Chapter 4

Families of Groups

In this chapter we will explore a few families of groups, some of which we are already familiar with.

4.1 Cyclic Groups

Recall that if G is a group and $g \in G$, then the **cyclic subgroup generated by** g is given by

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

It is important to point out that $\langle g \rangle$ may be finite or infinite. In the finite case, the Cayley diagram with generator g gives us a good indication of where the word "cyclic" comes from (see Problem 4.21). If there exists $g \in G$ such that $G = \langle g \rangle$, then we say that G is a **cyclic group**.

Problem 4.1. List all of the elements in each of the following cyclic subgroups.

(a) $\langle r \rangle$, where $r \in D_3$

(b) $\langle r \rangle$, where $r \in R_4$

(c) $\langle rs \rangle$, where $rs \in D_4$

(d) $\langle r^2 \rangle$, where $r^2 \in R_6$

(e) $\langle i \rangle$, where $i \in Q_8$

(f) $\langle 6 \rangle$, where $6 \in \mathbb{Z}$ and the operation is ordinary addition

Problem 4.2. Consider the group of invertible 2×2 matrices with real number entries under the operation of matrix multiplication. This group is denoted by $\mathrm{GL}_2(\mathbb{R})$. List the elements in the cyclic subgroups generated by each of the following matrices.

(a) $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ (b) $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ (c) $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$

Problem 4.3. Determine whether each of the following groups is cyclic. If the group is cyclic, find at least one generator.

(a) S_2
(b) R_3
(c) R_4
(d) V_4
(e) R_5
(f) R_6
(g) D_3
(h) R_7
(i) R_8
(j) $\mathrm{Spin}_{1\times 2}$
(k) D_4
(l) Q_8

Problem 4.4. Determine whether each of the following groups is cyclic. If the group is cyclic, find at least one generator. If you believe that a group is not cyclic, try to sketch an argument.

(a) $(\mathbb{Z}, +)$
(b) $(\mathbb{R}, +)$
(c) $(\mathbb{R}^+, \cdot)$
(d) $(\{6^n \mid n \in \mathbb{Z}\}, \cdot)$
(e) $\mathrm{GL}_2(\mathbb{R})$ under matrix multiplication
(f) $\{(\cos(\pi/4) + i\sin(\pi/4))^n \mid n \in \mathbb{Z}\}$ under multiplication of complex numbers

Theorem 4.5. If G is a cyclic group, then G is abelian.

Problem 4.6. Provide an example of a finite group that is abelian but not cyclic.

Problem 4.7. Provide an example of an infinite group that is abelian but not cyclic.

Theorem 4.8. If G is a group and $g \in G$, then $\langle g \rangle = \langle g^{-1} \rangle$.

Theorem 4.9. If G is a cyclic group such that G has exactly one element that generates all of G, then the order of G is at most order 2.

Theorem 4.10. If G is a group such that G has no proper nontrivial subgroups, then G is cyclic.

Recall that the order of a group G, denoted $|G|$, is the number of elements in G. We define the **order** of an element g, written $|g|$, to be the order of $\langle g \rangle$. That is, $|g| = |\langle g \rangle|$. It is clear that G is cyclic with generator g if and only if $|G| = |g|$.

Problem 4.11. What is the order of the identity in any group?

Problem 4.12. Find the orders of each of the elements in each of the groups in Problem 4.3.

Problem 4.13. Consider the group $(\mathbb{Z}, +)$. What is the order of 1? Are there any elements in $\mathbb{Z}$ with finite order?

Problem 4.14. Find the order of each of the matrices in Problem 4.2.

The next result follows immediately from Theorem 4.8.

Theorem 4.15. If G is a group and $g \in G$, then $|g| = |g^{-1}|$.

The next result should look familiar and will come in handy a few times in this chapter. We'll take the result for granted and not worry about proving it.

Theorem 4.16 (Division Algorithm)**.** If n is a positive integer and m is any integer, then there exist unique integers q (called the **quotient**) and r (called the **remainder**) such that $m = nq + r$, where $0 \leq r < n$.

For the forward implication in the next theorem, if $\langle g \rangle$ is finite, then there exists distinct positive integers i and j such that $g^i = g^j$. Can you find a useful way to rewrite this equation? For the reverse implication, let $m \in \mathbb{Z}$ and use the Division Algorithm with m and n.

Theorem 4.17. Suppose G is a group and let $g \in G$. The subgroup $\langle g \rangle$ is finite if and only if there exists $n \in \mathbb{N}$ such that $g^n = e$.

Corollary 4.18. If G is a finite group, then for all $g \in G$, there exists $n \in \mathbb{N}$ such that $g^n = e$.

Note that Theorem 4.17 together with the Well-Ordering Principle guarantees the existence of a smallest positive integer n such that $g^n = e$ for every g in a finite group G. In the following theorem, the claim that the set contains n distinct elements is not immediate. You need to argue that there are no repeats in the list. Choose distinct $i, j \in \{0, 1, \ldots, n-1\}$ such that $i \neq j$ and then show that $g^i \neq g^j$. Consider a proof by contradiction and try to contradict the minimality of n.

Theorem 4.19. Suppose G is a group and let $g \in G$ such that $\langle g \rangle$ is a finite group. If n is the smallest positive integer such that $g^n = e$, then $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ and this set contains n distinct elements.

The next result provides an extremely useful interpretation of the order of an element.

Corollary 4.20. If G is a group and $g \in G$ such that $\langle g \rangle$ is a finite group, then the order of g is the smallest positive integer n such that $g^n = e$.

Problem 4.21. Suppose G is a finite cyclic group such that $G = \langle g \rangle$. Using the generating set $\{g\}$, what does the Cayley diagram for G look like?

Problem 4.22. Suppose G is a finite cyclic group of order n with generator g. If we write down the group table for G using $e, g, g^2, \ldots, g^{n-1}$ as the labels for the rows and columns, are there any interesting patterns in the table?

Problem 4.23. Notice that in the definition for $\langle g \rangle$, we allow the exponents on g to be negative. Explain why we only need to use positive exponents when $\langle g \rangle$ is a finite group.

The Division Algorithm should come in handy when proving the next theorem.

Theorem 4.24. Suppose G is a group and let $g \in G$ such that $|g| = n$. Then $g^i = g^j$ if and only if n divides $i - j$.

Corollary 4.25. Suppose G is a group and let $g \in G$ such that $|g| = n$. If $g^k = e$, then n divides k.

Recall that for $n \geq 3$, R_n is the group of rotational symmetries of a regular n-gon, where the operation is composition of actions.

Theorem 4.26. For all $n \geq 3$, R_n is cyclic.

Theorem 4.27. Suppose G is a finite cyclic group of order n. Then G is isomorphic to R_n if $n \geq 3$, S_2 if $n = 2$, and the trivial group if $n = 1$.

Most of the previous results have involved finite cyclic groups. What about infinite cyclic groups?

For the forward implication in the following theorem, try a proof by contradiction and suppose there exists integers i and j such that $g^i = g^j$.

Theorem 4.28. Suppose G is a group and let $g \in G$. The subgroup $\langle g \rangle$ is infinite if and only if each g^k is distinct for all $k \in \mathbb{Z}$.

Theorem 4.29. If G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$ (under the operation of addition).

The upshot of Theorems 4.29 and 4.27 is that up to isomorphism, we know exactly what all of the cyclic groups are.

We now turn our attention to two new groups. Recall that two integers are **relatively prime** if the only positive integer that divides both of them is 1. That is, integers n and k are relatively prime if and only if $\gcd(n, k) = 1$.

Definition 4.30. Let $n \in \mathbb{N}$ and define the following sets.

(a) $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$

(b) $U_n := \{k \in \mathbb{Z}_n \mid \gcd(n, k) = 1\}$

Example 4.31. For example, $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ while $U_{12} = \{1, 5, 7, 11\}$ since 1, 5, 7, and 11 are the only elements in $\mathbb{Z}_{12}$ that are relatively prime to 12.

For each set in Definition 4.30, the immediate goal is to determine a binary operation that will yield a group. The key is to use modular arithmetic. Let n be a positive integer. To calculate the sum (respectively, product) of two integers modulo n (we say "mod n" for short), add (respectively, multiply) the two numbers and then find the remainder after dividing the sum (respectively, product) by n. For example, $4 + 9$ is 3 mod 5 since 13 has remainder 3 when divided by 5. Similarly, $4 \cdot 9$ is 1 mod 5 since 36 has remainder 1 when divided by 5. The hope is that these two operations turn $\mathbb{Z}_n$ and U_n into groups.

We write $i \equiv j \pmod{n}$, and say "i is equivalent to j modulo n" or "i is equal to j modulo n", if i and j both have the same remainder when divided by n. It is common to abbreviate "modulo" as "mod". It is also common to write $i \equiv_n j$, or even $i = j$ if the context is perfectly clear.

It is well-known, and not too hard to prove, that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. The corresponding equivalence classes are called congruence classes. The elements of a single congruence class are the integers that all have the same remainder when divided by n. According to the Division Algorithm, there are n congruence classes modulo n, one for each of the remainders $0, 1, \ldots, n-1$. We can think of $\mathbb{Z}_n$ as the set of canonical representatives of these equivalence classes.

Theorem 4.32. Let n be a positive integer and let $i, j \in \mathbb{Z}$. Then $i \equiv j \pmod{n}$ if and only if n divides $i - j$.

The next result follows immediately from Theorems 4.32 and 4.24.

Corollary 4.33. Suppose G is a group and let $g \in G$ such that $|g| = n$. Then $g^i = g^j$ if and only if $i \equiv j \pmod{n}$.

There are two things to prove in the next theorem. First, you need to prove that $\mathbb{Z}_n$ is a group under addition mod n, and then you need to argue that the group is cyclic.

Theorem 4.34. The set $\mathbb{Z}_n$ is a cyclic group under addition mod n.

Like the previous theorem, there are two things to prove for the next theorem. First, prove that U_n is a group under multiplication mod n, and then argue that the group is abelian.

Theorem 4.35. The set U_n is an abelian group under multiplication mod n.

Problem 4.36. Consider $\mathbb{Z}_4$.

(a) Find the group table for $\mathbb{Z}_4$.

(b) Is $\mathbb{Z}_4$ cyclic? If so, list elements of $\mathbb{Z}_4$ that individually generate $\mathbb{Z}_4$. If $\mathbb{Z}_4$ is not cyclic, explain why.

(c) Is $\mathbb{Z}_4$ isomorphic to either of R_4 or V_4? Justify your answer.

(d) Draw the subgroup lattice for $\mathbb{Z}_4$.

The next two problems illustrate that U_n may or may not be cyclic.

Problem 4.37. Consider $U_{10} = \{1, 3, 7, 9\}$.

(a) Find the group table for U_{10}.

(b) Is U_{10} cyclic? If so, list elements of U_{10} that individually generate U_{10}. If U_{10} is not cyclic, explain why.

(c) Is U_{10} isomorphic to either of R_4 or V_4? Justify your answer.

(d) Is U_{10} isomorphic to $\mathbb{Z}_4$? Justify your answer.

(e) Draw the subgroup lattice for U_{10}.

Problem 4.38. Consider $U_{12} = \{1, 5, 7, 11\}$.

(a) Find the group table for U_{12}.

(b) Is U_{12} cyclic? If so, list elements of U_{12} that individually generate U_{12}. If U_{12} is not cyclic, explain why.

(c) Is U_{12} isomorphic to either of R_4 or V_4? Justify your answer.

(d) Draw the subgroup lattice for U_{12}.

The upshot of the next theorem is that for $n \geq 3$, $\mathbb{Z}_n$ is just the set of exponents in the set $R_n = \{e, r, r^2, \ldots, r^{n-1}\}$ (where $e = r^0$).

Theorem 4.39. For $n \geq 3$, $\mathbb{Z}_n \cong R_n$. Moreover, $\mathbb{Z}_2 \cong S_2$ and $\mathbb{Z}_1$ is isomorphic to the trivial group.

The next result can be thought of as a repackaging of Theorems 4.27 and 4.29.

Theorem 4.40. Let G be a cyclic group. If the order of G is infinite, then G is isomorphic to $\mathbb{Z}$. If G has finite order n, then G is isomorphic to $\mathbb{Z}_n$.

Now that we have a complete description of the cyclic groups, let's focus our attention on subgroups of cyclic groups.

Theorem 4.41. Suppose G is a cyclic group. If $H \leq G$, then H is also cyclic.

It turns out that for proper subgroups, the converse of Theorem 4.41 is not true.

Problem 4.42. Provide an example of a group G such that G is not cyclic, but all proper subgroups of G are cyclic.

The next result officially settles Problem 3.17(d) and also provides a complete description of the subgroups of infinite cyclic groups up to isomorphism.

Corollary 4.43. The subgroups of $\mathbb{Z}$ are precisely the groups $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

Let's further explore finite cyclic groups. By Corollary 4.20, the order of g^m is the smallest positive exponent k such that $(g^m)^k = e$. To prove the next theorem, first verify that $k = \frac{n}{\gcd(n,m)}$ has the desired property and then verify that it is the smallest such exponent.

Theorem 4.44. If G is a finite cyclic group with generator g such that $|G| = n$, then for all $m \in \mathbb{Z}$, $|g^m| = \dfrac{n}{\gcd(n, m)}$.

Here is an extensive hint for proving the next theorem. Use Theorem 4.44 for the forward implication. For the reverse implication, first prove that for all $m \in \mathbb{Z}$, $\langle g^m \rangle = \langle g^{\gcd(m,n)} \rangle$ by proving two set containments. To show $\langle g^m \rangle \subseteq \langle g^{\gcd(m,n)} \rangle$, use the fact that there exists an integer q such that $m = q \cdot \gcd(m,n)$. For the reverse containment, you may freely use a fact known as Bezout's Lemma, which states that $\gcd(m,n) = nx + my$ for some integers x and y.

Theorem 4.45. If G is a finite cyclic group with generator g such that $|G| = n$, then $\langle g^m \rangle = \langle g^k \rangle$ if and only if $\gcd(m,n) = \gcd(k,n)$.

Problem 4.46. Suppose G is a cyclic group of order 12 with generator g.

(a) Find the orders of each of the following elements: g^2, g^7, g^8.

(b) Which elements of G individually generate G?

Corollary 4.47. Suppose G is a finite cyclic group with generator g such that $|G| = n$. Then $\langle g \rangle = \langle g^k \rangle$ if and only if n and k are relatively prime. That is, g^k generates G if and only if n and k are relatively prime.

Problem 4.48. Theorem 4.44, Theorem 4.45, and Corollary 4.47 are written using multiplicative notation. Rewrite both of these results using additive notation.

Problem 4.49. Consider $\mathbb{Z}_{18}$.

(a) Find all of the elements of $\mathbb{Z}_{18}$ that individually generate all of $\mathbb{Z}_{18}$.

(b) Draw the subgroup lattice for $\mathbb{Z}_{18}$. For each subgroup, list the elements of the corresponding set. Moreover, circle the elements in each subgroup that individually generate that subgroup. For example, $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$. In this case, we should circle 2, 4, 8, 10, 14, and 16 since each of these elements individually generate $\langle 2 \rangle$ and none of the remaining elements do. I'll leave it to you to figure out why this is true.

Problem 4.50. Repeat the above exercise, but this time use $\mathbb{Z}_{12}$ instead of $\mathbb{Z}_{18}$.

Corollary 4.51. If G is a finite cyclic group such that $|G| = p$, where p is prime, then G has no proper nontrivial subgroups.

Problem 4.52. If there is exactly one group up to isomorphism of order n, then to what group are all the groups of order n isomorphic?

Problem 4.53. Suppose G is a group and $x, y \in G$ such that $|x| = m$ and $|y| = n$. Is it true that $|xy| = mn$? If this is true, provide a proof. If this is not true, then provide a counterexample.

The punchline of the next two theorems is Theorem 4.56. To prove the next theorem, first verify that $(xy)^{mn} = e$ and then suppose $|xy| = k$. What do you immediately know about the relationship between k and mn? Next, consider $(xy)^{kn}$. Argue that m divides kn and then argue that m divides k. Similarly, n divides k. Ultimately, conclude that $mn = k$.

Theorem 4.54. Suppose G is a finite abelian group and let $x, y \in G$ such that $|x| = m$ and $|y| = n$. If $\gcd(m, n) = 1$, then $|xy| = mn$.

Here is a hint for proving the next theorem. Suppose $g \in G$ such that $|g| = n$. Let h be an arbitrary element in G such that $|h| = m$. You need to show that m divides n. For sake of a contradiction, assume otherwise. Then there exists a prime p whose multiplicity as a factor of m exceeds that of n. Let p^a be the highest power of p in m and p^b be the highest power of p in n, so $a > b$. Consider the elements g^{p^a} and h^{m/p^b}.

Theorem 4.55. Suppose G is a finite abelian group. If n is the maximal order among all elements in G, then the order of every element in G divides n.

Recall that every cyclic group is abelian (see Theorem 4.5). However, we know that not every abelian group is cyclic (see Problem 4.6). The next theorem tells us that abelian groups with some additional properties are cyclic.

Here is one method of attack for proving the next theorem. Let n be the maximal order among the elements of G and let $g \in G$ be an element with order n. Prove that $G = \langle g \rangle$.

Theorem 4.56. If G is a finite abelian group with at most one subgroup of any order, then G is cyclic.

Problem 4.57. Is the converse of Theorem 4.56 true for finite groups? That is, if G is a finite cyclic group, does that imply that G contains at most one subgroup of each order? If the answer is yes, then prove it. Otherwise, provide a counterexample.

We conclude this section with a couple interesting counting problems involving the number of generators of certain cyclic groups.

Problem 4.58. Let p and q be distinct primes. Find the number of generators of $\mathbb{Z}_{pq}$.

Problem 4.59. Let p be a prime. Find the number of generators of $\mathbb{Z}_{p^r}$, where r is an integer greater than or equal to 1.

4.2 Dihedral Groups

We can think of finite cyclic groups as groups that describe rotational symmetry. In particular, R_n is the group of rotational symmetries of a regular n-gon. Dihedral groups are those groups that describe both rotational and reflectional symmetry of regular n-gons.

Definition 4.60. For $n \geq 3$, the **dihedral group** D_n is defined to be the group consisting of the symmetry actions of a regular n-gon, where the operation is composition of actions.

For example, as we've seen, D_3 and D_4 are the symmetry groups of equilateral triangles and squares, respectively. The symmetry group of a regular pentagon is denoted by D_5. It is a well-known fact from geometry that the composition of two reflections in the plane is a rotation by twice the angle between the reflecting lines.

Theorem 4.61. The group D_n is a non-abelian group of order $2n$.

Theorem 4.62. Fix $n \geq 3$ and consider D_n. Let r be rotation clockwise by $360°/n$ and let s and s' be any two adjacent reflections of a regular n-gon. Then

(a) $D_n = \langle r, s \rangle = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, sr^2, \ldots, sr^{n-1}}_{\text{reflections}}\}$ and

(b) $D_n = \langle s, s' \rangle =$ all possible products of s and s'.

The next result is an obvious corollary of Theorem 4.62.

Corollary 4.63. For $n \geq 3$, $R_n \leq D_n$.

The following theorem generalizes many of the relations we have witnessed in the Cayley diagrams for the dihedral groups D_3 and D_4.

Theorem 4.64. Fix $n \geq 3$ and consider D_n. Let r be rotation clockwise by $360°/n$ and let s and s' be any two adjacent reflections of a regular n-gon. Then the following relations hold.

(a) $r^n = s^2 = (s')^2 = e$,

(b) $r^{-k} = r^{n-k}$ (special case: $r^{-1} = r^{n-1}$),

(c) $sr^k = r^{n-k}s$ (special case: $sr = r^{n-1}s$),

(d) $\underbrace{ss's\cdots}_{n \text{ factors}} = \underbrace{s'ss'\cdots}_{n \text{ factors}}$.

Problem 4.65. From Theorem 4.62, we know

$$D_n = \langle r, s \rangle = \{\underbrace{e, r, r^2, \ldots, r^{n-1}}_{\text{rotations}}, \underbrace{s, sr, sr^2, \ldots, sr^{n-1}}_{\text{reflections}}\}.$$

If you were to create the group table for D_n so that the rows and columns of the table were labeled by $e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}$ (in exactly that order), do any patterns arise? Where are the rotations? Where are the reflections?

Problem 4.66. What does the Cayley diagram for D_n look like if we use $\{r, s\}$ as the generating set? What if we use $\{s, s'\}$ as the generating set?

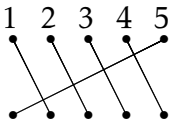
4.3 Symmetric Groups

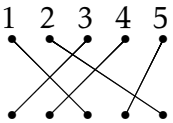
Recall the groups S_2 and S_3 from Problems 2.63 and 2.23. These groups act on two and three coins, respectively, that are in a row by rearranging their positions (but not flipping them over). These groups are examples of symmetric groups. In general, the **symmetric group** on n objects is the set of permutations that rearranges the n objects. The group operation is composition of permutations. Let's be a little more formal.

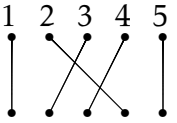
Definition 4.67. A **permutation of a set** A is a function $\sigma : A \to A$ that is both one-to-one and onto.

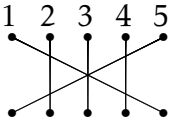
You should take a moment to convince yourself that the formal definition of a permutation agrees with the notion of rearranging the set of objects. The do-nothing action is the identity permutation, i.e., $\sigma(a) = a$ for all $a \in A$. There are many ways to represent a permutation. One visual way is using **permutation diagrams**, which we will introduce via examples.

Consider the following diagrams:

$\alpha =$ 

$\sigma =$ 

$\beta =$ 

$\gamma =$ 

Each of these diagrams represents a permutation on five objects. I've given the permutations the names α, β, σ, and γ. The intention is to read the diagrams from the top down. The numbers labeling the nodes along the top are identifying position. Following an edge from the top row of nodes to the bottom row of nodes tells us what position an object moves to. It is important to remember that the numbers are referring to the position of an object, not the object itself. For example, β is the permutation that sends the object in the second position to the fourth position, the object in the third position to the second position, and the object in the fourth position to the third position. Moreover, the permutation β doesn't do anything to the objects in positions 1 and 5.

Problem 4.68. Describe in words what the permutations σ and γ do.

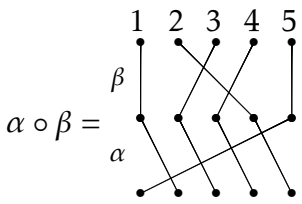
Problem 4.69. Draw the permutation diagram for the do-nothing permutation on 5 objects. This is called the **identity permutation**. What does the identity permutation diagram look like in general for arbitrary n?

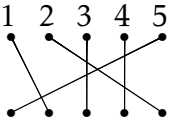
Definition 4.70. The set of all permutations on n objects is denoted by S_n.

Problem 4.71. Draw all the permutation diagrams for the permutations in S_3.

Problem 4.72. How many distinct permutations are there in S_4? How about S_n for any $n \in \mathbb{N}$?

If S_n is going to be a group, we need to know how to compose permutations. This is easy to do using the permutation diagrams. Consider the permutations α and β from earlier. We can represent the composition $\alpha \circ \beta$ via

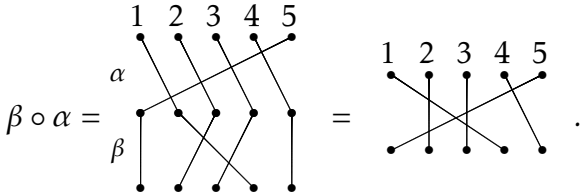
$\alpha \circ \beta =$ 

$=$ 

.

As you can see by looking at the figure, to compose two permutations, you stack the one that goes first in the composition (e.g., β in the example above) on top of the other and just follow the edges from the top through the middle to the bottom. If you think about how function composition works, this is very natural. The resulting permutation is determined by where we begin and where we end in the composition.

We already know that the order of composition matters for functions, and so it should matter for the composition of permutations. To make this crystal clear, let's compose α and β in the opposite order. We see that



The moral of the story is that composition of permutations does not necessarily commute.

Problem 4.73. Consider α, β, σ, and γ from earlier. Can you find a pair of permutations that do commute? Can you identify any features about your diagrams that indicate why they commuted?

Problem 4.74. Fix $n \in \mathbb{N}$. Convince yourself that any $\rho \in S_n$ composed with the identity permutation (in either order) equals ρ.

If S_n is going to be a group, we need to know what the inverse of a permutation is.

Problem 4.75. Given a permutation $\rho \in S_n$, describe a method for constructing ρ^{-1}. Briefly justify that $\rho \circ \rho^{-1}$ will yield the identity permutation.

At this point, we have all the ingredients we need to prove that S_n forms a group under composition of permutations.

Theorem 4.76. The set of permutations on n objects forms a group under the operation of composition. That is, $(S_n, \circ)$ is a group. Moreover, $|S_n| = n!$.

Note that it is standard convention to omit the composition symbol when writing down compositions in S_n. For example, we will simply write $\alpha\beta$ to denote $\alpha \circ \beta$.

Permutation diagrams are fun to play with, but we need a more efficient way of encoding information. There are several compact and efficient notations for describing permutations in S_n. For our purposes, it will be handy for us to describe permutations using **cycle notation**. The **cycle** $(a_1, a_2, \ldots, a_m)$ is the permutation that sends a_i to a_{i+1} for $1 \leq i \leq m-1$ and sends a_m to a_1. In general, for each $\sigma \in S_n$, the numbers 1 through n will be rearranged and grouped into k cycles of the form

$$(a_1, a_2, \ldots, a_{m_1})(a_{m_1+1}, a_{m_1+2}, \ldots, a_{m_2}) \cdots (a_{m_{k-1}+1}, a_{m_{k-1}+2}, \ldots, a_{m_k})$$

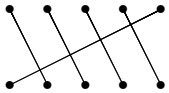
from which the action of σ on any number from 1 to n can easily be determined. In particular, for any $i \in \{1, 2, \ldots, n\}$, locate i in the expression above. Then $\sigma(i)$ is the next number in the corresponding cycle that is cyclicly to the right (i.e., if i is not at the right

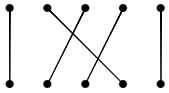
end of a cycle, $\sigma(i)$ is the next number to the right, while if i is at the right end of a cycle, $\sigma(i)$ is the number at the left end of the same cycle. The product of all the cycles is called the **cycle decomposition** of σ.

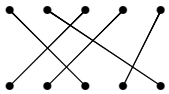
Notice that we can start writing a cycle with any of the numbers appearing in the cycle. What matters is that each number in the cycle is followed by the appropriate number. For example, $(1,3,2) = (3,2,1) = (2,1,3)$. The **length** of a cycle is the number of entries appearing in it. If a cycle has length m, then it is called an m-**cycle**. Two cycles are said to be **disjoint** if they have no entries in common.

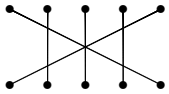
Example 4.77. Consider $\sigma = (1,12,8,10,4)(2,13)(3)(5,11,7)(6,9)$ in S_{13}. This cycle decomposition for σ consists of five pairwise disjoint cycles: a 5-cycle, a 2-cycle, a 1-cycle, a 3-cycle, and another 2-cycle. For convenience, it is common to omit any 1-cycles in the decomposition. So, we may also write $\sigma = (1,12,8,10,4)(2,13)(5,11,7)(6,9)$, keeping in mind that the absence of a number means that the permutation maps that number to itself.

Example 4.78. Consider α, β, σ, and γ in S_5 that we had previously drawn permutation diagrams for. Below I have indicated what each permutation is equal to using cycle notation.

$\alpha =$  $= (1,2,3,4,5)$

$\beta =$  $= (2,4,3)$

$\sigma =$  $= (1,3)(2,5,4)$

$\gamma =$  $= (1,5)$

Example 4.79. The cycle decomposition of the identity permutation in S_n is $(1)(2)\cdots(n)$. It is common to simply write this as (1), again keeping in mind that the the absence of a number means that the permutation maps that number to itself. One disadvantage to this approach is that we lose information about what n is.

Problem 4.80. Suppose $\sigma \in S_9$ is defined by

$$\sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 1, \sigma(4) = 9, \sigma(5) = 8, \sigma(6) = 2, \sigma(7) = 5, \sigma(8) = 7, \sigma(9) = 6.$$

Find the cycle decomposition of σ. What are the lengths of the corresponding cycles?

Problem 4.81. Write down all 6 elements in S_3 using cycle notation.

Problem 4.82. Write down all 24 elements in S_4 using cycle notation.

Suppose $\sigma \in S_n$. Since σ is a bijection, it is clear that it is possible to write σ as a product of disjoint cycles such that each $i \in \{1, 2, \ldots, n\}$ appears exactly once.

Let's see if we can figure out how to multiply elements of S_n using cycle notation. Consider the permutations $\alpha = (1, 3, 2)$ and $\beta = (3, 4)$ in S_4. To compute the composition $\alpha\beta = (1, 3, 2)(3, 4)$, let's explore what happens in each position. Since we are doing function composition, we should work our way from right to left. Since 1 does not appear in the cycle notation for β, we know that $\beta(1) = 1$ (i.e., β maps 1 to 1). Now, we see what $\alpha(1) = 3$. Thus, the composition $\alpha\beta$ maps 1 to 3 (since $\alpha\beta(1) = \alpha(\beta(1)) = \alpha(1) = 3$). Next, we should return to β and see what happens to 3—which is where we ended a moment ago. We see that β maps 3 to 4 and then α maps 4 to 4 (since 4 does not appear in the cycle notation for α). So, $\alpha\beta(3) = 4$. Continuing this way, we see that β maps 4 to 3 and α maps 3 to 2, and so $\alpha\beta$ maps 4 to 2. Lastly, since $\beta(2) = 2$ and $\alpha(2) = 1$, we have $\alpha\beta(2) = 1$. Putting this altogether, we see that $\alpha\beta = (1, 3, 4, 2)$. Now, you should try a few. Things get a little trickier if the composition of two permutations results in a permutation consisting of more than a single cycle.

Problem 4.83. Consider α, β, σ, and γ for which we drew the permutation diagrams. Using cycle notation, compute each of the following.

(a) $\alpha\gamma$

(b) $\gamma\alpha$

(c) $\sigma\alpha$

(d) $\alpha\sigma$

(e) β^2

(f) β^3

(g) β^4

(h) σ^3

(i) σ^6

Problem 4.84. Write down the group table for S_3 using cycle notation.

In Problem 4.82, one of the permutations you should have written down is $(1, 2)(3, 4)$. This is a product of two disjoint 2-cycles. It is worth pointing out that each cycle is a permutation in its own right. That is, $(1, 2)$ and $(3, 4)$ are each permutations. It just so happens that their composition does not "simplify" any further. Moreover, these two disjoint 2-cycles commute since $(1, 2)(3, 4) = (3, 4)(1, 2)$. In fact, this phenomenon is always true.

Theorem 4.85. Suppose α and β are two disjoint cycles. Then $\alpha\beta = \beta\alpha$. That is, products of disjoint cycles commute.

Problem 4.86. Compute the orders of all the elements in S_3. See Problem 4.81.

Problem 4.87. Compute the orders of any twelve of the elements in S_4. See Problem 4.82.

Computing the order of a permutation is fairly easy using cycle notation once we figure out how to do it for a single cycle. In fact, you've probably already guessed at the following theorem.

Theorem 4.88. If $\alpha \in S_n$ such that α consists of a single k-cycle, then $|\alpha| = k$.

Recall that $\text{lcm}(k_1, \ldots, k_m)$ is the **least common multiple** of $\{k_1, \ldots, k_m\}$.

Theorem 4.89. Suppose $\alpha \in S_n$ such that α consists of m disjoint cycles of lengths $k_1, \ldots, k_m$. Then $|\alpha| = \text{lcm}(k_1, \ldots, k_m)$.

Problem 4.90. Is the previous theorem true if we do not require the cycles to be disjoint? Justify your answer.

Problem 4.91. What is the order of $(1,4,7)(2,5)(3,6,8,9)$?

Problem 4.92. Draw the subgroup lattice for S_3.

Problem 4.93. Now, using $(1,2)$ and $(1,2,3)$ as generators, draw the Cayley diagram for S_3. Look familiar?

Problem 4.94. Consider S_3. It turns out that $S_3 = \langle (1,2), (1,3), (2,3) \rangle$.

(a) Using $(1,2)$, $(1,3)$, and $(2,3)$ as generators, draw the Cayley diagram for S_3.

(b) Is $\{(1,2), (1,3), (2,3)\}$ a minimal generating set for S_3? If so, explain why. If not, find a subset of $\{(1,2), (1,3), (2,3)\}$ that is a minimal generating set.

Problem 4.95. Recall that there are $4! = 24$ permutations in S_4.

(a) Pick any 12 permutations from S_4 and verify that you can write them as words in the 2-cycles $(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)$. In most circumstances, your words will not consist of products of disjoint 2-cycles. For example, the permutation $(1,2,3)$ can be decomposed into $(1,2)(2,3)$, which is a word consisting of two 2-cycles that happen to not be disjoint.

(b) Using your same 12 permutations, verify that you can write them as words only in the 2-cycles $(1,2), (2,3), (3,4)$.

By the way, it might take some trial and error to come up with a way to do this. Moreover, there is more than one way to do it.

As the previous exercises hinted at, the 2-cycles play a special role in the symmetric groups. In fact, they have a special name. A **transposition** is a single cycle of length 2. In the special case that the transposition is of the form $(i, i+1)$, we call it an **adjacent transposition**. For example, $(3,7)$ is a (non-adjacent) transposition while $(6,7)$ is an adjacent transposition.

It turns out that the set of transpositions in S_n is a generating set for S_n. In fact, the adjacent transpositions form an even smaller generating set for S_n. To get some intuition, let's play with a few examples.

Problem 4.96. Try to write each of the following permutations as a product of transpositions. You do not necessarily need to use adjacent transpositions.

(a) $(3,1,5)$

(b) $(2,4,6,8)$

(c) $(3,1,5)(2,4,6,8)$

(d) $(1,6)(2,5,3)$

The products you found in the previous exercise are called **transposition representations** of the given permutation.

Problem 4.97. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). Find a way to write this permutation as a product of 2-cycles.

Problem 4.98. Consider the arbitrary 2-cycle (a, b) from S_n. Find a way to write this permutation as a product of adjacent 2-cycles.

The previous two problems imply the following theorem.

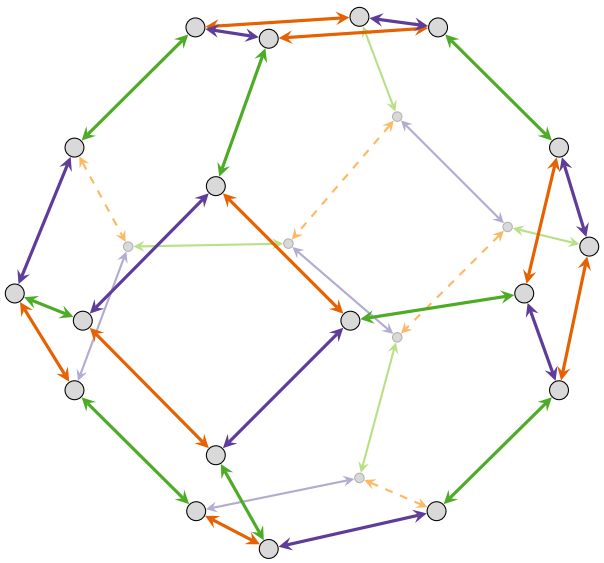
Theorem 4.99. Consider S_n.

(a) Every permutation in S_n can be written as a product of transpositions.

(b) Every permutation in S_n can be written as a product of adjacent transpositions.

Corollary 4.100. The set of transpositions (respectively, the set of adjacent transpositions) from S_n forms a generating set for S_n.

Problem 4.101. The following diagram is an unlabeled version of the Cayley diagram for S_4 using the adjacent transpositions $(1,2)$, $(2,3)$, and $(3,4)$ as generators. Pick a vertex to correspond to the identity, make a suitable choice for which arrows correspond to which generators, and then label the remaining vertices with permutations in S_4. The graph given below is drawn on the a three-dimensional solid called the **permutahedron** (which is a **truncated octahedron**).

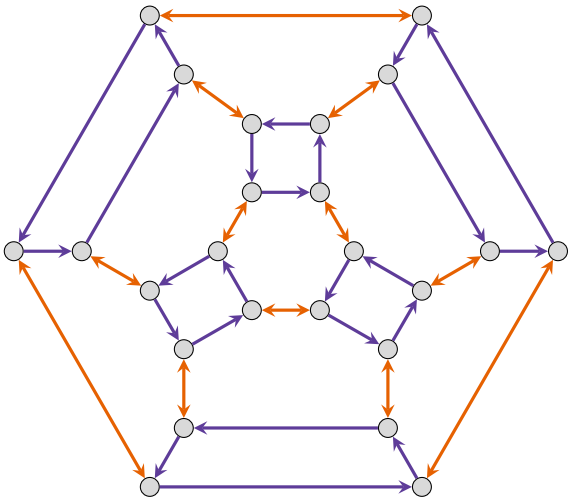


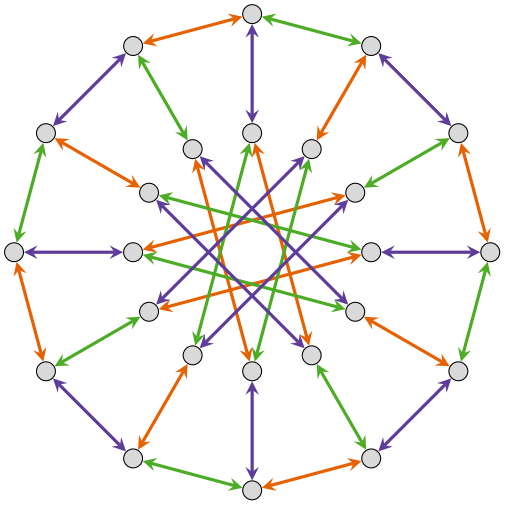
It is important to point out that the transposition representation of a permutation is not unique. That is, there are many words in the transpositions that will equal the same permutation. This is exhibited in the previous problem where there are multiple paths from the vertex corresponding to the identity to another vertex in the Cayley diagram for S_4 using the adjacent transpositions as the generators. However, as we shall see in the next section, given two transposition representations for the same permutation, the number of transpositions will have the same parity (i.e., even versus odd).

Problem 4.102. It turns out that

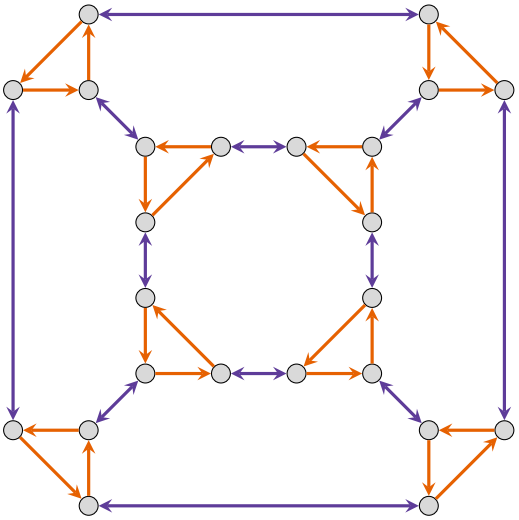
$$S_4 = \langle (1,2),(1,3),(1,4) \rangle = \langle (1,2,3,4),(1,2) \rangle.$$

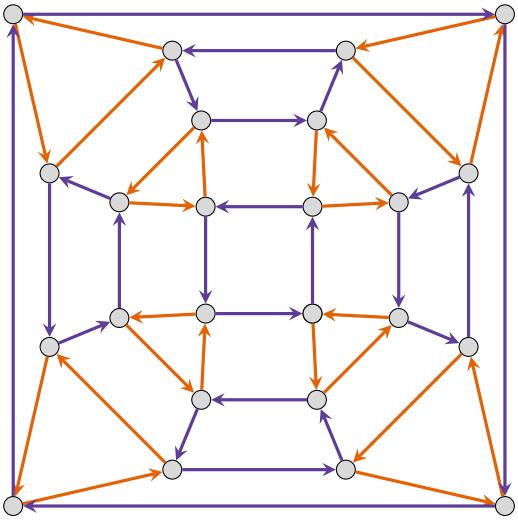
Determine which of the generating sets listed above yield each of the Cayley diagrams given below. Label the vertices in each diagram with permutations (written in cycle notation as a product of disjoint cycles) of S_4. The graph on the right is sometimes called the **Nauru graph**.





Problem 4.103. Two Cayley diagrams for the symmetric group S_4 are given below.





Determine what generating sets will yield these Cayley diagrams. Then label the nodes with permutations in cycle notation, written as a product of disjoint cycles.

Here is an interesting fact that I will let you ponder. The group of rigid motion symmetries for a cube is isomorphic to S_4. Is there a Cayley diagram in one of the last two problems that helps you visualize this fact?

4.4 Permutation Groups and Cayley's Theorem

It turns out that the subgroups of symmetric groups play an important role in group theory.

Definition 4.104. Every subgroup of a symmetric group is called a **permutation group**.

The proof of the following theorem isn't too bad, but we'll take it for granted. After tinkering with a few examples, you should have enough intuition to see why the theorem is true and how a possible proof might go.

Theorem 4.105 (Cayley's Theorem)**.** Every finite group is isomorphic to some permutation group. In particular, if G is a group of order n, then G is isomorphic to a subgroup of S_n.

Cayley's Theorem guarantees that every finite group is isomorphic to a permutation group and it turns out that there is a rather simple algorithm for constructing the corresponding permutation group. I'll briefly explain an example and then let you try a couple.

Consider the Klein four-group $V_4 = \{e, v, h, vh\}$. Recall that V_4 has the following group table.

$*$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

If we number the elements e, v, h, and vh as $1, 2, 3$, and 4, respectively, then we obtain the following table.

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Comparing each of the four columns to the leftmost column, we can obtain the corresponding permutations. In particular, we obtain

$$\begin{aligned} e &\leftrightarrow (1) \\ v &\leftrightarrow (1,2)(3,4) \\ h &\leftrightarrow (1,3)(2,4) \\ vh &\leftrightarrow (1,4)(2,3). \end{aligned}$$

Do you see where these permutations came from? The claim is that the set of permutations $\{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ is isomorphic to V_4. In this particular case, it's fairly clear that this is true. However, it takes some work to prove that this process will always result in an isomorphic permutation group. In fact, verifying the algorithm is essentially the proof of Cayley's Theorem.

Since there are potentially many ways to rearrange the rows and columns of a given table, it should be clear that there are potentially many isomorphisms that could result from the algorithm described above.

Here's another way to obtain a permutation group that is isomorphic to a given group. Let's consider V_4 again. Recall that V_4 is a subset of D_4, which is the symmetry group for a square. Alternatively, V_4 is the symmetry group for a non-square rectangle. Label the corners of the rectangle 1, 2, 3, and 4 by starting in the upper left corner and continuing clockwise. Recall that v is the action that reflects the rectangle over the vertical midline. The result of this action is that the corners labeled by 1 and 2 switch places and the corners labeled by 3 and 4 switch places. Thus, v corresponds to the permutation $(1,2)(3,4)$. Similarly, h swaps the corners labeled by 1 and 4 and the corners labeled by 2 and 3, and so h corresponds to the permutation $(1,4)(2,3)$. Notice that this is not the same answer we got earlier and that's okay as there may be many permutation representations for a given group. Lastly, vh rotates the rectangle 180° which sends ends up swapping corners labeled 1 and 3 and swapping corners labeled by 2 and 4. Therefore, vh corresponds to the permutation $(1,3)(2,4)$.

Problem 4.106. Consider D_4.

(a) Using the method outlined above, find a subgroup of S_8 that is isomorphic to D_4.

(b) Label the corners of a square 1–4. Find a subgroup of S_4 that is isomorphic to D_4 by considering the natural action of D_4 on the labels on the corners of the square.

Problem 4.107. Consider $\mathbb{Z}_6$.

(a) Using the method outlined earlier, find a subgroup of S_6 that is isomorphic to $\mathbb{Z}_6$.

(b) Label the corners of a regular hexagon 1–6. Find a subgroup of S_6 that is isomorphic to $\mathbb{Z}_6$ by considering the natural action of $\mathbb{Z}_6$ on the labels on the corners of the hexagon.

4.5 Alternating Groups

In this section, we describe a special class of permutation groups. To get started, let's play with a few exercises.

Problem 4.108. Write down every permutation in S_3 as a product of 2-cycles in the most efficient way you can find (i.e., use the fewest possible transpositions). Now, write every permutation in S_3 as a product of adjacent 2-cycles, but don't worry about whether your decompositions are efficient. Any observations about the number of transpositions you used in each case? Think about even versus odd.

Theorem 4.109. If $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a collection of 2-cycles in S_n such that $\alpha_1\alpha_2\cdots\alpha_k = (1)$, then k must be even.

Proof. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a collection of 2-cycles in S_n such that $\alpha_1\alpha_2\cdots\alpha_k = (1)$. We need to show that k is even. We proceed by strong induction. First, it is clear that the statement is not true when $k = 1$, but is true when $k = 2$.

Now, assume that $k > 2$ and if $j \leq k-1$ and we have a product of j 2-cycles that equals the identity, then j is even. Consider $\alpha_1\alpha_2$. The only possibilities are:

(i) $\alpha_1\alpha_2 = (a,b)(a,b)$,

(ii) $\alpha_1\alpha_2 = (a,b)(a,c)$,

(iii) $\alpha_1\alpha_2 = (a,b)(c,d)$,

(iv) $\alpha_1\alpha_2 = (a,b)(b,c)$.

If case (i) happens, then

$$(1) = \alpha_1\alpha_2\cdots\alpha_k = \alpha_3\alpha_4\cdots\alpha_k.$$

Since the expression on the right consists of $k-2$ factors, $k-2$ must be even by induction, which implies that k is even. Now, suppose we are in one of cases (ii), (iii), or (iv). Observe that:

(ii) $(a,b)(a,c) = (b,c)(a,b)$,

(iii) $(a,b)(c,d) = (c,d)(a,b)$,

(iv) $(a,b)(b,c) = (b,c)(a,c)$.

In each case, we were able to move a from the original left 2-cycle to a new right 2-cycle. That is, we were able to rewrite $\alpha_1\alpha_2$ so that a does not appear in the left 2-cycle. Systematically repeat this process for the pairs $\alpha_2\alpha_3$, $\alpha_3\alpha_4, \ldots, \alpha_{k-1}\alpha_k$. If we ever encounter case (i) along the way, then we are done by induction. Otherwise, we are able to rewrite $\alpha_1\alpha_2\cdots\alpha_k$ so that a only appears in the rightmost 2-cycle. But this implies that $\alpha_1\alpha_2\cdots\alpha_k$ does not fix a, which contradicts $\alpha_1\alpha_2\cdots\alpha_k = (1)$. This implies that at some point we must encounter case (i), and hence k is even by induction. □

Theorem 4.110. If $\sigma \in S_n$, then every transposition representation of σ has the same parity.

The previous theorem tells us that the following definition is well-defined.

Definition 4.111. A permutation is **even** (respectively, **odd**) if one of its transposition representations consists of an even (respectively, odd) number of transpositions.

Problem 4.112. Classify all of the permutations in S_3 as even or odd.

Problem 4.113. Classify all of the permutations in S_4 as even or odd.

Problem 4.114. Identify the even permutations in the Cayley diagrams for S_4 given in Problems 4.102 and 4.103. Notice any nice patterns?

Problem 4.115. Determine whether $(1,4,2,3,5)$ is even or odd. How about $(1,4,2,3,5)(7,9)$?

Problem 4.116. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). When will this cycle be odd versus even? Briefly justify your answer.

Problem 4.117. Conjecture a statement about when a permutation will be even versus odd. Briefly justify your answer.

And finally, we are ready to introduce the alternating groups.

Definition 4.118. The set of all even permutations in S_n is denoted by A_n and is called the **alternating group**.

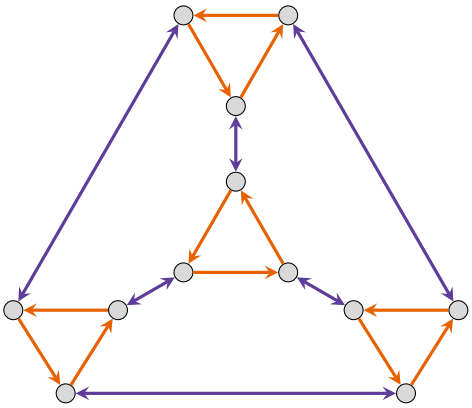
Since we referred to A_n as a group, it darn well better be a group! To show that A_n is a group, argue that A_n is a subgroup of S_n using the Two-Step Subgroup Test (see Theorem 3.6). As expected, for $n > 1$, the order of A_n is exactly half the order of S_n. To show that $|A_n| = n!/2$ for $n > 1$, prove that the number of even permutations in S_n is the same as the number of odd permutations in S_n. Here is one way to accomplish this. Define $f : A_n \to S_n \setminus A_n$ via $f(\sigma) = (1,2)\sigma$. Note that $S_n \setminus A_n$ is the set of odd permutations in S_n. Show that f is a bijection.

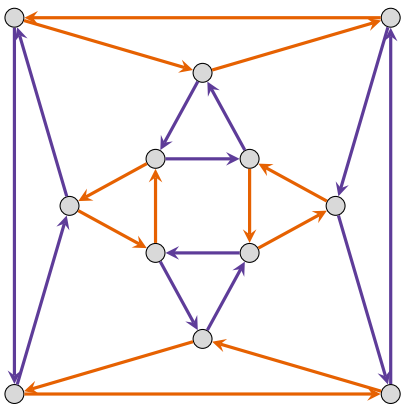
Theorem 4.119. The set A_n forms a group under composition of permutations and has order $n!/2$ when $n > 1$.

Problem 4.120. Find A_3. What group is A_3 isomorphic to?

Problem 4.121. Find A_4 and then draw its subgroup lattice. Is A_4 abelian?

Problem 4.122. Two Cayley diagrams for A_4 are shown below.





Determine what generating sets will yield these Cayley diagrams. Then label the nodes with permutations in cycle notation, written as a product of disjoint cycles.

Problem 4.123. What is the order of A_5? Is A_5 abelian?

Problem 4.124. What orders of elements occur in S_6 and A_6? What about S_7 and A_7?

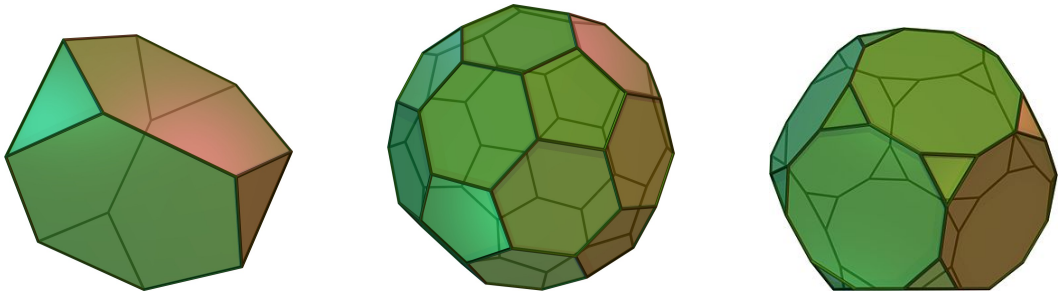
Problem 4.125. Does A_8 contain an element of order 15? If so, find one. If not, explain why no such element exists.

Remark 4.126. Below are a few interesting facts about A_4 and A_5, which we will state without proof.

(a) The group of rigid motion symmetries for a regular tetrahedron is isomorphic to A_4.

(b) You can arrange the Cayley diagram for A_4 with generators $(1,2)(3,4)$ and $(2,3,4)$ (see the left diagram in Problem 4.122) on a truncated tetrahedron, which is depicted in Figure 4.1(a).

(c) You can arrange the Cayley diagram for A_5 with generators $(1,2)(3,4)$ and $(1,2,3,4,5)$ on a truncated icosahedron, which is given in Figure 4.1(b). You can also arrange the Cayley diagram for A_5 with generators $(1,2,3)$ and $(1,5)(2,4)$ on a truncated dodecahedron seen in Figure 4.1(c).



(a) (b) (c)

Figure 4.1. Truncated tetrahedron, truncated icosahedron, and truncated dodecahedron. [Image source: Wikipedia]