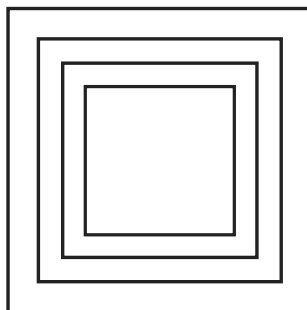


Some Abstract Algebra - A Primer *and some Number Theory*



Richard Grassl
University of Northern Colorado
Emeritus Professor of Mathematical Sciences
richard.grassl@unco.edu

Edited and typeset in LaTeX by Michael K. Petrie

Contents

Three Tables	53
Closure	54
Residue Classes	58
Modular Arithmetic	59
Cancellation	61
Permutations	62
Subgroups	64
Order	65
Group Tables	66
Complex Numbers	67
Table of Roots	69
Sixth Roots of Unity	70
Eighth Roots of Unity	71
Composition of Functions	72
Euler ϕ -Function	74
Invertibles	76
Preservation of Operation	77
A Special Isomorphism	78
Matching Groups	79
Groups of Order 8	80
Five Groups of Order 8	85
Group Tables, Isomorphisms	86
Fundamental Theorem	87
Which Direct Product	89
Rings, But Not I.D.	90
Polynomials in $Z_n[x]$	91
Another Ring	93
Summary of Rings	94
A Field With 9 Elements	95
Application of a Famous Theorem	96

DAY 1 PROPERTIES OF THREE TABLES

• = usual complex multiplication

•	1	-1	i	-i	PROPERTIES, OBSERVATIONS
1					1.
-1					2.
i					3.
-i					

⊗ = units digit in regular multiplication

⊗	1	3	7	9	
1					1.
3					2.
7					3.
9					

⊕ = bitwise addition, 0 if same, 1 if different

⊕	00	01	10	11	
00					1.
01					2.
10					3.
11					

WORKSHEET ON CLOSURE I

A set $S = \{a, b, c, \dots\}$ is closed under a binary operation \circ if whenever x and y are elements of S so is $x \circ y$.

For each of the following if the answer is yes, give a reason and if no, provide a counterexample.

Task 1 Is $E = \{0, 2, 4, 6, 8, \dots\}$ closed under the binary operation of addition?

☐ yes, ☐ no Reason: Let $2m$ and $2n$ be arbitrary elements in E .

Then since ...

How about under multiplication?

Task 2 Is $A = \{0, 1, 4, 9, 16, \dots\}$ closed under addition?

Under subtraction?

Under multiplication?

Task 3 Is the set of all rational numbers of the form $2^m 3^n$, where $m, n \in \mathbb{Z}$, closed under multiplication?

Task 4 Is the set of all positive rational numbers closed under addition? Multiplication?

Task 5 Are the complex numbers of the form $m + ni$ where m and n are integers closed under multiplication?

Task 6 Is the set $\{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$ closed under multiplication?

Task 7 Are the irrationals closed under multiplication? Under subtraction?

WORKSHEET ON CLOSURE II

Let $Z = \{\dots, -2, -1, 0, 1, 2, \dots\}$

QUESTION: Which of the sets $3Z$, $1 + 3Z$, $2 + 3Z$ are closed under subtraction?

Task 1 List the elements of $3Z$; choose two and subtract them.

Task 2 What does it mean to say $3Z$ is closed under subtraction?

Task 3 Is $3Z$ closed under subtraction? If yes, prove it.

Task 4 Is $1 + 3Z$ closed under subtraction?

Task 5 Is $2 + 3Z$ closed under subtraction?

Task 6 Why must a set of integers contain 0 to be closed under subtraction?

WORKSHEET ON CLOSURE III

PROBLEM: Prove that if S and T are sets of integers closed under subtraction so is the intersection $S \cap T$.

Task 1 Say in your own words what it means to say S is closed under subtraction.

Task 2 What do you have to show in order to check that $S \cap T$ is closed under subtraction?

Task 3 Draw a Venn diagram as an aid, and resolve the problem.

Task 4 If S and T are sets of integers closed under subtraction is the union $S \cup T$ also closed under subtraction? If yes, prove it, if no give a counterexample.

WORKSHEET ON RESIDUE CLASSES

Congruence Modulo m is an EQUIVALENCE RELATION on Z , the set of all integers.

R – REFLEXIVE: $a \equiv a(m)$

S – SYMMETRIC: If $a \equiv b(m)$ then $b \equiv a(m)$

T – TRANSITIVE: $a \equiv b(m)$ and $b \equiv c(m)$ then $a \equiv c(m)$

The relation *congruence* partitions Z into disjoint EQUIVALENCE CLASSES or RESIDUE CLASSES.

When $m = 2$, Z is partitioned into the classes $2Z$ and $1 + 2Z$.

$$2Z = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

$$1 + 2Z = \{\dots, -3, -1, 1, 3, 5, 7, \dots\}$$

Task 1 Explain why the classes $2Z$ and $1 + 2Z$ are disjoint.

Task 2 What the residue classes when $m = 3$? Are they disjoint? Why?

Task 3 When $m = 4$? Explain.

WORKSHEET ON MODULAR ARITHMETIC

$a \equiv b \pmod{m}$ means a and b have the same remainder when divided by m ; or that $a - b$ is divisible by m , or $a - b = mk$. An example: $17 \equiv 9 \pmod{4}$ since 4 divides $17 - 9$.

Task 1 Complete the missing four rows:

	0	1	2	3	4	5	6	7	8	9	10	11	12
Mod 2													
Mod 3	0	1	2	0	1	2	0	1	2	0	1	2	0
Mod 4													
Mod 5													
Mod 6													

Task 2 Tables of addition Mod 5 and Mod 6 would look like:

\oplus	0	1	2	3	4
0					
1	1	2	3	4	0
2					
3					
4					

\oplus	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

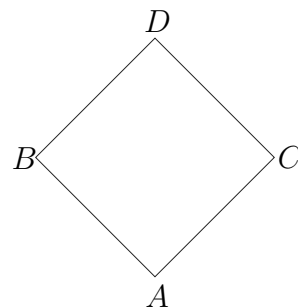
Let $Z_6 = \{0, 1, 2, 3, 4, 5\}$ be the six elements you used to make the 6 by 6 table in Task 2. If you examine that addition table, you can see that each of the following subsets are closed under the binary operation \oplus . The relationship among these subsets is shown in the diagram.

$$A = \{0\}$$

$$B = \{0, 3\}$$

$$C = \{0, 2, 4\}$$

$$D = \{0, 1, 2, 3, 4, 5\}$$



Task 3 Make the \oplus table for $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, list all the subsets closed under \oplus , and make a diagram as above.

\oplus	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

$$A = \{0\}$$

$$B =$$

$$C =$$

$$D =$$

Task 4 Without making the addition table, can you give all the closed subsets of Z_{12} ?

WORKSHEET ON CANCELLATION

Cancellation Theorem: If either $ab = ac$ or $ba = ca$ in a group G , then $b = c$.

Task 1 Let's try to prove right cancellation.

The hypothesis for right cancellation is:

If the element a is in G , _____ is also in G .

Now show how to use this latter element on $ba = ca$ and conclude that $b = c$.

– CONNECTIONS –

Task 2 Let A, B, C be sets in a universe S . If $A \cup B = A \cup C$ is it necessarily true that $B = C$?

Task 3 Does $A \cap B = A \cap C$ imply $B = C$?

Task 4 For 2 by 2 matrices A, B, C does $AB = AC$ imply $B = C$?

Task 5 For real numbers x, y, z does $x + y = x + z$ imply $y = z$?

PERMUTATIONS

Each permutation on $X_4 = \{1, 2, 3, 4\}$ is a 1-1, onto function f . For example, the permutation $1 \rightarrow 2, 2 \rightarrow 4, 3 \rightarrow 3, 4 \rightarrow 1$ has the function table

x	1	2	3	4
$f(x)$	2	4	3	1

and can be expressed in cycle form as (124) . With “multiplication” being composition of functions the product $(124)(23)$ is (1324) , operating left to right. The cycle form (124) means $1 \rightarrow 2 \rightarrow 4 \rightarrow 1$ with 3 fixed. The product $(124)(23)$ can be written as two-rowed arrays as:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = (1324)$$

We list cycles in standard form as follows:

1. Smallest number first
2. Omission of a number m means $m \rightarrow m$ is fixed

<u>Task 1</u>	$a=(1342)$	$a=(24675)$
	$a^2 =$	$a^2 =$
	$a^3 =$	$a^3 =$
	$a^4 =$	$a^4 =$
		$a^5 =$

Task 2 If $\beta=(26)$, $\beta^{-1} =$

What is the inverse of any transposition (ab) ?_____

Task 3 Let $\alpha = (132)(4675)$. What is the smallest positive integer s so that

$$\alpha^s = (1)? \quad s = \underline{\hspace{2cm}}.$$

Repeat with $\beta = (12)(3465)$: $s = \underline{\hspace{2cm}}.$

Give the order of each element by filling in the chart:

α	(13)	(132)	(12)(34)	(1432)	(132)(23)	(13)(12)
order α						

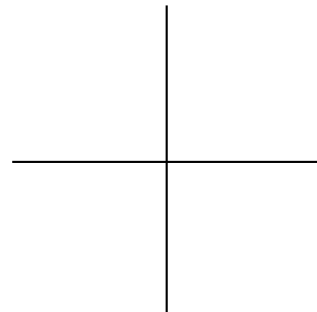
What is the order of $\beta = (13)(257)(4689)$?

What is the order of $\gamma = (13)(234)$?

WORKSHEET ON SUBGROUPS

Let $H = \{\alpha : \alpha = a + bi, |\alpha| \leq 1\}$. Is H a subgroup of the multiplicative group of non-zero complex numbers?

Task 1 Draw a picture showing all α with $|\alpha| \leq 1$.
Recall $|a + bi| = \sqrt{a^2 + b^2}$.



Task 2 To show that H is a subgroup we need to show, for one thing, that if $\alpha \in H$ so is α^{-1} . What is the inverse of $a + bi$? Try this on $\alpha = \frac{1}{2} + \frac{1}{2}i$. What is α^{-1} ?

Is $\alpha \in H$? You need to compute $\sqrt{\frac{1}{4} + \frac{1}{4}}$.

Draw α and α^{-1} in your picture as vectors. How are their angles related? How do you multiply two complex numbers to show $\alpha\alpha^{-1} = 1$?

Task 3 Give an α not in H .

Task 4 Do you now need to check closure?

WORKSHEET ON ORDER

The order of an element a of a group G is the order of the cyclic subgroup $[a]$ generated by a in G . Equivalently, it is the smallest positive integer m so that $a^m = e$.

Task 1 Let G be a cyclic group of order 18 generated by a . Then

$$G = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}, a^{12}, a^{13}, a^{14}, a^{15}, a^{16}, a^{17}\}.$$

Give the order of each element of G by filling out the chart:

x	e	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
order x									

x	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}
order x									

Task 2 Repeat Task 1 with G being a cyclic group of order 24.

WORKSHEET ON GROUP TABLES

Give as many reasons as you can why each of these tables cannot be group operation tables. You can state a group axiom that fails, or appeal to some of our theorems and results.

	a	b	c	d	e
a	c	e	a	b	d
b	d	c	b	e	a
c	a	b	c	d	e
d	e	a	d	c	b
e	b	d	e	a	c

	a	b	c	d	e
a	c	e	a	b	d
b	d	a	b	e	c
c	a	b	c	d	e
d	e	c	d	a	b
e	b	d	e	c	a

	a	b	c	d	e
a	e	d	b	c	a
b	c	e	d	a	b
c	d	a	e	b	c
d	b	c	a	e	d
e	a	b	c	d	e

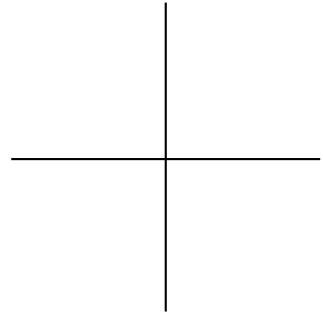
WORKSHEET ON COMPLEX NUMBERS

Task 1 $i^2 =$

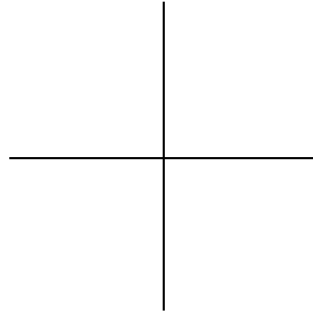
$$(1 + i)(2 - 3i) =$$

Task 2 Locate each of the following in the cartesian plane.

(a) $1, (-1 + i\sqrt{3})/2, (-1 - i\sqrt{3})/2$



(b) $1, -1, i, -i$



(c) Connect each of the points in (a) and describe the properties of the figure. Repeat with (b).

(d) What are the roots of $x^3 - 1 = 0$, $x^4 - 1 = 0$, and how is this question related to the above parts?

Task 3 If r and s are roots of $x^2 - 7x + 43 = 0$, what are $r + s$ and rs ?

Task 4 Use $(x - a)(x - b) = x^2 - (a + b)x + ab$ to resolve Task 3.

Give a similar expression for $(x - a)(x - b)(x - c)$.

What is the sum of the roots of $x^3 - 3x^2 + 2x - 14 = 0$? The product of the roots?

Let $1, r, s$ be roots of $x^3 - 1 = 0$.

The product of the roots is $1rs = \underline{\hspace{2cm}}$, so that $rs = \underline{\hspace{2cm}}$.

Also, $r^3 = \underline{\hspace{2cm}}$, $s^3 = \underline{\hspace{2cm}}$.

Explain why $r^2 = -r - 1$ and $r = \frac{1}{s}$ and $r^3 = \frac{r^2}{s}$.

Why is $r^2 = s$?

MULTIPLICATION TABLE OF ROOTS

Task 1 Use $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ to complete the chart:

	FACTORS	ROOTS
$x^2 - 1 = 0$	$(x - 1)(x + 1)$	1, -1
$x^3 - 1 = 0$		
$x^4 - 1 = 0$		

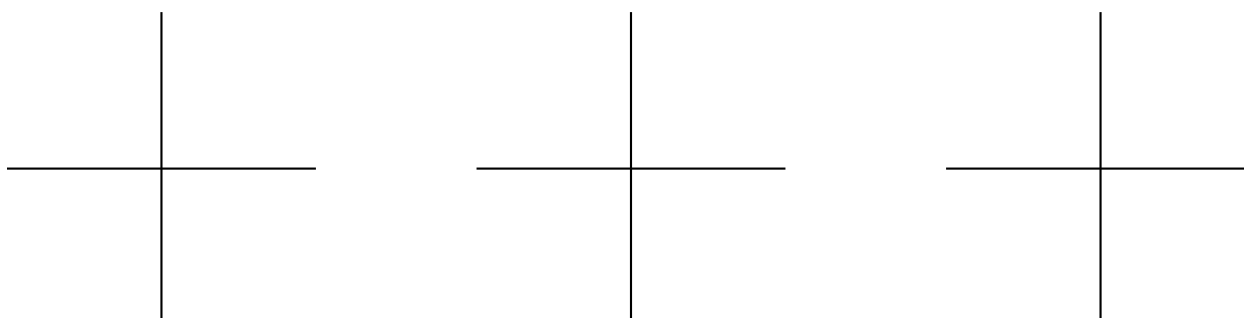
For convenience, you might want to label the roots of $x^3 - 1 = 0$ as 1, β , γ .

Task 2 Make the multiplication table for each set of roots:

	1	-1
1		
-1		

	1	β	γ
1			
β			
γ			

Task 3 Plot separately the set of roots for $x^2 - 1 = 0$, $x^3 - 1 = 0$, and $x^4 - 1 = 0$.



Connect the points and describe the geometrical figure produced.

Task 4 Conjecture what happens for $x^5 - 1 = 0$, $x^6 - 1 = 0$.

GROUP TABLE FOR THE SIXTH ROOTS OF UNITY

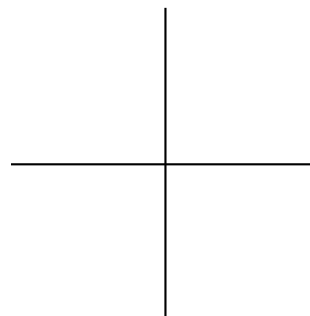
The goal here is to find the six roots of $x^6 - 1 = 0$, plot them, and make their group table.

Task 1 Factor $x^6 - 1 = (x^3 - 1)(\quad) = (\quad)(\quad)(\quad)(\quad)$

The six roots are:

Task 2 Plot these six complex numbers.

Connect them, forming a _____



Task 3 Label the six roots $1, r, s, -1, -r, -s$ where $1, r, s$ are the roots of $x^3 - 1 = 0$. Show why the last three are negatives of the first three. Show why $rs = 1, r^2 = s, s^2 = r$.

Task 4 Make the group table

	1	r	s	-1	$-r$	$-s$
1						
r						
s						
-1						
$-r$						
$-s$						

MULTIPLICATION TABLE FOR THE ROOTS OF $x^8 - 1 = 0$

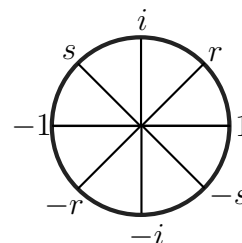
FACTOR: $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. The roots of $x^4 - 1 = 0$ are _____

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - (\sqrt{2}x)^2 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

The other roots are:

$$\begin{aligned} r &= \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} & -r &= \frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}} \\ s &= \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}} & -s &= \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} \end{aligned}$$

These eight roots are spread evenly around a unit circle 45° apart.



Task 1 Use the fact that when you multiply complex numbers you add their arguments to express each of the following in terms of $1, -1, i, -i, r, s, -r, -s$.

$$r^2 =$$

$$ir =$$

$$s^2 =$$

$$rs =$$

$$is =$$

Task 2 Complete the multiplication table

	1	-1	i	$-i$	r	s	$-r$	$-s$
1								
-1								
i								
$-i$								
r								
s								
$-r$								
$-s$								

COMPOSITION OF FUNCTIONS

Let $f_1(x)=x$ $f_4(x)=\frac{1}{x}$

$f_2(x)=\frac{1}{1-x}$ $f_5(x)=1-x$

$f_3(x)=\frac{x-1}{x}$ $f_6(x)=\frac{x}{x-1}$

The following “multiplication” table can be formed using composition of functions as the operation

EXAMPLE: $f_2 \circ f_6 = f_5$ since $f_2\left(\frac{x}{x-1}\right) = \frac{1}{1-\frac{x}{x-1}} = 1-x = f_5(x)$

\circ	x	$\frac{1}{1-x}$	$\frac{x-1}{x}$	$\frac{1}{x}$	$1-x$	$\frac{x}{x-1}$
$f_1 = x$	x	$\frac{1}{1-x}$	$\frac{x-1}{x}$	$\frac{1}{x}$	$1-x$	$\frac{x}{x-1}$
$f_2 = \frac{1}{1-x}$	$\frac{1}{1-x}$	$\frac{x-1}{x}$	x	$\frac{x}{x-1}$	$\frac{1}{x}$	$1-x$
$f_3 = \frac{x-1}{x}$	$\frac{x-1}{x}$					
$f_4 = \frac{1}{x}$	$\frac{1}{x}$					
$f_5 = 1-x$	$1-x$					
$f_6 = \frac{x}{x-1}$	$\frac{x}{x-1}$					

COMPOSITION OF FUNCTIONS (CONT)

Rewrite the table using $f_1, f_2, f_3, f_4, f_5, f_6$

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1						
f_2						
f_3						
f_4						
f_5						
f_6						

List properties of this table.

Complete the table showing inverses

f	f_1	f_2	f_3	f_4	f_5	f_6
f^{-1}						

List all the subsets of $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ that are closed under \circ .

EULER ϕ -FUNCTION

$\phi(n)$ is the number of positive integers less than n that are relatively prime to n . Here is a partial table:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10					

Task 1 Complete the table. Any conjectures?

Task 2 Conjecture and prove a formula for $\phi(p)$, p a prime.

Task 3 Prove a formula for $\phi(p^2)$.

Task 4 Compute $\phi(7^3)$ by listing the integers.

Task 5 Prove a formula for $\phi(p^n)$.

Task 6 Prove that $\phi(11^n)$ is a multiple of 10, for all n .

Task 7 Show that $\phi(16) \cdot \phi(9) = \phi(16 \cdot 9)$

Task 8 Find all x such that $\phi(x) = n$ where:

(a) $n = 1$

(b) $n = 2$

(c) $n = 4$

Task 9 The notation $(a, b) = 1$ means that a and b are relatively prime.

Prove that if $(a, m) = 1$, then $(m - a, m) = 1$.

Task 10 Prove that $\phi(n)$ is even for $n \geq 3$.

Task 11 It can be proved that if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Use this to compute $\phi(72)$; also compute $\phi(120)$.

Task 12 Prove that if $n = p_1^{e_1} p_2^{e_2} p_3^{e_3}$, then $\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right)$.

WORKSHEET ON INVERTIBLES

Let $Z_m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{m-1}\}$ and V_m be the set of invertibles of Z_m consisting of those elements of Z_m that have *multiplicative* inverses. For each Z_m make a table of inverses of those elements that have multiplicative inverses and list V_m . Here the “bar” indicates an equivalence class. $\bar{2}$ indicates the set of all integers in Z whose remainder is 2 upon division by m . Once understood, the “bar” is omitted.

SAMPLE:

$$Z_3 = \{0, 1, 2\}$$

x	0	1	2
x^{-1}		1	2

$$V_3 = \{1, 2\}$$

$$Z_4 = \{0, 1, 2, 3\}$$

x	0	1	2	3
x^{-1}				

$$V_4 = \{ \quad \quad \quad \}$$

$$Z_5 = \{0, 1, 2, 3, 4\}$$

x	0	1	2	3	4
x^{-1}					

$$V_5 = \{ \quad \quad \quad \}$$

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

x	0	1	2	3	4	5
x^{-1}						

$$V_6 = \{ \quad \quad \quad \}$$

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

x	0	1	2	3	4	5	6
x^{-1}							

$$V_7 = \{ \quad \quad \quad \}$$

Can you conjecture which elements of Z_{30} are invertibles?

How many invertibles does Z_p have where p is a prime?

How is the Euler ϕ -function related to these questions?

PRESERVATION OF OPERATION

In the following chart you are asked to verify whether certain familiar functions satisfy

$f(a \circ b) = f(a) \square f(b)$. The operations \circ and \square can be addition or multiplication or a mixture.

FUNCTION	YES OR NO	REASON
$f(x) = x^3$	yes	$f(xy) = (xy)^3 = x^3y^3 = f(x)f(y)$
$f(x) = x^4$		
$f(x) = e^x$		
$f(x) = \frac{3}{2}x$		
$f(x) = 2x + 1$		
$f(x) = \ln x$		
$f(x) = x $		
$f(x) = \sqrt{x}$		
$f(x) = 2x^3$		
$f(x) = \det x$		
$\theta(f) = f'$ (the derivative)		

A SPECIAL ISOMORPHISM

Task 1 Show that the mapping $\theta : G \rightarrow G$ given by $\theta(g) = g^{-1}$ is an isomorphism if G is abelian.

STEP 1 θ is 1-to-1. To show this we need to show that if $\theta(g_1) = \theta(g_2)$ then

_____. Since $\theta(g_1) = \theta(g_2)$ we get

_____. Now by taking inverses, we obtain

_____.

STEP 2 Show that θ is onto.

STEP 3 Show that θ preserves the operation

Task 2 Use $\theta(g) = g^{-1}$ to tabulate an isomorphism from S_3 , the group of symmetries of an equilateral triangle, to itself.

g	
$\theta(g)$	

Task 3 Show that the above result is false if G is not abelian.

MATCHING GROUPS

There are two nonisomorphic groups of order 4, the cyclic group and the Klein 4-group whose elements x satisfy $x^2 = e$.

For each of the following groups, label A if it is isomorphic to the cyclic group and B if it is isomorphic to the Klein group.

_____ [(1234)]

A. Cyclic B. Klein

_____ [$-i$]

_____ $\{e, a, a^2, a^3\}$

_____ [i]

_____ Rectangle Group

_____ $\{1, -1, i, -i\}$

_____ $\{0, 1, 2, 3\}$ under addition mod 4

_____ $\{(1), (12), (34), (12)(34)\}$

WORKSHEET ON AN 8×8 GROUP TABLE – Z_8

Task 1 Fill in the following table where each of the 64 entries is found by addition modulo 8; i.e. add the two numbers, divide by 8, and record the remainder.

\oplus	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

MAKE A TABLE OF INVERSES

DRAW THE LATTICE OF SUBGROUPS.

	0	1	2	3	4	5	6	7

LABEL AND LIST ALL THE SUBGROUPS.

WORKSHEET ON AN 8×8 GROUP TABLE – $Z_2 \times Z_4$

Task 1 Fill in the following table using bitwise addition mod 2 in the left-most slot and bitwise addition mod 4 in the right-most slot.

\oplus	00	01	02	03	10	11	12	13
00								
01								
02								
03								
10								
11								
12								
13								

MAKE A TABLE OF INVERSES

--	--

DRAW THE LATTICE OF SUBGROUPS.

LABEL AND LIST ALL THE SUBGROUPS.

WORKSHEET ON AN 8×8 GROUP TABLE – $Z_2 \times Z_2 \times Z_2$

Task 1 Fill in the following table using bitwise addition mod 2.

\oplus	000	001	010	011	100	101	110	111
000								
001								
010								
011								
100								
101								
110								
111								

MAKE A TABLE OF INVERSES

--	--

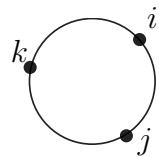
**DRAW THE LATTICE
OF SUBGROUPS.**

**LABEL AND LIST ALL THE
SUBGROUPS.**

WORKSHEET ON AN 8×8 GROUP TABLE –
THE QUATERNIONS

Task 1 Fill in the following table using the operations:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$



\otimes	1	-1	i	$-i$	j	$-j$	k	$-k$
1								
-1								
i								
$-i$								
j								
$-j$								
k								
$-k$								

MAKE A TABLE OF INVERSES

DRAW THE LATTICE
OF SUBGROUPS.



LABEL AND LIST ALL THE
SUBGROUPS.

WORKSHEET ON AN 8×8 GROUP TABLE – THE OCTIC GROUP

Task 1 Fill in the following table using $fr = r^3f$. These eight elements are the eight symmetries of a square.

\square	1	r	r^2	r^3	f	rf	r^2f	r^3f
1								
r								
r^2								
r^3								
f								
rf								
r^2f								
r^3f								

MAKE A TABLE OF INVERSES

DRAW THE LATTICE OF SUBGROUPS.



LABEL AND LIST ALL THE SUBGROUPS.

FIVE NONISOMORPHIC GROUPS OF ORDER 8

Listed next are the elements of these five groups along with their names. You are asked to show why certain pairs are not isomorphic.

CYCLIC $\{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}$

QUATERNIONS $\{1, -1, i, -i, j, -j, k, -k\}$

OCTIC $\{(1), \rho, \rho^2, \rho^3, \phi, \rho\phi, \rho^2\phi, \rho^3\phi\}$

BIT STRINGS
or $Z_2 \times Z_2 \times Z_2$ $\{000, 001, 010, 011, 100, 101, 110, 111\}$

$Z_2 \times Z_4$ $\{00, 01, 02, 03, 10, 11, 12, 13\}$

Task 1 Give two reasons why the QUATERNIONS are not isomorphic to the OCTIC group.

Task 2 Why is $Z_2 \times Z_4$ not isomorphic to $Z_2 \times Z_2 \times Z_2$?

Task 3 Why is the CYCLIC group not isomorphic to any of the other four?

WORKSHEET ON GROUP TABLES, ISOMORPHISMS

Complete the following table using \circ to mean composition of functions. For example.

$$f_2 \circ f_3 = f_2(f_3(x)) = f_2(1 - x) = \frac{1}{1 - x} = f_4$$

The six functions are:

$$f_1(x) = x \quad f_2(x) = \frac{1}{x} \quad f_3(x) = 1 - x \quad f_4(x) = \frac{1}{1 - x} \quad f_5(x) = \frac{x - 1}{x} \quad f_6 = \frac{x}{x - 1}$$

\circ	f_1	f_2	f_3	f_4	f_5	f_6
f_1						
f_2						
f_3						
f_4						
f_5						
f_6						

Display an isomorphism between this group and either S_3 or Z_6 .

FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

THEOREM: Every finite abelian group can be written as a product of cyclic groups of prime power order.

EXAMPLES: The Klein 4-Group is $Z_2 \times Z_2$; the cyclic group of order 4 is Z_4 . The abelian group of order 6 is Z_6 which is isomorphic to the direct product $Z_2 \times Z_3$.

Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ be a group of order 16 under multiplication mod 65. G is isomorphic to one of:

Z_{16}	
$Z_2 \times Z_8$	BUT WHICH ONE?
$Z_4 \times Z_4$	
$Z_2 \times Z_2 \times Z_4$	LOOK AT ORDERS!
$Z_2 \times Z_2 \times Z_2 \times Z_2$	

x	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
order x	1	4	4	2		4	4			4	4	4		4	4	

Task 1 Why is G not Z_{16} ?

Task 2 Why is G not $Z_2 \times Z_8$?

Task 3 What are the orders of elements in $Z_2 \times Z_2 \times Z_2 \times Z_2$?

Task 4 Which one must G be?

Task 5 $G = \{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ is a group of order 9 under multiplication modulo 91. Is G isomorphic to Z_9 or $Z_3 \times Z_3$? Why are these the only two possibilities?

Make the table of orders and inverses.

x	1	9	16	22	29	53	74	79	81
Order x									

x	1	9	16	22	29	53	74	79	81
x^{-1}									

Task 6 Identify all abelian groups (up to isomorphism) of order 360 by doing the following:

A. Express 360 as a product of prime numbers

B. List the six direct product possibilities

[illegible]

RINGS THAT ARE NOT INTEGRAL DOMAINS

A commutative ring D with unity 1, having no zero-divisors is called an integral domain.

Task 1 Explain why Z_{10} is not an integral domain.

Task 2 Why is Z_{12} not?

Task 3 For which m is Z_m not an integral domain?

Task 4 Is $Z_2 \times Z_2$ an integral domain?

Task 5 Let A and B be integral domains. Is $A \times B$ an integral domain?

Task 6 Is the set of all 2×2 matrices with real entries with the usual addition and multiplication of matrices an integral domain?

WORKSHEET ON POLYNOMIALS IN $Z_n[x]$

Task 1 Tabulate each of $(x + \bar{2})(x + \bar{5})$ and $x(x + \bar{7})$ in Z_{10} and thus show that they are equal.

x	0	1	2	3	4	5	6	7	8	9
$(x + \bar{2})(x + \bar{5})$			8							
$x(x + \bar{7})$			8							

Task 2 Show that $(x + \bar{3})(x + \bar{5}) = x(x + \bar{8})$ in $Z_{15}[x]$.

Task 3 Show that $(x + \bar{6})^2 = x^2$ in $Z_{12}[x]$.

Task 4 Our experience leads us to expect that $\deg \alpha\beta = \deg \alpha + \deg \beta$

for polynomials α and β .

But ... Show that $(\bar{2}x + \bar{1})(\bar{3}x + \bar{5}) = x + \bar{5}$ in $Z_6[x]$.

Task 5 Show that in $Z_6[x]$

$$(\bar{2}x + \bar{5})(\bar{3}x + \bar{2}) = (x + \bar{4})$$

$$(\bar{3}x + \bar{3})(\bar{4}x^2 + \bar{2}) = \bar{0}$$

Task 6 In $Z_5[x]$, $(\bar{2}x + \bar{1})(\bar{4}x + \bar{3}) = (x + \bar{3})(\bar{3}x + \bar{1})$

Make these linear factors monic (leading coefficient is $\bar{1}$) by factoring out $\bar{2}, \bar{4}$, and $\bar{3}$. For example $(\bar{2}x + \bar{1}) = \bar{2}(x + \bar{3})$. Then both sides become

WORKSHEET ON ANOTHER RING

Define “addition” and “multiplication” as follows:

$$a \oplus b = a + b - 1$$

$$a \otimes b = a + b - ab$$

show that $(\mathbb{Z}, \oplus, \otimes)$ is a ring by doing the following:

Task 1 Determine the “0”, the additive identity. Is there a unity?

Task 2 What is the additive inverse of a ? Why?

Task 3 Is \oplus associative? Is \otimes associative?

Task 4 Show that \otimes is distributive over \oplus .

SUMMARY OF RINGS AND THEIR PROPERTIES

Ring	Form of Element	Unity	Abelian	Integral Domain	Field
Z	k	1	Yes	Yes	No
Z_n, n composite					
Z_p, p prime					
$Z[x]$					
$nZ, n > 1$					
$M(Z), 2 \times 2$ matrices					
$Z[i]$					
$Z_3[i]$					
$Z_2[i]$					
$Z[\sqrt{2}]$					
$Q[\sqrt{2}]$	$a + b\sqrt{2}$				
$Z \oplus Z$					

$Z_3[i]$ IS A FIELD WITH 9 ELEMENTS

This field consists of all elements of the form $m + ni$ where m and n are in $\{0,1,2\}$. The multiplication table is:

	1	2	i	$1 + i$	$2 + i$	$2i$	$1 + 2i$	$2 + 2i$
1	1	2	i	$1 + i$	$2 + i$	$2i$	$1 + 2i$	$2 + 2i$
2	2	1	$2i$	$2 + 2i$	$1 + 2i$	i	$2 + i$	$1 + i$
i	i	$2i$						
$1 + i$	$1 + i$	$2 + 2i$						
$2 + i$	$2 + i$	$1 + 2i$						
$2i$	$2i$	i						
$1 + 2i$	$1 + 2i$	$2 + i$						
$2 + 2i$	$2 + 2i$	$1 + i$						

Task 1 Complete the table of inverses and orders:

x	1	2	i	$1 + i$	$2 + i$	$2i$	$1 + 2i$	$2 + 2i$
x^{-1}								
order of x								

Task 2 Which familiar group is the multiplicative group isomorphic to?

APPLICATION OF A FAMOUS THEOREM

PROBLEM: Explain why $x^7 - x = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ in $Z_7[x]$.

There are a number of ways of approaching this problem, several motivated by a similar question you could ask in the 8th grade. Explain why $x^2 - 5x + 6 = (x-2)(x-3)$. The following tasks guide you through three solutions.

Task 1 Use a calculator and show that each of 1, 2, 3, 4, 5, 6 satisfies $x^7 - x = 0$; then use the factor theorem.

Task 2 Simplify the right hand side algebraically using $x-6 = x+1$, $x-5 = x+2$, $x-4 = x+3$.

Task 3 What famous Theorem has $x^7 - x \equiv 0$ or $x^7 \equiv x$ in it?