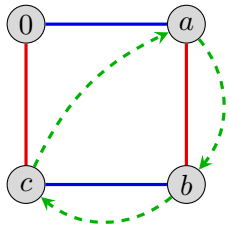
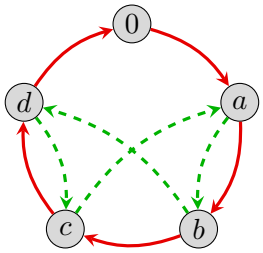
Read the following, which can all be found either in the textbook or on the course website.

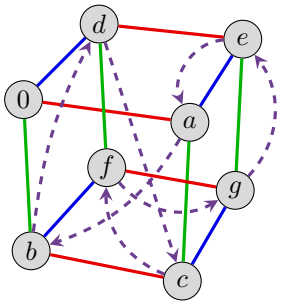
- Chapters 10.1–10.5 of *Visual Group Theory* (VGT).
- VGT Exercises 10.1, 10.2, 10.4, 10.5, 10.8–10.14, 10.21, 10.30.

Write up solutions to the following exercises.

1. There is a unique field $\mathbb{F}_q$ of order $q = p^k$ for every prime p and positive integer k. For all other $q \in \mathbb{N}$, there is no finite field of order q. For each of the fields $\mathbb{F}_4$, $\mathbb{F}_5$, and $\mathbb{F}_8$, the Cayley diagrams for addition and multiplication are shown below, overlayed on the same set of nodes. The solid arrows are the Cayley diagrams for addition and the dashed arrows are the Cayley diagrams for multiplication.







   (a) For each field above, determine whether or not the addition and multiplication operations are in fact, addition and multiplication modulo some number. If yes, relabel the vertices accordingly. If no, explain why it fails.

   (b) Create Cayley diagrams for the finite fields $\mathbb{F}_3$ and $\mathbb{F}_7$.

2. The roots of the polynomial $f(x) = x^n - 1$ are the n complex numbers $\{e^{2k\pi i/n} : k = 0, 1, \ldots, n-1\}$. These are called the n^{th} *roots of unity*.

   (a) For each $n = 3, \ldots, 8$, sketch the n^{th} roots of unity in the complex plane. Use a different set of axes for each n.

   (b) The n^{th} roots of unity form a group under multiplication. Give a minimal generating set. What group is this isomorphic to?

3. (a) Find a basis for the extension field $\mathbb{Q}(\sqrt[4]{3})$ of $\mathbb{Q}$. That is, find a minimal set of $v_1, \ldots, v_k \in \mathbb{Q}(\sqrt[4]{3})$ such that every $x \in \mathbb{Q}(\sqrt[4]{3})$ can be written as a unique linear combination of the v_i's. [*Hint*: Start by taking $v_1 = 1$ and $v_2 = \sqrt[4]{3}\ldots$]

   (b) Sketch the roots of the polynomial $f(x) = x^4 - 3$ in the complex plane. Write each one as $a + bi$, where $a, b \in \mathbb{Q}$. Additionally, write each root in polar form: $z = Re^{i\theta}$.

   (c) The field $\mathbb{Q}(\sqrt[4]{3}, i)$ is called the *splitting field* of f over $\mathbb{Q}$, because it is the smallest extension field of $\mathbb{Q}$ that contains the roots of f. Find a basis for $\mathbb{Q}(\sqrt[4]{3}, i) = \mathbb{Q}(\sqrt[4]{3})(i)$ over $\mathbb{Q}$. What is its dimension as a $\mathbb{Q}$-vector space?

4. Thus far in class, we have seen a number of algebraic extensions of $\mathbb{Q}$, including:

$$\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{6}), \quad \mathbb{Q}(\sqrt{2},\sqrt{3}), \quad \mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{-3},\sqrt[3]{2}), \quad \mathbb{Q}(\sqrt[4]{3},i), \quad \mathbb{Q}(\sqrt[4]{3}).$$

Arrange these fields in a subfield lattice, and include $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ as well. Note that there will be (many!) "missing" fields, so only include those listed above. Include the degree of each extension, but only for the actual edges in your lattice.

5. Consider the function

$$\phi\colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2}), \qquad \phi(a+b\sqrt{2}) = a - b\sqrt{2}.$$

Show that ϕ is a field automorphism, meaning that it satisfies the following equations for all $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$:

$$\phi(\alpha+\beta) = \phi(\alpha) + \phi(\beta), \qquad \phi(\alpha\cdot\beta) = \phi(\alpha)\cdot\phi(\beta).$$

6. Consider the following extension field of $\mathbb{Q}$:

$$K = \mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + d\sqrt{2}i \mid a,b,c,d \in \mathbb{Q}\}.$$

(a) Find the Galois group $G = \mathrm{Gal}(K)$ of K over $\mathbb{Q}$. For each automorphism $\phi \in G$, write down where it sends the generators $\sqrt{2}$ and i, and then write down

$$\phi(a + b\sqrt{2} + ci + d\sqrt{2}i).$$

(b) Write out a multiplication table for G, and a minimal generating set.

(c) Write down the subfield lattice of K and the subgroup lattice of G. Each subgroup should be expressed by its generators, rather than what subgroup it is isomorphic to.

(d) For each subgroup $H \leq G$, determine the largest subfield of K that H fixes.

(e) For each subfield $F \subseteq K$, determine the largest subgroup of G that fixes F.