CS 207: Discrete Structures

Abstract algebra and Number theory

Lecture 35
Oct 25 2016
Last topic of this course

Abstract algebra and Number theory: An introduction
Recall

Definition

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

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

Examples:

- Permutations of $\{1, \ldots, n\}$
- Automorphisms 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 $\text{GL}_2(\mathbb{R})$. 
Recall

Definition

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

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

Examples:

- Permutations of $\{1, \ldots, n\}$,
- Automorphisms 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 $m$. 

What is the order of $(\mathbb{Z}_n, +)$; $(\mathbb{Z}_p \{0\}, \times)$? 

Definition

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

- 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 $\text{GL}_n(\mathbb{R})$... set of invertible matrices with determinant 1, called $\text{SL}_n(\mathbb{R})$. 


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 $m$.

What is the order of $(\mathbb{Z}_n, +_n)$; $(\mathbb{Z}_p \setminus \{0\}, \times_p)$?
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 $m$.

What is the order of $(\mathbb{Z}_n, +_n)$; $(\mathbb{Z}_p \setminus \{0\}, \times_p)$?

**Definition**

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

What is the order of $(\mathbb{Z}_n, +_n); (\mathbb{Z}_p \setminus \{0\}, \times_p)$?

**Definition**

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

- Does every group have a subgroup?
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 $m$.

What is the order of $(\mathbb{Z}_n, +_n); (\mathbb{Z}_p \setminus \{0\}, \times_p)$?

**Definition**

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

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

What is the order of $(\mathbb{Z}_n, +_n); (\mathbb{Z}_p \setminus \{0\}, \times_p)$?

Definition

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

- 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 $GL_n(\mathbb{R})$...
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 \( m \).

What is the order of \((\mathbb{Z}_n, +_n); (\mathbb{Z}_p \setminus \{0\}, \times_p)\)?

**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!
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!
Commutativity

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

- In a group $G$, for $a, b \in G$, $a \ast b \neq b \ast a$ in general. Can you give such an example?
- When $a \ast b = b \ast a$ 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 $\text{GL}_2(\mathbb{R})$. 

- 6
Commutativity

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

▶ When $a \ast b = b \ast a$ 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.
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 $GL_2(\mathbb{R})$. 
Another special type of group: cyclic group

**Definition**

A group $G$ is said to be **cyclic** if it contains an element $x$ and every member of $G$ is a power of $x$, i.e., obtained by repeatedly (possible zero times) applying $x$ to itself!
Another special type of group: cyclic group

Definition

A group $G$ is said to be cyclic if it contains an element $x$ and every member of $G$ is a power of $x$, i.e., obtained by repeatedly (possible zero times) applying $x$ to itself!

- $x$ is said to generate $G$ and we write $G = \langle x \rangle$.
- If $G = \langle x \rangle$ and all powers of $x$, i.e., $\ldots x^{-2}, x^{-1}, e, x^1, x^2, \ldots$ are distinct, then $G$ is called an infinite cyclic group.
Another special type of group: cyclic group

Definition

A group $G$ is said to be **cyclic** if it contains an element $x$ and every member of $G$ is a power of $x$, i.e., obtained by repeatedly (possible zero times) applying $x$ to itself!

- $x$ is said to **generate** $G$ and we write $G = \langle x \rangle$.
- If $G = \langle x \rangle$ and all powers of $x$, i.e., $\ldots x^{-2}, x^{-1}, e, x^1, x^2, \ldots$ are distinct, then $G$ is called an **infinite cyclic group**.

- Give an example of an infinite and a finite cyclic group.
Another special type of group: cyclic group

Definition
A group $G$ is said to be cyclic if it contains an element $x$ and every member of $G$ is a power of $x$, i.e., obtained by repeatedly (possible zero times) applying $x$ to itself!

▶ $x$ is said to generate $G$ and we write $G = \langle x \rangle$.
▶ If $G = \langle x \rangle$ and all powers of $x$, i.e., $\ldots x^{-2}, x^{-1}, e, x^1, x^2, \ldots$ are distinct, then $G$ is called an infinite cyclic group.

▶ Give an example of an infinite and a finite cyclic group. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +_n)$, symmetries of a polygon?
Another special type of group: cyclic group

Definition

A group $G$ is said to be cyclic if it contains an element $x$ and every member of $G$ is a power of $x$, i.e., obtained by repeatedly (possible zero times) applying $x$ to itself!

- $x$ is said to generate $G$ and we write $G = \langle x \rangle$.
- If $G = \langle x \rangle$ and all powers of $x$, i.e., $\ldots x^{-2}, x^{-1}, e, x^1, x^2, \ldots$ are distinct, then $G$ is called an infinite cyclic group.

- Give an example of an infinite and a finite cyclic group. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +_n)$, rotational symmetries of a polygon.