# CS 207: Discrete Structures

## Abstract algebra and Number theory

Lecture 35
Oct 13 2015

# Next topic

**Abstract algebra and Number theory: An introduction**

# Definition of a group

**Definition**

A group is a set $S$ along with a operator $*$ such that the following conditions are satisfied:

- Closure: $\forall a, b \in S$, $a * b \in S$.
- Associativity: $\forall a, b, c \in S$, $a * (b * c) = (a * b) * c$.
- Identity: $\exists e \in S$ s.t., $\forall a \in S, a * e = e * a = a$.
- Inverse: $\forall a \in S, \exists a' \in S$ s.t., $a * a' = a' * a = e$.

# Examples of groups

- Every permutation group is an abstract group
  - A permutation group is a subset of permutations of a set $X$ which satisfy the group properties.
  - The set of all permutations of $\{1, \ldots, n\}$ is a special group, called the symmetric group, $S_n$.
- Every automorphism group is an abstract group.
  - The set of all automorphisms of a graph is a group.

# Examples of groups

- Every permutation group is an abstract group
  - A permutation group is a subset of permutations of a set $X$ which satisfy the group properties.
  - The set of all permutations of $\{1, \ldots, n\}$ is a special group, called the symmetric group, $S_n$.
- Every automorphism group is an abstract group.
  - The set of all automorphisms of a graph is a group.
- What about the following?
  1. $(\mathbb{Z}, +)$ is a group. Yes.
  2. $(\mathbb{Z}, \times)$.
  3. $(\mathbb{Q} \setminus \{0\}, \times)$
  4. $(\mathbb{Z}_n, +_n)$
  5. $(\mathbb{Z}_n, \times_n)$
  6. $(\mathbb{Z}_n \setminus \{0\}, \times_n)$.

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
  - Suppose not. Let $e_1 \neq e_2$ be the identity elements.
  - Then, $\forall a$, $a * e_1 = e_1 * a = a$, implies $e_2 * e_1 = e_1 * e_2 = e_2$
  - Also $\forall a$, $a * e_2 = e_2 * a = a$, implies $e_1 * e_2 = e_2 * e_1 = e_1$.
  - Implies $e_1 = e_2$, a contradiction.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

- Is it the case that $(a * b) = (b * a)$? What if you add this?

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

- Is it the case that $(a * b) = (b * a)$? What if you add this?
- Abstract groups vs permutation groups (subset of permutations satisfying the group properties)?

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

- Is it the case that $(a * b) = (b * a)$? What if you add this?
- Abstract groups vs permutation groups (subset of permutations satisfying the group properties)?
- Every permutation group is an abstract group. What about the converse?

# Simple properties of groups

## Properties of groups

- A group has a unique identity element.
- Let $G$ be a group. For all $a, b, c \in G$, $a * b = a * c$ implies $b = c$.
- Every element in a group has a unique inverse.
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$.

- Is it the case that $(a * b) = (b * a)$? What if you add this?
- Abstract groups vs permutation groups (subset of permutations satisfying the group properties)?
- Every permutation group is an abstract group. What about the converse?

## Cayley's theorem

Every abstract group is "isomorphic" to a permutation group.

# Two more examples

## Geometrical example: symmetries of a triangle

- Consider an equilateral triangle and look at transformations that move it to itself (called symmetries).

# Two more examples

## Geometrical example: symmetries of a triangle

- Consider an equilateral triangle and look at transformations that move it to itself (called symmetries).
- That is, before and after it must occupy same position in space.

# Two more examples

## Geometrical example: symmetries of a triangle

- Consider an equilateral triangle and look at transformations that move it to itself (called symmetries).
- That is, before and after it must occupy same position in space.
- How many such transformations are there?

# Two more examples

## Geometrical example: symmetries of a triangle

- Consider an equilateral triangle and look at transformations that move it to itself (called symmetries).
- That is, before and after it must occupy same position in space.
- How many such transformations are there?
- What is the composition of two such transformations?

# Two more examples

## Geometrical example: symmetries of a triangle

- Consider an equilateral triangle and look at transformations that move it to itself (called symmetries).
- That is, before and after it must occupy same position in space.
- How many such transformations are there?
- What is the composition of two such transformations?
- The symmetry transformations of an equilateral triangle form a group!

# Two more examples (contd)

## Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.

# Two more examples (contd)

## Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.
- What is an operation here?

# Two more examples (contd)

## Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.
- What is an operation here? matrix multiplication.
- Is this a group?

# Two more examples (contd)

## Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.
- What is an operation here? matrix multiplication.
- Is this a group? No!

# Two more examples (contd)

## Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.
- What is an operation here? matrix multiplication.
- Is this a group? No!
- Consider the set of invertible matrices over $\mathbb{R}$, denoted $GL_2(\mathbb{R})$.
- Does this form a group

## Two more examples (contd)

### Matrices

- Consider set of all $2 \times 2$ matrices over $\mathbb{R}$. This is denoted $M_2(\mathbb{R})$.
- What is an operation here? matrix multiplication.
- Is this a group? No!
- Consider the set of invertible matrices over $\mathbb{R}$, denoted $GL_2(\mathbb{R})$.
- Does this form a group yes!

## Some more basic notions

- The order of a finite group is the number of elements in it.

# Some more basic notions

- The order of a finite group is the number of elements in it.
- If $x$ is an element of a finite group, then the order of $x$ in $G$ is the least positive integer $m$ such that $x^m = e$.

## Some more basic notions

- The order of a finite group is the number of elements in it.
- If $x$ is an element of a finite group, then the order of $x$ in $G$ is the least positive integer $m$ such that $x^m = e$.

**Prop**

Let $x$ be an element of order $m$ in a finite group $G$. $x^s = e$ iff

# Some more basic notions

- The order of a finite group is the number of elements in it.
- If $x$ is an element of a finite group, then the order of $x$ in $G$ is the least positive integer $m$ such that $x^m = e$.

**Prop**

Let $x$ be an element of order $m$ in a finite group $G$. $x^s = e$ iff $s$ is a multiple of $m$.