Chapitre 21

Polynômes

Sommaire.

Les propositions marquées de ★ sont au programme de colles.

1 Polynômes à travers leurs coefficients.

1.1 Combinaisons linéaires et produits de polynômes formels.

Définition 1

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

L'**ensemble des polynômes** à coefficients dans $\mathbb{K}$ est 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 $(1, 0, 0, ...)$ est un polynôme. Il est appelé polynôme constant égal à 1 et noté 1.
- La suite $(0, 1, 0, ...)$ 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 de rang n qui vaut 1 est un polynôme qu'on notera X^n. On l'appelle **monôme** d'ordre n.

Définition 2

Soient $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ deux polynômes de $\mathbb{K}[X]$. Soit $\lambda \in \mathbb{K}$.
La suite $(a_k + b_k)_{k\in\mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$, qui sera noté $P + Q$.
La suite $(\lambda a_k)_{k\in\mathbb{N}}$ est un polynôme de $\mathbb{K}[X]$, qui sera noté $\lambda\mathcal{P}$.

Corrolaire 3

Soit $P = (a_k)_{k\in\mathbb{N}}$ un polynome de $\mathbb{K}[X]$ et m un entier tel que $\forall k > m,\ a_k = 0$. Alors

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

Notation

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

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

Il s'agit juste d'une notation, qui permet d'oublier que les polynômes, formellement, sont des suites (on n'a pas besoin de savoir cela dans la pratique).

Corrolaire 4

Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$ deux polynômes de $\mathbb{K}[X]$ et λ, μ deux scalaires de $\mathbb{K}$. Alors

$$\lambda P + \mu Q = \sum (\lambda a_k + \mu b_k) X^k.$$

Définition 5

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 pour tout $k \in \mathbb{N}$ par

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

La suite c est un polynôme : on l'appelle **produit** de P et Q et on le note PQ :

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

1.2 Évaluation d'un polynôme.

Définition 6: où l'on retrouve les fonctions polynomiales.

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

$$P(\alpha) = \sum_{k=0}^{+\infty} a_k \alpha^k \quad (P \in \mathbb{K}[X] \text{ et } P(\alpha) \in \mathbb{K});$$

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

Exemple 7

1. Soit $P = X^3 - 3X + 4$. Évaluer P en 2 et -1.
2. Quelle est la fonction polynomiale associée à $P = X^2 - 1$? à $Q = X$?

Solution :

$\boxed{1.}$ $P(2) = 6$ et $P(-1) = 6$.
$\boxed{2.}$ $\widetilde{P} : x \mapsto x^2 - 1, \quad \widetilde{Q} : x \mapsto x$.

Proposition 8: opérations et évaluations.

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

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

Exemple 9: Méthode de Horner.

Soit $n \in \mathbb{N}$ et $a_0, ..., a_n \in \mathbb{K}$, et $P = \sum a_k X^k$. Soit $\alpha \in \mathbb{K}$. On peut calculer $P(\alpha)$ ainsi :

$$P(\alpha) = ((...((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + ...)\alpha + a_1)\alpha + a_0.$$

Le nombre d'opérations à effectuer est en $O(n)$.

Définition 10

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

Exemple 11

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

Solution :

- On a $P(1) = 0$.
- L'ensemble des racines est $\mathbb{U}_5$

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

Théorème 12

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

Preuve :

Preuve hors-programme. Écrite dans l'autre poly.

Proposition 13: Cohérence de la notation X^n

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

Exemple 14

Dans la pratique, on calcule en se ramenant à faire des produits de monômes X^k comme on le faisait avec les fonctions polynomiales.

- Développer $(X^3+3)(X^4-5X^2+X)$.
- À l'aide d'identités remarquables, factoriser $1+X^4+X^8$.

Solution :

- C'est $X^7-5X^5+4X^4-15X^2+3X$.
- $1+X^4+X^8 = 1+2X^4+X^8-X^4 = (1+X^4)^2-X^4 = (X^4+1-X^2)(X^4+1+X^2)$.

Exemple 15: Formule de Vandermonde. ★

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

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

Solution :

On a $(X+1)^p(X+1)^q = (X+1)^{p+q} = \sum_{k=0}^{p+q} \binom{p+q}{k} X^k$ d'une part.
D'autre part :

$$(X+1)^p(X+1)^q = \left(\sum_{i=0}^{p} \binom{p}{i} X^i\right)\left(\sum_{i=0}^{q} \binom{q}{i} X^i\right) = \sum_{n\in\mathbb{N}} \sum_{i=0}^{n} \binom{p}{i}\binom{q}{n-i} X^n.$$

Par unicité, on a $\displaystyle\binom{p+q}{n} = \sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k}$.

1.4 Composition.

Définition 16: Composition.

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

$$P \circ Q = \sum_{k\in\mathbb{N}} a_k Q^k.$$

Remarques.

1. On vérifiera que $X \circ P = P \circ X = X$, ce qui explique que l'on écrit parfois $P(X)$ au lieu de P.
2. De la même façon, on écrira $P(X^2)$, ou $P(Q(X))$ pour désigne $P \circ X^2$ et $P \circ Q$.
3. L'écriture $P(X+1)$ peut être trompeuse : il s'agit de $P \circ (X+1)$, et non de $P \times (X+1)$. Pour le produit, on écrira $(X+1)P$.

1.5 Degré.

Définition 17

Soit $P = \sum a_k X^k$ 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 $\deg(0_{\mathbb{K}[X]}) = -\infty$.

Définition 18

Soit $P = \sum a_k X^k$ et $d \in \mathbb{N}$.

$$\deg(P) = d \iff \left(P = a_d X^d + \sum_{k=0}^{d-1} a_k X^k \ \text{ et } \ a_d \neq 0\right).$$

Si P est un polynôme non nul de degré $d \in \mathbb{N}$, alors a_d est appelé **coefficient dominant** de P.
Si ce coefficient vaut 1, le polynôme P est dit **unitaire.**
Notation locale du coefficient dominant de P : $\mathrm{cd}(P)$.

Exemple 19

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

Solution :

On a:

$$\begin{aligned} P &= \sum_{k=0}^{n} \binom{n}{k} X^k 2^{n-k} - \sum_{k=0}^{n} \binom{n}{k} X^l = \sum_{k=0}^{n} \binom{n}{k} X^k (2^{n-k} - 1) \\ &= (2^{n-n+1} - 1) X^{n-1} + \sum_{k=0}^{n-2} \binom{n}{k} X^k (2^{n-k} - 1) = nX^{n-1} + \ldots \end{aligned}$$

Donc $\deg(P) = n - 1$ et $\mathrm{cd}(P) = n$.

Proposition 20: ★

Soient $P, Q \in \mathbb{K}[X]$ deux polynômes. On a les résultats suivants :

1. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$, avec égalité si $\deg(P) \neq \deg(Q)$.
2. $\forall \lambda \in \mathbb{K},\ \deg(\lambda P) \leq \deg(P)$ avec égalité si $\lambda \neq 0$.
3. $\boxed{\deg(PQ) = \deg(P) + \deg(Q)}$.

Preuve :

$\boxed{1.}$ Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$.
— Si l'un est nul (supposons P), alors $P + Q = Q$ donc $\deg(P+Q) = \deg(Q) = \max(\deg(P), \deg(Q))$.
— Si $P \neq 0$ et $Q \neq 0$. On note $p = \deg(p)$ et $q = \deg(Q)$.
Alors $P + Q = \sum_{k=0}^{m} (a_k + b_k) X^k$ où $m = \max(p, q)$ donc $\deg(P+Q) \leq m = \max(p, q)$.
• Supposons $p \neq q$.
— Si $p < q$, alors $P + Q = b_q X^q + \ldots$ donc $\deg(P+Q) = q$.
— Si $p > q$, alors $P + Q = a_p X^p + \ldots$ donc $\deg(P+Q) = p$.
$\boxed{2.}$ Trivial.
$\boxed{★}$ Soient $P = \sum a_k X^k$ et $Q = \sum b_k X^k$.
1er cas. $P = 0$ ou $Q = 0$ (supposons $Q = 0$ SPDG).
D'une part, $\deg(PQ) = \deg(0) = -\infty$.
D'autre part, $\deg(P) + \deg(Q) = \deg(P) + (-\infty) = -\infty$.
2e cas. $P \neq 0$ et $Q \neq 0$. Notons $p = \deg(P)$ et $q = \deg(Q)$.
Alors $PQ = a_p b_q X^{p+q} + \ldots$, donc $\deg(PQ) = p + q = \deg(P) + \deg(Q)$.
Bonus : $\mathrm{cd}(PQ) = \mathrm{cd}(P)\mathrm{cd}(Q)$.

Complément. $\deg(P \circ Q) = \deg(P) \times \deg(Q)$ (avec $Q \neq 0$).

Exemple 21: Polynômes de Tchebychev. ★

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

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

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 $\theta \in \mathbb{R}$, $\cos(n\theta) = T_n(\cos(\theta))$.

Solution :

$\boxed{1.}$ $T_2 = 2X^2 - 1$, $T_3 = 4X^3 - 3X$, $T_4 = 8X^4 - 8X^2 + 1$, $T_5 = 16X^5 - 20X^3 + 5X$.
$\boxed{2.}$ Conjectures : pour $n \in \mathbb{N}$, $\deg(T_n) = n$ et $\mathrm{cd}(T_n) = 2^{n-1}$. Par récurrence sur n:
Initialisation. Faux au rang 0, mais vrai aux rangs 1 et 2.
Hérédité. Soit $n \in \mathbb{N}^*$ tel que les conjectures sont vraies aux rangs n et $n+1$.

$$T_{n+2} = 2XT_{n+1} - T_n \quad \text{donc} \quad \deg(T_{n+2}) \leq \max(\deg(2XT_{n+1}), \deg(-T_n)) = \max(n+2, n) = n+2.$$

Il y a égalité car $n + 2 \neq n$ donc $\deg(T_{n+2}) = n + 2$. La première conjecture est vérifiée.
De plus, $\exists Q_n \in \mathbb{K}[X] \mid T_{n+1} = 2^n X^{n+1} + Q_n$ et $\deg(Q_n) \leq n$.
Or $T_{n+2} = 2X(2^n X^{n+1} + Q_n) - T_n = 2^{n+1} X^{n+2} + (2XQ_n - T_n)$ on a bien $\mathrm{cd}(T_{n+2}) = 2^{n+1} = 2^{n+2-1}$.
Par récurrence, on conclut.
$\boxed{3.}$ Soit $\theta \in \mathbb{R}$ fixé. Pour $n \in \mathbb{N}$, on pose $\mathcal{P}_n$: « $\cos(n\theta) = T_n \cos(\theta)$ ».
Initialisation. On a $T_0(\cos(\theta)) = 1 = \cos(0)$; $\quad T_1(\cos(\theta)) = \cos(\theta)$ donc $\mathcal{P}_0$ et $\mathcal{P}_1$ sont vérifiées.
Hérédité. Soit $n \in \mathbb{N}$ tel que $\mathcal{P}_n$ et $\mathcal{P}_{n+1}$.
On rappelle que $2\cos(a)\cos(b) = \cos(a+b) + \cos(a-b)$ et que cos est paire.

$$\begin{aligned} T_{n+2}(\cos\theta) &= (2XT_{n+1} - T_n)(\cos\theta) = 2\cos\theta T_{n+1}(\cos\theta) - T_n(\cos\theta) \\ &= 2\cos\theta\cos((n+1)\theta) - \cos(n\theta) = \cos((n+2)\theta) + \cos(-n\theta) - \cos(n\theta) \\ &= \cos((n+2)\theta). \end{aligned}$$

Donc $\mathcal{P}_{n+2}$ est vraie. Par récurrence, on conclut.

Corrolaire 22

Pour $n \in \mathbb{N}$, on notera $\mathbb{K}_n[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$, de degré inférieur ou égal à n. Cet ensemble contient le polynôme nul et est stable par combinaisons linéaires.

Preuve :

Soit $n \in \mathbb{N}$.
- $\deg(0_{\mathbb{K}[X]}) \leq n$ donc $0_{\mathbb{K}[X]} \in \mathbb{K}_n(X)$.
- Soient $P, Q \in \mathbb{K}_n[X]$ et $\lambda, \mu \in \mathbb{K}$: $\deg(\lambda P + \mu Q) \leq \max(\deg(P), \deg(Q)) \leq n$.

Corrolaire 23

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

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

Ainsi, pouvouns-nous « simplifier » par un polynôme non nul :

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

Preuve :

Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $\deg(P) + \deg(Q) = -\infty$ alors $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$ alors $P = 0$ ou $Q = 0$.
Soient $A, B, C \in \mathbb{K}[X]$ tels que $AB = AC$ et $A \neq 0$. Alors $A(B - C) = 0$ donc $B - C = 0$ donc $B = C$.

Corrolaire 24: Les inversibles de l'anneau des polynômes sont ceux constants non nuls.

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

Preuve :

Soit $P \in U(\mathbb{K}[X])$: $\exists Q \in \mathbb{K}[X] \mid PQ = 1_{\mathbb{K}[X]}$.
Alors $\deg(P) + \deg(Q) = \deg(1_{\mathbb{K}[X]}) = 0$, alors $\deg(P) = \deg(Q) = 0$ donc $\exists a \in \mathbb{K} \mid P = a1_{\mathbb{K}[X]}$.

1.6 Dérivation dans $\mathbb{K}[X]$.

Définition 25

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.

Proposition 26

Soit $P \in \mathbb{R}[X]$. La fonction polynomiale associée au polynôme dérivé P' est la dérivée de la fonction polynomiale associée à P.

Preuve :

Soit $P \in \mathbb{R}[X] \mid P = \displaystyle\sum_{k=0}^{n} a_k X^k$, on pose $\widetilde{P} : x \mapsto \displaystyle\sum_{k=0}^{n} a_k x^k$ dérivable : $\widetilde{P}' : x \mapsto \displaystyle\sum_{k=0}^{n-1} (k+1) a_{k+1} x^k$.
Donc pour $x \in \mathbb{R}$, $P'(x) = \widetilde{P}'(x)$.

Proposition 27

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

Preuve :

Soit $P = \sum a_k X^k$.

$$\begin{aligned} P \text{ est constant } &\iff \forall k \geq 1,\ a_k = 0 \iff \forall k \geq 0,\ a_{k+1} = 0 \\ &\iff \forall k \geq 0,\ (k+1) a_{k+1} = 0 \iff P' = 0_{\mathbb{K}[X]}. \end{aligned}$$

Proposition 28: Degré du polynôme dérivé.

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

Preuve :

Soit $P = \sum a_k X^k$. On suppose $P \neq 0$. On note $n = \deg(P)$. On a $P = a_n X^n + ...$ donc $P' = n a_n X^{n-1} + ...$
- Si $n \geq 1$, $n a_n \geq 0$ donc $\deg(P') = n - 1 = \deg(P) - 1$.
- Si $n = 0$, $P = a_0$ donc $P' = 0_{\mathbb{K}[X]}$ donc $\deg(P') = -\infty$.

Proposition 29: Dérivation et opérations.

Soient $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$.

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

Définition 30

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

$$P^{(0)} = P \quad \text{et} \quad \forall k \in \mathbb{N},\ P^{(k+1)} = (P^{(k)})'.$$

Exemple 31

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

Solution :

Soient $n, k \in \mathbb{N}$ et $a \in \mathbb{K}$.
On a $((X-a)^n)^{(1)} = n(X-a)^{n-1}$, $((X-a)^n)^{(2)} = n(n-1)(X-a)^{n-2}$.
En itérant: $((X-a)^n)^{(k)} = n(n-1)...(n-(k-1))(X-a)^{n-k}$.
Si $k > n$, alors $((X-a)^n)^{(k)} = 0$, sinon $((X-a)^n)^{(k)} = \frac{n!}{(n-k)!}(X-a)^{n-k}$.

Proposition 32: Linéarité de la dérivée $n$ème et formule de Leibniz (admis).

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

Proposition 33: Formule de Taylor pour les polynômes

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

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

Preuve :

Initialisation. $\frac{P^{(0)}(a)}{0!}(X-a)^0 = P(a)$ avec $P \in \mathbb{K}_0[X]$, or P constant donc $P = P(a)$. Vrai.
Hérédité. Soit $n \in \mathbb{N}$ tel que la propriété soit vraie. Soit $P \in \mathbb{K}_{n+1}[X]$, alors $P' \in \mathbb{K}_n[X]$:

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

On pose $Q = \sum_{k=0}^{n+1} \frac{P^{(k)}(a)}{k!}(X-a)^k$ donc $(P-Q)' = ... = 0$ donc $\exists c \in \mathbb{K} \mid P - Q = c$.
Or $Q(a) = ... = P(a)$ donc $c = 0$ donc $P = Q$ donc la propriété est vraie au rang $n+1$.
Par récurrence, la propriété est vraie pour tout $n \in \mathbb{N}$.

2 Racines et factorisation d'un polynôme.

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

Définition 34

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 35

Tous les polynômes divisent le polynôme nul.
Pour $n \in \mathbb{N}^*$, $X - 1$ divise $X^n - 1$:

$$X^n - 1 = (X-1)\sum_{k=0}^{n-1} X^k, \quad \text{notamment} \quad X^3 - 1 = (X-1)(X^2 + X + 1).$$

Proposition 36

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

Preuve :

Supposons $B \mid A$ et $A \neq 0$: $\exists Q \in \mathbb{K}[X] \mid A = BQ$.
Donc $\deg(A) = \deg(BQ) = \deg(B) + \deg(Q)$ donc $\deg(A) - \deg(B) = \deg(Q) \geq 0$ car $Q \neq 0$.
On a bien $\deg(B) \leq \deg(A)$.

Définition 37

La relation divise sur $\mathbb{K}[X]$ est réflexive et transitive, mais elle n'est pas antisymétrique :

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

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

Théorème 38: ★

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

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

Preuve :

Unicité. Soient (Q_1, R_1) et (Q_2, R_2) dans $\mathbb{K}[X]^2$ tels que ...
On a $BQ_1 + R_1 = BQ_2 + R_2$ donc $B(Q_1 - Q_2) = R_2 - R_1$: $\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1)$.
Or $\deg(R_2 - R_1) \leq \max(\deg(R_2), \deg(R_1)) \leq \deg(B)$ donc $\deg(B) + \deg(Q_1 - Q_2) < \deg(B)$.
Donc $\deg(Q_1 - Q_2) < 0$ donc $Q_1 - Q_2 = 0$, puis $R_1 - R_2 = 0$: $(Q_1, R_1) = (Q_2, R_2)$.

Exemple 39

Poser la division de $A = X^5 + 3X^3 - 2X^2 + 1$ par $B = X^2 - 2X - 1$.

Solution :

$X^5 + 2X^2 + 8X + 16 = (X^2 - 2X - 1)(X^2 + 2X^2 + 8X + 16) + 40X + 16$.

Corrolaire 40

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.

Preuve :

$\boxed{\Longleftarrow}$ Trivial.
$\boxed{\Longrightarrow}$ Si $B \mid A$, alors $\exists Q \in \mathbb{K}[X] \mid A = BQ$ donc $A = BQ + 0$. Par unicité de la division euclidienne, le reste est nul.

Exemple 41

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

Solution :

On a $X^2 + 1 \neq 0$ donc $\exists!(Q, R) \in \mathbb{K}[X]^2 \mid P = (X^2 + 1)Q + R$ et $\deg(R) < 2$, donc $\exists a, b \in \mathbb{K} \mid R = aX + b$.
Alors $(\sin\theta X + \cos\theta)^n = (X^2 + 1)Q + aX + b$, et en évaluant en i : $e^{in\theta} = ai + b$.
Par unicité, $a = \sin(n\theta)$ et $b = \cos(n\theta)$, donc $R = \sin(n\theta)X + \cos(\theta)$.
Ainsi, $R = 0 \iff \sin(n\theta) = \cos(n\theta) = 0$, impossible car $\cos^2(n\theta) + \sin^2(n\theta) = 1$. Donc $R \neq 0$.

2.2 Racines et divisibilité.

Définition 42: bis.

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 $P(\alpha) = 0$.

Théorème 43: Racine et divisibilité par un polynôme de degré 1. ★

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

$$P(\alpha) = 0 \iff X - \alpha \mid P.$$

Preuve :

$\boxed{\Longrightarrow}$ Supposons $P(\alpha) = 0$. On a $\exists!(Q, R) \in \mathbb{K}[X]^2 \mid P = (X - \alpha)Q + R$ et $\deg(R) < \deg(X - a)$.
Donc R est constant : $\exists \lambda \in \mathbb{K} \mid R = \lambda \cdot 1_{\mathbb{K}[X]}$ donc $P = (X - \alpha)Q + \lambda$.
Évaluons en α : $P(\alpha) = \lambda = 0$ donc $\lambda = 0$ donc $R = 0$ et $(X - \alpha) \mid P$.
$\boxed{\Longleftarrow}$ Supposons que $X - \alpha \mid P$: $\exists Q \in \mathbb{K}[X] \mid P = (X - \alpha)Q$. Alors $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$.

Proposition 44

Soit $P \in \mathbb{K}[X]$ et $p \in \mathbb{N}^*$ et $\alpha_1, ..., \alpha_p \in \mathbb{K}$ deux-à-deux distincts.

$$\alpha_1, ..., \alpha_p \text{ sont racines de } P \iff \exists Q \in \mathbb{K}[X] \mid P = Q \prod_{k=1}^{p} (X - \alpha_k).$$

Preuve :

$\boxed{\Longleftarrow}$ Trivial.
$\boxed{\Longrightarrow}$ Supposons que $\alpha_1, ..., \alpha_p$ sont racines de P.
En particulier, α_1 est racine de P donc $X - \alpha_i \mid P$ donc $\exists Q_1 \in \mathbb{K}[X] \mid P = (X - \alpha_1)Q_1$.
Évaluons en α_2 : $P(\alpha_2) = (\alpha_2 - \alpha_1)Q_1(\alpha_2) = 0$ or $\alpha_2 \neq a_1$ donc $Q_1(\alpha_2) = 0$ donc $X - \alpha_2 \mid Q$.
Ainsi, $\exists Q_2 \in \mathbb{K}[X] \mid Q_1 = (X - \alpha_2)Q_2$, puis $P = (X - \alpha_1)(X - \alpha_2)Q_2$, on itère...
On a alors $\exists Q_p \in \mathbb{K}[X] \mid P = (X - \alpha_1)(X - \alpha_2)...(X - \alpha_p)Q_p$.

Exemple 45

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

Solution :

On sait que $X^2 + X + 1 = (X - j)(X - \overline{j})$. Vérifions que $j, \overline{j}$ sont racines de P.
On a $P(j) = j^{3p+2} + j^{3q+1} + j^{3r} = j^2 + j + 1 = 0$; $P(\overline{j}) = \overline{j}^{3p+2} + \overline{j}^{3q+1} + \overline{j}^{3r} = \overline{j^{3p+2} + j^{3q+1} + j^{3r}} = \overline{0} = 0$.
Donc $j, \overline{j}$ sont racines distinctes de P, donc $(X - j)(X - \overline{j}) \mid P$ dans $\mathbb{C}[X]$.
Donc $\exists Q \in \mathbb{C}[X] \mid P = (X^2 + X + 1)Q$.

Définition 46

Soit $P \in \mathbb{K}[X]$. On dit que P est **scindé** sur $\mathbb{K}$ s'il s'écrit comme produit de polynômes de degré 1.

Corrolaire 47

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

$$\exists \lambda \in \mathbb{K}^* \mid P = \lambda \prod_{i=1}^{n} (X - \alpha_i), \quad (\lambda = \mathrm{cd}(P)).$$

Preuve :

On a $\exists Q \in \mathbb{K}[X] \mid P = Q \prod_{i=1}^{n} (X - \alpha_i)$.
Ainsi, $\deg(P) = \deg(Q) + n$ donc $\deg(Q) = 0$ donc $\exists \lambda \in \mathbb{K}^* \mid Q = \lambda \cdot 1_{\mathbb{K}[X]}$.

2.3 Racines et rigidité des polynômes.

Théorème 48

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

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

Preuve :

$\boxed{1.}$ Supposons $P \neq 0$ et possède p racines $\alpha_1, ..., \alpha_p$ distinctes.
Alors $\exists Q \in \mathbb{K}[X] \mid P = Q \prod_{i=1}^{p} (X - \alpha_i)$. Or $P \neq 0$ donc $\deg(\prod(X - \alpha_i)) \leq \deg(P)$ donc $p \leq \deg(P)$.
$\boxed{2.}$ Contraposée.
$\boxed{3.}$ Conséquence de 2.

Corrolaire 49: 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 $\mathbb{K}$, alors $P = Q$.
En particulier, lorsque les fonctions polynomiales associées à P et Q sont égales, $P = Q$.

Preuve :

On a $P - Q \in \mathbb{K}[X]$. D'après le théorème, si $P - Q$ a $n + 1$ racines, alors $P - Q = 0$.

Exemple 50

Trouver tous les polynômes P de $\mathbb{R}[X]$ tels que $\forall n \in \mathbb{N},\ P(n) = n^{666}$.

Solution :

Soit $P \in \mathbb{R}[X] \mid \forall n \in \mathbb{N},\ P(n) = n^{666}$. Alors $\forall n \in \mathbb{N},\ (P - X^{666})(n) = 0$.
Ainsi, $P - X^{666}$ a une infinité de racines, dont $P = X^{666}$.

Exemple 51: Factorisation des polynômes de Tchebychev.

Reprenons la suite $(T_n)_{n\in\mathbb{N}}$ définie par $T_0 = 1$, $T_1 = X$ et $\forall n \in \mathbb{N},\ T_{n+2} = 2XT_{n+1} - T_n$.

Nous avons démontré que pour tout $n \in \mathbb{N}^*$, T_n est de degré n, de coefficient dominant 2^{n-1} et que pour tout θ réel, $T_n(\cos\theta) = \cos(n\theta)$.

1. Démontrer que T_n est l'unique polynôme de $\mathbb{R}[X]$ tel que $\forall\theta \in \mathbb{R},\ T_n(\cos\theta) = \cos(n\theta)$.
2. Démontrer que pour tout $n \in \mathbb{N}^*$,

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

Solution :

$\boxed{1.}$ Soit $n \in \mathbb{N}$. Soit $\widetilde{T_n} \in \mathbb{R}[X] \mid \forall\theta \in \mathbb{R},\ \widetilde{T_n}(\cos(\theta)) = \cos(n\theta)$.
Alors $\forall\theta \in \mathbb{R}$, $(T_n - \widetilde{T_n})(\cos\theta) = 0$. donc $T_n - \widetilde{T_n}$ possède une infinité de racines d'où $T_n = \widetilde{T_n}$.
$\boxed{2.}$ Soient $n \in \mathbb{N}$ et $\theta \in \mathbb{R}$.

$$\cos(n\theta) = 0 \iff n\theta \equiv \frac{\pi}{2}[\pi] \iff \exists k \in \mathbb{Z} \mid n\theta = \frac{\pi}{2} + k\pi.$$

Donc pour $k \in \mathbb{Z}$, $\theta_k = \frac{\pi}{2n} + \frac{k\pi}{n}$ et $\forall k \in \mathbb{Z},\ T_n(\cos(\theta_k)) = 0$.
On a que les nombres $\cos\theta_k$ avec $k \in [\![0, n-1]\!]$ sont distincts par stricte décroissance de cos sur $[0,\pi]$.
On a donc n racines donc T_n est scindé et :

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

2.4 Multiplicité d'une racine.

Définition 52

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

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

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 53: ★

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. $\exists Q \in \mathbb{K}[X] \mid P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$.

Preuve :

$\boxed{\Longrightarrow}$ Supposons que $(X-\alpha)^m \mid P$ et $(X-\alpha)^{m+1} \nmid P$: $\exists Q \in \mathbb{K}[X] \mid P = (X-\alpha)^m Q$.
Par l'absurde, on suppose que $Q(\alpha) = 0$. Alors $X-\alpha \mid Q$ donc $\exists\widetilde{Q} \in \mathbb{K}[X] \mid Q = (X-\alpha)\widetilde{Q}$ donc $P = (X-\alpha)^{m+1}\widetilde{Q}$.
C'est absurde, donc $Q(\alpha) \neq 0$.
$\boxed{\Longleftarrow}$ Supposons que $\exists Q \in \mathbb{K}[X] \mid P = (X-\alpha)^m Q$ et $Q(\alpha) \neq 0$.
Supposons que $(X-\alpha)^{m+1}$ divise P : $\exists\widetilde{Q} \in \mathbb{K}[X] \mid P = (X-\alpha)^{m+1}\widetilde{Q}$.
Alors $(X-\alpha)^m Q = (X-\alpha)^{m+1}\widetilde{Q}$ donc $Q = (X-\alpha)\widetilde{Q}$ par intégrité de $\mathbb{K}[X]$.
On évalue en α : $Q(\alpha) = 0$, absurde donc $(X-\alpha)^{m+1} \nmid P$.

Lemme 54

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

Preuve :

Supposons que $(X-\alpha)^k \mid P$: $\exists Q \in \mathbb{K}[X] \mid P = (X-\alpha)^k Q$.
Alors $P' = k(X-\alpha)^{k-1}Q + (X-\alpha)^k Q' = (X-\alpha)^{k-1}(kQ + (X-\alpha)Q')$.

Théorème 55: Caractérisation de la multiplicité.

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

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

Preuve :

• Supposons α de multiplicité au moins m.
Alors $(X-\alpha)^m \mid P$ donc $(X-\alpha)^{m-1} \mid P', ..., (X-\alpha)^1 \mid P^{(m-1)}$.
• Supposons $P(\alpha) = P'(\alpha) = ... = P^{(m-1)}(\alpha) = 0$.
Taylor : $P = ... = (X-\alpha)^m \sum_{k=m}^{n} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^{k-m}$.
Alors $(X-\alpha)^m \mid P$ donc (3) $\iff$ (4).
• Notons p la multiplicité de α :

$$\begin{aligned} p = m &\iff p \geq m \text{ et } \neg(p \geq m+1) \\ &\iff P(\alpha) = P'(\alpha) = ... = P^{(m-1)}(\alpha) = 0 \text{ et } \neg(P(\alpha) = P'(\alpha) = ... = P^{(m)}(\alpha) = 0) \\ &\iff P(\alpha) = P'(\alpha) = ... = P^{(m-1)}(\alpha) = 0 \text{ et } P^{(m)}(\alpha) \neq 0 \end{aligned}$$

Donc (1) $\iff$ (2).

Exemple 56

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

Solution :

On a $P(-1) = 0$, $P' = 4X^3 + 3X^2 - 14X - 13$ et $P'(-1) = 0$, $P'' = 12X^2 + 6X - 14$ et $P''(-1) = -8$.
Alors -1 est racine de multiplicité 2 par théorème.
Donc $P = (X+1)^2(X^2 - X - 6) = (X + 1^2)(X+2)(X-3)$.

Corrolaire 57

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

$$\alpha \text{ est racine simple de } P \iff P(\alpha) = 0 \text{ et } P'(\alpha) \neq 0.$$

Proposition 58

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

Corrolaire 59

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

1. Si $P \neq 0$ et $P \in \mathbb{K}_n[X]$, alors P admet au plus n racines comptées avec leurs multiplicité.
2. Si $P \in \mathbb{K}_n[X]$ et P admet au moins $n+1$ racines comptées avec leur mulitplicité, alors $P = 0$.

Corrolaire 60: 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 $\alpha_1, ..., \alpha_p$ dans $\mathbb{K}$, de multiplicités $m_1, ..., m_p$ et si $m_1 + ... + m_p = n$, alors P est scindé sur $\mathbb{K}$.

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

Théorème 61: de d'Alembert-Gauss, ou théorème fondamental de l'algèbre (admis).

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

Exemple 62

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

Solution :

Soit $\omega \in \mathbb{C}$. D'après d'Alembert-Gaus, $P - \omega$ admet une racine complexe, donc $\exists \alpha \in \mathbb{C} \mid P(\alpha) = \omega$.

Proposition 63: une racine réelle.

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

Preuve :

On a $\widetilde{P} : x \mapsto P(x)$ est continue et change de signe donc $\exists c \in \mathbb{R} \mid \widetilde{P}(c) = 0$ par TVI.

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

Proposition 64

Soit $P \in \mathbb{K}[X]$ non constant.
Il est irréductible dans $\mathbb{K}[X]$ si ses seuls diviseurs sont constants ou associés à P.

Proposition 65

Un polynôme P est irréductible ssi ses diviseurs sont de degré 0 ou $\deg P$ et que P est non constant.

Preuve :

Soit $P \in \mathbb{K}[X] \setminus \mathbb{K}_0[X]$.
$\boxed{\Longrightarrow}$ Supposons P irréductible. Soit Q un diviseur de P.
— Si Q est constant, alors $\deg(Q) = 0$.
— Si $\exists \lambda \in \mathbb{K}^* \mid Q = \lambda P$, alors $\deg(Q) = \deg(P)$.
$\boxed{\Longleftarrow}$ Supposons que les diviseurs de P sont de degré 0 ou $\deg P$. Soit Q un diviseur de P.
— Si $\deg Q = 0$, alors Q est constant non nul.
— Si $\deg Q = \deg P$, alors $\exists \widetilde{Q} \in \mathbb{K}_0[X] \mid P = Q\widetilde{Q}$.
Donc $\exists \lambda \in \mathbb{K}^* \mid \widetilde{Q} = \lambda \cdot 1_{\mathbb{K}[X]}$ donc $P = \lambda Q$.

Proposition 66

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

Preuve :

$\boxed{\Longleftarrow}$ Soit $P \in \mathbb{C}[X]$ de degré 1. Ses diviseurs sont de degré 0 ou $1 = \deg(P)$ donc P irréductible.
$\boxed{\Longrightarrow}$ Supposons P irréductible et non constant. Alors il admet une racine $\alpha \in \mathbb{C}$ et $(X - \alpha) \mid P$.
Or P est irréductible donc $\deg(P) = \deg(X - \alpha) = 1$.

Proposition 67: 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 $P \in \mathbb{C}[X]$, il existe $\lambda \in \mathbb{C}$, $p \in \mathbb{N}^*$, $\alpha_1, ..., \alpha_p \in \mathbb{C}$ deux-à-deux distincts et $m_1, ..., m_p \in \mathbb{N}^*$ tels que

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

Preuve :

Soit $P \in \mathbb{C}[X]$. D'après d'Alembert-Gauss, P a une racine α_1 dont on note m_1 la multiplicité.
Alors $\exists Q \in \mathbb{C}[X] \mid P = (X - \alpha_1)^{m_1} Q$ et $Q(\alpha_1) \neq 0$.
Si Q est constant, on s'arrête, sinon Q a une racine $\alpha_2 \neq \alpha_1$...

Lemme 68

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 $\overline{a}$ aussi et B_α^m divise P dans $\mathbb{R}[X]$.

Preuve :

Notons $P \sum^n a_k X^k$ où $n \in \mathbb{N}$ et $a_0, ..., a_n \in \mathbb{R}$. Supposons $P(\alpha) = 0$.

$$P(\overline{\alpha}) = \sum_{k=0}^{n} a_k \overline{\alpha}^k = \sum_{k=0}^{n} \overline{a_k \alpha^k} = \overline{P(\alpha)} = 0.$$

Puisque $\alpha \notin \mathbb{R}$, $(X - \alpha)(X - \overline{\alpha}) \mid P$ dans $\mathbb{C}[X]$: $\exists Q \in \mathbb{C}[X] \mid P = (X - \alpha)(X - \widetilde{\alpha})Q$.
On note $B_\alpha = (X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha} = X^2 + 2\mathrm{Re}(\alpha)X + |\alpha|^2$. Donc $P = B_\alpha Q$.
On a $B_\alpha \neq 0$. Donc $\exists!(\widetilde{Q}, R) \in \mathbb{R}[X]^2 \mid P = B_\alpha \widetilde{Q} + R$ et $\deg(R) < \deg(B_\alpha)$.
C'est aussi la division euclidienne de P par B_α sur $\mathbb{C}[X]$, mais $P = B_\alpha Q + 0$ avec $\deg(0) < \deg(B_\alpha)$.
Par unicité de la division euclidienne, $R = 0$ et $Q = \widetilde{Q}$.

Proposition 69

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

Preuve :

$\boxed{\Longleftarrow}$ Soit $P \in \mathbb{R}_2[X]$.
— Si P de degré 1, alors irréductible.
— Si P de degré 2 sans racines réelles, on prend Q diviseur de P, alors $\deg(Q) \leq 2$.
On a $\deg(Q) \neq 1$ car sinon Q a une racine réelle, donc $\deg Q = 0$ ou $\deg(P)$ donc P irréductible.
$\boxed{\Longrightarrow}$ Supposons P irréductible non constant. On a $P \in \mathbb{C}[X]$ donc il admet une racine $\alpha \in \mathbb{C}$.
— Si $\alpha \in \mathbb{R}$, alors $X - \alpha \mid P$ donc P est irréductible car $\deg(P) = \deg(X - \alpha) = 1$.
— Si $\alpha \notin \mathbb{R}$, alors $\overline{\alpha}$ est racine de P dont $B_\alpha = (X - \alpha)(X - \overline{\alpha}) \in \mathbb{R}[X]$ divise P.
Or P est irréductible donc $\deg(B_\alpha) = \deg(P) = 2$. P est sans racine réelle, il aurait sinon un diviseur de degré 1.

Proposition 70: Factorisation en produit d'irréductibles à coeff. dans $\mathbb{R}$.

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

Méthode : Factorisation d'un polynôme en produit d'irréductibles.

- Renseignements utiles : le degré de P et son coefficient dominant.
- 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 $\mathbb{C}[X]$.
- 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 68. On obtient une factorisation dans $\mathbb{R}[X]$.

Exemple 71: ★

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

Solution :

On a

$$\begin{aligned} X^6-1 &= (X+1)(X-1)(X-j)(X-j^2)(X+j)(X+j^2) \\ &= (X-1)(X+1)(X^2-X+1)(X^2+X+1) \end{aligned}$$

3 Compléments.

3.1 Relations coefficients-racines pour un polynôme scindé.

Définition 72

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

$$\forall k \in [\![1, n]\!],\ \sigma_k = \sum_{i_1<i_2<...<i_k} x_{i_1}x_{i_2}...x_{i_k}.$$

On a notamment

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

Exemple 73

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

$$x^2+y^2+z^2 = \sigma_1^2 - 2\sigma_2$$

$$x^3+y^3+z^3 = \sigma_1^3 + 3\sigma_3 - 3\sigma_1\sigma_2$$

Solution :

On a:

$$\sigma_1^2 - 2\sigma_2 = x^2 + \cancel{xy+xz+yx} + y^2 + \cancel{yz+zx+zy} + z^2 - \cancel{2xy-2xz-2yz} = x^2+y^2+z^2.$$

Proposition 74: 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 $a_0, ..., a_n$ sont ses coefficients et $\alpha_1, ..., \alpha_n$ ses racines, répétées avec leur multiplicité. On a

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

avec $\sigma_1, ..., \sigma_n$ les fonctions symétriques élémentaires des racines $\alpha_1, ..., \alpha_n$.
Ces nombres s'expriment donc en fonction des coefficients de P :

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

En particulier, pour la somme des racines σ_1 et le produit des racines σ_n,

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

Preuve :

En colle : savoir énoncer la proposition, et la prouver dans le cas $n = 3$.
Soit $P = \lambda(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ avec $\lambda \in \mathbb{K}$. On a:

$$\begin{aligned} P &= \lambda(X^3 + (-\alpha_1-\alpha_2-\alpha_3)X^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)X - \alpha_1\alpha_2\alpha_3) \\ &= \lambda(X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3). \end{aligned}$$

Exemple 75

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

$$x+y+z = 2; \quad x^2+y^2+z^2 = 14; \quad x^3+y^3+z^3 = 20.$$

Solution :

On a:

$$\begin{aligned} (x,y,z) \text{ solution } &\iff \begin{cases} \sigma_1 = 2 \\ \sigma_1^2 - 2\sigma_2 = 14 \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 20 \end{cases} \iff \begin{cases} \sigma_1 = 2 \\ \sigma_2 = -5 \\ \sigma_3 = -6 \end{cases} \\ &\iff (X^3 - 2X^2 + (-5)X - (-6)) \text{ a pour racines } x, y, z \\ &\iff (X^2 - X - 6)(X-1) \text{ a pour racines } x, y, z \\ &\iff (x, y, z) \text{ est une permutation de } (1, -2, 3). \end{aligned}$$

3.2 Interpolation de Lagrange.

Définition 76

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

$$\forall i \in [\![1, n]\!], , \ L_i = \prod_{k=1 k \neq i}^{n} \frac{X - x_k}{x_i - x_k}$$

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

Exemple 77

Écrire la famille des quatre polynômes de Lagrage associés à $(-1, 0, 1, 2)$.

Proposition 78

Soit $n \in \mathbb{N}^*$ et $(L_1, ..., L_n)$ la famille de polynômes de Lagrange associés à un n-uplet $(x_1, ..., x_n)$ de scalaires deux-à-deux distincts.
Tous les polynômes L_i sont de degré $n-1$. De plus, $\forall (i, j) \in [\![1, n]\!]^2, \ L_i(x_j) = \delta_{i,j}$.

Théorème 79: ★

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

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

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

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

Preuve :

Existence. Soit $P \sum_{i=1}^{n} y_i L_i$. On a $\deg(P) \leq n-1$ car les $L_i \in \mathbb{K}_{n-1}[X]$ sont stables par combinaisons linéaires.
Soit $k \in [\![1, n]\!]$. $P(x_k) = \sum_{i=1}^{n} y_i L_i(x_k) = y_k L_k(x_k) = y_k$.

Unicité. Soient $P, Q \in \mathbb{K}_{n-1}[X]$ tels que $\forall i \in [\![1, n]\!], \ P(x_i) = y_i = Q(x_i)$.
Alors $P - Q$ a n racines, donc $P - Q = 0$ donc $P = Q$.

Corrolaire 80: L'ensemble des polynômes interpolateurs.

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

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

Preuve :

On a:

$$\begin{aligned} \forall i \in [\![1, n]\!], \ Q(x_i) = y_i = P(x_i) &\iff Q - P \text{ a } x_1, ..., x_n \text{ pour racines} \\ &\iff \prod_{i=1}^{n} (X - x_i) \mid Q - P \\ &\iff \exists A \in \mathbb{K}[X], \ Q = P + A \prod_{i=1}^{n} (X - x_i) \end{aligned}$$

4 Exercices. ★

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

Exercice 1: ♦♦♢ ★

On note $I =]-\frac{\pi}{2}, \frac{\pi}{2}[$.

1. Montrer que pour tout $n \in \mathbb{N}$, il existe un polynome $P_n \in \mathbb{R}[X]$ tel que
$$\forall x \in I,\ \tan^{(n)}(x) = P_n(\tan(x)).$$
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.

Solution :

$\boxed{★}$ Soit $x \in I$. Pour $n \in \mathbb{N}$, on note l'énoncé H_n. Montrons le par récurrence.
Initialisation. C'est vrai pour $n = 0$: $\forall x \in I,\ \tan(x) = X(\tan(x))$.
Hérédité. Soit $n \in \mathbb{N}$ tel que H_n. On a $\tan^{(n+1)}(x) = (1+\tan^2(x))P_n'(\tan(x))$ donc $P_{n+1} = (1+X^2)P_n'$
Alors H_{n+1} est vraie et $\forall n \in \mathbb{N}, H_n$ par récurrence.
$\boxed{2.}$ Supposons qu'il en existe un autre, Q_n, on a $\forall x \in I, P_n(\tan x) - Q_n(\tan x) = 0$ donc $P_n = Q_n$.
$\boxed{3.}$ Pour $n \in \mathbb{N}$, on note H_n: «$\deg(P_n) = n+1$, $\mathrm{cd}(P_n) = n!$».
Initialisation. Triviale.
Hérédité. Soit $n \in \mathbb{N}$ tel que H_n.
On a $P_{n+1} = (1+X^2)P_n'$ donc $\deg(P_{n+1}) = \deg(P_n) - 1 + 2 = n+1$ car $\deg(P_n) \geq 0$.
On a $\mathrm{cd}(P_{n+1}) = \mathrm{cd}(P_n') = (n+1)\cdot \mathrm{cd}(P_n) = (n+1)!$
Alors H_{n+1} est vraie et $\forall n \in \mathbb{N}, H_n$ par récurrence.
$\boxed{4.}$ Pour $n \in \mathbb{N}$, on note l'énoncé H_n.
Initialisation. Triviale.
Hérédité. Soit $n \in \mathbb{N}$ tel que H_n. On note $(\alpha_k)_{k\in\mathbb{N}}$ les coefficients de P_n, entiers.

$$P_{n+1} = (1+X^2)P_n' = (1+X^2)\sum_{k=0}^{n}(k+1)\alpha_{k+1}X^k = \sum_{k=0}^{n}(k+1)\alpha_{k+1}X^k + \sum_{k=2}^{n+2}(k-1)\alpha_{k-1}X^k$$

Les coefficients de P_{n+1} sont donc des sommes et produits d'entiers, donc sont des entiers.
Par récurrence, $\forall n \in \mathbb{N},\ H_n$ est vrai.

Exercice 2: ♦♢♢

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

Solution :

D'une part

$$\begin{aligned}(1-X^2)^n = (1-X)^n(1+X)^n &= \sum_{i=0}^{n}\binom{n}{i}(-1)^i X^i \sum_{j=0}\binom{n}{j}X^j \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n}\binom{n}{i}\binom{n}{j}(-1)^i X^{i+j}\end{aligned}$$

Donc le coefficient devant X^n est $\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}(-1)^i$.
D'autre part, $(1-X^2)^n = \sum_{i=0}^{n}\binom{n}{i}(-1)^i X^{2i}$. Donc si n est impair, le coefficient devant X^n est nul.
Si n est pair, il est $\binom{n}{n/2}(-1)^{n/2}$.
On en déduit l'identité:
$$\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i}(-1)^i = \binom{n}{n/2}(-1)^{n/2}$$

Exercice 3: ♦♦♢

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

Solution :

Soit P un tel polynôme on suppose P non constant.
On a $\deg(P) = 2\cdot(\deg(P)-1)$ donc $\deg(P) = 2\deg(P) - 2$ donc $\deg(P) = 2$.
Alors $\exists (a,b,c) \in \mathbb{R}^* \times \mathbb{R}^2 \mid P = aX^2 + bX + c$.
Donc $4a^2X^2 + 4abX + b^2 = 4aX^2 + 4bX + 4c$ donc $4a^2 = 4a$, $ab = b$ et $b^2 = 4c$.
Alors $a = 1$, $b \in \mathbb{R}$ et $c = \frac{b^2}{4}$.
Les solutions sont donc dans $\{0\} \cup \{X^2 + bX + \frac{b^2}{4} \mid b \in \mathbb{R}\}$.

Exercice 4: ♦♦♢

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

Solution :

Soit $P \neq 0$ un tel polynôme. On pose $n = \deg(P)$. On note $P = \sum a_k X^k$.
Analyse. On a $P(X+1) = \sum_{k=0}^{n} a_k(X+1)^k \overset{\text{hyp.}}{=} \sum_{k=0}^{n-1}(k+1)a_{k+1}X^{k+1} = \sum_{k=1}^{n} k a_k X^k$.
Donc $a_n = n a_n$ donc $n = 0$ ou $n = 1$ car $a_n \neq 0$.
On vérifie facilement que les polynômes constants ne sont pas solution, donc $n = 1$.
Notons $P = aX + b$. On a $aX + a + b = aX$ donc $a + b = 0$.
Synthèse. Soit un polynôme $P = aX + b$ tels que $a + b = 0$. Alors $P(X+1) = aX + a + b = aX = XP'$.

Exercice 5: ♦♦♦

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

Solution :

Soient A, B deux solutions de l'équation. On a $A - A' = B - B' = Q$.
Alors $A - B = A' - B'$ donc $(A - B) = (A - B)'$ donc $\deg(A - B) = \deg(A - B) - 1$.
Cela est uniquement possible si $A - B = 0$. Donc $A = B$.

Racines et factorisation d'un polynôme.

Exercice 6: ♦♦♢ Approximation de π par $\frac{22}{7}$.

1. Poser la division euclidienne de $X^4(1 - X)^4$ par $X^2 + 1$.
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 $\frac{1}{1260} \leq \frac{22}{7} - \pi \leq \frac{1}{630}$.

Solution :

$\boxed{1.}$ On a $X^4(1 - X)^4 = (X - X^2)^4 = X^8 - 4X^7 + 6X^6 - 4X^5 + X^4$.
Alors $X^4(1 - X)^4 = (X^2 + 1)(X^6 - 4X^5 + 5X^4 - 4X^2 + 4) - 4$.
$\boxed{2.}$

$$\begin{aligned}\int_0^1 \frac{x^4(1-x)^4}{1+x^2}\mathrm{d}x &= \int_0^1 (x^6 - 4x^5 + 5x^4 - 4x^2 + 4)\mathrm{d}x - 4\int_0^1 \frac{1}{x^2+1}\mathrm{d}x \\ &= \left[\frac{x^7}{7} - \frac{4x^6}{6} + x^5 - \frac{4x^3}{3} + 4x\right]_0^1 - 4\left[\arctan(x)\right]_0^1 \\ &= \frac{1}{7} - \frac{4}{6} + 1 - \frac{4}{3} + 4 - \pi = \frac{22}{7} - \pi.\end{aligned}$$

$\boxed{3.}$ $\forall x \in [0, 1]$, $\frac{1}{2} \leq \frac{1}{x^2+1} \leq 1$. De plus, $\frac{1}{2}\int_0^1 x^4(1 - x)^4\mathrm{d}x = \frac{1}{1260}$ et $\int_0^1 x^4(1 - x)\mathrm{d}x = \frac{1}{630}$.
Donc $\frac{1}{1260} \leq \frac{22}{7} - \pi \leq \frac{1}{630}$.

Exercice 7: ♦♦♢

Donner le reste dans la division euclidienne de $X^{2023} + X^3 + 1$ par
a) $X^2 - 1$, b) $(X - 1)^2$.

Solution :

$\boxed{a)}$ $\exists Q \in \mathbb{C}[X] \mid X^{2023} + X^3 + 1 = (X^2 - 1)Q + aX + b$ avec $a, b \in \mathbb{C}$.
En évaluant en 1 et -1 : $3 = a + b$ et $-1 = b - a$ donc $(a, b) = (2, 1)$. Le reste est $2X + 1$.
$\boxed{b)}$ $\exists Q \in \mathbb{C}[X] \mid X^{2023} + X^3 + 1 = (X - 1)^2Q + aX + b$ avec $a, b \in \mathbb{C}$.
La racine 1 est de multiplicité 2, c'est une racine du polynôme dérivé.
Ce polynôme dérivé est : $2023X^{2022} + 3X^2 = 2(X - 1)Q + (X - 1)^2Q' + a$.
On évalue en 1 les deux polynômes: $a + b = 3$ et $2026 = a$ donc $(a, b) = (2026, -2023)$. Le reste est $2026X - 2023$.

Exercice 8: ♦♦♢

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

Solution :

On a $\exists(Q, R) \in \mathbb{C}[X] \mid B = AQ + R$ donc $B \circ P = (A \circ P)(Q \circ P) + R \circ P$.
Or $A \circ P \mid B \circ P$ donc $R \circ P = 0$ car $\deg(R \circ P) < \deg(A \circ P)$. Or $\deg P > 0$ donc $R = 0$.
Ainsi, $B = AQ$ donc $A \mid B$.

Exercice 9: ♦♦♢

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

Solution :

Soit $P \in \mathbb{R}[X]$ tel que $(X + 4)P(X) = XP(X + 1)$.
On évalue en 0 : $4P(0) = 0$ donc 0 est racine. On en déduit que $-3, -2, -1, 0$ sont racines.
Alors $P = X(X + 1)(X + 2)(X + 3)\widetilde{P}$ avec $\widetilde{P} \in \mathbb{R}[X]$.
Ainsi, $X(X + 1)(X + 2)(X + 3)(X + 4)\widetilde{P}(X) = X(X + 2)(X + 3)(X + 4)(X + 5)\widetilde{P}(X + 1)$.
Donc $(X + 1)\widetilde{P}(X) = (X + 5)\widetilde{P}(X + 1)$ donc $\widetilde{P}(1) = 0$ donc $P(1) = 0$.
À partir de là, on peut montrer que tout entier naturel est racine de P. Donc $P = 0$.
Il n'y a que le polynôme nul qui est solution.

Exercice 10: ♦◇◇

Démontrer qu'il n'existe pas de polynôme P dans $\mathbb{R}[X]$ tel que

$$\forall n \in \mathbb{N},\ P(n) = n^{666} + (-1)^n.$$

Solution :

Soit $P \in \mathbb{R}[X]$. On suppose que $\forall n \in \mathbb{N},\ P(n) = n^{666} + (-1)^n$. Soit $n \in \mathbb{N}$.
On a $(P - X^{666})(n) = (-1)^n$ donc $P - X^{666}$ change de signe une infinité de fois.
Il a donc un nombre infini de racines par TVI, et donc c'est le polynôme nul. Ainsi $P = X^{666}$.
C'est absurde car $X^{666}(n) \neq n^{666} + (-1)^n$. Donc il n'existe pas de tel polynôme.

Exercice 11: ♦◇◇

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

Solution :

Soit α racine de P. On a $\alpha \neq 0$ car $P(0) = 1$.
On a $P' = \displaystyle\sum_{k=1}^{n} \frac{kX^{k-1}}{k!} = \sum_{k=0}^{n-1} \frac{X^k}{k!}$ donc $P'(\alpha) = P(\alpha) - \dfrac{\alpha^n}{n!} = -\dfrac{\alpha^n}{n!} \neq 0$ car $\alpha \neq 0$.
C'est donc une racine simple.

Exercice 12: ♦◇◇

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

Solution :

Montrons que 1 est racine triple de P_n.
• On a $P_n(1) = n - n - 2 + n + 2 - n = 0$.
• On a $P_n'(1) = n(n+2) - (n+1)(n+2) + (n+2) = 0$.
• On a $P_n''(1) = n(n+1)(n+2) - n(n+1)(n+2) = 0$.
C'est bien une racine de multiplicité 3, donc $(X-1)^3 \mid P_n$.

Factorisation de polynômes.

Exercice 13: ♦♦◇

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

Solution :

On a $X^6 + X^3 + 1 = (X^3)^2 + X^3 + 1$ donc z est solution ssi $z^3 \in \{j, j^2\}$.
• Si $z^3 = j$, alors $z^3 / \left(e^{\frac{2i\pi}{9}}\right)^3 = 1$ donc $z \in \{e^{\frac{2i\pi}{9}}, je^{\frac{2i\pi}{9}}, j^2 e^{\frac{2i\pi}{9}}\} = \{e^{\frac{2i\pi}{9}}, e^{\frac{8i\pi}{9}}, e^{\frac{14i\pi}{9}}\}$.
• Si $z^3 = j^2 = \bar{j}$, alors $z \in \{e^{-\frac{2i\pi}{9}}, e^{-\frac{8i\pi}{9}}, e^{-\frac{14i\pi}{9}}\}$. On va noter α, β, γ ces valeurs.
Alors $X^6 + X^3 + 1 = (X^2 - 2\mathrm{Re}(\alpha) + |\alpha|^2)(X^2 - 2\mathrm{Re}(\beta) + |\beta|^2)(X^2 - 2\mathrm{Re}(\gamma) + |\gamma|^2)$.

Exercice 14: ♦♦♦

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

Solution :

On a:

$$\begin{aligned} P_n &= \sum_{k=0}^{n} \binom{n}{k} X^{n-k} i^k - \sum_{k=0}^{n} \binom{n}{k} X^{n-k} (-i)^k = \sum_{k=0}^{n} \binom{n}{k} X^{n-k} \left(i^k - -(i)^k\right) \\ &= \sum_{k=1}^{n} \binom{n}{k} X^{n-k} \left(i^k - (-i)^k\right) \end{aligned}$$

Soit $z \in \mathbb{C}$, on a

$$\begin{aligned} (z+i)^n = (z-i)^n \text{ et } z \neq \pm i &\iff \left(\frac{z+i}{z-i}\right)^n = 1 \\ &\iff \exists k \in [\![1, n-1]\!],\ \frac{z+i}{z-i} = e^{\frac{2ik\pi}{n}} \\ &\iff \exists k \in [\![1, n-1]\!],\ z + i = e^{\frac{2ik\pi}{n}}(z - i) \\ &\iff \exists k \in [\![1, n-1]\!],\ z = -i \times \frac{1 + e^{\frac{2ik\pi}{n}}}{1 - e^{\frac{2ik\pi}{n}}} = -i \times \frac{e^{\frac{ik\pi}{n}} + e^{-\frac{ik\pi}{n}}}{e^{\frac{ik\pi}{n}} - e^{-\frac{ik\pi}{n}}} \\ &\iff \exists k \in [\![1, n-1]\!],\ z = -\mathrm{cotan}\left(\frac{k\pi}{n}\right) \end{aligned}$$

Or P_n est de degré $n-1$ et a $n-1$ racines distinctes et $\mathrm{cd}(P_n) = 2ni$, donc:

$$P_n = 2ni \prod_{i=1}^{n-1} \left(X + \mathrm{cotan}\left(\frac{k\pi}{n}\right)\right)$$

Exercice 15: ♦♦♦

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

Solution :

On a:

$$\sum_{k=0}^{n-1} X^k = \frac{X^n - 1}{X-1} = \prod_{k=1}^{n-1}\left(X - e^{\frac{2ik\pi}{n}}\right)$$

On évalue en 1.

$$\begin{aligned}\sum_{k=0}^{n-1} 1^k = n = \prod_{k=1}^{n-1}\left(1 - e^{\frac{2ik\pi}{n}}\right) &= \prod_{k=1}^{n-1} -e^{\frac{ik\pi}{n}} \prod_{k=1}^{n-1} 2i\sin\left(\frac{k\pi}{n}\right) \\ &= 2^{n-1} i^{n-1} (-1)^{n-1} \exp\left(\frac{i\pi}{n-1}\sum_{k=1}^{n-1} k\right)\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right) \\ &= 2^{n-1}\exp\left(2(n-1)i\pi\right)\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right) \\ &= 2^{n-1}\prod_{k=1}^{n-1}\sin\left(\frac{k\pi}{n}\right)\end{aligned}$$

Donc $\prod\limits_{k=1}^{n}\sin\left(\frac{k\pi}{n}\right) = \frac{n}{2^{n-1}}$.

Divers.

Exercice 16: ♦◊◊

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.

Solution :

On note $P = \sum_{k=0}^{n} a_k X^k$.
$\boxed{1.}$ Soient $(\alpha_1, ..., \alpha_n) \in \mathbb{R}^n$ les racines de P, ordonnées par ordre croissant.
On applique le théorème de Rolle sur les intervalles $[\alpha_i, \alpha_{i+1}]$ pour $i \in [\![1, n-1]\!]$.
On obtient qu'il existe $\beta_i \in]\alpha_i, \alpha_{i+1}[$ racine de P' pour tout $i \in [\![1, n-1]\!]$.
Alors P' est scindé à racines simples car les intervalles sont distincts.
$\boxed{2.}$ On a $\sum_{i=1}^{n} \alpha_n = -\frac{a_{n-1}}{a_n}$ donc la moyenne des α_i vaut $-\frac{a_{n-1}}{na_n}$.
De plus, $P' = \sum_{k=1}^{n} k a_k X^{k-1}$ donc $\sum_{i=1}^{n-1} \beta_i = -\frac{(n-1)a_{n-1}}{na_n}$ donc la moyenne des β_i vaut $-\frac{a_{n-1}}{na_n}$.
Les moyennes arithmétiques sont égales.

Exercice 17: ♦♦◊

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.

Solution :

Soit $n \in \mathbb{N}$. Notons $\mathcal{E}_n$ l'ensemble de ces polynômes. Soit $P \in \mathcal{E}_n$ de racines $\omega_1, ..., \omega_n \in \mathbb{C}$.

$$P = \left(X^n + \sum_{k=1}(-1)^n \sigma_k X^{n-k}\right) = \prod_{k=1}^{n}(X - \omega_k)$$

On a que $\forall k \in [\![1, n]\!],\ |\sigma_k| = \left|\sum\limits_{I \in \mathcal{P}_k([\![1,n]\!])} \prod\limits_{i \in I} \omega_i\right| \leq \sum\limits_{I \in \mathcal{P}_k([\![1,n]\!])} \prod\limits_{i \in I} 1 = \binom{n}{k}$.
Donc $|\mathcal{E}| \leq \sum\limits_{k=1}^{n} |\sigma_k| \leq \sum\limits_{k=1}^{n} \binom{n}{k} \leq 2^n - 1$. C'est un ensemble fini.

Exercice 18: ♦♦◊

Soit $n \in \mathbb{N}^*$ et $P = nX^n - \sum\limits_{k=0}^{n-1} X^k$.

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.

Solution :

$\boxed{1.}$ $P(1) = n - n = 0$. $P'(1) = n^2 - \frac{n(n-1)}{2} = \frac{n(n-1)}{2} \neq 0$.
$\boxed{2.}$ Soit $\omega \in \mathbb{C}$ racine de P. On a $P(0) = -1$ donc on peut supposer $\omega \notin \{0, 1\}$.

$$(X-1)P = (X-1)(nX^n - \sum_{k=0}^{n-1} X^k) = ... = nX^{n+1} - (n+1)X^n + 1.$$

Donc $(X-1)P' = n(n+1)(X^n - X^{n-1})$ et $(\omega - 1)P'(\omega) = \omega^{n-1} n(n+1)(\omega - 1) \neq 0$ car $\omega \notin \{0, 1\}$.
Donc $P'(\omega) \neq 0$ par intégrité de $\mathbb{C}[X]$, donc ω est racine simple de P.
$\boxed{3.}$ La somme des racines est $\frac{1}{n}$, le produit est $\frac{(-1)^n}{n}$.

Exercice 19: ♦♦♦

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

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

Solution :

$\boxed{1.}$ Le polynôme X^n est évident.
On pose L_j les polynômes de Lagrange associés à $(0, ..., n)$. On a $P = \sum_{i=0}^{n} i^n L_i$.

$$P = \sum_{i=0}^{n} i^n \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{X-j}{i-j} = \sum_{i=0}^{n} i^n (-1)^{n-i} \prod_{j=0}^{i-1} \frac{1}{i-k} \prod_{j=i+1}^{n} \frac{1}{k-i} \prod_{k\neq i} (X-k)$$

$\boxed{2.}$ Le coefficient dominant est 1. Ainsi:

$$\sum_{i=0}^{n} i^n (-1)^{n-i} \frac{1}{i!} \cdot \frac{1}{(n-i)!} = 1.$$

On multiplie par $n!$ des deux côtés :

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