Cours de mathématiques M.P.S.I.

D'après les cours de M. De Granrut

Henriet Quentin
Ausseil Lucas
Perard Arsène
Philipp Maxime

Polynômes à une indéterminée

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

I. L'ensemble $\mathbb{K}[X]$

I.1. Suite presque nulle

Définition :

On appelle polynôme à 1 indéterminée à coefficient dans $\mathbb{K}$ toute suite $(a_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telle que :
$\exists N\in\mathbb{N}$ tel que $\forall n>N,\ a_n=0$.

Opérations :

Soient $A=(a_n)_{n\in\mathbb{N}}$ et $B=(b_n)_{n\in\mathbb{N}}$
$\exists N\in\mathbb{N}$ tel que $\forall n>N,\ a_n=0$ $\quad$ $\exists M\in\mathbb{N}$ tel que $\forall n>M\ , b_n=0$

$C=A+B \quad C=(c_n)_{n\in\mathbb{N}} \quad \forall n\in\mathbb{N},\ c_n=a_n+b_n$

$D=A\times B \quad D=(d_n)_{n\in\mathbb{N}} \quad \forall n\in\mathbb{N},\ d_n=\sum_{k=0}^{n} a_k b_{n-k}$

$E=\lambda.A \quad E=(e_n)_{n\in\mathbb{N}} \quad \forall n\in\mathbb{N},\ e_n=\lambda.a_n$

Proposition :

$A+B$, $A\times B$ et $\lambda.A$ sont des polynômes.

Preuve :

Il est évident que $(c_n),(d_n),(e_n)\in\mathbb{K}^{\mathbb{N}}$. Il reste à prouver qu'elles sont presques nulles.

$\forall n>\max(N,M),\quad c_n=a_n+b_n=0$

$\forall n>N,\quad e_n=\lambda.a_n=0$

$$\forall n>N+M,\quad d_n=\sum_{k=0}^{n} a_k b_{n-k}=\underbrace{\sum_{k=0}^{N} a_k \underbrace{b_{n-k}}_{=0}}_{\text{car } n-k\leqslant n-N<M}+\underbrace{\sum_{k=N+1}^{n} \underbrace{a_k}_{=0} b_{n-k}}_{\text{car } k\geqslant N+1>N}=0$$

Remarque :

$$d_{N+M}=\underbrace{\sum_{k=0}^{N-1} a_k \underbrace{b_{N+M-k}}_{=0}}_{\text{car } N+M-k\geqslant M+1>M}+a_N b_M+\underbrace{\sum_{k=N+1}^{N+M} \underbrace{a_k}_{=0} b_{N+M-k}}_{\text{car } k>N}$$

Donc $d_{N+M}=a_N b_M$

Propriétés des opérations :

$+$: loi associative et commutative
neutre : $(0,0,0,\ldots,0,0) = 0$
opposé : $-(a_0,\ldots,a_N,0,\ldots,0) = (-a_0,\ldots,-a_N,0,\ldots,0)$

$\times$: loi associative et commutative
neutre : $(1,0,\ldots,0) = 1$

Distributivité entre $+$ et $\times$.

Remarque :

$(0,1,0,\ldots,0)^n = (0,\ldots,0,\underbrace{1}_{\text{rang } n},0,\ldots,0)$

Définition :

Soit $A = (a_0, a_1, a_2, \ldots, a_n, 0, \ldots, 0)$

$A = a_0(1,0,0,\ldots,0)+a_1(0,1,0,\ldots,0)+a_2(0,0,1,0,\ldots,0)+\ldots+a_n(0,\ldots,0,1,0,\ldots,0)$

On note $X=(0,1,0,\ldots,0)$

Alors $A = a_0+a_1X+a_2X^2+\ldots+a_nX^n$

X est appelée l'indéterminée.

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

Propriété :

$(\mathbb{K}[X],+,\times)$ est un anneau commutatif.

Remarque :

Soit $A=a_0+a_1X+a_2X^2+...+a_nX^n$

$A=0 \Leftrightarrow (a_0,a_1,\ldots,a_n,0,\ldots,0)=(0,0,0,\ldots,0) \Leftrightarrow \forall k\in\mathbb{N},\ a_k=0.$

1.2. Degré

Définition :

Soit $P\in\mathbb{K}[X],\ P=(a_k)_{k\in\mathbb{N}}$

Si $P\neq 0$, on appelle degré de P et on note $\deg(P)$ le plus grand entier n tel que $a_n\neq 0$.

Si $P=0$, on pose par convention que $\deg(P)=-\infty$.

Définitions :

- On appelle polynômes constants les polynômes de degré inférieur ou égal à 0.
- On dit qu'un polynôme est unitaire ou normal si son terme de plus haut degré est $1\times X^n$.
- On appelle coefficient dominant le coefficient du terme de plus haut degré.

Proposition :

$\forall P,Q \in\mathbb{K}[X]$

1. $\forall \lambda\in\mathbb{K}^*,\ \deg(\lambda.P)=\deg(P)$
2. $\deg(PQ)=\deg(P)+\deg(Q)$
3. $\deg(P+Q)\leqslant\max(\deg(P),\deg(Q))$
   Si $\deg(P)\neq\deg(Q)$, alors $\deg(P+Q)=\max(\deg(P),\deg(Q))$.

Preuve :

$n=\deg(P)\geqslant 0,\ m=\deg(Q)\geqslant 0,\ P=a_0+a_1X+\ldots+a_nX^n,\ a_n\neq 0,\ Q=b_0+b_1X+\ldots+b_nX^n,\ b_n\neq 0,\ \forall\lambda\neq 0$:

1. $\lambda.P = \lambda a_0+\lambda.a_1X+\ldots+\underbrace{\lambda.a_n}_{\neq 0}X^n$ donc $\deg(\lambda.P)=n$
2. $D=PQ\quad \forall k>n+m,\ d_k=0$ et $d_{n+m}=a_nb_m\neq 0$ donc $\deg(PQ) = n+m = \deg(P)+\deg(Q)$
3. $C=P+Q\quad c_k=a_k+b_k\quad \forall k>\max(n,m),\ c_k=0$ donc $\deg(P+Q)\leqslant\max(n,m)$
   Si $\deg(P)\neq\deg(Q)$, par ex. $n<m$: $c_m=\underbrace{a_m}_{=0}+b_m=b_m\neq 0$ donc $\deg(P+Q)=m=\max(\deg(P),\deg(Q))$

Remarque :

Si $P=0$: $\deg(P)=-\infty$

$P\times Q=0\quad \deg(P\times Q)=-\infty=-\infty+\deg(Q)$

$P+Q=Q\quad \deg(P+Q)=\deg(Q)=\max(-\infty,\deg Q)$

Corollaire :

$(\mathbb{K}[X],+,\times)$ est intègre, c'est-à-dire : $P\times Q=0 \Rightarrow P=0$ ou $Q=0$.

Preuve :

Par contraposition : $P\neq 0$ et $Q\neq 0 \Rightarrow P\times Q\neq 0$

$P\neq 0$ et $Q\neq 0 \Rightarrow \begin{cases}\deg(P)\geqslant 0\\ \deg(Q)\geqslant 0\end{cases} \Rightarrow \deg(P\times Q)=\deg(P)+\deg(Q)\geqslant 0 \Rightarrow P\times Q\neq 0.$

Définition :

On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur ou égal à n.

Proposition :

$(\mathbb{K}_n[X], +)$ est un sous-groupe de $(\mathbb{K}[X], +)$.

Preuve :

- $\mathbb{K}_n[X] \subset \mathbb{K}[X]$
- $\deg(0) = -\infty$ donc $0 \in \mathbb{K}_n[X]$ donc $\mathbb{K}_n[X] \neq \emptyset$
- $\forall P, Q \in \mathbb{K}_n[X]$

$$\begin{aligned}\deg(P-Q) &= \deg(P+(-Q)) \\ &\leqslant \max(\deg(P), \deg(-Q)) \\ &\leqslant \max(\deg(P), \deg(Q)) \quad \text{Or, } \deg(P) \leqslant n \text{ et } \deg(Q) \leqslant n \\ &\leqslant n\end{aligned}$$

Donc $(P-Q) \in \mathbb{K}_n[X]$, donc $\mathbb{K}_n[X]$ est un sous-groupe de $\mathbb{K}[X]$.

Remarque :

On peut toujours écrire $P = \sum_{k=0}^{\deg(P)} a_k X^k = \sum_{k=0}^{\infty} a_k X^k$ (somme finie).

1.3. Dérivation

Définition :

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$

On appelle polynôme dérivé et on note $P' = \sum_{k=1}^{n} k a_k X^{k-1} \left(= \sum_{k=0}^{n} k a_k X^{k-1} \right)$.

Proposition :

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

1. $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$
2. $(PQ)' = P'Q + PQ'$

Preuve :

1. $P = \sum_{k=0}^{n} a_k X^k, \quad Q = \sum_{k=0}^{n} b_k X^k, \quad R = \lambda P + \mu Q = \sum_{k=0}^{\max(n,m)} (\lambda a_k + \mu b_k) X^k$

   Alors $R' = \sum_{k=1}^{n} k(\lambda a_k + \mu b_k) X^{k-1} = \sum_{k=1}^{n} (\lambda k a_k X^{k-1} + \mu k b_k X^{k-1}) = \lambda \sum_{k=1}^{n} k a_k X^{k-1} + \mu \sum_{k=1}^{n} k b_k X^{k-1} = \lambda P' + \mu Q'$.
2. Soit $S = P \cdot Q$

   1er cas : $Q = X^k$ (cas particulier d'un monôme)

   $$S = P \cdot X^k = \sum_{i=0}^{n} a_i X^i \cdot X^k = \sum_{i=0}^{n} a_i X^{i+k}$$

   $$S' = \sum_{i=0}^{n} a_i (i+k) X^{i+k-1} \qquad Q' = k X^{k-1} \qquad P' = \sum_{i=0}^{n} a_i i X^{i-1} \quad (=0 \text{ si } i=0)$$

   $$P'Q + PQ' = \sum_{i=0}^{n} a_i i X^{i-1} X^k + \sum_{i=0}^{n} a_i X^i k X^{k-1} = \sum_{i=0}^{n} a_i (i+k) X^{i+k-1} = S' = (PQ)'$$

   2ème cas : cas général

   $$Q = \sum_{k=0}^{m} b_k X^k \qquad S = PQ = \sum_{k=0}^{m} b_k P X^k$$

   $$S' = \sum_{k=0}^{m} b_k (P X^k)' \quad \text{(d'après le 1.)} \qquad S' = \sum_{k=0}^{m} b_k (P' X^k + P k X^{k-1}) = P' \sum_{k=0}^{m} b_k X^k + P \sum_{k=0}^{m} b_k k X^{k-1}$$

   D'où $S' = P'Q + PQ'$.

Proposition :

$\deg(P') = \deg(P)-1$ si $\deg(P)\geqslant 1$ (P non constant)
$= -\infty$ sinon.

Corollaire :

P est constant $\Leftrightarrow$ $P'=0$.

Proposition :

$\forall P,Q\in\mathbb{K}[X],\quad \forall \lambda,\mu\in\mathbb{K},\quad \forall n\in\mathbb{N}$

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

Remarque :

On appelle dérivée $n^{\text{ième}}$ de P et on note :
$P^{(n)}=P$ si $n=0$
$=P'$ si $n=1$
$=(P^{(n-1)})'=(P')^{(n-1)}$ si $n\geqslant 2$

Proposition :

$\deg(P^{(n)})=\deg(P)-n$ si $\deg(P)\geqslant n$
$=-\infty$ si $\deg(P)<n$

Corollaire :

$P\in\mathbb{K}_{n-1}[X]$ $\Leftrightarrow$ $P^{(n)}=0$

Preuve de la formule de Leibniz :

Récurrence sur n :

– Pour $n=0$: $(PQ)^{(0)}=PQ=P^{(0)}Q^{(0)}$ La proposition est vraie au rang 0.

– Supposons $n\in\mathbb{N}$ et la proposition vraie au rang n

$$(PQ)^{(n+1)}=((PQ)^{(n)})'=\left(\sum_{k=0}^{n}\binom{n}{k}P^{(k)}Q^{(n-k)}\right)'=\sum_{k=0}^{n}\binom{n}{k}\left(P^{(k)}Q^{(n-k)}\right)'=\sum_{k=0}^{n}\binom{n}{k}\left(P^{(k+1)}Q^{(n-k)}+P^{(k)}Q^{(n-k+1)}\right)$$
$$=\sum_{k=1}^{n+1}\binom{n}{k-1}(P^{(k)}Q^{(n-(k-1))})+\sum_{k=0}^{n}\binom{n}{k}(P^{(k)}Q^{(n+1-k)})=\sum_{k=1}^{n}\left[\binom{n}{k-1}+\binom{n}{k}\right](P^{(k)}Q^{(n+1-k)})+P^{(n+1)}Q+PQ^{(n+1)}$$
$$=\sum_{k=0}^{n+1}\binom{n+1}{k}P^{(k)}Q^{(n+1-k)}$$

La propriété est vraie au rang $n+1$.

En vertu du principe de récurrence, la propriété est vraie pour tout $n\in\mathbb{N}$.

Proposition : Formule de Taylor :

$\forall P\in\mathbb{K}_n[X],\quad \forall a\in\mathbb{K}$

$P=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}(X-a)^k$ ou $P(a+X)=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}(X)^k$

Preuve :

Récurrence sur n :

– Pour $n=0$: $P=c$ $\sum_{k=0}^{0}\frac{P^{(0)}(a)}{0!}(X-a)^0=c=P$ La propriété est vraie au rang 0.

– Supposons $n\in\mathbb{N}$ et la propriété vraie au rang n.

Soit $P\in\mathbb{K}_{n+1}[X]$

$\exists Q\in\mathbb{K}_n[X]$ tel que $P=Q+cX^{n+1}$

$$E=\sum_{k=0}^{n+1}\frac{P^{(k)}(a)}{k!}(X-a)^k=\sum_{k=0}^{n+1}\frac{(Q+cX^{n+1})^{(k)}(a)}{k!}(X-a)^k=\sum_{k=0}^{n+1}\frac{Q^{(k)}(a)}{k!}(X-a)^k+\sum_{k=0}^{n+1}\frac{(cX^{n+1})^{(k)}(a)}{k!}(X-a)^k$$

$Q\in\mathbb{K}_n[X]\ \Rightarrow\ Q^{(n+1)}=0$

$$(X^{n+1})^{(k)}=(n+1)n(n-1)\ldots(n+2-k)X^{n+1-k}=\frac{(n+1)!}{(n+1-k)!}X^{n+1-k}\qquad \text{si } k\leqslant n+1$$
$$=0\qquad \text{si } k>n+1$$
$$=(n+1)!\qquad \text{si } k=n+1$$

$$E=\sum_{k=0}^{n}\frac{Q^{(k)}(a)}{k!}(X-a)^k+c\sum_{k=0}^{n+1}\frac{(n+1)!}{(n+1-k)!k!}a^{n+1-k}(X-a)^k=Q+\sum_{k=0}^{n+1}\binom{n+1}{k}a^{n+1-k}(X-a)^k$$
$$=Q+c(a+X-a)^{n+1}=Q+cX^{n+1}=P$$

La propriété est vraie au rang $n+1$.

Par récurrence, la propriété est vraie pour tout $n\in\mathbb{N}$.

2. Arithmétique dans $\mathbb{K}[X]$

2.1. Diviseurs et multiples

Définition :

Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B ou que B est un multiple de A si $\exists P \in \mathbb{K}[X]$ tel que $B = P \times A$.

Remarque :

Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les diviseurs de 1, c'est-à-dire $\mathbb{K}^*$.

Si $AB = 1$:

$\Rightarrow$: $\deg(A) + \deg(B) = 0 \Rightarrow \deg A = 0 \Rightarrow \exists c \in \mathbb{K}^*$ tel que $A = c$

$\Leftarrow$: Si $A = c$ et que $c \in \mathbb{K}^*$ $\quad A^{-1} = \frac{1}{c}$

Remarque :

Si on note $A\mathbb{K}[X]$ les multiples de A, on a :

$A|B \Leftrightarrow B\mathbb{K}[X] \subset A\mathbb{K}[X]$.

Définition :

Deux polynômes A et B sont dits associés si $A|B$ et $B|A$.

Proposition :

Soient $A, B \in \mathbb{K}[X]$.

Les assertions suivantes sont équivalentes :

1. $A|B$ et $B|A$
2. $A\mathbb{K}[X] = B\mathbb{K}[X]$
3. $\exists c \in \mathbb{K}^*$ tel que $A = cB$.

Preuve :

1. $\Leftrightarrow$ 2. : d'après la remarque

1. $\Rightarrow$ 3. : $\exists P, Q \in \mathbb{K}[X]$ tels que $B = PA$ et $A = QB$: $B = PQB$
si $B = 0$ et $A = 0$, $c = 1$ convient
sinon $PQ = 1$, P et $Q \in \mathbb{K}^*$ donc $c = Q$ et $A = cB$

3. $\Rightarrow$ 1. : $A = cB \Rightarrow B|A$ $\quad B = \frac{1}{c}A \Rightarrow A|B$ $\quad c \neq 0$

2.2. Division euclidienne

Théorème :

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, alors il existe un unique couple de polynômes (Q, R) tel que

$$\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$$

Preuve :

− Existence :

· 1er cas : B est un polynôme constant non nul : $B = b \in \mathbb{K}^*$ $\quad \forall A \in \mathbb{K}[X]$, $A = \frac{A}{b} \times b + 0$: $R = 0$ et $\frac{A}{b} = Q \in \mathbb{K}[X]$

· 2ème cas : $\deg(B) = p > 0$ $\quad p \in \mathbb{N}^*$

H_n : $\forall A \in \mathbb{K}_n[X]$, $\exists (Q, R) \in \mathbb{K}[X]^2$ tel que $\begin{cases} A = BQ + R \\ \deg(R) < \deg(B) \end{cases}$

· H_{p-1} est vraie si $\deg(A) \leqslant p - 1 < p = \deg(B)$ $\quad A = B \times 0 + A$

· Supposons $n \in \mathbb{N}$, $n \geqslant p - 1$ et H_n vraie

Soit $A \in \mathbb{K}_{n+1}[X]$: $A = a_{n+1}X^{n+1} + A_1$

Où $A_1 \in \mathbb{K}_n[X]$, $a_{n+1} \in \mathbb{K}$ $\quad$ On pose la division :

$$\begin{array}{l|l} a_{n+1}X^{n+1} + A_1 & B = b_p X^p + \ldots + b_0 \\ -a_{n+1}X^{n+1} + \ldots & \hline \frac{a_{n+1}}{b_p}X^{n+1-p} \\ = \quad A_2 & \\ (\deg(A_2) \leqslant n) & \end{array}$$

$A_2 = A - \frac{a_{n+1}}{b_p}X^{n+1-p}B \quad \in \mathbb{K}_n[X] \Rightarrow \exists (Q_2, R_2) \in \mathbb{K}[X]^2$ tel que $A_2 = BQ_2 + R_2$ et $\deg(R_2) < \deg(B)$.

$$A = BQ_2 + R_2 + \frac{a_{n+1}}{b_p}X^{n+1-p}B = \left(\frac{a_{n+1}}{b_p}X^{n+1-p} + Q_2\right)B + R_2 = BQ + R$$

La propriété est vraie au rang $n+1$.

Par récurrence, la propriété est vraie pour tout n.

– Unicité : Si $A = BQ_1+R_1 = BQ_2+R_2$ avec $\deg(R_1)<\deg(B)$ et $\deg(R_2)<\deg(B)$
$(Q_1-Q_2)B=R_1-R_2$ donc $\deg(R_1-R_2) \leqslant \max(\deg(R_2),\deg(R_1)) < \deg(B)$
$\deg((Q_1-Q_2)B)=\deg(Q_1-Q_2)+\deg(B) \Rightarrow \deg(Q_1-Q_2)<0 \Rightarrow \deg(Q_1-Q_2)=-\infty \Rightarrow Q_1=Q_2$ et $R_1=R_2$.

2.3. Diviseurs communs

Définition :
On désigne par $\mathscr{D}(A)$ l'ensemble des diviseurs d'un polynôme A.

Lemme :
Si A et B sont deux polynômes avec $B\neq 0$, si R désigne le reste de A par B, alors $\mathscr{D}(A)\cap\mathscr{D}(B)=\mathscr{D}(B)\cap\mathscr{D}(R)$.

Lemme :
Si A est un polynôme, alors $\mathscr{D}(A)\cap\mathscr{D}(0)=\mathscr{D}(A)$

Algorithme d'Euclide :
On note $R_0=A$ et $R_1=B$, de sorte que $\mathscr{D}(A)\cap\mathscr{D}(B)=\mathscr{D}(R_0)\cap\mathscr{D}(R_1)$.
– Étape 1 :
– Si $R_1=0$, on a $\mathscr{D}(R_0)\cap\mathscr{D}(R_1)=\mathscr{D}(R_0)$.
– Sinon, on divise R_0 par R_1¿, ce qu'on écrit $R_0=Q_1R_1+R_2$ avec $\deg(R_2)<\deg(R_1)$.
On a alors $\mathscr{D}(R_0)\cap\mathscr{D}(R_1)=\mathscr{D}(R_1)\cap\mathscr{D}(R_2)$.
Si l'algorithme n'est pas achevé avant l'étape k, celle-ci se déroule de même :
– Étape k :
– Si $R_k=0$, on a $\mathscr{D}(R_{k-1})\cap\mathscr{D}(R_k)=\mathscr{D}(R_{k-1})$.
– Sinon, on divise R_{k-1} par R_k, ce qu'on écrit $R_{k-1}=Q_kR_k+R_{k+1}$ avec $\deg(R_{k+1})<\deg(R_k)$.
On a alors $\mathscr{D}(R_{k-1})\cap\mathscr{D}(R_k)=\mathscr{D}(R_k)\cap\mathscr{D}(R_{k+1})$.
La suite des entiers $\deg(R_k)$ étant strictement décroissante, il existe un rang N tel que $R_{N+1}=0$ et $\deg(R_N)\geqslant 0$.
On a alors $\mathscr{D}(R_A)\cap\mathscr{D}(R_B)=\mathscr{D}(R_N)\cap\mathscr{D}(0)=\mathscr{D}(R_N)$.
On retient : les diviseurs communs à A et B sont les diviseurs du dernier reste non nul de l'algorithme.

Proposition :
Pour tout couple de polynôme (A,B), il existe un unique polynôme unitaire (ou nul) D tel que :
1. D divise A et B
2. Tout diviseur de A et B divise D.

Preuve :
– Unicité :
Si D et D' vérifient les conditions, D divise A et B, c'est donc un diviseur commun de A et B donc D divise D'.
De même D' divise D. Par conséquent, D et D' sont associés, étant unitaires, ils sont égaux.
– Existence :
Soit R_N le dernier reste non nul de l'algorithme d'Euclide, on a $\mathscr{D}(A)\cap\mathscr{D}(B)=\mathscr{D}(R_N)$.
Donc R_N divise A et B et tout diviseur de A et B divise R_N. Il suffit de diviser R_N par son coefficient dominant pour obtenir un polynôme unitaire.

Définition :
Cet unique polynôme est appelé plus grand commun diviseur de A et B. On le note $A\wedge B$.
C'est le dernier reste non nul de l'algorithme d'Euclide.

Proposition :
Pour tout couple de polynôme (A,B), il existe un couple (U,V) de polynômes (mais pas unique) vérifiant l'égalité de Bézout : $UA+VB=A\wedge B$.
On peut s'inspirer de la preuve dans $\mathbb{Z}$ pour cette proposition.

Remarque :
On obtient U et V de la même manière que dans $\mathbb{Z}$.

2.4. Polynômes premiers entre eux

Définition :

On dit que deux polynômes A et B sont premiers entre eux si leur PGCD est égal à 1,
c'est-à-dire si les seuls diviseurs communs à A et B sont les polynômes constants non nuls.

Théorème de Bézout :

On considère un couple (A, B) de polynômes. Les assertions suivantes sont équivalentes :

1. Les polynômes A et B sont premiers entre eux
2. Il existe deux polynômes U, V tels que $UA+VB=1$.

Théorème de Gauss :

On considère trois polynômes A, B, C.
Si A divise BC et si A est premier avec B, alors A divise C.

Corollaires :

1. Si A et B divisent C et si A et B sont premiers entre eux, alors AB divise C.
2. Si A et C ainsi que B et C sont premiers entre eux alors AB et C sont premiers entre eux.

Proposition :

Pour tout polynômes non nuls A, B et D unitaires, $D=A\wedge B$ si et seulement s'il existe des polynômes A_1 et B_1 tels que : $A=DA_1$, $B=DB_1$ et $A_1\wedge B_1=1$.

2.5. PPCM

Proposition :

Pour tout couple (A, B) de polynômes, il existe un unique polynôme unitaire (ou nul) M tel que :

1. M est un multiple de A et B.
2. tout multiple de A et B est un multiple de M.

Preuve :

- Existence :

  Le cas où l'un des deux polynômes A et B est nul est immédiat.
  Sinon, soit D le PGCD de A et B, on peut écrire $A=aDA'$ et $B=bDB'$ où a et b sont les coefficients dominants de A et B et avec $A'\wedge B'=1$

  Considérons alors le polynôme $M=DA'B'=\dfrac{AB}{abD}$ on constate que :

  - C'est un multiple de A et B car $M=DA'B'=\dfrac{AB'}{a}=\dfrac{A'B}{b}$
  - Tout multiple N de A et de B est un multiple de M.

  En effet, si $N=UA=VB$ avec $U, V\in\mathbb{K}[X]$, on a $UA'=VB'$ en simplifiant par D. Donc A' divise VB'.
  Comme il est premier avec B', il divise V (théorème de Gauss). Ainsi, il existe $K\in\mathbb{K}[X]$ tel que $V=KB'$.
  D'où $N=UA=KDA'B'=KM$.

- Unicité :

  Si M et M' vérifient 1. et 2. , chacun d'eux est un multiple de A et de B.
  M' est un multiple de A et B $\Rightarrow$ M' est un multiple de M, et de même, M est un multiple de M'.
  Ainsi, M et M' se divisent l'un l'autre , ils sont donc associés, et comme ils sont unitaires, ils sont égaux.

Définition :

Cet unique polynôme est appelé plus petit commun multiple de A et B. On le note $A\vee B$.
Il est nul si B est nul : $A\vee 0=0$.

Proposition :

Pour tout couple de polynôme (A, B), de coefficients dominants a et b, on a :
$ab(A\vee B)(A\wedge B)=AB$

2.6. Polynômes irréductibles

Définition :

On dit qu'un polynôme non constant $P \in \mathbb{K}[X]$ est irréductible dans l'anneau $\mathbb{K}[X]$ si ses seuls diviseurs sont les inversibles et les polynômes associés à P, c'est-à-dire si : $\forall A, B \in \mathbb{K}[X],\ P = AB \Rightarrow \deg(A) = 0$ ou $\deg(B) = 0$.

Lemme :

Tout polynôme non constant possède au moins un diviseur irréductible.

Preuve :

Récurrence sur $n = \deg(P)$:

- Pour $n = 1$, le résultat est acquis puisqu'un polynôme de degré 1 est irréductible.
- Supposons $n \geqslant 1$ et le résultat vrai pour tout polynôme non constant de degré inférieur à n. Soit P de degré $n+1$:
  - Si P est irréductible, le résultat est vrai
  - Sinon, il existe $A, B \in \mathbb{K}[X]$ tels que $P = AB$ où $0 < \deg(A) < n+1$ et $0 < \deg(B) < n+1$.
    On applique l'hypothèse de récurrence à A ou B : il existe un polynôme irréductible divisant A ou B donc P
    Le résultat est vraie au rang $n+1$.

Par récurrence, tout polynôme non constant possède un diviseur irréductible.

Lemme :

On considère un polynôme irréductible unitaire P et un polynôme A. Alors :

1. Soit P ne divise pas A, ce qui équivaut à $P \wedge A = 1$;
2. Soit P divise A, ce qui équivaut à $P \wedge A = P$.

Preuve :

L'ensemble des diviseurs communs à un polynôme A et un polynôme irréductible P est évidemment inclus dans l'ensemble des diviseurs de P, qui sont les polynômes constants non nuls et les polynômes associés à P.
Il en résulte que le PGCD de A et de P est égal ici à 1 ou à P, d'où les cas suivants:

- Soit P divise A, et ceci équivaut à $P \wedge A = P$. En effet, $P \wedge A = P$, alors P divise A, et inversement, si P divise A, il divise A et P donc il divise $P \wedge A$. Comme $P \wedge A = 1$ ou P, on a alors $P \wedge A = P$.
- Soit P ne divise pas A, et ceci équivaut à $P \wedge A = 1$. En effet, il suffit de contraposer le résultat précédent.

Lemme :

On considère un polynôme irréductible et des polynômes $A_1, \ldots, A_n (n \geqslant 1)$.
Si P divise le produit $A_1, \ldots, A_n$ alors il divise l'un des facteurs $A_1, \ldots, A_n$.

Preuve :

Par l'absurde, si P ne divise aucun des facteurs $A_1, A_2, \ldots, A_n$, alors il est premier avec chacun d'entre eux, donc avec leur produit (d'après un corollaire du théorème de Gauss). Mais il ne divise plus leur produit, d'où la contradiction.

Théorème fondamental de l'arithmétique dans $\mathbb{K}[X]$ ***:***

Pour tout polynôme A non constant, il existe un entier $m \geqslant 1$, m polynômes irréductibles unitaire $P_1, \ldots, P_m$ m entiers positifs $r_1, \ldots, r_m$ tel qu'on ait :
$A = \lambda P_1^{r_1} P_2^{r_2} \cdots P_m^{r_m} \qquad (\lambda \in \mathbb{K}^*)$
C'est une factorisation de A en produit de polynômes irréductibles, et celle-ci est unique, à l'ordre près.

Remarque :

Le scalaire λ est le coefficient dominant de A.

Preuve :

- Existence de la décomposition : on procède par récurrence sur $n = \deg(A)$:
  - Pour $n = 1$, A est de degré 1 donc irréductible, il suffit de sortir le coefficient dominant.
  - Supposons $n \geqslant 1$ et le résultat vrai pour tout polynôme de degré inférieur à n. Soit A de degré $n+1$.
    Si A est irréductible, il suffit de le diviser par son coefficient dominant. Sinon, A possède un diviseur irréductible P et A s'écrit $A = PQ$, et on a $1 \leqslant \deg(Q) \leqslant n$. On peut appliquer l'hypothèse de récurrence à Q.
    On a alors une factorisation de A en produit de polynômes irréductibles. Le résultat est donc vrai au rang $n+1$.

Par récurrence, la propriété est vraie pour tout $n \geqslant 1$.

– Unicité de la factorisation : on procède par récurrence sur $n=\deg(A)$:
  · Pour $n=1$, A étant irréductible, le résultat est vrai.
  · Supposons $n\geqslant 1$ et le résultat vrai pour tout polynôme de degré inférieur à n. Soit A de degré $n+1$.
  Supposons que A ait deux factorisations distinctes : $A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m} = \lambda Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_k^{\beta_k}$
  Le polynôme irréductible P_1 divise A, il divise donc le produit $Q_1^{\beta_1} Q_2^{\beta_2} \dots Q_k^{\beta_k}$ ¿ donc l'un des facteurs $Q_1, \dots, Q_k$, par ex. Q_1 quitte à changer la numérotation. Le polynôme irréductible P_1 divise le polynôme irréductible Q_1
  Ils sont donc associés, et étant unitaires, ils sont égaux. On peut alors simplifier l'égalité précédente par P_1 :
  $\lambda P_1^{\alpha_1-1} P_2^{\alpha_2} \dots P_m^{\alpha_m} = \lambda Q_1^{\beta_1-1} Q_2^{\beta_2} \cdots Q_k^{\beta_k}$
  Il s'agit d'un polynôme de degré strictement inférieur à $n+1$ donc inférieur à n : on peut donc lui appliquer l'hypothèse de récurrence. On a donc $m=k$ et quitte à changer la numérotation, $P_1=Q_1, P_2=Q_2, \dots, P_m=Q_m$ et $\alpha_1-1=\beta_1-1, \alpha_2=\beta_2, \dots, \alpha_m=\beta_m$. Le résultat est donc vrai au rang $n+1$.

Par récurrence, la propriété est vraie pour tout $n\geqslant 1$.

Remarque :

Comme dans $\mathbb{Z}$, on établira que :

– Les diviseurs de A sont du type $D=\mu P_1^{d_1} P_2^{d_2} \dots P_m^{d_m}$ où $\mu\in\mathbb{K}^*$ et $d_i\in[\![0, r_i]\!]$ $(1\leqslant i\leqslant m)$.

– Les PGCD et PPCM de deux polynômes peuvent être obtenus à partir de leurs factorisations en produit de polynômes irréductibles.

3. Fonction polynomiales et racines

3.1. Isomorphisme

Définition :

On appelle fonction polynômiale toute fonction f, définie sur $\mathbb{K}$, telle que :

$\exists n\in\mathbb{N},\ a_0,\dots,a_n\in\mathbb{K},\ x\in\mathbb{K}$ tels que $f(x)=a_0+a_1x+\dots+a_nx^n$.

On note $\mathscr{P}_{\mathbb{K}}$ l'ensemble des fonctions polynômiales sur $\mathbb{K}$.

Proposition :

$$\varphi : \begin{array}{ccc} (\mathbb{K}[X],+,\times) & \to & \mathscr{F}(\mathbb{K},\mathbb{K})=(\mathbb{K}^{\mathbb{K}},+,\times) \\ P=\sum_{k=0}^{n} a_k X^k & \mapsto & f(x)=\sum_{k=0}^{n} a_k x^k \end{array}$$ est un isomorphisme injectif d'anneaux.

Preuve :

· $\varphi(1) = x\mapsto 1 = 1_{\mathbb{K}^{\mathbb{K}}}$

· $\forall P,Q\in\mathbb{K}[X],\ P=\sum_{k=0}^{n} a_k X^k \quad Q=\sum_{k=0}^{p} b_k X^k \quad P+Q=\sum_{k=0}^{\max(n,p)} (a_k+b_k)X^k \quad PQ=\sum_{k=0}^{n+p}\sum_{i=0}^{k}(a_i b_{k-i})X^k$

$$\varphi(P+Q) = x\mapsto \sum_{k=0}^{\max(n,p)} (a_k+b_k)x^k = x\mapsto\sum_{k=0}^{n} a_k x^k+\sum_{k=0}^{p} b_k x^k = x\mapsto\sum_{k=0}^{n} a_k X^k+x\mapsto\sum_{k=0}^{p} b_k X^k$$
$$= \varphi(P)+\varphi(Q)$$
$$\varphi(PQ)=x\mapsto\sum_{k=0}^{n+p}\left(\sum_{i=0}^{k}(a_i b_{k-i})\right)x^k=\left(x\mapsto\sum_{i=0}^{n} a_i x^i\right)\left(x\mapsto\sum_{j=0}^{p} b_j x^j\right)=\varphi(P)\varphi(Q)$$

$$P\in\mathrm{Ker}(\varphi) \Leftrightarrow \varphi(P)=x\mapsto 0 \Leftrightarrow \forall x\in\mathbb{K},\sum_{k=0}^{n} a_k X^k=0$$

On évalue en $x=0$: $a_0=0$, on dérive : $\forall x\in\mathbb{K},\ a_1+2a_2x+\dots+na_nx^{n-1}$, on évalue en 0 : $a_1=0$

De proche en proche, $\forall k\in\mathbb{N},\ a_k=0 \Rightarrow P=0 \Rightarrow \varphi(0)=x\mapsto 0 \quad \mathrm{Ker}(\varphi)=\{0\}$

Corollaire :

1. $\mathscr{P}_{\mathbb{K}}\ (=\mathrm{Im}(\varphi))$ est un sous anneau de $\mathbb{K}^{\mathbb{K}}$
2. φ réalise un isomorphisme d'anneau de $\mathbb{K}[X]$ sur $\mathscr{P}_{\mathbb{K}}$.

3.2. Racines

Définition :

On dit qu'un scalaire $a\in\mathbb{K}$ est une racine (ou un zéro) d'un polynôme P si $P(a)=0$.

Proposition :

$P(a)=0 \Leftrightarrow X-a|P$.

Remarque :

Le reste de la division euclidienne de P par $X-a$ est $P(a)$.

Preuve :

$\Leftarrow$: $X-a|P \Leftrightarrow \exists Q\in\mathbb{K}[X]$ tel que $(X-a)\times Q=P \quad P(a)=(a-a)Q(a)=0$

$\Rightarrow$: $\exists!(Q,R)\in\mathbb{K}[X]^2$ tel que $\begin{cases} P=(X-a)Q+R \\ \deg(R)<\deg(X-a) \end{cases}$

$\deg(R)<\deg(X-a) \Rightarrow R=c$ donc $P(a)=c$

Or, $P(a)=0$ donc $R=0$ donc $X-a|P$.

Proposition :

Soient $P\in\mathbb{K}[X]$, $a_1,a_2\ldots,a_n$ n scalaires deux à deux distincts. Les assertions suivantes sont équivalentes :

1. $(X-a_1)(X-a_2)\ldots(X-a_n)|P$
2. $P(a_1)=P(a_2)=\ldots=P(a_n)=0$.

Preuve :

1. $\Rightarrow$ 2. : $\exists Q\in\mathbb{K}[X]$ tel que $P=(X-a_1)(X-a_2)\ldots(X-a_n)Q \quad \forall k\in[\![1,n]\!],\ P(a_k)=0$
2. $\Rightarrow$ 1. : Récurrence sur n :
   - Pour $n=1$: voir proposition précédente
   - Supposons $n\geqslant 1$ et la proposition vraie au rang n

     Soient $a_1,\ldots,a_{n+1}$ $n+1$ racines distinctes de P, $P(a_{n+1})=0 \Leftrightarrow \exists Q\in\mathbb{K}[X]$ tel que $P=(X-a_{n+1})Q$

     $\forall k\in[\![1,n]\!],\ 0=P(a_k)=\underbrace{(a_k-a_{n+1})}_{\neq 0}Q(a_k)$ donc $Q(a_k)=0$

     On applique l'hypothèse de récurrence à Q : $\exists S\in\mathbb{K}[X]$ tel que $Q=(X-a_n)(X-a_{n-1})\ldots(X-a_1)S$

     Donc $(X-a_1)\ldots(X-a_{n+1})S=P$ donc $(X-a_1)\ldots(X-a_{n+1})S|P$

     La propriété est vraie au rang $n+1$.

   Par récurrence, la propriété est vraie $\forall n\in\mathbb{N}$.

Corollaire :

1. Si $P\neq 0$ a n racines distinctes, alors $\deg(P)\geqslant n$
2. Si $\deg(P)\leqslant n$ et si P a au moins $n+1$ racines distinctes, alors $P=0$
3. Si P a une infinité de racines, alors $P=0$.

3.3. Racines multiples

Proposition :

Soit $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$, $r\in\mathbb{N}^*$

Les assertions suivantes sont équivalentes :

1. $(X-a)^r|P$
2. $\begin{cases} P(a)=0 \\ P'(a)=0 \\ \quad\vdots \\ P^{(r-1)}(a)=0 \end{cases}$

Définition :

On dit alors que a est racine de multiplicité au moins r pour P.

Preuve :

Soit $n=\deg(P)\geqslant r$

Taylor : $P=\sum_{k=0}^{n}\frac{P^{(k)}(a)}{k!}(X-a)^k=\underbrace{\sum_{k=0}^{r-1}\frac{P^{(k)}(a)}{k!}(X-a)^k}_{=R}+(X-a)^r\underbrace{\sum_{k=r}^{n}\frac{P^{(k)}(a)}{k!}(X-a)^{k-r}}_{=Q}$

$\deg(R)\leqslant r-1<\deg(X-a)^r$, R est le reste de la division euclidienne de P par $(X-a)^r$

1. $\Leftrightarrow(X-a)|P \Leftrightarrow R=0 \Leftrightarrow \sum_{k=0}^{r-1}\frac{P^{(k)}(a)}{k!}(X-a)^k=0 \Leftrightarrow P(a)+P'(a)(X-a)+\ldots+\frac{P^{(r-1)}(a)}{(r-1)!}=0$

On évalue en $X=a$: $P(a)=0$. On dérive, on évalue en $X=a$: $P'(a)=0$.

De proche en proche, $P(a)=P'(a)=\ldots=P^{(r-1)}(a)=0 \Leftrightarrow$ 2.

Proposition :

Soient $P\in\mathbb{K}[X]$, $a\in\mathbb{K}$, $r\in\mathbb{N}^*$

Les assertions suivantes sont équivalentes :

1. $(X-a)^r|P$ et $(X-a)^{r+1}\nmid P$
2. $\exists Q\in\mathbb{K}[X]$ tel que $P=(X-a)^rQ$ et $Q(a)\neq 0$
3. $\begin{cases}P(a)=0\\P'(a)=0\\\vdots\\P^{(r-1)}(a)=0\\P^{(r)}(a)\neq 0\end{cases}$

Définition :

On dit de a est racine d'ordre de multiplicité r pour P.

Preuve :

1. $\Rightarrow$ 2. : $\exists Q\in\mathbb{K}[X]$ tel que $P=(X-a)^rQ$
   Si $Q(a)=0$, $(X-a)|Q$ donc $\exists R\in\mathbb{K}[X]$ tel que $Q=(X-a)R$
   D'où $P=(X-a)^{r+1}R$ Contredit $(X-a)^{r+1}\nmid P$, donc $Q(a)\neq 0$
2. $\Rightarrow$ 3. : D'après la proposition précédente, $(X-a)^r|P \Rightarrow P(a)=0\ P'(a)=0\ \ldots\ P^{(r-1)}(a)=0$
   Donc $P=(X-a)^rQ$
   Si $P^{(r)}(a)=0$ alors $(X-a)^{r+1}|P$ (proposition précédente) : $\exists R\in\mathbb{K}[X]$ tel que $P=(X-a)^r(X-a)R$
   Donc $Q=(X-a)R$ donc $Q(a)=0$ Impossible, donc $P^{(r)}(a)\neq 0$
3. $\Rightarrow$ 1. : $P(a)=0\ P'(a)=0\ \ldots\ P^{(r-1)}(a)=0\ P^{(r)}(a)\neq 0 \Rightarrow (X-a)^r|P$
   Si $(X-a)^{r+1}|P$ alors (proposition précédente) $P(a)=0\ P'(a)=0\ \ldots\ P^{(r)}(a)=0$ Impossible
   Donc $(X-a)^{r+1}\nmid P$.

Proposition :

Soient $P\in\mathbb{K}[X]$, $M\in\mathbb{N}^*$, $a_1,a_2,\ldots,a_m$ m racines distinctes, $r_1,r_2,\ldots,r_m\in\mathbb{N}^*$

Si $\forall k\in[\![1,m]\!],a_k$ est racine de multiplicité r_k alors :

$(X-a_1)^{r_1}(X-a_2)^{r_2}\ldots(X-a_m)^{r_m}|P$

Preuve :

$i\neq j \Rightarrow a_i\neq a_j \quad (X-a_i)\wedge(X-a_j)=1$ car $\frac{1}{a_j-a_i}(X-a_i)-\frac{1}{a_i-a_j}(X-a_j)=1$

Or $\begin{cases}A\wedge B=1\\A\wedge C=1\end{cases} \Rightarrow A\wedge BC=1$ donc $(X-a_i)^{r_i}\wedge(X-a_j)^{r_j}=1$

Or $(X-a_i)|P$ et $\begin{cases}A|C\\B|C\\A\wedge B=1\end{cases} \Rightarrow AB|C$

Donc $(X-a_1)^{r_1}(X-a_2)^{r_2}\ldots(X-a_m)^{r_m}|P$

Remarque :

$\deg\left[(X-a_1)^{r_1}(X-a_2)^{r_2}\ldots(X-a_m)^{r_m}\right]=\sum_{k=0}^{n}r_k.$

Corollaire :

1. Si $P \neq 0$ admet m racines différentes de multiplicité respectives $r_1, r_2, \ldots, r_m$, alors $\deg(P) \geqslant r_1 + r_2 + \ldots + r_m$
2. Si $\deg(P) \leqslant n$ et si P a au moins $n+1$ racines comptés avec leurs ordres de multiplicité, alors $P = 0$.

Proposition :

Soit $P \in \mathbb{R}[X]$, $a \in \mathbb{C}$, $m \in \mathbb{N}^*$

a est racine de multiplicité m pour $P \Leftrightarrow \overline{a}$ est racine de multiplicité m pour P.

Preuve :

$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \quad a_0, a_1, a_2, \ldots, a_n \in \mathbb{R}$

$P(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n \quad \overline{P(z)} = \overline{a_0} + \overline{a_1}\overline{z} + \overline{a_2}\overline{z}^2 + \ldots + \overline{a_n}(\overline{z})^n = a_0 + a_1\overline{z} + a_2\overline{z}^2 + \ldots + a_n\overline{z}^n = P(\overline{z})$

$$a \text{ est racine de multiplicité } m \text{ de } P \Leftrightarrow \begin{cases} P(a) = 0 \\ P'(a) = 0 \\ \vdots \\ P^{(m-1)}(a) = 0 \\ P^{(m)}(a) \neq 0 \end{cases} \Leftrightarrow \begin{cases} \overline{P(a)} = 0 \\ \overline{P'(a)} = 0 \\ \vdots \\ \overline{P^{(m-1)}(a)} = 0 \\ \overline{P^{(m)}(a)} \neq 0 \end{cases} \Leftrightarrow \begin{cases} P(\overline{a}) = 0 \\ P'(\overline{a}) = 0 \\ \vdots \\ P^{(m-1)}(\overline{a}) = 0 \\ P^{(m)}(\overline{a}) \neq 0 \end{cases}$$

$\Leftrightarrow \overline{a}$ est une racine de multiplicité m pour P.

4. Polynômes scindés

Définition :

Un polynôme P, non nul, est dit scindé sur $\mathbb{K}$ s'il existe $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n \in \mathbb{K}$, $\lambda \in \mathbb{K}^*$ tels que :
$P = \lambda(X - a_1)(X - a_2)\ldots(X - a_n)$.

Remarques :

1. $n = \deg(P)$
2. $\{a_i\}$: racines de P
3. λ est le coefficient dominant
4. Cette factorisation est unique à l'ordre des facteurs près.

Théorème de d'Alembert-Gauss (admis) :

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

Corollaire :

Tout polynôme de $\mathbb{C}[X]$ non nul est scindé sur $\mathbb{C}$.

Preuve du corollaire :

Récurrence sur $n = \deg(P)$

- Pour $n = 0$: $P = \lambda$ avec $\lambda \in \mathbb{C}^*$, P est scindé.
- Supposons $n \in \mathbb{N}^*$ et la propriété vrai au rang n. Soit P de degré $n+1 \geqslant 1$
  Théorème de Gauss $\Rightarrow$ P admet une racine complexe : $\exists Q \in \mathbb{C}[X]$ tel que $P = (X - a_0)Q \quad \deg(Q) = n$
  On applique l'hypothèse de récurrence à Q : $\exists \lambda \in \mathbb{C}^*$, $\exists a_1, a_2, \ldots, a_n \in \mathbb{C}$ tels que :
  $Q = \lambda(X - a_1)(X - a_2)\ldots(X - a_n) \Rightarrow P = \lambda(X - a_0)(X - a_1)\ldots(X - a_n)$ donc P est scindé.
  La propriété est vraie au rang $n+1$.

Par récurrence, la propriété est vraie pour tout $n \in \mathbb{N}$.

Proposition :

Les polynômes irréductibles différents de 0 de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1.

Preuve :

- Les polynômes de degré 1 sont irréductibles.
- Si $\deg(P) \geqslant 2$ d'après le corollaire, P est scindé, $P = \lambda(X - a_1)(X - a_2)\ldots(X - a_n)$
  P n'est pas irréductible car $(X - a_1) | P$ et $(X - a_1)$ n'est pas constant s'il est associé à P.

Proposition :

Les polynômes irréductibles non constants de $\mathbb{R}[X]$ sont exactements ceux de degré 1 et ceux de degré 2 à $\Delta<0$.

Preuve :

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

- Si $\deg(P)=1$, P est irréductible.
- Si $\deg(P)=2$ et $\Delta<0$, P est irréductible.
- Soit P irréductible tel que $\deg(P)>1$. D'après le théorème de Gauss , P admet un racine complexe a ($a\notin\mathbb{R}$)
  $P\in\mathbb{R}[X]\ \Rightarrow\ \overline{a}$ est racine de P et $a\notin\mathbb{R}\ \Rightarrow\ \overline{a}\neq a\ \Rightarrow\ (X-a)(X-\overline{a})\mid_{\mathbb{C}} P$
  $(X-a)(X-\overline{a})=X^2-2\Re(a)X+|a|^2\in\mathbb{R}[X]$ donc $(X-a)(X-\overline{a})\mid_{\mathbb{R}} P$
  P est irréductible $\Rightarrow\ \exists\lambda\in\mathbb{R}^*$ tel que $P=\lambda(X^2-2\Re(a)X+|a|^2)$ donc $\deg(P)=2\quad\Delta=4(\Re(a)^2-|a|^2)<0$

5. Relations coefficients / racines

5.1. $n=2$

Si $P=aX^2+bX+c$ a pour racines x_1,x_2, on pose $\begin{cases}\sigma_1=x_1+x_2\\ \sigma_2=x_1x_2\end{cases}$ et on a $\begin{cases}\sigma_1=\dfrac{-b}{a}\\ \sigma_2=\dfrac{c}{a}\end{cases}$

5.2. $n=3$

Soit P un polynôme de degré 3, scindé : P possède 3 racines x_1,x_2,x_3.

$P=aX^3+bX^2+cX+d=a(X-x_1)(X-x_2)(X-x_3)$

$P=aX^3-aX^2(x_1+x_2+x_3)+aX(x_1x_2+x_2x_3+x_1x_3)-x_1x_2x_3$

On pose $\begin{cases}\sigma_1=x_1+x_2+x_3=\dfrac{-b}{a}\\ \sigma_2=x_1x_2+x_2x_3+x_1x_3=\dfrac{c}{a}\\ \sigma_3=x_1x_2x_3=\dfrac{-d}{a}\end{cases}$ $\sigma_1,\sigma_2,\sigma_3$: relations symétriques élémentaires.

5.3. $n\in\mathbb{N}$

Soit P un polynôme de degré $n\geqslant 1$, scindé : P possède n racines $x_1,x_2,\ldots,x_n$.

$P=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_1X^1+a_0=a_n(X-x_1)(X-x_2)\ldots(X-x_n)$

$P=a_n\left[X^n-(x_1+x_2+\ldots+x_n)X^{n-1}+\left(\sum_{1\leqslant i<j\leqslant n}x_ix_j\right)X^{n-2}+\ldots+(-1)^n(x_1x_2\ldots x_n)\right]$

On pose : $\begin{cases}\sigma_1=x_1+x_2+\ldots+x_n=\dfrac{-a_{n-1}}{a_n}\qquad\sigma_2=\displaystyle\sum_{1\leqslant i<j\leqslant n}x_ix_j=\dfrac{a_{n-2}}{a_n}\\ \sigma_k=\displaystyle\sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n}x_{i_1}x_{i_2}\ldots x_{i_k}=(-1)^k\dfrac{a_{n-k}}{a_n}\\ \sigma_n=x_1x_2\ldots x_n=(-1)^n\dfrac{a_0}{a_n}\end{cases}$

* * * * *