CS 207: Discrete Structures

Abstract algebra and Number theory

— subgroups, cyclic groups, group isomorphisms

Lecture 37

Oct 26 2015

Recap

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

Recap

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

Egs:

1. permutations of a set,
2. automorphisms of a graph,
3. symmetries of geometrical figures,
4. Numbers $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \times)$, etc
5. Modular counting $(\mathbb{Z}_p \setminus 0, \times)$,
6. Invertible matrices $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$.

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

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

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

- 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 types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

- 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 types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

- 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.

Some types of groups

- If any two elements in a group commute, then the group is called a commutative or an Abelian group.
- Let G be a group under operation $*$. A subset H of G is called a subgroup if H is also a group under $*$.

Proposition

$H \subseteq G$ is a subgroup of G iff $H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

- 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 $(\mathbb{Z}_n, +_n)$; $(\mathbb{Z}_p \setminus \{0\}, \times_p)$?

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 $G =< x >$.
- If $G =< x >$ 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 $G =< x >$.
- If $G =< x >$ 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 $G =< x >$.
- If $G =< x >$ 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 $G =< x >$.
- If $G =< x >$ 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

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 $G =< x >$.
- If $G =< x >$ 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
- Are any two cyclic groups of same order the "same"?

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 $G =< x >$.
- If $G =< x >$ 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
- Are any two cyclic groups of same order the "same"?
- In general, when are two groups the "same"?

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 $G =< x >$.
- If $G =< x >$ 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
- Are any two cyclic groups of same order the "same"?
- In general, when are two groups the "same"?
- What about $(\mathbb{Q} \setminus \{0\}, \times)$ and $(\mathbb{Z}, +)$?

“Sameness” in groups: group isomorphisms

Definition

- If G_1 and G_2 are groups, then a bijection $f : G_1 \to G_2$ is called an isomorphism if for all $g, g' \in G$, $f(gg') = f(g)f(g')$.
- G_1 and G_2 are said to be isomorphic, denoted $G_1 \equiv G_2$, if there exists an isomorphism f between them.

"Sameness" in groups: group isomorphisms

Definition

- If G_1 and G_2 are groups, then a bijection $f : G_1 \to G_2$ is called an isomorphism if for all $g, g' \in G$, $f(gg') = f(g)f(g')$.
- G_1 and G_2 are said to be isomorphic, denoted $G_1 \equiv G_2$, if there exists an isomorphism f between them.

Questions:

- Do $g, f(g)$ have the same order?

"Sameness" in groups: group isomorphisms

Definition

- If G_1 and G_2 are groups, then a bijection $f : G_1 \to G_2$ is called an isomorphism if for all $g, g' \in G$, $f(gg') = f(g)f(g')$.
- G_1 and G_2 are said to be isomorphic, denoted $G_1 \equiv G_2$, if there exists an isomorphism f between them.

Questions:

- Do $g, f(g)$ have the same order?
- Is the isomorphism relation, $\equiv$, an equivalence relation?

"Sameness" in groups: group isomorphisms

Definition

- If G_1 and G_2 are groups, then a bijection $f : G_1 \to G_2$ is called an isomorphism if for all $g, g' \in G$, $f(gg') = f(g)f(g')$.
- G_1 and G_2 are said to be isomorphic, denoted $G_1 \equiv G_2$, if there exists an isomorphism f between them.

Questions:

- Do $g, f(g)$ have the same order?
- Is the isomorphism relation, $\equiv$, an equivalence relation?
- Show that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

"Sameness" in groups: group isomorphisms

Definition

- If G_1 and G_2 are groups, then a bijection $f : G_1 \to G_2$ is called an isomorphism if for all $g, g' \in G$, $f(gg') = f(g)f(g')$.
- G_1 and G_2 are said to be isomorphic, denoted $G_1 \equiv G_2$, if there exists an isomorphism f between them.

Questions:

- Do $g, f(g)$ have the same order?
- Is the isomorphism relation, $\equiv$, an equivalence relation?
- Show that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.
- Which of the following are isomorphic: $(\mathbb{R}, +), (\mathbb{Z}, +), (\mathbb{R}^+, \times), (\mathbb{C}, +)$?