Polynômes

Université Claude Bernard Lyon 1
L1 - parcours PMI de Mathématiques : Algèbre II
Année 2013–2014

Motivations :
- insuffisance des fonctions polynômiales sur certains corps, tel $\mathbb{Z}/2\mathbb{Z}$ où les fonctions $x \mapsto x^2+x^4$ et $x \mapsto x^3+x^8$ coïncident alors qu'on voudrait distinguer les « expressions » ;
- on verra plus tard, avec les matrices, des expressions de la forme $a_0\mathrm{Id} + a_1A + a_2A^2 + \cdots$, où A est une matrice carrée (*cf.* cours de L2) ;
- le calcul de primitives comme $\int \frac{3x+1}{(x^2+1)^3x^4(x^2-1)}\mathrm{d}x$ demande des méthodes algébriques.

I Anneaux

1° Anneaux unitaires

(a) Définition

On appelle *anneau* la donnée d'un ensemble A muni de deux opérations, la somme $+ : A\times A \to A$, $(a,b) \mapsto a+b$ et le produit $\cdot : A \times A \to A$, $(a,b) \mapsto ab$, telles que pour a, b, c quelconques dans A, on ait :

(i) $a+(b+c) = (a+b)+c$;

(ii) il existe un élément neutre pour la somme, noté 0, tel que $a+0 = a = 0+a$; cet élément est alors unique car si 0 et $0'$ conviennent, on a : $0 = 0+0' = 0'$;

(iii) tout élément possède un *opposé* : il existe a' tel que $a+a' = 0 = a'+a$; cet élément est alors unique, on le note $-a$;

(iv) l'addition soit commutative : $a+b = b+a$;

(v) la multiplication est *associative* : $a(bc) = (ab)c$;

(vi) le produit est distributif sur la somme : $a(b+c) = ab+ac$ et $(b+c)a = ba+ca$.

On dit que l'anneau A est

1. *unitaire* s'il existe un neutre pour le produit, noté 1, tel que $a1 = a = 1a$;
2. *commutatif* si le produit est commutatif : $ab = ba$ pour tous les éléments a, b de A.

Sauf mention explicite du contraire, un *anneau* est un *anneau commutatif unitaire*.
Exemples : $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$.
Exemples de calculs :
- pour tout élément a de A, on a : $0a = 0$; on dit que 0 est *absorbant* ; en effet, $0+0 = 0$ donne, par distributivité : $0a+0a = 0a$, d'où on tire en ajoutant l'opposé de $0a$ à chaque membre : $0a = 0$;
- pour tout a de A, on a : $(-1)a = -a$; en effet, $a+(-1)a = (1+(-1))a = 0a = 0$.

On définit les puissances d'un élément a dans un anneau unitaire A par récurrence en posant :

$$a^0 = 1, \quad a^1 = a, \quad \forall n \in \mathbb{N},\ a^{n+1} = aa^n.$$

Si A n'a pas d'unité, on peut quand même définir a^n pour $n \geq 1$.

(b) Morphisme d'anneau

Soient A et B deux anneaux. On appelle *morphisme* de A dans B une application $\varphi : A \to B$ telle que pour tous a, a' de A, on ait :

(i) $\varphi(a+a') = \varphi(a)+\varphi(a')$;

(ii) $\varphi(aa') = \varphi(a)\varphi(a')$;

(iii) si A et B ont unitaires, on demande que $\varphi(1) = 1$.

On a toujours : $\varphi(0) = 0$ car $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$.

(c) Formule du binôme de Newton

Soient a et b deux éléments d'un anneau unitaire A. On ne suppose pas que A est commutatif, mais [1] on suppose que $ab = ba$. Alors, pour $n \in \mathbb{N}$, on a :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

La démonstration se fait par récurrence de la même façon qu'avec les réels ou les complexes.

(d) Une factorisation à connaître

Soient a et b deux éléments d'un anneau unitaire A. On ne suppose pas que A est commutatif, mais [2] on suppose que $ab = ba$. Alors, pour $n \in \mathbb{N}^*$, on a :

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

On peut démontrer cette formule en développant le membre de droite et en faisant un changement de variable.

2° Arithmétique dans $\mathbb{Z}$

(a) Division euclidienne

Théorème. *Soit a et b deux entiers, b non nul. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases}$$

(b) PGCD, etc.

Soient a et b deux entiers. On dit que a divise b et on note $a|b$ s'il existe k entier tel que $b = ak$. Par exemple, $a|0$ pour tout a (prendre $k = 0$), $1|b$ pour tout b et $b|b$ (prendre $k = b$ ou $k = 1$).
Soient a et b deux entiers. On appelle PGCD de a et b un entier d qui divise a et b et tel que si e divise a et b, alors e divise d :

$$\begin{cases} d|a \text{ et } d|b \\ e|a \text{ et } e|b \implies e|d. \end{cases}$$

L'existence d'un PGCD ne résulte pas de la définition. En revanche, on voit facilement que si d et d' sont deux PGCD de a et b, alors $d' = \pm d$. On peut éventuellement parler « du » PGCD comme étant, s'il existe, le positif des deux.
L'algorithme d'Euclide assure l'existence d'un PGCD.
Relation de Bézout : si d est un PGCD de a et b, il existe u et v entiers tels que

$$au + bv = d.$$

On dit que a et b sont premiers entre eux si leur PGCD est 1 (ou -1). On note alors : $a \wedge b = 1$.
Par la relation de Bézout, il existe u et v tels que $au + bv = 1$. On a alors une réciproque : s'il existe u et v tels que $au + bv = 1$, alors a et b sont premiers entre eux.
Lemme de Gauss : si $a|bc$ et $a \wedge b = 1$, alors $a|c$.

1. Cela paraît artificiel mais c'est utile en pratique, par exemple, dans le cadre des matrices, quand on a deux matrices qui commutent.
2. Même remarque que ci-dessus...

3° Inversibilité

(a) Élément inversible

Un élément *inversible* dans un anneau unitaire A est un élément a pour lequel il existe un élément a' tel que $aa' = a'a = 1$. Alors, a' est unique (vérifier) : on le note a^{-1} ou, dans un contexte commutatif, $\frac{1}{a}$, et on l'appelle *inverse* de a.
Par exemple, pour $A = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, tout élément non nul est inversible. En revanche, un entier $n \in \mathbb{Z}$ est inversible si et seulement si il vaut -1 ou 1. Le neutre de l'addition 0 n'est jamais inversible [3].

(b) Corps

On appelle *corps* un anneau commutatif unitaire dans lequel tout élément non nul est inversible (et dans lequel $0 \neq 1$).
Exemples : $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ (avec les opérations $0 + 0 = 0 = 1 + 1$, $0 + 1 = 1 = 1 + 0$, $0 \times 1 = 0 \times 0 = 1 \times 0 = 0$, $1 \times 1 = 1$) sont des corps ; $\mathbb{Z}$ n'en est pas un.

Désormais, on fixe un corps $\mathbb{K}$.

II Anneaux de polynômes

1° Construction de l'anneau des polynômes

(a) Définition

Je copie la définition dans le poly. de Pierre Lavaurs. On dit qu'un anneau A est un anneau de polynômes sur $\mathbb{K}$ si :

1. A contient $\mathbb{K}$ (ou mieux : il existe un morphisme injectif de $\mathbb{K}$ dans A) ;
2. il existe X dans A (*indéterminée*) tel que pour tout élément P de A différent de 0, il existe $d \in \mathbb{N}$ unique et $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ unique avec $P = \sum_{k=0}^{d} a_k X^k$ et $a_d \neq 0$.

Proposition. *Il existe un anneau de polynômes sur $\mathbb{K}$. Si A et A' en sont deux et si X et X' sont les indéterminées respectives, il existe un morphisme bijectif d'anneaux $\varphi : A \to A'$ tel que $\varphi(a) = a$ lorsque $a \in \mathbb{K}$ et $\varphi(X) = X'$ (et donc $\varphi(\sum_{k=0}^{d} a_k X^k) = \sum_{k=0}^{d} a_k (X')^k$ où...).*

Sens : « Ça » existe et « c »'est unique (à isomorphisme près).

Notation. L'anneau des polynômes est noté $\mathbb{K}[X]$. Les éléments de $\mathbb{K}[X]$ sont 0 et les expressions $\sum_{k=0}^{d} a_k X^k$ avec $d \in \mathbb{N}$, $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ et $a_d \neq 0$. Si on n'insiste pas sur l'unicité, on peut ajouter des termes en posant $a_k = 0$ et écrire tout élément sous la forme $\sum_{k=0}^{n} a_k X^k$ avec $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$.

On va démontrer la proposition ci-dessus, la partie délicate étant l'existence.

(b) Construction

On définit A comme l'ensemble des suites presque nulles de scalaires. Ici, on dit qu'une suite $(a_n)_{n\in\mathbb{N}}$ à valeurs dans $\mathbb{K}$ est *presque nulle* si elle est nulle à partir d'un certain rang, c'est-à-dire si :

$$\exists N \in \mathbb{N},\ \forall n > N, \quad a_n = 0.$$

La somme de deux suites $P = (a_n)$ et $Q = (b_n)$ est définie comme on imagine : $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$. Comme $a_n = 0$ et $b_n = 0$ si n est supérieur à un entier N convenable, la somme est presque nulle.
Le produit, lui, demande plus de soin. On définit PQ comme la suite $(c_n)_{n\in\mathbb{N}}$ définie par :

$$\forall n \in \mathbb{N}, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

3. Sauf dans le cas trivial où $0 = 1$. On retiendra que même Chuck Norris ne peut pas diviser par zéro.

Si a_n et b_n sont nuls pour $n > N$, alors $c_n = 0$ pour $n > N$. En effet, si k est compris entre 0 et $n > N$, alors $k > N$ ou $n - k > N$. Le produit PQ est bien une suite presque nulle.
(c) Montrons que ces opérations font de A un anneau. En fait, on va se contenter de faire le minimum, c'est-à-dire préciser qui sont les éléments neutres et l'opposé... Le neutre de l'addition est la suite nulle $0 = (0)_{n\in\mathbb{N}}$.
Le neutre de la multiplication est la suite $1 = (1, 0, \dots)$, c'est-à-dire la suite $(u_n)_{n\in\mathbb{N}}$ telle que $u_0 = 1$ et $u_n = 0$ si $n \geq 1$. En calculant $P1$, le seul terme non nul de c_n est le terme correspondant à $k = n$ (de sorte que $b_{n-k} = b_0 = 1$), ce qui donne : $c_n = a_n$, et ce pour tout n. D'où : $P1 = P$.
L'associativité du produit et la distributivité demandent plein d'indices, on passe.
(d) On identifie une indéterminée. Soit

$$X = (0, 1, 0, \dots) = (x_n)_{n\in\mathbb{N}} \quad \text{où } x_0 = 0,\ x_1 = 1,\ \forall n \geq 2,\ x_n = 0.$$

On calcule : $X^2 = (0, 0, 1, 0, \dots)$, et on montre par récurrence que l'on a pour tout $n \in \mathbb{N}$:

$$X^n = (0, \dots, 0, 1, 0, \dots) \quad \text{(le 1 est en } (n+1)^{\text{e}} \text{ position.)}$$

De cette expression, il résulte que si $P = (a_n)_{n\in\mathbb{N}}$, on peut en fait écrire :

$$P = \sum_{n\geq 0} a_n X^n,$$

où la somme est finie car il n'y a qu'un nombre fini de coefficients a_n non nuls.
On en déduit immédiatement que si $\sum_{n\geq 0} a_n X^n = 0$, alors $a_n = 0$ pour tout n. Cela entraîne l'unicité de l'écriture de P comme expression de la forme $\sum_{n\geq 0} a_n X^n$.
Au bilan, on a montré que A est un anneau de polynômes. On le note $\mathbb{K}[X]$.
(e) Pour l'unicité à isomorphisme près, on se donne un autre anneau de polynômes A'. Tout élément non nul P de A' s'écrit de façon unique sous forme $\sum_{n\geq 0} a_n X'^n$: il s'agit de montrer que l'application qui à $P \in A'$ associe le polynôme $\sum_{n\geq 0} a_n X^n \in \mathbb{K}[X]$, qui est bien définie et bijective par définition de ce qu'est un anneau de polynômes, est un morphisme d'anneaux : c'est un calcul trivial (malgré les apparences ?).

2° Expression des opérations

Coefficients de la somme et du produit. À peu près inutile si on a lu le paragraphe précédent.

3° Degré et valuation

(a) Définition. Soit P un polynôme non nul. Il posède une unique écriture de la forme $\sum_{k=0}^{d} a_d X^d$ avec $d \in \mathbb{N}$ et $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$ et $a_d \neq 0$. On appelle *degré* de P et on note $\deg(P)$ ou $\mathrm{d}^{\mathrm{o}}P$ l'entier d. On appelle *terme dominant* le monôme $a_d X^d$ et *coefficient dominant* le scalaire a_d. On dit que P est *normalisé* ou *unitaire* si son coefficient dominant vaut 1.
On appelle valuation de P et on note $\mathrm{val}(P)$ le plus indice d'un coefficient non nul de P, c'est-à-dire : $\mathrm{val}(P) = \min\{k \in \mathbb{N},\ a_k \neq 0\}$.
Si P est le polynôme nul, on convient que sont degré est $-\infty$ et sa valuation est $+\infty$.
(b) Degré et opérations
On étend légèrement la somme et le maximum de $\mathbb{N}$ à $\mathbb{N}\cup\{-\infty\}$ et à $\mathbb{N}\cup\{+\infty\}$ (on n'ajoute pas les deux infinis à la fois) en définissant : $k + (-\infty) = -\infty$ et $\max(k, -\infty) = k$ si $k \in \mathbb{N}\cup\{-\infty\}$, de même avec $+\infty$. On a alors, pour P et Q polynômes quelconques :

$$\begin{cases} \deg(P+Q) \leq \max(\deg P, \deg Q) \\ \deg(PQ) = \deg P + \deg Q \end{cases} \qquad \begin{cases} \mathrm{val}(P+Q) \geq \min(\mathrm{val}P, \mathrm{val}Q) \\ \mathrm{val}(PQ) = \mathrm{val}P + \mathrm{val}Q. \end{cases}$$

Démonstration. Soient $d = \deg P$, $e = \deg Q$, on note $P = \sum_{k=0}^{d} a_k X^k$ et $Q = \sum_{\ell=0}^{e} b_k X^\ell$. On pose enfin $a_k = 0$ si $k > d$ et $b_\ell = 0$ si $\ell > e$, de sorte que $P = \sum_{k\geq 0} a_k X^k$ et $Q = \sum_{\ell\geq 0} b_k X^\ell$. On a : $P + Q = \sum_{k\geq 0}(a_k + b_k)X^k$, et l'on a : $a_k + b_k = 0$ si $k > d$ et $k > e$. Cela donne la majoration : $\deg(P + Q) \leq \max(d, e)$.
On calcule aussi (ou bien on se rappelle la définition en termes de suites presque nulles) :

$$PQ = \sum_{k\geq 0}\sum_{\ell\geq 0} a_k b_\ell X^k X^\ell = \sum_{m\geq 0}\sum_{k=0}^{m} a_k b_{m-k} X^m;$$

malgré les apparences, ces sommes sont des sommes *finies* ; pour passer de la première à la deuxième, on a regroupé ensemble les termes correspondant à une même puissance de X ; autrement dit, on a fait le changement de variable $(m, k) = (k + \ell, k)$ qui envoie bijectivement un couple $(k, \ell) \in \mathbb{N} \times \mathbb{N}$ sur le couple $(k + \ell, k) \in \big\{(m, k) \in \mathbb{N}^2,\ k \leq m\big\}$.
Soit $m \geq d + e + 1$. Pour $k \in \{0, \ldots, m\}$, on a : $k \geq d + 1$ ou $m - k \geq e + 1$ (car $k \leq d$ et $m - k \leq e$ entraînent $m = k + m - k \leq d + e$). Par suite, $a_k = 0$ ou $b_{m-k} = 0$, de sorte que $a_k b_{m-k} = 0$. Ainsi, le coefficient de X^m est nul.
Soit $m = d + e$. Pour $k > d$, on a : $a_k = 0$; pour $k < d$, on a : $m - k = e + d - k < e$ donc $b_{m-k} = 0$. Il vient : $\sum_{k=0}^{d+e} a_k b_{m-k} = a_d b_e$, qui n'est pas nul puisque $a_d \neq 0$ et $b_e \neq 0$ et $\mathbb{K}$ est un corps. Cela prouve que le degré de PQ est $d + e$.

Remarque. Un polynôme est de degré ≥ 0 si et seulement s'il n'est pas nul.

(c) Intégrité de $\mathbb{K}[X]$

Proposition. *Un produit de polynômes est nul SSI l'un des facteurs est nul.*

Démonstration. On sait que si l'un des facteurs est nul, le produit est nul. Réciproquement, si les deux polynômes ne sont pas nuls, le produit a pour degré la somme des degrés, qui est un entier, de sorte que le produit n'est pas nul.

(d) Inversibles de $\mathbb{K}[X]$

Proposition. *Les polynômes inversibles dans $\mathbb{K}[X]$ sont les polynômes de degré 0 – les constantes non nulles.*

Démonstration. Si P est un polynôme de degré 0, c'est-à-dire un polynôme constant non nul $a_0 \in \mathbb{K}^*$, alors P est inversible et son inverse est le polynôme constant $1/a_0$. Réciproquement, si P est inversible, alors il existe un polynôme Q tel que $PQ = 1$. Mais alors, on a : $\deg(P) + \deg(Q) = \deg(1) = 0$, si bien que $\deg(P)$ et $\deg(Q)$ sont nécessairement des entiers, donc ils valent nécessairement 0.

4° Évaluation

(a) Définition de l'évaluation d'un polynôme $P \in \mathbb{K}[X]$ en un élément α de A, où A est un anneau contenant $\mathbb{K}$: c'est

$$P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k \quad \text{si } P = \sum_{k=0}^{d} a_k X^k \ (d \in \mathbb{N},\ a_0, \ldots, a_d \in \mathbb{K}).$$

Exemple : si $A = \mathbb{K}$, l'évaluation permet de définir une *fonction polynomiale* associée au polynôme P par :

$$\tilde{P} : \mathbb{K} \to \mathbb{K}, \quad a \mapsto P(a).$$

Sous-exemple troublant : prenons $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ et $P = X^2 + X$. Alors, pour $\alpha = 0$ et $\alpha = 1$, on a : $P(0) = P(1) = 0$, c'est-à-dire que $\tilde{P} = 0$. Pourtant, P n'est pas le polynôme nul...

Exemple : Prenons $A = \mathbb{K}[X]$ et $\alpha = Q$. Alors, $P(Q)$ est le polynôme obtenu en remplaçant X par $Q = Q(X)$ dans l'expression de $P = \sum_{k=0}^{n} a_k X^k$. On note souvent $P \circ Q$ ce polynôme, car la fonction polynômiale associée est $\tilde{P} \circ \tilde{Q}$.
Sous-exemple : $P = X^2 + 1$, $Q = X + 3$ dans $\mathbb{R}[X]$. Alors : $P(Q) = (X+3)^2 + 1 = X^2 + 6X + 1$. Attention à faire la différence avec $Q(P) = (X^2 + 1) + 3 = X^2 + 4$.

(b) Racine : une *racine* d'un polynôme P est un élément $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

III Arithmétique

Idée-clé : $\mathbb{K}[X]$ « se comporte comme » $\mathbb{Z}$.

1° Divisibilité

Définition. Soit A et B deux polynômes. On dit que B divise A et on note[4] $B|A$ s'il existe un polynôme Q tel que $A = BQ$.

Exemples. On a : $1|A$ pour tout A. On a : $B|0$ pour tout B. En particulier, on a : $0|0$, bien qu'on ne puisse pas calculer $0/0$.
Comme exercice, montrer que $X - \alpha$ divise un polynôme P si et seulement si α est une racine de P. Rechercher les diviseurs de $X^4 + 7$ dans $\mathbb{R}[X]$ et de $X^4 + 1$ dans $\mathbb{C}[X]$.

2° Division euclidienne

Théorème. *Soit $a, b \in \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < |b|$.*

Théorème. *Soit $A, B \in \mathbb{K}[X]$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.*

Définition. Dans les notations du théorème, Q est appelé le *quotient* et R le *reste* de la division euclidienne de A par B.

Exemple. Si B est de degré 0, c'est-à-dire que $B = \alpha \in \mathbb{K}^*$, la division s'écrit simplement : $A = \frac{1}{\alpha} A \cdot B + 0$, c'est-à-dire que $Q = A/\alpha$ et $R = 0$ (seul polynôme de degré $< \deg(B) = 0$).

Exemple. Étudions le cas où $B = X - x_0$. Pour cela, écrivons : $A = \sum_{k=0}^{d} a_k X^k$, où $d \in \mathbb{N}$ et $a_k \in \mathbb{K}$. On a :

$$A(X) = \sum_{k=0}^{d} a_k X^k - \sum_{k=0}^{d} a_k x_0^k + A(x_0) = (X - x_0) \sum_{k=1}^{d} a_k \sum_{j=0}^{k-1} X^j x_0^{k-j-1} + A(x_0).$$

Avec la formule de Taylor, on obtient la division par $(X - x_0)^m$ ($m \geq 1$). Posant $b_j = A^{(j)}(x_0)/j!$ pour $j \leq d$, il vient :

$$A = \sum_{j=0}^{d} b_j (X - x_0)^j = (X - x_0)^m \sum_{j=m}^{d} b_j (X - x_0)^{j-m} + \sum_{i=0}^{m-1} b_i (X - x_0)^i,$$

où le deuxième terme est donc le reste.

Démonstration. Commençons par l'unicité. Si on peut écrire $A = BQ + R = BQ_1 + R_1$ avec $\deg(R) < \deg(B)$ et $\deg(R_1) < \deg(B)$, alors il vient : $B(Q - Q_1) = R_1 - R$. Le degré de ce polynôme est :

$$\deg(Q - Q_1) + \deg(B) = \deg(R_1 - R) \leq \max(\deg R_1, \deg R) < \deg B,$$

4. Attention : la barre est *verticale* pour faire la différence avec un quotient B/A – si $A = BQ$, on pourrait noter $Q = A/B$, mais A/B a un sens dans les fraction rationnelles même si B ne divise pas A

d'où : $\deg(Q-Q_1)=-\infty$, puis $Q=Q_1$ et $R=R_1$.
Pour l'existence, on fixe B et on fait une récurrence sur le degré de A. On a traité en exemple ci-dessus le cas trivial où B est constant. On suppose donc que le degré de B vaut au moins 1. Pour $\deg(A)<\deg(B)$, la division est triviale : $Q=0$ et $R=A$ conviennent.
Soit $n\in\mathbb{N}$, on suppose que pour tout polynôme de degré strictement inférieur à n, on peut effectuer la division euclidienne. Soit A un polynôme de degré n : on peut l'écrire $A=a_nX^n+A_1$, où $a_n\in\mathbb{K}^*$ et A_1 est un polynôme de degré au plus $n-1$. On écrit d'autre part $B=b_dX^d+B_1$, où $d=\deg(B)$, $b_d\in\mathbb{K}^*$ et B_1 est un polynôme de degré au plus $d-1$. On pose

$$\tilde{A}=A-\frac{a_n}{b_d}X^{n-d}B=a_nX^n+A_1-\frac{a_n}{b_d}X^{n-d}(b_dX^d+B_1)=A_1-\frac{a_n}{b_d}X^{n-d}B_1.$$

Le degré de ce polynôme est majoré par $\deg(A_1)<n$ et par $n-d+\deg(B_1)<n$. Par hypothèse de récurrence, on peut trouver $\tilde{Q}$ et $\tilde{R}$ tels que $\tilde{A}=B\tilde{Q}+\tilde{R}$ et $\deg(\tilde{R})<\deg(B)$. Alors, en posant $Q=\frac{a_n}{b_d}X^{n-d}+\tilde{Q}$ et $R=\tilde{R}$, on a bien : $A=BQ+R$ et $\deg(R)<\deg(B)$.

3° PGCD (non exigible)

(a) PGCD de deux polynômes

Définition. Soit deux polynômes A et B. On dit qu'un polynôme D est un PGCD de A et B si D est un diviseur commun ($D|A$ et $D|B$) et si, pour tout diviseur commun E, on a : $E|D$.

Remarque. L'existence d'un PGCD n'est pas garantie par la définition. Néanmoins, l'algorithme d'Euclide donne une preuve d'existence et un moyen de calcul.
Du côté de l'unicité, si D_1 et D_2 sont deux PGCD de A et B, alors $D_1|D_2$ car D_2 est un diviseur commun et D_1 est un PGCD et, inversement, $D_2|D_1$. Par suite, $D_1=\alpha D_2$ pour $\alpha\in\mathbb{K}^*$ convenable. Ainsi, le PGCD est unique à un scalaire (non nul) près.

Notation (ambiguë, à cause du coefficient α de la remarque précédente). $A\wedge B=D$ ou $(A,B)=D$. Si on veut lever l'ambiguïté, on dit que *le* PPGCD est le polynôme unitaire (s'il existe).

(b) Algorithme d'Euclide

Soient $A,B\in\mathbb{K}[X]$, $B\neq 0$. On construit une suite $(R_i)_{i\in\mathbb{N}}$ par récurrence :
- on pose $R_0=A$ et $R_1=B$;
- soit $i\in\mathbb{N}^*$, supposons avoir construit $R_0,\dots,R_i$:
  - si $R_i=0$, on pose $R_j=0$ pour $j\geq i$;
  - si $R_i\neq 0$, on définit R_{i+1} comme le reste de la division de R_{i-1} par R_i ; on note aussi Q_i le quotient, si bien que

$$R_{i-1}=Q_iR_i+R_{i+1}\quad\text{et}\quad\deg(R_{i+1})<\deg(R_i).$$

On vérifie par récurrence le *point-clé* : pour tout $i\geq 1$, $\deg(R_{i+1})\leq\deg(R_i)-1$. (Valable même si $R_i=0$.)
Par suite, on a pour tout $i\geq 1$: $\deg(R_i)\leq\deg(R_1)-i+1$, si bien que pour i assez grand, $\deg R_i<0$, c'est-à-dire que $R_i=0$. On note r l'unique entier tel que $R_r\neq 0$, $R_{r+1}=0$.
Affirmation : R_r est un PGCD de A et B.
En effet, notons $\mathcal{D}(P,Q)$ désigne l'ensemble des diviseurs communs à deux polynômes quelconques P et Q. On montre par récurrence finie que pour $0\leq i\leq r$, on a : $\mathcal{D}(A,B)=\mathcal{D}(R_i,R_{i+1})$. Pour $i=0$, il n'y a rien à démontrer. Soit $i\leq r-1$, on suppose que $\mathcal{D}(A,B)=\mathcal{D}(R_{i-1},R_i)$. On se rappelle que : $R_{i+1}=Q_iR_i+R_{i-1}$: si D divise R_i et R_{i-1}, alors D divise $Q_iR_i+R_{i-1}=R_{i+1}$. Inversement, si D divise R_i et R_{i+1}, alors D divise R_i et $Q_iR_i+R_{i+1}=R_{i-1}$. D'où : $\mathcal{D}(R_i,R_{i-1})=\mathcal{D}(R_i,R_{i+1})$, ce qui permet de conclure.
Pour $i=r$, on en déduit que $\mathcal{D}(A,B)=\mathcal{D}(R_r,0)$ et l'affirmation en découle.

Proposition (Euclide)**.** *Soit $A, B \in \mathbb{K}[X]$, $B \neq 0$. Dans la suite des restes (R_i) produite par l'algorithme d'Euclide, le dernier reste non nul est un PGCD de A et B.*

Remarque. Il peut arriver que l'on ait $\deg(A) < \deg(B)$: cela n'a pas d'importance ! Dans ce cas, la première division s'écrit : $A = 0B + A$, c'est-à-dire $Q_1 = 0$ et $R_2 = A$. En d'autres termes, la première division a pour effet de permuter A et B.

(c) Relation de Bézout

Proposition (Bézout)**.** *Soit $A, B \in \mathbb{K}[X]$ et D un PGCD de A et B. Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.*

Démonstration. On peut supposer $B \neq 0$, sinon c'est trivial ($D = \alpha A$ pour $\alpha \in \mathbb{K}^*$). On exhibe par récurrence finie sur $i \in \{0, \dots, r\}$ deux polynômes U_i, V_i tels que $R_i = AU_i + BV_i$.

Exemples. Déterminer le PGCD de $A = X - a$ et $B = X - b$ si a et b sont deux scalaires distincts. Trouver U et V tels que $AU + BV = 1$.
Dans $\mathbb{Z}$, calculer les coefficients de Bezout pour $a = 25$ et $b = 115$.

(d) Extension à plusieurs polynômes

Définition. Soit $m \in \mathbb{N}^*$ et $A_1, \dots, A_m \in \mathbb{K}[X]$. On dit que D est un *PGCD* de $A_1, \dots, A_m$ si $D|A_k$ pour tout k et si, dès que $E|A_k$ pour tout k, on a : $E|D$.

Proposition. *« Ça » existe et « c'est » unique à scalaire près.*

Idée de la preuve : Avec une récurrence sur m et des notations « évidentes », on a : $\operatorname{pgcd}(A_1, \dots, A_m) = \operatorname{pgcd}(A_1, \dots, A_{m-2}, \operatorname{pgcd}(A_{m-1}, A_m))$.

4° Polynômes premiers entre eux

(a) Définition de deux polynômes premiers entre eux (les seuls diviseurs communs à A et B sont les polynômes de degré 0 ; notation : $A \wedge B = 1$) ; d'une famille de polynômes premiers entre eux dans leur ensemble (les seuls diviseurs communs à tous les polynômes sont les constantes non nulles), premiers entre eux deux à deux (comme son nom l'indique).

Exemple. Les polynômes $(X-1)(X-2)$, $X(X-2)$ et $X(X-1)$ sont premiers entre eux dans leur ensemble mais pas deux à deux (vérifier).

(b) Relation de Bézout (bis, non exigible)

Proposition. *Soient $A, B \in \mathbb{K}[X]$. Alors $A \wedge B = 1$ SSI $\exists U, V,\ AU + BV = 1$.*

Exemple. Si $a, b \in \mathbb{K}$, $a \neq b$, $X - a$ et $X - b$ sont premiers entre eux (vérifier) et l'on a : $\frac{1}{a-b}(X-a) + \frac{1}{a-b}(X-b) = 1$.

(c) Lemme de Gauss (hors programme mais bien commode)

Proposition. *Soient $A, B, C \in \mathbb{K}[X]$. Si $A|BC$ et $A \wedge B = 1$, alors $A|C$.*

Exemple. Si $a \neq b$ dans $\mathbb{K}$, $A = (X-a)^m$, $B = (X-b)^n$, alors $A \wedge B = 1$. (Le lemme de Gauss est appliqué plusieur fois à $X - a$.)

Corollaire. *Soient $A_1, A_2, B \in \mathbb{K}[X]$. Si $A_1|B$ et $A_2|B$ et $A_1 \wedge A_2 = 1$, alors $A_1A_2|B$.*

Démonstration. Par hypothèse, on peut trouver Q tel que $B = A_1Q$. Comme $A_2|B$ et $A_2 \wedge A_1 = 1$, il vient : $A_2|Q$, d'où l'on déduit : $A_1A_2|B$.

Corollaire. *Un polynôme non nul de degré n possède au plus n racines distinctes.*

Démonstration. Soit A un polynôme ayant n racines distinctes $x_1, \dots, x_n$. Alors les polynômes $X - x_k$ $(1 \leq k \leq n)$ sont premier entre eux deux à deux. Par une utilisation répétée du corollaire précédent, on en déduit que le produit $\prod_{k=1}^{n}(X - x_k)$ divise A, de sorte que le degré de A est supérieur ou égal à n.

5° Polynômes irréductibles, factorisation (exigible)

(a) Polynômes irréductibles

Définition. On appelle *polynôme irréductible* tout polynôme non constant P dont les seuls diviseurs ont pour degré 0 ou $\deg(P)$. Cela signifie que P n'est divisible que par les constantes et les multiples de lui-même : si $D|P$, alors il existe $\alpha \in \mathbb{K}^*$ tel que $D = \alpha$ ou $D = \alpha P$.

On appellera *diviseur non trivial* d'un polynôme P un diviseur qui n'est pas de degré 0 ni $\deg(P)$.

Remarque. Lorsque P est irréductible et Q est quelconque, il est souvent commode d'utiliser l'alternative : $P \wedge Q = 1$ ou $P|Q$.

Exemples. Regardons en petit degré :
- en degré 0, pas d'irréductible ;
- en degré 1, tous les polynômes sont irréductibles ;
- sur $\mathbb{K}$ quelconque, en degré ≤ 2, P est irréductible SSI P n'a pas de racine ;
  en effet, P n'est pas irréductible SSI il a un diviseur non trivial SSI il a un diviseur de degré 1 SSI il existe $\alpha \in \mathbb{K}^*$ et $x_0 \in \mathbb{K}$ tel que $\alpha(X - x_0)$ divise P SSI il existe $x_0 \in \mathbb{K}$ tel que $P(x_0) = 0$;
- sur $\mathbb{C}$, en degré 2, il n'y a donc pas d'irréductible ;
- sur $\mathbb{R}$, en degré 2, un polynôme est irréductible SSI son discriminant est strictement négatif ;
- sur $\mathbb{K}$ quelconque, en degré 1, 2 ou 3, irréductible SSI pas de racine (exercice) ;
- sur $\mathbb{R}$, en degré 3, il n'y a pas d'irréductible par le théorème des valeurs intermédiaires ;
- en degré 4, un polynôme peut être réductible sans avoir de racines ; par exemple, dans $\mathbb{R}[X]$: $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.

(b) Irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème (D'Alembert-Gauss ou « fondamental de l'algèbre », admis)**.** *Tout polynôme complexe non constant admet une racine complexe.*

Corollaire. *Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 : $a(X-z)$, ($a \in \mathbb{C}^*$, $z \in \mathbb{C}$).*

Démonstration. Soit P un polynôme irréductible. Par le théorème de D'Alembert, P admet une racine z_0. Cela signifie que $X - z_0$ divise P. Par irréductibilité, on obtient que $P = \alpha(X - z_0)$ pour $\alpha \in \mathbb{C}^*$ convenable.

Corollaire. *Les irréductibles de $\mathbb{R}[X]$ sont :*
- *les polynômes de degré 1 : $a(X - x)$ ($a \in \mathbb{R}^*$, $x \in \mathbb{R}$),*
- *les polynômes de degré 2 qui n'ont pas de racine : aX^2+bX+c ($a, b, c \in \mathbb{R}$, $a \neq 0$, $b^2-4ac < 0$).*

Démonstration. Soit P un polynôme irréductible dans $\mathbb{R}[X]$. Un réel étant un complexe qui s'ignore, on peut considérer que P est un élément de $\mathbb{C}[X]$. Il a donc une racine dans $\mathbb{C}$, qu'on note z_0.
Premier cas : $z_0 \in \mathbb{R}$. Alors, on a : $P(z_0) = 0$ exprime que le polynôme réel $X - z_0$ divise P, qui est irréductible dans $\mathbb{R}[X]$: par suite, $P = \alpha(X - z_0)$ pour $\alpha \in \mathbb{R}^*$ convenable.
Deuxième cas : $z_0 \in \mathbb{C} \setminus \mathbb{R}$. Écrivons $P = \sum_{k=0}^{d} a_k X^k$, où $a_k \in \mathbb{R}$ pour tout k. Puisque $\overline{a_k} = a_k$ pour tout k, l'égalité $P(z_0) = 0$ donne, après un coup de barre :

$$0 = \overline{\sum_{k=0}^{d} a_k z_0^k} = \sum_{k=0}^{d} \overline{a_k}\,\overline{z_0}^k = \sum_{k=0}^{d} a_k \overline{z_0}^k = P(\overline{z_0}).$$

En d'autres termes, $\overline{z_0}$ est une racine de P, une autre que z_0 qui n'est pas réel. Mais alors, on a dans $\mathbb{C}[X]$: $(X-z_0)|P$, $(X-\overline{z_0})|P$ et $(X-z_0)\wedge(X-\overline{z_0})=1$, d'où : $(X-z_0)(X-\overline{z_0})|P$ (corollaire du lemme de Gauss). Constatons que : $B=(X-z_0)(X-\overline{z_0})=X^2-bX+c$ où $b=z_0+\overline{z_0}=2\,\mathrm{Re}(z_0)$ et $c=|z_0|^2$ sont deux réels. En d'autres termes, $B\in\mathbb{R}[X]$.
À présent, effectuons la division euclidienne de P par B dans $\mathbb{R}[X]$: on trouve Q et R dans $\mathbb{R}[X]$ tels que $P=BQ+R$ et $\deg(R)<2$. Mais on peut interpréter Q et R comme le quotient et le reste *dans* $\mathbb{C}[X]$! Et on sait que dans $\mathbb{C}[X]$, B divise P : par unicité de la division euclidienne dans $\mathbb{C}[X]$, on a : $R=0$. Ainsi, B divise P, mais à présent dans $\mathbb{R}[X]$. Par irréductibilité de P, on en déduit que $P=\alpha B$ pour $\alpha\in\mathbb{R}^*$ convenable, si bien que P est un polynôme de degré 2 sans racine réelle.

6° Factorisation

(a) Sur un corps quelconque

Théorème (factorisation (v. 0))**.** *Tout entier non nul se décompose comme produit de nombres premiers. Une telle décomposition est unique à l'ordre des facteurs et à des changements de signes près. (Ici, un nombre premier peut être positif ou négatif.)*

Théorème (factorisation (v. 1))**.** *Tout polynôme non nul se décompose comme produit de polynômes irréductibles. Une telle décomposition est unique à l'ordre des facteurs et à des produits par des constantes non nulles près.*

Théorème (factorisation (v. 2))**.** *Soit $A\in\mathbb{K}[X]$, A non nul.*

(i) *Il existe $\alpha\in\mathbb{K}$, $n\in\mathbb{N}$, $P_1,\dots,P_n$ irréductibles unitaires tels que $A=\alpha P_1\cdots P_n$.*

(ii) *Si, de plus, il existe $\beta\in\mathbb{K}^*$, $p\in\mathbb{N}$, $Q_1,\dots,Q_p$ irréductibles unitaires tels que $A=\beta Q_1\cdots Q_p$, alors $\alpha=\beta$, $n=p$ et il existe une bijection σ de $\{1,\dots,n\}$ dans lui-même et des constantes non nulles $\gamma_1,\dots,\gamma_n$ telles que $Q_k=\gamma_k P_{\sigma(k)}$ pour tout k.*

Esquisse de preuve : l'existence se prouve par récurrence (« forte ») sur le degré ; l'unicité par récurrence sur n, fondée sur le lemme de Gauss.
Démonstration. (i) On procède par récurrence sur le degré du polynôme. Si A est constant, on prend $\alpha=A$ et $n=0$. Si A est de degré 1, A est irréductible et on prend $\alpha=1$, $n=1$, $P_1=A$. Soit d un entier non nul. Supposons que tout polynôme de degré au plus d puisse s'écrire comme produit de polynômes irréductibles. Soit A un polynôme de degré $d+1$. Si A est irréductible, on prend $\alpha=1$, $n=1$ et $P_1=A$ et l'assertion est prouvée. Sinon, il existe deux polynômes non constants A_1 et A_2 tels que $A=A_1A_2$. Par hypothèse de récurrence, on peut trouver α_1, α_2, n_1, n_2, $P_1,\dots,P_{n_1},Q_1,\dots,Q_{n_2}$ irréductibles tels que $A_1=\alpha_1P_1\cdots P_{n_1}$ et $A_2=\alpha_2Q_1\cdots Q_{n_2}$. Alors, $A=\alpha_1\alpha_2P_1\cdots P_{n_1}Q_1\cdots Q_{n_2}$, ce qui prouve l'existence en prenant $\alpha=\alpha_1\alpha_2$, $n=n_1+n_2$, $P_{n_1+1}=Q_1,\dots,P_{n_1+n_2}=Q_{n_2}$.
(ii) On montre par récurrence sur n la propriété H_n : si un polynôme A possède une écriture avec au plus n facteurs irréductibles comme dans l'assertion (i), alors pour toute autre écriture $P=\beta Q_1\cdots Q_p$, on a $n=p$ et $Q_k=\gamma_kP_{\sigma(k)}$ pour tout k.
Pour $n=0$, A est un polynôme constant donc si $A=\beta Q_1\cdots Q_p$, nécessairement $p=0$, c'est-à-dire qu'il n'y a pas de polynôme dans le produit ; en effet, le degré d'un polynôme irréductible est strictement positif.
Supposons que $n=1$, $A=\alpha P_1$ est donc irréductible. Si $A=\beta Q_1\cdots Q_p$, alors, par le lemme de Gauss, P_1 divise l'un des Q_j (si P_1 ne divise par Q_1, alors $P_1\wedge Q_1=1$, si bien que P_1 divise $Q_2\cdots Q_p$, et ainsi de suite). Quitte à renuméroter, on peut supposer que P_1 divise Q_p ; comme Q_p est irréductible, $Q_p=\gamma_pP_1$ pour $\gamma_p\in\mathbb{K}^*$ convenable ; mais alors, $\alpha=\beta\gamma_pQ_1\cdots Q_{p-1}$:

par une considération de degré, on voit que $p = 1$, c'est-à-dire qu'il n'y a pas de polynômes $Q_1, \dots, Q_{p-1}$. Ceci prouve H_1 (en fait, cette étape n'est pas nécessaire...).
Soit $n \in \mathbb{N}^*$, on suppose la propriété H_{n-1} vraie. Soit A un polynôme qui peut s'écrire $A = \alpha P_1 \cdots P_n$ comme dans (i). Supposons qu'il ait une deuxième écriture du même type : $A = \beta Q_1 \cdots Q_p$. Le polynôme P_n divise A, donc il divise l'un des Q_j (en particulier, $p \geq 1$). Quitte à renuméroter, on peut supposer que c'est Q_p. Mais alors, comme Q_p est irréductible, il existe γ_p tel que $Q_p = \gamma_p P_n$. Mais alors, on obtient en simplifiant : $\alpha P_1 \cdots P_{n-1} = \beta\gamma_p Q_1 \cdots Q_{p-1}$. Par hypothèse de récurrence, $n - 1 = p - 1$ et les P_j coïncident avec les Q_j à une constante près (pour $j \leq n - 1$). On peut conclure.

Si on regroupe les polynômes irréductibles égaux entre eux, on obtient une autre formulation.

Théorème (factorisation (v. 3))**.** *Soit $A \in \mathbb{K}[X]$, A non nul. Il existe $\alpha \in \mathbb{K}^*$, $r \in \mathbb{N}$, $P_1, \dots, P_r$ irréductibles unitaires deux à deux distincts, $(m_1, \dots, m_r) \in (\mathbb{N}^*)^r$ tels que $A = \alpha P_1^{m_1} \cdots P_r^{m_r}$. Le scalaire α, l'entier r sont uniques et la famille des couples $\big((P_k, m_k)\big)_k$ est unique à l'ordre près.*

Remarque. Dans le théorème, on a : $m_k = \max\{j \in \mathbb{N},\ P_k^j | A\}$ pour tout k.

Pour la dernière formulation, on introduit l'ensemble $\mathcal{P}$ des polynômes irréductibles unitaires.

Théorème (factorisation (v. 4))**.** *Soit $A \in \mathbb{K}[X]$, A non nul. Il existe un unique scalaire $\alpha \in \mathbb{K}^*$ et une unique famille $(v_P(A))_{P\in\mathcal{P}}$ d'entiers naturels, tous nuls sauf un nombre fini d'entre eux, tels que $A = \alpha \prod_{P\in\mathcal{P}} P^{v_P(A)}$.*

(b) Factorisation et racines

Soit A un polynôme non nul. On appelle *multiplicité* d'un scalaire $z \in \mathbb{K}$ comme racine de A le plus grand entier $m \in \mathbb{N}$ tel que $(X - z)^m$ divise A. (Nécessairement, m est au plus égal au degré de A.) Par exemple, z est une racine de multiplicité 0 si et seulement si $A(z) \neq 0$, c'est-à-dire si z n'est pas une racine de A...
Soient $x_1, \dots, x_s$ les racines de A et $m_1, \dots, m_s$ leurs multiplicités respectives : le *nombre de racines* de A comptées avec multiplicités est $\sum_{k=1}^s m_k$.

Exemple. Le nombre de racines de $X^2 + 2X - 3$ est 2 (deux racines simples), de même que celui de $X^2 - 2X + 1$ (une racine double).

Proposition. *Le nombre de racines comptées avec multiplicités est au plus le degré. Autrement dit, un polynôme de degré d possède au plus d racines comptées avec multiplicité : $\sum_{k=1}^s m_k \leq d$.*

Définition. Un polynôme est scindé si le nombre de ses racines, comptées avec multiplicités, est égal à son degré.

Au cours de la preuve est apparue la formule : $A = \alpha \prod_{k=1}^s (X - x_k)^{m_k} \prod_{j=s+1}^r P_j^{m_j}$, où les P_j sont les facteurs irréductibles de A qui n'ont pas de racine.

Exemple. Pour $n \in \mathbb{N}^*$, on a dans $\mathbb{C}[X]$ l'égalité : $X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2i\pi k/n})$. (En déduire la somme des racines de l'unité.)

(c) Factorisation sur $\mathbb{C}$ et $\mathbb{R}$

Reformulation du théorème de factorisation.

IV Dérivation et applications

Dans cette partie, on suppose que $\mathbb{K}$ est inclus dans $\mathbb{C}$. La raison n'apparaîtra pas, il s'agit de s'assurer que tous les entiers sont différents de 0 dans $\mathbb{K}$ (alors que pour $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, on a par exemple $2 = 0$).

1° Définition de la dérivation

Soit P un polynôme, que l'on écrit $P = \sum_{k=0}^{d} a_k X^k$ avec $d \in \mathbb{N}$ et $(a_0, \dots, a_d) \in \mathbb{K}^{d+1}$. On définit le *polynôme dérivé* de P par :

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

On vérifie que si $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$, on a : $(P+Q)' = P' + Q'$ et $(\lambda P)' = \lambda P'$. On appellera *linéarité* cette propriété.

2° Formule de Leibniz

Proposition. *Soient P et Q dans $\mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors :*

(i) $(PQ)' = P'Q + PQ'$,

(ii) $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Démonstration. (i) Par linéarité de la dérivation, il suffit de montrer l'assertion pour $P = X^k$ et $Q = X^\ell$ (vérifier). Mais dans ce cas elle est immédiate : $(PQ)' = \left(X^{k+\ell}\right)' = (k+\ell)X^{k+\ell-1}$ et $P'Q + PQ' = kX^{k-1+\ell} + \ell X^{k+\ell-1}$.
(ii) Par récurrence sur n. Si la propriété est vraie pour un entier n donné, on a :

$$\begin{aligned}
(PQ)^{(n+1)} &= \left((PQ)^{(n)}\right)' = \left(\sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}\right)' = \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k)} Q^{(n-k)}\right)' \\
&= \sum_{k=0}^{n} \binom{n}{k} \left(P^{(k+1)} Q^{(n-k)} + P^{(k)} Q^{(n-k+1)}\right) \\
&= \sum_{\ell=1}^{n+1} \binom{n}{\ell-1} P^{(\ell)} Q^{(n+1-\ell)} + \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n+1-k)}
\end{aligned}$$

et l'on conclut avec : $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$.

3° Formule de Taylor

Proposition. *Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors :* $P = \sum_{k=0}^{\deg(P)} \frac{P^{(k)}(a)}{k!} (X-a)^k$.

Démonstration. Par linéarité, il suffit de prouver la formule pour $P = X^n$ (vérifier !). Et dans ce cas, elle est évidente si on remarque que $\left(X^n\right)^{(k)} = n(n-1)\cdots(n-k+1)X^{n-k}$ (ou 0 si $k > n$). En effet, on a alors :

$$\sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X-a)^k = \sum_{k=0}^{n} \frac{n(n-1)\cdots(n-k+1)}{k!} a^k (X-a)^k = \sum_{k=0}^{n} \binom{n}{k} a^k (X-a)^k = (X-a+a)^n.$$

4° Racine et dérivées

Proposition. *Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. Sont équivalentes :*

(i) $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$;

(ii) *il existe un polynôme Q tel que $P = (X-a)^m Q$.*

Démonstration. Si (i) est satisfaite, on déduit (ii) de la formule de Taylor (les k premiers termes de la somme sont nuls). Si (ii) est satisfaite, la formule de Leibniz permet de vérifier (i).