Lecture Outline for Mathematical Structures

- Main topics
  - Groups: Definition
  - Semi-group & Monoid: Definition
  - Identification of different structures
  - Polynomials
  - Operations modulo *n*
  - Results about groups
- Section 8.1 of text (only portions covered in class)

Properties on Binary Relations

- Consider a set S and a binary relation o on S
  - The relation has to be closed under S
- The relation o can have various properties
  - Associative: $x o (y o z) = (x o y) o z$
  - Commutative: $x o y = y o x$
  - Identity element: $x o i = i o x = x$
  - Inverse element: $x o x^{-1} = x^{-1} o x = i$

8/4÷4/8

(8/4)/2 ≠ 8/(4/2)

2+0=0+2 =2

2+(-2)=0

Properties on Binary Relations

- Note
  - Identity element is common to all elements in set S
  - Inverse is specific to the element
  - Identity and inverse must also lie in the same set
  - Identity and inverse definitions use commutativity
- Example: [Z, +]

Definitions: Group, Semigroup, Monoid

- Each of these structures pertain to the set and the binary operation
- Group: Associative, Identity element, Inverse element
- Commutative Group: Add commutative property
- Monoid: All group properties except inverse element
- Semi-group: All group properties except inverse element and identity element

Identifications

- Say which of the following are what mathematical structure
  - [Z, +]
  - [R^+, *]
  - [R, *]
- Consider 2 × 2 matrices on Z ($M_2(Z)$)
  - What is the identity element for [$M_2(Z)$, *]?
- What mathematical structure is
  [$M_2(Z)$, *]?

More Identifications

- Given that the following are semi-groups. What additional property can you tell?
  - [N, +]
  - [N, *]
  - [R^+, +]
  - [Q, *]
  - [R, +]

Polynomials

- Consider polynomial in *x* with real number coefficients
  - $a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$, where $a_n \neq 0$, $a_i \in R$
- The set of polynomials is called R[x]
- Note:
  - [R[x], +] is a ?
  - [R[x], *] is a ?

Operations modulo n

- Consider addition modulo 5
  - $x +_5 y = (x+y) \bmod 5$
  - $3 +_5 4 = 2$
- Consider multiplication modulo 5
  - $x *_5 y = (x*y) \bmod 5$
  - $3 *_5 4 = 2$
- Consider set $Z_5 = \{0,1,2,3,4\}$
- What structures are the following
  - $[Z_5, +_5]$
  - $[Z_5, *_5]$

Basic Results about Groups

1. Theorem 1: Identity element is unique in a group or a monoid
2. Theorem 2: The inverse of an element is unique in a group
3. Theorem 3: If x and y are members of a group [G,o], then $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$
4. Theorem 4: If x and y are members of a group [G,o], then
   - $x \circ z = y \circ z \Rightarrow x = y$ (Right cancellation law)
   - $z \circ x = z \circ y \Rightarrow x = y$ (Left cancellation law)
5. Theorem 5: If a and b are members of a group [G,o], then $a \circ x = b$ and $x \circ a = b$ have unique solutions for x in G.

Examples

- In $[Z_5, +_5]$, compute the following
  - $(1 +_5 3)^{-1}$
- If x, y are members of a group [Z, +]
  - $x+5 = y+5 \Rightarrow$?
  - $5+x = 5+y \Rightarrow$?
- In $[Z_5, +_5]$, solve for x
  - $x +_5 3 = 2$