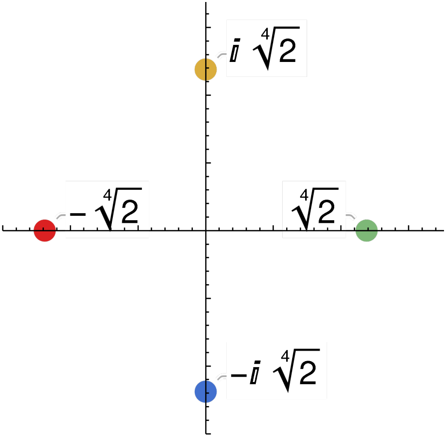
What are...Galois extensions?

Or: Shuffling roots

Splitting fields

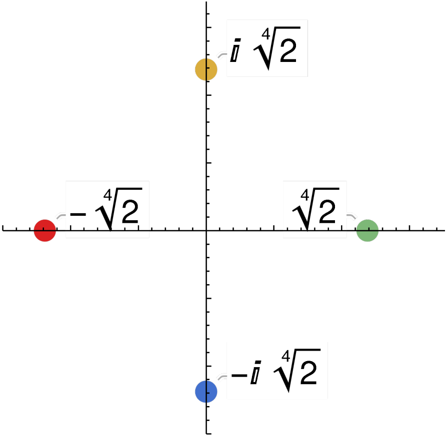
$X^4 - 2$ has roots $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$



What makes $\mathbb{L} = \mathbb{Q}(\text{roots of } X^4 - 2)$ "better" than *e.g.* $\mathbb{Q}(\sqrt[4]{2})$?

Symmetries of the roots

$G \circlearrowright$

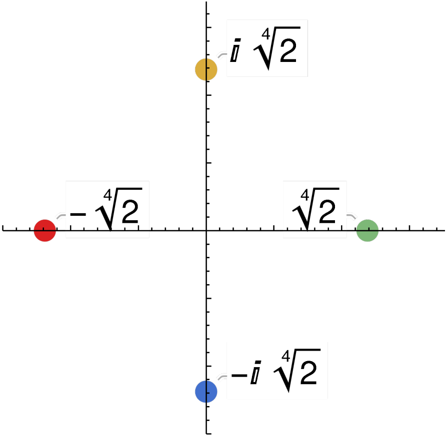


$$f: \text{complex conjugation}, \quad g: \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ \text{“Rest fixed”} \end{cases}$$

- $G = \langle f, g \mid f^2 = g^4 = (gf)^2 = 1 \rangle \cong D_8$, the dihedral group of order eight
- Most of these symmetries are not visible in $\mathbb{Q}(\sqrt[4]{2})$: $G_{\mathbb{Q}(\sqrt[4]{2})} = \langle g^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$

More symmetries of the roots?

$D_8 \circlearrowright$



orbit $D_8.\sqrt[4]{2} = \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$, fixed field $\mathbb{L}^{D_8} = \mathbb{Q}(\text{roots of } X^4 - 2)^{D_8} = \mathbb{Q}$

- $[\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{L}^{D_8}] \cdot [\mathbb{L}^{D_8} : \mathbb{Q}] = |D_8| \cdot [\mathbb{L}^{D_8} : \mathbb{Q}]$, thus $[\mathbb{L} : \mathbb{Q}] = 8 = |D_8|$
- $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4 \neq |\mathbb{Z}/2\mathbb{Z}|$

For completeness: The formal definition/statements

The following are equivalent for an algebraic field extension $\mathbb{L}$ of $\mathbb{K}$:

(a) $\mathbb{L}$ is the splitting field of a separable polynomial in $\mathbb{K}[X]$

(b) $\mathbb{L}$ is normal and separable over $\mathbb{K}$

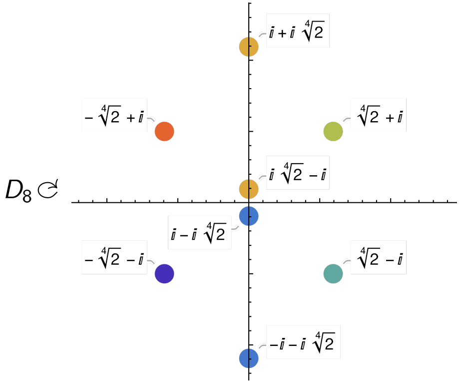
(c) $\mathrm{Aut}(\mathbb{L}/\mathbb{K}) = [\mathbb{L} : \mathbb{K}]$

(d) $\mathbb{L}^{\mathrm{Aut}(\mathbb{L}/\mathbb{K})} = \mathbb{K}$

If any of these are true, $\mathbb{L}$ is Galois over $\mathbb{K}$

- $G(\mathbb{L}/\mathbb{K}) = \mathrm{Aut}(\mathbb{L}/\mathbb{K})$ is called the Galois group of $\mathbb{L}$ over $\mathbb{K}$
- The first two conditions involve polynomials, the other the Galois group
  Roots and symmetries
- Every separable extension can be embedded into a Galois extension
- If $\mathbb{K}$ is of characteristic 0 or finite, then the separability conditions always hold

Different polynomial, same Galois group



f : complex conjugation, $\quad g : \begin{cases} \sqrt[4]{2} \mapsto i\sqrt[4]{2} \\ \text{"Rest fixed"} \end{cases}$

- $\mathbb{Q}(\text{roots of } X^4 - 2) = \mathbb{Q}(\text{roots of } X^8 + 4X^6 + 2X^4 + 28X^2 + 1) = \mathbb{Q}(\sqrt[4]{2}, i)$
- The orbit $D_8.(i + \sqrt[4]{2}) =$ roots of $X^8 + 4X^6 + 2X^4 + 28X^2 + 1$
- The minimal polynomial id $m_{i+\sqrt[4]{2}} = X^8 + 4X^6 + 2X^4 + 28X^2 + 1$

Thank you for your attention!

I hope that was of some help.