Discrete Structures (Monsoon 2022)

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

If a finite monoid $(M, \circ, e)$ is a group, then the identity element $e \in M$ is its only idempotent.

Proof.

Given M is a finite monoid and it is a group.
R.T.P. (Required to Prove): If $x \circ x = x$, $x = e$ 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

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 $h_1, h_2 \in H$.

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.

Subgroup

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."

Subgroup

Problem:

Prove that a group $\langle G, \cdot \rangle$ is abelian, if and only if $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$, for all $a, b \in G$.