$\mathbb{K}$ désigne un corps commutatif.
Dans la pratique $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

1 Notion de polynôme formel

Définition 1 *On appelle polynôme à coefficients dans $\mathbb{K}$ en l'indéterminée X tout objet noté $P = \sum_{k=0}^{+\infty} a_k X^k$, où $(a_k)_{k\in\mathbb{N}}$ est une suite d'éléments de $\mathbb{K}$ nuls à partir d'un certain rang, appelée suite des coefficients de P.*
Pour tout $k \in \mathbb{N}$, le coefficient a_k est appelé le coefficient de degré k du polynôme.
On note $\mathbb{K}[X]$ l'ensemble de ces éléments.

Remarques 1
- *La suite $(a_k)_{k\in\mathbb{N}}$ est nulle à partir d'un certain rang, c'est-à-dire qu'il existe n tel que pour tout $k > n$, $a_k = 0$ et $a_n \neq 0$.*
  On en déduit que la somme $\sum_{k=0}^{+\infty} a_k X^k$ est finie et P s'écrit : $a_0 + a_1 X + \cdots + a_n X^n$.
- *L'indéterminée X n'est pas une variable, c'est une lettre qui permet de désigner les coefficients respectifs d'un polynôme.*

Exemple 1
- *$2+X-X^2$ est un polynôme de $\mathbb{R}[X]$ dont la suite des coefficients est $(2, 1, -1, 0, 0, 0, \cdots)$.*
- *X^4 est un polynôme de $\mathbb{R}[X]$ dont la suite des coefficients est $(0, 0, 0, 0, 1, 0, 0, 0, \cdots)$.*
- *0 est un polynôme de $\mathbb{R}[X]$ dont la suite des coefficients est $(0, 0, 0, \cdots)$.*

Définition 2 *Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$.*
*$P = Q$ **si et seulement si** pour tout $k \in \mathbb{N}$, $a_k = b_k$.*

Définition 3
*Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$ **non nul**.*
*Le plus grand indice k pour lequel $a_k \neq 0$ est appelé le **degré de** P et est noté $\partial° P$ ou $\deg(P)$.*
Le coefficient de degré $\partial° P$ de P est appelé son coefficient dominant.
*S'il est égal à 1, on dit que le polynôme P est **unitaire**.*
Par convention le polynôme nul est de degré $-\infty$.

Définition 4 *On dit qu'un polynôme $P \in \mathbb{K}[X]$ est associé à un polynôme $Q \in \mathbb{K}[X]$ s'il exite $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.*

On montre que l'association de polynômes définit une relation d'équivalence sur $\mathbb{K}[X]$.

Remarques 2 *Deux polynômes associés ayant le même coefficient dominant sont égaux.*

Définition 5 *Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$.*

- *On appelle **somme** de P et Q le polynôme $\sum_{k=0}^{+\infty} (a_k + b_k) X^k$, noté $P + Q$.*
- *On appelle **produit** de P et Q le polynôme $\sum_{k=0}^{+\infty} c_k X^k$ où , pour tout $k \in \mathbb{N}$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, noté $P \times Q$ ou PQ.*

Justification de la définition de somme et produit de deux polynômes

Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$.

- Montrons que $\sum_{k=0}^{+\infty}(a_k+b_k)X^k \in \mathbb{K}[X]$:

  $\forall k > \max(\partial^\circ P, \partial^\circ Q),\ a_k = \cdots$ et $b_k = \cdots$,
  donc :
  $\forall k > \max(\partial^\circ P, \partial^\circ Q),\ a_k + b_k = \cdots$.
  La suite $(a_k+b_k)_{k\in\mathbb{N}}$ est donc nulle à partir d'un certain rang, donc : $\sum_{k=0}^{+\infty}(a_k+b_k)X^k \in \mathbb{K}[X]$.

- Montrons que $\sum_{k=0}^{+\infty} c_k X^k \in \mathbb{K}[X]$ où, pour tout $k \in \mathbb{N}$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$:

  Posons $N = \max(\partial^\circ P, \partial^\circ Q)$.
  On a : $\forall i > N,\ a_i = 0$ et $b_i = 0$.
  - ⋆ Soit $k > 2N$. Montrons que $c_k = 0$.
    - ⋄ Fixons $i \in [\![0, k]\!]$.
      On a : $i > N$ ou $k - i > N$,
      donc : $a_i = 0$ ou $b_{k-i} = 0$,
      donc : $a_i b_{k-i} = 0$.

    On en dÃ©duit que : $c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0$.

  On a montré que, pour tout $k > 2N$, $c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0$. Donc : $\sum_{k=0}^{+\infty} c_k X^k$ (où, pour tout $k \in \mathbb{N}$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$) est un polynôme.

- Cas particulier de la multiplication par un polynôme constant

  Soient $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$ avec $\begin{cases} b_0 = \lambda \\ b_i = 0 \text{ pour } i \geqslant 1 \end{cases}$ On a alors :

$$QP = \sum_{k=0}^{+\infty} c_k X^k = \sum_{k=0}^{+\infty}\left(\sum_{i=\cdots}^{\cdots} \cdots\cdots\cdots\right) X^k = \sum_{k=0}^{+\infty} \cdots\cdots X^k$$

  On confondra le polynôme $Q = \lambda$ et le nombre $\lambda \in \mathbb{K}$.
  La loi externe : $\begin{array}{ccc} \mathbb{K} \times \mathbb{K}[X] & \to & \mathbb{K}[X] \\ \left(\lambda, \sum_{k=0}^{+\infty} \lambda a_k X^k\right) & \mapsto & \sum_{k=0}^{+\infty} \lambda a_k X^k \end{array}$
  coincide avec la multiplication interne d'un polynôme constant par un polynôme quelconque.

□

Proposition 1 *Soient $P, Q \in \mathbb{K}[X]$.*

- $\partial^\circ(P+Q) \leqslant max(\partial^\circ P, \partial^\circ Q)$
  *L'inégalité est stricte **si et seulement si** les coefficients dominants de P et Q sont opposés.*
- $\partial^\circ(PQ) = \partial^\circ P + \partial^\circ Q$

Proposition 2 $(\mathbb{K}[X], +, \times)$ *est un anneau commutatif intègre d'élément nul le polynôme nul et d'élément unité le polynôme constant égal à* 1.

Rappelons qu'un anneau est un ensemble muni de deux lois de composition interne, dans le cas de $\mathbb{K}[X]$, on a :

- l'addition de polynômes (qui est fait déjà une groupe commutatif)
- la multiplication (interne) de polynômes qui est associative, commutative, dont le neutre est 1, et qui est distributive par rapport à l'addition.

L'ensemble de ces propriétés donne une structure d'anneau commutatif unitaire à $\mathbb{K}[X]$.
De plus, $\mathbb{K}[X]$ est intègre c'est à dire que si P et Q sont deux éléments de $\mathbb{K}[X]$, $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$. (Ceci se montre en utilisant la propriété sur le degré $\partial^\circ(PQ) = \partial^\circ P + \partial^\circ Q$ pour P et Q non nul).

Remarques 3 $\mathbb{K}[X]$ *muni de l'addition + (interne), et de la multiplication externe · est un* $\mathbb{K}$*-espace vectoriel . On rappelle que l'on note* $K_n[X]$ *l'espace vectoriel des polynômes de degré inférieur ou égal à* n*, dont une base est donnée par* $(1, X, \ldots, X^n)$*, et* $\dim \mathbb{K}_n[X] = n + 1$*.*

Remarques 4 $\mathbb{K}[X]$ *muni des lois + (interne), · (externe) et × (interne) est aussi une* $\mathbb{K}$*-algèbre unitaire associative et commutative.*

2 Racines d'un polynôme

2.1 Valeur d'un polynôme en un point

Définition 6 (Evaluation polynomiale et fonction polynomiale)
Soit $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$*.*

- *Pour tout* $\lambda \in \mathbb{K}$*, on note* $P(\lambda)$ *l'élément de* $\mathbb{K}$ *défini par :* $P(\lambda) = \sum_{k=0}^{+\infty} a_k \lambda^k$*.*
- *L'application* $\widetilde{P} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & P(x) \end{array}$ *est appelée fonction polynômiale associée à* P*.*

Il faut distinguer :
- la fonction polynomiale $\widetilde{P}$ (application) du polynôme sous-jacent P (expression)
- l'élément x (de $\mathbb{K}$) de l'indéterminée X (lettre permettant de décrire le polynôme).

Proposition 3 *L'application* $\begin{array}{ccc} \mathbb{K}[X] & \to & \mathbb{K}^{\mathbb{K}} \\ P & \mapsto & \widetilde{P} \end{array}$ *est un morphisme d'anneaux.*

Rappelons que $\mathbb{K}^{\mathbb{K}}$ est l'ensemble des applications de $\mathbb{K}$ dans $\mathbb{K}$; c'est une $\mathbb{K}$-algèbre commutative, associative et unitaire pour les lois usuelles.
On vérifie que c'est un morphisme d'anneau en montrant que $\widetilde{P + \alpha Q} = \widetilde{P} + \alpha\widetilde{Q}$ et $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$ où $P, Q \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

Remarques 5 *Dans ce cas où* K *est un corps infini, on peut identifier tout polynôme à sa fonction polynômiale. Dans ce cas, nous noterons* $P = \widetilde{P}$ *suivant la commodité.*

2.2 Définition de racines d'un polynôme

Définition 7 *Soient* $P \in \mathbb{K}[X]$ *et* $a \in \mathbb{K}$*.*
On dit que a *est racine de* P *(dans* $\mathbb{K}$*)**si et seulement si*** $P(a) = 0$*.*

La notion de racine de P dans $\mathbb{K}$ n'est pas superflue. Le polynôme $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$ mais il en a deux dans $\mathbb{C}$.

3 Arithmétique dans $\mathbb{K}[X]$

3.1 Relation de divisibilité

Définition 8 *Soient* $A, B \in \mathbb{K}[X]$*.*
On dit que A ***divise*** B*, **si et seulement si** il existe* $P \in \mathbb{K}[X]$ *tel que* $B = AP$*.*
Cette relation se note $A|B$*.*

Remarques 6 *On dit également* A *est **un diviseur de*** B*, ou* B *est **divisible par*** A*, ou* B *est **un multiple de*** A*.*

Exemple 2
- *$X-3$ divise X^2-4X+3 dans $\mathbb{R}[X]$ en effet :*

- *Un polynôme constant λ non nul divise tout polynôme P en effet :*

- *Tout polynôme A divise le polynôme nul en effet :*

- *0 ne divise aucun polynôme $B \neq 0$ en effet :*

Proposition 4 *Soient $A, B, C, D \in \mathbb{K}[X]$.*
1. *$A|A$.*
2. ***Si** $A|B$ et $B|C$ **alors** $A|C$.*
3. *$(A|B$ et $B|A \iff A$ et B sont associés$)$.*
4. ***Si** $A|B$ et $A|C$ **alors**, pour tout $Q, R \in \mathbb{K}[X]$, $A|(QB+RC)$.*
5. ***Si** $A|B$ et $C|D$ **alors** $AC|BD$.*
6. *Si $D \neq 0$: $A|B \iff AD|BD$.*

3.2 Division euclidienne

Théorème 1 *Soient $A, B \in \mathbb{K}[X]$, $B \neq 0$.*
Il existe un unique couple $(Q, R) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que

$$A = BQ + R \text{ et } \partial^\circ R < \partial^\circ B$$

A est appelé le dividende, B le diviseur, Q le quotient et R le reste.

Ce théorème a été démontré en PeiP1.

Exemple 3 *Effectuer la division euclidienne de $A = X^4+2X^3-X+6$ par $B = X^3-6X^2+X+4$ dans $\mathbb{R}[X]$.*

Proposition 5 *Soient $A, B \in \mathbb{K}[X]$ et $B \neq 0$.*
*B divise A **si et seulement si** le reste de la division euclidienne de A par B est nul.*

Proposition 6 *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.*
*a est racine de P **si et seulement si** $X-a$ divise P.*

Définition 9 *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.*
- *L'ensemble $\{k \in \mathbb{N}, (X-a)^k$ divise $P\}$ possède un plus grand élément m appelé **multiplicité** de a dans P.*
- *Une racine est dite simple si $m=1$, double si $m=2$, etc...*
- *Plus concrêtement, m est caractérisé par deux propositions équivalentes :*
  1. *P est divisible par $(X-a)^m$ mais pas par $(X-a)^{m+1}$*
  2. *Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^m Q$ et $Q(a) \neq 0$.*

Exemple 4 *La multiplicité de 1 dans $P = X^4+3X^3-3X^2-7X+6$ est égale à 2.*

3.3 PGCD

Définition 10 *Soient $A, B \in \mathbb{K}[X]$.*

- *On appelle* ***diviseur commun*** *de A et B tout polynôme D qui est à la fois diviseur de A et diviseur de B.*
- *On appelle* ***multiple commun*** *de A et B tout polynôme M qui est à la fois multiple de A et multiple de B.*

Exemple 5

- *Soient A et B deux polynômes quelconques, tous les polynômes constants non nuls sont des diviseurs communs à A et B.*
- *$X-1$ est un diviseur commun à X^4-1 et X^2-3X+2.*

Proposition 7 *Soient $A, B \in \mathbb{K}[X]$ et $B \neq 0$.*
Si $A = BQ + R$ alors tout diviseur commun de A et B est aussi diviseur commun de B et R.

Définition 11 *Soient $A, B \in \mathbb{K}[X]$.*
On appelle plus grand commun diviseur (PGCD) de A et de B tout polynôme $D \in \mathbb{K}[X]$ tel que :

- *D est un diviseur commun de A et B : $D|A$ et $D|B$;*
- *D est un multiple de tout diviseur commun de A et B : $\forall \Delta \in \mathbb{K}[X], (\Delta|A$ et $\Delta|B) \Rightarrow \Delta|D$.*

Théorème 2 (Existence et unicité du PGCD) *Soient $A, B \in \mathbb{K}[X]$.*

- *Si $A \neq 0$ ou $B \neq 0$, il existe un unique PGCD* ***unitaire*** *de A et B, noté PGCD(A, B).*
  Il est clair que 0 est l'unique PGCD de 0 et 0 et on peut poser $PGCD(0,0) = 0$.
- *Les autres PGCD de A et B sont tous les $\lambda PGCD(A, B)$ où $\lambda \in \mathbb{K}^*$.*

L'existence du PGCD est établie par l'algorithme d'Euclide, qui en fournit aussi une construction.
Preuve du théorème 2

Montrons l' unicité du PGCD unitaire

Soient D_1 et D_2 deux PGCD de A et B **unitaires**.
D_1 est un PGCD de A et B et D_2 est un diviseur commun de A et B donc : ....
D_2 est un PGCD de A et B et D_1 est un diviseur commun de A et B donc : ....
On en déduit que D_1 et D_2 sont associés ;
Si l'un est nul alors l'autre aussi et $D_1 = D_2$.
S'ils ne sont pas nuls, ils sont unitaires et associés donc égaux.

Montrons l' existence du PGCD unitaire

- Si $A = B = 0$ alors $D = 0$ convient.
- Sinon, quitte à échanger A et B on peut supposer $B \neq 0$.
  Posons $A = A_0$ et $A_1 = B$. On réalise les divisions euclidiennes suivantes tant que les restes obtenus sont non nuls.

$$\begin{array}{rcl} A_0 & = & A_1Q_1 + A_2 \text{ avec } \partial^\circ A_2 < \partial^\circ A_1 \\ \vdots & = & \vdots \\ A_{m-2} & = & A_{m-1}Q_m + A_m \text{ avec } \partial^\circ A_m < \partial^\circ A_{m-1} \\ A_{m-1} & = & A_mQ_m + 0 \end{array}$$

  Ce processus s'arrête puisque $\partial^\circ A_1 > \partial^\circ A_2 > \ldots$ et ces quantités sont des entiers naturels.
  Alors, tout diviseur commun de $A = A_0$ et $B = A_1$ est aussi diviseur commun de A_{m-1} et A_{m-1} et aussi diviseur commun de A_m et 0 .
  Le polynôme D unitaire associé à A_m convient donc.

Exemple 6 *Déterminons* $D = PGCD(X^3 + X^2 - 2, X^3 + X - 2)$. *Par divisions euclidiennes successives :*
$X^3 + X^2 - 2 = (X^3 + X - 2) \times 1 + X^2 - X$,
$X^3 + X - 2 = (X^2 - X)(X + 1) + 2X - 2$,
$X^2 - X = (2X - 2) \times \frac{1}{2}X + 0$.
Donc D *est le polynôme unitaire associé au dernier reste non nul, i.e. associé à* $2X - 2$. *Ainsi* $D = X - 1$.

Théorème 3 (Théorème de Bézout, version 1) *Soient* $A, B \in \mathbb{K}[X]$. *Si* $D = PGCD(A, B)$ *alors il existe* $U, V \in \mathbb{K}[X]$ *tels que* $D = AU + BV$

☠☠☠ Le couple (U, V) n'est pas unique.

Preuve du théorème 3

- Si $A = B = 0$ alors $D = 0$ et U, V quelconques conviennent.
- Sinon, on réalise comme ci-dessus l'algorithme d'Euclide puis on écrit successivement les A_i sous la forme $AU_i + BV_i$ avec $U_i, V_i \in \mathbb{K}[X]$. A terme on parvient à écrire D sous la forme $AU + BV$.

Exemple 7 *Reprenons* $A = X^3 + X^2 - 2$ *et* $B = X^3 + X - 2$ *pour lesquels* $D = PGCD(A, B) = X - 1$.
En renversant les divisions euclidiennes précédentes
$X^2 - X = A - B$,
$2X - 2 = B - (X + 1)(X^2 - X) = B - (X + 1)(A - B)$,
puis
$D = 12(X + 2)B - 12(X + 1)A = AU + BV$ *avec* $U = -12(X + 1)$ *et* $V = 12(X + 2)$

3.4 Polynômes premiers entre eux

Définition 12 *Soient* $A, B \in \mathbb{K}[X]$.
On dit que A *et* B *sont premiers entre eux* ***si et seulement si*** $PGCD(A, B) = 1$.

Exemple 8 *Soient* $a, b \in \mathbb{K}$. ***Si*** $a \neq b$ ***alors*** $X - a$ *et* $X - b$ *sont premiers entre eux.*

Théorème 4 (Théorème de Bézout, version 2) *Soient* $A, B \in \mathbb{K}[X]$. *Les assertions suivantes sont équivalentes :*

(i) A *et* B *sont premiers entre eux.*

(ii) Il existe deux polynômes $U, V \in \mathbb{K}[X]$ *tels que* $AU + BV = 1$.

Preuve :

- On suppose que A et B sont premiers entre eux.
  Par définition $\text{PGCD}(A, B) = 1_{\mathbb{K}[X]}$, en appliquant le théorème de Bezout version 1, on en déduit qu' il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1_{\mathbb{K}[X]}$.

- On supppose qu' il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1_{\mathbb{K}[X]}$.
  Soit D un diviseur commun de A et B.
  Alors D divise $AU + BV$, c'est-Ã -dire que D divise $1_{\mathbb{K}[X]}$.
  Or les seuls diviseurs de $1_{\mathbb{K}[X]}$ dans $\mathbb{K}[X]$ sont les constantes non nulles.
  On en déduit que $\text{PGCD}(A, B)$ est une constante non nulle.
  Or le PGCD est unitaire, donc $PGCD(A, B) = 1_{\mathbb{K}[X]}$.
  On en déduit que A et B sont premiers entre eux. □

Corollaire 1 *Soient* $A, B, C \in \mathbb{K}[X]$.
Si $PGCD(A, B) = 1$ *et* $PGCD(A, C) = 1$ ***alors*** $PGCD(A, BC) = 1$.

Preuve :
On suppose que PGCD$(A,B)=1$ et PGCD$(A,C)=1$.
On en déduit qu'il existe $U_1,U_2,V_1,V_2\in\mathbb{K}[X]$ tels que : $AU_1+BV_1=1 \quad (\star)$ et $AU_2+CV_2=1$.
En multipliant $(\star)$ par CV_2 on en déduit que : $AU_1CV_2+BCV_1V_2=CV_2$.
Or $CV_2=1-AU_2$, donc : $AU_1CV_2+BCV_1V_2=1-AU_2$.
Finalement :

$$A\underbrace{(U_1CV_2+U_2)}_{\in\mathbb{K}[X]}+BC\underbrace{(V_1V_2)}_{\in\mathbb{K}[X]}=1$$

En appliquant le théorème de Bezout (version 2), on en déduit que PGCD$(A,BC)=1$. □

Exemple 9 *Soient $a,b\in\mathbb{K}$ et $\alpha,\beta\in\mathbb{N}$.* ***Si*** *$a\neq b$* ***alors*** *$(X-a)^\alpha$ et $(X-b)^\beta$ sont premiers entre eux.*

Remarques 7 *Pour $\mathbb{K}=\mathbb{R}$ ou $\mathbb{C}$.*
Deux polynômes sont premiers entre eux ***si et seulement si*** *ils n'ont pas de racines complexes communes.*