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 $a*b = 1+ab$. 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 $T \subseteq S$. 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 $T \subseteq S$ 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 $T \subseteq S$ 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 solutions 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.)