Algebraic Structures

TexPREP Curriculum: PREP 2

Student Manual

Third Edition

Alma Potter, Editor

Adapted for UVU Prep (2014)

Produced and Distributed by
TEXAS PREFRESHMEN ENGINEERING PROGRAM (TexPREP)
Manuel P. Berriozàbal, Coordinator
The University of Texas at San Antonio
San Antonio, Texas 78249-0661

The first edition was part of a TexPREP Writing Project funded by
National Science Foundation
Instructional Materials Development Program
and
Young Scholars Program

Course Syllabus* for **Your Name Here** **Algebraic Structures** Classes—Summer, Current Year

Instructor Contact Information: **Your email address.**

Materials Needed: Paper and pencil. **ALL** work is to be done in pencil unless otherwise specified. Work done in anything other than pencil will **NOT** be accepted. (Colored pencils, liquid pencils, or erasable pens are not acceptable.)

Course Topics: Include, but may not be limited to, the following: Basic concepts of Set Theory; proofs involving sets, natural numbers, whole numbers, integers, rational numbers, and real numbers; mathematical systems: groups within the sets of real numbers and 2 x 2 matrices; and symmetry groups.

Homework Policy: Homework will be assigned daily, and will be due at the beginning of the next class period. Late work will **NOT** be accepted. The three lowest HW grades will be dropped at the end of the course. Every 3 assignments missed after the first three will count as an absence from prep.

Quiz Policy: Daily quizzes will be administered during the summer. The lowest quiz grade will be dropped **IF** all quizzes have been taken. If a quiz is missed and not made up, a zero will be averaged into the student's grade. If a student misses a quiz due to an absence, the quiz must be made up the first day that regular classes are held upon the student's return from the absence.

Test Policy: Two tests will be given during the summer. The lower test grade will be replaced with the grade earned on the Final Exam, if the grade on the Final is higher. As with quizzes, this courtesy will be extended **IF** all tests have been taken. If a test is missed and not made up, a zero will be averaged into the student's grade. If a student misses a test due to an absence, the test must be made up the first day that regular classes are held upon the student's return from the absence.

Grade Breakdown for Algebraic Structures: HW—10%; Quizzes—20%; Tests—40%; Final—30%

Regarding Cheating: Don't do it.

Regarding Extra Credit: There isn't any.

Behavior on Campus: Remember that we are guests of this campus, and must behave accordingly. If you are contemplating saying or doing anything that you would not want your parents or guardians to see you doing, then do not do it.

Miscellaneous: Turn off all electronic devices during the school day. Also, food, drinks, and chewing gum are not allowed in class.

*This syllabus is subject to change if necessary.

- Concepts Covered: "Is a/Has a" Form of a Definition, Terminology of Sets (elements of a set; how to denote sets)

Legend:	**Symbol or Abbreviation**	**Meaning**
	defn	definition
	$\in$	is an element or member of
	$\notin$	is **NOT** an element or member of
	IOW	in other words
	$\therefore$	therefore
	$<$	is less than
	$\leq$	is less than or equal to
	$>$	is greater than
	$\geq$	is greater than or equal to

"Is a/Has a" Form of a Definition

"Is a" component—tells what something is

"Has a" component—tells which properties that something has, or what it does

Example 1
pencil—is a writing instrument that has the property that it uses graphite to make marks on a writing surface

Alternately, "a writing instrument that uses graphite to make marks on a writing surface."

Even though the phrases "is a" or "has a" may not appear in a definition, it is still possible to pick out the "is a" and "has a" parts of the definition. This is illustrated in Example 2:

Example 2
order of operations—a set of rules that details the sequence in which operations in a mathematical expression or equation should be performed: First, grouping symbols; Second, exponents; Third, division or multiplication from left to right; Finally, subtraction or addition from left to right

"is a" part: a set of rules
"has a" part: that details the sequence in which operations in a mathematical expression or equation should be performed: First, ...

Terminology of Sets

The word "set" is undefined in mathematics, but we can provide a description of a set:
Any **well-defined** list, collection, or class of objects.

Example 1
The set of all PREP students at UVU.

Example 2
The set of all whole numbers between 5 and 13.

Example 3
The set of all whole numbers greater than 3.

Example of a set that is **NOT** well-defined:
The set of all objects that are warm.

Because "warm" has different meanings to different people, we cannot adequately determine whether or not something is warm. IOW, given an object, we do not have a good or reasonable way to measure whether that object should be contained in the set of all objects that are warm.

What to call those objects that are contained in a set?

defn: element or member (of a set)—any object contained within a set

Example 1
In the set of all whole numbers between 5 and 13, the elements or members of this set are 6, 7, 8, 9, 10, 11, 12.

Example 2
In the set of all whole numbers greater than 3, the elements or members of this set are 4, 5, 6, 7, 8, 9,... .

Note: Sets are denoted with capital letters; and elements or members of a set are denoted with lowercase letters.

Example 3
Let A = the set of whole numbers between 1 and 6.
Then A = {2, 3, 4, 5}, and we can say that $2 \in A$; $3 \in A$; $4 \in A$; and $5 \in A$.
However, for example, $1 \notin A$ and $6 \notin A$.

Example 4
Let T = {x, y, z}.
Then $x \in T$; $y \in T$; and $z \in T$.
But, for example, $a \notin T$ and $m \notin T$.

Day 0 • Pre-Test • Begin Day 1 Material if time allows **Day 1** • "Is a"/"Has a" form of a definition ○ Terminology of Sets (elements of a set; how to denote sets) • Calendar, Timeline, Syllabus, Legend • Day 1 Assignment	**Day 2** • Sets of Numbers: ○ Natural Numbers ○ Whole Numbers ○ Integers ○ Rational and Irrational Numbers ○ Real Numbers • Set-builder notation • Day 1 Quiz • Day 2 Assignment
Day 3 • Finite and Infinite Sets • The empty set • Subsets • Day 2 Quiz • Day 3 Assignment	**Day 4** • Equality of Sets ○ Operations on sets (intersection, union, difference) ○ Inclusive and exclusive "or" ○ Universal sets • Day 3 Quiz • Day 4 Assignment
Day 5 • Properties of sets • Two-column and paragraph proofs: $A \cup B = B \cup A$ • Set Properties handout • Day 4 Quiz • Day 5 Assignment	**Day 6** • Proofs of Set Properties: ○ $(A \cap B) \cap C = A \cap (B \cap C)$ ○ $A \cup (B \cap C) =$ $(A \cup B) \cap (A \cup C)$ • Day 5 Quiz • Day 6 Assignment
Day 7 • More proofs of set properties: ○ $(A \cup B)^C = A^C \cap B^C$ ○ $(A - C)$ • Day 6 Quiz • Day 7 Assignment	**Day 8** • Even more proofs of set properties: ○ $A - (B \cap C) = (A - B) \cup (A-C)$ • Day 7 Quiz • Day 8 Assignment
Day 9 • Still even more proofs of set properties ○ $(A^C)^C = A$ ○ $\varnothing \subset S$, for any set S ○ $U^C = \varnothing$ • Day 8 Quiz • Day 9 Assignment	**Day 10** • Power Sets: ○ Defn & Cardinality • Day 9 Quiz • Day 10 Assignment

Day 11 Test 1—Days 1-10	**Day 12** • Clock Arithmetic o Addition and multiplication on a 12-clock o Addition, multiplication, and subtraction on a 5-clock o Day 12 Assignment
Day 13 • More on Clock Arithmetic: o Closure in $\mathbb{N}$ o Additive identity and inverse in $\mathbb{R}$ & $\mathbb{N}$ o Multiplicative identity and inverse in $\mathbb{R}$ & $\mathbb{N}$ o 5-clock within $\mathbb{N}$ & $\mathbb{W}$ —add. and mult. iden. and inv. • Day 12 Quiz • Day 13 Assignment	**Day 14** • Congruence classes in $\mathbb{N}$ • Day 13 Quiz • Day 14 Assignment
Day 15 • Day 12 Quiz • $\mathbb{Z}_n$ • Modular Arithmetic • Solving Equations in $\mathbb{Z}_n$ • Day 14 Quiz • Day 15 Assignment	**Day 16** • Units in $\mathbb{Z}_n$, specifically $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_9$ o U_4, U_6, U_8, U_9 • Properties of groups (memorize for Day 17) • Day 15 Quiz • Day 16 Assignment
Day 17 • Defn of "group" • Determining whether $\mathbb{Z}_5$ or U_5 is a group under multiplication • Showing that a set G is a group under $*$ • Day 16 Quiz • Day 17 Assignment	**Day 18** • More on Groups • Day 17 Quiz • Day 18 Assignment
Day 19 • Even more on groups • Day 18 Quiz • Day 19 Assignment	**Day 20** Test 2—Days 12-19
Day 21 Review for Final Examination	**Day 22** Final Examination—Days 1-20

Day 1	Symbol or Abbreviation	Meaning
	defn	definition
	$\in$	is an element or member of
	$\notin$	is **NOT** an element or member of
	IOW	in other words
	$\therefore$	therefore
	$<$	is less than
	$\leq$	is less than or equal to
	$>$	is greater than
	$\geq$	is greater than or equal to

Day 2	Symbol or Abbreviation	Meaning
	$\neq$	is not equal to
	$\mathbb{N}$	set of natural numbers
	$\mathbb{W}$	set of whole numbers
	$\mathbb{Z}$	set of integers
	$\mathbb{Q}$	set of rational numbers
	$\mathbb{R}$	set of real numbers
	$\mathbb{R} - \mathbb{Q}$	set of irrational numbers
	i.e.	that is
	$\ni$ or $\vert$	such that
	no.	number
	nos.	numbers
	aka	also known as
	±	positive or negative

Day 3	Symbol or Abbreviation	Meaning
	int.	integer
	ints.	integers
	$\varnothing$ or { }	empty set (or null set)
	$\{\varnothing\}$	the set that contains the empty set
	$\subset$	is a subset of
	$\not\subset$	is not a subset of
	$\forall$	for each OR for all OR for every
	BTW	by the way

Day 4	Symbol or Abbreviation	Meaning
	spse	suppose
	iff	if and only if
	$S \cap T$	intersection of sets S and T
	$S \cup T$	union of sets S and T
	$S - T$	difference of sets S and T
	U	Universal Set
	S^C	complement of set S
	NTS	need to show
Day 5	Symbol or Abbreviation	Meaning
	$\Rightarrow$	implies
	$(S^C)^C$	complement of the complement of Set S
	prop	property
	props	properties
	$\Leftrightarrow$	is equivalent to
	pf	proof
	asme	assume
	Q.E.D.	that which was to be proved (signifies the end of a proof)
Day 6	Symbol or Abbreviation	Meaning
	$\exists$	there exists
	$\nRightarrow$	does not imply
	$\nLeftrightarrow$	is not equivalent to
Day 7	Symbol or Abbreviation	Meaning
	DNE	does not exist
Day 8	Symbol or Abbreviation	Meaning
	$\equiv$	is congruent to
	$\not\equiv$	is not congruent to
Day 9	None	
Day 10	Symbol	Meaning
	$\mathcal{P}(S)$	power set of Set S
Days 11-14	None	
Day 15	Symbol	Meaning
	$a \mid b$	*a* divides *b*
Days 16-24	None	

Name: ________________________________Group: ________________________________

Concepts Covered: "Is a/Has a" Form of a Definition, Terminology of Sets (elements of a set; how to denote sets)

List all the elements of each of the given sets.

1. A = All whole numbers between 20 and 25.

   ____

2. A = All letters of the alphabet after m but before t.

   ____

3. B = All odd whole numbers less than 18.

   ____

4. S = All even whole numbers between 26 and 44.

   ____

5. C = All positive multiples of 7 less than 56.

   ____

6. T = All even multiples of 3 greater than or equal to 9.

   ____

Provide an "is a/has a" definition of each of the given words. Look up these words in a dictionary...do not make up your own definitions. Make sure to adequately label the "is a" and "has a" parts of each definition.

7. automobile:
   ____
   ____
   ____

8. calculator:
   ____
   ____
   ____

9. calendar:
   ____
   ____
   ____

- Concepts Covered: Sets of Numbers (Natural Numbers, Whole Numbers, Integers, Rational and Irrational Numbers, Real Numbers), Set-builder notation

Legend:	Symbol or Abbreviation	Meaning
	$\neq$	is not equal to
	$\mathbb{N}$	set of natural numbers
	$\mathbb{W}$	set of whole numbers
	$\mathbb{Z}$	set of integers
	$\mathbb{Q}$	set of rational numbers
	$\mathbb{R}$	set of real numbers
	$\mathbb{R} - \mathbb{Q}$	set of irrational numbers
	i.e.	that is
	∍ or |	such that
	no.	number
	nos.	numbers
	aka	also known as
	±	positive or negative

Sets of Numbers

$\mathbb{N}$ = set of natural numbers = {1, 2, 3, 4, ...}
$\mathbb{N}$ is aka the set of counting numbers.

$\mathbb{W}$ = set of whole numbers = {0, 1, 2, 3, 4, ...}
$\mathbb{W}$ = set containing 0 and all elements of $\mathbb{N}$

$\mathbb{Z}$ = set of integers = {..., –3, –2, –1, 0, 1, 2, 3, ...} = {0, ±1, ±2, ±3, ...}
$\mathbb{Z}$ = set containing 0, the natural numbers, and the negatives of the natural numbers

Note: There is a difference between, "negative natural numbers," and "the negatives of the natural numbers." The former set does not exist, while the latter set does.

$\mathbb{Z}^+$ = set of positive integers = {1, 2, 3, 4, ...}
Note: $\mathbb{N} = \mathbb{Z}^+$

$\mathbb{Z}^-$ = set of negative integers = {–1, –2, –3, –4, ...}
$\mathbb{Q}$ = set of rational numbers
$\mathbb{Q}^+$ = set of positive rational numbers
$\mathbb{Q}^-$ = set of negative rational numbers

defn: rational number—a real number of the form $\frac{p}{q}$,

where $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, and $q \neq 0$.

Examples of rational numbers

$\frac{2}{7}$, $\frac{-1}{13}$, $\frac{4}{9}$, 0, –18, 12.7, 0.777...

In decimal form, rational numbers are either repeating or terminating:

Repeating decimal: 0.888... = $\frac{8}{9}$

Terminating decimal: 1.7 = $1\frac{7}{10}$ = $\frac{17}{10}$

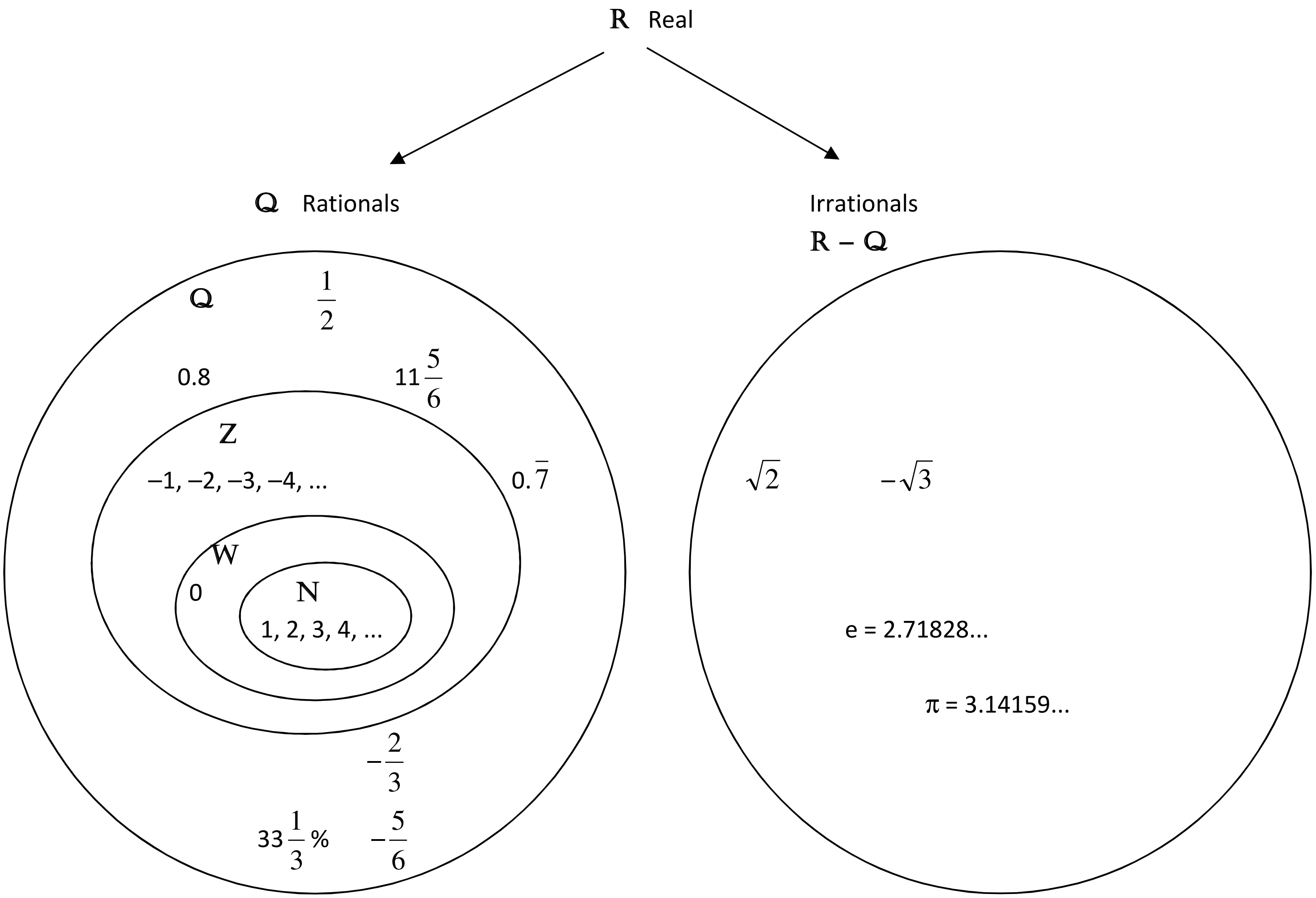
Some statements we can make thus far:

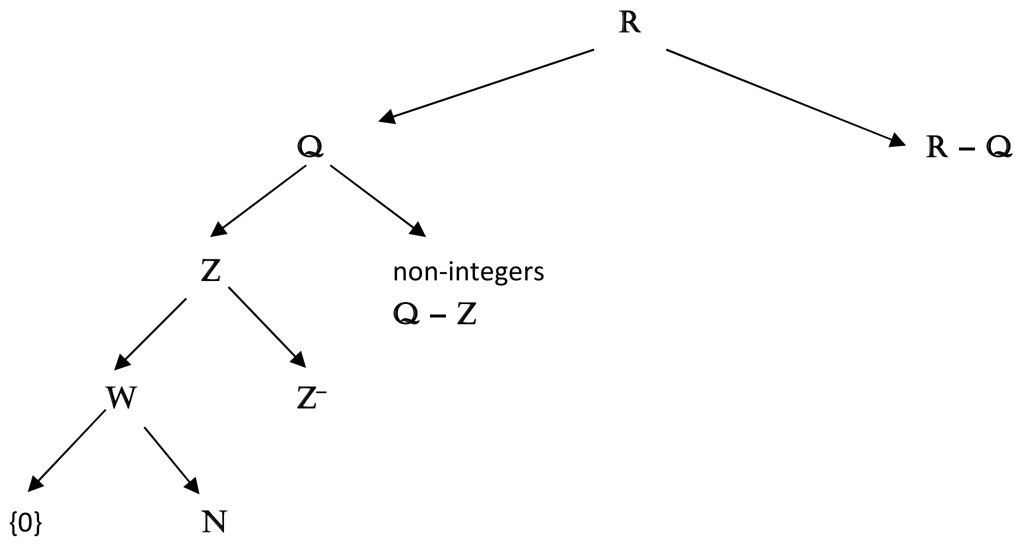
1. **Every** whole number is an integer, but not every integer is a whole number.

2. **No** element of $\mathbb{Z}^-$ is also an element of $\mathbb{N}$.

3. **Some** rational numbers are also negative integers.

4. **All** natural numbers are rational numbers.


R Real
Q Rationals
Irrationals
R – Q
Q
$\frac{1}{2}$
0.8
$11\frac{5}{6}$
Z
−1, −2, −3, −4, ...
$0.\overline{7}$
W
0
N
1, 2, 3, 4, ...
$-\frac{2}{3}$
$33\frac{1}{3}$ %
$-\frac{5}{6}$
$\sqrt{2}$
$-\sqrt{3}$
e = 2.71828...
π = 3.14159...


R
Q
R – Q
Z
non-integers
Q – Z
W
Z^-
{0}
N

$\mathbb{R}$ = set of real numbers
$\mathbb{R}$ = the set containing the set of rational numbers **AND**
the set of irrational numbers ($\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$)
$\mathbb{R} - \mathbb{Q}$ = set of irrational numbers

defn: irrational number—a real number that **cannot** be expressed in the form $\frac{p}{q}$, where $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, and $q \neq 0$.

In decimal form, irrational numbers are nonrepeating, nonterminating decimals:

$\sqrt{2}$ = 1.41421...

π = 3.14159...

0.56556555655556...

Note: Every real number is either rational or irrational, but **NOT** both.

Note: The sum of two rationals is also rational.
For example, 1.24 + 0.89 = 2.13; and $\frac{2}{3} + \frac{4}{5} = \frac{22}{15}$.

Note: The sum of two irrationals may or may not be irrational.
For example, $3\sqrt{2} + 4\sqrt{2} = 7\sqrt{2} \in \mathbb{R} - \mathbb{Q}$.
However, $\pi + -\pi = 0 \in \mathbb{Q}$.

Set-Builder Notation

In order to define a set using set-builder notation, one must state the property or properties that all elements in that set must satisfy.

Example 1
Let A = $\{x \mid x \in \mathbb{Z}^+\}$.
IOW, A is the set of all numbers x such that x is a positive integer.
That is, A = {1, 2, 3, 4, ...}.

Example 2
Let S = $\{y \mid y \in \mathbb{Z}, 2 < y < 8\}$.
IOW, S is the set of all numbers y such that y is an integer between 2 and 8.
Alternately, S is the set of all numbers y such that y is an integer greater than two but less than 8.
That is, S = {3, 4, 5, 6, 7}.

Name: ________________________________Group: ________________________________

Concepts Covered: Sets of Numbers; Set-Builder Notation

For problems 1-5, define each of the given sets using set-builder notation.

1. The Set A of all numbers x such that x is an integer between 9 and 13.

   ____

2. The Set S of all numbers x such that x is a natural number greater than 33.

   ____

3. The Set B of all numbers y such that y is an even rational number.

   ____

4. The Set S of all numbers x such that x is a negative odd integer.

   ____

5. The Set D of all numbers y such that y is a negative whole number.

   ____

For problems 6-10, translate each set into words.

6. $A = \{x \mid x \in Z, x < 20\}$

   ____

7. $S = \{y \mid y \in N, y > 13\}$

   ____

8. $A = \{y \mid y \in R, -3 < y \leq 5.6\}$

   ____

9. $S = \{x \mid x \in Q^{+}, 13 < x < 15\}$

   ____

10. $C = \{x \mid x \in Z^{-}, x > -76\}$

    ____

- Concepts Covered: Finite & Infinite Sets, The Empty Set, Subsets

Legend:	Symbol or Abbreviation	Meaning
	int.	integer
	ints.	integers
	$\varnothing$ or $\{\ \}$	empty set (or null set)
	$\{\varnothing\}$	the set that contains the empty set
	$\subset$	is a subset of
	$\not\subset$	is not a subset of
	$\forall$	for each OR for all OR for every
	BTW	by the way

Finite and Infinite Sets

defn: finite set—a set containing a finite number of elements

It is possible to list all the elements of a finite set.

Example 1

$S = \{3, 5, 7, 9\}$

Example 2

$A = \{x \mid x \in \mathbb{N}, x \le 7\} = \{1, 2, 3, 4, 5, 6, 7\}$

Example 3

$B = \{ x \mid x \in \mathbb{N}, x \le 1{,}000{,}000{,}000\}$

$= \{1, 2, 3, \ldots, 999{,}999{,}998, 999{,}999{,}999, 1{,}000{,}000{,}000\}$

defn: infinite set—a set containing an infinite number of elements

It is not possible to list all the elements of an infinite set.

Example 1

$S = \{1, 2, 3, 4, \ldots\}$

Example 2

$A = \{x \mid x \in \mathbb{Z}^{-}\} = \{-1, -2, -3, -4, \ldots\}$

Determine whether each of the following sets is finite or infinite:

1. $A = \{ x \mid x \in \mathbb{N} \}$ Answer: Infinite

2. $B = \{ x \mid x \in \mathbb{N} \ni x > 18\}$ Answer: Infinite

3. $C = \{ x \mid x \in \mathbb{N} \ni 3 \leq x < 13 \}$ Answer: Finite

4. $D = \{ x \mid x \in \mathbb{Q} \ni 3 \leq x < 13 \}$ Answer: Infinite

defn: empty set—a set that contains no elements; aka the null set; denoted by $\varnothing$ or { }

Note: The empty set is NOT denoted by $\{\varnothing\}$, which is actually the set that contains the empty set. $\varnothing$ contains zero elements, whereas $\{\varnothing\}$ contains one element.

Subsets

Given two sets A and B, A is a **subset** of B if every element of A is also an element of B.

IOW, $A \subset B$ if $\forall\, x \in A, x \in B$.

BTW, every set is a subset of itself; and the empty set is a subset of every set.

Examples

Consider the following sets:

$A = \mathbb{N}$
$B = \{3, 4, 5, 6\}$
$C = \mathbb{Q}^{+}$
$D = \{3, \pi, 4\}$

Then the following is true:

$B \subset A$, but $A \not\subset B$.
$A \subset C$, but $C \not\subset A$.
$A \not\subset D$, and $D \not\subset A$.
$B \subset C$, but $C \not\subset B$.
$B \not\subset D$, and $D \not\subset B$.
$C \not\subset D$, and $D \not\subset C$.

Name: ________________________________Group: ________________________________

Concepts Covered: Finite & Infinite Sets; Empty Set; Subsets

Consider the following sets:

$A = \{3, 4, 5, 6, 7\}$ $B = \{1, \sqrt{2}, \sqrt{3}, 2\}$ $C = \{x \mid x \in Z \ni 2 < x < 8\}$

$D = \{x \mid x \in Z \ni 2 \leq x \leq 8\}$ $E = Z^+$ $F = Q^+$

Compare each set with every other set to determine which are subsets. For each pair of sets, circle the correct answer: $\subset$ or $\not\subset$.

A $\subset$ $\not\subset$ B	B $\subset$ $\not\subset$ A
A $\subset$ $\not\subset$ C	C $\subset$ $\not\subset$ A
A $\subset$ $\not\subset$ D	D $\subset$ $\not\subset$ A
A $\subset$ $\not\subset$ E	E $\subset$ $\not\subset$ A
A $\subset$ $\not\subset$ F	F $\subset$ $\not\subset$ A
B $\subset$ $\not\subset$ C	C $\subset$ $\not\subset$ B
B $\subset$ $\not\subset$ D	D $\subset$ $\not\subset$ B
B $\subset$ $\not\subset$ E	E $\subset$ $\not\subset$ B
B $\subset$ $\not\subset$ F	F $\subset$ $\not\subset$ B
C $\subset$ $\not\subset$ D	D $\subset$ $\not\subset$ C
C $\subset$ $\not\subset$ E	E $\subset$ $\not\subset$ C
C $\subset$ $\not\subset$ F	F $\subset$ $\not\subset$ C
D $\subset$ $\not\subset$ E	E $\subset$ $\not\subset$ D
D $\subset$ $\not\subset$ F	F $\subset$ $\not\subset$ D
E $\subset$ $\not\subset$ F	F $\subset$ $\not\subset$ E

- Concepts Covered: Equality of Sets, Operations on sets (Intersection, Union, Difference) , Inclusive and exclusive "or", Universal Sets,

Legend:

Symbol or Abbreviation	Meaning
spse	suppose
iff	if and only if
$S \cap T$	intersection of sets S and T
$S \cup T$	union of sets S and T
$S - T$	difference of sets S and T
U	Universal Set
S^C	complement of set S
NTS	need to show

Equality of Sets

For any two sets A and B, $A = B$ iff $A \subset B$ and $B \subset A$.
IOW, $A = B$ iff $\forall x \in A, x \in B$, and $\forall x \in B, x \in A$.

Example 1
Let $A = \{3, 4, 5, 6, 7\}$ and
$C = \{x \mid x \in \mathbb{Z} \ni 2 < x < 8\} = \{3, 4, 5, 6, 7\}$.
$A \subset C$ and $C \subset A$, $\therefore$ $A = C$.

Example 2
Consider $\mathbb{N}$ and $\mathbb{Z}^+$.
$\mathbb{N} \subset \mathbb{Z}^+$ and $\mathbb{Z}^+ \subset \mathbb{N}$, so $\mathbb{N} = \mathbb{Z}^+$.

Operations on Sets

For any two sets S and T, their **intersection** is given by $S \cap T = \{x \mid x \in S$ **and** $x \in T\}$.

Note: The intersection of two sets is also a set.

Example 1
Let $S = \{1, 2, 3\}$ and $T = \{3, 4, 5\}$.
Then $S \cap T = \{3\}$.

Example 2

Let C = {3, 5, 7} and D = {2, 4, 6}.
Then $C \cap D = \varnothing$.
IOW, C and D are **disjoint**, i.e., the two sets have no elements in common.

Example 3

$\mathbb{N} \cap \mathbb{Q} = \mathbb{N}$.

Example 4

$\mathbb{N} \cap \mathbb{Z}^{-} = \varnothing$.

For any two sets S and T, their **union** is given by $S \cup T = \{x \mid x \in S$ **or** $x \in T\}$.

Note: The union of two sets is also a set.

Note: In mathematics, the word "or" is usually used in the **inclusive** sense, meaning "one or the other or both." For example, if $x \in S \cup T$, then x could be in S or T or both. Outside the world of mathematics, "or" is usually used in the **exclusive** sense, meaning "one or the other but not both." For example, when your parents say that you may have a candy bar or a bag of chips, they usually mean you can have the candy bar or the bag of chips, but not both.

Example 1

Let S = {1, 2, 3} and T = {3, 4, 5}.
Then $S \cup T = \{1, 2, 3, 4, 5\}$.

Example 2

$\mathbb{N} \cup \mathbb{Q} = \mathbb{Q}$.

Example 3

$\mathbb{Z}^{-} \cup \mathbb{N} = \{x \mid x \in \mathbb{Z} \ni x \neq 0\}$.

For any two sets S and T, their **difference** is given by $S - T = \{x \mid x \in S \text{ and } x \notin T\}$.

Note: The difference of two sets is also a set.

Example 1

Let A = {1, 2, 3} and B = {–1, 0, 1}.
A – B = {2, 3}
B – A = {–1, 0}

Example 2

Let A = {1, 3, 5, 7} and C = {1, 3, 5, 7}.

$A - C = \varnothing$

$C - A = \varnothing$

Note: If two sets S and T are equal, then $S - T = T - S = \varnothing$. IOW, if two sets are equal, then there is no element in either set that is not in the other set.

Example 3

$\mathbb{Z} - \mathbb{W} = \mathbb{Z}^-$

$\mathbb{W} - \mathbb{Z} = \varnothing$

Example 4

$\mathbb{Z} - \mathbb{N} = \mathbb{Z}^- \cup \{0\}$

$\mathbb{N} - \mathbb{Z} = \varnothing$

Example 5

$\mathbb{R} - \mathbb{Q}$ = set of irrationals

$\mathbb{Q} - \mathbb{R} = \varnothing$

Universal Sets

defn: Universal Set—the set whose subsets are under consideration in a particular discussion; denoted by U

defn: Consider a Set $S \ni S \subset U$. The **complement** of S, denoted by S^C, is given by the following: $S^C = \{x \mid x \in U \text{ and } x \notin S\}$.

Note: The complement of a set is also a set.

Example 1

Let U = {1, 2, 3, ... , 10, 11, 12},
A = {1, 3, 5, 7, 9, 11},
B = {2, 4, 6, 8, 10}, and
C = {3, 6, 9, 12}.

Then the following is true:
$A^C = \{2, 4, 6, 8, 10, 12\}$,
$B^C = \{1, 3, 5, 7, 9, 11, 12\}$,
$C^C = \{1, 2, 4, 5, 7, 8, 10, 11\}$, and
$U^C = \varnothing$.

Name: ________________________________Group: ________________________________

Concepts Covered: Equality of Sets, Operations on Sets, Inclusive and Exclusive "or", Universal Sets

Consider the following sets: $U = Z$

$A = W$

$B = Z^{-}$

$C = \{ x \mid x \in Z^{-} \ni x \leq -7 \}$

$D = \{ x \mid x \in Z^{+} \ni 3 \leq x < 10 \}$

$E = \{ x \mid x \in Z^{+} \ni x \geq 10 \}$

Find the following:

1. $A \cup B$ ____________________
2. $A \cap B$ ____________________
3. $B \cup C$ ____________________
4. C^C ____________________
5. $D \cup E$ ____________________
6. E^C ____________________
7. U^C ____________________
8. $D \cap E$ ____________________
9. $U \cap A$ ____________________
10. $E \cap U$ ____________________
11. $(D^C)^C$ ____________________
12. $U \cap D$ ____________________
13. $C \cup C^C$ ___________________

- Concepts Covered: Properties of Sets, Two-column and Paragraph proofs ($A \cup B = B \cup A$)

Legend:	Symbol or Abbreviation	Meaning
	$\Rightarrow$	implies
	$(S^C)^C$	complement of the complement of Set S
	prop	property
	props	properties
	$\Leftrightarrow$	is equivalent to
	pf	proof
	asme	assume
	Q.E.D.	that which was to be proved (signifies the end of a proof)

Note: For the most part, definitions tell us something about what an object is, whereas properties tell us something about the way an object behaves. However, the properties of an object are usually included in its definition.

Some Props that may be derived/inferred from Day 4 Assignment:

$A \cap A^C = \varnothing$ (exercise 2)
$A \cup A^C = U$ (exercise 1)
$U \cap A = A$ (exercise 9)
$(A^C)^C = A$ (exercise 11)
$U^C = \varnothing$ (exercise 7)

Note: Remember from logic that for any two statements p and q,
$p \Leftrightarrow q$ means that $p \Rightarrow q$ and $q \Rightarrow p$. ($p \Leftrightarrow q$ can also be written as p iff q.)

Some Defns and Props of Sets

(Note to Instructor: To illustrate these defns and props, you may want to produce Venn Diagrams for the students. This is optional, however, as students should have been taught Venn Diagrams in Logic last summer.)

Consider the sets U, A, and B, where U is the Universal Set; $A \subset U$; and $B \subset U$.
Then the following is true:

1. ***defn* of set intersection:** $x \in A \cap B \Leftrightarrow x \in A$ and $x \in B$, which means that
   $x \in A \cap B \Rightarrow x \in A$ and $x \in B$ **AND**
   $x \in A$ and $x \in B \Rightarrow x \in A \cap B$.

2. ***props*** **of set intersection:** $(A \cap B) \subset A$
$(A \cap B) \subset B$
$x \notin A \Rightarrow x \notin A \cap B$

3. ***defn*** **of set union:** $x \in A \cup B \Leftrightarrow x \in A$ or $x \in B$

4. ***props*** **of set union:** $A \subset (A \cup B)$
$B \subset (A \cup B)$
$x \in A \Rightarrow x \in A \cup B$

5. ***defn*** **of set difference:** $x \in A - B \Leftrightarrow x \in A$ and $x \notin B$

6. ***defn*** **of set complement:** $x \in A \Leftrightarrow x \notin A^C$
$x \notin A \Leftrightarrow x \in A^C$

Other relevant props of sets are on the handout.

Note: Remember from logic that for any two statements p and q, both their disjunction (p or q) and their conjunction (p and q) are commutative. This will help us prove that for any two sets A and B, $A \cup B = B \cup A$.

Two-Column and Paragraph Proofs

Given: Sets A and B, where A and B are not both empty.
Prove: $A \cup B = B \cup A$.

Two-column Proof:

Part I: Prove $(A \cup B) \subset (B \cup A)$.
Pf:

Statements	Reasons
1. Let $x \in A \cup B$	1. Given
2. $x \in A$ or $x \in B$	2. Defn of set union
3. $x \in B$ or $x \in A$	3. Commutativity of disjunction
4. $x \in B \cup A$	4. Defn of set union
5. $(A \cup B) \subset (B \cup A)$	5. Defn of subset

Part II: Prove $(B \cup A) \subset (A \cup B)$.

Pf:

Statements	Reasons
1. Let $x \in B \cup A$	1. Given
2. $x \in B$ or $x \in A$	2. Defn of set union
3. $x \in A$ or $x \in B$	3. Commutativity of disjunction
4. $x \in A \cup B$	4. Defn of set union
5. $(B \cup A) \subset (A \cup B)$	5. Defn of subset

Conclusion: Since $(A \cup B) \subset (B \cup A)$ and $(B \cup A) \subset (A \cup B)$, then by the defn of set equality, $A \cup B = B \cup A$, Q. E. D.

Paragraph Proof:

Part I: Show that $(A \cup B) \subset (B \cup A)$.

Pf: Let $x \in A \cup B$. (Since A and B are not both empty, $A \cup B \neq \emptyset$.) Then by the defn of set union, $x \in A$ or $x \in B$. Since the operation of disjunction is commutative, $x \in B$ or $x \in A$. The defn of set union says that $x \in B \cup A$; so by the defn of subset, $(A \cup B) \subset (B \cup A)$.

Part II: Prove $(B \cup A) \subset (A \cup B)$.

The pf of Part II is similar to Part I, and our conclusion with the paragraph method is the same as with the two-column method.

More Properties of Sets

1. $(A^C)^C = A$
2. $U^C = \varnothing$
3. $\varnothing^C = U$
4. $A - A = \varnothing$
5. $A - \varnothing = A$
6. $A - B = A \cap B^C$
7. $A \cup \varnothing = A$
8. $A \cap U = A$
9. $A \cup U = U$
10. $A \cap \varnothing = \varnothing$
11. $A \cup A = A$
12. $A \cap A = A$
13. $A \cup A^C = U$
14. $A \cap A^C = \varnothing$

Commutative Laws

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$

Associative Laws

1. $(A \cup B) \cup C = A \cup (B \cup C)$
2. $(A \cap B) \cap C = A \cap (B \cap C)$

Distributive Laws

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan's Laws

1. $(A \cup B)^C = A^C \cap B^C$
2. $(A \cap B)^C = A^C \cup B^C$
3. $A - (B \cup C) = (A - B) \cap (A - C)$
4. $A - (B \cap C) = (A - B) \cup (A - C)$

Name: ________________________________Group: ________________________________

Concepts Covered: Properties of Sets, Two-Column & Paragraph Proofs ($A \cup B = B \cup A$)

Complete the following proofs:

1. Using two-column form, prove that $A \cap B = B \cap A$. (Assume $A \cap B \neq \varnothing$ and $B \cap A \neq \varnothing$.)

Part I:
Pf:

Statements	Reasons

Part II:
Pf:

Statements	Reasons

Conclusion:

2. Use paragraph form to show that $A \cap B = B \cap A$. (Assume $A \cap B \neq \varnothing$ and $B \cap A \neq \varnothing$.)

- Concepts Covered: Proofs of Set Properties - $(A \cap B) \cap C = A \cap (B \cap C)$,
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Legend:

Symbol or Abbreviation	Meaning
$\exists$	there exists
$\not\Rightarrow$	does not imply
$\not\Leftrightarrow$	is not equivalent to

1. Given: Sets A, B, and C. (Asme all relevant sets are non-empty.)
   Prove: $(A \cap B) \cap C = A \cap (B \cap C)$.

Part I: Show that $(A \cap B) \cap C \subset A \cap (B \cap C)$.

Pf: Let $x \in (A \cap B) \cap C$. (Since all relevant sets are non-empty, $(A \cap B) \cap C \neq \varnothing$.) By the defn of set intersection, $x \in A \cap B$ **and** $x \in C$. Also by the defn of set intersection, $x \in A$ and $x \in B$. Since $x \in B$ and $x \in C$, $x \in B \cap C$. We now have that $x \in A$ and $x \in B \cap C$, so by the defn of set intersection, $x \in A \cap (B \cap C)$. By the defn of subset, $(A \cap B) \cap C \subset A \cap (B \cap C)$.

Part II: Show that $A \cap (B \cap C) \subset (A \cap B) \cap C$. The proof of Part II is similar to that of Part I.

Since $(A \cap B) \cap C \subset A \cap (B \cap C)$ and $A \cap (B \cap C) \subset (A \cap B) \cap C$, then $(A \cap B) \cap C = A \cap (B \cap C)$, Q. E. D.

2. Given: Sets A, B, and C. (Asme all relevant sets are non-empty.)
   Prove: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Part I: Show that $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$.

Pf:

Statements	Reasons
1. Let $x \in A \cup (B \cap C)$	1. Instantiation
2. $x \in A$ or $x \in B \cap C$	2. defn of set union
3. Spse $x \in A$. Then $x \in A \cup B$ and $x \in A \cup C$	3. prop of set union
$\Rightarrow x \in (A \cup B) \cap (A \cup C)$	defn of set intersection
4. Spse $x \in B \cap C$. Then $x \in B$ and $x \in C$	4. defn of set intersection
$\Rightarrow x \in B \cup A$ and $x \in C \cup A$	prop of set union
$\Leftrightarrow x \in A \cup B$ and $x \in A \cup C$	comm. of set union
$\Rightarrow x \in (A \cup B) \cap (A \cup C)$	defn of set intersection
5. $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$	5. defn of subset

Part II: Show that $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$.

Pf:

Statements	Reasons
1. Let $x \in (A \cup B) \cap (A \cup C)$	1. Instantiation
2. $x \in (A \cup B)$ and $x \in (A \cup C)$	2. defn of set intersection
3. $x \in (A \cup B) \Rightarrow x \in A$ or $x \in B$, and	3. defn of set union
$x \in (A \cup C) \Rightarrow x \in A$ or $x \in C$	defn of set union
4. If $x \in A$, then $x \in A \cup (B \cap C)$	4. prop of set union
5. If $x \notin A$, then $x \in B$ and $x \in C$	5. defn of set union
$\Rightarrow x \in B \cap C$	defn of set intersection
$\Rightarrow x \in (B \cap C) \cup A$	prop of set union
$\Leftrightarrow x \in A \cup (B \cap C)$	comm. of set union
6. $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$	6. defn of subset

Since $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$, then by the defn of set equality, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, Q. E. D.

Name: ________________________________Group: ________________________________

Concepts Covered: Proofs of Set Properties - $(A \cap B) \cap C = A \cap (B \cap C)$,
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

1. Provide a **paragraph** proof of the following property: $(A \cup B) \cup C = A \cup (B \cup C)$. (Asme all relevant sets are non-empty.)

2. Provide a **two-column** proof of the following property: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (Asme all relevant sets are non-empty.)

- Concepts Covered: More proofs of set properties $(A \cup B)^C = A^C \cap B^C$

Legend:	Symbol or Abbreviation	Meaning
	DNE	does not exist

Note: Given a statement, "If p, then q," its contrapositive is "If not q, then not p." The contrapositive of a statement is logically equivalent to the statement. So, if a statement is true, then its contrapositive is true as well. (Also, if a statement is false, then its contrapositive is false as well.)

Example 1

Given: Sets A and B. (Asme all relevant sets are non-empty.)

Prove: $(A \cup B)^C = A^C \cap B^C$

Part I: Show that $(A \cup B)^C \subset (A^C \cap B^C)$.

Pf:

Statements	Reasons
1. Let $x \in (A \cup B)^C$	1. instantiation
2. $x \notin A \cup B$	2. defn of set complement
3. $x \notin A$ and $x \notin B$	3. defn of set union (contrapositive)
4. $x \in A^C$ and $x \in B^C$	4. defn of set complement
5. $x \in A^C \cap B^C$	5. defn of set intersection
6. $(A \cup B)^C \subset (A^C \cap B^C)$	6. defn of subset

Part II: Show that $(A^C \cap B^C) \subset (A \cup B)^C$.

Pf:

Statements	Reasons
1. Let $x \in A^C \cap B^C$	1. instantiation
2. $x \in A^C$ and $x \in B^C$	2. defn of set intersection
3. $x \notin A$ and $x \notin B$	3. defn of set complement
4. $x \notin (A \cup B)$	4. defn of set union (contrapositive)
5. $x \in (A \cup B)^C$	5. defn of set complement
6. $(A^C \cap B^C) \subset (A \cup B)^C$	6. defn of subset

Since $(A \cup B)^C \subset (A^C \cap B^C)$ and $(A^C \cap B^C) \subset (A \cup B)^C$, then by the defn of set equality, $(A \cup B)^C = A^C \cap B^C$, Q. E. D.

Name: _________________________________Group: _________________________________

Concepts Covered: More proofs of set properties $(A \cup B)^C = A^C \cap B^C$

Provide a two-column proof of the following property: $(A \cap B)^C = A^C \cup B^C$. Asme all relevant sets are non-empty.

Part I:

Part II:

- Concepts Covered: Even More Proofs of Set Properties $A - (B \cap C) = (A - B) \cup (A - C)$

Legend:

Symbol or Abbreviation	Meaning
$\equiv$	is congruent to
$\not\equiv$	is not congruent to

Example

Given: Sets A, B, and C. (Asme all relevant sets are non-empty.)

Prove: $A - (B \cap C) = (A - B) \cup (A - C)$

Part I: Show that $A - (B \cap C) \subset (A - B) \cup (A - C)$

Pf:

Statements	Reasons
1. Let $x \in A - (B \cap C)$	1. instantiation
2. $x \in A$ and $x \notin B \cap C$	2. defn of set difference
3. $x \notin B \cap C \Rightarrow x \notin B$ or $x \notin C$	3. defn of set intersection contrapositive
4. Spse $x \notin B$. Then since $x \in A$, $x \in A - B$	4. defn of set difference
$\Rightarrow x \in (A - B) \cup (A - C)$	prop of set union
$\Rightarrow A - (B \cap C) \subset (A - B) \cup (A - C)$	defn of subset
5. Spse $x \notin C$. Then since $x \in A$, $x \in A - C$	5. defn of set difference
$\Rightarrow x \in (A - C) \cup (A - B)$	prop of set union
$\Leftrightarrow x \in (A - B) \cup (A - C)$	comm. of set union
$\Rightarrow A - (B \cap C) \subset (A - B) \cup (A - C)$	defn of subset

Part II and the **Conclusion** make up Problem 1 of Day 8 Assignment.

Name: ________________________________Group: ________________________________

Concepts Covered: Even More Proofs of Set Properties $A - (B \cap C) = (A - B) \cup (A - C)$

1. In two-column form, show that $(A - B) \cup (A - C) \subset A - (B \cap C)$.
   (This is the second half of the proof begun in class.) Do not forget to include a conclusion at the end of your proof.

2. Using two-column form, prove that $A - (B \cup C) = (A - B) \cap (A - C)$. (Asme all relevant sets are non-empty.)

- Concepts Covered: Still Even More Proofs of Set Properties: $(A^C)^C = A$, $\varnothing \subset S$, for any set S, $U^C = \varnothing$

Example 1

Prove that $(A^C)^C = A$. (Asme all relevant sets are non-empty.)

Part I: Prove that $(A^C)^C \subset A$.

Pf: Let $x \in (A^C)^C$. Then by the defn of set complement, $x \notin A^C$, which implies that $x \in A$ (also by the defn of set complement). By the defn of subset, $(A^C)^C \subset A$.

Part II: Prove that $A \subset (A^C)^C$.

Pf: Let $x \in A$. Then by the defn of set complement, $x \notin A^C \Rightarrow x \in (A^C)^C$ (also by the defn of set complement). By the defn of subset, $A \subset (A^C)^C$.

Conclusion: Since $(A^C)^C \subset A$ and $A \subset (A^C)^C$, then by the defn of set equality, $(A^C)^C = A$, Q. E. D.

Example 2

Prove that the empty set is a subset of every set. IOW, given any set S, show that $\varnothing \subset S$.

Pf (by contradiction): Spse $\varnothing \not\subset S$. Then by the defn of subset, $\exists\, x \in \varnothing \ni x \notin S$. However, by the defn of empty set, $x \notin \varnothing$, a contradiction. Therefore, $\varnothing \subset S$; i.e., the empty set is a subset of every set, Q. E. D.

Example 3

Show that $U^C = \varnothing$.

Part I: Show that $U^C \subset \varnothing$.

Pf: Let $x \in U^C$. Then by defn of set complement, $U^C = \{x \mid x \in U \text{ and } x \notin U\}$. No element of a set can also be a non-element of the same set, so U^C must be an empty set. Since the empty set is a subset of every set, $U^C \subset \varnothing$.

Part II: Show that $\varnothing \subset U^C$.

Pf: From Example 2 above, we know that the empty set is a subset of every set, so $\varnothing \subset U^C$.

Conclusion: Since $U^C \subset \varnothing$ and $\varnothing \subset U^C$, then by the defn of set equality, $U^C = \varnothing$, Q. E. D.

Name: ________________________________Group: ________________________________

Concepts Covered: Still Even More Proofs of Set Properties: $(A^C)^C = A$, $\varnothing \subset S$, for any set S, $U^C = \varnothing$

In paragraph form, answer each of the following. For each, asme all relevant sets are non-empty.

1. Prove that $\varnothing^C = U$.
2. Show that $A \cap \varnothing = \varnothing$.
3. Show that $A \cap A^C = \varnothing$

- Concepts Covered: Power Sets, Defn & Cardinality

<u>Note to Instructor:</u> Test 1, which covers Days 1-10, is scheduled for Day 11. Consequently, there is no quiz for Day 10.

<u>Legend:</u>	<u>Symbol</u>	<u>Meaning</u>
	$\mathcal{P}(S)$	power set of Set S

<u>Power Sets</u>

defn: power set of Set S—denoted by $\mathcal{P}(S)$, it is the collection of all subsets of S

<u>Example 1</u>
Let S = {5, 6}.
$\mathcal{P}(S) = \{\varnothing, \{5, 6\}, \{5\},\{6\}\}$ **<u>or</u>** $\mathcal{P}(S) = \{\varnothing, S, \{5\},\{6\}\}$

<u>Example 2</u>
Let T = {x, y, z}.
$\mathcal{P}(T) = \{\varnothing, T, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}\}$

<u>Example 3</u>
Let A = {1, 3, 5}.
$\mathcal{P}(A) = \{\varnothing, A, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{1, 5\}, \{3, 5\}\}$

<u>Example 4</u>
Let B = $\varnothing$.
$\mathcal{P}(B) = \{\varnothing\}$

Example 5
Let C = {7}.
$\mathcal{P}(C) = \{\varnothing, C\}$

<u>Note:</u> The elements of a power set are SETS, not numbers or letters.

In <u>Example 1</u>,

$5 \in S$	$\varnothing \subset S$	$\varnothing \in \mathcal{P}(S)$
$6 \in S$	$S \subset S$	$\{5\} \in \mathcal{P}(S)$
	$\{5\} \subset S$	$\{6\} \in \mathcal{P}(S)$
	$\{6\} \subset S$	$\{5,6\} \in \mathcal{P}(S)$

Cardinality of Sets

defn: cardinality of a set—the number of elements contained in the set

Cardinality of a Power Set

Notice the pattern in the following table:

Cardinality of a Set S	Cardinality of $\mathcal{P}$(S)
0	1
1	2
2	4
3	8
4	16
5	32
:	:
n	2^n

Thus, for any given Set S, the cardinality of $\mathcal{P}$(S) is 2^n, where n is the number of elements in S.

S = {5, 6} has 2 elements, so the cardinality of $\mathcal{P}$(S) is $2^2 = 4$.

T = {x, y, z} has 3 elements, so the cardinality of $\mathcal{P}$(T) is $2^3 = 8$.

A = {1, 3, 5} also has 3 elements, so the cardinality of $\mathcal{P}$(A) is also $2^3 = 8$.

B = $\varnothing$ has 0 elements, so the cardinality of $\mathcal{P}$(B) is $2^0 = 1$.

Note: The empty set contains 0 elements, whereas its power set contains one element.

C = {7} has 1 element, so the cardinality of $\mathcal{P}$(C) is $2^1 = 2$.

Day 10 Homework

Name: ________________________________Group: ________________________________

Concepts Covered: Power Sets, Defn & Cardinality

Provide the power set of each of the following sets.

1. A = {7, 8}

   $\mathcal{P}$ (A) = ____

   ____

2. B = {–3, –1, 0}

   $\mathcal{P}$ (B) = ____

   ____

3. C = {–2, 0, 2, 4}

   $\mathcal{P}$ (C) = ____

   ____

4. D = {a, b, 2}

   $\mathcal{P}$ (D) = ____

   ____

5. S = {1, 2, c, ∅}

   $\mathcal{P}$ (S) = ____

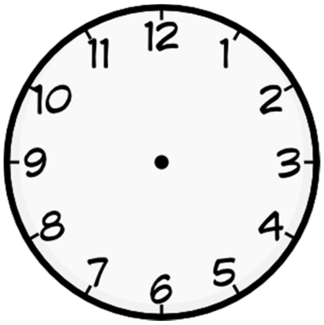
   ____

Day 12 Notes

- Concepts Covered: Clock Arithmetic, Addition and multiplication on a 12-clock, Addition, multiplication, and subtraction on a 5-clock

Clock Arithmetic

Consider an analog clock with the numbers 1-12 on it, and an hour hand. On this clock, let us say that only the integers from 1 to 12 exist. (We will not consider minutes or seconds.) How would we perform arithmetic (i.e., addition, subtraction, multiplication, or division) operations in 12-clock?



3 + 2 = 5 (2 hours past 3 o'clock is 5 o'clock)
9 + 2 = 11 (2 hours past 9 o'clock is 11 o'clock)

11 + 2 = 13 = 1 (2 hours past 11 o'clock is 1 o'clock)
8 + 7 = 15 = 3 (7 hours past 8 o'clock is 3 o'clock)

How can we figure out the last two problems easily? IOW, when the result is a number greater than 12, is there a shortcut we can use?

Day 12 Notes

The following table provides all the possible answers when any two elements of 12-clock are **ADDED**:

+	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Which patterns can be detected?

1. Each row and each column contains every integer from 1 to 12.

2. Along the main diagonal (upper left to lower right), we have the pattern 2, 4, 6, 8, 10, 12, 2, 4, 6, 8, 10, 12.

3. Each integer from 1 to 12 appears 12 times in the table.

4. Through each diagonal increasing from left to right, the same number appears. For example, we have a diagonal containing only 1's, another diagonal containing only 2's, etc.

Day 12 Notes

The following table provides all the possible answers when any two elements in 12-clock are **MULTIPLIED**:

x	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	2	4	6	8	10	12
3	3	6	9	12	3	6	9	12	3	6	9	12
4	4	8	12	4	8	12	4	8	12	4	8	12
5	5	10	3	8	1	6	11	4	9	2	7	12
6	6	12	6	12	6	12	6	12	6	12	6	12
7	7	2	9	4	11	6	1	8	3	10	5	12
8	8	4	12	8	4	12	8	4	12	8	4	12
9	9	6	3	12	9	6	3	12	9	6	3	12
10	10	8	6	4	2	12	10	8	6	4	2	12
11	11	10	9	8	7	6	5	4	3	2	1	12
12	12	12	12	12	12	12	12	12	12	12	12	12

Which patterns can be detected?

1. The bottom row and the right-most column each contain only 12's.

   Note: Two natural numbers are relatively prime if their greatest common factor (gcf) is 1.
2. In a row or column where the leading number is relatively prime with 12, each integer from 1 to 12 appears. (The rows and columns that lead with 1, 5, 7, and 11 are such examples.)

3. In a row or column where the leading number is NOT relatively prime with 12, there is a repeating pattern in the numbers that appear in that row or column. (The rows and columns that lead with 2, 3, 4, 6, 8, 9, 10, and 12 are such examples.)

4. The diagonals increasing from left to right are palindromic, i.e., they read the same forward as backward. For example, one of the diagonals has the pattern 3, 4, 3; another is 8, 2, 6, 8, 8, 6, 2, 8.

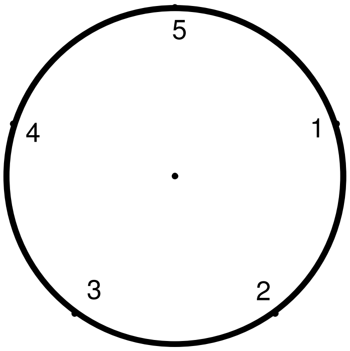
5. If two elements of 12-clock add up to 12, then the row (or column) for one element will be the mirror image of the row (or column) for the other element. For example, the row that leads with 5 is the mirror image of the row that leads with 7. (Note that this mirror-image "property" does not include the 12's that occur in the rows or columns.)

Day 12 Notes

Arithmetic on a 5-clock (Addition and Multiplication)

Imagine a clock with the integers from 1 to 5 on it. As with the 12-clock, there is an hour hand, but we will not consider minutes or seconds.

+	**1**	**2**	**3**	**4**	**5**
1	2	3	4	5	1
2	3	4	5	1	2
3	4	5	1	2	3
4	5	1	2	3	4
5	1	2	3	4	5



x	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	1	3	5
3	3	1	4	2	5
4	4	3	2	1	5
5	5	5	5	5	5

Subtraction in 5-clock

5 – 3 = 2
4 – 3 = 1
3 – 3 = 5
2 – 3 = 4 (3 hours before 2 o'clock)
1 – 3 = 3 (3 hours before 1 o'clock)

1 – 5 = 1
2 – 5 = 2
3 – 5 = 3
4 – 5 = 4
5 – 5 = 5

How does 5 behave in 5-clock? It behaves like zero does in the set of real numbers. IOW, it acts as the additive identity. That is, just as 0 is the additive identity for $\mathbb{R}$, 5 is the additive identity for 5-clock.

Name: ________________________________Group: ________________________________

Concepts Covered: Clock Arithmetic, Addition and multiplication on a 12-clock, Addition, multiplication, and subtraction on a 5-clock

Use a 7-clock to answer the following problems:

1. 5 + 2 = __________

2. 3 + 6 = __________

3. 5 + 6 = __________

4. 7 + 2 = __________

5. 4 + 4 = __________

6. 2 x 2 = __________

7. 2 x 3 = __________

8. 2 x 4 = __________

9. 3 x 4 = __________

10. 4 x 7 = __________

11. 7 – 3 = __________

12. 3 – 6 = __________

13. 4 – 5 = __________

14. 1 – 6 = __________

15. 5 – 7 = __________

16. How does 7 behave in...

    a. ...addition?

    b. ...multiplication?

    c. ...subtraction?

17. EXPLAIN how division would work on a 7-clock.

- Concepts Covered: More on Clock Arithmetic: Closure in N, Additive identity and inverse in R & N, Multiplicative identity and inverse in R & N, 5-clock within N & W (add and multiply, identity and inverse)

Closure

defn: closure—a Set S is closed under an operation $*$ if $\forall$ x , y $\in$ S, x $*$ y $\in$ S

For example, consider N = {1, 2, 3, 4, 5, ...}.

Given any two natural numbers x and y...

...their **sum** is also a natural number, so N is closed under addition.
For example, 2 $\in$ N and 8 $\in$ N, so 2 + 8 = 10 $\in$ N.

...their **difference** may not exist in N, so N is not closed under subtraction.
For example, 2 $\in$ N and 8 $\in$ N, but 2 – 8 = –6 $\notin$ N.

...their **product** is also a natural number, so N is closed under multiplication.
For example, 2 $\in$ N and 8 $\in$ N, so 2 x 8 = 16 $\in$ N.

...their **quotient** may not exist in N, so N is not closed under division.
For example, 2 $\in$ N and 8 $\in$ N, but $\frac{2}{8} = \frac{1}{4} \notin$ N.

In a nutshell, N is closed under addition and multiplication, but N is **not** closed under subtraction or division.

Identities and Inverses

Example 1: Consider R, and let x $\in$ R.

$x + \mathbf{0} = x$
↑
additive
identity element
for R

$x + \boldsymbol{-x} = 0$
↑
additive
inverse of *x*

$x \cdot \mathbf{1} = x$
↑
multiplicative
identity element
for R

$x \cdot \frac{1}{x} = 1$
↑
multiplicative
inverse of *x*, $x \neq 0$

For example, if x = 4, then...

...4 + **0** = 4.
...4 + **–4** = 0.
...4 · **1** = 4.
...4 · $\frac{1}{4}$ = 1.

For example, if x = –5, then...

... –5 + **0** = –5.
... –5 + –**(–5)** = 0
... –5 · **1** = –5.
... –5 · $\frac{1}{-5}$ = 1.

Example 2: Consider N. Then the following is true:

1. Since 0 ∉ N, N does not contain an additive identity. As a result, no element of N has an additive inverse.

2. The multiplicative identity of N is 1. However, except for 1, no element of N has a multiplicative inverse.

Note: In a particular set of numbers, the existence of an additive identity is necessary for the existence of additive inverses. However, the existence of an additive identity does not guarantee the existence of additive inverses. (A similar statement can be made with regard to multiplication.)

IOW, the existence of an additive identity is necessary, but not sufficient, for the existence of additive inverses. (Again, a similar statement can be made regarding multiplication.)

Note to Instructor: Doing the following optional example makes it difficult to get through Example 3 in the class time allotted. I have included it because it provides a good segue into Example 3. However, if you do not have time to do both, it is better to skip the optional example and do Example 3.

Optional Example

Consider 5-clock in N, i.e., consider 5-clock = {1, 2, 3, 4, 5}.

+	**1**	**2**	**3**	**4**	**5**
1	2	3	4	5	1
2	3	4	5	1	2
3	4	5	1	2	3
4	5	1	2	3	4
5	1	2	3	4	5

The additive identity is **5**:

1 + **5** = 1
2 + **5** = 2
3 + **5** = 3
4 + **5** = 4
5 + **5** = 5

Each element has an additive inverse:

1 + **4** = 5, i.e., 1^{-1} = 4
2 + **3** = 5, i.e., 2^{-1} = 3
3 + **2** = 5, i.e., 3^{-1} = 2
4 + **1** = 5, i.e., 4^{-1} = 1
5 + **5** = 5, i.e., 5^{-1} = 5

x	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	1	3	5
3	3	1	4	2	5
4	4	3	2	1	5
5	5	5	5	5	5

The multiplicative identity is 1:	1 x **1** = 1	Each element,	1 x **1** = 1, i.e., 1^{-1} = 1
	2 x **1** = 2	except 5, has a	2 x **3** = 1, i.e., 2^{-1} = 3
	3 x **1** = 3	multiplicative	3 x **2** = 1, i.e., 3^{-1} = 2
	4 x **1** = 4	inverse:	4 x **4** = 1, i.e., 4^{-1} = 4
	5 x **1** = 5		5^{-1} DNE

<u>Example 3</u>

Consider 5-clock in W. Since 5 behaves in 5-clock the way that 0 behaves in W, let us now replace 5 with 0, i.e., 5-clock = {0, 1, 2, 3, 4}.

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The additive identity is **0**:	1 + **0** = 1	Each element has	1 + **4** = 0, i.e., 1^{-1} = 4
	2 + **0** = 2	an additive inverse:	2 + **3** = 0, i.e., 2^{-1} = 3
	3 + **0** = 3		3 + **2** = 0, i.e., 3^{-1} = 2
	4 + **0** = 4		4 + **1** = 0, i.e., 4^{-1} = 1
	0 + **0** = 0		0 + **0** = 0, i.e., 0^{-1} = 0

x	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The mult. iden. is 1:	1 x **1** = 1	Each element,	1 x **1** = 1, i.e., 1^{-1} = 1
	2 x **1** = 2	except 0, has a	2 x **3** = 1, i.e., 2^{-1} = 3
	3 x **1** = 3	multiplicative	3 x **2** = 1, i.e., 3^{-1} = 2
	4 x **1** = 4	inverse:	4 x **4** = 1, i.e., 4^{-1} = 4
	0 x **1** = 0		0^{-1} DNE

Name: ________________________________Group: ________________________________

Concepts Covered: More on Clock Arithmetic: Closure in N, Additive identity and inverse in R & N, Multiplicative identity and inverse in R & N, 5-clock within N & W (add and multiply, identity and inverse)

Directions: For both of the following problems, refer to Example 3 in Day 13 notes.

1. For 8-clock, construct BOTH an addition table and a multiplication table. Use those tables to determine the identity element for each operation. Then, find the additive and multiplicative inverses for each element in 8-clock.
   BTW, 8-clock = {0, 1, 2, 3, 4, 5, 6, 7}.

2. For 10-clock, construct BOTH an addition table and a multiplication table. Use those tables to determine the identity element for each operation. Then, find the additive and multiplicative inverses for each element in 10-clock. BTW, 10-clock = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}.

- Concepts Covered: Congruence Classes in N

Congruence Classes in N

Consider the number 6 in N. Let us consider the remainders when we divide each element of W by 6, beginning with 0:

Dividend	Divisor	Remainder
0	6	0
1	6	1
2	6	2
3	6	3
4	6	4
5	6	5
6	6	0
7	6	1
8	6	2
9	6	3
10	6	4
11	6	5
12	6	0

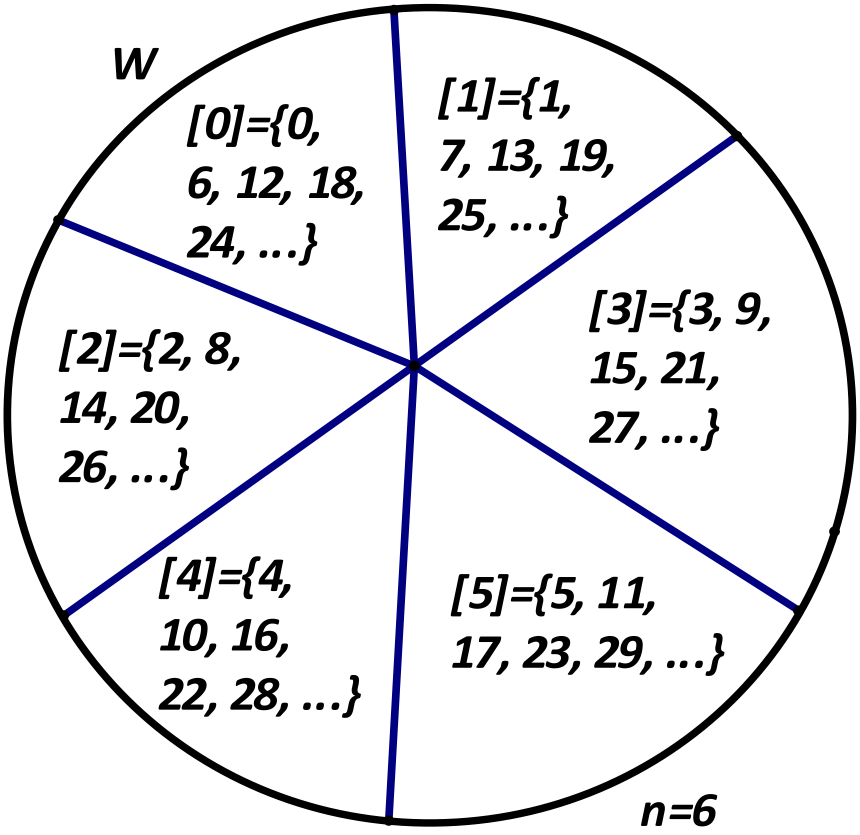
From the few problems we have done, we notice a pattern: After every 6 whole numbers, the remainders repeat, and we can group them this way:

Remainder	Whole Numbers with This Remainder
0	0, 6, 12, 18, 24, 30, 36, ...
1	1, 7, 13, 19, 25, 31, 37, ...
2	2, 8, 14, 20, 26, 32, 38, ...
3	3, 9, 15, 21, 27, 33, 39, ...
4	4, 10, 16, 22, 28, 34, 40, ...
5	5, 11, 17, 23, 29, 35, 41, ...

Each of these subsets of whole numbers is called a **congruence class** for 6.

Given a natural number *n*, there exist *n* congruence classes for *n*: [0], [1], [2], ..., [*n* – 1]. These are read as, "congruence class 0, congruence class 1, congruence class 2, etc." The names of all congruence classes for *n* represent all the possible remainders when an integer is divided by *n*.

For *n* = 6, the congruence classes are [0], [1], [2], [3], [4], [5].



<u>**Things to notice:**</u>

1. EVERY whole number is contained in one of the congruence classes for *n*.
2. NO whole number is contained in more than one of the congruence classes for *n*.
3. EACH congruence class represents an infinite subset of W.
4. The UNION of ALL the congruence classes of *n* is W.

IOW, the congruence classes for *n* divide W into *n* disjoint sets; and the union of these *n* disjoint sets is W.

Name: ________________________________Group: ________________________________

Concepts Covered: Congruence Classes in N

For EACH of the natural numbers *n* = 1, 2, 3, ..., 12, draw a circle to represent the congruence classes. For each congruence class of each *n*, list the first few elements of that set

- Concepts Covered: Z_n, Modular Arithmetic, Solving Equations in Z_n

Legend:	Symbol	Meaning
	$a \mid b$	*a* divides *b*

Z_n—aka Congruence Modulo *n*

defn: Z_n—For $n \in$ N, Z_n is the set of all congruence classes for *n*;
i.e., $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$.
We read Z_n as "Z modulo *n*," or "Z mod *n*."

Things to notice about Z_n:

1. We are now assigning the elements of Z, as opposed to just the elements of W, to congruence classes, which we did in Day 14.
2. Each element of Z_n is itself a set. IOW, Z_n is a collection of sets.
3. Z_n is a finite set since it contains *n* elements. However, each element of Z_n is an infinite set. IOW, Z_n is a finite set whose elements are infinite sets.

For $n = 6$, $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$, which we read as, "Z mod 6 is the set that contains congruence class 0, congruence class 1, congruence class 2, congruence class 3, congruence class 4, and congruence class 5."

Note: The difference of any two elements of any congruence class in Z_6 is a multiple of 6. In Z_6, consider $[4] = \{\ldots, -14, -8, -2, 4, 10, 16, 22, 28, 34, \ldots\}$. Notice, for example, that $28 - 16 = 12$, which is a multiple of 6; and $10 - (-8) = 18$, which is also a multiple of 6. This property is true for any congruence class for any Z_n.

Modular Arithmetic

Given any two integers *a* and *b*, *a* is congruent to *b* modulo *n* iff *a* and *b* are in the same congruence class for Z_n. This relationship is expressed as $a \equiv b \pmod{n}$; or $n \mid (a - b)$.

Example 1

In Z_3, $8 \equiv 5 \pmod{3}$, since $3 \mid (8 - 5)$ $5 \in [2]_3$ and $8 \in [2]_3$

$10 \equiv 4 \pmod{3}$, since $3 \mid (10 - 4)$ $10 \in [1]_3$ and $4 \in [1]_3$

Example 2

In Z_5, $9 \equiv 19 \pmod{5}$, since $5 \mid (9 - 19)$ $9 \in [4]_5$ and $19 \in [4]_5$

$11 \equiv 1 \pmod{5}$, since $5 \mid (11 - 1)$ $11 \in [1]_5$ and $1 \in [1]_5$

Example 3

In Z_6, $8 \equiv 32 \pmod 6$, since $6 \mid (8 - 32)$ $8 \in [2]_6$ and $32 \in [2]_6$

$-14 \equiv 4 \pmod 6$, since $6 \mid (-14 - 4)$ $-14 \in [4]_6$ and $4 \in [4]_6$

$-11 \equiv -23 \pmod 6$, since $6 \mid (-11 - (-23))$ $-11 \in [1]_6$ and $-23 \in [1]_6$

Solving Equations in Z_n (no unique solutions)

Example 1

$x \equiv 1 \pmod 6$

We are looking for all elements x such that $6 \mid (x - 1)$. IOW, we are looking for all elements x such that x – 1 is a multiple of 6. The following numbers will make the statement true:

$1 \in [1]_6$

$7 \in [1]_6$

$13 \in [1]_6$

$19 \in [1]_6$

.
.
.

Every element of $[1]_6$ will satisfy the equation: $[1]_6 = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$. Note that each element of $[1]_6$ is 1 more than a multiple of 6.

Example 2

$x \equiv 4 \pmod 5$

We are looking for all elements x such that $5 \mid (x - 4)$: $4 \in [4]_5$

$9 \in [4]_5$

$14 \in [4]_5$

$19 \in [4]_5$

.
.
.

Every element of $[4]_5$ will satisfy the equation: $[4]_5 = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$. Note that each element of $[4]_5$ is 4 more than a multiple of 5.

Example 3

$x + 2 \equiv 6 \pmod 8$

We are looking for all elements x such that $8 \mid (x + 2 - 6)$; or $8 \mid (x - 4)$:

$4 \in [4]_8$

$12 \in [4]_8$

$20 \in [4]_8$

$28 \in [4]_8$

.
.
.

Every element of $[4]_8$ will satisfy the equation: $[4]_8 = \{..., -20, -12, -4, 4, 12, 20, ...\}$. Note that the symmetry in the elements of $[4]_8$ is a coincidence. It is not always the case that both a number and its opposite will be elements of the same congruence class.

Example 4

$x + 3 \equiv 9 \pmod 5$

We are looking for all elements x such that $5 \mid (x + 3 - 9)$; or $5 \mid (x - 6)$: $6 \in [1]_5$

$11 \in [1]_5$

$16 \in [1]_5$

$21 \in [1]_5$

.

.

.

Every element of $[1]_5$ will satisfy the equation: $[1]_5 = \{..., -14, -9, -4, 1, 6, 11, 16, ...\}$.

Name: ________________________________Group: ________________________________

Concepts Covered: Z_n, Modular Arithmetic, Solving Equations in Z_n

1. For **EACH** Z_n, where $3 \le n \le 12$, provide three numbers that are congruent to 5 (mod n). IOW, provide three numbers that are congruent to 5 (mod 3); three numbers that are congruent to 5 (mod 4); three numbers that are congruent to 5 (mod 5), and so on, until you get to 5 (mod 12).

For EACH of the following equations, provide three possible solutions.

2. $x \equiv 4 \pmod 7$ ___________ ___________ ___________
3. $x \equiv 4 \pmod 9$ ___________ ___________ ___________
4. $x \equiv 7 \pmod{10}$ ___________ ___________ ___________
5. $x \equiv 8 \pmod 3$ ___________ ___________ ___________
6. $x + 1 \equiv 4 \pmod 9$ ___________ ___________ ___________
7. $x + 3 \equiv 5 \pmod 7$ ___________ ___________ ___________
8. $x + 2 \equiv 7 \pmod 5$ ___________ ___________ ___________
9. $x + 3 \equiv 2 \pmod 4$ ___________ ___________ ___________
10. $x + 6 \equiv 8 \pmod 3$ ___________ ___________ ___________
11. $x + 4 \equiv 6 \pmod 4$ ___________ ___________ ___________

- Concepts Covered: Units in Z_n, specifically Z_4, Z_6, Z_8, and Z_9, U_4, U_6, U_8, U_9, Properties of Groups (Memorize for Day 17)

Units

Example 1

Consider Z_6 with multiplication:

x	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	**1**	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	**1**

The following is true: --mult. iden. = 1

--only 1 and 5 have mult. inverses:

0^{-1} DNE
$1^{-1} = 1$, since $1 \times 1 = 1$
2^{-1} DNE
3^{-1} DNE
4^{-1} DNE
$5^{-1} = 5$, since $5 \times 5 = 1$

Example 2

Consider Z_4 with multiplication:

x	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	**1**	2	3
2	0	2	0	2
3	0	3	2	**1**

The following is true: --mult. iden. = 1

--only 1 and 3 have mult. inverses:

0^{-1} DNE
$1^{-1} = 1$, since $1 \times 1 = 1$
2^{-1} DNE
$3^{-1} = 3$, since $3 \times 3 = 1$

defn: For multiplication in Z_n, any element of Z_n that has an inverse is called a **unit** of Z_n. The set containing the units for Z_n is denoted by U_n.

For Z_6, $U_6 = \{1, 5\}$; and for Z_4, $U_4 = \{1, 3\}$.

Example 3

Consider Z_8 with multiplication:

x	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	**1**	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	**1**	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	**1**

The following is true: --mult. iden. = 1

--only 1, 3, 5, and 7 have mult. inverses:

0^{-1} DNE
$1^{-1} = 1$, since 1 x 1 = 1
2^{-1} DNE
$3^{-1} = 3$, since 3 x 3 = 1
4^{-1} DNE
$5^{-1} = 5$, since 5 x 5 = 1
6^{-1} DNE
$7^{-1} = 7$, since 7 x 7 = 1

-- $U_8 = \{1, 3, 5, 7\}$

Example 4

Consider Z_9 with multiplication:

x	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8
2	0	2	4	6	8	**1**	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	**1**	5
5	0	5	**1**	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	**1**	8	6	4	2
8	0	8	7	6	5	4	3	2	**1**

The following is true: --mult. iden. = 1

--only 1, 2, 4, 5, 7, and 8 have mult. inverses:

0^{-1} DNE
$1^{-1} = 1$, since 1 x 1 = 1
$2^{-1} = 5$, since 2 x 5 = 1
3^{-1} DNE
$4^{-1} = 7$, since 4 x 7 = 1

$5^{-1} = 2$, since $5 \times 2 = 1$
6^{-1} DNE
$7^{-1} = 4$, since $7 \times 4 = 1$
$8^{-1} = 8$, since $8 \times 8 = 1$

--$U_9 = \{1, 2, 4, 5, 7, 8\}$

Note: The elements of Z_6 that are also elements of U_6 are those integers (1 and 5) that are relatively prime with 6.

The elements of Z_4 that are also elements of U_4 are those integers (1 and 3) that are relatively prime with 4.

The elements of Z_8 that are also elements of U_8 are those integers (1, 3, 5, 7) that are relatively prime with 8. (Note to Instructor: No need to mention this one if you skipped Example 3 above.)

The elements of Z_9 that are also elements of U_9 are those integers (1, 2, 4, 5, 7, 8) that are relatively prime with 9.

The elements of Z_n that are also elements of U_n are those that are relatively prime with *n.*

Note: The following is true: $U_6 \subset Z_6$
$U_4 \subset Z_4$
$U_8 \subset Z_8$
$U_9 \subset Z_9$

In general, $U_n \subset Z_n$.

Note to Instructor: Example 5 is optional, although recommended.

Example 5:
Find U_{10} without making a table for Z_{10}.

The elements of Z_{10} are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Of those, 1, 3, 7, and 9 are relatively prime with 10. Therefore, $U_{10} = \{1, 3, 7, 9\}$.

Memorize the following for Day 17, as we will begin our discussion of groups on that day.

There are FOUR properties associated with groups:

1. Closure
2. Associativity
3. Identity
4. Inverse

Name: _________________________________Group: _________________________________

Concepts Covered: Units in Z_n, specifically Z_4, Z_6, Z_8, and Z_9, U_4, U_6, U_8, U_9, Properties of Groups (Memorize for Day 17)

Find U_{12}, U_{15}, U_{18}, and U_{21}; and provide the multiplication table for each one. You may have empty cells left over.

1. U_{12} = _______________________________

x											

2. U_{15} = _______________________________

x											

3. U_{18} = ________________________________

x											

4. U_{21} = ________________________________

x													

- Concepts Covered: Defn of "Group", Determining whether Z_5 or U_5 is a group under multiplication, Showing that a set G is a group under $*$

Groups

defn: A **group** is a set G equipped with an operation $*$ such that the following is true:

1. G is **closed** under $*$.
   That is, $\forall\, a, b \in G, a * b \in G$.

2. G is **associative** under $*$.
   That is, $\forall\, a, b, c \in G, a * (b * c) = (a * b) * c$.

3. G contains an **identity** element e.
   That is, $\exists\, e \in G \ni a * e = a = e * a\ \forall\, a \in G$.

4. G contains an **inverse** element for every a in G.
   That is, $\forall\, a \in G, \exists\, a^{-1} \in G \ni a * a^{-1} = e = a^{-1} * a$.

Note: In order to show that a particular set G is a group under $*$, it is necessary to show that each of the four properties of a group holds for G.

Example 1: Is Z_5 a group under multiplication?

x	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

1. Check for **closure:** It is clear from the table that for any two elements of Z_5, their product is also an element of Z_5, so Z_5 is closed under multiplication.

2. Check for **associativity:** It would be extremely tedious and time-consuming to check all possible combinations, so we will check only two of them. Most of the time, however, we will need to do a formal proof for associativity.

   1 x (2 x 3) = 1 x (1) = 1 **and** (1 x 2) x 3 =(2) x 3 = 1, so 1 x (2 x 3) = (1 x 2) x 3.
   1 x (2 x 4) = 1 x (3) = 3 **and** (1 x 2) x 4 = (2) x 4 = 3, so 1 x (2 x 4) = (1 x 2) x 4.

   Thus, Z_5 is associative.

3. Check for a multiplicative **identity:** 0 x 1 = 0,
   1 x 1 = 1,
   2 x 1 = 2,

$3 \times 1 = 3$, and
$4 \times 1 = 4$, so 1 is the mult. iden. for Z_5.

4. Check to see whether each element has a multiplicative **inverse:**

   From the table, it is clear that every element except 0 has a multiplicative inverse. Since 0^{-1} DNE, we say that Z_5 fails at inverse. Hence Z_5 is **not** a group under multiplication.

Example 2: Is U_5 a group under multiplication?

x	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1. Check for **closure:** It is clear from the table that the product of any two elements in U_5 is also an element of U_5, so U_5 is closed under multiplication.

2. Check for **associativity:** As with Z_5, we will check only two combinations:

   $2 \times (1 \times 4) = 2 \times (4) = 3$ **and** $(2 \times 1) \times 4 = (2) \times 4 = 3$, so $2 \times (1 \times 4) = (2 \times 1) \times 4$.
   $4 \times (2 \times 3) = 4 \times (1) = 4$ **and** $(4 \times 2) \times 3 = (3) \times 3 = 4$, so $4 \times (2 \times 3) = (4 \times 2) \times 3$.

   Thus U_5 is associative.

3. The multiplicative **identity** for U_5 is 1, since $1 \times 1 = 1$,
   $2 \times 1 = 2$,
   $3 \times 1 = 3$, and
   $4 \times 1 = 4$.

4. Every element of U_5 has a multiplicative **inverse:** $1^{-1} = 1$,
   $2^{-1} = 3$,
   $3^{-1} = 2$, and
   $4^{-1} = 4$.

Since U_5 is closed under multiplication; is associative with regard to multiplication; has a multiplicative identity element; and a multiplicative inverse exists for every element of U_5, U_5 is a group under multiplication, Q. E. D.

Example 3: Show that G with the indicated operation is a group:
$G = Q$; $a * b = a + b + 3$

Note to Instructor: If you need to use particular/specific elements of Q to help students understand closure, associativity, identity, and inverse under $*$, then do so. Keep in mind, however, that students need to know that producing an ***example*** of closure does not ***prove*** closure under $*$; producing an ***example*** of associativity does not ***prove*** associativity under $*$; and so on. Also be aware that if too much time is spent on specific examples, there will not be enough time in class to do the actual proof.

1. **Closure:** Since Q is closed under addition, and $*$ in G is defined in terms of addition of rationals, G is closed under $*$.

2. **Associativity:** Show that for $\forall\, a, b, c \in$ G, $a * (b * c) = (a * b) * c$:

$a * (b * c)$	$(a * b) * c$
$= a * (b + c + 3)$	$= (a + b + 3) * c$
$= a + (b + c + 3) + 3$	$= (a + b + 3) + c + 3$
$= a + b + c + 6$	$= a + b + c + 6$

$\therefore$ G is associative under $*$.

3. **Identity:** Show that $\exists\, e \in$ G $\ni a * e = a = e * a\ \forall\, a \in$ G.

We first need to find a candidate for e, and then verify that the candidate is, in fact, the identity element e.

According to how $*$ is defined in G, we know that $a * e = a + e + 3$. We want the value of e such that $a + e + 3 = a$. Solving this last equation for e yields $e = –3$. We now need to verify that –3 is the identity element for G:

$a * –3 = a + –3 + 3 = a$ $\qquad$ $–3 * a = –3 + a + 3 = a$

Since $a * –3 = a = –3 * a$, $e = –3$ is the identity element for G.

4. **Inverse:** Show that $\forall\, a \in$ G, $\exists\, a^{–1} \in$ G $\ni a * a^{–1} = e = a^{–1} * a$.
IOW, show that $\forall\, a \in$ G, $a * a^{–1} = –3 = a^{–1} * a$.

We first need to find a candidate for $a^{–1}$, and then verify that the candidate is, in fact, the inverse element for a.

According to how $*$ is defined in G, we know that $a * a^{–1} = a + a^{–1} + 3$. We want the value of $a^{–1}$ such that $a + a^{–1} + 3 = –3$. Solving this last equation for $a^{–1}$ yields
$a^{–1} = –a – 6$. We now need to verify that $–a – 6$ is the inverse element for a:

$a * (–a – 6) = a + (–a – 6) + 3 = –3$ $\qquad$ $(–a – 6) * a = (–a – 6) + a + 3 = –3$

Since $a * (–a – 6) = e = (–a – 6) * a$, $–a – 6$ is the inverse of a in G.

Since G is closed under $*$; is associative under $*$; has an identity element e;
and has an inverse $a^{–1}$ for every element a in G, G is a group under $*$, Q. E. D.

Name: ________________________________Group: ________________________________

Concepts Covered: Defn of "Group", Determining whether Z_5 or U_5 is a group under multiplication, Showing that a set G is a group under $*$

Show that each of the following sets is a group under the indicated operation.

1. $G = U_8$
   $a * b = a \cdot b$
   (Only show 2 examples when testing for associativity.)

2. $G = Q$
   $a * b = a + b + 2$

3. $G = Z$
   $a * b = a + b - 3$

- Concepts Covered: More on Groups

Example 1

Show that G is a group with the given operation: **G = {x $\in$ Q | x $\neq$ 0}**

***a* ∗ *b* =** $\frac{ab}{2}$

Pf:

i. Check for closure: Because x $\neq$ 0, we need to check for the possibility that $\frac{ab}{2}$ = 0:

To show that $\frac{ab}{2} \neq 0$, spse $\frac{ab}{2}$ = 0: Part I: Solve $\frac{ab}{2}$ = 0 for *a*: *ab* = 0

a = 0 or *b* = 0, a contradiction since *a*, *b* $\in$ G

Part II: Solve $\frac{ab}{2}$ = 0 for *b*: *ab* = 0

a = 0 or *b* = 0, a contradiction since *a*, *b* $\in$ G

Since Q is closed under multiplication and division by 2; and $\frac{ab}{2} \neq 0$,

G is closed under ∗.

ii. Show that $(a * b) * c = a * (b * c)\ \forall\ a, b, c \in$ G:

$(a * b) * c$	$a * (b * c)$
$= \frac{ab}{2} * c$	$= a * \frac{bc}{2}$
$= \frac{\frac{ab}{2}c}{2}$	$= \frac{a\frac{bc}{2}}{2}$
$= \frac{\frac{abc}{2}}{2}$	$= \frac{\frac{abc}{2}}{2}$
$= \frac{abc}{4}$	$= \frac{abc}{4}$

Clearly, G is associative under ∗.

iii. Find identity element *e*, if it exists.

According to the way $*$ is defined in G, $a * e = \frac{ae}{2}$.

We want $\frac{ae}{2} = a$. Solving for *e* yields $ae = 2a \Leftrightarrow e = 2$.

Now verify that $e = 2$: $a * 2 = \frac{a(2)}{2} = a$

$$2 * a = \frac{2(a)}{2} = a$$

Thus, $e = 2$ is the identity element for G.

iv. Find a^{-1} for each $a \in$ G, if it exists.

According to the way $*$ is defined in G, $a * a^{-1} = \frac{aa^{-1}}{2}$.

We want $\frac{aa^{-1}}{2} = 2$. Solving for a^{-1} yields $aa^{-1} = 4 \Leftrightarrow a^{-1} = \frac{4}{a}$.

Now verify that $a^{-1} = \frac{4}{a}$: $a * \frac{4}{a} = \frac{a\frac{4}{a}}{2} = \frac{4}{2} = 2 = e$.

$$\frac{4}{a} * a = \frac{\frac{4}{a}a}{2} = \frac{4}{2} = 2 = e.$$

Thus, a^{-1} exists in G for every *a* in G.

Since all four properties of a group hold for G, G is a group under $*$, Q. E. D.

Example 2

Show that G is a group with the given operation: **G = {x | x $\in$ Q and x $\neq$ 1}**

$$\boldsymbol{a * b = a + b - ab}$$

Pf:

i. Check for closure: Because $x \neq 1$, we need to check for the possibility that $a + b - ab = 1$:

Part I: To show that $a + b - ab \neq 1$, spse $a + b - ab = 1$: Part I: Solve $a + b - ab = 1$ for *a*:

$a - ab + b = 1$
$1a - ab + b = 1$
$a(1 - b) + b = 1$
$a(1 - b) = 1 - b$

$$a = \frac{1-b}{1-b}$$

$$a = 1,$$

A contradiction since no element of G can be 1.

Part II: Solve $a + b - ab = 1$ for b: Pf is similar to Part I; we reach the same contradiction.

Since Q is closed under addition and subtraction; and $a + b - ab \neq 1$, G is closed under $*$.

ii. Show that $(a * b) * c = a * (b * c)\ \forall\ a, b, c \in$ G:

$$\begin{aligned}&(a * b) * c\\ =\ &(a + b - ab) * c\\ =\ &(a + b - ab) + c - (a + b - ab)c\\ =\ &(a + b - ab) + c - ac - bc + abc\\ =\ &a + b + c - ab - ac - bc + abc\end{aligned}$$

$$\begin{aligned}&a * (b * c)\\ =\ &a * (b + c - bc)\\ =\ &a + (b + c - bc) - a(b + c - bc)\\ =\ &a + (b + c - bc) - ab - ac + abc\\ =\ &a + b + c - bc - ab - ac + abc\\ =\ &a + b + c - ab - ac - bc + abc\end{aligned}$$

Clearly, G is associative under $*$.

iii. Find identity element e, if it exists.

According to the way $*$ is defined in G, $a * e = a + e - ae$.

We want $a + e - ae = a$. Solving for e yields $e - ae = 0 \Leftrightarrow e(1 - a) = 0 \Leftrightarrow e = 0$.
(Since $a \neq 1$, $1 - a \neq 0$, so it is permissible to divide both sides of the equation by $1 - a$.)

Now verify that $e = 0$:

$$a * 0 = a + 0 - a \bullet 0 = a + 0 - 0 = a$$
$$0 * a = 0 + a - 0 \bullet a = 0 + a - 0 = a$$

Thus, the identity element e for G is 0.

iv. Find a^{-1} for each $a \in$ G, if it exists.

According to the way $*$ is defined in G, $a * a^{-1} = a + a^{-1} - aa^{-1}$.

We want $a + a^{-1} - aa^{-1} = 0$. Solving for a^{-1} yields

$$\begin{aligned}&a^{-1} - aa^{-1} = -a\\ \Leftrightarrow\ &a^{-1}(1 - a) = -a\\ \Leftrightarrow\ &a^{-1} = \frac{-a}{1-a} = \frac{-1a}{-1(a-1)} = \frac{a}{a-1}\end{aligned}$$

Now verify that $a^{-1} = \dfrac{a}{a-1}$:

$$a * \frac{a}{a-1} = a + \frac{a}{a-1} - a \bullet \frac{a}{a-1}$$
$$= a + \frac{a}{a-1} - \frac{a^2}{a-1}$$

$$= \frac{a(a-1)}{a-1} + \frac{a}{a-1} - \frac{a^2}{a-1}$$

$$= \frac{a^2 - a + a - a^2}{a-1}$$

$$= \frac{0}{a-1}$$

$$= 0$$

$$\frac{a}{a-1} * a = \frac{a}{a-1} + a - \frac{a}{a-1} \bullet a$$

$$= \frac{a}{a-1} + \frac{a(a-1)}{a-1} - \frac{a^2}{a-1}$$

$$= \frac{a + a^2 - a - a^2}{a-1}$$

$$= \frac{0}{a-1}$$

$$= 0$$

Thus, a^{-1} exists in G for every a in G.

Since all four properties of a group hold for G, G is a group under $*$, Q. E. D.

Name: ________________________________Group: ________________________________

Concepts Covered: More on Groups

Show that each of the following sets is a group under the indicated operation.

1. $G = \{ x \in Q \mid x \neq -1 \}$
   $a * b = a + b + ab$

2. $G = \{ x \in Q \mid x \neq 0 \}$
   $a * b = \dfrac{ab}{3}$

- Concepts Covered: Even More on Groups

Note to Instructor: Test 2, which covers Days 12-19, is scheduled for Day 20. Consequently, there is no quiz for Day 19.

Even More on Groups

For examples 1 and 2, determine whether the given set G with operation $*$ is a group.

Example 1: G = {x | x $\in$ Q, x $\neq$ 0}

$a * b = \frac{a+b}{ab}$

a. Closure—Spse a = 3 and b = –3. Then $\frac{a+b}{ab} = \frac{3+(-3)}{3(-3)} = 0$. Since no element of G can equal 0, G is not closed under $*$. Therefore, G is **not** a group under $*$.

Example 2: G = Q

$a * b = \frac{a+b}{2}$

a. Closure—Since Q is closed under addition and division by 2, and $*$ in G is defined in terms of rational addition and division, G is closed under $*$.

b. Associativity—Show that $a * (b * c) = (a * b) * c$.

$a * (b * c)$	$(a * b) * c$
$= a * \frac{b+c}{2}$	$= \frac{a+b}{2} * c$
$= \frac{a + \frac{b+c}{2}}{2}$	$= \frac{\frac{a+b}{2} + c}{2}$
$= \frac{\frac{2a+b+c}{2}}{2}$	$= \frac{\frac{a+b+2c}{2}}{2}$
$= \frac{2a+b+c}{4}$	$= \frac{a+b+2c}{4}$

Since G is not associative under $*$, G is **not** a group under $*$.

Name: ________________________________Group: ________________________________

Concepts Covered: Even More on Groups

Prove or disprove that each of the following sets is a group under the indicated operation.

1. G = Q; $a * b = \dfrac{a+b}{3}$

2. G = Q; $a * b = a + b - 5$

3. G = $\{x \in Q \mid x \neq 0\}$; $a * b = \dfrac{a-b}{ab}$

4. G = Z; $a * b = a^b + b^a$

Day 1

"Is a/Has a" form of a definition

"Is a" component—tells what something is

"Has a" component—tells which properties that something has, or what it does

Terminology of Sets

The word "set" is undefined in mathematics, but we can provide a description of a set: Any **well-defined** list, collection, or class of objects.

What to call those objects that are contained in a set?

defn: element or member (of a set)—any object contained within a set

Day 2

Sets of Numbers

N = set of natural numbers = {1, 2, 3, 4, ...}

N aka the set of counting numbers.

W = set of whole numbers = {0, 1, 2, 3, 4, ...}

W = set containing 0 and all elements of N

$Z \ = \ \text{set of integers} \ = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\} \ = \ \{0,\pm1,\pm2,\pm3,\ldots\}$

Z = set containing 0, the natural numbers, and the negative of each natural number

Z^+ = set of positive integers = {1, 2, 3, 4, ...}

$Z^- \ = \ \text{set of negative integers} \ = \ \{-1,-2,-3,-4,\ldots\}$

Note: N = Z^+

Q = set of rational numbers

Q^+ = set of positive rational numbers

$Q^{?}$ = set of negative rational numbers

defn: rational number—a real number of the form $\frac{p}{q}$, where $p \in Z$, $q \in Z$, and $q \neq 0$.

R = set of real numbers

R = set containing all rational AND irrational numbers

R - Q = set of irrational numbers

defn: irrational number—a real number that **cannot** be expressed in the form

$\frac{p}{q}$, where $p \in Z$, $q \in Z$, and $q \neq 0$.

Set-Builder Notation

In order to define a set using set-builder notation, one must state the property or properties that all elements in that set must satisfy.

Day 3

Finite and Infinite Sets

defn: finite set—is a set containing a finite number of elements

It is possible to list all the elements of a finite set.

defn: infinite set—is a set containing an infinite number of elements

It is not possible to list all the elements of an infinite set.

defn: empty set—a set that contains no elements; aka the null set; denoted by $\varnothing$ or { }

***Note:** The empty set is NOT denoted by $\{\varnothing\}$, which is actually the set that contains the empty set. $\varnothing$ contains zero elements, whereas $\{\varnothing\}$ contains one element.

Subsets

Given two sets A and B, we say that A is a subset of B if every element of A is also an element of B. IOW, $A \subset B$ if $\forall\ x \in A$, $x \in B$.

Day 4

Equality of Sets

For any two sets A and B, $A = B$ iff $A \subset B$ and $B \subset A$.

IOW, $A = B$ iff $\forall\, x \in A$, $x \in B$, and $\forall\, x \in B$, $x \in A$.

Operations on Sets

For any two sets S and T, their **intersection** is given by $S \cap T = \{x \mid x \in S$ **and** $x \in T\}$.

For any two sets S and T, their **union** is given by $S \cup T = \{x \mid x \in S$ **or** $x \in T\}$.

For any two sets S and T, their **difference** is given by $S - T = \{x \mid x \in S \text{ and } x \notin T\}$.

Universal Sets

defn: Universal Set—the set whose subsets are under consideration in a particular discussion; denoted by U

defn: Consider a Set $S \ni S \subset U$. The **complement** of S, denoted by S^C, is given by the following: $S^C = \{x \mid x \in U \text{ and } x \notin S\}$.

Day 5

Some Defns and Props of Sets

Consider the sets U, A, and B, where U is the Universal Set; $A \subset U$; and $B \subset U$. Then the following is true:

1. defn of set intersection: $x \in A \cap B \Leftrightarrow x \in A \text{ and } x \in B$
2. props of set intersection: $(A \cap B) \subset A$
   $(A \cap B) \subset B$
   $x \notin A \Rightarrow x \notin A \cap B$
3. defn of set union: $x \in A \cup B \Leftrightarrow x \in A \text{ or } x \in B$
4. props of set union: $A \subset (A \cup B)$
   $B \subset (A \cup B)$
   $x \in A \Rightarrow x \in A \cup B$
5. defn of set difference: $x \in A - B \Leftrightarrow x \in A \text{ and } x \notin B$
6. props of set complement: $x \in A \Rightarrow x \notin A^C$
   $x \in A^C \Rightarrow x \notin A$

Day 9

Prove that the empty set is a subset of every set. IOW, given any set S, show that $\varnothing \subset S$.

Pf (by contradiction): Spse $\varnothing \not\subset S$. Then by the defn of subset, $\exists\, x \in \varnothing \ni x \notin S$. However, by the defn of empty set, $x \notin \varnothing$, a contradiction. Therefore, $\varnothing \subset S$; i.e., the empty set is a subset of every set, Q. E. D.

Day 10

Power Sets

defn: power set of Set S—denoted by P(S), it is the collection of all subsets of S

Cardinality of Sets

defn: cardinality of a set—the number of elements contained in the set

For any given Set S, the cardinality of P(S) is 2^n, where n is the number of elements in S.

Day 13

Closure

defn: closure—a Set S is closed under an operation $*$ if $\forall$ x , y $\in$ S, x $*$ y $\in$ S

Identities and Inverses

Consider R, and let x $\in$ R.

$$x + \underset{\substack{\uparrow\\ \text{additive}\\ \text{identity element}\\ \text{for R}}}{\mathbf{0}} = x \qquad\qquad x + \underset{\substack{\uparrow\\ \text{additive}\\ \text{inverse of } x}}{\mathbf{-x}} = 0$$

$$x \cdot \underset{\substack{\uparrow\\ \text{multiplicative}\\ \text{identity element}}}{\mathbf{1}} = x \qquad\qquad x \cdot \underset{\substack{\uparrow\\ \text{multiplicative}\\ \text{inverse of } x,\ x\ ⍰\ 0}}{\frac{1}{x}} = 1$$

Note: In a particular set of numbers, the existence of an additive identity is necessary for the existence of additive inverses. However, the existence of an additive identity does not guarantee the existence of additive inverses. (A similar statement can be made for multiplication.)

Day 14

Congruence

Given a natural number *n*, there exist *n* congruence classes for *n*: [0], [1], [2], ..., [*n* − 1]. These are read as, "congruence class 0, congruence class 1, congruence class 2, etc." The names of all congruence classes for *n* represent all the possible remainders when an integer is divided by *n*.

Day 15

Z_n—aka Congruence Modulo *n*

defn: Z_n—For $n \in$ N, Z_n is the set of all congruence classes for *n*;
i.e., Z_n = {[0], [1], [2], ... , [*n* − 1]}.
We read Z_n as "Z modulo *n*," or "Z mod *n*."

Modular Arithmetic

Given any two integers *a* and *b*, *a* is congruent to *b* modulo *n* if *a* and *b* are in the same congruence class for Z_n. This relationship is expressed as $a \equiv b$ (mod *n*); or $n|(a - b)$.

Solving Equations in Z_n (no unique solutions)

Example

x ≡ 1 (mod 6)

We are looking for all elements x such that 6|(x − 1). IOW, we are looking for all elements x such that x− 1 is a multiple of 6. The following numbers will make the statement true:

$1 \in [1]_6$
$7\in [1]_6$
$13 \in [1]_6$
$19 \in [1]_6$

Every element of $[1]_6$ will satisfy the equation: $[1]_6$ = {..., −11, −5, 1, 7, 13, ...}. Note that each element of $[1]_6$ is 1 more than a multiple of 6.

Day 16

defn: For multiplication in Z_n, any element of Z_n that has an inverse is called a **unit** of Z_n. The set containing the units for Z_n is denoted by U_n.

The elements of Z_n that are also elements of U_n are those that are relatively prime with *n.*

Note: In general, $U_n \subset Z_n$.

Days 17, 18, 19

Groups

defn: A **group** is a set G equipped with an operation * such that the following is true:

1. G is **closed** under $*$.
   IOW, $\forall\ a, b \in \mathrm{G}, a * b \in \mathrm{G}$.
2. G is **associative** under $*$.
   IOW, $\forall\ a, b, c \in \mathrm{G}, a * (b * c) = (a * b) * c$.
3. G contains an **identity** element e.
   IOW, $\exists\ e \in \mathrm{G} \ni \forall\ a \in \mathrm{G}, a * e = a = e * a$.
4. G contains an **inverse** element for every a in G.
   IOW, $\forall\ a \in \mathrm{G}, \exists\ a^{-1} \in \mathrm{G} \ni a * a^{-1} = e = a^{-1} * a$.

Note: In order to show that a particular set G is a group under ⍰, it is necessary to show that each of the four properties of a group hold for G.

Rules for Reference Card

1. If you choose to use a reference card for the Final Exam, you must use the index card that I provide for you. (Make sure you do not lose your card, because replacement cards will not be available.)

2. You may mark only on the side of the card that does NOT have your name on it.

3. You may write any information on the card that you think will help you during the Final Exam. Definitions, problems from your notes, and quiz or test questions with the correct answers, are examples of the type of information that you may write on your index card.

4. Whichever information you place on the card must be handwritten on the card itself. For example, you may not print the information from a computer file, word processor, or typewriter, and then paste or tape it to the index card.

5. During the Final Exam, you may not trade cards with any other student. Doing so, or attempting to do so, will constitute cheating.

If these rules are not followed, you will lose the use of your reference card for the Final Exam.