can classify the rational orbits inside a k_s-orbit using Galois cohomology.

Proposition 26. *Let G an algebraic group over k, and $x \in G(k)$ with k_s-orbit $O_x := (G(k_s) \cdot x) \cap X(k)$. Then we have a natural bijection*

$$\{O \subseteq O_x \text{ rational orbit}\} = \ker(H^1(k, G_x) \to H^1(k, G)),$$

where G_x is the centralizer.

Proof. We construct the bijection explicitly. Given $y \in O_x$, pick $g \in G(k_s)$ such that $g \cdot x = y$. Then consider the Galois cocycle $s \mapsto a_s := g^{-1}s(g)$. This is certainly a continuous cocycle (indeed by definition coboundary) valued in $G(k_s)$, and since x and y are Galois-stable

$$g^{-1}s(g) \cdot x = g^{-1}s(g \cdot x) = g^{-1}s(y) = x,$$

so $a_s \in G_x(k_s)$ for all s and we have found a G_x-cocycle in the claimed kernel. If we chose some other y' in the same rational orbit as y, the corresponding cocycle would be the same (the difference would be absorbed in the middle of $g^{-1}s(g)$).

Conversely, given such a class in $H^1(k, G_x)$, since it becomes a coboundary for G each $a_s = h^{-1}s(h)$ for some $h \in G(k_s)$, so we obtain a rational orbit $[h \cdot x]$ in the same k_s-orbit. A cohomologous cocycle $a'_s = b^{-1}a_s s(b)$ (for $b \in G_x(k_s)$) will give the same element $hb \cdot x = h \cdot x$, hence the same rational orbit. Note that beginning from an orbit $[g \cdot x]$, the element h above need not recover g, but we must have $h^{-1}s(h) = g^{-1}s(g)$, so $gh^{-1} \in G(k)$ and so $g \cdot x$ and $h \cdot x$ are in the same rational orbit. □

VIII.3. **Conjugacy.** We can apply the above framework both to $G \curvearrowright G$ and the adjoint action $G \curvearrowright \mathfrak{g}$ to understand the relationship between rational and geometric conjugacy in both settings. For example, when $G = \mathrm{GL}_n$, the theory of Frobenius normal form implies directly that rational, k_s, and $\overline{k}$-conjugacy in the adjoint action coincide. Along with Hilbert's theorem 90 above, we deduce the following.

Corollary 27. *For $x \in \mathrm{GL}_n(k)$, we have $H^1(k, G_x) = 0$.*

TODO weird!

For other groups, the various notions of conjugacy do not coincide.

Example 28. Let $k = \mathbb{R}$, $G = \mathrm{SL}_2$, and $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then the $\overline{k} = \mathbb{C}$-conjugacy class consists of all matrices with determinant 1 and trace zero, but the matrix $y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is not conjugate over $\mathbb{R}$ to x: we compute

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} -bd - ac & a^2 + b^2 \end{pmatrix}$$

has no solutions over $\mathbb{R}$ because squares are positive.

Our vanishing results in cohomological dimension 1 also apply.

Corollary 29. *If k is a field of dimension ≤ 1 and G_x is a connected reductive group for $x \in G(k)$, then the conjugacy and stable conjugacy classes for G coincide. For example,*

Another important question people have extensively considered is whether a stable conjugacy class (i.e. the fiber over a point in the GIT quotient) contains any rational points at all. TODO maybe split some of this off into the other document on GIT stuff.

IX. Hasse Invariants and Gerbes

[TODO]

References

[Mil98a] James S Milne. "Algebraic geometry". In: *Lecture Notes* 6 (1998), p. 02.

[Mil98b] James S Milne. "Lectures on étale cohomology". In: *Available on-line at http://www. jmilne. org/math/CourseNotes/LEC. pdf* (1998).

[Ols16] Martin Olsson. *Algebraic spaces and stacks*. Vol. 62. American Mathematical Soc., 2016.

[Sch14] Stefan Schröer. *Points in the fppf topology*. 2014. DOI: 10.48550/ARXIV.1407.5446. URL: https://arxiv.org/abs/1407.5446.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*. Vol. 5. Springer Science & Business Media, 1994.

[Sta22] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2022.