Polynômes en une indéterminée

$\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

I. Construction de l'anneau des polynômes

1°) Polynômes

Déf : On appelle polynôme à coefficients dans $\mathbb{K}$ en l'indéterminée X tout objet noté $P=\sum_{n=0}^{+\infty}a_nX^n=a_0+a_1X+...+a_nX^n+...$ où $(a_n)_{n\in\mathbb{N}}$ est une suite d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang, appelée suite des coefficients de P. On note $\mathbb{K}[X]$ l'ensemble de ces éléments.

Déf : Deux polynômes $P=\sum_{n=0}^{+\infty}a_nX^n$ et $Q=\sum_{n=0}^{+\infty}b_nX^n\in\mathbb{K}[X]$ sont dits égaux ssi ils ont les mêmes coefficients. Ainsi : $P=Q\Leftrightarrow\forall n\in\mathbb{N},a_n=b_n$.

Déf : Soit $C\in\mathbb{K}$. On appelle polynôme constant égal à C le polynôme $C+0.X+\cdots=C$.

Déf : On appelle monôme, tout polynôme de la forme : $0+0.X+\cdots+0.X^{n-1}+aX^n+0.X^{n+1}+\cdots=aX^n$ avec $a\in\mathbb{K}$, $n\in\mathbb{N}$.

Déf : Soit $P=\sum_{n=0}^{+\infty}a_nX^n\in\mathbb{K}[X]$. On dit que P est un polynôme pair (resp. impair) ssi $\forall p\in\mathbb{N},a_{2p+1}=0$ (resp. $a_{2p}=0$).

2°) L'espace vectoriel des polynômes

Déf : Soit $P=\sum_{n=0}^{+\infty}a_nX^n\in\mathbb{K}[X]$ et $Q=\sum_{n=0}^{+\infty}b_nX^n\in\mathbb{K}[X]$.

On définit le polynôme $P+Q\in\mathbb{K}[X]$ par : $P+Q=\sum_{n=0}^{+\infty}(a_n+b_n)X^n$.

Déf : Soit $P=\sum_{n=0}^{+\infty}a_nX^n\in\mathbb{K}[X]$ et $\lambda\in\mathbb{K}$.

On définit le polynôme $\lambda.P\in\mathbb{K}[X]$ par : $\lambda.P=\sum_{n=0}^{+\infty}(\lambda.a_n)X^n$.

Théorème :

$(\mathbb{K}[X],+,.)$ est un $\mathbb{K}$-espace vectoriel dont l'élément nul est le polynôme nul.

3°) Degré

Déf : On appelle degré de $P=\sum_{n=0}^{+\infty}a_nX^n\in\mathbb{K}[X]$ polynôme non nul le plus grand $n\in\mathbb{N}$ tel que $a_n\neq0$

On le note $n=\deg P$.

Déf : Le coefficient a_n est alors appelé coefficient dominant de P.

Convention :

Si $P=0$, on pose $\deg P=-\infty$.

Prop : $\forall P\in\mathbb{K}[X],\forall\lambda\in\mathbb{K},\deg(\lambda.P)=\begin{cases}\deg P \text{ si } \lambda\neq0\\ -\infty \text{ si } \lambda=0\end{cases}$.

Prop : $\forall P,Q\in\mathbb{K}[X],\deg(P+Q)\leq\max(\deg P,\deg Q)$

avec égalité lorsque $\deg(P)\neq\deg(Q)$.

4°) Le sous-espace vectoriel $\mathbb{K}_n[X]$

Déf : Pour $n \in \mathbb{N}$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur à n. Ainsi $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] / \deg P \leq n\}$.

Théorème :

$\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ de dimension $n+1$ dont la famille $\mathcal{B} = (1, X, ..., X^n)$ est une base, dite base canonique.

Cor : Il en découle que $\dim \mathbb{K}[X] = +\infty$.

5°) L'anneau des polynômes

On définit une multiplication sur $\mathbb{K}[X]$ en imitant le principe de multiplication des expressions polynomiales.

Déf : Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[X]$ et $Q = \sum_{n=0}^{+\infty} b_n X^n \in \mathbb{K}[X]$.

On définit le polynôme PQ par : $PQ = \sum_{n=0}^{+\infty} c_n X^n$ avec

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k+\ell=n} a_k b_\ell = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 .$$

Théorème :

$(\mathbb{K}[X], +, \times)$ est un anneau commutatif d'élément nul le polynôme nul et d'élément unité le polynôme constant égal à 1.

6°) Degré d'un produit

Théorème :

$\forall P, Q \in \mathbb{K}[X]$, $\deg PQ = \deg P + \deg Q$

Cor : Les polynômes inversibles sont les polynômes constants non nuls.

Cor : $\forall P, Q \in \mathbb{K}[X], PQ = 0 \Rightarrow P = 0$ ou $Q = 0$.

Ainsi, dans $\mathbb{K}[X]$, il n'y a pas de diviseurs de zéro.

7°) Fonctions polynomiales

a) valeur d'un polynôme en un point

Déf : Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{K}[X]$ et $x \in \mathbb{K}$.

On appelle valeur de P en x le scalaire $P(x) = a_0 + a_1 x + \cdots + a_n x^n$.

Prop : Soit $P, Q \in \mathbb{K}[X]$, $\lambda, \mu \in \mathbb{K}$ et $x \in \mathbb{K}$.

$(\lambda.P + \mu.Q)(x) = \lambda P(x) + \mu Q(x)$, $(PQ)(x) = P(x)Q(x)$ et $(P \circ Q)(x) = P(Q(x))$.

Déf : On appelle racine (ou zéro) d'un polynôme $P \in \mathbb{K}[X]$ tout $x \in \mathbb{K}$ tel que $P(x) = 0$.

Déf : On appelle équation algébrique, tout équation de la forme $P(x) = 0$ d'inconnue $x \in \mathbb{K}$ et où $P \in \mathbb{K}[X]$.

Le degré de P est alors appelé degré de l'équation $P(x) = 0$.

b) fonction polynomiale

Déf : On appelle fonction polynomiale associée à $P \in \mathbb{K}[X]$ définie sur $\mathcal{D} \subset \mathbb{K}$ l'application :

$$\tilde{P} : \begin{cases} \mathcal{D} \to \mathbb{K} \\ x \mapsto \tilde{P}(x) = P(x) \end{cases}.$$

Lorsque $\mathcal{D} = \mathbb{K}$, on parle de fonction polynomiale associée à P.

Prop : Soit $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$. $\widetilde{\lambda.P + \mu.Q} = \lambda.\widetilde{P} + \mu.\widetilde{Q}$, $\widetilde{P \times Q} = \widetilde{P} \times \widetilde{Q}$.

8°) Composition de polynômes

Déf : Soit $P=\sum_{n=0}^{+\infty}a_nX^n\in\mathbb{K}[X]$ et $Q\in\mathbb{K}[X]$.

On définit le polynôme composé $P\circ Q$ (aussi noté $P(Q)$) par : $P\circ Q=P(Q)=\sum_{n=0}^{+\infty}a_nQ^n\in\mathbb{K}[X]$.

Prop : $\forall P,Q,R\in\mathbb{K}[X]$ et $\forall\lambda,\mu\in\mathbb{K}$:

$(\lambda.P+\mu.Q)\circ R=\lambda.P\circ R+\mu.Q\circ R$ et $(PQ)\circ R=(P\circ R)\times(Q\circ R)$.

II. Dérivation

1°) Dérivée première

Déf : Soit $P=\sum_{n=0}^{+\infty}a_nX^n=a_0+a_1X+...+a_nX^n+...\in\mathbb{K}[X]$.

On appelle polynôme dérivé de P, le polynôme noté P' défini par :

$P'=a_1+2a_2X+\cdots+na_nX^{n-1}+\cdots=\sum_{n=1}^{+\infty}na_nX^{n-1}=\sum_{n=0}^{+\infty}(n+1)a_{n+1}X^n$.

Prop : Soit $P\in\mathbb{K}[X]$.

Si P est constant : $P'=0$.

Si P non constant : $\deg P'=\deg P-1$ et $\text{coeff}(P')=\deg P.\text{coeff}(P)$.

Dans les deux cas : $\deg P'\leq\deg P-1$.

Cor : $P'=0\Leftrightarrow P$ polynôme constant.

Prop : $\forall\lambda,\mu\in\mathbb{K}$, $\forall P,Q\in\mathbb{K}[X]$, $(\lambda P+\mu Q)'=\lambda P'+\mu Q'$ et $(PQ)'=P'Q+PQ'$.

Cor : $(P_1P_2...P_n)'=\sum_{i=1}^{n}(P_1...\hat{P}_i...P_n)P_i'$ et $(P^n)'=nP'P^{n-1}$.

Prop : $\forall P,Q\in\mathbb{K}[X]$, $(P\circ Q)'=Q'\times P'\circ Q$.

Déf : Soit $P\in\mathbb{K}[X]$. On appelle polynôme primitif de P tout polynôme Q tel que $Q'=P$.

2°) Dérivée d'ordre supérieur

Soit $D:\mathbb{K}[X]\to\mathbb{K}[X]$ défini par $D(P)=P'$.

D est un endomorphisme de $\mathbb{K}[X]$.

On note $D^0=\text{Id}, D^1=D, D^2=D\circ D,\ldots,D^n=D\circ D\circ\ldots\circ D$ (n termes)

Déf : Soit $n\in\mathbb{N}$ et $P\in\mathbb{K}[X]$. Le polynôme $P^{(n)}=D^n(P)$ est appelé polynôme dérivé d'ordre n de P.

Prop : Soit $P\in\mathbb{K}[X]$ et $n\in\mathbb{N}$.

Si $\deg P<n$ alors $\deg P^{(n)}=-\infty$.

Si $\deg P\geq n$ alors $\deg P^{(n)}=\deg P-n$.

Prop : $\forall\lambda,\mu\in\mathbb{K},\forall P,Q\in\mathbb{K}[X]$:

$(\lambda P+\mu Q)^{(n)}=\lambda P^{(n)}+\mu Q^{(n)}$ et $(PQ)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}$.

3°) Formule de Taylor

Théorème :

$\forall P\in\mathbb{K}[X],\forall a\in\mathbb{K},P=\sum_{n=0}^{+\infty}\frac{P^{(n)}(a)}{n!}(X-a)^n$.

III. Arithmétique des polynômes

1°) Divisibilité

a) polynômes associés

Déf : Soit $P, Q \in \mathbb{K}[X]$. On dit que P et Q sont associés ssi $\exists \lambda \in \mathbb{K}^*, P = \lambda Q$.

Prop : Si P et Q sont associés et ont mêmes coefficients dominants alors $P = Q$.

Déf : Un polynôme $P \in \mathbb{K}[X]$ est dit unitaire (ou normalisé) ssi son coefficient dominant est égal à 1.

Prop : Tout polynôme $P \in \mathbb{K}[X]$ non nul est associé à unique polynôme unitaire.

b) relation de divisibilité

Déf : Soit $A, B \in \mathbb{K}[X]$. On dit que A divise B ssi $\exists U \in \mathbb{K}[X], B = AU$.
On note alors $A \mid B$.

Déf : Soit $A \in \mathbb{K}[X]$. On note $\text{Div}(A)$ l'ensemble des diviseurs et $\text{Mul}(A)$ l'ensemble des multiples de A.

Prop : Soit A et B des polynômes respectivement associés à C et D. On a $A \mid B \Leftrightarrow C \mid D$.

c) propriétés de la divisibilité

Prop : $\forall A, B, C \in \mathbb{K}[X]$
$A \mid B$ et $B \mid C \Rightarrow A \mid C$,
$A \mid B$ et $B \mid A \Rightarrow A$ et B associés,
$A \mid B$ et $B \neq 0 \Rightarrow \deg A \leq \deg B$,
$A \mid B$ et $\deg A = \deg B \Rightarrow A$ et B associés.

Prop : $\forall A, B, C, D \in \mathbb{K}[X]$
$A \mid B$ et $A \mid C \Rightarrow A \mid B + C$,
$A \mid B$ et $C \mid D \Rightarrow AC \mid BD$,
$A \mid B \Rightarrow \forall n \in \mathbb{N}, A^n \mid B^n$.

2°) Division euclidienne

a) énoncé

Théorème :
$\forall A, B \in \mathbb{K}[X]$ avec $B \neq 0$, $\exists !(Q, R) \in \mathbb{K}[X]^2$ tel que :
$A = BQ + R$ et $\deg R < \deg B$
Les polynômes Q et R sont appelés quotient et reste de la division euclidienne de A par B.

b) applications

Prop : Soit $A, B \in \mathbb{K}[X]$ tels que $B \neq 0$. On a :
$B \mid A \Leftrightarrow$ le reste de la division euclidienne de A par B est nul.

Prop : Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. a est racine de $P \Leftrightarrow (X - a) \mid P$.

3°) Pgcd et ppcm de deux polynômes

a) pgcd

Déf : On note $\text{Div}(A, B) = \text{Div}(A) \cap \text{Div}(B)$ l'ensemble des diviseurs communs à A et B.

Prop : Si $A = BQ + R$ alors $\text{Div}(A, B) = \text{Div}(B, R)$.

Théorème :
Soit $A, B \in \mathbb{K}[X]$, il existe un unique polynôme $D \in \mathbb{K}[X]$ unitaire ou nul, tel que $\text{Div}(A, B) = \text{Div}(D)$.

Déf : Ce polynôme D est appelé pgcd des polynômes A et B.
On note $D = \text{pgcd}(A, B)$ ou $D = A \wedge B$.

Théorème : (Egalité de Bézout)

Si $D = \text{pgcd}(A,B)$ alors $\exists U,V \in \mathbb{K}[X]$ tels que $D = AU + BV$.

Prop : $\text{pgcd}(A,B) = \text{pgcd}(B,A)$.

Si $A \mid B$ alors $\text{pgcd}(A,B)$ est associé à A.

Prop : Si C est unitaire alors $\text{pgcd}(AC,BC) = \text{pgcd}(A,B) \times C$.

b) ppcm

Déf : On note $\text{Mul}(A,B) = \text{Mul}(A) \cap \text{Mul}(B)$ l'ensemble des multiples communs à A et B.

Théorème :

Soit $A,B \in \mathbb{K}[X]$, il existe un unique polynôme unitaire ou nul tel que $\text{Mul}(A,B) = \text{Mul}(M)$.

Déf : M est alors appelé ppcm de A et B.
On note $M = \text{ppcm}(A,B)$ ou $A \vee B$.

Prop : $\text{ppcm}(A,B) = \text{ppcm}(B,A)$

Si $A \mid B$ alors $\text{ppcm}(A,B)$ est associé à B.

Prop : Si C est unitaire alors $\text{ppcm}(AC,BC) = \text{ppcm}(A,B) \times C$.

4°) Polynômes premiers entre eux

a) définition

Déf : Deux polynômes A et B sont dits premiers entre eux ssi leurs seuls diviseurs communs sont les polynômes constants non nuls.
Ceci signifie encore $\text{pgcd}(A,B) = 1$. On note alors $A \wedge B = 1$.

b) théorème de Bézout

Théorème :

On a équivalence entre :
(i) A et B sont premiers entre eux,
(ii) $\exists U,V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Cor : $A \wedge B$ et $A \wedge C = 1 \Rightarrow A \wedge (BC) = 1$,
$A \wedge B_1 = 1, ..., A \wedge B_n = 1 \Rightarrow A \wedge (B_1 ... B_n) = 1$,
$A \wedge B = 1 \Rightarrow \forall m,n \in \mathbb{N}, A^m \wedge B^n = 1$.

c) théorème de Gauss

Théorème :

$A \mid BC$ et $A \wedge B = 1 \Rightarrow A \mid C$.

Théorème :

$A \mid C, B \mid C$ et $A \wedge B = 1 \Rightarrow AB \mid C$.

Cor : Si $A_1, ..., A_n$ sont des diviseurs de P deux à deux premiers entre eux
alors $A_1 ... A_n \mid P$.

d) produit du pgcd et du ppcm

Théorème :

$\forall A,B \in \mathbb{K}[X], \text{pgcd}(A,B) \times \text{ppcm}(A,B)$ est associé à AB.

5°) Décomposition en produit de facteurs irréductibles

Déf : Soit $P \in \mathbb{K}[X]$ un polynôme non constant.

On dit que P est irréductible dans $\mathbb{K}[X]$ ssi ses seuls diviseurs sont ses diviseurs triviaux.

Sinon, P est dit composé.

Prop : Soit $A \in \mathbb{K}[X]$ et P un polynôme irréductible de $\mathbb{K}[X]$.

Si $P \nmid A$ alors $P \wedge A = 1$.

Prop : Soit $A, B \in \mathbb{K}[X]$ et P un polynôme irréductible dans $\mathbb{K}[X]$.

$P \mid AB \Rightarrow P \mid A$ ou $P \mid B$.

Théorème :

Soit A un polynôme non constant de $\mathbb{K}[X]$.

$\exists \lambda \in \mathbb{K}^*, \exists N \in \mathbb{N}^*, \exists P_1, ..., P_N$ polynômes irréductibles de $\mathbb{K}[X]$ unitaires et deux à deux distincts et

$\exists \alpha_1, ..., \alpha_N \in \mathbb{N}^*$ tels que :

$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} ... P_N^{\alpha_N}$.

De plus cette décomposition est unique à l'ordre près des facteurs, on l'appelle décomposition primaire de A.

IV. Racines d'un polynôme

1°) Racines et degré

Prop : Soit $P \in \mathbb{K}[X]$.

Si $a_1, ..., a_n$ sont des racines deux à deux distinctes de P

alors $(X - a_1)...(X - a_n) \mid P$

Théorème :

Si P est un polynôme non nul alors P ne peut avoir plus de racines que son degré.

Cor : Un polynôme de degré n possède au plus n racines.
Une équation algébrique de degré $n \in \mathbb{N}$ possède au plus n solutions.

Cor : Soit $P \in \mathbb{K}_n[X]$.

Si P possède au moins $n+1$ racines alors $P = 0$.

Cor : Soit $P \in \mathbb{K}[X]$.

Si P possède une infinité de racines alors $P = 0$.

2°) Polynôme et fonction polynomiale

Soit $\mathcal{D}$ une partie infinie de $\mathbb{K}$.

Déf : On note $\mathcal{P}(\mathcal{D}, \mathbb{K})$ l'ensemble des fonctions polynomiales de $\mathcal{D}$ vers $\mathbb{K}$.

Théorème :

L'application qui à P associe $\tilde{P}$ est un isomorphisme du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]$ vers $\mathcal{P}(\mathcal{D}, \mathbb{K})$.

Cor : Si deux fonctions polynomiales prennent les mêmes valeurs une infinité de fois, c'est qu'elles sont issues du même polynôme. Ainsi :

$(\forall x \in \mathcal{D}, a_0 + a_1 x + a_2 x^2 + \cdots = b_0 + b_1 x + b_2 x^2 + \cdots) \Rightarrow \forall n \in \mathbb{N}, a_n = b_n$.

C'est le principe d'identification des coefficients des fonctions polynomiales.

3°) Multiplicité des racines

Déf : Soit $P \in \mathbb{K}[X]$ tel que $P \neq 0$ et $a \in \mathbb{K}$.

On appelle ordre de multiplicité de a en tant que racine de P le plus grand $\alpha \in \mathbb{N}$ tel que $(X - a)^\alpha \mid P$.

Si $\alpha = 0$ alors a n'est pas racine de P.
Si $\alpha = 1$ on parle de racine simple.
Si $\alpha \geq 2$ on parle de racine multiple (double, triple,…)

Convention :

Si $P = 0$ alors tout $a \in \mathbb{K}$ est dit racine de multiplicité $+\infty$ de P.

Prop : Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}$.

On a équivalence entre :
(i) a est racine de multiplicité α de P,
(ii) $(X - a)^\alpha \mid P$ et $(X - a)^{\alpha+1} \nmid P$,
(iii) $\exists Q \in \mathbb{K}[X]$ tel que $P = (X - a)^\alpha Q$ et $Q(a) \neq 0$.

Prop : Soit $P \in \mathbb{K}[X]$ et $a_1,...,a_n$ des racines deux à deux distinctes de P de multiplicités respectives au moins égales à $\alpha_1,...,\alpha_n$.

On a $(X-a_1)^{\alpha_1}...(X-a_n)^{\alpha_n} \mid P$.

Théorème :

Si P est un polynôme non nul alors la somme des multiplicités de ses racines ne peut excéder son degré.

Cor : Soit $P \in \mathbb{K}_n[X]$.

Si P admet des racines dont la somme des multiplicités est au moins $n+1$ alors $P=0$.

Cor : Soit P un polynôme de degré $n \in \mathbb{N}$.

Si P admet au moins n racines distinctes alors il n'y en n'a pas d'autres et celles-ci sont simples.

4°) Multiplicité et dérivation

Théorème :

Si a est racine de multiplicité $\alpha \in \mathbb{N}^*$ de P

alors a est racine de multiplicité $\alpha-1$ de P'.

Cor : Les racines de P sont simples ssi P et P' n'ont pas de racines communes.

Théorème :

Soit $P \in \mathbb{K}[X]$ non nul, $a \in \mathbb{K}$ et $\alpha \in \mathbb{N}^*$.

On a équivalence entre :

(i) a est racine d'ordre de multiplicité α de P,

(ii) $P(a)=P'(a)=...=P^{(\alpha-1)}(a)=0$ et $P^{(\alpha)}(a) \neq 0$.

V. Polynômes scindés

1°) Définition

Déf : Un polynôme $P \in \mathbb{K}[X]$ est dit scindé dans $\mathbb{K}[X]$ ssi

$\exists \lambda \in \mathbb{K}^*, \exists n \in \mathbb{N}^*, \exists x_1,\ldots,x_n \in \mathbb{K}, P=\lambda(X-x_1)...(X-x_n)$.

Théorème :

Soit $P \in \mathbb{K}[X]$ un polynôme non constant.

On a équivalence entre :

(i) P est scindé dans $\mathbb{K}[X]$,

(ii) La somme des multiplicités des racines de P égale son degré.

2°) Polynôme complexe

a) théorème de d'Alembert-Gauss

Théorème : (admis)

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

On dit que $\mathbb{C}$ algébriquement clos.

Cor : Les polynôme irréductibles de $\mathbb{C}[X]$ sont ceux de degré 1.

Théorème :

Soit $P \in \mathbb{C}[X]$ non constant.

$\exists \lambda \in \mathbb{K}^*, \exists N \in \mathbb{N}^*, \exists a_1,...,a_N \in \mathbb{C}$ deux à deux distincts et $\exists \alpha_1,...,\alpha_N \in \mathbb{N}^*$ tels que

$P=\lambda(X-a_1)^{\alpha_1}...(X-a_N)^{\alpha_N}$.

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

Cor : Tout polynôme non constant de $\mathbb{C}[X]$ est scindé.

Tout polynôme de $\mathbb{C}[X]$ de degré $n \in \mathbb{N}$ possède n racines comptées avec multiplicité.

Toute équation algébrique complexe de degré $n \in \mathbb{N}^*$ possède n solutions complexes comptées avec multiplicité.

b) arithmétique et racines

Prop : Soit $A,B\in\mathbb{C}[X]$. On a équivalence entre :

(i) $A\mid B$,

(ii) les racines de A sont aussi racines de B de multiplicité au moins égale.

Prop : Soit $A,B\in\mathbb{C}[X]$. On a équivalence entre :

(i) $A\wedge B=1$,

(ii) A et B n'ont pas de racines en commun.

c) polynôme conjugué

Déf : Soit $P=a_nX^n+...+a_1X+a_0\in\mathbb{C}[X]$.

On appelle polynôme conjugué de P le polynôme $\overline{P}=\overline{a}_nX^n+...+\overline{a}_1X+\overline{a}_0\in\mathbb{C}[X]$.

Prop : Soit $P,Q\in\mathbb{C}[X]$.

$\overline{\overline{P}}=P$, $\overline{P+Q}=\overline{P}+\overline{Q}$, $\overline{PQ}=\overline{P}\overline{Q}$,

$P\mid Q\Leftrightarrow\overline{P}\mid\overline{Q}$,

$\forall a\in\mathbb{C},\overline{P(a)}=\overline{P}(\overline{a})$.

Prop : Soit $P\in\mathbb{C}[X]$, $a\in\mathbb{C}$ et $\alpha\in\mathbb{N}$.

On a équivalence entre :

(i) a est racine de multiplicité α de P,

(ii) $\overline{a}$ est racine de multiplicité α de $\overline{P}$.

3°) Polynôme réel

Déf : Soit $P\in\mathbb{R}[X]$. On appelle racine complexe de P toute racine de P vu comme polynôme complexe.

Prop : Soit $P\in\mathbb{R}[X]$ un polynôme de degré $n\in\mathbb{N}$. P admet exactement n racines complexes comptées avec multiplicité.

Prop : Les racines complexes de $P\in\mathbb{R}[X]$ sont deux à deux conjuguées et deux racines conjuguées ont même multiplicité.

Prop : Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

+ les polynômes de degré 1,

+ les polynômes de degré 2 de discriminant <0 (i.e. sans racines réelles).

Théorème :

Soit $P\in\mathbb{R}[X]$ non constant.

$\exists\lambda\in\mathbb{R}^*$, $\exists N,M\in\mathbb{N}$,

$\exists a_1,...,a_N\in\mathbb{R}$ deux à deux distincts,

$\exists(p_1,q_1),...,(p_M,q_M)\in\mathbb{R}^2$ deux à deux distincts, tels que $\Delta_j=p_j^2-4q_j<0$, $\exists\alpha_1,...,\alpha_N\in\mathbb{N}*$ et

$\exists\beta_1,...,\beta_M\in\mathbb{N}*$ tels que :

$$P=\lambda\prod_{i=1}^{N}(X-a_i)^{\alpha_i}\prod_{j=1}^{M}(X^2+p_jX+q_j)^{\beta_j}.$$

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

Cor : Les polynômes de degré impair possèdent au moins une racine réelle.

4°) Relations entre racines et coefficients d'un polynôme scindé

Soit $P=a_nX^n+\cdots+a_1X+a_0$ un polynôme scindé de degré $n\in\mathbb{N}^*$ réel ou complexe.

Soit $x_1,...,x_n$ les racines de P comptées avec multiplicité.

On a $P=a_nX^n+\cdots+a_1X+a_0=a_n(X-x_1)\ldots(X-x_n)$.

En développant le second membre, on peut exprimer les coefficients de P en fonction de ses racines.

Déf : Soit $n \in \mathbb{N}^*$ et $x_1,\ldots,x_n \in \mathbb{K}$.

On appelle expressions symétriques élémentaires des $x_1,...,x_n$ les quantités suivantes :

$\sigma_1 = \sum_{i=1}^{n} x_i$, $\sigma_2 = \sum_{1\le i<j\le n} x_i x_j$, $\sigma_3 = \sum_{1\le i<j<k\le n} x_i x_j x_k$, …, $\sigma_p = \sum_{1\le i_1<i_2<\ldots<i_p\le n} x_{i_1} x_{i_2} \ldots x_{i_p}$ (pour $1 \le p \le n$),

…, $\sigma_n = x_1 x_2 \ldots x_n$.

Ainsi σ_p apparaît comme étant la somme de tous les produits possibles de p éléments d'indices distincts choisis dans $x_1,...,x_n$.

Prop : Soit $n \in \mathbb{N}^*$, $x_1,\ldots,x_n \in \mathbb{K}$ et $\sigma_1,\ldots,\sigma_n$ les expressions symétriques élémentaires en les $x_1,...,x_n$. On a

$(X-x_1)\ldots(X-x_2) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^k \sigma_k X^{n-k} + \cdots + (-1)^n \sigma_n$.

Théorème :

Soit $P = a_n X^n + ... + a_1 X + a_0$ un polynôme de degré $n \in \mathbb{N}*$.

et $x_1,...,x_n \in \mathbb{K}$. On a équivalence entre :

(i) $x_1,...,x_n$ sont les racines de P comptées avec multiplicité,

(ii) $\forall 1 \le k \le n, \sigma_k = \dfrac{(-1)^k a_{n-k}}{a_n}$.

En Particulier :

Soit $P = aX^2 + bX + c$ avec $a \neq 0$.

x_1 et x_2 sont les racines de P comptées avec multiplicité ssi $\begin{cases} x_1 + x_2 = -b/a \\ x_1 x_2 = c/a \end{cases}$.

En Particulier :

Soit $P = aX^3 + bX^2 + cX + d$ avec $a \neq 0$.

x_1, x_2, x_3 sont les racines de P comptées avec multiplicité ssi $\begin{cases} x_1 + x_2 + x_3 = -b/a \\ x_1 x_2 + x_2 x_3 + x_3 x_1 = c/a \\ x_1 x_2 x_3 = -d/a \end{cases}$.