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

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

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

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 $a, b \in G$.

Cosets

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Definition (Left Coset)

Let H be a subgroup of a group $\langle G, \cdot \rangle$. The left cosets of G relative of H are defined by

$$g \cdot H = \{g \cdot h | h \in H\}, \forall g \in G.$$

If $\cdot = +$, then

$$g \cdot H = g + H = \{g + h | h \in H\}.$$

Definition (Right Coset)

Let H be a subgroup of a group $\langle G, \cdot \rangle$. The right cosets of G relative of H are defined by

$$H \cdot g = \{h \cdot g | h \in H\}, \forall g \in G.$$

Cosets

Example

Let $\underline{3} = \{1, 2, 3\}$ be a finite set. Considering all $3! = 6$ permutations on $\underline{3}$, define a set $S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. Then, S_3 forms a group under permutation composition (multiplication). Also, S_3 is called a symmetric group of degree 3. Find the left and right cosets of S_3 relative to a subgroup $H = \{e, (1\,2)\} \subseteq S_3$, where e is the identity permutation defined on $\underline{3}$.

Group

Problem: If H be a subgroup of a group $\langle G, \circ \rangle$ and $h \in H$, then $h \circ H = H \circ h = H$.

Group

Problem: For each g in a group $[G, .]$, the set $N_g = \{h | h.g.h^{-1} = g\}$ is called the *normalizer* of g. Show that N_g is a subgroup of G for every g.

Subgroup

Theorem

The left (right) cosets of a group G relative to a subgroup H form a partition of G. Moreover, all of the left or right cosets of G relative to H have equal number of elements.

Subgroup

Definition (Left coset relation)

Let G be a group with subgroup H. The **left coset relation** on G with respect to H is the relation R with the property that ${}_{g_1}R_{g_2}$ iff $g_1^{-1} \cdot g_2 \in H, \forall g_1, g_2 \in G$.

Definition (Right coset relation)

Let G be a group with subgroup H. The **right coset relation** on G with respect to H is the relation R with the property that ${}_{g_1}R_{g_2}$ iff $g_1 \cdot g_2^{-1} \in H, \forall g_1, g_2 \in G$.

Subgroup

Theorem

The left (right) coset relation is an equivalence relation on a group G, and the equivalence classes are the left (right) cosets of G with respect to a subgroup H of G.

Normal Subgroup

Definition (Normal Subgroup)

A subgroup H of a group G is said to be a **normal subgroup** if the left coset partition induced by H is identical to the right coset partition induced by H.
Equivalently, H is normal if

$$g \cdot H = H \cdot g, \forall g \in G.$$

Theorem

*A subgroup H of a group G is **normal** if and only if*

$$g^{-1} \cdot H \cdot g \subseteq H, \forall g \in G.$$

*In other words, a subgroup H of a group G is **normal** if and only if*

$$g^{-1} \cdot h \cdot g \in H, \forall g \in G \, and \, h \in H.$$

Quotient group

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Theorem

If H is a normal subgroup of a group $\langle G, \cdot \rangle$, then the quotient structure $\langle G/H, \circ \rangle$ is a group, where $\circ$ is the composition of cosets defined by

$$[g] \circ [h] = [g \cdot h]$$

where $[g]$ denotes a left (right) coset of G relative to H and it is defined by $[g] = g \cdot H, \forall g \in G$, with respect to the left coset operation.

The group $\langle G/H, \circ \rangle$ is called the “quotient group” or “factor group” of G relative to the normal subgroup H.

Homomorphism

Definition (Homomorphism of semigroups)

Let $[S, \cdot]$ and $[T, *]$ be two semigroups. A mapping (function) $\theta : [S, \cdot] \rightarrow [T, *]$ is called a morphism (or homomorphism) of two semigroups $[S, \cdot]$ and $[T, *]$, if $\forall s_1, s_2 \in S$, $\theta(s_1 \cdot s_2) = \theta(s_1) * \theta(s_2)$.

Definition (Homomorphism of monoids)

Let $[S, \cdot, e_S]$ and $[T, *, e_T]$ be two monoids. A mapping (function) $\theta : [S, \cdot, e_S] \rightarrow [T, *, e_T]$ is called a morphism (or homomorphism), if the following conditions are met:

- (i) $\forall s_1, s_2 \in S$, $\theta(s_1 \cdot s_2) = \theta(s_1) * \theta(s_2)$.
- (ii) $\theta(e_S) = e_T$, where e_S and e_T denote the identity elements in the monoids $[S, \cdot, e_S]$ and $[T, *, e_T]$, respectively.

Homomorphism

Definition (Homomorphism of groups)

Let $[G, \cdot]$ and $[G', *]$ be two groups. A mapping (function) $\mu : [G, \cdot] \to [G', *]$ is called a morphism (or homomorphism), if the following conditions are met:

- (i) $\forall g, g' \in G$, $\mu(g \cdot g') = \mu(g) * \mu(g')$.
- (ii) $\mu(e_G) = e_{G'}$, where e_G and $e_{G'}$ denote the identity elements in the groups $[G, \cdot]$ and $[G', *]$, respectively.
- (iii) $[\mu(g)]^{-1} = \mu(g^{-1})$, $\forall g \in G$.

Homomorphism

Definition

Let g be a homomorphism from a structure $[X, \cdot]$ to another structure $[Y, *]$.

- If $g : X \to Y$ is onto (surjective), then g is called an **epimorphism**.
- If $g : X \to Y$ is one-one (injective), then g is called an **monomorphism**.
- If $g : X \to Y$ is one-one (injective) and onto (surjective) (that is, g is bijective), then g is called an **isomorphism**.
- If $g : X \to Y$ is called an **automorphism**, if $X = Y$ and g is a bijection.

Homomorphism

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Theorem

Let $[G, \cdot]$ and $[G', *]$ be two groups. A mapping (function) $\mu : [G, \cdot] \rightarrow [G', *]$ is called a morphism (or homomorphism) of the groups $[G, \cdot]$ and $[G', *]$ if and only if

$$\mu(g \cdot g') = \mu(g) * \mu(g'), \forall g, g' \in G.$$

Homomorphism

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Example

Let G be the group of non-zero real numbers under the multiplication operation. Determine whether the following functions are morphisms or not:

- (i) $\phi : G \to G$, where $\phi(x) = x^2$, for all $x \in G$.
- (ii) $\psi : G \to G$, where $\psi(x) = 2^x$, for all $x \in G$.

Homomorphism

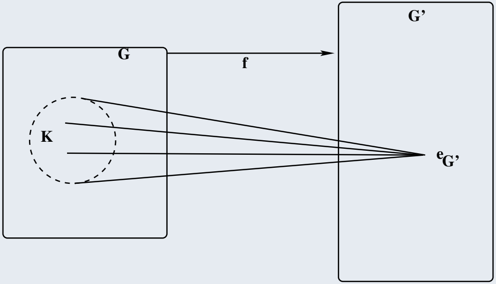
Theorem

Let H be a normal subgroup of G. Then, the mapping $f : G \to G/H$, $f(g) = [g]$, is a group epimorphism. Here, $[g]$ denotes a left (right) coset of G relative to H and it is defined by $[g] = g \cdot H, \forall g \in G$, with respect to the left coset operation.

Kernal of group homomorphism

Definition

The **kernal** of a group homomorphism is the set of domain elements that is mapped onto the identity element in the range.



If $f : G \to G'$ be a group homomorphism and $K \subseteq G$ is the kernal of f, then $f(K) = \{e'_G\}$, where G and G' are groups and $e_{G'}$ is the identity in G'. In other words, $f(x) = e_{G'}, \forall x \in K$.

Kernal of group homomorphism

Theorem (Fundamental theorem of group homomorphism)

*Let $f : G \to G'$ be any group homomorphism, where G and G' be two groups. Then, the kernal of the homomorphism f is a **normal subgroup** of G.*

Order of a group

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Theorem (Lagrange's theorem)

The order of a finite group G is divided by the order of its subgroup H.

Proof. Let G be a finite group of order n and $H \subseteq G$ be its subgroup of order m.
Then, $|G| = n$ and $|H| = m$.
RTP: $m|n$, that is, $n = mk$ for some positive integer k.
Let $H = \{h_1, h_2, \ldots, h_m\} \subseteq G$ be a subgroup of G. Then,

$$a \cdot H = \{a \cdot h_1, a \cdot h_2, \ldots, a \cdot h_m\}, a \in G$$

contains m elements and these elements are distinct, since

$$a \cdot h_i = a \cdot h_j \Rightarrow h_i = h_j,$$

by the left cancellation law in G.

Order of a group

$$a \cdot h_i = a \cdot h_j \Rightarrow (a^{-1} \cdot a) \cdot h_i = (a^{-1} \cdot a) \cdot h_j \Rightarrow e \cdot h_i = e \cdot h_j \Rightarrow h_i = h_j,$$

where $e \in G$ as well as $e \in H$ is the identity.
Now, G is a finite group. Therefore, the number of distinct left (right) cosets is also finite. Let the number of distinct left cosets be k, that is, $a_1 \cdot H, a_2 \cdot H, \cdots a_k \cdot H$ so that the number of elements of the k cosets is km, and this is the total number of elements of G. Since the disjoint left (right) cosets of G form a partition of G, so

$$G = (a_1 \cdot H) \cup (a_2 \cdot H) \cup \cdots \cup (a_k \cdot H).$$

Therefore,

$$|G| = |a_1 \cdot H| + |a_2 \cdot H| + \cdots + |a_k \cdot H|$$

and $n = km$. This proves that the order of H, i.e., m, is a divisor of n, which is the order of G.

Order of a group

Example

Let $G = S_3$ be a symmetric group of order 3 on the set $\underline{3} = \{1, 2, 3\}$, which contains $3! = 6$ permutations, and $H = \{e, (1\,2)\} \subseteq S_3$ is subgroup order 2.
Thus, $|G| = 6$ and $|H| = 2$. Hence, $2|6$.

Order of a group

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Corollary

The index k of a subgroup H of a finite group G is a divisor of the order of G.

Proof. Since $n = mk$, where $|G| = n$ and $|H| = m$, so $k|n$.
Note: The index of H under G, $[G : H] = k$ is the number of distinct left (right) cosets of G relative to H.

Order of a group

Corollary

The order of every element of a finite group G is a divisor of the order of the group G.

Proof. Let $a \in G$ and order of a in G is $Ord_G(a) = m$.
Then, m is the least positive integer such that $a^m = e$, the identity in G.
Therefore,

$$a^1, a^2, a^3, \cdots, a^{m-1}, a^m = e$$

are all distinct elements in G.
Now, construct a subset $H = \{a^1, a^2, a^3, \cdots, a^{m-1}, a^m = e\}$.
We see that $|H| = m$ and it is a subgroup of G. Since the order of H divides the order of G, so $n = mk$, for some positive integer k, $|G| = n$.
Thus, the order of $a \in G$ divides the order of the group G.

Order of a group

Corollary

If G be a finite group of order n and $a \in G$, then $a^n = e$, where $e \in G$ is the identity element in G.

Proof. Given $|G| = n$.
If the order of an element a in G is $Ord_G(a) = m$, then $m|n$, that is, $n = mk$ for some positive integer k.
Since $Ord_G(a) = m$, so $a^m = e$.
Now,

$$\begin{aligned} a^n &= a^{mk} \\ &= (a^m)^k \\ &= e^k \\ &= e. \end{aligned}$$