Chapitre 4

Rings of Polynomials

Introduction

In this chapter, we introduce the concept of polynomials over a field or a commutative unitary ring. Throughout the chapter, $\mathbb{K}$ denotes a field and $\mathbb{A}$ denotes a commutative unitary ring.

4.1 Definitions

Definition 4.1.
Let $(\mathbb{A}, +, \cdot)$ be a commutative unitary ring. A polynomial P in one indeterminate X with coefficients in $\mathbb{A}$ is any algebraic expression of the form :

$$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n + \ldots$$

where the coefficients $a_i \in \mathbb{A}$ are zero for all but finitely many i.

Another definition is given by :

Definition 4.2.
A polynomial in one indeterminate x with coefficients in $\mathbb{A}$ is any sequence $P = (a_n)_{n \in \mathbb{N}}$ of elements from $\mathbb{A}$, all zero from some point onwards.

1. The a_n are called the coefficients of P.

2. The highest index n such that $a_n \neq 0$ (if it exists) is called the degree of P, denoted $\deg(P)$. In this case, $a_n X^n$ is called the leading term of P.
3. If all coefficients a_i are zero, P is called the zero polynomial, denoted 0, and conventionally $\deg(0) = -\infty$.
4. If the leading term of P is $1X^n$, then P is called monic.
5. Every element $a \in \mathbb{A}$ is a polynomial, called a constant polynomial.
6. The set of polynomials in one indeterminate X with coefficients in $\mathbb{A}$ is denoted $\mathbb{A}[X]$.

Polynomials are equipped with the usual operations of addition, polynomial multiplication, and scalar multiplication by $\lambda \in \mathbb{A}$: Let $P = (a_n)_{n\in\mathbb{N}}, Q = (b_n)_{n\in\mathbb{N}}$ be two polynomials in one indeterminate with coefficients in $\mathbb{A}$. Then :

1. $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$
2. $PQ = (c_n)_{n\in\mathbb{N}}$ where $c_n = \sum_{0\leq k\leq n} a_k b_{n-k}$
3. $\lambda P = (\lambda a_n)_{n\in\mathbb{N}}$

Definition 4.3.
The set $\mathbb{A}[X]$, consisting of polynomials in one indeterminate with coefficients in $\mathbb{A}$, equipped with the addition and multiplication defined above, forms a commutative ring.

Proposition 4.4.
If $\mathbb{A}$ is an integral domain, then for all $P, Q \in \mathbb{A}[X]$, we have :

1. $\deg(PQ) = \deg(P) + \deg(Q)$
2. $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$

Proof 4.5.

1. *If one of the polynomials is zero, then $PQ = 0$ and $\deg(PQ) = -\infty$ which is true. Assume both P and Q are non-zero. Let $n = \deg(P)$ and $m = \deg(Q)$. Write $P = \sum a_i X^i$ and $Q = \sum b_i X^i$ with $a_i, b_i \in \mathbb{A}$. Then the coefficient of the leading term in PQ is $a_n b_m$. Since $a_n \neq 0$ and $b_m \neq 0$, and $\mathbb{A}$ is an integral domain, we have $a_n b_m \neq 0$, implying $\deg(PQ) = n + m$.*
2. *Trivial.*

Let $\mathbb{U}(\mathbb{A})$ denote the units (invertible elements) of $\mathbb{A}$.

Proposition 4.6.

If $\mathbb{A}$ is an integral domain, then the units of $\mathbb{A}[X]$ are exactly the constant polynomials $P = a$ where $a \in \mathbb{U}(\mathbb{A})$.

Proof 4.7.

Let P be invertible in $\mathbb{A}[X]$. There exists $Q \in \mathbb{A}[X]$ such that $PQ = 1$. Thus, $\deg(P) + \deg(Q) = 0$ *implies* $\deg(P) = \deg(Q) = 0$. *Hence, P and Q are constant invertible elements.*

4.2 Polynomial Arithmetic

4.2.1 Associated Polynomials

Definition 4.8.

Two polynomials P and Q in $\mathbb{A}[X]$ are said to be associated if there exists $a \in \mathbb{U}(A)$ such that $P = aQ$.

Example 4.1.

The set of polynomials associated with $X^2 + 1$ in $\mathbb{Z}[X]$ is

$$\{X^2 + 1, -(X^2 + 1)\}$$

since the only units in $\mathbb{Z}$ are 1 and -1.

Proposition 4.9.

1. *The relation "being associated" is an equivalence relation on $\mathbb{A}[X]$.*
2. *If P and Q are associated and have the same leading coefficient, then $P = Q$.*
3. *If $\mathbb{A}$ is a field, then every polynomial P is associated with a unique unitary polynomial.*

4.2.2 Division

Definition 4.10.

Let $P, Q \in \mathbb{A}[X]$. We say that P divides Q, denoted as $P|Q$, if there exists $R \in \mathbb{A}[X]$ such that $Q = PR$.

Example 4.2.

1. *The polynomial* $X - 1$ *divides* $X^2 - 1$ *in* $\mathbb{Z}[X]$.
2. *The polynomial* $X - 3$ *does not divide* $X^2 - 1$ *in* $\mathbb{Z}[X]$.

Proposition 4.11.
Let $P, Q, R, S \in A[X]$.

1. *If* $P|Q$ *and* $Q|R$, *then* $P|R$.
2. *If* $P|Q$ *and* $P|R$, *then* $P|(Q + R)$.
3. *If* $P|Q$ *and* $Q \neq 0$, *then* $\deg(P) \leq \deg(Q)$.
4. *If* $P|Q$ *and* $R|S$, *then* $PR|QS$.
5. *If* $P|Q$, *then* $P^n|Q^n$ *for all* $n \geq 1$.

Proof 4.12.
See textbook.

Proposition 4.13.
Let $P, Q, R, S \in A[X]$.

1. *If* $P|Q$ *and* $Q|P$, *then* P *and* Q *are associated.*
2. *If* P *is associated with* R *and* Q *is associated with* S, *then* $P|Q \iff R|S$.

4.2.3 Euclidean Division

Théorème 4.14. *(Euclidean Division)*
Let $A, B \in K[X]$ *be two polynomials with coefficients in a field* K *such that* $B \neq 0$. *Then there exists a unique pair* (Q, R) *of* $K[X]$ *such that* $A = BQ + R$ *and* $\deg(R) < \deg(B)$.

Example 4.3.
Let $A = x^3 + x + 1$ *and* $B = x + 1$. *Then we have* $A = B(x^2 - x + 2) - 1$.

Recall that a subset I of a ring $\mathbb{A}$ is an ideal if the following two conditions hold :

1. $(I, +)$ is a subgroup of $(A, +)$,
2. For every $a \in A$, $aI \subset I$. In other words, for all $a \in A$ and $x \in I$, $ax \in I$.

Théorème 4.15.
The ring $\mathbb{K}[X]$ *is principal.*

Proof 4.16.

Proof. Let I be an ideal of $\mathbb{K}[X]$ containing a nonzero polynomial. We want to show that I is principal, i.e., there exists a polynomial P such that I is exactly the set of multiples of P. Let $D = \{\deg(S) \mid S \in I, S \neq 0\}$. This is a non-empty subset of $\mathbb{N}$, so it has a minimum n. Let P be a polynomial of degree n in I. Since I is an ideal, all multiples of P are in I. Conversely, we want to show that every element of I is a multiple of P. So let $A \in I$. We know there exist Q, R such that $A = PQ + R$ with $\deg(R) < n$. Since $-PQ \in I$, we have $R = A - PQ \in I$. As $\deg(R) < n$, by the definition of n, we have $R = 0$, i.e., $A = PQ$, and A is indeed a multiple of P.

4.2.4 Irreducible Polynomials

Recall that the invertible polynomials in $\mathbb{A}[X]$ are the constant polynomials $P = a \in \mathbb{U}(A)$. Thus, since all non-zero elements in a field are invertible, the invertible polynomials in $\mathbb{K}[X]$ are the non-zero constant polynomials.

Definition 4.17.
A polynomial $P \in \mathbb{K}[X]$ is called irreducible if it is not invertible and if the equality $P = QR$ implies that either Q or R is invertible.

We say that a polynomial P is reducible if it is not irreducible.

Example 4.4.

1. *The polynomial $P(X) = 3$ is invertible in $\mathbb{Q}[X]$, so it is not irreducible.*
2. *The polynomial $P(X) = X^2 + 1$ is irreducible if we consider it as an element of $\mathbb{R}[X]$, but it is reducible if we consider it as an element of $\mathbb{C}[X]$, because $X^2 + 1 = (X - i)(X + i)$.*

The notion of irreducible polynomials depends on the field $\mathbb{K}$.

Proposition 4.18.

1. *Reducible polynomials in $\mathbb{K}[X]$ have degree greater than or equal to 2.*
2. *All polynomials of degree 1 are irreducible.*

Proof 4.19.
See textbook.

4.2.5 Greatest Common Divisor

Let $P_1, ..., P_n \in \mathbb{K}[X]$. Since $\mathbb{K}[X]$ is principal, the ideal

$$< P_1, ..., P_n >= \{P_1 A_1, ..., P_n A_n / A_1, ..., A_n \in \mathbb{K}[X]\}$$

is generated by a unique unit polynomial P. This polynomial is called the gcd of P_i and is denoted

$$P = \gcd(P_1, ..., P_n).$$

Proposition 4.20. *Properties of gcd*
Let $P, Q \in \mathbb{K}[X]$. Then

1. $\gcd(P, Q)$ *is a common divisor of P and Q.*
2. *If D is another common divisor of P and Q, then D divides* $\gcd(P, Q)$.
3. *There exist polynomials $(U, V) \in \mathbb{K}[X]^2$ such that*

$$PU + QV = \gcd(P, Q).$$

Definition 4.21.
Let $P, Q \in \mathbb{K}[X]$. We say that P and Q are coprime if $\gcd(P, Q) = 1$.

In other words, if $\gcd(P, Q) = 1$, then only non-zero constants divide both P and Q.

4.2.6 Factorization

Théorème 4.22.
Let $P \in \mathbb{K}[X]$ be a non-zero polynomial. Then P decomposes uniquely up to the order of factors as :

$$P = \alpha P_1^{\alpha_1} P_2^{\alpha_2} ... P_n^{\alpha_n}$$

where P_i are distinct, unit, irreducible polynomials in $\mathbb{K}[X]$ and $\alpha \in \mathbb{K}^*$ is the leading coefficient of P.

Example 4.5.
Consider the polynomial $P = x^2 + 1$. Then P exists in both $\mathbb{R}[X]$ and $\mathbb{C}[X]$. However, care must be taken as its factorization differs in these two rings :

1. *P factors as $(X - i) \cdot (X + i)$ in $\mathbb{C}[X]$.*
2. *P is irreducible in $\mathbb{R}[X]$.*

Proposition 4.23.

Let P and Q be two non-zero polynomials. Let $P = aP_1^{\alpha_1}P_2^{\alpha_2}...P_n^{\alpha_n}$ and $Q = bP_1^{\beta_1}P_2^{\beta_2}...P_n^{\beta_n}$ be their decompositions into irreducible factors where $\alpha_i, \beta_i \geq 0$ for all $i \in \{1, ..., n\}$. Then

$$\frac{P}{Q} \Leftrightarrow \alpha_j \leq \beta_j$$

for all $1 \leq j \leq n$.

4.3 Polynomial Functions

Let $P \in \mathbb{K}[X]$. We denote by f_P the polynomial function associated with P, defined as :

$$f_P : \mathbb{K} \longrightarrow \mathbb{K}$$
$$x \mapsto P(x).$$

Definition 4.24.

Let $P \in \mathbb{K}[X]$. We say that $x \in \mathbb{K}$ is a root of P if $f_P(x) = 0$ (or $P(x) = 0$).

Proposition 4.25.

Let $P \in \mathbb{K}[X]$ and $\alpha \in \mathbb{K}$. Then α is a root of P if and only if the polynomial $(x - \alpha)/P$.

Definition 4.26.

Let $P \in \mathbb{K}[X]$ and let α be a root of P. We say that α has multiplicity k if and only if $(x - \alpha)^k$ divides P and $(x - \alpha)^{k+1}$ does not divide P.

In other words, α is a root of P of multiplicity k if and only if
$P = (x - \alpha)^k Q$ and $Q(\alpha) \neq 0$.

Example 4.6.

To determine the multiplicity of a root, we can perform successive Euclidean divisions. Let $P = x^3 - 3x^2 + 4$. It can be verified easily that 2 is a root of P. Furthermore, we find $P(x) = (x - 2)^2 Q(x)$ with $Q(x) = x + 1$ and $Q(2) \neq 0$.

Théorème 4.27.

Let $P \in \mathbb{K}[X]$ and $\alpha_1, ..., \alpha_r$ be pairwise distinct roots of multiplicative $k_1, ..., k_r$, respectively. Then, there exists $Q \in \mathbb{K}[X]$ such that

$$P = (x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2}...(x - \alpha_r)^{k_r} Q$$

and $Q(\alpha_i) \neq 0$ for all i. In particular, P has a degree of at least $k_1 + ... + k_r$.

4.4 Exercises

Exercice 4.28.

Find the polynomial P of degree less than or equal to 3 such that : $P(0) = 1$, $P(1) = 0$, $P(-1) = -2$, and $P(2) = 4$.

Exercice 4.29.

Perform the Euclidean division of A by B for the following cases :

1. $A = 3X^5 + 4X^2 + 1$ *and* $B = X^2 + 2X + 3$.
2. $A = 3X^5 + 2X^4 - X^2 + 1$ *and* $B = X^3 + X + 2$.
3. $A = X^4 - X^3 + X - 2$ *and* $B = X^2 - 2X + 4$.

Exercice 4.30.

Let $P, Q, R, S \in A[X]$.

1. *If* $P|Q$ *and* $Q|R$ *then* $P|R$.
2. *If* $P|Q$ *and* $P|R$ *then* $P|Q + R$.
3. *If* $P|Q$ *and* $Q \neq 0$ *then* $\deg(P) \leq \deg(Q)$.
4. *If* $P|Q$ *and* $R|S$ *then* $PR|QS$.
5. *If* $P|Q$ *then* $P^n|Q^n$ *for all* $n \geq 1$.

Exercice 4.31.

Let $P, Q, R, S \in A[X]$.

1. *If* $P|Q$ *and* $Q|P$ *then* P *and* Q *are associated.*
2. *If* P *is associated to* R *and* Q *is associated to* S *then* $P|Q \Leftrightarrow R|S$.

Exercice 4.32.

Find the gcd of the following polynomials :

1. $X^3 - X^2 - X - 2$ *and* $X^5 - 2X^4 + X^2 - X - 2$.
2. $X^4 + X^3 - 2X + 1$ *and* $X^3 + X + 1$.

Exercice 4.33.

1. *Reducible polynomials in* $\mathbb{K}[X]$ *have degree greater than or equal to* 2.
2. *All polynomials of degree* 1 *are irreducible.*