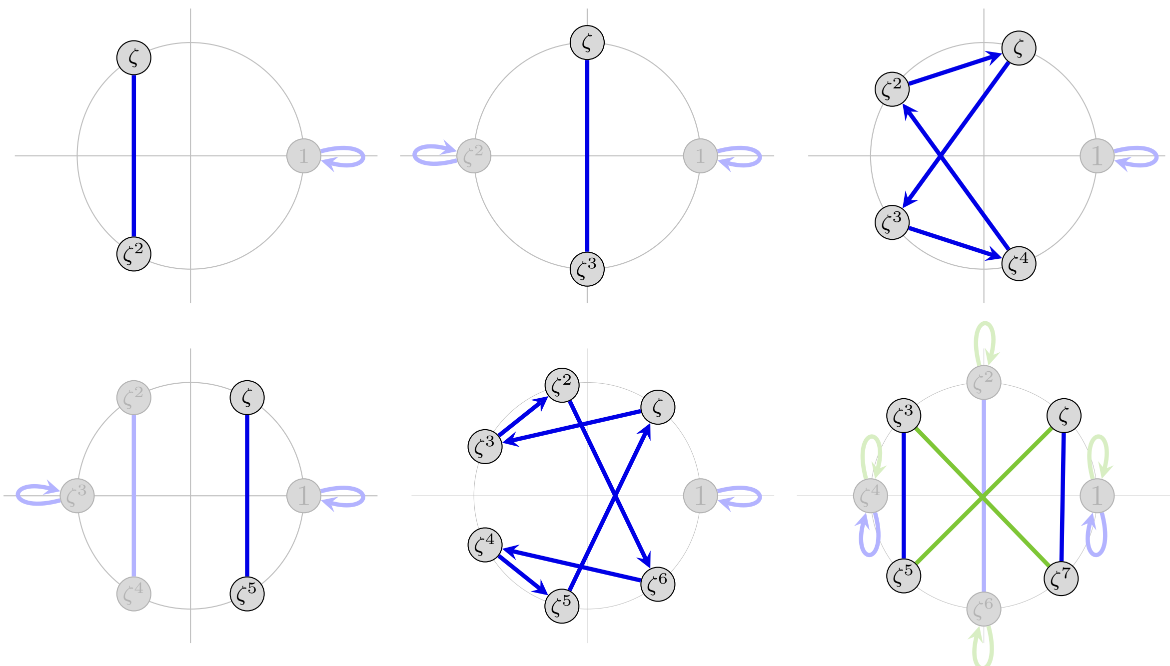
1. The Galois group of $x^n - 1$ naturally acts on the n^{th} roots of unity; this is shown below for $n = 3, \dots, 8$. The primitive roots are highlighted.



   (a) Construct analogous diagrams for $n = 9$, 10, and 16.

   (b) For each of these three, write the splitting field of $x^n - 1$ with elements that do not involve ζ. If possible, write the generating automorphism(s) of $\mathrm{Gal}(x^n - 1)$ in terms of them. For example, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i)$, and $\mathrm{Gal}(x^8 - 1) = \langle \sigma, \tau \rangle \cong \mathbb{Z}_8^\times \cong V_4$, where

$$\begin{cases} \sigma\colon \sqrt{2} \longmapsto \sqrt{2} \\ \sigma\colon \quad i \longmapsto -i \end{cases} \qquad \begin{cases} \tau\colon \sqrt{2} \longmapsto -\sqrt{2} \\ \tau\colon \quad i \longmapsto i \end{cases}$$

   (c) Draw the subgroup lattice of $\mathrm{Gal}(x^n - 1)$ and the subfield lattice of $\mathbb{Q}(\zeta)$.

2. Consider the following polynomial that is irreducible over $\mathbb{Q}$:

$$f(x) = x^4 - x^2 - 5 = \left(x^2 - \sqrt{\tfrac{1}{2} + \tfrac{\sqrt{21}}{2}}\right)\left(x^2 - \sqrt{\tfrac{1}{2} - \tfrac{\sqrt{21}}{2}}\right).$$

   Denote its roots by r_1, r_2, r_3, r_4, its splitting field by $K = \mathbb{Q}(r_1, r_2, r_3, r_4)$, and its Galois group over $\mathbb{Q}$ by $G = \mathrm{Gal}(f(x))$.

   (a) Since $f(x)$ is irreducible, $[\mathbb{Q}(r_i) : \mathbb{Q}] = 4$. Use this to find a lower bound on $[K : \mathbb{Q}]$.

   (b) By the tower law, $[K : \mathbb{Q}] = [\mathbb{Q}(r_1, r_2, r_3, r_4) : \mathbb{Q}]$ is equal to

$$[\mathbb{Q}(r_1, r_2, r_3, r_4) : \mathbb{Q}(r_1, r_2, r_3)] \cdot [\mathbb{Q}(r_1, r_2, r_3) : \mathbb{Q}(r_1, r_2)] \cdot [\mathbb{Q}(r_1, r_2) : \mathbb{Q}(r_1)] \cdot [\mathbb{Q}(r_1) : \mathbb{Q}].$$

   Use this to find an upper bound on $[K : \mathbb{Q}]$.

   (c) Find $[K : \mathbb{Q}] = |\,\mathrm{Gal}(f(x))|$, and then the Galois group by process of elimination.

3. Suppose $\alpha \neq 0$ is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is odd.

   (a) Show that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha + \alpha^{-1})$.

   (b) Give an example to show how this can fail if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is even.

   (c) Repeat the previous two parts, but for the subfield $\mathbb{Q}(\alpha^2 - \alpha)$.