Read Chapters 10.6–10.7 of *Visual Group Theory* or Chapter 22 of *AATA*. Then write up solutions to the following exercises.

1. The splitting field of $f(x) = x^4 - 3$ is $K = \mathbb{Q}(\sqrt[4]{3}, i)$. Since this is a degree-8 extension over $\mathbb{Q}$ (see HW 11), its Galois group has order 8.

   (i) In the complex plane, sketch the roots of $f(x)$, and all 4^{th} roots of unity: $\pm 1, \pm i$.

   (ii) Compute the Galois group of $f(x)$. Write down two automorphisms, r and f, that generate it. It suffices to specify where they send the generators $\sqrt[4]{3}$ and i.

   (iii) Draw the subgroup lattice of G. Each subgroup should be expressed by its generators, rather than what subgroup it is isomorphic to. Label the edges by index, and circle the subgroups that are normal in G.

   (iv) Draw the subfield lattice of K. Label the edges by degree, and circle the subfields that are normal extensions of $\mathbb{Q}$. [*Hint*: The two subfields that are "easiest" to overlook are $\mathbb{Q}((1+i)\sqrt[4]{3})$ and $\mathbb{Q}((1-i)\sqrt[4]{3})$.]

   (v) For each intermediate subfield $\mathbb{Q} \subseteq F \subseteq K$, write down the largest subgroup of G that fixes F.

   (vi) For each subgroup $H \leq G$, write down the largest intermediate subfield fixed by H.

   (vii) For each normal extension F of $\mathbb{Q}$, find a polynomial $g(x)$ whose splitting field is F.

   (viii) For each non-normal extension E of $\mathbb{Q}$, find a polynomial that has one, but not all, of its roots in E.

2. The roots of $f(x) = x^n - 1$ are the n complex numbers $C_n := \{e^{2k\pi i/n} : k = 0, 1, \dots, n-1\}$, and are called the n^{th} *roots of unity*. A *primitive* root of unity is $\zeta = e^{2k\pi i/n}$ for which $\gcd(n, k) = 1$. It is easy to see that $\mathbb{Q}(\zeta)$ is the splitting field of $x^n - 1$.

   (a) For each $n = 3, \dots, 8$, sketch the n^{th} roots of unity in the complex plane. Use a different set of axes for each n. Next to each root, write its order, as an element of C_n. Make it clear (e.g., star, or draw darker) which are the primitive roots of unity.

   (b) Prove that for any primitive root of unity $\zeta_k = e^{2k\pi i/n}$, the mapping

   $$\phi_k \colon \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta), \qquad \phi_k(\zeta) = \zeta^k$$

   is a field automorphism. That is, prove that ϕ_k is a surjective field homomorphism (every nonzero field homomorphism is injective). Why is this not an automorphism if $\gcd(n, k) \neq 1$?

   (c) Make a muliplication table of $\mathrm{Gal}(x^n - 1)$ for $n = 3, \dots, 8$.

   (d) Describe the group $\mathrm{Gal}(x^n - 1)$. This is a class of groups that we have previously encountered.

3. For each of the following polynomials, determine if it is irreducible. If it is not, then factor it into irreducible factors.

   (a) $f(x) = x^4 - 10x^3 + 12x^2 - 8x + 6$ over $\mathbb{Q}$.

   (b) $f(x) = x^4 + x^3 + x^2 + x + 1$ [*Hint*: Let $u = x + 1$, and change variables.]

   (c) $f(x) = x^5 - 1$ over $\mathbb{Q}$.

   (d) $f(x) = x^6 - 1$ over $\mathbb{Q}$. [*Hint*: Google "cyclotomic polynomial."]

   (e) $f(x) = x^8 - 1$ over $\mathbb{Q}$.

   (f) $f(x) = x^{12} - 1$ over $\mathbb{Q}$.

   (g) $f(x) = x^3 + x^2 + x + 1$ over $\mathbb{Z}_2$.

   (h) $f(x) = x^3 + x + 2$ over $\mathbb{Z}_3$.

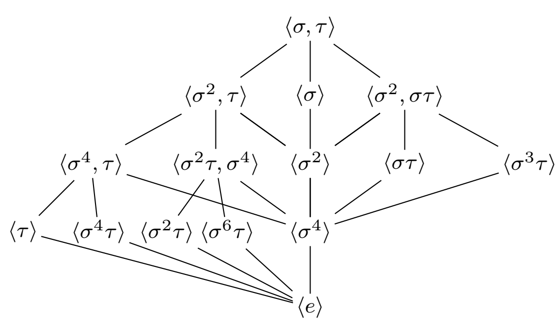
4. The splitting field of $f(x) = x^8 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[8]{2}, \zeta) = \mathbb{Q}(\sqrt[8]{2}, i)$, where $\zeta = e^{2\pi i/8} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$, a primitive 8^{th} root of unity. The Galois group is generated by the automorphisms

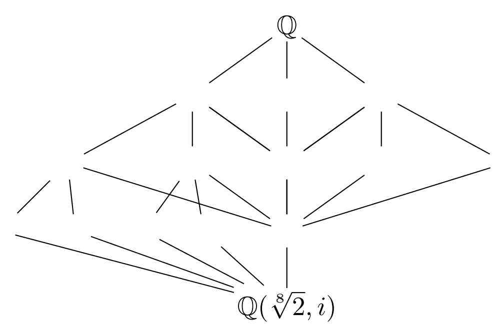
$$\begin{cases} \sigma\colon \sqrt[8]{2} \longmapsto \zeta\sqrt[8]{2} \\ \sigma\colon \quad \zeta \longmapsto \zeta \end{cases} \qquad\qquad \begin{cases} \tau\colon \sqrt[8]{2} \longmapsto \sqrt[8]{2} \\ \tau\colon \quad i \longmapsto -i\,. \end{cases}$$

It is isomorphic to the *quasidihedral group*, with group presentation

$$QD_8 = \langle \sigma, \tau \mid \sigma^8 = 1,\ \tau^2 = 1,\ \tau\sigma\tau = \sigma^3 \rangle,$$

and subgroup lattice shown below.





   (a) Draw Cayley diagrams of both QD_8 and the regular dihedral group, D_8.

   (b) Sketch the roots of $f(x) = x^8 - 2$ on the complex plane, along with all 8^{th} roots of unity: $\zeta^0, \zeta^1, \dots, \zeta^7$.

   (c) For each subgroup $H \leq \text{Gal}(x^8 - 2)$, find the largest subgroup of $\mathbb{Q}(\sqrt[8]{2}, i)$ fixed by H, and write it in the corresponding place on the subfield lattice on the right.
   It is helpful to know that the proper subfields of $\mathbb{Q}(\sqrt[8]{2}, i)$ are: $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[8]{2})$, $\mathbb{Q}(\sqrt{2}i)$, $\mathbb{Q}(\sqrt[4]{2}i)$, $\mathbb{Q}(\sqrt[8]{2}i)$, $\mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt[4]{2}, i)$, $\mathbb{Q}((1+i)\sqrt[4]{2})$, $\mathbb{Q}((1-i)\sqrt[4]{2})$, $\mathbb{Q}(\zeta\sqrt[8]{2})$, $\mathbb{Q}(\zeta^3\sqrt[8]{2})$.

   (d) Circle each subfield E that is a normal extension of $\mathbb{Q}$, and find a polynomial whose splitting field over $\mathbb{Q}$ is E.