Problem Sequence for MAT 511

By Dana C. Ernst
Northern Arizona University

1 Introduction to Groups

1.1 Binary Operations

Definition 1.1. A **binary operation** $*$ on a set A is a function from $A \times A$ into A. For each $(a,b) \in A \times A$, we denote the element $*(a,b)$ via $a * b$. If the context is clear, we may abbreviate $a * b$ as ab.

Do not misunderstand the use of $*$ in this context. We are not implying that $*$ is the ordinary multiplication of real numbers. We are using $*$ to represent a generic binary operation. Notice that since the codomain of a binary operation on a set A is A, binary operations require that we yield an element of A when combining two elements of A. In this case, we say that A is **closed** under $*$. Binary operations have this closure property by definition. Also, since binary operations are functions, any attempt to combine two elements from A should result in a *unique* element of A. Moreover, since the domain of $*$ is $A \times A$, it must be the case that $*$ is defined for *all* pairs of elements from A.

Problem 1.2. Let A be a set. Feel free to consult outside resources for parts (a) and (d).

(a) If $*$ is a binary operation on A, what does it mean for $*$ to be **associative**?

(b) Provide an example of a set together with a binary operation that is associative.

(c) Provide an example of a set together with a binary operation that is *not* associative.

(d) If $*$ is a binary operation on A, what does it mean for $*$ to be **commutative**?

(e) Provide an example of a set together with a binary operation that is commutative.

(f) Provide an example of a set together with a binary operation that is *not* commutative.

Problem 1.3. Provide an example of a set A and a binary operation $*$ on A such that $(a*b)^2 \neq a^2 * b^2$ for some $a, b \in A$. Under what conditions will $(a*b)^2 = a^2 * b^2$ for all $a, b \in A$? *Note:* The notation x^2 is shorthand for $x * x$.

Problem 1.4. Determine whether each of the following binary operations is (i) associative and (ii) commutative.

(a) The operation $\star$ on $\mathbb{R}$ defined via $a \star b = 1 + ab$. In this case, ab denotes the ordinary multiplication of the real numbers a and b.

(b) The operation $\circ$ on $\mathbb{Q}$ defined via $a \circ b = \dfrac{a+b}{5}$.

(c) The operation $\circledcirc$ on $\mathbb{Z} \times \mathbb{Z}$ defined via $(a,b) \circledcirc (c,d) = (ad + bc, bd)$.

(d) The operation $\circledast$ on $\mathbb{Q} \setminus \{0\}$ defined via $a \circledast b = \dfrac{a}{b}$.

(e) The operation $\ominus$ on $\mathbb{R}/I := \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ defined via $a \ominus b = a + b - \lfloor a + b \rfloor$ (i.e., $a \ominus b$ is the fractional part of $a + b$).

Problem 1.5. Prove that if A is a nonempty set and F is the set of functions from A to A, then function composition is an associative binary operation on F.

When the set A is finite, we can represent a binary operation on A using a table in which the elements of the set are listed across the top and down the left side (in the same order). The entry in the ith row and jth column of the table represents the output of combining the element that labels the ith row with the element that labels the jth column (order matters).

Example 1.6. Consider the following table.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

This table represents a binary operation on the set $A = \{a, b, c\}$. In this case, $a * b = c$ while $b * a = a$. This shows that $*$ is not commutative.

Problem 1.7. What property must the table for a binary operation have in order for the operation to be commutative?

Problem 1.8. Consider the following table that displays the binary operation $*$ on the set $\{x, y, z\}$.

$*$	x	y	z
x	x	y	z
y	y	x	x
z	y	x	x

(a) Determine whether $*$ is commutative.

(b) Determine whether $*$ is associative.

Problem 1.9. Let n be a fixed positive integer. Define $\equiv_n$ on $\mathbb{Z}$ via

$$a \equiv_n b \text{ if and only if } n \mid (b - a).$$

It turns out that $\equiv_n$ is an equivalence relation (you may take this for granted). If $a \equiv_n b$, then we say, "a is congruent to b mod n." The equivalence classes determined by $\equiv_n$ are defined via

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}.$$

There are precisely n equivalence classes mod n, namely $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ determined by the possible remainders after division by n. We denote the collection of equivalence classes mod n by $\mathbb{Z}/n\mathbb{Z}$. For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, we define **addition mod** n via

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Similarly, we define **multiplication mod** n via

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Prove each of the following.

(a) Addition mod n is a well-defined binary operation on $\mathbb{Z}/n\mathbb{Z}$.

(b) Multiplication mod n is a well-defined binary operation on $\mathbb{Z}/n\mathbb{Z}$.

Problem 1.10. Write down the table that represents addition mod 4 on $\mathbb{Z}/4\mathbb{Z}$.

Definition 1.11. Suppose $*$ is a binary operation on a set A and let $T \subseteq A$. If the restriction of $*$ to T is a binary operation on T, then we say that T is **closed under** $*$.

Problem 1.12. Provide an example of a set A and a proper subset T of A together with a binary operation $*$ on A such that T is closed under $*$.

Problem 1.13. Provide an example of a set A and a proper subset T of A together with a binary operation $*$ on A such that T is *not* closed under $*$.

Problem 1.14. Suppose $*$ is an associative binary operation on A and let $T \subseteq A$ such that T is closed under $*$. Is $*$ an associative binary operation on T? Justify your assertion.

Problem 1.15. Suppose $*$ is a commutative binary operation on A and let $T \subseteq A$ such that T is closed under $*$. Is $*$ a commutative binary operation on T? Justify your assertion.

1.2 Groups

Definition 1.16. A **group** $(G,*)$ is a set G together with a binary operation $*$ such that the following axioms hold.

(0) The set G is closed under $*$.

(1) The operation $*$ is associative.

(2) There is an element $e \in G$ such that for all $g \in G$, $e*g = g*e = g$. We call e the **identity**.[1]

(3) Corresponding to each $g \in G$, there is an element $g' \in G$ such that $g*g' = g'*g = e$. In this case, g' is said to be an **inverse** of g.

The **order** of G, denoted $|G|$, is the cardinality of the set G. If $|G|$ is finite, then we say that G has finite order. Otherwise, we say that G has infinite order.

In the definition of a group, the binary operation $*$ is not required to be commutative. If $*$ is commutative, then we say that G is **abelian**[2]. A few additional comments are in order.

- Axiom 2 forces G to be nonempty.
- If $(G,*)$ is a group, then we say that G **is a group under** $*$.
- We refer to $a*b$ as the **product** of a and b even if $*$ is not actually multiplication.
- For simplicity, if $(G,*)$ is a group, we will often refer to G as being the group and suppress any mention of $*$ whatsoever. In particular, we will often abbreviate $a*b$ as ab.
- We shall see that each $g \in G$ has a unique inverse. From that point on, we will denote *the* inverse of g by g^{-1}.

Problem 1.17. Explain why Axiom 0 is unnecessary.

Problem 1.18. Explain why every group is nonempty.

Problem 1.19. Consider a square puzzle piece that fits perfectly into a square hole. Let R_4 be the set of net actions consisting of the rotations of the square by an appropriate amount so that it fits back into the hole. For example, rotating by 90° clockwise and 270° counterclockwise are considered the same net action. Assume we can tell the corners of the square apart from each other so that if the square has been rotated and put back in the hole we can notice the difference. Each net action is called a **symmetry** of the square.

(a) Describe all of the distinct symmetries in R_4. How many distinct symmetries are in R_4?

(b) Explain why R_4 is a group under composition of symmetries.

(c) Describe the identity of this group.

(d) Describe the inverse of each element in this group.

(e) Is R_4 an abelian group?

Let's pause for a moment to make sure we understand our use of the word symmetry in this context. A fundamental question in mathematics is "When are two things the same?", where "things" can be whatever mathematical notion we happen to be thinking about at a particular moment. Right now we need to answer, "When do we want to consider two symmetries to be the same?" To be clear, this is a choice, and different choices can lead to different, interesting, and equally valid mathematics. For symmetries, one natural thought is that symmetries are equal when they produce the same net action on the square, meaning that when applied to a square in a particular starting position, they both yield the same ending position. In general, two symmetries are equal if they produce the same net action on the object in question. Notice that we are really defining an equivalence relation here.

The set R_4 is called the rotation group for the square. For $n \geq 3$, R_n is the **rotation group** for the regular n-gon and consists of the rotational symmetries for a regular n-gon. Every R_n really is a group under composition of symmetries.

[1] The origin of using the letter e for the identity of a group appears to be due to German mathematician Heinrich Weber, who uses "einheit" (German for "unit" or "unity") and e in his *Lehrbuch der Algebra* (1896).

[2] Commutative groups are called abelian in honor of the Norwegian mathematician Niels Abel (1802–1829).

Problem 1.20. Consider a puzzle piece like the one in the previous problem, except this time, let's assume that the piece and the hole are an equilateral triangle. Let D_3 be the full set of symmetries that allow the triangle to fit back in the hole. In addition to rotations, we will also allow the triangle to be flipped over—called a reflection.

(a) Describe all of the distinct symmetries in D_3. How many distinct symmetries are in D_3?

(b) Explain why D_3 is a group under composition of symmetries.

(c) Describe the identity of this group.

(d) Describe the inverse of each element in this group.

(e) Is D_3 an abelian group?

Problem 1.21. Repeat the above problem, but do it for a square instead of a triangle. The corresponding group is called D_4.

The sets D_3 and D_4 are examples of dihedral groups. In general, for $n \geq 3$, D_n consists of the symmetries (rotations and reflections) of a regular n-gon and is called the **dihedral group of order** $2n$. Do you see why D_n consists of $2n$ net actions? As expected, every D_n really is a group.

Problem 1.22. Consider the set S_3 consisting of the net actions that permute the positions of three coins (without flipping them over) that are sitting side by side in a line. Assume that you can tell the coins apart.

(a) Write down all distinct net actions in S_3 using verbal descriptions. Some of these will be tricky to describe. How many distinct net actions are in S_3?

(b) Explain why S_3 is a group under composition of symmetries.

(c) Describe the identity of this group.

(d) Describe the inverse of each element in this group.

(e) Is S_3 an abelian group?

The set S_3 is an example of a symmetric group. In general, S_n is the **symmetric group on** n **objects** and consists of the net actions that rearrange the n objects. Such rearrangements are called **permutations**. Later we will prove that each S_n is a group under composition of permutations.

Problem 1.23. Determine whether each of the following is a group. If the pair is a group, determine the order, identify the identity, describe the inverses, and determine whether the group is abelian. If the pair is not a group, explain why.

(a) $(\mathbb{Z}, +)$

(b) $(\mathbb{N}, +)$

(c) $(\mathbb{Z}, \cdot)$

(d) $(\mathbb{Z}, \div)$

(e) $(\mathbb{R}, +)$

(f) $(\mathbb{C}, +)$

(g) $(\mathbb{R}, \cdot)$

(h) $(\mathbb{Q} \setminus \{0\}, \cdot)$

(i) $(\mathbb{Z} \setminus \{0\}, \cdot)$

(j) $(M_{2\times 2}(\mathbb{R}), +)$

(k) $(M_{2\times 2}(\mathbb{R}), *)$, where $*$ is matrix multiplication.

(l) $([0,1], *)$, where $a * b := \min(a, b)$

(m) $(\{a,b,c\},*)$, where $*$ is the operation determined by the table in Example 1.6.

(n) $(\{x,y,z\},*)$, where $*$ is the operation determined by the table in Problem 1.8.

(o) $\mathbb{Z}/n\mathbb{Z}$ under addition mod n.

(p) $\mathbb{Z}/n\mathbb{Z}$ under multiplication mod n.

(q) Set of rational numbers in lowest terms whose denominators are odd under addition. *Note:* Since we can write $0 = 0/1$, 0 is included in this set.

(r) Set of rational numbers in lowest terms whose denominators are even together with 0 under addition.

(s) Set of rational numbers of absolute value less than 1 under addition.

(t) $\mathbb{R}/I$ under $\ominus$ as defined in Problem 1.4(e).

Problem 1.24. Let $G = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. Prove each of the following.

(a) The set G is a group under addition.

(b) If $H = G \setminus \{0\}$, then H is a group under multiplication.

Notice that in Axiom 2 of Definition 1.16, we said *the* identity and not *an* identity. Implicitly, this implies that the identity is unique. You'll notice that I even said "the identity" in Problems 1.19–1.23.

Problem 1.25. Prove that if G is a group, then there is a unique identity element in G. That is, there is only one element $e \in G$ such that $ge = eg = g$ for all $g \in G$.

Problem 1.26. Provide an example of a group of order 1. Can you find more than one such group?

Any group of order 1 is called a **trivial group**. It follows immediately from the definition of a group that the element of a trivial group must be the identity.

It is important to note that if we have an equation involving the product of group elements, we can still "do the same thing to both sides" and maintain equality. However, because general groups are not necessarily abelian, we have to be careful that we truly operate in the same way on each side. For example, if we have the equation $g = h$ in some group, then we also have $ag = ah$, where we "multiplied" both sides on the left by the group element a. We could not necessarily conclude that $ag = ha$, unless one pair of the elements happen to commute with each other.

The following theorem is crucial for proving many theorems about groups.

Problem 1.27 (Cancellation Law)**.** Let G be a group and let $g,x,y \in G$. Prove that $gx = gy$ if and only if $x = y$. Similarly, we have $xg = yg$ if and only if $x = y$.

Problem 1.28. Show that $(\mathbb{R},\cdot)$ fails the Cancellation Law confirming the fact that it is not a group.

Recall that Axiom (3) of Definition 1.16 states that each element of a group has at least one inverse. The next theorem tells us that each element has exactly one inverse. Again, you'll notice that I already cheated at wrote "the inverse" in Problems 1.19–1.23.

Problem 1.29. Prove that if G is a group, then each $g \in G$ has a unique inverse.

In light of the previous problem, the unique inverse of $g \in G$ will be denoted as g^{-1}. In groups, it turns out that inverses are always "two-sided". That is, if G is a group and $g,h \in G$ such that $gh = e$, then it must be the case that $hg = e$, as well. In this case, $g^{-1} = h$ and $h^{-1} = g$. However, there are mathematical structures where a "left inverse" exists but the "right inverse" does not.

Problem 1.30. Prove that if G is a group, then for all $g,h \in G$, the equation $gx = h$ has a unique solution for x in G. Similarly, the equation $xg = h$ has a unique solution.

The next result should not be surprising.

Problem 1.31. Prove that if G is a group, then $(g^{-1})^{-1} = g$ for all $g \in G$.

The next result is analogous to the "socks and shoes theorem" for composition of functions.

Problem 1.32. Prove that if G is a group, then $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$.

Problem 1.33 (Generalized Associative Law)**.** Prove that if G is a group, then for any $g_1, g_2, \ldots, g_n \in G$, the value of $g_1 g_2 \cdots g_n$ is independent of how the product is bracketed. Consider using induction on n.

Definition 1.34. If G is a group and $g \in G$, then for all $n \in \mathbb{N}$, we define:

(a) $g^n = \underbrace{gg\cdots g}_{n \text{ factors}}$

(b) $g^{-n} = \underbrace{g^{-1}g^{-1}\cdots g^{-1}}_{n \text{ factors}}$

(c) $g^0 = e$

Remark 1.35. If G is a group under $+$, then we can reinterpret Definition 1.34 as:

(a) $ng = \underbrace{g + g + \cdots + g}_{n \text{ summands}}$

(b) $-ng = \underbrace{-g + -g + \cdots + -g}_{n \text{ summands}}$

(c) $0g = 0$

Notice all that we have done is taken the statements of Definition 1.34, which use multiplicative notation for the group operation, and translated what they say in the case that the group operation uses additive notation.

The good news is that the many of the rules of exponents you are familiar with still hold for groups.

Problem 1.36. Prove that if G is a group and $g \in G$, then for all $n, m \in \mathbb{Z}$, we have the following:

(a) $g^n g^m = g^{n+m}$,

(b) $(g^n)^{-1} = g^{-n}$,

(c) $(g^n)^m = g^{nm}$.

Problem 1.37. Reinterpret problem 1.36 if G is a group under addition.

Unfortunately, there are some rules of exponents that do not apply for general groups.

Problem 1.38. Assume G is a group and let $a, b \in G$. Is it true that $(ab)^n = a^n b^n$? If not, under what minimal conditions would it be true? Prove the statement that you think is true.

Problem 1.39. Assume G is a group. Prove that if $g^2 = e$ for all $g \in G$, then G is abelian. Is the converse true?

Problem 1.40. Assume $G = \{e, a, b, c\}$ is a group under $\star$ with the property that $x^2 = x^4$ for all $x \in G$ (where e is the identity). Complete the following **group table**, where $x \star y$ is defined to be the entry in the row labeled by x and the column labeled by y.

$\star$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

Is your table unique? That is, did you have to fill it out the way you did? Deduce that G is abelian.

Problem 1.41. Assume G is a finite group. Prove that every element of G must appear exactly once in every row and column of the group table for G. (Of course, we are not counting the row and column headings.)

Problem 1.42. Prove that if G is a group and $g \in G$, then the two functions $l_g(x) := gx$ and $r_g(x) := xg$ are both permutations of G (i.e., l_g and r_g are bijections from G to G).

1.3 Generating Sets

In this section, we explore the concept of a generating set for a group.

Definition 1.43. Let G be a group and let S be a subset of G. A finite product (under the operation of G) consisting of elements from S or their inverses is called a **word** in S. That is, a word in S is of the form

$$s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n},$$

where each $s_i \in S$ and $\varepsilon_i \in \{\pm 1\}$. Each s_i is called a **letter** and the set S is called the **alphabet**. By convention, the identity of G can be represented by the **empty word**, which is the word having no letters. The set of elements of G that can be written as words in S is denoted by $\langle S \rangle$ and is called the **group generated by** S.

It is worth mentioning that we are slightly abusing notation here. For nonempty $S \subseteq G$, we can form infinitely many words in $\langle S \rangle$, but often there are many words that represent the same group element. We can partition the collection of words in the alphabet S into equivalence classes based on which group element a word represents. Strictly speaking, each group element is an equivalence class of words. When we say two words are equal in the group, what we really mean is that both words are in the same equivalence class.

Moreover, while S and $\langle S \rangle$ are both sets, the latter set is the set of elements we can build using letters and their inverses from S. It turns out that if S is itself a group, then $S = \langle S \rangle$. Otherwise, S is a proper subset of $\langle S \rangle$.

If we know what the elements of S actually are, then we will list them inside the angle brackets without the set braces. For example, if $S = \{a, b, c\}$, then we will write $\langle a, b, c \rangle$ instead of $\langle \{a, b, c\} \rangle$. In the special case when the generating set S consists of a single element, say g, we have

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

and say that G is a **cyclic group**. As we shall see, $\langle g \rangle$ may be finite or infinite.

Example 1.44. Suppose G is a group such that $a, b, c \in G$ and let $S = \{a, b, c\}$. Then ab, $c^{-1}acc$, and $ab^{-1}caa^{-1}bc^{-1}$ are words in $\langle S \rangle$. If any one of these words is not equal to a, b, or c, then S is a proper subset of $\langle S \rangle$.

Problem 1.45. Prove that if G is a group under $*$ and S is a subset of G, then $\langle S \rangle$ is also a group under $*$.

Definition 1.46. If G is a group and S is a subset of G such that $G = \langle S \rangle$, then S is called a **generating set** of G. In other words, S is a generating set of G if every element of G can be expressed as a word in S. In this case, we say S **generates** G. A generating set S for G is a **minimal generating set** if $S \setminus \{x\}$ is no longer a generating set for G for all $x \in S$.

A generating set for a group is analogous to a spanning set for a vector space and a minimal generating set for a group is analogous to a basis for a vector space.

Problem 1.47. Consider the rotation group R_4 that we introduced in Problem 1.19. Let r be the element of R_4 that rotates the square by 90° clockwise.

(a) Describe the action of r^{-1} on the square and express r^{-1} as a word using r only.

(b) Prove that $R_4 = \langle r \rangle$ by writing every element of R_4 as a word using r only.

(c) Is $\{r\}$ a minimal generating set for R_4?

(d) Is R_4 a cyclic group?

Problem 1.48. Consider the dihedral group D_3 introduced in Problem 1.20. To give us a common starting point, let's assume the triangle and hole are positioned so that one of the tips of the triangle is pointed up. Let r be rotation by 120° in the clockwise direction and let s be the reflection in D_3 that fixes the top of the triangle.

(a) Describe the action of r^{-1} on the triangle and express r^{-1} as a word using r only.

(b) Describe the action of s^{-1} on the triangle and express s^{-1} as a word using s only.

(c) Prove that $D_3 = \langle r, s \rangle$ by writing every element of D_3 as a word in r or s.

(d) Is $\{r, s\}$ a minimal generating set for D_3?

(e) Explain why there is no single generating set for D_3 consisting of a single element. This proves that D_3 is not cyclic.

It is important to point out that the fact that $\{r, s\}$ is a minimal generating set for D_3 does not immediately imply that D_3 is not a cyclic group. There are examples of cyclic groups that have minimal generating sets consisting of more than one element as the next problem illustrates.

Problem 1.49. Let R_6 denote the group of rotational symmetries of a regular hexagon and let r be rotation by 60° clockwise.

(a) Is R_6 cyclic?

(b) Is R_6 abelian?

(c) Write r^{-1} as a word in r.

(d) Can you find a shorter word to describe r^8?

(e) Does r^2 generate the group?

(f) Does r^3 generate the group?

(g) Does r^5 generate the group?

(h) Is $\{r^2, r^3\}$ a minimal generating set for R_6?

Problem 1.50. Let's consider the group D_3 again. Let s be the same reflection as in Problem 1.48 and let s' be the reflection in D_3 that fixes the bottom right corner of the triangle.

(a) Express r as a word in s and s'.

(b) Use part (a) together with Problem 1.48 to prove that $\langle s, s' \rangle = D_3$.

Problem 1.51. Consider the dihedral group D_4 introduced in Problem 1.21. Let r be clockwise rotation by 90° and let s be the reflection over the vertical midline of the square.

(a) Describe the action of r^{-1} on the square and express r^{-1} as a word using r only.

(b) Describe the action of s^{-1} on the square and express s^{-1} as a word using s only.

(c) Prove that $\{r, s\}$ is generating set for D_4.

(d) Is $\{r, s\}$ a minimal generating set for D_4?

(e) Find a different generating set for D_4.

(f) Is D_4 a cyclic group?

Problem 1.52. Consider the symmetric group S_3 that was introduced in Problem 1.22. Let s_1 be the action that swaps the positions of the first and second coins and let s_2 be the action that swaps the positions of the second and third coins.

(a) Prove that $S_3 = \langle s_1, s_2 \rangle$.

(b) Is $\{s_1, s_2\}$ a minimal generating set for S_3?

Problem 1.53. Consider a rectangle (which may or may not be a square) oriented so that one side is parallel to the ground. Let h be the symmetry that reflects the rectangle over the horizontal midline and let v be the symmetry that reflects the rectangle over the vertical midline. Define $V_4 := \langle v, h \rangle$. This group is called the **Klein group** (or **Vierergruppe**, which is German for "four-group") after the German mathematician Felix Klein (1849–1925).

(a) Verify that $|V_4| = 4$ by describing the symmetries in the group.

(b) Is V_4 abelian?

(c) Is V_4 cyclic?

Problem 1.54. Prove that the group $(\mathbb{Z}/n\mathbb{Z}, + \bmod n)$ is cyclic.

Problem 1.55. Consider the group $(\mathbb{Z}, +)$.

(a) Find a generating set that consists of a single element. Is $\mathbb{Z}$ a cyclic group under addition?

(b) If possible, find a minimal generating set that consists of two elements. If this is not possible, explain way.

Problem 1.56. Consider the group $(\mathbb{Q}, +)$.

(a) Find a generating set that is a proper subset of $\mathbb{Q}$.

(b) Is your generating set a minimal generating set?

Problem 1.57. Prove that if G is a cyclic group, then G is abelian.

Problem 1.58. Is the converse of the previous problem true? If so, prove it. Otherwise, find a counterexample.

1.4 Group Presentations

In this section, we introduce the notion of a **presentation** of a group. We'll only touch the surface here. There's a lot more going on behind the scenes!

Definition 1.59. Let G be a group and suppose $S \subseteq G$ such that $G = \langle S \rangle$. Any equation that the generators satisfy is called a **relation**.

Example 1.60. Here are a few examples of relations.

(a) Recall that $D_3 = \langle r, s \rangle$, where r and s are the actions described in Problem 1.48. In D_3, it's easy to verify that $r^3 = e$, $s^2 = e$, and $sr = r^2 s$. Each of these equations is an example of a relation in D_3.

(b) We also have $D_3 = \langle s, s' \rangle$, where s and s' are the actions described in Problem 1.50. Using this set of generators, D_3 satisfies the relations $s^2 = e$ (same as part (a)), $(s')^2 = e$, and $ss's = s'ss'$.

(c) Similar to part (a), $D_4 = \langle r, s \rangle$. In this case, D_4 satisfies the relations $r^4 = e$, $s^2 = e$, and $sr = r^3 s$.

(d) According to Problem 1.52, $S_3 = \langle s_1, s_2 \rangle$. It is easy to verify that S_3 satisfies the relations $s_1^2 = e$, $s_2^2 = e$, and $s_1 s_2 s_1 = s_2 s_1 s_2$.

(e) Using the generating set $\{1\}$ for $\mathbb{Z}$, it turns out that there are no relations.

Problem 1.61. Complete each of the following.

(a) Prove that $r^5 = r^2$, $(sr)^2 = e$, and $(ss')^3 = e$ are relations in D_3 using the relations provided in parts (a) and (b) of Example 1.60.

(b) Prove that $sr^2 = r^2 s$ is a relation in D_4 using the relations provided in part (c) of Example 1.60.

(c) Prove that $(s_2 s_1)^3 = e$ is a relation in S_3 using the relations provided in part (d) of Example 1.60.

Definition 1.62. Let G be a group and suppose $S \subseteq G$ such that $G = \langle S \rangle$. If there is a collection of relations, say $w_1 = e, w_2 = e, \ldots, w_m = e$, where each w_i is a word consisting of elements from S or inverses of elements from S, such that any relation among the elements of S can be derived from $w_1 = e, w_2 = e, \ldots, w_m = e$, we say that $(S, w_1 = e, w_2 = e, \ldots, w_m = e)$ is a **presentation** of G and write

$$G = \langle S \mid w_1 = e, w_2 = e, \ldots, w_m = e \rangle.$$

Officially, this is a **finite presentation** for G since there are finitely many relations. If instead we utilize infinitely many relations, the corresponding presentation is an **infinite presentation**.

Example 1.63. It is not immediately obvious, but it turns out that the relations described in Example 1.60 determine presentations for D_3, D_4, S_3, and $\mathbb{Z}$. In Problem 1.61, we verified that we can derive some additional relations from the ones given in Example 1.60. The not obvious part is that *every* relation in each of these groups can be deduced from the relations that were listed. That is, we have:

(a) $D_3 = \langle r, s \mid r^3 = e, s^2 = e, sr = r^2 s \rangle = \langle s, s' \mid s^2 = e, (s')^2 = e, ss's = s'ss' \rangle$.

(b) $D_4 = \langle r, s \mid r^4 = e, s^2 = e, sr = r^3 s \rangle$

(c) $S_3 = \langle s_1, s_2 \mid s_1^2 = e, s_2^2 = e, s_1 s_2 s_1 = s_2 s_1 s_2 \rangle$

(d) $\mathbb{Z} = \langle 1 \rangle$

It turns out that that the relations in each of the presentations are also minimal in the sense that we cannot eliminate one of the relations and use the remaining ones to produce the eliminated one.

For $n \geq 3$, define the **dihedral group** D_n to be the group of symmetries of a regular n-gon. It's not too hard to prove that D_n consists of n distinct rotations and n distinct reflections, so that $|D_n| = 2n$. In particular, one can prove using geometric arguments that

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

where r is equal to rotation by $360°/n$ clockwise, s is any fixed reflection, and each of the elements listed above is distinct. It follows from geometric arguments that $r^{-1} = r^{n-1}$ and $s^{-1} = s$. Later, we will prove that

$$D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{n-1} s \rangle$$

is a group presentation for D_n. It is easy to very that r and s satisfy the relations described in the presentations, but it is not obvious that these relations are enough to determine the group. In this section, we will take for granted that this is a presentation for D_n.

We can also define groups using presentations. If we define a group G via a presentation, say $G = \langle S \mid w_1 = e, w_2 = e, \ldots, w_m = e \rangle$, we mean that G is the group generated by S that satisfies all of the relations we can derive from $w_1 = e, w_2 = e, \ldots, w_m = e$. For example, we can define

$$D_2 := \langle r, s \mid r^2 = s^2 = e, sr = rs \rangle,$$

which fills in the case when $n = 2$ for the dihedral groups.

Problem 1.64. There's no such thing as a 2-gon, but can you describe an object that D_2 is the symmetry group for? There is more to proving your claim than you might expect. Don't worry about proving this carefully, but do consider what needs to be verified.

Problem 1.65. Consider D_n for $n \geq 3$.

(a) Prove that if $x \in D_n$ such that x is not a power of r, then $rx = xr^{-1}$.

(b) Assume $x \in D_n$ such that x is not a power of r. Geometrically, this implies that $x^2 = e$. Verify this fact using the relations provided in the presentation for D_n.

(c) Assume $n = 2k$ is even such that $n \geq 4$. By the description above for D_n in terms of rotations and reflection, we know $r^k \neq e$. Prove that $(r^k)^2 = e$. Moreover, prove that r^k is the only nonidentity element that commutes with every element of D_n.

(d) Assume n is odd such that $n \geq 3$. Prove that the identity is the only element of D_n that commutes with every element of D_n.

(e) Prove that $\langle a, b \mid a^2 = b^2 = (ab)^n = e \rangle$ is a presentation for D_n in terms of the generators $a = s$ and $b = sr$.

It follows from parts (c) and (d) of the previous problem that D_n is not abelian for all $n \geq 3$. This comes as no surprise since it is easy to see geometrically that $sr \neq rs$.

Utilizing presentations is tricky business. First, if you have a particular group in mind, it can often be difficult to find a presentation. Second, if you define a group using a presentation, it may be difficult

(or even impossible!) to determine when two elements of the group (expressed as words in the generators) are equal. As a result, we may have some difficulty determining the order of a group given by a presentation. In particular, it may not be easy to determine whether the corresponding group is even finite or infinite!

Similar to the last part of Problem 1.65, one can show that $\langle a, b \mid a^2 = b^2 = (ab)^2 = e\rangle$ is a presentation for D_2 (where $a = r$ and $b = s$). It turns out that $|D_2| = 4$. In particular, any group with a similar presentation is finite (specifically order 4). However, if you consider the similar-looking presentation $\langle a, b \mid a^3 = b^3 = (ab)^3 = e\rangle$, it turns out that the corresponding group is infinite! This is not obvious at all. Loosely speaking, it must be the case that in the presentation $\langle a, b \mid a^2 = b^2 = (ab)^2 = e\rangle$ there are sufficiently many relations that can be deduced from the given relations that a massive amount of "collapsing" occurs to make the group finite. In contrast, not enough collapsing occurs in $\langle a, b \mid a^3 = b^3 = (ab)^3 = e\rangle$ to make the group finite.

This collapsing makes it difficult to even determine lower bounds on the order for the group being presented. Sometimes even innocent-looking presentations can collapse considerably.

Problem 1.66. Define $G = \langle x, y \mid x^4 = y^3 = e, xy = y^2x^2\rangle$.

(a) Show that $y^2 = y^{-1}$.

(b) Show that y commutes with x^3. *Hint:* Show that $y^2x^3y = x^3$ by writing the left hand side as $(y^2x^2)(xy)$ and using the relations to reduce this to the right hand side. Then use part (a).

(c) Show that y commutes with x. *Hint:* Show that $x^9 = x$ and then use part (b).

(d) Show that $xy = e$ *Hint:* Use part (c) and the last relation.

(e) Show that $x = e$, and then deduce that $y = e$. *Hint:* Use part (d) and the relation $x^4y^3 = e$.

(f) Conclude that $|G| = 1$.

1.5 Subgroups

According to Problem 1.45, if S is any subset of a group G under $*$, then $\langle S\rangle$ is also a group under $*$. However, notice that $\langle S\rangle$ may not be equal to G. That is, $\langle S\rangle$ may be a proper subset of G that is a group in its own right (using the same binary operation as G). We can give a name to this phenomenon.

Definition 1.67. Let G be a group and let H be a subset of G. Then H is a **subgroup** of G, written $H \leq G$, provided that H is a group in its own right under the binary operation inherited from G.

The phrase "under the binary operation inherited from G" means that to combine two elements in H, we should treat the elements as if they were in G and perform the binary operation of G.

As an example, the group of rotations of a square is a subgroup of the full group of symmetries of a square. That is, $R_4 \leq D_4$.

Problem 1.68. Let G be a group and let $H \subseteq G$. If we wanted to determine whether H is a subgroup of G, can we skip checking any of the axioms? Which axioms must we verify?

Let's make the observations of the previous problem a bit more formal.

Problem 1.69 (Two Step Subgroup Test)**.** Suppose G is a group and H is a nonempty subset of G. Prove that $H \leq G$ if and only if (i) for all $h \in H$, $h^{-1} \in H$, as well, and (ii) H is closed under the binary operation of G.

Notice that one of the hypotheses of Problem 1.69 is that H be nonempty. This means that if we want to prove that a certain subset H is a subgroup of a group G, then one of the things we must do is verify that H is in fact nonempty. In light of this, the "Two Step Subgroup Test" should probably be called the "Three Step Subgroup Test".

Problem 1.70. Suppose G is a group and H is a nonempty subset of G. Conjecture and prove a "One Step Subgroup Test" that streamlines Problem 1.69.

As Problems 1.71 and 1.72 will illustrate, there are a couple of subgroups that every group contains.

Problem 1.71. Prove that if G is a group, then $\{e\} \leq G$.

The subgroup $\{e\}$ is referred to as the **trivial subgroup**. All other subgroups are called **nontrivial**. Subgroups are not required to be proper subsets of the "parent" group.

Problem 1.72. Prove that if G is a group, then $G \leq G$.

We refer to subgroups that are not equal to the whole group as **proper subgroups**. If H is a proper subgroup, then we may write $H < G$.

Let's take Problem 1.45 a step further.

Problem 1.73. Prove that if G is a group and $S \subseteq G$, then $\langle S \rangle$ is the smallest subgroup of G containing S.

The subgroup $\langle S \rangle$ is called the **subgroup generated by** S. In the special case when S equals a single element, say $S = \{g\}$, then

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

which is called the (**cyclic**) **subgroup generated by** g. Every subgroup can be written in the "generated by" form. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. In particular, $\langle H \rangle = H$ for $H \leq G$, and as a special case, we have $\langle G \rangle = G$.

Problem 1.74. Consider D_4. Let h be the reflection of the square over the horizontal midline and let v be the reflection over the vertical midline. Which of the following are subgroups of D_4? In each case, justify your answer. If a subset is a subgroup, try to find a minimal generating set.

(a) $\{e, r^2\}$

(b) $\{e, h\}$

(c) $\{e, h, v\}$

(d) $\{e, h, v, r^2\}$

Problem 1.75. Consider $(\mathbb{R}^3, +)$, where $\mathbb{R}^3$ is the set of all 3-entry row vectors with real number entries (e.g., (a, b, c) where $a, b, c \in \mathbb{R}$) and $+$ is ordinary vector addition. It turns out that $(\mathbb{R}^3, +)$ is an abelian group with identity $(0, 0, 0)$.

(a) Let H be the subset of $\mathbb{R}^3$ consisting of vectors with first coordinate 0. Is H a subgroup of $\mathbb{R}^3$? Prove your answer.

(b) Let K be the subset of $\mathbb{R}^3$ consisting of vectors whose entries sum to 0. Is K a subgroup of $\mathbb{R}^3$? Prove your answer.

(c) Construct a subset of $\mathbb{R}^3$ (different from H and K) that is *not* a subgroup of $\mathbb{R}^3$.

Problem 1.76. Consider the group $(\mathbb{Z}, +)$ (under ordinary addition).

(a) Show that the odd integers are not a subgroup of $\mathbb{Z}$.

(b) Show that all subsets of the form $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$ are subgroups of $\mathbb{Z}$.

(c) For $n \in \mathbb{Z}$, write the subgroup $n\mathbb{Z}$ in the "generated by" notation. That is, find a set S such that $\langle S \rangle = n\mathbb{Z}$. Can you find more than one way to do it?

(d) Find n such that $\langle 6, 9 \rangle = n\mathbb{Z}$. Justify your assertion.

(e) Are there any other subgroups besides the ones listed in part (b)? State a conjecture and perhaps prove it.

Problem 1.77. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \cdot)$. Explain why $\mathbb{R} \setminus \{0\}$ is not a subgroup of $\mathbb{R}$ despite the fact that $\mathbb{R} \setminus \{0\} \subseteq \mathbb{R}$ and both are groups (under the respective binary operations).

Problem 1.78. Prove that if G is an abelian group and $H \leq G$, then H is an abelian subgroup.

Problem 1.79. Is the converse of the previous theorem true? If so, prove it. Otherwise, provide a counterexample.

Recall that the order of a group G, denoted $|G|$, is the number of elements in G.

Definition 1.80. 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 a group G is cyclic with generator g if and only if $|G| = |g|$.

Problem 1.81. What is the order of the identity in any group?

Problem 1.82. 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) D_3

(g) S_3

(h) D_4

Problem 1.83. Consider the group $(\mathbb{Z}, +)$. What is the order of 1? Are there any elements in $\mathbb{Z}$ with finite order?

Problem 1.84. Prove that if G is a group and $g \in G$, then $\langle g \rangle = \langle g^{-1} \rangle$.

The next result follows immediately from Problem 1.84.

Problem 1.85. Prove that if G is a group and $g \in G$, then $|g| = |g^{-1}|$.

1.6 Centers, Centralizers, and Normalizers

In this section, we introduce three special subgroups. As we've seen, some groups are abelian and some are not.

Definition 1.86. If G is a group, then we define the **center** of G to be

$$Z(G) := \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Notice that if G is abelian, then $Z(G) = G$. However, if G is not abelian, then $Z(G)$ will be a proper subset of G. In some sense, the center of a group is a measure of how close G is to being abelian.

Problem 1.87. Prove that if G is a group, then $Z(G)$ is an abelian subgroup of G.

Problem 1.88. Find the center of each of the following groups.

(a) S_2

(b) V_4

(c) S_3

(d) $\mathbb{Z}/n\mathbb{Z}$

(e) R_n

(f) D_n

(g) $(\mathbb{Z}, +)$

(h) $(\mathbb{R} \setminus \{0\}, \cdot)$

Definition 1.89. Let G be a group and let A be a nonempty subset of G. Define the **centralizer** of A in G via

$$C_G(A) := \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

If $A = \{a\}$, we will write $C_G(a)$ instead of $C_G(\{a\})$.

Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G that commute with every element of A. The product gag^{-1} is called the **conjugate** of a by g. Notice that $C_G(G) = Z(G)$.

Problem 1.90. Prove that if G is a group and A be a nonempty subset of G, then $C_G(A)$ is a subgroup of G.

Definition 1.91. Let G be a group and let A be a nonempty subset of G. Define the **normalizer** of A in G via

$$N_G(A) := \{g \in G \mid gAg^{-1} = A\},$$

where $gAg^{-1} := \{gag^{-1} \mid a \in A\}$.

Notice that $C_G(A)$ is the set of elements of G that fix the set A *pointwise* using conjugation while $N_G(A)$ is the set of elements of G that fix the set A *setwise* using conjugation. It's clear that $C_G(A) \subseteq N_G(A)$.

Problem 1.92. Prove that if G is a group and A be a nonempty subset of G, then $N_G(A)$ is a subgroup of G. Is it true that $C_G(A)$ is a subgroup of $N_G(A)$?

Problem 1.93. Let G be a group and let A be a nonempty subset of G. Determine whether the following statement is true or false: $Z(G) \leq C_G(A) \leq N_G(A)$. If it is true, prove it. Otherwise, find a counterexample.

Problem 1.94. Suppose G is an abelian group and A is a nonempty subset of G. What can you say about $C_G(A)$ and $N_G(A)$?

Problem 1.95. For each group G and subset A, determine $C_G(A)$ and $N_G(A)$.

(a) $G = D_4$, $A = \langle r \rangle$

(b) $G = D_4$, $A = \langle s \rangle$

(c) $G = D_4$, $A = \langle s, r^2 \rangle$

(d) $G = S_3$, $A = \langle s_1 \rangle$

Problem 1.96. Let G be a group and let A and B be subsets of G such that $A \subseteq B$. What is the relationship between $C_G(A)$ and $C_G(B)$? Justify your assertion.

Problem 1.97. Let H be a subgroup of a group G.

(a) Prove that $H \leq N_G(H)$.

(b) Prove that $H \leq C_G(H)$ if and only if H is abelian.

1.7 Subgroup Lattices

Suppose we wanted to find all of the subgroups of a finite group G. Problems 1.71 and 1.72 tell us that $\{e\}$ and G itself are subgroups of G, but there may be others. Problem 1.69 tells us that if we want to find other subgroups of G, we need to find nonempty subsets of G that are closed and contain all the necessary inverses. So, one method for finding subgroups would be to find all possible nonempty subsets of G and then go about determining which subsets are subgroups by verifying whether a given subset is closed under inverses and closed under the operation of G. This is very time consuming!

Another approach would be to utilize the fact that every subgroup H of G has a generating set. That is, if H is a subgroup of a group G, then there always exists a subset S of G such that $\langle S \rangle = H$. Given a subset S of G, $\langle S \rangle$ is guaranteed to be closed under inverses and the operation of the group G. So, we could determine all of the subgroups of G by generating groups with various subsets S of G. Of course, one drawback is that it might take a bit of effort to determine what $\langle S \rangle$ actually is. Another drawback is that two different subsets S and T may generate the same subgroup.

Let's make this a bit more concrete by exploring an example.

Example 1.98. Consider the group R_4. What are the subgroups of R_4? Since the order of R_4 is 4, we know that there are $2^4 - 1 = 15$ nonempty subsets of R_4. Some of these are subgroups, but most of them are not. We know that $\{e\}$ and R_4 itself are subgroups of R_4. That's 2 out of 15 so far. Are there any others? Let's do an exhaustive search by playing with generating sets. We can certainly be more efficient, but below we list all of the possible subgroups we can generate using subsets of R_4. As you scan the list, you should take a moment to convince yourself that the list is accurate.

$\langle e \rangle = \{e\}$

$\langle r \rangle = \{e, r, r^2, r^3\}$

$\langle r^2 \rangle = \{e, r^2\}$

$\langle r^3 \rangle = \{e, r^3, r^2, r\}$

$\langle e, r \rangle = \{e, r, r^2, r^3\}$

$\langle e, r^2 \rangle = \{e, r^2\}$

$\langle e, r^3 \rangle = \{e, r^3, r^2, r\}$

$\langle r, r^2 \rangle = \{e, r, r^2, r^3\}$

$\langle r, r^3 \rangle = \{e, r, r^2, r^3\}$

$\langle r^2, r^3 \rangle = \{e, r, r^2, r^3\}$

$\langle e, r, r^2 \rangle = \{e, r, r^2, r^3\}$

$\langle e, r, r^3 \rangle = \{e, r, r^2, r^3\}$

$\langle e, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$

$\langle r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$

$\langle e, r, r^2, r^3 \rangle = \{e, r, r^2, r^3\}$

Let's make a few observations. Scanning the list, we see only three distinct subgroups:

$$\{e\}, \{e, r^2\}, \{e, r, r^2, r^3\}.$$

Out of 15 nonempty subsets of R_4, only 3 subsets are subgroups. Our exhaustive search guarantees that these are the only subgroups of R_4. It is also worth pointing out that if a subset contains either r or r^3, then that subset generates all of R_4. The reason for this is that $\{r\}$ and $\{r^3\}$ are each minimal generating sets for R_4. More generally, observe that if we increase the size of the generating subset using an element that was already contained in the subgroup generated by the set, then we don't get anything new. For example, consider $\langle r^2 \rangle = \{e, r^2\}$. Since $e \in \langle r^2 \rangle$, we don't get anything new by including e in our generating set.

Problem 1.99. Let G be a group and let $S \subseteq G$. Prove that if $x \in \langle S \rangle$, then $\langle S \rangle = \langle S \cup \{x\} \rangle$.

In the previous theorem, we are not claiming that S is a generating set for G—although this may be the case. Instead, are simply making a statement about the subgroup $\langle S \rangle$, whatever it may be.

We can capture the overall relationship between the subgroups of a group G using a **subgroup lattice**. Given a group G, the **lattice of subgroups** of G is the partially ordered set whose elements are the subgroups of G with the partial order relation being set inclusion. It is common to depict the subgroup lattice for a group using a **Hasse diagram**. The Hasse diagram of subgroup lattice is drawn as follows:

(1) Each subgroup H of G is a vertex.

(2) Vertices corresponding to subgroups with smaller order are placed lower in the diagram than vertices corresponding to subgroups with larger order. In particular, the vertex for $\{e\}$ is placed at the bottom of the diagram and the vertex for G is placed at the top.

(3) There is an edge going up from H to K if $H \leq K$ and there is no subgroup L such that $H \leq L \leq K$ with $L \neq H, K$.

Notice that there is an upward path of edges in the Hasse diagram from H to K if and only if $H \leq K$. For convenience we will not make a distinction between the subgroup lattice for a group G and the corresponding Hasse diagram.

Example 1.100. The Hasse diagram for the subgroup lattice for R_4 is given in Figure 1.

Example 1.101. Let's see what we can do with $V_4 = \{e, v, h, vh\}$. Using an exhaustive search, we find that there are five subgroups:

$\langle e \rangle = \{e\}$

$\langle h \rangle = \{e, h\}$

$\langle v \rangle = \{e, v\}$

$\langle vh \rangle = \{e, vh\}$

$\langle v, h \rangle = \langle v, vh \rangle = \langle h, vh \rangle = \{e, v, h, vh\} = V_4$

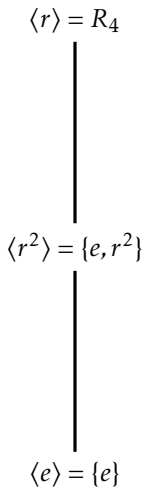


Figure 1: Subgroup lattice for R_4.

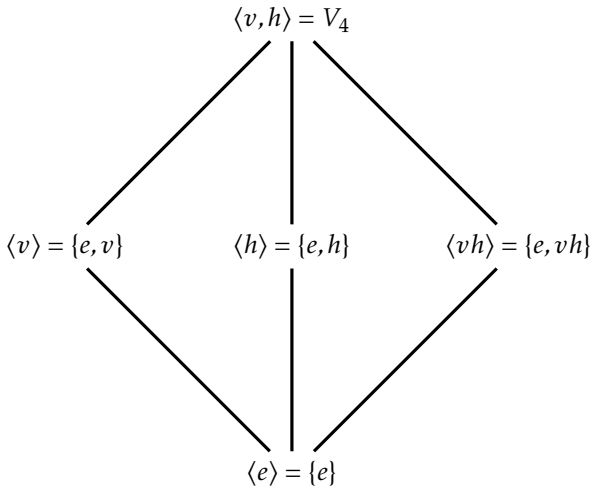


Figure 2: Subgroup lattice for V_4.

For each subgroup above, we've used minimal generating sets to determine the subgroup. The subgroup lattice for V_4 is given in Figure 2. Notice that there are no edges among $\langle v \rangle, \langle h \rangle$, and $\langle vh \rangle$. The reason for this is that none of these groups are subgroups of each other.

The next two problems provide some further insight into the overall structure of subgroups of a group.

Problem 1.102. Prove that if G is a group such that $H, K \leq G$, then $H \cap K \leq G$. Moreover, $H \cap K$ is the largest subgroup contained in both H and K.

It turns out that we cannot simply replace "intersection" with "union" in the previous problem.

Problem 1.103. Provide an example of a group G and subgroups H and K such that $H \cup K$ is not a subgroup of G.

Problem 1.104. Prove that if G is a group such that $H, K \leq G$, then $\langle H \cup K \rangle \leq G$. Moreover, $\langle H \cup K \rangle \leq G$ is the smallest subgroup containing both H and K.

Problems 1.102 and 1.104 justify the use of the word "lattice" in "subgroup lattice". In general, a lattice is a partially ordered set in which every two elements have a unique **meet** (also called a **greatest lower bound** or **infimum**) and a unique **join** (also called a **least upper bound** or **supremum**). In the case of a subgroup lattice for a group G, the meet of subgroups H and K is $H \cap K$ and the join is $\langle H \cup K \rangle$.

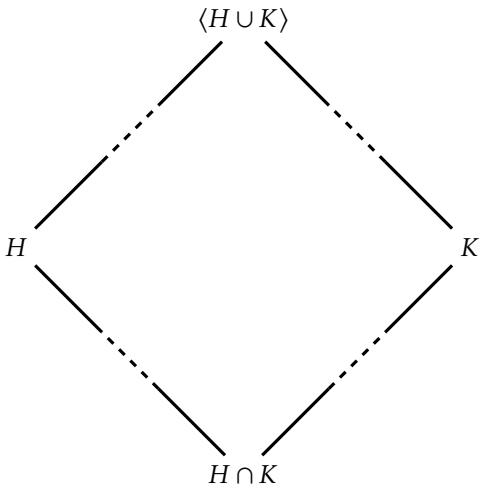


Figure 3: Meet and join for subgroups H and K.

Figure 3 illustrates the meet (Problem 1.102) and join (Problem 1.104) in the case when H and K are not comparable.

In the next problem, you are asked to create subgroup lattices. As you do this, try to minimize the amount of work it takes to come up with all the subgroups.

Problem 1.105. Find all the subgroups for each of the following groups and then draw the subgroup lattice.

(a) R_5

(b) R_6

(c) D_3

(d) S_3

(e) D_4

1.8 Cayley Diagrams

In this section, we will introduce visual way of encoding the abstract structure of the group in terms of a specified generating set.

Definition 1.106. Suppose G is a group and S is a generating set of G. The **Cayley diagram**[3] for G with generating set S is a colored directed graph constructed as follows:

(a) The vertices correspond to elements of G.

(b) Each generator $s \in S$ is assigned a color, say c_s.

(c) For $g \in G$ and $s \in S$, there is a directed edge from g to sg with color c_s.

Note that following the arrow from g to sg with color c_s corresponds to applying the action of s to g. Moreover, following the arrow backwards from sg to g corresponds to applying s^{-1} to sg. If a generator is its own inverse, then the arrows corresponding to that generator are two-way arrows.

Example 1.107. Let R_6 denote the group of rotational symmetries of a regular hexagon and let r be rotation by 60° clockwise. It's not too hard to see that $R_6 = \langle r \rangle$ and $|R_6| = 6$. The Cayley diagram for R_6 with generating set $\{r\}$ is given in Figure 4. In the diagram, following a purple (solid) arrow backwards corresponds to the element r^{-1}.

[3] Cayley diagrams are named after their inventor Arthur Cayley, a nineteenth century British mathematician.

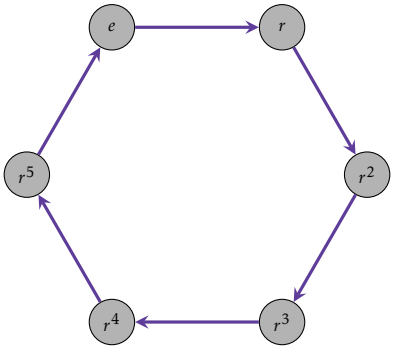


Figure 4: Cayley diagram for R_6 with generating set $\{r\}$.

Example 1.108. The Cayley diagram for the group D_3 with generating set $\{r, s\}$ is given in Figure 5. Notice that we labeled the lower right corner of the Cayley diagram with the word r^2s. This means that we first followed a orange (dashed) arrow out of e and then two purple (solid) arrows. However, we could also get to this vertex by first doing a purple (solid) arrow out of e followed by a orange (dashed) arrow. So, we could also have labeled this vertex with the word sr. The upshot is that the diagram exhibits the relation $r^2s = sr$. Notice that this relation is true no matter where we start in the diagram!

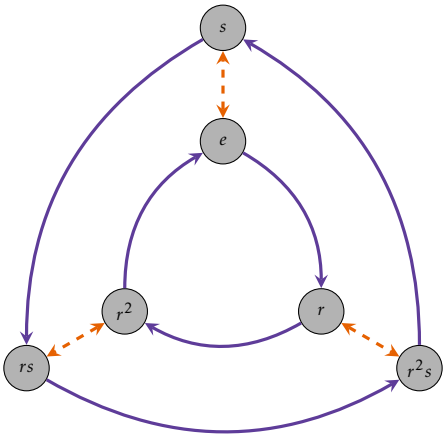


Figure 5: Cayley diagram for D_3 with generating set $\{r, s\}$.

Problem 1.109. Construct a Cayley diagram for each of the following groups using the specified generating set.

(a) S_2 with generating set $\{s\}$

(b) R_4 with generating set $\{r\}$

(c) V_4 with generating set $\{v, h\}$

(d) D_3 with generating set $\{s, s'\}$

(e) S_3 with generating set $\{s_1, s_2\}$

(f) D_4 with generating set $\{r, s\}$

(g) D_4 with generating set $\{s, sr\}$

Problem 1.110. Consider two light switches on a wall side by side. Let ℓ_1 be the action that toggles the position of left light switch and let ℓ_2 be the action that toggles the position of right light switch. Define $\text{Light}_2 := \langle \ell_1, \ell_2 \rangle$. Draw the Cayley diagram for Light_2 using the generating set $\{\ell_1, \ell_2\}$.

Problem 1.111. Consider three light switches on a wall side by side. Let ℓ_1 be the action that toggles the position of left light switch, let ℓ_2 be the action that toggles the position of middle light switch, and let ℓ_3 be the action that toggles the position of middle light switch. Define $\text{Light}_3 := \langle \ell_1, \ell_2, \ell_3 \rangle$. Draw the Cayley diagram for Light_3 using the generating set $\{\ell_1, \ell_2, \ell_3\}$.

Problem 1.112. Consider two coins sitting side by side. Let s be the action that swaps the positions of the two coins and let t be the action that flips over the left coin. Define $\text{Coin}_2 := \langle s, t \rangle$. Draw the Cayley diagram for Coin_2 using the generating set $\{s, t\}$.

Not only are Cayley diagrams visually appealing, but they provide a map for the group in question. That is, they provide a method for navigating the group. Following sequences of arrows tells us how to achieve a net action. However, each Cayley diagram very much depends on the set of generators that are chosen to generate the group. If we change the generating set, we may end up with a very different looking Cayley diagram. For example, compare the Cayley diagram for D_3 that you constructed in Problem 1.109(d) with the one in Example 1.108. Similarly, compare the Cayley diagrams for D_4 that you constructed in Parts (f) and (g) of Problem 1.109.

Problem 1.113. Consider the group $(\mathbb{Z}, +)$.

(a) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{1\}$.

(b) Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{-1\}$. How does this diagram compare to the one in part (a)?

(c) It turns out that $\mathbb{Z} = \langle 2, 3 \rangle$. Construct a portion of the Cayley diagram for $(\mathbb{Z}, +)$ with generating set $\{2, 3\}$.

Problem 1.114. Assume G is a group. Suppose that S and S' are two different sets that generate G. If you draw the Cayley diagram for G using S and then draw the Cayley diagram for G using S', what features of the two graphs are the same and which are potentially different?

Problem 1.115. Consider the diagram given in Figures 6. Explain why this diagram is not the Cayley diagram for a group.

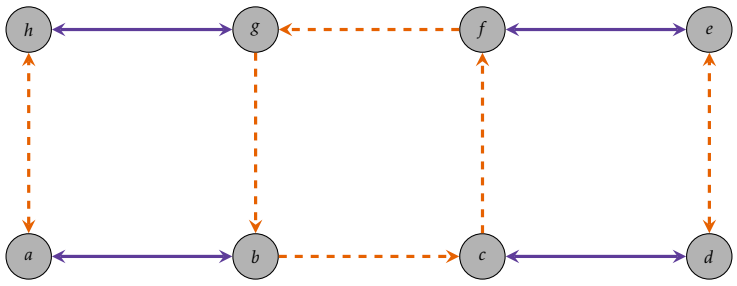


Figure 6: Example of a diagram that is not a Cayley diagram for a group.

Problem 1.116. Suppose G is a group with generating set S and consider the corresponding Cayley diagram. Prove each of the following.

(a) For every $g \in G$ and $s \in S$, there is exactly one arrow with color c_s pointing from $s^{-1}g$ to g and exactly one arrow with color c_s pointing from g to sg.

(b) The Cayley diagram for G with generating set S is connected. That is, for every pair of vertices g and h, there is a path of forward or backward arrows connecting g and h.

(c) Suppose G is a *finite* group and $s \in S$. If we follow a sequence of (forward) arrows of color c_s out of e, we eventually end up back at e after a finite number of steps.

(d) Every relation involving the generators is realized as a sequence of arrows from a vertex in the Cayley diagram back to the same vertex. Moreover, the sequence is independent of starting vertex. Loosely speaking, this says that every local pattern holds globally in the Cayley diagram.

Problem 1.117. Suppose S is a generating set for a group G. Can you determine whether S is a minimal generating set using the Cayley diagram for G with generating set S?

Problem 1.118. Suppose $\{g_1,\dots,g_n\}$ is a generating set for a group G.

(a) Explain why $\{g_1^{-1},\dots,g_n^{-1}\}$ is also a generating set for G.

(b) How does the Cayley diagram for G with generating set $\{g_1,\dots,g_n\}$ compare to the Cayley diagram with generating set $\{g_1^{-1},\dots,g_n^{-1}\}$?

Problem 1.119. Suppose G is an abelian group with generating set S and consider the corresponding Cayley diagram.

(a) If $s,t \in S$, then what relationship must be true about the corresponding arrows?

(b) Is the converse of your claim in part (a) true? That is, if every pair of arrows in the Cayley diagram for G has the property you stated above, will the group be abelian?

Let's introduce a group we haven't seen yet. Define the **quaternion group** to be the group $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ having the Cayley diagram with generating set $\{i,j,-1\}$ given in Figure 7. In this case, 1 is the identity of the group.

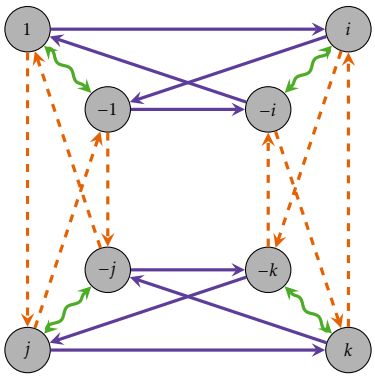


Figure 7: Cayley diagram for Q_8 with generating set $\{-1,i,j\}$.

Notice that I didn't mention what the actions actually do. For now, let's not worry about that. The relationship between the arrows and vertices tells us everything we need to know. Also, let's take it for granted that Q_8 actually is a group.

Problem 1.120. Consider the Cayley diagram for Q_8 given in Figure 7.

(a) Which arrows correspond to which generators in our Cayley diagram for Q_8?

(b) What is i^2 equal to? That is, what element of $\{1,-1,i,-i,j,-j,k,-k\}$ is i^2 equal to? How about i^3, i^4, and i^5?

(c) What are j^2, j^3, j^4, and j^5 equal to?

(d) What is $(-1)^2$ equal to?

(e) What is ij equal to? How about ji?

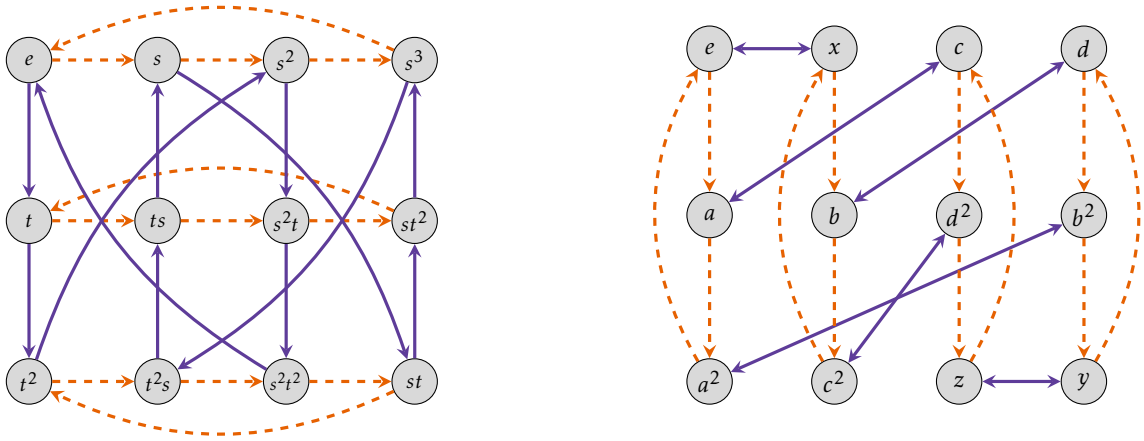
(f) Can you determine what k^2 and ik are equal to?

(g) Can you identify a generating set consisting of only two elements? Can you find more than one?

(h) What subgroups of Q_8 can you visually witness in the Cayley diagram in Figure 7?

(i) Find a subgroup of Q_8 that is not easily seen in the Cayley diagram in Figure 7.

Problem 1.121. The Cayley diagrams of two groups of order 12 are shown below.



(a) Create a group table for each group. For consistency, please order the elements in the first group by $e, t, t^2, s, ts, t^2s, s^2, s^2t, s^2t^2, s^3, st^2, st$ and those in second by $e, x, y, z, a, b, c, d, a^2, b^2, c^2, d^2$.)

(b) Find the inverse of each element.

(c) Find the order of each element in each group.

(d) Find a presentation for each group.

(e) Squint your eyes. Do you see any patterns in these tables?

Problem 1.122. Consider the groups given by the following presentations:

(a) $G_1 = \langle g, h \mid h^2 = e, gh = hg \rangle$

(b) $G_2 = \langle g, h \mid h^2 = e, gh = hg^{-1} \rangle$

(c) $G_3 = \langle g, h \mid gh = hg \rangle$

(d) $G_4 = \langle g, h \mid g^2 = e, h^2 = e, gh = hg \rangle$

(e) $G_5 = \langle g, h \mid g^2 = e, h^2 = e \rangle$

(f) $G_6 = \langle g, h \mid \rangle$ (no relations!)

Draw the Cayley diagram for each group with the specified generating set. If the group is finite, draw the whole diagram. If the group is infinite, draw a portion of the diagram. At least one of these groups provides a presentation for the **infinite dihedral group**, which we have not officially defined. Can you take a guess which one(s)?

1.9 Lagrange's Theorem

The goal of this section is to prove Lagrange's Theorem, which states that for finite groups the order of an element divides the order of the group. We begin with defining a relation on a group that depends on a subgroup.

Let G be a group and let $H \leq G$. Define $\sim$ on G via

$$a \sim b \text{ if and only if } b = ah \text{ for some } h \in H.$$

Problem 1.123. Prove that $\sim$ is an equivalence relation on G.

Since $\sim$ is an equivalence relation, the corresponding equivalence classes form a partition of G. If $a \in G$, then the equivalence class containing a is given by

$$[a] = \{b \in G \mid a \sim b\}.$$

The next problem provides a nice description for $[a]$.

Problem 1.124. Let G be a group and let $H \leq G$. Prove that $[a] = aH := \{ah \mid h \in H\}$.

In the previous problem, the set aH is called a **left coset**. Note that if $a \notin H$, then $aH \neq H$. In particular, if $a \notin H$, then aH is not a subgroup of G. We will explore cosets in more detail in a later section.

Problem 1.125. Let G be a group, $H \leq G$, and $a \in G$. Define $\phi : H \to aH$ via $\phi(h) = ah$. Prove that ϕ is a bijection.

It follows immediately from the previous problem that all of the left cosets of H are the same cardinality as H. In other words $\#(aH) = |H|$ for all $a \in G$, where $\#(aH)$ denotes the cardinality of aH. Note that everything works out just fine even if H has infinite order.

We're finally ready to state Lagrange's Theorem, which is named after the Italian born mathematician Joseph Louis Lagrange. It turns out that Lagrange did not actually prove the theorem that is named after him. The theorem was actually proved by Carl Friedrich Gauss in 1801.

Problem 1.126 (Lagrange's Theorem)**.** Prove that if G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

This simple sounding theorem is extremely powerful. One consequence is that groups and subgroups have a fairly rigid structure. Suppose G is a finite group and let $H \leq G$. Since G is finite, there must be a finite number of distinct left cosets, say $H, a_2H, \ldots, a_nH$. By earlier discussion, we know that each of these cosets has the same cardinality. In particular, Lagrange's Theorem implies that for each $i \in \{1, \ldots, n\}$, $|a_iH| = |G|/n$, or equivalently $n = |G|/|a_iH|$. This is depicted in Figure 8, where each rectangle represents a coset and we've labeled a single coset representative in each case.

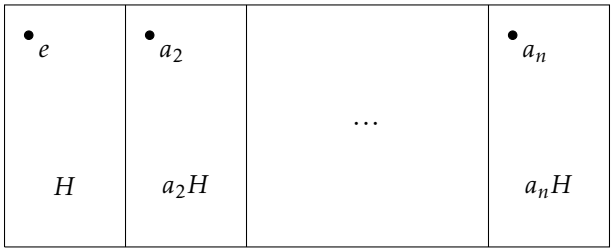


Figure 8: Left cosets as a partition of G into equal size blocks.

One important consequence of Lagrange's Theorem is that it narrows down the possible sizes for subgroups.

Problem 1.127. Suppose G is a group of order 48. What are the possible orders for subgroups of G?

Lagrange's Theorem tells us what the possible orders of a subgroup are, but if $k \in \mathbb{N}$ is a divisor of the order of a group, it does not guarantee that there is a subgroup of order k. It's not too hard to show that the converse of Lagrange's Theorem is true for cyclic groups. However, it's not true, in general. We'll discover a counterexample in a later section.

The next problem is a corollary of Lagrange's Theorem.

Problem 1.128. Prove that if G is a finite group and $a \in G$, then $|a|$ divides $|G|$.

The converse to the previous problem is not true either.

Problem 1.129. Provide an example of a finite group G and a divisor $k \in \mathbb{N}$ of $|G|$ such that G does not have an element of order k.

Problem 1.130. Suppose G is a group such that $|G| = p$, where p is prime. Prove that G is cyclic.

1.10 More on 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. If there exists $g \in G$ such that $G = \langle g \rangle$, then we say that G is a **cyclic group**.

Problem 1.131. Prove that if G is a group such that G has no proper nontrivial subgroups, then G is cyclic.

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

Theorem 1.132 (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 $0 \leq r < n$.

Problem 1.133. Suppose G is a group and let $g \in G$. Prove that the subgroup $\langle g \rangle$ is finite if and only if there exists $n \in \mathbb{N}$ such that $g^n = e$. It immediately follows that if G is a finite group, then for all $g \in G$, there exists $n \in \mathbb{N}$ such that $g^n = e$.

Problem 1.134. Suppose G is a group and let $g \in G$ such that $\langle g \rangle$ is a finite group. Prove that 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. Note that the previous problem together with the Well-Ordering Principle guarantees the existence of a smallest positive integer n such that $g^n = e$.

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

Problem 1.135. Prove that if G is a group and $g \in G$ such that $\langle g \rangle$ is a finite subgroup, then the order of g is the smallest positive integer n such that $g^n = e$.

Problem 1.136. 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.

Problem 1.137. Suppose G is a group and let $g \in G$. Prove that the subgroup $\langle g \rangle$ is infinite if and only if each g^k is distinct for all $k \in \mathbb{Z}$.

Problem 1.138. Suppose G is a cyclic group with generator $g \in G$.

(a) If G is finite, what conclusions can you make about Cayley diagram for G with generating set $\{g\}$?

(b) If G is infinite, what conclusions can you make about Cayley diagram for G with generating set $\{g\}$?

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

Problem 1.139. Suppose G is a group and let $g \in G$ such that $|g| = n$. Prove that $g^i = g^j$ if and only if n divides $i - j$. It immediately follows that $g^i = g^j$ if and only if $i \equiv j \pmod{n}$.

Problem 1.140. Suppose G is a group and let $g \in G$ such that $|g| = n$. Prove that if $g^k = e$, then n divides k.

Problem 1.141. Suppose G is a cyclic group. Prove that if $H \leq G$, then H is also cyclic.

It turns out that for proper subgroups, the converse of Problem 1.141 is not true.

Problem 1.142. Provide an example of a group G such that G is not cyclic, but all proper subgroups of G are cyclic.

One implication of the previous problem is that the subgroups of $\mathbb{Z}$ are precisely the groups $n\mathbb{Z} = \langle n \rangle$ for $n \in \mathbb{Z}$.

Problem 1.143. Prove that if G is a finite cyclic group with generator g such that $|G| = n$, then for all $m \in \mathbb{Z}$, $|g^m| = \dfrac{n}{\gcd(n, m)}$.

Problem 1.144. Prove that 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 $\gcd(m, n) = \gcd(k, n)$. Use Problem 1.143 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.

Suppose G is a finite cyclic group with generator g such that $|G| = n$. It follows from Problem 1.144 that $\langle g \rangle = \langle g^k \rangle$ 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 1.145. 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?

Problem 1.146. Consider $\mathbb{Z}/18\mathbb{Z}$.

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

(b) Draw the subgroup lattice for $\mathbb{Z}/18\mathbb{Z}$. For each subgroup, list the elements of the corresponding set. Moreover, circle the elements in each subgroup that individually generate that subgroup.

Problem 1.147. Suppose G is a finite cyclic group of order n and let k be a positive divisor of n. Prove that there is exactly one subgroup of order k for every positive divisor k of n.

Problem 1.148. Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. What if G is an abelian group, not necessarily cyclic, of order n?

2 Group Homomorphisms

2.1 Isomorphisms

As we have been exploring various groups, I'm sure you've noticed that some groups seem to look and behave the same.

Suppose G is a finite group and consider the group table for G. A **coloring** for the group table is an assignment of a unique color to each element of the group. For example, Figure 9 depicts a coloring for the group table of V_4.

$\circ$	e	v	h	vh
e	e	v	h	vh
v	v	e	vh	h
h	h	vh	e	v
vh	vh	h	v	e

Figure 9: A coloring for the group table of V_4.

We say that two finite groups have an **identical table coloring**, if we can arrange the rows and columns of each table and choose colorings for each table so that the pattern of colors is the same for both tables. Clearly, this is only possible if the two groups have the same order.

Problem 2.1. Determine whether V_4 and Light_2 (see Problem 1.110) have an identical table coloring.

Since a group table encodes all of the information about a group, if two groups have an identical table coloring, then the two groups have the same exact structure while the elements may have different names. In particular, if two finite groups G_1 and G_2 have an identical table coloring, then

the product of corresponding elements yields the corresponding result.

This is the essence of what it means for two groups to have the same structure.

Let's try to make this a little more precise. Suppose $(G_1,*)$ and $(G_2,\odot)$ are two finite groups that have an identical table coloring and let $x_1, y_1 \in G_1$. Then these two elements have corresponding elements in the group table for G_2, say x_2 and y_2, respectively. In other words, x_1 and x_2 have the same color while y_1 and y_2 have the same color. Since G_1 is closed under its binary operation $*$, there exists $z_1 \in G_1$ such that $z_1 = x_1 * y_1$. But then there must exist a $z_2 \in G_2$ such that z_2 has the same color as z_1. What must be true of $x_2 \odot y_2$? Since the two tables exhibit the same color pattern, it must be the case that $z_2 = x_2 \odot y_2$. This is what it means for the product of corresponding elements to yield the corresponding result. Figure 10 illustrates this phenomenon for group tables.

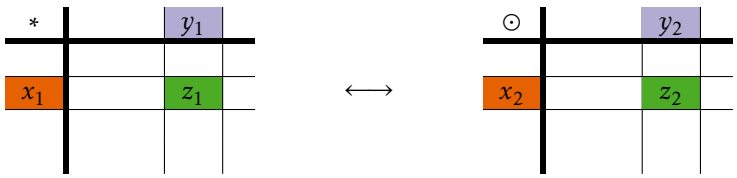


Figure 10:

We can describe the identical table matching between G_1 and G_2 using a function. Let $\phi : G_1 \to G_2$ be the one-to-one and onto function that maps elements of G_1 to their corresponding elements in G_2. Then $\phi(x_1) = x_2$, $\phi(y_1) = y_2$, and $\phi(z_1) = z_2$. Since $z_2 = x_2 \odot y_2$, we obtain

$$\phi(x_1 * y_1) = \phi(z_1) = z_2 = x_2 \odot y_2 = \phi(x_1) \odot \phi(y_1).$$

In summary, it must be the case that

$$\phi(x_1 * y_1) = \phi(x_1) \odot \phi(y_1).$$

We are now prepared to state a formal definition of what it means for two groups to be isomorphic.

Definition 2.2. Let $(G_1, *)$ and $(G_2, \odot)$ be two groups. Then G_1 is **isomorphic** to G_2, written $G_1 \cong G_2$, if and only if there exists a one-to-one and onto function $\phi : G_1 \to G_2$ such that

$$\phi(x * y) = \phi(x) \odot \phi(y). \tag{1}$$

The function ϕ is referred to as an **isomorphism**. Equation 1 is often referred to as the **homomorphic property**.

Problem 2.3. Consider the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \cdot)$, where $\mathbb{R}^+$ is the set of positive real numbers. It turns out that these two groups are isomorphic, but this would be difficult to discover using our previous techniques because the groups are infinite. Define $\phi : \mathbb{R} \to \mathbb{R}^+$ via $\phi(r) = e^r$ (where e is the natural base, not the identity). Prove that ϕ is an isomorphism.

Problem 2.4. Show that the groups $(\mathbb{Z}, +)$ and $(2\mathbb{Z}, +)$ are isomorphic.

Perhaps one surprising consequence of the previous problem is that when dealing with infinite groups, a group may have a proper subgroup that it is isomorphic to. Of course, this never happens with finite groups.

Problem 2.5. Suppose $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$. Prove each of the following:

(a) $|g| = |\phi(g)|$ for all $g \in G$.

(b) G_1 and G_2 have the same number of elements of order n for each $n \in \mathbb{N}$.

(c) G_1 is abelian if and only if G_2 is abelian.

Problem 2.6. For each pair of groups given below, explain why the groups are not isomorphic to each other.

(a) D_4 and Q_8

(b) D_4 and Light_3

(c) $\mathbb{R}$ and $\mathbb{Q}$ (both additive groups)

(d) $\mathbb{Z}$ and $\mathbb{Q}$ (both additive groups)

(e) $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ (both multiplicative groups)

Problem 2.7. Prove that any two cyclic groups of the same order are isomorphic. Be sure to handle both the finite and infinite cases. In the finite case, do you need to worry about your proposed function being well defined?

It turns out that "isomorphic" ($\cong$) determines an equivalence relation on the class of all possible groups. The next three problems justify that $\cong$ is reflexive, symmetric, and transitive.

Problem 2.8. Prove that if G is a group, then the identity map from G to G is an isomorphism.

Problem 2.9. Prove that if $\phi : G_1 \to G_2$ is an isomorphism from the group $(G_1, *)$ to the group $(G_2, \odot)$, then the function $\phi^{-1} : G_2 \to G_1$ is an isomorphism.

Problem 2.10. Prove that if $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ are isomorphisms from the groups $(G_1, *)$ to $(G_2, \odot)$ and $(G_2, \odot)$ to $(G_3, \star)$, respectively, then the composite function $\psi \circ \phi$ is an isomorphism of G_1 and G_3.

In light of the previous problem, we now know that if $\mathcal{G}$ is any nonempty collection of groups, then the relation $\cong$ is an equivalence relation on $\mathcal{G}$.

Mathematicians love to classify things. In particular, mathematicians want to classify groups. One can think of this pursuit as a taxonomy of groups. In order to simplify the task, one can classify isomorphism classes (i.e., the equivalence classes determined by $\cong$) instead of classifying groups individually. If two groups are isomorphic, then we say that the groups are **the same up to isomorphism**. If there are k isomorphism classes of order n, then we say that there are k **groups of order** n **up to isomorphism**. A natural question to ask is: how many groups are there of order n?

Certainly, there is only one group of order 1 up to isomorphism. It follows from Problems 1.130 and 2.7 that up to isomorphism, there is only one group of order p if p is prime.

It turns out that up to isomorphism, there are two groups of order 4. In particular, every group of order 4 is isomorphic to R_4 if cyclic or isomorphic to V_4 if not cyclic. This isn't too hard to prove by examining all the possible ways one could fill out a group table for a group of order 4.

How about order 6? We've seen four groups of order 6, namely $\mathbb{Z}/6\mathbb{Z}$, R_6, D_3, and S_3. Since $\mathbb{Z}/6\mathbb{Z}$ and R_6 are both cyclic groups of order 6, these two groups are isomorphic. We know that neither D_3 nor S_3 are cyclic, so neither of these groups below to the same isomorphism class as R_6. Below, we will justify that $D_3 \cong S_3$. This implies that there are at least two groups up to isomorphism of order 6. But are there others? It turns out that the answer is no, but why?

We've encountered several groups of order 8, namely D_4, Coin_2, Q_8, R_8, and Light_3. Of these, only D_4 and Coin_2 are isomorphic (see Problem 2.11). Thus, there are at least four groups up to isomorphism of order 8. Are these the only isomorphism types? It turns out that there are five groups of order 8 up to isomorphism. We will encounter the fifth isomorphism type later.

You can also utilize Cayley diagrams to determine whether two finite groups are isomorphic. If two groups G_1 and G_2 have generating sets T_1 and T_2 such that we can color the edges of the corresponding Cayley diagrams so that the diagrams are identical up to relabeling of the vertices, then we say that there is a **matching** between G_1 and G_2 (or more formally, the Cayley diagrams are isomorphic as directed and colored graphs).

For example, Figure 11 makes it easy to describe a matching between D_3 and S_3. It's important to emphasize that the existence of a matching between two groups depends on our choice of generating set! If two Cayley diagrams do not look alike, it does not immediately imply that there is not a matching between the groups since it might be the case that choosing different generating sets for the two groups leads to a matching. It turns out that two groups G_1 and G_2 are isomorphic if and only if there exists choices of generating sets T_1 and T_2 for G_1 and G_2, respectively, such that there is a matching between the corresponding Cayley diagrams. Do you see why this is true?

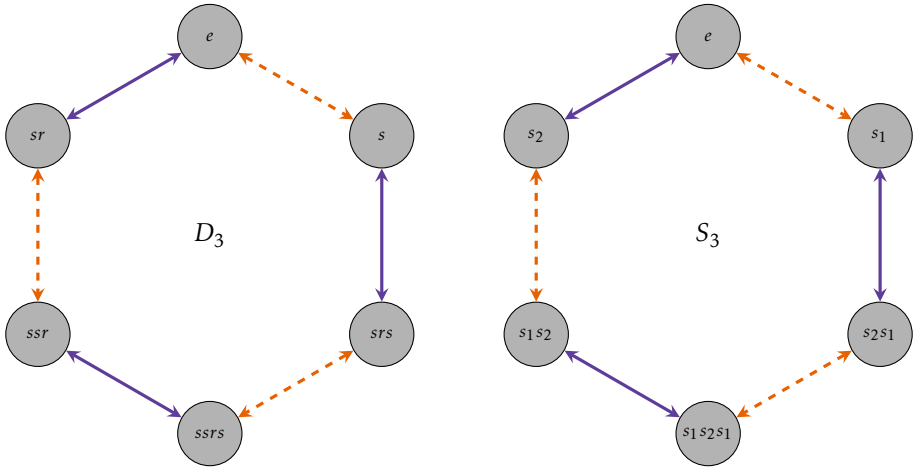


Figure 11: Cayley diagrams for D_3 and S_3 with generating sets $\{s, sr\}$ and $\{s_1, s_2\}$, respectively.

Problem 2.11. Explain why D_4 and Coin_2 are isomorphic.

Problem 2.12. Determine which of the following groups are isomorphic to each other: S_2, $\langle -1 \rangle$ in Q_8, R_3, R_4, V_4, Light_2, $\langle i \rangle$ in Q_8, $\langle sr, sr^3 \rangle$ in D_4, R_5, R_6, D_3, S_3, R_7, R_8, D_4, Coin_2, Q_8, Light_3.

Problem 2.13. What claims can be made about the subgroup lattices of two groups that are isomorphic? What claims can be made about the subgroup lattices of two groups that are not isomorphic? What claims can be made about two groups if their subgroup lattices look nothing alike?

2.2 Homomorphisms

Recall that a group isomorphism is a bijection between two groups that satisfies the homomorphic property. What if we drop the one-to-one and onto requirements?

Definition 2.14. Let $(G_1, *)$ and $(G_2, \odot)$ be groups. A function $\phi : G_1 \to G_2$ is a **homomorphism** if and only if ϕ satisfies the homomorphic property:

$$\phi(x * y) = \phi(x) \odot \phi(y)$$

for all $x, y \in G_1$. At the risk of introducing ambiguity, we will usually omit making explicit reference to the binary operations and write the homomorphic property as

$$\phi(xy) = \phi(x)\phi(y).$$

Group homomorphisms are analogous to linear transformations on vector spaces that one encounters in linear algebra.

Problem 2.15. Define $\phi : \mathbb{Z}/3\mathbb{Z} \to D_3$ via $\phi(\overline{k}) = r^k$. Prove that ϕ is a well-defined homomorphism and then determine whether ϕ is one-to-one or onto. Also, try to draw a picture of the homomorphism in terms of Cayley diagrams.

There is always at least one homomorphism between two groups.

Problem 2.16. Let G_1 and G_2 be groups. Define $\phi : G_1 \to G_2$ via $\phi(g) = e_2$ (where e_2 is the identity of G_2). This function is often referred to as the **trivial homomorphism** or the 0-**map**. Prove that ϕ is a homomorphism.

Problem 2.17. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Prove each of the following.

(a) If e_1 and e_2 are the identity elements of G_1 and G_2, respectively, then $\phi(e_1) = e_2$.

(b) For all $g \in G_1$, we have $\phi(g^{-1}) = [\phi(g)]^{-1}$.

(c) For all $g \in G_1$ and $n \in \mathbb{Z}$, we have $\phi(g^n) = \phi(g)^n$.

(d) If $H \leq G_1$, then $\phi(H) \leq G_2$, where

$$\phi(H) := \{y \in G_2 \mid \text{there exists } h \in H \text{ such that } \phi(h) = y\}.$$

Note that $\phi(H)$ is the **image** of H. A special case is when $H = G_1$. Notice that ϕ is onto exactly when $\phi(G_1) = G_2$.

(e) If ϕ is injective, then $G_1 \cong \phi(G_1)$.

The following theorem is a consequence of Lagrange's Theorem.

Problem 2.18. Let G_1 and G_2 be groups such that G_2 is finite and let $H \leq G_1$. Prove that if $\phi : G_1 \to G_2$ is a homomorphism, then $|\phi(H)|$ divides $|G_2|$.

The next theorem tells us that under a homomorphism, the order of the image of an element must divide the order of the pre-image of that element.

Problem 2.19. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Prove that if $g \in G_1$ such that $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.

Every homomorphism has an important subset of the domain associated with it.

Definition 2.20. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. The **kernel** of ϕ is defined via

$$\ker(\phi) := \{g \in G_1 \mid \phi(g) = e_2\} = \phi^{-1}(\{e_2\}).$$

The kernel of a homomorphism is analogous to the null space of a linear transformation of vector spaces.

Problem 2.21. Identify the kernel and image for the homomorphism given in Problem 2.15.

Problem 2.22. What is the kernel of a trivial homomorphism.

Problem 2.23. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Prove each of the following.

(a) $\ker(\phi) \leq G_1$.

(b) $N_{G_1}(\ker(\phi)) = G_1$.

Part (b) of the previous problem says that the kernel of every homomorphism is fixed setwise under the action of conjugation by every element of G. The next theorem tells us that two elements in the domain of a group homomorphism map to the same element in the codomain if and only if they are in the same left (or right) coset of the kernel.

Problem 2.24. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Prove that $\phi(a) = \phi(b)$ if and only if $a \in b\ker(\phi)$.

One consequence of Problem 2.24 is that if the kernel of a homomorphism has order k, then the homomorphism is k-to-1 (since left cosets of $\ker(\phi)$ always have the same cardinality; see Problem 1.125). That is, every element in the range has exactly k elements from the domain that map to it. In particular, each of these collections of k elements corresponds to a left coset of the kernel.

Problem 2.25. Suppose $\phi : \mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ is a group homomorphism such that $\ker(\phi) = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$. If $\phi(\overline{13}) = \overline{8}$, determine all elements that ϕ maps to $\overline{8}$.

The next result is a special case of Problem 2.24.

Problem 2.26. Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Prove that ϕ is one-to-one if and only if $\ker(\phi) = \{e_1\}$, where e_1 is the identity in G_1.

Let G_1 and G_2 be groups and suppose $\phi : G_1 \to G_2$ is a homomorphism. Given a generating set for G_1, the homomorphism ϕ is uniquely determined by its action on the generating set for G_1. In particular, if you have a word for a group element written in terms of the generators, just apply the homomorphic property to the word to find the image of the corresponding group element. However, it is important to point out that you can't just map the generators about willy nilly and expect to get a homomorphism.

Problem 2.27. Let $\phi : Q_8 \to V_4$ be the map satisfying $\phi(i) = h$ and $\phi(j) = v$. It turns out that ϕ is a group homomorphism.

(a) Find $\phi(1)$, $\phi(-1)$, $\phi(k)$, $\phi(-i)$, $\phi(-j)$, and $\phi(-k)$.

(b) Find $\ker(\phi)$.

(c) Draw a picture of this homomorphism in terms of Cayley diagrams?

(d) There is a natural bijection from the collection of left cosets of $\ker(\phi)$ to the image of ϕ. Describe this map.

The next four problems will be a good test of our current understanding.

Problem 2.28. Let G be a group. Prove that the map $\phi : G \to G$ defined via $\phi(g) = g^2$ is a group homomorphism if and only if G is abelian.

Problem 2.29. Find a non-trivial homomorphism from $\mathbb{Z}/10\mathbb{Z}$ to $\mathbb{Z}/6\mathbb{Z}$.

Problem 2.30. Find all non-trivial homomorphisms from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/6\mathbb{Z}$.

Problem 2.31. Prove that the only homomorphism from D_3 to $\mathbb{Z}/3\mathbb{Z}$ is the trivial homomorphism.

3 Automorphisms

Recall that two groups G_1 and G_2 are isomorphic if there exists a bijection $\phi : G_1 \to G_2$ that satisfies the homomorphic property. In Problem 2.8, we learned that a group G is isomorphic to itself by using the identity map. However, it is possible that there are additional isomorphisms from a group to itself.

Definition 3.1. Let G be a group. If $\phi : G \to G$ is an isomorphism, then we say that ϕ is an **automorphism** of G. The collection of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

By Problem 2.8, we know that $\mathrm{Aut}(G)$ is always nonempty.

Problem 3.2. Prove that for each $k \in \mathbb{Q} \setminus \{0\}$, the map $\phi_k : \mathbb{Q} \to \mathbb{Q}$ defined via $\phi_k(q) = kq$ is an automorphism of $\mathbb{Q}$.

Problem 3.3. Let G be an abelian group and let $k \in \mathbb{Z}$.

(a) Prove the map $\phi_k : G \to G$ defined via $\phi_k(g) = g^k$ is a homomorphism.

(b) Prove that if $k = -1$, the homomorphism ϕ_k is actually an automorphism of G.

(c) Are there other situations under which ϕ_k will be an automorphism?

Problem 3.4. Let G be a group. Prove that $\mathrm{Aut}(G)$ is a group under function composition. We call $\mathrm{Aut}(G)$ the **automorphism group** of G.

Suppose G is a group and let $g \in G$. Define $\phi_g : G \to G$ via $\phi_g(x) = gxg^{-1}$. The map ϕ_g is called **conjugation** by g.

Problem 3.5. Prove that if G is a group and $g \in G$, then conjugation by g is an automorphism of G.

Problem 3.6. Prove that if H is any subgroup of G and $g \in G$, then $H \cong gHg^{-1}$.

Problem 3.5 tells us that conjugation by any element in G is always an element of $\mathrm{Aut}(G)$. Let $\mathrm{Inn}(G)$ denote the subset of $\mathrm{Aut}(G)$ consisting of all automorphisms of G that are equal to conjugation by g for some $g \in G$. Each conjugation is sometimes called an **inner automorphism** of G, which is where the notation $\mathrm{Inn}(G)$ comes from.

Problem 3.7. Prove that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

Problem 3.8. Explain why G is abelian if and only if $\mathrm{Inn}(G)$ is trivial.

Problem 3.9. Prove one of the following.

(a) $\mathrm{Inn}(Q_8) \cong V_4$

(b) $\mathrm{Inn}(D_4) \cong V_4$

Problem 3.10. Let G be a finite group and let $\sigma \in \mathrm{Aut}(G)$ such that $\sigma(g) = g$ if and only if $g = e$ (i.e., the identity is the only element fixed by σ). Prove that if σ^2 is the identity map from G to G, then G must be abelian. *Hint:* Show that every element in G is of the form $x^{-1}\sigma(x)$ and apply σ.

In preparation for the next problem, define $U_n := \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(n,k) = 1\}$. The set is also sometimes denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$. For example, $U_{12} = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. It turns out that the set U_n is an abelian group under multiplication mod n. We will take this fact for granted. Notice that the order of U_n is the number of elements from $\{1, 2 \ldots, n-1\}$ that are relatively prime to n. That is, $|U_n|$ is the value of Euler's ϕ-function at n.

Problem 3.11. Let G be a cyclic group of order n. For each $k \in \mathbb{Z}$, define $\sigma_k : G \to G$ via $\sigma_k(x) = x^k$ for all $x \in G$.

(a) Prove that σ_k is an automorphism of G if and only if n and k are relatively prime.

(b) Prove that $\sigma_k = \sigma_m$ if and only if $k \equiv m \pmod{n}$.

(c) Prove that every automorphism of G is equal to σ_k for some $k \in \mathbb{Z}$.

(d) Prove that $\sigma_k \circ \sigma_m = \sigma_{km}$.

(e) Deduce that $\mathrm{Aut}(G)$ is isomorphic to U_n.

Problem 3.12. Prove that $N_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = \mathrm{Aut}(G)$.

4 Symmetric Groups

Recall the groups S_2 and S_3 are the groups that 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.

Recall that a **permutation of a set** A is a bijective function $\sigma : A \to A$. In the special case that $A = \{1, 2, \ldots, n\}$, we let S_n denote the collection of all permutations on $\{1, 2, \ldots, n\}$. We can turn S_n into a group by using composition of permutations. In this case, we call S_n the **symmetric group** on n objects.

Problem 4.1. Prove that $(S_n, \circ)$ is a group such that $|S_n| = n!$.

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 4.2. 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 4.3. 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 4.4. 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 4.5. Given in $\sigma \in S_n$, how do we obtain the cycle decomposition of σ^{-1} from the cycle decomposition for σ?

Computing products in S_n is straightforward as long as you keep in mind that when computing $\sigma \circ \tau$ in S_n, we applty the permutations from *right to left* while reading each cycle from *left to right*!

Example 4.6. Let $\sigma = (1, 2)(3, 4), \tau = (1, 2, 3) \in S_4$. To compute $\sigma \circ \tau$, a natural place to start is by asking where 1 gets sent. Since $\tau(1) = 2$ while $\sigma(2) = 1$, it must be the case that

$$\sigma \circ \tau(1) = \sigma(\tau(1)) = \sigma(2) = 1.$$

So, $\sigma \circ \tau$ maps 1 to itself, which implies that (1) is one cycle in the cycle decomposition of $\sigma \circ \tau$. At this point, we need to start constructing a new cycle. We can consider any value that we have not yet utilized to start a new cycle. Since 2 is the smallest number have not yet used, let's start there. We see that

$$\sigma \circ \tau(2) = \sigma(\tau(2)) = \sigma(3) = 4.$$

Since we are attempting to construct a cycle, we should now consider where $\sigma \circ \tau$ maps 4. We see that

$$\sigma \circ \tau(4) = \sigma(\tau(4)) = \sigma(4) = 3.$$

And finally, we see that

$$\sigma \circ \tau(3) = \sigma(\tau(3)) = \sigma(1) = 2.$$

We can conclude that $(2,4,3)$ is another cycle in the cycle decomposition for $\sigma \circ \tau$. Since all numbers have been accounted for, we obtain $\sigma \circ \tau = (1)(2,4,3) = (2,4,3)$. As expected, the order in which we compose often matters. In this case, we get $\tau \circ \sigma = (1,3,4) \neq \sigma \circ \tau$, which shows that S_4 is not abelian.

From this moment forward, we will suppress $\circ$ and simply write products of permutations using juxtaposition. Just keep in mind that we are always composing from right to left!

Problem 4.7. Let $\alpha = (1,2,3,4,5)$, $\beta = (2,4,3)$, $\sigma = (1,3)(2,5,4)$, and $\gamma = (1,5)$ be permutations in S_5. Compute the cycle decomposition for 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^5

Problem 4.8. Prove that for $n \geq 3$, S_n is non-abelian.

Despite the fact that S_n is non-abelian for $n \geq 3$, there are still situations in which permutations commute.

Problem 4.9. Explain why the product of disjoint cycles commute. Is this the only time permutations commute?

Problem 4.10. What orders occur for permutations in S_4?

Problem 4.11. What is the order of $(1,4,7)$?

Problem 4.12. What is the order of $(1,4,7)(2,5)(3,6,8,9)$?

Problem 4.13. Prove that if $\sigma \in S_n$ such that σ consists of a single k-cycle (ignoring any 1-cycles), then $|\sigma| = k$.

Problem 4.14. Suppose $\sigma \in S_n$ such that σ consists of m disjoint cycles of lengths $k_1, \ldots, k_m$. Prove that $|\sigma| = \operatorname{lcm}(k_1, \ldots, k_m)$.

Problem 4.15. Is the previous theorem true if we do not require the cycles to be disjoint? Justify your answer.

Problem 4.16. Consider the k-cycle $\sigma = (1,2,\ldots,k)$. Prove that σ^i is also a k-cycle if and only if i is relatively prime to k.

Problem 4.17. 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 4.18. 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 4.19. 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 4.20. Consider the arbitrary 2-cycle (i, j) from S_n with $i < j$. Find a way to write this permutation as a product of adjacent 2-cycles.

The previous two problems imply the following result.

Problem 4.21. Consider S_n.

(a) Explain why every permutation in S_n can be written as a product of transpositions.

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

Problem 4.22. Explain why 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 a 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).

Problem 4.23. Prove that the transpositions $(1,2),(1,3),\ldots,(1,n)$ generate S_n.

Problem 4.24. Prove that for $n \geq 3$, $Z(S_n)$ is trivial.

Problem 4.25. Find a subgroup of S_4 that is isomorphic to D_4.

Problem 4.26. Explain why there is not a subgroup of S_4 that is isomorphic to R_6.

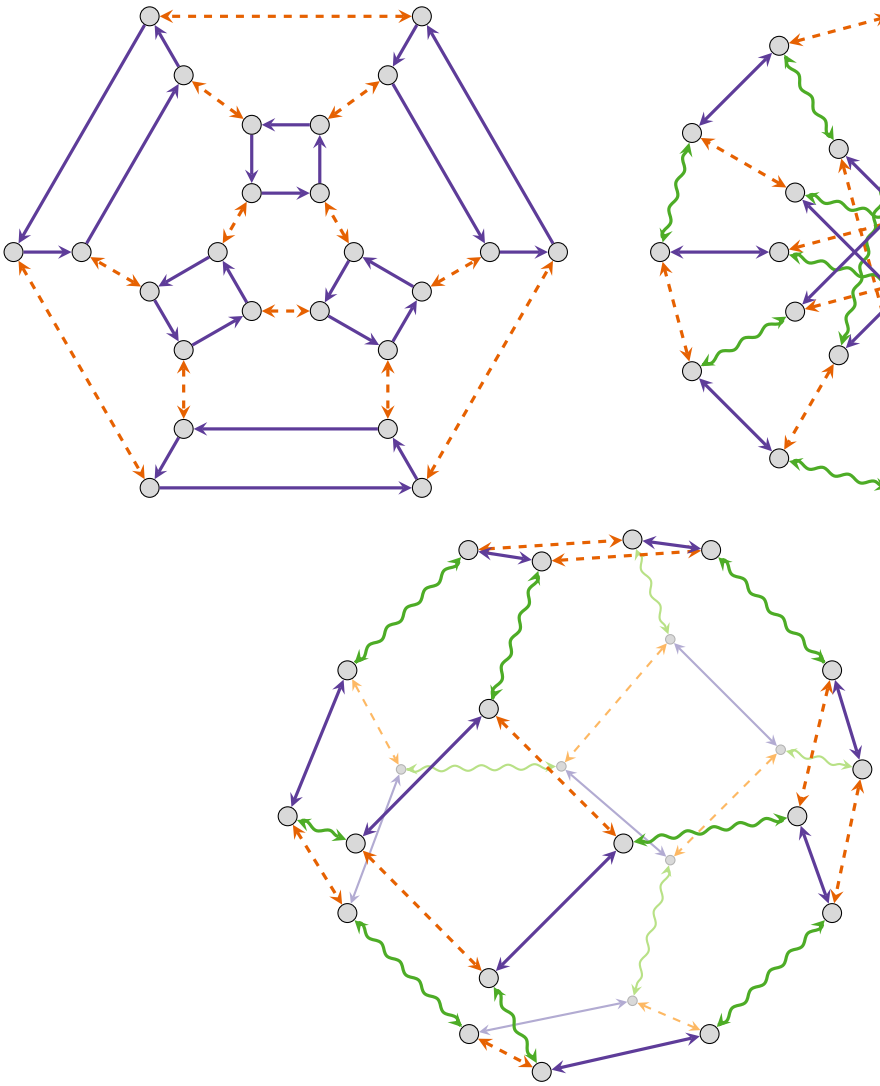
Problem 4.27. Explain why there is not a subgroup of S_4 that is isomorphic to Q_8.

Problem 4.28. Find a subgroup of S_6 that is isomorphic to R_6.

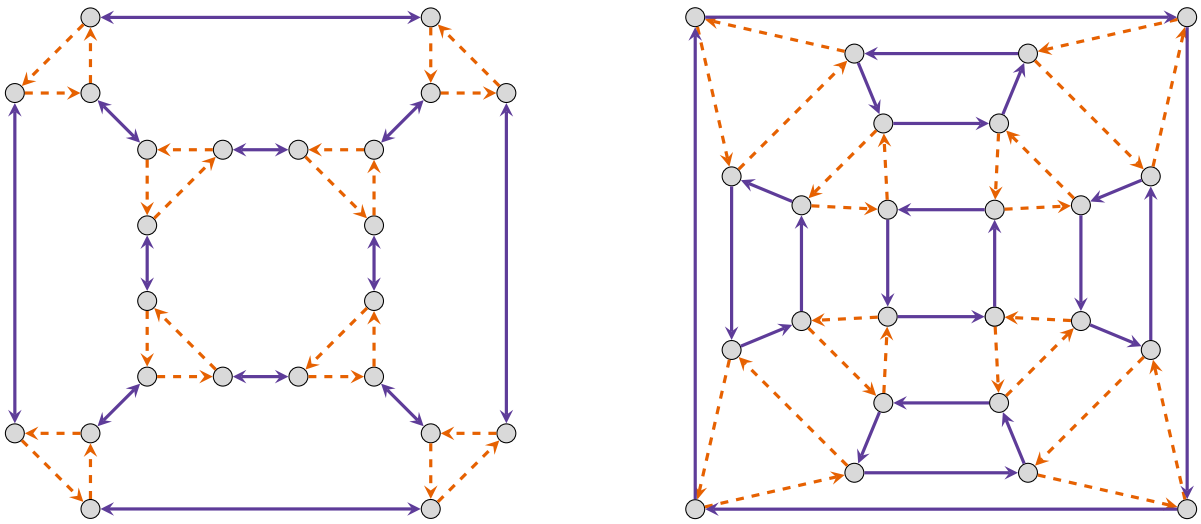
Problem 4.29. It turns out that

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

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. Fun Facts: The top right graph is called the Nauru graph, the bottom graph is drawn on the permutahedron (which is a truncated octahedron).



Problem 4.30. 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.

5 Alternating Groups

In this section, we describe a special subgroup of S_n. To get started, let's play with a few examples.

Problem 5.1. 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.

We include the proof of the following lemma.

Lemma 5.2. 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. □

Use the previous lemma to prove the following result.

Problem 5.3. Prove that 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 5.4. A permutation is **even** (respectively, **odd**) if one of its transposition representations consists of an even (respectively, odd) number of transpositions.

Problem 5.5. Classify all of the permutations in S_4 as even or odd.

Problem 5.6. Determine whether $(1,4,2,3,5)$ is even or odd. How about $(1,4,2,3,5)(7,9)$?

Problem 5.7. Consider the arbitrary k-cycle $(a_1, a_2, \ldots, a_k)$ from S_n (with $k \leq n$). When will this cycle be an odd versus even permutation? Briefly justify your answer.

Problem 5.8. Conjecture a statement about when a permutation will be an even versus odd permutation. Briefly justify your answer.

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

Definition 5.9. 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!

Problem 5.10. Prove that A_n is a subgroup of S_n with order $n!/2$. *Hint:* To show that $|A_n| = n!/2$, 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.

Problem 5.11. Find A_3. What group is A_3 isomorphic to?

Problem 5.12. Prove that the subgroup of A_4 generated by any element of order 2 and any element of order 3 is all of A_4.

Problem 5.13. Find the subgroup lattice for A_4. Is A_4 abelian?

Problem 5.14. Prove that A_n is non-abelian for $n \geq 3$.

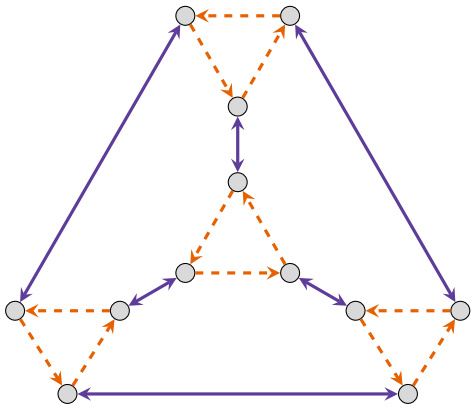
Problem 5.15. What is the order of A_5? Is A_5 abelian?

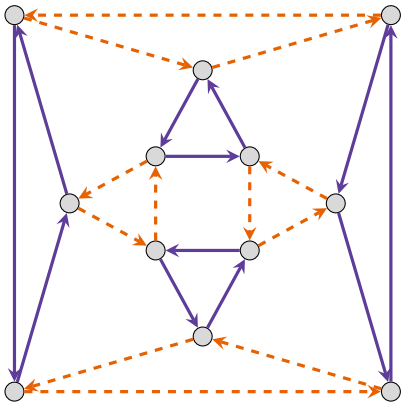
Problem 5.16. What orders of elements occur in S_6 and A_6? What about S_7 and A_7?

Problem 5.17. Does A_8 contain an element of order 15? If so, find one. If not, explain why no such element exists.

Problem 5.18. Identify the even permutations in the Cayley diagrams for S_4 given in Problems 4.29 and 4.30. Notice any nice patterns?

Problem 5.19. 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.

6 Products of Groups

Suppose $(G,*)$ and $(H,\circ)$ are groups. Recall that the Cartesian product of G and H is defined to be

$$G \times H = \{(g,h) \mid g \in G, h \in H\}$$

Define $\star$ on $G \times H$ via $(g_1,h_1) \star (g_2,h_2) = (g_1 * g_2, h_1 \circ h_2)$. This looks fancier than it is. We're just doing the operation of each group in the appropriate component.

Problem 6.1. Prove that if G and H are groups, then $G \times H$ is a group under the operation described above, where:

(i) If e_G and e_H are the identity elements of G and H, respectively, then (e_G, e_H) is the identity element in $G \times H$.

(ii) If $(g,h) \in G \times H$, then $(g,h)^{-1} = (g^{-1}, h^{-1})$.

We refer to $G \times H$ as the **direct product** of the groups G and H. In this case, each of G and H is called a **factor** of the direct product. We often abbreviate $(g_1,h_1) \star (g_2,h_2) = (g_1 * g_2, h_1 \odot h_2)$ by $(g_1,h_1)(g_2,h_2) = (g_1 g_2, h_1 h_2)$. One exception to this is if we are using the operation of addition in each component. For example, consider $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ under the operation of addition mod 4 in the first component and addition mod 2 in the second component. Then

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{2},\overline{0}), (\overline{3},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{1}), (\overline{2},\overline{1}), (\overline{3},\overline{1})\}.$$

In this case, we will use additive notation in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For example, in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ we have

$$(\overline{2},\overline{1}) + (\overline{3},\overline{1}) = (\overline{1},\overline{0}).$$

Moreover, the identity of the group is $(\overline{0},\overline{0})$. As an example, the inverse of $(\overline{1},\overline{1})$ is $(\overline{3},\overline{1})$ since $(\overline{1},\overline{1}) + (\overline{3},\overline{1}) = (\overline{0},\overline{0})$. There is a very natural generating set for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, namely, $\{(\overline{1},\overline{0}), (\overline{0},\overline{1})\}$ since $\overline{1} \in \mathbb{Z}/4\mathbb{Z}$ and $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$ generate $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, respectively. The corresponding Cayley diagram is given in Figure 12.

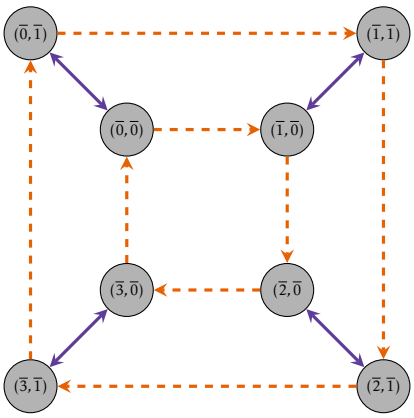


Figure 12: Cayley diagram for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with generating set $\{(\overline{1},\overline{0}), (\overline{0},\overline{1})\}$.

Problem 6.2. Consider the group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Is this group abelian? Is the group cyclic? Determine whether $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to any of D_4, Q_8, R_8, or Light_3.

The upshot of the previous problem is that there are at least five groups of order 8 up to isomorphism. It turns out that there are exactly five groups of order 8 up to isomorphism. In particular, every group of order 8 is isomorphic to one of the following groups:

(a) $\mathbb{Z}/8\mathbb{Z} \cong R_8$,

(b) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

(c) Light_3,

(d) $D_4 \cong \text{Coin}_2$, and

(e) Q_8.

Three of the isomorphism classes correspond to abelian groups while the other two correspond to non-abelian groups. Unfortunately, we will not develop the tools necessary to prove that this classification is complete.

Problem 6.3. For each of the following groups, find a generating set and then construct a Cayley diagram using your generating set.

(a) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(c) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Problem 6.4. Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \text{Light}_2 \cong V_4$.

Problem 6.5. Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \text{Light}_3$.

Problem 6.6. Prove that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong R_6$.

The next two theorems should not be terribly surprising.

Problem 6.7. Prove that if G_1 and G_2 are groups, then $G_1 \times G_2 \cong G_2 \times G_1$.

Problem 6.8. Suppose G_1 and G_2 are groups with identities e_1 and e_2, respectively. Prove that $\{e_1\} \times G_2 \cong G_2$ and $G_1 \times \{e_2\} \cong G_1$.

There's no reason we can't take the direct product of more than two groups. Recall that if $A_1, A_2, \ldots, A_n$ is a collection of sets, we define

$$\prod_{i=1}^{n} A_i := A_1 \times A_2 \times \cdots \times A_n.$$

Each element of $\prod_{i=1}^n A_i$ is of the form $(a_1, a_2, \ldots, a_n)$, where $a_i \in A_i$.

Problem 6.9. Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \prod_{i=1}^n G_i$, define

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Prove that $\prod_{i=1}^n G_i$, the **direct product** of $G_1, \ldots, G_n$, is a group under this binary operation.

One way to think about direct products is that we can navigate the product by navigating each factor simultaneously but independently. Computing the order of a group that is a direct product is straightforward.

Problem 6.10. Let $G_1, G_2, \ldots, G_n$ be groups. Prove that $|G_1 \times G_2 \times \cdots \times G_n|$ is infinite if and only if at least one $|G_i|$ is infinite. Moreover, if each G_i is finite, then

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1| \cdot |G_2| \cdots |G_n|.$$

The following theorem should be clear.

Problem 6.11. Let $G_1, G_2, \ldots, G_n$ be groups. Prove that $\prod_{i=1}^n G_i$ is abelian if and only if each G_i is abelian.

The next theorem tells us how to compute the order of an element in a direct product of groups.

Problem 6.12. Suppose $G_1, G_2, \ldots, G_n$ are groups and let $(g_1, g_2, \ldots, g_n) \in \prod_{i=1}^n G_i$. Prove that if each $|g_i|$ is finite, then $|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2| \ldots, |g_n|)$.

Problem 6.13. Find the order of each of the following elements.

(a) $(\overline{6}, \overline{5}) \in \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

(b) $(r, i) \in D_3 \times Q_8$.

(c) $((1,2)(3,4), \overline{3}) \in S_4 \times \mathbb{Z}/15\mathbb{Z}$.

Problem 6.14. Find the largest possible order of elements in each of the following groups.

(a) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

(b) $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

(c) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$

Problem 6.15. Prove that the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if m and n are relatively prime.

Problem 6.16. Prove that the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/mn\mathbb{Z}$ if and only if m and n are relatively prime.

The previous results can be extended to more than two factors.

Problem 6.17. Prove that the group $\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$ is cyclic and isomorphic to $\mathbb{Z}/m_1 m_2 \cdots m_n\mathbb{Z}$ if and only if every pair from the collection $\{m_1, m_2, \ldots, m_n\}$ is relatively prime.

Problem 6.18. Determine whether each of the following groups is cyclic.

(a) $\mathbb{Z}_7 \times \mathbb{Z}_8$

(b) $\mathbb{Z}_7 \times \mathbb{Z}_7$

(c) $\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_8$

(d) $\mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}_8$

Problem 6.19. Suppose $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$, where each p_i is a distinct prime number. Prove that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_2^{n_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{n_r}\mathbb{Z}.$$

The next theorem tells us that the direct product of subgroups is always a subgroup.

Problem 6.20. Suppose G_1 and G_2 are groups such that $H_1 \leq G_1$ and $H_2 \leq G_2$. Prove that $H_1 \times H_2 \leq G_1 \times G_2$.

However, not every subgroup of a direct product has the form above.

Problem 6.21. Find an example that illustrates that not every subgroup of a direct product is the direct product of subgroups of the factors.

The next theorem describes precisely the structure of finite abelian groups. We will omit its proof, but allow ourselves to utilize it as needed.

Theorem 6.22 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}} \times \mathbb{Z}^k,$$

where each p_i is a prime number (not necessarily distinct). The product is unique up to rearrangement of the factors.

Note that the number k is called the **Betti number**. A finitely generated abelian group is finite if and only if the Betti number is 0.

Problem 6.23. Use the previous theorem to find all abelian groups up to isomorphism of order 8.

Problem 6.24. Find all abelian groups up to isomorphism for each of the following orders.

(a) 16

(b) 12

(c) 25

(d) 30

(e) 60

7 Introduction to Quotient Groups

Under some special circumstances, we can "fold up" a group "along a subgroup" to form a new group. These groups are called **quotient groups**. It turns out that studying quotient groups is equivalent to studying homomorphisms.

Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. By Problem 2.23, $\ker(\phi)$ is subgroup of G consisting of all elements in G that map to the identity in H. Moreover, we know that the left cosets of $\ker(\phi)$ partition G in such away that all of the left cosets have the same cardinality according to Problem 1.125.

Problem 7.1. Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. Use Problem 2.24 to explain why for each $g \in G$, there exists $h \in H$ such that $g\ker(\phi) = \phi^{-1}(\{h\})$. In particular, $\ker(\phi) = \phi^{-1}(\{e_H\})$, where e_H is the identity in H.

The preimage $\phi^{-1}(\{h\})$ is often referred to as the **fiber** of h under ϕ. For simplicity, it is common to abbreviate $\phi^{-1}(\{h\})$ by $\phi^{-1}(h)$, but some care is needed here since we are not assuming that the inverse function of ϕ exists. Problem 7.1 says that each left coset of $\ker(\phi)$ is a fiber of some element in G (and vice versa). Figure 13 provides a visual representation of Problem 7.1 in the case when ϕ is surjective and H is finite.

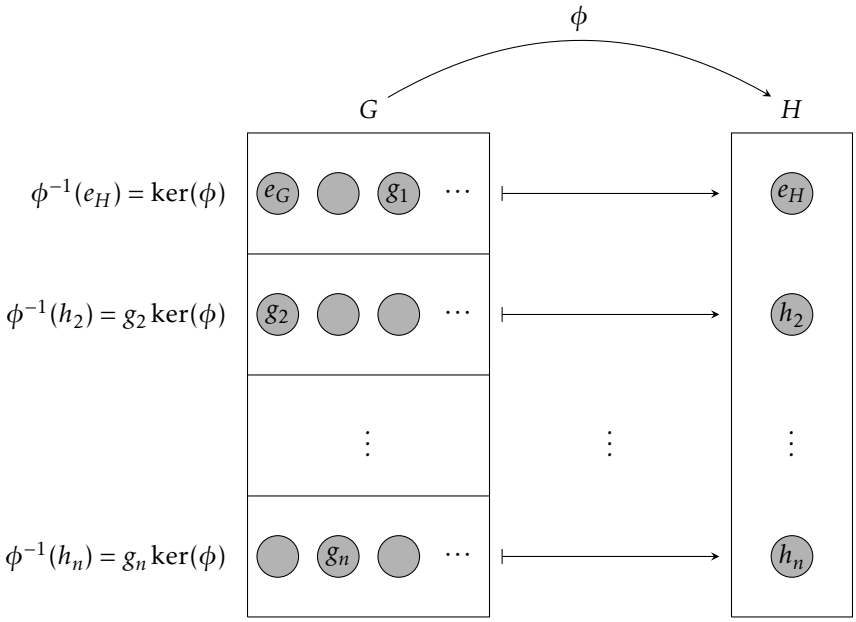


Figure 13: Left cosets of $\ker(\phi)$ correspond to fibers of ϕ.

Figure 13 suggests that the fibers of ϕ have a group structure inherited from the group structure of the image of ϕ:

$$\phi^{-1}(h')\phi^{-1}(h) = \phi^{-1}(hh').$$

Our current goal is to formalize this idea.

Problem 7.2. Draw a figure that captures the spirit of Problem 7.1 in terms of Cayley diagrams for the homomorphism given in Problem 2.27.

Problem 7.3. Define $\phi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ via $\phi(k) = \overline{k}$. Draw a figure that captures the spirit of Problem 7.1 in terms of Cayley diagrams for the homomorphism ϕ.

Example 7.4. Since Q_8 is finite, we can also visually represent the phenomenon in Problem 7.2 by cleverly rearranging the rows and columns of the group table for Q_8. In particular, if we organize the rows and columns of the group table for Q_8 according to the left cosets determined by the kernel of the homomorphism (i.e., the fibers of ϕ) in Problem 2.27, we obtain the nice visualization of the homomorphism ϕ that is given in Figure 14. As expected, this table suggests that there is a group structure on the fibers of ϕ. If we consider the 2×2 blocks as elements, it appears that we have a group table for a group with 4 elements.

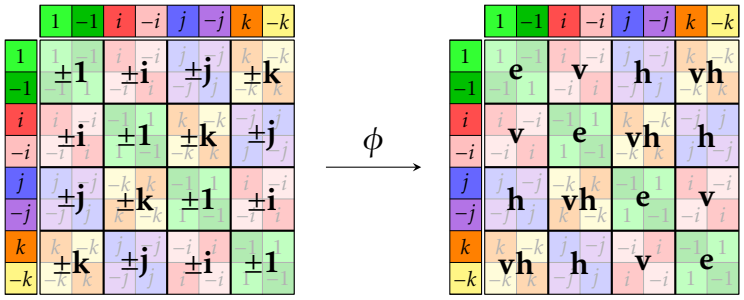


Figure 14: Visual representation of a homomorphism from Q_8 to V_4 in terms of group tables.

Closer inspection reveals that this looks just like the group table for V_4. Figure 14 suggests that we have two ways of understanding the underlying binary operation on the collection of 2×2 blocks (i.e., fibers of ϕ):

1. First map the fibers to their corresponding image in V_4, multiply in V_4, and then determine the fiber of the corresponding product.

2. Multiply representatives of the corresponding left cosets and then determine which left coset the resulting product is contained in.

For example, the table suggests that the fiber $j\ker(\phi) = \{\pm j\}$ times the fiber $i\ker(\phi) = \{\pm i\}$ is equal to $k\ker(\phi) = \{\pm k\}$ despite the fact that $ji = -k \neq k$. Yet, it is true that the product $ji = -k$ is an element in the fiber $k\ker(\phi)$. If we pick any two fibers, the product of any element of the first fiber times any element of the second fiber will always result in an element in the same fiber regardless of which representatives we chose.

Definition 7.5. Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. Define the **quotient group** (or **factor group**) $G/\ker(\phi)$ (pronounced "$G/\ker(\phi)$" as "G mod the kernel of ϕ") to be the group whose elements are the fibers of ϕ (i.e., left cosets of $\ker(\phi)$) with group operation defined as follows: if X_h is the fiber of $h \in \phi(G)$ and $X_{h'}$ is the fiber of $h' \in H$, then the product of X_h and $X_{h'}$ is the fiber of $hh' \in \phi(G)$. That is,

$$X_h X_{h'} := X_{hh'},$$

or equivalently, we can write

$$\phi^{-1}(h)\phi^{-1}(h') = \phi^{-1}(hh').$$

Problem 7.6. Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. Prove that $G/\ker(\phi)$ is a group under the binary operation described in Definition 7.5, where the identity of $G/\ker(\phi)$ is $\ker(\phi)$.

The definition of $G/\ker(\phi)$ explicitly requires the map ϕ since the multiplication of fibers is performed by first mapping the fibers to H via ϕ, multiplying in H, and then determining the fiber of the corresponding product. However, since each fiber corresponds to a unique left coset, we hope that we can multiply fibers by simply multiplying representatives of the corresponding left cosets. Let's verify that this process is well defined and behaves as expected.

Definition 7.7. Let G be a group and let $K \leq G$. Define G/K (read "G mod K") to be the collection of left cosets of K in G.

Notice that we did not say that G/K was a group! The following theorem provides sufficient conditions under which G/K will be a group.

Problem 7.8. Let G be a group and let K be the kernel of some homomorphism from G to another group. Prove that G/K is a group under the operation given by

$$g_1 K \circ g_2 K := (g_1 g_2)K.$$

In particular, this operation is well defined in the sense that if $a \in g_1 K$ and $b \in g_2 K$, then $ab \in (g_1 g_2)K$, so that multiplication does not depend on the choice of representatives for the cosets.

The upshot of the previous problem is that if we are given a subgroup K of a group G that we know is the kernel of some homomorphism, we may define the quotient group G/K without needing to explicitly appeal to the corresponding homomorphism. Later in this chapter, we address the question of whether G/K forms a group for any subgroup K. It turns out that the answer is no, in general. We shall see that the cosets of K form a group if and only if K is the kernel of some homomorphism (and there are subgroups for which this is not true).

Problem 7.9. Let G be a group and let K be the kernel of some homomorphism from G to another group. Prove that for each $gK \in G/K$, $(gK)^{-1} = g^{-1}K$.

Let's tinker with a few examples of quotient groups that arise from homomorphisms.

Problem 7.10. Define $\phi : \mathbb{R}\setminus\{0\} \to \{\pm 1\}$ via $\phi(x) = \frac{|x|}{x}$. Note that $\{\pm 1\}$ is a group of order 2 under ordinary multiplication.

(a) Prove that ϕ is a surjective homomorphism.

(b) Determine $\ker(\phi)$.

(c) Describe the fibers of ϕ.

(d) What is the isomorphism type of $(\mathbb{R} \setminus \{0\})/\ker(\phi)$?

Problem 7.11. For $n \geq 2$, define $\phi : S_n \to \mathbb{Z}/2\mathbb{Z}$ via

$$\phi(\sigma) = \begin{cases} \overline{0}, & \sigma \text{ even} \\ \overline{1}, & \sigma \text{ odd.} \end{cases}$$

Prove that ϕ is a surjective homomorphism and then describe the isomorphism type of $S_n/\ker(\phi)$.

Problem 7.12. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ via $\pi((x,y)) = x$.

(a) Prove that π is a surjective homomorphism.

(b) Determine $\ker(\pi)$ and describe this set geometrically.

(c) Describe the fibers of π geometrically.

(d) Any guesses for the isomorphism type of $\mathbb{R}^2/\ker(\pi)$?

Problem 7.13. Define $\phi : \mathbb{R}^2 \to \mathbb{R}$ via $\phi((x,y)) = x + y$.

(a) Prove that ϕ is a surjective homomorphism.

(b) Determine $\ker(\phi)$ and describe this set geometrically.

(c) Describe the fibers of ϕ geometrically.

(d) Any guesses for the isomorphism type of $\mathbb{R}^2/\ker(\phi)$?

Problem 7.14. Define $\phi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ via $\phi(\overline{a}) = \overline{a}$.

(a) Prove that ϕ is a well-defined homomorphism.

(b) Prove that ϕ is surjective.

(c) Determine $\ker(\phi)$.

(d) Describe the fibers of ϕ.

(e) Determine whether $(\mathbb{Z}/8\mathbb{Z})/\ker(\phi)$ is cyclic. Is $(\mathbb{Z}/8\mathbb{Z})/\ker(\phi)$ isomorphic to R_4 or V_4?

Problem 7.15. Suppose G and H are groups and define $\phi : G \to H$ via $\phi(g) = e_H$, where e_H is the identity in H. Prove that $G/\ker(\phi)$ is a trivial group.

Problem 7.16. Suppose $\phi : G \to H$ is an injective homomorphism. Prove that $G/\ker(\phi) \cong G$.

At this point, you might be thinking there is something special about "left" versus "right" cosets of the kernel. Let's take a moment to convince ourselves that this is not true.

Problem 7.17. Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. Prove that for all $g \in G$, we have $g\ker(\phi) = \ker(\phi)g$. That is, the left and right cosets of the kernel are identical.

The previous problem tells us that it does not matter whether we consider left or right cosets of the kernel as they are always the same.

We now turn our attention to the question of whether we can define the quotient group G/H for any subgroup H of G. Recall that in our approach to Problem 7.8, we utilized the fact that $g\ker(\phi)g^{-1} = \ker(\phi)$ (which is a consequence of Problem 2.23). This should help you make connections when tackling the next result.

Problem 7.18. Let G be a group and let $H \leq G$. Prove that the binary operation on the set of left cosets of H in G given by

$$g_1H \circ g_2H = (g_1g_2)H$$

is well defined if and only if $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$.

If the operation given in the previous problem is well defined, it is easy to verify that G/H is a group under this binary operation. In particular, associativity in G/H follows from associativity in G, the identity in G/H is the left coset $eH = H$, and the inverse of gH is $g^{-1}H$.

The subgroups that satisfy the criterion in Problem 7.18 are given a special name.

Definition 7.19. A subgroup N of G is called **normal** if every element of G normalizes N, i.e., $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G, then we write $N \trianglelefteq G$.

Problem 7.20. Let N be a subgroup of the group G. Prove that the following are equivalent.

(a) $N \trianglelefteq G$.

(b) $N_G(N) = G$.

(c) $gN = Ng$ for all $g \in G$.

(d) The operation on left cosets of N in G described in Problem 7.18 makes the set of left cosets into a group.

(e) $gNg^{-1} \subseteq N$ for all $g \in G$.

Problem 7.21. Suppose $N \trianglelefteq G$. Prove that $(gN)^n = g^nN$ for all $g \in G$ and $n \in \mathbb{Z}$.

Problem 7.22. If G is a group, prove that $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$. Explain why $G/\{e\} \cong G$ and G/G is the trivial group.

Problem 7.23. Consider the group Q_8.

(a) Prove that every subgroup of Q_8 is normal.

(b) For each subgroup, identify the isomorphism type of the corresponding quotient.

Problem 7.24. Consider the group D_3.

(a) Prove that $\langle r \rangle \trianglelefteq D_3$.

(b) What is the isomorphism type of $D_3/\langle r \rangle$?

(c) Prove that $\langle s \rangle$ is not a normal subgroup of D_3.

(d) Let $H = \langle s \rangle$. Find specific examples of $a, b, c, d \in D_3$ such that

$$(aH)(bH) \neq (cH)(dH)$$

even though $aH = cH$ and $bH = dH$. This is an example of left coset multiplication not being well defined!

Problem 7.25. Consider the group D_4.

(a) Find all normal subgroups of D_4.

(b) For each normal subgroup, identify the isomorphism type of the corresponding quotient.

(c) Identify a subgroup of D_4 that is not normal in D_4.

Problem 7.26. Let G be an abelian group.

(a) Explain why every subgroup of G is normal in G.

(b) Prove that G/H is abelian for every $H \leq G$.

Problem 7.27. Let G be a cyclic group.

(a) Explain why every subgroup of G is normal in G.

(b) Prove that G/H is cyclic for every $H \leq G$.

Problem 7.28. Provide an example of a nonabelian group G and a normal subgroup N of G such that G/N is abelian.

Problem 7.29. Provide an example of a noncyclic group G and a normal subgroup N of G such that G/N is cyclic.

Problem 7.30. Let $N \trianglelefteq G$. Define $\pi : G \to G/N$ via $\pi(g) = gN$. Prove that π is a surjective homomorphism with $\ker(\pi) = N$.

The homomorphism in the previous problem is called the **natural projection** of G onto G/N.
We now prove that normal subgroups are precisely the kernels of homomorphisms.

Problem 7.31. Prove that a subgroup N of G is normal if and only if N is the kernel of some homomorphism.

Here's the big picture of what we have discovered so far. Given a homomorphism $\phi : G \to H$, multiplication of fibers turns $G/\ker(\phi)$ into a group. The binary operation on left cosets via representatives is a well-defined binary operation and agrees with the binary operation on fibers. Moreover, $\ker(\phi)$ is normal in G since $N_G(\ker(\phi)) = G$. On the other hand, if N is a subgroup of G, then the binary operation on left cosets of N is well defined if and only if N is a normal subgroup of G. That is, G/N is a group (under standard left coset multiplication) if and only if N is a normal subgroup of G. However, N is a normal subgroup of G if and only if N is the kernel of some homomorphism.

We will close out this chapter by exploring the order of elements in quotient groups.

Problem 7.32. Suppose $N \trianglelefteq G$ and let $gN \in G/N$ have finite order k. Prove that k is the smallest positive integer such that $g^k \in N$.

Problem 7.33. Give an example to show that the order of gN in G/N might be strictly smaller than the order of g in G.

Problem 7.34. Find the order of the given element in the quotient group. You may assume that we are taking the quotient by a normal subgroup.

(a) $s\langle r\rangle \in D_4/\langle r\rangle$

(b) $j\langle -1\rangle \in Q_8/\langle -1\rangle$

(c) $\overline{5} + \langle\overline{4}\rangle \in \mathbb{Z}_{12}/\langle\overline{4}\rangle$

(d) $(\overline{2},\overline{1}) + \langle(\overline{1},\overline{1})\rangle \in (\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(\overline{1},\overline{1})\rangle$

(e) $(\overline{1},\overline{3}) + \langle(\overline{0},\overline{2})\rangle \in (\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(\overline{0},\overline{2})\rangle$

Problem 7.35. For each quotient group below, describe the group. If possible, state what group each is isomorphic to. You may assume that we are taking the quotient by a normal subgroup.

(a) $V_4/\langle h\rangle$

(b) $A_4/\langle(1,2)(3,4),(1,3)(2,4)\rangle$

(c) $(\mathbb{Z}_2 \times \mathbb{Z}_2)/\langle(\overline{1},\overline{1})\rangle$

(d) $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{\overline{0}\} \times \mathbb{Z}_2)$

Problem 7.36. Consider the quotient group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(\overline{0},\overline{1})\rangle$.

(a) What is the order of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(\overline{0},\overline{1})\rangle$?

(b) Is the group abelian? Why?

(c) Write down all the elements of $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(\overline{0},\overline{1})\rangle$.

(d) Does one of the elements generate the group?

(e) What well-known group is $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(\overline{0},\overline{1})\rangle$ isomorphic to?

Here are few additional exercises. These ones are a bit tougher.

Problem 7.37. For each quotient group below, describe the group. If possible, state what group each is isomorphic to. You may assume that we are taking the quotient by a normal subgroup.

(a) $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(\overline{0},\overline{2})\rangle$

(b) $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$

(c) $\mathbb{Q}/\langle 1\rangle$ (the operation on $\mathbb{Q}$ is addition)

8 More on Normal Subgroups

In this chapter, we collect several additional results concerning normal subgroups. Our first result generalizes the fact that the kernel of a homomorphism is always a normal subgroup of the domain.

Problem 8.1. Let $\phi : G \to H$ be a group homomorphism. Prove that if $K \trianglelefteq H$, then $\phi^{-1}(K) \trianglelefteq G$.

The next result below provides a method for simplifying computations when verifying that a subgroup is normal.

Problem 8.2. Let G be a group and let $N = \langle S \rangle$ for some subset S of G. Prove that if for all $g \in G$, we have $gSg^{-1} \subseteq N$, then $N \trianglelefteq G$.

Problem 8.3. Let G be a group and let $N = \langle x \rangle$ for some $x \in G$. Prove that if for all $g \in G$, we have $gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$, then $N \trianglelefteq G$.

Definition 8.4. Let G be a group and let $H \leq G$. The **index** of H in G is the number of cosets (left or right) of H in G. Equivalently, if G is finite, then the index of H in G is equal to $|G|/|H|$. We denote the index via $[G : H]$.

Problem 8.5. Let $H = \langle (1,2)(3,4), (1,3)(2,4) \rangle$.

(a) Find $[A_4 : H]$.

(b) Find $[S_4 : H]$.

Problem 8.6. Find $[\mathbb{Z} : 4\mathbb{Z}]$.

Problem 8.7. Prove that if G is a group and $H \leq G$ such that $[G : H] = 2$, then $H \trianglelefteq G$.

It is important to emphasize that being index 2 is a sufficient condition for a subgroup to be normal, but it is not a necessary condition. There are many examples of normal subgroups that are not index 2.

Problem 8.8. Provide an example of a group G and a subgroup H such that $H \trianglelefteq G$ yet $[G : H] \neq 2$.

It turns out that normality is not transitive.

Problem 8.9. Consider $\langle s \rangle = \{e, s\}$ and $\langle r^2, sr^2 \rangle = \{e, r^2, sr^2, s\}$. It is clear that

$$\langle s \rangle \leq \langle r^2, sr^2 \rangle \leq D_4.$$

Show that $\langle s \rangle \trianglelefteq \langle r^2, sr^2 \rangle$ and $\langle r^2, sr^2 \rangle \trianglelefteq D_4$, but $\langle s \rangle \not\trianglelefteq D_4$.

The previous problem illustrates that $H \trianglelefteq K \trianglelefteq G$ does not imply $H \trianglelefteq G$.

Problem 8.10. Prove that if H and K are normal subgroups of G, then $H \cap K \trianglelefteq G$.

In fact, a much stronger statement than the previous result is true. The intersection of arbitrarily nonempty collection of normal subgroups of a fixed group is a normal subgroup. The proof of this only requires a slight modification of the proof of the previous problem.

Problem 8.11. Suppose G is a group and $H \leq G$ such that H is the unique subgroup of a particular order in G. Prove that $H \trianglelefteq G$.

Problem 8.12. Let G be a group. Explain why we always have $Z(G) \trianglelefteq G$.

Problem 8.13. Let G be a group. Prove that if $G/Z(G)$ is cyclic, then G is abelian.

Problem 8.14. Is the converse of the previous result true? Justify your assertion.

Problem 8.15. Let G a finite group such that $|G| = pq$, where p and q are primes (not necessarily distinct). Prove that either G is abelian or $Z(G)$ is trivial.

Definition 8.16. Let G be a group and let $H, K \leq G$. Define

$$HK := \{hk \mid h \in H, k \in K\}.$$

In general, HK may not be a subgroup.

Problem 8.17. Let $G = S_3$, $H = \langle (1,2) \rangle$, and $K = \langle (2,3) \rangle$. Compute HK. Is HK a subgroup of S_3?

Problem 8.18. Let G be a group and let $H, K \leq G$. Prove that HK is a union of left cosets of K. That is, prove that

$$HK = \bigcup_{h \in H} hK.$$

Problem 8.19. Let G be a group and let $H, K \leq G$. Prove that if H and K have finite order, then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Problem 8.20. Let G be a group and let $H, K \leq G$. Prove that $HK \leq G$ if and only if $HK = KH$.

Problem 8.21. Let G be a group and let $H, K \leq G$. Prove that if $K \trianglelefteq G$, then $HK \leq G$.

9 The Isomorphism Theorems

In this chapter, we state some consequences of the relations between quotient groups and homomorphisms. The first result is essentially a restatement of our observations from Chapter 7 (see Figure 13). This theorem is sometimes called the **Fundamental Theorem of Homomorphisms**.

Problem 9.1 (The First Isomorphism Theorem)**.** Suppose $\phi : G \to H$ is a group homomorphism from a group G to a group H. Prove that $G/\ker(\phi) \cong \phi(G)$. To do this, establish an explicit function $\psi : G/\ker(\phi) \to \phi(G)$ and then show that ψ satisfies the homomorphic property and is a bijection.

An immediate consequence of the First Isomorphism Theorem is that $[G : \ker(\phi)] = |\phi(G)|$.

Problem 9.2. Use the First Isomorphism Theorem to prove that $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) \cong \mathbb{Z}_4$.

Problem 9.3. Consider the map ϕ given in Problem 7.10. Use the First Isomorphism Theorem to conclude that $(\mathbb{R} \setminus \{0\})/\ker(\phi) \cong \mathbb{R}^+$.

Problem 9.4. Consider the map π given in Problem 7.12. Use the First Isomorphism Theorem to conclude that $\mathbb{R}^2/\ker(\pi) \cong \mathbb{R}$.

Problem 9.5. Suppose G and H are groups. Use the First Isomorphism Theorem to prove that $(G \times H)/(\{e_G\} \times H) \cong G$ (and $\{e_G\} \times H \trianglelefteq G \times H$). Certainly, we also have $(G \times H)/(G \times \{e_H\}) \cong H$.

Problem 9.6. Consider the map ϕ given in Problem 7.13. Use the First Isomorphism Theorem to conclude that $\mathbb{R}^2/\ker(\phi) \cong \mathbb{R}$.

Problem 9.7. Consider the map ϕ given in Problem 7.14. Use the First Isomorphism Theorem to conclude that $(\mathbb{Z}/8\mathbb{Z})/\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$.

The next theorem is a generalization of Problem 2.19 and follows from the First Isomorphism Theorem together with Lagrange's Theorem.

Problem 9.8. Suppose $\phi : G \to H$ is a group homomorphism. Prove that if G is finite, then $|\phi(G)|$ divides $|G|$.

Problem 9.9 (The Second Isomorphism Theorem)**.** Let G be a group with $H \leq G$ and $N \trianglelefteq G$. Prove each of the following.

(a) $HN \leq G$;

(b) $N \trianglelefteq HN$;

(c) $H \cap N \trianglelefteq H$;

(d) $HN/N \cong H/(H \cap N)$.

The Second Isomorphism Theorem is sometimes called the **Diamond Isomorphism Theorem** in light of Figure 15. The double edges in the lattice indicate which quotients are isomorphic.

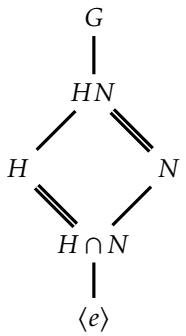


Figure 15: Visual representation of the Second Isomorphism Theorem.

Problem 9.10 (The Third Isomorphism Theorem)**.** Let G be a group with $H, K \trianglelefteq G$ and $K \leq H$. Prove that $H/K \trianglelefteq G/K$ and

$$G/H \cong (G/K)/(H/K).$$

The upshot of the Third Isomorphism Theorem is that we gain no new structural information by taking quotients of quotients.

The final isomorphism theorem, sometimes called the **Lattice Isomorphism Theorem**, describes the relationship between the lattice of subgroups of the quotient group G/N and the lattice of subgroups of G. In particular, the lattice for G/N can be read off from the lattice for G by collapsing the group N to the identity. There is a one-to-one correspondence between subgroups of G containing N and the subgroups of G/N.

Problem 9.11 (The Fourth Isomorphism Theorem)**.** Let G be a group with $N \trianglelefteq G$. Prove that there is a bijection from the collection of subgroups of G that contain N onto the collection of subgroups of G/N. In particular, every subgroup of G is of the form H/N for some subgroup H of G containing N (namely, its preimage in G under the canonical projection homomorphism from G to G/N). This bijection has the following properties: for all $H, K \leq G$ with $N \leq H$ and $N \leq K$, we have

(a) $H \leq K$ if and only if $H/N \leq K/N$

(b) If $H \leq K$, then $[K : H] = [K/N : H/N]$

(c) $\langle H, K\rangle/N = \langle H/N, K/N\rangle$

(d) $(H \cap K)/N = H/N \cap K/N$

(e) $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$.

Problem 9.12. Consider the group Q_8 and the normal subgroup $\langle -1\rangle$. Draw the subgroup lattice for Q_8 and indicate which edges in the lattice correspond to edges in the lattice for $Q_8/\langle -1\rangle$. We previously proved that $Q_8/\langle -1\rangle \cong V_4$. You ought to be able to witness the subgroup lattice for V_4 in your drawing.

Problem 9.13. Consider the group D_4 and the normal subgroup $\langle r^2\rangle$. Draw the subgroup lattice for D_4 and indicate which edges in the lattice correspond to edges in the lattice for $D_4/\langle r^2\rangle$. Notice that there are subgroups of D_4 that do not directly correspond to subgroups of $D_4/\langle r^2\rangle$, namely the subgroups of D_4 that do not contain $\langle r^2\rangle$.

10 Introduction to Group Actions

We begin with a definition.

Definition 10.1. A **group action** of a group G on a set A is a map from $G \times A \to A$, written as $g \cdot a$ for all $g \in G$ and $a \in A$, satisfying:

(i) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and

(ii) $e_G \cdot a = a$ for all $a \in A$.

A few comments are in order:

- Informally, we say that "G acts on A".
- Axiom (i) is like associativity, but formally it is not!
- Axiom (ii) says that the identity does not do anything to the set A.
- The function $\cdot$ is not a binary operation.
- The expression $g \cdot a$ will often be written as ga when there is no danger of confusing the group action with the operation in the group or otherwise.
- Technically, we defined "left" group actions. There is an equivalent notion of "right" group actions.

Definition 10.2. Suppose G acts on A. For each $g \in G$, define $\sigma_g : A \to A$ via

$$\sigma_g(a) = g \cdot a.$$

Problem 10.3. Prove that each σ_g is a permutation of A.

Let S_A be the collection of permutations of A. It is clear that S_A is a group under function composition.

Problem 10.4. Suppose G acts on A. Define $\phi : G \to S_A$ via $\phi(g) = \sigma_g$. Prove that ϕ is a group homomorphism.

The map from the previous problem is called the **permutation representation** of G on A.

Problem 10.5. Suppose $\theta : G \to S_A$ is a group homomorphism for some set A. Define $g \cdot a = \theta(g)(a)$ (where $\theta(g)(a)$ is the image of a using the permutation $\theta(g)$). Prove that this determines a group action of G on A.

The upshot of the previous theorem is that the actions of a group G on a set A and the homomorphisms from G into S_A are in bijection.

Problem 10.6. Explain why each of the following is indeed a group action. In each case, describe the corresponding permutation representation. In particular, determine whether the permutation representation is injective.

(a) Let G be a group and let A be a set. Then G acts on A via $g \cdot a = a$ for all $g \in G$ and $a \in A$. This is called the **trivial action** of G on A.

(b) Assume $A \neq \emptyset$. Then S_A acts on A via $\sigma \cdot a = \sigma(a)$ for all $\sigma \in S_A$ and $a \in A$.

(c) Let $A = \{1, 2, \ldots, n\}$. Label the vertices of a regular n-gon with $1, 2, \ldots, n$ in a clockwise manner. Then D_n acts on A as follows. For $g \in D_n$ and $a \in A$, define $g \cdot a$ to be the label we obtain using the natural action of g on the n-gon.

(d) Suppose n is even. Then D_n acts on the set consisting of pairs of opposite vertices of a regular n-gon as follows. For $g \in D_n$ and $\{a, b\}$ a pair of opposite vertices, define $g \cdot \{a, b\}$ to be the pair of opposite vertices that we obtain using the natural action of g on the n-gon.

(e) Suppose $G = \langle S \rangle$ and consider the Cayley diagram for G determined by S. Then G acts on the vertices of the Cayley diagram as follows. For $g \in G$ and $a \in G$, define $g \cdot a$ to be the vertex of the Cayley diagram we obtain by starting at the vertex a and then following any sequence of arrows that corresponds to a word in S that equals g.

(f) Let G be any group and let $A = G$. Then G acts on itself via left multiplication: $g \cdot a = ga$. This action is called the **left regular action** of G on itself.

(g) Let G be any group and let $A = G$. Then G acts on itself via conjugation: $g \cdot a = gag^{-1}$.

(h) Let G be a group, $H \leq G$, and let A be the collection of left cosets of H in G. Then G acts on A via $g \cdot xH = (gx)H$.

It might be useful to see an example of something that is not quite a group action.

Problem 10.7. Label the vertices of a square $1, 2, 3, 4$ clockwise. Let $A = \{\{1, 2\}, \{3, 4\}\}$. For $g \in D_4$ and $\{x, y\} \in A$ define $g \cdot \{x, y\}$ to be $\{gx, gy\}$, where gx and gy are the labels we obtain using the natural action of g on the square. Explain why this is not a group action.

Definition 10.8. Suppose G acts on A. Define the **kernel** of the action to be $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.

The kernel of an action is the set of elements in G that fix *all* the elements in A. That is, these are the elements in G that behave like the identity on A.

Problem 10.9. Find the kernel of each action described in Problem 10.6.

Problem 10.10. Suppose G acts on A. Prove that the kernel of the action is the same as the kernel of the associated permutation representation.

One consequence of the previous problem is that the kernel of an action is always a normal subgroup of G.

Definition 10.11. Suppose G acts on A. If the associated permutation representation is injective, we say that the action is **faithful**.

A faithful action is one in which distinct elements in G induce distinct permutations of A.

Problem 10.12. Determine which actions in Problem 10.6 are faithful.

Problem 10.13. Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the trivial group.

Observe that two group elements induce the same permutation on A if and only if they are in the same coset of the kernel. Thus, an action of G on A can be viewed as a faithful action of the quotient group $G/\ker(\phi)$ on A.

Problem 10.14. Prove that the group of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.

Problem 10.15. Prove that the group of rigid motions of a cube is isomorphic to S_4. *Hint:* S_4 naturally acts on the collection of four pairs of opposite vertices.

Problem 10.16. Explain why the natural action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful and find the kernel of this action.

11 Stabilizers and Orbits of Group Actions

Definition 11.1. Suppose G acts on A and let $a \in A$. We define the **stabilizer** of a in G to be the set

$$\mathrm{Stab}_G(a) := \{g \in G \mid g \cdot a = a\}.$$

In some books, the stabilizer of a in G is denoted G_a.

Note that if a is a fixed element of A, then the kernel of the action is contained in $\mathrm{Stab}_G(a)$. In particular, the kernel of an action is the intersection of all of the stabilizers for individual elements in A. That is, the kernel of the action is equal to $\bigcap_{a \in A} \mathrm{Stab}_G(a)$.

Problem 11.2. For $n \in \mathbb{N}$, the group S_n acts on $\{1, 2, \ldots, n\}$ via $\sigma \cdot i = \sigma(i)$ for all $i \in \{1, 2, \ldots, n\}$. Determine $\mathrm{Stab}_{S_n}(i)$ for each $i \in \{1, 2, \ldots, n\}$. Is this action faithful? What is the associated permutation representation?

Problem 11.3. Label the vertices of a square $1, 2, 3, 4$ clockwise so that 1 is the label of the upper left corner of the square. Consider the natural action of D_4 on $\{1, 2, 3, 4\}$ using this labeling. Assume r is clockwise rotation by a quarter turn of the square and assume s is reflection across the line through the vertices labeled by 1 and 3.

(a) Find σ_r, σ_s, and σ_{sr}.

(b) Find $\mathrm{Stab}_{D_4}(1)$.

(c) What is the kernel of this action? Is this action faithful?

Problem 11.4. Label the vertices of a square as in the previous problem. Let $A = \{\{1, 3\}, \{2, 4\}\}$. Consider the natural action of D_4 on this set.

(a) Find σ_r, σ_s, and σ_{sr}.

(b) Find $\mathrm{Stab}_{D_4}(\{1, 3\})$.

(c) What is the kernel of this action? Is this action faithful?

Problem 11.5. Suppose G acts on A. Prove that for $a \in A$, $\mathrm{Stab}_G(a)$ is a subgroup of G.

Definition 11.6. Suppose G acts on a nonempty set A. Define $\sim_G$ on A via

$$a \sim_G b \text{ if and only if } a = g \cdot b \text{ for some } g \in G.$$

Problem 11.7. Suppose G acts on a nonempty set A. Prove that the relation defined above is an equivalence relation.

Note that the corresponding equivalence classes are given by $\{g \cdot a \mid g \in G\}$ and these sets partition A.

Definition 11.8. Suppose G acts on a nonempty set A. The equivalence class of $a \in A$ induced by $\sim_G$ is called the **orbit** of G containing a and we write

$$\mathrm{Orb}_G(a) := \{g \cdot a \mid g \in G\}.$$

The **length** (or **size**) of an orbit, denoted $|\mathrm{Orb}_G(a)|$, is the cardinality of the orbit. The collection of orbits is sometimes denoted by A/G or A_G.

Definition 11.9. Suppose G acts on a nonempty set A. We say that the action of G on A is **transitive** (or that G acts **transitively** on A) if there is only one orbit for the action.

Problem 11.10. Let $A = \{(i, j) \mid 1 \leq i, j \leq 3\}$. Let S_3 act on A via $\sigma \cdot (i, j) = (\sigma(i), \sigma(j))$. Find the orbits of this action.

Problem 11.11. Suppose G acts trivially on a nonempty set A.

(a) Determine $\mathrm{Stab}_G(a)$ for $a \in A$.

(b) Determine $\mathrm{Orb}_G(a)$ for $a \in A$.

(c) Is this action ever transitive?

Problem 11.12. Determine whether the actions described in Problems 11.2–11.4 are transitive.

If G acts on A, then any subgroup of H of G also acts on A.

Problem 11.13. Consider the natural action on $\{1,2,3,4\}$ by the subgroup $\langle (1,2),(2,4)\rangle$ of S_4. Determine the orbits of this action.

The previous problem illustrates that if a group acts transitively on a set, a subgroup may not act transitively.

Problem 11.14. Consider the natural action on $\{1,2,3,4,5\}$ by the subgroup $\langle (1,2)(3,4,5)\rangle$ of S_5. Determine the orbits of this action.

The next theorem is often called the **Orbit Stabilizer Theorem**. This might be my favorite theorem in mathematics!

Problem 11.15 (The Orbit Stabilizer Theorem)**.** Prove that if G acts on a nonempty set A, then for each $a \in A$, we have

$$|\mathrm{Orb}_G(a)| = [G : \mathrm{Stab}_G(a)].$$

Try to draw a picture that captures the essence of this theorem.

Problem 11.16. Let G be a group, $H \leq G$, and let G act on the collection A of left cosets of H in G. Let ϕ be the associated permutation representation. Prove each of the following.

(a) G acts transitively on A.

(b) $\mathrm{Stab}_G(H) = H$.

(c) $\ker(\phi) = \bigcap_{g \in G} gHg^{-1}$ and $\ker(\phi)$ is the largest normal subgroup of G contained in H.

We can use the previous theorem to prove the next result, which is often referred to as **Cayley's Theorem**.

Problem 11.17 (Cayley's Theorem)**.** Prove that if G is a group of order n, then G is isomorphic to a subgroup of S_n. *Hint:* Let H be the trivial subgroup of G and apply the previous problem.

Problem 11.18. Prove that if G is a group of order n and p is the smallest prime dividing the order of G, then any subgroup of index p is normal in G.

12 Conjugation and the Class Equation

Recall that if G is a group, then one way in which G may act on itself is via conjugation. We say that $a, b \in G$ are **conjugate** if there exists $g \in G$ such that $b = gag^{-1}$. That is, two elements are conjugate if and only if they are in the same orbit of G under the action of conjugation. The orbits of G under the action of conjugation are called the **conjugacy classes** of G.

Problem 12.1. Suppose G is an abelian group. Explain why the action of G on itself by conjugation is the trivial action. What is the conjugacy class for each $a \in G$?

Problem 12.2. Determine all of the conjugacy classes for S_3.

Unlike the action of G on itself by left multiplication, the action of G on itself by conjugation is never transitive if the group is nontrivial.

Problem 12.3. Suppose $|G| > 1$.

(a) What is the conjugacy class of the identity in G?

(b) Prove that the conjugacy class of $a \in G$ is $\{a\}$ if and only if $a \in Z(G)$.

We can generalize the notion of a group acting on itself via conjugation by letting G act on the power set $\mathcal{P}(G)$ via conjugation: $g \cdot S = gSg^{-1}$ for $g \in G$ and $S \subseteq G$. It's easy to verify that this is indeed a group action. We say that two subsets S and T of a group G are **conjugates** in G if there exists $g \in G$ such that $T = gSg^{-1}$.

Problem 12.4. Consider the action of a group G on the subsets of G via conjugation.

(a) Prove that $\mathrm{Stab}_G(S) = N_G(S)$ for each $S \subseteq G$.

(b) Use the Orbit Stabilizer Theorem to prove that the number of conjugates of a subset S of G equals the index $[G : N_G(S)]$.

(c) Prove that the number of conjugates of $a \in G$ is equal to the index $[G : C_G(a)]$.

The upshot is that the action of a group G on itself via conjugation partitions G into conjugacy classes of G, each of whose cardinalities may be computed using Problem 12.4. The next result, referred to as the **Class Equation**, formalizes this for finite groups.

Problem 12.5 (The Class Equation)**.** Let G be a finite group and let $g_1, \ldots, g_k$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Prove that

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)].$$

Problem 12.6. Using Problem 12.2, find the class equation by writing $|S_3|$ in terms of the corresponding summation.

Problem 12.7. Determine the distinct conjugacy classes in Q_8 and then find the class equation by writing $|Q_8|$ in terms of the corresponding summation.

Problem 12.8. Determine the distinct conjugacy classes in D_4 and then find the class equation by writing $|D_4|$ in terms of the corresponding summation.

Problem 12.9. Let $g_1, \ldots, g_k$ be representatives of the conjugacy classes of a finite group G and suppose these elements pairwise commute. Prove that G is abelian.

Problem 12.10. Prove that if p is a prime and P is a group of order p^m for some $m \in \mathbb{N}$, then P has a nontrivial center (i.e., $|Z(P)| > 1$).

Problem 12.11. Prove that if p is a prime and P is a group of order p^2, then P is abelian. In particular, P is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Problem 12.12. Prove that if p is a prime and P is a group of order p^m for some $m \in \mathbb{N}$, then P has a subgroup of order p^k for every $0 \leq k \leq m$. Consider using a previous problem and induction. **Problem 13.4 is useful here! You may use it even though it comes later. This isn't circular.**

Problem 12.13. Let $\sigma, \tau \in S_n$ and suppose σ has cycle decomposition

$$(a_{1,1}, a_{1,2}, \ldots, a_{1,k_1})(a_{2,1}, a_{2,2}, \ldots, a_{2,k_2}) \cdots (a_{m,1}, a_{m,2}, \ldots, a_{m,k_m}).$$

Prove that $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_{1,1}), \tau(a_{1,2}), \ldots, \tau(a_{1,k_1}))(\tau(a_{2,1}), \tau(a_{2,2}), \ldots, \tau(a_{2,k_2})) \cdots (\tau(a_{m,1}), \tau(a_{m,2}), \ldots, \tau(a_{m,k_m})).$$

That is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.

Definition 12.14. If $\sigma \in S_n$ is the product of disjoint cycles of lengths $k_1, k_2, \ldots, k_m$ with $k_1 \leq k_2 \leq \cdots \leq k_m$ (including 1-cycles), then the integers $k_1, k_2, \ldots, k_m$ are called the **cycle type** of σ.

Problem 12.15. Let $\sigma = (3,5)(8,9)(2,4,7,6)$ and $\tau = (1,3,4,2,5,7,6,9)$ in S_9. Compute $\tau\sigma\tau^{-1}$.

Problem 12.16. Prove that two elements of S_n are conjugate if and only if they have same cycle type.

Problem 12.17. Prove that for $n \geq 3$, $Z(S_n)$ is trivial.

Definition 12.18. A group G is called **simple** if its only normal subgroups are $\{e\}$ and G.

Problem 12.19. Prove that A_5 is simple.

13 The Sylow Theorems

In this chapter, we prove a partial converse to Lagrange's Theorem. We begin with a definition.

Definition 13.1. Let G be a group and let p be prime.

(a) A group of order p^k for some $k \geq 0$ is called a p-**group**. Subgroups of G that are p-groups are called p-**subgroups**.

(b) If G is a group of order $p^k m$, where p does not divide m, then a subgroup of order p^k is called a **Sylow** p-**subgroup** of G.

(c) The set of Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G is denoted by $n_p(G)$ (or simply n_p when the context is clear).

Note that if G is a finite group and p is a prime such that p does not divide the order of G, then the Sylow p-subgroup of G is the trivial group. If $|G| = p^k$, where p is prime, then G is the unique Sylow p-subgroup of G.

Problem 13.2. Find all of the Sylow 2-subgroups and all of the Sylow 3-subgroups of S_3.

Problem 13.3. Find all of the Sylow 2-subgroups and all of the Sylow 3-subgroups of A_4.

The next problem is sometimes referred to as Cauchy's Theorem for abelian groups.

Problem 13.4. Prove that if G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p. *Hint:* Proceed by complete induction on $|G|$.

Use the Fundamental Theorem of Finitely Generated Abelian Groups (Problem 6.22) to prove the following result.

Problem 13.5. Assume G is a finite abelian group. Prove that G has a unique Sylow p-subgroup for each prime p.

Problem 13.6. Let G be a group and let $P \in \mathrm{Syl}_p(G)$. Prove that if Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$. *Hint:* The reverse containment should be straight forward. For the forward containment, let $H = N_G(P) \cap Q$ and then argue that PQ is a p-subgroup of G containing both P and Q. Next, argue that $PQ = P$.

We are now prepared to prove Sylow's Theorem! To prove Part (a) below, proceed by induction on $|G|$ and then utilize Problem 13.4 and the Class Equation. Here's an outline to get you started on proving Parts (b) and (c). By Part (a), there exists a Sylow p-subgroup P. Let $\mathcal{S} = \{P_1, \ldots, P_r\}$ be the collection of conjugates of P, and let Q be any p-subgroup of G. Notice that Q acts on $\mathcal{S}$ via conjugation. Then we can partition $\mathcal{S}$ into disjoint orbits under this action by Q, say $\mathcal{S} = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_s$, where $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$. Renumber the elements of $\mathcal{S}$ so that the first s elements of $\mathcal{S}$ are representatives of the Q-orbits: $P_i \in \mathcal{O}_i$ for $1 \leq i \leq s$. What does Orbit Stabilizer Theorem tell us about $|\mathcal{O}_i|$? Explain why $N_Q(P_i) = N_G(P_i) \cap Q$ and then apply the previous problem. Since Q was arbitrary, one possibility is that $Q = P_1$. Compute $|\mathcal{O}_1|$ and $|\mathcal{O}_i|$ for all $2 \leq i \leq s$.

Problem 13.7 (Sylow's Theorem)**.** Let G be a group of order $p^k m$, where p is a prime that does not divide m. Prove each of the following.

(a) $\mathrm{Syl}_p(G) \neq \emptyset$.

(b) If $P \in \mathrm{Syl}_p(G)$ and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate in G.

(c) The number of Sylow p-subgroups of G is of the form $1 + \ell p$ (i.e., $n_p \equiv 1 \pmod{p}$). Moreover, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, and hence n_p divides m.

Problem 13.8. Explain why any two Sylow p-subgroups of a group G are isomorphic.

Problem 13.9. Compute n_2 for S_4. What well-known group is every Sylow 2-subgroup of S_4 equal to?

Problem 13.10. Let P be a Sylow p-subgroup of G. Prove that the following are equivalent.

(a) P is the unique Sylow p-subgroup of G (i.e., $n_p = 1$).

(b) $P \trianglelefteq G$.

(c) $\phi(P) = P$ for all $\phi \in \mathrm{Aut}(G)$. *Note:* The fancy lingo here is that P is **characteristic** in G.

(d) All subgroups generated by elements of p-power order are p-groups (i.e., if S is any subset of G such that $|x|$ is a power of p for all $x \in S$, then $\langle S \rangle$ is a p-group).

Problem 13.11. Suppose $|G| = pq$ for primes p and q with $p < q$. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$.

(a) Prove that $Q \trianglelefteq G$.

(b) Prove that if P is also normal in G, then G is cyclic.

Problem 13.12. Prove that if G is a group of order 30, then G has a normal subgroup of order 15 that is isomorphic to $\mathbb{Z}_{15}$.

Problem 13.13. Prove that if G is a group of order 12, then either G has a normal Sylow 3-subgroup or $G \cong A_4$. Note that in the latter case, G has a normal Sylow 2-subgroup.

Problem 13.14. Let G be a group of order p^2q where p and q are distinct primes. Prove that G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup.

Problem 13.15. Let G be a group of order pqr where p, q, and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q, or r.

The next problem is known as **Cauchy's Theorem**.

Problem 13.16 (Cauchy's Theorem)**.** Prove that if G is a finite group and p is a prime dividing the order of G, then G has an element of order p.

Problem 13.17. Prove that if G is a group of order 60 such that G has more than one Sylow 5-subgroup, then G is simple (i.e., the only normal subgroups of G are $\{e\}$ and G).

Problem 13.18. Use the previous problem to argue that A_5 is simple.

Problem 13.19. Prove that if G is a group of order 280, then G is not simple.

Problem 13.20. Prove that if G is a group of order 396, then G is not simple.

14 Semidirect Products

In this chapter, we briefly introduce the notion of the semidirect product of two groups H and K, which is a generalization of the direct product of H and K.

Problem 14.1. Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $\cdot$ denote the left action of K on H determined by ϕ (i.e., $k \cdot h = \phi(k)(h)$). Let G be the set of ordered pairs (h,k) with $h \in H$ and $k \in K$ and define the following multiplication on G:

$$(h_1,k_1)(h_2,k_2) = (h_1(k_1 \cdot h_2), k_1k_2).$$

Prove each of the following.

(a) The binary operation defined above makes G into a group, where the identity is (e_H, e_K), $(h,k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$, and $|G| = |H||K|$.

(b) The sets $\{(h, e_K) \mid h \in H\}$ and $\{(e_H, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, e_K)$ for $h \in H$ and $k \mapsto (e_H, k)$ for $k \in K$ are isomorphisms of these groups with the groups H and K, respectively. For simplicity, we identify H and K with their isomorphic copies in G.

(c) $|H \cap K| = 1$.

(d) For all $h \in H$ and $k \in K$, $khk^{-1} = k \cdot h = \phi(k)(h)$.

(e) $H \trianglelefteq G$.

Definition 14.2. Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. The group described in Problem 14.1 is called the **semidirect product** of H and K with respect to ϕ and is denoted by $H \rtimes_\phi K$. When the context is clear, we will simply write $H \rtimes K$.

The notation is meant to help us remember that the left factor is normal in the semidirect product.

Problem 14.3. Recall $S_2 = \langle s \rangle$. For $n \geq 3$, define $\phi : S_2 \to \mathrm{Aut}(R_n)$ where $\phi(e)$ is the identity automorphism and $\phi(s)$ is the automorphism of inversion on H (i.e., $h \mapsto h^{-1}$). One can quickly show that ϕ is a group homomorphism. Let $G = R_n \rtimes S_2$ as in Problem 14.1 (so that the associated action is $s \cdot h = h^{-1}$ for all $h \in R_n$).

(a) Prove that $shs^{-1} = h^{-1}$ for all $h \in R_n$.

(b) Prove that $D_n \cong R_n \rtimes S_2$.

It is useful to have a way for recognizing when semidirect products are actually direct products.

Problem 14.4. Let H and K be group and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Prove that the following are equivalent.

(a) The identity set map between $H \rtimes K$ and $H \times K$ is a group homomorphism (and hence isomorphism).

(b) ϕ is the trivial homomorphism from K into $\mathrm{Aut}(H)$.

(c) $K \trianglelefteq H \rtimes K$.

It is also useful to have a method for determining whether a given group is isomorphic to a semidirect product.

Problem 14.5. Suppose G is a group with subgroups H and K such that $H \trianglelefteq G$ and $H \cap K = \{e\}$. Let $\phi : K \to \mathrm{Aut}(H)$ be the homomorphism defined by mapping $k \in K$ to the automorphism that is conjugation by k on H. Prove that $HK \cong H \rtimes K$. Notice that if $G = HK$, then it follows that G is a semidirect product.

Problem 14.6. Let G be a group of order 12. Let $V \in \mathrm{Syl}_2(G)$ and $T \in \mathrm{Syl}_3(G)$. By Problem 13.13, we know that either V or T is normal in G. By Lagrange's Theorem, $|V \cap T| = 1$. It follows from Problem 14.5 that G is isomorphic to a semidirect product of V and T. Note that V is isomorphic to either R_4 or V_4 while T is isomorphic to R_3. Classify all of the groups of order 12 up to isomorphism.

