RING OF POLYNOMIALS

Ring of polynomials

Definition 1. *Let A be a commutative ring , and x an arbitrary symbol. Every expression of the form*

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

is called a polynomial in x with coefficients in A, or more simply, a polynomial in x over **A**. *The expressions $a_k x^k$, for $k \in \{1, \ldots, n\}$, are called the terms of the polynomial, and a_k is called the coefficient of x^k. Polynomials in x are designated by symbols such as $p(x), b(x), q(x), f(x), g(x)$ and the set of polynomials in x are designated by $A[x]$.*

Definition 2. *The polynomial $p(x) = a_0$ is called a constant polynomial. If $a_0 = 0$ then p is the zero polynomial, denoted by 0 or 0_x . We can also say that $p(x) = a_i x^i$ for $i \geq 1$ is a monomial.*

Examples

1- $2 + 3x + 7x^2$ is a polynomial with coefficients in $\mathbb{Z}$.

2- $2 + \sqrt{3}x + 7x^2$ is a polynomial with coefficients in $\mathbb{R}$.

Proposition 1. *Let A be a field (or ring). Let p and$q \in A[x]$, such that: $p(x) = \sum\limits_{n=0}^{k} a_n x^n$, $q(x) = \sum\limits_{n=0}^{m} b_n x^n$. We define the following two binary operations:*

$$\begin{aligned}(p+q)(x) &= \sum_{n=0}^{max(k,m)} (a_n + b_n)x^n \\ (pq)(x) &= \sum_{n=0}^{k+m} c_n x^n, where c_n = \sum_{i+j=n} a_i b_j.\end{aligned}$$

The set $A[x]$ equipped by these two binary operations is a ring . (exercise)

Example 1. $\mathbb{Z}[x]$, $\mathbb{R}[x]$ *and* $\mathbb{C}[x]$ *are rings.*

1.1. The degree of a polynomial.

Definition 3. *Let A be a commutative ring, and let $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial in $A[x]$. The degree of $p(x)$, $deg(p)$, is the largest $k \geq 0$, such that $a_k \neq 0$. The non zero coefficient a_k is known as the leading coefficient and a_kx^k is called the leading term.*

Remarks

- If the polynomial p is nonzero constant i.e, $p(x) = a_0$ then $deg(p) = 0$.
- If the polynomial p is zero i.e, $p(x) = 0$ then by convention $deg(p) = -\infty$.

Proposition 2. *Let A be a field, then $\forall\ p, q \in A[x]$-$\{0\}$, we have:*

$$\begin{aligned} \deg(p+q) &\leq max(\deg(p), \deg(q)), \\ \deg(pq) &= \deg(p) + \deg(q). \end{aligned}$$

Definition 4. *The polynomial $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ of degree n is called the monic polynomial when $a_n = 1$.*

Example

The polynomial $4 + 2x - x^2 - 2x^3$ is of degree 3, it is not monic polynomial.
The polynomial $x^5 - 6x + 1$ is a monic polynomial of degree 5.

Notation

-In the following F design the field $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.
-We denote by $F_n[X]$ the set of polynomials of a coefficients in F of degree $\leq n$.

2. Euclidean division,

Theorem 1. *Let F be a field and let f and g be polynomials in $F[x]$, with $g \neq 0_x$. Then there exist unique polynomials q and r in $F[x]$ such that*

(a) $\deg(r) < \deg(g)$, *and*

(b) $f = qg + r$.

Polynomials q and r are, respectively, known as the quotient and remainder when dividing f by g.

Examples

1- Let $A = \mathbb{R}$ and $f(x) = x^2 + 3x - 1, g(x) = x - 1$ then $q(x) = x + 4, g(x) = 3$

2- For each of the following polynomials $f(x), g(x)$ in $\mathbb{Q}[x]$, find the quotient $q(x)$ and the remainder $r(x)$ for the division of $f(x)$ by $g(x)$.

(a) $f(x) = x^3 - 2x^2 + 3x - 1, g(x) = x - 1$

(b) $f(x) = 2x^4 - x + 1, g(x) = x^2 + 1$

(c) $f(x) = 3x^3 - 2x^2 + 1, g(x) = 2x + 1$

Definition 5. *Let F be a field and let f and g be polynomials in $F[x]$, with $g \neq 0$. Then we say that g divides f (written $g \mid f$) if r is the zero polynomial or if there exists a polynomial q in $F[x]$ such that $f = qg$.*

Properties

Let F be a field, and let f, g and h be non-zero polynomials in $F[x]$. Prove the following statements.

(a) If g divides f then g divides $f + gh$ for any polynomial $h \in F[x]$.

(b) If h divides g and g divides f then h divides f.

(c) If h divides f and h divides g then h divides $af + bg$ for any polynomials $a, b \in F[x]$.

(d) Polynomials f and g are associates if and only if, g divides f and f divides g.

Examples

(a) $g(x) = x - 1$ divides $f(x) = x^3 - 2x^2 + 1$

(b) $f(x) = 2x^2 + 1$ and $g(x) = 10x^2 + 5$ are associates.

2.2. Derivative of a polynomial.

Definition 6. *The derivative of the polynomial*

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x],$$

is the polynomial $p'(x) \in F[x]$ given by

$$p'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

The derivative of order k of the polynomial $p(x)$, denoted by $p^{(k)}(x)$, where k is a non negative integer, is given by the following recurrence relation

$$p^{(0)} = p \text{ and } p^{(k+1)} = \left(p^{(k)}\right)' \text{ for } k \geq 0.$$

Root of a polynomial

Definition 7. *Let $p(x) = \sum_{n=0}^{N} a_n x^n \in F[x]$ be a polynomial. We say that z_0 is a root of p if $p(z_0) = 0$ which is equivalent to $(x - z_0)$ divides p.*

Definition 8. *Let $p \in K[x]$ and let α be a root of p. The multiplicity of the root α is the integer $k \geq 1$ verifying*

$$p(x) = (x-\alpha)^k q(x), q \in K[x] \text{ and } q(\alpha) \neq 0.$$

When $k = 1$ (resp. $k = 2, k = 3$), we say that α is a simple (resp. double, triple) root.

Example

Let $p(x) = x^3 - 3x - 2 \in \mathbb{R}[x]$. We have

$$p(x) = (x+1)^2(x-2),$$

Then -1 is a double root and 2 is a simple root.

Proposition 3.
(1) *If $z_1, \ldots, z_p$ are distinct roots of p, then $(x-z_1), \ldots, (x-z_p)$ divides p.*
(2) *A polynomial of degree $n \geq 0$ admits at most n roots.*
(3) *We say that z is a root of p of multiplicity $k \geq 0$ if $p(z) = p'(z) = \cdots = p^{(k-1)}(z) = 0$ and $p^{(k)}(z) \neq 0$, (where$p^{(k)}$ is the derivative of the order k of p).*

Theorem 4. *Let $p \in F[x]$, $z \in F$ and $k \in \mathbb{N}$. Then we have z is root of multiplicity k of p if and only if $(x-z), \ldots, (x-z)^k$ divides p, and $(x-z)^{k+1}$ does not divide p.*

Theorem 5. *Any polynomial of $\mathbb{C}[x]$ non-constant admits a root in $\mathbb{C}$.*

Theorem 6. *If z is a root of a polynomial $p \in \mathbb{R}[x]$ then its conjugate is a root of p $\mathbb{C}$.*

3. Factoring a polynomial over $\mathbb{R}$ and $\mathbb{C}$

Let F be a field, factoring a polynomial f in $F[x]$ means writing it as a product of polynomials of degree less than to the degree of f.

Polynomial irreducible

Definition 9. *Let $p \in F[x]$. We say that p is irreducible in $F[x]$ if all the divisors of p are the constant and the associated polynomial .*

Examples

A polynomial $p(x) = x^2 + 3$ is irreducible in $\mathbb{R}[x]$ and is not irreducible in $\mathbb{C}[x]$.

Remark

1) A polynomial that is not irreducible is called reducible.

2) The irreducible polynomials in $\mathbb{C}[x]$ are the polynomials of degree 1.

3)The polynomial irreducible in $\mathbb{R}[x]$ are the polynomials of degree 1 or the polynomials of degree 2 , $(ax^2 + bx + c)$ with $b^2 - 4ac < 0$.

Decomposition into product of irreducible in $\mathbb{C}[x]$

The irreducible polynomials of $\mathbb{C}[x]$ are the polynomials of degree 1, and any polynomial $p \in \mathbb{C}[x]$ non-constant is factorized as follows

$$p(x) = a_r \prod_{k=1}^{N} (x - z_k)^{\eta_k}$$

where $z_1, \ldots, z_N$ are the distinct roots of p in $\mathbb{C}$ of respective multiplicities $\eta_1, \ldots, \eta_N$.

Decomposition into product of irreducible in $\mathbb{R}[x]$

The irreducible polynomials of $\mathbb{R}[x]$ are the polynomials of degree 1 or degree 2 of strictly negative discriminant. Any polynomial $p \in \mathbb{R}[x]$ non-constant is factorized as follows:

$$p(x) = a_r \prod_{k=1}^{N} (x - z_k)^{\eta_k} \prod_{k=1}^{s} (x^2 + \beta_k x + \gamma_k)^{\nu_k}$$

where $z_1, \ldots, z_N$ are the distinct roots of p in $\mathbb{R}$ of respective multiplicities $\eta_1, \ldots, \eta_N$, with $\beta_k^2 - 4\gamma_k < 0$ for each $k \in \{1, ..., s\}$.

Definition 10. *A polynomial $p \in F[x]$ of degree N is said to be split if it factors as follows*

$$P(x) = a_N \prod_{j=1}^{N} (x - z_j).$$

Example

Let $p(x) = 5x^3 - 15x - 10 \in \mathbb{R}[x]$, p is split polynomial because

$$p(x) = 5(x+1)^3(x-2).$$

On the other hand, the polynomial $q(x) = x^2 + 1$ is not split, because it cannot be expressed as the product of two polynomials of degree 1 .

3.1. Greatest common divisor (Highest common factor) of two polynomials.

Definition 11. *Let F be a field, and f, g two polynomials in $F[x]$, not both equal to 0_x. Then the greatest common divisor of f and g, written gcd (f, g), is a monic polynomial of largest degree satisfying the following:*

(a) gcd (f, g) divides both f and g.

(b) Any polynomial $d \in F[x]$ that divides both f and g must also divide $\gcd(f, g)$.

Theorem 7. *Let F be a field, and f, g two polynomials in $F[x]$, not both equal to 0_x. Then* $\gcd(f, g)$ *is unique, and there exist polynomials $a, b \in F[x]$ such that*

$$\gcd(f, g) = af + bg.$$

Definition 12. *Let F be a field, and let f, g be polynomials in $F[x]$, not both equal to 0_x. If $\gcd(f, g) = 1_x$ then we say that f and g are coprime.*

Lemma 1. *(Bézout) The polynomials $f, g \in F[x]$, not both equal to 0_x, are coprime if, and only if, there exist polynomials $a, b \in F[x]$ such that $af + bg = 1_x$.*

Lemma 2. *Let F be a field, and let f, g and h be polynomials in $F[x]$.*

(a) If $\gcd(f, g) = 1_x$ *and both f and g divide h, then fg divides h.*

(b) If f divides gh and $\gcd(f, g) = 1_x$, *then f divides h.*

3.2. **The Euclidean Algorithm.** In this subsection, we will see how to apply the Division Algorithm to carry out practical calculation of the greatest common divisor.

Given a field F, and two polynomials $f, g \in F[x]$, not both equal to 0_x, let $f^* = f$ and $g^* = g$.

1. Apply the division Algorithm to f^*, g^* to find $q, r \in F[x]$ for which $f^* = qg^* + r$.
2. If $r = 0_x$ then stop: $\gcd(f, g) = a^{-1}g^*$, where $a \in F$ is the coefficient of the highest power of x in g^*.
3. Otherwise, $r \neq 0_x$. Replace f^* by g^*, and g^* by r, and go back to step 1.

Example

Let's apply the Euclidean algorithm to find the GCD of the polynomials:

$$A(x) = x^3 - 2x^2 + x - 2$$

$$B(x) = x^2 + x - 1$$