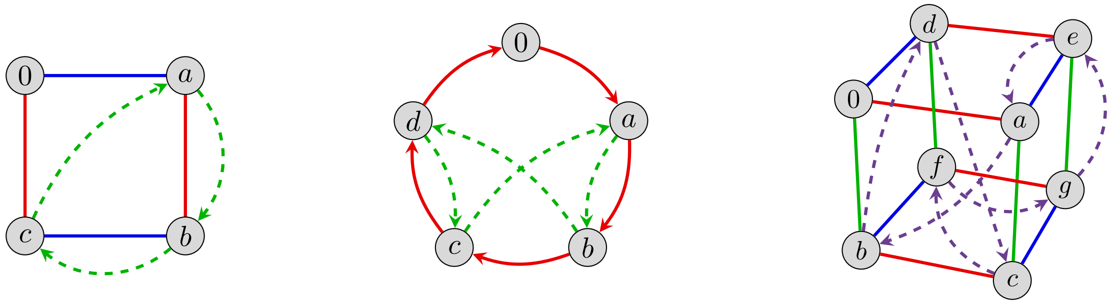
Read Chapters 10.1–10.5 of *Visual Group Theory* or Chapters 20.1–20.2 of *AATA*. Then write up solutions to the following exercises.

1. There is a unique *finite* 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 field $\mathbb{Q}(\sqrt[4]{3}, i)$ is called the *splitting field* of the polynomial $f(x) = x^4 - 3$ over $\mathbb{Q}$ because it is the smallest extension field of $\mathbb{Q}$ that contains all roots of $f(x)$.

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

   (b) Find a basis for the extension field $\mathbb{Q}(\sqrt[4]{3})$ of $\mathbb{Q}$ and compute its dimension as a $\mathbb{Q}$-vector space. 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.

   (c) Is $\mathbb{Q}(\sqrt[4]{3})$ the splitting field of some polynomial $g(x)$ over $\mathbb{Q}$? If yes, find $g(x)$. If no, explain why not.

   (d) Find a basis for $\mathbb{Q}(\sqrt[4]{3}, i) := \mathbb{Q}(\sqrt[4]{3})(i) = \mathbb{Q}(i)(\sqrt[4]{3})$ over each of the fields $\mathbb{Q}(\sqrt[4]{3})$, $\mathbb{Q}(i)$, and $\mathbb{Q}$. What is its dimension as a vector space over each of these fields?

   (e) $\mathbb{Q}(\sqrt[4]{3}, i)$ is the splitting field of what polynomial over $\mathbb{Q}(\sqrt[4]{3})$? And of what polynomial over $\mathbb{Q}(i)$?

3. 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. For each edge in this lattice, which corresponds to an extension field $E \supseteq F$, write the degree of the extension of E over F, which by definition is the dimension of E as an F-vector-space.

4. 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 $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$:

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

5. 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 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.