Lecture 3 Groups, Rings, Fields

Def. A **group** consists of a set G together with an operation which we will denote $*$ such that the following properties hold:

(Closure) $a,b \in G \Rightarrow a * b \in G$
(Associative Law) $a,b,c \in G \Rightarrow a*(b*c) = (a*b)*c$
(Identity Law) There is an $e \in G$ such that $a \in G \Rightarrow a*e = e*a = a$
(Inverse Law) For each element $a \in G$ there exists an element $a^{-1} \in G$ such that
$a*a^{-1} = a^{-1}*a = e$

G is a called a commutative or abelian group if the follow property also holds
(Commutative Law) $a,b \in G \Rightarrow a*b = b*a$

Ex:
(1) $G = Z$ and * = addition is a commutative group with $e = 0,\ a^{-1} = -a$. This is an infinite group

(2) $G = Z_n$ and * = addition (mod n) is a commutative group with $e = 0,\ a^{-1} = -a$ This is a group of order *n*.

(3) $G = Z_p^*$ with *p* a prime number and * = multiplication (mod p) is a commutative group with $e = 1,\ a^{-1} =$ multiplicative inverse mod *n*. This

(4) $G = Z$ and * = multiplication is not a group (not all elements have inverses).

Def. Let *G* be a group and for $a \in G$ there exists a positive integer *d* which is the smallest positive integer for which $a^d = e$, then *d* is called the **order** of *a*. We say that *a* is an element of finite order.

Thm: Let *G* be a finite group, then every element of *G* has finite order. If $a \in G$ has order *d* and for some integer *k* we have $a^k = e$ then $d \mid k$.

Lagrange's Theorem. If *G* is a finite group and $a \in G$ then the order of *a* divides the order of *G*.

Def: A set *R* is a **ring** if it has two operations +,* such that
(1) R,+ is a commutative group with identity 0
(2) R,* satisfies Closure, Associative Law, Identity, and Commutative Law, with identity 1.
Note: elements need not have multiplicative inverses.
(3) (Distributive Law) $a,b,c \in G \Rightarrow a*(b+c) = (a*b)+(a*c)$

Def: A set F is a **field** if it has two operations +,* such that
(1) F is a ring
(2) All non-zero elements of F have multiplicative inverses.

Ex:
(1) $\boldsymbol{R} = \boldsymbol{Z}$ and usual addition and multiplication is a ring (but not a field)

(2) $\boldsymbol{F} = \boldsymbol{Z}_p = \boldsymbol{F}_p$ with p a prime number and addition and multiplication defined mod p is a field. In particular, it is an example of a finite field.

(3) $\boldsymbol{F} = \boldsymbol{Z}_n$ with n not a prime number and addition and multiplication defined mod n is a ring, but not a field.

The concept of congruence modulo m can be extended to arbitrary rings.

Def: Let R be a ring and let m be a non-zero element of R. We say $\boldsymbol{a,b \in R}$ are **congruent modulo *m*** if $\boldsymbol{m \mid (a-b)}$ and we write $\boldsymbol{a \equiv b \pmod{m}}$.

Def: Let R be a ring and $\boldsymbol{a \in R}$, we define the **congruence class of *a* mod *m*** as the set $\boldsymbol{\overline{a} = \{x \in R \mid\ x \equiv a \pmod{m}\}}$

Def: Let R be a ring and let m be a non-zero element of R. We define the **quotient ring of *r* mod *m*** by $\boldsymbol{R/(m) = R/mR = \{\overline{a} \mid a \in R\}}$