Chapter 6

Families of Groups

In this chapter we will explore a few families of groups.

6.1 Cyclic Groups

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

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

According to Theorem 5.66, $\langle a \rangle$ is the smallest subgroup containing a. We call $\langle a \rangle$ the **cyclic group generated by** a. It is important to point out that $\langle a \rangle$ may be finite or infinite. In the finite case, the Cayley diagram with generator a gives us a good indication where the word cyclic comes from.

Exercise 6.1. Suppose $\langle a \rangle$ is a finite group. Since $\langle a \rangle$ is a group in its own right, we can draw a Cayley diagram for this group. Using the generator a, what does the Cayley diagram for $\langle a \rangle$ look like? To rigorously prove that your intuitive thinking is correct, we'll need some results that appear later in this section.

Definition 6.2. Suppose $(G,*)$ is a group and let $a \in G$. We define the **order** of a, written $|a|$, to be the order of $\langle a \rangle$. That is,

$$|a| = |\langle a \rangle|.$$

Exercise 6.3. What is the order of the identity in any group?

Exercise 6.4. Find the orders of each of the elements in each of the following groups.

(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) D_4

(k) Q_8

Exercise 6.5. Consider the group $(\mathbb{Z},+)$. What is the order of 1? Are there any elements in $\mathbb{Z}$ with finite order?

Exercise 6.6. Consider the group of invertible 2×2 matrices with real number entries under the operation of matrix multiplication. This group is denoted $\mathrm{GL}_2(\mathbb{R})$. Find the order of each of the following elements in this group.

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

Theorem 6.7. Suppose $(G,*)$ is a finite group and let $a\in G$. Then there exists a positive integer m such that $a^m = e$, where e is the identity in G.

In fact, we can say something even stronger. You likely noticed the following fact while exploring Exercise 6.4.

Theorem 6.8. Suppose $(G,*)$ is a group and let $a\in G$.

(a) If $|a| = n < \infty$, then $a^n = e$ and $1, a, a^2, \ldots, a^{n-1}$ are all distinct elements of $\langle a\rangle$.

(b) If $|a| = \infty$, then $a^n \neq e$ for all $n\neq 0$ and $a^n \neq a^m$ whenever $n\neq m$ in $\mathbb{Z}$.

Corollary 6.9. Suppose $(G,*)$ is a finite group and let $a\in G$. Then the order of a is the smallest positive integer n such that $a^n = e$.

Exercise 6.10. Notice that in the definition for $\langle a\rangle$, we allow the exponents on a to be negative. Explain why we only need to use positive exponents when $\langle a\rangle$ is a finite group. What about when $\langle a\rangle$ is infinite?

Problem 6.11. Suppose $(G,*)$ is a group $a\in G$ with $|a| = n$. For what other exponents k will it be true that $a^k = e$? You'll have an opportunity to prove your claim later.

We are finally ready to introduce our family of interest for this section.

Definition 6.12. Suppose $(G,*)$ is a group. Then we say that G is a **cyclic group** if and only if there exists $a\in G$ such that $\langle a\rangle = G$.

It is clear that if G is cyclic with generator a, then $|G| = |a|$. In fact, if $a\in G$, the converse is true, as well.

Exercise 6.13. Determine which of the groups from Exercise 6.4 are cyclic. If the group is cyclic, find at least one generator.

Exercise 6.14. Determine whether each of the following groups are cyclic. If the group is cyclic, find at least one generator.

(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 6.15. If $(G, *)$ is a cyclic group, then G is abelian.

Exercise 6.16. Provide an example of a finite group that is abelian but not cyclic.

Exercise 6.17. Provide an example of an infinite group that is abelian but not cyclic.

Theorem 6.18. Suppose $(G, *)$ is a group and let $a \in G$. Then $\langle a \rangle = \langle a^{-1} \rangle$. In particular, $|a| = |a^{-1}|$.

Theorem 6.19. Suppose $(G, *)$ 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 6.20. Suppose $(G, *)$ is a group such that G has no proper nontrivial subgroups. Then G is cyclic.

Theorem 6.21. Suppose $(G, *)$ is an infinite cyclic group. Then G is isomorphic to $\mathbb{Z}$ (under the operation of addition).

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

Theorem 6.23. Suppose $(G, *)$ is a finite cyclic group of order $n \geq 2$. Then G is isomorphic to R_n if $n \geq 3$ and S_2 if $n = 2$.

The upshot of Theorems 6.21 and 6.23 is that up to isomorphism, we know exactly what all of the cyclic groups are.

Exercise 6.24. Suppose $(G, *)$ is a finite cyclic group of order n with generator a. If we write down the group table for G using $e, a, a^2, \ldots, a^{n-1}$ as the labels for the rows and columns, are there any interesting patterns in the table?

Recall that two integers are **relatively prime** if they have no factors other than 1 in common. That is, integers n and k are relatively prime iff $\gcd(n, k) = 1$.

Definition 6.25. Let $n \in \mathbb{N}$ and define the following sets.

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

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

For each set above, the immediate goal is to find a binary operation that will yield a group. The key is to use modular arithmetic. To calculate the sum (respectively, product) of two integers mod n, 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 being divided by 5. Similarly, $4 \cdot 9$ is 1 mod 5 since 36 has remainder 1 when being divided by 5.

Theorem 6.26. The set $(\mathbb{Z}_n, + \bmod n)$ is a group.

Theorem 6.27. The set $(U(n), \cdot \bmod n)$ is a group.

Exercise 6.28. 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 $\mathbb{Z}_4$.

Exercise 6.29. 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 $U(10)$.

Exercise 6.30. 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 $U(12)$.

In light of Exercise 6.29 and 6.30, $U(n)$ may or may not be cyclic. Nonetheless, as the next theorem illustrates, $U(n)$ is always abelian.

Theorem 6.31. For all n, $U(n)$ is abelian.

The upshot of the next theorem is that $\mathbb{Z}_n$ is just the set of (smallest nonnegative) exponents on r in R_n.

Theorem 6.32. For $n \geq 3$, $\mathbb{Z}_n \cong R_n$. Moreover, $\mathbb{Z}_2 \cong S_2$.

One consequence of the previous theorem is that $\mathbb{Z}_n$ is always cyclic. Combining the results of Theorems 6.23 and 6.21 together with Theorem 6.32, we immediately obtain the following.

Theorem 6.33. Let $(G,*)$ be a cyclic group with generator a. 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 $(\mathbb{Z}_n,+ \bmod n)$.

Now that we have a complete description of the cyclic groups, let's focus our attention on subgroups of cyclic groups. The next result should look familiar and will come in handy. In particular, it will be useful when proving Theorems 6.35 and6.37. We'll take the result for granted and not worry about proving it right now.

Theorem 6.34 (Division Algorithm for $\mathbb{Z}$)**.** If m is a positive integer and n is any integer, then there exist unique integers q (called the **quotient**) and r (called the **remainder**) such that $n = mq + r$, where $0 \leq r < m$.

Theorem 6.35. Suppose $(G,*)$ is a group and let $a \in G$ such that $|a| = n$. Then $a^i = a^j$ iff n divides $i - j$.

Compare the next result to Problem 6.11.

Corollary 6.36. Suppose $(G,*)$ is a group and let $a \in G$ such that $|a| = n$. If $a^k = e$, then $|a|$ divides k.

Theorem 6.37. 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 6.37 is not true.

Exercise 6.38. 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 Exercise 5.56(d) and also provides a complete description of the subgroups of infinite cyclic groups up to isomorphism.

Corollary 6.39. The subgroups of $\mathbb{Z}$ are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.

What about finite cyclic groups?

Theorem 6.40. Suppose $(G,*)$ is a finite cyclic group with generator a such that $|G| = n$.

(a) Then $|a^s| = \dfrac{n}{\gcd(n,s)}$.

(b) Moreover, $\langle a^s \rangle = \langle a^t \rangle$ iff $\gcd(s,n) = \gcd(t,n)$.

Exercise 6.41. Suppose $(G,*)$ is a cyclic group of order 12 with generator a.

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

(b) Which elements of G individually generate G?

Corollary 6.42. Suppose $(G,*)$ is a finite cyclic group with generator a such that $|G| = n$. Then $\langle a\rangle = \langle a^r\rangle$ iff n and r are relatively prime. That is, a^r generates G iff n and r are relatively prime.

Exercise 6.43. Consider $(\mathbb{Z}_{18}, + \bmod 18)$.

(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 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 do you to figure out why this is true.

Exercise 6.44. Repeat the above exercise, but this time use $\mathbb{Z}_{12}$ instead of $\mathbb{Z}_{18}$.

Corollary 6.45. Suppose $(G,*)$ is a finite cyclic group with generator a such that $|G| = p$, where p is prime. Then G has no proper nontrivial subgroups.

Problem 6.46. Let p and q be distinct primes. Find the number of generators of $\mathbb{Z}_{pq}$.

Problem 6.47. 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.

Problem 6.48. If there is exactly one group up to isomorphism of order n, then to what group are all the groups of order n isomorphic?

6.2 Dihedral Groups

We can think of 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 reflection symmetry of regular n-gons.

Definition 6.49. 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 6.50. The group D_n is a non-abelian group of order $2n$.

Theorem 6.51. For $n \geq 3$, $R_n \leq D_n$.

Theorem 6.52. 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'.

Theorem 6.53. 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) $\underbrace{ss's\cdots}_{n \text{ factors}} = \underbrace{s'ss'\cdots}_{n \text{ factors}}$.

Exercise 6.54. From Theorem 6.52, 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? *Hint:* Where are the rotations? Where are the reflections?

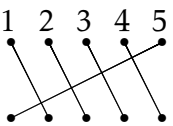
6.3 Symmetric Groups

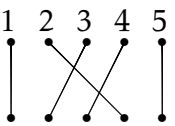
Recall the group S_3 from Exercise 4.27. This group acts on three coins that are in a row by rearranging their positions (but not flipping them over). This group is an example of a **symmetric group**. In general, the symmetric group on n objects is the set of permutations that rearranges the n objects. The group operation is composition of permutations. Let's be a little more formal.

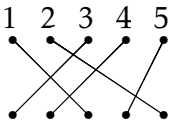
Definition 6.55. A **permutation of a set** A is a function $\sigma : A \to A$ that is both one-to-one and onto.

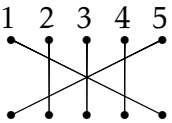
You should take a moment to convince yourself that the formal definition of a permutation agrees with the notion of rearranging the set of objects. The do-nothing action is the identity permutation, i.e., $\sigma(a) = a$ for all $a \in A$. There are many ways to represent a permutation. One visual way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

Consider the following diagrams:

$\alpha =$ 

$\beta =$ 

$\sigma =$ 

$\gamma =$ 

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.

Exercise 6.56. Describe in words what the permutations σ and γ do.

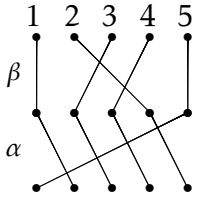
Exercise 6.57. Draw the permutation diagram for the do-nothing permutation on 5 objects. This is called the **identity permutation**. What does the identity permutation diagram look like in general for arbitrary n?

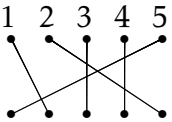
Definition 6.58. The set of all permutations on n objects is denoted by S_n.

Exercise 6.59. Draw all the permutation diagrams for the permutations in S_3.

Exercise 6.60. 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

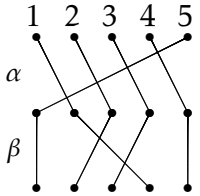
$\alpha \circ \beta =$ 

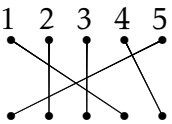
$=$ 

.

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

$\beta \circ \alpha =$ 

$=$ 

.

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

Exercise 6.61. 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?

Exercise 6.62. 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.

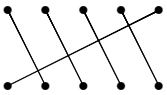
Problem 6.63. Given a permutation $\rho \in S_n$, describe a method for constructing ρ^{-1}. Briefly justify that $\rho \circ \rho^{-1}$ will yield the identity permutation.

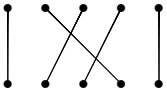
At this point, we have all the ingredients we need to prove that S_n forms a group under composition of permutations.

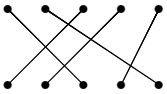
Theorem 6.64. The set of permutations on n objects forms a group under the operation of composition. That is, $(S_n, \circ)$ is a group. Moreover, $|S_n| = n!$.

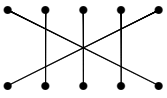
Note that it is standard convention to omit the composition symbol when writing down compositions in S_n. For example, we will simply write $\alpha\beta$ to denote $\alpha \circ \beta$.

Permutation diagrams are fun to play with, but we need a more efficient way of encoding information. One way to do this is using **cycle notation**. Consider α, β, σ, and γ in S_5 from the previous examples. Below I have indicated what each permutation is equal to using cycle notation.

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

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

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

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

Each string of numbers enclosed by parentheses is called a **cycle** and if the string of numbers has length k, then we call it a k-cycle. For example, α consists of a single 5-cycle, whereas σ consists of one 2-cycle and one 3-cycle. In the case of σ, we say that σ is the product of two **disjoint cycles**.

One observation that you hopefully made is that if an object in position i remains unchanged, then we don't bother listing that number in the cycle notation. However, if

we wanted to, we could use the 1-cycle (i) to denote this. For example, we could write $\beta = (1)(2,3,4)(5)$. In particular, we could denote the identity permutation in S_5 using $(1)(2)(3)(4)(5)$. Yet, it is common to simply use (1) to denote the identity in S_n for all n.

Notice that the first number we choose to write down for a given cycle is arbitrary. However, the numbers that follow are not negotiable. Typically, we would use the smallest possible number first, but this is not necessary. For example, the cycle $(2,4,7)$ could also be written as $(4,7,2)$ or $(7,2,4)$.

Exercise 6.65. Write down all 6 elements in S_3 using cycle notation.

Exercise 6.66. Write down all 24 elements in S_4 using cycle notation.

Suppose $\sigma \in S_n$. Since σ is one-to-one and onto, 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.

Exercise 6.67. 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) α^2

(c) α^3

(d) α^4

(e) α^5

(f) $\sigma\alpha$

(g) $\alpha^{-1}\sigma^{-1}$

(h) β^2

(i) β^3

(j) $\beta\gamma\alpha$

(k) σ^3

(l) σ^6

Exercise 6.68. Write down the group table for S_3 using cycle notation.

In Exercise 6.66, 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 6.69. Suppose α and β are two disjoint cycles. Then $\alpha\beta = \beta\alpha$. That is, products of disjoint cycles commute.

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 6.70. Suppose $\alpha \in S_n$ such that α consists of a single k-cycle. Then $|\alpha| = k$.

Theorem 6.71. 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 6.72. Is the previous theorem true if we do not require the cycles to be disjoint? Justify your answer.

Exercise 6.73. Compute the orders of all the elements in S_3. See Exercise 6.65.

Exercise 6.74. Compute the orders of all the elements in S_4. See Exercise 6.66.

Exercise 6.75. What is the order of $(1,4,7)(2,5)(3,6,8,9)$?

Exercise 6.76. Draw the subgroup lattice for S_3.

Exercise 6.77. Now, using $(1,2)$ and $(1,2,3)$ as generators, draw the Cayley diagram for S_3. Look familiar?

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

Definition 6.78. Every subgroup of a symmetric group is called a **permutation group**.

The proof of the following theorem isn't too bad, but for now we'll take it for granted.

Theorem 6.79 (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.

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

$*$	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 $(1,3)(2,4)$.

Exercise 6.80. Find a permutation group that is isomorphic to D_4.

Exercise 6.81. Find a permutation group that is isomorphic to $\mathbb{Z}_6$.

Exercise 6.82. Consider S_3.

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

(b) In the previous part, we used a generating set with three elements. Is there a smaller generating set? If so, what is it?

Exercise 6.83. Recall that there are $4! = 24$ permutations 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 S_n. To get some intuition for these facts, let's play with a few examples.

Exercise 6.84. 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 6.85. 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 6.86. 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 6.87. Consider S_n.

1. Every permutation in S_n can be written as a product of transpositions.
2. Every permutation in S_n can be written as a product of adjacent transpositions.

Corollary 6.88. The set of transpositions (respectively, the set of adjacent transpositions) from S_n forms a generating set for S_n.

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. 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).

Random thoughts that I'll elaborate on next time I teach the course:

1. The rigid motion symmetry group for the cube is isomorphic to S_4.
2. You can arrange the Cayley diagram for S_4 with generators $(1,2)$ and $(1,2,3,4)$ on a truncated cube.

6.4 Alternating Groups

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

Theorem 6.89. Let $\sigma \in S_n$. Then every transposition representation of σ has the same parity.

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

Definition 6.90. A permutation is **even** (respectively, **odd**) if one of its transposition representations consists of an even (respectively, odd) number of transpositions.

Exercise 6.91. Classify all of the permutations in S_3 as even or odd.

Exercise 6.92. Classify all of the permutations in S_4 as even or odd.

Exercise 6.93. Determine whether $(1,4,2,3,5)$ is even or odd. How about $(1,4,2,3,5)(7,9)$?

Problem 6.94. 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 6.95. 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.