Résumé de cours :
Semaine 25, du 30 mars au 3 avril.

Les polynômes (suite)

1 Composition de polynômes

Définition. Si $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ et $Q \in A[X]$, $P \circ Q = \sum_{k=0}^{n} a_k Q^k = P(Q)$.

Propriété. Pour tout $P, Q, R \in A[X]$,
- $(P+Q) \circ R = P \circ R + Q \circ R$,
- $(PQ) \circ R = (P \circ R) \times (Q \circ R)$,
- $(P \circ Q) \circ R = P \circ (Q \circ R)$.

Propriété. Soit $P, Q \in A[X]$ Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.
Il faut savoir le démontrer.

Propriété. Pour tout $P, Q \in A[X]$, $\widetilde{P \circ Q} = \tilde{P} \circ \tilde{Q}$.

2 Dérivation formelle

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k \in A[X]$, on pose $P' \triangleq \sum_{k \in \mathbb{N}^*} k a_k X^{k-1} = \sum_{k \in \mathbb{N}} (k+1) a_{k+1} X^k$.

Remarque. On peut écrire $P' = \sum_{k \in \mathbb{N}} k a_k X^{k+1}$, si l'on convient que $0X^{-1} = 0$.

Définition. Si $P = \sum_{k \in \mathbb{N}} a_k X^k$, $P^{(0)} = P$ et
pour tout $n \in \mathbb{N}$, $P^{(n)} = \sum_{k \geq n} \frac{k!}{(k-n)!} a_k X^{k-n} = \sum_{k \in \mathbb{N}} \frac{(k+n)!}{k!} a_{k+n} X^k$.

Propriété. Pour tout $P \in \mathbb{R}[X]$ et $n \in \mathbb{N}$, $\widetilde{P^{(n)}} = \tilde{P}^{(n)}$.

Propriété. Pour tout $P \in A[X]$, $\deg(P') \leq \deg(P) - 1$.

Propriété. Pour tout $P \in A[X] \setminus \{0\}$, $P^{(\deg(P)+1)} = 0$.

Propriété. Soit $P, Q \in A[X]$, $a \in A$ et $n \in \mathbb{N}$.
- $(P+Q)' = P' + Q'$, et plus généralement, $(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$.
- $(aP)' = aP'$, et plus généralement, $(aP)^{(n)} = aP^{(n)}$.
- $(PQ)' = P'Q + PQ'$

Propriété. Pour tout $n \in \mathbb{N}$ et $P_1, \dots, P_n \in A[X]$, $(P_1 \times \cdots \times P_n)' = \sum_{i=1}^{n} P_i' \prod_{j \neq i} P_j$.

Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Propriété. Pour tout $P, Q \in A[X]$, $(P \circ Q)' = Q' \times (P' \circ Q)$.

3 La structure d'algèbre de $\mathbb{K}[X]$.

Pour la suite de ce chapitre, $\mathbb{K}$ désigne un corps.

Propriété. $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre.

Propriété. La base canonique de $\mathbb{K}[X]$ est la famille $(X^n)_{n\in\mathbb{N}}$.

Propriété. Soit $n \in \mathbb{N}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ dont une base est $(1, X, \dots, X^n)$, encore appelée la base canonique de $\mathbb{K}_n[X]$. On en déduit que $\dim(\mathbb{K}_n[X]) = n + 1$.

> **Exercice.** Soit $(P_n)_{n\in\mathbb{N}}$ une suite de polynômes de $\mathbb{K}[X]$. On suppose que cette suite de polynômes est étagée c'est-à-dire que, $\forall n \in \mathbb{N} \quad \deg(P_n) = n$.
> Montrer que pour tout $N \in \mathbb{N}$, $(P_n)_{0\leq n\leq N}$ est une base de $\mathbb{K}_N[X]$.
> En déduire que $(P_n)_{n\in\mathbb{N}}$ est une base de $\mathbb{K}[X]$.
> Il faut savoir le démontrer.

4 Division euclidienne entre polynômes

Théorème. Soit $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Alors il existe un unique couple $(P, Q) \in \mathbb{K}[X]^2$ tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$: Q est le quotient de la division euclidienne du dividende A par le diviseur B et que R en est le reste.
Il faut savoir le démontrer.

Définition. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est une racine de A si et seulement si $\tilde{A}(a) = 0$.

Propriété. Soit $A \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Le reste de la division euclidienne de A par $X - a$ est égal au polynôme constant $\tilde{A}(a)$.
Il faut savoir le démontrer.

Corollaire. a est racine de A si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $A = (X - a)Q$.

Propriété. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$. Alors, pour tout $(A, B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$, les quotient et reste de la division euclidienne sont les mêmes que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

5 Arithmétique

5.1 Divisibilité

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b$ si et seulement si $\exists m \in A \;\; b = ma$. On dit alors que a est un ***diviseur*** de b et que b est un ***multiple*** de a.

Remarque. $0|a \iff a = 0$ et, pour tout $a \in A$, $a|0$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ tels que $P \mid Q$ et $Q \neq 0$. Alors $\deg(Q) \geq \deg(P)$.

Propriété. Soit $P, Q \in \mathbb{K}[X]$ avec $Q \neq 0$. $P \mid Q$ si et seulement si le reste de la divison euclidienne de P par Q est nul.

Propriété. Soit $\mathbb{L}$ un sous-corps d'un corps $\mathbb{K}$. Soit $P, Q \in \mathbb{L}[X]$.
Alors $P \mid Q$ dans $\mathbb{L}[X]$ si et seulement si $P \mid Q$ dans $\mathbb{K}[X]$.
Il faut savoir le démontrer.

Propriété. Soient A un anneau commutatif et $a, b, c, d \in A$.
- Si $b \mid a$ et $b \mid c$, alors $b \mid (a + c)$.
- Si $b \mid a$ et $d \mid c$, alors $bd \mid ac$.
- si $b \mid a$, pour tout $p \in \mathbb{N}$, $b^p \mid a^p$.

Propriété. Soient A un anneau commutatif et $b, a_1, \ldots, a_p, c_1, \ldots, c_p \in A$.
Si pour tout $i \in \{1, \ldots, p\}$, $b \mid a_i$, alors $b \mid \sum_{i=1}^{p} c_i a_i$.

Propriété. Soient A un anneau commutatif et $(a, b) \in A^2$. $a|b \iff bA \subseteq aA$.

Propriété. Soit A un anneau commutatif. La relation de divisibilité est réflexive et transitive.

Définition. Soient A un anneau commutatif et $(a, b) \in A^2$.
a et b sont ***associés*** si et seulement si $a|b$ et $b|a$.
La relation "être associé à" est une relation d'équivalence, on la notera "$\sim$".

Propriété. Dans un anneau commutatif, si $a \sim b$ et $c \sim d$, alors $ac \sim bd$.

Hypothèse : Jusqu'à la fin de ce paragraphe, on suppose que A est intègre et commutatif.

Propriété. Soit $a, b \in A$. a et b sont associés si et seulement s'il existe $\lambda \in U(A)$ tel que $a = \lambda b$.
Il faut savoir le démontrer.

Exemple. Dans $\mathbb{Z}$, n et m sont associés si et seulement si $|n| = |m|$.
Dans $\mathbb{K}[X]$, P et Q sont associés si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda P$.

Propriété. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.
La relation de divisibilité est une relation d'ordre sur l'ensemble des polynômes unitaires de $\mathbb{K}[X]$.

Définition. Soit $p \in A$. p est irréductible dans A si et seulement si $p \notin U(A)$ et si, pour tout $a, b \in A$, $p = ab \implies (a \in U(A)) \vee (b \in U(A))$.
Ainsi p est irréductible dans A si et seulement si p n'est pas inversible et a pour seuls diviseurs les éléments associés à 1 ou à p.

Remarque. Si p est irréductible, il est non nul.

Propriété. Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

Exemple. Dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps), un polynôme P est irréductible si et seulement si il est de degré supérieur ou égal à 1 et si, pour tout $A, B \in \mathbb{K}[X]$, $P = AB \implies (\deg(A) = 0) \vee (\deg(B) = 0)$.

Remarque. Dans $\mathbb{K}[X]$:
- tout polynôme de degré 1 est irréductible ;
- tout polynôme de degré ≥ 2 possédant une racine dans $\mathbb{K}$ est réductible ;
- tout polynôme de degré 2 ou 3 sans racine dans $\mathbb{K}$ est irréductible.

Il faut savoir le démontrer.

Définition. Soit $a, b \in A$. On dit que a et b sont premiers entre eux (ou étrangers) si et seulement si les seuls diviseurs communs de a et b sont les éléments inversibles.

Définition. Soit $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \ldots, a_n \in A$.
- $a_1, \ldots, a_n$ sont deux à deux premiers entre eux si et seulement si, pour tout $i, j \in \{1, \ldots, n\}$ avec $i \neq j$, a_i et a_j sont premiers entre eux.

— $a_1, \dots, a_n$ sont globalement premiers entre eux si et seulement si les seuls diviseurs communs de $a_1, \dots, a_n$ sont les éléments inversibles de A.

Propriété. Soit $p \in A$ un élément irréductible et $a \in A$: $p|a$, ou bien p et a sont premiers entre eux.
Il faut savoir le démontrer.

5.2 PGCD

Théorème. Si $\mathbb{K}$ est un corps, alors $\mathbb{K}[X]$ est un anneau principal.
Il faut savoir le démontrer.

Notation. Jusqu'à la fin de ce chapitre "arithmétique", on fixe un anneau A que l'on suppose principal.

Définition. Soit $(a, b) \in A^2$. d est un PGCD de a et b si et seulement si $aA + bA = dA$.

Caractérisation du PGCD par divisibilité : d est un PGCD de $(a, b) \in A^2$ si et seulement si d est un diviseur commun de a et b et si, pour tout diviseur commun d' de a et b, d' divise d.
Il faut savoir le démontrer.

Propriété. a et b sont premiers entre eux si et seulement si 1 est un PGCD de a et b.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, on dit que d est un PGCD de $a_1, \dots, a_k$ si et seulement si $dA = a_1A + \dots + a_kA$, i.e si et seulement si d est un commun diviseur de $a_1, \dots, a_k$ tel que si d' est un autre commun diviseur de $a_1, \dots, a_k$, alors d' divise d.
Soit B une partie quelconque de A. d est un PGCD de B si et seulement si $dA = Id(B)$, i.e si et seulement si d est un diviseur commun des éléments de B tel que si d' est un autre diviseur commun des éléments de B, alors d' divise d.

Propriété. Lorsque $A = \mathbb{Z}$ (resp : $A = \mathbb{K}[X]$), en imposant au PGCD d'être positif (resp : unitaire) il est unique. On le note alors $a \wedge b$.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,
— Commutativité du PGCD :
pour tout $\sigma \in \mathcal{S}_k$, $PGCD(a_1, \dots, a_k) \sim PGCD(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
— Associativité du PGCD :
$PGCD(a_1, \dots, a_k) \sim PGCD(PGCD(a_1, \dots, a_h), PGCD(a_{h+1}, \dots, a_k))$.
— Distributivité de la multiplication par rapport au PGCD : pour tout $\alpha \in A$,
$PGCD(\alpha a_1, \dots, \alpha a_k) \sim \alpha PGCD(a_1, \dots, a_k)$.
Il faut savoir le démontrer.

5.3 PPCM

Définition. Soit $(a, b) \in A^2$. m est un PPCM de a et b si et seulement si $aA \cap bA = mA$.

Caractérisation du PPCM par divisibilité : m est un PPCM de $(a, b) \in A^2$ si et seulement si m est un multiple commun de a et b et si, pour tout multiple commun m' de a et b, m' est un multiple de m.

Définition. Plus généralement, si $k \in \mathbb{N}^*$ et si $a_1, \dots, a_k \in A$, m est un PPCM de $a_1, \dots, a_k$ si et seulement si $mA = a_1A \cap \dots \cap a_kA$, i.e si et seulement si m est un commun multiple de $a_1, \dots, a_k$ tel que si m' est un autre commun multiple de $a_1, \dots, a_k$, alors m' est un multiple de m.
Soit B est une partie quelconque de A. m est un PPCM de B si et seulement si $mA = \bigcap_{b \in B} bA$, i.e si et seulement si m est un multiple commun des éléments de B tel que si m' est un autre multiple commun des éléments de B, alors m' est un multiple commun de m.

Propriété. Soit $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$ et $h \in \{1, \dots, k\}$.
Alors, en convenant de noter $a \sim b$ lorsque a et b sont associés,
- Commutativité du PPCM :
  pour tout $\sigma \in \mathcal{S}_k$, $PPCM(a_1, \dots, a_k) \sim PPCM(a_{\sigma(1)}, \dots, a_{\sigma(k)})$.
- Associativité du PPCM :
  $PPCM(a_1, \dots, a_k) \sim PPCM(PPCM(a_1, \dots, a_h), PPCM(a_{h+1}, \dots, a_k))$.
- Distributivité de la multiplication par rapport au PPCM :
  pour tout $\alpha \in A$, $PPCM(\alpha a_1, \dots, \alpha a_k) \sim \alpha PPCM(a_1, \dots, a_k)$.

5.4 Les théorèmes de l'arithmétique

Théorème de *Bézout*. Soit $(a, b) \in A^2$.
a et b sont premiers entre eux si et seulement si : $\exists (u, v) \in A^2 \ \ ua + vb = 1$.

Propriété. Soit $(a, b) \in A^2$. Notons d un PGCD de a et b. Alors
il existe $(a', b') \in A^2$, avec a' et b' premiers entre eux, tel que $a = a'd$ et $b = b'd$.

Théorème de *Gauss*. Soit $(a, b, c) \in A^3$. Si $a|bc$ avec a et b premiers entre eux, alors $a|c$.

Corollaire. Soit $p, a, b \in A$. Si $p \mid ab$ avec p irréductible, alors $p \mid a$ ou $p \mid b$.

Propriété. Soit $(a, b, c) \in A^3$, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in A$.
On désigne par $a \wedge b$ un PGCD de a et b et par $a \vee b$ un PPCM de a et b.
- ◇ Si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
- ◇ Si $a \wedge b = 1$, $\forall (k, l) \in (\mathbb{N}^*)^2 \ \ a^k \wedge b^l = 1$.
- ◇ Si $a|b$, $c|b$ et $a \wedge c = 1$ alors $ac|b$.

Si pour tout $i \in \{1, \dots, n\}$, $a_i|b$ et si $i \neq j \Longrightarrow a_i \wedge a_j = 1$, alors $a_1 \times \cdots \times a_n \mid b$.
- ◇ $ab \sim (a \wedge b)(a \vee b)$. En particulier, $a \wedge b = 1 \Longrightarrow a \vee b \sim ab$.

Il faut savoir le démontrer.

6 $\mathbb{K}[X]$ est un anneau factoriel

Notation. On suppose ici que $A \in \{\mathbb{Z}, \mathbb{K}[X]\}$ ($\mathbb{K}$ étant un corps quelconque).
Si $A = \mathbb{Z}$, on pose $\mathcal{P} = \mathbb{P}$, et si $A = \mathbb{K}[X]$, $\mathcal{P}$ est l'ensemble des polynômes irréductibles et unitaires.

Théorème. Soit $a \in A$ avec $a \neq 0$. Il existe un unique couple $(u, (\nu_p)_{p \in \mathcal{P}})$, où $u \in U(A)$ et où $(\nu_p)_{p \in \mathcal{P}}$ est une famille presque nulle d'entiers, tel que $a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$: c'est la ***décomposition de a en facteurs irréductibles***. ν_p s'appelle la valuation p-adique de a.
Il faut savoir le démontrer.

Propriété. Soit $(a, b) \in (A \setminus \{0\})^2$, dont les décompositions en facteurs irréductibles sont $a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$ et $b = v \prod_{p \in \mathcal{P}} p^{\mu_p}$. Alors $a \mid b \Longleftrightarrow [\forall p \in \mathcal{P}, \ \ \nu_p \leq \mu_p]$.
De plus, $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p, \mu_p)}$ et $a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p, \mu_p)}$. En particulier, a et b sont premiers entre eux si et seulement si aucun élément de $\mathcal{P}$ n'intervient à la fois dans la décomposition en facteurs irréductibles de a et dans celle de b.

Lemme d'Euclide. Soient $(a, b) \in A^2$ avec $b \neq 0$, et q, r tels que $a = bq + r$. Alors $a \wedge b = b \wedge r$.

Algorithme d'Euclide. Soit $(a_0, a_1) \in A^2$.
- Pour $i \geq 1$, tant que $a_i \neq 0$, on note a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i. On définit ainsi une suite finie $(a_i)_{0 \leq i \leq N}$ d'éléments de A telle que $a_N = 0$ et, pour tout $i \in \{0, \dots, N-1\}$, $a_0 \wedge a_1 = a_i \wedge a_{i+1}$. En particulier, pour $i = N - 1$, on obtient $a_0 \wedge a_1 = a_{N-1}$.

• Supposons maintenant que $a_0 \wedge a_1 = a_{N-1} = 1$. D'après le théorème de Bézout, il existe $(s,t) \in A^2$ tel que $sa_0 + ta_1 = 1$. La suite de l'algorithme d'Euclide permet le calcul d'un tel couple (s,t) : Notons q_i le quotient de la division euclidienne de a_{i-1} par a_i. Ainsi, $a_{i+1} = a_{i-1} - q_i ai$.
En particulier, avec $i = N-2$, on obtient $1 = a_{N-3} - q_{N-2}a_{N-2}$.
Supposons que, pour un entier $i \in \{1, \dots, N-3\}$, on dispose d'entiers s_i et t_i tels que $1 = s_i a_i + t_i a_{i+1}$.
Alors $1 = s_i a_i + t_i(a_{i-1} - a_i q_i) = (s_i - t_i q_i)a_i + t_i a_{i-1}$, ce qui donne des entiers s_{i-1} et t_{i-1} tels que $1 = s_{i-1}a_{i-1} + t_{i-1}a_i$.
Par récurrence descendante, on peut donc calculer des entier s_0 et t_0 tels que $1 = s_0 a_0 + t_0 a_1$.

Corollaire. Supposons que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ et soit $(A,B) \in \mathbb{L}[X] \times (\mathbb{L}[X] \setminus \{0\})$.
Les PGCD et PPCM de A et B sont les mêmes, que l'on regarde A et B comme des polynômes de $\mathbb{L}[X]$ ou de $\mathbb{K}[X]$.

Exercice. Soit $a, b, c \in A$ avec a et b non nuls.
Résoudre l'équation de Bézout (B) : $au + bv = c$ en l'inconnue $(u,v) \in A^2$.
Il faut savoir le démontrer.

7 Identification entre polynômes formels et applications polynomiales

Notation. On fixe un corps $\mathbb{K}$ quelconque.

Propriété. Soit $P \in \mathbb{K}[X]$ et $a_1, \dots, a_k$ k éléments de $\mathbb{K}$ deux à deux distincts :
$a_1, \dots, a_k$ sont toutes racines de P si et seulement si P est un multiple de $(X - a_1) \times \cdots \times (X - a_k)$.
Il faut savoir le démontrer.

Corollaire. Un polynôme non nul admet au plus $\deg(P)$ racines.

Principe de rigidité des polynômes : si $P \in \mathbb{K}[X]$ possède une infinité de racines, alors $P = 0$.

Propriété. Soit $n \in \mathbb{N}$ et $P, Q \in \mathbb{K}_n[X]$.
Si $\{x \in \mathbb{K} \ / \ \tilde{P}(x) = \tilde{Q}(x)\}$ contient au moins $n+1$ scalaires, alors $P = Q$.

Théorème. On peut identifier l'ensemble $\mathbb{K}[X]$ des polynômes formels avec l'ensemble $\mathcal{P}_{\mathbb{K}}$ des applications polynomiales de $\mathbb{K}$ dans $\mathbb{K}$ si et seulement si $\mathbb{K}$ est de cardinal infini.

Remarque. Si $\mathbb{K}$ est fini de cardinal q, alors $\displaystyle\prod_{a \in \mathbb{K}} (X - a) = X^q - X$.

Il faut savoir le démontrer.

8 Polynôme d'interpolation de Lagrange

Notation. Dans tout ce paragraphe, on fixe un corps quelconque $\mathbb{K}$, $n \in \mathbb{N}$ et une famille $a_0, \dots, a_n \in \mathbb{K}$ de $n+1$ scalaires deux à deux distincts.
Pour tout $i \in \{0, \dots, n\}$, posons $L_i = \displaystyle\prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j}$.
Les L_i sont appelés les polynômes de Lagrange associés à $(a_0, \dots, a_n)$.

Propriété. Pour tout $i, k \in \{0, \dots, n\}$, $\widetilde{L_i}(a_k) = \delta_{i,k}$.

Propriété. Pour tout $P \in \mathbb{K}_n[X]$, $P = \displaystyle\sum_{i=0}^{n} \tilde{P}(a_i) L_i$.

Il faut savoir le démontrer.

Théorème. Soit $(b_0, b_1, \dots, b_n) \in \mathbb{K}^{n+1}$ une famille quelconque de scalaires. Il existe un unique polynôme P_0 de degré inférieur ou égal à n tel que, pour tout $i \in \{0, \dots, n\}$, $\widetilde{P_0}(a_i) = b_i$. P_0 est appelé le polynôme d'interpolation de Lagrange (associé aux deux familles $(a_0, a_1, \dots, a_n)$ et $(b_0, b_1, \dots, b_n)$).
On dispose de la formule suivante : $P_0 = \sum_{i=0}^{n} \left(b_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{X - a_j}{a_i - a_j} \right)$. Enfin, l'ensemble des polynômes P vérifiant, pour tout $i \in \{0, \dots, n\}$, $\tilde{P}(a_i) = b_i$, est égal à $P_0 + (\prod_{i=0}^{n}(X - a_i))\mathbb{K}[X]$.

9 Polynôme dérivé

Notation. Dans ce paragraphe, on suppose que $\mathbb{K}$ est un corps de caractéristique nulle.

Propriété. Pour tout $P \in \mathbb{K}[X]$ tel que $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$.

Corollaire. Soit $P \in \mathbb{K}[X]$. P est un polynôme constant si et seulement si $P' = 0$.

Corollaire. Si $P \in \mathbb{K}[X]$, $\deg(P) \geq n \implies \deg(P^{(n)}) = \deg(P) - n$ et $P^{(n)} = 0 \iff \deg(P) < n$.

Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors $P = \sum_{n \in \mathbb{N}} \frac{(X-a)^n}{n!.1_{\mathbb{K}}} P^{(n)}(a)$.

Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $k \in \mathbb{N}$. Alors
le reste de la division euclidienne de P par $(X-a)^k$ est égal à $\sum_{h=0}^{k-1} \frac{(X-a)^h}{h!.1_{\mathbb{K}}} P^{(h)}(a)$.

10 Racines multiples

Notation. $\mathbb{K}$ désigne un corps quelconque.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est une racine de P de multiplicité m si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = (X-a)^m Q(X)$ avec $\tilde{Q}(a) \neq 0$.

Remarque. a n'est pas racine de P si et seulement si a est racine de P de multiplicité nulle.

Définition. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$.
a est racine de P de multiplicité au moins m si et seulement si $(X-a)^m \mid P$.
Ainsi, a est racine de P de multiplicité m si et seulement si elle est racine de P de multiplicité au moins m, mais n'est pas racine de P de multiplicité au moins $m+1$.

Définition. On dit que $a \in \mathbb{K}$ est une racine simple (resp : double, triple) de $P \in \mathbb{K}[X]$ si et seulement si a est une racine de P de multiplicité 1 (resp : 2, 3).

Définition. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Posons $\{a_1, \dots, a_k\} = \{x \in \mathbb{K} / \tilde{P}(x) = 0\}$. Pour tout $h \in \mathbb{N}_k$, notons m_h la multiplicité de a_h pour le polynôme P. On dit alors que le nombre de racines de P, **comptées avec multiplicité**, est égal à $\sum_{h=1}^{k} m_h$.
Et k est le nombre de racines de P comptées sans multiplicité.

Propriété. Soit $P \in \mathbb{K}[X]$, $a_1, \dots, a_k \in \mathbb{K}$ et $m_1, \dots, m_h \in \mathbb{N}$. Pour tout $h \in \{1, \dots, k\}$, a_h est racine de P de multiplicité au moins m_h si et seulement si P est un multiple de $\prod_{h=1}^{k} (X - a_h)^{m_h}$.

Propriété. Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Le nombre de racines de P, comptées avec multiplicité est inférieur ou égal au degré de P.

Hypothèse : Pour la suite de ce paragraphe, on suppose que $\text{car}(\mathbb{K}) = 0$.

Théorème. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité au moins m si et seulement si $\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$.
Il faut savoir le démontrer.

Corollaire. Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}$. a est racine de P de multiplicité m si et seulement si $\forall i \in \{0, \dots, m-1\}$, $P^{(i)}(a) = 0$ et $P^{(m)}(a) \neq 0$.

Corollaire. Si $a \in \mathbb{K}$ est racine de $P \in \mathbb{K}[X]$ de multiplicité $m \in \mathbb{N}^*$, alors a est racine de P' de multiplicité $m - 1$.

11 Polynômes scindés

Notation. $\mathbb{K}$ désigne un corps quelconque.

Définition. $P \in \mathbb{K}[X] \setminus \{0\}$ est scindé dans $\mathbb{K}[X]$ si et seulement si sa décomposition en polynômes irréductibles dans $\mathbb{K}[X]$ ne fait intervenir que des polynômes de degré 1.

Propriété. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. P est scindé dans $\mathbb{K}[X]$ si et seulement si le nombre de racines de P dans $\mathbb{K}$, comptées avec multiplicité, est égal au degré de P.
Il faut savoir le démontrer.