Dept. of Mathematics

B.Sc. Part II, Paper III

Abstract Algebra (Notion of a Group)

A group $(G, \cdot)$ is a nonempty set G together with a binary operation $\cdot$ on G such that the following conditions hold:

(i) Closure :- For all $a, b \in G$ the element $a \cdot b$ is a uniquely defined element of G.

(ii) Associativity :- For all $a, b, c \in G$, we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c .$$

(iii) Identity :- There exists an identity element $e \in G$ such that

$$e \cdot a = a \quad \text{and} \quad a \cdot e = a \quad \text{for all } a \in G.$$

(iv) Inverses :- For each $a \in G$ there exists an inverse element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = e \quad \text{and} \quad a^{-1} \cdot a = e .$$

We can write ab for the $a \cdot b$.

Proposition (Cancellation Property for Groups)

Let G be a group, and let $a, b, c \in G$.

(a) If $ab = ac$, then $b = c$.

(b) If $ac = bc$, then $a = b$.

* A Group G is said to be abelian if $ab = ba$ for all $a, b \in G$.

* A group G is said to be a finite group if the set G has a finite number of elements. Number of elements is called the order of G, denoted by $|G|$.

* Let a be an element of the group G. If there exists a positive integer n such that $a^n = e$, then a is said to have finite order, and the smallest such positive integer is called the order of a, denoted by O(a).

If there does not exist a positive integer n such that $a^n = e$, then a is said to have infinite order.

* Let G is a group, and let H be a subset of G. Then H is called a subgroup of G if H is itself a group, under the operation induced by G.

Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H$, for all $a, b \in H$,

(ii) $e \in H$; (iii) $a^{-1} \in H$ for all $a \in H$.

Lagrange Theorem :- If H is a subgroup of the finite group G, then the order of H is a divisor of the order of G.

Corollary :- Let G be a finite group of order n.

(a) For any $a \in G$, O(a) is a divisor of n.

(b) For any $a \in G$, $a^n = e$.

Note :- Any group of prime order is cyclic.

Let G_1 and G_2 be groups, and let $\theta : G_1 \to G_2$ be a function. Then θ is said to be a group isomorphism if (i) θ is one-to-one and onto and (ii) $\theta(ab) = \theta(a)\theta(b)$ for all $a, b \in G_1$.