

ALGÈBRE DES POLYNÔMES

Dans tout le chapitre, \mathbb{K} désigne \mathbb{R} ou \mathbb{C} .

I — Rappels de MPSI

1) Polynômes, indéterminée

Définitions (1)

Soit $(a_0, \dots, a_p) \in \mathbb{K}^{p+1}$.

- (1) : $P = \sum_{n=0}^p a_n X^n$ est un polynôme à une indéterminée à coefficients dans \mathbb{K} . **Notation** : $\mathbb{K}[X]$.
- (2) : Un monôme est un polynôme dont tous les coefficients sont nuls sauf un seul.
- (3) : Si $P \neq 0$, le degré de P est $\max\{n \in \mathbb{N} \mid a_n \neq 0\}$. **Notation** : $\deg P$. Par convention, $\deg 0 = -\infty$.
- (4) : On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg P \leq n\}$.
- (5) : Si $P \neq 0$, $a_{\deg P}$ est le coefficient dominant de P et si $a_{\deg P} = 1$, on dit que P est unitaire ou normalisé.
- (6) : Si $P \neq 0$, la valuation de P est $\min\{n \in \mathbb{N} \mid a_n \neq 0\}$. **Notation** : $\text{val } P$. Par convention, $\text{val } 0 = +\infty$.
- (7) : Un polynôme est pair (resp. impair) lorsque tous ses coefficients d'indices impairs (resp. pairs) sont nuls.

Remarques (2)

(1) : L'objet X s'appelle l'indéterminée du polynôme ; ce n'est ni un élément de \mathbb{K} ni une "variable". C'est un objet figé, comme le nombre entier π , le booléen "vrai", ou l'application \exp . Tout polynôme est donc un objet figé, mais n'est ni une application, ni même une expression.

On n'écrira pas "posons $X = 1$ " mais plutôt : "substituons 1 à X ".

(2) : Pour simplifier certaines notions, dans la suite, on considérera que si $P = \sum_{n=0}^p a_n X^n$, au delà de p , les coefficients a_n sont définis, mais tous nuls (on parle aussi de suite presque nulle ou nulle à partir d'un certain rang). On pourra dans ce cas écrire $P = \sum_{n=0}^{+\infty} a_n X^n$.

2) Opérations sur les polynômes

Lois de composition (3)

Soient $P = \sum_{n=0}^{+\infty} a_n X^n$ et $Q = \sum_{n=0}^{+\infty} b_n X^n$ deux éléments de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On définit trois lois sur $\mathbb{K}[X]$:

- (1) : L'addition : $P + Q = \sum_{n=0}^{+\infty} (a_n + b_n) X^n$.
- (2) : La multiplication : $PQ = \sum_{n=0}^{+\infty} (\sum_{k=0}^n a_k b_{n-k}) X^n = \sum_{n=0}^{+\infty} (\sum_{p+q=n} a_p b_q) X^n$, appelée produit de Cauchy.
- (3) : La loi dite externe : $\lambda P = \sum_{n=0}^{+\infty} (\lambda a_n) X^n$.

Rappel (4)

Soit $(P, Q) \in \mathbb{K}[X]^2$, alors $\deg(P + Q) \leq \max(\deg P, \deg Q)$ et $\deg(PQ) = \deg P + \deg Q$. Et donc si $P \neq 0$ et $Q \neq 0$, alors $PQ \neq 0$.

Théorème (5)

- (1) : L'addition et la multiplication sont deux l.c.i sur $\mathbb{K}[X]$, et $(\mathbb{K}[X], +, \times)$ est un anneau intègre.
- (2) : $(\mathbb{K}[X], +, \times, \cdot)$ est une \mathbb{K} -algèbre commutative.

Corps des fractions rationnelles (6)

- (1) : Puisque l'anneau $\mathbb{K}[X]$ est intègre, on peut définir le corps des fractions constituées de polynômes, appelé corps des fractions rationnelles. **Notation** : $\mathbb{K}(X)$.
- (2) : Soit $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X] \setminus \{0\}$. On appelle degré de la fraction rationnelle $\frac{A}{B}$ le nombre $\deg A - \deg B$. **Notation** : $\deg \frac{A}{B}$.

II — Arithmétique dans l'anneau des polynômes

1) Division euclidienne de polynômes

Définition - Théorème (7)

- (1) : Soit $(A, B) \in \mathbb{K}[X]^2$. On dit que B divise A lorsqu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$; B est un diviseur de A et A un multiple de B .
- (2) : Soit $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$. Alors il existe un unique couple $(Q, R) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ et $\deg R < \deg B$ (division euclidienne de A par B).
- (3) : Si $\frac{A}{B}$ désigne un élément de $\mathbb{K}(X)$, alors il existe un unique polynôme $E \in \mathbb{K}[X]$ (appelé partie entière de $\frac{A}{B}$) et une unique fraction rationnelle $G \in \mathbb{K}(X)$ (appelé partie polaire de $\frac{A}{B}$) tels que $\deg G < 0$ et $\frac{A}{B} = E + G$.

2) PGCD de polynômes

PGCD et algorithme d'Euclide (8)

- (1) : Si A et B sont deux polynômes non nuls, alors $A\mathbb{K}[X] + B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. Il existe donc $D \in \mathbb{K}[X]$ tel que $A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$. Un tel D est appelé un PGCD de A et de B .
- (2) : Soient A et B deux polynômes non nuls tels que $\deg A \geq \deg B$. On peut définir une suite de polynômes par divisions euclidiennes successives : $A = BQ_1 + R_1$, $B = R_1Q_2 + R_2, \dots, R_k = R_{k+1}Q_{k+2} + R_{k+2}$ pour tout $k \geq 1$. La suite $(\deg R_k)$ décroît. Le dernier reste non nul est un PGCD de A et B .
- (3) : Un tel polynôme D est un diviseur commun de A et B , le plus grand (à un facteur scalaire près) pour la relation d'ordre de divisibilité des polynômes et donc de plus grand degré aussi.

Le PGCD (9)

Sous les mêmes hypothèses, il existe un unique PGCD unitaire : on l'appelle **LE** PGCD de A et de B .

Définition - Théorème (10)

- (1) : Soient A et B deux polynômes non nuls. On dit que A et B sont premiers entre eux si leurs seuls diviseurs communs sont les polynômes constants (i.e. leurs PGCD sont les constantes).
- (2) : Soient A et B deux polynômes non nuls. Si D est un PGCD de A et de B , alors il existe $(U, V) \in \mathbb{K}[X]^2$ tels que $AU + BV = D$.
- (3) : **Théorème de Bézout** : soient A et B deux polynômes non nuls. Alors A et B sont premiers entre eux si et seulement s'il existe $(U, V) \in \mathbb{K}[X]^2$ tels que $AU + BV = 1$.
- (4) : Ce théorème peut être démontré à partir de l'algorithme d'Euclide ou bien avec le résultat sur le PGCD et les idéaux de $\mathbb{K}[X]$.

Corollaires (11)

- (1) : Soient A , B_1 et B_2 trois polynômes non nuls. Si A est premier avec B_1 et avec B_2 , alors A est premier avec B_1B_2 .
- (2) : Soient A et B deux polynômes non nuls. Si on divise A et B par un de leurs PGCD, on obtient deux polynômes premiers entre eux.

Théorème de Gauss (12)

- (1) : Soient A, B et C trois polynômes non nuls. Si A divise BC et si A et B sont premiers entre eux, alors A divise C .
- (2) : Corollaire : soient A, B et C trois polynômes non nuls. Si A et B divisent C et si A et B sont premiers entre eux, alors AB divise C .

3) PPCM de deux polynômes

Définition (13)

Si A et B sont deux polynômes non nuls, alors $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$. Il existe donc $M \in \mathbb{K}[X]$ tel que $M\mathbb{K}[X] = A\mathbb{K}[X] \cap B\mathbb{K}[X]$. Un tel M est appelé un PPCM de A et de B .

Théorème (14)

- (1) : Un tel polynôme est un multiple commun à A et B , le plus petit (à un scalaire près) pour la relation d'ordre de divisibilité des polynômes et donc de plus petit degré aussi.
- (2) : Soient A et B deux polynômes non nuls et D un PGCD de A et B . Alors le polynôme $\frac{AB}{D}$ est un PPCM de A et B .

4) Polynômes irréductibles

Définition - Remarque (15)

- (1) : Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible sur \mathbb{K} lorsqu'il est non constant et lorsque ses seuls diviseurs dans $\mathbb{K}[X]$ sont, à un scalaire multiplicatif près, 1 et lui-même.
- (2) : Exemple : Tout polynôme de degré 1 est irréductible.

Attention (16)

Le corps de base a une importance. Ainsi, $X^2 + 1$ est irréductible sur \mathbb{R} , mais pas sur \mathbb{C} .

Théorème (17)

- (1) : Soit $P, Q \in \mathbb{K}[X]$. Si P est irréductible et ne divise pas Q , alors P et Q sont premiers entre eux.
- (2) : Si un polynôme irréductible divise un produit de polynômes, il divise au moins un de ces polynômes.

5) Corps algébriquement clos

Définition - Théorème (18)

- (1) : Un corps \mathbb{K} est algébriquement clos lorsque tout polynôme non constant de $\mathbb{K}[X]$ admet au moins une racine dans \mathbb{K} .
- (2) : Un corps \mathbb{K} est algébriquement clos si et seulement si l'une des deux propositions suivantes est vraie :
- les seuls polynômes irréductibles à coefficients dans \mathbb{K} sont ceux de degré 1
 - tout polynôme de $\mathbb{K}[X]$ non constant est scindé sur \mathbb{K} .

6) Décomposition des polynômes de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$

Théorème de d'Alembert-Gauss (19)

- (1) : Le corps \mathbb{C} est algébriquement clos.
- (2) : Tout polynôme réel est scindé sur \mathbb{C} .
- (3) : Factorisation dans $\mathbb{C}[X]$: soit $P \in \mathbb{C}[X]$. On suppose que P est non constant et admet pour racines complexes a_1, \dots, a_p d'ordres respectifs $\alpha_1, \dots, \alpha_p$. Alors il existe $\lambda \in \mathbb{C}$ tel que $P = \lambda \prod_{j=1}^p (X - a_j)^{\alpha_j}$. Cette écriture est unique à l'ordre des facteurs près.

Théorème (20)

- (1) : Soit $P \in \mathbb{R}[X]$, $p \in \mathbb{N}^*$ et $a \in \mathbb{C}$. Alors a est racine d'ordre p exactement de P si et seulement si \bar{a} est racine d'ordre p exactement de P .
- (2) : Soit $P \in \mathbb{R}[X]$. Alors la parité de la somme des ordres de multiplicité des racines réelles de P est égale à la parité du degré de P .
- (3) : factorisation dans $\mathbb{R}[X]$: soit $P \in \mathbb{R}[X]$. On suppose que P est non constant et admet pour racines réelles a_1, \dots, a_p d'ordres respectifs $\alpha_1, \dots, \alpha_p$ et pour racines complexes non réelles $u_1 \pm iv_1, \dots, u_q \pm iv_q$ d'ordres respectifs β_1, \dots, β_q . Alors il existe $\lambda \in \mathbb{R}$ tel que $P = \lambda \prod_{j=1}^p (X - a_j)^{\alpha_j} \prod_{k=1}^q ((X - u_k)^2 + v_k^2)^{\beta_k}$. Cette écriture est unique à l'ordre des facteurs près.
- (4) : factorisation des polynômes réels bicarrés : soit $p, q \in \mathbb{R}$. On pose $P = X^4 + pX^2 + q$, $Q = X^2 + pX + q$ et $\Delta = p^2 - 4q$. On cherche à factoriser P dans $\mathbb{R}[X]$:
- Si $\Delta \geq 0$, on cherche les racines de Q et on avise suivant leurs signes.
 - Si $\Delta < 0$, alors $q > 0$ et $P = (X^2 + \sqrt{q})^2 - (2\sqrt{q} - p)X^2 = (X^2 - \sqrt{2\sqrt{q} - p}X + \sqrt{q})(X^2 + \sqrt{2\sqrt{q} - p}X + \sqrt{q})$.

Théorème : Polynômes irréductibles (21)

- (1) : Les polynômes irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.
- (2) : Les polynômes irréductibles de $\mathbb{R}[X]$ sont exactement les polynômes de degré 1 et ceux de degré 2 dépourvus de racines réelles.

III — Compléments sur les polynômes**1) Composition****Définition (22)**

Soit $(P, Q) \in \mathbb{K}[X]^2$. On suppose que $P = \sum_{n=0}^p a_n X^n$. On appelle composé des polynômes P et Q le polynôme $\sum_{n=0}^p a_n Q^n$, obtenu par substitution de Q , élément de la \mathbb{K} -algèbre $\mathbb{K}[X]$, à X .

Notation : $P(Q)$ ou encore $P \circ Q$.

Remarque : $P(X) = X(P) = P$.

2) Fonctions polynomiales**Définition (23)**

Soit $P \in \mathbb{K}[X]$. On suppose que $P = \sum_{n=0}^p a_n X^n$. Pour tout élément x de \mathbb{K} (considérée comme une \mathbb{K} -algèbre), on peut définir $P(x) = \sum_{n=0}^p a_n x^n$, par substitution de x à X . On appelle fonction polynomiale associée à P l'application $\mathbb{K} \rightarrow \mathbb{K}$; $x \mapsto P(x)$. **Notation** : \tilde{P} ou bien f_P .

Théorème (24)

(1) : L'application $\mathbb{K}[X] \rightarrow \mathbb{K}^{\mathbb{K}}$; $P \mapsto f_P$ est un morphisme d'algèbres.

(2) : Si \mathbb{K} est un corps général, ce morphisme n'est pas injectif. Cependant, dans le cadre du programme officiel ($\mathbb{K} = \mathbb{R}$ ou \mathbb{C}), il est injectif, ce qui se traduit par : l'égalité numérique implique l'égalité formelle. Par abus de notation, on pourra donc dans la suite utiliser P au lieu de \tilde{P} .

3) Dérivation et formule de Taylor**Définition (25)**

Soit $P \in \mathbb{K}[X]$. On suppose que $P = \sum_{n=0}^{+\infty} a_n X^n$. On appelle polynôme dérivé de P le polynôme $\sum_{n=1}^{+\infty} n a_n X^{n-1}$.

Notation : P' .

On définit récursivement, pour tout $k \in \mathbb{N}^*$, $P^{(k+1)} = (P^{(k)})'$. On convient que $P^{(0)} = P$.

Théorème (26)

Quelques propriétés de la dérivation formelle des polynômes :

- (1) : Il s'agit d'une application linéaire.
- (2) : Pour tout $(P, Q) \in \mathbb{K}[X]^2$, $(PQ)' = P'Q + PQ'$.
- (3) : Pour tout $P \in \mathbb{K}[X]$ et tout $k \in \mathbb{N}^*$, $(P^k)' = kP'P^{k-1}$.
- (4) : Pour tout $(P, Q) \in \mathbb{K}[X]^2$ et tout $k \in \mathbb{N}^*$, $(PQ)^{(k)} = \sum_{j=0}^k \binom{k}{j} P^{(j)} Q^{(k-j)}$.
- (5) : Pour tout $(P, Q) \in \mathbb{K}[X]^2$, $(P \circ Q)' = Q' \cdot P'(Q)$.
- (6) : Pour tout $P \in \mathbb{K}[X]$ et tout $a \in \mathbb{K}$, $(P(X+a))' = P'(X+a)$.
- (7) : Pour tout $P \in \mathbb{K}[X]$, $\tilde{P} \in \mathcal{D}(\mathbb{R}, \mathbb{K})$ et $(\tilde{P})' = P'$.

formule de Mac-Laurin (27)

Soit $P \in \mathbb{K}[X]$. Alors $P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(0)}{n!} X^n$.

Formule de Taylor (28)

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

Alors $P(X+a) = \sum_{n=0}^{+\infty} \frac{P^{(n)}(a)}{n!} X^n$ ou encore, $P = \sum_{n=0}^{+\infty} \frac{P^{(n)}(a)}{n!} (X-a)^n$.

4) Racines d'un polynôme**Définition - Théorème (29)**

- (1) : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est racine ou zéro du polynôme P lorsque P est divisible par $X - a$.
- (2) : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est racine de P si et seulement si $P(a) = 0$.
- (3) : Soit $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $a \in \mathbb{K}$. On dit que a est racine d'ordre p exactement du polynôme P lorsqu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^p Q$ et $Q(a) \neq 0$.
- (4) : caractérisations d'une racine d'ordre p Soit $P \in \mathbb{K}[X]$, $p \in \mathbb{N}^*$ et $a \in \mathbb{K}$. Alors a est racine d'ordre p exactement du polynôme P si et seulement si l'une des propositions suivantes est vérifiée :
 - P est divisible par $(X-a)^p$ sans l'être par $(X-a)^{p+1}$.
 - $P(a) = P'(a) = \dots = P^{(p-1)}(a) = 0$ et $P^{(p)}(a) \neq 0$.

5) Majoration du nombre de racines avec multiplicité**Théorème (30)**

- (1) : Soit $P \in \mathbb{K}[X]$. Alors P a pour racines distinctes a_1, \dots, a_r , d'ordres respectifs $\alpha_1, \dots, \alpha_r$ **au moins**, si et seulement s'il existe $Q \in \mathbb{K}[X]$ tel que $P = Q \prod_{j=1}^r (X - a_j)^{\alpha_j}$.
- (2) : Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Alors la somme des ordres de multiplicité des racines de P est inférieure ou égale au degré de P .
- (3) : Si $(P, Q) \in \mathbb{K}_n[X]^2$ coïncident en $n+1$ points (au moins) distincts, alors $P = Q$.
- (4) : Puisque $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} , l'application $\mathbb{K}[X] \rightarrow \mathbb{K}^{\mathbb{K}}$; $P \mapsto f_P$ est injective. Si on la corestreint à l'ensemble des fonctions polynomiales, c'est donc un isomorphisme.

IV — Exercices TD**Exercice 1 : Reste d'une division euclidienne**

Soit $(a, b) \in \mathbb{K}^2$ tels que $a \neq b$ et $P \in \mathbb{K}[X]$. Exprimer le reste de la division euclidienne de P par $(X-a)(X-b)$ en fonction de $P(a)$ et $P(b)$.

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

Exprimer le reste de la division euclidienne de P par $(X-a)^2$ en fonction de $P(a)$ et $P'(a)$.

Exercice 2 : Euclide

Soient $n, m \in \mathbb{N}^*$.

1. De la division euclidienne de n par m , déduire celle de $X^n - 1$ par $X^m - 1$.
2. Établir que

$$\text{pgcd}(X^n - 1, X^m - 1) = X^{\text{pgcd}(n,m)} - 1$$

Exercice 3 : Polynôme de degré impair

Montrer qu'un polynôme de degré impair admet au moins une racine réelle

Exercice 4 : Factorisation et relation coefficients-racines

Factoriser dans $\mathbb{C}[X]$ le polynôme $X^n - 1$. En déduire les valeurs de $\sum_{k=0}^{n-1} \exp\left(\frac{2ik\pi}{n}\right)$ et de $\prod_{k=0}^{n-1} \exp\left(\frac{2ik\pi}{n}\right)$.

Exercice 5 : Factorisation dans $\mathbb{R}[X]$

Factoriser dans $\mathbb{R}[X]$ les polynômes $X^4 - 1$ puis $X^5 - 1$.

Exercice 6 : Factorisation classique

Soient $a \in]0; \pi[$ et $n \in \mathbb{N}^*$. Factoriser dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ le polynôme $X^{2n} - 2 \cos(na)X^n + 1$

Exercice 7 : CNS de divisibilité

Déterminer une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que $X^2 + X + 1 \mid X^{2n} + X^n + 1$

Exercice 8 : Polynôme à racines simples

Montrer que le polynôme $P_n = \sum_{k=0}^n \frac{1}{k!} X^k$ est scindé dans $\mathbb{C}[X]$ à racines simples. Qu'en est-il dans $\mathbb{R}[X]$?

V — Encore un peu d'algèbre linéaire**Exercice 9 : Endomorphisme ?**

Soit $f : P \mapsto 5P - XP'$. L'application f est-elle un endomorphisme de $\mathbb{K}[X]$? de $\mathbb{K}_n[X]$ pour tout $n \in \mathbb{N}$? Déterminer un endomorphisme de $\mathbb{K}[X]$ qui ne soit pas un endomorphisme de $\mathbb{K}_n[X]$ pour aucun $n \in \mathbb{N}$.

Exercice 10 : Familles échelonnées

Montrer que toute suite de polynômes non nuls de degrés deux à deux distincts est libre.
Montrer que toute suite de polynômes non nuls de valuations deux à deux distinctes est libre.

Exercice 11 : Une base de $\mathbb{R}_n[X]$

$E = \mathbb{R}_n[X]$. Pour $0 \leq k \leq n$, soit $P_k = X^k(1 - X)^{n-k}$. Montrer que $(P_k)_{0 \leq k \leq n}$ est une base de E .

Exercice 12 : Polynômes interpolateurs de Lagrange

Soient a_0, \dots, a_n $n + 1$ nombres complexes deux à deux distincts et b_0, \dots, b_n $n + 1$ nombres complexes. Montrer qu'il existe une unique famille de $n + 1$ polynômes à coefficients complexes de degré n exactement vérifiant $\forall (i, j) \in \llbracket 0, n \rrbracket, L_i(a_j) = 1$ si $i = j$ et 0 sinon.
Montrer que la famille $(L_i)_{0 \leq i \leq n}$ est une base de $\mathbb{C}_n[X]$.
Montrer qu'il existe un unique polynôme P de degré inférieur ou égal à n vérifiant $\forall i \in \llbracket 0, n \rrbracket, P(a_i) = b_i$.
Expliciter P puis déterminer tous les polynômes vérifiant les égalités précédentes.

Exercice 13 : Reste

Soit $E = \mathbb{R}_3[X]$. Pour P élément de E , soit $f(P)$ le reste de la division euclidienne de AP par B où $A = X^4 - 1$ et $B = X^4 - X$.
Vérifier que f est un endomorphisme de E puis déterminer $\text{Ker} f$, $\text{Im} f$ et les valeurs et vecteurs propres de f .

Exercice 14 : Reste bis

Soient A un polynôme non nul de $\mathbb{R}[X]$ et $r: \mathbb{R}[X] \rightarrow \mathbb{R}[X]$ l'application définie par $r: \forall P \in \mathbb{R}[X], r(P)$ est le reste de la division euclidienne de P par A . Montrer que r est un endomorphisme de $\mathbb{R}[X]$ tel que $r^2 = r \circ r = r$. Déterminer le noyau et l'image de cet endomorphisme.

Exercice 15 : P(X+1)-P(X)

Soit $\Delta: \mathbb{C}[X] \rightarrow \mathbb{C}[X]$ l'application définie par $\Delta(P) = P(X+1) - P(X)$

1. Montrer que Δ est un endomorphisme et que pour tout polynôme P non constant $\deg(\Delta(P)) = \deg P - 1$.
2. Déterminer $\text{Ker } \Delta$ et $\text{Im } \Delta$.
3. Soit $P \in \mathbb{C}[X]$ et $n \in \mathbb{N}$. Montrer $\Delta^n(P) = (-1)^n \sum_{k=0}^n (-1)^k \binom{n}{k} P(X+k)$
4. En déduire que, si $\deg P < n$, alors $\sum_{k=0}^n \binom{n}{k} (-1)^k P(k) = 0$

Exercice 16 : Théorème du rang

Soit $\varphi: \mathbb{K}_{n+1}[X] \rightarrow \mathbb{K}_n[X]$ définie par $\varphi(P) = (n+1)P - XP'$.

1. Justifier que φ est bien définie et que c'est une application linéaire.
2. Déterminer le noyau de φ et en déduire que φ est surjective.

Exercice 17 : Matrice compagnon

Soit $E = \mathbb{K}^4$ muni de la base canonique. Soit $f: E \rightarrow E$ l'endomorphisme tel que $f(e_1) = e_2, f(e_2) = e_3, f(e_3) = e_4$ et $f(e_4) = e_1 - e_3 + e_4$. Vérifier que $X^4 - X^3 + X^2 - 1$ est un polynôme annulateur de f . En déduire une matrice carrée A vérifiant $A^4 - A^3 + A^2 - I = 0$.

VI — Exercices d'oraux autres que CCP :**Exercice 18 : Centrale**

1. Soit $n \in \mathbb{N}$. Exprimer $\sin((2n+1)\alpha)$ en fonction de $\sin \alpha$ et $\cos \alpha$.
2. En déduire que les racines du polynôme :

$$P(X) = \sum_{p=0}^n (-1)^p \binom{2n+1}{2p+1} X^{n-p}$$

sont de la forme $x_k = \cotan^2 \beta_k$. Déterminer les β_k .

Exercice 19 : Centrale

Soit $P \in \mathbb{Z}[X]$ et a, b deux entiers relatifs avec $b > 0$ et \sqrt{b} irrationnel.

1. Exemple : montrer que $\sqrt{6}$ est irrationnel.
2. Quelle est la forme de $(a + \sqrt{b})^n$?
3. Montrer que si $a + \sqrt{b}$ est racine de P alors $a - \sqrt{b}$ aussi.
4. On suppose que $a + \sqrt{b}$ est racine double de P . Montrer que $P = RQ^2$ avec R et Q dans $\mathbb{Z}[X]$.

Exercice 20 : Centrale

On pose

$$f(x) = \frac{1}{\cos x}$$

Démontrer l'existence d'un polynôme P_n de degré n et à coefficients positifs ou nul vérifiant

$$\forall n \geq 1, f^{(n)}(x) = \frac{P_n(\sin x)}{(\cos x)^{n+1}}$$

Préciser P_1, P_2, P_3 et calculer $P_n(1)$.