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 $S \subset G$, 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) $S_3 = \langle s_1, s_2 \mid s_1^2 = e, s_2^2 = e, s_1s_2s_1 = s_2s_1s_2\rangle$

(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

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

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 $G = \langle S \mid w_1 = e, w_2 = e, \dots, w_m = e\rangle$, we mean that G is the group generated by S that satisfies all of the relations we can derive from $w_1 = e, w_2 = e, \dots, w_m = e$. 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 $g_1,g_2,\ldots,g_n \in G$. Prove that if $x \in \langle g_1,g_2,\ldots,g_n\rangle$, then $\langle g_1,g_2,\ldots,g_n\rangle = \langle g_1,g_2,\ldots,g_n,x\rangle$.

In the previous theorem, we are not claiming that $\{g_1,g_2,\ldots,g_n\}$ is a generating set for G—although this may be the case. Instead, are simply making a statement about the subgroup $\langle g_1,g_2,\ldots,g_n\rangle$, 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:

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

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

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

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

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

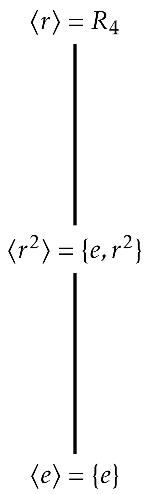

Figure 1: Subgroup lattice for R_4.

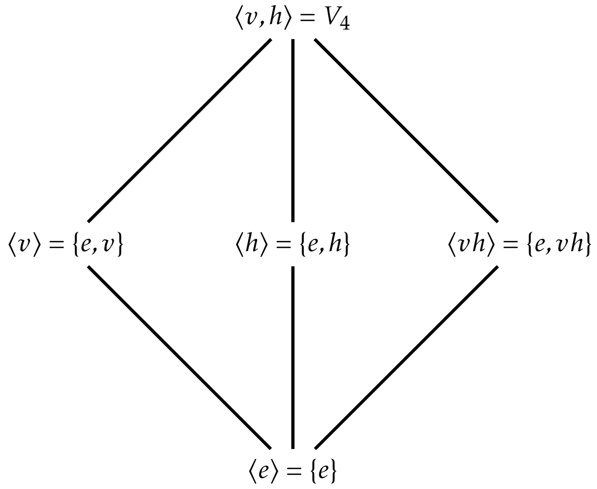
$\langle v, h\rangle = V_4$
$\langle v\rangle = \{e, v\}$
$\langle h\rangle = \{e, h\}$
$\langle vh\rangle = \{e, vh\}$
$\langle e\rangle = \{e\}$

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 $\langle H \cup K\rangle$.

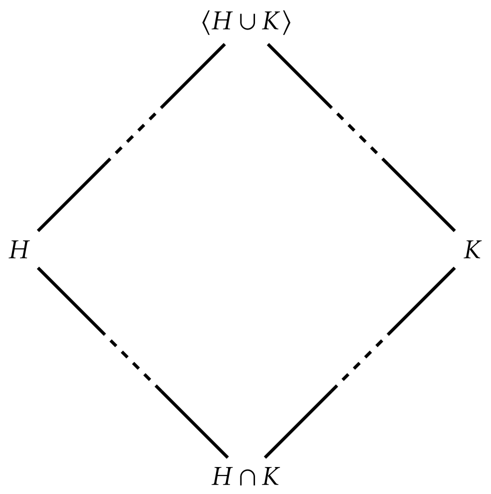

Figure 3: Meet and join for subgroups H and K.

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