=

Lectures on Galois Theory. Some steps of generalizations

Jean-Jacques Szczeciniarz. *University Paris 7*

Journée Galois UNICAMP 2011bis, ter Ubatuba ?===

Content:

I want to present you Galois theory in the more general frame : descent theory. My first part will concern the descent of objects of fibered categories.

The second part will concern descent theory for quasi-coherent sheaves

The third part will concern the descent theory for morphism of schemas

The fourth part will concern descent along torsors. And inside this last theory Galois theory will take a natural place. I need some concepts as a preliminary

There is an obvious notion of left action of a functor into groups on a functor into sets

Definition. A left action of a functor $G : \mathcal{C}^{op} \to (Grp)$ on a functor $F : \mathcal{C}^{op} \to (Set)$ is a natural transformation $G \times F \to F$ such that for any object U of $\mathcal{C}$ $G(U) \times F(U) \to F(U)$ is an action of the group $G(U)$ on the set $F(U)$.

We denote the by $G \times F$ the functor that sends an object U of $\mathcal{C}$ to the product underlying the group GU with the set FU. In other words, $G \times F$ is the product $\tilde{G} \times F$ where G is the composite of G with the forgetful functor $(Grp) \rightarrow (Set)$.

Comment on the forgetful functor. It a conceptual tool in order to come back to the underlying level, in particular to the set (no)structure

Equivalently, a left action of G on F consists of an action of $G(U)$ on $F(U)$ for all objects U of $\mathcal{C}$, such that for any arrow $f : U \to V$ in $\mathcal{C}$, any $g \in G(V)$ and any $x \in F(V)$ we have $f^*g \cdot f^*x = f^*(g \cdot x) \in F(U)$

We can reformulate this definition in terms of commutative diagrams. Giving a left action of a group object G on an object X is equivalent to assign an arrow $\alpha : G \times X \to G$ such that the following two diagrams commute

(i) the identity of G acts like the identity on X:

$$\begin{array}{ccc} pt \times Y & \xrightarrow{e_G \times id_X} & G \times X \\ & \searrow \quad \swarrow {\scriptstyle \alpha} & \\ & X & \end{array}$$

(ii) the action is associative with respect to the multiplication on G

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{m_G \times id_X} & G \times X \\ \downarrow {\scriptstyle id_G \times \alpha} & & \downarrow {\scriptstyle \alpha} \\ G \times X & \xrightarrow{\alpha} & D \end{array}$$

f is G-equivariant if the diagram
$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ \downarrow{\scriptstyle id_G \times f} & & \downarrow{\scriptstyle f} \\ G \times Y & \longrightarrow & Y \end{array}$$
where the rows are given by the actions, commutes

Descent for modules over commutative rings

If A is a commutative ring, we will denote by Mod_A the category of modules over A. Consider a ring homomorphism $f : A \to B$. If M is an A-module we denote by

$$\iota_M : M \bigotimes_A B \simeq B \bigotimes_A M$$

the usual isomorphism of A- modules defined by $\iota_M(\eta \bigotimes b) = b \bigotimes \eta$. Furthermore one denote by $\alpha_M : M \to B \bigotimes_A M$ the homomorphism defined by $\alpha_M(m) = 1 \bigotimes m$ For each $r \geq 0$ set

$$B^{\bigotimes} = \overbrace{B \bigotimes_A B \bigotimes_A \cdots \bigotimes_A B}^{r \ \ times}$$

A B-module N becomes a module over $B^{\bigotimes 2}$ in two different ways as $N \bigotimes_A B$ and $B \bigotimes_A N$. In both cases the multiplication is defined by the formula: $(b_1 \bigotimes b_2)(x_1 \bigotimes x_2) = b_1x_1 \bigotimes b_2x_2$. Analogously, N becomes a module over $B^{\bigotimes 3}$as $N \bigotimes_A B \bigotimes_A B$, $B \bigotimes_A N \bigotimes_A B$, $B \bigotimes_A B \bigotimes_A N$. Let us assume that we have a homomorphism of $B^{\bigotimes 2}$ -modules $\psi : \; N \bigotimes_A B \to B \bigotimes_A N$

Then there are three associated homomorphisms of $B^{\bigotimes 3}$ modules:

$$\psi_1 : B \bigotimes_A N \bigotimes_A A \to B \bigotimes_A B \bigotimes_A N$$

$$\psi_2 : N \bigotimes_A B \bigotimes_A B \to B \bigotimes_A B \bigotimes_A N$$

$$\psi_3 : N \bigotimes_A B \bigotimes_A B \to B \bigotimes_A N \bigotimes_A B$$

by inserting the identity in the first, second and third position respectively

Let us define a category $Mod_{A\to B}$ as follows. Its objects are pairs (N,ψ) where N is a B-module and $\psi : N\otimes_A B \simeq B\otimes_A N$ is an isomorphism of $B^{\otimes 2}$ module such that :

$$\psi_2=\psi_1\circ\psi_3 : N\otimes_A B\otimes_A B \to B\otimes_A B\otimes_A N$$

An arrow $\beta : (N, \psi) \to (N', \psi')$ is a homomorphism of B-modules $\beta' : N \to N'$ making the diagram

$$\begin{array}{ccc} N \otimes_A B & \xrightarrow{\psi} & B \otimes_A N \\ \downarrow{\scriptstyle \beta \otimes id_B} & & \downarrow{\scriptstyle id_B \otimes \beta} \\ N' \otimes_A B & \xrightarrow{\psi'} & B \otimes_A N'' \end{array}$$

commutative We have a functor $F : Mod_A \to Mod_{A \to B}$ sending an A-module M to the pair $(B \otimes_A M, \psi_M)$ where

$$\psi_M : (B \otimes_A M) \otimes_A B \to B \otimes_A (B \otimes_A M)$$

is defined by the rule

$$\psi_M((b \otimes m \otimes b') = b \otimes b' \otimes m$$

It is checked that ψ_M is an isomorphism of $B^{\otimes 2}$-modules,

and that in fact $(M \otimes_A B, \psi_M)$ is an object of $Mod_{A\to B}$.
If $\alpha : M \to M'$ is a homomorphism of A-modules, one sees that $id_B \otimes \alpha : B \otimes_A M \to B \otimes_A M'$ is an arrow in $Mod_{A\to B}$. And this defines the desired functor$F$.

I want to present a theorem that explicits for this structure A-modules) the descent theory.
THEOREM. If B is faithfully flat over A, the functor

$$F : Mod_A \to Mod_{A\to B}$$

defined above is an equivalence of categories.
The proof is not so complicated. Let us define a functor $G : ModA \to B \to Mod_A$. And we have to show that GF is isomorphic to identity.
We can construct a natural transformation $\theta : id \to FG$ and then check that θ is an isomorphism.

This result states that quasi-coherent sheaves satisfy descent with respect to either topology. This is quite remarkable, because quasi-coherent sheaves are sheaves in that Zariski topology , which is much coarser, so a priori one would not expect this to happen.

Given a scheme S I recall that we can construct the fibered category $(QCoh/S)$ of quasi-coherent sheaves, whose fiber of a scheme$U$ over S is the category $QCoh(U)$ of quasi-coherent sheaves on U. And then we have the structural theorem THEOREM. Let S be a scheme. The fibered category $(QCoh/S)$ over (Sch/S) is stack with respect to the fpqc topology.

One of the most interesting examples of descent is descent theory for quasi-coherent sheaves along fpqc torsors. This can be considered as a vast generalization of the well-known equivalence between the category of real vector spaces and the category of complex vector spaces with anti-linear involution. Torsors are generalizations of principal fiber bundles in topology. Among the simplest examples of torsors are Galois field extensions, Angelo Vistoli says [].

Before I present you this descent theory, I need to recall some important tools. First of all I want to explain what the fpqc topology consists in

Because of difficulties to get a topology that well behaved, Steve Kleinman suggested the following definition.

PROPOSITION.Let $f : X$ be a surjective morphism of schemes. Then the following properties are equivalent.

(i) Every quasi-compact open subset of Y is the image of a quasi-compact open subset of X.

(ii) There exists a covering $\{V_i\}$ of Y by affine subschemes, such that each V_i is the image of a quasi-compact open subset.

(iii) Given a point $x \in X$, there exists an open neighborhood U of x in X, such that the image fU is open in Y and the restriction $f \to fU$ of f is quasi-compact.

(iv) Given a point $x \in X$ there exists a quasi-compact open neighborhood U of x in X, such that the image fU is open and affine in Y.

Some definitions

A morphism of schemes is a faithfully flat morphism that satisfies the equivalent conditions above. The abbreviation fpqc stands for "fidèlement plat et quasi-compact". A topological space is quasi-compact if every open cover of it has a finite subcover. Compact space for some people means quasi-compact and Hausdorff space.

An affine scheme is a locally ringed space isomorphic to $Spec(A)$ (the space of prime ideals of A) for some commutative ring$A$. A scheme is a locally ringed space X admitting a covering by open sets U s.t. the restriction of the structure sheaf O_X to each U_i is an affine scheme.

A ringed space is a pair $(X, O_X$, where X is topological space and O_X is a sheaf of rings on X.
A morphism of ringed spaces from $(X, O_X$ to (Y, O_Y) is a pair $(f, f^\sharp)$ where $f : X \to Y$ is a morphism of topological spaces and $f^\sharp O_Y \to f * O_Y$ is a morphism of rings on Y.

A morphism of schemes $f : X \to Y$ is *faithfully flat* if it is flat and surjective.
A morphism of schemes $f : X \to Y$ is flat if for any $x \in X$ the local ring $O_{X,x}$ is flat as a module over $O_{Y,f(x)}$
I recall this very important equivalence Let B be an algebra over A
(i) B is faithfully flat over A
(ii) A sequence of A- modules $M' \to M \to M''$ is exact if and only if the induced sequence of B-modules
$M' \bigotimes_A B \to M \bigotimes_A B \to M'' \bigotimes_A B$ is exact. Comment on the exact sequences and the tensor product.

minimal material for the descent theory along torsors

In a Grothendieck topology the open set of a space are the maps into this space. Instead of the intersections we have to look at fibered products while unions play no role.
Let C a category. A *Grothendieck topology* on C is the assignment to each object U of C of a collection of sets of arrows $\{U_i \to U\}$ called *coverings of* U, so that the following conditions are satisfied.
(i)If UV is an isomorphism, then the set of $\{U\}$ is a covering.
(ii)If $\{U_i \to U\}$ is a covering and $\{V \to U\}$ is any arrow then the fibered products exist $U_i \times_U V\}$ exists and the collection of projections $\{U_i \times_U V \to V\}$ is a covering.
(iii) If $\{U_i \to U\}$ is a covering, and for each index i we have a covering $V_{ij} \to U_i\}$ (here j varies on a set depending on i), the collection of composites $\{\{V_{ij} \to U_i \to U\}$ is a covering of U.

A representable functor on (Sch/S) is a sheaf in the fpqc topology. This amount to saying that, given two topological spaces U and X, an open covering $\{U_i \subseteq U\}$, and continuous functions : $f_i \to X$ with the property that the restriction of f_i and f_j to $U_i \cap \{U_j$ coincide for all i and j, there exists a unique continuous function $U \to X$ whose restriction $U_i \to X$ is f_i.
A topology $\mathcal{T}$ on a category C is called *subcanonical* if every representable functor on C is a sheaf with respect to $\mathcal{T}$.
Comment

torsors

Torsors are what in other fields of mathematics are called *principal bundles*.

Suppose that we have an object X of C, with a left action $\alpha : G \times X \to X$ of G. An arrow $X \to Y$ is called *invariant* if for each object U of C the induced function $X(U) \to Y(U)$ is invariant with respect to the action of $G(U)$ on $X(U)$. Another way of saying this is that the composites of $X \to Y$ with the two arrows α and pr_2 are equal.

Yet another equivalent definition is that the arrow f is G-equivariant when Y is given the trivial G -action $pr_2 : G \times Y \to Y$ by f Comment This "abstract" form sets a subtle kind of invariance. the fact that Y as an image of X is unchanged by an action on X

If $\pi : X \to Y$ is an invariant arrow and $f' : Y' \to Y$ is an arrow there is an induced action of G on $Y' \times_Y X$; this is the unique actions that makes the first projection

$$pr_1 : Y' \times_Y X \to Y' \text{ and the second projection} pr_2 Y' \times_Y X \to X$$

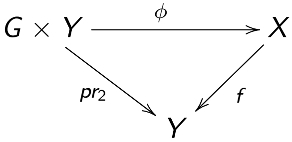
G-equivariant.

The first example of a torsor is the trivial torsor. For each object Y of $\mathcal{C}$ consider the product $G \times Y$. This has an action of G defined by the formula

$$g \cdot (h, x) = (gh, x)$$

for all objects U of $\mathcal{C}$ all g and h in $G(U)$ and all x in $X(U)$.

More generally, a *trivial torsor* consists of an object X of $\mathcal{C}$ with a left action of G together with an invariant arrow $f : X \to Y$ such that there is a G-equivariant isomorphism $\phi : G \times Y \simeq X$ making the diagram



commutative.

A *G-torsor* of $\mathcal{C}$ with an action of G and an invariant arrow $\pi : X \to Y$ that locally on Y is a trivial torsor.
DEFINITION
A *G-torsor* in $\mathcal{C}$ consists of an object X of $\mathcal{C}$ with an action of G and an invariant arrow $\pi : X \to Y$ such that there exists a covering $\{Y_i \to Y\}$ of Y with the property that for each i the arrow $pr_1 : Y_i \times_Y X \to Y_i$ is a trivial torsor
Comment. As a general objet a torsor is defined as being locally a trivial torsor exactly as for the scheme, for the bundle etc.

Every time we have an action $\alpha : G \times X \to X$ of G on an object X and an invariant arrow $f : X \to Y$ we get an arrow $\delta_a : G \times X \to X \times_Y Y$ defined as a natural transformation by the formula $(g, x) \mapsto (gx, x)$ for any object U of $\mathcal{C}$ and any $g \in G(U)$ and $x \in X(U)$. It is a characterization of torsors.

I want to present a very general proposition that is on essential properties of a G-torsor. Let X be an object of $\mathcal{C}$ with an action of G. An invariant arrow $\pi : X \to Y$ is a G-torsor if and only if
(i) There exists a covering $\{Y_i \to Y\}$ such that every arrow $Y_i \to Y$ factors through $\pi : X \to Y$
(ii) The arrow $\delta_a : G \times X \to X \times_Y Y$ is an isomorphism.

Let $K \subseteq L$ be a finite Galois extension with Galois group G. Denote by G_K the dicrete group scheme $G \times SpecK \to SpecK$ associated with G. The action G on $SpecL$ defines an action

$$\alpha : G_K \times_{SpecK} Spec\ L = G \times SpecL \to Spec\ L$$

of G_K on $Spec\ L$ which leaves the morphism $Spec\ L \to Spec\ K$ invariant. (Writing the action of G on L on the right, is for convenience).

By the primitive element theorem, L is generated as an extension of K by a unique element u. Let us denote by $f \in K[x]$its minimal polynomial. Then $L = K[x]/f(x)$. The acts on the roots of f simply transitively, so $f(x) = \prod_{g \in G}(x - ug) \in L[x]$

The morphism

$$\delta_\alpha : G \times Spec\ L \to Spec\ L \times_{SpecK} Spec\ L = Spec(L \bigotimes_K L)$$

corresponds to the homomorphism of K - algebras $L \bigotimes_K L \to L^G$ defined as $a \otimes b \to ((ag)b)_{g\in G}$ where L^G means the product of copies of L indexed by G

We have an isomorphism

$$L \bigotimes_K L = K[x]/(\prod_{g \in G}(x - ug)) \otimes_K L \backsimeq L[x]/(\prod_{g \in G}(x - ug))$$

by the chinese remainder theorem, the projection

$$L[x]/(\prod_{g \in G}(x - ug)) \to \prod_{g \in G} L[x]/(x - ug) \backsimeq L^G$$

is an isomorphism Thus we get an isomorphism $L \otimes L \backsimeq L^G$, that can seen to coincide with the hommoorphims corresponding to δ_α. Thus δ_α is an isomorphism. And since *Spec* $L \to$ *Spec* is étale , this show that *Spec*Ł is A G_K- torsor over *Spec* K
This the end of the explaining of the Galoisian example.