Galois theorem for Commutative Algebras

Animesh Renanse

Department of Mathematics & Statistics, IISER Kolkata

DMS Foundation Day, 2023

Classical Galois theorem of fields

The classical theorem of Galois states that for finite dimensional field extensions L/K where for each element of L the minimal polynomial in $K[x]$ exists and factors into distinct linear factors over L, we get the following isomorphism of posets

$$\{M \mid L \supseteq M \supseteq K\} \cong \{G \mid G \leq \mathbf{Gal}\,(L/K)\}$$

established by antitone maps $\mathbf{Fix}\,(-)$ and $\mathbf{Gal}\,(L/-)$. The theorem also states that $\dim L/K = |\mathbf{Gal}\,(L/K)|$. This theorem is used crucially in order to prove that n^{th} degree general polynomial has Galois group as S_n. This combined with the unsolvability of S_n for $n \geq 5$ yields unsolvability of quintic polynomials, also known as Abel-Ruffini theorem.

The general idea of Galois theory is to study an object by it's automorphism group. Here the objects are field extensions. Grothendieck around 1960s, motivated by a similar theorem in the topological setting with fundamental group, developed a far reaching generalization of the aforementioned theorem to a setting which allows to give *Galois like* theorems about other algebraic objects, like finite dimensional commutative K-algebras with 1.

Galois theorem for commutative algebras

Let L/K be a finite dimensional Galois field extension. A K-algebra A is said to be split by L if the minimal polynomial of each element of A is linearly factored into distinct roots over L. Let $\mathbf{Split}_K(L)_{\text{Fin}}$ denote all finite dimensional commutative K-algebras split by L, which is a full subcategory of $K-\mathbf{Alg}$, and let $\mathbf{Gal}\,(L/K)-\mathbf{Set}_{\text{Fin}}$ denote all finite sets with an action of Galois group $\mathbf{Gal}\,(L/K)$. The Galois theorem of Grothendieck then says that the functor

$$\mathrm{Hom}_K(-,L) : \mathbf{Split}_K(L)^{\text{op}}_{\text{Fin}} \longrightarrow \mathbf{Gal}\,(L/K)-\mathbf{Set}_{\text{Fin}}$$

establishes a contravariant equivalence between $\mathbf{Split}_K(L)_{\text{Fin}}$ and $\mathbf{Gal}\,(L/K)-\mathbf{Set}_{\text{Fin}}$.

Galois theorem for fields $\hookrightarrow$ Galois theorem for commutative algebras

As uselessly abstract the above theorem might seem, we can rederive the classical Galois theorem for fields from it. Indeed, take any Galois field extension L/K and consider an intermediate extension $K \hookrightarrow M \hookrightarrow L$.

- By the above contravariant equivalence, we get the following surjection of $\mathbf{Gal}\,(L/K)$ sets

$$\mathrm{Hom}_K(L,L) \twoheadrightarrow \mathrm{Hom}_K(M,L) \twoheadrightarrow \mathrm{Hom}_K(K,L).$$

- Now, it turns out that $\mathrm{Hom}_K(L,L)$ is just the Galois group $\mathbf{Gal}\,(L/K)$ and $\mathrm{Hom}_K(K,L)$ is a singleton, so the second surjection is trivial. Hence the above diagram further reduces to following in the category of finite $\mathbf{Gal}\,(L/K)$ sets

$$\mathbf{Gal}\,(L/K) \overset{\phi}{\twoheadrightarrow} \mathrm{Hom}_K(M,L).$$

- Hence we have that

$$\begin{array}{c} \{M \mid K \hookrightarrow M \hookrightarrow L\} \\ \cong \\ \{Q \mid \mathbf{Gal}\,(L/K) \twoheadrightarrow Q\} \end{array}.$$

- Since for any group G, the subgroups of G are in one-to-one correspondence with quotient G-sets of the G-set G, therefore we further get the following equivalence

$$\begin{array}{c} \{M \mid K \hookrightarrow M \hookrightarrow L\} \\ \cong \\ \{H \mid H \leq \mathbf{Gal}\,(L/K)\} \end{array}.$$

Hence we have the classical Galois theorem.

Sketch of a proof

An important part of this proof is to use following result due to Gelfand which characterizes the split K-algebras in a lot less *elemental* manner

Theorem (Characterization of split algebras)

Let L/K be a field extension with $\dim_K L < \infty$ and let A be a K-algebra with $\dim_K A < \infty$. Then, the following are equivalent

- *L splits A.*
- $L \otimes_K A \cong L^{Hom_L(L\otimes_K A, L)} \cong L^{Hom_K(A,L)}$.
- $L \otimes_K A \cong L^{\dim_K A}$.
- $|Hom_K(A,L)| = |Hom_L(L \otimes_K A, L)| = \dim_K A$.

Using the above theorem, the main ideas of the proof are as follows.

- In order to check that $\mathrm{Hom}_K(-,L)$ is full, one would need to produce a $\xi : A \to B$ for a $\varphi : \mathrm{Hom}_K(B,L) \to \mathrm{Hom}_K(A,L)$. This one can do from following observations.
  1. If A is split by L, then $L^{\mathrm{Hom}_K(A,L)}$ is a $\mathbf{Gal}\,(L/K)$-set.
  2. If A is split by L, then $A \cong \mathbf{Fix}\,(L \otimes_K A) = \{x \in L \otimes_K A \mid g \otimes \mathrm{id}(x) = x \; \forall g \in \mathbf{Gal}\,(L/K)\}$.

  Indeed, the natural choice for ξ then is the following

$$\begin{tikzcd} A \arrow[r, "i_A"] \arrow[d, "\xi"'] & L \otimes_K A \arrow[r, "\theta_A", "\cong"'] \arrow[d, "\overline{L^{\varphi}}"'] & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(A,L)} \arrow[d, "L^{\varphi}"] \\ B \arrow[r, "i_B"'] & L \otimes_K B \arrow[r, "\cong", "\theta_B"'] & L^{\mathrm{Hom}_{\mathbf{K\text{-}Alg}}(B,L)} \end{tikzcd}$$

- In order to check the essential surjectivity of $\mathrm{Hom}_K(-,L)$, for any finite $\mathbf{Gal}\,(L/K)$-set X, we have to obtain a K-algebra A split by L such that $\dim_K A < \infty$ and $\mathrm{Hom}_K(A,L) \cong A$. This will follow from the following observations.
  1. For any group G and a finite G-set X,
  $$X \cong \coprod_{i=1}^{n} Q_i$$
  where Q_i are quotient G-sets of G-set G.
  2. For any two K-algebras A, B split by L, we have
  $$\mathrm{Hom}_K(A \times B, L) \cong \mathrm{Hom}_K(A,L) \amalg \mathrm{Hom}_K(B,L)$$
  in $\mathbf{Gal}\,(L/K)-\mathbf{Set}_{\text{Fin}}$.
  3. In $\mathbf{Gal}\,(L/K)-\mathbf{Set}_{\text{Fin}}$, if Q is a quotient $\mathbf{Gal}\,(L/K)$-set of $\mathbf{Gal}\,(L/K)$, then there exists a K-algebra A split by L such that
  $$\mathrm{Hom}_K(A,L) \cong Q.$$

  With these three observations, the essential surjectivity of $\mathrm{Hom}_K(-,L)$ now follows.

Example : The K-algebra $K[x]/\langle p(x) \rangle$

Pick any field extension L/K and a polynomial $p(x) \in K[x]$ which is the minimal polynomial of some $a \in L$. One always has the following bijection (Proposition 2.2.5, [BJ01])

$$\mathrm{Hom}_K\left(\frac{K[x]}{\langle p(x)\rangle}, L\right) \cong \{l \in L \mid p(l) = 0 \text{ in L}\} = V_L(p(x)).$$

Note that $K[x]/\langle p(x) \rangle$ is a finite dimensional commutative K-algebra, where $\dim_K K[x]/\langle p(x) \rangle = \deg p(x)$. If L is a finite dimensional Galois extension of K, then by extension of scalars, we have

$$L \otimes_K \frac{K[x]}{\langle p(x) \rangle} \cong \frac{L[x]}{\langle p(x) \rangle}.$$

Since $\left|\mathrm{Hom}_L\left(\frac{L[x]}{\langle p(x)\rangle}, L\right)\right| = |V_L(p(x))| = \deg p(x)$. Hence L splits $K[x]/\langle p(x) \rangle$ and as is clear, we have the finite $\mathbf{Gal}\,(L/K)$-set $\mathrm{Hom}_K(K[x]/\langle p(x) \rangle, L)$.

The Galois phenomenology

In a first course in algebraic topology, one usually learns a very powerful theorem about classification of covering spaces. If X is a path-connected and semi-locally simply connected space, then we have the following isomorphism of posets

$$\begin{tikzcd} \{\text{Connected covers of } (X,x_0)\}/\text{equivalence} \arrow[r, bend left, "(\tilde{X}{,}p) \longmapsto p_*(\pi_1(\tilde{X}{,}\tilde{x}_0))"] & \{\text{Subgroups of } \pi_1(X,x_0)\}/\text{conjugacy} \arrow[l, bend left, "X_H \longleftarrow\!\shortmid H"] \end{tikzcd}$$

But with a little bit of exploring one sees the following stronger equivalence

Theorem (Galois theorem of covering spaces)

Let X be a connected and locally simply connected space, $\boldsymbol{Cov}\,(X)$ be the category of covering spaces over X and $\pi_1(X)-\boldsymbol{Set}$ be the category of all sets with an action of $\pi_1(X)$. Then, there is an equivalence of categories

$$\boldsymbol{Cov}\,(X) \equiv \pi_1(X) - \boldsymbol{Set}$$

given by $p \mapsto p^{-1}(x)$ where x is the base point of X.

- Moreover, one can get back the above isomorphism from the aforementioned theorem by restricting the above equivalence to the $\pi_1(X)$ sets obtained by identifying all subgroups of $\pi_1(X)$ conjugate to each other.
- Just like classical Galois theory of fields, the above correspondence is equally usable in topology, using which we can classify, for example, all connected coverings of $\mathbb{RP}^n$.
- One then wonders how this topological and algebraic pictures are related to each other. Indeed, the work of Grothendieck, which led to the generalization of Galois theory to commutative K-algebras, was not limited to just this, as the setting of work in which he stated his general Galois theorem was of schemes, and it is in this language do both algebraic and topological pictures of the Galois theory come together. For more information, see [Len08].
- Another way of understanding the source of this phenomenon is to abstractly characterize those categories where there might be an *inherent* Galois theorem. Indeed this is what is done in Chapter 5 of [BJ01].

References

- F. Borceux, G. Janelidze, Galois Theories, Camb. Stud. Adv. Math. 72, Cambridge: Cambridge University Press (2001).
- H.W. Lenstra, Galois theory for schemes, available online at https://websites.math.leidenuniv.nl/algebra/GSchemes.pdf (2008).