Chapitre 16 : Polynômes

Programme officiel PCSI

a) Ensemble des polynômes à une indéterminée

Ensemble $\mathbb{K}[X]$.	La construction de $\mathbb{K}[X]$ est hors programme.
Combinaison linéaire et produit de polynômes, formule du binôme.	
Degré, coefficient dominant, polynôme unitaire.	Ensemble $\mathbb{K}_n[X]$ des polynômes de degré au plus n.
Degré d'une somme, d'un produit.	Le produit de deux polynômes non nuls est non nul.
Composition.	

b) Divisibilité et division euclidienne

Divisibilité dans $\mathbb{K}[X]$, diviseurs, multiples.	
Théorème de la division euclidienne.	Algorithme de la division euclidienne.

c) Fonctions polynomiales et racines

Fonction polynomiale associée à un polynôme. Racine (ou zéro) d'un polynôme, caractérisation en termes de divisibilité.	Lien avec l'introduction aux équations algébriques de la section « Nombres complexes ». Méthode de Horner pour l'évaluation polynomiale.
Le nombre de racines d'un polynôme non nul est majoré par son degré.	Détermination d'un polynôme par la fonction polynomiale associée.
Multiplicité d'une racine.	
Polynôme scindé.	
Expressions de la somme et du produit des racines d'un polynôme scindé en fonction de ses coefficients.	Les fonctions symétriques élémentaires sont hors programme.

d) Dérivation

Dérivée formelle d'un polynôme.	Pour $\mathbb{K} = \mathbb{R}$, lien avec la dérivée de la fonction polynomiale associée.
Opérations sur les polynômes dérivés : combinaison linéaire, produit. Formule de Leibniz.	
Formule de Taylor polynomiale.	
Caractérisation de la multiplicité d'une racine par les polynômes dérivés successifs.	

e) Polynômes irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$

Théorème de d'Alembert-Gauss.	La démonstration est hors programme.
Polynômes irréductibles de $\mathbb{C}[X]$. Théorème de décomposition en facteurs irréductibles dans $\mathbb{C}[X]$.	Caractérisation de la divisibilité dans $\mathbb{C}[X]$ à l'aide des racines et des multiplicités. Factorisation de $X^n - 1$ dans $\mathbb{C}[X]$.
Polynômes irréductibles de $\mathbb{R}[X]$. Théorème de décomposition en facteurs irréductibles dans $\mathbb{R}[X]$.	Deux racines complexes conjuguées d'un polynôme de $\mathbb{R}[X]$ ont même multiplicité.

f) Décomposition en éléments simples de certaines fonctions rationnelles	
Expression de la décomposition en éléments simples sur $\mathbb{C}$ et $\mathbb{R}$ des fonctions rationnelles à pôles simples.	La démonstration est hors programme. Dans le cas où le dénominateur possède une racine multiple ou un facteur irréductible de degré 2, la forme cherchée doit être fournie. Application au calcul de primitives, de dérivées k-ièmes.

Plan du résumé

Résumé

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

I – Polynômes à une indéterminée

1. Vocabulaire et notations

Définitions :

Un polynôme (formel) à une indéterminée sur $\mathbb{K}$ est une suite $(a_n)_{n\in\mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$ nulle à partir d'un certain rang. Les termes de cette suite sont appelés les coefficients du polynôme.

Notations :

- On note $\mathbb{K}[X]$ l'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$.
- On écrit : $P = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 = \sum_{k=0}^{+\infty} a_k X^k$. Les $a_k X^k$ sont les termes de P.

Propriété :

$\forall (P, Q) \in \mathbb{K}[X]\times\mathbb{K}[X]$, tels que $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$, $P = Q \Leftrightarrow \forall k \in \mathbb{N},\ a_k = b_k$.

Définitions :

Le polynôme nul est la suite nulle, et est noté 0.

Un polynôme ne comportant qu'un seul terme est appelé monôme.

Si $P = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \neq 0$ avec $a_n \neq 0$, l'entier n est appelé degré de P, noté $\deg P$, le nombre a_n est le coefficient dominant de P et le nombre a_0 est le terme constant de P.

Si le coefficient dominant de P vaut 1, on dit que P est unitaire ou normalisé.

Un polynôme de degré 0 est dit constant.

Notation : $\forall n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré *inférieur ou égal* à n.

2. Fonctions polynomiales

Définitions :

A tout polynôme $P = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0 \in \mathbb{K}[X]$, on associe la fonction polynômiale ou polynôme $\tilde{P} : \mathbb{K} \mapsto \mathbb{K}\ ; x \mapsto a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ définie sur $\mathbb{K}$ et à valeurs dans $\mathbb{K}$.

Une équation algébrique est une équation de la forme $\tilde{P}(x) = 0$ où $\tilde{P}$ est une fonction polynômiale.

Notation : L'ensemble des fonctions polynômiales sur $\mathbb{K}$ est noté $\mathbb{K}[x]$.

Propriété :

L'application $\varphi : \mathbb{K}[X] \mapsto \mathbb{K}[x]\ ; P \mapsto \tilde{P}$ est bijective.

3. Opérations

a. Combinaisons linéaires :

Sur $\mathbb{K}[X]$, on définit les opérations suivantes. $\forall (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$, avec $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$:

- Somme : $P+Q$ est le polynôme $P+Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k$.
- Produit par un nombre : $\forall \lambda \in \mathbb{K}$, λP est le polynôme $\lambda P = \sum_{k=0}^{+\infty} \lambda a_k X^k$.

Propriété :

Si P et Q sont deux polynômes de degrés n et p et de coefficients dominants a et b respectivement, alors :

- Si $n \neq p$, $P+Q$ est de degré $\max(n,p)$ et de coefficient dominant celui du polynôme de plus haut degré.
- Si $n = p$, $P+Q$ est de degré inférieur ou égal à n avec égalité si et seulement $a + b \neq 0$. Dans ce cas, son coefficient dominant est $a+b$.
- $\forall \lambda \in \mathbb{K}^*$, λP est de degré n et de coefficient dominant λa où a est celui de P.

Propriétés :

- $(\mathbb{K}[X], +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
- Pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n+1$.

Propriétés :

L'application $\varphi : \mathbb{K}[X] \to \mathbb{K}[x] ; P \mapsto \tilde{P}$ est un isomorphisme.

$\forall a \in \mathbb{K}$, L'application $\varphi_a : \mathbb{K}[X] \to \mathbb{K} ; P \mapsto \tilde{P}(a)$ est linéaire.

Définition :

On dit qu'une famille $(P_1, P_2, ..., P_n)$ de $\mathbb{K}[X]$ est échelonnée en degrés, si $\deg P_1 < \deg P_2 < ... < \deg P_n$.

Propriétés et définition :

- Toute famille de polynômes non nuls de $\mathbb{K}[X]$ échelonnée en degrés est libre.
- La famille $(1, X, ..., X^n)$ est une base de $\mathbb{K}_n[X]$ appelée base canonique de $\mathbb{K}_n[X]$.
- Toute famille de $n+1$ polynômes non nuls de $\mathbb{K}_n[X]$ échelonnée en degrés est une base de $\mathbb{K}_n[X]$.

b. Produit :

$\forall (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$, avec $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$, on définit le produit de P et Q par :

$$P \times Q = PQ = \sum_{k=0}^{+\infty} c_k X^k \text{ où } \forall k \in \mathbb{N},\ c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Remarque : $\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} b_i a_{k-i}$ donc le produit est commutatif.

Propriété :

Si $\varphi : \mathbb{K}[X] \to \mathbb{K}[x] ; P \mapsto \tilde{P}$, alors $\forall (P,Q) \in \mathbb{K}[X] \times \mathbb{K}[X]$, $\varphi(PQ) = \varphi(P)\varphi(Q)$, soit $\widetilde{PQ} = \tilde{P}\tilde{Q}$.

Propriété :

Si P et Q sont deux polynômes de degrés respectifs n et p et de coefficients dominants respectifs a et b, alors PQ est de degré $n+p$ et de coefficient dominant ab.

Remarque : Avec combinaisons linéaires et produit commutatif, les identités remarquables, dont la formule du binôme sont valables dans $\mathbb{K}[X]$.

Propriété :

$\forall (P,Q) \in \mathbb{K}[X]^2$, $PQ = 0$ si et seulement si $P = 0$ ou $Q = 0$. On dit que $\mathbb{K}[X]$ est *intègre*.

c. Composée :

Définition :

Si P et Q sont deux polynômes avec $Q = \sum_{k=0}^{+\infty} b_k X^k$, alors la composée, $Q \circ P$, de P par Q est définie par :

$$Q \circ P = Q(P) = \sum_{k=0}^{+\infty} b_k P^k .$$

Propriété :

Si P et Q sont deux polynômes non nuls de degrés respectifs n et p et de coefficients dominants respectifs a et b, alors $Q \circ P$ est de degré np et de coefficient dominant $a^p b$.

4. Polynôme dérivé

Définition :

Si $P \in \mathbb{K}[X]$ avec $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$, le polynôme dérivé de P, noté P', est 0 si $n \le 0$ et $n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \ldots + 2 a_2 X + a_1$ si $n > 0$.

Propriétés :

- Pour tout $P \in \mathbb{K}[X]$ et tout $k \in \mathbb{N}$, on a $\deg P^{(k)} = \deg P - k$ si $k \le \deg P$ et $P^{(k)} = 0$ si $k > \deg P$.
- Pour tous $P, Q \in \mathbb{K}[X]$, tous $\lambda, \mu \in \mathbb{K}$ et tout $n \in \mathbb{N}$, on a $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.
- *Formule de Taylor* : Pour tout $P \in \mathbb{K}[X]$ et tout $a \in \mathbb{K}$, on a $P = \sum_{k=0}^{+\infty} \frac{P^{(k)}(a)}{k!} (X-a)^k$.
- *Formule de Leibniz* : Pour tous $P, Q \in \mathbb{K}[X]$ et tout $n \in \mathbb{N}$, on a $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

II – Arithmétique dans $\mathbb{K}[X]$

1. Multiples et diviseurs

Définitions :

Soit $(P,Q)\in\mathbb{K}[X]^2$ avec $Q\neq 0$. On dit que Q divise P, et on note $Q\mid P$, s'il existe $R\in\mathbb{K}[X]$ tel que $P=RQ$. Dans ce cas, on dit aussi que Q est un diviseur de P et que P est un multiple de Q.

Propriétés :

- La relation « divise » est réflexive et transitive.
- Si Q divise P_1 et P_2, alors pour tous $R_1,R_2\in\mathbb{K}[X]$, Q divise $P_1R_1+P_2R_2$.

Définition :

Soit $(P,Q)\in\mathbb{K}[X]^2$. Si $Q\mid P$ et $P\mid Q$, alors on dit que P et Q sont des polynômes associés.

Propriété :

Deux polynômes P et Q sont associés si et seulement si $\exists\lambda\in\mathbb{K}^*$ tel que $P=\lambda Q$.

2. Division euclidienne

Théorème et définition :

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 $A=QB+R$ et $\deg R<\deg B$.

Cette écriture est la division euclidienne de A par B, R est le reste et Q le quotient de la division.

Propriété :

Soit $(P,L)\in\mathbb{K}[X]^2$ avec $L\neq 0$. $L\mid P$ si et seulement si le reste de la division euclidienne de P par L est nul.

Propriété :

Soit $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$. Le reste de la division euclidienne de P par $X-a$ est $P(a)$.

III – Racines d'un polynôme

1. Racines

Définition :

Soit $P\in\mathbb{K}[X]$. On dit que $a\in\mathbb{K}$ est racine (ou zéro) de P si $P(a)=0$.

Propriété :

Soit $P\in\mathbb{K}[X]$. Un scalaire $a\in\mathbb{K}$ est racine de P si et seulement si $(X-a)\mid P$.

Corollaires :

- Soit $P \in \mathbb{K}[X]$ et $a_1, a_2, ..., a_n$ sont n racines *distinctes* de P, alors $\prod_{1 \le i \le n} (X - a_i)$ divise P.
- Soit $P \in \mathbb{K}[X]$ de degré $n \ge 0$ (donc non nul). P possède au plus n racines distinctes.

Méthode de Horner

La méthode de Horner est un algoritheme qui permet de calculer la valeur d'un polynôme P en un scalaire x_0 (réel ou complexe) en utilisant une forme (obtenue à partir de la forme développée) qui réduit le nombre d'opérations à effectuer pour obtenir $P(x_0)$:

$$P(x_0) = a_n x_0^n + a_{n-1} x_0^{n-1} + ... + a_1 x_0 + a_0 = \Big(\big(...(a_n x_0 + a_{n-1})\, x_0 + ...\big)\, x_0 + a_1\Big)\, x_0 + a_0 .$$

Elle est aussi utilisée en informatique pour trouver des valeurs approchées des racines d'un polynôme.

2. Ordre de multiplicité

Dans ce qui suit, on considère $P \in \mathbb{K}[X]$ non nul.

Propriété et définition :

Soit $a \in \mathbb{K}$ une (éventuelle) racine de P. Il existe un unique entier naturel $\alpha \ge 1$ tel que $(X - a)^{\alpha}$ divise P et pas $(X - a)^{\alpha+1}$. α est appelé ordre de multiplicité ou multiplicité de a.

Si $\alpha = 1$, on dit que a est une racine simple ; si $\alpha \ge 2$, on dit que a est une racine multiple (double pour $\alpha = 2$, triple pour $\alpha = 3$, …)

On dit qu'une racine de P est comptée avec multiplicité si elle est comptée autant de fois que son ordre de multiplicité.

Propriété :

Un nombre $a \in \mathbb{K}$ est racine de P de multiplicité $\alpha \ge 1 \Leftrightarrow P = (X - a)^{\alpha} Q$ avec $Q(a) \ne 0$.

Corollaires :

- Si $a_1, a_2, ..., a_n$ sont n racines *distinctes* de P d'ordres de multiplicité respectifs $\alpha_1, \alpha_2, ..., \alpha_n$, alors $\prod_{1 \le i \le n} (X - a_i)^{\alpha_i}$ divise P et les a_i ne sont pas racines du « quotient ».
- Un polynôme de degré $n \ge 1$ admet au plus n racines comptées avec multiplicité.
- Si $a_1, a_2, ..., a_n$ sont racines de P, d'ordres de multiplicité respectifs $\alpha_1, \alpha_2, ..., \alpha_n$, alors :

$$P = \lambda \prod_{1 \le i \le n} (X - a_i)^{\alpha_i} \quad \Leftrightarrow \quad \alpha_1 + \alpha_2 + ... + \alpha_n = \deg P$$

où λ est le coefficient dominant de P.

Propriété :

Un nombre $a \in \mathbb{K}$ est racine de P de multiplicité $\alpha \ge 1 \Leftrightarrow \forall\, k \in [\![0 ; \alpha - 1]\!]$, $P^{(k)}(a) = 0$ et $P^{(\alpha)}(a) \ne 0$.

IV – Factorisation

1. Polynôme scindé

a. Définition :

Définition :

Soit $P \in \mathbb{K}[X]$ non constant. On dit que P est scindé sur $\mathbb{K}$ s'il peut s'écrire $P = a\prod_{i=1}^{n}(X-\lambda_i)$.

b. Somme et produit des racines d'un polynôme scindé :

Propriété :

Soit $P \in \mathbb{K}[X]$ de degré n et scindé sur $\mathbb{K}$.

Si $P = a_n X^n + ... + a_1 X + a_0$, alors la somme des n racines de P (distinctes ou non) vaut $-\frac{a_{n-1}}{a_n}$ et le produit des racines vaut $(-1)^n \frac{a_0}{a_n}$.

2. Polynôme irréductible

a. Définition :

Définition :

Soit $P \in \mathbb{K}[X]$ non constant. On dit que P est irréductible sur $\mathbb{K}$ lorsque dans toute décomposition $P = AB$ avec A et B polynômes, A ou B est constant.

b. Description des polynômes irréductibles de $\mathbb{C}[X]$:

Théorème : *de d'Alembert-Gauss*

Tout polynôme non constant à coefficients réels ou complexes possède au moins une racine complexe.

Corollaire :

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

c. Description des polynômes irréductibles de $\mathbb{R}[X]$:

Propriété :

Soit $P \in \mathbb{R}[X]$ non constant . Si z est une racine complexe de P de multiplicité α, alors $\overline{z}$ est aussi une racine complexe de P de multiplicité α.

Propriété :

Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle (de discriminant < 0).

3. Décomposition d'un polynôme en produit de facteurs irréductibles

a. Décomposition sur $\mathbb{C}$:

Théorème : *Corollaire du théorème de d'Alembert-Gauss*

Tout polynôme non constant à coefficients réels ou complexes est scindé sur $\mathbb{C}$.

b. Décomposition sur $\mathbb{R}$:

Propriété :

Tout polynôme P de $\mathbb{R}[X]$ non constant se factorise en produit de polynômes irréductibles sur $\mathbb{R}$.

Plus précisément, si λ est le coefficient dominant de P, $x_1, x_2, ..., x_p$ sont les racines réelles de P de multiplicités respectives $\alpha_1, \alpha_2, ..., \alpha_p$ et $z_1, \overline{z}_1, z_2, \overline{z}_2, ..., z_q, \overline{z}_q$ sont les racines complexes non réelles et deux à deux conjuguées de P avec z_j de multiplicité β_j, on a :

$$P = \lambda \prod_{i=1}^{p} (X - x_i)^{\alpha_i} \prod_{j=1}^{q} \left(X^2 - 2\,\mathrm{Re}(z_j) X + | z_j |^2 \right)^{\beta_j}.$$

V – Décomposition en éléments simples

Définition :

Une fraction rationnelle est un quotient (formel) $\frac{P}{Q}$ de deux polynômes de $P, Q \in \mathbb{K}[X]$ avec Q non nul.

Propriété :

Soit $P, Q \in \mathbb{K}[X]$ et L le quotient de la division euclidienne de P par Q.

- Si $Q = \prod_{i=1}^{p} (X - x_i)$ avec les x_i distincts (Q est scindé à racines simples), alors :

$$\frac{P}{Q} = L + \sum_{i=1}^{p} \frac{a_i}{X - x_i}$$

  où les a_i sont des scalaires.

- Si $Q = X^2 - aX + b$ sans racines, alors $\frac{P}{Q} = L + \frac{\alpha X + \beta}{X^2 - aX + b}$ où $\alpha X + \beta$ est le reste de la division euclidienne de P par Q.
- On peut généraliser à Q quelconque.