Chapter 2

Polynomials

In this chapter, fix a commutative field $(\mathbb{K}, +, \times)$ (for instance $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$). We denote

- 0 the additive identity
- $-a$ the additive inverse of an element $a \in \mathbb{K}$
- 1 the multiplicative identity
- a^{-1} the multiplicative inverse of an element $a \in \mathbb{K}^* = \mathbb{K} - \{0\}$

2.1 The ring $\mathbb{K}[X]$

2.1.1 Definition and operations

Definition 2.1 (*Polynomial*)

Let $(a_n)_{n\in\mathbb{N}} = (a_0, a_1, a_2, \dots, a_n, \dots)$ be an infinite sequence of elements in $\mathbb{K}$ which are eventually equal to zero, that is

$$\exists d \in \mathbb{N}/\ \forall n > d,\ a_n = 0$$

*The **polynomial** with **coefficients** $(a_n)_{n\in\mathbb{N}}$ is the following formal expression*

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d = \sum_{n=0}^{d} a_nX^n = \sum_{n=0}^{+\infty} a_nX^n$$

Moreover

- *the formal symbol X is called the **variable***
- *the formal symbols $X^0 = 1, X^1 = X, X^2, \dots, X^n, \dots$ are called the **powers of X***
- *for any $n \in \mathbb{N}$, a_n is called the **coefficient of the term with degree n***
- *a_0 is called the **constant term***

We denote $\mathbb{K}[X]$ the set of all polynomials with coefficients in $\mathbb{K}$.

Examples : $P(X) = X + X^3 + X^5 = 0 + 1X + 0X^2 + 1X^3 + 0X^4 + 1X^5$ is a polynomial in $\mathbb{K}[X]$ but also $Q(X) = X^2$ or $R(X) = 0$. $S(X) = \frac{1}{2} - \sqrt{2}X^2 + 5X^4$ is a polynomial in $\mathbb{R}[X]$ or $\mathbb{C}[X]$ but not in $\mathbb{Q}[X]$.

Definition 2.2 (*Addition in* $\mathbb{K}[X]$)

Let $P(X)$ and $Q(X)$ be two polynomials in $\mathbb{K}[X]$ with coefficients respectively $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$. We define the sum of $P(X)$ and $Q(X)$, denoted $(P+Q)(X)$, to be the polynomial in $\mathbb{K}[X]$ with coefficients $(a_n+b_n)_{n\in\mathbb{N}}$. That provides a binary operation $+$ on $\mathbb{K}[X]$.

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

Example : For instance, we have in $\mathbb{R}[X]$:

$$\begin{aligned}(1+2X+3X^3)+(4-X+5X^4) &= (1+4)+(2-1)X+(0+0)X^2+(3+0)X^3+(0+5)X^4\\ &= 5+X+3X^3+5X^4\end{aligned}$$

Definition 2.3 (*Multiplication in* $\mathbb{K}[X]$)

Let $P(X)$ and $Q(X)$ be two polynomials in $\mathbb{K}[X]$ with coefficients respectively $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$. We define the product of $P(X)$ and $Q(X)$, denoted $(PQ)(X)$, to be the polynomial in $\mathbb{K}[X]$ with coefficients $(\sum_{k=0}^{n} a_k b_{n-k})_{n\in\mathbb{N}}$. That provides a binary operation $\times$ on $\mathbb{K}[X]$.

$$P(X)Q(X)=(PQ)(X)=\sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n=\sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\ k+\ell=n}}a_kb_\ell\right)X^n$$

Remark : The previous definition is natural with respect to the following property

$$\forall(k,\ell)\in\mathbb{N}^2,\ X^kX^\ell=X^{k+\ell}$$

Example : For instance, we have in $\mathbb{R}[X]$:

$$\begin{aligned}(3-X-2X^2)(2+6X+4X^2) &= 6+(18-2)X+(12-6-4)X^2+(-4-12)X^3-8X^4\\ &= 6+16X+2X^2-16X^3-8X^4\end{aligned}$$

Proposition 2.4

$(\mathbb{K}[X],+,\times)$ is a commutative unital ring whose identity elements are respectively the constant polynomials 0 for addition and 1 for multiplication.

Proof : At first, $\mathbb{K}[X]$ is nonempty (for instance the constant polynomial 0 is in $\mathbb{K}[X]$).

1. $+$ and $\times$ are binary operations on $\mathbb{K}[X]$ by definition.
2. We have:
   (a) $+$ is associative on $\mathbb{K}$, so the same does on $\mathbb{K}[X]$ as well.
   (b) The constant polynomial $0\in\mathbb{K}[X]$ is the additive identity for $+$ in $\mathbb{K}[X]$.
   (c) For any polynomial in $\mathbb{K}[X]$ with coefficients $(a_n)_{n\in\mathbb{N}}$, the polynomial in $\mathbb{K}[X]$ with coefficients $(-a_n)_{n\in\mathbb{N}}$ is its additive inverse.
   (d) $+$ is commutative on $\mathbb{K}$, so the same does on $\mathbb{K}[X]$ as well.

   Consequently $(\mathbb{K}[X],+)$ is an abelian group.

3. Let $P(X)$, $Q(X)$ and $R(X)$ be three polynomials in $\mathbb{K}[X]$ with coefficients respectively $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$. We have:
$$\begin{aligned}
\left[P(X)Q(X)\right]R(X) &= \left[\sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\k+\ell=n}} a_k b_\ell\right)X^n\right]\sum_{j=0}^{+\infty} c_j X^j \\
&= \sum_{N=0}^{+\infty}\left(\sum_{\substack{n,j\in\mathbb{N}\\n+j=N}}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\k+\ell=n}} a_k b_\ell\right)c_j\right)X^N \\
&= \sum_{N=0}^{+\infty}\left(\sum_{\substack{k,\ell,j\in\mathbb{N}\\k+\ell+j=N}} a_k b_\ell c_j\right)X^N \\
&= \sum_{N=0}^{+\infty}\left(\sum_{\substack{k,m\in\mathbb{N}\\k+m=N}} a_k\left(\sum_{\substack{\ell,j\in\mathbb{N}\\\ell+j=m}} b_\ell c_j\right)\right)X^N \\
&= \sum_{k=0}^{+\infty} a_k X^k\left[\sum_{m=0}^{+\infty}\left(\sum_{\substack{\ell,j\in\mathbb{N}\\\ell+j=m}} b_\ell c_j\right)X^m\right] \;=\; P(X)\left[Q(X)R(X)\right]
\end{aligned}$$
Thus, $\times$ is associative on $\mathbb{K}[X]$.
4. Let $P(X)$, $Q(X)$ and $R(X)$ be three polynomials in $\mathbb{K}[X]$ with coefficients respectively $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ and $(c_n)_{n\in\mathbb{N}}$. We have:
$$\sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\k+\ell=n}} a_k(b_\ell+c_\ell)\right)X^n = \sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\k+\ell=n}} a_k b_\ell\right)X^n + \sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\k+\ell=n}} a_k c_\ell\right)X^n$$
Equivalently, $P(X)\left(Q(X)+R(X)\right) = P(X)Q(X) + P(X)R(X)$. And the same goes for $\left(Q(X)+R(X)\right)P(X) = Q(X)P(X) + R(X)P(X)$. Thus, $\times$ is distributive over $+$ on $\mathbb{K}[X]$.
5. Let $P(X)$ be a polynomial in $\mathbb{K}[X]$ with coefficients $(a_n)_{n\in\mathbb{N}}$. Since every coefficient of the constant polynomial $1\in\mathbb{K}[X]$ is equal to zero except the constant term equal to 1, we have:
$$P(X)1 = \sum_{n=0}^{+\infty}\left(a_0 0 + a_1 0 + \cdots + a_{n-1}0 + a_n 1\right)X^n = \sum_{n=0}^{+\infty} a_n X^n = P(X)$$
And the same goes for $1P(X) = P(X)$. Thus, the constant polynomial $1\in\mathbb{K}[X]$ is the multiplicative identity for $\times$ in $\mathbb{K}[X]$.
6. $+$ and $\times$ are commutative on $\mathbb{K}$, so the same goes for $\times$ on $\mathbb{K}[X]$ as well.

Finally, $\mathbb{K}[X]$ satisfies all conditions to be a commutative unital ring. ■

Remark : But $(\mathbb{K}[X],+,\times)$ is not a field. For instance, the polynomial $P(X) = X \in \mathbb{K}[X]-\{0\}$ has no multiplicative inverse in $\mathbb{K}[X]$: there is no polynomial $Q(X)\in\mathbb{K}[X]$ such that $XQ(X)=1$.

Proof : For any polynomial $Q(X) = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d \in \mathbb{K}[X]$, the constant term of $XQ(X) = a_0X + a_1X^2 + a_2X^3 + \cdots + a_dX^d \in \mathbb{K}[X]$ is 0 but that one of the constant polynomial $1\in\mathbb{K}[X]$ is 1. So the equality can not hold. ■

2.1.2 Degree

Definition 2.5 (*Degree*)

*The **degree** of a polynomial $P(X) \in \mathbb{K}[X]$, denoted $\mathbf{deg(P(X))}$ or shortly $\mathbf{deg(P)}$, is the highest exponent for terms with non zero coefficient. More precisely if $(a_n)_{n\in\mathbb{N}}$ are the coefficients of $P(X)$ then $\deg(P)$ is an element of $\mathbb{N} \cup \{-\infty\}$ defined by*

$$\deg(P) = \begin{cases} -\infty & \text{if } P(X) = 0 \\ \max\{n \in \mathbb{N} \,/\, a_n \neq 0\} & \text{otherwise} \end{cases}$$

*Moreover, the coefficient $a_{\deg(P)} \in \mathbb{K}^*$ (in case $P(X) \neq 0$) is called the **leading coefficient**.*

Some examples :

a) The (non zero) **constant polynomials** $P(X) = a_0 \in \mathbb{K}[X]$ where $a_0 \neq 0$ are of degree 0.

b) The **linear polynomials** $P(X) = a_0 + a_1 X \in \mathbb{K}[X]$ where $a_1 \neq 0$ are of degree 1.

c) The **quadratic polynomials** $P(X) = a_0 + a_1 X + a_2 X^2 \in \mathbb{K}[X]$ where $a_2 \neq 0$ are of degree 2.

d) The **cubic polynomials** $P(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 \in \mathbb{K}[X]$ where $a_3 \neq 0$ are of degree 3.

etc.

Remark : It is usefull to define the degree of the zero constant polynomial to be $-\infty$ (furthermore it is convenient to take $\max \emptyset = -\infty$ as a convention). In the following, we introduce the rules:

$$\forall k \in \mathbb{N} \cup \{-\infty\}, \quad \begin{cases} -\infty \leqslant k \\ \max\{k, -\infty\} = k \\ k + (-\infty) = (-\infty) + k = -\infty \end{cases}$$

Proposition 2.6

Let $P(X)$ and $Q(X)$ be two polynomials in $\mathbb{K}[X]$. Then the following properties hold

1. $\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}$ *with equality if* $\deg(P) \neq \deg(Q)$
2. $\deg(PQ) = \deg(P) + \deg(Q)$

Proof : We write $P(X) = \sum_{n=0}^{\deg(P)} a_n X^n$ and $Q(X) = \sum_{n=0}^{\deg(Q)} b_n X^n$.

1. In case $\deg(P) < \deg(Q)$ we get

$$(P+Q)(X) = \sum_{n=0}^{\deg(P)} (a_n + b_n) X^n + \sum_{n=\deg(P)+1}^{\deg(Q)} b_n X^n$$

And $b_{\deg(Q)} \neq 0$ implies that $\deg(P+Q) = \deg(Q) = \max\{\deg(P), \deg(Q)\}$. The same goes when $\deg(P) > \deg(Q)$. Now if $\deg(P) = \deg(Q) = d$ then

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

Consequently, we have $\deg(P+Q) \leqslant d = \max\{\deg(P), \deg(Q)\}$.

2. We have:

$$(PQ)(X) = \sum_{n=0}^{+\infty}\left(\sum_{\substack{k,\ell\in\mathbb{N}\\ k+\ell=n}} a_k b_\ell\right)X^n = \sum_{n=0}^{+\infty}\left(\sum_{\substack{k\leqslant\deg(P)\\ \ell\leqslant\deg(Q)\\ k+\ell=n}} a_k b_\ell\right)X^n = \sum_{n=0}^{\deg(P)+\deg(Q)}\left(\sum_{\substack{k\leqslant\deg(P)\\ \ell\leqslant\deg(Q)\\ k+\ell=n}} a_k b_\ell\right)X^n$$

Moreover the coefficient of the term with degree $n = \deg(P) + \deg(Q)$ is

$$\sum_{\substack{k\leqslant\deg(P)\\ \ell\leqslant\deg(Q)\\ k+\ell=\deg(P)+\deg(Q)}} a_k b_\ell = a_{\deg(P)} b_{\deg(Q)} \neq 0$$

The conclusion follows. ■

Remarks :

- The results remain true if $P(X)$ or $Q(X)$ (or both) is the zero constant polynomial.
- In the first property, the sufficient condition for equality is not necessary. For instance

$$\deg(X + X) = \deg(2X) = 1 = \deg(X)$$

Actually if $P(X)$ and $Q(X)$ are two polynomials of same degree $d \in \mathbb{N}$ whose their leading coefficients are respectively a_d and b_d then

$$\deg(P + Q) = d \Leftrightarrow a_d \neq -b_d$$

2.1.3 Polynomial arithmetic

Theorem 2.7 (*Polynomial division algorithm*)

For any given two polynomials $P(X)$ and $D(X)$ with $D(X) \neq 0$, there exist unique polynomials $Q(X)$ and $R(X)$ such that

$$\begin{cases} P(X) = Q(X)D(X) + R(X) \\ \deg(R) < \deg(D) \end{cases}$$

The polynomial $Q(X)$ is called the ***quotient****, $R(X)$ the* ***remainder****, $D(X)$ the* ***divisor*** *and $P(X)$ the* ***dividend****.*

Proof : Existence. Fix a polynomial $D(X) \in \mathbb{K}[X]$ with $D(X) \neq 0$ and call $d \geqslant 0$ its degree. Remark that if $d = 0$, that is $D(X) = b_0 \neq 0$, then $Q(X) = b_0^{-1}P(X)$ and $R(X) = 0$ are suitable. So we may assume that $d \geqslant 1$.

We will prove by induction the following property for every $k \geqslant 0$

$$\mathcal{P}_k = \text{“the existence part is true for every } P(X) \in \mathbb{K}[X] \text{ with } \deg(P) \leqslant k\text{”}$$

At first, if $\deg(P) \leqslant d - 1$ then $Q(X) = 0$ and $R(X) = P(X)$ are suitable. Hence, $\mathcal{P}_k$ is satisfied for every integer k such that $0 \leqslant k \leqslant d - 1$ (and at least for $k = 0$ since $d \geqslant 1$).

Now assume $\mathcal{P}_k$ is satisfied for a given integer $k \geqslant d - 1$. Let $P(X)$ be a polynomial in $\mathbb{K}[X]$ of degree $\deg(P) = k + 1 \geqslant d$. We write:

$$\begin{array}{rcll} P(X) & = & a_0 + a_1X + a_2X^2 + \cdots + a_dX^d + \cdots + a_{k+1}X^{k+1} & \text{with } a_{k+1} \neq 0 \\ D(X) & = & b_0 + b_1X + b_2X^2 + \cdots + b_dX^d & \text{with } b_d \neq 0 \end{array}$$

Consider the polynomial $P_1(X) = P(X) - a_{k+1}b_d^{-1}X^{k+1-d}D(X) \in \mathbb{K}[X]$. From Proposition 2.6, we have:

$$\deg(a_{k+1}b_d^{-1}X^{k+1-d}D(X)) = \deg(a_{k+1}b_d^{-1}X^{k+1-d}) + \deg(D) = (k+1-d) + d = k+1$$

and

$$\deg(P_1) \leqslant \max\left\{\deg(P), \deg(a_{k+1}b_d^{-1}X^{k+1-d}D(X))\right\} = \max\{k+1, k+1\} = k+1$$

Moreover the coefficient of the term in P_1 with degree $k+1$ is $a_{k+1} - a_{k+1}b_d^{-1}b_d = 0$. Then we have $\deg(P_1) \leqslant k$. By inductive hypothesis $\mathcal{P}_k$ applied to $P_1(X)$, there exist two polynomials $Q_1(X)$ and $R_1(X)$ such that

$$\begin{cases} P_1(X) = Q_1(X)D(X) + R_1(X) \\ \deg(R_1) < d \end{cases}$$

Now take $Q(X) = a_{k+1}b_d^{-1}X^{k+1-d} + Q_1(X)$ and $R(X) = R_1(X)$ then we get

$$\begin{cases} P(X) = a_{k+1}b_d^{-1}X^{k+1-d}D(X) + P_1(X) = Q(X)D(X) + R(X) \\ \deg(R) < d \end{cases}$$

Consequently $\mathcal{P}_{k+1}$ is satisfied and the conclusion follows by induction.

Uniqueness. By contradiction, assume $Q_1(X)$, $R_1(X)$ and $Q_2(X)$, $R_2(X)$ are such that

$$\begin{cases} P(X) = Q_1(X)D(X) + R_1(X) \\ \deg(R_1) < \deg(D) \end{cases} \quad \text{and} \quad \begin{cases} P(X) = Q_2(X)D(X) + R_2(X) \\ \deg(R_2) < \deg(D) \end{cases}$$

Then $Q_1(X)D(X) + R_1(X) = Q_2(X)D(X) + R_2(X)$ or equivalently

$$(Q_1(X) - Q_2(X))\,D(X) = R_2(X) - R_1(X)$$

From Proposition 2.6, we have:

$$\begin{cases} \deg\left((Q_1 - Q_2)\,D\right) & = & \deg\left(Q_1 - Q_2\right) + \deg(D) \\ \deg(R_2 - R_1) & \leqslant & \max\left\{\deg(R_1), \deg(R_2)\right\} < \deg(D) \end{cases}$$

So we get $\deg(Q_1 - Q_2) < 0$ (since $D(X) \neq 0$ implies $\deg(D) \geqslant 0$) that is $\deg(Q_1 - Q_2) = -\infty$ and hence $Q_1(X) - Q_2(X) = 0$. It follows $Q_1(X) = Q_2(X)$ and hence $R_1(X) = R_2(X)$. Finally the quotient and the remainder of the polynomial division algorithm are unique. ■

Examples : In order to compute the quotient and the remainder of a polynomial division algorithm, one may use a long division algorithm as follows

a) For $P(X) = X^3 - 12X^2 - 42$ and $D(X) = X - 3$

$$\begin{array}{rrcrcl} X^3 & & = & X^2 & (X-3) & +3X^2 \\ -12X^2 & +3X^2 & = & -9X & (X-3) & -27X \\ 0 & -27X & = & -27 & (X-3) & -81 \\ -42 & -81 & = & 0 & (X-3) & -123 \end{array}$$

and the sum of all these equalities gives after simplifications

$$X^3 - 12X^2 - 42 = (X^2 - 9X - 27)(X-3) - 123$$

that is $Q(X) = X^2 - 9X - 27$ and $R(X) = -123$

b) For $P(X) = X^4 + 7X^3 - 3X^2 - 11X + 5$ and $D(X) = X^2 - 2X - 3$

$$\begin{array}{rlcrll}
X^4 & & = & X^2 & (X^2-2X-3) & +2X^3+3X^2 \\
7X^3 & +2X^3 & = & 9X & (X^2-2X-3) & +18X^2+27X \\
-3X^2 & +3X^2+18X^2 & = & 18 & (X^2-2X-3) & +36X+54 \\
-11X & +27X+36X & = & 0 & (X^2-2X-3) & +52X \\
5 & +54 & = & 0 & (X^2-2X-3) & +59
\end{array}$$

and the sum of all these equalities gives after simplifications

$$X^4 + 7X^3 - 3X^2 - 11X + 5 = (X^2 + 9X + 18)(X^2 - 2X - 3) + 52X + 59$$

that is $Q(X) = X^2 + 9X + 18$ and $R(X) = 52X + 59$

c) For $P(X) = X^5 + X^4 - X - 1$ and $D(X) = X^2 - 1$

$$\begin{array}{rlcrll}
X^5 & & = & X^3 & (X^2-1) & +X^3 \\
X^4 & & = & X^2 & (X^2-1) & +X^2 \\
0 & +X^3 & = & X & (X^2-1) & +X \\
0 & +X^2 & = & 1 & (X^2-1) & +1 \\
-X & +X & = & 0 & (X^2-1) & \\
-1 & +1 & = & 0 & (X^2-1) &
\end{array}$$

and the sum of all these equalities gives after simplifications

$$X^5 + X^4 - X - 1 = (X^3 + X^2 + X + 1)(X^2 - 1)$$

that is $Q(X) = X^3 + X^2 + X + 1$ and $R(X) = 0$

Definition 2.8 (*Multiple and divisor*)

*Let $A(X)$ and $B(X)$ be two polynomials in $\mathbb{K}[X]$. We say $B(X)$ **divides** $A(X)$ or equivalently $A(X)$ is a **multiple** of $B(X)$ if*

$$\exists Q(X) \in \mathbb{K}[X] /\ A(X) = Q(X)B(X)$$

In this case, we write $\boldsymbol{B(X)|A(X)}$ or shortly $\boldsymbol{B|A}$.

Remark: A polynomial $B(X) \in \mathbb{K}[X]$ divides a polynomial $A(X) \in \mathbb{K}[X]$ if and only if

- either $B(X) = 0$ and $A(X) = 0$
- or $B(X) \neq 0$ and the remainder from the polynomial division algorithm with dividend $A(X)$ and divisor $B(X)$ is $R(X) = 0$

Proposition 2.9

Let $A(X)$ and $B(X)$ be two polynomials in $\mathbb{K}[X]$. If $B|A$ with $A(X) \neq 0$ then

$$\deg(B) \leqslant \deg(A)$$

Proof: There exists a polynomial $Q(X) \in \mathbb{K}[X]$ such that $A(X) = Q(X)B(X)$. Moreover $Q(X) \neq 0$ since $A(X) \neq 0$. In particular $\deg(Q) \geqslant 0$ and from Proposition 2.6

$$\deg(A) = \deg(QB) = \deg(Q) + \deg(B) \geqslant \deg(B)$$

■

Proposition 2.10

The ring $(\mathbb{K}[X], +, \times)$ *has no zero divisor. That is*

$$\forall (A(X), B(X)) \in (\mathbb{K}[X])^2,\ A(X)B(X) = 0 \Longrightarrow \textit{either } A(X) = 0 \textit{ or } B(X) = 0$$

Proof: Assume $A(X)B(X) = 0$ with $B(X) \neq 0$. The polynomial division algorithm with dividend 0 and divisor $B(X)$ is

$$0 = 0 \times B(X) + 0$$

But we have

$$0 = A(X) \times B(X) + 0$$

Consenquently the uniqueness part of Theorem 2.7 gives $A(X) = 0$. ∎

2.2 Polynomial maps

2.2.1 Definition

Definition 2.11 (*Polynomial map*)

Let $P(X)$ *be a polynomial in* $\mathbb{K}[X]$ *with coefficients* $(a_n)_{n\in\mathbb{N}}$*. The* ***polynomial map*** *associated to* $P(X)$ *is the following map*

$$\begin{array}{rccl} P: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & P(x) = \displaystyle\sum_{n=0}^{+\infty} a_n x^n \end{array}$$

Some examples:

a) The polynomial map associated to $P(X) = 0$ is the constant map $x \mapsto 0$.

b) The polynomial map associated to $P(X) = X$ is the identity map $x \mapsto x$.

c) The polynomial map associated to $P(X) = -1 + 2X + X^3 \in \mathbb{R}[X]$ is the cubic map

$$\begin{array}{rccl} P: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & P(x) = x^3 + 2x - 1 \end{array}$$

d) Recall that $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ is a commutative field since 2 is a prime number. Moreover we have

$$\overline{0} + \overline{0} \times \overline{0} = \overline{0} \quad \text{and} \quad \overline{1} + \overline{1} \times \overline{1} = \overline{2} = \overline{0}$$

Consequently the polynomial map associated to $P(X) = X + X^2 \in \mathbb{Z}/2\mathbb{Z}[X]$ is the constant map

$$\begin{array}{rccl} P: & \mathbb{Z}/2\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z} \\ & x & \mapsto & P(x) = \overline{0} \end{array}$$

But notice $P(X) \neq 0$.

Proposition 2.12

Denote $\mathcal{F}(\mathbb{K})$ the set of all functions from $\mathbb{K}$ to itself. $\mathcal{F}(\mathbb{K})$ has a natural ring structure coming from that one of $\mathbb{K}$. Then the following map

$$\begin{array}{rcl} \mathbb{K}[X] & \to & \mathcal{F}(\mathbb{K}) \\ P(X) & \mapsto & P \end{array}$$

is a ring homomorphism. In particular for any given $\alpha \in \mathbb{K}$, the following map

$$\begin{array}{rcl} \mathbb{K}[X] & \to & \mathbb{K} \\ P(X) & \mapsto & P(\alpha) \end{array}$$

is a ring homomorphism as well.

Proof: Everything comes from the definitions of addition and multiplication of two polynomials and from the ring homomorphism $\mathcal{F}(\mathbb{K}) \to \mathbb{K},\ f \mapsto f(\alpha)$. ■

2.2.2 Derivative polynomial

Definition 2.13 (*Derivative polynomial*)

Let $P(X)$ be a polynomial in $\mathbb{K}[X]$ with coefficients $(a_n)_{n\in\mathbb{N}}$. The ***derivative polynomial*** *of $P(X)$ is the following polynomial*

$$P'(X) = a_1 + 2a_2X + 3a_3X^2 + \cdots = \sum_{n=0}^{+\infty}(n+1)a_{n+1}X^n = \sum_{n=1}^{+\infty} na_nX^{n-1}$$

By induction over $k \geqslant 1$, we define the ***k^{th} order polynomial derivative****, denoted* $\boldsymbol{P^{(k)}(X)}$*, to be the polynomial derivative of $P^{(k-1)}(X)$ with the notation $P^{(0)} = P$ (and then $P^{(1)} = P'$).*

Remarks:

- Notice that any integer $n \in \mathbb{N}$ may be considered in $\mathbb{K}$ if we write it as follows

$$n = \underbrace{1+1+1+\cdots+1}_{n \text{ times}} \in \mathbb{K} \quad \text{with } 1 \in \mathbb{K}$$

  In particular the derivative polynomial of any polynomial with coefficients in $\mathbb{K}$ is well in $\mathbb{K}[X]$.
- The polynomial map P' associated to the derivative polynomial $P'(X)$ of a polynomial $P(X)$ is the derivative of the map P as expected. But limit, differentiation or any calculus tool are not needed here to define the derivative of a polynomial map.

Example: Consider $P(X) = -7 + 8X - 5X^2 + 2X^3 - X^5 \in \mathbb{R}[X]$. Then

$$\begin{array}{rcl} P'(X) = P^{(1)}(X) & = & 8 - 10X + 6X^2 - 5X^4 \\ P^{(2)}(X) & = & -10 + 12X - 20X^3 \\ P^{(3)}(X) & = & 12 - 60X^2 \\ P^{(4)}(X) & = & -120X \\ P^{(5)}(X) & = & -120 \\ P^{(6)}(X) & = & 0 \\ \text{etc.} & & \end{array}$$

Proposition 2.14

The following properties hold

1. $\forall (P(X),Q(X)) \in (\mathbb{K}[X])^2 \quad \begin{cases} (P+Q)'(X) = P'(X)+Q'(X) \\ (PQ)'(X) = P'(X)Q(X)+P(X)Q'(X) \end{cases}$

2. *Consider the polynomial* $P(X) = X^n$ *with* $n \in \mathbb{N}$. *Then*

$$\forall k \geqslant 1,\ (P)^{(k)}(X) = \begin{cases} \frac{n!}{(n-k)!}X^{n-k} & \text{if } 1 \leqslant k \leqslant n \\ 0 & \text{if } k \geqslant n+1 \end{cases}$$

where $\frac{n!}{(n-k)!} = n(n-1)(n-2)\dots(n-k+1)$

3. $P(X) \in \mathbb{K}[X]$ *is a constant polynomial if and only if* $P'(X) = 0$

4. *If* $P(X) \in \mathbb{K}[X]$ *is a non constant polynomial then* $\deg(P') = \deg(P) - 1$
More generally, if $P^{(k)}(X) \neq 0$ *for some* $k \geqslant 1$ *then* $\deg(P^{(k)}) = \deg(P) - k$

Proof: 1. Denote respectively $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ the coefficients of $P(X)$ and $Q(X)$. Then

$$(P+Q)'(X) = \sum_{n=1}^{+\infty} n(a_n+b_n)X^{n-1} = \sum_{n=1}^{+\infty} na_nX^{n-1} + \sum_{n=1}^{+\infty} nb_nX^{n-1} = P'(X)+Q'(X)$$

And, using new indices $n' = n-1$, $k' = k-1$ and $\ell' = \ell - 1$, we get

$$\begin{aligned}
(PQ)'(X) &= \sum_{n=1}^{+\infty} n \left(\sum_{\substack{k,\ell\in\mathbb{N} \\ k+\ell=n}} a_k b_\ell \right) X^{n-1} \\
&= \sum_{n=1}^{+\infty} \left(\sum_{\substack{k,\ell\in\mathbb{N} \\ k+\ell=n}} (k+\ell) a_k b_\ell \right) X^{n-1} \\
&= \sum_{n'=0}^{+\infty} \left(\sum_{\substack{k',\ell\in\mathbb{N} \\ k'+\ell=n'}} (k'+1) a_{k'+1} b_\ell \right) X^{n'} + \sum_{n'=0}^{+\infty} \left(\sum_{\substack{k,\ell'\in\mathbb{N} \\ k+\ell'=n'}} a_k (\ell'+1) b_{\ell'+1} \right) X^{n'} \\
&= \left(\sum_{k'=0}^{+\infty} (k'+1)a_{k'+1}X^{k'} \right) \left(\sum_{\ell=0}^{+\infty} b_\ell X^\ell \right) + \left(\sum_{k=0}^{+\infty} a_k X^k \right) \left(\sum_{k'=0}^{+\infty} (\ell'+1) b_{\ell'+1} X^{\ell'} \right) \\
&= P'(X)Q(X) + P(X)Q'(X)
\end{aligned}$$

2. An induction over the order $k \geqslant 1$ gives the result.

3. If $P(X) = a_0 \in \mathbb{K}$ then $P'(X) = 0$ by definition of the polynomial derivative. Conversely, $P'(X) = \sum_{n=1}^{+\infty} na_nX^{n-1} = 0$ implies that $a_n = 0$ for every $n \geqslant 1$. The result follows.

4. Let $P(X)$ be a non constant polynomial in $\mathbb{K}[X]$ and denote by $a_{\deg(P)}$ its leading coefficient. By definition of the polynomial derivative, we have $\deg(P') \leqslant \deg(P) - 1$. Moreover the coefficient of the term with degree $n = \deg(P) - 1$ is $\deg(P)a_{\deg(P)}$ which is not zero since $\deg(P) \geqslant 1$ (P is non constant) and $a_{\deg(P)} \neq 0$ (as leading coefficient of $P(X)$). Thus, we have $\deg(P') = \deg(P) - 1$. The remain follows by induction over the order $k \geqslant 1$. ■

Corollary 2.15

Let $P(X)$ be a polynomial in $\mathbb{K}[X]$ of degree $d = \deg(P)$. Then

$$\forall k \geqslant d+1,\ P^{(k)}(X) = 0$$

Theorem 2.16 (*Exact Taylor's formula*)

Let $P(X)$ be a polynomial in $\mathbb{K}[X]$ of degree $d = \deg(P)$. Then

$$P(X) = P(0) + P'(0)X + \frac{P^{(2)}(0)}{2}X^2 + \cdots + \frac{P^{(d)}(0)}{d!}X^d = \sum_{n=0}^{d} \frac{P^{(n)}(0)}{n!}X^n$$

where $\frac{1}{n!} = (1 \times 2 \times 3 \times \cdots \times n)^{-1}$

More generally, for any $a \in \mathbb{K}$ we have

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

Proof: Call $R(X)$ the following polynomial

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

We will prove by induction for every integer k with $0 \leqslant k \leqslant d$ that $R^{(d-k)}(X) = 0$. In particular, $k = d$ will give the result. At first, using Proposition 2.6, we have:

$$\det(R) \leqslant \max\left\{\deg(P), \deg\left(\sum_{n=0}^{d} \frac{P^{(n)}(a)}{n!}(X-a)^n\right)\right\} \leqslant d$$

Then from Corollary 2.15 and Proposition 2.14, we get $(R^{(d)})'(X) = R^{(d+1)}(X) = 0$ that is $R^{(d)}(X)$ is a constant polynomial. Consequently Proposition 2.14 gives

$$R^{(d)}(X) = R^{(d)}(a) = P^{(d)}(a) - \sum_{n=0}^{d-1} \frac{P^{(n)}(a)}{n!}0 - \frac{P^{(d)}(a)}{d!}d! = P^{(d)}(a) - P^{(d)}(a) = 0$$

So the inductive hypothesis is true for $k = 0$. Now assume the inductive hypothesis is satisfied for a given integer k with $0 \leqslant k \leqslant d-1$. Then $(R^{(d-k-1)})'(X) = R^{(d-k)}(X) = 0$ that is $R^{(d-k-1)}(X)$ is a constant polynomial. Consequently Proposition 2.14 gives

$$\begin{aligned}
R^{(d-k-1)}(X) &= R^{(d-k-1)}(a) \\
&= P^{(d-k-1)}(a) - \sum_{n=0}^{d-k-2} \frac{P^{(n)}(a)}{n!}0 - \frac{P^{(d-k-1)}(a)}{(d-k-1)!}(d-k-1)! \\
&\quad - \sum_{n=d-k}^{d} \frac{P^{(n)}(a)}{n!}\frac{n!}{(n-(d-k-1))!}(a-a)^n \\
&= P^{(d-k-1)}(a) - 0 - P^{(d-k-1)}(a) - 0 \\
&= 0
\end{aligned}$$

Finally the inductive hypothesis is still true for $k+1$. The result follows by induction. ■

2.2.3 Root

Definition 2.17 (*Root*)

*$\alpha \in \mathbb{K}$ is said to be a **root** of a polynomial $P(X) \in \mathbb{K}[X]$ if $P(\alpha) = 0$.*

Example: 1 and 3 are roots of $P(X) = 3-4X+X^2$ since $P(1) = 3-4+1 = 0$ and $P(3) = 3-12+9 = 0$. Actually $P(X) = (X-1)(X-3)$ in order that $(X-1)|P(X)$ and $(X-3)|P(X)$.

Example: 1 and -1 are roots of $P(X) = 1-2X^2+X^4 = (X^2-1)^2 = (X-1)^2(X+1)^2$.

Proposition 2.18

$\alpha \in \mathbb{K}$ is a root of $P(X) \in \mathbb{K}[X]$ if and only if $(X-\alpha)|P(X)$.

Proof: **Sufficient.** If $(X-\alpha)|P(X)$ then there exists a polynomial $Q(X) \in \mathbb{K}[X]$ such that $P(X) = (X-\alpha)Q(X)$ and then $P(\alpha) = (\alpha-\alpha)Q(\alpha) = 0$.

Necessary. From Theorem 2.7, we get two polynomials $Q(X)$ and $R(X)$ such that

$$\begin{cases} P(X) = (X-\alpha)Q(X) + R(X) \\ \deg(R) < \deg(X-\alpha) = 1 \end{cases}$$

In particular, $R(X)$ is a constant polynomial that is $R(X) = r \in \mathbb{K}$. But α is a root of $P(X)$ implies

$$0 = P(\alpha) = (\alpha-\alpha)Q(\alpha) + r = r$$

Consequently $R(X) = 0$ and $P(X) = (X-\alpha)Q(X)$ as needed. ■

Further example:

a) The polynomial $P(X) = 1+X^2 \in \mathbb{R}[X]$ has no root since $\forall x \in \mathbb{R},\ P(x) = 1+x^2 \geqslant 1 > 0$. In particular, $P(X)$ can not be written as a product of two linear polynomials in $\mathbb{R}[X]$.

b) But $\imath$ and $-\imath$ are roots of $Q(X) = 1+X^2 \in \mathbb{C}[X]$ since $Q(X) = (X-\imath)(X+\imath)$.

Definition 2.19 (*Root of higher multiplicity*)

*Let $k \geqslant 1$ be a positive integer. $\alpha \in \mathbb{K}$ is said to be a **root of multiplicity k** of a polynomial $P(X) \in \mathbb{K}[X]$ if $(X-\alpha)^k|P(X)$ and $(X-\alpha)^{k+1} \nmid P(X)$, or equivalently if*

$$\exists Q(X) \in \mathbb{K}[X]/\ P(X) = (X-\alpha)^k Q(X) \text{ and } Q(\alpha) \neq 0$$

*Furthermore, the **multiplicity** of a root $\alpha \in \mathbb{K}$ of a polynomial $P(X) \neq 0$ is the following positive integer*

$$k_\alpha = \max\left\{k \geqslant 1 \ /\ (X-\alpha)^k|P(X)\right\}$$

Proposition 2.20

$\alpha \in \mathbb{K}$ is a root of multiplicity $k \geqslant 1$ of the polynomial $P(X) \neq 0$ if and only if

$$P(\alpha) = P'(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \quad \text{and} \quad P^{(k)}(\alpha) \neq 0$$

Proof: Sufficient. The Taylor's formula (see Theorem 2.16) gives

$$\begin{aligned} P(X) &= \sum_{n=0}^{+\infty} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n \\ &= \sum_{n=0}^{k-1} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n + \sum_{n=k}^{+\infty} \frac{P^{(n)}(\alpha)}{n!}(X-\alpha)^n \\ &= 0 + (X-\alpha)^k \sum_{n=0}^{+\infty} \frac{P^{(n+k)}(\alpha)}{(n+k)!}(X-\alpha)^n \\ &= (X-\alpha)^k Q(X) \end{aligned}$$

with $Q(\alpha) = \frac{P^{(k)}(\alpha)}{k!} + \sum_{n=1}^{+\infty} \frac{P^{(n+k)}(\alpha)}{(n+k)!}(\alpha-\alpha)^n = \frac{P^{(k)}(\alpha)}{k!} + 0 \neq 0$ since $P^{(k)}(\alpha) \neq 0$

Necessary. If $P(X) = (X-\alpha)^k Q(X)$ with $Q(\alpha) \neq 0$ then Proposition 2.14 gives

$$P(\alpha) = P'(\alpha) = P^{(2)}(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0 \quad \text{and} \quad P^{(k)}(\alpha) = k!Q(\alpha) \neq 0$$

■

Proposition 2.21

Let $P(X) \neq 0$ be a polynomial in $\mathbb{K}[X]$. Denote by $k_1, k_2, \ldots, k_n$ the multiplicities of the roots of $P(X)$. Then

$$k_1 + k_2 + \cdots + k_n \leqslant \deg(P)$$

In particular $P(X)$ has at most $\deg(P)$ roots.

Proof: Denote by $\alpha_1, \alpha_2, \ldots, \alpha_n$ the roots of $P(X)$ associated to the multiplicities $k_1, k_2, \ldots, k_n$. Then the polynomial $(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\ldots(X-\alpha_n)^{k_n}$ divides $P(X)$. But from Proposition 2.6 we have:

$$\deg\Big((X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\ldots(X-\alpha_n)^{k_n}\Big) = k_1 + k_2 + \cdots + k_n$$

Hence, the conclusion follows from Proposition 2.9. ■

To conclude, just state the following important and powerful result without proof.

Theorem 2.22 (*Fundamental theorem of algebra*)

Every non constant polynomial in $\mathbb{C}[X]$ has at least one root.

Remark: In particular, the inequality of Proposition 2.21 becomes an equality in $\mathbb{C}[X]$. More precisely, any non constant polynomial $P(X) \in \mathbb{C}[X]$ may be written as a product of linear polynomials:

$$P(X) = C(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\ldots(X-\alpha_n)^{k_n}$$

where

- $C \in \mathbb{C}^*$ is the leading coefficient of $P(X)$
- $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of $P(X)$
- $k_1, k_2, \ldots, k_n$ are their associated multiplicities