Chapitre XIV

Polynômes

On fixe dans tout ce chapitre un corps $\mathbb{K}$ égal à $\mathbb{R}$ ou $\mathbb{C}$.

1.⁻ L'algèbre $\mathbb{K}[X]$

a) Polynômes à une indéterminée

Définition XIV.1. On appelle **polynôme à une indéterminé** toute suite $(a_n)_n \in \mathbb{K}^{\mathbb{N}}$ telle que :

$$\exists\, d \in \mathbb{N},\ \forall n \geq d,\ a_n = 0\,.$$

Les termes de cette suite sont appelés **coefficients** du polynôme.

Vocabulaire. Une suite vérifiant la propriété *supra* est dite **presque nulle** : seul un nombre fini de ses termes sont en effet différents de 0.

Notation.

- L'ensemble des polynômes à une indéterminée sur $\mathbb{K}$ est noté $\mathbb{K}[X]$.
- Le polynôme correspondant à la suite nulle sera noté 0.
- Le polynôme correspondant à la suite $(1, 0, \ldots)$ est noté 1 ou X^0.
- De façon générale, le polynôme correspondant à la suite $(\delta_{k,n})_n$ pour $k \geq 0$ est noté X^k, où $\delta_{k,n}$ est le **symbole de Kronecker** valant 0 si $k \neq n$ et 1 sinon.

Proposition XIV.1. $(\mathbb{K}[X], +)$ est un sous–groupe de $(\mathbb{K}^{\mathbb{N}}, +)$. Il s'agit donc d'un groupe abélien de neutre $(0)_n$.

Démonstration. Trivial. □

➠ **Exemple XIV.1.** $1 + X$ est le polynôme correspondant à la suite $(1, 1, 0\ldots)$.

Remarquons ensuite que si $\lambda \in \mathbb{K}$ et $P = (a_n)_n$ est un polynôme, nous pouvons définir (de façon compatible avec l'addition des suites) le polynôme

$$\lambda P = (\lambda a_n)_n \ \in \mathbb{K}[X].$$

In fine, nous avons donc additionner les polynômes entre eux et les multiplier par des éléments de $\mathbb{K}$ (nous parlerons plus tard de **scalaires**, *cf.* chapitre XVIII). De plus, nous pouvons avec ces conventions écrire, pour $P = (a_n)_n \in \mathbb{K}[X]$ que :

$$P = a_0X^0 + a_1X + a_2X^2 + \dots$$

soit

$$P = \sum_{k=0}^{\infty} a_kX^k \ .$$

✖ **Attention :** cette somme n'est **PAS** réellement infinie, étant donné que seul un nombre fini des termes a_k sont non nuls.

Définition XIV.2. Soit $P \in \mathbb{K}[X]$. On appelle **degré** de P la quantité

$$\deg(P) = \begin{cases} \max\{N \in \mathbb{N} \,|\, a_N \neq 0\} \text{ si } P \neq 0 \\ -\infty \text{ si } P = 0 \end{cases} .$$

Un polynôme de degré nul ou $-\infty$ est dit **constant**.

✌ **Remarque XIV.1.** Le degré est bien défini car toute partie de $\mathbb{N}$ non vide et majorée admet un plus grand élément (proposition I.7).

➠ **Exemple XIV.2.** $\deg(1) = 0$, $\deg(X^{17} - X) = 17$.

Notation. Pour $d \in \mathbb{N} \cup \{-\infty\}$, on note $\mathbb{K}_d[X]$ l'ensemble des polynômes de degré inférieur ou égal à d. Rappelons que par convention sur la droite réelle achevée, $-\infty$ est strictement inférieur à tout entier naturel.

Par conséquent, si $P = (a_n)_n \in \mathbb{K}[X]$ est de degré $d \geq 0$, nous pouvons écrire :

$$P = \sum_{k=0}^{d} a_kX^k \ .$$

✌ **Remarque XIV.2.** Il découle de tout ceci que si $P = (a_n)_n, Q = (b_n)_n \in KK[X]$ alors :

$$P = Q$$
$$\iff$$
$$(\deg(P) = \deg(Q)) \wedge (\forall k \leq \deg(P),\ a_k = b_k) \ .$$

Définition XIV.3. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. On appelle **coefficient dominant** de P son coefficient non nul d'indice le plus élevé. Si le coefficient dominant de P est égal à 1, le polynôme est dit **unitaire**.

Notation. $\mathrm{cd}(P)$

✌ **Remarque XIV.3.** Si P est non nul de degré d, $\mathrm{cd}(P)$ est le coefficient placé devant X^d dans l'écriture de P en tant que somme.

Convention. $\mathrm{cd}(0) = 0$ (et il s'agit donc du seul polynôme de coefficient dominant nul).

➠ **Exemple XIV.3.** $\mathrm{cd}(1 + X^2 + 2X^4) = 2$.

Proposition XIV.2. Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}^*$. Alors :

(i) $\deg(\lambda P) = \deg(P)$;

(ii) $\deg(P+Q) \leq \max(\deg(P), \deg(Q)$ avec égalité si $\deg(P) \neq \deg(Q)$.

Démonstration.

(i) Trivial.

(ii) Posons $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{k=0}^{d'} b_k X^k$ avec $(d, d') = (\deg(P), \deg(Q))$. Alors :
— si $d \neq d'$, par exemple $d < d'$ $P + Q$ admet $b_{d'}$ et son degré est clairement d'.
— si $d = d'$ alors pour tout $k > d$ on a $a_k + b_k = 0$ ce qui entraîne le résultat. Pour un contre exemple à l'égalité dans le cas où les degrés sont égaux, additionner 1 et -1.

□

b) Produit de polynômes

Proposition/définition XIV.4. Soient $P, Q \in \mathbb{K}[X]$, de coefficients respectifs $(a_i)_i$ et $(b_i)_i$. Alors :

(i) la suite de terme général (pour $k \geq 0$)

$$\sum_{j=0}^{k} a_j b_{k-j}$$

est un polynôme, appelé produit de P et Q et noté PQ ;

(ii) $\deg(PQ) = \deg(P) + \deg(Q)$.

✌ **Remarque XIV.4.** On vérifie par récurrence que, pour tout $k \in \mathbb{N}^*$, $\prod_{i=1}^{k} X = X^k$, ce qui est rassurant.

Démonstration. Si P ou Q est le polynôme nul, inutile de trop se fatiguer. Dans le cas contraire, posons $d = \deg(P)$ et $d' = \deg(Q)$. Alors, pour tout $k > d + d'$ on a :

$$R_k = \sum_{j=0}^{k} a_j b_{k-j} = 0$$

car si $j > d$, $a_j = 0$ et si $j \leq d$ alors $k - j > d'$ et donc $b_{k-j} = 0$. Le produit PQ est donc bien un polynôme (suite presque nulle) et

$$\deg(PQ) \leq d + d' .$$

Pour obtenir l'égalité des degrés, il nous suffit de constater que

$$R_{d+d'} = a_d b_{d'} \neq 0 .$$

□

✌ **Remarque XIV.5.** On a de fait la formule suivante :

$$\left(\sum_{k=0}^{d} a_k X^k\right)\left(\sum_{k=0}^{d'} b_k X^k\right) = \sum_{k=0}^{d+d'}\left(\sum_{j=0}^{k} a_j b_{k-j}\right) X^k .$$

Corollaire XIV.2.a. $(\mathbb{K}[X], +, \times)$ est un anneau intègre (et donc commutatif) de neutres 0 et $1 = X^0$.

Démonstration. Tout a déjà été fait sauf la simplification par un élément non nul, qui découle de la formule du degré d'un produit. □

Proposition XIV.3. Les inversibles de $\mathbb{K}[X]$ sont les polynômes constants non nuls.

Démonstration. Si $P \in \mathbb{K}[X]^\times$, alors il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$. En passant au degré, on obtient que $\deg(P) + \deg(Q) = 0$, d'où le résultat. □

c) Composition

Définition XIV.5. Soient $P, Q \in \mathbb{K}[X]$, avec $P = \sum_{k=0}^{d} a_k X^k$. On appelle composée de P par Q le polynôme :

$$P \circ Q = \sum_{k=0}^{d} a_k Q^k .$$

✌ **Remarque XIV.6.** Il s'agit bien d'un polynôme par structure d'anneau sur $\mathbb{K}[X]$.

➠ **Exemple XIV.4.** $X^2 \circ (X + 1) = (X + 1)^2$.

Proposition XIV.4. Soient $P, Q \in \mathbb{K}[X]$ avec Q non constant. Alors :

$$\deg(P \circ Q) = \deg(P)\deg(Q)\,.$$

✖ **Attention :** cela est faux si $\deg(Q) = 0$; en effet, la composée de $X - 1$ par 1 est de degré $-\infty$.

Démonstration. Posons $d = \deg(P)$ et $P = \sum_{k=0}^{d} a_k X^k$. Alors

$$P \circ Q = \sum_{k=0}^{d} a_k Q^k$$

donc, par somme et comme tous les $\deg(Q^k)$ sont distincts car Q est non constant, $\deg(P \circ Q) = \max_{k \leq d} \deg(a_k Q^k)$, ce dernier étant égal à $\deg(Q^d)$ car $a_d \neq 0$. □

Proposition XIV.5. La composition des polynômes est associative, non commutative, admet X pour neutre et est distributive **à droite** par rapport à l'addition.

Démonstration. Hastur, Hastur, Hastur. □

En résumé, il convient de retenir que :
- $X^2 \circ (X+1) = (X+1)^2 \neq (X+1) \circ X^2 = X^2 + 1$;
- si $P, Q, H \in \mathbb{K}[X]$ on a $P \circ (Q \circ H) = (P \circ Q) \circ H$ et $(P+Q) \circ H = P \circ Q + Q \circ H$ mais, comme vu *supra*, $P \circ (Q + H) \neq P \circ Q + P \circ H$.

2.⁻ Arithmétique des polynômes

a) Multiples, diviseurs

Définition XIV.6. Soient $A, B \in \mathbb{K}[X]$. On dira que A **divise** B, ou que B est un **multiple** de A, si il existe $C \in \mathbb{K}[X]$ tel que $B = AC$.

Notation.
- $A|B$.
- On notera $\mathscr{D}(A)$ l'ensemble des diviseurs de A et $A\mathbb{K}[X]$ l'ensemble de ses multiples.

✌ **Remarque XIV.7.**
- Comme sur $\mathbb{Z}$, 0 est divisible par tout polynôme et $A|B \Leftrightarrow B\mathbb{K}[X] \subset A\mathbb{K}[X]$.
- Soit $P \in \mathbb{K}[X]$ et soit $\lambda \in \mathbb{K}^*$. Alors $P = (\lambda P) \times \frac{1}{\lambda}$ et donc $\lambda | P$.
- Par degré d'un produit, si $A|B$ alors $\deg(A) \leq \deg(B)$ lorsque $B \neq 0$.

✍ **Exercice XIV.1.** Soient $a, b, c, r \in \mathbb{C}$ tels que $a \neq 0$. À quelle condition sur a, b, c et r a–t–on $(X - r) \,|\, aX^2 + bX + c$?

Proposition XIV.6. La relation "|" est réflexive et transitive. De plus, pour tous $A, B \in \mathbb{K}[X]$ on a :

$$(A|B) \wedge (B|A) \Leftrightarrow \exists\, \lambda \in \mathbb{K}^*,\ A = \lambda B.$$

On dit alors que les polynômes A et B sont **associés**.

Démonstration. Le premier point se traite de façon analogue à ce que nous avons vu au chapitre X. Pour le second, le sens "bas vers haut" est trivial et si A, B sont tels que $(A|B) \wedge (B|A)$ alors il existe $P, Q \in \mathbb{K}[X]$ tels que $A = PB$ et $B = AQ$ et donc $A = PQA$, *i.e* $A(1 - PQ) = 0$, ce qui entraîne que soit $A = 0$ (et dans ce cas $B = 0$) soit $PQ = 1$ ce qui n'est possible que si $P, Q \in \mathbb{K}[X]^\times = \mathbb{K}^*$. □

Théorème XIV.7 (Division euclidienne)**.**
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que :
- $A = BQ + R$;
- $\deg(R) < \deg(B)$.

Vocabulaire. Comme dans le cas entier, on parle de quotient, reste, diviseur et dividende.

➠ **Exemple XIV.5.** $X^2 + X + 1 = X(X + 1) + 1$ est une division euclidienne.

Démonstration.

Existence. Si $\deg(A) < \deg(B)$ ou $A = 0$ alors $Q = 0$ et $R = A$ conviennent. Dans le cas contraire, démontrons l'existence du couple (Q, R) par récurrence forte sur $d = \deg(A)$. **Attention à la formulation de l'hypothèse de récurrence :** nous voulons montrer que, pour tout $d \geq 0$, pour tous polynômes A, B tels que $d = \deg(A) \geq deg(B)$ il existe un couple (Q, R) vérifiant les conclusions du théorème.
- Si $d = 0$, alors A et B sont inversibles ($\deg(B) \leq \deg(A)$) et donc $A = B \times \frac{A}{B} + 0$.
- Si on suppose l'hypothèse vérifiée jusqu'à un certain rang $d \geq 0$ et que l'on se donne $A = \sum_{k=0}^{d+1} a_k X^k$ et $B = \sum_{k=0}^{d'} b_k X^k$ deux polynômes tels que $d + 1 = \deg(A) \geq d' = \deg(B)$ alors :

$$A' = A - \frac{a_{d+1}}{b_{d'}} X^{d+1-d'} B$$

est un polynôme de degré au plus d. Par hypothèse de récurrence (ou, au pire, car $\deg(B) > \deg(A')$), il existe donc $(Q, R) \in \mathbb{K}[X]^2$ tels que $A' = BQ + R$ et $\deg(R) < \deg(B)$. Ceci entraîne que :

$$A = B\left(\frac{a_{d+1}}{b_{d'}} X^{d+1-d'} + Q\right) + R$$

d'où le résultat.

Unicité. Si il existe deux couples (Q,R) et (Q',R') vérifiant les conclusions du théorème alors $B(Q-Q')=R'-R$ et donc

$$\deg(B)+\deg(Q-Q')=\deg(R'-R)<\deg(B)$$

d'où $\deg(Q-Q')=-\infty$ et le résultat.

□

✌ **Remarque XIV.8.** La démonstration du théorème XIV.7 nous livre un algorithme récursif implémentable en pratique.

b) PGCD

Proposition/définition XIV.7. Soient $A,B\in\mathbb{K}[X]$ tels que $B\neq 0$. On appelle **plus grand commun diviseur** de A et B tout élément de degré maximal de $\mathscr{D}(A)\cap\mathscr{D}(B)$.

Démonstration. Un tel élément existe car $\{\deg(P)\,|\,P\in\mathscr{D}(A)\cap\mathscr{D}(B)\}$ est une partie de $\mathbb{N}$ (car $B\neq 0$ donc $\mathscr{D}(B)$ ne contient pas $-\infty$) non vide (il contient 0 car les constantes non nulles divisent tout polynôme) et majorée par $\max(\deg(A),\deg(B))$.
□

✖ **Attention :** il n'y a pas unicité : X^2 et X^2+X admettent (entre autres) X et $-X$ comme PGCD. En fait, c'est même bien pire que cela : si D est un PGCD de A et B alors λD l'est également pour tout $\lambda\in\mathbb{K}^*$ ...

Proposition XIV.8. Soient $A,B\in\mathbb{K}[X]$ tels que $B\neq 0$ et soit $\Delta\in\mathbb{K}[X]$. Alors :

$$\Delta \text{ est } \textbf{un} \text{ PGCD de } A \text{ et } B \iff \mathscr{D}(A)\cap\mathscr{D}(B)=\mathscr{D}(\Delta)\,.$$

Démonstration. Analogue au cas entier vu dans le chapitre X. □

Corollaire XIV.8.a. Soient $A,B\in\mathbb{K}[X]$ tels que $B\neq 0$ et soient Δ,Δ' deux PGCD de A et B. Alors Δ et Δ' sont associés.

✌ **Remarque XIV.9.** Par conséquent, si Δ est **un** PGCD de A et B alors l'ensemble des PGCD de ces deux polynômes est

$$\{\lambda\Delta\,|\,\lambda\in\mathbb{K}^*\}\,.$$

Cet ensemble contient donc un unique polynôme unitaire.

Définition XIV.8. On appelle PGCD de deux polynômes leur unique PGCD unitaire.

Notation. $A \wedge B$

Ceci nous permet d'énoncer une caractérisation du PGCD de $A, B \in \mathbb{K}[X]$ analogue à celle vue au chapitre X :

$$\Delta = A \wedge B \iff \begin{cases} \mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(\Delta) \\ \text{cd}(\Delta) = 1 \end{cases}.$$

✌ **Remarque XIV.10.** Si $A \neq 0$ alors $A \wedge 1 = 1$ et $A \wedge A = \frac{A}{\text{cd}(A)}$.

À la question "comment trouver le PGCD de deux polynômes ?", nous donnerons la réponse suivante : il faut commencer par suivre l'algorithme d'Euclide vu dans le chapitre X puis ensuite diviser le dernier reste non nul par son coefficient dominant. Il est **essentiel de ne pas omettre cette dernière étape.**

➠ **Exemple XIV.6.**
— $(X^2 + 3X + 1) \wedge (X + 1) = 1$;
— $(X^2 - 3X + 2) \wedge (X^3 - 2X^2 + X - 2) = X - 2$.

✌ **Remarque XIV.11.** Comme dans le cas entier, l'algorithme d'Euclide étendu permet d'obtenir un couple U, V tel que $AU + BV = A \wedge B$.

c) Bézout et Gauss

Définition XIV.9. Deux polynômes A et B sont dits **premiers entre eux** si $A \wedge B = 1$.

Le théorème qui suit est, contrairement au théorème X.10, réellement du à Étienne Bézout(français, 1730—1783).

Théorème XIV.9 (Bézout)**.**
Soient $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. Alors :

$$A \text{ et } B \text{ sont premiers entre eux} \iff \exists U, V \in \mathbb{K}[X],\ AU + BV = 1.$$

Démonstration. Analogue au cas entier. □

De la même façon, le lemme de Gauss vu au chapitre X se généralise au cas d'anneaux de polynômes.

Théorème XIV.10 (Lemme de Gauss)**.**
Soient $A, B, C \in \mathbb{K}[X]$ tels que $B \neq 0$. On suppose que :
— $A | BC$;
— $A \wedge B = 1$.
Alors A divise C.

Démonstration. Analogue au cas entier. □

✍ **Exercice XIV.2.** Résoudre dans $\mathbb{K}[X]$ l'équation $(X^3-1)U+(X^2+1)V = 2X^2$.

➥ **Correction :** *Il s'agit d'adapter la méthode vue lors de l'étude des équations diophantiennes. Comme X^3-1 et X^2+1 sont premiers entre eux, on trouve par Euclide étendu que :*

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

et donc on trouve une solution particulière $U_0 = X^2(X-1)$, $V_0 = X^2(1+X-X^2)$ et on démontre à l'aide du lemme de Gauss que les seules solutions sont alors de la forme $(U_0+(X^2+1)C, V_0-(X^3-1)C)$, avec $C \in \mathbb{K}[X]$.

d) PPCM et généralisations

De la même façon, on définit le PPCM de deux polynômes A et B comme l'unique polynôme **unitaire** $A\vee B$ tel que $A\mathbb{K}[X]\cap B\mathbb{K}[X] = (A\vee B)\mathbb{K}[X]$. Il s'agit de l'unique élément unitaire de degré minimal de $A\mathbb{K}[X]\cap B\mathbb{K}[X]$. On retrouve alors l'égalité :

$$(A\wedge B)(A\vee B) = \frac{AB}{\mathrm{cd}(AB)}\,.$$

De plus, on peut définir le PGCD (resp. le PPCM) d'une famille de polynômes de la même façon que pour les entiers. On généralise également l'existence de relations de Bézout aux familles de n polynômes premiers entre eux dans leur ensemble.

3.⁻ Fonctions polynomiales

a) C'est quoi ?

Définition XIV.10. Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$. On appelle **fonction polynomiale associée à** P l'application

$$\begin{aligned} f : \mathbb{K} &\longrightarrow \mathbb{K} \\ x &\mapsto \sum_{k=0}^{d} a_k x^k\,. \end{aligned}$$

Notation. On note $\mathbb{K}[x]$ l'ensemble des fonctions polynomiales sur $\mathbb{K}$.

✖ **Attention :** si $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, la quantité "$P(a)$" n'a a priori aucun sens. Si f est la fonction polynomiale associée à P, $f(a)$ est par contre bien défini. On parle malgré tout d'**évaluation** du polynôme P en a.

➠ **Exemple XIV.7.** La fonction polynomiale associée à X^2 est (normalement) bien connue du lecteur.

✌ **Remarque XIV.12.**
— On montre aisément que $(\mathbb{K}[x], +, \times)$ est un sous–anneau de $\mathbb{K}^{\mathbb{K}}$.
— De plus, si $\lambda \in \mathbb{K}$ et $f \in \mathbb{K}[x]$ alors $\lambda f \in \mathbb{K}[x]$.
— Soit $P = \sum_{k=0}^{d} a_k X^k$ un polynôme de degré $d \geq 0$. On appelle **forme de Hörner** (nommée en l'honneur William George Hörner, mathématicien britannique, 1786—1837, bien que l'on en retrouve des traces dans des écrits chinois et perses des siècles plus tôt) de P l'écriture

$$P = a_0 + X(a_1 + X(a_2 + X(\dots X(a_{d-1} + a_d X))) \, .$$

Par exemple, la forme de Hörner de X^3+3X^2+X+7 est $7+X(1+X(3+X))$. Cette forme est intéressante car elle permet d'évaluer un polynôme de degré n à l'aide de n multiplications et n additions, ce qui est la complexité algorithmique optimale d'une telle opération.

◇ **Lien à la choucroute**

On considère désormais l'application suivante, que l'on sait surjective par construction :

$$\begin{aligned} \varphi : \mathbb{K}[X] &\longrightarrow \mathbb{K}[x] \\ \sum_{k=0}^{d} a_k X^k &\mapsto \left(x \mapsto \sum_{k=0}^{d} a_k x^k \right) \, . \end{aligned}$$

Ceci signifie, rappelons le, que toute fonction polynôme correspond à (au moins) un polynôme. Cool. Mais encore ? Eh bien on peut vérifier que, pour tous $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ on a :

$$\varphi(P + \lambda Q) = \varphi(P) + \lambda\varphi(Q) \quad \text{et} \quad \varphi(PQ) = \varphi(P)\varphi(Q) \, .$$

L'application φ est donc un morphisme d'anneaux (et une application linéaire, *cf.* chapitre XVIII).

La question qui nous brûle les lèvres à ce stade est naturellement la suivante : φ est–elle injective ? À savoir, étant donné deux polynômes P, Q tels que $\varphi(P) = \varphi(Q)$, a–t–on $P = Q$? La réponse devra hélas attendre quelques temps ...

b) Racines

Définition XIV.11. Soit $P \in \mathbb{K}[X]$ et soit $f = \varphi(P)$. On appelle **racine** (ou zéro) **de** P tout scalaire $a \in \mathbb{K}$ vérifiant $f(a) = 0$.

Notation. On notera $\mathrm{Rac}(P)$ l'ensemble des racines de P. Il sera souvent utile de spécifier le corps sur lequel nous travaillons ; on notera alors $\mathrm{Rac}_{\mathbb{K}}(P)$.

➠ **Exemple XIV.8.**
— $\mathrm{Rac}_{\mathbb{C}}(X^2+1) = \{i, -i\}$;
— $\mathrm{Rac}_{\mathbb{R}}(X^2+1) = \emptyset$;

— $\mathrm{Rac}_{\mathbb{C}}(X^n - 1) = \mathbb{U}_n$ pour tout $n \geq 1$.

Proposition XIV.11. Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{K}$. Alors :

$$a \in \mathrm{Rac}(P) \iff X - a \text{ divise } P.$$

Démonstration.

(⇑) Immédiat : si $P = (X-a)Q$ avec $Q \in \mathbb{K}[X]$ alors $\varphi(P) = x \mapsto (x-a)\varphi(Q)(x)$.

(⇓) Supposons que $a \in \mathrm{Rac}(p)$. Par division euclidienne, il existe un unique couple (Q, R) de polynômes tels que

$$P = (X - a)Q + R$$

et $\deg(R) < 1$. De fait, R est constant et comme $\varphi(P)(a) = 0$ on a $\varphi(R)(a) = 0$. Ainsi, $R = 0$ (car il est constant).

□

Corollaire XIV.11.a. Soit $P \in \mathbb{K}[X]$ et soient $a_1, \dots a_n \in \mathrm{Rac}(P)$ deux à deux distincts. Alors $\prod_{k=1}^{n}(X - a_k)$ divise P.

Démonstration. Par récurrence à l'aide du lemme de Gauss (théorème XIV.10). □

On déduit de tout ceci la proposition fondamentale suivante, qui sera centrale à l'étude des racines de polynômes.

Proposition XIV.12. Soit $P \in \mathbb{K}[X]$ de degré $n \geq 0$. Alors $\mathrm{Rac}(P)$ contient au plus n éléments.

Démonstration. Si $a_1, \dots, a_k$ sont des racines deux à deux distinctes de P on a que

$$\prod_{i=1}^{k}(X - a_i) \text{ divise } P$$

et donc

$$k = \deg\left(\prod_{i=1}^{k}(X - a_i)\right) \leq \deg(P) = n\,,$$

d'où le résultat. □

✌ **Remarque XIV.13.** On déduit de ceci le résultat suivant, fort utile en pratique : **tout polynôme admettant plus de racines que son degré est nul**.

Théorème XIV.13.
L'application φ est bijective.

Démonstration. Il ne reste qu'à montrer que φ est injective. Si on suppose trouvé $P \in \mathbb{K}[X]$ tel que $P \in \mathrm{Ker}(\varphi)$, alors $\varphi(P) = 0$ et donc

$$\forall a \in \mathbb{K}, \quad \varphi(P)(a) = 0\,.$$

Ceci entraîne, comme le corps $\mathbb{K}$ est infini, que P admet une infinité de racines. Il s'agit donc du polynôme nul, *ergo* $P = 0$. □

✌ **Remarque XIV.14.** Il nous sera donc possible d'identifier (comme vous le faisiez probablement depuis un bon moment) fonctions polynomiales et polynômes. Ceci entraîne qu'il est désormais permis d'écrire des choses sulfureuses comme "$P(a)$" en toute impunité.

Définition XIV.12. Soit $P \in \mathbb{K}[X] \setminus \{0\}$ et soit $a \in \mathbb{K}$. On appelle **multiplicité de a relativement à P** la quantité

$$\mu_P(a) = \max\{k \in \mathbb{N} \,|\, (X-a)^k | P\}\,.$$

Vocabulaire. Si $\mu_P(a) = 1$, on parle de racine simple ; si $\mu_P(a) \geq 2$, on parle de racine multiple (double, triple,...).

✌ **Remarque XIV.15.** Il apparaît clairement que $a \in \mathrm{Rac}(P) \Leftrightarrow \mu_P(a) \neq 0$.

➠ **Exemple XIV.9.** On pourra faire le parallèle avec le cours de première et les racines simples, doubles, des trinômes du second degré.

Définition XIV.13. Un polynôme $P \in \mathbb{K}[X] \setminus \{0\}$ est dit **scindé sur** $\mathbb{K}$ si la relation suivante est vérifiée :

$$\sum_{a \in \mathrm{Rac}_{\mathbb{K}}(P)} \mu_P(a) = \deg(P)\,.$$

➠ **Exemple XIV.10.** Tout polynôme de degré 2 est scindé sur $\mathbb{C}$.

✖ **Attention :** le caractère scindé dépend lui aussi du corps : comparer $X^2 + 1$ vu comme polynôme à coefficients complexes et son jumeau maléfique dans $\mathbb{R}[X]$...

Proposition XIV.14. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Alors :

$$P \text{ est scindé}$$

$$\Longleftrightarrow$$

$$P = \mathrm{cd}(P) \prod_{a \in \mathrm{Rac}(P)} (X-a)^{\mu_P(a)}\,.$$

Démonstration.

(⇑) Trivial.

(⇓) Par définition de la multiplicité, pour tout $a \in \mathrm{Rac}(P)$, $(X-a)^{\mu_P(a)}$ divise P ; ces polynômes étant premiers entre eux on a, par lemme de Gauss :

$$\prod_{a\in\mathrm{Rac}(P)} (X-a)^{\mu_P(a)} \mid P\,.$$

De plus, le degré de ces deux polynômes sont, comme P est scindé, égaux. On en déduit que leur quotient est de degré 0. Ce dernier est alors obligatoirement égal à $\mathrm{cd}(P)$ par identification des coefficients dominants.

□

c) Relations coefficients–racines

Autorisons nous à présent une (relativement) brève digression ; si $P = aX^2+bX+c \in \mathbb{K}[X]$ est un trinôme du second degré (avec donc $a \neq 0$), et que son discriminant est $\Delta = b^2 - 4ac$, il admet deux racine(s) (éventuellement égale(s)) donnée(s) par la formule

$$r_\pm = \frac{-b \pm \delta}{2a}$$

avec $\delta^2 = \Delta$. On en déduit que :

$$\begin{cases} r_+ + r_- = -\dfrac{b}{a} \\ r_+ r_- = \dfrac{b^2-\Delta}{4a^2} = \dfrac{c}{a} \end{cases}$$

ce qui entraîne que :

$$\begin{aligned} aX^2+bX+c &= a\left(X^2 + \frac{b}{a}X + \frac{c}{a}\right) \\ &= a(X^2 - (r_+ + r_-)X + r_+r_-) \\ &= a(X-r_+)(X-r_-)\,. \end{aligned}$$

Ces relations entre coefficients et racines sont appelées, dans un élan d'originalité à faire pâlir un scénariste de chez Marvel, des **relations coefficients–racines**.

En dégré 3, on voit apparaître des choses similaires ; en effet, si $P = (X-x_1)(X-x_2)(X-x_3)$ est un polynôme scindé de degré 3, on obtient, en développant :

$$\begin{aligned} P &= (X-x_1)(X-x_2)(X-x_3) \\ &= X^3 + aX^2 + bX + c \end{aligned}$$

avec

$$\begin{cases} a = -(x_1+x_2+x_3) \\ b = x_1x_2 + x_1x_3 + x_2x_3 \\ c = -x_1x_2x_3 \end{cases}.$$

De façon plus générale, si $n, k \in \mathbb{N}^*$ sont tels que $k \leq n$, on appelle k–**ième fonction symétrique élémentaire à n variables** l'application

$$\begin{aligned} \sigma_k : \mathbb{K}^n &\longrightarrow \mathbb{K}^n \\ (x_1,\dots,x_n) &\to \sum_{1\leq i_1<\dots<i_k\leq n} x_{i_1}\dots x_{i_k}\,. \end{aligned}$$

En particulier, pour tout $(x_1, \dots, x_n) \in \mathbb{K}^n$, on a :

$$\sigma_1(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i \,,$$

$$\sigma_2(x_1, \dots, x_n) = \sum_{i=1}^{n} \sum_{j=i+1}^{n} x_i x_j$$

et

$$\sigma_n(x_1, \dots, x_n) = \prod_{i=1}^{n} x_i \,.$$

Ces fonctions ont un lien fort avec les relations que nous venons de voir pour les degrés 2 et 3. Celles–ci se généralisent via le théorème suivant (sont exigibles les formules pour σ_1 et σ_n ; les autres doivent "pouvoir être retrouvées rapidement").

Théorème XIV.15 (Relations coefficients–racines)**.**
Soit $P = \sum_{k=1}^{n} a_k X^k$ un polynôme scindé de degré n dont les racines (comptées avec multiplicité) sont notées $r_1, \dots, r_n$. Alors :

$$\forall k \in [\![1, n]\!], \quad \sigma_k(r_1, \dots, r_n) = (-1)^k \frac{a_{n-k}}{a_n} \,.$$

✍ **Exercice XIV.3.** Résoudre :

$$\begin{cases} x+y+z &= 2 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z} &= \frac{5}{6} \\ xyz &= -6 \end{cases} .$$

➥ **Correction :** *En multipliant la ligne 2 par la ligne 3, on arrive au système :*

$$\begin{cases} x+y+z &= 2 \\ yz+xz+xy &= -5 \\ xyz &= -6 \end{cases} .$$

Les solutions sont donc les racines du polynôme $X^3-2X^2-5X+6 = (X-1)(X^2-X-6)$.

4.⁻ Dérivation

a) Dérivée formelle d'un polynôme

Définition XIV.14. Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{K}[X]$. On appelle **dérivée** (formelle) de P le polynôme

$$P' = \sum_{k=1}^{d} k a_k X^{k-1} \,.$$

➠ **Exemple XIV.11.** $(X^3 + X + 1)' = 3X^2 + 1$.

✌ **Remarque XIV.16.**
- On définit par récurrence les dérivées formelles d'ordre supérieur d'un polynôme.
- On vérifie aisément que la fonction polynomiale (lorsque $\mathbb{K} = \mathbb{R}$) associée à la dérivée formelle d'un polynôme est la dérivée de la fonction polynomiale associée à ce même polynôme. En particulier, les fonctions polynomiales sont de classe $\mathscr{C}^\infty(\mathbb{R})$.
- Il découle du point précédent que les formules usuelles de dérivation se généralisent à la dérivée formelle, quitte dans la cas complexe à travailler sur la restriction de la fonction polynomiale à $\mathbb{R}$. On peut également vérifier ces résultats par le calcul.

Proposition XIV.16. Soit $P \in \mathbb{K}[X]$ un polynôme **non constant**. Alors $\deg(P') = \deg(P) - 1$.

Démonstration. Immédiat par définition. □

✍ **Exercice XIV.4.** Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geq 2$ admettant $2 \leq k \leq n$ racines réelles distinctes. Que dire des racines de P' ?

b) Formule de Taylor polynomiale

Proposition XIV.17. Soit $P \in \mathbb{K}[X]$ et soit $a \in \mathbb{K}$. Alors

$$P = \sum_{k=0}^{\infty} \frac{(X-a)^k}{k!} P^{(k)}(a) \, .$$

✌ **Remarque XIV.17.**
- La notation "$P^{(k)}(a)$" est abusive, mais nous sommes entre gens de bonne compagnie.
- Comme de coutume, la somme apparaissant dans la formule est en faite finie, car (par décroissance du degré), $\exists\, N \in \mathbb{N}$, $\forall n \geq N$, $P^{(n)} = 0$.
- On peut donc déduire des valeurs successives des dérivées d'un polynôme en un point l'expression générale de celui–ci.
- Un conséquence de cette formule est que si l'on note $(a_k)_k$ les coefficients de P on a :
$$\forall k \in \mathbb{N}, \quad a_k = \frac{P^{(k)}(0)}{k!} \, .$$

Démonstration. Vous l'aurez deviné, c'est reparti pour une récurrence sur le $n = \deg(P)$ ...
- Si P est constant, tout va bien.
- Sinon, yaka appliquer l'hypothèse de récurrence à P' et "primitiver", puis être content.

□

➠ **Exemple XIV.12.** La formule de Taylor permet de déterminer l'unique polynôme P de degré inférieur ou égal à deux vérifiant $P(0) = 0$, $P'(0) = 2$ et $P'(0) = 3$.

Nous verrons dans le chapitre XVII que la formule de Taylor permet d'approximer des fonctions à l'aide de polynômes.

Corollaire XIV.17.a. Soit $a \in \mathbb{K}$, $k \in \mathbb{N}$ et $P \in \mathbb{K}[X]$. Alors :

$$\mu_p(a) = k \iff \begin{cases} P(a) = P'(a) = \ldots = P^{(k-1)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}.$$

Démonstration.

(⇐) Cela découle de la formule de Taylor : P est divisible par $(X-a)$, $(X-a)^2$, …, $(X-a)^{k-1}$ mais pas par $(X-a)^k$.

(⇒) Par définition, il existe un polynôme Q tel que $Q(a) \neq 0$ et $P = (X-a)^k Q$. Par formule de Taylor, il existe $q_0, \ldots, q_n \in \mathbb{K}$ avec q_0 non nul tels que :

$$Q = \sum_{i=0}^{n} q_i (X-a)^i$$

et donc :

$$P = \sum_{i=0}^{n} q_i (X-a)^{i+k}.$$

En admettant (temporairement, *cf.* chapitre XVIII) que l'on peut identifier les coefficients entre deux polynômes de Taylor égaux, on obtient le résultat en appliquant la formule de Taylor à P.

□

5.⁻ Irréductibilité

a) C'est quoi ?

Définition XIV.15. Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible** si :
- P est non constant ;
- si $P = QR$ avec $Q, R \in \mathbb{K}[X]$ alors Q ou R est constant.

➠ **Exemple XIV.13.** Les polynômes de degré 1 sont constants sur $\mathbb{R}$ ou $\mathbb{C}$ et les polynômes de degré deux de discriminant négatif sur $\mathbb{R}$.

✖ **Attention :** l'irréductibilité dépend du corps sur lequel on travaille : $X^2+1 = (X-i)(X+i)$ sur $\mathbb{C}$.

Théorème XIV.18.
Tout polynôme non constant s'écrit de façon unique (à l'ordre près des facteurs et à constante multiplicative près) comme produit de polynômes irréductibles.

✌ **Remarque XIV.18.** Ce résultat est analogue à la proposition X.14 (décomposition en produits de facteurs premiers sur $\mathbb{Z}$). Ceci n'est pas une coïncidence.

➠ **Exemple XIV.14.** $X^3-1=(X-1)(X-j)(X-j^2)=(X-1)(X^2+X+1)$; on remarque que la décomposition dépend (sans surprise) du corps sur lequel on travaille.

Démonstration. **Existence.** Youpi, une récurrence forte sur le degré ! Attention à la formulation de l'hypothèse. . ..
- $d=1$**.** C'est plié.
- **Supposons la propriété vérifiée pour tout** $k\in[\![1,n]\!]$ **avec** $n\geq 1$ **fixé.** Si P est irréductible, c'est fini. Sinon, il existe deux polynômes $Q,R\in\mathbb{K}[X]$ non constants tels que $P=QR$. Nous pouvons appliquer l'hypothèse de récurrence à ceux–ci et voila, c'est plié.

Unicité. Nous en parlerons plus tard. Là, j'ai water–poney.

□

➠ **Exemple XIV.15.** Le polynôme X^n-1 (pour $n\geq 1$) admet exactement n racines sur $\mathbb{C}$: les éléments de $\mathbb{U}_n$. Ceci entraîne la factorisation suivante (**sur** $\mathbb{C}$) :

$$X^n-1=\prod_{\xi\in\mathbb{U}_n}(X-\xi)\,.$$

b) C'est qui (édition complexe) ?

Le théorème central de ce paragraphe est le suivant, parfois appelé théorème fondamental de l'algèbre. Son histoire est complexe (ah ah) et intrinsèquement lié à celle du corps $\mathbb{C}$ dont on peut considérer qu'il est la motivation première pour l'étude. On trouve des traces de ce résultat chez François Viète (français, 1540—1603), Albert Girard (français, 1595—1632) et Renée Descartes, que l'on ne présente plus (1596—1650), entre autres.

Une première démonstration de ce résultat est esquissée par Jean le Rond d'Alembert (français, 1717—1783). Celle–ci est incomplète, malgré quelques ajouts ultérieurs par Jean–Robert Agrand (amateur suisse, 1768—1822). Une démonstration complète n'apparaîtra que suite aux efforts (indépendants) de Lagrange, Euler et Gauss, qui en produit la première démonstration complète (et fort analytique) en 1816.

Théorème XIV.19 (D'Alembert—Gauss)**.**
Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.

Démonstration. Admis. □

Corollaire XIV.19.a. Les polynômes irréductibles de $\mathbb{C}$ sont les polynômes de degré un.

Démonstration. Il est clair que les polynômes de degré un sont irréductibles. Réciproquement, si $P \in \mathbb{C}[X]$ est irréductible, il admet une racine $a \in \mathbb{C}$ d'après le théorème XIV.19 et donc est divisible par $X - a$. Par irréductibilité, P est de la forme $\lambda(X - a)$ avec $\lambda \in \mathbb{K}$. □

✌ **Remarque XIV.19.** La décomposition apparaissant dans le théorème XIV.18 est donc unique car déterminée par les racines. Plus précisément, si $P \in \mathbb{C}[X]$, on a :

$$P = \mathrm{cd}(P) \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)} (X - \alpha)^{\mu_P(\alpha)} .$$

Proposition XIV.20. Soient $P, Q \in \mathbb{C}[X]$. Alors :

$$P|Q \iff \begin{cases} \mathrm{Rac}_{\mathbb{C}}(P) \subset \mathrm{Rac}_{\mathbb{C}}(Q) \\ \forall \alpha \in \mathbb{C},\ \mu_P(\alpha) \leq \mu_Q(\alpha) \end{cases} .$$

Démonstration. Ceci découle de la décomposition énoncée **supra**. □

➠ **Exemple XIV.16.** Comparer les racines de $X^2 + X + 1$ et $(X^3 - 1)^2$.

✌ **Remarque XIV.20.** Ceci entraîne que si $P, Q \in \mathbb{C}[X] \setminus \{0\}$ on a :

$$P \wedge Q = \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \cap \mathrm{Rac}_{\mathbb{C}}(Q)} (X - \alpha)^{\min(\mu_P(\alpha), \mu_Q(\alpha))}$$

et

$$P \vee Q = \prod_{\alpha \in \mathrm{Rac}_{\mathbb{C}}(P) \cup \mathrm{Rac}_{\mathbb{C}}(Q)} (X - \alpha)^{\max(\mu_P(\alpha), \mu_Q(\alpha))} .$$

Corollaire XIV.20.a. Deux polynômes de $\mathbb{C}[X]$ non constants sont premiers entre eux si et seulement si ils n'ont pas de racine commune.

c) C'est qui (retour au(x) réel(s)) ?

Les choses se compliquent : il est temps de dégainer les lemmes ...

Lemme XIV.1. Soit $P \in \mathbb{R}[X]$. Alors, pour tout $\alpha \in \mathbb{C}$:

$$(\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)) \Rightarrow (\overline{\alpha} \in \mathrm{Rac}_{\mathbb{C}}(P)) .$$

Démonstration. Si $P = \sum_{k=0}^{d} a_k X^k$, on a :

$$\begin{aligned} 0 &= \overline{P(\alpha)} \\ &= \overline{\sum_{k=0} a_k \alpha^k} \\ &= \sum_{k=0} a_k \overline{\alpha}^k \\ &= P(\overline{\alpha}) \end{aligned}$$

d'où le résultat. □

Lemme XIV.2. Soit $P \in \mathbb{R}[X]$ de degré supérieur ou égal à 3. Alors P est réductible sur $\mathbb{R}$.

Démonstration. Si P admet une racine réelle, Bob's your uncle. Sinon, d'après le théorème de d'Alembert Gauss (XIV.19), il existe $\alpha \in \mathrm{Rac}_{\mathbb{C}}(P)$ (avec $\alpha \notin \mathbb{R}$) et $\overline{\alpha}$ est également une racine de P (distincte de α). De fait, il existe $Q \in \mathbb{C}[X]$ tel que :

$$P = (X-\alpha)(X-\overline{\alpha})Q\,.$$

Or $(X-\alpha)(X-\overline{\alpha}) = X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2 \in \mathbb{R}[X]$ donc, par unicité dans la division euclidienne (théorème XIV.7), $Q \in \mathbb{R}[X]$. Ce polynôme est de plus non constant car $\deg(P) \geq 3$, d'où le résultat. □

Théorème XIV.21.
Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant négatif.

Démonstration. Les polynômes cités sont clairement irréductibles. Réciproquement, si P est irréductible de degré 2, son discriminant est négatif (sans quoi il admet des racines réelles et donc une factorisation). Le cas du degré 3 et supérieur a été traité dans le lemme précédent. □

✌ **Remarque XIV.21.** La décomposition apparaissant dans le théorème XIV.18 est unique : cela découle du fait que la décomposition complexe est unique. On a de plus la formule suivante, pour tout $P \in \mathbb{R}[X]$:

$$P = \mathrm{cd}(P) \prod_{\alpha \in \mathrm{Rac}_{\mathbb{R}}(P)} (X-\alpha)^{\mu_P(\alpha)} \prod_{\substack{\beta \in \mathrm{Rac}_{\mathbb{C}}(P) \setminus \mathrm{Rac}_{\mathbb{R}}(P) \\ \text{tel que } \mathrm{Im}(\beta)>0}} (X^2 - 2\mathrm{Re}(\beta)X + |\beta|^2)^{\mu_P(\beta)}\,,$$

la condition sur $\mathrm{Im}(\beta)$ nous permettant de nous assurer qu'aucune racine complexe ne soit comptée "en double". Notons que ceci entraîne que deux racines complexes conjuguées d'un polynôme à coefficients réels sont de même multiplicité.

➠ **Exemple XIV.17.**

$$\begin{aligned} X^4 - 1 &= (X-1)(X+1)(X-i)(X+i) \\ &= (X-1)(X+1)(X^2+1)\,. \end{aligned}$$

6.⁻ Interpolation de Lagrange

Dans ce paragraphe, nous nous intéressons à la question suivante : étant donné $(x_0, y_0), \dots, (x_n, y_n) \in \mathbb{K}^2$, comment trouver un polynôme $P \in \mathbb{K}[X]$ tel que :

$$\forall k \in [\![0, n]\!],\ P(x_k) = y_k\ ? \qquad (\textbf{E} :\text{XIV.1})$$

Pour $n = 0$, le polynôme constant égal à y_0 fera l'affaire. Pour $n = 1$, nous avons deux points à relier ; une droite (et donc un polynôme de degré 1) conviendra. Dans ces deux cas, la solution au problème semble unique.

Proposition XIV.22. Soit $n \geq 0$ et soient $x_0, \dots x_n \in \mathbb{K}$ deux à deux distincts. Alors, pour toute famille $y_0, \dots, y_n \in \mathbb{K}$, il existe un unique polynôme $P \in \mathbb{K}_n[X]$ tel que :

$$\forall k \in [\![0, n]\!],\ P(x_k) = y_k\ .$$

Démonstration. **Unicité.** Si deux tels polynômes existent, leur différence admet $n + 1$ racines (les x_k) et est donc nulle par argument de degré.

Existence. Posons, pour $k \in [\![0, n]\!]$:

$$L_k = \prod_{j \neq k} \frac{(X - x_j)}{(x_k - x_j)}\ .$$

On a alors l'égalité $L_k(x_j) = \delta_{k,j}$ pour tous $k, j \in [\![0, n]\!]$ et donc

$$P = \sum_{k=0}^{n} y_k L_k$$

convient.

□

✌ **Remarque XIV.22.** L'unicité n'est plus garantie si la condition de degré est supprimée ; il existe même une infinité de solutions possibles à l'équation **E** :XIV.1.

➠ **Exemple XIV.18.** $X+1$ interpole les couples $(0, 1)$ et $(1, 2)$. Mais $(X+1)+X(X-1)$ aussi ...

✌ **Remarque XIV.23.** Tout ceci se code très bien en `python`. Une instabilité numérique est présente si n est très grand, car le polynôme "cherche" toujours à s'annuler autant de fois que son degré. La fonction suivante prend en argument les listes `X` et `Y` contenant respectivement les x_k et les y_k.

```
def lagrange(X,Y,a):
    def L(k,X,a):
        p=1
        for i in range(len(X)):
            if i != k:
                p*=(a-X[i])/(X[k]-X[i])
        return p
```

```
    if len(X) != len(Y):
        raise ValueError("Tailles␣incompatibles")
    n = len(X)
    res=0
    for k in range(n):
        res+=Y[k]*L(k,X,a)
    return res
```