# CS 207

# Discrete Structures

Nutan Limaye

21 OCT 2013

# Module 4

## Abstract Algebra.

Last few classes:

Module 3 (Graph Theory)

- bipartite graphs
- hall's condition
- stable matchings
- computing maximum matchings
- tournament graphs
- dominating sets. . . .

Today:

Group theory

- definition of groups
- examples of groups
- applications of group theory.
- properties of groups.

A set $S$ along with an operator $*$, $(S,*)$, is called a group if the operator satisfies the following properties wrt to the elements of $S$:

Closure : $\forall a,b \in S \quad a*b \in S$

Associativity : $\forall a,b,c \in S \quad a*(b*c) = (a*b)*c$

Identity : $\exists e \in S$ s.t. $\forall a \in S \quad a*e = e*a = a$

Inverse : $\forall a \in S \ \exists a' \in S$ s.t. $a*a' = e$

Examples

| | Group | Not a Group |
|---|---|---|
| 1. $(\mathbb{Z}_p, \times_p)$ | | |
| 2. $(\mathbb{Z}_p, +_p)$ | | |
| 3. $(\mathbb{Z}_p^*, \times_p)$ | | |

$p$ : a prime

$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$

$\times_p :=$ multiplicatn mod $p$

$+_p :=$ addition mod $p$

$\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$

Examples

| | Group | Not a Group |
|---|---|---|
| 1. $(\mathbb{Z}_p, \times_p)$ | | ✓ |
| 2. $(\mathbb{Z}_p, +_p)$ | ✓ | |
| 3. $(\mathbb{Z}_p^*, \times_p)$ | ✓ | |

$p$: a prime

$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$

$\times_p :=$ multiplicatn mod $p$

$+_p :=$ addition mod $p$

$\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\}$

Application of Group Theory (Cryptography).

Application of Group Theory (Cryptography).

Akbar

# Application of Group Theory (Cryptography).

Akbar

Birbal.

Application of Group Theory (Cryptography).

Akbar

(from Mumbai)

$\longrightarrow$

$\longleftarrow$

Birbal.

(from Chennai)

⋮

Trying to communicate over an insecure channel.

- Share a secrete key
- communicate using the shared secrete.

- But how can they share a secrete securely?

Akbar Birbal.

Akbar

Birbal.

Choose $p$ a prime,

$g$ an element from $\mathbb{Z}_p$

let $\alpha$ be a private key

let $A \leftarrow g^{\alpha} \bmod p$

Akbar Birbal.

Choose $p$ a prime,
$g$ an element from $\mathbb{Z}_p$

let $\alpha$ be a private key
let $A \leftarrow g^{\alpha} \bmod p$

$\xrightarrow{g,\ p,\ A}$

Akbar | Birbal.
---|---
Choose $p$ a prime, | 
$g$ an element from $\mathbb{Z}_p$ | 
let $\alpha$ be a private key | 
let $A \leftarrow g^{\alpha} \bmod p$ | 

$$\xrightarrow{g,\, p,\, A}$$

| | |
|---|---|
| | let $\beta$ be private key |
| | let $B \leftarrow g^{\beta} \bmod p$ |

Akbar | Birbal.

Choose $p$ a prime,
$g$ an element from $\mathbb{Z}_p$

let $\alpha$ be a private key
let $A \leftarrow g^{\alpha} \bmod p$

$$\xrightarrow{\quad g,\ p,\ A \quad}$$

let $\beta$ be private key
let $B \leftarrow g^{\beta} \bmod p$

$$\xleftarrow{\quad B \quad}$$

Akbar | Birbal

Choose $p$ a prime,
$g$ an element from $\mathbb{Z}_p$

let $\alpha$ be a private key
let $A \leftarrow g^{\alpha} \bmod p$

$\xrightarrow{g,\ p,\ A}$

let $\beta$ be private key
let $B \leftarrow g^{\beta} \bmod p$

$\xleftarrow{B}$

compute $B^{a} \bmod p$

Akbar

Birbal.

Choose $p$ a prime,

$g$ an element from $\mathbb{Z}_p$

let $\alpha$ be a private key

let $A \leftarrow g^{\alpha} \bmod p$

$$\xrightarrow{\quad g,\ p,\ A \quad}$$

let $\beta$ be private key

let $B \leftarrow g^{\beta} \bmod p$

$$\xleftarrow{\quad B \quad}$$

compute $B^{a} \bmod p$

Compute $A^{\beta} \bmod p$

Akbar | Birbal.
---|---
Choose $p$ a prime, | 
$g$ an element from $\mathbb{Z}_p$ | 
let $\alpha$ be a private key | 
let $A \leftarrow g^{\alpha} \bmod p$ | 

$$\xrightarrow{g,\ p,\ A}$$

let $\beta$ be private key

let $B \leftarrow g^{\beta} \bmod p$

$$\xleftarrow{B}$$

compute $B^{a} \bmod p$

Compute $A^{\beta} \bmod p$

!! Shared Secrete $g^{\alpha\beta} \bmod p$ !!

Simple properties of groups

- A group has a unique identity.

## Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.

## Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.

Suppose $\exists e_1 \neq e_2$ s.t. $\forall a \in S$
$$a * e_1 = e_1 * a = a$$
$$a * e_2 = e_2 * a = a$$

## Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.

Suppose $\exists e_1 \neq e_2$ s.t. $\forall a \in S$ $\quad a * e_1 = e_1 * a = a$

$a * e_2 = e_2 * a = a$

$e_2 * e_1 = e_1 * e_2 = e_2$

# Simple properties of groups

$\boxed{(S,*) \text{ is a group}}$

- A group has a unique identity.

Suppose $\exists e_1 \neq e_2$ s.t. $\forall a \in S$ $\quad a*e_1 = e_1*a = a$

$a*e_2 = e_2*a = a$

$e_2*e_1 = e_1*e_2 = e_2$

$e_1*e_2 = e_2*e_1 = e_1$

# Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.

Suppose $\exists e_1 \neq e_2$ s.t. $\forall a \in S$ $\quad a*e_1 = e_1*a = a$

$a*e_2 = e_2*a = a$

$$e_2*e_1 = e_1*e_2 = e_2$$

$$e_1*e_2 = e_2*e_1 = e_1$$

$$\therefore \quad e_1 = e_2 \quad \Rightarrow\Leftarrow$$

# Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.
- Every element has a unique inverse

# Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.
- Every element has a unique inverse

Suppose $\exists a$: $a_1^{-1}, a_2^{-1}$ are its two distinct inverses

Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse

Suppose $\exists a$: $a_1^{-1}, a_2^{-1}$ are its two distinct inverses

$$a * a_1^{-1} = e \Rightarrow a * a_1^{-1} * a_1 = e * a_1 \Rightarrow a = a_1$$

# Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.
- Every element has a unique inverse

Suppose $\exists a$: $a_1^{-1}, a_2^{-1}$ are its two distinct inverses

$$a * a_1^{-1} = e \Rightarrow a * a_1^{-1} * a_1 = e * a_1 \Rightarrow a = a_1$$

$$a * a_2^{-1} = e \Rightarrow a * a_2^{-1} * a_2 = e * a_2 \Rightarrow a = a_2$$

# Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse

Suppose $\exists a$: $a_1^{-1}, a_2^{-1}$ are its two distinct inverses

$$a * a_1^{-1} = e \Rightarrow a * a_1^{-1} * a_1 = e * a_1 \Rightarrow a = a_1$$

$$a * a_2^{-1} = e \Rightarrow a * a_2^{-1} * a_2 = e * a_2 \Rightarrow a = a_2$$

$\therefore a_1 = a_2$

## Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

# Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b) * (a*b)^{-1} = e$$

$(S, *)$ is a group

# Simple properties of groups

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b) * (a*b)^{-1} = e$$

$$\Rightarrow \quad a^{-1} * (a*b) * (a*b)^{-1} = a^{-1} * e$$

# Simple properties of groups

$\boxed{(S, *) \text{ is a group}}$

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b) * (a*b)^{-1} = e$$

$$\Rightarrow \quad a^{-1} * (a*b) * (a*b)^{-1} = a^{-1} * e$$

$$\Rightarrow \quad (a^{-1} * a) * b * (a*b)^{-1} = a^{-1} \qquad \text{(Associativity, identity)}$$

## Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b) * (a*b)^{-1} = e$$

$$\Rightarrow \quad a^{-1} * (a*b) * (a*b)^{-1} = a^{-1} * e$$

$$\Rightarrow \quad (a^{-1} * a) * b * (a*b)^{-1} = a^{-1} \qquad \text{(Associativity, identity)}$$

$$\Rightarrow \quad e * b * (a*b)^{-1} = a^{-1} \qquad \text{(Inverse)}$$

Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b)*(a*b)^{-1} = e$$

$$\Rightarrow \quad a^{-1}*(a*b)*(a*b)^{-1} = a^{-1}*e$$

$$\Rightarrow \quad (a^{-1}*a)*b*(a*b)^{-1} = a^{-1} \qquad \text{(Associativity, identity)}$$

$$\Rightarrow \quad e*b*(a*b)^{-1} = a^{-1} \qquad \text{(Inverse)}$$

$$\Rightarrow \quad b^{-1}*b*(a*b)^{-1} = b^{-1}*a^{-1} \quad \text{(Identity)}$$

## Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a*b)^{-1} = b^{-1} * a^{-1}$

$$(a*b)*(a*b)^{-1} = e$$

$$\Rightarrow \quad a^{-1}*(a*b)*(a*b)^{-1} = a^{-1}*e$$

$$\Rightarrow \quad (a^{-1}*a)*b*(a*b)^{-1} = a^{-1} \qquad \text{(Associativity, identity)}$$

$$\Rightarrow \quad e*b*(a*b)^{-1} = a^{-1} \qquad \text{(Inverse)}$$

$$\Rightarrow \quad b^{-1}*b*(a*b)^{-1} = b^{-1}*a^{-1} \qquad \text{(Identity)}$$

$$\Rightarrow \quad (a*b)^{-1} = b^{-1}*a^{-1} \qquad \text{(Inverse, identity).}$$

## Simple properties of groups

$(S, *)$ is a group

- A group has a unique identity.
- Every element has a unique inverse
- For any two elements $(a * b)^{-1} = b^{-1} * a^{-1}$

CS 207

Discrete Structures

Nutan Limaye

24 OCT 2013

# Module 4

## Abstract Algebra.

## Last Time

- Definition of groups
- Examples of groups
- Application of group theory.
- Simple properties of groups

Today:

- More examples of groups
- Abelian and non-abelian groups
- Subgroups & simple properties of subgroups
- Another application of groups.

A set $S$ along with an operator $*$, $(S,*)$, is called a group if the operator satisfies the following properties wrt to the elements of $S$:

Closure : $\forall a,b \in S \quad a*b \in S$

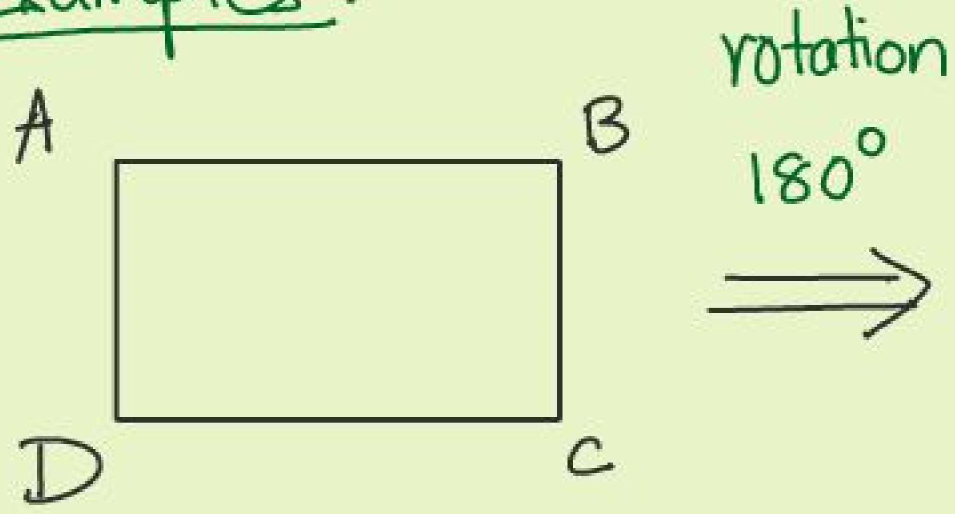
Associativity : $\forall a,b,c \in S \quad a*(b*c) = (a*b)*c$

Identity : $\exists e \in S$ s.t. $\forall a \in S \quad a*e = e*a = a$

Inverse : $\forall a \in S \ \exists a' \in S$ s.t. $a*a' = e$

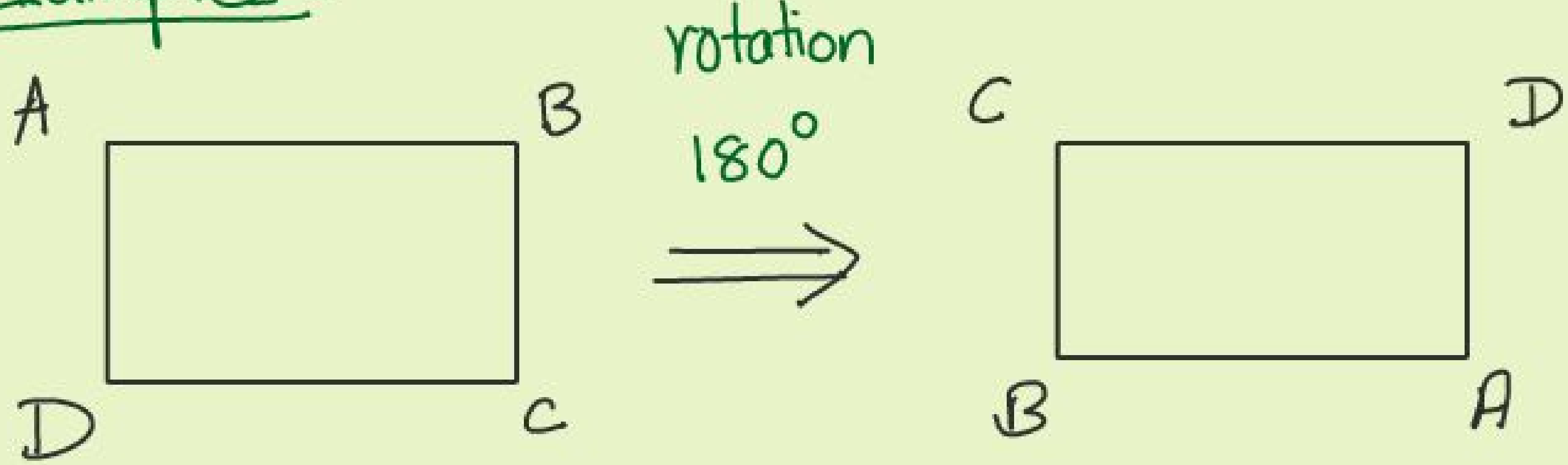
A rigid motion of an object which maps the object to itself is called a <u>symmetry</u>

<u>Examples</u>:



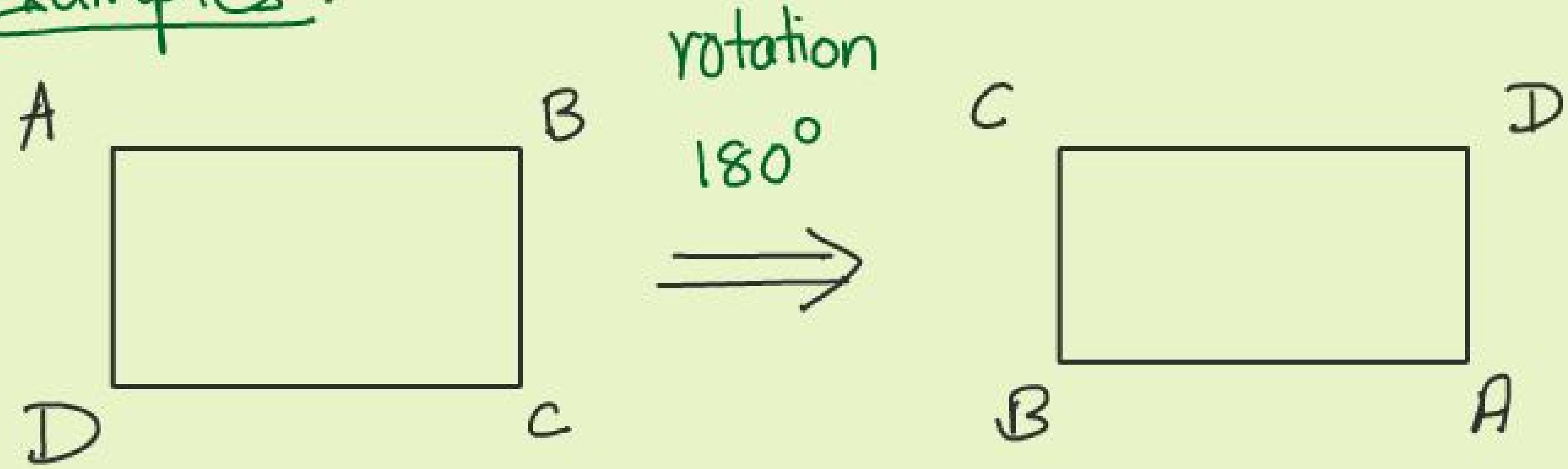
A rigid motion of an object which maps the object to it self is called a <u>symmetry</u>

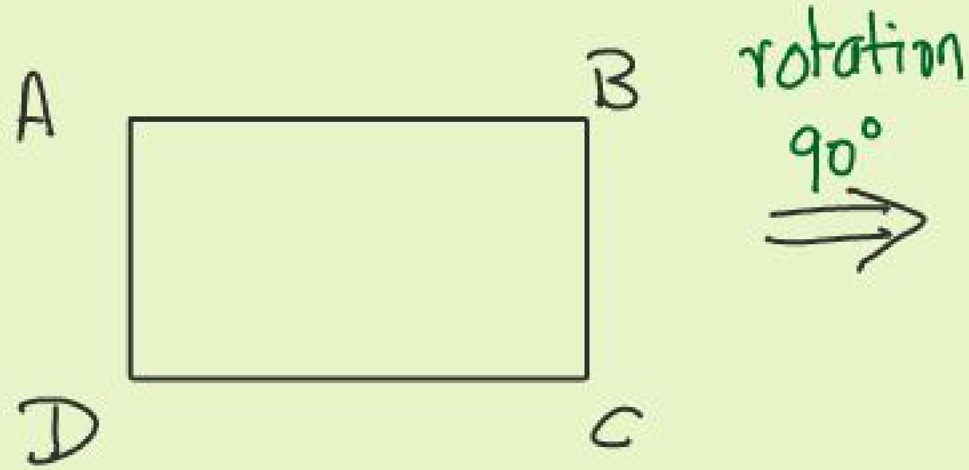
Examples:



A rigid motion of an object which maps the object to itself is called a <u>symmetry</u>

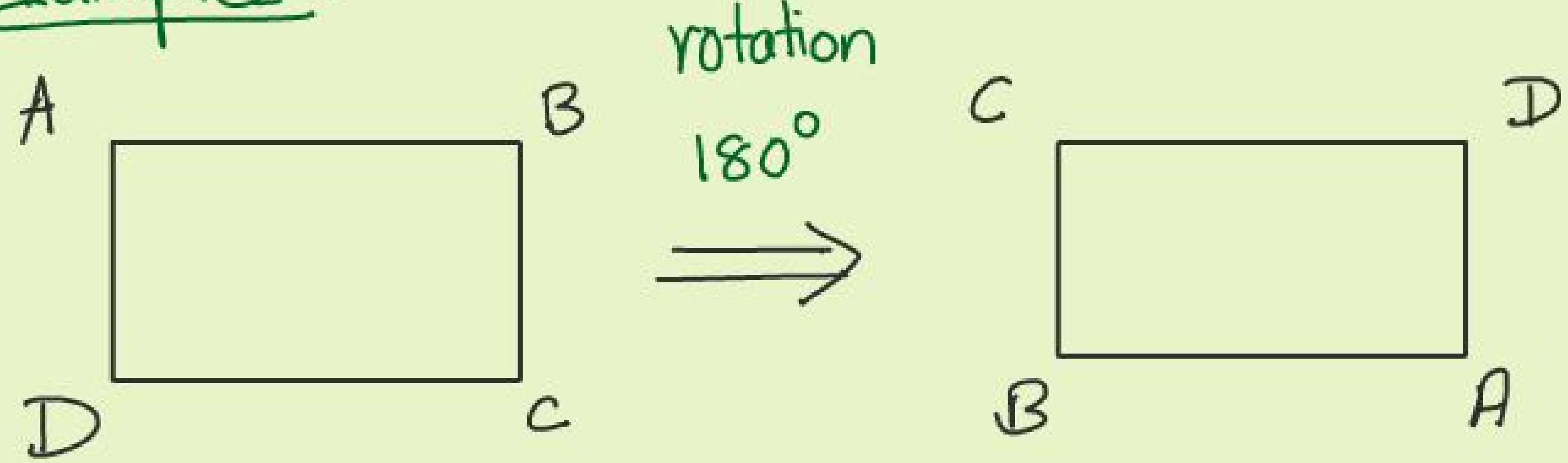
<u>Examples</u>:

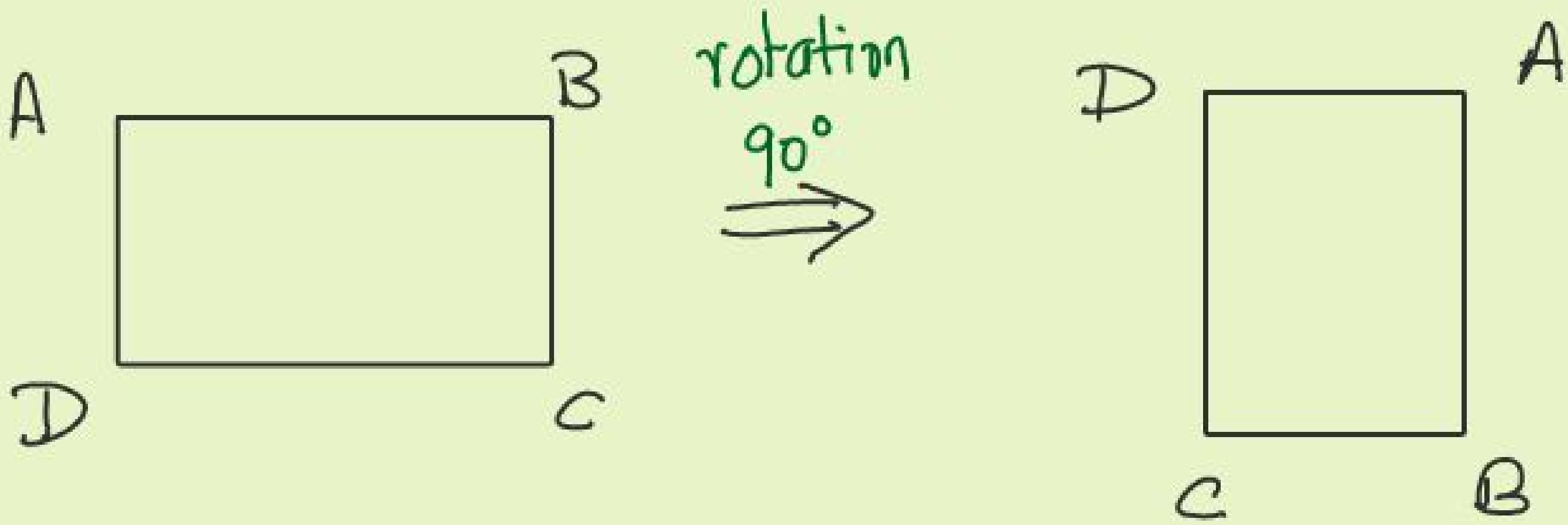


A rigid motion of an object which maps the object to it self is called a symmetry

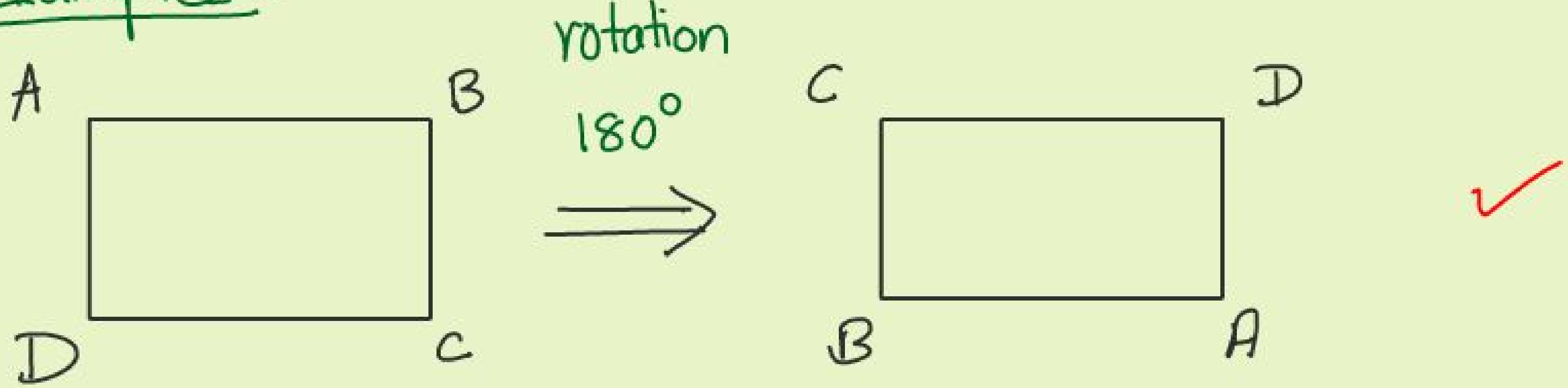
Examples:

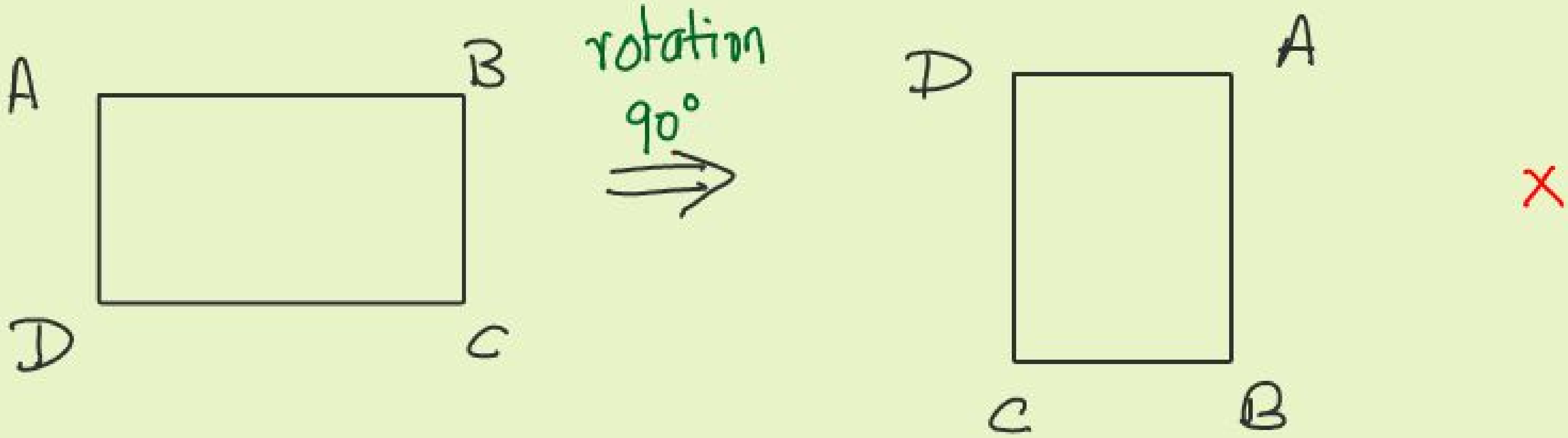


A rigid motion of an object which maps the object to itself is called a symmetry

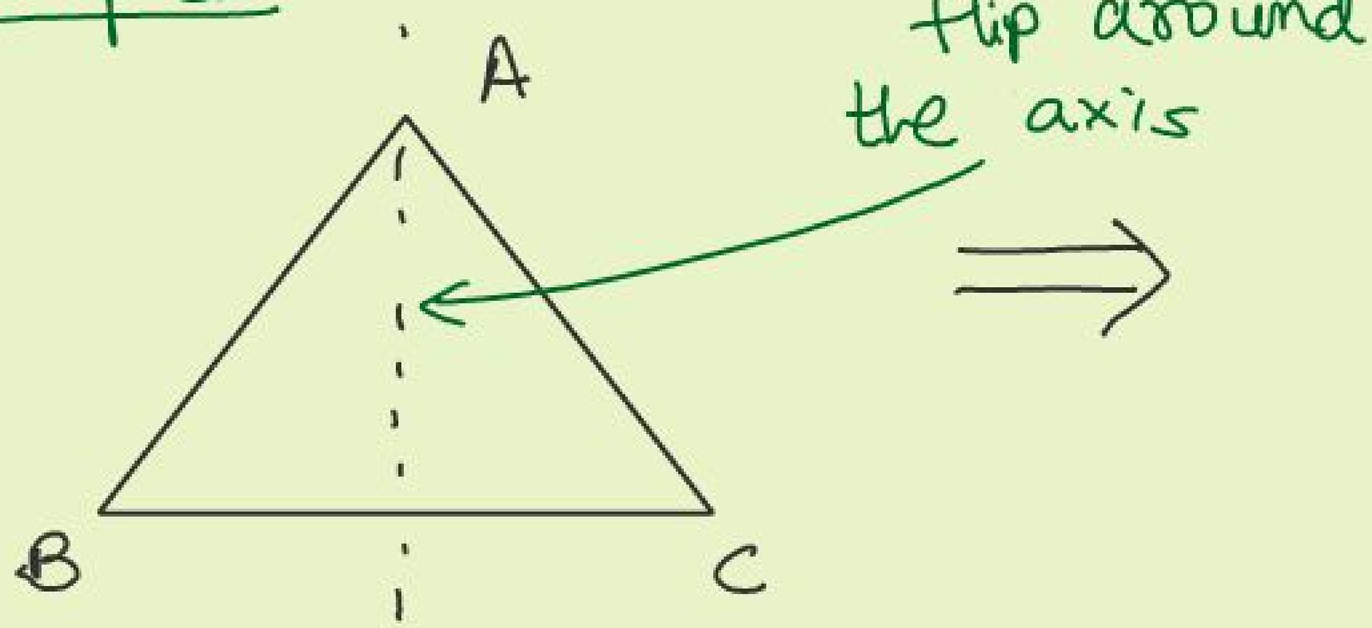
Examples:



A rigid motion of an object which maps the object to it self is called a **symmetry**

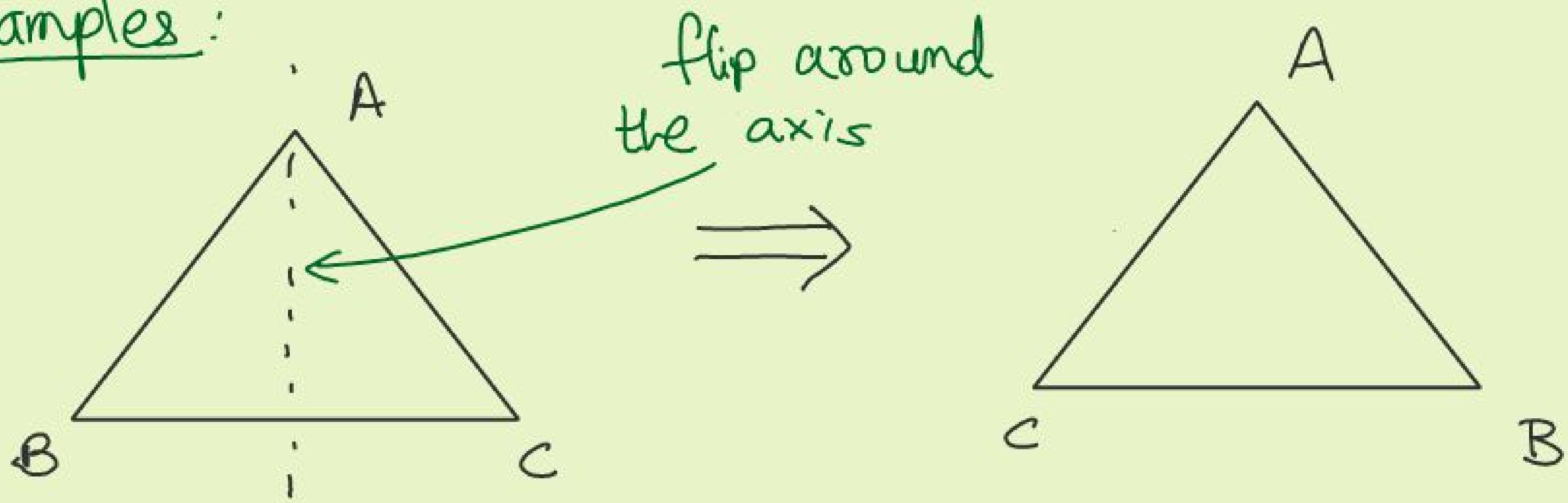
Examples:




$\Longrightarrow$

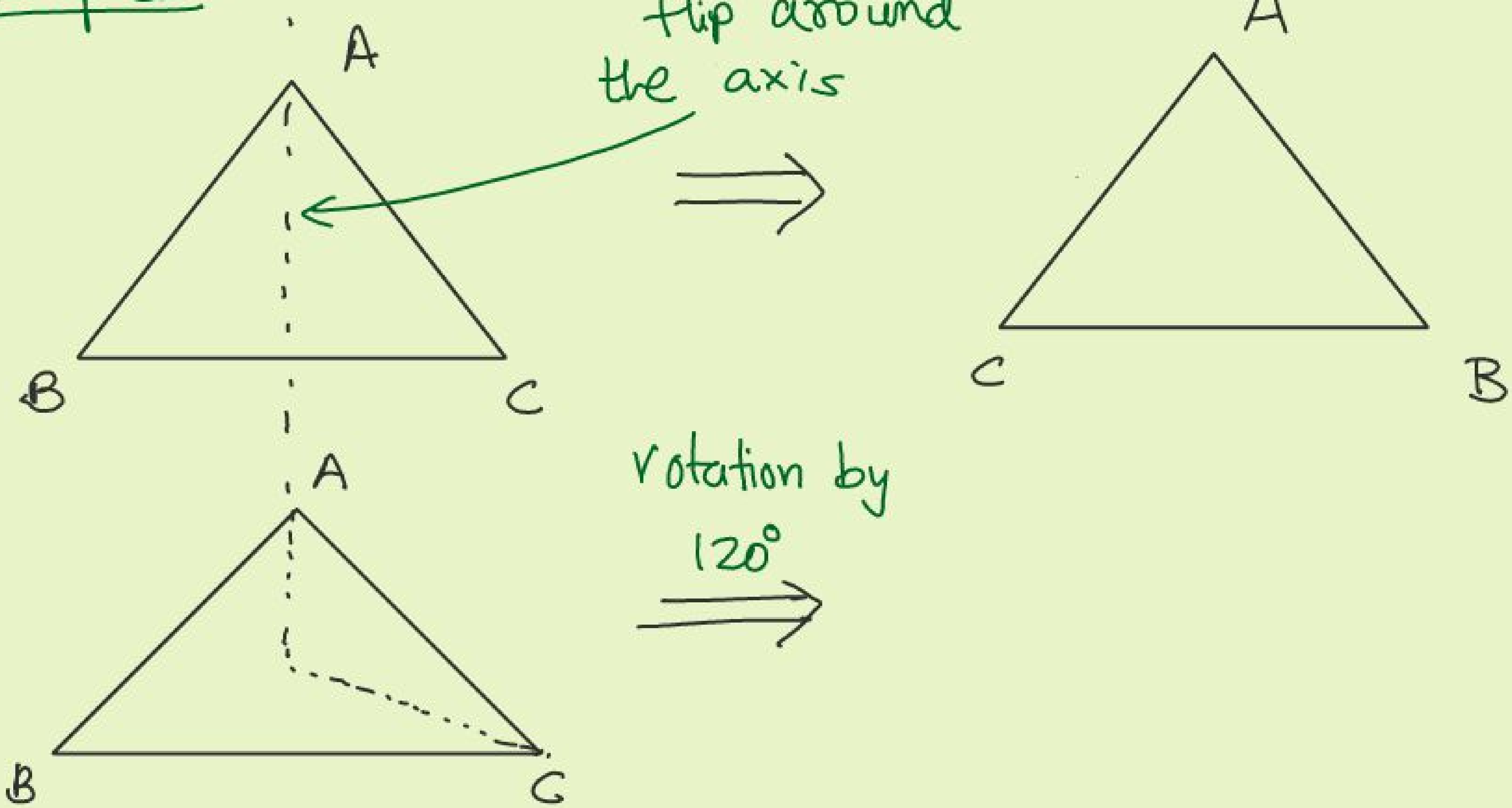
A rigid motion of an object which maps the object to itself is called a **symmetry**

Examples:



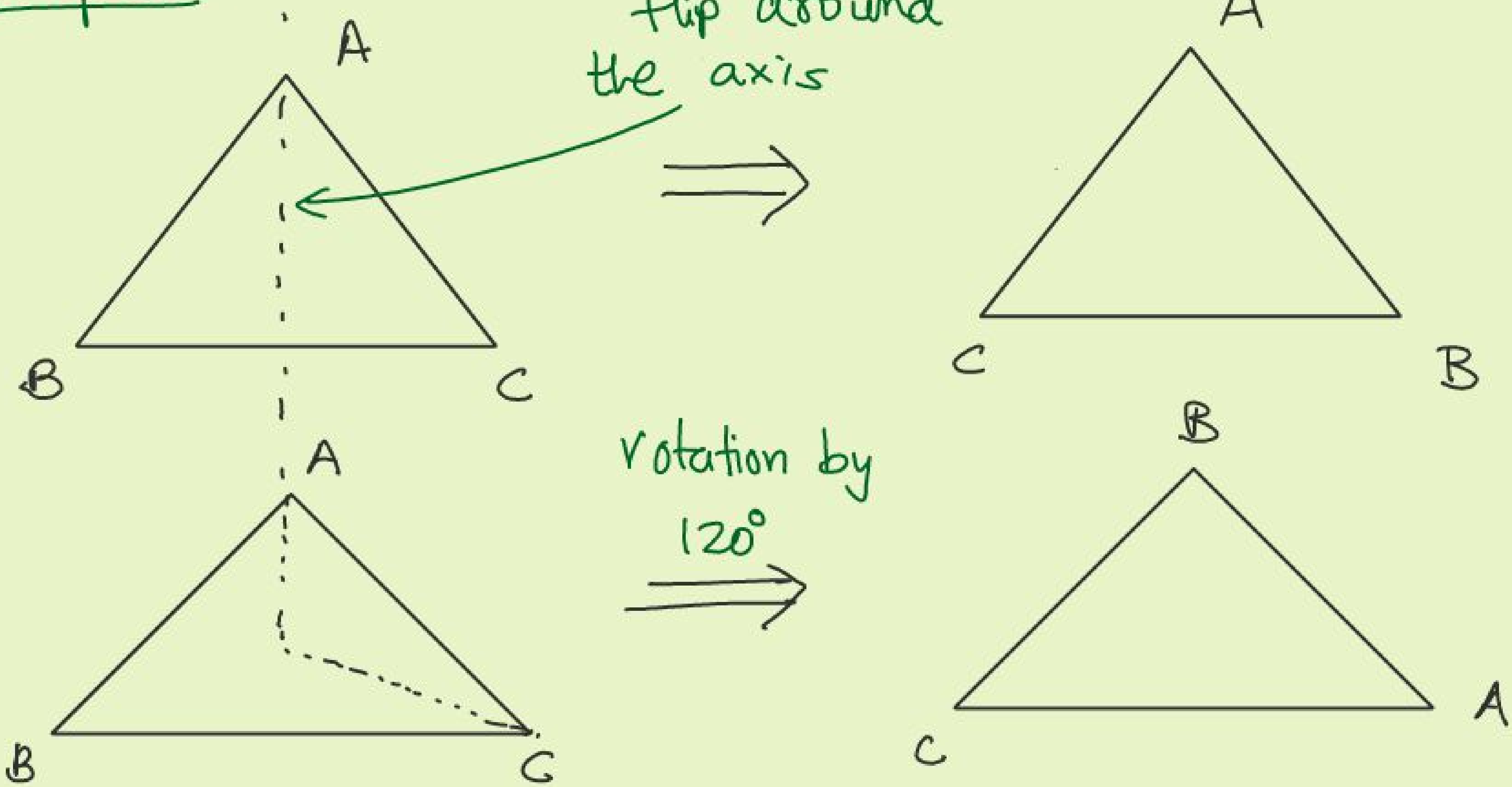
A rigid motion of an object which maps the object to itself is called a <u>symmetry</u>

Examples:



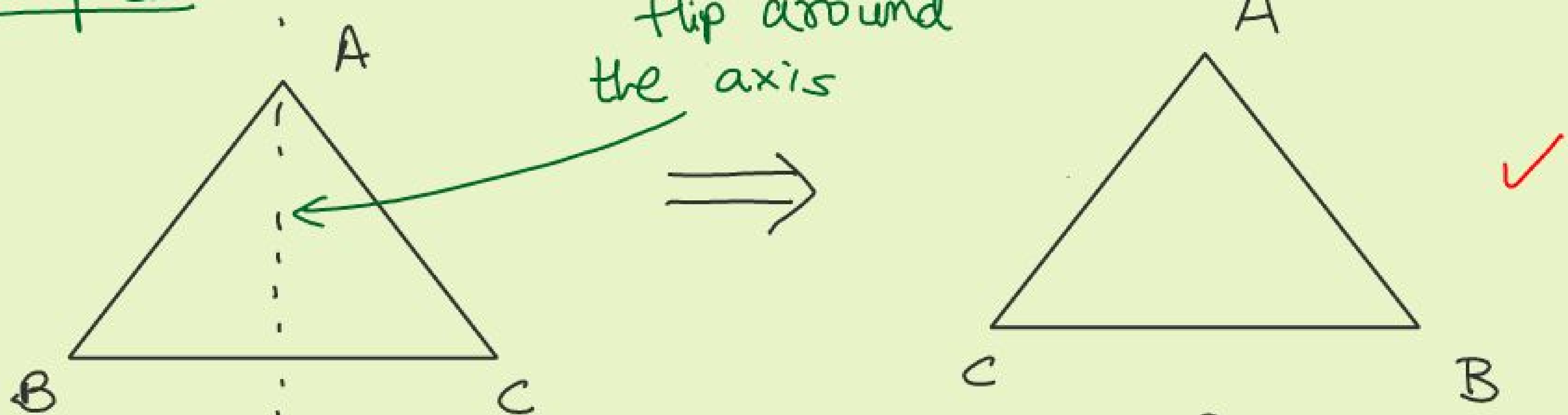
A rigid motion of an object which maps the object to it self is called a symmetry

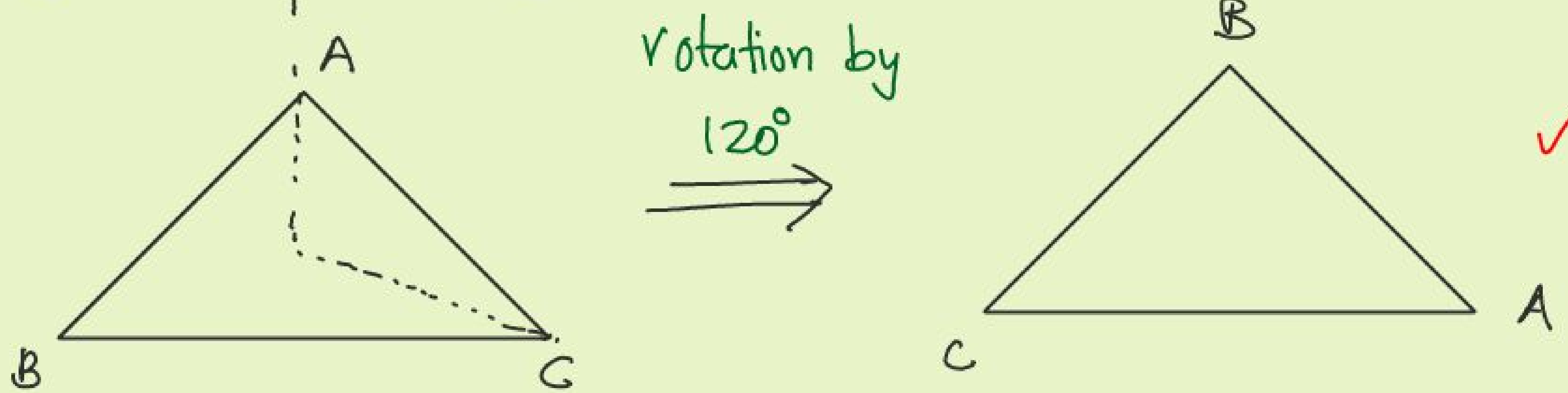
Examples:



A rigid motion of an object which maps the object to itself is called a **symmetry**

## Examples:

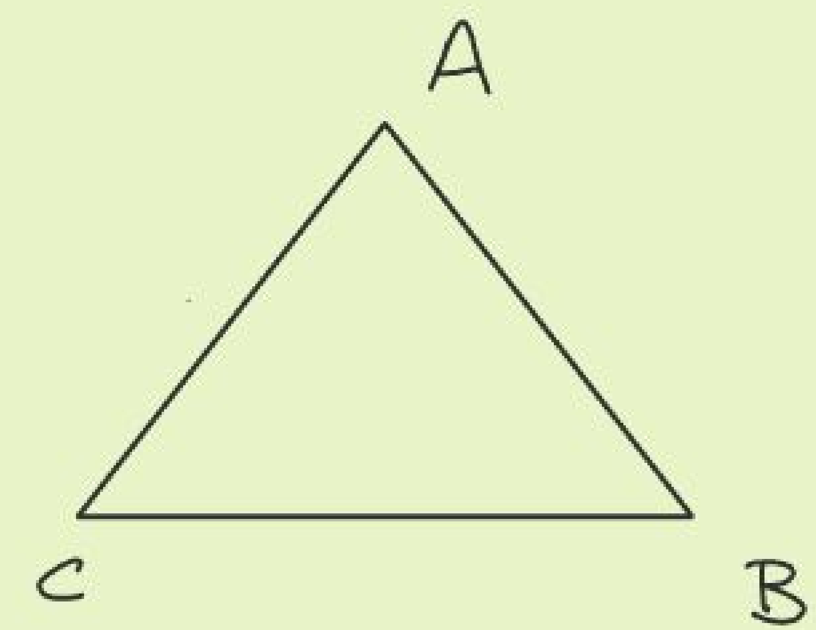


A rigid motion of an object which maps the object to itself is called a symmetry

Examples:

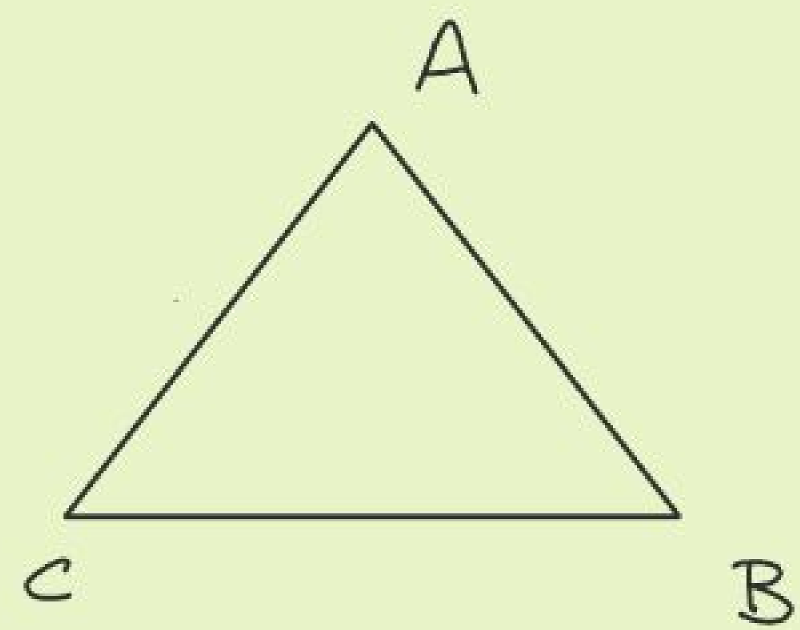
- How many distinct symmetries does an equilateral triangle have?



A rigid motion of an object which maps the object to it self is called a symmetry

Examples:

- How many distinct symmetries does an equilateral triangle have?




- What is a composition of two symmetries?

# Examples of groups

1. $S :=$ Symmetries of an equilateral triangle
   $* :=$ composition of symmetries

$(S, *)$ as defined above forms a group

- closure
- associativity of $*$
- identity
- inverse.

## Examples of groups

2. $S_n =$ all permutations of $\{1, 2, \dots, n\}$

$*$ = composition of permutations

$(S_n, *)$ defined as above forms a group.

## Examples of groups

- Let $S = M_2(\mathbb{R}) \leftarrow$ set of all $2\times 2$ matrices over $\mathbb{R}$.

# Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $*$ = matrix multiplication.

  $(S, *)$ defined above forms a group.

# Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $*$ = matrix multiplication.

  $(S, *)$ defined above forms a group. ✗

## Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $* =$ matrix multiplication.

  $(S, *)$ defined above forms a group. ✗

- Let $S = M_2(\mathbb{R}) \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

  $* =$ matrix multiplication.

## Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $* =$ matrix multiplication.

  $(S,*)$ defined above forms a group. ✗

- Let $S = M_2(\mathbb{R}) \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

  $* =$ matrix multiplication.

  $(S,*)$ defined as above forms a group

## Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $* =$ matrix multiplication.

  $(S,*)$ defined above forms a group. ✗

- Let $S = M_2(\mathbb{R}) \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

  $* =$ matrix multiplication.

  $(S,*)$ defined as above forms a group ✗

## Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $*$ = matrix multiplication.

  $(S,*)$ defined above forms a group. ✗

- Let $S = M_2(\mathbb{R}) \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

  $*$ = matrix multiplication.

  $(S,*)$ defined as above forms a group ✗

- Let $S = GL_2(\mathbb{R})$ ← set of all invertible matrices over $\mathbb{R}$

  $*$ = matrix multiplication

  $(S,*)$ defined as above forms a group

## Examples of groups

- Let $S = M_2(\mathbb{R})$ ← set of all $2\times 2$ matrices over $\mathbb{R}$.

  $*$ = matrix multiplication.

  $(S,*)$ defined above forms a group. ✗

- Let $S = M_2(\mathbb{R}) \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

  $*$ = matrix multiplication.

  $(S,*)$ defined as above forms a group ✗

- Let $S = GL_2(\mathbb{R})$ ← set of all invertible matrices over $\mathbb{R}$

  $*$ = matrix multiplication

  $(S,*)$ defined as above forms a group ✓

A group $(S, *)$ is called <u>abelian</u> if $\forall a, b \in S$

$$a * b = b * a.$$

A group $(S, *)$ is called <u>abelian</u> if $\forall a, b \in S$

$$a * b = b * a.$$

## Examples

Abelian

$(\mathbb{Z}_p, +_p)$

$(\mathbb{Z}_p, \times_p)$

Non-abelian

?

Let $G = (S, *)$ be a group. Let $T \subseteq S$

$H = (T, *)$ is called a <u>subgroup</u> of $G$ if $H$ is a group.

Let $G = (S, *)$ be a group. Let $T \subseteq S$

$H = (T, *)$ is called a **subgroup** of $G$ if $H$ is a group.

## Examples of subgroups :

1. Let $SL_2(\mathbb{R})$ be all $2 \times 2$ matrices with determinant 1.

   $(SL_2(\mathbb{R}), \times)$ is a subgroup of $(GL_2(\mathbb{R}), \times)$

Let $G = (S, *)$ be a group. Let $T \subseteq S$

$H = (T, *)$ is called a **subgroup** of $G$ if $H$ is a group.

## Examples of subgroups :

1. Let $SL_2(\mathbb{R})$ be all $2 \times 2$ matrices with determinant 1.

   $(SL_2(\mathbb{R}), \times)$ is a subgroup of $(GL_2(\mathbb{R}), \times)$

2. Let $G = (S, *)$ be a group. Let $a \in S$.

   Let $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$

   $(\langle a \rangle, *)$ is a subgroup of $G$.

CS 207

Discrete Structures

Nutan Limaye

28 OCT 2013

# Module 4

## Abstract Algebra.

## Last time

- Examples of groups
- Abelian and non-abelian groups
- Subgroups & examples of subgroups
  - cyclic subgroup

Today:

- Properties of subgroups
- Properties of cyclic subgroups.
- Cosets & Lagrange's theorem.

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \emptyset$
- whenever $g, h \in T$ then $gh^{-1} \in T$

<u>Proof</u>: $(\Rightarrow)$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \emptyset$
- whenever $g, h \in T$ then $gh^{-1} \in T$

Proof: $(\Rightarrow)$ suppose $H$ is a subgroup of $G$. Then $T \neq \emptyset$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

<u>Proof</u> : ($\Rightarrow$) suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

($\Leftarrow$) Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

<u>Proof</u>: ($\Rightarrow$) suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

($\Leftarrow$) Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$.

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

<u>Proof</u>: $(\Rightarrow)$ suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

$(\Leftarrow)$ Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$. — (identity)

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

<u>Proof</u>: $(\Rightarrow)$ suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

$(\Leftarrow)$ Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$. — (identity)
- Let $h$ be any element in $T$. Then

$$e \cdot h^{-1} = h^{-1} \in T$$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

Proof: ($\Rightarrow$) suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$. Then $h^{-1} \in T \therefore gh^{-1} \in T$

($\Leftarrow$) Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$. — (identity)
- Let $h$ be any element in $T$. Then

$e \cdot h^{-1} = h^{-1} \in T$ — (inverse)

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

Proof: ($\Rightarrow$) suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

($\Leftarrow$) Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$. — (identity)
- Let $h$ be any element in $T$. Then

$$e \cdot h^{-1} = h^{-1} \in T$$ — (inverse)

- $\forall g, h \in T$, $h^{-1} \in T$. $\therefore g(h^{-1})^{-1} \in T \Rightarrow gh \in T$

Let $G = (S, *)$ be a group. Let $T \subseteq S$. And let $H = (T, *)$. $H$ is a subgroup of $G$ iff.

- $T \neq \phi$
- whenever $g, h \in T$ then $gh^{-1} \in T$

Proof ($\Rightarrow$) suppose $H$ is a subgroup of $G$. Then $T \neq \phi$

Now suppose $g, h \in T$ Then $h^{-1} \in T$ $\therefore gh^{-1} \in T$

($\Leftarrow$) Suppose $T = \phi$ and $\forall g, h \in T$ $gh^{-1} \in T$

- Then for $g = h$ $g \cdot g^{-1} = e$ is in $T$. — (identity)
- Let $h$ be any element in $T$. Then

$$e \cdot h^{-1} = h^{-1} \in T \quad \text{— (inverse)}$$

- $\forall g, h \in T$, $h^{-1} \in T$. $\therefore g(h^{-1})^{-1} \in T \Rightarrow gh \in T$ — (Closure)

Every cyclic group is abelian.

Every cyclic group is abelian.

<u>Proof</u>: Let $G = (S, *)$ be a group. For $a \in S$, $\langle a \rangle$ be called the cyclic subgroup generated by a

Every cyclic group is abelian.

<u>Proof</u>: Let $G = (S, *)$ be a group. For $a \in S$, $\langle a \rangle$ be called the cyclic subgroup <u>generated</u> by $a$

Let $g, h \in \langle a \rangle$

Every cyclic group is abelian.

<u>Proof</u>: Let $G = (S, *)$ be a group. For $a \in S$, $\langle a \rangle$ be called the cyclic subgroup <u>generated</u> by $a$

Let $g, h \in \langle a \rangle$

$\therefore\ g = a^r, \quad h = a^s$ for $r, s \in \mathbb{Z}$.

Every cyclic group is abelian.

<u>Proof</u>: Let $G = (S, *)$ be a group. For $a \in S$, $\langle a \rangle$ be called the cyclic subgroup <u>generated</u> by $a$

Let $g, h \in \langle a \rangle$

$\therefore\ g = a^r, \quad h = a^s$ for $r, s \in \mathbb{Z}$.

$\therefore\ gh = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r$

$= hg$

Every subgroup of a cyclic group is cyclic.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

Let $s \in \mathbb{N}$ be the smallest element s.t. $a^s \in T$.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

(WOP) $\leftarrow$ Let $s \in \mathbb{N}$ be the smallest element s.t. $a^s \in T$.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

(WOP) ← Let $s \in \mathbb{N}$ be the smallest element s.t. $a^s \in T$. We will prove that $T = \langle a^s \rangle$

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

(WOP) ← Let $s \in \mathbb{N}$ be the smallest element s.t. $a^s \in T$. We will prove that $T = \langle a^s \rangle$

Let $g \in T$. Let $g = a^k$ for some $k$.

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

Let $s \in \mathbb{N}$ be the smallest element s.t.

(WOP) $\leftarrow$ $a^s \in T$. We will prove that $T = \langle a^s \rangle$

Let $g \in T$. Let $g = a^k$ for some $k$.

$\therefore\ a^k = a^{sq+r} \Rightarrow a^k = a^{sq} \cdot a^r \Rightarrow a^r = a^k \cdot h^{-q}$

Every subgroup of a cyclic group is cyclic.

proof: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

Let $s \in \mathbb{N}$ be the smallest element s.t.

(WOP) $\leftarrow$ $a^s \in T$. We will prove that $T = \langle a^s \rangle$

Let $g \in T$. Let $g = a^k$ for some $k$.

$\therefore\ a^k = a^{sq+r} \Rightarrow a^k = a^{sq} \cdot a^r \Rightarrow a^r = a^k \cdot h^{-q}$

$\because\ a^k \in T$ and $h^{-q} \in T \Rightarrow a^r \in T$

Every subgroup of a cyclic group is cyclic.

<u>proof</u>: Let $G = (S, *)$ be a cyclic group generated by $a$.

Let $H = (T, *)$ be its subgroup, i.e. $T \subseteq S$ and $H$ is a group.

Let $s \in \mathbb{N}$ be the smallest element s.t.

(WOP) $\leftarrow$ $a^s \in T$. We will prove that $T = \langle a^s \rangle$

Let $g \in T$. Let $g = a^k$ for some $k$.

$\therefore$ $a^k = a^{sq+r}$ $\Rightarrow$ $a^k = a^{sq} \cdot a^r$ $\Rightarrow$ $a^r = a^k \cdot h^{-q}$

$\because$ $a^k \in T$ and $h^{-q} \in T$ $\Rightarrow$ $a^r \in T$

But $r < s$ $\Rightarrow\Leftarrow$

CS 207

Discrete Structures

Nutan Limaye

29 OCT 2013

# Module 4

## Abstract Algebra.

Last time :

- Properties of subgroups
- Properties of cyclic subgroups.

Today:

- Definition of cosets
- examples of cosets
- properties of cosets.

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup

A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup

A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

A right coset $H \cdot g$ is defined similarly.

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup

A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

A right coset $H \cdot g$ is defined similarly.

- Any coset of a group $G$ is a subgroup of $G$ ?

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup

A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

A right coset $H \cdot g$ is defined similarly.

- Any coset of a group $G$ is a subgroup of $G$

$G = (\mathbb{Z}_6, +_{mod\,6})$, $H = (\{0, 3\}, +_{mod\,6})$

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup
A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

A right coset $H \cdot g$ is defined similarly.

- Any coset of a group $G$ is a subgroup of $G$

$G = (\mathbb{Z}_6, +_{mod\,6})$, $H = (\{0, 3\}, +_{mod\,6})$

$g = 2 \qquad gH = \{ 2 +_{mod} 0, 2 +_{mod\,6} 3 \} = \{2, 3\}$

Let $G = (S, *)$ be a group and $H = (T, *)$ be its subgroup
A left coset of $G$ with representative $g \in S$ is defined to be

$$g \cdot H = \{ g * h \mid h \in T \}$$

A right coset $H \cdot g$ is defined similarly.

- Any coset of a group $G$ is a subgroup of $G$ ✗

$G = (\mathbb{Z}_6, +_{mod\,6})$, $H = (\{0, 3\}, +_{mod\,6})$

$g = 2$ $gH = \{ 2 +_{mod} 0, 2 +_{mod\,6} 3 \} = \{2, 3\}$

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

Let $H$ be a subgroup of $G = (S, *)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1 H = g_2 H$, (b) $H g_1^{-1} = H g_2^{-1}$, (c) $g_2^{-1} g_1 \in H$, (d) $g_2 \in g_1 H$

<u>proof</u>: $[(a) \Rightarrow (c)]$

Let $H$ be a subgroup of $G = (S, *)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1 H = g_2 H$, (b) $H g_1^{-1} = H g_2^{-1}$, (c) $g_2^{-1} g_1 \in H$, (d) $g_2 \in g_1 H$

<u>proof</u>: $[(a) \Rightarrow (c)]$ $g_1 H = g_2 H \Rightarrow g_2^{-1} g_1 H = H$.

$$\Rightarrow g_2^{-1} g_1 \in H.$$

Let $H$ be a subgroup of $G = (S, *)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1 H = g_2 H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1} g_1 \in H$, (d) $g_2 \in g_1 H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1 H = g_2 H \rightarrow g_2^{-1} g_1 H = H$.

$\Rightarrow g_2^{-1} g_1 \in H$.

[(c) $\Rightarrow$ (a)]

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1H = g_2H \implies g_2^{-1}g_1H = H$

$\implies g_2^{-1}g_1 \in H$.

[(c) $\Rightarrow$ (a)] $g_2^{-1}g_1 \in H \implies g_2^{-1}g_1H = H$

$\implies g_1H = g_2H$.

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) ⇒ (c)] $g_1H = g_2H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_2^{-1}g_1 \in H$.

[(c) ⇒ (a)] $g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_1H = g_2H$.

[(c) ⇒ (b)]

Let $H$ be a subgroup of $G = (S, *)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1 H = g_2 H$, (b) $H g_1^{-1} = H g_2^{-1}$, (c) $g_2^{-1} g_1 \in H$, (d) $g_2 \in g_1 H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1 H = g_2 H \Rightarrow g_2^{-1} g_1 H = H$

$\Rightarrow g_2^{-1} g_1 \in H$.

[(c) $\Rightarrow$ (a)] $g_2^{-1} g_1 \in H \Rightarrow g_2^{-1} g_1 H = H$

$\Rightarrow g_1 H = g_2 H$.

[(c) $\Rightarrow$ (b)] $g_2^{-1} g_1 \in H \Rightarrow H (g_2^{-1} g_1) = H$

$\Rightarrow H g_2^{-1} = H g_1^{-1}$.

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) ⇒ (c)] $g_1H = g_2H \Rightarrow g_2^{-1}g_1H = H$.

$\Rightarrow g_2^{-1}g_1 \in H$.

[(c) ⇒ (a)] $g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_1H = g_2H$.

[(c) ⇒ (b)] $g_2^{-1}g_1 \in H \Rightarrow H(g_2^{-1}g_1) = H$

$\Rightarrow Hg_2^{-1} = Hg_1^{-1}$.

[(c) ⇒ (d)]

Let $H$ be a subgroup of $G = (S, *)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1H = g_2H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_2^{-1}g_1 \in H$.

[(c) $\Rightarrow$ (a)] $g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_1H = g_2H$.

[(c) $\Rightarrow$ (b)] $g_2^{-1}g_1 \in H \Rightarrow H(g_2^{-1}g_1) = H$

$\Rightarrow Hg_2^{-1} = Hg_1^{-1}$.

[(c) $\Rightarrow$ (d)] $g_2^{-1}g_1 \in H \Rightarrow g_1^{-1}g_2 \in H$

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1H = g_2H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_2^{-1}g_1 \in H$.

[(c) $\Rightarrow$ (a)] $g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_1H = g_2H$.

[(c) $\Rightarrow$ (b)] $g_2^{-1}g_1 \in H \Rightarrow H(g_2^{-1}g_1) = H$

$\Rightarrow Hg_2^{-1} = Hg_1^{-1}$.

[(c) $\Rightarrow$ (d)] $g_2^{-1}g_1 \in H \Rightarrow g_1^{-1}g_2 \in H$

$\Rightarrow g_1^{-1}g_2 = h$ for some $h \in H$

Let $H$ be a subgroup of $G=(S,*)$. Let $g_1, g_2 \in S$. Then the following are equivalent:

(a) $g_1H = g_2H$, (b) $Hg_1^{-1} = Hg_2^{-1}$, (c) $g_2^{-1}g_1 \in H$, (d) $g_2 \in g_1H$

<u>proof</u>: [(a) $\Rightarrow$ (c)] $g_1H = g_2H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_2^{-1}g_1 \in H$.

[(c) $\Rightarrow$ (a)] $g_2^{-1}g_1 \in H \Rightarrow g_2^{-1}g_1H = H$

$\Rightarrow g_1H = g_2H$.

[(c) $\Rightarrow$ (b)] $g_2^{-1}g_1 \in H \Rightarrow H(g_2^{-1}g_1) = H$

$\Rightarrow Hg_2^{-1} = Hg_1^{-1}$.

[(c) $\Rightarrow$ (d)] $g_2^{-1}g_1 \in H \Rightarrow g_1^{-1}g_2 \in H$

$\Rightarrow g_1^{-1}g_2 = h$ for some $h \in H$

$\Rightarrow g_2 = g_1h$

$\Rightarrow g_2 \in g_1H$

All the left cosets of a group partition the group.

<u>proof</u>: if $g_1 \neq g_2$ then either $g_1 H = g_2 H$

or $g_1 H \cap g_2 H = \phi$

Suppose $g_1 = g_2$. . Let $f \in g_1 H \cap g_2 H$

$\therefore \exists h_1, h_2 \in H$ s.t. $g_1 h_1 = g_2 h_2 = f$

$g_2^{-1} g_1 h_1 = h_2$ i.e. $(g_2^{-1} g_1) \in h \Rightarrow g_1 H = g_2 H$

The same can be proved for right cosets.

let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

<u>proof</u>: To prove this, we define a function from left cosets to right cosets

And prove that it is a bijection.

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

Proof: To prove this, we define a function from left cosets to right cosets
And prove that it is a bijection.

Let the map be : $\varphi(gH) = Hg^{-1}$.

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

<u>proof</u>: To prove this, we define a function from left cosets to right cosets

And prove that it is a bijection.

Let the map be : $\varphi(gH) = Hg^{-1}$.

well-defined — ?

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

Proof: To prove this, we define a function from left cosets to right cosets

And prove that it is a bijection.

Let the map be : $\varphi(gH) = Hg^{-1}$.

well-defined — ✓

one-to-one — ?

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

Proof: To prove this, we define a function from left cosets to right cosets
And prove that it is a bijection.

Let the map be : $\varphi(gH) = Hg^{-1}$.

well-defined — ✓

one-to-one — ✓

onto — ?

Let $G$ be a group and $H$ be its subgroup. The number of left cosets of $H$ in $G$ is the same as the number of right cosets of $H$ in $G$.

<u>proof</u>: To prove this, we define a function from left cosets to right cosets
And prove that it is a bijection.

Let the map be : $\varphi(gH) = Hg^{-1}$.

well-defined — ✓

one-to-one — ✓

onto — ✓

# CS 207

# Discrete Structures

Nutan Limaye

11 NOV 2013

# Module 4

## Abstract Algebra.

Today:

- Counting necklaces – Pólya's theory of counting

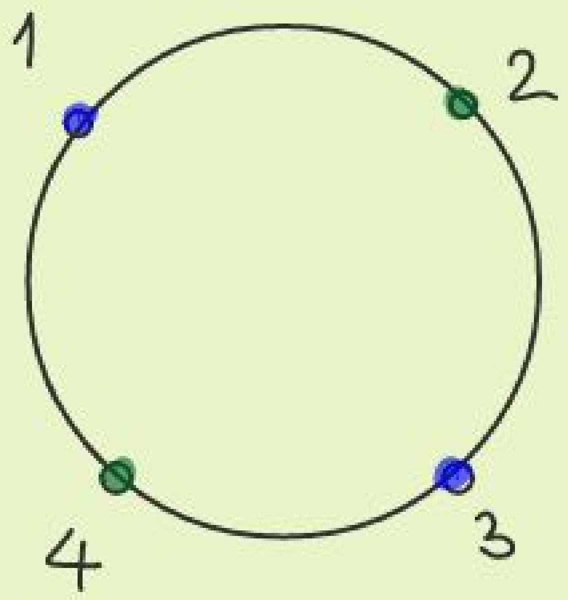
Given: $n$ beads of $m$ different colors $(m < n)$

Output: # different necklaces that can be formed?

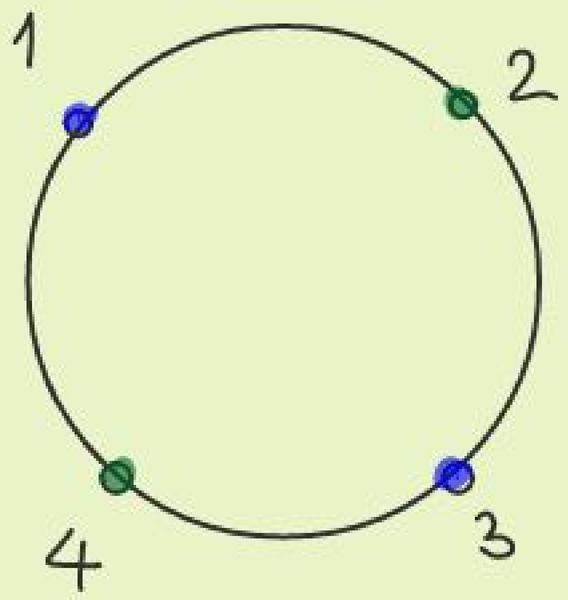
<u>Recall</u>: Defn of

- groups
- symmetric groups
- cyclic subgroup of a symmetric group
- group of symmetries of a regular $n$-gon.

Consider the case when $n = 4$ and $m = 2$

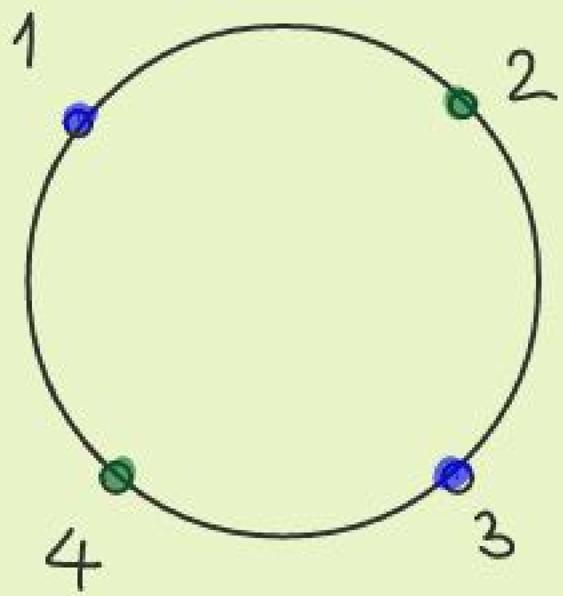


Consider the case when $n = 4$ and $m = 2$




$S = \{1, 2, 3, 4\}$

Consider the case when $n = 4$ and $m = 2$

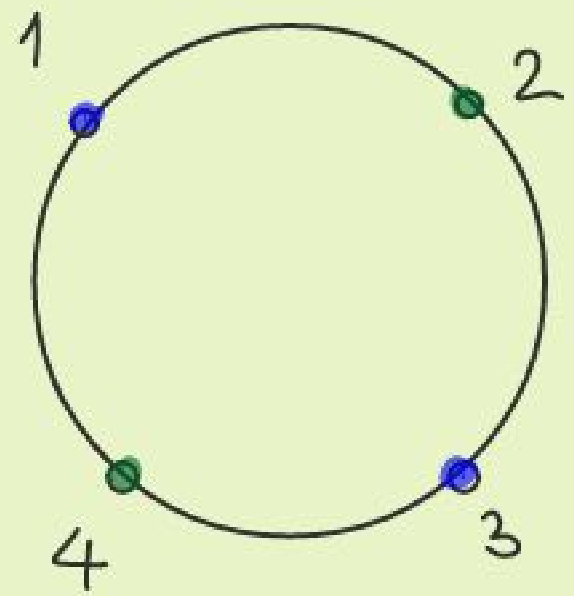



$S = \{1, 2, 3, 4\}$

$C = \{\text{set of all colorings}\}$

$= \{gggg, gggr, ggrg, \ldots\}$

Consider the case when $n = 4$ and $m = 2$



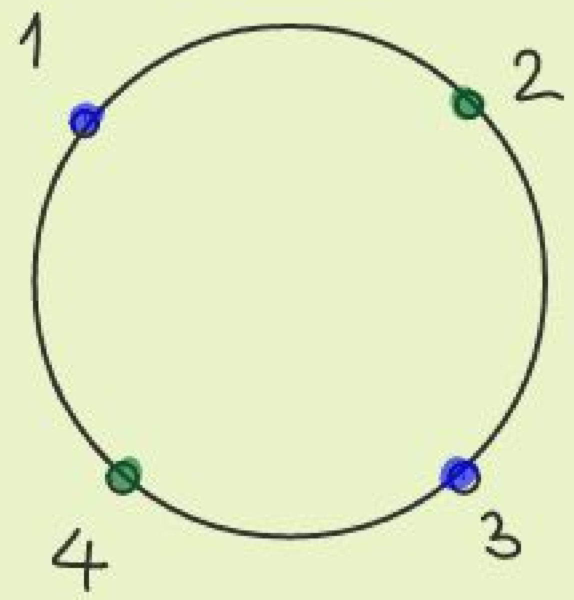

$S = \{1, 2, 3, 4\}$

$C = \{\text{set of all colorings}\}$

$= \{gggg, gggr, ggrg, \ldots\}$

Let $\pi = (12)(34)$

Consider the case when $n = 4$ and $m = 2$




$S = \{1, 2, 3, 4\}$

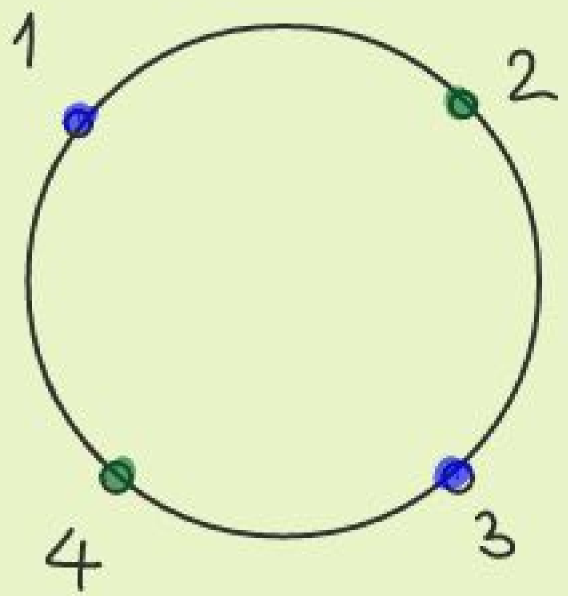
$C = \{\text{set of all colorings}\}$

$= \{gggg, gggr, ggrg, \ldots\}$

Let $\pi = (12)(34)$

Let $c = grgr$

Consider the case when $n = 4$ and $m = 2$




$S = \{1,2,3,4\}$

$C = \{\text{set of all colorings}\}$

$= \{gggg, gbgg, \ldots, \ldots\}$

Let $\pi = (12)(34)$

Let $c = gbgb$

then $\pi(c) = bgbg$

We say two colorings are equivalent if one is obtained from the other by the rotation of the necklace.

We say two colorings are equivalent if one is obtained from the other by the rotation of the necklace.

$\{gggg\}$

$\{gggb, ggbg, gbgg, bggg\}$

$\vdots$

We say two colorings are equivalent if one is obtained from the other by the rotation of the necklace.

$\{gggg\}$

$\{gggb, ggbg, gbgg, bggg\}$

$\vdots$

How many such sets?

In the above problem the set of symmetries
— formed a cyclic subgroup.

In general:

$S$ — set of $n$ bead positions
$G$ — symmetries of $n$-gon.
$C$ — collection of $m^n$ colorings.

Count # diff. necklaces. [i.e. $G$ defines notion of equivalence.]

## Some definitions:

Given $\pi \in G$ let $C_\pi = \{c \in C \mid \pi(c) = c\}$

Given $c \in C$ let $G_c = \{\pi \in G \mid \pi(c) = c\}$

Note: $G_c$ is a subgroup of $G$.

Given $c \in C$ let $\overline{c} = \{\pi(c) \mid \pi \in G\}$

$\overline{c}$ is called the orbit of $c$.

Examples :

Suppose a group $G$ acts on a set of colorings $C$. For any coloring $c \in C$ we have

$$|G_c| \cdot |\bar{c}| = |G|.$$

<u>proof</u>:

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

<u>Proof</u> : <u>R.H.S</u> =

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

Proof : R.H.S $= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

<u>Proof</u> : <u>R.H.S</u>

$$= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} \sum_{\pi \in G} [\pi^*(c) = c]$$

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

Proof : R.H.S $= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$

$$= \frac{1}{|G|} \sum_{c \in C} \sum_{\pi \in G} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} |G_c|$$

The no. of equivalence classes of the set $C$ in the presence of symmetries $G$ is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

Proof : R.H.S $= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$

$$= \frac{1}{|G|} \sum_{c \in C} \sum_{\pi \in G} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} |G_c| = \sum_{c \in C} \frac{1}{|\bar{c}|}$$

The no. of equivalence classes of the set $C$ in the presence of symmetries $G$ is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

<u>Proof</u> : <u>R.H.S</u> $= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$

$$= \frac{1}{|G|} \sum_{c \in C} \sum_{\pi \in G} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} |G_c| = \sum_{c \in C} \frac{1}{|\bar{c}|}$$

$$= \sum_{\bar{c}} \sum_{c \in \bar{c}} 1/|\bar{c}|$$

The no. of equivalence classes of the set C in the presence of symmetries G is given by

$$N = \frac{1}{|G|} \sum_{\pi \in G} |C_\pi|$$

<u>Proof</u> : <u>R.H.S</u>

$$= \frac{1}{|G|} \sum_{\pi \in G} \sum_{c \in C} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} \sum_{\pi \in G} [\pi^*(c) = c]$$

$$= \frac{1}{|G|} \sum_{c \in C} |G_c| = \sum_{c \in C} \frac{1}{|\bar{c}|}$$

$$= \sum_{\bar{c}} \sum_{c \in \bar{c}} 1/|\bar{c}| = \sum_{\bar{c}} 1 = N.$$