Algèbre 3 : Premier chapitre

ℌ.ℭ ℑ.ℨ

11 décembre 2020

Table des matières

1 Anneau des polynômes à une indéterminé

1.1 Rappel sur les Anneaux

1.1.1 Définitions

Définition 1.1.1 *Soit A un ensemble muni de deux lois internes notées " $+$ " et ".". On dit que $(A, +, .)$ est un* ***Anneau*** *si :*

(i) $(A, +)$ *est un groupe commutatif,*

(ii) La loi "." est associative,

(iii) La loi "." est distributive par rapport à la loi " $+$ ".

Si la loi "." admet un élément neutre, l'anneau A est dit unitaire ; Si la loi "." est commutative, A est commutatif ; Un élément de A est dit inversible s'il est pour la loi . de A.

Notation. Le neutre pour la loi " $+$ " est souvent noté 0, celui de la loi "." par 1_A.

Définition 1.1.2 *Un élément a de A est dit* ***diviseur*** *de 0 à droite (resp. à gauche) si $a \neq 0$ et s'il existe $b \neq 0$ tel que $ab = 0$ (resp. $ba = 0$).*

Définition 1.1.3 *Un anneau A est dit* ***intègre*** *s'il ne possède aucun diviseur de 0, autrement dit si ($a \neq 0$ et $b \neq 0 \Longrightarrow ab \neq 0$).*

Définition 1.1.4 *Un élément a de A est dit* ***nilpotent*** *s'il existe un entier naturel $n \neq 0$ tel que $a^n = 0$. L'indice (ou l'ordre) de nilpotence de a est le plus petit entier non nul n tel que $a^n = 0$.*

Définition 1.1.5 *Un sous-ensemble B de A est dit* ***sous-anneau*** *de A si $(B, +, .)$ est un anneau i.e :*

1) $\forall a, b \in A[a, b \in B \Longrightarrow a - b \in B]$.

2) $\forall a, b \in A[a, b \in B \Longrightarrow ab \in B]$.
Et si l'anneau A est unitaire

3) $1_A \in B$

Proposition 1.1.1 *Soit A un anneau et soit $A' \subset A$. Pour montrer que A' est anneau il suffit de montrer que A' est sous-anneau de A.*

Exemple 1.1.1

1. *$(\mathbb{Z}, +, .)$ est un anneau commutatif unitaire intègre*
   Soit $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$.
   On a $nk - nk' = n(k - k') \in n\mathbb{Z}$.
   Et on a $(nk)(nk') = n(nkk') \in n\mathbb{Z}$. Donc $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$
2. *Soit $\mathcal{M}_2(\mathbb{R})$: l'ensemble des matrices carrés d'ordre 2, muni de deux lois :*
   " $+$ " l'addition des matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix}$$

   " $.$ " *Le produit matriciel*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}$$

   Est un anneau unitaire non-commutatif.
   Les matrices

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}; \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

   Sont deux matrices non nulles de $\mathcal{M}_2(\mathbb{R})$. Mais

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1-1 & 1-1 \\ -1+1 & -1+1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

   Donc $\mathcal{M}_2(\mathbb{R})$ est non intègre.
3. *Soit $\mathcal{D}_2(\mathbb{R})$ l'ensemble $\{\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}; a, b \in \mathbb{R}\}$.*

   $\mathcal{D}_2(\mathbb{R})$ est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$ car :

   - $$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1-a_2 & 0 \\ 0 & b_1-b_2 \end{bmatrix} \in \mathcal{D}_2(\mathbb{R})$$
   - $$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & 0 \\ 0 & b_1b_2 \end{bmatrix} \in \mathcal{D}_2(\mathbb{R})$$
   - *Et de plus*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathcal{D}_2(\mathbb{R})$$

1.1.2 Idéaux

Définition 1.1.6 *Soit $I \subset A$. On dit que I est un* ***Idéal*** *de l'anneau A si :*

(i) I *est non vide,*

(ii) $\forall a, b \in I : a - b \in I$,

(iii) $\forall (a, i) \in A \times I : ai \in I$ *et* $ia \in I$.

Remarque 1.1.1 *1. Un idéal est sous-anneau.*

2. *Si l'anneau A est commutatif, pour tous x de A l'ensemble $xA = \{xa, a \in A\}$ est un idéal de A.*
3. *Si l'anneau A est unitaire et si $1_A \in I$ où I est un idéal de A alors $I = A$, (d'après la propriété (iii)).*
   Si un idéal I de A contient un élément inversible x de A, alors $I = A$ (on a $1_A = x^{-1}x \in I$ et donc $I = A$.
4. *Lorsque I vérifie (i), (ii) et vérifie seulement $ai \in I$ (resp. $ia \in I$) pour tous $(a, i) \in A \times I$, on dit que I est un idéal* ***à gauche*** *(resp.****à droite*** *de A. Si I est à la fois idéal à gauche et idéal à droite de A, I est un idéal de A.*

Exemple 1.1.2

- *$n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, pour tous n de $\mathbb{N}$ car : $nk - nk' = n(k - k') \in n\mathbb{Z}$ et $nkk' \in I$ et $k'nk \in I$, $\forall k, k' \in \mathbb{Z}$*
- *$\mathcal{D}_2(\mathbb{R})$ vérifie les propriétés (i) et (ii) mais (iii) n'est pas vérifiée dans $\mathcal{M}_2(\mathbb{R})$; Donc $\mathcal{D}_2(\mathbb{R})$ n'est pas un idéal dans $\mathcal{M}_2(\mathbb{R})$.*

Proposition 1.1.2 *Les $n\mathbb{Z}$ sont les seuls idéaux de $\mathbb{Z}$.*

Proposition 1.1.3 *Une intersection d'idéaux de A est un idéal de A. Une somme finie d'idéaux de A est un idéal de A.*

Définition 1.1.7 *Soit $(A, +, .)$ un anneau commutatif. Un idéal I de A est dit* ***principal*** *s'il existe $a \in A$ tel que $I = aA$. On note alors $I = (a)$.*
L'anneau A est dit ***principal*** *s'il est commutatif, unitaire, intègre et si tous les idéaux de A sont principaux.*

Exemple 1.1.3 *L'anneau $\mathbb{Z}$ est principal.*

Morphismes d'anneaux

Définition 1.1.8 *Soient A, A' deux anneaux. On appelle* ***morphisme d'anneaux*** *de A dans A' toute application $f : A \longrightarrow A'$ telle que $f(x+y) = f(x)+f(y)$ et $f(xy) = f(x)f(y)$ pour tous $x, y \in A$.*
*Lorsque f est bijective, on parle d'****isomorphisme d'anneaux****.*

Proposition 1.1.4 *Soient A, A' deux anneaux et $f : A \longrightarrow A'$ un morphisme d'anneaux.*

- *L'ensemble $Kerf = f^{-1}(\{0\})$ est un idéal de A et il vérifie (f est injective $\Longleftrightarrow Kerf = \{0\}$).*
- *Si I est un idéal de A et si f est surjective, alors $f(I)$ est un idéal de A'.*
- *Si I' est un idéal de A', alors $f^{-1}(I')$ est un idéal de A.*
- *L'image et l'image réciproque d'un sous-anneau est un sous-anneau.*

Caractéristique d'un anneau

Définition 1.1.9 *Soit A un anneau unitaire dont l'élément neutre pour la loi "." est noté e. Soit le morphisme d'anneau $f : \mathbb{Z} \longrightarrow A$ $n \mapsto ne$.*

- *Si $Kerf = \{0\}$ (i.e.$ne = 0 \Longrightarrow n = 0$). On dit que A est de caractéristique 0.*
- *Si $Kerf \neq \{0\}$, alors Si $Kerf$ est un idéal de $\mathbb{Z}$ principal, il existe un unique entier non nul n tel que $Kerf = n\mathbb{Z}$. L'entier n est aussi le plus petit entier strictement positif tel que $ne = 0$. On dit alors que A est de caractéristique n.*
  On a $ce = 0 \Longrightarrow n \mid c$ (n divise c).

Proposition 1.1.5 *La caractéristique d'un anneau unitaire intègre est soit 0, soit un nombre premier.*

Démonstration *Si la caractéristique n d'anneau A est non nul et si n n'est pas premier, on peut écrire $n = ab$ avec $1 < a < n$ et $1 < b < n$. Donc $0 = ne = (ae)(be)$, et comme A est intègre on en déduit $ae = 0$ ou $be = 0$, absurde car n est le plus petit entier > 0 tel que $ne = 0$.*

Groupe des inversibles d'un anneau unitaire

Définition 1.1.10 *Les éléments d'un anneau unitaire $(A, +, .)$ inversibles pour la loi "." sont appelés les inversibles de l'anneau A.*

Proposition 1.1.6 *L'ensemble des inversibles d'un anneau unitaire, muni de la loi multiplicative, est un groupe appelé groupe des inversibles de A.*

Exemple 1.1.4 *On a $(\mathbb{Z}, +, .)$ est un anneau unitaire. Les éléments inversibles de $\mathbb{Z}$ sont -1, et 1. D'après le tableau suivant*

.	-1	1
-1	1	-1
1	-1	1

on vois que ($\{-1, 1\}$,.) est un groupe.

Définition 1.1.11 *Soit A un anneau unitaire. L'ensemble $A^* = A - \{0\}$ des inversibles de A, est un corps, qui est commutatif si l'anneau A est commutatif.*
Souvent le corps est noté par $\mathbb{K}$.

Exemple 1.1.5 *$\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Q}$ sont des corps commutatifs*

1.2 Construction de l'anneau des polynômes

Soit A un anneau unitaire

Définition 1.2.1 *On appelle polynôme à une indéterminée à coefficient dans A toute suite $(a_i)_{i\in\mathbb{N}}$ d'éléments de A dont tous les termes sont nuls à partir d'un certain rang.*
Si tous les termes ne sont pas nul, le plus grand indice n, pour lequel $a_n \neq 0$ est appelé ***degré du polynôme*** *noté $d^oP = n$.*
Pour le ***polynôme nul****, noté 0, dont tous les termes sont nuls, on note $d^o0 = -\infty$.*
L'ensemble des polynômes à coefficients dans A est noté $A[X]$ dont X est l'indéterminée.

Exemple 1.2.1 *P un polynôme : $P = (a_i)_{i\in\mathbb{N}} = (a_0, a_1, \cdots, a_n, 0, 0, \cdots)$ et $d^oP = n$.*

Théorème 1.2.1 :Principe d'identification *Deux polynômes sont égaux si, et seulement si, leurs coefficients sont égaux.*

1.2.1 Somme et produit

Définition 1.2.2 *On définit dans $A[X]$ la somme et le produit de deux polynômes. Soient $P=(a_i)_{i\in\mathbb{N}}$ et $Q=(b_i)_{i\in\mathbb{N}}$:*

(a) $P+Q=(a_i+b_i)_{i\in\mathbb{N}}$

(b) $PQ=(c_n)_{n\in\mathbb{N}}$ *avec* $c_n=\sum_{k=0}^{n}a_kb_{n-k}$

Propriété : *La somme et le produit de deux polynômes sont des lois internes car la suite des coefficients $(a_i+b_i)_{i\in\mathbb{N}}$ et $(c_n)_{n\in\mathbb{N}}$ ont tous leurs termes nuls à partir d'un certain rang.*

Preuve : *Soit $m=max(d^oP,d^oQ)$*

– *Si $i>m$ alors, $a_i=b_i=0$ et donc $a_i+b_i=0$.*

– *Si $n>2m$ alors, $c_n=\sum_{k=0}^{n}a_kb_{n-k}=\sum_{k=0}^{m}a_k\underbrace{b_{n-k}}_{=0}+\sum_{k=m+1}^{n}\underbrace{a_k}_{=0}b_{n-k}=0$*

Définition 1.2.3 *Soit A un anneau commutatif unitaire.*

- *Deux polynômes $P,Q\in A[X]$ sont dits associés s'il existe $\lambda\in A$ inversible tel que $P=\lambda Q$.*
- *Un polynôme $P\in A[X]$ est dit* ***unitaire*** *si son coefficient dominant (i.e. le coefficient du monôme de plus haut degré de P) vaut 1).*

Proposition 1.2.1 *Si $A=\mathbb{K}$(corps commutatif), alors $\mathbb{K}[X]$ est un $\mathbb{K}-$espace vectoriel*

Dans la suite $\mathbb{K}$ désigne le corps des réels $\mathbb{R}$ ou le corps des complexes $\mathbb{C}$

1.2.2 Notation

Définition 1.2.4 *Dans $\mathbb{K}[X]$, on note $1=(1,0,0,\cdots)$ et $X=(0,1,0,0,\cdots)$.*
On en déduit alors : $X^2=(0,0,1,0,0,\cdots)$, $X^3=(0,0,0,1,0,0,\cdots)$etc.
Pour tout polynôme : $P=a_0+a_1X+a_2X_2+\cdots+a_nX^n=\sum_{i=1}^{n}a_iX^i$.

Remarque 1.2.1 – *On peut aussi écrire : $P=\sum_{i=1}^{+\infty}a_iX^i$*

– *La lettre X ne désigne plus un élément variant dans $\mathbb{R}$ (une variable), mais sert seulement à repéré les coefficients du polynôme, X correspond au polynôme dont le seul coefficient non nul, égal à 1, est celui du 1^{er} degré . Par exemple, dans le polynôme $P=X^2-3X+2$, le coefficient de degré 2 du polynôme P vaut 1, celui de degré 1 vaut -3, et le coefficient constant vaut 2*

Exemple 1.2.2 – *$P=X^3-2X+1$ est un polynôme unitaire de degré 3*

– *$Q=5X^4+3X+1$ est un polynôme de degré 4 et de coefficient dominant 5.*

1.2.3 L'anneau des polynômes

Théorème 1.2.2 *$\mathbb{K}[X]$ muni de la somme et du produit forme un anneau commutatif.*

Démonstration *$(\mathbb{K}[X],+)$ est un groupe commutatif avec le polynôme nul 0 comme élément neutre et comme opposé $-P$ dont tous les coefficients sont multipliés par -1.*
$(\mathbb{K}[X],\times)$ est commutatif associatif et possède un élément neutre noté 1.
Le produit est distributif par rapport à la somme.

Théorème 1.2.3 *Soient P et Q deux polynômes de $\mathbb{K}[X]$*
- *Degré de la somme : $d^o(P+Q) \leq \max(d^oP, d^oQ)$.*
- *Degré du produit : $d^o(PQ) = d^oP + d^oQ$.*

Démonstration *$P = (a_i)_{i\in\mathbb{N}}$ et $Q = (b_i)_{i\in\mathbb{N}}$ et p et q les degrés respectifs de P et Q.*

Pour le degré de la somme c'est immédiat.

Pour le degré du produit : si P ou Q sont nuls c'est aussi immédiat (d^oP ou d^oQ vaut $-\infty$), sinon

(a) $c_{p+q} = \sum_{k=0}^{p+q} a_k b_{p+q-k} = \sum_{k=0}^{p-1} a_k \underbrace{b_{p+q-k}}_{=0} + a_p b_q + \sum_{k=p+1}^{p+q} \underbrace{a_k}_{=0} b_{p+q-k} = a_p b_q \neq 0$

(b) $n > p+q, \quad c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{p} a_k \underbrace{b_{n-k}}_{=0} + \sum_{k=p+1}^{n} \underbrace{a_k}_{=0} b_{n-k} = 0$

de (a) et (b), on a bien $d^o(PQ) = p+q$

Théorème 1.2.4 *$\mathbb{K}[X]$ est un anneau intègre c'est à dire :*

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

Démonstration *On a*

$$PQ = 0 \Rightarrow d^o(PQ) = -\infty$$

or $d^o(PQ) = d^oP + d^oQ$ donc $d^oP + d^oQ = -\infty$, alors $d^oP = -\infty$ ou $d^oQ = -\infty$ donc $P = 0$ ou $Q = 0$

1.2.4 Dérivée d'un polynôme formelle

Définition 1.2.5 *Soit $P \in \mathbb{K}[X]$ tel que : $P = \sum_{k=0}^{+\infty} a_k X^k$.*
- *On appelle polynôme dérivé le polynôme, noté P', tel que : $P' = \sum_{k=0}^{+\infty} k a_k X^{k-1}$.*
- *On définit ensuite par récurrence les polynômes dérivés successifs avec la relation $P^{(n+1)} = \left(P^{(n)}\right)'$.*
- *Pour $n = 2$, on utilisera la notation P''*

Exemple 1.2.3 *Soit $P = 2X^3 - X^2 - 5X + 1$, on a :*

$$P' = 6X^2 - 2X - 5, \quad P'' = 12X - 2, \quad P^{(3)} = 12, \quad puis, \quad \forall n > 3, P^{(n)} = 0$$

Remarque 1.2.2 *Contrairement aux fonctions polynomiales, la dérivée des polynômes formelles ne fait pas appel à la notion de limite.*

Théorème 1.2.5 *Soit $P, Q \in \mathbb{K}[X]$ et $d^oP = p$.*
- *$\forall n \leq p, \quad d^oP^{(n)} = p - n \quad et \quad \forall n \geq p, \quad P^{(n)} = 0$*
- *$(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$.*
- *$(PQ)' = P'Q + PQ'$.*
- *Formule de Leibniz : $(PQ)^{(n)} = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} P^{(k)} Q^{(n-k)}$.*

1.2.5 Fonction polynomiale

Théorème 1.2.6 *Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.*
On appelle valeur de P en un point $x \in \mathbb{K}$, l'élément de $\mathbb{K}$: $P(x) = \sum_{k=0}^{n} a_k x^k$.
La fonction $x \mapsto P(x)$ de $\mathbb{K}$ dans $\mathbb{K}$ est appelée fonction polynomiale associée à P. Cette fonction est notée $\tilde{P}$ lorsqu'on veut la distinguer de P.

$$\forall P, Q \in \mathbb{K}[X], \quad \tilde{P+Q} = \tilde{P} + \tilde{Q}, \quad (\tilde{P'}) = (\tilde{P})'.$$

Remarque 1.2.3 *La plupart du temps, on n'utilisera pas la notation $\tilde{P}$, lorsqu'on voudra évaluer le polynôme en un point. On écrira par exemple $P(1)$, pour l'évaluation de P en 1.*

1.3 Divisibilité et division euclidienne

1.3.1 Multiple, diviseur

Définition 1.3.1 *Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B (ou B est divisible par A ou B est un multiple de A), s'il existe $P \in \mathbb{K}[X]$ tel que $B = PA$. Cette relation se note $A|B$*

Exemple 1.3.1 *$X - 2$ divise $X^2 + X - 6$ car $X^2 + X - 6 = (X - 2)(X + 3)$*

1.3.2 Division euclidienne

Théorème 1.3.1 *Soient $A, B \in \mathbb{K}[X]$ et $B \neq 0$.*
Il existe un unique couple $(Q, R) \in \mathbb{K}^2[X]$ pour lequel :

$$A = BQ + R \quad avec \quad d^oR < d^oB.$$

On appelle A le dividende, B le diviseur, Q le quotient et R le reste.

Exemple 1.3.2

$$\begin{array}{l|l} 2X^4 - X^3 - 2X^2 + 3X - 1 & X^2 - X + 1 \\ \overline{-2X^4 + 2X^3 - 2X^2} & \overline{2X^2 + X - 3} \\ \overline{0X^4 + X^3 - 4X^2} + 3X & \\ \overline{-X^3 + X^2 - X} & \\ \overline{0X^3 - 3X^2 + 3X} - 1 & \\ \overline{3X^2 - 3X + 3X} & \\ \overline{0X^2 - X + 2} & \end{array}$$

Donc : $2X^4 - X^3 - 2X^2 + 3X - 1 = (X^2 - X + 1)(2X^2 + X - 3) + (-X + 2)$.

Définition 1.3.2 *Soient $A, B \in \mathbb{K}[X]$. Il existe un polynôme unitaire unique $P \in \mathbb{K}[X]$ diviseur de plus haut degré divisant les polynômes A, B noté par $P = pgcd(A, B)$.*

L'algorithme d'Euclide *Pour trouver le $pgcd(A,B)$ de deux polynômes $A,B\in\mathbb{K}[X]$, on effectue à partir de A et B des divisions euclidiennes successives. On écrit*

$$A=BQ_0+R_0 \text{ avec } Q_0,R_0\in\mathbb{K}[X] \text{ et } deg(R_0)<deg(B),$$

et on recommence en divisant toujours le dividende par le reste :

$$B=R_0Q_1+R_1 \text{ avec } Q_1,R_1\in\mathbb{K}[X] \text{ et } deg(R_1)<deg(R_0).$$

Au rang k, on fait

$$R_{k-1}=R_kQ_{k+1}+R_{k+1} \text{ avec } Q_{k+1},R_{k+1}\in\mathbb{K}[X] \text{ et } deg(R_{k+1})<deg(R_k).$$

La suite $(deg(R_k)$ décroit strictement et donc il existe $n\in\mathbb{N}^*$ tel que $R_n=0$ et $R_{n-1}\neq 0$. On remarque alors que $pgcd(A,B)=pgcd(B,R_0)=\cdots=pgcd(R_{n-1},R_n)$, de sorte qu'a une constante prés, $pgcd(A,B)=R_{n-1}$.

Exemple 1.3.3 *Calculons $d=pgcd(X^3-X^2+X-1,X^2-1)$, par la division euclidienne on trouve :*

$$\begin{array}{l|l} X^3-X^2+X-1 & X^2-1 \\ 2X-2 & \overline{X-1} \end{array}$$

Et

$$\begin{array}{l|l} X^2-1 & \overline{2X-2} \\ 0 & \overline{\frac{X}{2}+\frac{1}{2}} \end{array}$$

Donc $d=2X-2$.

Définition 1.3.3 *Soient $A,B\in\mathbb{K}[X]$. On dit que A et B sont premier entre eux ssi $pgcd(A,B)$ est un polynôme constant non nul.*

Proposition 1.3.1 *Soient $A,B\in\mathbb{K}[X]$. On dit que A et B sont premier entre eux si et seulement s'il existe $U,V\in\mathbb{K}[X]$ tel que $UA+VB=1$.*

Exemple 1.3.4 *Soient les polynômes de $\mathbb{R}[X]$ $A(X)=X^4+2X^3+X+1$ et $B(X)=X^3+X-1$. Montrons que A et B sont premier entre eux avec l'algorithme d'Euclide :*
Première étape

$$\begin{array}{l|l} X^4+2X^3+0X^2+X+1 & X^3+X-1 \\ \overline{-X^4+0X^3-X^2+X+0} & \overline{X+2} \\ 0X^4+2X^3-X^2+2X+1 & \\ \overline{-2X^3+0X^2-2X+2} & \\ \overline{0X^3-X^2+0X+3} & \end{array}$$

Donc : $A(X)=B(X)Q_0(X)+R_0(X)$ tel que $Q_0(X)=X+2$ et $R_0(X)=-X^2+3$.
Deuxième étape

$$\begin{array}{l|l} X^3+X-1 & -X^2+3 \\ \overline{-X^3+3X} & \overline{-X} \\ 0X^3+4X-1 & \end{array}$$

Donc : $B(X) = R_0(X)Q_1(X) + R_1(X)$ *tel que* $Q_1(X) = -X \quad et \quad R_1(X) = 4X - 1.$

Troisième étape

$$\begin{array}{l|l} -X^2+3 & 4X-1 \\ \hline -X^2-\frac{1}{4}X & -\frac{1}{4}X-\frac{1}{16} \\ \hline 0X^2-\frac{1}{4}X+3 & \\ \frac{1}{4}X-\frac{1}{16} & \\ \hline 0X+\frac{47}{16} & \end{array}$$

Donc : $R_0(X) = R_1(X)Q_2(X) + R_2(X)$ *tel que* $Q_2(X) = -\frac{1}{4}X - \frac{1}{16}$ *et* $R_2(X) = \frac{47}{16}.$

Quatrième étape

On a $4X - 1 = \frac{47}{16}(\frac{16}{47}(4X - 1)) + 0$. *Donc* $R_3 = 0$ *et alors* $pgcd(A, B) = \frac{47}{16}.$

Donc A et B sont premier entre eux.

Cherchons Maintenant 2 polynômes U, V *de* $\mathbb{R}[X]$ *tel que* $UA + VB = 1$ *:*

On a

$$R_2(X) = R_0 - R_1Q_2(X).$$
$$R_1(X) = B(X) - R_0(X)Q_1(X).$$
$$R_0(X) = A(X) - B(X)Q_0(X).$$

Donc

$R_2(X) = R_0(X) - (B(X) - R_0(X)Q_1(X))Q_2(X)$

$= R_0(X)[1 + Q_1(X)Q_2(X)] - B(X)Q_2(X)$

$= [A(X) - B(X)Q_0(X)][1 + Q_1(X)Q_2(X)] - B(X)Q_2(X)$

$= A(X)[1 + Q_1(X)Q_2(X)] + B(X)[-Q_0(X) - Q_0(X)Q_1(X)Q_2(X) - Q_2(X)]$

$= [1 - X(-\frac{1}{4}X - \frac{1}{16})]A(X) + [-(X + 2) - (-X)(-\frac{1}{4}X - \frac{1}{16}) - (-\frac{1}{4}X - \frac{1}{16})]$

$= [\frac{1}{4}X^2 + \frac{1}{16}X + 1]A(X) + [-\frac{1}{4}X^3 - \frac{9}{16}X^2 - \frac{7}{8}X - \frac{31}{16}]B(X)$

On a donc

$$\frac{47}{16} = [\frac{1}{4}X^2 + \frac{1}{16}X + 1]A(X) + [-\frac{1}{4}X^3 - \frac{9}{16}X^2 - \frac{7}{8}X - \frac{31}{16}]B(X)$$

ce qui peut s'écrire :

$$1 = \frac{16}{47}[\frac{1}{4}X^2 + \frac{1}{16}X + 1]A(X) + \frac{16}{47}[-\frac{1}{4}X^3 - \frac{9}{16}X^2 - \frac{7}{8}X - \frac{31}{16}]B(X)$$

On a donc bien trouvé deux polynômes U *et* V *tel que* $UA + VB = 1$, *à savoir* $U(X) = \frac{4}{47}X^2 + \frac{1}{47}X + \frac{16}{47}$ *et* $V(X) = -\frac{4}{47}X^3 - \frac{9}{47}X^2 - \frac{14}{47}X - \frac{31}{47}.$

1.4 Racines d'un polynôme

Définition 1.4.1 *Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.*
On dit que λ est une racine de P sur $\mathbb{K}$ si, et seulement si, $P(\lambda) = 0$

Théorème 1.4.1 *Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.*
λ est une racine de P sur $\mathbb{K}$ si, et seulement si, P est divisible par $(X - \lambda)$

1.4.1 Multiplicité des racines

Définition 1.4.2 *Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.*
L'ensemble des entiers naturels k tel que $(X-\lambda)^k$ divise P possède un plus grand élément m appelé multiplicité de la racine λ dans P ou λ racine d'ordre m.

Proposition 1.4.1 *Si $P \in \mathbb{K}[X]$ et $a_1, \ldots, a_r \in \mathbb{K}$ des racines de P d'ordre $h_1, \ldots, h_r$ (les a_i étant deux à deux distincts). Alors il existe $Q \in \mathbb{K}[X]$ tel que*

$$P(X) = (X - a_1)^{h_1} \ldots (X - a_r)^{h_r} Q(X) \text{ et } \forall i, Q(a_i) \neq 0.$$

Remarque 1.4.1 *Si $P \in \mathbb{K}[X]$ est de degré $n \geq 1$, alors P a au plus n racines (comptées avec leur ordre de multiplicité).*

Définition 1.4.3 *Un polynôme $P \in \mathbb{K}[X]$ est dit **scindé** sur $\mathbb{K}$ si on peut écrire*

$$P(X) = \lambda(X - a_1)^{h_1} \ldots (X - a_r)^{h_r}.$$

avec $\lambda \in \mathbb{K}$ et pour tous i, $a_i \in \mathbb{K}$ et $h_i \in \mathbb{N}^*$.

Définition 1.4.4 *Un polynôme $P \in \mathbb{K}[X]$ est dit **irréductible** dans $\mathbb{K}[X]$ si P n'est pas constant (i.e. $deg(P) \geq 1$) et si seuls diviseurs dans $\mathbb{K}[X]$ sont les constantes non nulles et les polynômes associés à P. Si non il est dit réductible.*

Exemple 1.4.1 *Soit $P = X^2 + 1$ un polynôme unitaire de degré 2. Dans $\mathbb{R}[X]$, P est irréductible (ne possède aucune racine). Dans $\mathbb{C}[X]$, P s'écrit sous la forme $P = (X - i)(X + i)$ c à d P est réductible.*