25 # Polynômes

1 L'anneau des polynômes. 2
- 1.1 Combinaisons linéaires, degré. . . . 2
- 1.2 Produit. . . . 4
- 1.3 Structure d'anneau de $\mathbb{K}[X]$. . . . 5
- 1.4 Évaluation. . . . 6
- 1.5 Composition. . . . 7
- 1.6 Dérivation. . . . 7

2 Arithmétique dans $\mathbb{K}[X]$. 9
- 2.1 Divisibilité et division euclidienne dans $\mathbb{K}[X]$. . . . 9
- 2.2 PGCD de deux polynômes (ou plus). . . . 10
- 2.3 PPCM de deux polynômes. . . . 12
- 2.4 Polynômes premiers entre eux. . . . 13

3 Racines et factorisation. 15
- 3.1 Racines et divisibilité. . . . 15
- 3.2 Racines et rigidité des polynômes. . . . 16
- 3.3 Multiplicité d'une racine. . . . 16
- 3.4 Existence de racines : théorème de d'Alembert-Gauss. . . . 18
- 3.5 Décomposition en facteurs irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$. . . . 19

4 Compléments. 21
- 4.1 Relations coefficients-racines pour un polynôme scindé. . . . 21
- 4.2 Interpolation de Lagrange. . . . 22

Preuves 24

Exercices 27

1 L'anneau des polynômes.

1.1 Combinaisons linéaires, degré.

Définition 1.

On appelle **polynôme** à coefficients dans $\mathbb{K}$ une suite d'éléments de $\mathbb{K}$ nulle à.p.d.c.r.

L'**ensemble des polynômes** à coefficients dans $\mathbb{K}$ sera noté $\mathbb{K}[X]$.

- La suite nulle est un polynôme. Il est appelé **polynôme nul** et noté 0, ou $0_{\mathbb{K}[X]}$.
- La suite $(1, 0, 0, 0, \ldots)$ est un polynôme. Il est appelé polynôme constant égal à 1 et noté 1.
- La suite $(0, 1, 0, 0, \ldots)$ est un polynôme. Il est noté X et appelé **indéterminée**.
- Soit $n \in \mathbb{N}$. La suite dont tous les termes sont nuls sauf celui au rang n qui vaut 1 est un polynôme que l'on notera X^n. On l'appelle **monôme** d'ordre n :

$$X^n = (0, 0, \ldots, 0, \underbrace{1}_{\text{rang } n}, 0, 0, \ldots).$$

Définition 2.

Soit $P = (a_k)_{k\in\mathbb{N}}$ un polynôme de $\mathbb{K}[X]$, non nul.
On appelle **degré** de P, et on note $\deg(P)$ l'indice du dernier coefficient non nul de P :

$$\deg(P) = \max\{k \in \mathbb{N} : a_k \neq 0\}.$$

Par ailleurs, on pose $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Pour $n \in \mathbb{N}$, on a $\deg(X^n) = n$.

Proposition-Définition 3 (Somme de polynômes et son degré).

Soient $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$.
On appelle somme de P et Q, notée $P + Q$ la suite $(a_k + b_k)_{k\in\mathbb{N}}$.
C'est un polynôme de $\mathbb{K}[X]$ et

$$\deg(P + Q) \leq \max(\deg(P), \deg(Q)), \text{ avec égalité si } \deg(P) \neq \deg(Q);$$

Proposition 4.

$(\mathbb{K}[X], +)$ est un groupe abélien. Plus précisément,

1. $+$ est une loi de composition interne sur $\mathbb{K}[X]$, associative et commutative ;
2. il existe un polynôme dans $\mathbb{K}[X]$ qui est neutre pour l'addition : c'est le polynôme nul $0_{\mathbb{K}[X]}$;
3. tout polynôme P de $\mathbb{K}[X]$ possède un symétrique $-P$ dans $K[X]$.
   Si $P = (a_k)$, le polynôme $-P$ est la suite $(-a_k)$ et on a $-P + P = P + (-P) = 0_{\mathbb{K}[X]}$.

Proposition-Définition 5 (Multiplication par un scalaire et son degré).

Soient $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.
On note $\lambda \cdot P$, ou encore λP la suite $(\lambda a_k)_{k\in\mathbb{N}}$.
C'est un polynôme de $\mathbb{K}[X]$ et

$$\deg(\lambda P) \leq \deg(P), \text{ avec égalité si } \lambda \neq 0.$$

Proposition 6 (Propriétés de la multiplication par un scalaire).

- $\forall P \in \mathbb{K}[X] \quad 1_{\mathbb{K}} \cdot P = P$;
- $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}[X]$:

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall \lambda \in \mathbb{K} \quad \lambda \cdot (P+Q) = \lambda \cdot P + \lambda \cdot Q;$$

- $\cdot$ est distributive par rapport à l'addition dans $\mathbb{K}$:

$$\forall P \in \mathbb{K}[X] \quad \forall \lambda, \mu \in \mathbb{K} \quad (\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P;$$

- $\forall \lambda, \mu \in \mathbb{K} \quad \forall P \in \mathbb{K}[X] \quad \lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P.$

Proposition-Définition 7.

Soit $n \in \mathbb{N}$.
On note $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$, de degré inférieur ou égal à n.
Un polynôme $P = (a_k)_{k\in\mathbb{N}}$ qui appartient à $\mathbb{K}_n[X]$ s'écrit

$$P = \sum_{k=0}^{n} a_k X^k.$$

On a en particulier

$\mathbb{K}_0[X] = \{a \cdot 1_{\mathbb{K}[X]} \mid a \in \mathbb{K}\}$ $\quad$ $\mathbb{K}_1[X] = \{aX + b \mid (a,b) \in \mathbb{K}^2\}$ $\quad$ $\mathbb{K}_2[X] = \{aX^2 + bX + c \mid (a,b,c) \in \mathbb{K}^3\}$

Définition 8.

Les polynômes de $\mathbb{K}_0[X]$ sont appelés **polynômes constants**.

Attention, un polynôme constant est de degré 0... ou $-\infty$ s'il est nul !

Proposition 9.

Soit $n \in \mathbb{N}$. L'ensemble $\mathbb{K}_n[X]$ est stable par combinaisons linéaires :

$$\forall (P,Q) \in (\mathbb{K}_n[X])^2 \quad \forall (\lambda,\mu) \in \mathbb{K}^2 \quad \lambda P + \mu Q \in \mathbb{K}_n[X].$$

Notation.

Un polynôme $P = (a_k)_{k\in\mathbb{N}}$ de $\mathbb{K}[X]$ sera désormais noté

$$P = \sum a_k X^k,$$

Remarque. Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$. Par définition, les polynômes P et Q sont égaux si et seulement si les suites P et Q sont égales. Cela permettra « d'identifier » le coefficient devant X^k. Ainsi,

$$\boxed{\sum a_k X^k = \sum b_k X^k \quad \iff \quad \forall k \in \mathbb{N} \;\; a_k = b_k.}$$

Proposition-Définition 10.

Soit P un polynôme de $\mathbb{K}[X]$ et $d \in \mathbb{N}$.

$$\deg(P) = d \quad \iff \quad \Big(\exists (\lambda, R) \in \mathbb{K} \times \mathbb{K}[X] \;\mid\; P = \lambda X^d + R,\; \lambda \neq 0 \;\text{ et }\; \deg(R) < d\Big).$$

Si P est non nul et de degré $d \in \mathbb{N}$, alors λ est appelé **coefficient dominant** de P.
On pourra noter ce coefficient $\mathrm{cd}(P)$. Si ce coefficient vaut 1, le polynôme P est dit **unitaire**.

1.2 Produit.

Proposition-Définition 11 (Produit de deux polynômes).

Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes de $\mathbb{K}[X]$.
Soit $(c_k)_{k\geq 0}$ la suite définie par

$$\forall k \in \mathbb{N} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

La suite c est un polynôme : on l'appelle **produit** de P et Q, noté $P \times Q$, ou encore PQ :

$$\left(\sum_{k\in\mathbb{N}} a_k X^k\right)\left(\sum_{k\in\mathbb{N}} b_k X^k\right) = \sum_{k\in\mathbb{N}} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) X^k.$$

Proposition 12 (Degré et coefficient dominant d'un produit).

$$\boxed{\forall (P, Q) \in (\mathbb{K}[X])^2 \quad \deg(P \times Q) = \deg(P) + \deg(Q)}$$

$$\forall (P, Q) \in (\mathbb{K}[X] \setminus \{0\})^2 \quad \mathrm{cd}(P \times Q) = \mathrm{cd}(P) \times \mathrm{cd}(Q).$$

Proposition 13 (la balade du scalaire).

$$\forall (P, Q) \in (\mathbb{K}[X])^2 \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \quad (\lambda P)Q = P(\lambda Q) = \lambda(PQ) \quad \text{ et } \quad (\lambda P)(\mu Q) = (\lambda\mu)PQ.$$

1.3 Structure d'anneau de $\mathbb{K}[X]$.

Théorème 14.

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

Proposition 15 (Cohérence de la notation X^n).

Pour tout $n \in \mathbb{N}$, le polynôme X^n est bien le $n$ème itéré de X.

La preuve des deux résultats ci-dessus est en annexe.

Proposition 16 (Propriétés de l'anneau des polynômes).

L'anneau $\mathbb{K}[X]$ est intègre : il est commutatif, et sans diviseurs de zéro :

$$\forall P, Q \in \mathbb{K}[X] \qquad PQ = 0 \implies (P = 0 \text{ ou } Q = 0)\,.$$

Ainsi pouvons nous « simplifier » par un polynôme non nul :

$$\forall A, B, C \in \mathbb{K}[X] \quad (AB = AC \text{ et } A \neq 0) \implies B = C.$$

Les inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non nuls :

$$U(\mathbb{K}[X]) = \mathbb{K}_0[X] \setminus \{0\}.$$

Comme dans tout anneau commutatif, il est possible d'écrire des identités remarquables dans $\mathbb{K}[X]$, notamment le binôme, ou la factorisation de $P^n - Q^n$ par $P - Q$.

Exemple 17.

À l'aide d'identités remarquables, factoriser

$$X^3 - 1; \qquad X^3 + 1; \qquad X^4 - 1; \qquad 1 + X^4 + X^8.$$

Exemple 18.

Soit $n \in \mathbb{N}^*$ et $P = (X+2)^n - (X+1)^n$. Calculer le degré de P et son coefficient dominant.

Exemple 19 (Formule de Vandermonde).

Soient $(p, q, n) \in \mathbb{N}^3$. En considérant $(X+1)^p (X+1)^q$, montrer que

$$\sum_{k=0}^{n} \binom{p}{k} \binom{q}{n-k} = \binom{p+q}{n}.$$

1.4 Évaluation.

Définition 20 (où l'on retrouve les fonctions polynomiales).

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$.
Pour $x \in \mathbb{K}$, on appelle **évaluation** de P en x, et on note $P(x)$ le nombre

$$P(x) = \sum_{k=0}^{+\infty} a_k x^k \qquad (P \in \mathbb{K}[X] \text{ et } P(x) \in \mathbb{K}).$$

La somme précédente est *finie* puisque la suite (a_n) est par définition nulle à.p.d.c.r.
On parlera de $\widetilde{P} : x \mapsto P(x)$ comme de la **fonction polynomiale associée** au polynôme P.

Exemples 21.

1. Soit $P = X^3 - 3X + 4$. Évaluer P en 2 et -1.
2. Quelle est la fonction polynomiale associée à $X^2 - 1$? à X ?
3. Quel coefficient du polynôme obtient-on lorsqu'on l'évalue en 0 ?

Proposition 22 (opérations et évaluation).

Soient $P, Q \in \mathbb{K}[X]$, $x \in \mathbb{K}$ et $(\lambda, \mu) \in \mathbb{K}^2$.

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

Exemple 23 (Polynômes de Tchebychev.).

Soit $(T_n)_{n\in\mathbb{N}}$ une suite de polynômes définie par

$$T_0 = 1, \qquad T_1 = X \qquad \forall n \in \mathbb{N} \;\; T_{n+2} = 2XT_{n+1} - T_n.$$

1. Calculer T_2, T_3, T_4 et T_5.
2. Donner pour tout entier n le degré et le coefficient dominant de T_n.
3. Démontrer que pour tout $n \in \mathbb{N}$, et tout $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$.

Définition 24.

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

Exemple 25.

Donner une racine réelle de $P = X^5 - X^4 + X^3 - X^2 + X - 1$.
Donner les racines de $X^5 - 1$ dans $\mathbb{C}$.

1.5 Composition.

Définition 26.

Soient deux polynômes $P = \sum a_k X^k$ et Q. Leur **composée** $P \circ Q$ est définie par

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

La somme ci-dessus a un nombre fini de termes non nuls, la suite $(a_k)_{k\in\mathbb{N}}$ étant nulle à.p.d.c.r.

Exemple : Calcul de $P \circ Q$ et $Q \circ P$ avec $P = 1 + X^2$ et $Q = 2 - X$.

Remarques.

1. On vérifiera que $X \circ P = P$ et que $P \circ X = P$. Cette dernière égalité explique que l'on écrit parfois $P(X)$ à la place de P. De la même façon, on écrira $P(X^2)$ ou $P(Q(X))$ pour désigner respectivement les polynômes $P \circ X^2$ et $P \circ Q$.
2. L'écriture $P(X + 1)$ peut alors prêter à confusion : s'agit-il de $P \circ (X + 1)$ ou de $P \times (X + 1)$? La bonne réponse, c'est la composition : pour le produit, on préfèrera l'écriture $(X + 1)P$.
3. Assez clairement, si P et Q sont deux polynômes de $\mathbb{K}[X]$ et $x \in \mathbb{K}$, on a $P \circ Q(x) = P\,(Q(x))$.

Proposition 27.

$$\forall P \in \mathbb{K}[X] \quad \forall Q \in \mathbb{K}[X] \setminus \mathbb{K}_0[X] \quad \deg(P \circ Q) = \deg(P) \times \deg(Q).$$

1.6 Dérivation.

Définition 28.

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$. Le polynôme

$$P' = \sum_{k\in\mathbb{N}} (k + 1)a_{k+1} X^k$$

est appelé **polynôme dérivé** de P.

Remarque. Pas besoin de parler de dérivabilité ci-dessus : la définition ci-dessus est une opération purement *formelle* qui à la suite (a_k) associe la suite $((k + 1)a_{k+1})$.

Proposition 29.

Si P est un polynôme de $\mathbb{R}[X]$, la fonction polynomiale associée au polynôme dérivé P' est la dérivée de la fonction polynomiale associée à P.

Proposition 30.

$$\forall P \in \mathbb{K}[X] \qquad P \text{ est constant} \iff P' = 0_{\mathbb{K}[X]}.$$

Proposition 31 (Degré du polynôme dérivé).

$$\forall P \in \mathbb{K}[X] \quad \deg(P') = \begin{cases} \deg(P)-1 & \text{si } P \text{ n'est pas constant,} \\ -\infty & \text{si } P \text{ est constant.} \end{cases}$$

Proposition 32 (Dérivation et opérations).

Pour tous $P, Q \in \mathbb{K}[X]$, pour tous scalaires $\lambda, \mu \in \mathbb{K}$,

$$(\lambda P + \mu Q)' = \lambda P' + \mu Q' \qquad \text{et} \qquad (PQ)' = P'Q + PQ'.$$

$$\forall n \in \mathbb{N} \quad (P^n)' = nP'P^{n-1} \qquad \text{et} \qquad (P \circ Q)' = Q' \cdot P' \circ Q.$$

On peut s'étonner qu'une preuve soit nécessaire : ces résultats sont bien connus pour les *fonctions*... Mais attention : ici, la dérivation est une opération définie directement sur les suites de coefficients : pas de taux d'accroissement ici. Une preuve est donnée en annexe, à base de calculs formels sur les coefficients.
On peut se demander si le fait qu'on connaisse ces identités pour les fonctions polynomiales peut nous aider à prouver que le résultat est vrai pour les objets algébriques. La réponse est oui (voir la notion de rigidité polynomiale à la fin du cours).

Définition 33.

Soit $P \in \mathbb{K}[X]$ et $k \in \mathbb{N}$. On définit la **dérivée k-eme** de P, que l'on note $P^{(k)}$, en posant

$$P^{(0)} = P \qquad \text{et} \qquad \forall k \geq 1 \quad P^{(k)} = \left(P^{(k-1)}\right)'.$$

Exemple 34.

$$\forall n, k \in \mathbb{N} \quad \forall a \in \mathbb{K} \quad ((X-a)^n)^{(k)} = \begin{cases} \dfrac{n!}{(n-k)!}(X-a)^{n-k} & \text{si } 0 \leq k \leq n \\ 0 & \text{si } k > n \end{cases}$$

Proposition 35 (Linéarité de la dérivée $n$ème et formule de Leibniz).

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall (\lambda, \mu) \in \mathbb{K}^2 \quad \forall n \in \mathbb{N} \quad (\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$$

$$\forall (P,Q) \in (\mathbb{K}[X])^2 \quad \forall n \in \mathbb{N} \quad (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Théorème 36 (Formule de Taylor pour les polynômes).

Soit $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $a \in \mathbb{K}$. Alors,

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

Corollaire 37 (coefficients du polynôme à l'aide des dérivées).

Soit $P = \sum a_k X^k$ un polynôme de $\mathbb{K}[X]$. Alors,

$$\forall k \in \mathbb{N} \quad a_k = \frac{P^{(k)}(0)}{k!}.$$

2 Arithmétique dans $\mathbb{K}[X]$.

2.1 Divisibilité et division euclidienne dans $\mathbb{K}[X]$.

Définition 38.

Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que B **divise** A s'il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B \mid A$.

Exemple 39.

Tous les polynômes divisent le polynôme nul.

Pour $n \in \mathbb{N}^*$, $X - 1$ divise $X^n - 1$ dans $\mathbb{R}[X]$: on a $X^n - 1 = (X-1)\sum_{k=0}^{n-1} X^k$.

Proposition 40.

Soient deux polynômes A et B de $\mathbb{K}[X]$, A étant non nul. Si B divise A, alors $\deg(B) \leq \deg(A)$.

Proposition-Définition 41.

La relation divise sur $\mathbb{K}[X]$ est réflexive et transitive, mais elle n'est *pas* antisymétrique.
En effet, pour A et B deux polynômes,

$$(A \mid B \text{ et } B \mid A) \iff \exists \lambda \in \mathbb{K}^* \ A = \lambda B.$$

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

Tout polynôme non nul P est associé à un unique polynôme unitaire : λP, où $\lambda = \mathrm{cd}(P)^{-1}$.

Théorème 42 (de division euclidienne).

Soit $(A, B) \in \mathbb{K}[X]^2$, avec $B \neq 0$. Il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

Exemple 43.

Poser la division de $A = X^5 + 3X^3 - 2X^2 + 1$ par $B = X^2 - 2X - 1$.
L'évaluation (en 1 ou -1 par exemple) permet parfois de détecter une éventuelle erreur de calcul.

Corollaire 44.

Soit $(A, B) \in \mathbb{K}[X]^2$, avec $B \neq 0$.
On a que B divise A ssi le reste dans la division euclidienne de A par B est le polynôme nul.

Exemple 45 (juste le reste).

Soit $\theta \in \mathbb{R}$ et $n \geq 2$.
Déterminer le reste dans la division euclidienne de $(\sin\theta X + \cos\theta)^n$ par $X^2 + 1$.
Prouver qu'il n'existe aucune valeur de θ ni de n pour lesquelles $X^2 + 1$ divise $(\sin\theta X + \cos\theta)^n$.

2.2 PGCD de deux polynômes (ou plus).

L'ensemble des diviseurs d'un polynôme A sera noté $\mathcal{D}(A)$. Cet ensemble contient tous les polynômes constants non nuls. De plus, si $A \neq 0_{\mathbb{K}[X]}$, tous les éléments de $\mathcal{D}(A)$ ont un degré majoré par $\deg(A)$.

Ainsi, dans le cas où l'un des polynômes A ou B est non nul, les polynômes de $\mathcal{D}(A) \cap \mathcal{D}(B)$ ont leur degré majoré par $\max(\deg(A), \deg(B))$, ce qui permet de donner du sens à la définition ci-dessous.

Définition 46.

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

- Si $(A, B) \neq (0, 0)$,
  - tout diviseur commun à A et B de degré maximal est appelé *un* **PGCD** de A et B ;
  - l'unique polynôme unitaire parmi eux est appelé **PGCD unitaire** et noté $A \wedge B$.
- Si $A = B = 0$, on pose $A \wedge B = 0$.

Proposition 47.

Deux PGCD d'un même couple de polynômes sont associés.

Théorème 48 (PGCD par une relation de Bézout).

Soient A et B deux polynômes de $\mathbb{K}[X]$. Il existe $(U,V) \in (\mathbb{K}[X])^2$ tel que

$$A \wedge B = AU + BV.$$

L'égalité ci-dessus est appelée une **relation de Bézout**.
Le couple (U,V) peut-être désigné comme un couple de *coefficients de Bézout*, il n'est pas unique.

Remarque. Lorsque l'un des deux polynômes A ou B est non nul, on comprend dans la preuve que le PGCD est le polynôme unitaire de degré minimal appartenant à l'ensemble

$$A\mathbb{K}[X] + b\mathbb{K}[X] = \left\{AU + BV \ : \ (U,V) \in (\mathbb{K}[X]^2\right\}.$$

Proposition 49 (Les diviser tous les deux, c'est diviser leur PGCD).

Soit $(A,B) \in (\mathbb{K}[X])^2$. Alors

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

Les diviseurs communs de A et B sont exactement les diviseurs du PGCD unitaire de A et B.
Le PGCD unitaire peut être remplacé ici par n'importe quel PGCD.

Proposition 50.

$$\forall (A,B) \in \mathbb{K}[X]^2, \quad \forall P \in \mathbb{K}[X] \text{ (unitaire)}, \quad \mathrm{PGCD}\,(PA,PB) = P \cdot \mathrm{PGCD}(A,B).$$

Proposition 51 (Réduction du problème).

Soit $(A,B,C,Q) \in (\mathbb{K}[X])^4$ tel que $A = BQ + C$.
Alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(C)$. En particulier, $A \wedge B = B \wedge C$.

Théorème 52 (Algorithme d'Euclide).

Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$.

- On note $R_0 = A$ et $R_1 = B$.
- Tant qu'il existe $i \in \mathbb{N}^*$ tel que R_i est non nul, on définit R_{i+1} comme le reste dans la division euclidienne de R_{i-1} par R_i.

Cet algorithme termine : il existe $p \in \mathbb{N}^*$ tel que $R_1, \ldots, R_p$ sont non nuls et $R_{p+1} = 0$. Alors,

$$\boxed{R_p \text{ est un PGCD de } A \text{ et } B}$$

Méthode (Algorithme d'Euclide étendu).

Comme dans $\mathbb{Z}$, la remontée des divisions euclidienne fournit des coefficients de Bézout

Exemple 53.

Calculer un PGCD, ainsi qu'une relation de Bézout pour $A = X^3 - 2X^2 + 2X - 1$ et $B = X^3 - 1$.

Extension à un nombre fini de polynômes.

De la même façon que dans $\mathbb{Z}$, on peut définir les PGCD de n polynômes $A_1, \dots, A_n$ de $\mathbb{K}[X]$ non tous nuls. Le diviseur maximal en degré et unitaire étant noté

$$A_1 \wedge \cdots \wedge A_n.$$

Les résultats de l'arithmétique classique s'étendent, en particulier l'*associativité* du PGCD. Pour alléger cet exposé, on renvoie au cours d'arithmétique dans $\mathbb{Z}$ pour un énoncé précis.

2.3 PPCM de deux polynômes.

Soient A et B polynômes de $\mathbb{K}[X]$. L'ensemble $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est celui de leurs multiples communs. Si A et B sont non nuls, cette intersection contient au moins un polynôme non nul : AB.

Définition 54.

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

- Si A et B sont non nuls,
  - tout multiplie commun de A et B de degré minimal est appelé un **PPCM** de A et B ;
  - l'unique polynôme unitaire parmi eux est appelé **PPCM** unitaire et noté $A \vee B$.
- Si A ou B vaut 0, on pose $a \vee b = 0$.

Proposition 55.

Soit A et B dans $\mathbb{K}[X]$. Alors

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X].$$

Les multiples communs de A et B sont exactement les multiples du PPCM unitaire de A et B. Le PPCM unitaire peut être remplacé ici par n'importe quel PPCM.

Proposition 56.

$$\forall (A, B) \in (\mathbb{K}[X])^2 \quad (A \wedge B) \cdot (A \vee B) \text{ et } AB \text{ sont associés.}$$

2.4 Polynômes premiers entre eux.

Définition 57 (le cas d'un couple).

On dit que deux polynômes sont **premiers entre eux** si leur PGCD unitaire est égal à $1_{\mathbb{K}[X]}$. Ainsi, deux polynômes sont premiers entre eux si et seulement leurs seuls diviseurs communs sont les polynômes constants non nuls

Si deux polynômes sont premiers entre eux, au moins l'un d'entre eux est non nul.

Proposition 58 (se ramener à deux polynômes premiers entre eux).

Soient $(A, B) \in (\mathbb{K}[X])^2 \setminus \{(0,0)\}$ et D un PGCD de A et B.
Si A^* et B^* sont les deux polynômes tels que $A = DA^*$, $B = DB^*$, alors $A^* \wedge B^* = 1$.

Proposition 59.

Deux polynômes non nuls A et B sont premiers entre eux ssi AB est un PPCM de A et B.

Théorème 60 (de Bézout).

$$\forall A, B \in \mathbb{K}[X] \qquad A \wedge B = 1 \iff \exists (U, V) \in (\mathbb{K}[X])^2 \quad AU + BV = 1.$$

Corollaire 61.

Si A, B, C sont trois polynômes de $\mathbb{K}[X]$, alors

1. Si $A \wedge B = 1$ et $A \wedge C = 1$, alors $A \wedge (BC) = 1$.
2. Plus généralement, si A est premier avec chacun des m polynômes $B_1, \ldots, B_m$ où $m \in \mathbb{N}^*$, alors il est premier avec leur produit $B_1 \cdots B_m$.
3. Si $A \wedge B = 1$, alors pour tout $(n, p) \in \mathbb{N}^2$, $A^n \wedge B^p = 1$.

Exemple 62 (important).

Soient $(\alpha, \beta) \in \mathbb{K}^2$ tel que $\alpha \neq \beta$ et $(n, p) \in \mathbb{N}^2$. Montrer que $(X - \alpha)^n \wedge (X - \beta)^p = 1$.

Le produit de deux diviseurs n'est pas toujours un diviseur, mais...

Proposition 63 (Produit de diviseurs premiers entre eux).

$$\forall (A, B, C) \in (\mathbb{K}[X])^3 \qquad \begin{cases} A \mid C \text{ et } B \mid C \\ A \wedge B = 1 \end{cases} \implies AB \mid C.$$

Diviser un produit, ce n'est pas forcément diviser l'un des facteurs, mais...

Théorème 64 (Lemme de Gauss).

$$\forall (A,B,C) \in (\mathbb{K}[X])^3 \qquad \begin{cases} A \mid BC \\ A \wedge B = 1 \end{cases} \implies A \mid C.$$

Extension à un nombre fini de polynômes.

Dans ce paragraphe, n est un entier naturel supérieur à 2.

Définition 65.

Des polynômes $A_1, \dots, A_n$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD unitaire est égal à 1, ou de manière équivalente les seuls diviseurs communs à ces polynômes sont les polynômes constants non nuls.

Remarque. Si n polynômes non tous nuls ne sont pas premiers entre eux dans leur ensemble, on peut les diviser par leur PGCD pour obtenir n polynômes qui cette fois le sont.

Définition 66.

Les polynômes $A_1, \dots, A_n$ sont **deux à deux premiers entre eux** si

$$\forall (i,j) \in [\![1,n]\!]^2 \quad i \neq j \implies A_i \wedge A_j = 1.$$

Exemple 67 (*dans leur ensemble* VS *deux à deux*).

Si n polynômes sont premiers entre eux deux à deux, ils le sont dans leur ensemble.
Les polynômes $X(X+1)$, $X(X+2)$ et $(X+1)(X+2)$ sont premiers entre eux dans leur ensemble, mais deux quelconques d'entre eux ne sont pas premiers entre eux.

Proposition 68 (Théorème de Bezout généralisé).

Soit $(A_1, \dots, A_n) \in (\mathbb{K}[X])^n$

$A_1, \dots, A_n$ premiers entre eux dans leur ensemble $\iff \exists (U_1, \dots, U_n) \in (\mathbb{K}[X])^n \quad \sum_{i=1}^{n} A_i U_i = 1.$

Proposition 69 (Produit de diviseurs deux à deux premiers entre eux).

Soient n polynômes $A_1, A_2, \dots, A_n$ et un polynôme B.

Si tous les A_i divisent B et si les A_i sont deux à deux premiers entre eux,
alors le produit $A_1 \cdots A_n$ divise B.

3 Racines et factorisation.

3.1 Racines et divisibilité.

Théorème 70 (Racine et divisibilité par un polynôme de degré 1).

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Il y a équivalence entre les deux assertions suivantes.

1. α est une racine de P.
2. $X - \alpha$ divise P.

Proposition 71.

Soit $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $\alpha_1, \alpha_2, \dots \alpha_p \in \mathbb{K}$ des scalaires de $\mathbb{K}$ deux à deux distincts. On a

$$\alpha_1, \alpha_2 \dots, \alpha_p \text{ sont racines de } P \iff \prod_{k=1}^{p} (X - \alpha_k) \text{ divise } P.$$

Exemple 72.

Soit $(p, q, r) \in \mathbb{N}^3$. Justifier qu'il existe $Q \in \mathbb{C}[X]$ tel que $X^{3p+2} + X^{3q+1} + X^{3r} = (X^2 + X + 1)Q$.

Définition 73.

Un polynôme est dit **scindé** dans $\mathbb{K}[X]$ (ou « sur $\mathbb{K}$ ») s'il s'écrit comme produit polynômes de degré 1 à coefficients dans $\mathbb{K}$.

Exemple. Pour tout $n \in \mathbb{N}^*$, $X^n - 1$ est scindé sur $\mathbb{C}$: $X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}}\right)$.

Corollaire 74 (Condition suffisante pour que le polynôme soit scindé).

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.
Si P possède n racines deux à deux distinctes $\alpha_1, \dots, \alpha_n$ dans $\mathbb{K}$, alors il est scindé sur $\mathbb{K}$.

$$\exists \lambda \in \mathbb{K}^* \quad P = \lambda \prod_{k=1}^{n} (X - \alpha_k), \quad (\lambda \text{ est le coefficient dominant de } P).$$

Exemple 75 (Factorisation des polynômes de Tchebychev).

Reprenons la suite $(T_n)_{n\in\mathbb{N}}$ définie par $T_0 = 1$, $T_1 = X$ et $\forall n \in \mathbb{N}$ $T_{n+2} = 2XT_{n+1} - T_n$.
Fixons $n \in \mathbb{N}^*$. On a prouvé que T_n est de degré n, de coefficient dominant 2^{n-1} et on a prouvé que pour tout θ réel , $T_n(\cos\theta) = \cos(n\theta)$. Démontrer que

$$T_n = 2^{n-1} \prod_{k=0}^{n-1} \left(X - \cos\left(\frac{(2k+1)\pi}{2n}\right)\right).$$

3.2 Racines et rigidité des polynômes.

Théorème 76.

Le nombre de racines distinctes d'un polynôme non nul est majoré par son degré.

Corollaire 77 (Montrer qu'un polynôme est nul en prouvant qu'il a trop de racines).

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n+1$ racines deux à deux distinctes, alors $P = 0$.
2. Si P admet une infinité de racines alors $P = 0$.

Corollaire 78 (Montrer que $P = Q$ en prouvant que $P - Q$ a "trop" de racines).

Si P et Q sont de degré inférieur à n et que $P - Q$ possède $n+1$ racines, alors $P = Q$.
Notamment, si P et Q coïncident sur une infinité de valeurs de $\mathbb{K}$, P et Q sont le même polynôme.
En particulier, lorsque les fonctions polynomiales associées à P et Q sont égales, alors $P = Q$.

Exemple 79.

1. Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $\forall n \in \mathbb{N} \quad P(n) = n^{666}$.
2. Soit $n \in \mathbb{N}^*$. Prouver l'unicité du polynôme $T_n \in \mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R}\ T_n(\cos\theta) = \cos(n\theta)$.

3.3 Multiplicité d'une racine.

Définition 80.

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$ une racine de P. On dit que la racine α est de **multiplicité** $m \in \mathbb{N}^*$ si

$$(X-\alpha)^m \text{ divise } P \quad \text{et} \quad (X-\alpha)^{m+1} \text{ ne divise pas } P.$$

On dira que α est de multiplicité **au moins** égale à $k \in \mathbb{N}$ si $(X-\alpha)^k$ divise P.
Une racine de multiplicité 1 est dite **simple**. Une racine qui n'est pas simple est dite **multiple**.

Proposition 81.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Il y a équivalence entre les deux assertions suivantes.

1. α est racine de P de multiplicité m.
2. $\exists Q \in \mathbb{K}[X] \quad P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$.

Le polynôme $(X+1)X^2(X-5)^3$ a pour racines -1 (racine simple), 0 (racine double) et 5 (multiplicité 3).

Lemme 82.

Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $k \in \mathbb{N}^*$. Si $(X-\alpha)^k$ divise P, alors $(X-\alpha)^{k-1}$ divise P'.

Théorème 83 (Caractérisation de la multiplicité).

Soit $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $m \in \mathbb{N}^*$. On a (1) $\iff$ (2), ainsi que (3) $\iff$ (4).

1. α est une racine de P de multiplicité au moins m.
2. $P(\alpha) = P'(\alpha) = P''(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0$.
3. α est une racine de P de multiplicité m.
4. $P(\alpha) = P'(\alpha) = P''(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0 \quad$ et $\quad P^{(m)}(\alpha) \neq 0$.

Exemple 84.

En nous appuyant sur une racine multiple "facile", factorisons $P = X^4 + X^3 - 7X^2 - 13X - 6$.

Corollaire 85 (Caractérisation des racines simples).

Soit $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.

$$\alpha \text{ est une racine simple de } P \quad \text{ si et seulement si } \quad P(\alpha) = 0 \text{ et } P'(\alpha) \neq 0.$$

Proposition 86.

Soit $P \in \mathbb{K}[X]$ et $\alpha_1, \ldots, \alpha_p$, p racines de P distinctes deux à deux, de multiplicités respectives au moins égales à $k_1, \ldots, k_p$. Alors, $\prod_{i=1}^{p} (X-\alpha_i)^{k_i}$ divise P.

Exemple 87.

On peut compter les racines d'un polynôme
- en considérant les racines deux à deux distinctes,
- ou bien *avec leur multiplicité*, en répétant m fois une racine dans la liste lorsque sa multiplicité vaut m.

Par exemple, le polynôme $(X+1)X^2(X-5)^3$ possède
- trois racines distinctes : $-1, 0$ et 5,
- six racines comptées avec leur multiplicité : $-1, 0, 0, 5, 5, 5$.

Corollaire 88.

Soient $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. Si P est non nul, alors le nombre de ses racines dans $\mathbb{K}$, comptées avec multiplicité, est majoré par son degré.
2. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n+1$ racines comptées avec leur multiplicité, alors P est le polynôme nul.

Corollaire 89 (Cas d'un degré égal au nombre de racines, comptées avec leur multiplicité).

Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \in \mathbb{N}^*$.
Si P possède p racines $\alpha_1, \dots, \alpha_p$ dans $\mathbb{K}$, de multiplicités $m_1, \dots, m_p$, et si $m_1 + \cdots + m_p = n$, alors P est scindé sur $\mathbb{K}$. Plus précisément, il existe $\lambda \in \mathbb{K}^*$ tel que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k}, \quad (\lambda \text{ étant le coefficient dominant de } P).$$

3.4 Existence de racines : théorème de d'Alembert-Gauss.

Théorème 90 (de d'Alembert-Gauss, ou théorème fondamental de l'algèbre).

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.

Proposition 91.

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

Exemple 92.

Soit $P \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$. Montrer que $\widetilde{P} : z \mapsto P(z)$, application de $\mathbb{C}$ vers $\mathbb{C}$ est surjective.

Proposition 93 (une racine réelle).

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

Exemple 94 (Recherche d'une racine rationnelle).

1. Soit $P = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$.
   Montrer que si $\frac{p}{q}$ est racine de P avec $p \wedge q = 1$, alors p divise a_0 et q divise a_n.
2. Factoriser $X^3 + 2X^2 - 4X - 3$ dans $\mathbb{R}[X]$.

3.5 Décomposition en facteurs irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Définition 95.

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il est dit **irréductible** dans $\mathbb{K}[X]$ si ses seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes constants (non nuls) et les polynômes associés à P, c'est-à-dire ceux de la forme λP, $\lambda \in \mathbb{K}^*$.

Proposition 96.

Un polynôme non constant P est irréductible ssi tous ses diviseurs sont de degré 0 ou $\deg(P)$.

Les polynômes irréductibles sont à $\mathbb{K}[X]$ ce que les entiers premiers sont à $\mathbb{N}$ (ou $\mathbb{Z}$).

Proposition 97.

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1 à coefficients dans $\mathbb{C}$.

Proposition 98 (Factorisation en produit d'irréductibles à coeff. dans $\mathbb{C}$).

Tout polynôme non constant de $\mathbb{C}[X]$ est scindé dans $\mathbb{C}[X]$.

Plus précisément, pour tout $P \in \mathbb{C}[X] \setminus \mathbb{C}_0[X]$, il existe $\lambda \in \mathbb{C}^*$, $p \in \mathbb{N}^*$, $\alpha_1, \dots \alpha_p \in \mathbb{C}$, deux à deux distincts et $m_1, \dots m_p \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k}.$$

En particulier, le nombre de racines de P comptées avec multiplicité est égale au degré de P :

$$\sum_{k=1}^{p} m_k = \deg(P).$$

Lemme 99.

Soit $P \in \mathbb{R}[X]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$ et $m \in \mathbb{N}^*$. Si α est racine de P alors $\overline{\alpha}$ l'est aussi et

$$B_\alpha = (X - \alpha)(X - \overline{\alpha}) = (X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)$$

divise P dans $\mathbb{R}[X]$.

Si α a pour multiplicité m, alors $\overline{\alpha}$ aussi et B_α^m divise P dans $\mathbb{R}[X]$.

Proposition 100.

Les polynômes irréductibles de $\mathbb{R}[X]$ sont
- les polynômes de degré 1,
- les polynômes de degré 2, n'ayant pas de racines réelles.

Proposition 101 (Factorisation en produit d'irréductibles à coeff. dans $\mathbb{R}$).

Tout polynôme non constant de $\mathbb{R}[X]$ s'écrit comme produit de polynômes irréductibles de $\mathbb{R}[X]$.

Plus précisément, si $P \in \mathbb{R}[X] \setminus \mathbb{R}_0[X]$, il existe $\lambda \in \mathbb{R}^*$, $p \in \mathbb{N}$, $\alpha_1, \dots \alpha_p \in \mathbb{R}$ deux à deux distincts, et $m_1, \dots m_p \in \mathbb{N}^*$, et il existe $p' \in \mathbb{N}$, $(\beta_1, \gamma_1), \dots, (\beta_{p'}, \gamma_{p'}) \in \mathbb{R}^2$, $v_1, \dots v_{p'} \in \mathbb{N}^*$ tels que

$$P = \lambda \prod_{k=1}^{p} (X - \alpha_k)^{m_k} \prod_{k=1}^{p'} \left(X^2 + \beta_k X + \gamma_k\right)^{v_k} \quad \text{avec} \quad \forall k \in [\![1, p']\!] \ \ \beta_k^2 - 4\gamma_k < 0.$$

Méthode (Factorisation d'un polynôme en produit d'irréductibles).

- On repère le degré de P : il majore le nombre de racines. Il est même égal au nombre de racines comptées avec multiplicité dans $\mathbb{C}$.
- On repère le coefficient dominant : il figure dans la factorisation.
- On cherche les racines complexes de P en posant l'équation $P(z) = 0$ avec $z \in \mathbb{C}$, ainsi que la multiplicité de ces racines. On obtient une factorisation dans $\mathbb{C}[X]$ (cf P98).
- Les racines réelles donnent des facteurs de degré 1. Les racines non réelles sont "couplées" avec leur conjuguées pour obtenir des polynômes de degré 2 sans racines réelles, comme dans le lemme 99. On obtient une factorisation dans $\mathbb{R}[X]$ (du type de celle de la proposition 101)

Exemple 102.

Factorisation de $X^6 - 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

Quelques exemples de factorisation (dans $\mathbb{C}[X]$ puis $\mathbb{R}[X]$), laissées en exercice.

$$\begin{aligned} X^6 + 1 &= \left(X - e^{i\frac{\pi}{6}}\right)(X - i)\left(X - e^{5i\frac{\pi}{4}}\right)\left(X - e^{-5i\frac{\pi}{4}}\right)(X + i)\left(X - e^{-i\frac{\pi}{6}}\right) \\ &= \left(X^2 - \sqrt{3}X + 1\right)\left(X^2 + 1\right)\left(X^2 + \sqrt{3}X + 1\right). \end{aligned}$$

$$\begin{aligned} X^8 - 1 &= (X-1)(X+1)(X - e^{\frac{ik\pi}{4}})(X - e^{-\frac{ik\pi}{4}})(X-i)(X+i)(X - e^{\frac{3ik\pi}{4}})(X - e^{-\frac{3ik\pi}{4}}) \\ &= (X-1)(X+1)(X^2 - \sqrt{2}X + 1)(X^2+1)(X^2 + \sqrt{2}X + 1). \end{aligned}$$

4 Compléments.

4.1 Relations coefficients-racines pour un polynôme scindé.

Définition 103.

Soient $x_1, \dots, x_n \in \mathbb{K}$. On appelle **fonctions symétriques élémentaires** de $x_1, \dots, x_n$ les nombres définis par

$$\forall k \in [\![1, n]\!] \qquad \sigma_k = \sum_{A \in \mathcal{P}_k([\![1,n]\!])} \prod_{i \in A} x_i = \sum_{i_1 < i_2 < \dots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

On a notamment

$$\sigma_1 = \sum_{i=1}^{n} x_i, \qquad \sigma_n = \prod_{i=1}^{n} x_i, \qquad \sigma_2 = \sum_{i<j} x_i x_j.$$

Remarque. Dans le cas $n = 2$, il y a deux fonctions symétriques élémentaires de x_1, x_2 :

$$\sigma_1 = x_1 + x_2 \qquad \sigma_2 = x_1 x_2.$$

Dans le cas $n = 3$, il y a trois fonctions symétriques élémentaires de x_1, x_2, x_3 :

$$\sigma_1 = x_1 + x_2 + x_3, \qquad \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3, \qquad \sigma_3 = x_1x_2x_3.$$

Exemple 104.

Soient x, y, z trois scalaires de $\mathbb{K}$ et $\sigma_1, \sigma_2, \sigma_3$ les fonctions symétriques élémentaires associées. Démontrer que

$$\begin{array}{rcl} x^2 + y^2 + z^2 & = & \sigma_1^2 - 2\sigma_2 \\ x^3 + y^3 + z^3 & = & \sigma_1^3 + 3\sigma_3 - 3\sigma_1\sigma_2 \end{array}.$$

Théorème 105 (Relations coefficients-racines : formules de Viète).

Soit P un polynôme de degré $n \in \mathbb{N}^*$, scindé sur $\mathbb{K}$: il s'écrit donc

$$P = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad P = a_n \prod_{k=1}^{n} (X - \alpha_k),$$

où $a_0, \dots, a_n$ sont ses coefficients et $\alpha_1, \dots, \alpha_n$ ses racines, répétées avec leur multiplicité. On a

$$\boxed{P = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^k \sigma_k X^{n-k} + \dots + (-1)^n \sigma_n \right)},$$

avec $\sigma_1, \dots, \sigma_n$ les fonctions symétriques élémentaires des racines $\alpha_1, \dots, \alpha_n$.

Ces nombres s'expriment donc en fonction des coefficients de P :

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

Corollaire 106 (Somme et produit des racines d'un polynôme scindé).

Soit $P = \sum a_k X^k$ un polynôme de degré $n \in \mathbb{N}^*$, scindé sur $\mathbb{K}$.
La somme des racines σ_1 et le produit des racines σ_n valent

$$\sigma_1 = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad \sigma_n = (-1)^n \frac{a_0}{a_n}.$$

Remarque. Soit $aX^2 + bX + c$ un polynôme de degré 2 et α_1 et α_2 ses deux racines complexes. On retrouve

$$\alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \alpha_1\alpha_2 = \frac{c}{a}.$$

Preuve du théorème. Avant de développer $a_n(X-\alpha_1)\cdots(X-\alpha_n)$, on pourra commencer par examiner le cas $n = 3$ pour un polynôme unitaire :

$$P = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3) = X^3 - \underbrace{(\alpha_1+\alpha_2+\alpha_3)}_{=\sigma_1}X^2 + \underbrace{(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)}_{=\sigma_2}X - \underbrace{\alpha_1\alpha_2\alpha_3}_{=\sigma_3}.$$

□

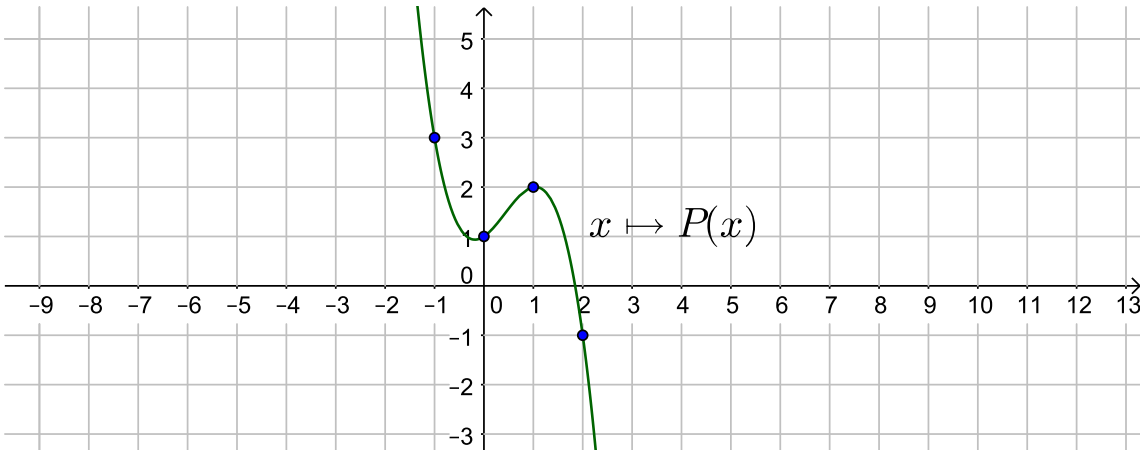
Exemple 107.

Trouver tous les triplets $(x, y, z) \in \mathbb{R}^3$ tels que

$$\begin{aligned} x + y + z &= 2 \\ x^2 + y^2 + z^2 &= 14 \\ x^3 + y^3 + z^3 &= 20 \end{aligned}.$$

4.2 Interpolation de Lagrange.

Interpoler, c'est proposer une fonction qui passe par un ensemble de points donnés. Ici, on a donné l'unique polynôme P de degré inférieur à 3 passant par les quatre points $(-1, 3)$, $(0, 1)$, $(1, 2)$ et $(2, -1)$.



Polynôme interpolateur.

Définition 108.

Soit $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in \mathbb{K}^n$, où les x_i sont deux à deux distincts. On pose

$$\forall i \in [\![1, n]\!] \quad L_i = \frac{\prod\limits_{\substack{k=1 \\ k \neq i}}^{n} (X - x_k)}{\prod\limits_{\substack{k=1 \\ k \neq i}}^{n} (x_i - x_k)}.$$

Les polynômes $(L_1, \dots, L_n)$ sont appelés **polynômes de Lagrange** associés à $(x_1, \dots, x_n)$.

Exemple 109 (Comprendre la définition avec un exemple).

Écrire la famille des quatre polynômes de Lagrange associés à $(x_1, x_2, x_3, x_4) = (-1, 0, 1, 2)$.

Proposition 110.

Soit $n \in \mathbb{N}^*$ et $(L_1, \dots, L_n)$ la famille de polynômes de Lagrange associés à un n-uplet $(x_1, \dots, x_n)$ de scalaires deux à deux distincts. Tous les polynômes L_i sont de degré $n - 1$ et

$$\forall (i, j) \in [\![1, n]\!]^2 \quad L_i(x_j) = \delta_{i,j}.$$

Théorème 111 (Interpolation de Lagrange).

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.

$$\exists! P \in \mathbb{K}_{n-1}[X] \quad \forall i \in [\![1, n]\!] \quad P(x_i) = y_i.$$

En notant $(L_1, \dots, L_n)$ la famille de polynômes de Lagrange associés à $(x_1, \dots, x_n)$, on a

$$P = \sum_{i=1}^{n} y_i L_i.$$

Corollaire 112 (L'ensemble des polynômes interpolateurs).

Soit $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ (scalaires deux à deux distincts) et $(y_1, \dots, y_n) \in \mathbb{K}^n$.
Soit P l'unique polynôme de $\mathbb{K}_{n-1}[X]$ tel que $\forall i \in [\![1, n]\!]$ $P(x_i) = y_i$.

Les polynômes $Q \in \mathbb{K}[X]$ tels que $\forall i \in [\![1, n]\!]$ $Q(x_i) = y_i$ sont ceux de la forme

$$Q = P + A \cdot \prod_{i=1}^{n} (X - x_i), \quad \text{où } A \in \mathbb{K}[X].$$

Preuves

Preuve du théorème 14.

Pour ne pas avoir à introduire des coefficients pour chaque polynôme ci-dessous, on convient de noter $[A]_k$, pour $k \in \mathbb{N}$ le coefficient d'ordre k d'un polynôme A. Dans toute la suite, k est un entier naturel fixé.

On se donne pour les calculs ci-dessous P, Q, R trois polynômes de $\mathbb{K}[X]$.

1) $(\mathbb{K}[X], +)$ est un groupe abélien, de neutre le polynôme nul.
Il est assez facile de vérifier, en effet, qu'il s'agit d'un sous-groupe de $(\mathbb{K}^{\mathbb{N}}, +)$, groupe abélien connu.

2) La loi $\times$ est une loi de composition interne sur $\mathbb{K}[X]$, cela a été établi par la proposition 11.

3) La loi $\times$ est commutative.

$$[PQ]_k = \sum_{i=0}^{k} [P]_i [Q]_{k-i} \underset{j=k-i}{=} \sum_{j=0}^{k} [P]_{k-j} [Q]_j = \sum_{i=0}^{k} [Q]_i [P]_{k-i} = [QP]_k.$$

4) Le polynôme $1 (= 1_{\mathbb{K}[X]})$ est neutre pour le produit.
Rappelons la définition du *symbole de Kronecker*, défini pour i et j entiers par

$$\delta_{i,j} = \begin{cases} 1 & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j \end{cases}$$

Le polynôme constant égal à 1 a tous ses coefficients nuls saufs celui d'ordre 0 qui vaut 1. Pour tout $i \in \mathbb{N}$, on a donc

$$[1_{\mathbb{K}[X]}]_i = \delta_{i,0}.$$

On calcule alors

$$[1_{\mathbb{K}[X]} \cdot P]_k \underset{3)}{=} [P \cdot 1_{\mathbb{K}[X]}]_k = \sum_{i=0}^{k} [P]_i \cdot [1_{\mathbb{K}[X]}]_{k-i} = \sum_{i=0}^{k} [P]_i \cdot \delta_{0,k-i} = 0 + [P]_k \cdot 1 = [P]_k.$$

5) Associativité. En écrivant de deux façons une somme triangulaire

$$\begin{aligned} [(PQ)R)]_k = \sum_{i=0}^{k} [PQ]_i [R]_{k-i} &= \sum_{i=0}^{k} \left(\sum_{j=0}^{i} [P]_j [Q]_{i-j} \right) [R]_{k-i} \\ &= \sum_{j=0}^{k} [P]_j \left(\sum_{i=j}^{k} [Q]_{i-j} [R]_{k-i} \right) \\ &\underset{l=i-j}{=} \sum_{j=0}^{k} [P]_j \left(\sum_{l=0}^{k-j} [Q]_l [R]_{k-j-l} \right) \\ &= \sum_{j=0}^{k} [P]_j [QR]_{k-j} = [P(QR)]_k. \end{aligned}$$

6) Distributivité.

$$[P(Q+R)]_k = \sum_{i=0}^{k} [P]_i [Q+R]_{k-i} = \sum_{i=0}^{k} [P]_i \left([Q]_{k-i} + [R]_{k-i} \right) = \sum_{i=0}^{k} [P]_i [Q]_{k-i} + \sum_{i=0}^{k} [P]_i [R]_{k-i} = [PQ]_k + [PR]_k.$$

□

Preuve de la proposition 15
• Le polynôme X^0 est la suite $(1, 0, \ldots)$: c'est bien le polynôme 1, par définition.
• Soit $n \in \mathbb{N}$. Vérifions que $X^{n+1} = X \times X^n$. Par définition, X^n est la suite dont tous les termes sont nuls saufs celui au rang n qui vaut 1. Ceci s'écrit

$$\forall k \in \mathbb{N} \quad [X^n]_k = \delta_{k,n}.$$

Fixons k et calculons le coefficient d'ordre k pour $X \times X^n$:

$$[X \times X^n]_k = \sum_{i=0}^{k} [X]_i [X^n]_{k-i} = \sum_{i=0}^{k} \delta_{i,1}\delta_{k-i,n}.$$

Le terme $\delta_{i,1}\delta_{k-i,n}$ est nul sauf si $i = 1$ **et** $k-i = n$, c'est-à-dire si $k = n+1$ **et** $i = 1$. Ainsi,

$$[X \times X^n]_k = \begin{cases} 0 & \text{si} \quad k \neq n+1 \\ \delta_{1,1}\delta_{n,n} = 1 & \text{si} \quad k = n+1 \end{cases}$$

On a bien $[X \times X^n]_k = \delta_{k,n+1} = [X^{n+1}]_k$, et ce pour tout k. On a bien vérifié que les polynômes $X \times X^n$ et X^{n+1} ont mêmes coefficients : ils sont égaux. □

Preuve de la proposition 32 Soient $P = \sum_{k\in\mathbb{N}} a_k X^k$ et $Q = \sum_{k\in\mathbb{N}} b_k X^k$ deux polynômes de $\mathbb{K}[X]$, et $\lambda, \mu \in \mathbb{K}$.

• La preuve de la première égalité est de routine. Fixons un entier naturel k et comparons les coefficients d'ordre k.

$$[(\lambda P + \mu Q)']_k = (k+1)[\lambda P + \mu Q]_{k+1} = (k+1)\left(\lambda a_{k+1} + \mu b_{k+1}\right) = \lambda [P']_{k+1} + \mu [Q']_{k+1} = [\lambda P' + \mu Q']_k.$$

• Pour la seconde égalité, on calcule le coefficient d'ordre k du membre de droite :

$$\begin{aligned}
[P'Q + PQ']_k &= [P'Q]_k + [PQ']_k \\
&= \sum_{i=0}^{k} [P']_i [Q]_{k-i} \; + \; \sum_{i=0}^{k} [P]_i [Q']_{k-i} \\
&= \sum_{i=0}^{k} (i+1) a_{i+1} b_{k-i} \; + \; \sum_{i=0}^{k} a_i (k-i+1) b_{k-i+1} \\
&= \sum_{j=1}^{k+1} j a_j b_{k-j+1} + \sum_{j=0}^{k} a_j (k-j+1) b_{k-j+1} \qquad \begin{cases} \text{première somme :} & j = i+1 \\ \text{seconde somme :} & i = j \end{cases} \\
&= (k+1) a_{k+1} b_0 + \sum_{j=1}^{k} (\not{j} + k - \not{j} + 1) a_j b_{k-j+1} + (k+1) a_0 b_{k+1} \\
&= (k+1) \sum_{j=0}^{k+1} a_j b_{k+1-j} = (k+1)[(PQ)]_{k+1} = [(PQ)']_k.
\end{aligned}$$

• L'identité $(P^n)' = nP'P^{n-1}$ est vraie pour $n = 0$. Supposons qu'elle le soit pour un entier naturel n donné. Alors, en utilisant la formule pour la dérivée d'un produit, on montre l'identité au rang $n+1$:

$$\left(P^{n+1}\right)' = (P \cdot P^n)' = P'P^n + P\left(P^n\right)' = P'P^n + P\left(nP'P^{n-1}\right) = (n+1)P'P^n,$$

• Notons $P = \sum_{k=0}^{n} a_k X^k$, où $n \geq \deg(P)$. On a

$$(P \circ Q)' = \left(\sum_{k=0}^{n} a_k Q^k\right)' = \sum_{k=0}^{n} a_k \left(Q^k\right)' = \sum_{k=0}^{n} a_k k Q' Q^{k-1} = Q' \sum_{k=0}^{n} k a_k Q^{k-1} = Q' \cdot P' \circ Q.$$

□

Preuve du théorème 42.
• Unicité. Preuve en classe.

• Existence. On va raisonner par récurrence sur le degré du polynôme à diviser.
Pour cela, fixons pour toute la preuve un polynôme B non nul, et notons p son degré qui est donc un entier naturel.

Pour $n \in \mathbb{N}$, on note

$$\mathcal{P}(n) \text{ « Pour tout polynôme } A \text{ de } \mathbb{K}_n[X] \text{ il existe un couple de polynômes } (Q,R) \text{ tel que } A = BQ + R \text{ et } \deg(R) < \deg(B). \text{ »}$$

⋆ Initialisation. Soit A un polynôme de $\mathbb{K}_0[X]$, c'est-à-dire un polynôme constant. On peut écrire $A = a_0 \cdot 1$. Deux cas se présentent. Si B est constant, alors on peut écrire $B = b_0 \cdot 1$, avec $b_0 \neq 0$ puisque B n'est pas nul. On écrit alors

$$a_0 \cdot 1 = \frac{a_0}{b_0} 1 \cdot b_0 1 + 0_{\mathbb{K}[X]}.$$

Cette division convient puisque le degré du reste $(-\infty)$ est strictement inférieur au degré de B (nul). Si B n'est pas constant, alors écrivons

$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$

De plus le degré du reste vaut $\deg(A) = 0 < \deg(B)$ (puisque B est non constant dans ce cas).

⋆ Hérédité. Soit $n \in \mathbb{N}$. Supposons $\mathcal{P}(n)$. Pour démontrer $\mathcal{P}(n+1)$ prenons A dans $\mathbb{K}_{n+1}[X]$. Si A est de degré inférieur à n, $\mathcal{P}(n)$ s'applique et nous donne l'existence d'un couple quotient reste comme il faut. Supposons dorénavant que A est de degré $n+1$.

♢ Si le degré de B, noté p, satisfait $p > n+1$, alors il suffit de poser

$$A = B \cdot 0_{\mathbb{K}[X]} + A.$$

Le reste vaut A et on a bien $\deg(A) = n+1 < p = \deg(B)$.

♢ Si $p \leq n+1$.

On peut écrire A et B sous la forme

$$\begin{array}{lllll} A = & a_{n+1}X^{n+1} & +\widetilde{A} & \text{avec } a_{n+1} \neq 0 & \text{et } \deg(\widetilde{A}) \leq n. \\ B = & b_p X^p & +\widetilde{B} & \text{avec } b_p \neq 0 & \text{et } \deg(\widetilde{B}) \leq p-1. \end{array}$$

On "commence" alors une division par B en s'occupant d'abord du terme de plus haut degré de A :

$$\begin{aligned} A &= \left(b_p X^p + \widetilde{B}\right) \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} - \frac{a_{n+1}}{b_p} X^{n+1-p}\widetilde{B} + \widetilde{A} \\ &= B \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} + C, \end{aligned}$$

où $C = \widetilde{A} - \frac{a_{n+1}}{b_p} X^{n+1-p}\widetilde{B}$. Le polynôme C est un polynôme de $\mathbb{K}_n[X]$, comme démontré par le calcul suivant :

$$\begin{aligned} \deg(C) &\leq \max\left[\underbrace{\deg(\widetilde{A})}_{\leq n}, \deg\left(\frac{a_{n+1}}{b_p} X^{n+1-p}\widetilde{B}\right)\right] \leq \max\left(n, (n+1-p) + \underbrace{\deg(\widetilde{B})}_{\leq p-1}\right) \\ &\leq \max(n,n) = n. \end{aligned}$$

D'après $\mathcal{P}(n)$, il existe deux polynômes ($\widetilde{Q}$ et $\widetilde{R}$) tels que $C = B\widetilde{Q} + \widetilde{R}$ avec $\deg(\widetilde{R}) < \deg(B)$. Réinjectons dans la division de A par B commencée plus haut :

$$A = B \cdot \frac{a_{n+1}}{b_p} X^{n+1-p} + B\widetilde{Q} + \widetilde{R} = B\left(\frac{a_{n+1}}{b_p} X^{n+1-p} + \widetilde{Q}\right) + \widetilde{R}.$$

On a bien ici une écriture du type $A = BQ + R$ avec $\deg(R) < \deg(B)$: $\mathcal{P}(n+1)$ est démontrée.

⋆ Conclusion. D'après le principe de récurrence, l'existence du couple quotient-reste est établie lorsque $A \in \mathbb{K}_n[X]$ et ce pour tout $n \in \mathbb{N}$. Puisque $\mathbb{K}[X] = \bigcup_{n=0}^{+\infty} \mathbb{K}_n[X]$, l'existence est établie pour tout polynôme A.

□

Exercices

Polynômes à travers leurs coefficients/ L'anneau $\mathbb{K}[X]$.

25.1 **[♦♦♢]** (1er TD : admettre la question 2)
On note $I =]-\frac{\pi}{2}, \frac{\pi}{2}[$.

1. Montrer que pour tout $n \in \mathbb{N}$, il existe un polynôme $P_n \in \mathbb{R}[X]$ tel que
$$\forall x \in I \quad \tan^{(n)}(x) = P_n(\tan(x)).$$
2. Montrer qu'un tel polynôme P_n est unique.
3. Donner pour tout entier n le degré et le coefficient dominant de P_n.
4. Démontrer que pour tout entier naturel n, les coefficients de P_n sont des entiers.

25.2 **[♦♢♢]** En calculant de deux façons différentes le coefficient devant X^n dans l'écriture développée de $(1-X^2)^n$, obtenir une identité sur les coefficients binomiaux.

25.3 **[♦♦♢]** Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $4P = (P')^2$.

25.4 **[♦♦♢]** Trouver tous les polynômes P dans $\mathbb{R}[X]$ qui satisfont
$$P(X+1) = XP'.$$

25.5 **[♦♦♦]** Soit Q un polynôme de $\mathbb{K}[X]$.
Démontrer que l'équation $P - P' = Q$ possède une unique solution dans $\mathbb{K}[X]$.

Racines et factorisation d'un polynôme.

25.6 **[♦♦♢]** Approximation de π par $\frac{22}{7}$.

1. Poser la division euclidienne de $X^4(1-X)^4$ par $1+X^2$.
2. Démontrer l'égalité $\int_0^1 \frac{x^4(1-x)^4}{1+x^2}\mathrm{d}x = \frac{22}{7} - \pi$.
3. Prouver l'inégalité $\frac{1}{1260} \leq \frac{22}{7} - \pi \leq \frac{1}{630}$.

25.7 **[♦♦♢]** Donner le reste dans la division euclidienne de $X^{2025} + X^3 + 1$ par
a) $X^2 - 1$, b) $(X-1)^2$.

25.8 **[♦♦♢]** Soient $(A, B, P) \in (\mathbb{K}[X])^3$ tels que P est non constant et $A \circ P | B \circ P$. Montrer que $A|B$.

25.9 **[♦♦♢]** Trouver tous les polynômes de $\mathbb{R}[X]$ tels que $(X+4)P(X) = XP(X+1)$.

25.10 **[♦♢♢]** Démontrer qu'il n'existe pas de polynôme P dans $\mathbb{R}[X]$ tel que
$$\forall n \in \mathbb{N} \quad P(n) = n^{666} + (-1)^n.$$

25.11 **[♦♢♢]** Soit $n \in \mathbb{N}^*$. Montrer que $(X-1)^3$ divise $P_n = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.

25.12 **[♦♢♢]** Montrer que, pour tout $n \in \mathbb{N}^*$, le polynôme $P = \sum_{k=0}^{n} \frac{X^k}{k!}$ n'a que des racines simples dans $\mathbb{C}$.

Arithmétique dans $\mathbb{K}[X]$

25.13 **[♦♦♢]** Soient p et q deux entiers naturels non nuls et r le reste dans la division euclidienne de p par q.

1. Montrer que $X^r - 1$ est le reste dans la division euclidienne de $X^p - 1$ par $X^q - 1$.
2. En déduire que $(X^p - 1) \wedge (X^q - 1) = X^{p \wedge q} - 1$.

25.14 **[♦♦♦]** Pour $n \in \mathbb{N}^*$, on pose $P_n = (X+1)^{n+1} - X^{n+1} - 1$. Donner une condition nécessaire et suffisante sur n pour que P_n et P_n' soient premiers entre eux.
Calculer leur PGCD quand ce n'est pas le cas.

Factorisation de polynômes

25.15 **[♦♦♢]** Factoriser $X^6 + X^3 + 1$ en produit d'irréductibles de $\mathbb{R}[X]$.

25.16 **[♦♦♦]** Soit $n \geq 2$. Factoriser $(X+i)^n - (X-i)^n$ en produit d'irréductibles de $\mathbb{C}[X]$.

25.17 **[♦♦♦]** Soit $n \in \mathbb{N}^*$. Factoriser $\sum_{k=0}^{n-1} X^k$ dans $\mathbb{C}[X]$. En déduire $\prod_{k=1}^{n-1} \sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$.

25.18 **[♦♦♦]** Soit $n \in \mathbb{N}^*$. Factoriser en produit d'irréductibles de $\mathbb{R}[X]$ le polynôme

$$\sum_{k=0}^{2n} X^k.$$

Divers

25.19 **[♦♢♢]** Soit P un polynôme de $\mathbb{R}[X]$ de degré $n \geq 2$ scindé dans $\mathbb{R}[X]$ à racines simples.

1. Montrer que P' est scindé à racines simples.
2. Prouver que la moyenne arithmétique des racines de P et celle des racines de P' sont égales.

25.20 **[♦♦♢]** Démontrer qu'il existe un nombre fini de polynômes unitaires de $\mathbb{Z}[X]$ ayant un degré égal à n et des racines complexes de module inférieur à 1.

25.21 **[♦♦♢]** Soit $n \in \mathbb{N}^*$ et $P = nX^n - \sum_{k=0}^{n-1} X^k$.

1. Prouver que 1 est racine simple de P.
2. (*) En vous intéressant à $(X-1)P$, démontrer que toutes les racines complexes de P sont simples.
3. Donner la somme et le produit des racines.

25.22 **[♦♦♦]** Soit $n \in \mathbb{N}$.

1. Exprimer de deux façons différentes l'unique polynôme P de degré n tel que $\forall i \in [\![0, n]\!]\ P(i) = i^n$.
2. En considérant son coefficient dominant, démontrer l'identité

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^n = n!$$
