CS 207: Discrete Structures

Abstract algebra and Number theory

— Cylic groups, Lagrange's theorem

Lecture 38

Oct 27 2015

Recap

Cyclic group

A group G is cyclic if there exists an element $x \in G$ such that every element of G is a power of x. x is called the generator and we write $G =< x >$.

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Z}_{\ltimes}, +_n)$, rotational symmetries of a polygon.

Recap

Cyclic group

A group G is cyclic if there exists an element $x \in G$ such that every element of G is a power of x. x is called the generator and we write $G =< x >$.

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Z}_{\ltimes}, +_n)$, rotational symmetries of a polygon.

Isomorphism

$(G_1, *)$ and $(G_2, \cdot)$ are isomorphic if there exists a bijection $f : G_1 \to G_2$ such that for all $g, g' \in G_1$, $f(g * g') = f(g) \cdot f(g')$.

- Show that every infinite cyclic group (where all powers are distinct) is isomorphic to $(\mathbb{Z}, +)$.

Recap

Cyclic group

A group G is cyclic if there exists an element $x \in G$ such that every element of G is a power of x. x is called the generator and we write $G =< x >$.

Examples: $(\mathbb{Z}, +)$, $(\mathbb{Z}_{\ltimes}, +_n)$, rotational symmetries of a polygon.

Isomorphism

$(G_1, *)$ and $(G_2, \cdot)$ are isomorphic if there exists a bijection $f : G_1 \to G_2$ such that for all $g, g' \in G_1$, $f(g * g') = f(g) \cdot f(g')$.

- Show that every infinite cyclic group (where all powers are distinct) is isomorphic to $(\mathbb{Z}, +)$.
- Which of the following are isomorphic: $(\mathbb{R}, +), (\mathbb{Z}, +), (\mathbb{R}^+, \times), (\mathbb{C}, +)$?

Refresher Quiz!

Consider group G and an element $g \in G$ of order m, i.e., m is the smallest no. s.t. $g^m = e$. Let $< g >= \{e, g^1, g^2, \ldots, g^{m-1}\}$.

1. Prove that $< g >$ is a subgroup of G.
2. Consider the additive group $(\mathbb{Z}_6, +_6)$,
   2.1 What are the orders of the elements 2 and 1 in $(\mathbb{Z}_6, +_6)$?
   2.2 Describe the subgroups $< 2 >$ and $< 1 >$, and their sizes.
3. Consider the multiplicative group $(\mathbb{Z}_7 \setminus \{0\}, \times_7)$.
   3.1 What are the orders of the elements 2 and 3 in $(\mathbb{Z}_7, \times_7)$?
   3.2 Describe the subgroups $< 2 >$ and $< 3 >$, and their sizes.

Regarding cyclic subgroups of a group

Consider group G and an element $g \in G$ of order m, i.e., m is the smallest no. s.t. $g^m = e$. Let $< g >= \{e, g^1, g^2, \ldots, g^{m-1}\}$.

1. Prove that $< g >$ is a subgroup of G.
2. Consider the additive group $(\mathbb{Z}_6, +_6)$,
   - 2.1 What are the orders of the elements 2 and 1 in $(\mathbb{Z}_6, +_6)$?
   - 2.2 Describe the subgroups $< 2 >$ and $< 1 >$, and their sizes.
3. Consider the multiplicative group $(\mathbb{Z}_7 \setminus \{0\}, \times_7)$.
   - 3.1 What are the orders of the elements 2 and 3 in $(\mathbb{Z}_7, \times_7)$?
   - 3.2 Describe the subgroups $< 2 >$ and $< 3 >$, and their sizes.

- $< g >$ is called the cyclic subgroup of G generated by g.
- Clearly, order of $< g >$ is the order of the element g in G.

Recall

Definition

A group is a set S along with an operator $*$ such that:

- 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., $a * a' = a' * a = e$.

Notation: Often we write gh instead of $g * h$ and 1 instead of e.

Recall

Definition

A group is a set S along with an operator $*$ such that:

- 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., $a * a' = a' * a = e$.

Notation: Often we write gh instead of $g * h$ and 1 instead of e.

Egs: permutations, automorphisms, symmetries of geometrical figures, $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \times)$, $(\mathbb{Z}_p \setminus 0, \times_p)$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$.

Recall

Definition

A group is a set S along with an operator $*$ such that:

- 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., $a * a' = a' * a = e$.

Notation: Often we write gh instead of $g * h$ and 1 instead of e.

Egs: permutations, automorphisms, symmetries of geometrical figures, $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \times)$, $(\mathbb{Z}_p \setminus 0, \times_p)$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$.

- The order of a finite group is the number of elements in it.
- A subset H of a group G is called a subgroup if H is also a group under the same operation.

Recall

Definition

A group is a set S along with an operator $*$ such that:

- 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., $a * a' = a' * a = e$.

Notation: Often we write gh instead of $g * h$ and 1 instead of e.

Egs: permutations, automorphisms, symmetries of geometrical figures, $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \times)$, $(\mathbb{Z}_p \setminus 0, \times_p)$, $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$.

- The order of a finite group is the number of elements in it.
- A subset H of a group G is called a subgroup if H is also a group under the same operation.

Question: What is the relation between order of a group and the order of any subgroup? (other than $|H| \leq |G|$...)

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

An application

Relating the size of a group and its subgroups

Theorem (Lagrange)

If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

An application

Fermat's little theorem

For any prime p, if $gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \mod p$.