Algèbre et analyse élémentaires II
Algèbre.
Polynômes.

Nous allons dans ce chapitre introduire la notion de polynômes puis comprendre la différence entre polynôme et fonction polynomiale.

1 Définitions. Généralités.

Définition 1.1. *On appelle $\mathbb{R}[X]$ l'ensemble des suites finies de réels. On a donc*

$$\mathbb{R}[X] = \{P \ ; \exists n \in \mathbb{N} \ ; P = (a_0, a_1, \ldots, a_n, 0, \ldots)\} \ .$$

Exemple 1.2. *La suite constante et égale à 0 est donc un polynôme (le polynôme nul).*

Remarque 1.3. *Soit a un nombre réel. Alors la suite $(a, 0, \ldots)$ est un polynôme. On dira qu'il s'agit d'un polynôme constant. Plus généralement, soit n un entier. Soient $(a_0, a_1, \ldots, a_n)$ la donnée de $n+1$ nombres réels. Alors la suite $(a_0, a_1, \ldots, a_n, \ldots)$ est un polynôme. En ce sens, on voit que tous les espaces $\mathbb{R}^{n+1}$ sont contenus dans $\mathbb{R}[X]$.*

Définition 1.4. *Soit P un polynôme non nul. Alors on appelle degré de P le plus grand indice pour lequel le coefficient a_n est non nul. Autrement dit*

$$P = (a_0, \ldots, a_n, 0, \ldots) \text{ avec } a_n \neq 0 \ .$$

On le note $\deg(P)$.

Vérification. Comme P est non nul, il admet au moins un coefficient non nul (un des termes de la suite n'est pas nul) mais, pour n assez grand, tous les termes doivent être nuls. Il y a donc un tel indice.

Remarque 1.5. *Le polynôme nul n'a donc pas de degré. Il peut être commode parfois d'adopter la convention*

$$\deg(0) = -\infty \ .$$

Pour l'instant, nous avons construit un ensemble. Ce n'est pas très intéressant. Il importe d'y définir très vite des opérations permettant de manipuler les polynômes.

Définition 1.6. *Soient $P = (a_0, \ldots, a_n, 0, \ldots)$ et $Q = (b_0, \ldots, b_m, 0, \ldots)$ deux polynômes. On pose*

$$P + Q = (a_0 + b_0, \ldots, a_i + b_i, \ldots)$$

pour tout entier i .

Vérification. En effet, si $i > n$ et $i > m$, $a_i + b_I = 0 + 0 = 0$. Il s'agit donc bien d'une suite finie. On remarquera que l'on a simplement copié la définition de l'addition dans $\mathbb{R}^n$.

Proposition 1.7. *L'addition des polynômes fait de $\mathbb{R}[X]$ un groupe abélien c'est à dire que*
— *Le polynôme nul est un élément neutre pour cette opération :*

$$\forall P \in \mathbb{R}[X] \ 0 + P = P + 0 = P \ ;$$

Tout polynôme P admet un opposé ; en effet

$$\forall P \in \mathbb{R}[X] \ ; (a_0, \ldots, a_n, 0, \ldots) + (-a_0, \ldots, -a_n, 0, \ldots) = (-a_0, \ldots, -a_n, 0, \ldots) + (a_0, \ldots, a_n, 0, \ldots) = 0 \ ;$$

on a noté $P = (a_0, \ldots, a_n, 0, \ldots)$;

L'addition est associative ; id est

$$\forall (P,Q,R) \in \mathbb{R}[X]^3 \ (P+Q)+R = P+(Q+R) \ ;$$

L'addition est commutative ; id est

$$\forall (P,Q) \in \mathbb{R}[X]^2 \ P+Q = Q+P \ .$$

Démonstration. Toutes ces propriétés sont immédiates puisqu'elles résultent de ce que notre opération est définie coefficient par coefficient et qu'elles sont vérifiées dans $\mathbb{R}$.

Proposition 1.8. *On a*

$$\deg(P+Q) \leq \sup(\deg(P), \deg(Q)) \ .$$

Vérification. En effet, si $i > \sup(\deg(P), \deg(Q))$, le coefficient d'indice i de $P+Q$ est somme de deux coefficients nuls comme on l'a vu dans la définition du degré.

Remarque 1.9. *On peut être plus précis. Soit P un polynôme de degré n et Q un polynôme de degré m . On note a_n (resp. b_m) le coefficient de plus haut degré de P (resp. Q). Alors*

$$\begin{array}{rcl} \deg(P) \neq \deg(Q) & \Rightarrow & \deg(P+Q) = \sup(\deg(P), \deg(Q)) \\ \deg(P) = \deg(Q) = n = m \text{ et } a_n + b_n \neq 0 & \Rightarrow & \deg(P+Q) = \sup(\deg(P), \deg(Q)) \\ \deg(P) = \deg(Q) \text{ et } a_n + b_m = 0 & \Rightarrow & \deg(P+Q) < \sup(\deg(P), \deg(Q)) \end{array} \ .$$

On remarquera que $\deg(P-P) = \deg(0) = -\infty$.

Vérification. Il s'agit juste de constater que le coefficient de plus haut degré de $P+Q$ est celui de P ou de Q dans le premier cas, vaut $a_n + b_n$ dans le second cas. Le seul cas où le degré de la somme est plus petit que $\sup(\deg(P), \deg(Q))$ est donc le dernier cas. La situation la plus extrême étant celle d'un polynôme auquel on ajoute son opposé puisqu'alors tous les coefficients de la somme sont nuls.

Définition 1.10. *Soit P un polynôme et λ un nombre réel (un scalaire). Alors, si $P = (a_0, \ldots, a_n, 0, \ldots)$, on note λP le polynôme*

$$\lambda P = (\lambda a_0, \ldots, \lambda a_n, 0, \ldots) \ .$$

Proposition 1.11. *L'ensemble $\mathbb{R}[X]$ est un espace vectoriel pour l'addition des polynômes et la multiplication par un scalaire. En effet*

- $1 \times P = P$ *;*
- *la multiplication par un scalaire est associative id est*

$$\forall (\lambda, \mu) \in \mathbb{R}^2 \ \forall P \in \mathbb{R}[X] \ (\lambda\mu)P = \lambda(\mu P) \ ;$$

- *la multiplication par un scalaire est distributive id est*

$$\forall (\lambda, \mu) \in \mathbb{R}^2 \ \forall P \in \mathbb{R}[X] \ (\lambda+\mu)P = \lambda P + \mu P \ ;$$

$$\forall \lambda \in \mathbb{R} \ \forall (P,Q) \in \mathbb{R}[X]^2 \ \lambda(P+Q) = \lambda P + \lambda Q \ .$$

Vérification. Toutes ces propriétés ne font que généraliser les propriétés correspondantes dans $\mathbb{R}^n$.

Remarque 1.12. *On notera que*

$$\forall P \in \mathbb{R}[X] \ (-1) \times P = -P \ .$$

Cela justifie l'écriture de l'opposé de P .

Corollaire 1.13. *On a la propriété essentielle suivante :*

$$\lambda \in \mathbb{R} : P \in \mathbb{R}[X]\ \lambda P = 0 \Rightarrow \lambda = 0 \text{ ou } P = 0\ .$$

Vérification. En effet le polynôme $(\lambda a_0, \dots, \lambda a_n, 0, \dots)$ ne peut être nul que si $\lambda = 0$ ou, si $\lambda \neq 0$, tous les coefficients de P le sont.

Corollaire 1.14. *Si λ est un scalaire non nul et P un polynôme non nul alors le degré de λP est celui de P .*

Mais l'opération la plus intéressante est la multiplication des polynômes entre eux.

Définition 1.15. *Soient (P, Q) un couple de polynômes. On notera $P = (a_0, \dots, a_n, 0, \dots)$ et $Q = (b_0, \dots, b_m, 0, \dots)$. On appelle PQ le polynôme dont le coefficient c_k est donné par*

$$\forall k \in \mathbb{N}\ c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{n} a_i b_{k-i} = \sum_{j=0}^{m} a_{k-j} b_j\ .$$

Vérification. Ces trois sommes coïncident puisque $i > n \Rightarrow a_i = 0$ et $j > m \Rightarrow b_j = 0$. On a donc

$$\forall k \in \mathbb{N}\ c_k = \sum_{i+j=k\ (0\leq i\leq n\ ,\ 0\leq j\leq m)} a_i b_j\ .$$

Exemple 1.16. *Soit P un polynôme constant. Il s'écrit donc $P = (a_0, 0, \dots)$. Soit Q un polynôme quelconque. On l'écrit $Q = (b_0, \dots, b_m, 0, \dots)$. Etudions PQ . Ses coefficients sont donc*

$$\forall k \in \mathbb{N}\ c_k = \sum_{i+j=k\ (0\leq i\leq 0\ ,\ 0\leq j\leq m)} a_i b_j = a_0 b_k\ .$$

Bref $PQ = a_0 Q$.

Exemple 1.17. *Soit P un polynôme de la forme $P = (0, a_1, 0, \dots)$. Soit Q un polynôme quelconque. On l'écrit $Q = (b_0, \dots, b_m, 0, \dots)$. Etudions PQ . Ses coefficients sont donc*

$$\forall k \in \mathbb{N}^*\ c_k = \sum_{i+j=k\ (0\leq i\leq 1\ ,\ 0\leq j\leq m)} a_i b_j = a_1 b_{k-1} \text{ et } c_0 = a_0 b_0 = 0\ .$$

Autrement il suffit de décaler tous les coefficients de Q d'un rang en les multipliant par a_1 .

Etudions alors un cas particulier. Ainsi, si l'on pose $X = (0, 1, 0, \dots)$, on aura

$$X \times X = (0, 0, 1, 0, \dots) \text{ et } X \times \dots\ (k - \text{fois } X = (0, \dots, 1, 0, \dots)$$

où le coefficient 1 intervient à la k-ième place. On a donc

$$X^k = (0, \dots, 1, 0, \dots)(1\ figurant\ en\ place\ k)\ .$$

Plus généralement $X^i X^j = X^{i+j}$ quelque soient les degrés i et j .

Remarque 1.18. *Nous avons ainsi montré que*

$$P = (a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1 X + \dots a_n X^n\ .$$

Si l'on ajoute la convention $X^0 = 1$, on voit que l'on a montré que tout polynôme P (de degré au plus n) s'écrit

$$P = \sum_{i=0}^{n} a_i X^i\ .$$

C'est cette notation que nous utiliserons désormais puisqu'elle est compatible aux trois opérations introduites sur $\mathbb{R}[X]$. En effet

$$\lambda P = \lambda(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \lambda a_i X^i \ ;$$

$$P + Q = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{\sup(n,m} (a_i + b^\circ i) X^i \ ;$$

$$PQ = \left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{i=0}^{m} b_i X^i\right) = \left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right) X^k\right) = \left(\sum_{k=0}^{n+m} c_k X^k\right) \ .$$

Définition 1.19. *Soit k un entier. Les polynômes X^k sont appelés monômes de degré k .*

Proposition 1.20. *L'ensemble des monômes de degré est appelé la base canonique (des monômes).*

Vérification. En effet tout polynôme est une combinaison linéaire (finie) de monômes. Et toute combinaison linéaire finie de monômes est un polynôme nul si et seulement tous ses coefficients sont nuls. Tout système fini de monômes est donc libre.

Remarque 1.21. *On notera que $\mathbb{R}[X]$ est un espace vectoriel engendré par un nombre infini de vecteurs.*

Remarque 1.22. *On note que la multiplication des polynômes est bilinéaire au sens où*

$$(\lambda P_1 + \mu P_2) \times Q = \lambda P_1 \times Q + \mu P_2 \times Q$$

et

$$P \times (\lambda Q_1 + \mu Q_2) = P\lambda Q_1 + P\mu Q_2 \ .$$

On dit que $\mathbb{R}[X]$ est une algèbre sur $\mathbb{R}$ (pour les trois opérations ainsi introduites).

Proposition 1.23. *Soit P un polynôme de degré n et Q un polynôme de degré m . Alors le polynôme PQ est exactement de degré $n + m$.*

Vérification. Comme $a_n \neq 0$ et $b_m \neq 0$, il suffit de remarquer que le coefficient non nul de plus haut degré est $a_n b_m$ (degré $n + m$).

Corollaire 1.24. *On a donc*

$$PQ = 0 \Rightarrow P = 0 \text{ ou } Q = 0 \ .$$

Définition 1.25. *Soit $P = \sum_{i=0}^{n} a_i X^i$ un polynôme de $\mathbb{R}[X]$. On appelle polynôme dérivé de P le polynôme $P' = \sum_{i=0}^{n-1}(i+1)a_{i+1}X^i$.*

Proposition 1.26. *L'application $P \mapsto P'$ est une application linéaire surjective de $\mathbb{R}[X]$ dans $\mathbb{R}[X]$ dont le noyau est formé par le sous-espace vectoriel formé des polynômes constants.*

Vérification. On a immédiatement que

$$\forall(\lambda, \mu) \in \mathbb{R}^2 \ \forall(P, Q) \in \mathbb{R}[X]^2 \ \ (\lambda P + \mu Q)' = \lambda P' + \mu Q' \ .$$

Donc notre application est bien linéaire. Son noyau est formé des polynômes tels que $P' = 0$ donc pour lesquels les coefficients a_{i+1} sont nuls dès que $i \geq 0$. Ce sont donc les polynômes $P = a_0$.

Soit maintenant $Q = (b_0, \ldots, b_m, 0, \ldots) = \sum_{j=0}^{m} b_j X^j$ un polynôme de $\mathbb{R}[X]$. Il est le dérivé du polynôme

$$P = \sum_{i=1}^{m+1} \frac{b_i}{i} X^i \ .$$

Proposition 1.27. *Soient P et Q deux polynômes éléments de $\mathbb{R}[X]$. Alors $(PQ)' = P'Q + PQ'$.*

Démonstration. Supposons tout d'abord que le polynôme P soit égal au monôme X^p . Alors, si $Q = q_0 + \ldots + b_q X^q$, nous avons à étudier

$$(X^p Q)' = (\sum_{i=0}^{q} b_i X^{p+i})' = \sum_{i=0}^{q} (p+i) b_i X^{p+i-1} = \sum_{i=0}^{q} p b_i X^{p+i-1} + \sum_{i=0}^{q} i b_i X^{p+i-1}$$

soit

$$(X^p Q)' = pX^{p-1}Q + X^p Q' \ .$$

Ainsi la formule est vérifiée pour les monômes. Par linéarité, la formule sera vérifiée pour tout polynôme :

$$(PQ)' = \left((\sum_{i=0}^{p} a_i X^i) Q \right)' = \left(\sum_{i=0}^{p} a_i X^i Q \right)' = \sum_{i=0}^{p} a_i (X^i Q)'$$

soit

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

Théorème 1. *Soit $\{Q_i\}$ une famille de polynômes de $\mathbb{R}[X]$ telle que $\forall i \in \mathbb{N}$ $\deg(Q_i) = i$. Alors cette famille est une base de $\mathbb{R}[X]$ (tout polynôme s'écrit comme une combinaison linéaire finie de polynômes de cette famille et la seule combinaison linéaire finie nulle est la combinaison linéaire nulle).*

Démonstration. Soit $\sum_{i=1}^{n} \lambda_i Q_{j_i}$ une combinaison linéaire nulle. La famille des indices j_i admet un plus grand élément. On le note j_{i_0} . C'est aussi, par construction de la famille $\{Q_i\}$, le degré du polynôme $Q_{j_{i_0}}$. Si $\lambda_{j_{i_0}}$ est non nul, alors le polynôme $\sum_{i=1}^{n} \lambda_i Q_{j_i}$ a ce degré. il ne peut être nul. Aussi $\lambda_{j_{i_0}} = 0$. On montre ainsi que tous les coefficients λ_i sont nuls. La famille est donc libre.

Il reste à vérifier par récurrence descendante que tout polynôme s'écrit comme une combinaison linéaire finie des polynômes Q_i . Tout polynôme constant est multiple de Q_0 . Si P est un polynôme de degré n , alors

$$P = aQ_n + R$$

où on a noté (a, R) le quotient (de degré 0) et le reste de la division euclidienne de P par Q_n . Ainsi R est de degré au plus $n-1$. Il est combinaison linéaire des Q_i pour $i \leq n-1$.

Corollaire 1.28. *Soit a un réel. Tout polynôme P de degré n s'écrit de façon unique*

$$P = \sum_{i=0}^{n} c_i (X-a)^i \ .$$

Vérification. En effet la famille $\{(X-a)^i\}$ vérifie les hypothèses du théorème.

Remarque. *Nous donnerons plus loin une expression pour les coefficients c_i .*

2 La division euclidienne des polynômes.

Définition 2.1. *on dit que le polynôme Q divise le polynôme P si et seulement s'il existe un polynôme Q' tel que $P = QQ'$.*

Exemple 2.2. *Soit Q un polynôme constant non nul. Donc $Q = q_0 X^0 = q_0$ avec $q_0 \neq 0$. Alors il divise tout polynôme P . En effet si $P = a_0 + a_1 X + \ldots + a_n X^n$, on a*

$$P = q_0 \times \left(\frac{a_0}{q_0} + \frac{a_1}{q_0} X + \ldots + \frac{a_n}{q_0} X^n \right) \ .$$

Exemple 2.3. *Le monôme X divise tout polynôme sans terme constant. Il ne divise pas le polynôme $1+X$.*

Remarque 2.4. *On retrouve donc une situation analogue à ce qui se passe dans $\mathbb{Z}$. Tout nombre n'est pas divisible par tout autre (2 ne divise que les nombres pairs).*

On va introduire un outil analogue : la division euclidienne.

Proposition 2.5. *Soit A un polynôme de degré n et B un polynôme de degré m . On suppose que $n \geq m$. Alors il existe un unique polynôme R nul ou de degré strictement inférieur à m et un unique polynôme Q tels que*

$$A = BQ + R \ .$$

On appelle polynôme quotient de la division euclidienne de A par B le polynôme Q et reste de la division euclidienne de A par B le polynôme R .

Démonstration. Montrons tout d'abord l'unicité. Par l'absurde, si deux tels couples existaient on aurait

$$A = BQ_1 + R_1 \text{ et } A = BQ_2 + R_2 \text{ soit } B(Q_2 - Q_1) = R_1 - R_2 \ .$$

Comparons alors les degrés des deux polynômes. Le polynôme de gauche est nul ou de degré supérieur ou égal à celui de B . Le polynôme de droite est nul ou de degré inférieur ou égal au sup des degrés de R_1 et R_2 donc il est nul ou de degré strictement inférieur à m . La seule possibilité est donc que $B(Q_2 - Q_1) = R_1 - R_2 = 0$ soit $R_1 = R_2$ et $Q_1 = Q_2$.

Passons à l'existence. On va raisonner par récurrence (descendante) sur le degré n de A . On a donc

$$A = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \text{ et } B = b_m X^m + b_{m-1}X^{m-1} + \ldots + b_0 \ .$$

On constate alors que le polynôme

$$A_1 = A - \frac{a_n}{b_m} X^{n-m} B$$

est de degré au plus $n-1$. En effet le polynôme A est de degré n et le polynôme $\frac{a_n}{b_m}X^{n-m}B$ a pour degré $n-m+m$ d'après la formule sur le degré du produit. De plus le coefficient de degré n est

$$a_n - \frac{a_n}{b_m} b_m = a_n - a_n = 0 \ .$$

Ce polynôme ne comporte donc que des coefficients susceptibles d'être non nuls en degré au plus $n-1$. Soit le degré de A_1 est strictement inférieur à m et l'on a

$$A = \left(\frac{a_n}{b_m} X^{n-m} \right) B + A_1$$

avec $\deg A_1) < \deg(B)$. Soit le degré de A_1 est supérieur à m et l'on peut recommencer l'opération avec le couple (A_1, B) . Or le degré du premier polynôme décroît strictement donc il sera strictement inférieur à celui de B .

Exemple 2.6. *Soit $A = X^3 - X^2 + X - 1$ et $B = X + 1$. Alors on a successivement*

$$A_1 = A - X^{3-1}(X+1) = X^3 - X^2 + X - 1 - X^3 - X^2 = -2X^2 + X - 1$$

$$A_2 = A_1 - (-2X)(X+1) = -2X^2 + X - 1 + 2X^2 + 2X = 3X - 1$$

et enfin

$$A_3 = A_2 - 3(X+1) = 3X - 1 - 3X - 3 = -4 \ .$$

On a donc

$$A = \left(X^2 - 2X + 3\right) B - 4 \ .$$

On peut aussi "poser la division" comme on le fait à l'école primaire :

$$\begin{array}{rrrrcrcr}
X^3 & -X^2 & +X & -1 & | & X & + & 1 \\
\hline
X^3 & +X^2 & & & | & X^2 & & \\
\hline
 & -2X^2 & X & -1 & | & & & \\
 & -2X^2 & -2X & & | & & -2X & \\
\hline
 & & 3X & -1 & | & & & \\
 & & 3X & +3 & | & & & 3 \\
\hline
 & & & -4 & | & & &
\end{array}$$

et le reste (-4 vu comme polynôme constant) et le quotient $X^2 - 2X + 3$ apparaissent naturellement.

Remarque 2.7. *On notera que la détermination du polynôme quotient et du reste d'une division euclidienne est un algorithme. Ainsi les systèmes de calcul formel comportent cette opération.*

Remarque 2.8. *Soit A un polynôme de degré n et B un polynôme de degré m (avec $m \leq n$). Alors le polynôme B divise le polynôme A si et seulement si le reste dans la division euclidienne de A par B est le polynôme nul.*

Vérification. Bien sûr si $A = BQ + 0 = BQ$ alors B divise A . Inversement, si $A = BB'$, alors le couple $(Q, R) = (B', 0)$ est une (donc la) solution de la division euclidienne de A par B .

Définition 2.9. *On dit qu'un polynôme (non nul de degré au moins 1) est irréductible dans $\mathbb{R}[X]$ s'il n'admet pour seuls diviseurs que les polynômes constants et les multiples de lui-même.*

Exemple 2.10. *Les polynômes de degré 1 sont irréductibles.*

En effet écrivons $P = X + a = QQ'$ (où a est un nombre réel). Alors $1 = \deg(P) = \deg(Q) + \deg(Q')$. Ceci impose que $\deg(Q) = 0$ et $\deg(Q') = 1$ ou $\deg(Q) = 1$ et $\deg(Q') = 0$. Si Q (ou Q') sont de degré 1 , on remarque que

$$P = X + a = 1 \times (X + b) + (a - b) \ .$$

Ainsi $X + b$ ne divise $X + a$ que si $b = a$.

Proposition 2.11. *Tout polynôme (non nul) admet une décomposition en facteurs irréductibles.*

Vérification. Cela se vérifie simplement par récurrence descendante. On vient de voir que les polynômes de degré 1 sont irréductibles. Soit P un polynôme de degré n ($n > 1$). Alors soit il est irréductible soit il s'écrit $P = QQ'$ où $0 < \deg(Q) < n$ et $0 < \deg(Q') < n$. Alors Q et Q' ont une décomposition en facteurs irréductibles.

Théorème 2. *Tout polynôme (non nul) admet une unique décomposition en facteurs irréductibles.*

Ce résultat sera admis.

Proposition 2.12 (Division puissance croissante)**.** *Soient A et B deux polynômes de $\mathbb{R}[X]$. On suppose que $B \neq 0$ et que son coefficient constant b_0 est non nul. Alors, pour tout entier $h \geq 0$, il existe un unique couple de polynômes Q, R tels que*

$$A = BQ + X^{h+1} R$$

avec $Q = 0$ ou Q de degré au plus h .

Démonstration. Etudions l'unicité. Si $A = BQ_1 + X^{h+1}R_1 = ABQ_2 + X^{h+1}R_2$, alors on a l'identité

$$B(Q_1 - Q_2) = X^{h+1}(R_2 - R_1) \ .$$

En particulier, d'après l'écriture du second membre, on voit que tous les coefficients de ce polynôme de degré au plus h sont nuls. On sait que B a un coefficient constant non nul. Montrons (par récurrence) que tous les coefficients de $Q_1 - Q_2$ de degré au plus h sont nuls. Le coefficient constant de $B(Q_1 - Q_2)$ est le produit de b_0 par celui de $Q_1 - Q_2$. Il est donc nul. Appelons alors i l'indice du premier coefficient de $Q_1 - Q_2$ non nul. Alors le coefficient de degré i de $B(Q_1 - Q_2)$ est le produit de b_0 par premier coefficient non nul de $Q_1 - Q_2$. Si $i \leq h$, c'est impossible vu la forme du second membre. Mais $Q_1 - Q_2$ est de degré au plus h donc il est nul. Donc $R_1 - R_2$ est aussi nul.

Reste à étudier l'existence. Mais on voit facilement que, si $A = a_0 + \ldots + a_pX^p$, le polynôme $A' = A - \frac{a_0}{b_0}B$ n'a plus de coefficient constant. Par récurrence, si l'on suppose que, pour tout $k \leq h$, on a

$$A = BQ + X^{h+1}R$$

avec $Q = 0$ ou Q de degré au plus h, on voit que l'on peut écrire $R = \rho B + XR'$ (ou ρ est un scalaire réel) soit

$$A = BQ + \rho BX^{h+1} + X^{h+2}R' = B\left(Q + \rho X^{h+1}\right) + X^{h+2}R' \ .$$

Et le polynôme $Q + \rho X^{h+1}$ est bien de degré au plus $h + 1$.

Exemple 2.13. *Posons $A = 1 + X$ et $B = 1 + X^2$. Alors on a successivement :*

$$A = 1 + X = 1 \times (1 + X^2) + X - X^2 = B + X(1 - X) \text{ puis } A = B + X\left(1 \times B - X - X^2\right)$$

soit

$$A = (1 + X)B - X^2(1 + X) = (1 + X - X^2)B - X^3(1 - X) \ .$$

Et l'on voit que l'on peut continuer.

3 Fonctions polynômes.

Remarque 3.1. *Soit P un polynôme élément de $\mathbb{R}[X]$. Il s'écrit donc $P = a_0 + \ldots + a_pX^p$. Soit Q un autre polynôme élément de $\mathbb{R}[X]$. On l'écrit $Q = b_0 + \ldots + b_qX^q$. Considérons l'expression*

$$P\left(Q(X)\right) = \sum_{i=0}^{p} a_i \left(Q(X)\right)^i = \sum_{i=0}^{p} a_i \left(b_0 + \ldots + b_qX^q\right)^i \ .$$

Il s'agit d'un polynôme en X . Par ailleurs, si P et Q ne sont pas nuls, on voit que le terme de plus haut degré est $a_pb_q^pX^{pq}$ et, donc, que ce polynôme est de degré pq . On dira que l'on a substitué à l'indéterminée X l'expression $Y = Q(X)$.

Exemple 3.2. *On pourra ainsi utiliser*

$$P(X^2) = \sum_{i=0}^{p} a_iX^{2i} \text{ ou } P(X - a) = \sum_{i=0}^{p} a_i(X - a)^i \ .$$

Définition 3.3. *Soit $P = (a_0, \ldots, a_n, 0, \ldots) = \sum_{i=0}^{n} a_iX^i$ un polynôme de $\mathbb{R}[X]$. On lui associe la fonction polynôme $x \in \mathbb{R} \mapsto \sum_{i=0}^{n} a_ix^i \in \mathbb{R}$. On notera $P(x)$ ce dernier scalaire. On dira que l'on a substitué la variable x à l'indéterminée X .*

Proposition 3.4. *Soient P et Q deux polynômes réels. Soit λ un nombre réel. On a*

— $\forall x \in \mathbb{R}\ (P + Q)(x) = P(x) + Q(x)$;

— $\forall x \in \mathbb{R}\ (PQ)(x) = P(x)Q(x)$;
— $\forall x \in \mathbb{R}\ (\lambda P)(x) = \lambda P(x)$.
On résume en général ces propriétés en indiquant que l'application qui associe à P la fonction polynôme $x \mapsto P(x)$ est un morphisme d'algèbre.

Vérification. Vérifions l'une de ces propriétés. Les autres vérifications sont entièrement analogues. Notons n le degré de P et m le degré de Q . On a

$$(PQ)(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k = \left(\sum_{i=0}^{n} a_i x^i \right) \left(\sum_{j=0}^{m} b_j x^j \right) = P(x)Q(x) \ .$$

Proposition 3.5. *Soit P un polynôme réel. Alors*

$$\forall x \in \mathbb{R}\ P'(x) = (x \mapsto P(x))' \ .$$

Proposition 3.6. *Soit P un polynôme réel. Soit a un nombre réel. Alors le reste dans la division euclidienne de P par $X - a$ est égale à $P(a)$.*

Vérification. On a donc $P = Q(X - a) + c$ où (Q, c) représentent quotient et reste de cette division euclidienne. Substituons à X le nombre réel a (prenons les valeurs en a de ces deux polynômes) :

$$P(a) = Q(a)(X - a)(a) + c = 0 \times Q(a) + c = 0 \ .$$

On a bien

$$P = Q(X - a) + P(a) \ .$$

Théorème 3 (Formule de Taylor)**.** *Soit P un polynôme réel dont on notera n le degré. Alors*

$$P = \sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!}(X - a)^i \ .$$

Démonstration. On sait que

$$P = \sum_{i=0}^{n} c_i (X - a)^i = c_0 + (X - a) \left(\sum_{i=1}^{n} c_i (X - a)^{i-1} \right) \ .$$

D'après le résultat précédent, on voit que $c_0 = P(a)$. Par ailleurs on a

$$P' = \sum_{i=1}^{n} i c_i (X - a)^{i-1} = c_1 + (X - a) \left(\sum_{i=2}^{n} i c_i (X - a)^{i-2} \right)$$

soit $P'(a) = c_1$. Plus généralement on aura, pour tout entier $h \geq 1$,

$$P^{(h)} = \sum_{i=h}^{n} \frac{i!}{(i-h)!} c_i (X - a)^{i-h} = h! c_h + (X - a) \left(\sum_{i=h+1}^{n} \frac{i!}{(i-h)!} c_i (X - a)^{i-h-1} \right) \ .$$

Soit

$$\forall h\ 0 \leq h\ P^{(h)}(a) = h! c_h \ .$$

Corollaire 3.7. *Soit $x \mapsto P(x)$ une fonction polynomiale. On note n le degré de P . Alors*

$$P(x) = \sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!}(x - a)^i \ .$$

Remarque. *Cela revient à dire que la formule de Taylor est exacte (son reste est nul) lorsque la fonction est polynomiale pourvu qu'on l'écrive à un ordre plus grand ou égal à celui du degré de P .*

Nous avons vu précédemment que tout polynôme de degré 1 était irréductible. Qu'en est-il des polynômes de degré supérieur ?

Définition 3.8. *On dira que le réel a est une racine du polynôme P si et seulement si $P(a) = 0$ (ou si $X - a$ divise P) .*

Théorème 4 (D'Alembert)**.** *Tout polynôme à coefficient complexe de degré au moins* 1 *admet une racine complexe.*

Ce théorème dit aussi théorème fondamental de l'algèbre est admis ici. il est à noter que toutes les démonstrations connues utilisent des résultats d'analyse.

Corollaire 3.9. *La décomposition en facteurs irréductibles d'un polynôme complexe de degré au moins* 1 *est formée de polynômes de degré* 1 *.*

Vérification. Une simple récurrence.

Corollaire 3.10. *La décomposition en facteurs irréductibles d'un polynôme réel de degré au moins* 1 *est formée de polynômes de degré* 1 *ou de degré* 2 *sans racines réelles mais admettant deux racines complexes conjuguées.*

Vérification. Soit P un tel polynôme réel. Vu comme un polynôme complexe, il admet donc au moins une racine complexe c c'est à dire que $P(c) = 0$. Soit c est un nombre réel et P est divisible par $X - c$. Alors on est ramené à l'étude du quotient de P par $X - c$ (qui est de degré strictement inféieur à celui de P). Soit il est complexe. Alors on a aussi $P(\bar{c}) = 0$ puisque $P(\bar{c}) = \overline{P(c)} = 0$. Le polynôme $(X - c)(X - \bar{c}) = X^2 - (c + \bar{c}) + c\bar{c}$ est donc réel. On peut donc écrire

$$P = Q(X - c)(X - \bar{c}) + aX + b$$

où a et b sont réels. Par ailleurs on a $ac+b = 0$ et $a\bar{c}+b = 0$ (en évaluant notre polynôme en ces nombres complexes). Bref

$$a|c|^2 + b\bar{c} = 0 \text{ et } a|c|^2 + bc = 0$$

soit $b(c - \bar{c}) = 0$, $b = 0$ et $a = 0$. Donc P est divisible par $(X - c)(X - \bar{c}) = X^2 - (c + \bar{c})X + c\bar{c}$ (qui est bien un trinôme du second degré admettant deux racines complexes conjuguées). Son quotient est alors de degré inférieur à celui de P . Et l'on conclut par récurrence.

Il nous reste à faire le lien entre racines multiples et dérivée.

Définition 3.11. *On dit que a est une racine d'ordre m ($m \geq 1$) du polynôme P si et seulement si $P^{(h)}(a) = 0$ pour $h < m$.*

On retrouve le fait qu'une racine simple est un réel a qui annule P .

Proposition 3.12. *Le réel a est une racine d'ordre m ($m \geq 1$) du polynôme P si et seulement si $(X - a)^m$ divise P .*

Démonstration. Si a est une racine d'ordre m de P , la formule de Taylor s'écrit

$$P = \sum_{i=0}^{p} \frac{P^{(i)}(a)}{i!}(X - a)^i = \sum_{i=m}^{p} \frac{P^{(i)}(a)}{i!}(X - a)^i = (X - a)^m \sum_{h=0}^{p-m} \frac{P^{(h+m)}(a)}{(h + m)!}(X - a)^h$$

d'où le résultat.

Inversement, si $P = (X-a)^m Q$ alors

$$P^{(h)} = \sum_{i+j=h} \frac{h!}{i!j!} \left((X-a)^m\right)^{(i)} Q^{(j)} = \sum_{i+j=h} \frac{h!}{i!j!} \frac{m!}{i!} (X-a)^{m-i} Q^{(j)}$$

d'après la formule de Leibnitz. Mais, si $h < m$, on voit que le polynôme $(X-a)^{m-i}$ s'annule en a . Bref $P^{(h)}(a) = 0$ pour $h < m$.

Proposition 3.13 (Formule de Leibnitz)**.** *Soient P et Q deux polynômes de $\mathbb{R}[X]$. Alors*

$$(PQ)^{(n)} = \sum_{i+j=n} \frac{n!}{i!j!} P^{(i)} Q^{(j)} \ .$$

Démonstration. Si $n = 1$, cela correspond à la formule vue plus haut : $(PQ)' = P'Q + PQ'$. Etudions

$$(PQ)^{(n+1)} = \left((PQ)^{(n)}\right)' = \left(\sum_{i+j=n} \frac{n!}{i!j!} P^{(i)} Q^{(j)}\right)'$$

soit

$$(PQ)^{(n+1)} = \left((PQ)^{(n)}\right)' = \left(\sum_{i+j=n} \frac{n!}{i!j!} i P^{(i-1)} Q^{(j)}\right) + \left(\sum_{i+j=n} \frac{n!}{i!j!} P^{(i)} j Q^{(j-1)}\right)$$

et

$$(PQ)^{(n+1)} = \sum_{i=0}^{n} \frac{n!}{i!(n-i)!} P^{(i+1)} Q^{(n-i)} + \sum_{i=0}^{n} \frac{n!}{i!(n-i)!} P^{(i)} Q^{(n-i+1)} \ .$$

Transformons cette dernière égalité :

$$(PQ)^{(n+1)} = \sum_{h=1}^{n+1} \frac{n!}{(h-1)!(n+1-h)!} P^{(h)} Q^{(n+1-h)} + \sum_{i=0}^{n} \frac{n!}{i!(n-i)!} P^{(i)} Q^{(n-i+1)}$$

soit

$$(PQ)^{(n+1)} = \frac{n!}{n!} P^{(0)} Q^{(n+1)} + \sum_{i=1}^{n} \left(\frac{n!}{(i-1)!(n+1-i)!} + \frac{n!}{i!(n-i)!}\right) P^{(i)} Q^{(n+1-i)} + \frac{n!}{n!} P^{(n+1)} Q^{(0)} \ .$$

Il reste à étudier

$$(\text{pour } 1 \leq i \leq n) \ \frac{n!}{(i-1)!(n+1-i)!} + \frac{n!}{i!(n-i)!} = \frac{i \times n! + (n+1-i) \times n!}{i!(n+1-i)!} = \frac{(n+1)!}{i!(n+1-i)!} \ .$$

C'est ce que nous cherchions puisque

$$(PQ)^{(n+1)} = \frac{(n+1)!}{(n+1)!} P^{(0)} Q^{(n+1)} + \sum_{i=1}^{n} \frac{(n+1)!}{i!(n+1-i)!} P^{(i)} Q^{(n-i+1)} + \frac{(n+1)!}{(n+1)!} P^{(n+1)} Q^{(0)}$$

soit

$$(PQ)^{(n+1)} = \sum_{i+j=n+1} \frac{(n+1)!}{i!j!} P^{(i)} Q^{(j)} \ .$$

Proposition 3.14. *Soit P un polynôme réel non nul. Alors la somme des multiplicités des racines réelles ajoutée à la somme des multiplicités des racines complexes (non réelles) est égale au degré de P .*

Vérification. On sait que

$$P = \prod_{i=1}^{r}(X - a_i)^{m_i} \prod_{j=1}^{s}(X - c_j)^{n_j} \prod_{j=1}^{s}(X - \bar{c_j})^{n_j} \ .$$

On sait en effet que P , en tant que polynôme de $\mathbb{C}[X]$, est un produit de facteurs du premier degré et l'on sépare les facteurs introduisant des racines réelles et ceux introduisant des racines complexes. Le seul point à vérifier est que la multiplicité des racines complexes c_j est égale à celle des $\bar{c_j}$ mais on a évidemment

$$(0 \leq h \leq n_j)\ P(c_j) = \ldots = P^{(h)}(c_j) = 0 \text{ et } P^{(n_j)}(c_j) \neq 0) \Rightarrow P(\bar{c_j}) = \ldots = P^{(h)}(\bar{c_j}) = 0 \text{ et } P^{(n_j)}(\bar{c_j}) \neq 0$$

d'où le résultat puisque P est à coefficients réels (ainsi que tous ses polynômes dérivés).