A very short introduction to Galois theory

Galois Theory Lecture 1, University of Edinburgh, 2022–23
Tom Leinster

Chapter 1 of the notes is called ‘An overview of Galois theory’.

This lecture is an overview of the overview.

The most important idea in Galois theory

Every polynomial has a symmetry group

The rough idea

It's impossible to tell i and $-i$ apart.

Anything true of i is also true of $-i$.

The polynomial $t^2 + 1$ has roots $\pm i$.

Because i and $-i$ are indistinguishable, the symmetry group of $t^2 + 1$ is C_2.
Its elements are the identity on $\{i, -i\}$ and the transposition $i \leftrightarrow -i$.

Note We're going to focus on polynomials over $\mathbb{Q}$.

Polynomials over $\mathbb{R}$ turn out to be a bit trivial.

Conjugate tuples

Let $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ be k-tuples of complex numbers.

We say these two k-tuples are conjugate if they satisfy the same polynomials over $\mathbb{Q}$: that is, for all polynomials $p(t_1, \ldots, t_k)$ over $\mathbb{Q}$,

$$p(\alpha_1, \ldots, \alpha_k) = 0 \iff p(\beta_1, \ldots, \beta_k) = 0.$$

Example I claim that $(i, -i)$ is conjugate to $(-i, i)$.

Let's try some example polynomials p to see if this plausible:

- $t_1 + t_2 = 0$ when $(t_1, t_2) = (i, -i)\ldots$ and also when $(t_1, t_2) = (-i, i)$.
- $3t_1^5 t_2 - t_1^2 - 4t_2^4 = 0$ when $(t_1, t_2) = (i, -i)\ldots$ and also when $(t_1, t_2) = (-i, i)$.

Now the actual proof: for any polynomial $\sum_{r,s} a_{rs} t_1^r t_2^s$ over $\mathbb{Q}$,

$$\begin{aligned} \sum a_{rs} i^r (-i)^s = 0 &\iff \overline{\sum a_{rs} i^r (-i)^s} = 0 \\ &\iff \sum a_{rs} \bar{i}^r \overline{(-i)}^s = 0 \quad \iff \sum a_{rs} (-i)^r i^s = 0. \quad \checkmark \end{aligned}$$

The Galois group of a polynomial

The symmetry group of a polynomial is called its 'Galois group'.

Definition Let $f(t) \in \mathbb{Q}[t]$, with distinct roots $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$.

The Galois group of f is

$$\text{Gal}(f) = \{\sigma \in S_k \; : \; (\alpha_1, \ldots, \alpha_k) \text{ and } (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(k)}) \text{ are conjugate}\}.$$

Example Let $f(t) = t^2 + 1$.

Then f has roots $\alpha_1 = i$ and $\alpha_2 = -i$.

So $k = 2$ and $\text{Gal}(f)$ is a subgroup of S_2.

Which subgroup?

- Certainly $\text{id} \in \text{Gal}(f)$.
- Since $(i, -i)$ and $(-i, i)$ are conjugate, $(1\ 2) \in \text{Gal}(f)$.

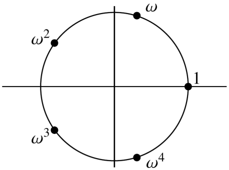
Hence $\text{Gal}(f) = S_2$.

A not so simple example

Let $f(t) = \frac{t^5-1}{t-1} = t^4 + t^3 + t^2 + t + 1$.

Its roots are $\omega = e^{2\pi i/5}$, ω^2, ω^3, ω^4.

What is $\mathrm{Gal}(f)$?



By definition, the elements of $\mathrm{Gal}(f)$ are the permutations $\sigma \in S_4$ such that

$$\left(\omega, \omega^2, \omega^3, \omega^4\right) \text{ and } \left(\omega^{\sigma(1)}, \omega^{\sigma(2)}, \omega^{\sigma(3)}, \omega^{\sigma(4)}\right)$$

satisfy the same polynomials over $\mathbb{Q}$. For instance:

- $(1\ 2) \notin \mathrm{Gal}(f)$, since $t_1^2 - t_2 = 0$ when

  $$(t_1, t_2, t_3, t_4) = (\omega, \omega^2, \omega^3, \omega^4)$$

  but not when

  $$(t_1, t_2, t_3, t_4) = (\omega^2, \omega, \omega^3, \omega^4).$$

- In fact, $\mathrm{Gal}(f)$ is the cyclic group C_4, generated by $(1\ 2\ 4\ 3)$.

What use is the Galois group? (One answer)

A radical number is one that can be constructed from the rationals using $+$, $-$, $\times$, $/$, *and taking nth roots* for any $n \in \mathbb{N}$. E.g.:

$$\left(1/2 + \sqrt[3]{\sqrt[7]{2} - \sqrt[2]{7}}\right) \Big/ \left(\sqrt[4]{6 + \sqrt[5]{2/3}}\right).$$

The roots of any quadratic over $\mathbb{Q}$ are radical:

$$\left(-b \pm \sqrt{b^2 - 4ac}\right)/2a.$$

In fact, the roots of any polynomial of degree 3 or 4 are radical too.

But this fails in degrees 5 and higher!

A polynomial f over $\mathbb{Q}$ is solvable by radicals if all its roots are radical.

Theorem (Galois) *f is solvable by radicals $\iff$ the group $\mathrm{Gal}(f)$ is solvable.*

Some quintics have unsolvable Galois group. They're not solvable by radicals.

Hence there's no 'quintic formula' like the quadratic formula.

Bird's eye view of this course

polynomial over K	$\mapsto$ field containing K	$\mapsto$ group
$f(t) \in \mathbb{Q}[t]$	smallest subfield M of $\mathbb{C}$ containing the roots of f	$\{$automorphisms of $M\}$
$t^2 + 1$	$\{a + bi \ : \ a, b \in \mathbb{Q}\}$	$\{\text{id}, \text{complex conj}\} \cong C_2$
$\dfrac{t^5 - 1}{t - 1}$	smallest subfield of $\mathbb{C}$ containing $e^{2\pi i/5}$	C_4
$t^5 - 6t + 3$ (not solvable by radicals)	*censored*	S_5 (not solvable)

What we'll need, what we'll touch, what we'll learn

We'll need. . .

group theory

ring theory

linear algebra

We'll touch. . .

number theory

classical Euclidean geometry

We'll learn. . .

lots of general lessons about abstract algebra.

Before Thursday's class:

- read Chapter 1 of the notes
- write down one question on a slip of paper.