GROTHENDIECK'S GALOIS THEORY

1. Classical Galois theory

These notes closely follow [DV00]. Last week Deik used the topos theoretical version of Grothendieck's Galois theory to construct the fundamental group of a topos. This week we will focus on the profinite case, originally developed by Grothendieck to construct the étale fundamental group of a scheme [GR04].

The goal of this talk will be to sketch the proof of, and hopefully motivate, Grothendieck's Galois correspondence. To start with, we recall the classical Galois correspondence.

Definition 1. A finite field extension K/F is **Galois** over F if $\#\operatorname{Aut}(K/F) = [K\colon F]$. Its corresponding group of automorphisms is denoted $\operatorname{Gal}(K/F) = \{\sigma\colon K \to K | \sigma x = x \,\forall x \in F\}$.

Theorem 1 (The Galois correspondence)**.** Let K/F be a Galois extension and $G := \operatorname{Gal}(K/F)$. Then there is an order reversing correspondence between the intermediate field extensions $F \subseteq L \subseteq K$ and the subgroups of $\operatorname{Gal}(K/F)$ given by:

$$\begin{aligned} L &\longmapsto \operatorname{Aut}(K/L) \\ \operatorname{Fix}(H) &\longleftarrow\!\shortmid H \end{aligned}$$

where $\operatorname{Fix}(H) = \{x \in K | \sigma(x) = x \,\forall \sigma \in H\}$.

We can reformulate this categorically by defining what it means for a group to act on an object A of a category $\mathcal{C}$. From now on let $\mathcal{C}$ be a category and $A \in \operatorname{Ob}(\mathcal{C})$.

Definition 2 (Group action)**.** Let $H \in \mathbf{Grp}$. A **left action** H **on** A is a group homomorphism $\alpha\colon H \to \operatorname{Aut(A)}^{\mathrm{op}}$.

Definition 3 (Quotienting by actions)**.** The **quotient** of A by H is a morphism $q\colon A \to A/H$ in $\mathcal{C}$ such that $q \circ \alpha(h) = q$ for all $h \in H$ such that for all $A \xrightarrow{x} X$ such that $x \circ \alpha(h) = x$ there exists a unique $\varphi\colon A/H \to X$ such that

$$\begin{tikzcd} A \arrow[r, "q"] \arrow[d, "x"'] & A/H \arrow[dl, dashed, "!\varphi"] \\ X & \end{tikzcd}$$

commutes.

Remark 1. Quotienting by a group action can be seen as taking a certain (finite) colimit.

Example 1. Let $\mathbf{Ext}_{K/F}$ be the category of intermediate field extensions $F \subseteq L \subseteq K$. Then for any subgroup $H \leq \operatorname{Gal}(K/F)$ the fixed field of H, $\operatorname{Fix}(H)$ is the quotient K/H. To see this, note that $\operatorname{Fix}(H)$ is the largest subfield of K fixed by H. I.e. the largest subfield such that for all $h \in H$, $h \circ i = i$ where $i\colon \operatorname{Fix}(H) \hookrightarrow K$ is the inclusion. Reformulating this in terms of $\mathbf{Ext}_{K/F}^{\mathrm{op}}$, the map $K \to \operatorname{Fix}(H)$ is the quotient of K by H.

In light of this example, we can reformulate the Galois correspondence in terms of these categorical group actions. First note that given an $L \in \mathbf{Ext}^{\mathrm{op}}_{K/F}$, $[K, L]$ is a transitive $G := \mathrm{Aut}(K/F)^{\mathrm{op}}$-Set under the action

$$G \times [K, L] \to [K, L], (g, x) \mapsto x \circ g.$$

We will denote this G-Set by $[K, L]_G$. Thus we can reformulate the Galois correspondence as:

Theorem 2 (Reformulated Galois correspondence)**.** Let K/F be Galois and $G := \mathrm{Gal}(K/F)$ then there is an equivalence of categories,

$$\begin{tikzcd} \mathbf{Ext}^{\mathrm{op}}_{K/F} \arrow[r, bend left, "{[K,-]_G}"] & G - \mathbf{Set}^{trans} \arrow[l, bend left, "K/-"] \end{tikzcd}$$

One can construct such an equivalence for a more general class of categories. Let $\mathcal{C}$ be a category and A an object in $\mathcal{C}$. Suppose that for all $X \in \mathrm{Ob}(\mathcal{C})$, $[A, X]_G$ is a transitive $G = \mathrm{Aut}(A)^{\mathrm{op}}$-Set. Note that for any $S \in G - \mathbf{Set}^{\mathrm{trans}}$ and $x_0 \in S$, $S \cong G/\operatorname{Fix}(\mathrm{x_0})$. We can construct its left adjoint as follows:

Construction 1 (The left adjoint)**.** We will show that the functor $[A, -]_G \colon \mathcal{C} \to G - \mathbf{Set}^{\mathrm{trans}}$ has a left adjoint. As pointed out in the lecture, we assume $\mathcal{C}$ has quotients. By noting that G itself is a G-Set with one generator, for any $E \in G - \mathbf{Set}^{\mathrm{trans}}$ there is a $1-1$ correspondence between the elements of E and G-equivariant maps $G \to E$ given by $(x \in E) \longmapsto \varphi$ where φ is the map given by $e \mapsto x$. Now take $E = [A, X]_G$ for any object X in $\mathcal{C}$. Again taking any G-Set S and $H = \mathrm{Fix}(x_0)$ for $x_0 \in S$, by the universal property of the quotient by an action, $A \to X$ factors through A/H if and only if $G \to [A, X]_G$ factors through $G \to G/H \cong S$. As a result $\mathrm{Hom}_{\mathcal{C}}(A/H, X) \cong \mathrm{Hom}_{G-\mathbf{Set}^{\mathrm{trans}}}(S, [A, X]_G)$. So the functor $[A, -]_G$ has a left adjoint $A/- : S \mapsto A/\operatorname{Fix}(x_0)$ where $x_0 \in S$:

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "{[K,-]_G}"] \arrow[r, phantom, "\top"] & G - \mathbf{Set}^{\mathrm{trans}}. \arrow[l, bend left, "K/-"] \end{tikzcd}$$

Before we put conditions on $\mathcal{C}$ such that this adjunction becomes an equivalence, we need to define what it means to be a strict epimorphism. We call $f \colon X \to Y$ an effective epimorphism if it is the coequalizer of its kernel pair.

In a category without pullbacks, we still want such a notion, and hence reexpress it in terms of its universal property, we call this a strict epimorphism.

Definition 4 (Strict epimorphism)**.** A morphism $f \colon X \to Y$ is **strictly epimorphic** if for any $g \colon X \to Z$ such that for all $x, y \colon C \to X$, $g \circ x = g \circ y$ implies that $f \circ x = f \circ y$ then there exists a unique $h \colon Y \to Z$ such that $g = h \circ f$.

A strict epimorphism is also an epimorphism, and a strictly epic monic is an iso. As we will see, in the representable case a strict epimorphism plays the role of a quotient of some distinguished object A by a subgroup of $\mathrm{Aut}(A)^{\mathrm{op}}$.

Theorem 3 (Representable Galois correspondence)**.** Let $\mathcal{C}$ be a category and A an object in $\mathcal{C}$ such that:

(1) For all X in $\mathcal{C}$ there exists an arrow $A \to X$ and every arrow $A \to X$ is a strict epimorphism
(2) For any $H \leq \mathrm{Aut}(A)$ the quotient A/H exists and is preserved by $[A, -]$
(3) $[A, A] = \mathrm{Aut}(A)$.

Then the adjunction:

$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "{[K,-]_G}"] \arrow[r, phantom, "\top"] & G - \mathbf{Set}^{\text{trans}} \arrow[l, bend left, "K/-"] \end{tikzcd}.$$

is an equivalence.

Proof. This proof is Remark 2.7 and the proofs of Proposition 2.8 and Proposition 3.6 in [DV00]. We will show that the unit and counit maps are isomorphisms.

For any G-Set E the unit map is given by $\eta\colon E \to [A, A/\mathrm{Fix}(x_0)]$ where $x_0 \in E$. We can show directly that E exhibits the universal property of the quotient $[A, A]/\mathrm{Fix}(x_0)$ and hence the two are isomorphic. Moreover, the second axiom says precisely that the natural map $[A, A]/H \to [A, A/H]$ is an isomorphism. By composing these two isomorphisms we see that the unit is an isomorphism.

For any $X \in \mathrm{Ob}(\mathcal{C})$, the counit map is given by $\epsilon\colon A/H \to X$. To show this is an isomorphism consider any $x\colon A \to X$. Since by the third axiom $[A, A] = \mathrm{Aut}(A)$ we can show that the map x factors through $[A, A]/\mathrm{Fix}(x)$ as an epimorphism $p\colon [A, A] \to [A, A]/\mathrm{Fix}(x_0)$ and a monomorphism $\psi\colon [A, A]/H \to [A, A/H]$. In fact, the following diagram commutes:

$$\begin{tikzcd} {[A,A]} \arrow[r, "q_*"] \arrow[rr, bend left, "x_*"] \arrow[dr] & {[A, A/\mathrm{Fix}(x_0)]} \arrow[r, "\epsilon_*"] & {[A, X]} \\ & {[A,A]/\mathrm{Fix}(\mathrm{x}_0)} \arrow[u, "\eta"] \arrow[ur] & \end{tikzcd}$$

where $q\colon A \to A/H$ is the quotient map and η is the unit. Therefore since ψ is injective and η is an isomorphism, ϵ_* is injective.

Now note that by the first axiom $[A, -]$ is faithful. For if $f, g\colon X \to Y$ such that $f_* = g_*$ then any $a\colon A \to X$ equalizes (f, g). By the first axiom a is strict epi and hence epi, thus $f = g$. So since faithful functors reflect monomorphisms, ϵ is a strict epi. So since it is also a mono, ϵ is an iso, finishing the proof. $\square$

Remark 2. The representable case encompasses two classical examples of a Galois correspondence. The category $\mathbf{Ext}^{\mathrm{op}}_{K/F}$ along with K satisfies the three given axioms.

Also, if X is a path-connected, locally path-connected, and semi-locally simply-connected topological space. Then the category of connected coverings of X along with the universal cover $\tilde{X}$ satisfies the three axioms above.

The most general statement we will encounter today is a characterization of a Galois category as the category of (not necessarily transitive) actions of a profinite group G on **FinSet** (the category of finite sets): Grothendieck's Galois theory. Before we sketch the proof of this we recall some properties of profinite groups.

2. Profinite group actions

Definition 5. A **profinite group** is an object in **Pro(FinGrp)**, i.e. a strict projective system $(G_i)_{i\in I}$ of finite groups. Equivalently it is the group $\varprojlim_{i\in I} G_i \subseteq \Pi_i G_i$ endowed with the subspace topology where the G_i are taken to be discrete.

Remark 3. Profinite groups can be characterized as those topological groups which are compact, Hausdorff, and totally disconnected, i.e. group objects in the category of Stone spaces. See Theorem 2.1.3 in [RZ10].

Definition 6. A profinite group G is said to **act on** $S \in \mathbf{Set}$ endowed with the discrete topology if there exists a continuous map $G \times S \to S$.

Proposition 1. Let $G \in \mathbf{Pro(FinGrp)}$ and $S \in \mathbf{Set}$. A transitive action $a\colon G \times S \to S$ is continuous if and only if there exists an $i \in I$ such that it factors as:

$$\begin{tikzcd} G \times S \arrow[r, two heads, "a"] \arrow[d, "\pi_i \times \mathrm{id}_S"'] & S \\ G_i \times S \arrow[ur] & \end{tikzcd}$$

Proof. We follow the proof of Proposition 3.16 in [DV00]. Let $x \in E$ and $H = \mathrm{Fix}(x)$. Since $\mathrm{Fix}(x) = a^{-1}(x) \cap (G \times \{x\})$, H is open. Recall that the subgroups $K_i = \ker \pi_i$ are a fundamental system of open neighborhoods of $e \in G$ (see Lemma 2.1.1 [RZ10]). So there exists an i such that $K_i \leq H$.

Now let $y \in E$ be arbitrary. Since the action is transitive, there exists a $g \in G$ such that $g \cdot x = y$. Therefore, since K_i is a normal subgroup,

$$K_i = gK_ig^{-1} \subseteq g\,\mathrm{Fix}(x)g^{-1} = \mathrm{Fix}(y).$$

Therefore the group action factors through $G_i \times S$. The converse follows since $G_i \times S$ is finite. $\square$

Remark 4. As transitive actions only have a single orbit, it follows from the above proposition that profinite groups can only act transitively if the set acted upon is finite.

Using the previous proposition and the fact **Cat** has all filtered colimits, $G - \mathbf{Set}^{\mathrm{trans}}$ can be expressed as a filtered colimit of $G_i - \mathbf{Set}^{\mathrm{trans}}$.

Proposition 2. Let G be a profinite group with surjective inverse system $(G_i)_{i\in I}$. Then:

(1) For any $i \in I$ there is a fully faithful embedding of categories:

$$G_i - \mathbf{Set}^{\mathrm{trans}} \hookrightarrow G - \mathbf{Set}^{\mathrm{trans}}$$

(2) $G - \mathbf{Set}^{\mathrm{trans}} = \varinjlim_{i\in I} G_i - \mathbf{Set}^{\mathrm{trans}}$.

Proof. The statements are Proposition 3.17 (2) and (3) in [DV00]. Any transitive G_i-Set is a transitive G-Set via the projections $\pi_i\colon G \twoheadrightarrow G_i$ (see Proposition 3.17 (1) [DV00]). The second statement follows from the previous proposition. $\square$

Proposition 3. G-**Set** is the free finite coproduct completion of G-$\mathbf{Set}^{\mathrm{trans}}$

3. Galois categories

Definition 7 (Galois category)**.** An essentially small category $\mathcal{C}$ along with a functor $F\colon \mathcal{C} \to$ **FinSet** is a **Galois category with fibre functor** F if:

Axioms on $\mathcal{C}$:

- $\mathcal{C}1$ $\mathcal{C}$ has finite (co)limits.
- $\mathcal{C}2$ Any morphism $f\colon X \to Y$ in $\mathcal{C}$ factors as an effective epi followed by a mono, $X \overset{e}{\twoheadrightarrow} I \overset{m}{\hookrightarrow} Y$ where I is a direct summand of Y.

Axioms on F:

- $F1$ F preserves finite (co)limits.
- $F2$ F reflects isomorphisms.

Note that by axioms $F1$ and $F2$, $X = \varnothing$ if and only if $F(X) = \varnothing$. This will be used several times later on.

Remark 5. In *Galois theory for schemes* Lenstra uses epimorphisms instead of strict epimorphisms in his definition of a Galois category.

Remark 6. In many sources, the existence of finite colimits in $\mathcal{C}$ and F preserving finite colimits are replaced by two slightly weaker axioms (the analogous statements but for the terminal object, finite coproducts and quotients by finite groups), however, the two definitions are equivalent (see Expose V, Remark 4.2 [GR04]).

Proposition 4. The diagram $\mathrm{Elts}(F)$ is filtered.

Proof. End of page 21 [DV00]. $\square$

Hence by the homework of the first week we see that for a locally small category $\mathcal{C}$ the functor $U \circ F\colon \mathcal{C} \to$ **Set** can be expressed as a colimit of representables, $U \circ F \overset{\sim}{\Longrightarrow} \mathrm{colim}_{(A,a)\in(\mathrm{Elts}(F))^{\mathrm{op}}}\, y_A$. Where $U\colon$ **FinSet** $\to$ **Set** is the forgetful functor. So we may write F as $\mathrm{Hom}_{\mathrm{Pro}(\mathcal{C})}(\varprojlim_{\mathrm{Elts}(F)} A, -)$, i.e. F is prorepresented by the cofiltered diagram of elements $P := (A)_{(A,a)\in\mathrm{Elts}(F)}$. By abuse of notation we will denote F by $[P, -]$.

Proposition 5. Hence F is prorepresented by an object $P := (A)_{(A,a)\in\mathrm{Elts}(F)} \in \mathbf{Pro}(\mathcal{C})$. Moreover, $\mathrm{Aut}_{\mathbf{Pro}(\mathcal{C})}(P)$ is a profinite group.

Recall from last week that an object is connected if it cannot be expressed as a coproduct of two non-empty sub-objects.

Theorem 4. Every object is $X \in \mathcal{C}$ is a finite coproduct of connected objects.

Proof. See Theorem 4.16 [DV00]. $\square$

Using this we can prove that F factors through the category of $\mathrm{Aut}(P)^{\mathrm{op}}$-Sets. We will give a proof later.

Proposition 6. For any $X \in \mathcal{C}$ there is a continuous left action of $\mathrm{Aut}(P)^{\mathrm{op}}$ on $[P, X]$. Hence F factors through a functor $H\colon \mathcal{C} \to \mathrm{Aut}(P)^{\mathrm{op}} - \mathbf{Set}$.

This allows us to state the main theorem of this lecture:

Theorem 5 (Grothendieck's Galois correspondence)**.** Let $\mathcal{C}$ be a Galois category with fibre functor F. Then F factors through a functor,

$$H\colon \mathcal{C} \to \mathrm{Aut}_{\mathbf{Pro}(\mathcal{C})}(P) - \mathbf{Set}$$

which is an equivalence.

4. The connected case

In this section we consider the case where $\mathcal{C}$ is a connected Galois category, i.e.:

Definition 8 (Connected Galois catogory)**.** A Galois category $\mathcal{C}$ is **connected** if all its objects are connected.

Proposition 7. If $\mathcal{C}$ is a connected Galois category, then the diagram $\mathrm{Elts}(F)$ has finite meets.

Proof. See Proposition 4.12 [DV00]. □

We will reduce the connected case to the representable case by showing that $\mathcal{C}$ and $G - \mathbf{Set}^{\mathrm{trans}}$ are cofiltered by the Galois objects. First we recall the definition of a Galois object.

Definition 9. An object A is Galois if and only if $\mathrm{Aut(A)} \xrightarrow{a*} [P, A]$ is a bijection for all $a \in [P, A]$.

Remark 7. Since connected objects are nonempty and $X \neq \varnothing \implies F(X) \neq \varnothing$, $[P, A] \neq \varnothing$ in the above definition.

We begin by expressing $\mathcal{C}$ as a filtered colimit.

Definition 10. Let $A \in \mathcal{C}$ be Galois. Define $\mathcal{C}_A$ to be the full subcategory of $\mathcal{C}$ consisting of those $X \in \mathcal{C}$ such that $[A, X] \xrightarrow{a*} [P, X]$ is a bijection. (I.e. those objects for which the functor is represented by A).

Proposition 8. A morphism of Galois objects $A \to B$ induces an inclusion $\mathcal{C}_A \hookrightarrow \mathcal{C}_B$.

Proof. Connected objects are nonempty, so $F(A) \neq \varnothing$. Therefore, there is a triangle

$$\begin{tikzcd} P \arrow[d, "a"'] \arrow[dr, "x \circ a"] & \\ A \arrow[r, "x"'] & B \end{tikzcd}$$

which induces an inclusion of categories by Proposition 3.9 [DV00] (this is not hard to see, in the reference it is stated without proof). □

Proposition 9. The category $\mathcal{C}_A$ along with A satisfy the conditions for the representable case, i.e. the adjunction:

$$\begin{tikzcd} \mathcal{C}_A \arrow[r, bend left, "{[K,-]_G}"] \arrow[r, phantom, "\top"] & (\mathrm{Aut}(A))^{\mathrm{op}} - \mathbf{Set}^{\mathrm{trans}}. \arrow[l, bend left, "K/-"] \end{tikzcd}$$

is an equivalence.

Proof. (1) It follows directly from axiom $\mathcal{C}2$ that all morphisms are strict epis. Together with $F(X) \neq \varnothing$ for all $X \in \mathcal{C}_A$ this implies the first axiom.
(2) We can verify that $\mathcal{C}_A$ is closed under quotients of actions by finite groups (Proposition 3.11 [DV00]). Hence by $F1$, the second axiom holds.

(3) $[A, A] = \mathrm{Aut}(A)$ (see Remark 3.3 [DV00]).

$\square$

Theorem 6. The subdiagram $\Lambda_F \subseteq \mathrm{Elts}(F)$ of Galois objects gives the same colimit F. Moreover $\mathcal{C}$ is the filtered colimit of $\mathcal{C}_A$ under the diagram $\Lambda_F \to \mathbf{Cat}, (A, a) \mapsto \mathcal{C}_A$.

Proof. See Theorem 3.14 [DV00]. $\square$

Theorem 7. If $\mathcal{C}$ is a Galois category with connected objects, then the functor $F \colon \mathcal{C} \to \mathbf{FinSet}$ factors through an equivalence $H \colon \mathcal{C} \to \mathrm{Aut}(P)^{\mathrm{op}} - \mathbf{Set}^{\mathrm{trans}}$.

Proof. That F factors through H follows from Proposition 3.20 [DV00]. Now since the diagram:

$$\begin{tikzcd}
\mathcal{C}_A \arrow[r, "{[A,-]_G}"] & G - \mathbf{Set}^{\mathrm{trans}} \\
\mathcal{C}_B \arrow[r, "{[B,-]_H}"] \arrow[u, hook] & H - \mathbf{Set}^{\mathrm{trans}} \arrow[u, hook]
\end{tikzcd}$$

commutes for all A, B Galois and equivalences are stable under filtered colimits (optional homework), H being the filtered colimit (by Theorem 6), we conclude that H is an equivalence. $\square$

5. Proof of the main theorem

First we begin by showing how Proposition 6 follows from the connected case.

Proof of Proposition 6. First we reduce to the connected case. In this manner decompose X into connected objects $\coprod_i X_i$. Since $[P, -]$ commutes with coproducts, $G \times [P, X] = G \times \coprod [P, X_i]$. But coproducts commute with products in the category of compact Hausdorff spaces so this becomes $\coprod G \times [P, X_i]$. So the Proposition follows from the connected case. $\square$

Proof sketch of main theorem. Can define a homotopy inverse of H by decomposing every G-Set into its orbits and sending those orbits through the homotopy inverse obtained in the connected case (i.e. maps into the full subcategory $\mathrm{Con}(\mathcal{C})$ of which $\mathcal{C}$ may be the free finite coproduct completion). $\square$

6. Optional Homework

(1.) Let X be a connected topological space $x \in X$ and $\mathbf{FinCov}_{/X}$ be the category of finite coverings over X.

i. Let G be a group. Show that the collection of normal subgroups of $N \leq G$, denoted I, is a cofiltered diagram under reverse inclusion. The *profinite completion* of G, $\hat{G}$ is defined to be $\varprojlim_{N \in I} G/N$. Show that $G - \mathbf{Set}$ is equivalent to $\hat{G} - \mathbf{Set}$ (i.e. category of finite G-Sets is equivalent to category of finite $\hat{G}$-Sets).

ii. In the lecture we mentioned that $\mathbf{FinCov}_{/X}$ along with a basepoint $x \in X$ and fibre functor $F_x \colon \mathbf{FinCov}_{/X} \to \mathbf{FinSet}$ sending a finite covering $f \colon Y \to X$ to its fibre at x $f^{-1}(x)$ is a Galois category. Hence it is equivalent to some $\hat{\pi}(X, x) - \mathbf{Set}$ for some profinite group $\hat{\pi}(X, x)$. If X is also path connected, locally path connected, and semi locally simply connected (so that the monodromy correspondence holds) show that in fact $\hat{\pi}(X, x) \cong \widehat{\pi(X, x)}$.

References

[DV00] E. J. Dubuc and C. Sanchez de la Vega. *On the Galois Theory of Grothendieck*. 2000. arXiv: `math/0009145 [math.CT]`. URL: `https://arxiv.org/abs/math/0009145`.

[GR04] Alexander Grothendieck and Michele Raynaud. *Revêtements étales et groupe fondamental (SGA 1)*. 2004. arXiv: `math/0206203 [math.AG]`. URL: `https://arxiv.org/abs/math/0206203`.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. ISBN: 978-3-642-01641-7. DOI: `10.1007/978-3-642-01642-4`.