An intuitive introduction to Absolute Galois group and its representation

Sachin Kumar
Faculty of Mathematics, University of Waterloo

Canadian Undergraduate Mathematics Conference (CUMC),
University of British Columbia, July 9, 2024

Outline

1. Abstract
2. Background (Classical Galois Theory)
3. Absolute Galois Group
4. Galois Representation
5. Thank You!

Abstract for this talk!

In this talk, we will embark on a fascinating journey to explore the algebraic structure of the absolute Galois group, and discover how representation theory and L-functions can be used to illuminate its hidden patterns. Through the use of intuitive examples, we will strive to make these complex ideas accessible and captivating to all.

Notation

We will follow the standard notations:

- $\mathbb{F}$ - Field (eg: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$, ...)
- $\mathbb{Q}$ - Set of Rational numbers
- $\mathbb{C}$ - Set of Complex numbers
- K - Number field (i.e., a finite extension of $\mathbb{Q}$)
- $\mathscr{O}_K$ - Ring of integers of the number field K
- $\overline{\mathbb{F}}$ - Algebraic closure of $\mathbb{F}$ (i.e., $\{\alpha \in \mathbb{C} : f(\alpha) = 0$ with $f(x) \in \mathbb{F}[x]\}$)
- $\mathrm{Gal}(L/K)$ - Galois group of the field extension L/K

Some Recap... (Classical Galois Theory)

Before delving into the theory of absolute Galois groups and its representations (Galois representations), we will recall some facts from Galois theory.

Let E and F be fields such that E/F is a *finite field extension*, i.e., $F \subsetneq E$ with a finite degree, $[E:F] = \dim_F(E) = n < \infty$, i.e., the dimension of E over F (viewed as a vector space) is the degree of E/F.

Example ($\mathbb{C}/\mathbb{R}$ is a finite field extension)

$[\mathbb{C}:\mathbb{R}] = 2$ is a finite field extension, since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$. Also, we can observe that $\mathscr{B} = \{1, i\}$ is the basis for $\mathbb{C}_{\mathbb{R}}$ as a vector space, so

$$[\mathbb{C}:\mathbb{R}] = \dim_{\mathbb{R}}(\mathbb{C}) = |\mathscr{B}| = 2$$

We also recall the following theorem,

Theorem 1.1

If L is an intermediate field of a finite extension E/F, then $[L:F] \mid [E:F]$.

Classical Galois Theory (Cont.)

Now, let's discuss two important types of field extensions, i.e., Separable and Normal extensions.

Let E/F be an algebraic field extension, such that for $\alpha \in E$, let $m(x) \in F[x]$ be the minimal polynomial of α.

Definition (Separable extension)

α is separable over F, if $m(x)$ is separable over F. $\forall \alpha \in E$, if α is separable over F, then we say E/F is separable extension.

Example

If $\mathrm{ch}(F) = 0$, then every irreducible polynomial $p(x) \in F[x]$ is separable implying that E/F is separable.

Definition (Normal extension)

E/F is a normal extension if for any irreducible polynomial $p(x) \in F[x]$, either $p(x)$ has no root in E or $p(x)$ has all roots in E.

Classical Galois Theory (Cont.)

By the following theorem, we can summarize the idea of normal and separable field extension.

Theorem 1.2

Let E/F be a finite field extension.

1. E is a splitting field of some $f(x) \in F[x]$ if and only if E/F is normal.
2. E is a splitting field of some separable polynomial $f(x) \in F[x]$, then E/F is separable.

Question?

Can we construct statement (2) of Theorem 1.2 into 'if and only if'?

Indeed yes! if we know a priori that E is the splitting field of some $f(x) \in F[x]$, then (2) becomes an 'if and only if ', since $\Leftarrow$ holds trivially.

Definition (Solvable Groups)

A group G is solvable if there exists a tower $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$ with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq (m-1)$.

Classical Galois Theory (Cont.)

Now, we have all the tools that we need in order to define Galois extensions and (finite) Galois groups.

Definition (Automorphism Group)

Let E/F be a field extension. If ψ is an automorphism of E, i.e., $\psi : E \to E$ is an isomorphism, such that $\psi|_F = 1_F$, we say ψ is an F-automorphism of E. So, The automorphism group of E/F is the set of ψ, i.e., F-automorphism from $E \to E$ (which is a group under composition), denoted by $\mathrm{Aut}_F(E)$.

Example

Let $\mathbb{C}/\mathbb{R}$ be a algebraic field extension. Then the $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{z \mapsto z, z \mapsto \bar{z}\}$. Complex conjugation is a field automorphism over $\mathbb{R}$. If we think more, we see $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \mathrm{id}, \mathrm{cc} \rangle \implies \#\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = 2$.

Definition (Galois extensions)

An algebraic extension E/F is Galois if it is normal and separable. If E/F is a Galois extension, the Galois group of E/F, $\mathrm{Gal}_F(E)$, is defined to be the automorphism group $\mathrm{Aut}_F(E)$.

What is Absolute Galois Group?

A Galois extension E/F is called abelian, cyclic, or solvable if $\mathrm{Gal}_F(E)$ has the corresponding properties.

All this while, we were only discussing finite Galois extensions. Now, let's think what would happen if the Galois extension is infinite.

Definition (Algebraic Closure of $\mathbb{Q}$)

The algebraic closure of $\mathbb{Q}$, denoted as $\overline{\mathbb{Q}}$ is the set

$$\{\alpha \in \mathbb{C} \mid f(\alpha) = 0 \text{ where } f(x) \in \mathbb{Z}[x] \text{ (or monic } \mathbb{Q}[x])\}$$

We can clearly observe that $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ are fields with $\mathbb{Q} \subsetneq \overline{\mathbb{Q}}$. So, we can conclude that $\overline{\mathbb{Q}}/\mathbb{Q}$ is a fields extension.
Now, naturally we would ask the following question:

Question?

Is $\overline{\mathbb{Q}}/\mathbb{Q}$ a finite or infinite field extension? And is it Galois?

The answer is...

Absolute Galois Group (Cont.)

Infinite and Yes! We will prove our claim.

Claim.

$\overline{\mathbb{Q}}/\mathbb{Q}$ is a *infinite* field extension, i.e., $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proof.

We will prove via contradiction.

1. Suppose for contradiction, $[\overline{\mathbb{Q}} : \mathbb{Q}] = n < \infty$.
2. Let $m := n+1$ and $\alpha := 2^{1/m}$ where $\alpha \in \overline{\mathbb{Q}}$.
3. So, α is a root of some $f(x) \in \mathbb{Z}[x]$, where $f(x) = x^m - 2$.
4. By Eisenstein's criterion, $f(x)$ is irreducible in $\mathbb{Q}[x]$.
5. Hence, $f(x)$ is the minimal polynomial in $\mathbb{Q}[x]$.
6. So, we get $m = \deg(f) = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [\overline{\mathbb{Q}} : \mathbb{Q}] = n = m - 1$
7. A contradiction.

Therefore, $\overline{\mathbb{Q}}/\mathbb{Q}$ is a infinite extension. □

Absolute Galois Group (Cont.)

Definition (Absolute Galois Group)

The absolute Galois group is the $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\overline{\mathbb{Q}}/\mathbb{Q}$ is a infinite Galois extension with $\overline{\mathbb{Q}}$ as the algebraic closure of $\mathbb{Q}$. It is usually denoted as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ or $G_{\mathbb{Q}}$.

Question?

But is this the most accurate definition of a Absolute Galois group of $\mathbb{Q}$?

"Absolutely" Not!

- We showed that $G_{\mathbb{Q}}$ is an infinite group (to be precise it is a uncountably infinite).

Question?

But why is it uncountably infinite?

Before discussing a more precise contstructive definition of $G_{\mathbb{Q}}$, we will discuss some history and why they came up with this.

A short history...

- For ~ 100 years after Évariste Galois, mathematicians have studied the behaviour of $\mathrm{Gal}(K/L)$ for $[K:L] < \infty$, where K and L are number fields.
- In the late 1950's, John Tate (one of the greatest number theorists) was having a conversation with Alexander Grothendieck (Father of modern algberaic geometry, he introduced the theory of schemes, Étale Cohomology, ...) about some problem he was thinking.
- That's when Grothendieck gave a suggesion to understand all Galois extension of $\mathbb{Q}$ *simultaneously*.
- That completely revolutionized Tate's approach and he started proving all sorts of amazing theorems about Galois Cohomology and Duality of Galois groups.

My favorite diagram!

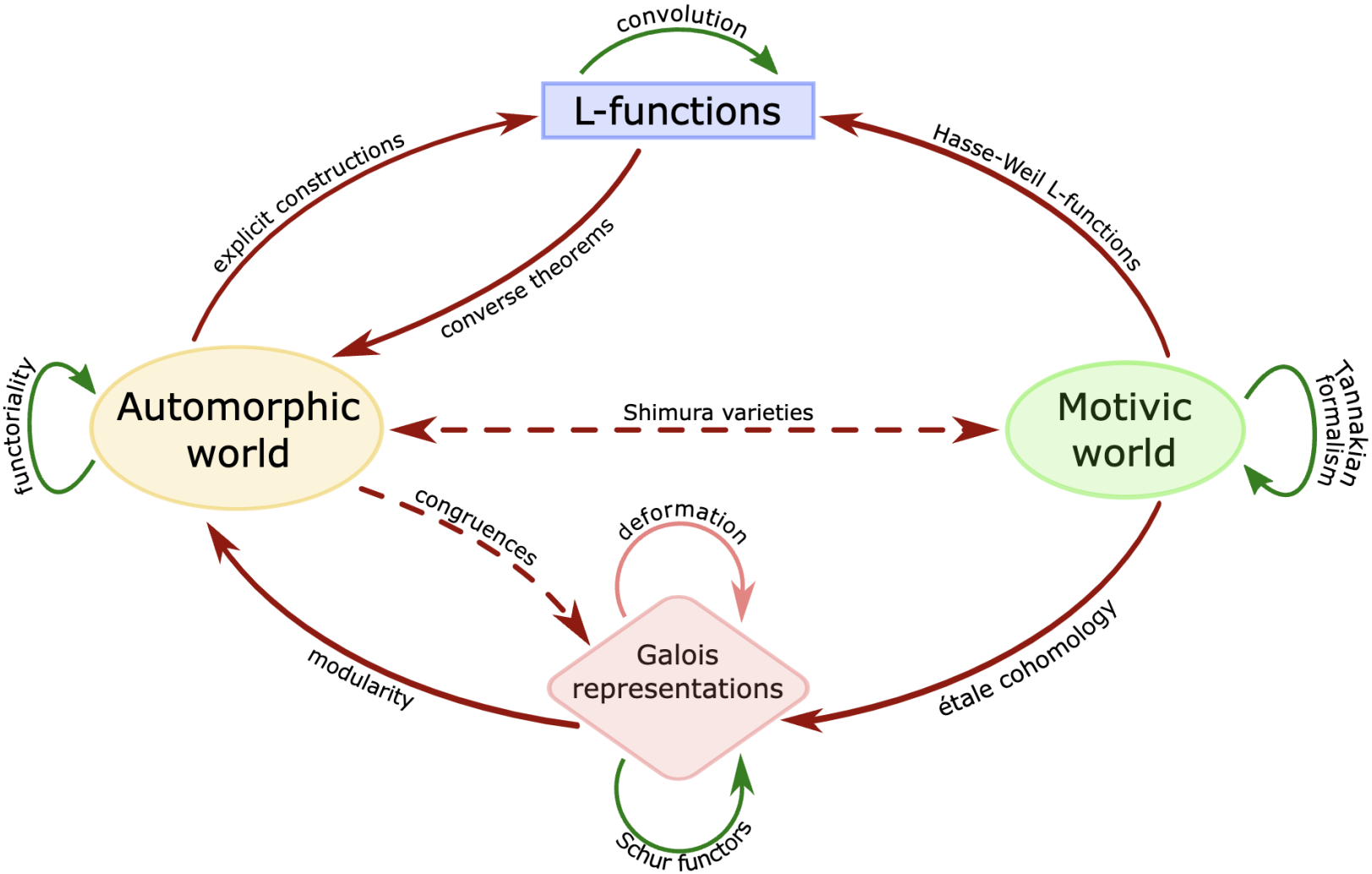

Figure: LMFDB Universe

Formal definition

By now, you would have guessed what the formal definition is! Let's state it.

Definition (Abolute Galois group of $\mathbb{Q}$)

Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then,

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{K} \mathrm{Gal}(K/\mathbb{Q})$$

where K is a number field.

In the previous slide, we asked the following question:

Question?

Why is $G_{\mathbb{Q}}$ uncountably infinite?

- We can observe that $G_{\mathbb{Q}} \subsetneq \mathrm{Bij}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}})$.
- We know $\overline{\mathbb{Q}}$ is countable, but the bijections from a countable set to a countable set is uncountable.
- So it's not surprising that $G_{\mathbb{Q}}$ is uncountable.
- Actually, $G_{\mathbb{Q}}$ is like a Riemann surface.

Examples

Time for an example...

Example

Let's consider the following Diophantine equation (specifically an elliptic curve, name it E_1):

$$y^2 = x^3 - 2$$

where $P_1 = (2, \sqrt{6}) \notin E_1(\mathbb{Q})$ is a real solution. Here's a another solution $P_2 = (3, \pm 5) \in E_1(\mathbb{Q})$. If we consider P_1, we know that $P_3 = (2, -\sqrt{6})$ is a solution too! We observe that $P_1 \in E(\overline{\mathbb{Q}})$, since $\sqrt{6}$ is an algebraic number. But, when $G_{\mathbb{Q}}$ is acting the set $E(\overline{\mathbb{Q}})$, we observe that $P_1 \notin E(\overline{\mathbb{Q}})^{G_{\mathbb{Q}}}$.

Moral

$G_{\mathbb{Q}}$ knows all solutions to all Diophantine equations.

$G_{\mathbb{Q}}$ is hard to understand...

After all this, it is fair to conclude the following:

Remark

$G_{\mathbb{Q}}$ is a very hard group to understand!

The following in an open problem on Galois groups:

Conjecture (Inverse Galois Problem).

Given a finite group G, there exists a field extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \cong G \twoheadleftarrow G_{\mathbb{Q}}$.

This conjecture is proven for the cases where, $G = S_n$ and A_n (Hilbert), $\mathbb{Z}/n$ (cyclic groups). Then it was also known for p-groups and solvable groups (Shafarevich, 1989).

What is a Group Representation?

Before, delving into the theory of Galois representations. We will recall what a group representation is.

Definition (Representation)

A representation of a group G on a module M over a commutative unitary ring R is a group homomorphism

$$\rho : G \to \mathrm{Aut}(M)$$

Alternatively, a representation is a R-module M together with a group action of G on M.

Often $M = V$, where V is a vector space over a field K with $\dim(V) = n$, so

$$\rho : G \to GL(V) \cong GL(n, K)$$

What is a Galois representation?

You could've guessed what Galois representation is! It is just the case where $G = G_{\mathbb{Q}}$, i.e., a group homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(M)$$

.

Question?

So, that's it?

Obviously not! We want ϕ to satisfy one two condition, since G is not some regular group.

- Since, $G_{\mathbb{Q}}$ is a Galois group, the representation should closed under the action of Galois correspondence.
- Also, $G_{\mathbb{Q}}$ is a topological "profinite" group, so in the representation it has to map to some structure that has a topology, hence we require M to be topological module.

So, when you work with homomorphisms in a category, you want the homomorphisms to respect the structure that the object has.

Example 1

Time for examples...

The following example is very interesting.

Example

Let V be a 1-dimensional over $\mathbb{C}$. Let $G_{\mathbb{Q}}$ act trivially on V. We have a group homomorphism:

$$\phi : G_{\mathbb{Q}} \to GL_1(\mathbb{C}) \text{ where } \sigma \mapsto 1$$

I would like to ask the following question:

Question?

Do we really understand this representation?

My claim is that "**we don't**"! But why? Let me explain.

Example 1 (Cont.)

For every prime p, there exists $\sigma_p \in G_{\mathbb{Q}}$. Under this map,

$$\sigma_p \mapsto \alpha_p = 1$$

So, we will construct an analytic function from the representation ϕ,

$$\prod \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} = \prod \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$$

which is just the Riemann zeta function.

Question?

So what is my argument?

If you claim that you understood this trivial 1-dimensional Galois representation, then you are claiming that you understood everything about the Riemann zeta function, which is bulls**t!

Example 2

We will use the Diophantine equation that we saw in the previous section.

Example

Let consider the same Diopahatine equation (Elliptic curve over $\mathbb{Q}$):

$$E/\mathbb{Q} : y^2 = x^3 - 2$$

and let $E[n] = \{P \in E(\mathbb{Q}) : nP = 0\}$, the n-torsion subgroup of $E(\mathbb{Q})$. As an abelian group,

$$E[n] \cong (\mathbb{Z}/n)^2$$

It turns out that $(\mathbb{Z}/n)^2$ are all algebraic points, so $G_{\mathbb{Q}}$ acts on $(\mathbb{Z}/n)^2$. So, we get representation

$$\phi : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/n)$$

Write $n = \ell^N$, where ℓ is a prime and let $N \to \infty$.

Example 2 (Cont.)

So. we get the following representation:

$$\phi_1 : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_\ell)$$
$$\sigma_p \mapsto \begin{pmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{pmatrix}$$

Similarly, we can construct following L-function,

$$L(E,s) = \prod \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1}$$

Here is the conjecture of the Birch and Swinnerton-Dyer:

Conjecture (BSD).

$\text{ord}_{s=1} L(E,s) = r$.

where r comes from the following theorem of Mordell-Weil:

theorem (Mordell-Weil)

$E(\mathbb{Q}) = \mathbb{Z}^r \oplus A$, where A is a finite group, usually
$A = E(\mathbb{Q})_{\text{tors}} = \{P \in E(\mathbb{Q}) \mid nP = \infty\}$, i.e., the set of all points with finite order.

Example 3

Let's consider another example.

Example

Consider the following Diophantine equation:

$$f(x) = x^2 + 3 = 0$$

- $f(x) = x^2 + 3 = (x + \sqrt{-3})(x - \sqrt{-3}) = 0.$
- We can construct a field that is generated by $\sqrt{-3}$, i.e., $\mathbb{Q}(\sqrt{-3})$.
- Also, we can construct a Galois representation:

$$\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mu_2 = \{\pm 1\}$$

with the following function:

$$\sigma \mapsto \frac{\sigma(\sqrt{-3})}{\sqrt{-3}} = \begin{cases} 1 & \text{if } \sigma(\sqrt{-3}) = \sqrt{-3} \\ -1 & \text{if } \sigma(\sqrt{-3}) = -(\sqrt{-3}) \end{cases}$$

Example 3 (Contd.)

Similar to the previous case, we can construct a corresponding L-function:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \cdots$$

where,

$$\begin{aligned} \chi : \mathbb{Z}/3\mathbb{Z} &\to \mu_2 \cup \{0\} \\ 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ 2 &\mapsto -1 \end{aligned}$$

Thank You!