An 8 hours course in Galois theory

Ken Lee

Autumn 2024

Contents

1 The main theorem of Galois theory

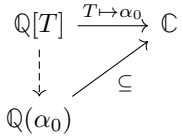
We show an example of the fundamental theorem of Galois theory. Consider the polynomial $f(T) = T^3 - 2 \in \mathbb{Q}[T]$. Let $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{C}$ be the roots of f.

Slogan : Galois theory studies the "symmetries" of roots of polynomials

To make this precise, let us first investigate the field obtained by chucking in $\alpha_0, \alpha_1, \alpha_2$ to $\mathbb{Q}$. Define

$$\mathbb{Q}_f := \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \text{ smallest field in } \mathbb{C} \text{ containing } \mathbb{Q}, \alpha_0, \alpha_1, \alpha_2$$

Question 0 : What does $\mathbb{Q}_f$ look like? We try to describe $\mathbb{Q}(\alpha_0)$ first. Consider the map $T \mapsto \alpha_0$



The image is $\mathbb{Q}[\alpha_0]$ the collection of polynomial expressions in α_0 with coefficients in $\mathbb{Q}$. Since $f \in \mathbb{Q}[T]$ is irreducible[1] we have $\mathbb{Q}[\alpha_0] = \mathbb{Q}[T]/(f)$ and hence this has a $\mathbb{Q}$-basis $1, \alpha_0, \alpha_0^2$.

– *Exercise 1 : show that for a field K and an K-algebra A which is finite dimensional as a K-vector space and an integral domain, A must be field.*

It follows that $\mathbb{Q}[\alpha_0]$ is a field and hence

$$\mathbb{Q}[\alpha_0] = \mathbb{Q}(\alpha_0)$$

Now we do a trick by observing that

$$\left(\frac{\alpha_1}{\alpha_0}\right)^3 = 2/2 = 1$$

Later on, we will give a way of checking when a polynomial has repeated roots so assume for now that all $\alpha_0, \alpha_1, \alpha_2$ are distinct. Then we get $\alpha_1 = \alpha_0\omega$ for some $\omega \neq 1 = \omega^3$, and similarly $\alpha_2 = \alpha_0\omega^2$. The ω, ω^2 here are called a *primitive cube roots of unity*. They are both roots of the polynomial $T^2 + T + 1 \in \mathbb{Q}[T]$.

– *Exercise 2 : Show that $\omega \notin \mathbb{Q}(\alpha_0)$.*[2]

Since $T^2 + T + 1$ is degree two and does not have a root in $\mathbb{Q}(\alpha_0)$, it is irreducible in $\mathbb{Q}(\alpha_0)[T]$ and so

$$\mathbb{Q}[\alpha_0, \omega] \simeq \mathbb{Q}[\alpha_0][T]/(T^2 + T + 1)$$

As a $\mathbb{Q}[\alpha_0]$-vector space, this has dimension two and hence is again a field by Exercise 1. We deduce **Answer 0 :**

$$\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$$

We now define *the Galois group of f* as

$$G_f := \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \{\sigma : \mathbb{Q}_f \to \mathbb{Q}_f \text{ s.t. } \sigma \text{ ring morphism and } \forall\, \lambda \in \mathbb{Q}\,,\, \sigma(\lambda) = \lambda\}$$

Question 1 : Why is this the "symmetries" of $\alpha_0, \alpha_1, \alpha_2$? Observation : any $\sigma \in G_f$ must permute $\{\alpha_0, \alpha_1, \alpha_2\}$. This is ***the* trick** that underlies Galois theory :

$$f(\sigma(\alpha_i)) = (\sigma(\alpha_i))^3 - 2 = \sigma(\alpha_i^3 - 2) = 0$$

Hence we have a well-define group morphism

$$G_f \to \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$$

Since $\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ any $\sigma \in G_f$ is determined by what it does on α_i hence the above morphism is injective. **Answer 1 : The above morphism defines an isomorphism**

$$G_f \simeq \{\sigma \in \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\} \text{ s.t. } \forall g \in \mathbb{Q}[X_0, X_1, X_2]\,, g(\alpha_0, \alpha_1, \alpha_2) = 0 \Rightarrow g(\sigma(\alpha_0), \sigma(\alpha_1), \sigma(\alpha_2)) = 0\}$$

in other words, G_f is the permutations of roots of f which preserves all algebraic relations over $\mathbb{Q}$.

[1] Can be checked by Eisenstein's criterion. Alternatively, a cubic over $\mathbb{Q}$ is reducible iff it has a root in $\mathbb{Q}$. This can be checked to be impossible by brute force.

[2] Hint : Suppose $\omega = \lambda_0 + \lambda_1\alpha_0 + \lambda_2\alpha_0^2$ with $\lambda_i \in \mathbb{Q}$. Then using $\omega^2 + \omega + 1 = 0$ show that α_0 satisfies a degree four polynomial over $\mathbb{Q}$. Then deduce that $\alpha_0 \in \mathbb{Q}$ for a contradiction.

Proof. $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ is precisely the image of the evaluation map

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\ ,\ X_i \mapsto \alpha_i$$

It follows that $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2] \simeq \mathbb{Q}[X_0, X_1, X_2]/I$ where I is the set of polynomials $g(X_0, X_1, X_2)$ with $g(\alpha_0, \alpha_1, \alpha_2)$. From this, it is clear that G_f lands inside the RHS. Now given $\tilde{\sigma}$ in RHS, one can evaluate

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\ ,\ X_i \mapsto \tilde{\sigma}(\alpha_i)$$

Then by definition I is in the kernel of this evaluation map so it factors through the quotient by I to give an automorphism of $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ preserving $\mathbb{Q}$. □

Let us now compute G_f. We have the following

$$\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0][\omega] \simeq \frac{\mathbb{Q}[\alpha_0][Y]}{(Y^2 + Y + 1)} \simeq \frac{\mathbb{Q}[X][Y]/(X^3 - 2)}{(X^3 - 2, Y^2 + Y + 1)/(X^3 - 2)} \simeq \frac{\mathbb{Q}[X, Y]}{(X^3 - 2, Y^2 + Y + 1)}$$

where the last isomorphism is the 3rd isomorphism theorem of rings. Consider the 3-cycle $\sigma := (\alpha_0\ \alpha_1\ \alpha_2)$. Knowing $\omega = \alpha_1/\alpha_0$ we send $X \mapsto \alpha_1, Y \mapsto \omega$.

$$\begin{array}{ccc} & & \overset{X \mapsto \alpha_1}{\underset{Y \mapsto \omega}{\longrightarrow}} \\ \mathbb{Q}[X, Y] & & \mathbb{Q}[\alpha_0, \omega] \\ {\scriptstyle X \mapsto \alpha_0 \atop Y \mapsto \omega} \downarrow & \nearrow_{\simeq} & \\ \mathbb{Q}[\alpha_0, \omega] & & \end{array}$$

We get the factoring because $\alpha_1^3 - 2 = 0 = \omega^2 + \omega + 1$ and so $\sigma \in G_f$. Now consider $\tau := (\alpha_0\ \alpha_1)$. Again, since $\omega = \alpha_1/\alpha_0$ we know τ should send $\omega \mapsto 1/\omega = \omega^2$ so we send $X \mapsto \alpha_0, Y \mapsto \omega^2$.

$$\begin{array}{ccc} & & \overset{X \mapsto \alpha_1}{\underset{Y \mapsto \omega^2}{\longrightarrow}} \\ \mathbb{Q}[X, Y] & & \mathbb{Q}[\alpha_0, \omega] \\ {\scriptstyle X \mapsto \alpha_0 \atop Y \mapsto \omega} \downarrow & \nearrow_{\simeq} & \\ \mathbb{Q}[\alpha_0, \omega] & & \end{array}$$

Again $\alpha_1^3 - 2 = 0 = (\omega^2)^2 + \omega^2 + 1$ gives the above factoring and hence $\tau \in G_f$. It follows that G_f is the whole of $\mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$.

Symmetry means "changes that cannot be observed". The symmetries of a triangle are the ways you can change the triangle such that you cannot tell the difference between before and after. In the same way, G_f are the ways you can swap of roots of f such that as far as $\mathbb{Q}$ can tell, nothing has changed. In this example, there is nothing special about α_0; the whole argument works starting with α_1 or α_2. The roots are equally ambiguous, which is reflected in the quantitative fact that $G_f \simeq S_3$. An example of less ambiguity is $T^3 - 1$. The roots are $1, \omega, \omega^2$. The Galois group of $T^3 - 1$ is cyclic order two generated by $\omega \mapsto \omega^2$. This reflects the

fact that 1 is more special than ω, ω^2 whilst the latter cannot be distinguished from each other. Indeed if one writes $\mu := \omega^2$ then $\omega = \mu^2$.

Back to $T^3 - 2$. Observe that $\mathbb{Q} \subseteq \mathbb{Q}_f^{G_f}$:= the set of elements in $\mathbb{Q}_f$ fixed by G_f. **Claim :** $\mathbb{Q} = \mathbb{Q}_f^{G_f}$**.** Let $x \in \mathbb{Q}_f$ be fixed by G_f. We approach $\mathbb{Q}_f$ this time by adding ω first then α_0. Since $\mathbb{Q}_f = \mathbb{Q}[\omega][\alpha_0]$ we can write

$$x = \lambda_0 + \lambda_1\alpha_0 + \lambda_2\alpha_0^2$$

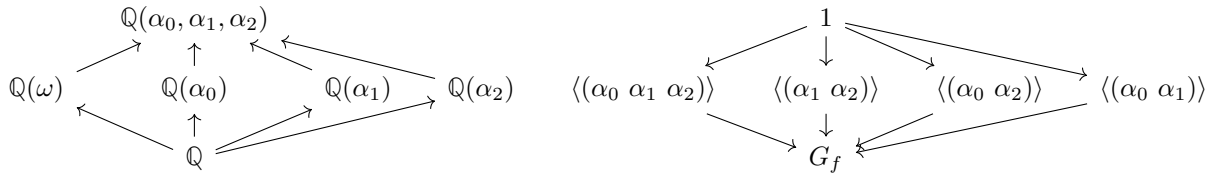
for $\lambda_i \in \mathbb{Q}(\omega)$. Then since $\sigma(\omega) = \omega$ we have

$$x = \sigma(x) = \lambda_0 + \lambda_1\omega\alpha_0 + \lambda_2\omega^2\alpha_0^2$$

Since $1, \alpha_0, \alpha_0^2$ are a $\mathbb{Q}(\omega)$-basis for $\mathbb{Q}_f$, we can compare coefficients to get $\lambda_1 = \lambda_1\omega$ and $\lambda_2 = \lambda_2\omega^2$ This implies $\lambda_1 = 0 = \lambda_2$ and so $x \in \mathbb{Q}(\omega)$. Now $x = \mu_0 + \mu_1\omega$ for $\mu_i \in \mathbb{Q}$. Then

$$x = \tau(x) = \mu_0 + \mu_1\omega^2 = (\mu_0 - \mu_1) - \mu_1\omega$$

which implies $\mu_1 = -\mu_1$ and so $\mu_1 = 0$. We find that $x \in \mathbb{Q}$. More generally, given any subgroup H of G_f we can compute the *fixed subfield* $\mathbb{Q}_f^H$. Here is a diagram of all the subgroups of G_f and their corresponding fixed subfields.



The fundamental theorem of Galois theory says this is all of them. To be more precise, we make some definitions.

Definition – Galois extension

Let $K \to L$ be an extension of fields. We often identify K with its image in L. We call it *Galois* when there is a finite group $G \subseteq \mathrm{Aut}_K L$ such that $K = L^G$.

The extension earlier $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ was an example of a Galois extension.

Proposition – Fundamental theorem of Galois theory

Let $K \to L$ be a Galois extension of fields and let $G := \mathrm{Aut}_K L$. Consider the following two constructions :

- Given a subgroup $H \subseteq G$, define L^H as the set of fixed points of L by H. This defines a field containing the image of K.
- Given a subfield $M \subseteq L$ containing K, define $\mathrm{Aut}_M L$ as the subgroup of G acting trivially on M.

Then we have an order reversing bijection

$$\{\text{subextensions } M \subseteq L\} \underset{L^{-}}{\overset{\text{Aut\_}L}{\underset{\simeq}{\rightleftarrows}}} \{\text{subgroups of } \mathrm{Aut}_K L\}$$

The Galois extension $\mathbb{Q}_f/\mathbb{Q}$ is an example of a *solvable* extension.

Definition
Let $K \to L$ be a field extensions. We say it is *radical* when there exists a chain of extensions

$$K = L_0 \to L_1 \to \cdots \to L_{n-1} \to L_n = L$$

such that each $L_{i+1} = L_i(\alpha_i)$ for some α_i with $\alpha_i^{d_i} \in L_i$ for some $d_i > 0$.
We say a polynomial $f \in K[T]$ is *solvable by radicals* when K_f/K is radical.

Notice that in the example, that the sequence of groups

$$1 \to \langle(\alpha_0\ \alpha_1\ \alpha_2)\rangle \to G_f$$

is such that one subgroup is normal in the next and furthermore that the factor groups are cyclic. This is an example of a *solvable group*.

Definition
Let G be a finite group. Then G is called solvable when there exists a chain

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

such that H_{n+1}/H_n is cyclic.

We will show the following by the end of the course.

Proposition – Characteristization of solvable polynomials
Let K be a field of characteristic zero and $f \in K[T]$. Then f is solvable by radicals iff G_f is solvable.

Proposition
The polynomial $T^5 - T - 1 \in \mathbb{Q}[T]$ has Galois group S_5 and hence is not solvable by radicals.