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) $\text{Spin}_{1\times 2}$

(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.

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 $i - j$.

[*]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.

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?

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

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.

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