Polynomials

Objectives of the course

- Introduction
- Definition
- Operations
- The indeterminate X
- Writing of a polynomial
- Constant polynomial, monomial
- Degree of a polynomial
- Rules of computation

Objectives of the course

- Leading coefficient, monic polynomial
- The ring structure
- Euclidean algorithm
- Division (ascending,,,)
- Evaluation and roots
- Derivative of a polynomial, Properties
- Taylor expansions
- Irreducible polynomials

Introduction

This course is devoted to polynomials with coefficients in a field K. In practice, it will be $\mathbb{R}$ or $\mathbb{C}$, sometimes $\mathbb{Q}$ or a finite field.

Most of you knows polynomials as « expression of the form » :

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

But what is X ? And what is the multiplication $a_i X^i$?

Introduction

This presentation makes sense when the a_i are real numbers and X is a real variable. However, in the general case, when X is an *indeterminate*, we need to be more precise. We will give below a rigorous definition of this mathematical object, and we will then study its properties.

Definition of a polynomial

Definition

Let K be a field. A polynomial with one indeterminate and coefficients in K is a sequence $(a_0, a_1, \dots, a_p, \dots)$ of elements of K such that $a_p = 0$ for almost all p.

The term « $a_p = 0$ for almost all p » means that :

$$\exists\ n \in \mathbb{N} \text{ such that } a_i = 0, \forall i > n.$$

Operations on polynomials

Let

$$P = (a_0, a_1, \ldots, a_p, \ldots)$$

and

$$Q = (b_0, b_1, \ldots, b_p, \ldots)$$

be two polynomials with one indeterminate and coefficients in K,

and let $\alpha \in K$. We define the following operations :

Sum of polynomials

Sum

$$P + Q =$$

$$(a_0 + b_0, a_1 + b_1, \ldots, a_p + b_p, \ldots)$$

Product of polynomials

Product

$$PQ = (c_0, c_1, \dots, c_p, \dots),$$

where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}, k \geq 0.$$

Multiplication by a scalar

Multiplication by a scalar

$$\alpha P = \left(\alpha a_0, \alpha a_1, \dots, \alpha a_p, \dots\right).$$

The indeterminate X

The indeterminate X is none other than the sequence given by

$$(0,1,0,\ldots,0,\ldots).$$

With the product defined previously, we obtain

$$X^2 = (0,0,1,0,\ldots,0,\ldots),$$

$$X^3 = (0,0,0,1,0,\ldots,0,\ldots), \text{ etc.}$$

We set by convention

$$X^0 = (1,0,\ldots,0,\ldots).$$

The product of a scalar $a \in K$ by X^i is given by

$$aX^i = (0,\ldots,0,a,0,\ldots,0,\ldots),$$

where a is at the $(i+1)$th position.

Writing a polynomial

With the definition of the indeterminate X and the operations given previously, a polynomial can be written *in ascending powers of* X

$$a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + a_n X^n \ ,$$

or *in descending powers of* X

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

the a_i being zero for all $i > n$.

Set of polynomials

Notation

The set of polynomials with coefficients in K and indeterminate X is denoted by $K[X]$.

An element of $K[X]$ will be denoted by $P(X)$, or simply P.

Constant polynomial, zero polynomial, monomial

Definition

The polynomial

$$P = a_0 + a_1 X + \cdots + a_n X^n$$

So that $a_i = 0$ for all $i \geq 1$ is called constant polynomial.

If $a_i = 0$ for all i, P is the zero polynomial, denoted by 0.

A monomial is a polynomial of the form

$$P = a_i X^i.$$

The sum

Definition

Let

$$P = a_0 + a_1X + \cdots + a_nX^n$$

and

$$Q = b_0 + b_1X + \cdots + b_mX^m$$

Two polynomials in $K[X]$. Set $r = max(m, n)$.

Then the sum of P and Q is given by

$$P + Q = \sum_{i=0}^{r} (a_i + b_i)X^i.$$

The product

Definition

Let

$$P = a_0 + a_1 X + \cdots + a_n X^n$$

and

$$Q = b_0 + b_1 X + \cdots + b_m X^m$$

two polynomials in $K[X]$.

Then the product of P by Q is given by

$$PQ = \sum_{k=0}^{m+n} c_k X^k \,,$$

where

$$\sum_{i=0}^{k} a_i b_{k-i}, k \geq 0.$$

The product by a scalar

Definition

Let

$$P = a_0 + a_1 X + \cdots + a_n X^n$$

a polynomial in $K[X]$ and let $\alpha \in K$. Then the product of α by P is given by

$$\alpha \sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} \alpha a_i X^i .$$

Rules of computation

If P, Q and R are polynomials in $K[X]$, then

- $P + Q = Q + P$,
- $(P + Q) + R = P + (Q + R)$,
- $PQ = QP$,
- $(PQ)R = P(QR)$,
- $(P + Q)R = PR + QR$,
- $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$.

Leading coefficient, monic polynomial

Definition

If $P = a_0 + a_1X + \cdots + a_nX^n$ is of degree n, a_n is called the leading coefficient of P. If, moreover, a_n=1, we say that P is a monic polynomial.

Example

The polynomial $3 + 4X - X^2 - 2X^3$ is of degree 3, it has -2 as leading coefficient, so it is not monic.

The polynomial $X^4 - 2X + 3$ is a monic polynomial of degree 4.

Degree of a polynomial

Definition

The degree of the polynomial

$$P = a_0 + a_1 X + \cdots + a_n X^n$$

is the greatest integer h such that $a_h \neq 0$.

We denote it by $degP$.

By convention, we set $deg(0) = -\infty$.

Properties of the degree

The degree verify the properties given in the next proposition.

Proposition

Let P and Q two polynomials in $K[X]$. Then we have

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

Ring structure

Proposition

Endowed with the sum and the product defined previously,

$K[X]$ is an integral domain.

The invertible elements of this ring are the nonzero constant polynomials.

Euclidean division

Theorem

Let A and B two polynomials in $K[X]$ with $B \neq 0$. Then there exists a unique ordered pair $(Q, R) \in K[X]^2$ such that

$$A = BQ + R \text{ and } degR < degB.$$

Definition

The polynomials Q and R are called respectively quotient and remainder of the Euclidean division of A by B.

Proof of the theorem

Existence

If $degA < degB$, it suffices to take $Q = 0$ and $R = A$.

If $degA \geq degB$, we proceed as follows. Let

$$A = a_m X^m + \cdots + a_1 X + a_0$$

and

$$B = b_n X^n + \cdots + b_1 X + b_0,$$

with $a_m \neq 0$ and $b_n \neq 0$, and set $D_0 = a_m / b_n X^{m-n}$. We have then

$$deg(A - D_0 B) \leq m - 1 < degA.$$

Proof of the theorem

If $deg(A - D_0B) < degB$, we take $Q = D_0$ and $R = A - D_0B$.

Otherwise, we choose D_1 as previously so that

$$deg(A - D_0B - D_1B) < deg(A - D_0B).$$

After a finite number of iterations, we obtain

$$deg(A - D_0B - \cdots - D_k\, B) < degB.$$

We take then

$$Q = D_0 + \cdots + D_k$$

and

$$R = A - D_0B - \cdots - D_k\, B.$$

Proof of the theorem

Unicity

Suppose that there exist two orderd pairs (Q_1, R_1) and (Q_2, R_2) in $K[X]^2$ so that $A = BQ_1 + R_1 = BQ_2 + R_2$ with $degR_i < degB$ for $1 \leq i \leq 2$. We have then

$R_2 - R_1 = B(Q_1 - Q_2)$, and so

$$deg(R_2 - R_1) = degB + deg(Q_1 - Q_2).$$

On the other hand, we have

$$deg(R_2 - R_1) \leq max(degR_1, degR_2) < degB,$$

which gives $degB + deg(Q_1 - Q_2) < degB$.

It follows that $deg(Q_1 - Q_2) = -\infty$, which means that $Q_1 = Q_2$ and, therefore, $R_1 = R_2$.

Example

Take $K = \mathbb{R}$, $A = X^3 + 2X^2 - X + 1$ and $B = X^2 + X + 1$.

$$\begin{array}{ccccc|c} X^3 & + & 2X^2 & -X & +3 & X^2+X+1 \\ \cline{6-6} & & & & & X \end{array}$$

Example

X^3	$+$	X^2	$-X$	$+3$	$X^2 + X + 1$
X^3	$+X^2$	$+X$			X

Example

$$
\begin{array}{llll|l}
X^3 & +2X^2 & -X & +3 & X^2+X+1 \\
\hline
-(X^3 & +X^2 & +X) & & X \\
 & +X^2 & -2X & +3 &
\end{array}
$$

Example

X^3	$+2X^2$	$-X$	$+3$	$X^2 + X + 1$
$-(X^3$	$+X^2$	$+X)$		$X + 1$
	$+X^2$	$-2X$	$+3$	
	$+X^2$	$+X$	$+1$	

Example

$$
\begin{array}{ccccc|c}
 & X^3 & +2X^2 & -X & +3 & X^2+X+1 \\ \cline{6-6}
 & -(X^3 & +X^2 & +X) & & X+1 \\
 & & +X^2 & -2X & +3 & \\
- & & (+X^2 & +X & +1) & \\
 & & & -3X & +2 &
\end{array}
$$

Example

Since the degree of $-3X + 2$ is less than the degree of $X^2 + X$ +1, then we have

$$Q = X + 1$$

and

$$R = -3X + 1.$$

Division in ascending powers

Theorem

Let A and B two polynomials in $K[X]$,

with $B(0) \neq 0$. Then, for any non negative integer k,

there exists a unique ordered pair $(Q, R) \in K[X]^2$ such that

$$A = BQ + X^{k+1}R \text{ and } degQ \leq k.$$

Remark

k is called the order of the division.

Example

2	$-X$	$+X^2$		$+X^3$	$1+X-X^2$
2	$+2X$		$-2X^2$		2

Example

2	$-X$	$+X^2$	$+X^3$	$1+X-X^2$
2	$+2X$	$-2X^2$		2
	$-3X$	$+3X^2$	$+X^3$	

Example

2	$-X$	$+X^2$	$+X^3$	$1+X-X^2$
2	$+2X$	$-2X^2$		$2-3X$
	$-3X$	$+3X^2$	$+X^3$	
	$-3X$	$-3X^2$	$+3X^3$	

Example

2	$-X$	$+X^2$	$+X^3$	$1+X-X^2$
2	$+2X$	$-2X^2$		$2-3X+6X^2$
	$-3X$	$+3X^2$	$+X^3$	
	$-3X$	$-3X^2$	$3X^3$	
		$6X^2$	$-2X^3$	
		$6X^2$	$+6X^3-6X^4$	
			$-8X^3+6X^4$	

Derivative of a polynomial

Definition

The derivative of the polynomial

$$P = a_n X^n + \cdots + a_1 X + a_0 \in K[X],$$

is the polynomial $P' \in K[X]$ given by

$$P' = n a_n X^{n-1} + \cdots + 2a_2 X + a_1.$$

The derivative of order k of the polynomial P, denoted by $P^{(k)}$, where k is a nonnegative integer, is given by the recurrence relation

$$P^{(0)} = P \text{ et } P^{(k+1)} = \left(P^{(k)}\right)' \text{ pour } k \geq 0.$$

Remark

This definition of the derivative is *formal*, ie, we do not use any notion of limit.

Properties of the derivatives

The rules of derivation are given by the next theorem.

Theorem

Let P and Q be two polynomials in $K[X]$ and let $\alpha \in K$. Then we have

1) $(P+Q)' = P' + Q'$,
2) $(\alpha P)' = \alpha P'$,
3) $(PQ)' = P'Q + PQ'$,
4) $(P^n)' = nP'P^{n-1}$, where n is a positive integer,
5) $(PQ)^{(k)} = \sum_{i=0}^{k} C_k^i P^{(i)} Q^{(k-i)}$.

Remark

The formula given in 5) is known as Leibniz formula.

Evaluation, root of a polynomial

Definition

Let

$$P = a_0 + a_1X + \cdots + a_nX^n \in K[X].$$

If we replace the indeterminate X by $\alpha \epsilon K$, we get an element of K denoted by

$$P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n,$$

called evaluation of P at α.

If $P(\alpha) = 0$, we say that α is a root of P.

Remark

Some authors use the term « zéro of P » instead of « root of P ».

Example

Example

The polynomial

$$P = X^2 + 1 \in \mathbb{R}[X] \subset \mathbb{C}[X]$$

has i et $-i$ as roots in $\mathbb{C}$, but it has no root in $\mathbb{R}$.

Taylor expansion

The following formula allows to develop any polynomial in $K[X]$ in ascending powers of $X - \alpha$, where α is an arbitrary element of K.

Theorem (Taylor expansion)

Let $P \in K[X]$ a polynomial of degree n and let $\alpha \in K$. Then we have

$$P(X) = P(\alpha) + \frac{P'(\alpha)}{1!}(X - \alpha) + \cdots + \frac{P^{(n)}(\alpha)}{n!}(X - \alpha)^n.$$

Example

Example

Consider in $\mathbb{R}[X]$ the polynomial

$$P = 2X^3 + 2X - 3$$

and let $\alpha = 1$.

We have

$$P' = 6X^2 + 2, P'' = 12X, \text{ and } P^{(3)} = 12,$$

which gives

$$P(X) = 1 + \frac{8}{1!}(X-1) + \frac{12}{2!}(X-1)^2 + \frac{12}{3!}(X-1)^3$$
$$= 1 + 8(X-1) + 6(X-1)^2 + 2(X-1)^3.$$

Multiple roots

Definition

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.

Multiple roots and derivatives

In the next proposition and the following theorem, we assume that the field K contains the field of rational numbers $\mathbb{Q}$.

Proposition

If α is a root of $P \in K[X]$ of multiplicity $k > 1$, then α is a root of P' of multiplicity $k - 1$.

Preuve

As α is a root of P of ordre k, then we can write

$P(X) = (X - \alpha)^k Q(X), Q \in K[X]$ with $Q(\alpha) \neq 0$.

Multiple roots and derivatives

Therefore

$$P'(X) = k(X-\alpha)^{k-1}Q(X) + (X-\alpha)^k Q'(X)$$
$$= (X-\alpha)^{k-1}\big(kQ(X) - (X-\alpha)Q'(X)\big).$$

Setting $Q_1(X) = kQ(X) - (X-\alpha)^k Q'(X)$, we obtain

$P'(X) = (X-\alpha)^{k-1}Q_1(X), Q_1 \in K[X]$ and

$$Q_1(\alpha) = kQ(\alpha) \neq 0,$$

which means that α is a root of P' of multiplicity $k-1$.

Multiplicity of a root

Theorem

Let $P \in K[X]$ a polynomial of degree $n \geq 1$ and let k be an integer such that $1 \leq k \leq n$. Then a root α of P has multiplicity k if and only if

$$P^{(i)}(\alpha) = 0 \text{ for } 0 \leq i \leq k-1 \text{ and } P^{(k)}(\alpha) \neq 0.$$

Example

Let $P(X) = X^3 - 3X - 2 \in \mathbb{R}[X]$. We have $P' = 3X^2 - 3$ and $P" = 6X$, then $P(-1) = P'(-1) = 0$ and $P"(-1) \neq 0$.

Therefore, -1 is a double root of P.

Proof of the theorem

Proof

If α is a root of P of multiplicity k, then, by the previous proposition, α is a root of P' of multiplicity $k-1$. By iteration, we obtain $P^{(i)}(\alpha)=0$ for $0 \leq i \leq k-1$ and $P^{(k)}(\alpha) \neq 0$, since α is a simple root of $P^{(k-1)}$.

Conversely, if $P^{(i)}(\alpha)=0$ for $0 \leq i \leq k-1$ and $P^{(k)}(\alpha) \neq 0$, the Taylor expansion gives

$$P(X)=\frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k+\cdots+\frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n$$

$$=(X-\alpha)^k\left(\frac{P^{(k)}(\alpha)}{k!}+\cdots+\frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^{n-k}\right).$$

Then $P(X)=(X-\alpha)^k Q(X)$, with $Q(\alpha)=\frac{P^{(k)}(\alpha)}{k!} \neq 0$. This proves that α is a root of P of multiplicity k.

Roots and divisibility in K[X]

Definition

Let $A, B \in K[X]$.

We say that B divides A in $K[X]$ if there exists Q in $K[X]$ such that $A = BQ$. We will say That A is a multiple of B in $K[X]$.

Theorem (D'Alembert-Gauss)

Any polynomial $P \in \mathbb{C}[X]$ has a root in $\mathbb{C}$.

Roots and divisibility in K[X]

Theorem

Let $a_1, a_2, \cdots, a_n$ be n distinct elements of K and $P \in K[X]$.

Then P is divisible by $(X - a_1)\,(X - a_2) \cdots (X - a_n)$ if, and only if, $P(a_1) = P(a_2) = \cdots = P(a_n) = 0$.

Theorem

Let $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$. Let $\frac{p}{q} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, such that $P\left(\frac{p}{q}\right) = 0$. Then p divides a_0 and q divides a_n.

Irreducible polynomial

Definition

Two polynomials $A, B \in K[X]$ are called associated if

$A = \lambda B,\ \lambda \in K^*$.

Definition

A polynomial $P \in K[X]$ is called irreducible in $K[X]$ if $deg P \geq 1$ and if the only divisors of P are the polynomials associated to 1 or to P.

Irreducible polynomial

Theorem

- The irreducible polynomials of $\mathbb{C}[X]$ are The polynomials of degree 1.
- The irreducible polynomials of $\mathbb{R}[X]$ are the polynomials of degree 1 and the polynomials of degree 2 with discriminant $\Delta < 0$.