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 $(G, *)$ 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 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