TRINITY COLLEGE FOR WOMEN NAMAKKAL
Department of Mathematics

ALGEBRAIC STRUCTURE

23PMA01– ODD SEMESTER

COMMON ALGEBRAIC STRUCTURE

Presented by
Dr. S. JEYANTHI
Assistant Professor
Department of Mathematics
http://www.trinitycollegenkl.edu.in/

ALGEBRAIC STRUCTURES

Cryptography requires sets of integers and specific operations that are defined for those sets. The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.

In this chapter, we will define three common algebraic structures: groups, rings, and fields.

GROUPS:

A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms).

A commutative group satisfies an extra property, commutativity:

- **Closure:**
- **Associativity:**
- **Commutativity:**
- **Existence of identity:**
- **Existence of inverse:**

CYCLIC SUBGROUP:

If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

LAGRANGE'S THEOREM:

Assume that G is a group, and H is a subgroup of G. If the order of G and H are |G| and |H|, respectively,

then, based on this theorem, |H| divides |G|.

ORDER OF AN ELEMENT:

The order of an element is the order of the cyclic group it generates.

EXAMPLES:

a. In the group G = $< z_6, + >$ the orders of the elements are:

ord(0) = 1, ord(1) = 6, ord(2) = 3,

ord(3) = 2, ord(4) = 3, ord(5) = 6.

- **b. In the group G =<z_{10^*}, X> ,the orders of the elements are:**

ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

RING :

A ring, R = <{…},·,> is an algebraic structure with two operations.

satisfies all five properties defined for the first operation except that the identity of the first. operation has no inverse.

PERMUTATION GROUPS:

A permutation of a set A is a function from A to A that is both one to one and onto.

THANK YOU

http://www.trinitycollegenkl.edu.in/