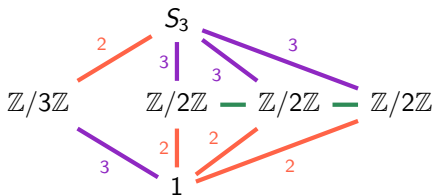


What is...the fundamental theorem of Galois theory?

Or: From roots to groups and back

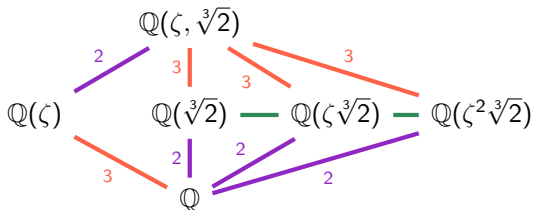
S_3 and its subgroup lattice



- ▶ S_3 has six subgroups, four up to conjugacy Green left-right arrow
- ▶ A copy of $\mathbb{Z}/3\mathbb{Z}$ of index 2
- ▶ Three copies of $\mathbb{Z}/2\mathbb{Z}$ of index 3
- ▶ $\mathbb{Z}/3\mathbb{Z}$ is normal, the three copies of $\mathbb{Z}/2\mathbb{Z}$ are not

We have seen this is for roots of polynomials

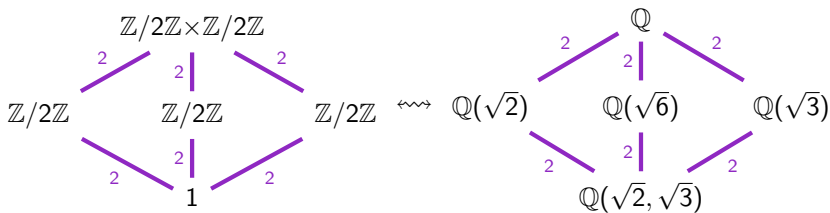
$\mathbb{Q}(\zeta = e^{2\pi i/3}, \sqrt[3]{2})$ and its subfield lattice



- ▶ $\mathbb{Q}(\zeta, \sqrt[3]{2})$ has six subfields, four up $\text{Aut}(\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q})$ Green left-right arrow
- ▶ A copy of $\mathbb{Q}(\zeta)$ of degree 3
- ▶ Three copies of $\mathbb{Q}(\sqrt[3]{2})$ of degree 2
- ▶ $\mathbb{Q}(\zeta)$ is Galois over \mathbb{Q} , the three copies of $\mathbb{Q}(\sqrt[3]{2})$ are not

Main observation This is the same as for S_3 , but upside down

A direct comparison



(a) On the subgroup side this is clear since
 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0), (1,0), (1,1), (0,1)\}$

(b) On the subfield side this is not so obvious:

► $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \{1, f, g, gf\}$ where

$$f = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}, \quad g = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$$

► The fixed field of f is $\mathbb{Q}(\sqrt{2})$, the fixed field of g is $\mathbb{Q}(\sqrt{3})$ and the fixed field of gf is $\mathbb{Q}(\sqrt{6} = \sqrt{2} \cdot \sqrt{3})$

► There are no other subfields

For completeness: The formal statement

If \mathbb{L} is Galois over \mathbb{K} with Galois group $G(\mathbb{L}/\mathbb{K}) = \text{Aut}(\mathbb{L}/\mathbb{K})$, then:

(a) \mathbb{L} is Galois over any $\mathbb{K} \subset \text{subfields } Z \subset \mathbb{L}$

(b) There are inverse bijections, the Galois correspondences:

$$\begin{aligned} \{\mathbb{K} \subset \text{subfields } Z \subset \mathbb{L}\} &\xrightarrow{\cong} \{\text{subgroups of } G(\mathbb{L}/\mathbb{K})\}, Z \mapsto G(\mathbb{L}/Z) \\ \{\text{subgroups } H \text{ of } G(\mathbb{L}/\mathbb{K})\} &\xrightarrow{\cong} \{\mathbb{K} \subset \text{subfields } Z \subset \mathbb{L}\}, H \mapsto \mathbb{L}^H \end{aligned}$$

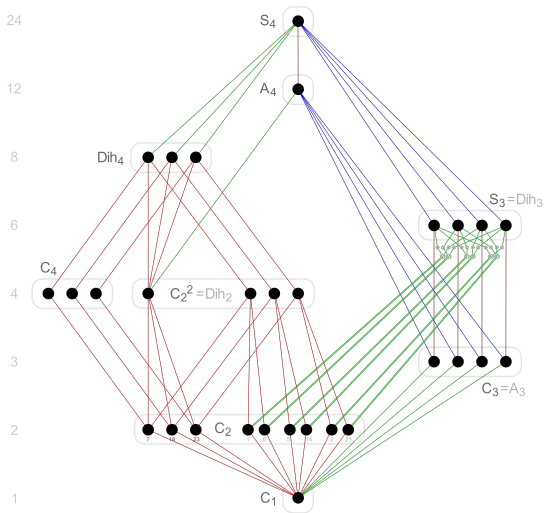
(c) $(Z \subset Z') \Leftrightarrow (G(\mathbb{L}/Z') \subset G(\mathbb{L}/Z))$ Upside down

(d) $[Z : \mathbb{K}] = |G(\mathbb{L}/\mathbb{K})|/|G(\mathbb{L}/Z)|$ (whenever this make sense) Order and index

(e) $(Z \text{ is Galois over } \mathbb{K}) \Leftrightarrow (G(\mathbb{L}/Z) \triangleleft G(\mathbb{L}/\mathbb{K}) \text{ is normal})$ Galois and normal

- The Galois correspondence for \mathbb{L} not Galois over \mathbb{K} still works, but is only surjective respectively injective

S_4 vs. explicit roots



- ▶ 30 subgroups (black dots), 11 up to conjugacy (gray rectangles – space indicates different conjugacy classes), only A_4 and 1 are normal
- ▶ Homework. Do the same for $\mathbb{Q}(\text{roots of } X^4 + X + 1)$;-)

Thank you for your attention!

I hope that was of some help.