Let $C$ be a site. Let $X$ and $Y$ be sheaves of sets on $C$.

Then we have presheaves on $C$:

\[ \text{Hom}(X,Y) : X \mapsto \text{Hom}_{C/X}(X|_X, Y|_X) \]

\[ \text{Isom}(X,Y) : X \mapsto \text{Isom}_{C/X}(X|_X, Y|_X) . \]

These presheaves are sheaves.

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

\[ \text{Sh}(C/X) \to (\text{Sh}(U) + \text{desc. data}) \]

is an equivalence; hence the $f_i : X|_U \to Y|_U$ inducing the $f_i$.

**Def.** $X$ and $Y$ are locally isomorphic if $\forall X \in C \exists$ a cover $U = (U_i \to X)_{i \in I}$ s.t. $\forall i \in I \; X|_{U_i}$ is isom. to $Y|_{U_i}$.

And of course we use the same notion for sheaves of $\mathbb{Z}$-modules, etc.

**Examples.**

1. Locally free $O_X$-modules of rank $n$ on a ringed space $(X,O_X)$

2. Central simple algebras of dim. $n^2$ over a field $k$ with
galois action, i.e., on Spec$(k)_e$ (small galois site).

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

Now assume that $X$ and $Y$ are locally isomorphic.

Then $\text{Aut}(Y) \subset \text{Isom}(X,Y) \cong \text{Aut}(X)$, commuting actions, is a typical example of a bi-tensor.

**Def.** Let $G$ be a sheaf of groups on $C$, $X$ a sheaf of sets with a $G$-action $G \times X \to X$, $(\forall X \in C : G(X) \times X(X) \to X(X)$ is a $G(X)$-action, functorial in $X$). The $X$ is a $G$-torsor if

\[ (G, X, \text{action}) \]

is locally isomorphic to $(G, G, \text{left-transl.})$.

Equivalently: $\forall X \in C : G(X)$ acts freely and transitively on $X(X)$, and $\exists$ a cover $(U_i \to X)_{i \in I}$ s.t. $X(U_i) \neq \emptyset$. 


Back to the previous situation: $X$ and $Y$ locally isomorphic in $\mathcal{C}$. Let $J = \text{Hom}(X, Y)$ and $G = \text{Aut}(X)$.

Then $J \times X \to Y$, $J(x) \times X(x) \to Y(x)$, $(i, x) \mapsto i(x)$ is the quotient for the right $G$-action $(i, x) \cdot g = (i \circ g, g(x))$.

**Notation:** $\mathcal{Y} = J \otimes_G X = \{ x \mapsto (J(x) \times X(x)) / G(x) \}^\#$.

**The $G$-tensors form a category $\{G$-tens$\}$, all morphisms in it are isomorphisms (it's a groupoid).**

**Relation with Čech cohomology:** let $T$ be a $G$-tens on $C$, $X \in \mathcal{C}$, and $(U \to X)_{i \in I}$ a covering s.t. $\forall i : T(U_i) \cong X$; then $\forall (i) \in I^2$ exists $g_{ij}$ in $T(U_i \cap U_j)$ s.t. $g_{ij} \cdot g_{ij} = 1_{U_i \cap U_j}$; then $\{ g_{ij} \}_{ij \in I}$ is a cocycle: $\forall i, j, k : g_{ij} \cdot g_{jk} = g_{ik}$ in $G(U_i \cap U_j \cap U_k)$; and any set $\{ u_i \in T(U_i) \}$ gives $g_{ij}$ differing by a coboundary.

**Examples.**

1. For $(X, O_X)$ a ringed space, $G = \text{Aut}_{O_X}$ - tensors $\varphi : \mathcal{O}_X \to \mathcal{E}$ is an equivalence.

2. Let $E/k$ be an ell. curve / a field, $n \in \mathbb{Z}_{\geq 1}$, inv. in $k$, $k \mapsto k^\text{sep}$ a separable closure, $G = \text{Aut}_{k^\text{sep}}(E)$ as top. group.

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

Equivalent: $E(k) \mapsto E \xrightarrow{n} E$ $(n)^{-1}(P)$ is a $E[n]$-tensor in $\text{Spec}(k)$. 

[Diagram]

Then And if $a$ not invertible in $k$: use $(\text{Sch}/k)^{fpf}$ or so.

3. For $S$ a scheme an $a \in \mathbb{Z}_{\geq 1}$, inv. on $S$, $\mathcal{O}_S \xrightarrow{\text{res}} \mathcal{G}_m \xrightarrow{n^{-1}} \mathcal{G}_m$ is exact on $(\text{Sch}/S)^{et}$, hence for every $a \in \mathcal{O}_S(S)^{\times}$, we get the $\mathcal{O}_S$-tens $\{ (n)^{-1}(a) \}$, e.g. if $S = \text{Spec}(O) : \text{Spec } O[\mathcal{E}] / (\mathcal{E}^n - a)$.

(see examples of $\mathcal{O}_E$-tens that the $a, n$-tensors are not trivial locally for finite topologies... -)
For $G_1 \to G_2$ a morphism of sheaves of groups on $C$, we have $3.$

$F : \{G_1, \text{torsor} \} \to \{G_2, \text{torsor} \}$, $F \to G_2 \otimes F$.

For $T_1$ a $G_1$-torsor and $T_2$ a $G_2$-torsor, $T_1 \times T_2$ is a $G_1 \times G_2$-torsor.

Hence for $G$ a sheaf of comm. groups, $T_1$ and $T_2$ $G$-torsors,

we have $\ast (T_1 \times T_2)$, the sum of $T_1$ and $T_2$, again a $G$-torsor.

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

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

**Step 1.** An $O$-module $F$: $H^0(C, \mathcal{O}) = \text{Hom}(\mathcal{O}, F)$ (as $\Gamma(C, \text{Hom}(\mathcal{O}, F))$

$\{ \text{compatible } s(x) \in F(x) \}$

$\{ \text{compatible } f(x) : \mathcal{O}(x) \to F(x), x \in C \}$

Hence: $H^1(C, \mathcal{O}) = (R^1 \text{Hom}(\mathcal{O}, -))(\mathcal{O}) \cong \text{Ext}_\mathcal{O}^1(\mathcal{O}, \mathcal{O})$.

**Step 2.** Let $A$ be an ab. cat. with suff. many injectives.

Then $\forall A, B$ in $\mathcal{A}$: $\text{Ext}^1(A, B) = \{ B \to E \to A \}/\cong$,

where the extensions of $A$ by $B$ form a groupoid:

$\begin{array}{ccc}
B & \xrightarrow{f} & E \\
\downarrow \cong & & \downarrow \cong \\
B & \xrightarrow{id_B} & E \\
\end{array}$

The extensions of $A$ by $B$ form a groupoid.

Note: $\text{Ext}^1(B \to E \to A) = \text{Hom}(A, B)$ ($f \mapsto f - id_E$).

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

Apply $\text{Hom}(A, -)$: $\text{Hom}(A, B) \to \text{Hom}(A, I) \to \text{Hom}(A, Q) \to \text{Ext}^1(A, B)$.

$\begin{array}{ccc}
B & \to & I \\
\uparrow \cong & & \uparrow \cong \\
B & \to & E \\
\end{array}$

For $B \to E \to A$, gives: $\{\text{extns} \}/\cong \to \text{Hom}(A, Q)$.

image of $\text{Hom}(A, I)$.
Step 3. Take $A = O$-mod. $(O$-module, on $C$).
For $F$ in $O$-mod; $H^i(C, F) = \left\{ \text{ext } F \to E \to O_C \right\} / \cong$.
Any extn $F \to E \to O$ is locally isomorphic to $F \to \mathcal{F} \otimes O$, because $\forall X \in C$ an covering $(U_i \to X)_{i \in I}$, $s \in E(U_i)$ st. $p(s) = 1 \in O(U_i)$.
Hence: $E = \text{Hom}(\mathcal{F} \otimes O, E) \otimes (\mathcal{F} \otimes O) / F$
We have an equivalence:
$$\{ \text{extn of } O \text{ by } F \} \cong \{ \text{F-trans} \}$$
This finishes the proof of: $H^i(C, F) = \{ \text{F-trans} \} / \cong$.

Application. Let $X$ be a scheme, $F$ a quasi-coherent $O_X$-module.
Then, for $i \in \mathbb{N}$, $H^i(X, F) = H^i((\text{Sch}/X)_{fqc}, F)$
For $H^0$: this is by definition.
Now $i=1$.
$H^1(X, F) = \{ F \to E \to O_X \text{ short ex. seq. of } O_X\text{-module} \} / \cong$
Note that such $E$ are quasi-coherent.
$H^1((\text{Sch}/X)_{fqc}, F) = \{ F \to E \to O \text{ sh. ex. seq. of } O\text{-modules} \}$
on $(\text{Sch}/X)_{fqc}$.
1. $H^1(X, F) \to H^1((\text{Sch}/X)_{fqc}, F)$: let $F \to E \to O_X$ on $X_{zar}$.
   It is locally split, hence $\forall f: Y \to X: f^*F \to f^*E \to \mathcal{O}_Y$ exact.
2. Let $F \to E \to O$ on $(\text{Sch}/X)_{fqc}$. Take a cover $(U_i \to X)_{i \in I}$ on $Y_{zar}$.
on which the extn splits. Then $E |_{U_i}$ is quasi-coherent. By
Taking descent, $E$ is quasi-coherent on $X$, and $F \to E \to O$ splits locally on $X_{zar}$. \hfill \Box
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. O-modules $\Rightarrow$ descent of affine schemes,
   - $\Rightarrow$ descent of projective schemes, quasi-affine, quasi-projective.

3. What kind of torsors are loc. trivial for what kind of topology? 

   - $\mathbb{G}_m$ good, $\mathbb{A}^n$ good, $\mathbb{G}_m$ not so good,
   - over finite fields: Lang's thm: for $G$ smooth and connected over $\mathbb{F}_q$, all torsors on $\text{Spec}(\mathbb{F}_q)$ are trivial.

   (Let $X$ be a torsor. As $G$ is quasi-projective (or do denominators in $G$) $\Rightarrow$ $X$ is represented by a scheme $\text{Spec}(R)$, smooth & connected. Take $x \in X(\mathbb{F}_q)$. The map $\mathbb{G}_m \to G$, defined by $\mathbb{G}_m \to G$ is surjective.

   We want a $x \in \mathbb{G}_m(\mathbb{F}_q)$ such that $F(g) \cdot x = g \iff F(g) \cdot x = F(x)$

   where $F: \mathbb{G}_m(\mathbb{F}_q) \to \mathbb{G}_m(\mathbb{F}_q)$ is the $\mathbb{F}_q$-Frobenius.

   (This last example, Lang's thm., proves Wedderburn's thm: every finite division algebra is a field.)
Let $k^s$ be a field, and $a$ not a square,
and $E_a = V(y^2 = x^3 + ax^2) \subseteq \mathbb{P}^2_k$.

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 $E_a^s$, with the usual group structure with
origin $(0:1:0)$, is isomorphic to $G_a$ after base change to $k' = k[t]/(t^2)$,
but not before, and not over any separable extn of $k$.

Indeed, $\text{Aut}_{k'}(G_a \mid k) = (k^s)^s$, hence there are no "$k$-bale twists" of $G_a$.
But over $k[t]$ ($t^2 = 0$) we have the automorphism
$x \mapsto x + t \cdot x^2$ of $G_a \mid k[t]$. (in fact, any $\sum q_i x^i$ with a nilptent
for $i > 0$.)

Write down an isomorphism $G_a \mid k \to E_a^s \mid k$, and the compute
the descent datum that $E_a^s \mid k$ inherits on $G_a \mid k$, via $\phi$.
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:

$$
E_{a,t} : \quad \begin{array}{c}
E_{a,t}^s \xrightarrow{\psi_{E_{a,t}}} E_{0,A}^s \xrightarrow{\psi_{E_{a,t}^s}} E_{a,t}^s
\end{array}
$$

$$
\psi_{E_{a,t}} : \quad \frac{x}{y+tx} \quad \xrightarrow{(u:1:u^2)} \quad (u:1+tu:u^2)
$$

$$
\psi_{E_{a,t}}^{-1} : \quad \frac{x}{y+tx} \quad \xleftarrow{(x:y:z)}
$$

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

$$
\xi_{E_{a,t_2}, E_{a,t_1}} : \quad u \mapsto (u:1+t_1u:u^2) \\ = \frac{u}{1+t_1u+t_2u} = \frac{u}{1+(t_1+t_2)u}
$$

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

$$
\xi_{E_{a,t_2}, E_{a,t_1}} = u + (t_1+t_2)u^2.
$$

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

$$
\xi_{E_{a,t_3}, E_{a,t_2}} : \quad u \mapsto u + (t_1+t_2)u^2 \\ = u + (t_1+t_3)u^2, \quad \text{indeed}.
$$