POLYNOMES

1 L'algèbre $\mathbb{K}[X]$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$

1.1 Polynômes

Définition 1 On appelle polynôme à coefficients dans $\mathbb{K}$, toute suite nulle à partir d'un certain rang $(a_0, a_1, ..., a_n, 0, .)$ d'éléments de $\mathbb{K}$.
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

Définition 2 On définit sur $\mathbb{K}[X]$ trois opérations : $+, .$ et $\times$.
Soient deux polynômes $A = (a_i),\ i > n \Rightarrow a_i = 0, B = (b_j),\ j > m \Rightarrow b_j = 0$
en posant :
Addition :
$A + B = (a_i + b_i)$. On a $a_k + b_k = 0$ dès que $k > \max\{m, n\}$

Multiplication par un scalaire :
$\lambda \in \mathbb{K},\ \lambda A = (\lambda a_i)$.

Produit de deux polynômes :
$A \times B = C$ où $C = (c_k)$
la suite (c_k) étant définie par : $\forall k \in \mathbb{N},\ \ c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}$.

C est un polynôme car $k > n + m \Rightarrow c_k = 0$ et $c_{n+m} = a_n b_m$.

Proposition 3 L'ensemble des ploynômes à coefficients dans $\mathbb{K}$, muni de l'addition et du produit de polynômes, a une struxture d'anneau commutatif intègre.

Notation définitive

Proposition 4 En notant $X = (0, 1, 0, 0, \cdots)$ on a
$X^i = (0, ..., 0, 1, 0, ...)$, le 1 se situant à la ième position, tout élément $A(a_i)$ de $\mathbb{K}[X]$ s'écrit sous la forme $\sum_{i=0}^{n} a_i X^i$, où n représente un rang à partir duquel tous les termes de la suite sont nuls.

On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$.

1.2 Degré d'un polynôme

Définition 5 Soit $P \in \mathbb{K}[X]$, si $P = 0$ on définit $\deg(P) = -\infty$ et $val(P) = +\infty$.
Si $P \neq 0$, on définit $\deg(P) = \max\{i \in \mathbb{N} \ |a_i \neq 0\}$ et $val(P) = \min\{i \in \mathbb{N},\ |a_i \neq 0\}$.
Si $P \neq 0$ et si $\deg(P) = n$, on appelle terme dominant de P, le terme $a_n X^n$ et on dit que P est unitaire si $a_n = 1$.
Un polynôme P est dit constant si $\deg(P) \leq 0$

On notera $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur ou égal à n (et non pas égal à n).

Théorème 6 Soient $(P, Q) \in \mathbb{K}[X]^2$ on a :
1) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$
$val(P + Q) \geq \min((P), val(Q))$ avec égalité si $val(P) \neq val(Q)$,
2) $\forall \lambda \in \mathbb{K}^*, \quad \deg(\lambda P) = \deg(P)$ et $val(\lambda P) = val(P)$,
3) $\deg(PQ) = \deg(P) + \deg(Q)$ et $val(PQ) = val(P) + val(Q)$.

Corollaire 7 $\mathbb{K}[X]$ est un anneau intègre, c'est à dire $PQ = 0 \Rightarrow P = 0$ ou $Q = 0$.

1.3 Composition de polynômes

Définition 8 Soient $A, B \in \mathbb{K}[X],\ A = \sum_{k=0}^{n} a_k X^k$. On définit $A \circ B = \sum_{k=0}^{n} a_k B^k$.
On a $deg(A \circ B) = deg(A).deg(B)$.

Remarque 1 a)Cette opération sur $\mathbb{K}[X]$ n'est pas commutative.
Si $A = 1$ et $B = X + 1$ on a $A \circ B = 1,\ B \circ A = 2$.
b) Si$B = X,\ A(B) = A(X) = A$ c'est pourquoi un polynôme peut être noté indifféremment Aou $A(X)$.

2 Divisibilité dans $\mathbb{K}[\mathbb{X}]$

2.1 Multiples, diviseurs

Définition 9 Soient $A, B \in \mathbb{K}[X]$ on dit que B est un multiple (respectivement A est un diviseur) de A (resp. de B) si il existe $C \in \mathbb{K}[X]$ tel que $B = A\,C$.
On note alors $A|B$.

Remarque 2
1. Le polynôme 0 est multiple de tout polynôme mais n'est divseur que de lui même.
2. $A, B \in \mathbb{K}[X]$, $A|B$ et $B \neq 0 \Longrightarrow deg(B) \geq deg(A)$.
3. $A, B \in \mathbb{K}[X]$, $A|B$ et $B|A \Longleftrightarrow \exists \lambda \in \mathbb{K}^*,\ B = \lambda A$.
   On dit alors que les polynômes A et B sont associés.

2.2 Division euclidienne

Théorème 10 Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]^*$, il existe un unique couple (Q, R) de polynômes tel que $A = BQ + R$ avec $\deg(R) < \deg(B)$.
R est appelé reste de la division euclidienne de A par B et Q est appelé quotient de la division euclidienne de A par B.

Exemple 11 $A = X^5 + 4X^4 + 2X^3 + X^2 - X - 1,\ B = X^3 - 2X + 3,\ \ A = B(X^2 + 4X + 4) + 6X^2 - 5X - 13$.
$Q = X^2 + 4X + 4,\ \ R = 6X^2 - 5X - 13$.

Remarque 3 Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X]^*$, A est divisible par B si et seulement si le reste de la division euclidienne de A par B est nul.

3 Racines d'un polynôme

3.1 Racines

Définition 12 A tout polynôme $P = \sum_{k=0}^{n} a_k X^k$ de $\mathbb{K}[X]$ on associe une application $\widetilde{P}$ appelée fonction polynôme associée à P définie de la manière suivante :

$$\begin{array}{cccc} \widetilde{P} & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & \sum_{k=0}^{n} a_k x^k \end{array}$$

Définition 13 Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$ on dit que a est une racine de P si $\widetilde{P}(a) = 0$.

Proposition 14 Le reste de la division du polynôme P par $(X - a)$ est $\widetilde{P}(a)$.

Corollaire 15 Le polynôme P est divisible par $(X - a)$ si et seulement si $\widetilde{P}(a) = 0$.

Proposition 16 Si $\alpha_1, \alpha_2, \cdots, \alpha_p$ sont p racines distinctes de A, alors $\prod_{i=1}^{p}(X - \alpha_i)|A$.

Corollaire 17 Soit $A \in \mathbb{K}[X]$ de degré n admettant n racines distinctes $\alpha_1, \alpha_2, \cdots, \alpha_n$, on a :
$A = \lambda \prod_{i=1}^{n}(X - \alpha_i)$ où λ est le coefficient dominant de A.

Théorème 18 Soit $P \in \mathbb{K}_n[X]$, si P admet au moins $n+1$ racines distinctes alors $P = 0$.
Un polynôme de $\mathbb{K}_n[X]$admet au plus n racines distinctes.

Théorème 19 Si K est infini alors l'application qui à un polynôme associe sa fonction polynôme est une bijection. On identifiera $\widetilde{P}$ et P sur $\mathbb{K}$ par la suite.

3.2 Racines multiples

Définition 20 Soient $A \in \mathbb{K}[X]$, $a \in \mathbb{K}$, $p \in \mathbb{N}^*$. Le scalaire a est racine d'ordre p de A si :
$(X-a)^p | A$ et A n'est pas divisible par$(X-a)^{p+1}$. Si $p \geq 2$ on dit que a est une racine multiple.

Proposition 21 Le scalaire $a \in \mathbb{K}$ est racine d'ordre p de $A \in \mathbb{K}[X]$ si et seulement si il existe $B \in \mathbb{K}[X]$ tel que :
$A = (X-a)^p B$ et $B(a) \neq 0$.

Proposition 22 Soient $\alpha_1, \alpha_2, \cdots, \alpha_p$, p racines distinctes de $A \in \mathbb{K}[X]$ d'ordre de multiplicité respectifs $r_1, r_2, \cdots, r_p$ alors
$\prod_{i=1}^{p} (X-\alpha_i)^{r_i} | A$

Corollaire 23 Un polynôme de degré n a au plus n racines comptées avec leur ordre de multiplicité.

3.3 Polynômes scindés

Définition 24 Le polynôme $A \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si $A = \lambda \prod_{i=1}^{n} (X-\alpha_i),\ \lambda, \alpha_1, \cdots \alpha_n \in \mathbb{K}$.

Les racines pouvant ne pas être distinctes, on peut écrire $A = \lambda \prod_{i=1}^{p} (X-\alpha_i)^{r_i},\ \lambda \in \mathbb{K},\ r_1 + \cdots + r_p = n$.

Définition 25 On défnit :

$$\sigma_1 = \sum_{i=1}^{n} x_i,\ \ \sigma_2 = \sum_{1 \leq i < j \leq n} x_i x_j,\ \ \cdots,\ \sigma_k = \sum_{1 \leq i_1 < i_2 \ldots < i_k \leq n} a_{i_1} a_{i_2} \ldots . a_{i_k},\ \cdots,\ \sigma_n = x_1 x_2 \cdots x_n.$$

Les $\sigma_i,\ i \in [\![1, n]\!]$ sont appelés fonctions symétriques des racines. Il faut noter qu'une racine d'ordre k est répétée k fois..

Proposition 26 Relations entre les coefficients et les racines en écrivant $A = \sum_{k=0}^{n} a_k X^k$, on a :

$$A = a_n \left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^p \sigma_p X^{n-p} + \cdots + (-1)^n \sigma_n \right),\ \ \sigma_k = (-1)^k \frac{a_{n-k}}{a_n},\ k \in [\![1, n]\!].$$

Exemple 27 $A = a_3 X^3 + a_2 X^2 + a_1 X + a_0 = a_3 (X-x_1)(X-x_2)(X-x_3)$ polynôme scindé de degré 3. En développant on obtient :
$A = a_3 (X^3 - (x_1+x_2+x_3) X^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3) X - x_1 x_2 x_3) = a_3 (X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3)$.

3.4 Polynômes de Lagrange

Proposition 28 Soient $n \in \mathbb{N}^*$ et $x_0, x_1, \cdots x_n \in \mathbb{K}$ $n+1$ scalaires deux à deux distincts. Pour tout $i \in [\![0, n]\!]$ il existe un unique polynôme L_i tel que :
$L_i \in \mathbb{K}_n[X]$ et $\forall j \in [\![0, n]\!],\ L_i(x_j) = \begin{cases} 0 & \text{si } j \neq i \\ 1 & \text{si } j = i \end{cases}$.
La famille de polynômess $(L_0, L_1, \cdots, L_n)$ est la famille de polynômes de Lagrange associée à la famille de scalaires $(x_0, x_1, \cdots, x_n)$.

Proposition 29 Avec les notations précédentes on a :

$$L_i(X) = \prod_{j=1,\ j \neq i}^{n} \left(\frac{X - x_j}{x_i - x_j} \right).$$

Proposition 30 Soient $n \in \mathbb{N}^*$ et $y_0, x_1, \cdots y_n \in \mathbb{K}$ $n+1$ scalaires quelconques. On considère $x_0, x_1, \cdots x_n \in \mathbb{K}$ $n+1$ scalaires deux à deux distincts. Il existe un polynôme unique $P \in \mathbb{K}_n[X]$ tel que $\forall i \in [\![0, n]\!],\ P(x_i) = y_i$.

$P(X) = \sum_{k=1}^{n} y_k\, L_k(X)$ est ce polynôme.

Exemple 31 Déterminer P tel que $P(1) = 2,\ P(2) = 3,\ P(3) = 6$.
$P(X) = \frac{(X-2)(X-3)}{2}.2 + \frac{(X-1)(X-3)}{-1}.3 + \frac{(X-1)(X-2)}{2}.6 = X^2 - 2X + 3.$

4 Polynôme dérivé

4.1 Définition

Soit $A = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On définit le polynôme dérivé A' par :
$A' = 0$ si $A = a \in \mathbb{K}$.
$A' = \sum_{k=1}^{n} a_k X^{k-1}$ si $n \geq 1$.

Remarque 4 Si $deg(A) > 0$ on a $deg(A') = deg(A) - 1$.

Proposition 32 $\forall (P, Q) \in \mathbb{K}[X]^2,\ \forall \lambda, \mu \in \mathbb{K},\ (\lambda P + \mu Q)' = \lambda P' + \mu Q'$.
$\forall (P, Q) \in \mathbb{K}[X]^2,\ (PQ)' = P'Q + QP'$.

4.2 Polynômes dérivés successifs

Définition 33 Soit $r \in \mathbb{N},\ A \in \mathbb{K}[X]$. On définit les polynômes dérivés successifs de A par :
$A^{(0)} = A,\ \forall r \in \mathbb{N},\ A^{(r+1)} = \left(A^{(r)}\right)'$.

Remarque 5 $\forall (P, Q) \in \mathbb{K}[X]^2,\ \forall \lambda, \mu \in \mathbb{K},\ (\lambda P + \mu Q)^{(r)} = \lambda P^{(r)} + \mu Q^{(r)}$.

Proposition 34 Formule de Leibniz
Soient $A, B \in \mathbb{K}[X]$, on a
$(A\,B)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} A^{(k)}\, B^{(n-k)}$.

Théorème 35 Formule de Taylor : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Supposons $\deg(P) = n$, on a :

$$P(X + a) = \sum_{j=0}^{n} \frac{P^{(j)}(a)}{j!} X^j \text{ equivalent a } P(X) = \sum_{j=0}^{n} \frac{P^{(j)}(a)}{j!} (X - a)^j.$$

Théorème 36

$$a \text{ est une racine d'ordre de multiplicité } k \iff \begin{cases} \forall i \in [\![0, k-1]\!],\ P^{(i)}(a) = 0 \\ P^{(k)}(a) \neq 0 \end{cases}$$

5 Plus grand commun diviseur et plus petit commun multiple

Algorithme 37 d'Euclide :
Soient A et B deux polynômes non nuls, soit R le reste de la division euclidienne de A par B ,
si $R \neq 0$ alors $\{Q \mid Q|A \text{ et } Q|B\} = \{Q \mid Q|B \text{ et } Q|R\}$,
si $R = 0$ alors $\{Q \mid Q|A \text{ et } Q|B\} = \{Q \mid Q|B\}$.

Théorème 38 Soient A et B deux polynômes, il existe un unique polynôme unitaire ou nul D tel que :
1) $D|A$ *et* $D|B$,
2) $Q|A$ *et* $Q|B \Rightarrow Q|D$.
Ces deux conditions sont équivalentes à dire que l'ensemble des diviseurs communs à A et B sont les diviseurs de D.
Ce polynôme est appelé plus grand commun diviseur de A et B et est noté $A \wedge B$ ou encore $p\gcd(A, B)$.
Il existe de plus deux polynômes U et V tels que $D = AU + BV$, il n'y a pas unicité du couple (U, V).

Remarque 6 $A \wedge B$ est le polynôme unitaire de degré maximal parmi les diviseurs communs de A et B.
$A \wedge B = 0 \Longleftrightarrow A = B = 0$.

Unicité : si D_1 et D_2 sont solutions on a $D_1|D_2$ et $D_2|D_1$ ce qui entraine $D_1 = D_2$.

Existence : Récurrence complète sur $m = deg(B)$.
H_m : Si $deg(B) < m$ alors pour tout $A \in \mathbb{K}[X]$ il existe D nul ou unitaire tel que les diviseurs communs à A et B sont les diviseurs de D et il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = D$.

Exemple 39 $A = X^4 + X^3 - 2X + 1$ et $B = X^2 + X + 1$.

Proposition 40 $\forall (A, B, C) \in \mathbb{K}[\mathbb{X}]^3$, $\forall (a, b) \in (\mathbb{K}^*)^2$ on a :
1) $(aA \wedge bB) = A \wedge B$,
2) $A \wedge B = B \wedge A$,
3) $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.
4) Si P est un polynôme unitaire on a $(PA) \wedge (PB) = P\,(A \wedge B)$.

5.1 Polynômes premiers entre eux

Définition 41 Les polynômes A et B non nuls sont dits premiers entre eux si leur $p\,\mathrm{gcd}$ est 1.
Les polynômes non nuls $A_1, ..., A_n$ sont dits premiers entre eux dans leur ensemble si leurs seuls diviseurs communs sont les polynômes constants non nuls.

Théorème 42 de Bezout :

$$A \text{ et } B \text{ sont premiers entre eux} \Leftrightarrow \exists (U, V) \in \mathbb{K}[X]^2 \;\; AU + BV = 1$$

Proposition 43 Soient A et B deux polynômes premiers entre eux.
1) $\forall P \in \mathbb{K}[X]$, $\exists !(U, V) \in \mathbb{K}[X]^2$ tel que $P = AU + BV$ et $\deg(V) < \deg(A)$,
2) si $\deg(A) \geq 1$ et $\deg(B) \geq 1$ alors $\exists !(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$ et $\deg(V) < \deg(A)$ et $\deg(U) < \deg(B)$.

Théorème 44 de Gauss :

$$A|BC \text{ et } A \wedge B = 1 \Rightarrow A|C$$

Proposition 45 1) $A \wedge B_1....B_n = 1 \Leftrightarrow \forall k \in \{1, ..., n\}$, $A \wedge B_k = 1$,
2) Si $A_1, ..., A_n$ sont premiers entre eux deux à deux et si $\forall k \in \{1, ..., n\}$ $A_k|B$ alors $A_1...A_n|B$.

5.2 Plus petit commun multiple

Théorème 46 Soient A et B deux polynômes non nuls. Il existe un unique polynôme unitaire M tel que :
1) $A|M$ et $B|M$,
2) $A|Q$ et $B|Q \Rightarrow M|Q$.
Ce polynôme est appelé plus petit commun multiple de A et B et est noté $A \vee B$ ou encore $ppcm(A, b)$.

Unicité : Démonstration identique à celle du pgcd.
Existence : M est le polynôme unitaire multiple de A et de B, de degré minimal parmi les multiples communs non nuls de A et de B.

Proposition 47 $\forall (A, B, C) \in \mathbb{K}[\mathbb{X}]^3$, $\forall (a, b) \in (\mathbb{K}^*)^2$ on a :
1) $(aA \vee bB) = A \vee B$,
2) $A \vee B = B \vee A$,
3) $(A \vee B) \vee C = A \vee (B \vee C)$.
4) Si P est un polynôme unitaire on a $(PA) \vee (PB) = P\,(A \vee B)$.

Proposition 48 Soient A et B deux polynômes de coefficient dominant respectif a et b on a : $AB = ab(A \wedge B)(A \vee B)$.

6 Décomposition d'un polynôme

Définition 49 Un polynôme P est dit irréductible si
1) $\deg(P) \geq 1$
2) les seuls diviseurs de P sont de la forme λ ou λP avec $\lambda \in \mathbb{K}^*$.

Proposition 50 Soit P un polynôme irréductible

$$A \wedge P = 1 \Leftrightarrow P \text{ n'est pas un diviseur de A}$$

Proposition 51 Les polynômes de degré 1 sont irréductibles.

Proposition 52 Tout polynôme de degré ≥ 1 admet au moins un diviseur irréductible.

Théorème 53 Soit A un polynôme non constant de $\mathbb{K}[X]$, il existe une famille $P_1, ...P_n$ de polynômes unitaires irréductibles deux à deux premiers entre eux , il existe $(\alpha_1, ..., \alpha_n) \in (\mathbb{N}^*)^n$ et il existe $\lambda \in \mathbb{K}$ tel que

$$A = \lambda P_1^{\alpha_1} .....P_n^{\alpha_n}$$

et cette décomposition est unique à l'ordre des facteurs près.

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

Théorème 54 de d'Alembert-Gauss : (admis)
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine.

Corollaire 55 Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.

Corollaire 56 Tout polynôme de $\mathbb{C}[X]$ est scindé.

Définition 57 On appelle polynôme conjugué du polynôme $P = \sum_{k=0}^{n} a_k X^k$, le polynôme $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k$.

Proposition 58 Soit P un polynôme de $\mathbb{C}[X]$.
1) $\overline{\overline{P}} = P$,
2) $\deg(\overline{P}) = \deg(P)$ et $val(\overline{P}) = val(P)$,
3) si a est une racine de P, alors $\overline{a}$ est une racine de $\overline{P}$ avec la même multiplicité.

Théorème 59 Les polynômes irréductibles de $\mathbb{R}[X]$ sont
1) les polynômes de degré un,
2) les polynômes de degré deux de disciminant strictement négatif.