IOAA Problem Bank

Table of Contents

Introduction

This problem bank is included in these materials as an additional resource for instructors who need to create homework sets, quizzes, and exams. Some of these problems are standard textbook problems while others are more tailored to the IOAA curriculum. The problems have been placed into sections (by curriculum unit) that indicate when in the course they would (first) be accessible to students. The first section "Strongly Recommended Problems" collects all of the problems that we recommend every instructor assign. These are problems that directly support or build on tasks in the curriculum. A note of explanation is included with each to indicate how it relates to tasks from the curriculum.

Note: A number of the problems also appear in the curriculum materials themselves or appear more than once (sometimes in a slightly different form and with different expectations for how students might attack them). This is meant to provide flexibility to instructors.

There is also a section called "Questions on Related or Supportive Topics". This includes, for example, questions about equivalence relations.

This document is included as a Word document to make it easy for instructors to copy items and modify them. It is also included as a PDF so that instructors can see how the problems are intended to look regardless of technological issues that may arise with the Word version.

Notation: D_{2n} signifies the symmetries of a regular n-gon (i.e., the dihedral group of order $2n$).

C_n signifies the rotations of an n-gon. (i.e. cyclic group of order n in multiplicative notation.)

R^* signifies the multiplicative group of the ring R.

Strongly Recommended Problems:

- Is this a group? [Can be assigned any time after group is defined in Unit 1 (Groups and Subgroups). Recommended to be assigned **before** starting Unit 3 (Quotient Groups)]

+	EVEN	ODD
EVEN		
ODD		

- Consider the group of symmetries of an equilateral triangle (R = 120° Clockwise Rotation and F = Reflection across the vertical axis):
  [Recommended to be assigned before starting subgroup part of Unit 1 (Groups). Modify to have notation that matches that developed in your class. Parts c) and d) prime students for thinking about subgroups.]

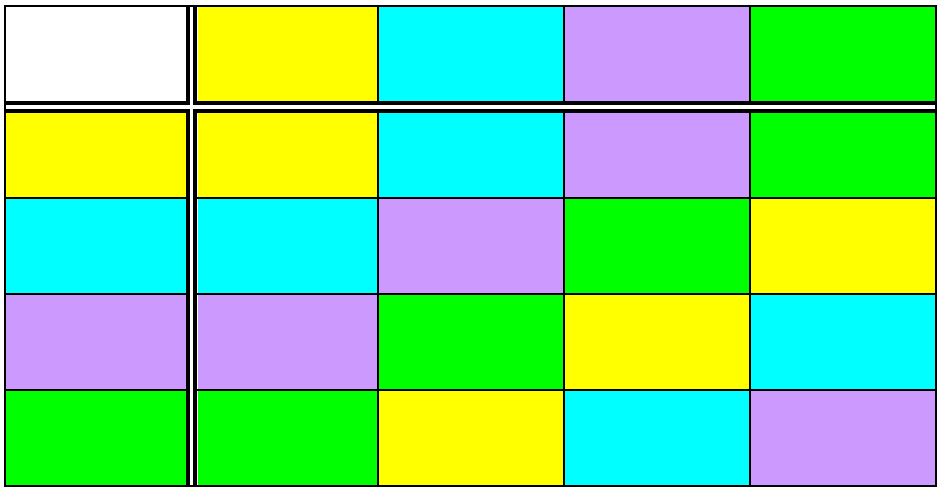
	F	FR	RF	I	R	RR
F	I	R	RR	F	FR	RF
FR	RR	I	R	FR	RF	F
RF	R	RR	I	RF	F	FR
I	F	FR	RF	I	R	RR
R	RF	F	FR	R	RR	I
RR	FR	RF	F	RR	I	R

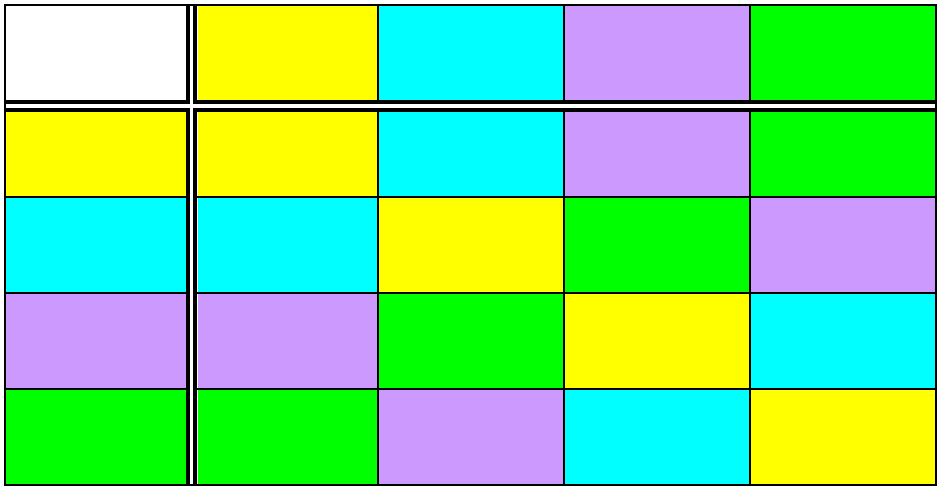
  a. Explain how you can tell that every element has an inverse *by looking at the table*.
  b. Demonstrate how to calculate $F(RF)FR$ using the definition of group and the rules (1) $RF = FRR$, (2) $FF = I$, and (3) $RRR = I$. Show all steps and justify each step (by naming a rule or part of the definition of group).

c. Can you eliminate one of these symmetries and have the remaining elements form a group? Justify your response.
d. Can you eliminate more than one of these symmetries and have the remaining elements form a group? Justify your response.

- Prove that any group of order 4 must be isomorphic to one of the two group given by the tables below:

[Recommended to be done before starting the quotient group unit (Lesson 2). This gives the instructor an option to have students use a colored handout rather than colored index cards when they attempt to build quotient groups of order 4.]

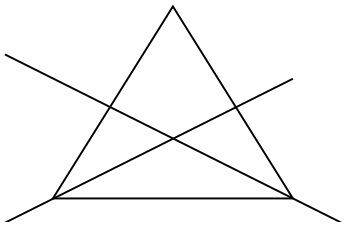




Groups

Problems that can work before *group* is defined

- If you assign either of the next 2 problems, be sure to think about the case of a line segment!
  - Explain why a bounded two-dimensional figure cannot have a *non-trivial* rotation symmetry AND *exactly one* reflection symmetry.
  - Can a bounded 2-D figure with a non-trivial rotation symmetry have exactly one reflection (flip) symmetry? Justify.
  - Is it possible to express all of the six symmetries (of an equilateral triangle) in terms of the two flips, $\boldsymbol{F}_1$ and $\boldsymbol{F}_2$, shown in the figure below? If so, make a table similar to the one we made in class expressing the symmetries in terms of the symbols $\boldsymbol{F}_1$ and $\boldsymbol{F}_2$. If not, provide a justification for why it cannot be done.



$\boldsymbol{F}_1$ is a flip across this line

$\boldsymbol{F}_2$ is a flip across this line

Assume the triangle is actually equilateral and the lines shown are actual lines of symmetry!

- The next two questions are the same but one uses additive notation while the other uses multiplicative. Similar alternative version can be created for a number of the problems.

- Which one of the 6 symmetries (of an equilateral triangle) is 2F + 3(R+F) + (-F) + (-2R) + 3F equivalent to? Prove it using the rules we have for calculating combinations of triangle symmetries.

- Which one of the 6 symmetries (of an equilateral triangle) is $F^2(RF)^3F^{-1}(R^2)^{-1}F^3$ equivalent to? Prove it using the rules we have for calculating combinations of triangle symmetries.

- How many symmetries does a square have?

- Half of the symmetries of an equilateral triangle are *flips* and the other half are *rotations*.
    a. Is the combination of two *flips* always, sometimes, or never a *flip*? Justify your response.
    b. Is the combination of two *rotations* always, sometimes, or never a *rotation*? Justify your response.
    c. Is the combination of a *rotation* and a *flip* always, sometimes, or never a *rotation*? Justify your response.

- Determine how many symmetries a non-square rectangle has.
    a. Write a verbal description of each symmetry.
    b. Draw a diagram to illustrate each symmetry.
    c. Create a symbol to represent each symmetry. The symbol should be simple enough to save writing but should be descriptive as well.
    d. For each combination of two symmetries, determine which of the original symmetries is equivalent to that combination.

- Consider the rotations of a square (ONLY the rotations in the plane, no flips). How many are there?
    a. Make a table that shows the result of combining any two of these rotations.
    b. Give a list of rules that is sufficient for filling in the table using calculations.
    c. Compare this system to the symmetries of a non-square rectangle and the symmetries of an equilateral triangle. (What is the same? What is different?)

- Prove that composition of functions is associative. (Don't just write a bunch of symbols without an explanation of what those symbols mean.)

- Prove function composition is associative. Let $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ and $\boldsymbol{D}$ be sets and f: $\boldsymbol{C}\rightarrow\boldsymbol{D}$, g:$\boldsymbol{B}\rightarrow\boldsymbol{C}$, and h: $\boldsymbol{A}\rightarrow\boldsymbol{B}$. Show that $f \circ (g \circ h) = (f \circ g) \circ h$

- How many 1-1 onto (bijective) functions are there from the set {A, B, C} to itself? (Describe each function.)

a. Prove that *in general* the composition of two bijective functions is also a bijective function.
b. Make a table that shows the result of composing any pair of these functions.
c. How does this table compare to the table of symmetries of a triangle?

- Consider all the symmetries of a square. How many are there?
  a. Make a table that shows the result of combining any two of these symmetries. *Hint: Try to develop a set of rules like those for the triangle and fill in the table by calculating*.
  b. How does this table compare to the composition table for the 1-1 onto functions from the set {A, B, C, D} to itself? *Hint: You should not have to make a table or even find all of the functions to answer this question*.

- What is the smallest number of "basic" moves that are needed to generate all of the symmetries of a square? Write each of the symmetries in terms of these basic moves.
  a. Create an operation table that gives the results of combining any two of the symmetries.
  b. Create a minimal set of rules needed to create the table without moving the square, and provide enough sample calculations to illustrate the use of each rule.

- Compile a list of properties that all four of the situations we have considered (symmetries of triangle, square, and non-square rectangle and the rotations of a square) have in common.

- Consider the pair of functions f and g given by: $f(x) = \frac{1}{x}$ for all $x \in$ R $\setminus\{0,1\}$ and $g(x) = \frac{1}{1-x}$ for all $x \in$ R $\setminus\{0,1\}$.
  b. How many total functions can be generated by composing combinations of any number of these two functions? Justify your assertion.
  c. Make a table that gives the result of composing any two of the functions that you generated to answer part (a).
  d. List at least 5 interesting properties/rules/relationships that you discovered while working on parts (a) and (b).

- Let ***S*** be the set of symmetries of an equilateral triangle. We developed the following short list of rules that can be used to calculate any combination of elements of ***S***.

Rules	
Rule #1	$I = F^2 = R^3$
Rule #2	$F = RFR$

(Associative)
$AI = IA = A$ where A is in $\boldsymbol{S}$ (Identity)
$\forall\ A \in \boldsymbol{S}\ \exists\ A^{-1} \in \boldsymbol{S}$ s.t. $AA^{-1} = A^{-1}A = I$ (Inverses)

Complete the following calculation using the rules above. **Be sure to include all steps and justify each step.**

F(FF)(FR)RR =

- Let $\boldsymbol{S}$ be the set of symmetries of an equilateral triangle. We developed the following short list of rules that can be used to calculate any combination of elements of $\boldsymbol{S}$.

Rules
Rule #1 $I = F^2 = R^3$
Rule #2 $F = RFR$
(Associative)
$AI = IA = A$ where A is in $\boldsymbol{S}$ (Identity)
$\forall\ A \in \boldsymbol{S}\ \exists\ A^{-1} \in \boldsymbol{S}$ s.t. $AA^{-1} = A^{-1}A = I$ (Inverses)

Prove the following statements using the rules in the table. **Be sure to include all steps and justify each step.**

a. (RF)(RF) = I
b. $RF = FR^2$

- Consider the set of complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbf{R}\}$. Show that the addition of complex numbers, where $(a + bi) + (c + di) = (a + c) + (b + d)i$, is associative.

- Consider the set of complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Show that the multiplication of complex numbers, where $(a + bi)\times(c + di) = (ac - bd) + (ad + bc)i$, is associative.

Problems that require the definition of *group*

- Write the definition of *group*.
- State and prove a cancellation law for groups.

- Prove or disprove the following are groups:

a. The set {-2, 0, 2} with regular addition.
b. The set {-1, 0, 1} with regular multiplication.
c. The set {-1, 1} with regular multiplication.

- Is this a group?

+	0	1
0		
1		

- Is this a group?

×	0	1
0		
1		

- Is this a group?

*	*a*	*b*
a	*b*	*a*
b	*a*	*b*

- Is this a group? [Recommended to be assigned before starting Unit 3 (Quotient Groups)]

+	EVEN	ODD
EVEN		
ODD		

- Consider the group of symmetries of an equilateral triangle (R = 120° Clockwise Rotation and F = Reflection across the vertical axis):
[Recommended to be assigned before starting subgroup part of Unit 1 (Groups)]

	F	*FR*	*RF*	*I*	*R*	*RR*
F	*I*	*R*	*RR*	*F*	*FR*	*RF*
FR	*RR*	*I*	*R*	*FR*	*RF*	*F*

RF	*R*	*RR*	*I*	*RF*	*F*	*FR*
I	*F*	*FR*	*RF*	*I*	*R*	*RR*
R	*RF*	*F*	*FR*	*R*	*RR*	*I*
RR	*FR*	*RF*	*F*	*RR*	*I*	*R*

e. Explain how you can tell that every element has an inverse *by looking at the table*.
f. Demonstrate how to calculate $F(RF)FR$ using the definition of group and the rules (1) $RF = FRR$, (2) $FF = I$, and (3) $RRR = I$. Show all steps and justify each step (by naming a rule or part of the definition of group).
g. Can you eliminate one of these symmetries and still have a group? Justify your response.
h. Can you eliminate of these symmetries and still have a group? Justify your response.

- Complete the following table to get a group AND prove that there is only one possible way to fill out the table.

•	*a*	*b*	*c*
a			
b			
c			*a*

- Let $\boldsymbol{G}$ be a group. Prove: If $(ab)^2 = a^2 b^2 \ \forall\ a, b \in \boldsymbol{G}$ then $\boldsymbol{G}$ is abelian (commutative).

- Let $\boldsymbol{G}$ be a group. Show that $\boldsymbol{G}$ is commutative if and only if $(ab)^2 = a^2b^2$ for all $a, b \in \boldsymbol{G}$.

- Let $\boldsymbol{G}$ be a group.
  a. Show that $\boldsymbol{G}$ is commutative if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in \boldsymbol{G}$.
  b. In general what is $(ab)^{-1}$? Prove your assertion.

- Let $\boldsymbol{G}$ be a group and let $a \in \boldsymbol{G}$.
  Prove that a is the identity of $\boldsymbol{G}$ if and only if $aa = a$.

- Let G be a group.
  a. Prove that each element of G occurs *at least once* in each row of the operation table for G.
  b. Prove or provide a counterexample:
     i. $(ab)^2 = a^2b^2 \ \forall\ a, b \in G$
     ii. $(ab)^{-1} = b^{-1}a^{-1} \ \forall\ a, b \in G$

- Let G be a group with identity I. Let $a, b \in G$. Suppose that $|a| = 2$, $|b| = 5$, and $ba = ab^4$.
  a. Prove that $b^2a = ab^3$.

b. Prove that G is *not* commutative.

- Find the order of each element of D_8.
- Let $\boldsymbol{G}$ be a group. Suppose that $a, b \in \boldsymbol{G}, |a| = 2, |b| = 4$ and $ab = b^3a$.

  a. Prove that $bab = a$.
  b. Prove that $ab^2 = b^2a$.

- Prove that the identity element of a group is unique.
- Is the identity of a group unique? (i.e. can a group only have one identity element?) Justify (prove) your response.
- Are these things groups?
  a. Rational numbers under multiplication
  b. Integers under subtraction
  c. {-2, 0, 2} under some kind of special addition
- Can you find set-operation pairs that satisfy the given properties?
  a. Can you find a set that is closed under an operation and has an identity element but is not a group?
  b. Can you find a set that is associative, has an identity element, and inverses, but is not closed?
  c. Can you find a set that is associative, is closed, and has inverses, but is not a group?
- Prove that in a group, inverse elements are unique.
- Prove the following about inverses:
  a. If b is an element of a group, what is $(b^{-1})^{-1}$? Prove it.
  b. If a and b are elements of an additive group, what is $-(a+b)$? Prove it.
- Let $(G, *)$ and $(H, \bullet)$ be groups. Consider the set $G \times H = \{(g, h) | g \in G \text{ and } h \in H\}$. (So the elements of $G \times H$ are ordered pairs where the first element in the pair is from G and the second element in the pair is from H.)

Define the operation, $\oplus$, on $G \times H$ by $(g_1, h_1) \oplus (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$.

a. Find the order of each element of $C_2 \times C_3$.

b. Is $C_2 \times C_3$ isomorphic to the symmetries of a triangle? Prove or disprove.

c. Is $C_2 \times C_3$ isomorphic to C_3? Prove or disprove.

[Because of the centrality of the dihedral groups in the curriculum, we often treat cyclic groups using multiplicative notation and denote these groups by C_n where the elements are either considered to be rotations of an n-gon. The $\mathbb{Z}_n$ groups appear at the end of the course as quotient groups when we discuss the Fundamental Homomorphism Theorem. Clearly if an instructor chooses to introduce $\mathbb{Z}_n$ groups less formally early in the course, questions like this can be adjusted to compensate.]

- Let $(G, *)$ and $(H, \#)$ be groups. Consider the set $G \times H = \{(g, h) | g \in G \text{ and } h \in H\}$. (So the elements of $G \times H$ are ordered pairs where the first element in the pair is from G and the second element in the pair is from H.)

  Define an operation, $\oplus$, on $G \times H$ by $(g_1, h_1) \oplus (g_2, h_2) = (g_1 * g_2, h_1 \# h_2)$.

  a. Make an operation table for $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$
  b. Prove that, if $(G, *)$ and $(H, \#)$ are groups then $(G \times H, \oplus)$ is a group.

- Definition: Let G be a group. The ***center*** of G, $Z(G)$, is defined to be the set $\{z \in G | zg = gz \text{ for all } g \in G\}$.

So, the center of G, $Z(G)$, is the set of elements that commute with all of the other elements in G.

Getting familiar with the center of a group (you don't have to prove these).

i. What is the center of D_6 (the symmetries of a triangle)?
ii. What is the center of D_8 (the symmetries of a square)?
iii. What is the center of an *abelian* group?

- Suppose that G is a finite group.
  (a) Finish the following definition: "G is commutative if . . ."
  (b) Provide an example of a finite commutative group. Also, provide a *brief* explanation of how you know this is a commutative group.
  (c) Provide an example of an infinite non-commutative group. Also, provide a *brief* explanation of how you know this is a non-commutative group.
  (d) Prove that if every non-identity element in G has order 2, then G is commutative.

- Let G be a group.
  a) Define the center $Z(G)$ of G.
  b) If $x \in Z(G)$ has order 4 and $y \in G$ has order 5, prove that xy has order 20.
  c) Suppose instead that $x \in Z(G)$ has order 4 and $y \in G$ has order 4. What is the

order of xy? *Extra Credit:* Suppose $x \in Z(G)$ has order m and $y \in G$ has order n. Find the order of xy.

- Under what conditions do real valued functions (under composition) form a group? Prove it.

- Definition: Let $\boldsymbol{G}$ be a group. The center of $\boldsymbol{G}$, $\boldsymbol{Z}(\boldsymbol{G})$, is $\{a \in \boldsymbol{G} : ag = ga \ \forall \ g \in \boldsymbol{G}\}$.
  a. In your own words, describe what the center of a group is.

  b. What is the center of D_6?

  c. What is the center of D_8?

  d. What is the center of an *abelian* group?
-

Subgroups

Problems that can work before *subgroup* is defined

- Let $\boldsymbol{G}$ be a group and $\boldsymbol{H}$ a subset of $\boldsymbol{G}$. $\boldsymbol{H}$ is a *subgroup* of $\boldsymbol{G}$ if it is a group with respect to the operation defined on $\boldsymbol{G}$.
  a. List all of the subgroups of $\boldsymbol{D}_6$ (the group of symmetries of an equilateral triangle.)
  b. List all of the subgroups of $\boldsymbol{D}_8$ (the group of symmetries of a square.)
  c. List all of the subgroups of $(\boldsymbol{Z}, +)$.

- Definition: Let $\boldsymbol{G}$ be a group. The center of $\boldsymbol{G}$, $\boldsymbol{Z}(\boldsymbol{G})$, is $\{a \in \boldsymbol{G} : ag = ga \ \forall \ g \in \boldsymbol{G}\}$.
  e. In your own words, describe what the center of a group is.

  f. What is the center of D_6?

  g. What is the center of D_8?

  h. What is the center of an *abelian* group?

- Let G be a group, and fix an element a in G.
  Consider the set $H_a = \{g \in G \mid ga = ag\}$.

  a) Let G be the symmetries of a triangle and let $a \in$ R. Find H_R.
  b) Let $(G, *)$ be a group and let $a \in$ G. Show that $(H_a, *)$ is a group.

- Let G be a finite group with g *in* G, such that g is not the identity. Show that $\langle g \rangle = \{g^n \mid n$ is a positive integer$\}$ is a group. (Show that you can express e as a positive power of g, and show that you can express g^{-k} as a positive power of g.)

- Let G be a group and $g \in G$ with $|g| = k$ where k is a non-negative integer. Define $\langle g \rangle = \{g^n: n \text{ is a non-negative integer}\}$. Basically $\langle g \rangle$ is just the set of all non-negative powers of g. It is called the *subgroup generated by g*. Prove that $\langle g \rangle$ is a subgroup of G.

- Definition: Let G be a group. The ***center*** of G, $Z(G)$, is defined to be the set $\{z \in G | zg = gz \text{ for all } g \in G\}$.

So, the center of *G, Z(G),* is the set of elements that commute with all of the other elements in *G*.

Getting familiar with the center of a group (you don't have to prove these).

i. What is the center of D_6 (the symmetries of a triangle)?
ii. What is the center of D_8 (the symmetries of a square)?
iii. What is the center of an *abelian* group?

- Let G be a group and g an element of G. The centralizer, C_g, of g is the set of elements of G that commute with g (i.e., $C_g = \{a \text{ in } G: ag = ga\}$).
  a. Find the centralizer of each element of D_8.
  b. Let G be a group and $a \in G$. Prove that the *centralizer* of a is a subgroup of G.

Problems that require the definition of *subgroup*

- Is $\{0, 1, 2\}$ a subgroup of $(Z, +)$?

- Find a subgroup of the rotations of a square and prove that it is a subgroup.

- List all the subgroups of $\boldsymbol{D}_8$.

- Describe 3 different subgroups of $(\mathbf{Z}, +)$. Prove each is a subgroup.

- List all the subgroups of $(Z, +)$.

- Consider the group of symmetries, $\{I, R, R^2, F, FR, FR^2\}$, of an equilateral triangle. This group is often denoted by D_3.

  a. Does D_3 have a *subgroup* that has exactly 3 elements? Prove your assertion.
  b. Does D_3 have a *subgroup* that has exactly 4 elements? Prove your assertion.

- Prove or disprove: For any group **G**, the center of **G** is a subgroup of **G**.

- Prove the following theorem: Let ***G*** be a group and ***H*** a subset of ***G***. Then ***H*** is a subgroup iff 1) ***H*** is nonempty, 2) ***H*** is closed under the operation defined on ***G***, and 3) each element of ***H*** has its inverse in ***H***.

- Let ***G*** be a group and ***H*** a *nonempty finite* subset of ***G***. If ***H*** is a closed under the operation defined on ***G*** then ***H*** is a subgroup of ***G***

- Let G be the set of 2×2 real-valued matrices and let $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a + d = 0 \right\}$

  a) Prove or disprove: H is a subgroup of G under addition
  b) Prove or disprove: H is a subgroup of g under multiplication

- ***True or False?*** Decide if each statement is true or false, and give a brief justification or counterexample to support your answer.
  a) $\boldsymbol{Z}_6^*$ is a group under the operation of multiplication
  b) If a nonempty subset H of a group G is closed under the operation of G, then H is a subgroup of G.
  c) There exists a group of order n for any positive integer n.
  d) **Z** is a group under the operation of subtraction.

- Prove that, for any group G, the center of G is a subgroup of G.

- Identity and Inverses in Subgroups
  a. Let $(G, +)$ be a group and let $(H, +)$ be a subgroup of G. Prove that the identity of G must be the same as the identity of H.
  b. Let $(G, +)$ be a group and let $(H, +)$ be a subgroup of G and let h be in H. Prove the inverse of h in H is the same as the inverse of h in G.

- Suppose that H and K are subgroups of a group G.
  a) Prove that the intersection $H \cap K$ is a subgroup of G.
  b) Find a counterexample that demonstrates the union $H \cup K$ is not necessarily a subgroup of G.

- *Prove or disprove:* If H and K are both subgroups of a group G, then the union of H and K is a subgroup of G. What about the intersection of H and K?

- Suppose that H and K are subgroups of a group G.
  a) Prove that the intersection $H \cap K$ is a subgroup of G.
  b) Find a counterexample that demonstrates the union $H \cup K$ is not necessarily a subgroup of G. *Extra Credit:* Determine necessary and sufficient conditions for H

$\cup K$ to be a subgroup.

- Let G be a group. The **center** of a group, G, is defined to be the subset consisting of all elements $c \in G$ such that $cx = xc$ for all $x \in G$ (*i.e.,* the elements that commute with everything in G). The center of G is usually denoted $Z(G)$.

a) Find the center of the symmetries of a square and justify your response.

b) Prove that $Z(G)$ is a subgroup of G

c) If $x \in Z(G)$ has order 4 and $y \in G$ has order 5, prove that xy has order 20.

- Let $G = \mathbb{Z}_{20}$.
  a) Determine all generators of G.
  b) Determine all subgroups of G and explain how you can be certain you have found all of them.
  c) Sketch a subgroup lattice of G. *Extra Credit:* Determine the group of units of G, also denoted $U(20)$, and build its operation table.

- Let G be a group and let a be any element in G. The set generated by a, $\langle a \rangle$, is all powers (or multiples) of a. i.e., with multiplicative notation $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ or with additive notation $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$
  a) Find an infinite group that is generated by a single element. (When a group is generated by a single element, we call it a *cyclic group*.)
  b) Let G be $\mathbb{Q}^*$ (the rational numbers excluding zero) under multiplication and let $H = \langle 2 \rangle = \{2^k \mid k \in \mathbb{Z}\}$. Show that H is a subgroup of G.
  c) If the order of a is 20, what is the order of a^6? (To prove that the $a^6 = k$, you must show that $(a^6)^k = e$ and that k is the smallest positive integer such that $(a^6)^n = e$.)
  d) Prove that for any group G and any element a in G, $\langle a \rangle$ is a subgroup of G.

- Let H be a subgroup of G and define $N(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}$.
  a) Prove that $N(H)$ is a subgroup of G. (N stands for the *normalizer* of H in G.)
  b) If $H = Z(G)$, where $Z(G)$ denotes the center of G, what is $N(H)$?
  c) *Extra Credit:* Compute the normalizer of the subgroup $H = \langle (123) \rangle$ in S_3.

Problems that require topics not included explicitly in the IOAA materials

- Consider the set of all 2×2 real-valued matrices.
  a) Is this a group under matrix multiplication?
  b) Is this a group under matrix addition?

-

Isomorphism

Problems that can work before *isomorphism* is defined

- Determine whether the table below could be an operation table for the *group of symmetries of a rectangle*. Show all work and completely justify your response.

*	A	B	C	D
A	B	A	D	C
B	A	B	C	D
C	D	C	A	B
D	C	D	B	A

- Determine whether the table below could be an operation table for the *group of rotations of a square*. Show all work and completely justify your response.

*	A	B	C	D
A	B	A	D	C
B	A	B	C	D
C	D	C	A	B
D	C	D	B	A

- I found this group table lying on my desk (I checked that it was associative by testing 216 cases, you can quickly check the other properties yourself!). Could this group be D_6?

*	A	B	C	D	E	G
A	B	A	D	C	G	E
B	A	B	C	D	E	G
C	G	C	B	E	D	A

D	E	D	A	G	C	B
E	D	E	G	A	B	C
G	C	G	E	B	A	D

For convenience, here is a table for D6.

	I	R	R^2	F	FR	FR^2
I	I	R	R^2	F	FR	FR^2
R	R	R^2	I	FR^2	F	FR
R^2	R^2	I	R	FR	FR^2	F
F	F	FR	FR^2	I	R	R^2
FR	FR	FR^2	F	R^2	I	R
FR^2	FR^2	F	FR	R	R^2	I

a. Why doesn't the correspondence
A $\leftrightarrow F$, B $\leftrightarrow I$, C $\leftrightarrow FR^2$, D $\leftrightarrow R$, E $\leftrightarrow FR$, G $\leftrightarrow R^2$ work for showing this group is D_6?

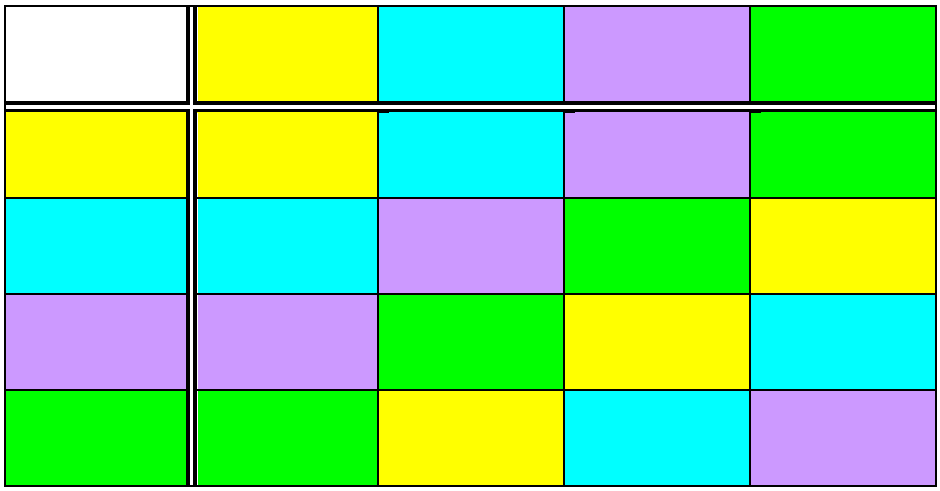
b. Suppose that I wanted to match up the elements by saying that C $\leftrightarrow F$ and G $\leftrightarrow R$. What would the other four correspondences have to be?

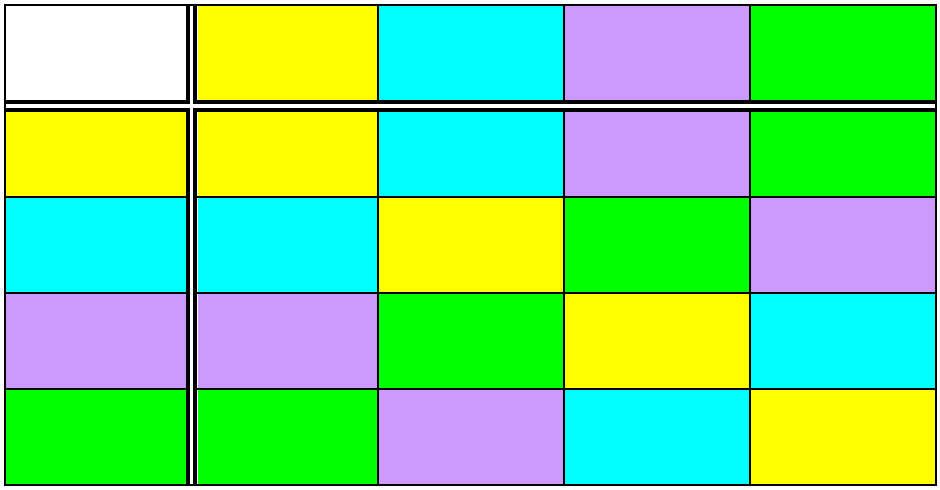
c. We use the term *isomorphic* to express the idea that two groups are essentially the same (equivalent but not necessarily equal). So the group given by the mystery table is isomorphic to $\boldsymbol{D}_6$.

d. Write a definition for isomorphic.

- How many groups are there with 4 elements? [If two groups are isomorphic, they should be considered the same – they count as just one group.]

- Prove that any group of order 4 must be isomorphic to one of the following groups:





- How many non-isomorphic groups of order 3 are there? Prove it. How many non-isomorphic groups of order 4 are there? Prove it. (i.e. How many *different* ways can you complete an operation table to make a group with this many elements?)

- Let $G = \mathbb{Z}_2 \times \mathbb{Z}_3$. Build the multiplication table for G. Is G isomorphic to D_6? Explain.

- Suppose that G is a finite group.
  (a) Finish the following definition: "G is **Abelian** if . . ."
  (b) Prove that if every non-identity element in G has order 2, then G is Abelian.

Extra Credit: Use the above result to explain why, structurally speaking, there must be exactly two groups of order 4.

Problems that require the definition of *isomorphism*

- Consider the group G defined by the following operation table:

*	**A**	**B**	**C**	**D**
A	D	C	B	A
B	C	A	D	B
C	B	D	A	C
D	A	B	C	D

G must be isomorphic to one of two groups. Name or otherwise identify these groups and prove that G is isomorphic to one of the two groups you named.

- Prove or disprove that the following table represents a group isomorphic to $\mathbf{D}_6$.

*	A	B	C	D	E	F
A	D	C	B	A	F	E
B	F	E	A	B	D	C
C	E	F	D	C	A	B
D	A	B	C	D	E	F
E	C	D	F	E	B	A
F	B	A	E	F	C	D

- Let $(G, \cdot)$ and $(H, *)$ be groups. And let $\varphi: G \to H$ be an isomorphism. Let e_G be the identity of G and e_H be the identity of H.
    a. Prove that if G is abelian, then H is abelian.
    b. Let $g \in G$ and $k \in N$. Prove $g^k = e_G$ iff $\varphi(g)^k = e_H$. (Recall that g^k means a "product" of k g's.)

- Let $(G, \cdot)$ and $(H, *)$ be groups. And let $\varphi: G \to H$ be an isomorphism. Let e_G be the identity of G and e_H be the identity of H.
    a. Prove that function φ has an inverse. (Remember it needs to be everywhere well-defined on H.)
    b. Prove that φ^{-1} is an isomorphism from H to G.

- Consider the group whose operation is given by the table below.
    a. Is it isomorphic to C_4, the rotations of a square? Justify using the definition.
    b. Is it isomorphic to $\boldsymbol{V}_4$, the symmetries of a non-square rectangle? Justify using the definition.

*	A	B	C	D
A	D	C	B	A
B	C	A	D	B
C	B	D	A	C
D	A	B	C	D

- Prove the following theorem: Suppose $(\boldsymbol{G}, \bullet)$ and $(\boldsymbol{H}, *)$ are isomorphic groups. Then if $\boldsymbol{G}$ is abelian then $\boldsymbol{H}$ is abelian.

- Suppose $(G, *)$ and $(H, +)$ are isomorphic. Prove that if G is commutative then H is commutative.

- Let $(G, \bullet)$ and $(H, *)$ be groups and $\phi: G \to H$ be an isomorphism. Let e be the identity in G. Prove that $\phi(e)$ is the identity in H.

- Suppose $(G, *)$ and $(H, +)$ are isomorphic and $\phi: G \longrightarrow H$ is an isomorphism. Then prove $\phi(e_G) = e_H$.

- Prove from first principles (as opposed to simply citing a theorem) that $\mathbb{Z}_4 \times \mathbb{Z}_2$ cannot be isomorphic to $\mathbb{Z}_8$.

- Let $(G, \bullet)$ and $(H, *)$ be groups and $\phi: G \to H$ be an isomorphism. Let $a, b \in G$. Prove that if a is the inverse of b, then $\phi(a)$ is the inverse of $\phi(b)$.

- Prove the following theorem: Suppose $(\boldsymbol{G}, \bullet)$ and $(\boldsymbol{H}, *)$ are groups and $\phi: \boldsymbol{G} \to \boldsymbol{H}$ is an isomorphism. Let $a \in \boldsymbol{G}$, then $\phi(a)^{-1} = \phi(a^{-1})$. Hint: You might want to make up and prove a little lemma about the identity first.

- Prove the following lemma: Suppose $(\boldsymbol{G}, \bullet)$ and $(\boldsymbol{H}, *)$ are groups and $\phi: \boldsymbol{G} \to \boldsymbol{H}$ is an isomorphism. Let $a \in \boldsymbol{G}$ and $n \in \boldsymbol{N}$, then $\phi(a)^n = \phi(a^n)$.

- Suppose (G, *) and (H, +) are isomorphic and $\phi: G \longrightarrow H$ is an isomorphism. Let a be in G and n be a natural number, prove $\phi(a^n) = \phi(a)^n$. [This should be a proof by mathematical induction.]

- Prove the following theorem: Suppose ($\boldsymbol{G}$, $\bullet$) and ($\boldsymbol{H}$, $*$) are groups and ϕ: $\boldsymbol{G}\rightarrow\boldsymbol{H}$ is an isomorphism. Let $a \in \boldsymbol{G}$. Then $|\phi(a)|=|a|$.

- Prove the following theorem: Suppose that ($\boldsymbol{G}$, $\bullet$) and ($\boldsymbol{H}$, $*$) are isomorphic group. If $\boldsymbol{G}$ is cyclic, then $\boldsymbol{H}$ is cyclic.

- Prove that if $\varphi : G \longrightarrow H$ is an isomorphism, then $Z(G) \cong Z(H)$.

- Is the group of *rotations* of a hexagon isomorphic to D_3? Justify your response.

- For each pair of groups, determine whether they are isomorphic (prove your assertion).
  b. ($\boldsymbol{Z}$, +) and ($2\boldsymbol{Z}$, +) [The integers under addition and the even integers under addition]
  c. ($\boldsymbol{R}$, +) and ($\boldsymbol{R}\backslash\{0\}$, $\bullet$) [The real numbers under addition and the non-zero real numbers under multiplication]
  d. $\boldsymbol{D}_8$ [The symmetries of a square] and $\boldsymbol{C}_8$ [The rotations of an octagon].
  e. $\boldsymbol{D}_6$ and the group of functions generated by functions f and g given by: $f(x) = \frac{1}{x}$ for all $x \in \mathbb{R} \backslash \{0,1\}$ and $g(x) = \frac{1}{1-x}$ for all $x \in \mathbb{R} \backslash \{0,1\}$. [Yes this was a group also! Can you prove it?]

- Prove the following about isomorphisms:
  a. The *group* $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to the *group* $\mathbb{Z}_6$.
  b. The *group* $\mathbb{Z}$ is isomorphic to the *group* $2\mathbb{Z}$.
  c. Is the *group* $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the *group* $\mathbb{Z}_4$?

- Consider the group of non-zero real numbers under multiplication. I can pick any non-identity element in this set (call this element x) and create a cyclic subgroup that is all of the integer powers of x.

  Fix x, some non-identity, non-zero element of the real numbers, and let $G = \{x^n$ for all $n \in \mathbb{Z}\}$. This is a group under multiplication. (You can prove it if you don't believe me.)

  Show that (G, *) is isomorphic to ($\mathbb{Z}$,+). If you define a function, don't worry about showing that it is indeed a function (i.e., well-defined and everywhere defined).

- Let $G = \{e, a, a^2, a^3\}$ be a cyclic group of order 4 and H be the multiplicative group $\{1, -1, i, -i\}$ of complex numbers, (where $i*i = -1$). Come up with 2 isomorphisms between G and H and explain why there are no others.

- Prove or disprove that the following table represents a group isomorphic to $\mathbf{C}_4$. Make sure your justification is as complete as possible – don't leave anything for the reader to verify. [$\mathbf{C}_4$ can be replaced by $\mathbf{Z}_4$ if that group is introduced by the instructor early in the course instead of later as a quotient group.]

*	A	B	C	D
A	D	C	B	A
B	C	A	D	B
C	B	D	A	C
D	A	B	C	D

- Prove or disprove that the *group of symmetries of a circle* is isomorphic to the *group of positive real numbers under multiplication*.

- Prove that if G is any cyclic group of order n, then $G \cong \mathbf{Z}_n$. (Please construct the isomorphism rather than simply citing a theorem.)

- Consider the groups $\mathbf{Z}_6$ and $U(7)$, the group of units of $\mathbf{Z}_7$ (also denoted $\mathbf{Z}_7^*$).
  a) List the elements in $U(7)$. What is the group operation in $U(7)$? What is the group operation in $\mathbf{Z}_6$?
  b) Prove that $\mathbf{Z}_6 \cong U(7)$.

- Let $G = (a)$ and $H = (b)$ be cyclic groups of order 6.
  a) Complete the following table so that α and β are isomorphisms from G to H.

x	**e**	a	a^2	a^3	a^4	a^5
$\alpha(x)$		b				
$\beta(x)$		b^5				

  b) Explain why these are the only two isomorphisms from G to H.

- Prove from first principles (as opposed to simply citing a theorem) that $\mathbb{Z}_4 \times \mathbb{Z}_2$ cannot be isomorphic to $\mathbb{Z}_8$.

- Let $G = \{e, a, a^2, a^3\}$ be a cyclic group of order 4 and H be the multiplicative group $\{1, -1, i, -i\}$ of complex numbers. Come up with 2 isomorphisms between G and H and explain why there are no others.

- Let $G = \mathbb{Z}_2 \times \mathbb{Z}_3$. Build the multiplication table for G. Is G isomorphic to S_3? Explain.

- If $G \cong H$, is $Z(G) \cong Z(H)$? Explain.

Homomorphism

[NOTE: Homomorphisms appear in Unit 3 (Quotient Groups) of the IOAA curriculum when the Fundamental Homomorphism Theorem is treated. However, instructors may choose to treat homomorphisms at the end of Unit 2 (Isomorphism).]

Problems that can work before *homomorphism* is defined

Problems that require the definition of *homomorphism*

- Prove that 1) one of these is not a function, 2) one is a function but not a homomorphism, and 3) one is a homomorphism.

$\theta_1: \mathbb{Z} \to C_4$ given by $\theta_1(n) = R^{2n}$ for all $n \in \mathbb{Z}$

$\theta_2: C_4 \to \mathbb{Z}$ given by $\theta_2(R^n) = n$ for all $R^n \in C_4$

$\theta_3: C_4 \to C_8$ given by: $I \to I$, $R \to R$, $R^2 \to R^2$, $R^3 \to R^3$

- Find the Kernel and Image of $\theta_1: \mathbb{Z} \to C_4$ given by $\theta_1(n) = R^{2n}$ for all $n \in \mathbb{Z}$
- Let G, H be groups and $\varphi: G \to H$ be a homomorphism. Prove that the Image and Kernel of φ are subgroups.

- Use $\mathbb{Z}_6$ and D_3 to come up with each of the following:

a. A homomorphism between two groups where one is commutative and the other is not.
b. A homomorphism where a self-inverse is hit by something other than a self-inverse.
c. A homomorphism where an order 6 element maps to an order 3 element.

- NOTE: The next 3 problems also assume students have completed at least part of the quotient group unit.

- Consider the homomorphism θ: $\mathbb{Z} \rightarrow C_4$ given by $\theta(n) = R^{2n}$ for all $n \in \mathbb{Z}$.
  a. Is θ 1-1? Justify.
  b. Is θ onto? Justify.
  c. *Without changing the rule for* θ, what can we change to make θ onto?
  d. *Without changing the rule for* θ *(much)*, what can we change to make θ 1-1?
  e. Make a table for the new domain group.
  f. describe the new isomorphism (say where each of the new domain elements go).

- Define a homomorphism θ: $\mathbf{Z} \rightarrow D_6$ whose image consists of 3 elements.
  e. Show θ is a homomorphism.
  f. Is θ 1-1? Justify.
  g. What is the Kernel of θ?
  h. Is θ onto? Justify.
  i. *Without changing the rule for* θ, what can we change to make θ onto?
  j. *Without changing the rule for* θ *(much)*, what can we do to make θ 1-1?
  k. Make a table for the new domain group.
  l. Make a table for the new codomain group.
  m. Describe the new isomorphism (say where each of the new domain elements go).

- Define a non-trivial homomorphism θ: $120\mathbf{Z} \rightarrow C_3$.
  a. Show θ is a homomorphism.
  b. Is θ 1-1? Justify.
  c. What is the Kernel of θ?
  d. Is θ onto? Justify.
  e. *Without changing the rule for* θ *(much)*, what can we do to make θ 1-1?
  f. Make a table for the new domain group.
  g. Describe the new isomorphism (say where each of the new domain elements go).

- Prove the following lemma: Let G, H be groups and θ: $G \rightarrow H$ be a homomorphism. Let a, $b \in G$. Then $\theta(a) = \theta(b) \Leftrightarrow b^{-1}a \in \text{Ker}\theta$.

- Find a group homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_4, \oplus)$.
  d. Prove that the mapping you found is in fact a group homomorphism.
  e. What is the kernel of your mapping?

- Prove that, if ϕ is a group homomorphism then Ker ϕ is a subgroup of R.

- Determine which of the following maps are homomorphisms and, for the ones that are homomorphisms, determine its kernel and image. (You do not need to prove your responses.)
  a. $\theta: (\mathbb{Z}, +) \longrightarrow (\mathbb{R}, +)$ defined by $\theta(n) = n$.
  b. $\theta: (\mathbb{R}, +) \longrightarrow (\mathbb{Z}, +)$ defined by $\theta(x) = the\ greatest\ integer \leq x$.
  c. $\theta: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2$ defined by $\theta(n) = the\ remainder\ of\ n\ when\ divided\ by\ 2$.

- Commutativity
  a. Suppose $\phi: G \longrightarrow H$ is an isomorphism. Prove that, if G is commutative then H is commutative.
  b. Explain why your proof fails to show that, if there exists a homomorphism, $\theta: G \longrightarrow H$, and G is commutative then H is commutative.
  c. Provide an example to show that it is possible for there to exist a homomorphism, $\theta: G \longrightarrow H$, where G is commutative and H is not.

- Let (**G**, •) and (**H**, ∗) be groups and ϕ:**G**→**H** be a homomorphism.
  a. Prove that the image of ϕ, ϕ(**G**) is a subgroup of **H**.
  b. Prove that Ker ϕ is a subgroup of **G**

- If $\theta: G \rightarrow H$ is a homomorphism, prove that $\theta(a^{-1}) = \theta(a)^{-1}$.

- Describe all possible homomorphisms from (**Z**, +) to $\mathbf{C}_6$. Describe the kernel and image of each homomorphism. Choose one of your non-trivial homomorphisms and prove that it is a homomorphism.

- Kernel of a Homomorphism (Suppose G and H are groups)
  a. Give the definition of a **homomorphism** from G to H.
  b. Suppose $\varphi : G \rightarrow H$ is a homomorphism. Define Kerφ, the **kernel** of the homomorphism.
  c. Given a homomorphism $\varphi : G \rightarrow H$, prove that Ker$\varphi$ is a subgroup of G (prove *everything* you need to show that this is a subgroup).
  d. Prove that Kerφ is a *normal* subgroup of G (if you get stuck – try a different version of the normality definition) [This last part requires that normal subgroup has been defined. We typically use this problem just before treating the Fundamental Homomorphism Theorem.]

Quotient Groups

Problems that can work before *quotient group* is defined

- Is this a group? [Recommended to be assigned before starting Unit 3 of IOAA]

+	EVEN	ODD
EVEN		
ODD		

- Half of the symmetries of an equilateral triangle are *flips* and the other half are *rotations*.
    d. Is the combination of two *flips* always, sometimes, or never a *flip*? Justify your response.
    e. Is the combination of two *rotations* always, sometimes, or never a *rotation*? Justify your response.
    f. Is the combination of a *rotation* and a *flip* always, sometimes, or never a *rotation*? Justify your response.

- Definition: Let G be a group. The center of G, $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$.

So, the center of *G, Z(G),* is the set of elements that commute with all of the other elements in *G*.

d. Construct a quotient group of D_8 where the identity element **is** the center of D_8. Show that what you constructed is a group.
e. Construct a quotient group of D_8 where the identity element **is not** the center of D_8. Show that what you constructed is a group.
f. Construct a quotient group of D_6 where the identity element **is not** the center of D_6. Show that what you constructed is a group.

[This problem requires the term quotient group but does not require the formal part of the quotient groups unit to have been completed. It could work as a nice homework problem between the informal and formal parts of the quotient group unit.]

- Let $\mathbb{Z}_7^*$ be the set of numbers in $\mathbb{Z}_7$ that have a ***multiplicative inverse***. (For instance, $6*6 = 36 \equiv 1 \pmod 7$. So, because 6 has a multiplicative inverse, is it in the set $\mathbb{Z}_7^*$.) Below is an operation table for $(\mathbb{Z}_7^*, \times)$.

×	1	2	3	4	5	6

1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a. Form a 3-element quotient group out of $(\mathbb{Z}_7^*,\times)$ and make an operation table of this new group.
b. Construct a homomorphism, θ, from $(\mathbb{Z}_7^*,\times)$ to $\mathbb{Z}_6$ such that the $ker\theta$ has two elements.
c. Show that the quotient group you constructed in part a. is isomorphic to the image of $\mathbb{Z}_7^*$ under the θ you constructed in part b.

- The last few problems in this set will work quite differently depending on whether students have advanced to the more formal parts of the quotient group unit or not.

  - Prove that if H is a normal subgroup then G/H is a group.

  - Consider the homomorphism θ: $\mathbb{Z} \rightarrow C_4$ given by $\theta(n) = R^{2n}$ for all $n \in \mathbb{Z}$.
    a. Is θ 1-1? Justify.
    b. Is θ onto? Justify.
    c. *Without changing the rule for* θ, what can we change to make θ onto?
    d. *Without changing the rule for* θ *(much)*, what can we change to make θ 1-1?
    e. Make a table for the new domain group.
    f. describe the new isomorphism (say where each of the new domain elements go).

  - Define a homomorphism θ: $\mathbf{Z} \rightarrow D_6$ whose image consists of 3 elements.
    a. Show θ is a homomorphism.
    b. Is θ 1-1? Justify.
    c. What is the Kernel of θ?
    d. Is θ onto? Justify.
    e. *Without changing the rule for* θ, what can we change to make θ onto?
    f. *Without changing the rule for* θ *(much)*, what can we do to make θ 1-1?
    g. Make a table for the new domain group.
    h. Make a table for the new codomain group.
    i. Describe the new isomorphism (say where each of the new domain elements go).

- Define a non-trivial homomorphism θ: $120\mathbf{Z} \rightarrow C_3$.
    h. Show θ is a homomorphism.
    i. Is θ 1-1? Justify.
    j. What is the Kernel of θ?
    k. Is θ onto? Justify.
    l. *Without changing the rule for* θ *(much)*, what can we do to make θ 1-1?
    m. Make a table for the new domain group.
    n. Describe the new isomorphism (say where each of the new domain elements go).

Problems that require the definition of *quotient group*

- Prove that if H is a normal subgroup then G/H is a group.

- Prove the Fundamental Homomorphism Theorem: Let G, H be groups and ϕ: $G \rightarrow H$ be a homomorphism. Then $G/Ker\phi$ is isomorphic to $Im\phi$.

- Let $G = D_8$, and $H = \{I, FR\}$. List all the cosets of H in G.

- Prove Lagrange's Theorem: Suppose that G is a finite group and H is a subgroup of G. Then $|H|$ divides $|G|$. [More precisely, this requires the definition of 'coset'. So this could be assigned as soon as cosets emerge in the quotient group reinvention sequence as the only way to partition a group that could result in a quotient group (even if the term quotient groups has not been introduced).]

- Suppose that the group G has order 12, that φ is a homomorphism from G to H, and that G has 3 normal subgroups: $\{0\}$, all of G, and K, a three element subgroup. Use the fundamental homomorphism theorem to determine the possible orders of $\varphi(G)$. Explain your solution.

- Suppose that the group G has order 8, that φ is a homomorphism from G to H, and that G has 4 normal subgroups: $\{0\}$, all of G, K_1, a two element subgroup, and K_2 a four element subgroup. Use the fundamental homomorphism theorem to determine the possible orders of $\varphi(G)$.

- Prove that, for any group G, the center of G is a normal subgroup of G. (Hint: Let $H = Z(G)$. Show that $gH=Hg$ for all g in G. Prove this by set inclusion.) [This is the first definition of normal that arises in this curriculum. The hint can be adjusted or removed after additional definitions have been introduced.]

- Kernel of a Homomorphism (Suppose G and H are groups)

e. Give the definition of a **homomorphism** from G to H.
f. Suppose $\varphi : G \to H$ is a homomorphism. Define Kerφ, the **kernel** of the homomorphism.
g. Given a homomorphism $\varphi : G \to H$, prove that Kerφ is a subgroup of G (prove *everything* you need to show that this is a subgroup).
h. Prove that Kerφ is a *normal* subgroup of G (if you get stuck – try a different version of the normality definition) [This last part requires that normal subgroup has been defined. We typically use this problem just before treating the Fundamental Homomorphism Theorem.]

- Describe 4 different homomorphisms from $(\mathbf{Z}, +)$ to $\mathbf{Z}_4$. Describe the kernel and image of each homomorphism. Prove each is a homomorphism. Hint: Once you have one that is non-trivial, modify it slightly to get the other 2 non-trivial homomorphisms. Explain why only these 4 homomorphisms are possible.

- Describe 4 different homomorphisms from Z_8 to $\mathbf{Z}_4$. Describe the kernel and image of each homomorphism. Prove each is a homomorphism. Explain why only these 4 homomorphisms are possible.

- Let G be a group.
  a) Give the formal definition of an *automorphism* of G.
  b) Prove that if the map φ: $G \to G$ defined by $\varphi(x) = x^{-1}$ is an automorphism, then G is abelian.

- Let G be a group.
  a. Give a definition of a **normal** subgroup of G. (You may state either our original definition or the one we later proved was equivalent.)
  b. Let n be a fixed integer and consider $H = \{g^n \mid g \in G\}$. Prove that H is a normal subgroup of G. (You may find the equivalent definition more useful than our original here.)
  c. Explain briefly why "normality" is an important property for a subgroup to have.

- Imagine you are talking to a freshman math major; she is a sharp student who knows calculus and what the real numbers are, for example, but has no specific knowledge of group theory. Describe to her what a *group* is in a few sentences, and try to give her a sense of the general content and purpose of group theory. What's the goal of the subject? Why, as a math major, should she be required to take a course in it?
  (Just a paragraph or two here.... I don't need a novel!)

- Consider the group $G = \mathbf{Z}_4 \times \mathbf{Z}_6$.
  a) What is $|G|$? List three elements in G and give their orders.
  b) Let $H = \langle(0, 1)\rangle$ be the cyclic subgroup of G generated by the element $(0, 1)$. List the elements in H and explain how you know (without any computation) that H

must be a normal subgroup of G.

c) How many (left) cosets does H have in G? List the elements in G/H by giving a representative for each coset.

d) Determine what group $(\mathbf{Z}_4 \times \mathbf{Z}_6)/\langle(0, 1)\rangle$ is isomorphic to and prove your answer.

- Let G be a group. Recall that $\text{Inn}(G) = \{\alpha_x \mid \alpha_x(g) = xgx^{-1} \text{ for all } g \in G\}$ is the set of all inner automorphisms of G. Define a map $\varphi : G \to \text{Inn}(G)$ by $\varphi(x) = \alpha_{x^{-1}}$.

a) Show that φ is a homomorphism.

b) Show that $\text{Im}\varphi = \text{Inn}(G)$ and $\text{Ker}\varphi = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. (Bonus point: the kernel is what familiar subgroup of G?)

c) When is φ an isomorphism? Be as specific as you can.

- Let G be a group. Recall that the **center** of G is $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$, the set of elements x that commute with *all* elements in G.

a) Explain why $Z(G)$ is a normal subgroup of G. Explain why H is normal in G when H is any subgroup $H \leq Z(G)$.

b) If $H \leq Z(G)$ and G/H is cyclic, prove that G is abelian.

- We say a group G is **generated** by a set of elements $\{g_1, g_2, \ldots, g_n\}$ if every element $a \in G$ can be written as a composition of these elements (under whatever operation is specified in the group). Explain why a homomorphism φ: $G \to H$ (and therefore an isomorphism and automorphism) is entirely determined by where φ sends the generators of G.

- Describe all the homomorphisms from $\mathbf{Z}_{24}$ to $\mathbf{Z}_{18}$.

- Define φ: $\mathbf{R} \to \mathbf{C}^*$ by $\varphi(x) = \cos x + i \sin x$. Show φ is a homomorphism, find its kernel and image, and apply the 1^{st} Isomorphism Theorem to obtain a description of a familiar group as a quotient of other familiar groups.

- Determine which of the following maps are homomorphisms. For each homomorphism, determine its kernel and image.

a) $\varphi : \mathbf{Z} \to \mathbf{R}$ (under addition) defined by $\varphi(n) = n$.

b) $\varphi : \mathbf{R} \to \mathbf{Z}$ (under addition) defined by $\varphi(x) =$ the greatest integer $\leq x$.

c) $\varphi : \mathbf{Z}_6 \to \mathbf{Z}_2$ defined by $\varphi(x) =$ the remainder of x when divided by 2.

d) $\varphi : \mathbf{R}^* \to GL_2(\mathbf{R})$ defined by $\varphi(x) = \begin{bmatrix} 1 & 0 \\ 0 & x \end{bmatrix}$

e) $\varphi : \mathbf{R} \to GL_2(\mathbf{R})$ defined by $\varphi(x) = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}$

f) $\varphi : GL_2(\mathbf{R}) \to \mathbf{R}$ defined by $\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$

g) $\varphi : GL_2(\mathbf{R}) \to \mathbf{R}^*$ defined by $\varphi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$

More Advanced Group Theory Topics

- State the **Fundamental Theorem of Finite Abelian Groups**.

- Suppose G is an abelian group of order 450.
  a. List the all the possible isomorphism types for G. Explain briefly how you know these isomorphism types are all distinct.
  b. What is the largest possible order of a cyclic subgroup of the group $H = \mathbf{Z}_{12} \times \mathbf{Z}_{15}$? Explain your answer.

- Classify, up to isomorphism, all Abelian groups of order 756 (where $756 = 2^2 3^3 7$). Your solution should refer to your argument above (or similar thinking) to justify that each isomorphism type you list is indeed unique.

- Let $G = \mathbf{Z}_{10}$.
  a) Prove that G is isomorphic to the internal direct product of subgroups $H \times K$, where $H = \{0, 5\}$ and $K = \{0, 2, 4, 6, 8\}$.
  b) By finding more familiar groups that are isomorphic to H and K, write $\mathbf{Z}_{10}$ as an (external) direct product of two different groups.

- Let $GL_2(\mathbf{Z}_2)$ be the group of invertible 2 x 2 matrices with entries in $\mathbf{Z}_2 = \{0, 1\}$.
  a. List the elements of $GL_2(\mathbf{Z}_2)$. (*Hint: they must be invertible!)*
  b. Show that every element in $GL_2(\mathbf{Z}_2)$ can be written as a product of the matrices $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
  c. Prove that $GL_2(\mathbf{Z}_2)$ is isomorphic to the symmetric group S_3.

- Let A = $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and B = $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ be elements in $GL_2(\mathbf{R})$.

a) Show that A and B each have finite order.
b) Show that AB does not have finite order.
c) Explain how parts (a) and (b) demonstrate that $A^nB^n \neq (AB)^n$ in $GL_2(\mathbf{R})$. What else can you deduce about the group from this fact? (*Hint*: Think about the $n = 2$ case…)

Bonus: Explain geometrically (in terms of linear transformations of the plane, for example) why A above has finite order. Can you do the same for B?

- Let $\alpha = (12345)$ and $\beta = (12)$ be elements of a subgroup H in S_5. You will determine the entire subgroup H by showing the following.

Note: the following composition of cycles is written in multiplicative notation, rather than in the function compositional notation your book uses.

(a) Deduce that $(23) \in H$ by computing $\alpha^{-1}\beta\alpha$.
(b) Deduce that $(34) \in H$ by computing $\alpha^{-1}(23)\alpha$.
(c) Show that (45) and (15) belong to H.
(d) Show that $\gamma = (23)\beta(23)$ belongs to H.
(e) Show (24), (35), (14), and (25) also belong to H.
(f) Finally, making use of Proposition 5.4 in your book, deduce a simple way to describe the subgroup H.

[Refers to Judson's free text: http://abstract.ups.edu/download/aata-20130816.pdf

The Proposition is: Proposition 5.4 Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

- Recall that an *inner automorphism* of a group G is an automorphism of the form $x \mapsto gxg^{-1}$ where g is a fixed element in G. The set of all inner automorphisms of G is $Inn(G) = \{\varphi_g \mid \varphi_g(x) = gxg^{-1} \text{ for } x \in G\}$.
  a) In HW, you verified that an inner automorphism is indeed an automorphism, so that $Inn(G)$ is a subset of $Aut(G)$, where $Aut(G)$ is the group of all automorphisms of G. Now prove that $Inn(G)$ is a subgroup of $Aut(G)$. (The group operation in $Aut(G)$ is function composition.)
  b) Give an example of a group, G, for which $Inn(G) = \{1\}$ and explain your example.
  c) Find and tabulate the inner automorphisms of $S3$ (*i.e.*, write down explicitly where each inner automorphism sends elements of $S3$, perhaps using a table similar to one you constructed in HW). Are there automorphisms of $S3$ other than the inner automorphisms? How do you know?
  d) Fill in the blank: "If G is abelian, then $Inn(G)$ consists of _____."
  e) Find and tabulate the inner automorphisms of D_8.

- How many isomorphism types are there of abelian groups with order 360? How many of these are cyclic?

- Suppose G is a finite group with elements g and h, where $|g| = 7$ and $|h| = 5$. What can you say about $|G|$?

- Define the **general linear group**, $GL_n(\mathbb{R})$, and the **special linear group**, $SL_n(\mathbb{R})$.
  a) Prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.
  b) Assuming that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$ for all $n \geq 1$, prove that $SL_n(\mathbb{R})$ is a *normal* subgroup of $GL_n(\mathbb{R})$ by recognizing it as the kernel of a homomorphism $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}$.

- State the **First Isomorphism Theorem** for groups.

- Let θ be a homomorphism from S_5 to S_2. Explain why Imθ has either 1 or 2 elements.
  a) For the same homomorphism θ, explain why $K = \text{Ker}\theta$ has index 1 or 2 in S_5 and conclude that K is either_or_____(fill in the blanks and justify your answer).
  b) Deduce that there are only 2 homomorphisms from S_5 to S_2. Tabulate these two homomorphisms.

- A group is **simple** if it has no nontrivial normal subgroups. Suppose G is a group of order 65. Use the Sylow Theorems to prove that G cannot be a simple group.

Questions on Related or Supportive Topics

- Prove or disprove: "$<$" is an equivalence relation on the set of real numbers.

- Prove or disprove: "$\Rightarrow$" is an equivalence relation on the set of mathematical statements.

- Prove or disprove: $\equiv_n$ defined by $a \equiv_n b$ if $a \equiv b \pmod{n}$ is an equivalence relation on $\boldsymbol{Z}$.

- Prove or disprove: $\sim$ defined by $(x, y) \sim (a, b)$ if $3x + y = 3a + b$ is an equivalence relation on $\boldsymbol{R}^2$.

- Prove or disprove: $\sim$ defined by $(x, y) \sim (a, b)$ if $x^2 + y^2 = a^2 + b^2$ is an equivalence relation on $\boldsymbol{R}^2$.

True / False Questions

- ***True or False?*** Decide if each statement is true or false, and give a brief justification or counterexample to support your answer.
  (a) Every finite group G with prime order p is cyclic.
  (b) An additive group cannot be isomorphic to a multiplicative group.
  (c) Suppose H is a subgroup of a group G and $x \in G$. If $x \notin H$ and $y \notin H$, then $xy \notin H$.
  (d) If N is a normal subgroup of G and $gN = N$ for some $g \in G$, then $g = e_G$.
  (e) $3\mathbb{Z} \times 6\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}$.
  (f) $S_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$
  (g) If n divides $|G|$, then G has an element of order n.
  (h) If $p \geq 3$ is prime, then any two Abelian groups of order $2p$ are isomorphic.
  (i) A group with 3 elements has exactly 2 automorphisms.
  (j) Suppose G is a group with $a^2 = e = b^2$ and $ab = ba$, but $a \neq e$, $b \neq e$, and $a \neq b$. $H = \{e, a, b, ab\}$ is a subgroup of G.
  (k) If a nonempty subset H of a group G is closed under the operation of G, then H is a subgroup of G.
  (l) Let a and b be elements in a group G, then $ab^n a^{-1} = (aba^{-1})^n$.
  (m) $\mathbb{Z}$ is a group under the operation of subtraction.
  (n) An isomorphism is a homomorphism
  (o) The order of every element of D_8 divides 8
  (p) C_3 is a subgroup of C_6.
  (q) C_3 is a subgroup of C_4.
  (r) The following is a homomorphism from D_6 to C_3.

$I \to I$ $R \to R$ $R^2 \to R^2$ $F \to I$ $FR \to R$ $FR^2 \to R^2$