CS 207: Discrete Structures

Abstract algebra and Number theory

Lecture 36

Oct 15 2015

Last topic of this course

Abstract algebra and Number theory: An introduction

Recall

Definition

A group is a set S along with an 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., $a * a' = a' * a = e$.

Recall

Definition

A group is a set S along with an 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:

- Permutations of $\{1, \ldots, n\}$,
- Automophisms of a (graph) structure,
- Over numbers: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \times)$, $(\mathbb{Z}_p \setminus 0, \times)$
- Symmetries of a triangle: Rigid motions (transformations) that move an equilateral triangle to itself.
- The set of invertible matrices over $\mathbb{R}$, denoted $GL_2(\mathbb{R})$.

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 $x^m = e$.

Proposition

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 $x^m = e$.

Proposition

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

Commutativity

- In a group G, for $a, b \in G$, $a * b \neq b * a$ in general. Can you give such an example?

Commutativity

- In a group G, for $a, b \in G$, $a * b \neq b * a$ in general. Can you give such an example?
- When $a * b = b * a$ for two elements they are said to commute.

Commutativity

- In a group G, for $a, b \in G$, $a * b \neq b * a$ in general. Can you give such an example?
- When $a * b = b * a$ for two elements they are said to commute.
- If any two elements in a group commute, then the group is called a commutative or an Abelian group.

Which of these are abelian groups?

- $(\mathbb{Z}, +)$,
- $(\mathbb{Q} \setminus 0, \times)$,
- Symmetries of a triangle: Rigid motions (transformations) that move an equilateral triangle to itself.
- The set of invertible matrices over $\mathbb{R}$, denoted $GL_2(\mathbb{R})$.

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Definition

Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Definition

Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

- Does every group have a subgroup?

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Definition

Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

- Does every group have a subgroup? Yes! $\{id\}$ and itself.

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Definition

Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

- Does every group have a subgroup? Yes! $\{id\}$ and itself.
- Other examples (of non-trivial subgroups):
  - Subgroup of rotations in group of symmetries (of a triangle).
  - Give an example of a subgroup of $GL_n(\mathbb{R})$...

Subgroups

- Consider the set of rotations of a triangle. What properties does it have?

Definition

Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

- Does every group have a subgroup? Yes! $\{id\}$ and itself.
- Other examples (of non-trivial subgroups):
  - Subgroup of rotations in group of symmetries (of a triangle).
  - Give an example of a subgroup of $GL_n(\mathbb{R})$...set of invertible matrices with determinant 1, called $SL_n(\mathbb{R})$.

A characterization of subgroups

Definition: A subset H of G is called a subgroup if H is also a group.

A characterization of subgroups

Definition: A subset H of G is called a subgroup if H is also a group.

Proposition?

A subset H of G is a subgroup if for all $x, y \in H$, $xy^{-1} \in H$.

A characterization of subgroups

Definition: A subset H of G is called a subgroup if H is also a group.

Proposition?

A subset H of G is a subgroup if for all $x, y \in H$, $xy^{-1} \in H$.

Proof: exercise! Done on board.

A characterization of subgroups

Definition: A subset H of G is called a subgroup if H is also a group.

Proposition

A subset H of G is a subgroup iff $H \neq \emptyset$ and for all $x, y \in H$, $xy^{-1} \in H$.

Proof: exercise! Done on board.