Rings and Fields

A ring R is a set with 2 operations $+, \cdot$ satisfying the following properties:

(1) $(R, +)$ is an Abelian Group.

(2) $\cdot$ is commutative, associative and has an identity element (1).

(3) $(a+b)\cdot c = (a\cdot c)+(b\cdot c) \quad \forall\, a, b, c \in R$.

A ring S is called the subring R if $S \subseteq R$ and S contains 1 of R.

Polynomial Rings

$R[x]$ represents all the set of polynomials over R

$R[x] = \{ a_n x^n + \cdots + a_1 x + a_0 \mid n \in \mathbb{N}$ and

$a_n, \ldots, a_0 \in R \}$

Let $f = a_n x^n + \cdots a_1 x + a_0$ and

$g = b_n x^n + \cdots + b_1 x + b_0$

where $a_n, \ldots, a_0 \in R$ and $b_n, \ldots, b_0 \in R$.

$\Rightarrow f + g = (a_n + b_n) x^n + \cdots + (a_0 + b_0)$ where

$(a_n + b_n), \ldots, (a_0 + b_0) \in R$.

Thus $R[x]$ is an Abelian Group under $+$.

$f \cdot g = p_{m+n} x^{m+n} + \cdots + p_0$ where

$$p_k = \sum_{i+j=k} a_i b_j \,, \quad 0 \leq k \leq (m+n).$$

- for polynomials $R[x]$ is commutative, associative and has identity element 1.

Also the distributive property holds.

$R[x]$ is thus a ring with the above defined $+$ and $\cdot$, called the polynomial ring.

All constant polynomials $(n=0)$ of $R[x]$ together form R. R is thus a subring of $R[x]$

$$R = \{a_0 \mid a_0 \in R[x]\}$$

Let $f, g \in R[x]$ where $f(x)$ is a monic polynomial $(a_n = 1)$. There exists unique $q(x)$ and $r(x)$ such that

$$g(x) = q(x) \cdot f(x) + r(x)$$

$\rightarrow$ Let $g(x) \in R[x]$ and $\alpha \in R$.

$(x - \alpha)$ is a monic polynomial

$$g(x) = q(x) \cdot (x - \alpha) + r(x)$$

Consider the case $\deg\{r(x)\} < \deg\{(x-a)\} = 1$

$$\Rightarrow \deg\{r(x)\} = 0$$

$r(x)$ is thus a constant. When $x = a$

$$g(a) = q(a)(a-a) + r(a)$$

$$\Rightarrow r(a) = g(a)$$

$$\Rightarrow r(x) = g(a)$$