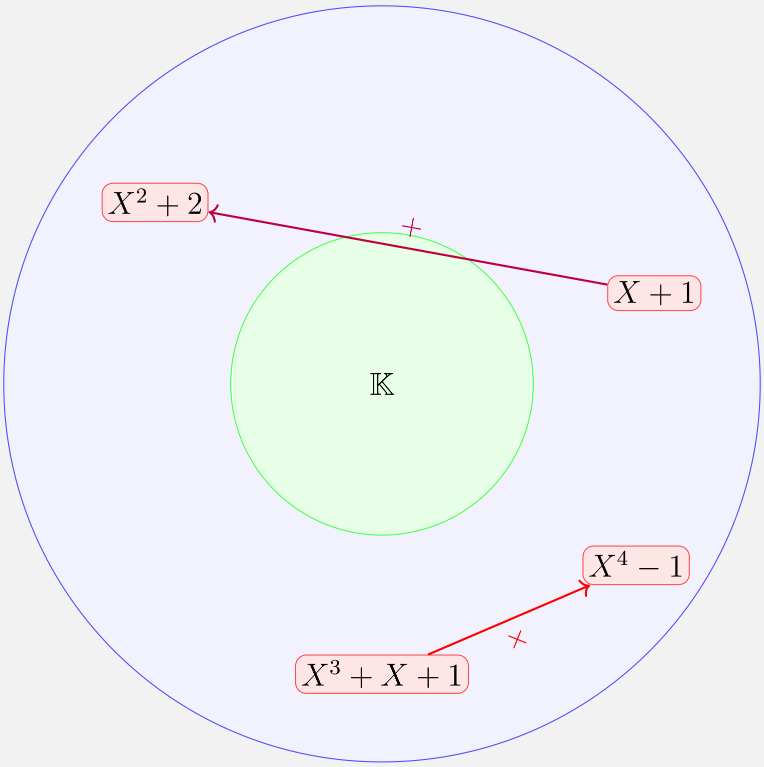
Faculty of Mathematics and Computer Science

Department of Mathematics

Chapter 05: Polynomial Rings

By: Brahimi Mahmoud



$\mathbb{K}[X]$ contains all polynomials with coefficients in $\mathbb{K}$

Academic Year 2024/2025

1 Polynomial

In this chapter, $\mathbb{K}$ will designate one of the fields $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.

Definition

A polynomial with coefficients in $\mathbb{K}$ is an expression of the form

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0,$$

with $n \in \mathbb{N}$ and $a_n, a_{n-1}, \ldots, a_2, a_1, a_0 \in \mathbb{K}$.

Remark

1. The set of polynomials is denoted $\mathbb{K}[X]$.
2. The elements a_i are called the coefficients of the polynomial.
3. If all the coefficients a_i are zero, P is called the zero polynomial, denoted by 0.
4. We call the degree of P the largest integer i such that $a_i \neq 0$.
5. The degree of the null polynomial is denoted, by convention, $\deg(0) = -\infty$.
6. A polynomial of the form $P = a_0$ with $a_0 \in \mathbb{K}$ is called a constant polynomial. If $a_0 \neq 0$, its degree is 0.

Example

- $X^4 - 4X^3 + X^2 + 1$ is a polynomial of degree 4.
- $X^n + 5$ is a polynomial of degree n.
- 3 is a constant polynomial of degree 0.

1.1 Operations on Polynomials

1. Equality. Let

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

and

$$Q(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_2 X^2 + b_1 X + b_0$$

be two polynomials with coefficients in $\mathbb{K}$. Then

$$P(X) = Q(X) \iff \forall i,\ a_i = b_i.$$

In this case, we say that P and Q are equal.

2. Addition. The polynomial $P + Q$ is defined by

$$P+Q = (a_n+b_n)X^n+(a_{n-1}+b_{n-1})X^{n-1}+\cdots+(a_2+b_2)X^2+(a_1+b_1)X+(a_0+b_0).$$

3. Multiplication. Let

$$P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

and

$$Q(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0.$$

The polynomial $P \times Q$ is defined by

$$P \times Q = c_rX^r + c_{r-1}X^{r-1} + \cdots + c_1X + c_0,$$

where $r = n + m$ and

$$c_k = \sum_{i+j=k} a_ib_j, \quad \text{for } k \in \{0, \ldots, r\}.$$

4. Multiplication by a Scalar. If $\lambda \in \mathbb{K}$, then $\lambda \cdot P$ is the polynomial whose i-th coefficient is λa_i.

2 Construction of the Polynomial Ring

Proposition

For $P, Q, R \in \mathbb{K}[X]$, the following properties hold:

$$0 + P = P, \quad P + Q = Q + P, \quad (P + Q) + R = P + (Q + R), \quad P + (-P) = 0,$$

$$1 \cdot P = P, \quad P \times Q = Q \times P, \quad (P \times Q) \times R = P \times (Q \times R),$$

$$P \times (Q + R) = P \times Q + P \times R.$$

Proposition

Let P and Q be two polynomials with coefficients in $\mathbb{K}$. Then

$$\deg(P \times Q) \leq \deg P + \deg Q, \quad \text{and} \quad \deg(P + Q) \leq \max(\deg P, \deg Q).$$

We denote

$$\mathbb{R}_n[X] = \{\, P \in \mathbb{R}[X] \mid \deg P \leq n \,\}.$$

If $P, Q \in \mathbb{R}_n[X]$, then $P + Q \in \mathbb{R}_n[X]$.

Definition

Polynomials with only one non-zero term (of the form $a_k X^k$) are called monomials.
Let
$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$
be a polynomial with $a_n \neq 0$. We call the term $a_n X^n$ the dominant term of P. The coefficient a_n is called the dominant coefficient of P.
If the dominant coefficient is 1, we say that P is a unitary polynomial.

3 Polynomial Arithmetic

3.1 Euclidean Division

Definition

Let $A, B \in \mathbb{K}[X]$. We say that B divides A if there exists $Q \in \mathbb{K}[X]$ such that
$$A = BQ.$$
We then write $B \mid A$.

We also say that A is a multiple of B, or that A is divisible by B.
Besides the obvious properties such as $A \mid A$, $1 \mid A$, and $A \mid 0$, we have the following:

Proposition

Let $A, B, C \in \mathbb{K}[X]$. Then:

(i) If $A \mid B$ and $B \mid A$, then there exists $\lambda \in \mathbb{K}^*$ such that $A = \lambda B$.

(ii) If $A \mid B$ and $B \mid C$, then $A \mid C$.

(iii) If $C \mid A$ and $C \mid B$, then $C \mid (AU + BV) \quad \forall U, V \in \mathbb{K}[X]$.

3.2 Euclidean Division of Polynomials

Theorem

Let $A, B \in \mathbb{K}[X]$, with $B \neq 0$. Then there exist unique polynomials Q and R such that
$$A = BQ + R, \quad \text{and} \quad \deg R < \deg B.$$

Remark

- Q is called the quotient and R the remainder, and this expression is called the Euclidean division of A by B.
- The condition $\deg R < \deg B$ means that $R = 0$ or $0 \leq \deg R < \deg B$.
- $R = 0$ if and only if $B \mid A$.

Example

- If
$$A = 2X^4 - X^3 - 2X^2 + 3X - 1 \quad \text{and} \quad B = X^2 - X + 1,$$
then we find
$$Q = 2X^2 + X - 3 \quad \text{and} \quad R = -X + 2.$$
- If
$$A = X^4 - 3X^3 - 2X^2 + X + 1 \quad \text{and} \quad B = X^2 + 2,$$
then we find
$$Q = X^2 - 3X - 2 \quad \text{and} \quad R = 7X + 5.$$

3.3 Greatest Common Divisor (gcd)

Proposition

Let $A, B \in \mathbb{K}[X]$, with $A \neq 0$ or $B \neq 0$. There exists a unique unit polynomial of greatest degree which divides both A and B. This unique polynomial is called the greatest common divisor (gcd) of A and B, denoted by

$$\gcd(A, B).$$

Remark

- $\gcd(A, B)$ is a unit polynomial.
- If $A \mid B$ and $A \neq 0$, then $\gcd(A, B) = \lambda A$, where λ is the dominant coefficient of A.
- For all $\lambda \in \mathbb{K}^*$, $\gcd(\lambda A, B) = \gcd(A, B)$.
- As for integers: if $A = BQ + R$, then
$$\gcd(A, B) = \gcd(B, R),$$
which justifies Euclid's algorithm for polynomials.

3.4 Euclid's Algorithm

Let A and B be polynomials with $B \neq 0$. We calculate the successive Euclidean divisions as follows:

$$\begin{aligned}
A &= BQ_1 + R_1, && \deg R_1 < \deg B, \\
B &= R_1Q_2 + R_2, && \deg R_2 < \deg R_1, \\
R_1 &= R_2Q_3 + R_3, && \deg R_3 < \deg R_2, \\
&\ \vdots \\
R_{k-2} &= R_{k-1}Q_k + R_k, && \deg R_k < \deg R_{k-1}, \\
R_{k-1} &= R_kQ_{k+1}.
\end{aligned}$$

The degree of the remainder decreases with each division. The algorithm is stopped when the remainder is zero. The greatest common divisor is the last non-zero remainder R_k.

Example

Let's calculate the gcd of

$$A = X^4 - 1 \quad \text{and} \quad B = X^3 - 1.$$

We apply Euclid's algorithm:

$$X^4 - 1 = X(X^3 - 1) + (X - 1),$$

$$X^3 - 1 = (X^2 + X + 1)(X - 1) + 0.$$

The gcd is the last non-zero remainder, so

$$\gcd(X^4 - 1, X^3 - 1) = X - 1.$$

Definition

Let $A, B \in \mathbb{K}[X]$. We say that A and B are coprime if

$$\gcd(A, B) = 1.$$

Example

Let

$$A = X^3 + X^2 + X + 1, \quad B = X^2 + X + 1.$$

These polynomials are coprime.

Remark

For any polynomials A, B, we can reduce them to coprime polynomials: If $\gcd(A, B) = D$, then A and B can be written as

$$A = DA', \quad B = DB',$$

with $\gcd(A', B') = 1$.

3.5 Bézout's Theorem

Theorem

Let $A, B \in \mathbb{K}[X]$ be polynomials such that $A \neq 0$ or $B \neq 0$. Let $D = \gcd(A, B)$. Then there exist polynomials $U, V \in \mathbb{K}[X]$ such that

$$AU + BV = D.$$

This theorem follows from Euclid's algorithm and, more specifically, from its **ascent** procedure, as illustrated in the following example.

Example

We have

$$\gcd(X^4 - 1, X^3 - 1) = X - 1$$

and

$$X^4 - 1 = X(X^3 - 1) + (X - 1) \quad \Longrightarrow \quad 1 \cdot (X^4 - 1) - X \cdot (X^3 - 1) = X - 1.$$

Hence, we can take

$$U = 1, \quad V = -X.$$

Corollary

Let A and B be two polynomials. A and B are coprime if and only if there exist polynomials U and V such that

$$AU + BV = 1.$$

Example

Let

$$A = X^3 + X^2 + X + 1, \quad B = X^2 + X + 1.$$

These polynomials are coprime because

$$X^3 + X^2 + X + 1 = X(X^2 + X + 1) + 1 \quad \Longrightarrow \quad A = XB + 1,$$

and hence

$$A \cdot 1 + B \cdot (-X) = 1.$$

Corollary

Let $A, B, C \in \mathbb{K}[X]$ be polynomials such that $A \neq 0$ or $B \neq 0$. If $C \mid A$ and $C \mid B$, then

$$C \mid \gcd(A, B).$$

3.6 Gauss Lemma

Corollary

Let $A, B, C \in \mathbb{K}[X]$. If $A \mid BC$ and $\gcd(A, B) = 1$, then

$$A \mid C.$$

3.7 Least common multiple (lcm)

Definition

Let $A, B \in \mathbb{K}[X]$ be non-zero polynomials. Then there exists a unique unitary polynomial M of minimal degree such that

$$A \mid M \quad \text{and} \quad B \mid M.$$

This unique polynomial is called the least common multiple (lcm) of A and B, denoted by

$$\operatorname{lcm}(A, B).$$

Example

$$\operatorname{lcm}\big(X(X-2)^2(X^2+1)^4,\ (X+1)(X-2)^3(X^2+1)^3\big) = X(X+1)(X-2)^3(X^2+1)^4.$$

Proposition

Let $A, B \in \mathbb{K}[X]$ be non-zero polynomials, and let

$$M = \operatorname{lcm}(A, B).$$

If $C \in \mathbb{K}[X]$ is a polynomial such that

$$A \mid C \quad \text{and} \quad B \mid C,$$

then

$$M \mid C.$$

4 Roots of a Polynomial

4.1 Roots and degree

Definition

Let
$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{K}[X],$$
and let $\alpha \in \mathbb{K}$. For $x \in \mathbb{K}$, we denote
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$
We say that α is a root (or zero) of P if
$$P(\alpha) = 0.$$

Example

$\alpha = 3$ is a root of
$$P(x) = x^2 - 5x + 6$$
because
$$P(3) = 0.$$

Proposition

$$P(\alpha) = 0 \iff X - \alpha \mid P.$$

Example

Let
$$P(x) = x^3 + 5x^2 + 3x - 9.$$
Since
$$P(-3) = 0,$$
it follows that $x + 3$ divides $P(x)$. Indeed, we can factor:
$$P(x) = (x+3)(x^2 + 2x - 3).$$

Definition

Let $k \in \mathbb{N}^*$. We say that α is a root of multiplicity k of P if $(X - \alpha)^k$ divides P while $(X - \alpha)^{k+1}$ does not.
When $k = 1$, we say that α is a simple root; when $k = 2$, a double root, etc. We also say that α is a root of order k.

Proposition

The following assertions are equivalent for $\alpha \in \mathbb{K}$ and $k \in \mathbb{N}^*$:

1. α is a root of multiplicity k of P.
2. There exists $Q \in \mathbb{K}[X]$ such that
$$P = (X - \alpha)^k Q, \quad \text{with } Q(\alpha) \neq 0.$$
3. $$P(\alpha) = P'(\alpha) = P''(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0, \quad \text{and } P^{(k)}(\alpha) \neq 0.$$

Example

Let
$$P(x) = x^5 - 14x^4 + 75x^3 - 194x^2 + 244x - 120.$$
The number 2 is a root of multiplicity 3 because
$$P(2) = P'(2) = P''(2) = 0 \quad \text{and} \quad P^{(3)}(2) \neq 0.$$
Indeed, for all $x \in \mathbb{R}$, we have
$$P'(x) = 5x^4 - 56x^3 + 225x^2 - 388x + 244,$$
$$P''(x) = 20x^3 - 168x^2 + 450x - 388,$$
$$P^{(3)}(x) = 60x^2 - 336x + 450.$$

4.2 d'Alembert-Gauss theorem

Theorem

Any polynomial with complex coefficients of degree $n \geq 1$ has at least one root in $\mathbb{C}$. Moreover, it admits exactly n roots if we count each root with its multiplicity.

Theorem

Let $P \in \mathbb{K}[X]$ be of degree $n \geq 1$. Then P admits at most n roots in $\mathbb{K}$.

4.3 Decomposition into a Product of Irreducible Factors

4.3.1 Irreducible polynomials

Definition

Let $P \in \mathbb{K}[X]$ be a polynomial of degree ≥ 1. We say that P is irreducible if for every $Q \in \mathbb{K}[X]$ dividing P, we have either
$$Q \in \mathbb{K}^* \quad \text{or} \quad \exists \lambda \in \mathbb{K}^* \text{ such that } Q = \lambda P.$$

Remark

- An irreducible polynomial P is therefore a non-constant polynomial whose only divisors are constants or P itself.
- The notion of irreducibility in $\mathbb{K}[X]$ corresponds to the notion of a prime number in $\mathbb{Z}$.
- Otherwise, we say that P is reducible; then there exist polynomials $A, B \in \mathbb{K}[X]$ such that
$$P = AB, \quad \deg A \geq 1, \quad \deg B \geq 1.$$

Example

- All polynomials of degree 1 are irreducible. Therefore, there are infinitely many irreducible polynomials.
- $X^2 - 4 = (X - 2)(X + 2)$ is reducible.
- $X^2 + 9 = (X - 3i)(X + 3i)$ is reducible in $\mathbb{C}[X]$ but irreducible in $\mathbb{R}[X]$.
- $X^2 - 3 = (X + \sqrt{2})(X - \sqrt{2})$ is reducible in $\mathbb{R}[X]$ but irreducible in $\mathbb{Q}[X]$.

4.3.2 Euclid's Lemma

Proposition

Let $P \in \mathbb{K}[X]$ be an irreducible polynomial, and let $A, B \in \mathbb{K}[X]$. If $P \mid AB$, then
$$P \mid A \quad \text{or} \quad P \mid B.$$

4.3.3 Factorization Theorem

Theorem

Any non-constant polynomial $A \in \mathbb{K}[X]$ can be written as a product of unitary irreducible polynomials:
$$A = \lambda P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r},$$
where $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $k_i \in \mathbb{N}^*$, and the P_i are distinct irreducible polynomials. Moreover, this decomposition is unique up to the order of the factors.

This is the analogue of the decomposition of an integer into prime factors.

4.4 Factorization in $\mathbb{C}[X]$ and $\mathbb{R}[X]$

Theorem

The irreducible polynomials in $\mathbb{C}[X]$ are exactly the polynomials of degree 1. Therefore, for $P \in \mathbb{C}[X]$ of degree $n \geq 1$, the factorization can be written as

$$P = \lambda(X - \alpha_1)^{k_1}(X - \alpha_2)^{k_2} \cdots (X - \alpha_r)^{k_r},$$

where $\alpha_1, \ldots, \alpha_r$ are the distinct roots of P and $k_1, \ldots, k_r$ are their multiplicities.

Example

Let

$$P(X) = (X - 1)^2(X^2 + 4)^2(X^2 + 2)(X^2 + X + 1).$$

This polynomial is already decomposed into irreducible factors in $\mathbb{R}[X]$.
Its decomposition in $\mathbb{C}[X]$ is

$$P(X) = (X - 1)^2(X - 2i)^2(X + 2i)^2(X - i\sqrt{2})(X + i\sqrt{2})(X - j)(X - j^2),$$

where

$$j = e^{\frac{2i\pi}{3}} = \frac{-1 + i\sqrt{3}}{2}.$$