

Chapitre B7

Polynômes

Dans tout ce chapitre on note \mathbb{K} pour \mathbb{R} ou \mathbb{C} .

I. Définitions

A. L'anneau $\mathbb{K}[X]$

Définition

Soit X une indéterminée. Un polynôme à coefficients dans \mathbb{K} est une somme

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^n a_kX^k$$

où n est un entier naturel et a_0, a_1, \dots, a_n sont des scalaires. On note aussi :

$$P = \sum_{k=0}^{+\infty} a_k X^k = \sum_{k \in \mathbb{N}} a_k X^k$$

en gardant bien en tête qu'à partir d'un certain rang les a_k sont tous nuls.

Proposition

Deux polynômes sont égaux si et seulement si leurs coefficients sont égaux.

$$\sum_{k \in \mathbb{N}} a_k X^k = \sum_{k \in \mathbb{N}} b_k X^k \quad \iff \quad \forall k \in \mathbb{N} \quad a_k = b_k$$

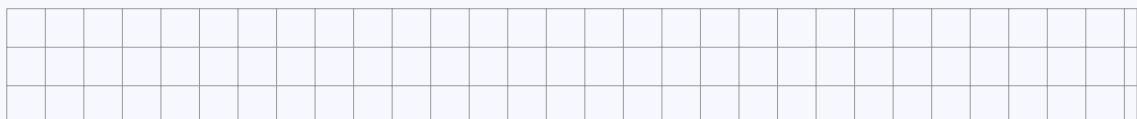
Notation

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .

Définitions (Opérations usuelles)

Soit $P = \sum_k a_k X^k$ et $Q = \sum_k b_k X^k$ deux polynômes. On définit les opérations :

- Addition : $P + Q = \sum_k (a_k + b_k)X^k$
- Multiplication : $PQ = \sum_k c_k X^k$ avec :



- Multiplication par un scalaire : pour tout $\lambda \in \mathbb{K}$ $\lambda P = \sum_k (\lambda a_k) X^k$
- Composition : $P \circ Q = P(Q(X))$

Définitions

- Un polynôme est *constant* si tous ses termes a_k sont nuls sauf éventuellement a_0 . L'ensemble des polynômes constants est naturellement identifié à \mathbb{K} , ce qui justifie l'inclusion $\mathbb{K} \subseteq \mathbb{K}[X]$.
- Le *polynôme nul* est le polynôme dont tous les coefficients sont nuls. Il est noté 0 ou $0_{\mathbb{K}[X]}$.

Proposition

Le triplet $(\mathbb{K}[X], +, \times)$ est un anneau.

- Son élément nul est le polynôme nul.
- L'opposé du polynôme $P = \sum_k a_k X^k$ est le polynôme $-P = \sum_k (-a_k) X^k$.
- L'élément unité est le polynôme constant égal à 1.
- Ses éléments inversibles sont les polynômes constants non-nuls : $\mathbb{K}[X]^* = \mathbb{K}^*$.

B. Degré**Définitions**

- Soit $P = \sum_k a_k X^k$ un polynôme non-nul. On appelle *degré* de P et on note $\deg P$ le plus grand entier k tel que a_k est non nul.

Si P est de degré n alors :

- Dans ce cas le coefficient a_n est appelé *coefficient dominant* de P .
- Si de plus $a_n = 1$ alors on dit que P est un polynôme *unitaire*.
- On convient que le polynôme nul est de degré $-\infty$.

Notation

Pour tout $n \in \mathbb{N}$ on note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} de degré *inférieur ou égal* à n :

Exemples.

• $\mathbb{K}_2[X] =$

• $\mathbb{K}_0[X] =$

• Si $n \leq m$ alors

Proposition

Pour tous polynômes P et Q :

$$\deg(P + Q)$$

$$\deg(PQ)$$

Si $\deg P > \deg Q$ alors

$$\deg(P + Q)$$

Remarque. On convient que $n + (-\infty) = -\infty$ et que $(-\infty) + (-\infty) = -\infty$, ainsi la propriété est valable également si l'un des deux polynômes P et Q est nul.

Démonstration. Si P ou Q est le polynôme nul la propriété se vérifie facilement.

Supposons que P et Q sont non-nuls. Soit $n = \deg P$ et $m = \deg Q$. Quitte à intervertir les deux polynômes on suppose que $n \geq m$. On note :

$$P = \sum_{k=0}^n a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^m b_k X^k$$

avec $a_n \neq 0$, et si $m < n$ alors $b_{m+1} = b_{m+2} = \dots = b_n = 0$. Alors :

$$P + Q = \sum_{k=0}^n (a_k + b_k) X^k$$

donc le degré de $P + Q$ est bien inférieur ou égal à n .

De plus :

- Si m est strictement inférieur à n alors le coefficient de degré n de $P + Q$ est a_n , il est non-nul, donc $P + Q$ est de degré n .
- Si $m = n$ alors le degré de $P + Q$ peut être strictement inférieur à n .

Pour la multiplication on utilise la formule :

$$PQ = \sum_{i=0}^n \sum_{j=0}^m a_i b_j X^{i+j}$$

Si $i \leq n$ et $j \leq m$ alors $i + j \leq n + m$, donc ce polynôme est de degré inférieur ou égal à $m + n$.

Si $i + j = m + n$, comme $i \leq n$ et $j \leq m$ alors $i = n$ et $j = m$, donc le coefficient de X^{m+n} est $a_n b_m$, il est non-nul donc PQ est de degré $m + n$. \square

Proposition

L'anneau $\mathbb{K}[X]$ est intègre. Autrement dit, pour tous polynômes P et Q :

$$PQ = 0 \implies P = 0 \text{ ou } Q = 0$$

Démonstration. On démontre la contraposée :

$$P \neq 0 \text{ et } Q \neq 0 \implies PQ \neq 0$$

En effet, si P et Q sont non-nuls alors ils sont de degrés positifs, et comme $\deg(PQ) = \deg P + \deg Q$ alors PQ est de degré positif et donc PQ est non-nul. \square

C. Spécialisation**Définition**

Soit P un polynôme et α un scalaire (*i.e.*, $\alpha \in \mathbb{K}$).

On note $P(\alpha)$ le scalaire obtenu en remplaçant X par α dans l'expression de P :

$$\text{Si } P = \sum_{k=0}^n a_k X^k \text{ alors } P(\alpha) = \sum_{k=0}^n a_k \alpha^k$$

On dit que $P(\alpha)$ est la *spécialisation* ou l'*évaluation* de P en α .

Remarque. On peut noter P ou $P(X)$ pour un polynôme P de $\mathbb{K}[X]$.

Par contre si $\alpha \in \mathbb{K}$ alors $P(\alpha) \in \mathbb{K}$.

Proposition

La spécialisation est compatible avec l'addition, la multiplication par un scalaire et la multiplication :

$$\begin{aligned} \forall (P, Q) \in \mathbb{K}[X]^2 \quad (P + Q)(\alpha) &= P(\alpha) + Q(\alpha) \\ \forall P \in \mathbb{K}[X] \quad \forall \lambda \in \mathbb{K} \quad (\lambda P)(\alpha) &= \lambda P(\alpha) \\ \forall (P, Q) \in \mathbb{K}[X]^2 \quad (PQ)(\alpha) &= P(\alpha)Q(\alpha) \end{aligned}$$

Définition

Une *fonction polynomiale* est une fonction de \mathbb{K} dans \mathbb{K} de la forme $x \mapsto P(x)$ où P est un polynôme.

Remarque. On note $\mathbb{K}[x]$ l'ensemble des fonctions polynomiales de \mathbb{K} dans \mathbb{K} . C'est un sous-anneau de $\mathcal{F}(\mathbb{K})$.

L'application $\mathbb{K}[X] \longrightarrow \mathbb{K}[x]$ est un morphisme d'anneaux.
 $P \longmapsto (x \mapsto P(x))$

D. Divisibilité

Définition

Si A, B deux polynômes. On dit que B divise A , et que A est un *multiple* de B s'il existe un polynôme C tel que $A = BC$.

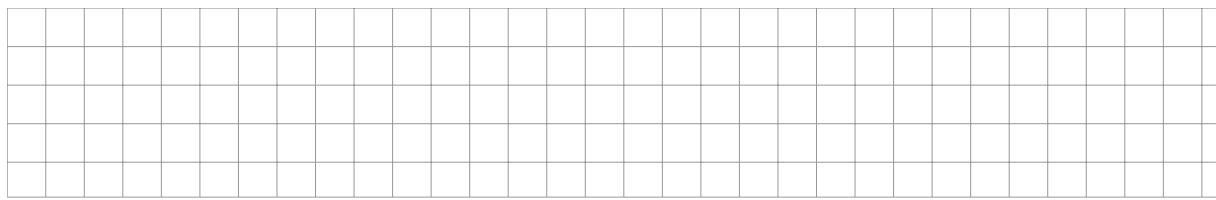
Notation

Si B divise A alors on note $B \mid A$.

Exemple 1.

- (i) $X - 4$ divise $X^2 - 3X - 4$
- (ii) Pour tout $n \in \mathbb{N}$: $X - 2$ divise $X^n - 2^n$
- (iii) X^2 divise $5X^6 + 7X^5 - 3X^3 + 2X^2$
- (iv) $2X - 3$ divise $X - \frac{3}{2}$
- (v) $X^3 - 3X^2 + 6X + 7$ ne divise pas $2X^2 - X + 10$.

Remarque. Si B divise A et A est non-nul alors $\deg B \leq \deg A$.



Propositions

- Si B divise A et A' alors B divise $(A + A')$.
- Si C divise B et B divise A alors C divise A .
- Le polynôme nul est multiple de tous les polynômes, le polynôme unité divise tous les polynômes.

Remarques.

- Si P est un polynôme et λ un scalaire non-nul alors P divise λP , et λP divise P , car $P = \frac{1}{\lambda}(\lambda P)$.
- La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{K}[X]$. Elle est réflexive, transitive, mais pas antisymétrique.

Par exemple $X^2 + 3$ divise $2X^2 + 6$ et $2X^2 + 6$ divise $X^2 + 3$ alors que ces deux polynômes ne sont pas égaux.

Définition

Deux polynômes P et Q sont dits *associés* si P divise Q et Q divise P .

Proposition

Deux polynômes P et Q sont associés si et seulement si il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Démonstration. D'après la remarque précédente, s'il existe λ non-nul tel que $Q = \lambda P$ alors P et Q sont associés.

Réciproquement, supposons que P et Q sont deux polynômes associés. Il existe alors deux polynômes A et B tels que $Q = AP$ et $P = BQ$.

On en déduit $P = BAP$.

Si P est nul, comme $Q = AP$ alors Q est nul. Il existe bien $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Si P est non-nul $\deg P = \deg A + \deg B + \deg P$, donc $\deg A = \deg B = 0$ car les degrés sont positifs.

Les polynômes de degrés nuls sont les polynômes constants non-nuls, donc il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda$. Ainsi $Q = \lambda P$ avec λ scalaire non-nul. \square

Théorème - Division euclidienne dans $\mathbb{K}[X]$

Soit A et B deux polynômes de $\mathbb{K}[X]$ avec B non-nul. Alors il existe un unique couple (Q, R) de polynômes tel que :

- $A = BQ + R$
- $\deg R < \deg B$

Les polynômes Q et R sont appelés respectivement *quotient* et *reste* de la division euclidienne de A par B .

Démonstration de l'existence. On fixe le polynôme B et on note p son degré. Comme B est non-nul alors p est un entier naturel. On considère la proposition :

\mathcal{P}_n : Pour tout polynôme A de degré n il existe un couple (Q, R) de polynômes tels que $A = BQ + R$ et $\deg R < \deg B$.

On démontre par *récurrence forte* que la proposition \mathcal{P}_n est vraie pour tout $n \in \mathbb{N} \cup \{-\infty\}$.

Initialisation. La propriété $\mathcal{P}_{-\infty}$ est vraie car si $A = 0$ alors il suffit de poser $Q = R = 0$: ceci donne bien $A = BQ + R$ et $\deg R < \deg B$.

Héritéité. Démontrons que pour tout $n \in \mathbb{N}$, si $\mathcal{P}_{-\infty}, \mathcal{P}_0, \mathcal{P}_1 \dots \mathcal{P}_{n-1}$ sont vraies, alors \mathcal{P}_n est vraie.

Soit $n \in \mathbb{N}$. Supposons que les propriétés $\mathcal{P}_{-\infty}, \mathcal{P}_0, \mathcal{P}_1 \dots \mathcal{P}_{n-1}$ sont vraies. Soit A un polynôme de degré n . On note

$$A = \sum_{k=0}^n a_k X^k \quad \text{et} \quad B = \sum_{k=0}^p b_k X^k$$

avec a_n et b_p non-nuls.

Si $n < p$ alors on pose $Q = 0$ et $R = A$, ce qui donne bien $A = BQ + R$ et $\deg R < \deg B$. Supposons maintenant que $n \geq p$. Soit $Q_1 = \frac{a_n}{b_p} X^{n-p}$. Alors

$$Q_1 B = a_n X^n + \frac{a_n}{b_p} b_{p-1} X^{n-1} + \cdots$$

donc $A - Q_1B$ est de degré strictement inférieur à n . Notons m ce degré.

On applique la proposition \mathcal{P}_m , qui est supposée vraie par hypothèse de récurrence :

Il existe des polynômes Q_2 et R tels que $A - Q_1 B = Q_2 B + R$ et $\deg R < \deg B$. En posant $Q = Q_1 + Q_2$ on obtient qu'il existe bien deux polynômes Q et R tels que $A = BQ + R$ et $\deg R < \deg B$.

Ceci démontre que la proposition \mathcal{P}_n est vraie. L'hérédité est établie.

Conclusion. Par récurrence forte la propriété \mathcal{P}_n est vraie pour tout $n \in \mathbb{N} \cup \{-\infty\}$.

En d'autres termes, pour tout $A \in \mathbb{K}[X]$ il existe des polynômes Q et R satisfaisant les conditions demandées.

Démonstration de l'unicité.

Méthode

On pose la division comme pour les entiers.

Exemple 2. Calcul de la division euclidienne de A par B où :

$$\begin{array}{lll}
 (i) & A = X^5 - X^4 - X^3 + 8X^2 - 2 & B = X^2 - X + 2 \\
 (ii) & A = 2X^5 + 3X^4 - 4X^3 - X^2 + 4X + 1 & B = X^3 + 2X^2 - 1
 \end{array}$$

► Exercice 1.

E. Représentation informatique

On peut considérer qu'un polynôme à coefficients dans \mathbb{K} est une suite finie de scalaires (a_0, a_1, \dots, a_n) , ou de façon équivalente une suite (a_0, a_1, \dots) nulle à partir d'un certain rang.

On dit plutôt qu'une suite est *presque nulle* si elle est nulle sauf pour un nombre fini d'indices.

Alors les éléments de \mathbb{K} sont les suites $(a_0, 0, 0, \dots)$, l'indéterminée est $X = (0, 1, 0, 0, \dots)$.

L'addition est définie par :

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

La multiplication est définie par :

$$\begin{aligned} (a_0, a_1, \dots) \times (b_0, b_1, \dots) &= (a_0 b_0, a_1 b_0 + a_0 b_1, \dots) \\ &= (c_0, c_1, \dots) \quad \text{avec} \quad \forall k \in \mathbb{N} \quad c_k = \sum_{i=0}^k a_i b_{k-i} \end{aligned}$$

On vérifie que l'ensemble des suites presque nulles muni de ces deux opérations est un anneau, et comme on a noté $X = (0, 1, 0, \dots)$ alors on a exactement :

$$\sum_{k=0}^n a_k X^k = (a_0, a_1, \dots, a_n, 0, \dots)$$

On définit aussi la multiplication par un scalaire :

$$\lambda(a_0, a_1, \dots) = (\lambda a_0, \lambda a_1, \dots)$$

Cette notation est en fait une définition alternative des polynômes, qui explique la notion d'indéterminée : c'est un objet différent des scalaires.

En **Python** on peut définir des suites de scalaires (de flottants en l'occurrence).

Par exemple le polynôme $P = X^3 - 5X^2 + 7$ est représenté par la liste `P=[7, 0, -5, 1]`, éventuellement avec des zéros à la suite, comme `P=[7, 0, -5, 1, 0, 0]`.

Le coefficient a_k est alors `P[k]`.

On peut définir des fonctions de calcul de :

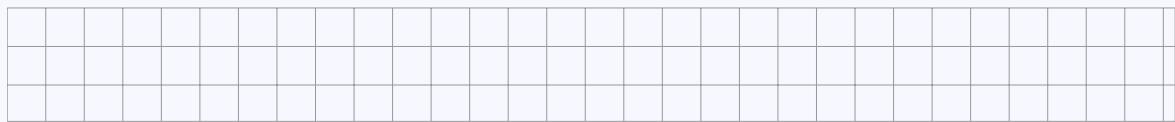
- Degré d'un polynôme
- Somme, produit de deux polynômes
- Produit d'un polynôme par un scalaire
- Spécialisation d'un polynôme en un scalaire
- Division euclidienne d'un polynôme non-nul (il suffit de suivre l'algorithme donné par la démonstration de l'existence du couple (Q, R))
- PGCD de deux polynômes
- etc.

II. Déivation

A. Dérivée formelle

Définition

Soit $P = \sum_{k=0}^n a_k X^k$ un polynôme. On appelle *polynôme dérivé* de P et on note P' le polynôme défini par :



Remarque. Si f est la fonction polynomiale de polynôme P , alors la fonction polynomiale associée à P' est la dérivée de f au sens usuel. En conséquence la dérivation des polynômes hérite des propriétés de la dérivation des fonctions :

Pour tous polynômes P et Q et tout scalaire λ :

- $(P + Q)' = P' + Q'$
- $(\lambda P)' = \lambda P'$
- $(PQ)' = P'Q + PQ'$
- $P' = Q' \iff \exists k \in \mathbb{K} \quad P = Q + k$

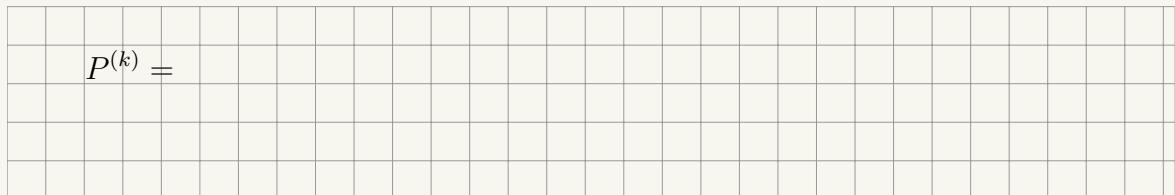
Proposition

Pour tout polynôme P non constant : $\deg(P') = \deg(P) - 1$

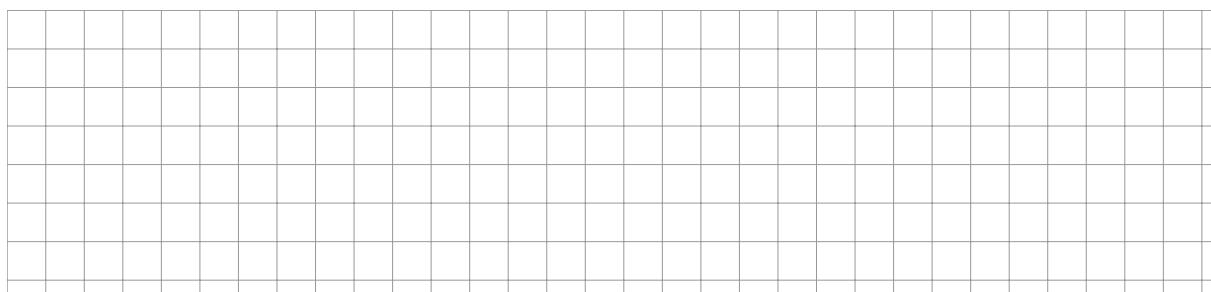
B. Dérivées k -èmes

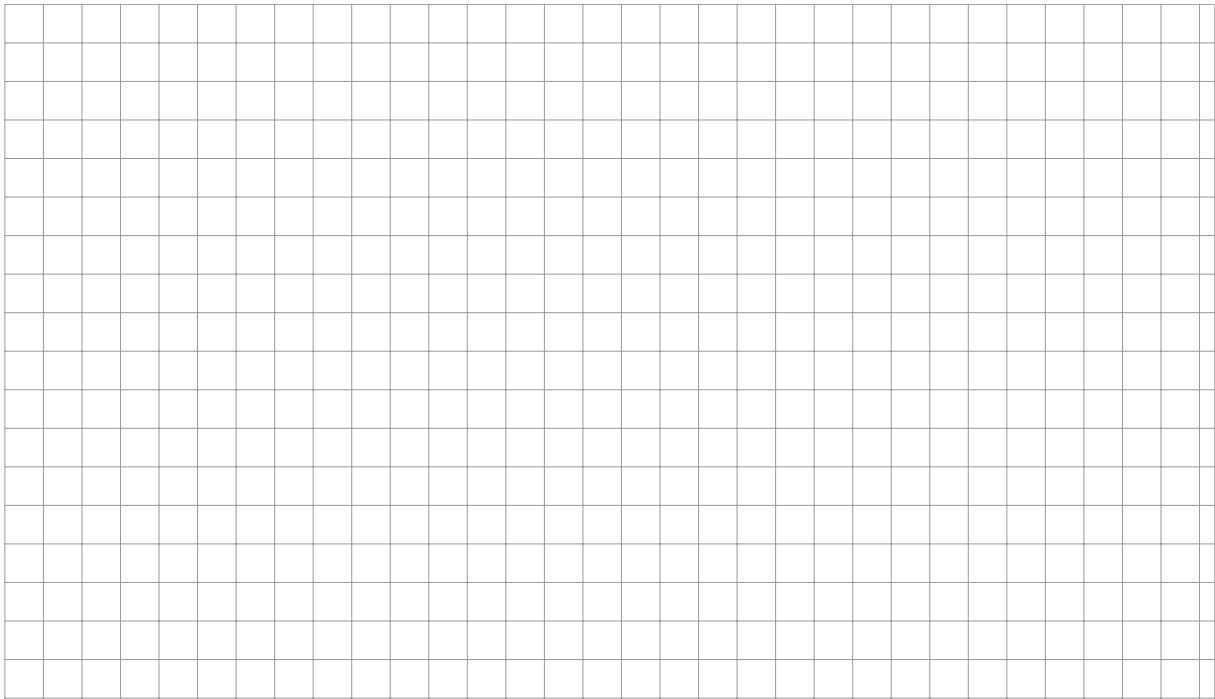
Proposition

Soit $P = X^n$ où $n \in \mathbb{N}$. Alors pour tout $k \in \mathbb{N}$:



Démonstration. On commence par démontrer par récurrence finie sur k que cette propriété est vraie pour tout $k \in \{0, \dots, n\}$.





Proposition - Formule de Leibniz

Soit A et B deux polynômes. Alors :

$$\forall n \in \mathbb{N} \quad (AB)^{(n)} =$$

Exemple. Premiers dérivés successifs du produit AB :

$$(AB)^{(0)} = AB$$

$$(AB)^{(1)} = A'B + AB'$$

$$(AB)^{(2)} =$$

$$(AB)^{(3)} =$$

Démonstration. On démontre cette formule par récurrence sur n , comme pour la formule du binôme de Newton. \square

► **Exercice 2.**

Théorème - Formule de Taylor

Soit P un polynôme de degré n et a un scalaire. Alors :

Démonstration. Si P est le polynôme nul alors la formule s'écrit $P = 0$, elle est juste.

Pour les autres cas on note \mathcal{P}_n la propriété : la formule de Taylor est vraie pour tout polynôme de degré n .

On démontre par récurrence que cette propriété est vraie pour tout $n \in \mathbb{N}$.

Initialisation. Si P est de degré nul alors P est constant. La formule s'écrit $P = P^{(0)}(a)$, elle est exacte.

Hérité. Supposons que pour un certain $n \in \mathbb{N}^*$ la propriété \mathcal{P}_{n-1} est vraie, c'est-à-dire que la formule est validée pour tout polynôme de degré $n - 1$.

On considère un polynôme P de degré n et on pose : $Q = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!}(X - a)^k$

La dérivée de Q est :

De plus, comme P' est de degré $n - 1$ alors par hypothèse de récurrence la formule est valide pour P' , ce qui donne :

Comme $P'^{(k)} = P^{(k+1)}$ pour tout entier k alors $Q' = P'$.

Ceci implique qu'il existe une constante $c \in \mathbb{K}$ telle que $Q = P + c$. Or $Q(a) = P(a)$, donc $c = 0$ et la formule est valide pour P .

L'hérédité est démontrée.

Conclusion. Par récurrence, la formule de Taylor est vraie pour tout polynôme.

Remarque. Pour tout polynôme P : $P^0 = 1$

Ceci montre que la spécialisation de $(X - a)^0$ en a est égale à 1.

Exemple 3. Application de la formule pour $P = X^3 + 2X - 5$ et $a = 1$.

► Exercice 3.

III. Racines

A. Définition

Définition

Soit P un polynôme de $\mathbb{K}[X]$. Une *racine* (ou un *zéro*) de P est un scalaire α tel que $P(\alpha) = 0$.

Exemples.

- Le polynôme $X + 3$ de $\mathbb{K}[X]$ a une racine : -3
- Le polynôme $X^2 + 1$ de $\mathbb{C}[X]$ a deux racines : i et $-i$
- Le polynôme $X^2 + 1$ de $\mathbb{R}[X]$ n'a pas de racine.
- Le polynôme 5 n'a pas de racine.
- Le polynôme nul a une infinité de racines : tous les éléments de \mathbb{K} .

Théorème

Soit P un élément de $\mathbb{K}[X]$ et α un élément de \mathbb{K} .

Alors α est racine de P si et seulement si $(X - \alpha)$ divise P .

Démonstration.

Exemple 4. Résoudre : $3x^3 - 5x^2 + 2 = 0$

► **Exercice 4.**

Corollaire

Soit P un polynôme et $k \in \mathbb{N}^*$.

Si $\alpha_1, \dots, \alpha_k$ sont k racines distinctes de P alors le polynôme $\prod_{i=1}^k (X - \alpha_i)$ divise P .

Démonstration. On note \mathcal{P}_k cette propriété et on démontre par récurrence qu'elle est vraie pour tout $k \in \mathbb{N}^*$

Initialisation. Le théorème précédent donne la propriété \mathcal{P}_1 .

Héritéité. Supposons que pour un certain entier $k \geq 2$ la propriété \mathcal{P}_{k-1} est vraie, démontrons qu'alors la propriété \mathcal{P}_k est vraie.

Soit $\alpha_1, \dots, \alpha_k$ des racines distinctes de P . Alors $\alpha_1, \dots, \alpha_{k-1}$ sont des racines distinctes de P , donc d'après la propriété \mathcal{P}_{k-1} (qui est vraie par hypothèse de récurrence) le polynôme $\prod_{i=1}^{k-1} (X - \alpha_i)$ divise P , *i.e.*, il existe un polynôme Q tel que :

$$P = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_{k-1})Q$$

Mais α_k est racine de P , donc en spécialisant en $X = \alpha_k$ dans l'égalité ci-dessus on obtient :

$$0 = (\alpha_k - \alpha_1) \cdots (\alpha_k - \alpha_{k-1})Q(\alpha_k)$$

Comme les α_i sont tous distincts alors les $\alpha_i - \alpha_k$ ne sont pas nuls. On en déduit que $Q(\alpha_k) = 0$, donc α_k est une racine de Q .

D'après le théorème ci-dessus il existe un polynôme Q_1 tel que $Q = (X - \alpha_k)Q_1$, ce qui donne :

$$P = (X - \alpha_1) \cdots (X - \alpha_{k-1})(X - \alpha_k)Q_1$$

On a donc démontré que la propriété \mathcal{P}_k est vraie. L'héritéité est établie.

Conclusion. Par récurrence, la propriété \mathcal{P}_k est vraie pour tout entier non-nul k . □

Corollaire

Soit n un entier naturel. Un polynôme de degré n possède au plus n racines distinctes.

Démonstration. Soit P un polynôme de degré n , et soit m racines distinctes $\alpha_1, \dots, \alpha_m$ de P . Alors d'après le corollaire précédent il existe un polynôme Q tel que :

$$P = \left(\prod_{i=1}^m (X - \alpha_i) \right) Q$$

Comme P est de degré $n \in \mathbb{N}$ alors P est non-nul, puis Q est non-nul. On déduit de l'égalité ci-dessus :

$$n = \deg P = \deg \left(\prod_{i=1}^m (X - \alpha_i) \right) + \deg Q = m + \deg Q$$

Le degré de Q est positif, donc $n \geq m$.

Ainsi P ne peut avoir plus de n racines distinctes. □

Corollaires

Soit n un entier naturel.

(i) Soit P un polynôme de degré inférieur ou égal à n .

Si P possède $n + 1$ racines distinctes alors $P = 0$.

(ii) Soit P et Q deux polynômes de degrés inférieurs ou égaux à n . S'il existe $n + 1$ scalaires distincts $\alpha_0, \dots, \alpha_n$ tels que pour tout $i = 0, \dots, n$ on a $P(\alpha_i) = Q(\alpha_i)$ alors $P = Q$.

(iii) Soit $f, g : \mathbb{K} \rightarrow \mathbb{K}$ deux fonctions polynomiales de degrés inférieurs ou égaux à n .

Si f et g sont égales en au moins $n + 1$ scalaires distincts alors f et g sont égales.

En d'autres termes une fonction polynomiale de degré au plus n est uniquement déterminée par $n + 1$ de ses valeurs.

Démonstration.

(i) On suppose que P est de degré au plus n et qu'il possède $n + 1$ racines.

Si P est non-nul alors il est de degré m avec $0 \leq m \leq n$, donc il possède au plus n racines, d'après le corollaire précédent.

Or P possède au moins $n + 1$ racines, donc il est nul.

(ii) On applique le point (i) au polynôme $P - Q$.

Ce polynôme est de degré au plus n , les α_i en sont racines, donc il possède au moins $n + 1$ racines, et donc il est nul. Ainsi $P = Q$.

(iii) Ce point est conséquence du précédent. □

Remarque.

Cette propriété signifie que l'application $\mathbb{K}[X] \rightarrow \mathbb{K}[x]$ est injective.

$$P \mapsto \begin{pmatrix} \mathbb{K} & \rightarrow & \mathbb{K} \\ x & \mapsto & P(x) \end{pmatrix}$$

Elle est surjective par définition d'une fonction polynomiale, donc elle est bijective.

On peut ajouter que c'est un isomorphisme d'anneau.

B. Ordre de multiplicité d'une racine

Définition

Soit P un polynôme non-nul et α une racine de P .

L'*ordre de multiplicité* de α dans P est le plus grand entier k tel que $(X - \alpha)^k$ divise P .

De façon équivalente, c'est l'entier naturel m tel que $(X - \alpha)^m$ divise P et $(X - \alpha)^{m+1}$ ne divise pas P .

Remarque. Il existe alors un polynôme Q tel que $P = (X - \alpha)^m Q$ et $Q(\alpha) \neq 0$.

Exemple 5.

(i) Soit $P = aX^2 + bX + c$ un polynôme du second degré. Si son discriminant est non-nul alors il possède deux racines de multiplicité 1, sinon il possède une racine de multiplicité 2.

(ii) Quelles sont les racines de $X^3 - X^2 - X + 1$ et quelles sont leurs multiplicités ?

(iii) Quelles sont les racines de $4X^{28} - X^{26}$ et quelles sont leurs multiplicités ?

Théorème

Soit P un polynôme, α un scalaire, et m un entier naturel. Alors les propriétés suivantes sont équivalentes :

(i) α est racine de P de multiplicité m .

(ii) α est racine de $P, P', P'', \dots, P^{(m-1)}$, mais pas de $P^{(m)}$.

Remarque. Un scalaire α est racine d'un polynôme P de multiplicité 0 si et seulement si $P(\alpha) \neq 0$.

Exemple 6. Soit $P = X^4 + 2X^3 - 12X^2 - 40X - 32$.

Chercher une racine évidente de P , déterminer son ordre de multiplicité et en déduire sa factorisation.

► Exercice 5.

Exemple. Démonstration dans le cas où $m = 3$.

Démonstration du sens direct. Supposons que α est racine de P d'ordre de multiplicité m . Ceci signifie qu'il existe un polynôme Q tel que :

$$P = (X - \alpha)^m Q \quad \text{et} \quad Q(\alpha) \neq 0$$

Notons $A = (X - \alpha)^m$. Les dérivés successifs de A sont :

$$\forall p \in \mathbb{N} \quad A^{(p)} = \begin{cases} \frac{m!}{(m-p)!} (X - \alpha)^{m-p} & \text{si } 0 \leq p \leq m \\ 0 & \text{si } p > m \end{cases}$$

Comme $P = AQ$ alors par application de la formule de Leibniz :

$$\forall n \in \mathbb{N} \quad P^{(n)} = \sum_{p=0}^n \binom{n}{p} A^{(p)} Q^{(n-p)}$$

Démontrons que α est racine de $P^{(0)} \dots P^{(m-1)}$.

Si $0 \leq n \leq m-1$ alors tout p allant de 0 à n vérifie $p \leq m-1$, ce qui donne $1 \leq m-p$ puis :

$$A^{(p)} = \frac{m!}{(m-p)!} (X - \alpha)^{m-p} \quad \text{et} \quad A^{(p)}(\alpha) = 0$$

Ainsi

$$P^{(n)}(\alpha) = \sum_{p=0}^n \binom{n}{p} A^{(p)}(\alpha) Q^{(n-p)}(\alpha) = 0$$

On a démontré que α est racine de $P^{(n)}$, ceci pour tout n compris entre 0 et $m-1$.

Posons maintenant $n = m$. On a vu que si p est compris entre 0 et $m-1$ alors $A^{(p)}(\alpha) = 0$, donc :

$$P^{(m)}(\alpha) = A^{(m)}(\alpha) Q^{(m-m)}(\alpha) = m! Q(\alpha)$$

Or $Q(\alpha) \neq 0$ donc α n'est pas racine de $P^{(m)}$.

Démonstration du sens indirect.

C. Relations entre coefficients et racines

Remarque. Soit $P = a_nX^n + \cdots + a_0$ un polynôme de $\mathbb{K}[X]$, $\alpha_1, \dots, \alpha_n$ ses racines, éventuellement complexes, non obligatoirement distinctes. On sait alors que :

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = a_n (X - \alpha_1) \cdots (X - \alpha_n) \quad (\dagger)$$

En développant le second terme et en identifiant on obtient l'expression des coefficients de P en fonction de ses racines.

Exemple 7.

(i) Pour $n = 2$ on obtient :

(ii) Pour $n = 3$ on obtient :

Proposition (formules de Viète : somme et produit des racines)

Avec les notations de la remarque ci-dessus :

Démonstration. Il suffit de considérer l'égalité (†).

Exemple 8. La somme des racines n -èmes de l'unité est nulle si $n > 1$, leur produit vaut $(-1)^{n-1}$.

Exemple 9. Résoudre les systèmes :

$$(i) \begin{cases} x + y = 7 \\ xy = 10 \end{cases} \quad (ii) \begin{cases} x + y = 2 \\ x^2 + y^2 = 10 \end{cases}$$

► Exercices 6, 7.

Proposition (cas général)

Avec les notations précédentes :

Démonstration. Ces formules proviennent du développement de l'égalité (†).

IV. Factorisation d'un polynôme

A. Polynômes scindés

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit *scindé* s'il est produit de polynômes de $\mathbb{K}[X]$ du premier degré.

Remarques.

- Un polynôme est donc scindé si et seulement si il peut s'écrire

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

avec $n = \deg P$ et $\lambda, \beta_1, \dots, \beta_n$ éléments de \mathbb{K} , les β_i n'étant pas obligatoirement distincts.

- Autre caractérisation : un polynôme de degré n est scindé si et seulement si il admet n racines, comptées avec leurs multiplicités.

Exemple.

- Dans $\mathbb{R}[X]$: $X^2 + 1$ n'est pas scindé, $X^2 - 1$ est scindé.
- Dans $\mathbb{C}[X]$: $X^2 + 1$ et $X^2 - 1$ sont scindés.

B. Factorisation dans $\mathbb{C}[X]$

Théorème fondamental de l'algèbre ou Théorème de d'Alembert-Gauss

Tout polynôme non constant de $\mathbb{C}[X]$ possède une racine.

Corollaire

Soit P un polynôme de degré n de $\mathbb{C}[X]$. Alors il existe des complexes $\lambda, \beta_1, \dots, \beta_n$ tels que :

$$P = \lambda(X - \beta_1) \cdots (X - \beta_n)$$

Remarque. En d'autres termes, tout polynôme de $\mathbb{C}[X]$ est scindé.

Démonstration. Admise. □

Remarque. On dit que \mathbb{C} est *algébriquement clos*. Ce n'est pas le cas de \mathbb{R} ni de \mathbb{Q} .

Par exemple le polynôme $X^2 + 1$ n'a pas de racine dans \mathbb{Q} ni dans \mathbb{R} .

Le polynôme $X^2 - 2$ a des racines dans \mathbb{R} mais pas dans \mathbb{Q} .

► Exercice 8.

Proposition

Soit P un polynôme de degré n . Soit $\alpha_1, \dots, \alpha_r$ ses racines complexes, et m_1, \dots, m_r leurs ordres de multiplicité respectifs.

Alors $n = m_1 + \cdots + m_r$.

Démonstration. En effet il existe $\lambda \in \mathbb{C}$ tel que $P = \lambda(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}$ □

C. Factorisation dans $\mathbb{R}[X]$

Exemple 10. Le polynôme $X^4 + 1$ est-il scindé dans $\mathbb{R}[X]$? Est-il possible de le factoriser dans $\mathbb{R}[X]$?

Remarque. Tout polynôme non constant de $\mathbb{R}[X]$ admet une racine, éventuellement complexe. En effet, si P est élément de $\mathbb{R}[X]$, alors P est en particulier élément de $\mathbb{C}[X]$, donc d'après le théorème de d'Alembert-Gauss il admet une racine dans \mathbb{C} .

Proposition

Soit P un polynôme de $\mathbb{R}[X]$ et α une racine de P , éventuellement complexe. Alors $\bar{\alpha}$ est racine de P .

Démonstration.

Proposition (suite)

Si α est de multiplicité m alors $\bar{\alpha}$ est de multiplicité m .

Démonstration. Par théorème, si α est racine de P d'ordre de multiplicité m alors :

$$P(\alpha) = P'(\alpha) = \cdots = P^{(m-1)}(\alpha) = 0 \quad \text{et} \quad P^{(m)}(\alpha) \neq 0$$

Les $P^{(n)}$ sont réels donc par conjugaison :

$$P(\bar{\alpha}) = P'(\bar{\alpha}) = \cdots = P^{(m-1)}(\bar{\alpha}) = 0 \quad \text{et} \quad P^{(m)}(\bar{\alpha}) \neq 0$$

Ceci montre bien que $\bar{\alpha}$ est racine de P d'ordre de multiplicité m . □

Théorème

Tout polynôme de $\mathbb{R}[X]$ est produit de polynômes de degré 1 et de polynômes de degré 2 à discriminants strictement négatifs.

Démonstration. Soit P un polynôme de $\mathbb{R}[X]$. Alors P est élément de $\mathbb{C}[X]$, donc il est scindé dans $\mathbb{C}[X]$. Parmi ses racines certaines sont réelles. Si une racine n'est pas réelle alors son conjugué est racine également.

On peut noter l'ensemble des racines par

$$\{\alpha_1, \dots, \alpha_r, \bar{\alpha}_1, \dots, \bar{\alpha}_r, \beta_1, \dots, \beta_s\}$$

où r et s sont des entiers naturels, les α_i sont des complexes non réels, et les β_j sont des réels.

On note ensuite m_i l'ordre de multiplicité de chaque α_i . Alors m_i est aussi l'ordre de multiplicité de chaque $\bar{\alpha}_i$, d'après la proposition précédente.

On note de plus ℓ_j l'ordre de multiplicité de chaque β_j , et enfin λ le coefficient dominant de P , qui est réel car P est élément de $\mathbb{R}[X]$.

On obtient :

Pour $i = 1 \dots r$ notons :

$$Q_i = (X - \alpha_i)(X - \bar{\alpha}_i)$$

La décomposition de P s'écrit alors :

_____ (★)

Or en développant Q_i on obtient :

Ainsi Q_i est un polynôme réel. Son discriminant est

$$\Delta_i =$$

Il est strictement négatif car α_i n'est pas réel.

La décomposition (\star) est bien une décomposition en produit de polynômes de degré 1 et polynômes de degré 2 à discriminants strictement négatifs. \square

Corollaire

Tout polynôme de degré impair de $\mathbb{R}[X]$ possède une racine réelle.

Démonstration. Si P est un polynôme sans racine réelle, alors d'après le théorème ci-dessus P est produit de polynômes de degré 2, donc son degré est pair. Ceci contredit l'hypothèse, donc P possède une racine réelle. \square

Autre démonstration. Notons $P = a_n X^n + \dots + a_0$ avec n impair et a_n non-nul. Alors :

$$P(x) \underset{(+\infty)}{\sim} a_n x^n$$

On en déduit :

$$\lim_{x \rightarrow +\infty} P(x) = (\operatorname{sgn} a_n) \infty \quad \text{et} \quad \lim_{x \rightarrow -\infty} P(x) = -(\operatorname{sgn} a_n) \infty$$

La fonction $x \mapsto P(x)$ est continue car elle est polynomiale, donc le théorème des valeurs intermédiaires permet de conclure que $P(\mathbb{R}) = \mathbb{R}$, donc que 0 admet un antécédent par cette fonction. Cet antécédent est racine de P , donc P admet une racine. \square

V. Arithmétique des polynômes

A. PGCD

Notation

Pour tout polynôme A on note $\mathcal{D}(A)$ l'ensemble de diviseurs de A .

Remarque. Soit A et B deux polynômes non tous les deux nuls.

Alors l'ensemble $\mathcal{D}(A) \cap \mathcal{D}(B)$ est non-vide car il contient le polynôme 1. L'ensemble R des degrés des éléments de $\mathcal{D}(A) \cap \mathcal{D}(B)$ est une partie de \mathbb{N} non-vide, car elle contient 0. De plus tout diviseur de A et de B est de degré inférieur aux degrés de A et de B s'ils sont non-nuls, donc l'ensemble R est majoré. Il contient donc un plus grand élément r .

Cet entier r est le degré d'un élément de $\mathcal{D}(A) \cap \mathcal{D}(B)$.

Ceci justifie la définition ci-dessous.

Définition

Soit A et B deux polynômes non tous les deux nuls. Un PGCD de A et B est un polynôme de degré maximal divisant A et B .

Remarque. Si D est un PGCD de A et B alors tout polynôme associé à D , donc tout polynôme λD pour $\lambda \in \mathbb{K}^*$, est un PGCD de A et B .

Lemme

Soit A, B, Q, R , quatre polynômes vérifiant $A = BQ + R$. Alors :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$$

Démonstration. Par double inclusion. □

Remarque. Étant donnés deux polynômes A et B avec B non-nul on crée par récurrence finie une suite finie $(R_k)_{0 \leq k \leq n+1}$ de polynômes (avec $n \in \mathbb{N}$) de la façon suivante : $R_0 = A$, $R_1 = B$, puis pour $k \geq 0$ si R_{k+1} est non-nul alors le polynôme R_{k+2} est le reste de la division euclidienne de R_k par R_{k+1} :

$$R_k = Q_{k+1}R_{k+1} + R_{k+2} \quad \deg R_{k+2} < \deg R_{k+1}$$

On a défini aussi la suite des quotients $(Q_k)_{1 \leq k \leq n}$.

La suite $(\deg R_k)_{1 \leq k}$ est une suite d'entiers naturels strictement décroissante donc elle est finie, ce qui montre que la suite $(R_k)_{k \geq 0}$ atteint le polynôme nul, auquel cas la construction s'arrête, et on note n l'indice du dernier polynôme R_k non-nul.

Ce dernier polynôme non-nul R_n est un PGCD de A et de B , car :

$$\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(R_n) \cap \mathcal{D}(R_{n+1}) = \mathcal{D}(R_n) \cap \mathcal{D}(0) = \mathcal{D}(R_n)$$

Ceci montre que l'algorithme d'Euclide pour le calcul du PGCD est valide.

Proposition

Si D_1 et D_2 sont deux PGCD de A et de B alors ils sont associés.

Il existe donc un unique PGCD de A et de B unitaire.

Démonstration. En effet, D_1 et D_2 sont deux diviseurs de degré maximal de R_n , donc ils sont associés à R_n . Il s'écrivent tous les deux λR_n pour un certain $\lambda \in \mathbb{K}^*$.

Si le coefficient dominant de R_n est a alors a est non-nul. Le polynôme $D = \frac{1}{a}R_n$ est alors un PGCD unitaire de A et de B , et c'est le seul polynôme unitaire associé à R_n . \square

Définition

Soit A et B deux polynômes non tous les deux nuls. Le PGCD de A et B est le polynôme unitaire de degré maximal divisant A et B . On le note $A \wedge B$.

De plus on convient que $0 \wedge 0 = 0$.

Exemple 11.

$$(10X^3 + 10X^2) \wedge (2X^2 + 4X + 2) =$$

Proposition

Le PGCD de A et B est le plus grand commun diviseur de A et B au sens de la relation de divisibilité. C'est-à-dire que si un polynôme P divise A et B alors il divise leur PGCD.

Démonstration. Ceci est conséquence de l'égalité $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(A \wedge B)$.

Exercice 9.

B. Relation de Bézout

Proposition

Soit A et B deux polynômes non tous les deux nuls. Alors il existe deux polynômes U et V tels que $AU + BV = A \wedge B$.

Ces deux polynômes U et V sont appelés *coefficients de Bézout* du couple (A, B) .

Démonstration. On utilise les Q_k et les R_k de l'algorithme d'Euclide.

Exercice 10.

Définition

Deux polynômes non tous les deux nuls sont dits *premiers entre eux* si leur PGCD est égal à 1.

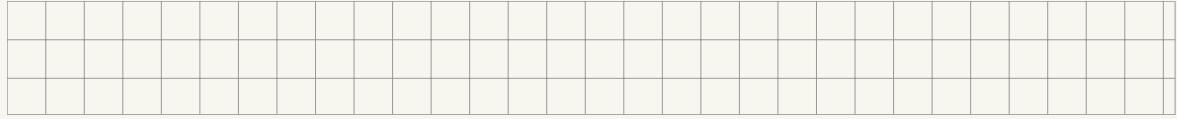
Théorème de Bézout

Deux polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.

Démonstration. Le sens direct est conséquence de la propriété précédente. Pour le sens indirect on remarque que si $AU + BV = 1$ alors tout diviseur de A et de B divise 1. \square

Proposition (Lemme de Gauss)

Soit A, B, C trois polynômes. Si A divise BC et A est premier avec B alors A divise C .



Démonstration. On utilise la relation de Bézout : il existe U et V tels que $AU + BV = 1$, donc $C = ACU + BCV$. Si A divise BC alors A divise $ACU + BCV = C$. \square

Proposition

Soit A et B deux polynômes et D leur PGCD. Alors il existe deux polynômes A_1 et B_1 tel que :

$$A = DA_1 \quad B = DB_1 \quad A_1 \wedge B_1 = 1$$

Démonstration. Laissée en exercice. \square

C. PPCM

Remarque. Soit A et B deux polynômes non-nuls.

Alors l'ensemble des multiples non-nuls de A et de B est non-vide car il contient le polynôme AB . Donc L'ensemble des degrés de ses éléments est une partie de \mathbb{N} non-vide. Elle admet donc un minimum.

Ainsi il existe un polynôme non-nul de degré minimal multiple de A et de B .

Définition

Soit A et B deux polynômes non-nuls. Un *PPCM* de A et B est un multiple non-nul de A et B de degré minimal.

Remarque. Si M est un PPCM de A et de B alors tout polynôme associé à M , donc tout polynôme λM pour $\lambda \in \mathbb{K}^*$, est un PPCM de A et B .

Proposition

Un PPCM de A et B est un plus petit commun multiple de A et B au sens de la divisibilité, c'est-à-dire que si un polynôme P est un multiple de A et B alors P est un multiple de tous leurs PPCM.

Démonstration. Soit M un PPCM de A et B . Soit P un multiple de A et B . Comme M est non-nul alors par division euclidienne il existe deux polynômes Q et R tels que $P = QM + R$ avec $\deg R < \deg M$.

Comme P et M sont multiples de A et B alors R est multiple de A et B . Comme son degré est strictement inférieur à celui de M qui est un multiple de A et B non-nul de degré minimal alors R est nul.

Ainsi M divise P .

Proposition

Si M_1 et M_2 sont deux PPCM de A et B alors ils sont associés.

Il existe donc un unique PPCM de A et de B unitaire.

Démonstration. En effet, M_1 et M_2 sont deux PPCM de A et B donc ils sont multiples l'un de l'autre d'après la propriété précédente, et ils sont donc associés. \square

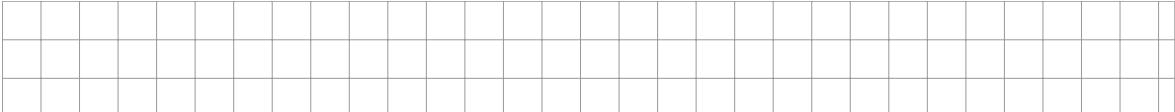
Définition

Soit A et B deux polynômes non-nuls. Le *PPCM* de A et B est le polynôme non-nul unitaire de degré minimal multiple de A et B . On le note $A \vee B$.

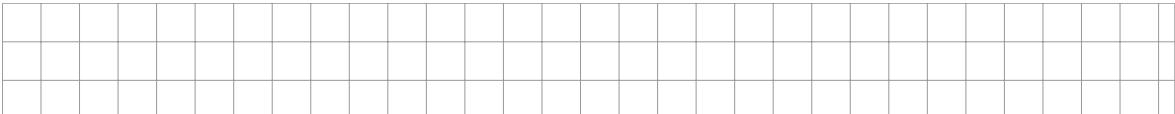
De plus on convient que $A \vee 0 = 0$ pour tout polynôme A .

Remarques.

- On a démontré ci-dessus que :



- En conséquence :



Lemme

Soit A, B, C trois polynômes non-nuls avec C unitaire. Alors $(AC) \vee (BC) = (A \vee B)C$.

► Exercice 11.

Proposition

Soit A et B deux polynômes non-nuls.

- (i) Si A et B sont premiers entre eux alors $A \vee B$ est associé à AB .
- (ii) Dans tous les cas $(A \wedge B)(A \vee B)$ est associé à AB .

Démonstration.

- (i) Le produit AB est un multiple commun de A et B , donc il est multiple de leur PPCM.

Soit $M = A \vee B$. Comme M est multiple de A alors il existe un polynôme Q tel que $M = AQ$. Comme M est multiple de B alors B divise $M = AQ$, et comme A et B sont premiers entre eux alors d'après le lemme de Gauss P divise Q . Il existe donc un polynôme R tel que $Q = BR$. On a alors $M = ABR$, i.e., M est multiple de AB .

Ainsi AB et $A \vee B$ sont associés.

- (ii) Notons $D = A \wedge B$. Alors il existe A_1 et B_1 premiers entre eux tels que $A = DA_1$ et $B = DB_1$, et donc $A \vee B = (A_1D) \vee (B_1D)$.

D'après le lemme précédent, comme D est unitaire alors $A \vee B = (A_1 \vee B_1)D$, puis d'après le (i) comme A_1 et B_1 sont premiers entre eux alors il existe $\lambda \in \mathbb{K}^*$ tel que $A \vee B = \lambda A_1 B_1 D$.

Enfin $(A \vee B)(A \wedge B) = \lambda A_1 B_1 D^2 = \lambda AB$. Comme λ est un scalaire non-nul alors $(A \wedge B)(A \vee B)$ est associé à AB . \square

D. Extension à un nombre fini de polynômes**Proposition**

Soit A_1, \dots, A_n une famille de n polynômes non tous nuls. Alors :

- Il existe un et un seul polynôme D unitaire de degré maximal divisant tous les A_i .
- De plus il existe des polynômes U_1, \dots, U_n tels que

$$A_1 U_1 + \dots + A_n U_n = D$$

- Si un polynôme P divise tous les A_i alors P divise D .

Définition

Le polynôme D de la proposition ci-dessus est appelé *PGCD* des polynômes A_1, \dots, A_n . Il est noté :

$$D = A_1 \wedge \dots \wedge A_n = \bigwedge_{i=1}^n A_i$$

Remarque. Cas extrêmes : $\bigwedge_{i=1}^1 A_i = A_1$ $\bigwedge_{i=1}^0 A_i = 0$

Définition

Soit $n \in \mathbb{N}^*$.

- Les polynômes A_1, \dots, A_n sont premiers entre eux dans leur ensemble si :

- Les polynômes A_1, \dots, A_n sont premiers entre eux deux à deux si :

Remarque. Si les polynômes A_1, \dots, A_n sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leur ensemble. La réciproque est fausse.

E. Polynômes irréductibles

Définition

Un polynôme P de $\mathbb{K}[X]$ est dit *irréductible* si :

- $\deg P \geq 1$
- Les seuls diviseurs de P sont les scalaires non-nuls et les polynômes associés à P .

Remarque. Les polynômes irréductibles de $\mathbb{K}[X]$ jouent le rôle des nombres premiers dans \mathbb{Z} .

Exemple 12.

- Pour tout $\alpha \in \mathbb{K}$, le polynôme $P = X - \alpha$ est irréductible. En effet il est de degré 1, et si on écrit $P = AB$ alors A ou B est de degré 0, donc la seule écriture possible comme produit est $P = \lambda\left(\frac{1}{\lambda}(X - \alpha)\right)$.
- Le polynôme $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Les résultats de la partie IV permettent d'énoncer les propriétés suivantes :

Proposition

Les polynômes irréductible de $\mathbb{C}[X]$ sont les $\lambda(X-\alpha)$ avec $\alpha \in \mathbb{C}$ et $\lambda \in \mathbb{C}^*$, c'est-à-dire les polynômes de degré 1.

Proposition

Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- Les $\lambda(X - \alpha)$ avec $\alpha \in \mathbb{R}$ et $\lambda \in \mathbb{R}^*$, c'est-à-dire les polynômes de degré 1.
- Les polynômes de degré 2 à discriminant strictement négatif.

Théorème

Tout polynôme de $\mathbb{K}[X]$ se décompose comme produit d'un élément de \mathbb{K}^* et de facteurs irréductibles unitaires de $\mathbb{K}[X]$.

Cette décomposition est unique à permutation des facteurs près.

Démonstration. Il reste à démontrer l'unicité. Pour ceci on remarque que l'ensemble des racines complexe d'un polynôme est uniquement déterminé, de même que la multiplicité des racines. Ceci justifie l'unicité de la décomposition dans $\mathbb{C}[X]$.

L'unicité dans $\mathbb{R}[X]$ en est conséquence. \square

Proposition

Soit A et B deux polynômes de $\mathbb{K}[X]$. Alors :

- (i) A divise B si et seulement si les racines complexes de A sont racines de B avec une multiplicité inférieure ou égale.
- (ii) A et B sont premiers entre eux si et seulement s'ils n'ont pas de racine complexe commune dans \mathbb{C} .

Démonstration.

(i) On considère la décomposition en facteurs premiers de B dans $\mathbb{C}[X]$:

$$B = \lambda(X - \alpha_1)^{m_1} \dots (X - \alpha_r)^{m_r}$$

Avec r entier naturel, λ complexe non-nul, $\alpha_1, \dots, \alpha_r$ complexes distincts, m_1, \dots, m_r entiers naturels strictement positifs.

Si A divise B alors il existe un polynôme Q tel que $B = AQ$. Si α est une racine de A alors $A(\alpha) = 0$, donc $B(\alpha) = 0$ et α est racine de B . De même les racines de Q sont racines de B , donc A et Q admettent des décompositions dans $\mathbb{C}[X]$ de la forme :

$$A = \mu(X - \alpha_1)^{k_1} \dots (X - \alpha_r)^{k_r} \quad \text{et} \quad Q = \nu(X - \alpha_1)^{\ell_1} \dots (X - \alpha_r)^{\ell_r}$$

où les k_i et les ℓ_i sont des entiers naturels éventuellement nuls.

Comme $B = AQ$ alors pour tout $i = 1, \dots, r$: $m_i = k_i + \ell_i$ donc $k_i \leq m_i$.

(ii) On démontre la négation de l'équivalence : A et B ne sont pas premiers entre eux si et seulement s'ils ont au moins une racine complexe commune.

Notons $D = A \wedge B$. Alors A et B ne sont pas premiers entre eux si et seulement si D est de degré au moins 1, donc si et seulement si D admet au moins une racine complexe.

Si D admet une racine complexe α alors $(X - \alpha)$ divise D . Or D divise A et B donc $(X - \alpha)$ divise A et B , donc α est racine commune de A et de B .

Réiproquement si A et B admettent une racine commune α alors $(X - \alpha)$ divise A et B donc $(X - \alpha)$ divise D et ainsi D admet au moins une racine. \square