Rings

Defn: A ring $(S, +, \cdot)$ is a set S with two binary operations $+$ and $\cdot$ defined on S such that

1) $(S, +)$ is a commutative group
2) The multiplication operation $\cdot$ is associative
   i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in S$
3) The left and right distributive laws hold
   i.e., $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(a + b) \cdot c = (a \cdot c) + (b c)$

— A ring is said to be a commutative ring if $a \cdot b = b \cdot a$ for every $a, b \in R$

— A ring is said to be a ring with identity if $\cdot$ has an identity element. This is typically denoted as 1_R

Notes — Notice that we do not require that the multiplication operation form a group. There may not be multiplicative inverses in a ring (even it has an identity). Nor is the multiplication operation necessarily commutative.

(2) Some of the elements of a ring may have a multiplicative inverse. An element "a" in a ring having a multiplicative inverse is said to be a unit

Ex: The set of 2×2 matrices under usual definitions of addition and multiplication form a ring. This ring is not commutative, nor does every element have an inverse

Ex: $S = \{0, 1, 2, 3, 4, 5\}$. $+ \longrightarrow$ mod 6 addition
$\cdot \longrightarrow$ mod 6 multiplication

$(S, +, \cdot)$ form a ring

Rings of Polynomials:

Let S be a ring

A polynomial $f(x)$ of degree n with coefficients in S is

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{where } a_n \neq 0$$

The symbol x is said to be an indeterminate

Defn: The set of all polynomials with an indeterminate x with coefficients in a ring S, using the usual operations for polynomial addition and multiplication, forms a ring called the polynomial ring. It is denoted as $R[x]$

3) Ex:

$S = \{0,1,2,3,4,5\}$ $+ \rightarrow$ mod 6 addition, $\cdot \rightarrow$ mod 6 multiplication

$R_6[x] \rightarrow$ polynomial ring

Some elements in $R[x]$ are

$0, 1, x, 1+x, 4+2x, 5+4x, 3+x^2$, etc.

Ex: $R_2[x]$ is the ring of polynomials with coefficients that are either 0 or 1 with operations modulo 2.

$1+x$, $1+x^2$ are some elements of $R_2[x]$

The convolution of the sequence

$\bar{a} = [a_0\ a_1\ a_2 \dots a_n]$

with the sequence

$\bar{b} = [b_0\ b_1 \dots b_m]$

can be accomplished by forming the polynomials

$a(x) = a_0 + a_1x + \dots + a_nx^n$

$b(x) = b_0 + b_1x + \dots + b_mx^m$

and multiplying them

$c(x) = a(x)\,b(x)$

then the coefficients of

$c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n+m}x^{n+m}$

are equal to the values obtained by convolving $\bar{a}$ & $\bar{b}$