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 $0 \leq r < n$.

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 $g^n = e$.

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.

Problem 4.24. Suppose G is a group and $g \in G$ with $|g| = n$. For what other exponents k do you think will it be true that $g^k = e$? You'll have an opportunity to prove your claim later.

*For the forward implication, 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.

†Note that Theorem 4.17 together with the Well-Ordering Principle guarantees the existence of a smallest positive integer n such that $g^n = e$. Let $m \in \mathbb{Z}$ and use the Division Algorithm with m and n. By the way, the claim that the set contains n distinct elements is not immediate. You need to argue that there are no repeats in the list.

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

Theorem 4.26. Suppose G is a finite cyclic group of order $n \geq 1$. 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?

Theorem 4.27. 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 4.28. If G is an infinite cyclic group, then G is isomorphic to $\mathbb{Z}$ (under the operation of addition).

The upshot of Theorems 4.28 and 4.26 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 4.29. 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 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 $a \equiv b \pmod{n}$, and say "a is equivalent to b mod n", if a and b both have the same remainder when divided by n. We may also write $a \equiv_n b$, or even $a = b$ 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 4.30. Let n be a positive integer and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if n divides $a - b$.

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

Theorem 4.31. The set $\mathbb{Z}_n$ is a group under addition mod n.

Theorem 4.32. The set U_n is a group under multiplication mod n.

Problem 4.33. 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 $\mathbb{Z}_4$.

Problem 4.34. 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 4.35. 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 Exercises 4.34 and 4.35, U_n may or may not be cyclic. Nonetheless, as the next theorem illustrates, U_n is always abelian.

Theorem 4.36. For all n, U_n is abelian.

The upshot of the next theorem is that for $n \geq 3$, $\mathbb{Z}_n$ is just the set of (smallest nonnegative) exponents on r in R_n.

Theorem 4.37. 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.

One consequence of the previous theorem is that $\mathbb{Z}_n$ is always cyclic. Combining the results of Theorems 4.26 and 4.28 together with Theorem 4.37, we immediately obtain the following.

Theorem 4.38. 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 $(\mathbb{Z}_n,+ \bmod n)$.

Now that we have a complete description of the cyclic groups, let's focus our attention on subgroups of cyclic groups. The Division Algorithm should come in handy when proving the next theorem.

Theorem 4.39. 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 $i - j$.

Compare the next result to Problem 4.24.

Corollary 4.40. Suppose G is a group and let $g \in G$ such that $|g| = n$. If $g^k = e$, then $|g|$ divides k.

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 3.16(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 $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.

Let's explore finite cyclic groups.

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

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.

[§]By Corollary 4.20, the order of g^m is the smallest positive exponent k such that $(g^m)^k = e$. First, verify that $k = \frac{n}{\gcd(n,m)}$ has the desired property and then verify that it is the smallest such exponent.

[¶]Use Theorem 4.44 for the forward implication. For the reverse implication, first prove that for all $m \in \mathbb{Z}$, $\langle g^s \rangle = \langle g^{\gcd(s,n)} \rangle$ 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.

Problem 4.48. 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 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 4.49. Repeat the above exercise, but this time use $\mathbb{Z}_{12}$ instead of $\mathbb{Z}_{18}$.

Corollary 4.50. If G is a finite cyclic group such that $|G| = p$, where p is prime, then G has no proper nontrivial subgroups.

Problem 4.51. Let p and q be distinct primes. Find the number of generators of $\mathbb{Z}_{pq}$.

Problem 4.52. 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 4.53. If there is exactly one group up to isomorphism of order n, then to what group are all the groups of order n isomorphic?

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 4.54. 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 4.55. The group D_n is a non-abelian group of order $2n$.

Theorem 4.56. For $n \geq 3$, $R_n \leq D_n$.

Theorem 4.57. 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'.