1. Cours 6: Anneau des polynômes

1.1. L'ensemble des polynômes à une indéterminée

Définitions: *Soit* $(A,+,.)$ *un anneau unitaire et commutatif*
On appelle polynôme à une indéterminée X *et à coefficients dans* A *toutes écriture algebrique de la forme* $a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$
où les $a_i \in A$ *sont nuls sauf un nombre fini.*
Si on note P *ce polynôme, alors:*
** Les* a_i *sont appelés les coefficients de* P*.*
** Le plus grand indice* n *vérifiant* $a_n \neq 0$ *(s'il existe) est appelé degré de* P *et noté* $\deg P$ *et dans ce cas* a_nX^n *est appelé terme dominant de* P*.*
** Si le terme dominant de* P *est* $1X^n$ *le polynôme* P *est dit unitaire.*
** Si tous les* a_i *sont nuls ,*P *est appelé polynôme nul noté* 0 *et par convention* $\deg 0 = -\infty$
** Chaque élément* a_0 *de* A *est un polynôme, appelé polynôme constant.*
L'ensemble des polynômes à une indéterminée X *à coefficients dans* A *est noté* $A[X]$.

Remarques:

1) Dans un polynôme, on omet souvent les a_iX^i pour les a_i nuls et on l'écrit suivant les puissances décroissantes de X.

2) On écrit souvent, X au lieu de X^1 et X^n au lieu de $1X^n$.

3) Soient $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$
et $Q = b_0 + b_1X^1 + ... + b_{n-1}X^{n-1} + b_nX^n + ...$

$$(P = Q) \Leftrightarrow (\forall i \in \mathbb{N} : a_i = b_i).$$

Exemples :

1) $P = X^n - 1$ (où $n \in \mathbb{N}^*$) est un polynôme unitaire de degré n à coefficients dans $\mathbb{Z}$, C.à.d $P \in \mathbb{Z}[X]$.
Le terme dominant de P est X^n et ses coefficients sont $(-1, 0, ..., 0, 1, 0, ..., 0, ...)$.
C.à.d: Tous les coefficients sont nuls sauf $a_0 = -1$, et $a_n = 1$.

2) $Q = 2X^3 - \sqrt{5}X$ est un polynôme non unitaire de degré 3 à coefficients dans $\mathbb{R}$, C.à.d $Q \in \mathbb{R}[X]$.
Le terme dominant de Q est $2X^3$ et ses coefficients sont $\left(0, -\sqrt{5}, 0, 2, 0, ..., 0, ...\right)$.
C.à.d: Tous les coefficients sont nuls sauf $a_1 = -\sqrt{5}$ et $a_3 = 2$.

3) $S = 4 + 2i$ est un polynôme non unitaire de degré 0 (polynôme constant) à coefficients dans $\mathbb{C}$, C.à.d $S \in \mathbb{C}[X]$.
Le terme dominant de S est $4 + 2i$ et ses coefficients sont $(4 + 2i, 0, ..., 0, ...)$;
C.à.d: Tous les coefficients sont nuls sauf $a_0 = 4 + 2i$.

1.2. Opérations sur l'ensemble $A[X]$

Définitions: *Soient* $P = a_0 + a_1X^1 + ... + a_{n-1}X^{n-1} + a_nX^n + ...$
et $Q = b_0+b_1X^1+...+b_{n-1}X^{n-1}+b_nX^n+...$ *deux polynômes de* $A[X]$
On définit la somme $P+Q$ *et le produit* $P.Q$ *par:*

$$P+Q = (a_0+b_0) + (a_1+b_1)X^1 + ... + (a_{n-1}+b_{n-1})X^{n-1} + (a_n+b_n)X^n + ...$$

$$P.Q = \left(\sum_{i+j=0} a_i.b_j\right) + \left(\sum_{i+j=1} a_i.b_j\right)X^1 + ... + \left(\sum_{i+j=n-1} a_i.b_j\right)X^{n-1} + \left(\sum_{i+j=n} a_i.b_j\right)X^n + ...$$

Remarques:

1) $c_0 = \sum_{i+j=0} a_i.b_j = a_0.b_0 = \sum_{i=0}^{0} a_i.b_{0-i}$

$c_1 = \sum_{i+j=1} a_i.b_j = a_0.b_1 + a_1.b_0 = \sum_{i=0}^{1} a_i.b_{1-i}$

.....

$c_n = \sum_{i+j=n} a_i.b_j = a_0.b_n + a_1.b_{n-1} + ... + a_n.b_0 = \sum_{i=0}^{n} a_i.b_{n-i}$

.....

2) Pour énoncer la proposition suivante, on adopte la convention suivante:
Pour tout $n \in \mathbb{N}$: $n + (-\infty) = (-\infty) + n = -\infty, \qquad -\infty < n$
et $(-\infty) + (-\infty) = -\infty$

Proposition: *Soient* $P,\ Q \in A[X]$, *alors:*
$\deg(P+Q) \leq \max(\deg P, \deg Q)$ *et* $\deg(P.Q) \leq \deg P + \deg Q$
et si A *est un corps, alors* $\deg(P.Q) = \deg P + \deg Q$

Preuve: Posons $n = \deg P$, $m = \deg Q$,
$P = a_0+a_1X^1+...+a_{n-1}X^{n-1}+a_nX^n$ et $Q = b_0+b_1X^1+...+b_{m-1}X^{m-1}+b_mX^m$
1^{er} cas) Si $P = 0$ ou $Q = 0$.
Par exemple si $P = 0$, alors $P+Q = Q$ et $P.Q = 0$ ainsi
$\deg(P+Q) = \deg Q = \max(-\infty, \deg Q) = \max(\deg P, \deg Q)$
$\deg(P.Q) = -\infty = -\infty + \deg Q = \deg P + \deg Q$
$2^{ème}$ cas) Si $P \neq 0$ et $Q \neq 0$, alors:
2.1) Les coefficients de $P+Q$ sont tous nuls après le rang $k = \max(n,m)$
donc $\deg(P+Q) \leq \max(n,m) = \max(\deg P, \deg Q)$
2.2) Les coefficients $c_k = \sum_{i+j=k} a_i.b_j$ de $P.Q$ vérifient pour tout $k \in \mathbb{N}^*$:

$$c_{(n+m)+k} = \sum_{i+j=n+m+k} a_ib_j = \underbrace{a_0b_{n+m+k} + ... + a_nb_{m+k}}_{\text{dans ce terme tous les } b_j \text{ sont nuls}} + \underbrace{a_{n+1}b_{m+k-1} + ... + a_{n+m+k}b_0}_{\text{dans ce terme tous les } a_i \text{ sont nuls}}$$

$$= 0$$

Ainsi $\deg(P.Q) \leq n+m = \deg P + \deg Q$.

$$c_{n+m} = \sum_{i+j=n+m} a_i.b_j = \underbrace{a_0.b_{n+m} + ... + a_{n-1}.b_{m+1}}_{\text{dans ce terme tous les } b_j \text{ sont nuls}} + a_n.b_m + \underbrace{a_{n+1}.b_{m-1} + ... + a_{n+m}.b_0}_{\text{dans ce terme tous les } a_i \text{ sont nuls}}$$

$$= a_n.b_m$$

Si A est un corps, alors $c_{n+m} = a_n.b_m \neq 0$ car $a_n \neq 0$ et $b_m \neq 0$.

D'où $\deg(P.Q) = n+m = \deg P + \deg Q$. ■

Exemples :

1) Dans $\mathbb{Q}[X]$, soient les polynômes:

$P = 3X^2 - 1$ C.à.d: $P = 3X^2 + 0X - 1$

et $Q = \frac{1}{2}X^3 + 4X$ C.à.d $Q = \frac{1}{2}X^3 + 0X^2 + 4X + 0$ alors,

$$P+Q = \left(0+\tfrac{1}{2}\right)X^3 + (3+0)X^2 + (0+4)X + (-1+0) \quad \text{et}$$
$$= \tfrac{1}{2}X^3 + 3X^2 + 4X - 1$$

$$P.Q = \left(3\times\tfrac{1}{2}\right)X^5 + \left(\left(0\times\tfrac{1}{2}\right) + (3\times 0)\right)X^4$$
$$+ \left(\left((-1)\times\tfrac{1}{2}\right) + (0\times 0) + (3\times 4) + (0\times 0)\right)X^3$$
$$+ \left(((-1)\times 0) + (0\times 4) + (3\times 0)\right)X^2 + \left((-1)\times 4 + 0\times 0\right)X + ((-1)\times 0)$$
$$= \tfrac{3}{2}X^5 + 0X^4 + \tfrac{23}{2}X^3 + 0X^2 - 4X + 0 \quad = \tfrac{3}{2}X^5 - \tfrac{23}{2}X^3 - 4X$$

Théoreme: $(A[X], +, .)$ *est un anneau unitaire et commutatif.*

Preuve:

Soient $P = p_0 + p_1X^1 + ... + p_{n-1}X^{n-1} + p_nX^n + ...$

$Q = q_0 + q_1X^1 + ... + q_{m-1}X^{m-1} + q_mX^m + ...$

et $S = s_0 + s_1X^1 + ... + s_{k-1}X^{k-1} + s_kX^k + ..$

1) $P+Q = (p_0+q_0) + (p_1+q_1)X^1 + ... + (p_{k-1}+q_{k-1})X^{k-1} + (p_k+q_k)X^k + ... \in A[X]$.

Alors l'addition des polynômes est une loi interne dans $A[X]$.

2) $(P+Q)+S = ((p_0+q_0)+s_0)+((p_1+q_1)+s_1)X^1+...+((p_{k-1}+q_{k-1})+s_{k-1})X^{k-1}$
$+ ((p_k+q_k)+s_k)X^k + ...$
$= (p_0+(q_0+s_0))+(p_1+(q_1+s_1))X^1+...+(p_{k-1}+(q_{k-1}+s_{k-1}))X^{k-1}$
$+ (p_k+(q_k+s_k))X^k + ...$
$= P+(Q+S)$

Alors l'addition des polynômes est une loi associative dans $A[X]$.

3) $P+Q = (p_0+q_0)+(p_1+q_1)X^1+...+(p_{k-1}+q_{k-1})X^{k-1}+(p_k+q_k)X^k+...$
$= (q_0+p_0)+(q_1+p_1)X^1+...+(q_{k-1}+p_{k-1})X^{k-1}+(q_k+p_k)X^k+...$
$= Q+P$

Alors l'addition des polynômes est une loi commutative dans $A[X]$.

4) Le polynôme nul $0 + 0X^1 + ... + 0X^{k-1} + 0X^k + ...$ est aussi noté 0.

$P + 0 = (p_0+0) + (p_1+0)X^1 + ... + (p_{k-1}+0)X^{k-1} + (p_k+0)X^k + ...$
$= P$

Alors le polynômes 0 est l'élement neutre de l'addition des polyômes dans $A[X]$.

5) Notons par $-P$ le polynôme

$$(-p_0) + (-p_1) X^1 + ... + (-p_{n-1}) X^{n-1} + (-p_n) X^n + ...$$

On a:

$$\begin{aligned} P+(-P) &= (p_0 - p_0)+(p_1 - p_1) X^1+...+(p_{n-1} - p_{n-1}) X^{n-1}+(p_n - p_n) X^n+... \\ &= 0 \end{aligned}$$

Alors $-P$ est le symétrique de P par rapport à l'addition des polyômes dans $A[X]$.

6) $$P.Q = \left(\sum_{i+j=0} p_i.q_j\right) + \left(\sum_{i+j=1} p_i.q_j\right) X^1 + ... + \left(\sum_{i+j=k-1} p_i.q_j\right) X^{k-1} + \left(\sum_{i+j=k} p_i.q_j\right) X^k + ... \in A[X].$$

Alors la multiplication des polynômes est une loi interne dans $A[X]$.

7) $$\begin{aligned} P.Q &= \left(\sum_{i+j=0} p_i.q_j\right)+\left(\sum_{i+j=1} p_i.q_j\right) X^1+...+\left(\sum_{i+j=k-1} p_i.q_j\right) X^{k-1} + \left(\sum_{i+j=k} p_i.q_j\right) X^k + ... \\ &= \left(\sum_{i+j=0} q_j.p_i\right)+\left(\sum_{i+j=1} q_j.p_i\right) X^1+...+\left(\sum_{i+j=k-1} q_j.p_i\right) X^{k-1} + \left(\sum_{i+j=k} q_j.p_i\right) X^k + ... \\ &= Q.P \end{aligned}$$

Alors la multiplication des pôlynomes est commutative dans $A[X]$.

8) Si $Q = 1 + 0X^1 + ... + 0X^{m-1} + 0X^m + ...$ .C.à.d: $q_0 = 1$ et $\forall j \in \mathbb{N}^*, q_j = 0$.

$$\begin{aligned} \text{Alors } P.Q &= \left(\sum_{i+j=0} p_i.q_j\right) + \left(\sum_{i+j=1} p_i.q_j\right) X^1 + ... + \left(\sum_{i+j=k-1} p_i.q_j\right) X^{k-1} \\ &\quad + \left(\sum_{i+j=k} p_i.q_j\right) X^k + ... \\ &= (p_0.1) + (p_1.1) X^1 + ... + (p_{k-1}.1) X^{k-1} + (p_k.1) X^k + ... \\ &= P \end{aligned}$$

Alors $Q = 1$ est l'élément neutre de la multiplication des pôlynomes dans $A[X]$.

9) Notons respectivement les coefficients de $(P.Q).S$, $P.(Q.S)$, $P.Q$ et $Q.S$ par $((P.Q).S)_l$, $(P.(Q.S))_l$, $(P.Q)_l$ et $(Q.S)_l$

$$\begin{aligned} ((P.Q).S)_l &= \sum_{r+k=l} (P.Q)_r .s_k = \sum_{r+k=l} \left(\sum_{i+j=r} p_i.q_j\right).s_k \\ &= \sum_{r+k=l} \left(\sum_{i+j+k=r+k} p_i.q_j.s_k\right) = \sum_{i+j+k=l} p_i.q_j.s_k \end{aligned}$$

$$\begin{aligned}(P.(Q.S))_l &= \sum_{i+r=l} p_i.(Q.S)_r = \sum_{i+r=l} p_i.\left(\sum_{j+k=r} q_j.s_k\right)\\ &= \sum_{i+r=l}\left(\sum_{i+j+k=i+r} p_i.q_j.s_k\right) = \sum_{i+j+k=l} p_i.q_j.s_k\end{aligned}$$

d'où $(P.Q).S = P.(Q.S)$ car ils ont les mêmes coefficients.

Alors la multiplication des pôlynomes est associative dans $A[X]$.

10) Gardons les notation de 7) et notons respectivement les coefficients de $(P+Q).S$, $P+Q$, $P.S$ et $Q.S$ par $((P+Q).S)_l$, $(P+Q)_l$, $(P.S)_l$ et $(Q.S)_l$, alors,

$$\begin{aligned}((P+Q).S)_l &= \sum_{r+k=l}(P+Q)_r.s_k = \sum_{r+k=l}(p_r+q_r).s_k\\ &= \sum_{r+k=l} p_r.s_k + \sum_{r+k=l} q_r.s_k = (P.S)_l + (Q.S)_l\\ &= (P.S+Q.S)_l\end{aligned}$$

d'où $(P+Q).S = P.S + Q.S$, car ils ont les mêmes coefficients.

Alors la multiplication est distributive par rapport à l'addition dans $A[X]$.

Par suite $(A[X], +, .)$ est un anneau commutatif et unitaire. ■

Proposition: *Si K est un corps commutatif, alors $(K[X], +, .)$ est un anneau intègre.*

C.à.d: $(\forall P, Q \in K[X] : P.Q = 0) \Rightarrow (P = 0 \ \vee \ Q = 0)$

Preuve:

$$\begin{aligned}P.Q = 0 &\Rightarrow \deg(P.Q) = \deg 0 = -\infty\\ &\Rightarrow \deg P + \deg Q = -\infty\\ &\Rightarrow \deg P = -\infty \vee \deg Q = -\infty\\ &\Rightarrow P = 0 \vee Q = 0\end{aligned}$$ ■

1.3. Arithmétique dans $K[X]$

Dans la suite, on suppose que K est un corps.

1.3.1. Divisibilité:

Soient P,$B \in K[X]$
On dit que B divise P , s'il exite $Q \in K[X]$ tel que $P = Q.B$

Exemples:

1) Tout élément $a \neq 0$ du corps K divise tout polynôme P de $K[X]$

Car: $P = a.(a^{-1}P)$ et $a^{-1}P$ est bien un polynôme.

2) Tout polynôme P divise le polynôme nul 0, car: $0 = 0.P$

3) $X+1$ divise X^2+X, car: $X^2+X=X(X+1)$

Remarques:

1) 0 ne divise que 0.

2) Les diviseurs de 1 sont les éléments de K^*, qui sont les seuls éléments inversibles dans $K[X]$.

En effet: Soit $B \in K[X]$

B divise $1 \Rightarrow \exists Q \in K[X] : 1 = QB$

$\Rightarrow \exists Q \in K[X] : \deg QB = 0$

$\Rightarrow \exists Q \in K[X] : \deg Q + \deg B = 0$

$\Rightarrow \exists Q \in K[X] : \deg Q = \deg B = 0$

Donc $Q = q_0 \in K$ et $B = b_0 \in K$ avec $1 = q_0.b_0$.

(si $1 = QB$, alors $0 = \deg 1 = \deg Q + \deg B$, d'où $\deg Q = \deg B = 0$ donc $Q = q_0$ et $B = b_0$ avec $1 = q_0 b_0$)

3) Si B divise P , on dit que P est un multiple de B.

4) Si B divise P et $P \neq 0$, alors $\deg B \leq \deg P$

En effet: B divise $P \Rightarrow \exists Q \in K[X] : P = Q.B$

$\Rightarrow \exists Q \in K[X] : \deg P = \deg Q + \deg B$

$\deg Q \geq 0$, sinon $\deg Q = -\infty$ donc $\deg P = \deg Q + \deg B = -\infty$ C.à.d: $P = 0$ ce qui contredit les hypothèses.

Alors $\deg P \geq \deg B$

1.3.2. Division euclidienne dans $K[X]$:

Soient P , $B \in K[X]$

Si $B \neq 0$*, alors il existe un couple unique* $(Q, R) \in K[X]^2$ *tels que*

$$P = QB + R \qquad \text{et } \deg R < \deg B$$

Preuve: a) Pour montrer l'existence, on a deux cas possibles.

a.1) Si $P = 0$, alors $P = 0.B + 0$. C.à.d: $Q = R = 0$, ce qui vérifie $\deg R < \deg B$ (car $\deg P = -\infty$ et $\deg B \geq 0$)

a.2) Si $P \neq 0$, $\deg P = n \in \mathbb{N}$ et $\deg B = m \in \mathbb{N}$, alors $P = p_0 + p_1 X + ... + p_n X^n$ et $B = b_0 + b_1 X + ... + b_m X^m$

Raisonnons par récurrence sur n.

* Si $n = 0$, c.à.d $P = p_0$, on a deux cas:

$1^{er} cas$: Si $m = 0$, alors $B = b_0$ d'où $P = p_0 b_0^{-1}.B + 0$. C.à.d: $Q = p_0 b_0^{-1}$ et $R = 0$, ce qui vérifie $\deg R < \deg B$ (car $\deg P = -\infty$ et $\deg B = 0$).

$2^{ème} cas$: Si $m > 0$, alors $P = 0.B + P$. C.à.d: $Q = 0$ et $R = P$, ce qui vérifie $\deg R < \deg B$ (car $\deg P = 0$ et $\deg B > 0$).

* Supposons le théorème vrai pour tout polynôme de degré inférieur ou égal à $n-1$ et montrons qu'il reste vrai pour les polynômes de degré n.

On a deux cas

$1^{er} cas$: Si $m > n$, alors $P = 0.B + P$. C.à.d: $Q = 0$ et $R = P$, ce qui vérifie $\deg R < \deg B$ (car $\deg R = n$ et $\deg B = m$).

$2^{ème} cas$: Si $m \leq n$, alors $\bar{P} = P - a_n b_n^{-1} X^{n-m}.B$ est de degré inférieur ou égal à $n-1$, alors d'après l'hypothèse de récurrence $\bar{P} = \bar{Q}B + \bar{R}$ avec $\deg \bar{R} < \deg B$

par conséquent $P = \bar{P} + a_n b_n^{-1} X^{n-m}.B = \left(\bar{Q} + a_n b_n^{-1} X^{n-m}\right) B + \bar{R}$, c.à.d: $Q = \bar{Q} + a_n b_n^{-1} X^{n-m}$ et $R = \bar{R}$, ce qui vérifie $\deg R < \deg B$ (car $\deg R = \deg \bar{R}$)

b) Pour montrer l'unicité, on suppose que $P = Q.B + R = Q_1.B + R_1$ tels que $\deg R < \deg B$ et $\deg R_1 < \deg B$.

Alors $(Q - Q_1).B = (R_1 - R)$ et par passage aux degrés, on obtient $\deg (Q - Q_1) + \deg B = \deg (R_1 - R) \leq \max (\deg R_1, \deg R) < \deg B$, d'où $\deg (Q - Q_1) = -\infty$, ainsi $Q - Q_1 = 0$ et par suite $R_1 - R = 0$ ■

Remarque: La preuve précédente montre que la division euclidienne de P par B, se ramène à la division euclidienne de $\bar{P}$ par B, avec $\deg \bar{P} < \deg P$.

Ceci est la base d'un procédé itératif appelé algorithme de la division euclidienne des polynômes.

Exemple: Divisons $P = 3X^5 - 2X^3 - 5X^2 + 1$ par $B = 2X^3 + \frac{1}{2}X^2 - X$

$3X^5 + 0X^4 - 2X^3 - 5X^2 + 0X + 1$	$\frac{1}{2}X^3 + 2X^2 - X + 0$
$-12X^4 + 4X^3 - 5X^2 + 0X + 1$	$6X^2 - 24X + 104$
$52X^3 - 29X^2 + 0X + 1$	
$-237X^2 + 104X + 1$	

donc le quotient $Q = 6X^2 - 24X + 104$ et le reste $R = -237X^2 + 104X + 1$

1.4. Fonctions polynômes d'une variable, polynôme dérivé et racine d'un polynôme

Définitions: *Soit* $P = a_0 + a_1 X^1 + ... + a_{n-1} X^{n-1} + a_n X^n$ *un polynôme de* $K[X]$.

1) On appelle fonction polynôme d'une variable x *associée à* P, *la fonction* $\widetilde{P} : K \to K$ *définie par:* $\widetilde{P}(x) = a_0 + a_1 x^1 + ... + a_{n-1} x^{n-1} + a_n x^n$

2) On dit qu'un élément α *est une racine ou zéro de* P, *si* $\widetilde{P}(\alpha) = 0$.

3) On appelle dérivé du polynôme P *le polynôme noté* P' *et défini par:*

$P' = a_1 + 2a_2 X^1 + ... + (n-1) a_{n-1} X^{n-2} + n a_n X^{n-1}$

Exemples:

1) La fonction polynôme associée au polynôme $P = X^2 + 2X - 3$ de $\mathbb{R}[X]$ est la fonction $\widetilde{P} : \mathbb{R} \to \mathbb{R}$ telle que $\widetilde{P}(x) = x^2 + 2x - 3$ et les seules racines de P sont -3 et 1, car $\widetilde{P}(-3) = \widetilde{P}(1) = 0$

Le polynôme dérivé de P est $P' = 2X + 2$

2)La fonction polynôme associée au polynôme $P = X^2 - 2$ de $\mathbb{Q}[X]$ est la fonction $\widetilde{P} : \mathbb{Q} \to \mathbb{Q}$ telle que $\widetilde{P}(x) = x^2 - 2$ et P n'a pas de racine car $\widetilde{P}(x) \neq 0$ pour tout $x \in \mathbb{Q}$.

Le polynôme dérivé de P est $P' = 2X$

Remarques:

1) On dit que $\widetilde{P}(x)$ est obtenu par substitution de x à X dans P.

2) On vérifie, facilement, que $\widetilde{P+Q} = \widetilde{P} + \widetilde{Q}$, $\widetilde{P.Q} = \widetilde{P}.\widetilde{Q}$, $\widetilde{P'} = \widetilde{P}'$, $(P+Q)' = P' + Q'$ et $(P.Q)' = P'.Q + P.Q'$

3) Si $\deg P \geq 1$, alors $\deg P' = \deg P - 1$ et si $\deg P < 1$, alors $\deg P' = -\infty$

Théorème: *Soit $P \in K[X]$ et $\alpha \in K$, alors:*

1) Le reste de la division euclidienne de P par $X - \alpha$ est $\widetilde{P}(\alpha)$.

2) α est une racine de P si, et seulement, si $X - \alpha$ divise P

Preuve: 1) On a $P = (X - \alpha) Q + R$ où R et Q sont, respectivement, le reste et le quotient de la division euclidienne de P par $X - \alpha$. Alors $\widetilde{P} = \widetilde{(X - \alpha)}\widetilde{Q} + \widetilde{R}$, ainsi $\widetilde{P}(\alpha) = \widetilde{R}(\alpha)$.

Or $\deg R < \deg(X - \alpha) = 1$, donc R et constant, d'où $\widetilde{R} = R$ et $\widetilde{R}(\alpha) = R$. Par conséquent $\widetilde{P}(\alpha) = R$.

2) Cette assertion est une conséquence directe de 1). ■

Exemple: -3 est une racine du polynôme $P = X^3 + 5X^2 + 3X - 9$ de $\mathbb{R}[X]$, alors $P = (X + 3) Q$ avec $Q = 2X + X^2 - 3$

Ordre de multiplicité d'une racine: *Soit $P \in K[X]^*$ et α une racine de P. On appelle ordre de multiplicité de la racine α de P, le plus grand $m \in \mathbb{N}$ tel que $(X - \alpha)^m$ divise P.*

** Si $m = 1$, on dit que α est une racine simple de P*

** Si $m = 2$, on dit que α est une racine double de P.*

** Si $m = 3$, on dit que α est une racine triple de P. ...etc*

Exemple: -3 est une racine double du polynôme $P = X^3 + 5X^2 + 3X - 9$ de $\mathbb{R}[X]$, car $P = (X + 3)^2 (X - 1)$

Théorème: *Soient $P \in K[X]^*$ et $\alpha \in K$.*

α est une racine simple de P si, et seulement, si $\widetilde{P}(\alpha) = 0$ et $\widetilde{P}'(\alpha) \neq 0$ (où $\widetilde{P}'$ est la dérivée de $\widetilde{P}$)

Preuve: α est une racine simple de P si, et seulement, s'il existe $Q \in K[X]$ tel que $P = (X-\alpha)Q$ et $Q(\alpha) \neq 0$.

Or $\widetilde{P}' = \widetilde{Q} + (x-\alpha)\widetilde{Q}'$ donc $\widetilde{P}'(\alpha) = Q(\alpha)$, d'où l'équivalence voulue. ■

Exemple: Soit le polynôme $P = X^3 + 5X^2 + 3X - 9$ de $\mathbb{R}[X]$,

On a $\widetilde{P}(1) = 0$ et $\widetilde{P}'(1) \neq 0$ $(\widetilde{P}'(x) = 3X^2 + 10X + 3)$

Proposition: *Si $\alpha_1, \alpha_2, ..., \alpha_r$ sont des racines deux à deux distinctes de P, d'ordres de multiplicité respectifs $m_1, m_2, ..., m_r$, alors $\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$ divise P.*

Preuve: Les α_i sont deux à deux distinctes, alors les polynômes $X - \alpha_i$ sont premiers entre eux et par suite $(X-\alpha_i)^{m_i}$sont premiers entre eux

Or $(X-\alpha_i)^{m_i}$ divise P donc $\prod_{i=1}^{r}(X-\alpha_i)^{m_i}$ divise P. ■

Corollaire: *1) Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines distinctes.*

2) *Si P possède une infinité de racines, alors P est le polynôme nul.*

Preuve: 1) Supposons $\alpha_1, \alpha_2, ..., \alpha_{n+1}$ des racines distinctes de P, alors d'après la proposition précédente, $\prod_{i=1}^{n+1}(X-\alpha_i)$ divise P, donc $n+1 = \deg\left(\prod_{i=1}^{n+1}(X-\alpha_i)\right) \leq \deg P = n$ ce qui est absurde.

2) L'assertion 1) montre que si P admet une infinité de racine, alors $\deg P \notin \mathbb{N}$, donc P est nul. ■

Théorème:(Théorème fondamental de l'algèbre): *Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$.*

Autrement dit: Tout polynôme de $\mathbb{C}[X]$ de degré $n \geq 1$ admet n racines.

(La preuve de ce théorème dépasse le cadre du cours d'algèbre de $1^{ère}$ année LMD)

Remarque: Il existe des formules donnant les racines d'un polynôme de degré $1, 2, 3$ et 4 de $\mathbb{C}[X]$. De telles formules n'existent pas pour un polynôme de degré $n \geq 5$, alors on ne peut décomposer un polynôme de $\mathbb{C}[X]$ que dans des cas particuliers.

Exemple: Soit $P = X^7 - 8X$

$$\begin{aligned} P &= X^7 - 8X = X(X^6 - 8) = X\left((X^2)^3 - 2^3\right) = X(X^2-2)(X^4+2X^2+4) \\ &= X(X^2-2)\left(X^2+1-i\sqrt{3}\right)\left(X^2+1+i\sqrt{3}\right) \\ &= X\left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right)\left(X-\tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X+\tfrac{1+i\sqrt{3}}{\sqrt{2}}\right)\left(X-\tfrac{1-i\sqrt{3}}{\sqrt{2}}\right)\left(X+\tfrac{1-i\sqrt{3}}{\sqrt{2}}\right) \end{aligned}$$

P admet 7 racines dans $\mathbb{C}$, 3 racines dans $\mathbb{R}$ et 1 racine dans $\mathbb{Q}$.

Cette écriture est une décomposition de P en facteurs indécomposables dans $\mathbb{C}[X]$.

Pour obtenir la décomposition en facteurs indécomposables dans $\mathbb{R}[X]$, il faut remplacer les facteurs dont les produits sont des polynômes indécomposables dans $\mathbb{R}[X]$ par leurs produits.

Cette écriture est une décomposition de P en facteurs indécomposables dans $\mathbb{R}[X]$.

Pour obtenir la décomposition en facteurs indécomposables dans $\mathbb{Q}[X]$, il faut remplacer les facteurs dont les produits sont des polynômes indécomposables dans $\mathbb{Q}[X]$ par leurs produits.

$$\begin{aligned} P &= X\left(X-\sqrt{2}\right)\left(X+\sqrt{2}\right)\left(X^2-\sqrt{2}X+2\right)\left(X^2+\sqrt{2}X+2\right) \\ &= X\left(X^2-2\right)\left(X^4+2X^2+4\right) \end{aligned}$$

cette écriture est une décomposition de P en facteurs indécomposables dans $\mathbb{Q}[X]$.