Read the following, which can all be found either in the textbook or on the course website.

- Chapters 10.6–10.7 of *Visual Group Theory* (VGT).
- VGT Exercises 10.3, 10.7, 10.16–10.18, 10.20, 10.22–10.28.

Write up solutions to the following exercises.

1. Recall that 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) Sketch the roots of $f(x)$ in the complex plane.

   (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 $f(x)$ 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. Recall that the roots of $f(x) = x^n - 1$ are the n complex numbers $\{e^{2k\pi i/n} : k = 0, 1, \dots, n-1\}$, 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. Make it clear (e.g., star, or draw darker) which of these are the primitive roots of unity.

   (b) Prove that if $\gcd(n, k) = 1$, then 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 $\mathbb{Z}_3$.