INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Discrete Structures (Monsoon 2021)

Ashok Kumar Das

Associate Professor
IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas
https://sites.google.com/view/iitkgpakdas/

Group Theory

Group

Definition

Let $(S, \circ)$ be a structure. An element $x \in S$ is said to be an *idempotent* if $x \circ x = x$.

Theorem

A finite monoid $(M, \circ, e)$ *is a group if and only if the identity element* $e \in M$ *is its only idempotent.*

Proof.

$(\Rightarrow)$: Given M is a finite monoid and it is a group.
R.T.P. If $x \circ x = x$, then $x = e$ is the identity in M, for $x \in M$.
Since M is a group, so x^{-1} exists for each $x \in M$.
Now, $x \circ x = x$. Then, $x^{-1} \circ (x \circ x) = x^{-1} \circ x$
$\Rightarrow (x^{-1} \circ x) \circ x = x^{-1} \circ x$
$\Rightarrow e \circ x = e$, since $x^{-1} \circ x = x \circ x^{-1} = e$, the identity in M
$\Rightarrow x = e$. $\square$

Subgroup

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition

A subgroup of a group G is a subset of the elements of the set G that forms a group under the composition of the group G.

Theorem

Let H be a subgroup of a group G. Then, the identity of H is the same as the identity of G.

Theorem

Let H be a subset of a group G. Then, H forms a subgroup of the group G if and only if $(h_1.h_2^{-1}) \in H$, for every $h_1, h_2 \in H$.

Subgroup

Theorem

Let $H \subseteq \langle G, \cdot \rangle$ be a finite subset of a group G which is closed under the binary composition '$\cdot$'. Then, H is a subgroup of G.

Proof. Given $H \subseteq \langle G, \cdot \rangle$ is a finite subset of a group G, and $\forall h_1, h_2 \in H, (h_1 \cdot h_2) \in H$.
RTP: H is a subgroup of G, that is,

$$\forall h_1, h_2 \in H, (h_1 \cdot h_2^{-1}) \in H.$$

In other words, it is sufficient to prove that

$$\forall h_2 \in H, h_2^{-1} \in H.$$

Let $h \in H$. Then start generating its positive powers. We have: $h^1, h^2, h^3, \cdots, h^{m+n} = h^m$, for some $n > 0$ as H is a finite subset.

Subgroup

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Now,

$$\begin{aligned} h^{m+n} &= h^m \\ \Rightarrow h^m \cdot h^n &= h^m \\ \Rightarrow h^n &= e\text{, identity element in } G \\ \Rightarrow h^{n-1} \cdot h = h \cdot h^{n-1} &= e\text{, for } n-1 \geq 0. \end{aligned}$$

Note that $h^0 = e$ is the identity in H, since $h^0 \cdot h = h \cdot h^0 = h$. Hence, h^{n-1} is the left as well as right inverse of $h \in H$. Thus, $h^{-1} = h^{n-1}$.
Since $\forall h \in H, h^{-1} \in H$, take $h_2 = h$.
Therefore, $\forall h_1, h_2 \in H, (h_1 \cdot h_2^{-1}) \in H$, since H is closed under $\cdot$. As a result, H is a subgroup of G.

Subgroup

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Problem:

- Prove that the intersection of two subgroups of a group G is also a subgroup.
- Discover whether the following statement is true or false:
  "The union of two subgroups of a group is also a subgroup."