Lecture One

Mathematical Basic Concepts

4. Group Theory

Definition (4.1):

1. $\mathbb{Z}_{>a}$ is the set of positive integers greater than a:

   $\mathbb{Z}_{>a}=\{a+1,a+2,\ldots\}$.

2. the set of all residue classes modulo a positive integer denoted by $\mathbb{Z}_n$:

   $\mathbb{Z}_n=\{0,1,2,\ldots,n-1\}$.

Definition (4.2):A **binary operation** * on a set A is a rule that assign to each ordered pair (a,b) of elements of A a unique element of A.

Example (4.1): Ordinary addition + and multiplication • are binary operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$.

Definition (4.2): A ***group***, denoted by $\langle G,*\rangle$ (or $(G,*)$), or simply G, is a $G\neq\varphi$ of elements together with a binary operation *, s.t. the following axioms are satisfied:

1. ***Closure***: $a*b\in G,\ \forall a,b\in G$.
2. ***Associativity***: $(a*b)*c=a*(b*c),\ \forall a,b,c\in G$.
3. ***Existence of identity***: $\exists!$ element $e\in G$, called the identity, s.t.

   $e*a=a*e=a,\ \forall a\in G$.

4. ***Existence of inverse***: $\forall a\in G$, $\exists!$ Element $b\in G$, s.t.

   $a*b=b*a=e$. This b is denoted by a^{-1} and called the ***inverse*** of a.

The group $\langle G,*\rangle$ is called ***commutative*** (***abelian***) group if it satisfies further axiom:

5. ***Commutativity***: $a*b=b*a, \forall a,b\in G$.

Example (4.2): the set $\mathbb{Z}^+$ with operation + is not group ($\exists$ no identity element), and it's not group with operation • ($\exists$ no inverse element in $\mathbb{Z}^+$).

Definition (4.3):

1. If the binary operation of a group is +, then the identity of group is 0 and the inverse of $a\in G$ is $-a$; this said to be an ***additive group***.
2. If the binary operation of a group is •, then the identity of a group is 1 or e, this group is said to be ***multiplicative group***.

Definition (4.4): A group is called a ***finite group*** if it has finite number of elements; otherwise it is called an ***infinite group***.

Definition (4.5): The ***order*** of the group G, denoted by $|G|$ (or by $\#(G)$) is the number of elements of G.

Example (4.3): the order of $\mathbb{Z}$ is $|\mathbb{Z}|=\infty$.

Definition (4.6): Let $a\in G$, where G is multiplicative group. The elements a^r, where r is an integer, form a subgroup of G, called the ***subgroup*** generated by a. A group G is ***cyclic*** if $\exists$ $a\in G$ s.t. the subgroup generated by a is the whole of G.

Remark (4.1): If G is a finite cyclic group with identity element e, the set of elements G may be written $\{e,a,a^2,\ldots,a^{n-1}\}$, where $a^n=e$ and n is the smallest such positive integer.

<u>Definition (4.7)</u>: A ***field*** by $\langle F,\oplus,\otimes\rangle$ (or $(F,\oplus,\otimes)$) or simply F, is abelian group w.r.t. addition, and F-{0} is abelian w.r.t. to multiplication.

<u>Definition (4.8)</u>: A ***finite field*** is a field that has a finite number of elements in it; we call the number the order of the field.

<u>Theorem (4.1)</u>: $\exists$ a field of order q iff q is ***prime power*** (i.e. $q=p^r$) with p prime and $r\in\mathbb{N}$.

<u>Remark (4.2)</u>: A field of order q with q prime power is called ***Galois field*** and is denoted by GF(q) or just $\mathbb{F}_q$.

<u>Example (4.4)</u>: The finite field $\mathbb{F}_5$ has elements {0,1,2,3,4} and is described by the table(4.1) addition and multiplication table.

Table (4.1) The addition and multiplication for $\mathbb{F}_5$.

$\oplus$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1