Lecture One

Mathematical Basic Concepts

5. Boolean Ring and Boolean Algebra

Definition (5.1): Let $A\neq\varphi$ be a set, f be a binary operation on a set A ($f:A\times A\rightarrow A$), we call the pair (A,f) as **mathematical system**.

Definition (5.2): Let X be the universal set, and let A and B be two subsets of X, then:

1. The operation + defined as $A+b=A\cup B$.
2. The operation $\oplus$ defined on the power P(X) set of X by:

   $A\oplus B=(A-B)\cup(B-A)$ s.t. $A-B=A\cap B'$, B' is the ***complement*** set of B.

   The operation $\oplus$ called ***Exclusive-OR*** (**XOR**) (or the ***symmetric difference***).
3. The operation • defined as $A\bullet B=A\cap B$.

Definition (5.3): Let (R,+,•) be a ring with identity element, if the **Idempotency law** be satisfied $a^2=a$, $\forall a\in R$, then the ring called **Boolean ring**.

Example (5.1): Let P(X) represents the set of all the subsets of the universal set X, then the ring $(P(X),\oplus,\bullet)$ is Boolean ring.

Definition (5.4): In Boolean ring $(B,\oplus,\bullet)$, we defined:

1. **Complement**: $\bar{a}=a\oplus 1$, $\forall a\in B$.
2. **Sum (OR)**: $a+b=a\oplus b\oplus a.b$ $\forall a,b\in B$.

Definition (5.5): The ***Boolean algebra*** is the mathematical system $(B,\vee,\wedge)$ where $B\neq\varphi$, and the binary operations $\vee$ and $\wedge$ defined on B as follows:

1. The operations $\vee$ and $\wedge$ are commutative.
2. The operations $\vee$ and $\wedge$ are satisfy the distribution law for each to other.
3. $\exists$ two identity distinct elements 0 and 1 of the operations $\vee$ and $\wedge$ respectively s.t. $a\vee 0=a$ and $a\wedge 1=a$, $\forall a\in B$.

Example (5.2): The system $(P(X),\bigcup,\bigcap)$ is boolean algebra, $X\neq\varphi$, we use $\varphi=0$ and $X=1$. If B be a set of subsets of X including φ and X which is closed on $\bigcup$ and complement then $(B,\bigcup,\bigcap)$ is boolean algebra too.

Theorem (5.1): Every boolean algebra $(B,\vee,\wedge)$ is boolean ring $(B,\oplus,\bullet)$ when we defined the operations $\oplus$ and $\bullet$ as follows:

1. $a\oplus b=(a\wedge b')\vee(a'\wedge b)$.
2. $a\bullet b=a\wedge b$.

$\forall a,b\in B$.

Theorem (5.2): Every ring $(B,\oplus,\bullet)$ is Boolean algebra $(B,\vee,\wedge)$ when we defined $\vee$ and $\wedge$ as follows: $\forall a,b\in B$.

1. $a\vee b=a\oplus b\oplus a\bullet b$.
2. $a\wedge b=a\bullet b$.

Theorem (5.3): The ring $(\mathbb{Z}_p,\oplus,\otimes)$ is field iff p is prime number s.t.

$a\oplus b=a+b \pmod p$.

$a\otimes b=a\bullet b \pmod p$.

This field is Galois field and is denoted by GF(p), $\forall a,b\in \mathbb{Z}_p$.