Dr. Aline Zanardini

aline.zanardini@epfl.ch

MA A1 354

Math 317 - Algebra V (Galois theory)

Introductory lecture (Sep 11, 2025)

Homework: before the next lecture, please read Chapter 1 in Milne's notes.

Today: A short introduction to Galois theory

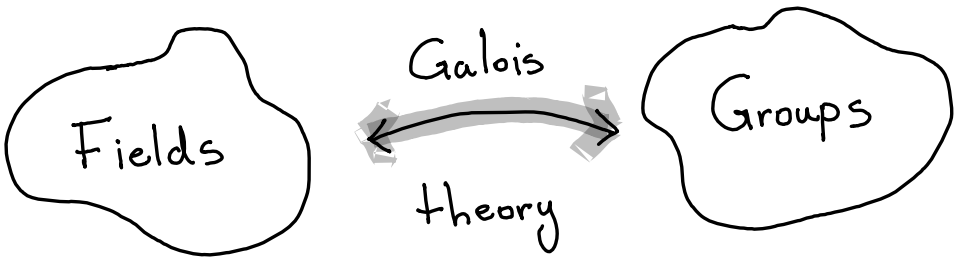
The beautiful idea that Evariste Galois had is the following:

Every polynomial has a symmetry group!

f

polynomial over a field K → A field containing K and the roots of f → A group, namely Gal(L/K) = Gal(f)

i.e. a field extension L/K



It allows us to prove the following theorem.

(Galois) A polynomial is solvable by radicals iff its Galois group is solvable (soluble).

Recall that a polynomial $f \in K[x]$ being solvable means that we can find a chain of finite field extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = L$$

such that

(1) $K_i = K_{i-1}[\alpha_i]$, where

α_i is a root of a polynomial of the form $x^{m_i} - a_i$ for some integer $m_i \geq 2$ and some $a_i \in K_{i-1}$

(2) L is a splitting field for f.

Similarly, a group G is called solvable (or soluble) if we can find a chain

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where each factor G_i / G_{i-1} is abelian.

Fundamental theorem of Galois theory:

Given L/K finite and Galois,

$$\exists$$

$$\left\{ \begin{array}{l} \text{intermediate} \\ \text{fields } K \subset F \subset L \end{array} \right\} \quad \longleftrightarrow \quad \left\{ \begin{array}{l} \text{Subgroups} \\ \text{of } G = \mathrm{Gal}(L/K) \end{array} \right\}$$

$$F = L^H = \{ \ell \in L ; h\ell = \ell \ \ \forall\, h \in H \} \quad \longleftarrow \quad H$$

The upshot: in this class we will need group theory, field/ring theory and linear algebra and we will bump into number theory and some geometry!

Galois theory also explains why the ancient greeks were not able to solve the following problems.

(A) Squaring the circle: given a circle, construct a square with the same area.

(B) trisecting the angle: given an arbitrary angle (of measure) α, construct $\alpha/3$.

(c) duplicating the cube: given a cube, construct a new cube whose volume is twice the volume of the first cube.

A historical interlude

- solutions to linear polynomial equations are trivial
- a formula for the roots of a quadratic polynomial is known since the Babylonians.
- solvability by radicals of cubics and quartics 16th & 17th centuries

  del Ferro, Ferrari, Cardano, Descartes ...

- Abel, 1824: The general equation of degree n is not solvable by radicals for any $n \geq 5$.

- Galois, 1831 : asks and answers

Why ?

Example The quintic polynomial $x^5 - 4x + 2$ is not solvable by radicals because the associated group of symmetries is S_5, which contains A_5. But A_5 is not solvable, since it is simple and non-abelian !

Another example (The symmetries of the solutions to $f(x) = x^3 - 2 = 0$)

* We consider $f \in \mathbb{Q}[x]$ $(K = \mathbb{Q})$

Let $\alpha = \sqrt[3]{2}$, $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

$$\omega^3 = 1$$

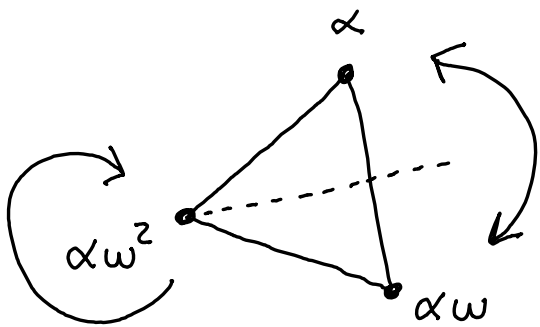
The roots of $f(x) = x^3 - 2$ are

$$\alpha,\ \alpha\omega \text{ and } \alpha\omega^2$$

Q What are the possible field symmetries of $\mathbb{Q}(\alpha, \omega)$?

$\updownarrow$

permutations of the roots $\rightsquigarrow S_3$



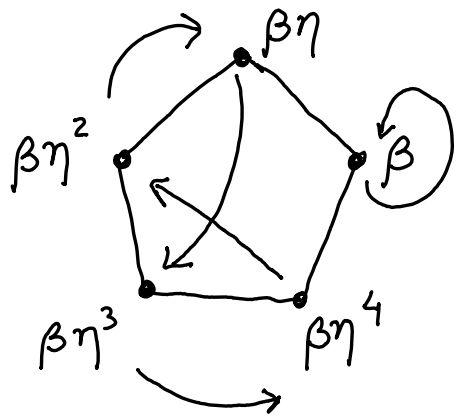
We have the symmetry $\begin{cases} \alpha \longmapsto \alpha\omega \\ \omega \longmapsto \omega^2 \end{cases}$

because $\mathbb{Q}(\alpha, \omega) \simeq \mathbb{Q}(\alpha\omega, \omega^2)$

Warning ⚠

Given a prime p, the polynomial $x^p - 2$ has $p(p-1)$ symmetries.

For example, for $x^5 - 2$, letting $\beta = \sqrt[5]{2}$ and $\eta^5 = 1$ we also have non-geometric permutations:



Exercises

1) Show there is an injection

$$C_3 \hookrightarrow S_3$$

with normal image and quotient $\simeq C_2$

2) Show there is an injection

$$C_2 \times C_2 \hookrightarrow A_4$$

with normal image and quotient $\simeq C_3$

Basics of fields

Definition: A field is a commutative ring $(K, +, \cdot, 0_K, 1_K)$ with at least two elements such that every non-zero element is invertible.

This means

(1) $(K, +, 0_K)$ is a commutative group;

(2) $(K^\times, \cdot, 1_K)$ is a commutative group;

(3) the distributive laws hold

A subfield of K is a subring that is closed under taking inverses.

Proposition Let K be a field.

The following statements are true.

1. K does not contain a non-zero proper ideal.
2. If $\varphi: K \longrightarrow A$ is a ring morphism φ is injective.
3. Any finitely generated K-module is free.
4. The polynomial ring $K[x]$ is a PID.

This means it is an integral domain

$\not\exists$ nonzero zero divisors

and every ideal is principal

generated by a single element

(5) For any $n \geq 1$,

$F := K[x_1, \ldots, x_n] = K[x_1, \ldots, x_{n-1}][x_n]$

is a UFD and is Noetherian

UFD: every $f \in F \setminus \{0_F, 1_F\}$ can be written as a product of irreducible elements

Noetherian: it satisfies ACC on ideals

(Recall: UFD $\Leftarrow$ PID)

Definition An extension of K is a field $L \supset K$. The degree of the extension, denoted by $[L:K]$ is the dimension of L as a K-vector space