Geometria Algébrica I

lecture 16: Galois coverings and Galois categories

Misha Verbitsky

IMPA, sala 232

October 15, 2018

Covering maps

DEFINITION: Let $\varphi : \tilde{M} \longrightarrow M$ be a continuous map of manifolds (or CW complexes). We say that φ is **a covering** if φ is locally a homeomorphism, and for any $x \in M$ there exists a neighbourhood $U \ni x$ such that is a disconnected union of several manifolds U_i such that the restriction $\varphi\big|_{U_i}$ is a homeomorphism.

REMARK: From now on, M **is connected, locally conntractible topological space.**

THEOREM: A local homeomorphism of compacts spaces is a covering.

DEFINITION: Let Γ be a discrete group continuously acting on a topological space M. This action is called **properly discontinuous** if M is locally compact, and the space of orbits of Γ is Hausdorff.

THEOREM: Let Γ be a discrete group acting on M properly discontinuously. Suppose that the stabilizer group $\Gamma' : \mathrm{St}_\Gamma(x)$ is the same for all $x \in M$. **Then $M \longrightarrow M/\Gamma$ is a covering.** Moreover, **all covering maps are obtained like that.**

These results are left as exercises.

Category of coverings

DEFINITION: Fix a topological space M. **The category of coverings of M** is defined as follows: its objects are coverings of M, its morphisms are maps $M_1 \longrightarrow M_2$ commuting with projection to M.

DEFINITION: **A trivial covering** is a covering $M \times S \longrightarrow M$, where S is a discrete set.

EXERCISE: Let M be a space with properly discontinuous action of Γ. Suppose that the stabilizer group $\Gamma' : \mathrm{St}_\Gamma(x)$ is the same for all $x \in M$. Prove that **the covering $\pi: M \longrightarrow M/\Gamma$ is trivial if and only if π has a continuous section.**

Finite coverings

EXAMPLE: A map $x \longrightarrow nx$ in a circle S^1 is a covering.

EXAMPLE: For any non-degenerate integer matrix $A \in \operatorname{End}(\mathbb{Z}^n)$, the corresponding map of a torus T^n is a covering.

CLAIM: Let $\varphi: \tilde{M} \longrightarrow M$ be a covering, with M connected. **Then the number of preimages $|\varphi^{-1}(m)|$ is constant in M.**

Proof: Since $\varphi^{-1}(U)$ is a disconnected union of several copies of U, this number is a locally constant function of m. ∎

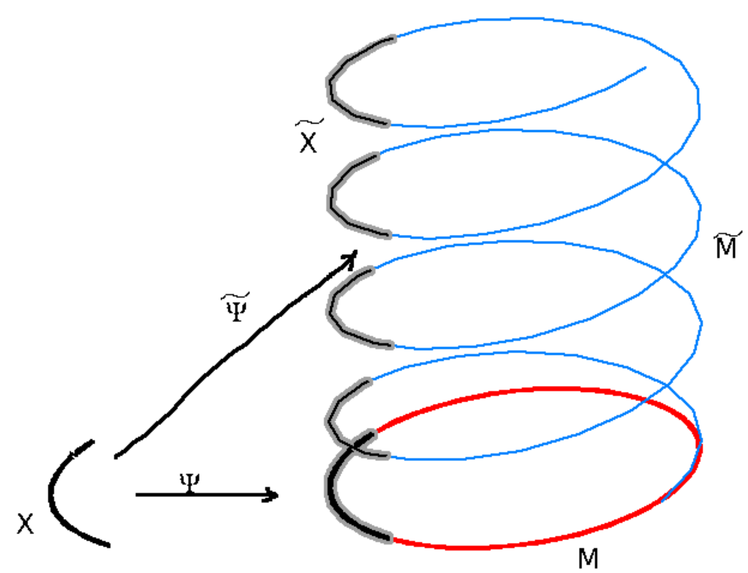
DEFINITION: Let $\varphi: \tilde{M} \longrightarrow M$ be a covering, with M connected. The number $|\varphi^{-1}(m)|$ is called **degree** of a map φ.

CLAIM: Any covering $\varphi: \tilde{M} \longrightarrow M$ with $\tilde{M}$ compact **has finite degree.**

Proof: Take U in such a way that $\varphi^{-1}(U)$ is a disconnected union of several copies of U, and let $x \in U$. Then $\varphi^{-1}(x)$ is discrete, and since $\tilde{M}$ is compact, any discrete subset of $\tilde{M}$ is finite. ∎

Homotopy lifting

LEMMA: ("Homotopy lifting lemma") The map $\varphi: \tilde{M} \longrightarrow M$ is a covering iff φ is locally a homeomorphism, and for any path $\Psi: [0,1] \longrightarrow M$ and any $x \in \varphi^{-1}(\Psi(0))$, **there is a lifting $\tilde{\Psi}: [0,1] \longrightarrow \tilde{M}$ such that $\tilde{\Psi}(0) = x$ and $\varphi(\tilde{\Psi}(t)) = \Psi(t)$.** Moreover, **the lifting is uniquely determined by the homotopy class of Ψ in the set of all paths connecting $\Psi(0)$ to $\Psi(1)$.**



Homotopy lifting

COROLLARY: If M is simply connected, **all connected coverings $\tilde{M} \longrightarrow M$ are isomorphic to M.** ■

Universal covering

THEOREM: Let M be a locally connected, locally simply connected space. **Then there exists a covering $\tilde{M} \longrightarrow M$, called universal covering, which is simply connected.** Moreover, **the universal covering is unique up to an isomorphism of coverings.**

Proof: Left as an exercise. ∎

CLAIM: In the above assumptions, let $\tilde{M}$ be connected. Then $\tilde{M}$ **is uniquely determined by a subgroup $G \subset \pi_1(M)$ of all loops which are lifted to closed loops.** Moreover, $M = \tilde{M}/G$, **where $\tilde{M}$ is the universal covering.**

Proof: Use the homotopy lifting lemma. ∎

Coverings and group actions

THEOREM: Fix a point $x \in M$. Then the category of coverings $\tilde{M} \xrightarrow{\sigma} M$ **is equivalent to the category of sets with $\Gamma := \pi_1(M, x)$-action.**

Proof. Step1: The set $\sigma^{-1}(x) \subset \tilde{M}$ is equipped with a natural Γ-action: for any loop $\gamma \subset M$ from x to itself representing $g \in \Gamma$, its lifting gives a map from $\sigma^{-1}(x)$ to itself, which is clearly compatible with the multiplication in $\pi_1(M, x)$.

Step 2: Let $\tilde{M}$ be the universal cover of M, and S be a set with Γ-action. Consider the set $S \times \tilde{M}/\Gamma \xrightarrow{\sigma} M$. This is clearly a covering over M, and $\sigma^{-1}(x) = S$ by construction. ■

Torsors

DEFINITION: Let G be a group. **G-Torsor** S is a set with free, transitive G-action. **Morphism** of G-torsors is a map of G-torsors which is compatible with G-action. **Trivialization** of a G-torsor is a choice of an isomorphism $S \cong G$, where G is considered as a G-torsor with left G-action.

REMARK: To chose a trivialization is the same as to chose an element $s \in S$. Indeed, the map taking unit to s is uniquely extended to an isomorphism $G \longrightarrow S$.

EXAMPLE: Affine space is a torsor over a linear space.

EXAMPLE: The set of all bases (basises) in a vector space $V = \mathbb{R}^n$ **is a torsor over a group $GL(n, \mathbb{R})$ of automorphisms of V.**

Torsors and quotient maps

EXAMPLE: Let $M_1 \xrightarrow{\pi} M = M_1/\Gamma$, where Γ freely acts on M_1. Then $\pi^{-1}(m)$ is Γ-torsor for any $m \in M$. However, to chose a trivialization of this torsor which depends continuously on m is the same as to chose a section, that is, trivialize the covering.

CLAIM: Let T be G-torsor. **Then $T \times T$ is naturally isomorphic to $T \times G$ as a G-torsor.**

Proof: For each $x, y \in T$, there exists a unique $g \in G$ such that $y = gx$. Therefore, the natural map $T \times G \longrightarrow T \times T$ mapping (x, g) to x, gx is an isomorphism of G-torsors. ■

Fibered products

DEFINITION: Let $X \xrightarrow{\pi_X} M, Y \xrightarrow{\pi_Y} M$ be maps of sets. **Fibered product** $X \times_M Y$ is the set of all pairs $(x, y) \in X \times Y$ such that $\pi_X(x) = \pi_Y(y)$.

CLAIM: Let $M_1 \longrightarrow M$ and $M_2 \longrightarrow M$ be coverings. **Then the fibered product $M_1 \times_M M_2$ is also a covering.**

Proof: The statement is local in M, hence it would suffice to prove it when $M_i = S_i \times M$, where S_i is a discrete set. Then $M_1 \times_M M_2 = S_1 \times S_2 \times M$, hence it is also a covering of M. ■

CLAIM: Let $M_1 \xrightarrow{\pi} M = M_1/\Gamma$, where Γ acts on M freely and properly discontinuously. **Then $M_1 \times_M M_1 = M_1 \times \Gamma$.**

Proof: Let $m \in M$. Then $\pi^{-1}(m)$ is a Γ-torsor. Using the natural isomorphism of Γ-torsors $\pi^{-1}(m) \times \pi^{-1}(m) = \pi^{-1}(m) \times G$, we obtain an isomorphism $M_1 \times_M M_1 = M_1 \times \Gamma$ of coverings. ■

Galois coverings

THEOREM: Let $\tilde{M} \xrightarrow{\sigma} M$ be a connected covering. **Then the following are equivalent.**

(i) $\pi_1(\tilde{M})$ is a normal subgroup in $\pi_1(M)$.

(ii) $\mathrm{Aut}_M(\tilde{M})$ acts freely on the set $\pi^{-1}(x)$, for any $x \in M$.

(iii) The fibered product $\tilde{M} \times_M \tilde{M}$ is isomorphic to $\tilde{M} \times S$, where S is a discrete set.

Proof: Left as a an exercise. ■

DEFINITION: A covering which satisfies any of these assumptions is called **a Galois covering**.

Galois theory for coverings

DEFINITION: Let $\tilde M \xrightarrow{\sigma} M$ be a covering, which is expressed as a composition

$$\tilde M \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M,$$

with $\tilde M$ and M_1 connected. In this case we say that M_1 is **an intermediate covering** between $\tilde M$ and M.

THEOREM: (**main theorem of Galois theory for coverings**)
Let $\tilde M \xrightarrow{\sigma} M$ be a Galois covering. **Then the intermediate coverings $M_1 \longrightarrow M$ are in bijective correspondence with the subgroups of the automorphism group $\operatorname{Aut}_M(\tilde M)$,** which is called **the Galois group of the covering**.

Galois extensions (reminder)

DEFINITION: Let $[K:k]$ be a finite extension. It is called **a Galois extension** if the algebra $K\otimes_k K$ is isomorphic to a direct sum of several copies of K.

EXERCISE: Let $K = k[t]/(P)$ be a primitive, separable extension, with $\deg P(t) = n$.

1. **Prove that $[K:k]$ is a Galois extension if and only if $P(t)$ has n roots in $K[t]$.**

2. Consider an extension $[K':K]$ obtained by adding all roots of all irreducible components of $P(t)\in K[t]$. **Prove that $[K':k]$ is a Galois extension.**

EXERCISE: Prove that $[K:k]$ is a Galois extension if and only if $\operatorname{Aut}_k(K)$ acts transitively on all components of $K\otimes_k \bar{k} = \bar{k}^n$.

Galois group (reminder)

EXERCISE: Let $[K : k]$ be a finite extension, and $G := \operatorname{Aut}_k K$ the group of k-linear automorphisms of K. Prove that **$[K : k]$ is a Galois extension if and only if the set K^G of G-invariant elements of K coincides with k.**

DEFINITION: Let $[K : k]$ be a Galois extension. Then the group $\operatorname{Aut}_k K$ is called **the Galois group of $[K : k]$**.

THEOREM: **(Main theorem of Galois theory)**
Let $[K : k]$ be a Galois extension, and $\mathcal{G}al_k K$ its Galois group. **Then the subgroups $H \subset \mathcal{G}al_k K$ are in bijective correspondence with the intermediate subfields $k \subset K^H \subset K$,** with K^H obtained as the set of H-invariant elements of K.

EXERCISE: Prove that for any $q = p^n$ there exists a finite field $\mathbb{F}_q$ of q elements. Prove that $[\mathbb{F}_q : \mathbb{F}_p]$ is a Galois extension. Prove that its Galois group is cyclic of order n, and generated by **the Frobenius automorphism** mapping x to x^p.

Limits and colimits of diagrams

DEFINITION: Diagram in a category $\mathcal{C}$ is an oriented graph with objects of $\mathcal{C}$ in vertices and morphism in edges.

DEFINITION: Let $S = \{X_i, \varphi_{ij}\}$ be a diagram in $\mathcal{C}$, and $\vec{\mathcal{C}}_S$ be a category of pairs (object X in $\mathcal{C}$, morphisms $\psi_i : X \longrightarrow X_i$, defined for all X_i) making the diagram formed by $(X, X_i, \psi_i, \varphi_{ij})$ commutative for each edge of S. The terminal object in this category is called **limit**, or **inverse limit** of the diagram S.

DEFINITION: Colimit, or **direct limit** is obtained from the previous definition by inverting all arrows and replacing "terminal" by "initial".

EXAMPLE: Let Γ be $\mathbb{Z}$ or some interval in $\mathbb{Z}$, and S a diagram in the category of sets with all maps $\varphi_{i,i+1} : X_i \longrightarrow X_{i+1}$ injective. Then **limit of S is intersection of all X_i, and colimit is their union.**

Products and coproducts

EXAMPLE: Let S be a diagram with two vertices X_1 and X_2 and no arrows. The inverse limit of S is called **product** of X_1 and X_2, and inverse limit **the coproduct**.

EXAMPLE: Products in the category of sets, vector spaces and topological spaces are the usual products of sets, vector spaces and topological spaces **(check this)**.

EXAMPLE: Coproduct in the category of groups is called **free product**, or **amalgamated product**. Coproduct of the group $\mathbb{Z}$ with itself is called **free group**. Coproduct in the category of vector spaces is also the usual product of vector spaces.

EXERCISE: Let $\mathcal{C}$ be the category of coverings of M. Prove that **the product in $\mathcal{C}$ is fibered product over M.** Prove that **coproduct is a disjoint union of coverings.**

EXERCISE: Let k be a field of characteristic 0 and $\mathcal{C}$ the category of finite-dimensional semisimple k-algebras. Prove that **the coproduct in $\mathcal{C}$ is tensor product over k and product is direct sum of fields.**

Fibered product (reminder)

DEFINITION: Consider the following diagram:

$$\begin{tikzcd} A \arrow[dr] & & B \arrow[dl] \\ & C & \end{tikzcd}$$

Its limit is called **fibered product** of A and B over C. Colimit of the diagram

$$\begin{tikzcd} & C \arrow[dl] \arrow[dr] & \\ A & & B \end{tikzcd}$$

is called **coproduct** of A and B over C.

EXERCISE: Prove that the **fibered product of algebraic varieties is the same as their product in the category of algebraic varieties.**

EXERCISE: Prove that the **coproduct of rings A and B over C is $A \otimes_C B$.** Prove that the **coproduct of reduced rings A and B over C in the category of reduced rings $A \otimes_C B/I$, where I is nilradical.**

Epimorphisms, monomorphisms, group quotients

DEFINITION: Let $\mathcal{C}$ be a category. A morphism $\varphi: X \longrightarrow Y$ is called **an epimorphism** if for any two distinct $\psi_1, \psi_2: Y \longrightarrow Z$, the compositions $\varphi \circ \psi_1$ and $\varphi \circ \psi_2$ are distinct. It is called **a monomorphism** if for any two distinct $\psi_1, \psi_2: Z \longrightarrow X$, the compositions $\psi_1 \circ \varphi$ and $\psi_2 \circ \varphi$ are distinct.

DEFINITION: **Group action** on an object X in category $\mathcal{C}$ is a map $\rho: G \longrightarrow \mathcal{M}or(X,X)$ from the group G to $\mathcal{M}or(X,X)$ compatible with the product. **G-invariant morphism** is a morphism $\varphi: X \longrightarrow Y$ such that for any $g \in G$, one has $\rho(g) \circ \varphi = \varphi$. **Group quotient** $Y = X/G$ is a G-invariant map $X \longrightarrow Y$ such that the composition map $\mathcal{M}or(Y,Z) \longrightarrow \mathcal{M}or(X,Z)$ induces a bijection between $\mathcal{M}or(Y,Z)$ and the set $\mathcal{M}or(X,Z)^G$ of G-invariant morphisms.

Galois categories

DEFINITION: Let $\mathcal{C}$ be a category equipped with a functor $F: \mathcal{C} \longrightarrow \mathcal{S}ets$ called **the fiber functor**. It is called **Galois category** if the following holds.

(i) $\mathcal{C}$ **contains a terminal object, initial object, fibered product of any two objects over a third, and finite coproducts ("direct sums")** of any objects in $\mathcal{C}$.

(ii) $\mathcal{C}$ **contains finite group quotients.**

(iii) Any morphism in $\mathcal{C}$ **is a composition of an epimorphism and a monomorphism.** Any monomorphism $\varphi: X \longrightarrow Y$ **is an isomorphism of** X **and a direct summand of** Y**.**

(iv) The fiber functor F **commutes with the fiber products, finite coproducts and finite group quotients.** Moreover, for any morphism u such that $F(u)$ is an isomorphism, u **is also an isomorphism.**

DEFINITION: Let G be a group. **Finite sets with G-action** form a category, with $\mathcal{M}or(X,Y)$ the set of all maps from X to Y compatible with the action of G. Clearly, **this category is a Galois category**.

EXAMPLE: Category of finite coverings of M is a Galois category.

EXAMPLE: Let $\mathcal{C}$ be the category of k-algebras isomorphic to finite direct sums of finite separable extensions of k. **Then its opposite $\mathcal{C}^{op}$ is a Galois category.** The fiber functor F maps $[K:k]$ to the set of irreducible idempotents in the algebra $K \otimes_k \overline{k} = \overline{k}^n$.

Finite sets with G-action

THEOREM: (Grothendieck)
Let $\mathcal{C}$ be a Galois category. **Then $\mathcal{C}$ is equivalent to a category of finite sets with action of a group $G(\mathcal{C})$.**

DEFINITION: Profinite completion $\hat{G}$ of a group G is a the limit of all its finite quotient groups. A group is called **profinite** if it is isomorphic to its profinite completion.

REMARK: Category of finite sets with G-action is clearly equivalent to the category of finite sets with $\hat{G}$-action. Indeed, **the set of homomorphisms from G to a finite group Γ is identified with the set of homomorphisms from $\hat{G}$ to Γ.**

THEOREM: In Grothendieck's theorem, the group $G(\mathcal{C})$ can be always replaced by its profinite completion $\hat{G}(\mathcal{C})$, **which is uniquely determined by the Galois category $\mathcal{C}$ and its fiber functor.** Moreover, **$\hat{G}(\mathcal{C})$ is isomorphic to the group of automorphisms of the fiber functor.**

DEFINITION: The group $\hat{G}(\mathcal{C})$ is called **the absolute Galois group of $\mathcal{C}$**.