Torsors in Algebraic Geometry

David Harari

Toronto-November 2000

Contents

1. Introduction 1
2. Torsors over a field 5
3. Torsors over a variety $X$ 17
4. Two ”concrete” applications of torsors 25

1. Introduction

The aim of these lectures is to provide an introduction to the theory of torsors. I’ll try to give some hints for the two following questions:

- What is a torsor?
- Why is this notion useful?

The presentation will not always be axiomatic because our goal is to explain how to work with torsors in usual situations.

To define a torsor, two basic data are needed: a base $X$ and a group $G$. Though in the most general context, $X$ is a scheme and $G$ a (smooth) $X$-group scheme, we will for the most part consider the following cases:

1. $X$ is a perfect field $k$ (e.g. $\text{Char } k = 0$) \(^1\).

\(^1\)strictly speaking $X$ is the scheme $\text{Spec } k$
2. $X$ is an algebraic variety defined over the field $\mathbb{C}$ of complex numbers. Such a variety can be affine (defined by polynomial equations $P_i(x_1, \ldots, x_n) = 0$ in the affine space $\mathbb{A}^n_\mathbb{C} := \mathbb{C}^n$) or projective (defined by homogeneous polynomial equations $P_i(x_0, x_1, \ldots, x_n) = 0$ in the projective space $\mathbb{P}^n_\mathbb{C}$).

3. (generalizes the first two cases) $X$ is an algebraic variety defined over a perfect field $k$. Here $X$ is defined by polynomials equations with coefficients in $k$.

**CAUTION:** When the field $k$ is not algebraically closed, such a variety is not at all characterized by its set $X(k)$ of $k$-points (that is: the set of elements in $k$ satisfying the equations of $X$). For example $X(k)$ can easily by empty (Take the equation $x^2 + y^2 + 1 = 0$ over the field $\mathbb{R}$ of real numbers). The important thing is the set $X(\overline{k})$ of points defined over the algebraic closure $\overline{k}$ of $k$. Strictly speaking, one even has to consider the ideal (or homogeneous ideal in the projective case) generated by the polynomials $P_i$ (for example in the sense of algebraic geometry, the varieties defined by $x = 0$ and $x^2 = 0$ are not the same), but working with $X(\overline{k})$ will be sufficient in the applications.

4. $X$ is a Dedekind ring $R$: e.g. $\mathbb{Z}$, the ring of integers of a number field, the ring $\mathbb{Z}_p$ of $p$-adic numbers.

Now let’s see what the group $G$ could be in these examples:

- The simplest case is when $X$ is a complex non-singular algebraic variety, and one takes for $G$ a complex algebraic group (it is possible to take a ”family” of algebraic groups over $X$, but this degree of generality will not be needed). For example $G$ can be an ”abstract” finite group, a connected linear group (e.g. the additive group $\mathbb{G}_a$, the multiplicative group $\mathbb{G}_m$, $GL_n$, $PGL_n$, $SL_n$...), a complex elliptic curve.

- If $X$ is a field $k$, or an algebraic variety over $k$, $G$ is an algebraic group\(^2\) over $k$. We still have the examples of $\mathbb{G}_a$, $\mathbb{G}_m$, $GL_n$...and also of an elliptic curve defined over $k$. But now the notion of finite $k$-group is a bit more difficult: this means $G(\overline{k})$ finite (not $G(k)$ finite). To define a finite $k$-group, one has to give the group $G(\overline{k})$ (as an abstract finite group) and the (left) action of the Galois group $\Gamma := \text{Gal}(\overline{k}/k)$ on $G(\overline{k})$. For example the group $\mu_n$ of roots of unity is in general not isomorphic (as a $k$-group) to the ”constant” group $\mathbb{Z}/n\mathbb{Z}$, because the Galois action

\(^2\)We will also assume that $G$ is smooth; this condition is always satisfied if $\text{Char } k = 0$. 

2
on $\mu_n(\overline{k})$ can be non trivial. Another way to see that these two groups are not isomorphic is to look at their $\mathbb{Q}$-points: $\mu_3(\mathbb{Q})$ has one element and $(\mathbb{Z}/3\mathbb{Z})(\mathbb{Q})$ has three.

- The case when $X$ is a Dedekind ring is more complicated. $G$ has to be a smooth $R$-group scheme. Essentially, this means that $G$ is defined by equations with coefficients in $R$, and the reduction modulo any non-zero prime ideal $\mathfrak{p}$ of $R$ must define a (smooth) algebraic group over the field $R/\mathfrak{p}$. For example $\mathbb{G}_a$, $\mathbb{G}_m$, $GL_n$ do work over $\mathbb{Z}$, but $\mu_p$ ($p$ prime number) is not good because the reduction mod. $p$ of the equation $x^p = 1$ provides a singular variety over the field $\mathbb{Z}/p\mathbb{Z}$.

We are now ready to define the notion of $X$-torsor under $G$ (or $G$-torsor over $X$, or principal homogeneous space of $G$ over $X$). Before giving definitions, here are some answers to the question "Why are torsors useful?":

- They appear naturally when you deal with certain varieties: curves of genus one, quotients of linear algebraic groups.
- They give a concrete interpretation of abstract cohomology groups or sets (conversely, the cohomological machinery helps to prove results about torsors).
- They classify objects which are "locally" isomorphic (in a sense to be made precise later). Over a field $k$ for example, locally isomorphic means isomorphic over $\overline{k}$.
- The notions of Galois covering and algebraic fundamental group are better understood by means of torsors.
- When $X$ is a variety defined over a number field $k$, an $X$-torsor provides interesting information about the closure of $X(k)$ in the set of adelic points of $X$ (this is part of "descent theory").

These topics will be treated in the next sections.

In the language of algebraic geometry, an $X$-torsor under $G$ is by definition a scheme $Y$, equipped with a surjective and flat morphism $f : Y \rightarrow X$ and a right action of $G$ on $Y : (y, g) \mapsto y.g$ such that the map $Y \times_k G \rightarrow Y \times_X Y$ which sends $(y, g)$ to $(y, y.g)$ is a (scheme-theoretic) isomorphism. That means that the action of $G$ on $Y$ preserves the fibers of $f$, and the action on each "geometric fiber" (the fiber considered over an algebraically closed field) is faithful and transitive. As this definition is not very tractable, let’s see what it means in our examples:
• Assume that $X$ is a complex algebraic variety and $G$ a complex algebraic group. Then an $X$-torsor under $G$ is a complex variety $Y$, equipped with a surjective algebraic morphism $f : Y \to X$ and a right\(^3\) algebraic action $(y, g) \mapsto y.g$ such that: $f(y.g) = f(y)$ for any $g \in G(\mathbb{C}), y \in Y(\mathbb{C})$, and for all $y_1, y_2 \in Y(\mathbb{C})$ s.t. $f(y_1) = f(y_2)$, there exists a unique $g \in G(\mathbb{C})$ such that $y_1.g = y_2$.

If $X$ and $Y$ are connected (non-singular) complex varieties and $G$ is a finite group, this is just the usual notion of Galois unramified covering with group $G$: we have $G = \text{Aut}(Y/X)$ (the group of those automorphisms of $Y$ which are compatible with $f$), and also $G = \text{Gal}(\mathbb{C}(Y)/\mathbb{C}(X))$, where $\mathbb{C}(X), \mathbb{C}(Y)$ are the fields of meromorphic functions of $X$ and $Y$.

For example, if $X = \mathbb{A}^1 - \{0\}$ (the affine line minus zero) and $Y$ is defined in the affine plane by the equations $y^2 = x, x \neq 0$, then the map $Y \to X$ which sends $(x, y)$ to $x$ makes $Y$ an $X$-torsor under the finite group $G = \mathbb{Z}/2$. The action of the non-trivial element of $G$ is given by $(x, y) \mapsto (x, -y)$. Of course this wouldn’t work with $X = \mathbb{A}^1$ because the action of $G$ on the fiber at zero would not be faithful (otherwise stated: the covering would be ramified at zero).

• If $X$ is a variety over a perfect field $k$, the definition is similar, but the morphism $f$ and the action $G \times Y \to Y$ must be defined over $k$. Moreover, this action should be faithful and transitive in the fibers over $\bar{k}$, that is: for any $y_1, y_2 \in Y(\bar{k})$ s.t. $f(y_1) = f(y_2)$, there exists a unique $g \in G(\bar{k})$ such that $y_1.g = y_2$. The trivial torsor is $Y = X \times G$, with the action $(x, g).g' = (x, gg')$.

The previous example $X = \mathbb{A}^1 - \{0\}, Y \subset \mathbb{A}^2 : y^2 = x, x \neq 0$ still works over an arbitrary field $k$ (with $\text{Char } k \neq 2$). Note that there are no $k$-points lying above elements $x \in k^* - k^*_1$, e.g. $k = \mathbb{Q}, x = 2$.

• In the case when $X$ is (the spectrum of) a field $k$, a $k$-torsor $Y$ under the algebraic $k$-group $G$ is a $k$-variety, equipped with a faithful and transitive action of $G(\bar{k})$ on $Y(\bar{k})$ which is compatible with the left action of $\text{Gal}(\bar{k}/k)$, that is $\gamma(y, g) = \gamma(y).\gamma(g)$ (the latter condition means that the action of $G$ is ”defined over $k$”). The trivial torsor is $Y = G$ (acting on itself by right translations).

If $G$ is finite, then $Y$ is a $k$-variety of dimension zero. It corresponds to a finite-dimensional $k$-algebra $\hat{L}$ (for example, if $Y$ is given by the

\(^3\)In these lectures, an action of an algebraic group means a right action, and an action of the Galois group of a field means a left action.
equation $P(x) = 0$ in the affine line, then $L = k[x]/P$, and the set $Y(\overline{k})$ is just the set $\text{Hom}_k(L, \overline{k})$. Thus $L$ is equipped with a $G$-torsor structure iff $\text{Hom}_k(L, \overline{k})$ is given a faithful and transitive action of $G(\overline{k})$ which is compatible with the action of $\Gamma = \text{Gal}(\overline{k}/k)$: for any $s \in \text{Hom}_k(L, \overline{k}), g \in G(\overline{k}), \gamma \in \Gamma$, we must have $\gamma(s.g) = \gamma(s).\gamma(g)$.

Let’s see some specific examples of this situation:

- Take a field $k$ of characteristic $\neq 2$, and $a \in k^* - k^{*2}$ (e.g. $k = \mathbb{Q}, a = 2$). Set $L = k(\sqrt{a})$. Then $\text{Hom}_k(L, \overline{k})$ consists of two conjugate embeddings, so the constant $k$-group $G = \mathbb{Z}/2$ acts faithfully and transitively on it, and this is compatible with the Galois action. Thus $L$ is a $k$-torsor under $\mathbb{Z}/2$.

- Take $k = \mathbb{Q}$ (imbedded in $\overline{\mathbb{Q}}$) and $L = \mathbb{Q}(\sqrt[3]{2})$. Fix a primitive cubic root of unity $j \in \overline{\mathbb{Q}}$. Then $\text{Hom}_Q(L, \overline{\mathbb{Q}}) = \{\sigma_0, \sigma_1, \sigma_2\}$, where $\sigma_s$ sends $\sqrt[3]{2}$ to $j^s\cdot\sqrt[3]{2}$ for $s = 0, 1, 2$. The cyclic group $C_3$ of order 3 acts (faithfully and transitively) on $\{\sigma_0, \sigma_1, \sigma_2\}$; but to obtain a Galois-compatible action, $C_3$ must be equipped with the non trivial action of $\text{Gal}(\mathbb{Q}(j)/\mathbb{Q})$ (check it !). Thus $L$ is a $\mathbb{Q}$-torsor under the finite (but non constant) group $\mu_3$, not under $\mathbb{Z}/3\mathbb{Z}$. Note that the field extension $L/\mathbb{Q}$ is not Galois.

- In the case when the base $X$ is a Dedekind ring, one has to use the language of schemes to define a torsor. This is essentially equivalent to the fiber of $f$ at each non-trivial prime ideal $\mathfrak{p}$ of $R$ (which is a variety over the field $R/\mathfrak{p}$) being a torsor under the fiber at $\mathfrak{p}$ of the $R$-group $G$. Looking at the fiber at $\mathfrak{p}$ is equivalent to take the reduction mod. $\mathfrak{p}$.

Exercise : Let $K/k$ be a finite field extension with Galois closure $M$. Assume that there exists a Galois subextension $L/k$ of $M/k$ such that $L \cap K = k$ and $M$ is generated as a field by $K, L$ (What does this condition mean for $\text{Gal}(M/k)$ and its subgroup $\text{Gal}(M/K)$ ?). Show that $K$ can be viewed as a $k$ torsor under a $k$-group $G$, with $G(\overline{k}) = \text{Gal}(M/L)$. When is the Galois action on $G(\overline{k})$ trivial ?

## 2. Torsors over a field

In this section, the base $X$ will be (the spectrum of) a perfect field $k$. Let $\Gamma := \text{Gal}(\overline{k}/k)$ be the absolute Galois group of $k$. Recall that a $k$-torsor
under an algebraic (smooth) $k$-group $G$ is a $k$-variety $Y$, equipped with a faithful and transitive (right) action of $G(\bar{k})$ on $Y(\bar{k})$ such that:

$\gamma(y,g) = \gamma(y),\gamma(g)$ for any $y \in Y(\bar{k}), g \in G(\bar{k}), \gamma \in \Gamma$.

Two $G$-torsors $Y$ and $Y'$ are isomorphic if there exists an isomorphism $\varphi : Y \to Y'$ of $k$-varieties such that $\varphi(y,g) = \varphi(y),g$ for any $y \in Y(\bar{k}), g \in G(\bar{k})$.

Note that since $\varphi$ is a $k$-morphism, it has also to satisfy $\varphi(\gamma(y)) = \gamma(\varphi(y))$ for each $y \in Y(\bar{k}), \gamma \in \Gamma$. A $k$-torsor $Y$ is trivial if it is isomorphic to the torsor $G$ (with the right action of $G$ by translation). In particular, $Y$ is trivial if and only if the set $Y(k)$ of $k$-points of $Y$ is not empty (the condition is necessary because $G(k) \neq \emptyset$; conversely, if $y_0 \in Y(k)$, then $G$ is isomorphic to $Y$ via $g \mapsto y_0,g$). For example any torsor over an algebraically closed field is trivial.

**Examples of $k$-torsors:**

1. Let $L/k$ be a finite Galois field extension. Set $G = \text{Gal}(L/k)$, we can see $G$ as a finite constant $k$-group (that is: $G(\bar{k}) := \text{Gal}(L/k)$ and the action of $\Gamma$ on $G(\bar{k})$ is trivial). Then $L$ is a $G$-torsor over $k$; indeed $\text{Hom}_k(L,\bar{k}) = \text{Gal}(L/k)$ (by definition of a Galois extension) and we can define the action of $G(\bar{k})$ on $\text{Hom}_k(L,\bar{k})$ by $y,g = yg$ (product in $\text{Gal}(L/k)$). Now, for each $\gamma \in \Gamma,y \in \text{Hom}_k(L,\bar{k}), \gamma(y) = \hat{\gamma}y$, where $\hat{\gamma}$ is the image of $\gamma$ in $\text{Gal}(L/k)$ (recall that $\text{Gal}(L/k)$ is the quotient of $\Gamma$ by $\text{Gal}(\bar{k}/L)$). Thus $\gamma(y,g) = \hat{\gamma}yg = \gamma(y),g = \gamma(y),\gamma(g)$ for any $y \in Y(\bar{k}), g \in G(\bar{k}), \gamma \in \Gamma$ (the last equality holds because the action of $\Gamma$ on $G(\bar{k})$ is trivial).

More generally, if $L$ is a finite-dimensional $k$-algebra, then ”$L$ is a $k$-torsor under the constant group $G”$ can be taken as a definition of ”$L$ is Galois with group $G”$. If $L$ is not a field, the group $G$ needs not be unique, e.g. $L = k^n$ is a $k$-torsor under any transitive subgroup of $S_n$.

2. Set $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$. Then $L$ is a $\mathbb{Q}$-torsor under $\mu_3$, but not under the constant group $\mathbb{Z}/3\mathbb{Z}$. (see the introduction).

3. Let $Y$ be a smooth and projective curve of genus one over $k$ (for example a smooth intersection of two quadrics in $\mathbb{P}^3$). Then the Jacobian variety $E$ of $Y$ is an elliptic curve and $Y$ is a $k$-torsor under $E$.

4. Let $K/k$ be a finite field extension. Fix a base $\omega_1,...,\omega_r$ of $K/k$ and let $N$ denote the norm map $K \to k$ (by definition $N(x)$ is the determinant of the multiplication by $x$ in the $k$-vector space $K$). Define a $k$-group $G$ by the equation:
\[ N(x_1 \omega_1 + \ldots + x_r \omega_r) = 1 \]

In particular \( G(k) \simeq \{ x \in K, N(x) = 1 \} \) and \( G(\overline{k}) \simeq (\overline{k}^*)^{r-1} \). Now for \( a \in k^* \) the \( k \)-variety \( Y \) defined by the affine equation:

\[ N(x_1 \omega_1 + \ldots + x_r \omega_r) = a \]

is a \( G \)-torsor. Indeed let \( y := (y_1, \ldots, y_r) \in Y(\overline{k}), g := (g_1, \ldots, g_r) \in G(\overline{k}) \). \( \omega_1, \ldots, \omega_r \) is also a base of \( K \otimes_k \overline{k} \) over \( \overline{k} \), set \( (y_1 \omega_1 + \ldots + y_r \omega_r), (g_1 \omega_1 + \ldots + g_r \omega_r) = (y_1 \cdot g_1) \omega_1 + \ldots + (y_r \cdot g_r) \omega_r \), and define \( y.g := (y_1, g_1, \ldots, y_r, g_r) \). By multiplicativity of the norm map, this clearly makes \( Y \) into a \( G \)-torsor. \( Y \) is trivial if and only if \( Y(k) \neq \emptyset \), that is if and only if \( a \) is a norm for the extension \( K/k \).

**Some functorial properties:**

- Let \( k \subset k' \) be a field extension, and \( Y \) a \( k \)-torsor under the group \( G \). Then \( Y \times_k k' \) is a \( k' \)-torsor under \( G \times_k k' \). For example consider the \( \mathbb{Q} \)-torsor \( L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) under \( \mu_3 \) and take \( k' = \mathbb{Q}(j) \), where \( j \) is a primitive cubic root of unity. Then \( L \otimes_k k' = \mathbb{Q}(\sqrt{2}, j) \) is a \( k' \)-torsor under \( G \times_k k' \), which is the constant group \( \mathbb{Z}/3\mathbb{Z} \) over \( k' \) (all cubic roots of unity belong to \( k' \)). One recovers the fact that \( \mathbb{Q}(\sqrt{2}, j) \) is a Galois field extension of \( \mathbb{Q}(j) \) with group \( \mathbb{Z}/3\mathbb{Z} \).

- Changing the group \( G \) is more difficult. Let \( p : G \to G' \) be a morphism of \( k \)-groups. We want to associate to a \( G \)-torsor \( Y \) a \( G' \)-torsor \( Y' \). Fix an isomorphism which identifies \( Y(\overline{k}) \) with \( G(\overline{k}) \); then the Galois action on \( Y'(\overline{k}) = G'(\overline{k}) \) must be defined by \( p(\gamma(y)) = \gamma(p(y)), y \in Y(\overline{k}), \gamma \in \Gamma \). The way to do that is to set \( Y' = Y \wedge^G G' \) by definition the contracted product \( Y \wedge^G G' \) is the quotient of \( Y \times G' \) by the right action of \( G \) defined by \( (y, g), g = (y, g, p(g)^{-1}g') \). It is true (but not obvious) that this quotient exists in the category of \( k \)-varieties. Now the right action of \( G' \) on \( Y' \) is just given by right translation on \( G' \).

An interesting special case is when \( G' = G/H \) is the quotient of \( G \) by a normal subgroup \( H \). Then \( Y' \) is just the quotient of \( Y' \) by the action of \( H \) (this is very similar to Galois theory).

Now we want to relate torsors to cohomology sets. We need some basic facts about Galois cohomology.

**Review of non-abelian group cohomology.**

7
Let $\Gamma$ be a profinite group, equipped with its profinite group topology. Let $A$ be a discrete group. Consider a continuous left action of $\Gamma$ on $A$ which is compatible with the group structure of $A$ (that is: $\gamma(ab) = \gamma(a)\gamma(b)$ for each $\gamma \in \Gamma$, $a, b \in A$). We will mainly consider the example $\Gamma = \text{Gal}(\bar{k}/k)$ (which is the projective limit of $\text{Gal}(L/k)$ for all finite Galois field extensions of $k$) and $A = G(\bar{k})$, where $G$ is an algebraic $k$-group. We shall often denote by $\gamma a$ the image of $a \in A$ by $\gamma \in \Gamma$.

Define $H^0(\Gamma, A) = A^\Gamma = \{a \in A, \forall \gamma \in \Gamma, \gamma(a) = a\}$ (In the example $H^0(\Gamma, G(\bar{k})) = G(k)$).

A cocycle is a continuous map $\Gamma \to A, \gamma \mapsto c_\gamma$ such that $c_{\gamma_1\gamma_2} = c_{\gamma_1} c_{\gamma_2}$ for any $\gamma_1, \gamma_2 \in \Gamma$. The set of cocycles in denoted by $Z^1(\Gamma, A)$.

The first cohomology set (denoted by $H^1(\Gamma, A)$) is by definition the quotient of $Z^1(\Gamma, A)$ by the equivalence relation:

c \sim c' \text{ if there exists } a \in A \text{ such that } c_\gamma = a^{-1} c_\gamma a \text{ for any } \gamma \in \Gamma.

This set has a distinguished element: the class of the trivial cocycle (denoted by 0). The class of $c$ is trivial if and only if there exists $a \in A$ such that $c_\gamma = a^{-1} \gamma a$ for any $\gamma \in \Gamma$.

The simplest case is when the action of $\Gamma$ on $A$ is trivial. Then $H^1(\Gamma, A)$ is the set of continuous homomorphisms from $\Gamma$ to $A$, modulo conjugation by a constant element of $A$.

When $\Gamma = \text{Gal}(\bar{k}/k), A = G(\bar{k}),$ and $L/k$ is a finite field extension, an element of $Z^1(\text{Gal}(L/k), G(L))$ can be pushed to $Z^1(\Gamma, G(\bar{k}))$ (recall that $\text{Gal}(L/k)$ is a quotient of $\Gamma$), and it is easy to see that this induces an injection $H^1(\text{Gal}(L/k), G(L)) \hookrightarrow H^1(\Gamma, G(\bar{k}))$. The continuity condition on cocycles implies that $H^1(\Gamma, G(\bar{k}))$ is the direct limit of $H^1(\text{Gal}(L/k), G(L))$, where $L$ runs over all finite Galois extensions of $k$. This is especially useful in computing Galois cohomology.

Set $H^1(k, G) := H^1(\Gamma, G(\bar{k}))$. We have the following behaviours:

- A field extension $k_1 \subset k_2$ induces a map $\text{Gal}(\bar{k}_2/k_2) \to \text{Gal}(\bar{k}_1/k_1)$. Since $G(k_1) \subset G(k_2)$, we obtain a map $Z^1(k_1, G) \to Z^2(k_2, G)$, and it is obvious that it is compatible with the equivalence relation defining $H^1$.

Thus the inclusion $k_1 \subset k_2$ induces a map$^4$ of pointed sets $H^1(k_1, G) \to H^1(k_2, G)$.

---

$^4$Actually one has to check that for any field $k$ and any field inclusion $k_1 \subset k_2$, the set $H^1(k, G)$ and the map $H^1(k_1, G) \to H^1(k_2, G)$ do not depend on the choice of the algebraic closures $\bar{k}, \bar{k}_1, \bar{k}_2$. See [Se94], II.1.1.

8
• If \( p : G \to G' \) is a morphism of \( k \)-groups, then an element of \( Z^1(k, G) \) can be pushed to \( Z^1(k, G') \), and this also induces a map \( H^1(k, G) \to H^1(k, G') \).

We are now ready to relate \( k \)-torsors to cohomology sets.

**Theorem 1** Let \( T^G_k \) be the set of isomorphism classes of \( G \)-torsors over \( k \). Then there exists a functorial bijection \( T^G_k \to H^1(k, G) \).

**Remark:** Here functorial means that the bijection is compatible with the changes of field \( k \) and of group \( G \), which have been defined for both sides. The bijection also sends the trivial torsor to 0.

**Proof:** Let \( Y \) be a \( k \)-torsor under \( G \). Fix \( y_0 \in Y(\kbar) \), then for any \( \gamma \in \Gamma \), there exists a unique \( c_\gamma \in G(\kbar) \) such that \( \gamma(y_0) = y_0.c_\gamma \) (by definition of a torsor). It is easy to check that \( c_\gamma \) is a cocycle, and that if one replaces \( y_0 \) by \( y_0 = y_0.g \) \( (g \in G(\kbar)) \), then \( c_\gamma \) is replaced by \( g^{-1}c_\gamma g \). Thus the class \([c]\) of \( c \) in \( H^1(k, G) \) does not depend on \( y_0 \). If \( \varphi : Y \to Y' \) is an isomorphism of torsors, then the equality \( \gamma(y_0) = y_0.c_\gamma \) implies \( \gamma(\varphi(y_0)) = \varphi(y_0).c_\gamma \), so we obtain a well defined map \( \lambda : T^G_k \to H^1(k, G) \).

Conversely, let \( c \in Z^1(k, G) \). Define a \( k \)-variety \( Y \) by \( Y \times_k \kbar = G \times_k \kbar \), and the Galois action on \( Y(\kbar) \) is given by \( \gamma(x) = c_\gamma.x \). Although not obvious, this does define a \( k \)-variety \( Y \).\(^5\) It is easy to check (using the cocycle property) that we have defined a left action of \( \Gamma \) on \( Y(\kbar) \), and the right action by translation of \( G(\kbar) \) on \( Y(\kbar) = G(\kbar) \) makes \( Y \) a \( G \)-torsor. One can also check that if \( c'_\gamma = g^{-1}c_\gamma g \), then the corresponding tensors \( Y.c' \) and \( Y.c \) are isomorphic via the left translation by \( g \) in \( G(\kbar) \). We obtain a map \( H^1(k, G) \to T^G_k \).

It is not difficult to see that \( \lambda \) and \( \mu \) are inverses of each other (for example, one can look at the action of \( \Gamma \) on the identity element of \( G(\kbar) \)). They are obviously compatible with the functorialities defined above for elements of \( T_k \) and \( H^1(k; G) \).

\( \square \)

**Exercise:** Make the correspondence of Theorem 1 explicit for \( G = \mathbb{Z}/2\mathbb{Z} \).

---

\(^5\)One has to take the quotient of \( G \times_k \kbar \) by the new Galois action. This quotient exists by Weil’s theorem on descent because the algebraic group \( G \times_k \kbar \) is quasi-projective. We had seen this difficulty when we were trying to define the change of group for a torsor.
The "long" exact sequence.

Let \( k \) be a perfect field and \( \Gamma := \text{Gal}(\bar{k}/k) \). Consider an exact sequence of (smooth) algebraic \( k \)-groups:

\[
1 \to A \to B \to C \to 1
\]

This means that the exact sequence of groups:

\[
1 \to A(\bar{k}) \to B(\bar{k}) \to C(\bar{k}) \to 1
\]

is exact.

**Theorem 2** There is an exact sequence of pointed sets:

\[
1 \to A(k) \to B(k) \to C(k) \to H^1(k, A) \to H^1(k, B) \to H^1(k, C)
\]

The proof is quite standard (for example using the explicit description of \( H^1 \) with cocycles) and can for example be found in Serre’s book [Se68], VII.

**Comments on Theorem 2:**

- "Exact sequence of pointed sets" means that the image of each map is the kernel (=inverse image of the distinguished element) of the following one.

- One has to be very careful with the maps \( H^1(k, A) \to H^1(k, B) \) and \( H^1(k, B) \to H^1(k, C) \). Even if \( A \) is abelian, these maps can have trivial kernel, and yet not be injective. To obtain more information, the exact sequence must be twisted: see [Se94], I.5.5.

The situation is somehow better if \( A(\bar{k}) \) is central in \( B(\bar{k}) \). Then the following properties hold (see [Se94], I.5.6 and I.5.7):

- The coboundary map \( \delta : C(k) \to H^1(k, A) \) is a group homomorphism and two elements of \( H^1(k, A) \) have the same image in \( H^1(k, B) \) if and only if they differ by an element of \( \text{Im} \, \delta \). For example, if \( B(k) \to C(k) \) is surjective (e.g. the morphism \( B \to C \) has a \( k \)-section), the map \( H^1(k, A) \to H^1(k, B) \) is surjective.

- The group \( H^1(k, A) \) acts on \( H^1(k, B) \), and two elements of \( H^1(k, B) \) have the same image in \( H^1(k, C) \) if and only if they are in the same orbit (in particular \( H^1(k, A) = 0 \) implies that the map \( H^1(k, B) \to H^1(k, C) \) is injective).
• The exact sequence of Theorem 2 extends to:
  
  \[ A(k) \to B(k) \to C(k) \to H^1(k, A) \to H^1(k, B) \to H^2(k, A) \]
  
  where \( H^2(k, A) \) makes sense because \( A \) is abelian. But even if \( C \) is abelian, the map \( H^1(k, C) \to H^2(k, A) \) is not necessarily a group homomorphism when \( B \) is not abelian.

Examples of computations of \( H^1 \).
1. The \( k \)-groups \( G_a \) and \( G_m \) are respectively defined via \( \mathbb{A}_k^1 \) (equipped with the addition) and \( \mathbb{A}_k^1 = \{ 0 \} \) (equipped with the multiplication).

**Theorem 3** \( H^1(k, G_a) = 0 \) for any field \( k \).

It is a consequence of the "normal base theorem" in Galois theory, cf. [Se68], X.1.

**Theorem 4 (**"Hilbert 90**\) \( H^1(k, G_m) = 0 \) for any field \( k \).

**Proof:** It is sufficient to show that \( H^1(\text{Gal}(L/k), L^*) = 0 \) for any finite Galois field extension \( L/k \). Let \( \Delta := \text{Gal}(L/k) \) and let \( c : \Delta \to L^* \) be a cocycle. For \( u \in L \), set \( a = \sum_{\delta \in \Delta} c_\delta(u) \). It is possible to find \( u \) such that \( a \neq 0 \), because the elements of \( \Delta \) are characters from \( L^* \) to \( L^* \), and are therefore linearly independent\(^6\) in the \( L \)-vector space \( \mathcal{F}(L^*, L) \) of applications \( L^* \to L \). Now for each \( \gamma \in \Delta \), we have:

\[
\gamma(a) = \sum_{\delta \in \Delta} \gamma(c_\delta)(\gamma \delta)(u) = \sum_{\delta \in \Delta} (c_\gamma)^{-1} c_\gamma \delta(\gamma \delta)(u) = \frac{a}{c_\gamma}
\]

Thus \( c_\gamma = \frac{\gamma(a)^{-1}}{a} \) and the class of \( c \) in \( H^1(\Delta, L^*) \) is zero.

\[\square\]

2. **Kummer sequence.** Let \( n \) be an integer which is not divisible by \( \text{Char} \ k \).

Then the sequence of \( k \)-groups

\[ 1 \to \mu_n \to \mathbb{G}_m \xrightarrow{\cdot a} \mathbb{G}_m \to 1 \]

is exact. Using Hilbert 90, we obtain the exact sequence:

\[ H^0(k, \mathbb{G}_m) \xrightarrow{\cdot a} H^0(k, \mathbb{G}_m) \to H^1(k, \mu_n) \to 0 \]

Finally \( H^1(k, \mu_n) \) is \( k^*/k^{*n} \): To \( a \in k^*/k^{*n} \) corresponds the \( \mu_n \)-torsor \( L = k(\sqrt[n]{a}) \).

\(^6\)This independance result is easy to show by induction on the number of morphisms.
3. Artin-Schreier sequence. Assume that $k$ is of characteristic $p > 0$. Then the map $\Phi: \bar{k} \to \bar{k}$ defined by $\Phi(x) = x^p - x$ is an additive morphism with kernel $\mathbb{Z}/p\mathbb{Z} \subset k$. Therefore the sequence of $k$-groups:

$$1 \to \mathbb{Z}/p\mathbb{Z} \to G_a \xrightarrow{\Phi} G_a \to 1$$

is exact. Using $H^1(k, G_a) = 0$ we get $H^1(k, \mathbb{Z}/p\mathbb{Z}) = k/\Phi(k)$. For $a \in k/\Phi(k)$, the corresponding $k$-torsor under $\mathbb{Z}/p$ is $L = k[t]/(t^p - t + a)$.

4. Let $K/k$ be a finite Galois field extension. Fix a base $(\omega_1, ..., \omega_r)$ of $K/k$ and denote by $G$ the $k$-group defined by the equation:

$$N_{K/k}(x_1\omega_1 + ... + x_r\omega_r) = 1$$

(cf. example 4 page 6; $G$ is often denoted by $R^1_{K/k}G_m$). Let $R_{K/k}G_m$ be the Weil restriction (from $K$ to $k$) of the multiplicative group $G_m$; $R_{K/k}G_m$ is defined by:

$$(x_1\omega_1 + ... + x_r\omega_r) \neq 0$$

In particular $(R_{K/k}G_m)(k) = K^*$ and $(R_{K/k}G_m)(K) = (K^*)^r$. The $k$-group $R_{K/k}G_m$ is equipped with the norm map: $N : R_{K/k}G_m \to G_m$ and the following sequence is exact:

$$1 \to G \to R_{K/k}G_m \xrightarrow{N} G_m \to 1$$

To compute, $H^1(k, G)$, we note that $H^1(k, R_{K/k}G_m) = H^1(K, G_m)$: indeed $(R_{K/k}G_m)(L) = (L \otimes_k K)^*$ for any field extension $L/k$; in particular the Galois module $(R_{K/k}G_m)(\bar{k})$ is the induced module of $G_m(\bar{k})$ via the inclusion $\text{Gal}(\bar{k}/K) \subset \Gamma$ and we apply [Se94], I.2.5. By Hilbert 90, $H^1(k, R_{K/k}G_m) = 0$ and we obtain the cohomology exact sequence:

$$H^0(k, R_{K/k}G_m) \xrightarrow{N} H^0(k, G_m) \to H^1(k, G) \to 0$$

that is: $H^1(k, G) = k^*/N K^*$. For $a \in k^*/N K^*$, the corresponding $k$-torsor is given by the equation (cf. example 4 page 6):

$$N_{K/k}(x_1\omega_1 + ... + x_r\omega_r) = a$$

\[\text{Similarly the Weil restriction from } C \text{ to } R \text{ of a complex variety } X \text{ is the usual real variety of dimension } 2 \dim X \text{ associated to } X.\]
5. Assume \( \text{Char } k \neq 2 \). Let \( a \in k^* - k^{*2} \), consider the orthogonal group \( O(q) \) of the quadratic form \( q = -a \) (e.g. \( k = \mathbb{R}, a = -1 \)). In other words \( O(q) \) is the group of \((2, 2)\) matrices \( g \), such that \( g^t g m g = m \), where \( m = \text{diag}(1,-a) \). Let \( SO(q) \) be the subgroup of \( O(q) \) consisting of matrices of determinant 1. The following sequence is exact and split:

\[ 1 \to SO(q) \to O(q) \overset{\text{det}}{\to} \mathbb{Z}/2\mathbb{Z} \to 1 \]

(For example \( g = \text{diag}(1, -1) \) belongs to \( O(q)(k) \) and has a non trivial determinant). The group \( SO(q) \) is isomorphic to \( R_{K/k}^1 G_m \) (cf. previous example) for \( K = k(\sqrt{a}) \), this because \( SO(q) \) consists of matrices

\[
\begin{pmatrix} \alpha & a\beta \\ \beta & \alpha \end{pmatrix}
\]

such that \( \alpha^2 - a\beta^2 = 1 \). Now using previous examples, and the fact that the map \( O(q) \to \mathbb{Z}/2\mathbb{Z} \) admits a section, we obtain the exact sequence of cohomology sets:

\[ 1 \to k^*/N K^* \to H^1(k; O(q)) \to k^*/k^{*2} \to 1 \]

In the case \( k = \mathbb{R}, a = -1 \), we obtain:

\[ 1 \to \mathbb{Z}/2\mathbb{Z} \to H^1(\mathbb{R}, O(q)) \to \mathbb{Z}/2\mathbb{Z} \to 1 \]

This does not imply that \( H^1(\mathbb{R}, O(q)) \) has 4 elements ! In fact \( H^1(\mathbb{R}, O(q)) \) has cardinality 3. The kernel of the map \( H^1(\mathbb{R}, O(q)) \to \mathbb{Z}/2\mathbb{Z} \) has order 2, but there is only one element of \( H^1(\mathbb{R}, O(q)) \) which is mapped to the non-trivial element of \( \mathbb{Z}/2\mathbb{Z} \). This can be checked directly, or using the notion of ”torsion” (see Serre, [Se94], I.5.3).

The point is that the exact sequence of cohomology gives an information about the kernel of \( H^1(k, O(q)) \to H^1(k, \mathbb{Z}/2\mathbb{Z}) \), but not about the equivalence relation defined by this map, because \( SO(q) \) is not central in \( O(q) \). We will see later that \( H^1(k, O(q)) \) is in bijection with equivalence classes of quadratic forms over \( k \), which implies immediately that \( H^1(\mathbb{R}, O(q)) \) has 3 elements.

6. The exact sequence of \( k \)-groups

\[ 1 \to G_m \to GL_n \to PGL_n \to 1 \]

is central, so there is an exact sequence:

\[ 1 \to H^1(k, GL_n) \to H^1(k, PGL_n) \to H^2(k, G_m) \]
Actually $H^1(k, GL_n) = 0$ (this is a generalization of Hilbert 90) and the map $H^1(k, PGL_n) \to H^2(k, G_m)$ is always injective (which is stronger than just saying that its kernel is trivial). See Serre, [Se68], X.5.

**Exercise.** Give an example of exact sequence of $k$-groups $1 \to A \to B \to C \to 1$ such that the map $H^1(k, B) \to H^1(k, C)$ has trivial kernel, but is not injective (use $SO(q)$ for a well chosen quadratic form $q$ of rank 2). Same question for the map $H^1(k, A) \to H^1(k, B)$ (take the symmetric group $S_3$ for $B$, with trivial action of $\Gamma$).

**Forms and torsors.**

Let $V$ be an algebraic variety defined over a perfect field $k$. Let $\overline{k}$ be the algebraic closure of $k$ and $V := V \times_k \overline{k}$. A $k$-form of $V$ is a $k$-variety $V'$ such that $V'$ is isomorphic to $V$. For example, a projective conic $C$ is a $k$-form of $\mathbb{P}_k^1$, and is isomorphic to $\mathbb{P}_k^1$ if and only if $C(k) \neq \emptyset$.

In the special case when $Y = G$ is an algebraic $k$-group, a $k$-form of $G$ is a $k$-group $G'$ such that $\overline{G}$ is isomorphic as a $\overline{k}$-group to $\overline{G'}$. For example, if $K = k(\sqrt{a})$ is a quadratic extension of $k$ (Char $k \neq 2$), the 1-dimensional $k$-group $R^1_{K/k} G_m$ defined by the affine equation $x^2 - ay^2 = 1$ is a $k$-form of the multiplicative group $G_m$.

**Theorem 5** Let $V$ be a quasi-projective $k$-variety (e.g. $V$ affine, $V$ projective, $V$ an algebraic $k$-group). Let $\Gamma := \text{Gal}(\overline{k}/k)$ act on $\text{Aut}(\overline{V})$ by $\gamma(g)(v) = \gamma(g)(\gamma^{-1}(v))$, $\gamma \in \Gamma, g \in \text{Aut}(\overline{V}), v \in \overline{V}(k)$. Then the set $E(V)$ of $k$-forms of $V$ (up to $k$-isomorphism) is in bijection with the Galois cohomology set $H^1(k, \text{Aut}(V)) := H^1(\Gamma, \text{Aut}(\overline{V}))$.

**Proof:** Let $V'$ be a $k$-form of $V$. Denote by $P$ the set of $\overline{k}$-isomorphisms $\varphi : V \to V'$. The set $P$ is equipped with the left action of $\Gamma$ given by $\gamma \cdot (\varphi) = \gamma V' \cdot \varphi \circ \gamma^{-1}$, where $\gamma V'$ is the action of $\gamma$ on $V'$ ($V'(k)$ and $V(\overline{k})$ are equal as sets, but the action of $\Gamma$ on them may differ). There is also the right action of $\text{Aut}(\overline{V})$ on $P$, given by $g \cdot \varphi = \varphi \circ g$, which is faithful, transitive, and compatible with the action of $\Gamma$. Thus $P$ is an $\text{Aut}(V)$-torsor. Isomorphic

---

8Moreover the bijection is functorial in $k$ and $V$ itself corresponds to the trivial element of $H^1(k, \text{Aut}(V))$.

9In general, the group-functor $\text{Aut}(V)$ defined by $\text{Aut}(V)(L) = \text{Aut}(V \times_k L)$ is not representable by an algebraic $k$-group: in this context an $\text{Aut}(V)$-torsor is just a non-empty set, equipped with a left action of $\Gamma$ and a compatible right action of $\text{Aut} (\overline{V})$. It is immediate to check that the correspondance torsors-$H^1$ still holds in this general framework.
$k$-forms $V'$ and $V''$ obviously give isomorphic $k$-torsors, and we obtain a map
$\theta : E(V) \to H^1(k, \text{Aut}(V))$.

Now $P$ is isomorphic to $\text{Aut}(\overline{V})$ as an $\text{Aut}(\overline{V})$-torsor over $\overline{k}$, and (replacing
$P$ by an isomorphic $k$-torsor if necessary), one can assume that the new Galois
action on $P$ is given by $\gamma_p(\varphi) = c_\gamma \circ \varphi$, where $c_\gamma$ is a cocycle corresponding to
$\theta(V')$ (this follows from the description of the $H^1$-torsors, see
above). Namely $\gamma_p(\varphi) = c_\gamma \circ \varphi \circ \gamma^{-1}$. We have also
$\gamma_{p'}(\varphi) = \gamma_{V'}(\varphi') = c_{\gamma'} \gamma'$. This immediately implies
that $\theta$ is injective. Conversely if $c \in Z^1(\Gamma, \text{Aut}(\overline{V}))$, then the $k$-variety $V'$
defined as the quotient of $\overline{V}$ by the twisted action $\gamma_{V'}(\varphi') = c_{\gamma'} \gamma'$(which is
well defined because $V$ is quasi-projective, by Weil’s theorem on descent) is
sent to $[c] \in H^1(\Gamma, \text{Aut}(\overline{V}))$ by $\theta$.

\[ \square \]

In the special case of a $k$-group $G$, one gets (in exactly the same way) that
the set of its $k$-forms (up to isomorphism) is in bijection with $H^1(k, \text{Aut}(G))$
(here $\text{Aut}(\overline{G})$ is the group of automorphisms of $\overline{G}$ as a $\overline{k}$-group).

**Examples:**

1. $\text{Aut}(G_a) = G_m$, so by Hilbert 90 $E(G_a)$ consists of $G_a$ itself.

2. Assume $\text{Char} \ k \neq 2$. Then $\text{Aut}(G_m) = \mathbb{Z}/2\mathbb{Z}$ and $E(G_m) = k^*/k^{*2}$.
   For $a \in k^*/k^{*2}$, the corresponding form is given by $R_{K/k}G_m$, where
   $K = k(\sqrt{a})$.

3. Let $A^1_k$ be the affine line. Then $\text{Aut}(A^1_k)$ consists of affine morphisms
   $x \mapsto ax + b, a \in k^*, b \in k$. Namely there is an exact sequence:
   
   \[ 1 \to G_a \to \text{Aut}(A^1_k) \to G_m \to 1 \]

   and using $H^1(k, G_a) = H^1(k, G_m) = 0$, we obtain $E(A^1_k) = \{A^1_k\}$.

4. The group of automorphisms of the projective space $P^{n-1}_k$ is $PGL_n$. In
general $H^1(k, PGL_n)$ is not trivial and there are several forms of $P^{n-1}_k$.
Such a form is called a *Severi-Brauer variety*.

5. Let $G$ be an algebraic $k$-group. Then the group of inner automorphisms
   of $G$ is isomorphic to $G^{ad} = G/Z$, where $Z$ is the center of $G$, and we
define $\text{Out}(G) := \text{Aut}(G)/G^{ad}$. An *inner* form of $G$ is a $k$-form $G'$
corresponding to a class in $H^1(k, \text{Aut}(G))$ which comes from $H^1(k, G^{ad})$.
This is equivalent to saying that the new Galois action on $G'$ is given
by $\gamma_G(g) = c_\gamma g c_\gamma^{-1}$, $\gamma \in \Gamma, g \in G(\overline{k}) = G'(\overline{k})$, where $\gamma \mapsto c_\gamma$ is a cocycle in $Z^1(k, G)$.

For example if $n \geq 3$ and $G = SL_n$, then $G^{ad} = PGL_n$ and $\text{Out}(G) = \mathbb{Z}/2$ (the non-trivial element of $\text{Out}(G)$ corresponds to the automorphism $x \mapsto x^{-1}$). We have also $\text{Aut}(GL_n) = \text{Aut}(SL_n)$, so the $k$-forms of $SL_n$ and of $GL_n$ are in one-to-one correspondence. See Serre, [Se94], III.1.4 for more details.

There are similar statements as Theorem 5 for other objects than $k$-varieties: for example $k$-algebras, $k$-quadratic forms. In particular if $q$ is a quadratic form over $k$, the set $H^1(k, O(q))$ corresponds to equivalence classes of quadratic forms over $k$ (two quadratic forms are always isomorphic over $\overline{k}$), and $H^1(k, SO(q))$ corresponds to equivalence classes of quadratic forms over $k$ with same discriminant as $q$.

To end this section about torsors over a field, let us quote (without proof) the three following deep results. Recall that a linear $k$-group is a smooth algebraic subgroup of $GL_n$. This is equivalent to saying that $G$ is an affine group variety over $k$.

**Theorem 6 (Steinberg)** Let $k$ be a perfect field of cohomological dimension at most 1 (e.g. : a finite field, an extension of $\mathbb{C}$ of transcendence degree 1). Then $H^1(k, G) = 0$ for any connected linear $k$-group $G$.

(See [Se94], III.2.3 and [St]).

**Theorem 7 (Kneser)** Let $G$ be a semi-simple connected linear $k$-group and $\tilde{G}$ its universal covering. Consider the central exact sequence:

$$1 \to F \to \tilde{G} \to G \to 1$$

($F$ is a finite and abelian $k$-group). Then the coboundary map $H^1(k, G) \to H^2(k, F)$ is a bijection when $k = \mathbb{R}$, $k$ is a $p$-adic field, or $k$ is a totally imaginary number field.

(See [Bor], Theorem 5.4.1).

**Theorem 8 (Borel-Serre)** Let $G$ be a (not necessarily connected) linear $k$-group. Then $H^1(k, G)$ is finite when $k = \mathbb{R}$ or $k$ is a $p$-adic field. If $k$ is a number field, the natural map: $H^1(k, G) \to \prod_{v \in \Omega} H^1(k_v, G)$ has finite fibers, where $\Omega$ denotes the set of all places of $k$.

(See [BS], 7.)
3. Torsors over a variety $X$

Let $X$ be a scheme and $G_X$ a smooth $X$-group scheme. It is possible to define the general notion of $X$-torsor under $G_X$. In this section, we will restrict ourselves to the case when $X$ is an algebraic variety defined over a perfect field $k$ and $G_X = G \times_k X$, where $G$ is an algebraic $k$-group. We shall frequently write $G$ instead of $G_X$.

Recall that an $X$-torsor under $G$ is a $k$-variety $Y$, equipped with a (flat) surjective morphism $f : Y \to X$ and a right action $(y, g) \mapsto y.g$ of $G$ on $Y$ such that $f(y, g) = f(y)$ for any $(y, g) \in Y \times G$, and $G(\bar{k})$ acts faithfully and transitively in each $\bar{k}$-fiber of $f$.

**Definition.** The trivial torsor is $Y = X \times G$, with the right action by translation of $G$ on the second component. Two $G$-torsors $f : Y \to X$ and $f' : Y' \to X$ are isomorphic if there exists an isomorphism of $k$-varieties $\varphi : Y \to Y'$ such that $f' \circ \varphi = f$ and $\varphi(y, g) = \varphi(y).g$ for each $y \in Y(\bar{k}), g \in G(\bar{k})$.

Note that an $X$-torsor $Y$ is trivial if and only if $f : Y \to X$ admits a section: indeed if $s$ is a section of $f$ then the trivial torsor $X \times G$ is isomorphic to $Y$ via $(x, g) \mapsto s(x).g$ , $x \in X(\bar{k}), g \in G(\bar{k})$.

A $G$-torsor can be viewed as an "algebraic family of $G$", so this notion is close to the notion of $G$-bundle in differential or analytic geometry. Therefore, it is important to understand whether a torsor, like a $G$-bundle, can be trivialized. The answer is clearly "no" if one restricts to the Zariski topology on $X$. For example, the only non empty Zariski open subset of Spec $k$ (the variety consisting of one $k$-point over $k$) is Spec $k$ itself, and we have seen many examples of non-trivial $k$-torsors in the first section. Even for a complex variety $X$, it is not difficult to construct torsors which are not locally trivial for the Zariski topology. The point is that the Zariski topology is too coarse. What is really needed is a generalization to arbitrary base fields of the complex topology, and this leads to the so-called \textit{étale} topology.

**Definition.** A (flat) morphism $f$ of $k$-varieties (or more generally of schemes) is \textit{étale} if all fibres of $f$ are smooth and finite. In particular an \textit{étale} $k$-algebra is a finite product of finite field extensions of $k$.

Now the fact that a $k$-torsor becomes trivial over a finite extension of $k$ extends via the following result: 

17
Theorem 9 Let $Y$ be an $X$-torsor under a smooth algebraic $k$-group $G$. Then there exists a family of étale morphisms $f_i : U_i \rightarrow X$ with $\bigcup_i f_i(U_i) = X$, such that for any $i$, the $U_i$-torsor $Y \times_X U_i$ is trivial.

This follows from the smoothness of $f : Y \rightarrow X$, which implies the existence of a section for the $U_i$-torsor $Y \times_X U_i$ if $U_i$ is well chosen\(^\text{10}\). See [EGA 4], 17.16.3 for more details. This statement means that any $X$-torsor is "locally trivial for the étale topology".\(^\text{11}\)

First examples of torsors:

1. Let $X \subset \mathbb{P}_k^n$ be a projective variety defined by homogeneous polynomial equations $P_i(x_0, \ldots, x_n) = 0$. Let $Y$ be the associated cone, defined in the affine space $\mathbb{A}^{n+1}_k$ by the equations $P_i(x_0, \ldots, x_n) = 0$, $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$. Then the projection $Y \rightarrow X$ makes $Y$ an $X$-torsor under $G_m$ via the obvious action $(x_0, \ldots, x_n) \lambda = (\lambda x_0, \ldots, \lambda x_n)$.

2. Let $G$ be a linear $k$-group and $H$ a closed subgroup. Then the quotient variety $X = G/H$ is well defined (by Chevalley’s theorem) and $X(\overline{k})$ is the set of left cosets of $G(\overline{k})$ modulo $H(\overline{k})$. The right action of $G$ on itself by translation makes $G$ an $X$-torsor under $H$.

3. Let $Y$ be a quasi-projective $k$-variety and $G$ be a finite $k$-group acting freely on $Y$ (that is: $y.g = y$ implies $g = 1$). Then $Y$ is a $G$-torsor over the quotient $X := Y/G$. In this case $Y \rightarrow X$ is étale.

Exercice. Let $X$ be a connected complex variety and $Y$ a connected unramified Galois covering of $X$ with group $G$ (in the usual sense). Show that $Y$ is an $X$-torsor under the group $G$, and that this torsor is not locally trivial for the Zariski topology if $G$ itself is not trivial.

Torsors and cohomology.

Let $X$ be an algebraic variety over a perfect field $k$ and $G$ a smooth algebraic $k$-group (one could also take a scheme $X$ and a smooth $X$-group scheme $G_X$). For any étale morphism $U \rightarrow X$, set $G(U) := \text{Hom}(U, G)$. Then $U \mapsto G(U)$ is a contravariant group functor; for any étale $X$-morphism

\(^{10}\)Since the $k$-variety $X$ is quasi-compact for Zariski topology, one $U_i$ is actually sufficient to trivialize a torsor.

\(^{11}\)The étale topology is not a topology in the usual sense. It is a "Grothendieck topology".
$U \to V$, the map $G(V) \to G(U)$ plays the same role as the restriction map associated to a presheaf on a topological space. This allows us to define Čech cohomology sets with the following construction\(^{12}\):

Let $\mathcal{U} = (U_i \xrightarrow{f_i} X)$ be an étale covering of $X$: that means that the maps $f_i$ are étale, and $\bigcup_i f_i(U_i) = X$. Set $U_{ij} = U_i \times_X U_j$ (this is the analog of the intersection of two open subsets in a topological space). A coycle (with respect to $\mathcal{U}$) is a family $g_{ij} \in G(U_{ij})$ such that $g_{ij}g_{jk} = g_{ik}$ on $U_{ijk} := U_i \times_X U_j \times_X U_k$ (this makes sense via the restriction maps $G(U_{ij}) \to G(U_{ijk}), G(U_{jk}) \to G(U_{ijk}), G(U_{ik}) \to G(U_{ijk})$). Let $Z^1(\mathcal{U}/X, G)$ be the set of cocycles. Then the cohomology set $H^1(\mathcal{U}/X, G)$ is the quotient of $Z^1(\mathcal{U}/X, G)$ by the equivalence relation: $(g_{ij}) \sim (g'_{ij})$ if there exists a family $h_i \in G(U_i)$ such that $g'_{ij} = h_i g_{ij} h_j^{-1}$ on $U_{ij}$. This set contains a distinguished element, the class of the trivial cocycle. As in the classical case of Čech cohomology on a topological space, the cohomology set $H^1(X, G)$ is then defined as the direct limit (on all étale coverings $\mathcal{U}$) of the pointed sets $H^1(\mathcal{U}/X, G)$.

Now let $Y$ be an $X$-torsor under $G$. There exists an étale covering $\mathcal{U}$ such that $Y$ is trivialized by $\mathcal{U}$. Fix local sections $y_i \in Y(U_i) := \text{Hom}_X(U_i, Y)$, then (by definition of a torsor) there exists a unique $g_{ij} \in G(U_{ij})$ such that $y_i g_{ij} = y_j$ on $Y(U_{ij})$. It is easy to check that $(g_{ij})$ is a cocycle whose class does not depend on the choice of the sections $y_i$, hence we obtain a map:

\[
\{ \text{Isomorphism classes of } X\text{-torsors under } G \text{ trivialized by } \mathcal{U} \} \to H^1(\mathcal{U}/X, G)
\]

and going over to the limit, this gives a map of pointed sets:

\[
\{ \text{Isomorphism classes of } X\text{-torsors under } G \} \to H^1(X, G)
\]

It is not difficult to see that this map is injective (a torsor is determined by the action of $G$ on a trivialization), but to prove the surjectivity (which is not true for any $G$), a good descent theory is needed (to go from the "sheaf of torsors" defined by a cocycle to a global torsor over $X$). As a matter of fact, this works if $G$ is a linear $k$-group or if $X$ is smooth and $G$ is an abelian variety (that is a projective algebraic $k$-group, e.g. an elliptic curve). See Milne, [Mil], III.4.3. We will always assume that one of these assumptions is satisfied.

If $X = \text{Spec } k$, one recovers the correspondence between $k$-torsors under $G$ and $H^1(k, G)$. In this case one can compute the cohomology with coverings $\mathcal{U}$ consisting of one map $f_1 : U_1 \to X$ of the form $\text{Spec } L \to \text{Spec } k$.

\(^{12}\)This would work with any "sheaf for the étale topology"; the contravariant functor $U \mapsto \text{Hom}_X(U, G_X)$ associated to an $X$-group scheme $G_X$ is a special case of étale sheaf.
(corresponding to the inclusion of fields $k \subset L$), where $L/k$ is a finite Galois extension. Then $U_{11} = \text{Spec } (L \otimes_k L)$, with $L \otimes_k L = \sum_{\gamma \in \text{Gal}(L/k)} L_{\gamma}$ (where $L_{\gamma} \cong L$); one can check that a Čech cocycle can now be viewed as a map $\text{Gal}(L/k) \to G(L)$ satisfying the classical cocycle condition in Galois cohomology (cf. Section 2).

If $G$ is commutative, then a comparison theorem states that the Čech cohomology set $H^1(X, G)$ agrees with the classical étale cohomology group (defined by derived functors).

**Properties of the cohomology set.**

The first four properties are very similar to the properties of Galois cohomology (cf. Section 2)

1. If $X' \to X$ is a morphism of $k$-varieties\(^{13}\), then there is an associated map $H^1(X, G) \to H^1(X', G)$. In terms of torsors, this sends the torsor $Y$ to the torsor $Y \times_X X'$.

2. If $p : G \to H$ is a morphisms of $k$-groups, there is a map $H^1(X, G) \to H^1(X, H)$. The torsor $Y$ is sent to the contracted product $Y' = Y \wedge^G H$.

In particular, if $H$ is the quotient of $G$ by a normal $k$-subgroup $H$, then $Y'$ is just the quotient of $Y$ by the action of $G$.

3. If $1 \to A \to B \to C \to 1$ is an exact sequence of $k$-groups, then there is an exact sequence of pointed sets

$$1 \to A(X) \to B(X) \to C(X) \to H^1(X, A) \to H^1(X, B) \to H^1(X, C)$$

where $A(X) = H^0(X, A) := \text{Hom}(X, A)$ is the set of morphisms of $k$-varieties $X \to A$. If $A$ is central in $B$, then there is a map $H^1(X, C) \to H^2(X, A)$ which extends the sequence.

4. Let $X' \to X$ be a Galois étale covering with group $E$ (that is: $X'$ is an $X$-torsor under the constant finite $k$-group $E$). Then we have the Hochschild-Serre exact sequence

$$1 \to H^1(E, H^0(X', G)) \to H^1(X, G) \to H^1(X', G)^E$$

Here $E$ acts on the group $H^0(X', G)$ and on the set $H^1(X', G)$ because $E$ acts on $X'$. Thus the cohomology set $H^1(E, H^0(X', G))$ makes sense and the set $H^1(X', G)^E$ of those elements of $H^1(X', G)$ which are invariant by $E$ is well defined too.

\(^{13}\)In the case of fields, an inclusion $k \subset L$ induces a morphism of $k$-varieties $\text{Spec } L \to \text{Spec } k$; we have sometimes written $X = k$ (abuse of notation) instead of $X = \text{Spec } k$. 

20
5. Let $A$ be a commutative $k$-algebra defined as the direct limit of $k$-algebras $A_i$. Set $U = \text{Spec} \ A$ and $U_i = \text{Spec} A_i$. Then $H^1(U, G)$ is the direct limit of the sets $H^1(U_i, G)$. If $X$ is an integral variety with function field $K$, we can apply this with $(U_i)$ consisting of all non empty open affine subsets of $X$, which gives: $H^1(K, G) = \lim H^1(U_i, G)$. In particular an $X$-torsor $Y$ under $G$ admits a local section for the Zariski topology if and only if the image of $[Y] \in H^1(X, G)$ in $H^1(K, G)$ ("restriction to the generic fibre") is trivial. $Y$ is locally trivial for the Zariski topology if and only if the image of $[Y]$ in $H^1(O_{X, m}, G)$ is trivial for any (scheme-theoretic) point $m$ of $X$ (where $O_{X, m}$ is the local ring of $X$ at $m$). The question to know whether the existence of a local section implies local triviality for the Zariski topology is quite delicate (this is part of the Grothendieck-Serre conjecture). In our context, it was solved affirmatively by Colliot-Thélène and Ojanguren ([CO], Theorem 3.2).

**Examples of cohomology sets.**

1. Let $G = G_a$. Then $H^1(K, G_a) = 0$ for any field $K$, so $X$-torsors under $G_a$ admit a generic section (that is: a section over a Zariski-dense open subset). One can show that $H^1(X, G_a) = H^1(X, O_X)$, where $H^1(X, O_X)$ is the classical Zariski cohomology group. This is zero as soon as $X$ is affine, hence $X$-torsors under $G_a$ are locally trivial for the Zariski topology.

2. Let $G = G_m$. By a slight generalization of Hilbert 90, one can prove that $H^1(\text{Spec} \ O, G_m) = 0$ (and even $H^1(\text{Spec} \ O, GL_n) = 0$ for each $n > 0$) for any local ring $O$, see [Mil], III.4.10). Thus $X$-torsors under $G_m$ (and also under $GL_n$) are locally trivial for the Zariski topology. It is possible to show that $H^1(X, G_m) = H^1(X, O_X)$, that is: $H^1(X, G_m)$ is the classical Picard group Pic $X$ of $X$. If $X = \text{Spec} \ A$, where $A$ is noetherian and is a unique factorization domain, then Pic $X = 0$.

3. Assume that $n$ is an integer which is not divisible by Char $k$. Then the Kummer exact sequence of $k$-groups

$$1 \to \mu_n \to G_m \xrightarrow{\alpha} G_m \to 1$$

gives rise to the exact sequence

$$k[X]^* \xrightarrow{\alpha} k[X]^* \to H^1(X, \mu_n) \to \text{Pic } X \xrightarrow{\alpha} \text{Pic } X$$

21
where $k[X]^*$ is the set of invertible functions on $X$. This can be rewritten as an exact sequence of abelian groups:

$$1 \to k[X]^*/k[X]^n \to H^1(X, \mu_n) \to \text{Pic } X$$

where $\text{Pic } X$ is the $n$-torsion part of $\text{Pic } X$. In particular, if $k$ is algebraically closed and $X$ projective, we obtain $H^1(X, \mu_n) = \text{n Pic } X$.

If Pic $X$ is torsion-free, then $H^1(X, \mu_n) = k[X]^*/k[X]^n$ and the torsor corresponding to $f \in k[X]^*/k[X]^n$ is given by the equations $u^n = f(x), x \in X$. We recover the case $X = \text{Spec } k, H^1(k, \mu_n) = k^*/k^*$. 

4. Assume $\text{Char } k = p > 0$. Let $F$ be the Frobenius automorphism $(F(x) := x^p)$. Then the Artin-Schreier exact sequence

$$1 \to \mathbb{Z}/p\mathbb{Z} \to G_a^{F-1} \to G_a \to 1$$

gives rise to the exact sequence of abelian groups

$$0 \to k[X]/(F - 1)k[X] \to H^1(X, \mathbb{Z}/p\mathbb{Z}) \to H^1(X, G_a)^F \to 0$$

where $k[X]$ is the set of regular functions on $X$ and $H^1(X, G_a)^F$ is the subgroup of $H^1(X, G_a)$ consisting of those elements which are invariant by the action of $F$ (induced by the action of $F$ on $G_a$). For example, if $k$ is algebraically closed and $X$ projective, then $H^1(X, \mathbb{Z}/p\mathbb{Z}) = H^1(X, G_a)^F$. If $X$ is affine $H^1(X, \mathbb{Z}/p\mathbb{Z}) = k[X]/(F - 1)k[X]$ and the torsor corresponding to $f \in k[X]/(F - 1)k[X]$ is given by the equations:

$$u^p - u + f = x, x \in X.$$ 

5. The exact sequence of $k$-groups

$$1 \to G_m \to GL_n \to PGL_n \to 1$$

is central and the induced map $GL_n(k) \to PGL_n(k)$ is surjective. Therefore there is an exact sequence of pointed sets

$$1 \to \text{Pic } X \to H^1(X, GL_n) \to H^1(X, PGL_n) \xrightarrow{\partial} H^2(X, G_m)$$

In particular, if $Y$ is an $X$-torsor under $PGL_n$, then there exists an $X$-torsor $Y'$ under $GL_n$ such that $Y \cong Y'/G_m$ if and only if $\partial([Y]) = 0$ in $H^2(X, G_m)$. 

6. **Torsors and the fundamental group.** Assume that $X$ is connected and fix $\bar{x} \in X(\bar{k})$. An $\bar{x}$-pointed Galois covering of $X$ is a pair $(Y, \bar{\gamma})$, where $Y \xrightarrow{f} X$ is a Galois étale covering of $X$ (that is: an $X$-torsor
under a finite and constant $k$-group) and $f(\bar{y}) = \bar{x}$. The *algebraic fundamental group* of $(X, \bar{x})$ is the projective limit, taken on all $\bar{x}$-pointed Galois connected coverings $(Y, \bar{y})$ of the groups $\text{Aut}(Y/X)$ (note that $\text{Aut}(Y/X)$ is just the structural group of the connected torsor $Y$). It is denoted by $\pi_1(X, \bar{x})$. If $\bar{x}'$ is another point of $X(\bar{k})$, then $\pi_1(X, \bar{x})$ and $\pi_1(X, \bar{x}')$ are isomorphic but the isomorphism is not canonical (it is defined up to conjugation, hence $\bar{x}$ is irrelevant if the fundamental group is abelian). $\pi_1(X, \bar{x})$ is a profinite group; for example if $\bar{x}$ corresponds to the inclusion $k \subset \bar{k}$, then $\pi_1(\text{Spec } k, \bar{x}) = \text{Gal}(\bar{k}/k)$ (the choice of $\bar{x}$ is equivalent to the choice of an algebraic closure of $k$).

Let $G$ be a finite group (equipped with the discrete topology). $G$ can also be viewed as a constant $k$-group. The datum of an $\bar{x}$-pointed Galois covering $(Y, \bar{y})$ of $X$ with group $G$ is equivalent to the datum of a continuous homomorphism $\pi_1(X, \bar{x}) \to G$. If we don’t specify the point $\bar{y}$, this homomorphism is defined only up to conjugation. In other words, we have an isomorphism of pointed sets from $H^1(X, G)$ to the set $\text{Hom}_c(\pi_1(X, \bar{x}), G)_{\text{conj}}$. The special case $X = \text{Spec } k$ is the classical equality $H^1(k, G) = \text{Hom}_c(\Gamma, G)_{\text{conj}}$, where $\Gamma = \text{Gal}(\bar{k}/k)$ (cf. Section 2).

When $X$ is a smooth complex algebraic variety, then $\pi_1(X, \bar{x})$ is the profinite completion of the classical topological fundamental group of $X$. The continuous representations $\pi_1^{\text{top}}(X) \to GL_n(C)$ are classified by a Čech cohomology set for the complex topology $H^1(X, GL_n(C))$. But this set is not the same as $H^1(X, GL_n)$ (defined via the étale topology): the sheaf associated to $GL_n$ is constant for the complex topology on $X$, but not for the étale topology. For example $H^1(X, C^*)$ is not equal in general to the Picard group $H^1(X, G_m)$ of $X$ (for $X = P^1$, $\text{Pic } X = \mathbb{Z}$ but $H^1(X, C^*) = 0$).

**Exercice.** Let $Y$ be an $X$-torsor under the group $SL_n$. Prove that $Y$ is locally trivial for Zariski topology (use the fact that the determinant map $GL_n \to G_m$ has a section).

**Torsors and $X$-forms.**

Recall (cf. Section 2) that $k$-forms of an algebraic variety $V$ are classified by the Galois cohomology set $H^1(k, \text{Aut}_V) := H^1(\Gamma, \text{Aut}_Y)$, where $\Gamma = \text{Gal}(\bar{k}/k)$ and $Y = X \times_k \bar{k}$. Similarly, if $V$ is a (not necessarily commutative) $k$-algebra, a quadratic space over $k$ etc., then $k$-forms of $V$
are classified by $H^1(k, \text{Aut}_{\mathcal{V}})$, where $\text{Aut}_{\mathcal{V}}$ is the group functor defined by $\text{Aut}_{\mathcal{V}}(L) = \text{Aut}(V \times_k L)$ (the automorphisms have to be taken for the considered structure). See [Se94], III.1 for more details.

Over an arbitrary $k$-variety (or a scheme) $X$, it works just the same. Let $Y \to X$ be an $X$-variety (resp. an $X$-presheaf of groups, algebras, vector spaces...for the étale topology, that is a contravariant functor $U \to Y(U)$ defined for any $U \to X$ étale). An $X$-form of $Y$ for the étale topology is an $X$-variety $Y' \to X$ (resp. an $X$-presheaf $Y'$) such that there exists an étale covering $\mathcal{U} = \{ U_i \to X \}$ satisfying: for any $i$, $Y(U_i) \cong Y'(U_i)$, where $Y(U_i) := Y \times_X U_i$ in the case when $Y$ is an $X$-variety.

Let $\text{Aut}_Y$ be the group functor $U \to \text{Aut}(Y(U))$, then the Čech cohomology sets $H^1(\mathcal{U}/X, \text{Aut}_Y)$ and $H^1(X, \text{Aut}_Y)$ are defined the same way as $H^1(X, G)$ for a $k$-group $G$.

Let $Y'$ be an $X$-form of $Y$ and $\mathcal{U} = \{ U_i \}$ be an étale covering of $X$ such that there exist isomorphisms $\varphi_i : Y \times_X U_i \to Y' \times_X U_i$ Set $U_{ij} = U_i \times_X U_j$ and $c_{ij} = \varphi_{ij}^{-1} \circ \varphi_j \in \text{Aut}_Y(U_{ij})$. Then $(c_{ij})$ is a cocycle whose class in $H^1(\mathcal{U}/X, \text{Aut}_Y)$ does not depend on the choice of $\varphi_i$. This class does not change if $Y'$ is replaced by an isomorphic $X$-form and we obtain a map of pointed sets:

\{ Isomorphism classes of $X$-forms trivialized by $\mathcal{U}$ \} $\to H^1(\mathcal{U}/X, \text{Aut}_Y)$

and going to the limit over all étale coverings $\mathcal{U}$ of $X$, this gives a map:

\{ Isomorphism classes of $X$-forms \} $\to H^1(X, \text{Aut}_Y)$

As usual, it is easy to prove that this map is injective. But surjectivity holds only if a good descent theory exists, so that one can obtain an $X$-form from forms defined locally (on each $U_i$). This will be the case in the following examples (cf. [SGA 1], VIII.7.8).

**Examples.**

1. A vector bundle of rank $n$ is a twisted form of the group scheme $G^n_k$ over $X$, so vector bundles of rank $n$ are classified by $H^1(X, GL_n)$. For $n = 1$, we recover the Picard group Pic $X$ as the set of isomorphism classes of line bundles over $X$. Note that for $X = \text{Spec } A$, a vector bundle of rank $n$ over $X$ is nothing but a projective $A$-module of rank $n$ ([Mil], I.2.9). Thus the property $H^1(O, GL_n) = 0$ for any local ring $O$ means that every projective $O$-module is free, and the same is true for any principal ideal domain $O$. The similar result when $X$ is the affine space (i.e. $A = k[T_1, ..., T_i]$) is the famous Serre’s problem, solved independently by Quillen and Suslin in 1976.
2. Let $X$ be a complex variety. Then a quadratic bundle of rank $n$ corresponds to a class in $H^1(X, O_n)$, where $O_n$ is the orthogonal group over $\mathbf{C}$. Recall the split exact sequence

$$1 \to SO_n \to O_n \rightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \to 1$$

Assume further that $X$ is a smooth and connected curve with field of meromorphic functions $C(X)$. Then $H^1(C(X), SO_n) = 0$ by Steinberg Theorem because $SO_n$ is connected and $C(X)$ is a field of cohomological dimension 1. In particular the map $H^1(C(X), O_n) \to H^1(C(X), \mathbb{Z}/2\mathbb{Z})$ has trivial kernel. This shows that a quadratic bundle over $X$ has a generic section if and only if the discriminant of the ”generic” quadratic form (which is defined over $\mathbf{C}(X)$) is trivial.

3. A Severi Brauer variety is a twisted form of $\mathbf{P}_X^n$ for the étale topology. An Azumaya algebra is a twisted form of $M_n(O_X)$ (this is the ”sheafified” version of a central simple algebra). Since $\text{Aut}(\mathbf{P}_X^n) = \text{Aut}(M_n(O_X)) = PGL_n \times X$, Severi Brauer varieties and Azumaya algebras are both classified by $H^1(X, PGL_n)$. Consider the central exact sequence

$$1 \to G_m \to GL_n \to PGL_n \to 1$$

and the associated cohomology sequence

$$\text{Pic} X \to H^1(X, GL_n) \to H^1(X, PGL_n) \xrightarrow{\partial} H^2(X, G_m)$$

The cohomological Brauer group of $X$ is defined as $H^2(X, G_m)$, and the Brauer group of $X$ is the subgroup of $H^2(X, G_m)$ consisting of the union of the images of the $\partial_n$’s for all $n \geq 2$. It is conjectured that the Brauer group is the whole $H^2(X, G_m)$ for any smooth variety $X$. When $X = \text{Spec} k$, this is a classical result of the theory of central simple algebras, cf. Serre, [Se68], X.5.

4. Two ”concrete” applications of torsors

i) Torsors and rational points

Let $k$ be a number field and $\Omega_k$ the set of its places. Denote by $k_v$ the completin of $k$ at $v$. For example, if $k = \mathbf{Q}$, then the completions are the $p$-adic fields $\mathbf{Q}_p$ ($p$ prime number) and the field $\mathbf{R}$ of real numbers.

Let $X$ be a projective and smooth $k$-variety. Set $X(\mathbf{A}_k) := \prod_{v \in \Omega_k} X(k_v)$ and assume that $X(\mathbf{A}_k)$ is not empty (that is: $X$ has points in any completion
of \( k \). The set \( X(k) \) of \( k \)-points of \( X \) is a subset of \( X(A_k) \) (via the diagonal embedding). In general, it is not true that \( X(k) \neq \emptyset \). Using torsors, we are going to give an obstruction to this property.

Let \( f : Y \to X \) be a torsor under a linear \( k \)-group \( G \) and \([Y]\) the class of \( Y \) in \( H^1(X, G) \). For each point \( P_v \in X(k_v) \), the evaluation \([Y](P_v)\) is an element of \( H^1(k_v, G) \). Denote by \( X(A_k)^f \) the subset of \( X(A_k) \) consisting of points \((P_v)_{v \in \Omega_k}\) such that \([Y](P_v)\) belongs to the image of \( H^1(k, G) \) (embedded into \( \prod_{v \in \Omega_k} H^1(k_v, G) \) by the diagonal map). Obviously we have \( X(k) \subset X(A_k)^f \).

Let us give a more general description of \( X(A_k)^f \). For any cocycle \( \sigma \in Z^1(k, G) \), the twisted torsor \( Y^\sigma \) is defined as follows: \( Y^\sigma \) is a \( k \)-form of \( Y \) (as a \( k \)-variety), and the action of \( \Gamma := \text{Gal}(k/k) \) on \( Y^\sigma \) is: \( \gamma(y) = y.\sigma^{-1}_y \), \( \gamma \in \Gamma, y \in Y(\bar{k}) \). Here \( \gamma y \) is the image of \( y \) by the action of \( \gamma \) on \( Y \), and \( \sigma^{-1} \) is the right action of \( \sigma^{-1} \in G(\bar{k}) \) on the \( G \)-torsor \( Y \). In particular \( Y^\sigma \) is a torsor under the twisted group \( G^\sigma \), which is an inner form of \( G \) (cf. Section 2). Recall that \( G^\sigma \) is a \( k \)-form of \( G \), the Galois action on \( G^\sigma \) being \( \gamma(g) = \sigma.\sigma^{-1}_\gamma \), \( \gamma \in \Gamma, g \in G(\bar{k}) \). If \( G \) is commutative, then \( G^\sigma = G \) and \([Y^\sigma] = [Y] - [\sigma] \) in the abelian group \( H^1(X, G) \), where the image of \([\sigma] \in H^1(k, G) \) in \( H^1(X, G) \) is still denoted by \([\sigma] \).

Now for any \( k_v \)-point \( P_v \) of \( X \), the condition \([Y](P_v) = [\sigma] \) is equivalent to \([Y^\sigma](P_v) = 0 \). Since \([Y^\sigma](P_v) = 0 \) is equivalent to: the fiber of \( Y^\sigma \) at \( P_v \) has a \( k_v \)-point, we obtain the description:

\[
X(A_k)^f = \bigcup_{[\sigma] \in H^1(k, G)} f^\sigma(Y^\sigma(A_k))
\]

where \( f^\sigma \) denotes the structural morphism \( Y^\sigma \to X \) of the torsor \( Y^\sigma \) and \( Y^\sigma(A_k) \) is the set of adelic points\(^{14} \) of \( Y^\sigma \).

In particular \( X(k) \neq \emptyset \) implies: there exists \( \sigma \in Z^1(k, G) \) such that \( Y^\sigma \) has points everywhere locally. The latter condition is more "computable" because it can be shown (as a corollary of Borel-Serre’s finiteness theorem) that there are only finitely many \([\sigma] \in H^1(k, G) \) such that \( Y^\sigma(A_k) \neq \emptyset \). Another consequence of this finiteness result is that not only \( X(k) \), but also the closure of \( X(k) \) in \( X(A_k) \) for the product of the \( v \)-adic topologies, is contained in \( X(A_k)^f \). See Skorobogatov, [Skö] for more details.

\[\text{2. The conjugacy problem}\]

Let \( k \) be a field of characteristic zero. Let \( M_1 \) and \( M_2 \) be two matrices of \( M_n(k) \). Assume that they are conjugate by an element of \( G(\bar{k}) \), where \( G \)

\(^{14}\) If \( G \) is not finite, then \( Y^\sigma \) is not proper over \( k \), so \( Y^\sigma(A_k) \) is not the direct product of the \( Y^\sigma(k_v) \)'s. Nevertheless, \( Y^\sigma(A_k) \neq \emptyset \) is equivalent to \( Y^\sigma(k_v) \neq \emptyset \) for all \( v \in \Omega_k \).
a linear $k$-group (embedded in $GL_n$). Are they conjugate by an element of $G(k)$?

Let $Z$ be the centralizer of $M_2$ in $G$ (this is the $k$-subgroup of $G$ defined by the equation $MM_2 = M_2M$). Set $Y_{M_1} (\bar{k}) = \{ M \in G(\bar{k}) \mid M^{-1} M_1 M = M_2 \}$. The natural Galois action on $Y_{M_1} (\bar{k})$ defines a $k$-variety $Y_{M_1}$, which is a torsor under the $k$-group $Z$, the action of $Z(\bar{k})$ on $Y_{M_1}(\bar{k})$ being $(y,z) \mapsto yz, y \in Y_{M_1}(\bar{k})$.

Fix $M_0 \in G(\bar{k})$ such that $M_0^{-1} M_1 M_0 = M_2$. Then $\gamma M_0 = M_0(M_0^{-1} \gamma M_0)$ for any $\gamma \in \Gamma$, so the class of $Y_{M_1}$ in $H^1(k, Z)$ is given by the cocycle $\gamma \mapsto c_\gamma = M_0^{-1} \gamma M_0$ (cf. Section 2). Conversely, if we fix $M_2$ and set $M_1 = M_0 M_2 M_0^{-1}$, then $c_\gamma = M_0^{-1} \gamma M_0$ is a cocycle of $Z^1(k, G)$ whose class in $H^1(k, G)$ is the same as the class of $Y_{M_1}$. Since cocycles (in $Z^1(k, Z)$) of the form $\gamma \mapsto M_0^{-1} \gamma M_0$ for some $M_0 \in G(\bar{k})$ are precisely the cocycles which are killed in $H^1(k, G)$, the problem reduces to the description of the kernel of the natural map $H^1(k, Z) \to H^1(k, G)$.

Examples:

- If $G = GL_n$, then $Z$ is an extension of a product of $R_{K_i/k}G_m$’s by $G^r$, so $H^1(k, Z) = 0$. Thus $M_1$ and $M_2$ are conjugate by an element of $GL_n(k)$ as soon as they are conjugate by an element of $GL_n(\bar{k})$. This is a classical result, which can be proven using the algebraic invariants.

- If $G = SL_n$, then $H^1(k, G) = 0$ (use the exact sequence $1 \to SL_n \to GL_n \to G_m \to 1$), but $H^1(k, Z)$ is not necessarily trivial. For example, it is easy to find a matrix $M_2$ such that $Z = R_{K/k}G_m$ for some finite field extension $K/k$. In this case $H^1(k, Z) = k^*/NK^*$ (cf. lecture 3). If $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, then the class of $-1$ is not trivial in $k^*/NK^*$, but $-1$ is a norm everywhere locally. This gives an example of two matrices with coefficients in $\mathbb{Q}$ which are conjugate by an element of $SL_n(\mathbb{Q}_p)$ for any prime number $p$ (and also by an element of $SL_n(\mathbb{R})$), but not by an element of $SL_n(\mathbb{Q})$.

- A more difficult question is the same conjugacy problem with rings instead of fields. Namely consider two matrices of $M_n(R)$, where $R$ is a Dedekind ring, and assume that they are conjugate by an element of $G(\bar{k})$, where $k$ is the field of fractions of $R$ and $G \subset GL_n$ is a linear $k$-group. If $G$ extends to a group scheme over $R$, we can define an $R$-torsor under the centralizer $Z$ as in the case of a field. If $G$ and $Z$ are smooth\(^\text{15}\), then we obtain a class in $\text{Ker}[H^1(R, Z) \to H^1(R, G)]$. Take

\(^{15}\)For non-smooth groups, the flat topology must be used instead of the étale topology.
for example $G = GL_2$. If $M_2 = \text{diag}(1, -1)$, then $Z = G_m \times G_m$ and $H^1(R, Z)$ is Pic $R \times$ Pic $R$. It can be shown that the map $H^1(R, GL_n) \to H^1(R, G_m)$ induced by the determinant is a bijection, so the kernel of Ker$[H^1(R, G_m \times G_m) \to H^1(R, GL_2)]$ is not trivial if $R$ is not principal. Note that in this case, the image of $H^1(R, Z)$ in $H^1(R/\varphi, Z)$ is zero for any non-zero prime ideal $\varphi$ of $R$ because $R/\varphi$ is principal. This gives examples of matrices which are conjugate "modulo $\varphi$" for any non-zero prime ideal $\varphi$ of $R$, but which are not conjugate by an element of $GL_2(R)$.

**Exercice:** Give explicit examples of matrices as above.

**References**

**Books.**


**Research papers.**

