Chapter 5

Polynomials ring

This chapter is depicted to the feild of polynomials, essential tools in various mathematical computations and applications. We'll explore the nature of polynomials, their degrees, roots, and properties within the context of polynomial rings.

5.1 Construction of polynomials ring

A polynomial with coefficients in $\mathbb{K}$ (ring) is defined as a finite sequence $(a_0, ..., a_n)$ of elements from $\mathbb{K}$. We denote this polynomial as $\sum_{n\geq 0} a_n X^n$, where X is referred to as the indeterminate. We denote $\mathbb{K}[X]$ as the set of polynomials with coefficients in $\mathbb{K}$.
We define the following operations on $\mathbb{K}[X]$: If $P(X) = \sum_{n\geq 0} a_n X^n$ and $Q(X) = \sum_{n\geq 0} b_n X^n$ (where the sequences (a_n) and (b_n) are zero from a certain rank), then we have:

$$(P+Q)(X) = \sum_{n\geq 0} (a_n + b_n) X^n,$$

and

$$(PQ)(X) = \sum_{n\geq 0} c_n X^n, \ where \ c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

These two operations make $\mathbb{K}[X]$ into a ring. Let A and B be in $\mathbb{K}[X]$, with $B = \sum_{n=0}^{N} b_n X^n$. Then, the composition of A by B in the polynomial ring $\mathbb{K}[X]$ is given as:

$$B \circ A = \sum_{n=0}^{N} b_n A^n.$$

5.2 Polynomial squares, degree and multiplicity

If $P = \sum_{n\geq 0} a_n X^n$ is not zero, there exists a larger index $n \in \mathbb{N}$ such that $a_n \neq 0$. This integer is called the degree of P, denoted $deg(P)$. The corresponding coefficient is called the leading coefficient of P. By convention, if P is zero, its degree is $-\infty$. A polynomial with a leading coefficient equal to 1 is called unitary (monic).
For all non-zero polynomials $P, Q \in \mathbb{K}[X]$, where $\mathbb{K}$ is an integral domain, we have

$$deg(P+Q) \leq max(deg(P), deg(Q)),$$

$$deg(PQ) \leq deg(P) + deg(Q),$$

Example 5.2.1. *$P(x) = 3x^2 + 4x - 2$ is a degree two polynomial in the ring $\mathbb{Z}_4[x]$, $Q(x) = x^3 - 2x + 3$ is of a degree three polynomial in the ring $\mathbb{R}[x]$.*

Example 5.2.2. *Consider $P(x) = 2x = 1$ and $Q(x) = 2x$, P and Q are of degree 1 polynomials in the ring $\mathbb{Z}_4[x]$,*
$deg(PQ) = deg(2x(2x+1)) = deg(2x) = 1$, and $deg(P) + deg(Q) = 2$.

Let $\mathbb{K}$ represents the field $\mathbb{R}$ or $\mathbb{C}$.
Derivation: For$P = \sum_{n\geq 0} a_n X^n$k, $P' = \sum_{n\geq 1} n a_n X^{n-1}$, called the derivative polynomial of P. If $deg(P) \geq 1$, then $deg(P') = deg(P) - 1$.
Leibniz's Formula: For$P, Q \in \mathbb{K}[X]$ and $n \in \mathbb{N}$, we have

$$(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Taylor's Formula: Let P be in $\mathbb{K}[X]$ and $a \in \mathbb{K}$. Then

$$P(X) = \sum_{n \geq 0} \frac{P^{(n)(a)}}{n!}(X-a)^n.$$

Divisibility, Euclidean Division: Let $A, B \in \mathbb{K}[X]$ with B nonzero polynomial. We say that B divides A if there exists $Q \in \mathbb{K}[X]$ such that $A = BQ$. We also say that B is a divisor of A or that A is a multiple of B.

Two nonzero polynomials A and B in $\mathbb{K}[X]$ are said to be associated if A divides B and B divides A. This is equivalent to saying that there exists $\lambda \in \mathbb{K}^*$ such that $A = \lambda B$.

Theorem 5.2.3. *(Euclidean Division of Polynomials). Let A, B be in $\mathbb{K}[X]$ with B nonzero polynomial. There exists a unique pair $(Q, R) \in \mathbb{K}[X]$ such that*

$$A = BQ + R \text{ and } deg(R) < deg(B).$$

Example 5.2.4. *The quotient and remainder on dividing $f(X) = X^5 - X^2 + 2$ by $g(X) = X^2 + 1$ in the following case are:*
$Q(X) = X^3 - X - 1$ and $R(X) = X + 3$.

Remark 5.2.5.

- *A polynomial $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{K}[X]$ defines a polynomial function $\widetilde{P} : K \to K$ as $\widetilde{P}(z) = \sum_{n=0}^{N} a_n z^n$. Often, we identify a polynomial with a polynomial function.*

- *We say that a is a root of P if $P(a) = 0$. This is equivalent to saying that $(X - a)$ divides P.*

- *In general, the rest of the Eucledian division of a polynomial $P(X)$ by $(X - a)$ is $P(a)$.*

Proposition 5.2.6. *If $a_1, ..., a_n$ are distinct roots of P, then $(X - a_1), ..., (X - a_n)$ divide P. A polynomial of degree n has at most n roots.*

Proposition 5.2.7. *Let P be in $\mathbb{K}[X]$, let $a \in \mathbb{K}$, and let $m \in \mathbb{N}$. We say that a is a root of multiplicity m if $P(a) = P'(a) = ... = P^{(m-1)}(a) = 0$ and $P^{(m)}(a) \neq 0$.*

Theorem 5.2.8. *Let $P \in \mathbb{K}[X]$, let $a \in \mathbb{K}$, and let $m \in \mathbb{N}$. The following statements are equivalent:*

1. *a is a root of P with multiplicity m.*

2. *$(X-a), ..., (X-a)^m$ divide P, and $(X-a)^{m+1}$ does not divide P.*

Definition 5.2.9. *A polynomial $P(x)$ of degree N is said to be factored if it can be expressed as follows:*

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

5.3 Arithmetics of polynomials

In terms of polynomial arithmetic, if A and B are non-zero polynomials in $\mathbb{K}[X]$, each common divisor of A and B of maximal degree is called the GCD of A and B.
We say that A and B are coprime if $A \wedge B = 1$.

Theorem 5.3.1. *(Bezout theorem) Let $A, B \in \mathbb{K}[X]$ be non-zero. Then $A \wedge B = 1$ if and only if there exist $U, V \in \mathbb{K}[X]$ such that $AU + BV = 1$.*

Lemma 5.3.2. *(Gauss lemma) Let $A, B, C \in \mathbb{K}[X]$ be non-zero. We assume $A \wedge B = 1$. Then if $A|BC$, we have $A|C$.*

Remark 5.3.3. *Let A, B be non-zero elements in $\mathbb{K}[X]$. Any common multiple of A and B with minimal degree is called the least common multiple (LCM) of A and B. All LCMs of A and B are associated. In particular, only one is unitary, sometimes referred to as the LCM of A and B. It's denoted as $A \vee B$.*

5.3.1 Irreducible Polynomials

Theorem 5.3.4. *d'Alembert-Gauss's Theorem: Every non-constant polynomial in $\mathbb{C}[X]$ has a root in $\mathbb{C}$.*

Therefore, every non-constant polynomial in $\mathbb{C}[X]$ is factorable.

A polynomial $P \in \mathbb{K}[X]$ is irreducible if it's of degree greater than or equal to 1, and if all its divisors are constant polynomials or polynomials associated with P (meaning the polynomials of the form λP where $\lambda \in \mathbb{K}$).

5.3.2 Decomposition into irreducible factors over $\mathbb{C}[X]$

The irreducible polynomials of $\mathbb{C}[X]$ are polynomials of degree 1.

Every non-zero polynomial is a product of its leading coefficient and unitary irreducible polynomials. This decomposition is unique up to the order of terms.

In particular, every non-constant polynomial P in $\mathbb{C}[X]$ factors into:

$$P(x) = a_N \prod_{k=1}^{r} (X - x_k)^{\nu_k}$$

where $x_1, x_2, ..., x_r$ are the distinct roots of P in $\mathbb{C}$ with respective multiplicities $\nu_1, \nu_2, ..., \nu_r$.

Corollary 5.3.5. *Let $A, B \in \mathbb{K}[X]$ with B non-zero. Then B divides A if and only if all the roots of B are roots of A, and their multiplicity as roots of A is greater than or equal to their multiplicity as roots of B.*

In particular, two non-zero polynomials in $\mathbb{C}[X]$ are coprime if and only if they have no common roots.