Bas Edixhoven. Etale cohomology seminar, 2011/03/15.

Title: torsors and H^1 (reference: de Jong's "Stacks project").

Let $\mathcal{C}$ be a site. Let $\mathcal{X}$ and $\mathcal{Y}$ be sheaves of sets on $\mathcal{C}$.
Then we have presheaves on $\mathcal{C}$:

$$\mathcal{H}om(\mathcal{X},\mathcal{Y}) : \quad X \mapsto \mathrm{Hom}_{\mathcal{C}/X}(\mathcal{X}|_X, \mathcal{Y}|_X)$$
$$\mathcal{I}som(\mathcal{X},\mathcal{Y}) : \quad X \mapsto \mathrm{Isom}_{\mathcal{C}/X}(\mathcal{X}|_X, \mathcal{Y}|_X).$$

These presheaves are sheaves.

Argument for that: let $X \in \mathcal{C}$, $\mathcal{U} = (U_i \to X)_{i\in I}$ in $\mathrm{Cov}(X)$, and $(f_i : \mathcal{X}|_{U_i} \to \mathcal{Y}|_{U_i})_{i\in I}$ compatible; descent for sheaves (almost a tautology) says that

$$\mathrm{Sh}(\mathcal{C}/X) \longrightarrow (\mathrm{Sh}(\mathcal{U}) + \text{desc. data}) \quad \text{is an equivalence;}$$

so $\exists!\ f : \mathcal{X}|_X \to \mathcal{Y}|_X$ inducing the f_i.

Def. $\mathcal{X}$ and $\mathcal{Y}$ are locally isomorphic if $\forall X \in \mathcal{C}$ $\exists$ a cover $\mathcal{U} = (U_i \to X)_{i\in I}$ s.t. $\forall i \in I$ $\mathcal{X}|_{U_i}$ is isom. to $\mathcal{Y}|_{U_i}$.
And of course we use the same notion for sheaves of $\mathbb{Z}$-modules, etc.

Examples. 1. Locally free $\mathcal{O}_X$-modules of rank n on a ringed space $(X, \mathcal{O}_X)$

2. Central simple algebras of dim. n^2 on a field k with étale top., i.e., on $\mathrm{Spec}(k)_{ét}$ (small étale site).

3. Finite etale covers of degree n, on X_{et} (small site).

Now assume that $\mathcal{X}$ and $\mathcal{Y}$ are locally isomorphic.
Then $\mathrm{Aut}(\mathcal{Y}) \circlearrowright \mathcal{I}som(\mathcal{X},\mathcal{Y}) \circlearrowleft \mathrm{Aut}(\mathcal{X})$, commuting actions, is a typical example of a bi-torsor.

Def. Let $\mathcal{G}$ be a sheaf of groups on $\mathcal{C}$, $\mathcal{X}$ a sheaf of sets with a $\mathcal{G}$-action $\mathcal{G} \times \mathcal{X} \to \mathcal{X}$, ($\forall X \in \mathcal{C}$: $\mathcal{G}(X) \times \mathcal{X}(X) \to \mathcal{X}(X)$ is a $\mathcal{G}(X)$-action, functorial in X). The $\mathcal{X}$ is a $\mathcal{G}$-torsor if $(\mathcal{G}, \mathcal{X}, \text{action})$ is locally isomorphic to $(\mathcal{G}, \mathcal{G}, \text{left-transl.})$
Equivalently: $\forall X \in \mathcal{C}$: $\mathcal{G}(X)$ acts freely and transitively on $\mathcal{X}(X)$, and $\exists$ a cover $(U_i \to X)_{i\in I}$ s.t. $\mathcal{X}(U_i) \neq \emptyset$.

Back to the previous situation: $\mathcal{X}$ and $\mathcal{Y}$ locally isomorphic on $\mathcal{C}$.

Let $\mathcal{I} = \mathcal{I}som(\mathcal{X}, \mathcal{Y})$ and $\mathcal{G} = Aut(\mathcal{X})$.

then $\mathcal{I} \times \mathcal{X} \longrightarrow \mathcal{Y}$, $\mathcal{I}(X) \times \mathcal{X}(X) \to \mathcal{Y}(X)$, $(i,x) \mapsto i(x)$

is the quotient for the right $\mathcal{G}$-action $(i,x)\cdot g = (i\circ g, g^{-1}(x))$

Notation: $\mathcal{Y} = \mathcal{I} \otimes_{\mathcal{G}} \mathcal{X} = \left(X \mapsto (\mathcal{I}(X) \times \mathcal{X}(X))/\mathcal{G}(X)\right)^{\#}$.

~~Torsors and~~

The $\mathcal{G}$-torsors form a category $\{\mathcal{G}\text{-torsors}\}$, all morphisms in it are isomorphisms (it's a groupoid).

Relation with Cech cohomology: let $\mathcal{T}$ be a $\mathcal{G}$-torsor on $\mathcal{C}$, X in $\mathcal{C}$, and $(U_i \to X)_{i\in I}$ a covering s.t. $\forall i$: $\mathcal{T}(U_i) \ni t_i$ then $\forall (i,j) \in I^2$ $\exists!\, g_{i,j}$ in $\mathcal{T}(U_i \times_X U_j)$ s.t. $g_{i,j}\cdot t_j|_{U_i\times_X U_j} = t_i|_{U_i \times_X U_j}$; then $(g_{i,j})_{i,j\in I}$ is a cocycle: $\forall i,j,k$: $g_{i,j}\, g_{j,k} = g_{i,k}$ in $\mathcal{G}(U_i \times_X U_j \times_X U_k)$; and any set $t_i' \in \mathcal{T}(U_i)$ gives $g_{i,j}'$ differing by a coboundary.

Examples. 1. For $(X, \mathcal{O}_X)$ a ringed space, $\{Gl_{n,X}\text{-torsors}\} \rightleftarrows \{\text{loc. free } \mathcal{O}_X\text{-mod. rank } n\}$

$$\mathcal{T} \longmapsto \mathcal{T} \otimes_{Gl_{n,X}} \mathcal{O}_X^n, \quad \mathcal{I}som(\mathcal{O}_X^n, \mathcal{E}) \longleftarrow\!\shortmid\ \mathcal{E}$$

is an equivalence.

2. Let E/k be an ell. curve / a field, $n \in \mathbb{Z}_{\geq 1}$ inv. in k, $k \to \bar{k}$ a separable closure, $G = Aut_k(\bar{k})$ as topol. group.

Then $E(\bar{k})[n] \rightarrowtail E(\bar{k}) \xrightarrow{n\cdot} E(\bar{k})$ short exact in cat. of discrete G-sets with contin. G-action. For every $P \in E(k)$ we get $(n\cdot)^{-1}\{P\}$ an $E(\bar{k})[n]$-torsor in $\{\text{discrete } G\text{-sets}\}$.

Equivalent: $E[n] \rightarrowtail E \xrightarrow{n\cdot} E$ $(n\cdot)^{-1}\{P\}$ is a $E[n]$-torsor in $\mathrm{Spec}(k)_{\acute{e}t}$.

$$\begin{array}{ccc} E & \xrightarrow{n\cdot} & E \\ \uparrow & \square & \uparrow P \\ (n\cdot)^{-1}\{P\} & \rightarrowtail & \mathrm{Spec}\, k \end{array}$$

~~And~~ And if n not invertible in k: use $(Sch/k)_{fppf}$ or so.

3. For S a scheme an $n \in \mathbb{Z}_{\geq 1}$ inv. on S, $\mu_{n,S} \rightarrowtail \mathbb{G}_{m,S} \xrightarrow{n\cdot} \mathbb{G}_{m,S}$ is exact on $(Sch/S)_{et}$, hence for every $a \in \mathcal{O}_S(S)^\times$, we get the $\mu_{n,S}$-torsor $(n\cdot)^{-1}\{a\}$, e.g. if $S = \mathrm{Spec}(\mathbb{Q})$: $\mathrm{Spec}\, \mathbb{Q}[t]/(t^n - a)$.

(get examples of fppf μ_n-torsors that ~~are not locally for~~ are not trivial locally for étale topology ...)

For $\mathcal{G}_1 \xrightarrow{f} \mathcal{G}_2$ a morphism of sheaves of groups on $\mathcal{C}$, we have

$f_* : \{\mathcal{G}_1\text{-torsors}\} \to \{\mathcal{G}_2\text{-torsors}\}$, $\quad \mathcal{T} \mapsto \mathcal{G}_2 \otimes_{\mathcal{G}_1} \mathcal{T}$.

For $\mathcal{T}_1$ a $\mathcal{G}_1$-torsor and $\mathcal{T}_2$ a $\mathcal{G}_2$-torsor, $\mathcal{T}_1 \times \mathcal{T}_2$ is a $\mathcal{G}_1 \times \mathcal{G}_2$-torsor.

Hence for $\mathcal{G}$ a sheaf of comm. groups, $\mathcal{T}_1$ and $\mathcal{T}_2$ $\mathcal{G}$-torsors, we have $\cdot_*(\mathcal{T}_1 \times \mathcal{T}_2)$, the <u>sum</u> of $\mathcal{T}_1$ and $\mathcal{T}_2$, again a $\mathcal{G}$-torsor.

Our aim now: for $(\mathcal{C}, \mathcal{O})$ a ringed site, $\mathcal{F}$ an $\mathcal{O}$-module:

$$H^1(\mathcal{C}, \mathcal{F}) = \{\mathcal{F}\text{-torsors}\}/\cong .$$

<u>Step 1.</u> $\forall$ $\mathcal{O}$-module $\mathcal{F}$: $\quad H^0(\mathcal{C}, \mathcal{F}) = \mathrm{Hom}(\mathcal{O}, \mathcal{F}) \quad (= \Gamma(\mathcal{C}, \mathcal{H}om(\mathcal{O}, \mathcal{F})))$

$H^0(\mathcal{C},\mathcal{F}) = \{\text{compatible } s(X) \in \mathcal{F}(X),\ X \text{ in } \mathcal{C}\}$, $\quad \mathrm{Hom}(\mathcal{O},\mathcal{F}) = \{\text{compatible } f(X) : \mathcal{O}(X) \to \mathcal{F}(X),\ X \text{ in } \mathcal{C}\}$, $\quad 1 \mapsto ?$

Hence: $H^1(\mathcal{C}, \mathcal{F}) = (R^1 \mathrm{Hom}(\mathcal{O}, -))\,\mathcal{F} \overset{\text{def}}{=} \mathrm{Ext}^1_{\mathcal{O}}(\mathcal{O}, \mathcal{F})$

<u>Step 2.</u> Let $\mathcal{A}$ be an ab. cat. with suff. many injectives.

Then $\forall$ A, B in $\mathcal{A}$: $\quad \mathrm{Ext}^1(A,B) = \{B \rightarrowtail E \twoheadrightarrow A\}/\cong$,

where the extensions of A by B form a groupoid:

$$\begin{array}{ccccc} B & \rightarrowtail & E_1 & \twoheadrightarrow & A \\ \downarrow{\scriptstyle id_B} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle id_A} \\ B & \rightarrowtail & E_2 & \twoheadrightarrow & A \end{array}$$

(f is nec. an isomorphism)

<u>Note</u>: $\mathrm{Aut}(B \rightarrowtail E \twoheadrightarrow A) = \mathrm{Hom}(A,B) \quad (f \mapsto f - id_E)$.

Here is how it works: take $B \rightarrowtail I \twoheadrightarrow Q$ with I injective.

Apply $\mathrm{Hom}(A,-)$: $\quad \mathrm{Hom}(A,B) \rightarrowtail \mathrm{Hom}(A,I) \to \mathrm{Hom}(A,Q) \to \mathrm{Ext}^1(A,B) \to 0$

$f \in \mathrm{Hom}(A,Q) \mapsto [E_f] \in \{\text{ext'ns}\}/\cong$; $\quad \mathrm{Hom}(A,Q) \to \{\text{ext'ns}\}/\cong$, $\quad \mathrm{Ext}^1(A,B) \to \{\text{ext'ns}\}/\cong$

$$\begin{array}{ccccc} B & \rightarrowtail & I & \twoheadrightarrow & Q \\ \uparrow{\scriptstyle id_B} & & \uparrow & \square & \uparrow{\scriptstyle f} \\ B & \rightarrowtail & E_f & \twoheadrightarrow & A \end{array} \qquad \text{split} \iff \begin{array}{ccc} I & \twoheadrightarrow & Q \\ & \nwarrow{\scriptstyle \exists} & \uparrow{\scriptstyle f} \\ & & A \end{array}.$$

For
$$\begin{array}{ccccc} B & \rightarrowtail & E & \twoheadrightarrow & A \\ \downarrow{\scriptstyle id} & & \vdots & & \vdots \\ B & \rightarrowtail & I & \twoheadrightarrow & Q \end{array}$$
, gives: $\{\text{extns}\}/\cong \;\to\; \dfrac{\mathrm{Hom}(A,Q)}{\text{image of } \mathrm{Hom}(A,I)}$.

Step 3. Take $A = \mathcal{O}$-mod. ($\mathcal{O}$-modules on $\mathcal{C}$).

For $\mathcal{F}$ in $\mathcal{O}$-mod: $H^1(\mathcal{C}, \mathcal{F}) = \{\text{ext'ns } \mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}\}/\cong$.

Any ext'n $\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}$ is locally isomorphic to $\mathcal{F} \overset{i}{\rightarrowtail} \mathcal{F}\oplus\mathcal{O} \overset{p}{\twoheadrightarrow} \mathcal{O}$,

because $\forall X \in \mathcal{C}$ $\exists$ covering $(U_i \to X)_{i\in I}$, $s_i \in \mathcal{E}(U_i)$ s.t. $p(s_i) = 1 \in \mathcal{O}(U_i)$.

Hence: $\mathcal{E} = \mathcal{I}som(\mathcal{F}\oplus\mathcal{O}, \mathcal{E}) \otimes_{\mathcal{F}} (\mathcal{F}\oplus\mathcal{O})$

We have an equivalence:

$$\{\text{ext'ns of } \mathcal{O} \text{ by } \mathcal{F}\} \rightleftarrows \{\mathcal{F}\text{-torsors}\}.$$

This finishes the proof of: $H^1(\mathcal{C}, \mathcal{F}) = \{\mathcal{F}\text{-torsors}\}/\cong$.

Application. Let X be a scheme, $\mathcal{F}$ a quasi-coherent $\mathcal{O}_X$-module.

Then, for $i \in \{0,1\}$: $H^i(X, \mathcal{F}) = H^i((Sch/X)_{fpqc}, \mathcal{F})$

for $Y \overset{f}{\to} X$, $\mathcal{F}(Y) = (f^*\mathcal{F})(Y)$. René has shown that this is a sheaf.

For H^0: this is by definition.

Now $i=1$.

$H^1(X, \mathcal{F}) = \{\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}_X \text{ short ex. seq. of } \mathcal{O}_X\text{-modules}\}/\cong$

Note that such $\mathcal{E}$ are quasi-coherent.

$H^1((Sch/X)_{fpqc}, \mathcal{F}) = \{\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}$ sh. ex. seq. of $\mathcal{O}$-modules on $(Sch/X)_{fpqc}\}$.

1. $H^1(X,\mathcal{F}) \to H^1((\ )_{fpqc}, \mathcal{F})$: let $\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}_X$ on X_{Zar}.
   It is locally split, hence $\forall f: Y \to X$: $f^*\mathcal{F} \rightarrowtail f^*\mathcal{E} \twoheadrightarrow \mathcal{O}_Y$ exact on Y_{Zar}.
2. Let $\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}$ on $(Sch/X)_{fpqc}$. Take a cover $(U_i \to X)_{i\in I}$ on which the ext'n splits. Then $\mathcal{E}|_{U_i}$ is quasi-coherent. By fpqc descent of q.c. $\mathcal{O}$-modules, $\mathcal{E}$ is quasicoherent on X, and $\mathcal{F} \rightarrowtail \mathcal{E} \twoheadrightarrow \mathcal{O}$ splits locally on X_{Zar}. $\boxtimes$

Some extra thoughts.

1. Have we seen enough examples? Torsors that are not loc trivial for weaker topologies??

2. In this lecture, we considered sheaves on sites .... It is good to keep in mind, in the case of schemes, which sheaves are represented by schemes.
Descent of q.c. $\mathcal{O}$-modules $\rightsquigarrow$ descent of relative affine schemes, $\rightsquigarrow$ descent of projective schemes, quasi-affine, quasi projective?

3. What kind of torsors are loc. trivial for what kind of topology??
GL_n good, PGL_n not so good, $\mathbb{P}^n$ not good ....,
over finite fields: Lang's thm: for G smooth and connected over $\mathbb{F}_q$, all torsors on $\mathrm{Spec}(\mathbb{F}_q)_{et}$ are trivial.
(Let X be a G-torsor. As G is quasi-projective (or do devissage on G) X is represented by a scheme $/\mathbb{F}_q$, smooth & connected.
Take $a \in X(\overline{\mathbb{F}}_q)$. The morph. $G \longrightarrow G$, $g \longmapsto F(g)^{-1} g$ is surjective.
We want a $g \in G(\overline{\mathbb{F}}_q)$ s.t. $F(g \cdot a) = g \cdot a$
where $F(g\cdot a) = F(g) \cdot F(a)$ $\iff$ $F(g)^{-1} \cdot g \cdot a = F(a)$
$F: X_{\overline{\mathbb{F}}_q} \to X_{\overline{\mathbb{F}}_q}$ is the $\mathbb{F}_q$-Frobenius.)
(This last example, Lang's thm, proves Wedderburn's thm: every finite division algebra is a field).

4. Here is an exercise.

Let $k \supset \mathbb{F}_2$ be a field, and $a \in k$ not a square, and $E_a = V(y^2z = x^3 + ax^2z) \subset \mathbb{P}^2_k$.

Note that it has a cusp at $(0:0:1)$: $(y/z)^2 = (x/z)^3 + a\cdot(x/z)^2$.

The non-singular part E_a^{sm}, with the usual group structure with origin $(0:1:0)$, is isomorphic to $\mathbb{G}_a$ after base change to $k' = k[t]/(t^2-a)$, but not before, and not over any separable ext'n of k.

Indeed, $\mathrm{Aut}_{k^{sep}}(\mathbb{G}_{a,k^{sep}}) = (k^{sep})^\times$, hence there are no "étale twists" of $\mathbb{G}_{a,k}$. But over $k[\varepsilon]$ $(\varepsilon^2 = 0)$ we have the automorphism $x \mapsto x + \varepsilon\cdot x^2$ of $\mathbb{G}_{a,k[\varepsilon]}$. (in fact, any $\sum a_i x^{2^i}$ with a_i nilpotent for $i > 0$.)

Write down an isomorphism $\mathbb{G}_{a,k'} \xrightarrow[\sim]{\varphi} E^{sm}_{a,k'}$ and the compute the descent datum that $E^{sm}_{a,k'}$ induces on $\mathbb{G}_{a,k'}$ via φ. And verify the cocycle condition.

Here is how I see it. Let $k \to A$ be a k-algebra, and let $t \in A$ s.t. $t^2 = a$.

Then we have:

$$\mathbb{G}_{a,A} \xrightarrow{\sim} \underset{y^2z = x^3}{E^{sm}_{0,A}} \xrightarrow{\sim} \underset{y^2z = x^3 + t^2x^2z}{E^{sm}_{a,A}}$$

$$\varphi_{A,t} : \quad u \longmapsto (u:1:u^3) \longmapsto (u : 1+tu : u^3)$$

$$\varphi_{A,t}^{-1} : \quad \frac{x}{y+tx} \longleftarrow (x:y:z)$$

Here is the descent datum: for all A and t_1, t_2 in A with $t_1^2 = a = t_2^2$:

$$\varphi_{A,t_1,t_2} : \varphi_{A,t_2}^{-1} \circ \varphi_{A,t_1} : \quad u \mapsto (u : 1+t_1u : u^3) \mapsto \frac{u}{1+t_1u+t_2u} = \frac{u}{1+(t_1+t_2)u} =$$

$$= u\cdot(1+(t_1+t_2)u)$$

$$\text{(of course!)} \quad = u + (t_1+t_2)u^2.$$

(Note: $(t_1+t_2)^2 = a + a = 0$.)

Then we have, for A, t_1, t_2, t_3:

$$\varphi_{t_2,t_3} \circ \varphi_{t_1,t_2} : \quad u \mapsto u + (t_1+t_2)u^2 \longmapsto u + (t_1+t_2)u^2 + (t_2+t_3)u^2$$

$$= u + (t_1+t_3)u^2, \quad \underline{\text{indeed}}!!$$