What are...group actions on fields?

Or: The beginning of Galois theory

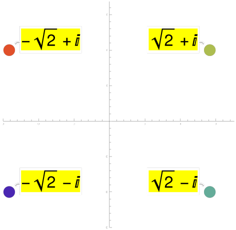
Groups in the wild

Groups naturally arise as automorphisms a.k.a. symmetries of objects, *e.g.*:

- Symmetry groups of the platonic solids Dice!

$S_4 \circlearrowright$  $S_4 \times \mathbb{Z}/2\mathbb{Z} \circlearrowright$   $A_5 \times \mathbb{Z}/2\mathbb{Z} \circlearrowright$  

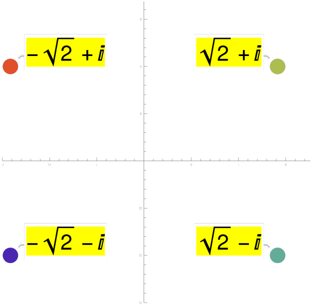
- Roots of polynomials also have certain symmetries

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \circlearrowright$ 

Question. What are the symmetry groups of fields?

Symmetries and field extensions

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \circlearrowright$

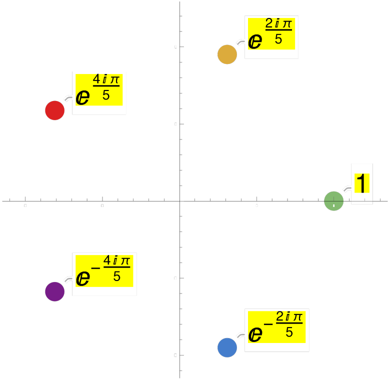


$$f: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ i \mapsto i \\ \mathbb{Q} \text{ fixed} \end{cases} \qquad g: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ i \mapsto -i \\ \mathbb{Q} \text{ fixed} \end{cases}$$

- f and g are automorphisms of $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$, both fix $\mathbb{Q}$
- The minimal polynomial of $\sqrt{2} + i$ is of degree $4 = |\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}|$

A badly behaved example

$\mathbb{Z}/5\mathbb{Z} \circlearrowleft$



$$f : \zeta_5^k = e^{k2\pi i/5} \mapsto \zeta_5^{k+1}$$

- f is not an automorphisms of $\mathbb{Q}(\zeta_5)$ and f does not fix $\mathbb{Q}$
- The minimal polynomial of ζ_5 is of degree 4, not $5 = |\mathbb{Z}/5\mathbb{Z}|$

For completeness: The formal definition/statements

(a) An automorphism $f \in \mathrm{Aut}(\mathbb{L})$ is a field isomorphism $\mathbb{L} \to \mathbb{L}$ A symmetry

(b) $\mathrm{Aut}(\mathbb{L})$ is a group

(c) For a subgroup $G \subset \mathrm{Aut}(\mathbb{L})$ we have the fixed (sub)field

$$\mathbb{L}^G = \{x \in \mathbb{L} \mid f(x) = x \forall f \in G\} \subset \mathbb{L}$$

(d) The orbit of $x \in \mathbb{L}$ is

$$G.x = \{f(x) \mid f \in G\}$$

Let $\mathbb{K} = \mathbb{L}^G$ for $G \subset \mathrm{Aut}(\mathbb{L})$ finite

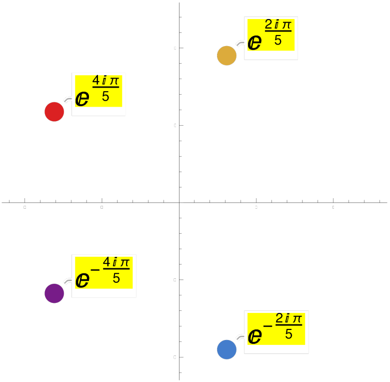
- If $G.x = \{x = x_1, ..., x_r\}$, then $[\mathbb{K}(x) : \mathbb{K}] = r$
- $[\mathbb{K}(x) : \mathbb{K}]$ divides $|G|$
- The minimal polynomial is

$$m_x = (X - x_1) \cdot ... \cdot (X - x_r)$$

- $[\mathbb{L} : \mathbb{K}] = |G|$

Back to the fifth root of unity ζ_5

$\mathbb{Z}/4\mathbb{Z} \circlearrowleft$



$$f : \zeta_5^k \mapsto \zeta_5^{2k}$$

- f is an automorphisms of $\mathbb{Q}(\zeta_5)$ and f does fix $\mathbb{Q}$
- The minimal polynomial of ζ_5 is

$$m_{\zeta_5} = (X - \zeta_5)(X - \zeta_5^2)(X - \zeta_5^3)(X - \zeta_5^4)$$

Thank you for your attention!

I hope that was of some help.