2024 CUMC Talk Notes (a planned script?)

Sachin Kumar

July 2024

Abstract

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.

Background (Classical Galois Theory)

Slide 1

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 $\mathcal{B} = \{1, i\}$ is the basis for $\mathbb{C}_{\mathbb{R}}$ as a vector space, so

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

We also recall the following theorem,

Theorem 1.1. If L is an intermediate field of a finite extension E/F, then $[L : F] \mid [E : F]$.
This means that if E/L and L/F are finite, then E/F is a finite extension and $[E : F] = [E : L] \cdot [L : F]$.

Slide 2

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

Let E/F be an algebraic field extension,
(i.e., $\forall \alpha \in E$, there exists $f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$)
such that for $\alpha \in E$, let $m(x) \in F[x]$ be the minimal polynomial of α.
(i.e., $m(x)$ is monic and irreducible polynomial of α)

Definition (Separable extension). α is separable over F, if $m(x)$ is separable over F.
(i.e., if $m(x)$ has no repeated root in any extension of F, also we can prove that $f(x)$ is s separable if and only if $\gcd(f, f') = 1$, using the fact that α is a repeated root of $f(x)$ if and only if $(x - a) \mid \gcd(f, f')$)
$\forall \alpha \in E$, 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.

(i.e., if $p(x)$ has a root in E, $p(x)$ splits over E, i.e., E contains all roots of $p(x)$, i.e., $f(x)$ is a product of linear factors in $E[x]$)

Slide 3

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 (**??**) 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 (**??**) 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 $0 \leq i \leq (m-1)$.
We can prove nice theorems about solvable groups , like:
1. If $H \leq G$, where G is solvable, then H is solvable.
2. If $N \lhd G$, where G is solvable, then G/N is solvable.
3. Let $N \lhd G$. If N and G/N are solvable, then G is solvable. In particular, a direct product of finitely many solvable groups is solvable.
4. Let $f(x) \in F[x] \setminus \{0\}$ where $\mathrm{ch}(F) = 0$. Then $f(x)$ is solvable by radical if and only if $\mathrm{Gal}(f)$ is solvable (This was the key fact in proving the unsolvability of the quintic equations via radicals).

Slide 4

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 $\mathrm{Aut}_F(E)$.
$|\mathrm{Aut}(E/F)| = [E : F]$
The only elements of E fixed by $\mathrm{Aut}(E/F)$ are in F.
It is silly, but I will still mention that all Galois groups are automorphism group, but not all automorphism groups are Galois groups

Example. Let $\mathbb{C}/\mathbb{R}$ be a algebraic field extension. Then the $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{z \mapsto z, z \mapsto \overline{z}\}$. 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 $\mathrm{Aut}_F(E)$.

Absolute Galois group

Slide 5

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.
But do such Galois extensions exist? Why not!

Definition (Algebraic Closure of $\mathbb{Q}$). The algebraic closure of $\mathbb{Q}$, denoted as $\overline{\mathbb{Q}}$ is the set

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

which is nothing but the set of algebraic numbers.

We know that an algebraic closure of a field exists by Zorn's lemma

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...

Slide 6

Infinite and Yes! We will prove our claim.
Showing that it is Galois is not so hard, we just have to apply the definition into Thm 1.2 and we are done!
But proving that it is infinite is not trivial, we will prove that fact now!

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. □

In other words, $\overline{\mathbb{Q}}$ contains arbitrarily large finite $\mathbb{Q}$-linearly independent set. Why tho?
Suppose we consider the set, $\{1, \sqrt[n]{2}, (\sqrt[n]{2})^2, \ldots, (\sqrt[n]{2})^{n-1}\}$ for all n.
Then the irreducibility of the polynomial $x^n - 2$ by the Eisenstein criterion can be used to observe the linear independence. Think about it!

By now, u guys would have guessed what an absolute Galois group is?

Slide 7

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!
Because I have not yet told how the group is constructed.

We showed that $G_{\mathbb{Q}}$ is an infinite group (to be precise it is a uncountably infinite).
What else do we know that is uncountably infinite, the $\mathbb{R}$ reals. We know that $\mathbb{R}$ has a property which every one has a mixed feelings about, i.e., Topology. So, we can be sure that $G_{\mathbb{Q}}$ also has some topology (specifically called Krull Topology), which is beyond the scope of this talk. But I would like to mention, that $G_{\mathbb{Q}}$ is a compact "profinite" group, I wont go too much of a detail into it but looks like a Cantor set, it is compact and totally disconnected. So, its a very strange looking object.

Question. But why is it uncountably infinite?
I will tell why when we discuss a more precise definition.

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

Slide 8

- 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.

Slide 9

Picture.
The goal of this diagram is to show how the theory of absolute Galois group sits in the center of all of algebraic number theory, primarily group theory, complex analysis (Lfunctions and modular forms) and algebraic geometry (elliptic curves and other algebraic varieties)

Slide 10

By now, you would have guessed what the formal definition is! Let's state it.
The idea was to study all Galois extensions of $\mathbb{Q}$ simultaneously, so we get the formal definition.

Definition. 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 $G_{\mathbb{Q}} \subsetneq \mathrm{Bij}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}})$.
  I should make a remark that $G_{\mathbb{Q}}$ is naturally contained in the bijections of $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$. Because an Automorphism of $\overline{Q}$, the algebraic closure in just the bijection between these two. But it preserves the arithmetic (specifically the arithmetic of complex conjugation must be preserved).
- 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.
  But on the other hand, it is not remotely equal to the set of bijecions because that's just a set theoretic thing and we are putting a lot of structure on these and it is still uncountable, that to me itself is fascinating.
- Actually, $G_{\mathbb{Q}}$ is like a Riemann surface.
  We get this using cohomology theory, which is way beyond the scope, but its good to know. At the finite level, when we were just studying about finite groups, this does not happen, they are just arbitrary finite groups, there is no beautiful theories But when you take the inverse limit and you look all of them put together, then

there is a really nice theory. But things dont always work out nicely because K is not a PID, which makes it to consist non-trivial class groups (which is just one of the reasons)

Slide 11

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 $P_2 = (3, \pm 5) \in E_1(\mathbb{Q})$.
By the way, it is a non-trivial exercise, but $(3, \pm 5)$ is the only integral solution to this Diophantine equation. Takes a little bit of work to prove that, you need to know that $\mathbb{Q}(\sqrt{-2})$ is in fact a PID, but its a fun exercise if you have never done it.

If we consider P_1, we know that $P_3 = (2, -\sqrt{6})$ is a solution too!
which is obvious, but why am I making a big deal about it, well the answer is that, we know that there is a field automorphism that switches $\sqrt{6} \to -\sqrt{6}$, like $a + b\sqrt{6}$ goes to $a - b\sqrt{6}$, its just like complex conjugation that we started with.

We observe that $P_1 \in E(\overline{\mathbb{Q}})$, since $\sqrt{6}$ is an algebraic number.
$x^2 - 6$ is a monic polynomial in $\mathbb{Q}[x]$. But, when you at those points that are invariant under this Galois action. Let G be a group and $X \neq \emptyset$ set. A group action on X is a mapping from $G \times X \to X$, denoted by $(a, x) \mapsto a \cdot x$ such that $1 \cdot x = x$ and $a \cdot (b \cdot x) = (ab) \cdot x$. So if a group acts on something and you put the group up here, we look at the invariance. Then its not invariant because there is an element in the Galois group that swaps P_1 and P_3.

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.

This Galois group knows the solutions to all Diophantine equations, just take the algebraic solutions and take their invariance. Of course, that's hard, I mean its not easy to figure it out, but this is the case. It knows solutions to all Diophantine equations.

Slide 12

But I want to convince you that this is a very hard group 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).
For cyclic groups, the proof I know uses Dirichlet's theorem on primes and progressions (i.e., there are infinitely many primes of the form $1 \pmod{20}$, which is a deep analytic result, its about the non-vanishing of a L-function).

Then, it was also known for p-groups and solvable groups (Shafarevich, 1989).
A p-group is a group in which every element has order equal to a non-negative power of a prime p (incl. p^0)

Galois Representation

Slide 13

The goal of this part of the talk, is to understand a tool that will help us to understand $G_{\mathbb{Q}}$ better! And this tool is called Galois representation

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

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

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

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

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

Slide 14

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

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

Question. So, that's it?

Obviously not! We want ϕ to satisfy one more condition, since G is not some regular group.
For ϕ to be a valid Galois representation, it has to satisfy a fact that ϕ should preserve the properties of the absolute Galois group, i.e., the Galois correspondence between the subgroups of your Galois group and the subfields in the tower that this Galois group is sort of parametrizing.

Slide 15 and 16

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:

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

$\sigma \mapsto 1$, since ϕ is a trivial action. So, here is my claim, you may think you understand this, but in reality you dont understand this representation. And that should strike you as strange, how can I not understand the trivial representation.

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.

For every prime p, there exists $\sigma_p \in G_{\mathbb{Q}}$ (there is an element associated to that prime, actually it is a conjugancy class and it depends on ϕ and it only exists for all most all the primes, but let's sweep that detail under the rug) Under this map,

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

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

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

and the analytic function we get is the Riemann zeta function. So my argument is that if you believe that you understand this representation completely, then you are claiming that you understand the Riemann zeta function completely, and I am sceptical about it!

So, we know that $\zeta(s)$ is defined for all $s \in \mathbb{C}$, where $\Re(s) > 1$. Also, $\zeta(s)$ meromorphically continues to $\mathbb{C}$ and has a function equation (we can prove the meromorphic continuation via the functional equation or actually get the meromorphic continuation one step at a time. There are many way to do it!).

By the way, again its interesting, earlier I said that you can solve a part of the IGP for cyclic groups using Dirichlet's theorem, an analytic result.

Now, we are studying a purely algebraic thing a group acting on a one-dimensional vector space, and looking at this representation, we get analytic object that tells us about the distribution of primes. If you study the Riemann zeta function, you know the central question is "where are the non-trivial zeroes of the $\zeta(s)$ in the critical strip (i.e., between 0 and 1)" and it is conjectured to lie on exactly on the line, where $\Re(s) = \frac{1}{2}$, and that is the Riemann hypothesis.

Slide 17 and 18

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 $E(\mathbb{Q})$ (since we know that elliptic curves are torus, its just product of two circles, $S^1 \times S^1$, and we know what the n-torsion on a circle is, if its the unit circle on the complex plane, its just $\mathbb{Z}/n$ or the n-th roots of unity). 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

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

Now, we will do something weird, but it turns out that it works! Write $n = \ell^N$, where ℓ is a prime and let $N \to \infty$. And we will build a system of them, its not going to be a direct system of them, but an inverse system and we will get a big representation. So. we get the following representation:

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

So, we get the following L-function,

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

So, you start with an arithmetic object and you build a family of Galois representations, Galois actions. Then you build an L-function here, a very strange looking object.

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.

The *order of vanishing* of an L-function $L(s)$ at a point $s = s_0$ is the largest integer m such that $(s - s_0)^m$ divides $L(s)$ in a neighborhood of s_0. In other words, it is the exponent of the zero of $L(s)$ at $s = s_0$. More formally, if $L(s) = (s - s_0)^m g(s)$, where $g(s)$ is a function that is analytic and non-zero at $s = s_0$, then the order of vanishing of $L(s)$ at $s = s_0$ is m. For example, if $L(s) = (s-1)^2(s-2)$, then the order of vanishing of $L(s)$ at $s = 1$ is 2, and at $s = 2$ is 1.

Here r is called the rank of an elliptic curve, which is the size of the smallest torsion-free subgroup of the Mordell-Weil group (in other words, it is the smallest set of points in order to generate all the other points on the elliptic curve.)

Slide 19 and 20

Let's consider another example.

Example. Consider the following Diophantine equation:

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

- $f(x) = x^2 + 3 = (x + \sqrt{-3})(x - \sqrt{-3}) = 0$. (roots in one projective line with two roots)
- We can construct a field that is generated by $\sqrt{-3}$, i.e., $\mathbb{Q}(\sqrt{-3})$ (basically, the roots of this polynomial lives in the number field $K = \mathbb{Q}(\sqrt{-3})$).
- Also, we can construct a Galois representation:

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

  with the following function:

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

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,

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

Here, χ is called a Dirichlet character.

- looking at what happens with my automorphisms that sends $\sqrt{-3}$ somewhere as $\sqrt{-3} \in \overline{\mathbb{Q}}$, and this ϕ keeps track of that. So it is going to send to either $\sqrt{-3}$ or $-\sqrt{-3}$ (i.e., it is either going to fix it or flip it).

- So, it is sending everything to ± 1. Also, this representation keeps track of all the arithmetic that you need for $\mathbb{Q}(\sqrt{-3})$.
- Out of that representation, we can build a character, which is called as Dirichlet character. And we are going to extend it, so that if you forget about $0 \mapsto 0$, that we can identify $\mu_2 = \{\pm 1\}$ with the units in $\mathbb{Z}/3\mathbb{Z}$ extended by 0 and use that character to define an analytic function, which is Dirichlet L-function attached to that character. And that L-function can be used again to give us information, somehow it remembers information about the field, then its special values can tell about the arithmetic properties of its number fields.

Lastly, I would like to talk about a main stream example. Suppose we consider the following elliptic curve over $\mathbb{Q}$,

$$E/\mathbb{Q} : y^2 = x^3 + 1$$

We can construct a non-trivial Galois representation

$$\begin{aligned}
\rho_E &: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T[E]) \\
\rho_E &: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_p(E)) \\
\rho_E &: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p^n])
\end{aligned}$$

where $\mathrm{Aut}(T[E]) \to \mathrm{Aut}(T_p(E)) \to \mathrm{Aut}(E[p^n])$. We can construct a following special function and a L-function of the elliptic curves for that special function,

$$\begin{aligned}
f(\tau) &= \sum_{p \text{ prime}} a_p q^p = q + 4q^7 + 2q^{13} + 8q^{19} + \cdots \\
L(E,s) &= \sum_{p \text{ prime}} \frac{a_p}{p^s} = 1 + \frac{4}{7^s} + \frac{2}{13^5} + \frac{8}{19^s} + \cdots
\end{aligned}$$

where a_p is the number of solutions mod p, where p is a prime and $q = e^{2\pi i \tau}$.

Before, I explain how I got the functions that I mention above. I would like to mention the following trick. To understand how the solutions of an elliptic curve behaves, we just have to observe how the mod p solutions behave. This is much more feasible idea, because there are only finitely many solutions for each p, so there exists algorithms in computation number theory to compute such solutions. By, fundamental theorem of arithmetic and Chinese remainder theorem, we know how the solutions behave for all positive $n \in \mathbb{Z}$.

Going back to our example, we get the following table:

p	a_p
1	1
2	0
3	0
5	0
7	4
11	0
13	2
17	0
19	8
$\vdots$	$\vdots$

So, we can we observe how we got the following functions above. In early 20th century, an Indian mathematician named Srinivasa Ramanujan, studied function of the form $f(\tau)$ and conjectured that if we have information of only the coefficients of prime powers, then we can predict the coefficients of composite powers by prime factorizing

and multiplying the respective prime powers. This conjecture was later proved by Pierre Deligne in the late 20th century.

The special function $f(\tau)$ is a called a modular form (a special case of an automorphic form, an important object in harmonic analysis), which are highly symmetric functions on the complex plane. It was conjectured in the mid 20th century by two Japanese mathematicians Yutaka Taniyama and Goro Shimura and later refined by André Weil, that every elliptic curves over $\mathbb{Q}$ has a corresponding modular form. This conjecture was proved for a special class of elliptic curves called semi-stable elliptic curves by Andrew Wiles in 1995, in order to prove Fermat's Last theorem. The full conjecture was proved by Brian Conrad, Fred Diamond and Richard Taylor in 2001. The most general case connecting the correspondence between abelian varieties and automorphic form lies at the heart of a vast set of conjectures called the "Langland's Program", usually called the "Grand Unified Theory of Mathematics"!.

THANK YOU!