Chapitre 10

Polynômes : quelques propriétés algébriques.

---

1 Polynômes : quelques propriétés utiles

On s'intéresse dans une première partie aux propriétés **algébriques** des polynômes (à coefficients réels ou complexes). On notera

- $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients réels,
- $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients complexes.

On sera amené à utiliser la notation $K[X]$ pour désigner l'ensemble des polynômes à coefficients dans K où K représentera soit l'ensemble des nombres réels soit l'ensemble des nombres complexes lorsque les polynômes auront des propriétés communes (qu'ils soient à coefficients réels ou complexes). On devra distinguer $\mathbb{R}[X]$ ou $\mathbb{C}[X]$ lorsque les propriétés seront différentes.
On a évidemment $\mathbb{R}[X] \subset \mathbb{C}[X]$.

Un polynôme à coefficients réels (ou complexes) de degré n s'écrit comme une **combinaison linéaire** de monômes, soit

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

où pour tout i, $a_i \in \mathbb{R}$ (respectivement $a_i \in \mathbb{C}$), $a_n \neq 0$.
Les polynômes de degré 0 sont les constantes non nulles. Le polynôme nul est de degré égal à $-\infty$ par convention.
Si P et Q sont dans $K[X]$, $\deg(PQ) = \deg(P) + \deg(Q)$.

Exemple 1 *$P(X) = X^2 + 2X + 3$, P est un polynôme de $\mathbb{R}[X]$ de degré 2, c'est également un polynôme qui appartient à $\mathbb{C}[X]$. Par contre le polynôme Q défini par $Q(X) = X^3 + 2iX + 2 - 3i$ est un polynôme de $\mathbb{C}[X]$ uniquement.*

1.1 Division Euclidienne

Ici nous allons voir une division possible concernant des polynômes appelée division euclidienne (analogue de la division euclidienne des entiers étudiée à l'école primaire).
On admet le théorème suivant :

Théorème 1 *Soit A et B deux polynômes de $K[X]$, on suppose B non nul. Alors il existe des polynômes Q et R dans $K[X]$ uniques tels que $A = BQ + R$ avec $\deg(R) < \deg(B)$.*

On dira que Q est le **quotient** dans la division euclidienne de A par B et R est le **reste**. On ne doit pas confondre la division euclidienne des polynômes (qu'on appelle aussi division suivant les puissances décroissantes) et la division selon les puissances croissantes que l'on a vu dans le cahpitre précédent et qui permet (sous certaines conditions d'obtenir le DL en 0 d'un quotient de fonctions).

Exercice 1 Effectuez la division euclidienne de $A = 2X^3 + X^2 + X + 2$ par $B = X^2 + X + 1$.
Exercice 2 Effectuez la division euclidienne de $A = X^3 - 1$ par $B = X - 1$.

1.2 Racines d'un polynôme

Définition 1 *Soit $P \in K[X]$. On dit que $\alpha \in K$ est une* **racine** *du polynôme P dans K si $P(\alpha) = 0$.*

Exemple 2 *Soit $Q(X) = X^2 - X + 1$, $Q \in \mathbb{R}[X]$, son discriminant $\Delta = -3 < 0$, donc Q n'admet pas de racine dans $\mathbb{R}$. Si on considère Q comme élément de $\mathbb{C}[X]$, alors Q admet deux racines dans $\mathbb{C}$, à savoir $\alpha = \dfrac{1 + i\sqrt{3}}{2}$ et $\beta = \dfrac{1 - i\sqrt{3}}{2}$.*

Remarque importante Lorsqu'on parle de racines de polynômes, il est important de préciser l'ensemble dans lequel on travaille : $\mathbb{R}[X]$ ou $\mathbb{C}[X]$.

On a alors le théorème suivant :

Théorème 2 *Soit P un polynôme de $K[X]$ et α un élément de K. α est racine de P dans K si et seulement si on peut écrire $P(X) = (X - \alpha)Q(X)$ où le polynôme Q appartient à $K[X]$ (i.e $X - \alpha$ peut-être mis en facteur dans l'écriture de P ou encore on dit que $X - \alpha$ divise le polynôme P dans $K[X]$).*

Ce théorème est très important pour plusieurs raisons. Par exemple, si vous connaissez une racine évidente α de P dans K, pour trouver les autres, vous pouvez effectuer la division euclidienne de P par $X - \alpha$, vous déterminez le quotient Q et ensuite il vous reste à déterminer les racines de Q dans K.

Démonstration du théorème

Si $P(X) = (X - \alpha)Q(X)$ alors $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$ donc par définition, α est bien une racine de P dans K.

Réciproquement : supposons que α est une racine de P dans K. Effectuons la division euclidienne de P par $X - \alpha$. Il existe des polynômes Q (quotient) et R (reste) uniques tels que

$$P(X) = (X - \alpha)Q(X) + R(X), \ \deg(R) < 1$$

On a alors

- soit $\deg(R) = 0$ mais dans ces conditions $R(X) = R$ est une constante non nulle et $P(\alpha) = (\alpha - \alpha)Q(\alpha) + R = R \neq 0$ ce qui contredit le fait que α est une racine de P.

- soit $\deg(R) = -\infty$ et dans ce cas $R = 0$ et on a bien démontré que P s'écrit $P(X) = (X - \alpha)Q(X)$.

A quoi peut servir ce théorème ? On donne l'exercice suivant pour illustrer une application

Exercice 3 On considère le polynôme P de degré 3 dans $\mathbb{C}[X]$ défini par $P(X) = X^3 + 1$. Déterminez ses racines dans $\mathbb{C}$.

On peut utiliser la méthode vue en début d'année : on cherche les racines de P dans $\mathbb{C}$ en utilisant l'écriture exponentielle, on résout alors l'équation $P(X) = 0 \iff X^3 = -1$.
Ou bien, on voit que $\alpha_0 = -1$ est une racine évidente de P dans $\mathbb{C}$ car $P(-1) = 0$. On va effectuer la division euclidienne de P par $X - (-1) = X + 1$. On trouve

$$P(X) = X^3 + 1 = (X + 1)(X^2 - X + 1)$$

Il reste alors à déterminer les racines du polynôme $Q(X) = X^2 - X + 1$ dans $\mathbb{C}$ (déjà fait plus haut). En résumé P admet trois racines dans $\mathbb{C}$: -1, $\frac{1+i\sqrt{3}}{2}$ et $\frac{1-i\sqrt{3}}{2}$. On peut alors écrire

$$P(X) = (X + 1)(X - \frac{1+i\sqrt{3}}{2})(X - \frac{1-i\sqrt{3}}{2})$$

Remarque importante vous voyez au travers de cet exemple qu'il est important de savoir si on travaille dans $\mathbb{C}[X]$ ou dans $\mathbb{R}[X]$. En effet, en tant que polynôme de $\mathbb{C}[X]$, P admet trois racines dans $\mathbb{C}$ et on obtient alors sa factorisation (en produit de polynômes de $C[X]$ de degré 1) sous la forme

$$P(X) = (X + 1)(X - \frac{1+i\sqrt{3}}{2})(X - \frac{1-i\sqrt{3}}{2}).$$

Par contre, si on considère P comme un polynôme de $\mathbb{R}[X]$, il admet une seule racine dans $\mathbb{R}$ et on obtient alors sa factorisation (en produit de polynômes de $\mathbb{R}[X]$) sous la forme

$$P(X) = (X + 1)(X^2 - X + 1)$$

On ne peut pas faire mieux !

– **Racines multiples d'un polynôme**.

Définition 2 *Soit P appartenant à $K[X]$ et α appartenant à K. α est une racine de P d'ordre m (ou de multiplicité m) s'il existe Q dans $K[X]$ tel que*

i) $P(X) = (X - \alpha)^m Q(X)$

ii) $Q(\alpha) \neq 0$.

Si $m = 1$, on dit que α est une racine simple de P, si $m = 2$ on dit que α est une racine double.

Exemple 3 *Soit* $P(X) = X^2 + 2X + 1$*,* $P \in \mathbb{R}[X]$ *admet une racine double (ou encore on dit une racine d'ordre 2 ou une racine de multiplicité 2) dans* $\mathbb{R}$ *; en effet si vous calculez son discriminant* $\Delta = 0$*. Mais ici c'est inutile car on remarque facilement que* $P(X) = (X+1)^2$ *donc* -1 *est une racine double de* P *dans* $\mathbb{R}$*.*

Pour être complet et si vous avez déjà oublié ou si ce n'était pas acquis vous devez revoir le chapitre sur les nombres complexes et le TD 2.

On peut aussi déduire du théorème précédent, la propriété importante suivante :

Propriété 1 *Soit* $P \in K[X]$ *de degré* $n \geq 1$*. Alors* P *a au plus* n *racines dans* K*.*

En effet, à chaque fois que α est racine de P dans K, on peut mettre en facteur $X - \alpha$ dans l'écriture de P. Or si P est de degré n ceci peut se faire au plus n fois. Un polynôme de $K[X]$ ne peut pas admettre plus de racines dans K que son degré !

Dans la pratique vous savez parfaitement déterminer les racines d'un polynôme de degré 2 à coefficients réels ou complexes par la méthode du discriminant, pour les polynômes de degré superieur ou égal à 3, vous ne savez pas.

Remarque qui peut vous aider

Lien entre racines et coefficients (cas particulier des polynômes de degré 2)
Prenons un polynôme de degré 2 de la forme $P(X) = X^2 + bX + c$ où b et c sont des réels. Supposons que α et β soient les racines de P dans $\mathbb{R}$ alors P s'éxcrit

$$P(X) = (X - \alpha)(X - \beta) = ...$$

Voir tableau.
Prendre l'exemple du polynôme $P(X) = X^2 + 2X - 3$.
Cette propriété reste valable dans $\mathbb{C}[X]$.

Définition 3 *Polynôme irréductible*
Soit $P \in K[X]$ *(où* $K = \mathbb{R}$ *ou* $K = \mathbb{C}$*) avec* $\deg(P) \geq 1$*. On dit que* P *est un polynôme irréductible de* $K[X]$ *s'il ne peut pas s'écrire comme le produit de deux polynômes de degré strictement inférieur dans* $K[X]$*.*

Exemple 4 *Les polynômes de degré 1 sont irréductibles dans* $K[X]$ *(*$K = \mathbb{R}$ *ou* $K = \mathbb{C}$*), le polynôme* P *définie par* $P(X) = X^2 + 1$ *n'est pas irréductible dans* $\mathbb{C}[X]$ *car on peut l'écrire dans* $\mathbb{C}[X]$*, sous la forme* $P(X) = (X - i)(X + i)$*. Par contre, il est irréductible dans* $\mathbb{R}[X]$ *car il ne peut pas s'écrire comme le produit de deux polynômes de degré strictement inférieur (i.e. comme produit de deux polynômes de degré 1) dans* $\mathbb{R}[X]$ *sinon cela impliquerait que* P *a des racines dans* $\mathbb{R}$ *ce qui n'est pas le cas.*

Lorsqu'on parle de polynômes irréductibles, il est important de préciser l'ensemble dans lequel on travaille là encore !

1.3 Particularité de l'ensemble des polynômes à coefficients complexes

Dans ce paragraphe, on travaille dans $\mathbb{C}(X]$.

On admet le théorème fondamental suivant :

Théorème 3 *Théorème de d'Alembert*
Tout polynôme de $\mathbb{C}[X]$ dont le degré est supèrieur ou égal à 1 admet au moins une racine dans $\mathbb{C}$.

Attention : ce résultat est faux dans l'ensemble des polynômes à coefficients réels. Par exemple, le polynôme $P(X) = X^2 + 4$ est un polynôme à coefficients réels qui n'admet aucune racine dans $\mathbb{R}$ (c'est un polynôme de degré 2 dont le discriminant est strictement négatif). Par contre, ce polynôme peut aussi être considéré comme un élément de $\mathbb{C}[X]$, et il admet deux racines distinctes dans $\mathbb{C}$, à savoir $2i$ et $-2i$. On a alors $P(X) = (X - 2i)(X + 2i)$.
Une conséquence importante de ce théorème est la propriété suivante :

Propriété 2 *Tout polynôme de $\mathbb{C}[X]$ de degré $n \geq 1$ admet exactement n racines dans $\mathbb{C}$ (éventuellement des racines multiples)*

Cette propriété est une conséquence immédiate du théorème de d'Alembert, on la démontre par récurrence sur le degré du polynôme. Vous pouvez faire la démonstration pour vous entraîner.
Cette propriété est **fondamentale**, on l'a souvent utilisée en début d'année lorsqu'on cherchait les solutions d'équations dans $\mathbb{C}$ (chercher les solutions d'une équation algébrique dans $\mathbb{C}$ de degré n revient à chercher les racines d'un polynôme de $\mathbb{C}[X]$ de degré n).

On revient sur l'exercice 3. Soit $P(X) = X^3 + 1$, P est un polynôme de degré 3, d'après la propriété précédente, il admet exactement 3 racines dans $\mathbb{C}$. Une autre façon de les déterminer est d'utiliser la méthode vue en début d'année dans le chapitre des nombres complexes.

Trouver les racines de P dans $\mathbb{C}$ c'est résoudre l'équation : $P(X) = 0 \iff X^3 = -1$. On va utiliser l'écriture exponentielle, on pose $X = \rho e^{i\theta}$ où $\rho > 0$ (c'est le module !) et $\theta \in \mathbb{R}$. On sait que $-1 = e^{i\pi}$ donc l'équation s'écrit : $\rho^3 e^{3i\theta} = e^{i\pi}$

$$\iff \begin{cases} \rho^3 = 1 \\ 3\theta = \pi + 2k\pi, \ k \in \mathbb{Z} \end{cases} \iff \begin{cases} \rho = 1 \\ \theta = \dfrac{\pi}{3} + \dfrac{2k\pi}{3}, \ k \in \{0, 1, 2\} \end{cases}$$

Pour $k = 0$, on obtient $X_0 = e^{i\frac{\pi}{3}} = \dfrac{1 + i\sqrt{3}}{2}$, pour $k = 1$, $X_1 = e^{i\frac{3\pi}{3}} = e^{i\pi} = -1$ et enfin pour $k = 2$, $X_2 = e^{5i\frac{\pi}{3}} = \dfrac{1 - i\sqrt{3}}{2}$. On a $X_2 = \overline{X_0}$. On va rappeler (ou enfin expliquer) dans le paragraphe suivant pourquoi X_0 et X_2 sont forcément conjuguées.

La partie qui suit est à retenir, elle nous sera très utile dans le paragraphe suivant.

Décomposition en polynômes irréductibles dans $\mathbb{C}[X]$

Tout polynôme de $\mathbb{C}[X]$ de degré $n \geq 1$, $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ où $a_n \neq 0$ peut s'écrire sous la forme

$$P(X) = a_n(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

où les α_i sont les racines du polynôme P (éventuellement confondues). On peut toujours écrire, dans $\mathbb{C}[X]$, P comme un produit de n polynômes de degré 1. On dit qu'il s'agit de **la décomposition de P en produit de polynômes irréductibles dans** $\mathbb{C}[X]$.

Propriété 3 *Les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes (de $\mathbb{C}[X]$) de degré 1.*

Exercice 4 Décomposer en polynômes irréductibles dans $\mathbb{C}[X]$, les polynômes $P(X) = X^4 - 1$ et $Q(X) = X^4 + 4$.

Correction Voir tableau

L'objectif principal de la fin de ce chapitre sur les polynômes est d'obtenir la **décomposition d'un polynôme P à coefficients réels en polynômes irréductibles dans** $\mathbb{R}[X]$.

1.4 Décomposition d'un polynôme à coefficients réels en polynômes irréductibles dans $\mathbb{R}[X]$

Reprenons le premier exemple vu ci dessus.
On a décomposé le polynôme $P(X) = X^4 - 1$ en polynômes irréductibles dans $\mathbb{C}[X]$ et on a obtenu la décomposition suivante :

$$P(X) = (X - 1)(X + 1)(X - i)(X + i)$$

Comme on l'a déjà dit, cette décomposition n'est pas valable dans $\mathbb{R}[X]$ car les deux derniers polynômes $X - i$ et $X + i$ ne sont pas à coefficients réels. On veut obtenir une décomposition de P en polynômes irréductibles dans $\mathbb{R}[X]$ ($P \in \mathbb{R}[X]$). Pour cela, on remarque que i et $-i$ sont des nombres complexes conjugués et si on fait le produit de $(X - i)(X + i) = X^2 + 1$, on obtient un polynôme à coefficients réels de degré 2 dont le discriminant est < 0. C'est un polynôme irréductible dans $\mathbb{R}[X]$, et on obtient donc la décomposition du polynôme P en polynômes irréductibles dans $\mathbb{R}[X]$:

$$P(X) = (X - 1)(X + 1)(X^2 + 1)$$

Pourquoi peut-on toujours se ramener à une telle décomposition ?

Propriété 4 *Soit $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polynôme à coefficients réels i.e. $a_i \in \mathbb{R}$ pour tout $0 \leq i \leq n$. Si P admet une racine complexe $\alpha \in \mathbb{C}$ alors $\overline{\alpha}$ est également racine de P.*

En effet, soit $\alpha \in \mathbb{C}$ une racine de P donc $P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$. On a alors

$$\overline{P(\alpha)} = \overline{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n} = 0.$$

$$\iff \overline{a_0} + \overline{a_1}\ \overline{\alpha} + \overline{a_2}\ \overline{\alpha^2} + \cdots + \overline{a_n}\ \overline{\alpha^n} = 0$$

Mais les coefficients a_i sont réels, donc $\overline{a_i} = a_i$ pour tout $0 \leq i \leq n$, on obtient donc

$$a_0 + a_1\overline{\alpha} + a_2\overline{\alpha}^2 + \cdots + a_n\overline{\alpha}^n = 0.$$

On a donc $P(\overline{\alpha}) = 0$, $\overline{\alpha}$ est donc aussi une racine de P dans $\mathbb{C}$.

Attention ! Ce résultat est faux dans $\mathbb{C}[X]$, les racines d'un polynôme à coefficients complexes ne sont pas nécessairement conjuguées.

Remarque : une conséquence importante de cette propriété est qu'un polynôme de degré impair à coefficients réels admet toujours au moins une racine réelle. On déduit aussi la propriété suivante :

Propriété 5 Les polynômes irréductibles dans $\mathbb{R}[X]$ *sont les polynômes de* $\mathbb{R}[X]$ *de degré 1 et les polynômes de* $\mathbb{R}[X]$ *de degré 2 dont le discriminant* $\Delta < 0$.

Soit $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polynôme à coefficients réels qui admet une racine complexe α, il admet également $\overline{\alpha}$ comme racine. On va pouvoir l'écrire dans $\mathbb{C}[X]$: $P(X) = (X - \alpha)(X - \overline{\alpha})Q(X)$. Les polynômes $X - \alpha$ et $X - \overline{\alpha}$ ne sont pas à coefficients réels mais si on fait le produit de ces deux polynômes on obtient toujours

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}.$$

Or $\alpha + \overline{\alpha} = 2\text{Re}(\alpha) \in \mathbb{R}$ et $\alpha\overline{\alpha} = |\alpha|^2 \in \mathbb{R}$ donc $X^2 - 2\text{Re}(\alpha)X + |\alpha|^2$ est un polynôme de degré 2 à coefficients réels dont le discriminant est strictement négatif (puisqu'il admet des racines complexes α et $\overline{\alpha}$), c'est donc un polynôme irréductible dans $\mathbb{R}[X]$. Il apparait dans la décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$.

En conclusion : soit $P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, $P \in \mathbb{R}[X]$, on suppose P de degré $n \geq 1$ (donc $a_n \neq 0$), on note $\alpha_1, \alpha_2, \cdots, \alpha_r$ les r racines réelles distinctes du polynôme P de multiplicité respective $m_1, m_2, \cdots, m_r$ (où les nombres m_i sont des entiers ≥ 1) alors **la décomposition de P en polynômes irréductibles dans** $\mathbb{R}[X]$ est toujours de la forme

$$P(X) = a_n(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}(X^2 + p_1X + q_1)^{t_1} \cdots (X^2 + p_sX + q_s)^{t_s}$$

où les polynômes $(X - \alpha_1), \cdots, (X - \alpha_r)$ sont les facteurs irréductibles de degré 1 qui correspondent aux racines réelles de P et les polynômes suivants $(X^2 + p_1X + q_1), \cdots, (X^2 + p_sX + q_s)$ sont les facteurs irréductibles de degré 2 dont le discriminant $\Delta < 0$ et qui correspondent aux racines complexes et non réelles du polynôme P.
Reprenons les deux exemples de l'exercice 4 (voir tableau) :

Exemple 5 *a) Soit $P(X) = X^4 - 1$:*

- *sa décomposition en polynômes irréductibles dans $\mathbb{C}[X]$ est*

$$P(X) = (X-1)(X+1)(X-i)(X+i).$$

- *sa décomposition en polynômes irréductibles dans $\mathbb{R}[X]$ est*

$$P(X) = (X-1)(X+1)(X^2+1).$$

b) Soit $Q(X) = X^4 + 4$:

- *sa décomposition en polynômes irréductibles dans $\mathbb{C}[X]$ est*

$$Q(X) = (X - z_0)(X - \overline{z}_0)(X - z_1)(X - \overline{z}_1).$$

$$Q(X) = (X - \sqrt{2}e^{i\frac{\pi}{4}})(X - \sqrt{2}e^{-i\frac{\pi}{4}})(X - \sqrt{2}e^{i\frac{3\pi}{4}})(X - \sqrt{2}e^{-i\frac{3\pi}{4}})$$

- *sa décomposition en polynômes irréductibles dans $\mathbb{R}[X]$ Voir tableau.*

Exercice 5 On considère les polynômes P et T définis par $P(X) = X^4 - 3X^3 + X^2 + 4$ et $T(X) = X^2 - 4X + 4$.

a) Effectuer la division euclidienne du polynôme P par le polynôme T.

b) En utilisant la question précédente, montrer que 2 est une racine double de P puis donner la décomposition de P en irréductibles dans $\mathbb{R}[X]$.

En résumé : que faut-il retenir sur ce chapitre ?

- Savoir ce qu'est un polynôme irréductible (définition 3), savoir quels sont les polynômes irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}(X)$ (propriétés 3 et 5).
- Effectuez une division euclidienne de deux polynômes (dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$) voir Théorème 1.
- Savoir que si α est une racine de P dans K alors P sécrit $P(X) = (X - \alpha)Q(X)$ où $Q \in K[X]$ (définition 1 et théorème 2).
- Connaître par coeur le théorème de d'Alembert et sa conséquence (Théorème 3 et propriété 2)
- Savoir décomposer certains polynômes à coefficients complexes en polynômes irréductibles dans $\mathbb{C}[X]$ (exercice 4)
- Savoir décomposer certains polynômes à coefficients réels en polynômes irréductibles dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ (exemple 5)

Exercice 6

a) Déterminez les racines dans $\mathbb{C}$ du polynôme T défini par $T(X) = X^3 - 27i$.

b) En déduire la décomposition de T en polynômes irréductibles dans $\mathbb{C}[X]$.