Groups

Modular Systems

Chapter 10 – Section 1

Definition

- A group is a mathematical system consisting of a set and one binary operation defined on it such that it has the following properties;
  - Closure
  - Associative
  - Identity
  - Inverse

No in-class assignment problem

Integers and Addition – A Group?

- Closure
- Associative
- Identity
- Inverse

The integers under addition form a group.

- 2 +-3 = -1 belongs t o I → yes closed.
- -4+(-2+7) = -1
  (-4+-2)+7 = -1 → yes, associative.
- -6 +0 = -6
  0 +-6 = -6 → yes, 0 is the identity
- -2+2 = 2+-2 = 0 → yes each integer has its opposite

In-class Assignment 23 - 1

A finite system – Is it a Group?

- Given B = {x, y, z} and the operation Δ defined by the table at the right.
- Closure – any strangers?
- Associative –(x Δ z) Δ z = y Δ z = z and x Δ (z Δ z) = x Δ x = z . No easy way.

Δ	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

- Identity – is there a row and column with the elements in the same order as at the top? If there is the identity will be the heading of that row and column.
- Inverse – is the identity once and only once in each row and
- column. Look up to the headings. z and x are inverses of each other.
- Yes it is a group.

In-class Assignment 23 - 2

An Abelian Group

- If a mathematical system is a group and it also has the commutative property then the system is called an Abelian group.
- The commutative property is recognized in a finite system if there is symmetry about a line from upper left to lower right

Δ	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

There is symmetry about the line, therefore the system is an Abelian group.

In-class Assignment 23 - 3

Modular Systems

- A modular systems is a finite mathematical system whose size is determined by the mod (modular number) *m*.
- The finite set of elements is unually numbers 0, 1, 2, 3, …, *m* −1.
- Every element in a mod system represents an infinite number of numbers called an equivalence class.

No in-class assignment problem

Mod 7

- Array W into 7 equivalence classes.

0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	continue in this manner			

Every number under 2 is equivalent to 2. 16 ≡ 23(mod 7)
a ≡ b (mod m) if a and b when divided by m yield the same remainder.

In-class Assignment 23 - 4

399 in Mod 7

- In which equivalence class and row in the array is 399?
  - Need to know the remainder when 399 is divided by 7.
- Remainder is 0 so 399 is in the 0 equivalence class.
- The quotient is 57 so 399 is in 57^{th} row down under the heading row.

$$
\begin{array}{r}
57 \\
7\overline{)399} \\
-35 \\
\hline
49 \\
-49 \\
\hline
0
\end{array}
$$

In-class Assignment 23 4

Equivalency Without the Array

- To determine whether or not two numbers belong to the same equivalence class in a mod system
  - Divide each of the numbers by the mod.
  - If the remainders are the same the two numbers are equivalent and they both belong to the equivalence classed named by the remainder.
  - If the remainders are not the same the two numbers are not equivalent in that mod.

  - 38 ≡ 62 (mod 6). Call them 2 (mod 6).

In-class Assignment 23 - 5