Structured Sets

CS1200, CSE IIT Madras

Meghana Nasre

April 24, 2020

Structured Sets

- Relational Structures
  - Properties and closures ✓
  - Equivalence Relations ✓
  - Partially Ordered Sets (Posets) and Lattices ✓
- Algebraic Structures
  - Groups and Rings

Algebraic Structures: Recap

Set A with a binary operator $*$

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.
- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.
- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.

Example: For any positive integer n, let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let $\oplus_n$ be the binary operator as follows.

$$\begin{aligned} a \oplus_n b &= a + b && \text{if } a + b < n \\ &= a + b - n && \text{otherwise} \end{aligned}$$

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.
- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.

Example: For any positive integer n, let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let $\oplus_n$ be the binary operator as follows.

$$\begin{aligned} a \oplus_n b &= a + b && \text{if } a + b < n \\ &= a + b - n && \text{otherwise} \end{aligned}$$

Verify that $(Z_n, \oplus_n)$ is a group for any n. This is called the group of integers modulo n.

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.
- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.

Example: For any positive integer n, let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let $\oplus_n$ be the binary operator as follows.

$$\begin{aligned} a \oplus_n b &= a + b && \text{if } a + b < n \\ &= a + b - n && \text{otherwise} \end{aligned}$$

Verify that $(Z_n, \oplus_n)$ is a group for any n. This is called the group of integers modulo n.

If $(A, *)$ is a group and $*$ is commutative, then $(A, *)$ is called a commutative or Abelian group.

Algebraic Structures: Recap

Set A with a binary operator $*$

- If $*$ is closed and associative, then $(A, *)$ is a semi-group.
- If $*$ is closed and associative, and an identity element e exists, then $(A, *)$ is a monoid.
- If $*$ is closed and associative, and an identity element e exists, and every element $b \in A$ has an inverse then $(A, *)$ is a group.

Example: For any positive integer n, let $Z_n = \{0, 1, 2, \ldots, n-1\}$. Let $\oplus_n$ be the binary operator as follows.

$$\begin{aligned} a \oplus_n b &= a + b && \text{if } a + b < n \\ &= a + b - n && \text{otherwise} \end{aligned}$$

Verify that $(Z_n, \oplus_n)$ is a group for any n. This is called the group of integers modulo n.

If $(A, *)$ is a group and $*$ is commutative, then $(A, *)$ is called a commutative or Abelian group. $(Z_n, \oplus_n)$ is a commutative group.

Subgroups

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

Subgroups

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ $(Z, +)$ is a group.

Subgroups

$$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad (Z, +) \text{ is a group.}$$

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group?

Subgroups

$$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad (Z, +) \text{ is a group.}$$

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group?
  verify that $(E, +)$ satisfies the four conditions of a group.

Subgroups

$$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad (Z, +) \text{ is a group.}$$

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group?
  verify that $(E, +)$ satisfies the four conditions of a group.
- What about $(O, +)$, where $O = \{\ldots, -3, -1, 1, 3, \ldots\}$? identity element is not present, hence not a group.

Subgroups

$$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \quad (Z, +) \text{ is a group.}$$

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group?
  verify that $(E, +)$ satisfies the four conditions of a group.
- What about $(O, +)$, where $O = \{\ldots, -3, -1, 1, 3, \ldots\}$? identity element is not present, hence not a group.

Let $(A, *)$ be a group and B be a subset of A.

Subgroups

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ $(Z, +)$ is a group.

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group? verify that $(E, +)$ satisfies the four conditions of a group.
- What about $(O, +)$, where $O = \{\ldots, -3, -1, 1, 3, \ldots\}$? identity element is not present, hence not a group.

Let $(A, *)$ be a group and B be a subset of A. Then, $(B, *)$ is called a subgroup of A if $(B, *)$ is a group by itself.

Subgroups

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ $(Z, +)$ is a group.

- Consider $E = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$. Is $(E, +)$ a group?
  verify that $(E, +)$ satisfies the four conditions of a group.
- What about $(O, +)$, where $O = \{\ldots, -3, -1, 1, 3, \ldots\}$? identity element is not present, hence not a group.

Let $(A, *)$ be a group and B be a subset of A. Then, $(B, *)$ is called a subgroup of A if $(B, *)$ is a group by itself.

To verify that $(B, *)$ is a subgroup, ensure that all four properties of a group are satisfied and $B \subseteq A$.

Subgroups

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Subgroups

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ $(Z_6, \oplus_6)$ is a group.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \qquad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \qquad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \qquad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2.

Subgroups

$$Z_6 = \{0,1,2,3,4,5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse.

$$Z_6 = \{0,1,2,3,4,5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group?

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group? No!

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group? No! Since $1 \oplus_6 1 = 2$ and $2 \notin B_3$. Similarly, $5 \oplus_6 5 = 4 \notin B_3$.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group? No! Since $1 \oplus_6 1 = 2$ and $2 \notin B_3$. Similarly, $5 \oplus_6 5 = 4 \notin B_3$. (recall that $5 \oplus_6 5 = 5 + 5 - 6 = 4$)

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group? No! Since $1 \oplus_6 1 = 2$ and $2 \notin B_3$. Similarly, $5 \oplus_6 5 = 4 \notin B_3$. (recall that $5 \oplus_6 5 = 5 + 5 - 6 = 4$)

Verify that $(\{0\}, \oplus_6)$, $(\{0, 3\}, \oplus_6)$, $(\{0, 2, 4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$.

Subgroups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

We would like to list subgroups of Z_6 (if any).

Observations: Let $B \subseteq Z_6$ such that $(B, \oplus_6)$ is a subgroup.

1. The element 0 must belong to B else identity will be missing.
2. $\oplus_6$ must be closed on B, hence if $2 \in B$ and $3 \in B$, it implies that $5 \in B$.

- Let $B_1 = \{0\}$. Verify that $(B_1, \oplus_6)$ is indeed a subgroup.
- Let $B_2 = \{0, 1\}$. $\oplus_6$ is closed for B_2. However, inverse for 1 which is 5 does not exist. Hence $(B_2, \oplus_6)$ is not a group.
- Let $B_3 = \{0, 1, 5\}$. Now we have fixed the issue of inverse. So is $(B_3, \oplus_6)$ a group? No! Since $1 \oplus_6 1 = 2$ and $2 \notin B_3$. Similarly, $5 \oplus_6 5 = 4 \notin B_3$. (recall that $5 \oplus_6 5 = 5 + 5 - 6 = 4$)

Verify that $(\{0\}, \oplus_6)$, $(\{0, 3\}, \oplus_6)$, $(\{0, 2, 4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$.

Ex: List non-trivial subgroups of $(Z_5, \oplus_5)$ (trivial ones are $(\{0\}, \oplus_5)$ and $(Z_5, \oplus_5)$).

Subgroup and properties

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Subgroup and properties

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ $(Z_6, \oplus_6)$ is a group.

Consider the following:

- $1 \oplus_6 1 = 2$;

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$;

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$;

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$?

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$? It can "generate" every element in Z_6.

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$? It can "generate" every element in Z_6. Such an element is called a generator.

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$? It can "generate" every element in Z_6. Such an element is called a generator.

Ex: Are there other generators of Z_6? How about 3?

Subgroup and properties

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$? It can "generate" every element in Z_6. Such an element is called a generator.

Ex: Are there other generators of Z_6? How about 3?
Ans: 5 is another generator, verify this.

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Consider the following:

- $1 \oplus_6 1 = 2$; we write this as $1^2 = 2$ (in this context).
- $1 \oplus_6 1 \oplus_6 1 = 3$; we write this as $1^3 = 3$.
- $1 \oplus_6 1 \oplus_6 1 \oplus_6 1 = 4$; we write this as $1^4 = 4$; $1^5 = 5$ and $1^6 = 0$.

What is special about 1 in the context of $(Z_6, \oplus_6)$? It can "generate" every element in Z_6. Such an element is called a generator.

Ex: Are there other generators of Z_6? How about 3?
Ans: 5 is another generator, verify this. The element 3 is not a generator; list some elements that cannot be generated using 3 alone.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad i$ times.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad i$ times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

A group $(A, *)$ is cyclic if there exists some $b \in A$ such that $\langle b \rangle = A$.

Examples: $(Z_6, \oplus_6)$ is a cyclic group, with generator $\langle 1 \rangle$.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

A group $(A, *)$ is cyclic if there exists some $b \in A$ such that $\langle b \rangle = A$.

Examples: $(Z_6, \oplus_6)$ is a cyclic group, with generator $\langle 1 \rangle$. Similarly $(Z, +)$ is a cyclic group with generator $\langle 1 \rangle$.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ $\quad$ i times.

Let $b^0 = e$ $\quad$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

A group $(A, *)$ is cyclic if there exists some $b \in A$ such that $\langle b \rangle = A$.

Examples: $(Z_6, \oplus_6)$ is a cyclic group, with generator $\langle 1 \rangle$. Similarly $(Z, +)$ is a cyclic group with generator $\langle 1 \rangle$.
Are all groups cyclic?

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ i times.

Let $b^0 = e$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

A group $(A, *)$ is cyclic if there exists some $b \in A$ such that $\langle b \rangle = A$.

Examples: $(Z_6, \oplus_6)$ is a cyclic group, with generator $\langle 1 \rangle$. Similarly $(Z, +)$ is a cyclic group with generator $\langle 1 \rangle$.
Are all groups cyclic? Not necessarily.

Generators and cyclic groups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

We write $b * b = b^2$. In general $b^i = b * b * \ldots * b$ i times.

Let $b^0 = e$ identity element of the group.

Let b^{-1} denote the inverse of b in $(A, *)$. Analogously define $b^{-2} = b^{-1} * b^{-1}$.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Note that all the powers of b need not be distinct.

A group $(A, *)$ is cyclic if there exists some $b \in A$ such that $\langle b \rangle = A$.

Examples: $(Z_6, \oplus_6)$ is a cyclic group, with generator $\langle 1 \rangle$. Similarly $(Z, +)$ is a cyclic group with generator $\langle 1 \rangle$.
Are all groups cyclic? Not necessarily. Construct example.

Powers and subgroups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

Powers and subgroups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

- Associativity: Follows since $*$ is associative.

Powers and subgroups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

- Associativity: Follows since $*$ is associative.
- Closure: By construction of $\langle b \rangle$.

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

- Associativity: Follows since $*$ is associative.
- Closure: By construction of $\langle b \rangle$.
- Identity: We know that $b^0 = e \in \langle b \rangle$.

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

- Associativity: Follows since $*$ is associative.
- Closure: By construction of $\langle b \rangle$.
- Identity: We know that $b^0 = e \in \langle b \rangle$.
- Inverse: Let $x = b^i$

Powers and subgroups

Let $(A, *)$ be any group. Let $b \in A$ be some element.

$$\langle b \rangle = \{\ldots, b^{-3}, b^{-2}, b^{-1}, e, b, b^2, b^3, \ldots\} = \{b^n \mid n \in Z\}$$

Claim: The system $(\langle b \rangle, *)$ forms a group and hence a subgroup of $(A, *)$.

Proof: Need to show that $(\langle b \rangle, *)$ satisfies all properties of a group.

- Associativity: Follows since $*$ is associative.
- Closure: By construction of $\langle b \rangle$.
- Identity: We know that $b^0 = e \in \langle b \rangle$.
- Inverse: Let $x = b^i$ then b^{-i} is the inverse of x since $b^i * b^{-i} = b^0 = e$. Hence every element has an inverse in $\langle b \rangle$.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present:

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Inverse for any element c exists:

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Inverse for any element c exists: If $j - i > 1$, then $c^{j-i} = c * c^{j-i-1}$,

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Inverse for any element c exists: If $j - i > 1$, then $c^{j-i} = c * c^{j-i-1}$, then since $c^{j-i} = e$, we conclude that c^{j-i-1} is the inverse of c.

Groups and Finite subsets

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Inverse for any element c exists: If $j - i > 1$, then $c^{j-i} = c * c^{j-i-1}$, then since $c^{j-i} = e$, we conclude that c^{j-i-1} is the inverse of c. If $j - i = 1$, then $c^i = c^i * c$. Thus, c must be the identity and its own inverse.

Let $(A, *)$ be any group. Let $B \subseteq A$.

Claim: If B is finite and $*$ is closed on B, then $(B, *)$ is a subgroup of $(A, *)$.

$(Z_6, \oplus_6)$ is a group. Consider $B = \{0, 3\}$. Observe that $\oplus_6$ is closed under B. Verify that $(B, \oplus_6)$ is a group.

Proof: By assumption $*$ is closed on B. We need to only show that every element has its inverse in B and identity element belongs to B.

Identity is present: Because $*$ is closed on B, for any $c \in B$, we have $c, c^2, c^3, \ldots,$ belong to B. Since B is finite, it must be the case that $c^i = c^j$ for some $i < j$. Thus, $c^i = c^i * c^{j-i}$. Thus c^{j-i} is the identity element and is included in B.

Inverse for any element c exists: If $j - i > 1$, then $c^{j-i} = c * c^{j-i-1}$, then since $c^{j-i} = e$, we conclude that c^{j-i-1} is the inverse of c. If $j - i = 1$, then $c^i = c^i * c$. Thus, c must be the identity and its own inverse.

Ex: Make sure you work out the proof on the example above by taking $c = 3$ and $c = 0$ and observe how you fall in the two cases.

Order of group for finite groups

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Order of group for finite groups

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ $(Z_6, \oplus_6)$ is a group.

Order of group for finite groups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

Order of group for finite groups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

- Order of $(Z_6, \oplus_6)$ is 6.

Order of group for finite groups

$$Z_6 = \{0,1,2,3,4,5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

- Order of $(Z_6, \oplus_6)$ is 6.
- Recall that $(\{0\}, \oplus_6)$, $(\{0,3\}, \oplus_6)$, $(\{0,2,4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$

Order of group for finite groups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

- Order of $(Z_6, \oplus_6)$ is 6.
- Recall that $(\{0\}, \oplus_6)$, $(\{0, 3\}, \oplus_6)$, $(\{0, 2, 4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$ respectively of order 1, 2 and 3.

Order of group for finite groups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

- Order of $(Z_6, \oplus_6)$ is 6.
- Recall that $(\{0\}, \oplus_6)$, $(\{0, 3\}, \oplus_6)$, $(\{0, 2, 4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$ respectively of order 1, 2 and 3.

Qn: Is there any relation between the order of a finite group and the order of its subgroups?

Order of group for finite groups

$$Z_6 = \{0, 1, 2, 3, 4, 5\} \quad (Z_6, \oplus_6) \text{ is a group.}$$

Order of a group: For a finite group $(A, *)$ we say that $|A|$ is the order of the group.

- Order of $(Z_6, \oplus_6)$ is 6.
- Recall that $(\{0\}, \oplus_6)$, $(\{0, 3\}, \oplus_6)$, $(\{0, 2, 4\}, \oplus_6)$ and $(Z_6, \oplus_6)$ are the only subgroups of $(Z_6, \oplus_6)$ respectively of order 1, 2 and 3.

Qn: Is there any relation between the order of a finite group and the order of its subgroups?

Lagrange's Theorem: The order of any subgroup of a finite group divides the order of the group.

Corollary: For any prime p, the group $(Z_p, \oplus_p)$ does not have any non-trivial sub-group.

Summary

- Subgroups: definition, examples.
- Generator of a group and cyclic groups.
- Finite subsets and subgroups.
- Order of a group.

Summary

- Subgroups: definition, examples.
- Generator of a group and cyclic groups.
- Finite subsets and subgroups.
- Order of a group.
- References: Section 11.3, 11.4 of Elements of Discrete Maths, C.L. Liu.