Homomorphism

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

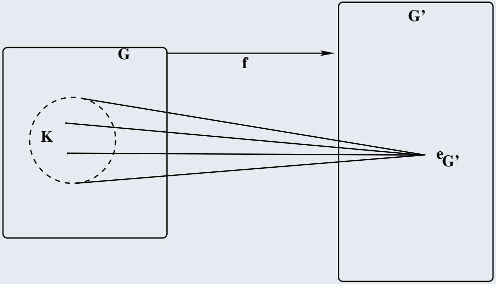
Theorem

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 $[g] = g \circ H, \forall g \in G$, with respect to the left coset operation $\circ$.

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 $f : G \rightarrow G'$ 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

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 $H = \{h_1, h_2, \dots, h_m\} \subseteq G$ be a subgroup of G. Then,

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

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

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

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

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,

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