Aix-Marseille Université Facultés des sciences - Aix-Montperrin

Géométrie et Polynômes

Guillemette Chapuisat

guillemette.chapuisat@univ-amu.fr

voir aussi le site http://www.aiezzi.it/enseignement/geometrie.html

Licences de Mathématiques et d'Informatique,
1er semestre
2016-2017

Chapitre 3

Polynômes

I. Les polynômes

1. Définitions

Définition 3.1

Un polynôme à une variable est une expression de la forme

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = \sum_{k=0}^{n} a_k X^k$$

où X est un symbole appelé indéterminée ou variable du polynôme. Les a_i sont les coefficients.
On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficient dans $\mathbb{K}$. Ici, $\mathbb{K} = \mathbb{R}$, $\mathbb{C}$ ou $\mathbb{Q}$.

Définition 3.2

La fonction polynôme associée à $P = \sum_{k=0}^{n} a_k X^k$ est l'application notée par abus $P : \mathbb{K} \to \mathbb{K}$ définie par $P(x) = \sum_{k=0}^{n} a_k x^k$.

Remarque: Ne pas confondre polynôme, qui est une suite finie de coefficients comme un vecteur mais avec des règles de calcul différentes, et fonction polynôme, qui est une application.

Définition 3.3

Si $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$, on dit que P est de degré n et on note $\deg P = n$, a_n est appelé coefficient dominant de P et si $a_n = 1$, on dit que P est unitaire.

Notation 3.4

Par convention, le polynôme nul $P = 0$ est de degré $-\infty$.

Exemple: $P = 3X^2 + 2$, alors $\deg(P) = 2$. $Q = X^5 + 3X^4 + 2X^3 - 4X + e$ est unitaire de degré 5. $R = 2$ est de degré 0.

Définition 3.5 (*Somme et produit*)

On effectue la somme et le produit de polynômes comme pour les fonctions classiques. En regroupant les termes de même degré, on peut si besoin écrire les formules générales : Si $P = a_0 + \cdots + a_n X^n$ et $Q = b_0 + \cdots + b_m X^m$, alors on définit la somme de P et Q par

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

et le produit de P et Q par

$$PQ = \left(\sum_{k=0}^{n} a_k X^k\right)\left(\sum_{i=0}^{m} b_i X^i\right) = \sum_{j=0}^{n+m}\left(\sum_{i=0}^{j} a_i b_{j-i}\right) X^j$$

en posant $a_i = 0$ pour $i > n$ et $b_j = 0$ pour $j > m$.

Définition 3.6 (*Composée et dérivée*)

Si $P = a_0 + \ldots a_n X^n$ et $Q = b_0 + \cdots + b_m X^m$, alors on définit le polynôme dérivé de P par

$$P' = \sum_{k=1}^{n} n a_n X^{n-1}$$

et on définit la composée de P par Q par

$$P(Q) = \sum_{k=0}^{n} a_k \left(\sum_{i=0}^{m} b_i X^i\right)^k$$

Lemme 3.7

Pour tout $P, Q \in \mathbb{C}[X]$ on a

$$\deg(P+Q) \leq \max(\deg(P), \deg(Q)),$$

$$\deg(PQ) = \deg(P) + \deg(Q),$$

$$\deg(P') = \deg(P) - 1 \text{ si } \deg(P) \geq 1,$$

$$\deg(P(Q)) = \deg(P)\deg(Q).$$

Démonstration : D'après les formules ci-dessus. ■

Exemple: Attention, l'inégalité dans le degré d'une somme peut être stricte : $X^2 + 1 + (-X^2 + 3X) = 3X + 1$.

2. Division euclidienne

Théorème 3.8

Soient A, B deux polynômes avec $B \neq 0$. Alors il existe un unique couple de polynômes Q, R vérifiant

$$A = BQ + R \quad et \quad \deg(R) < \deg(B).$$

Les polynômes Q et R sont respectivement le **quotient** *et le* **reste** *de la division de A par B. Si $R = 0$, on dit que B divise A ou que A est un multiple de B.*

Démonstration : Pour l'unicité supposons que $BQ+R = BQ'+R'$, on arrive à la relation $B(Q-Q') = R'-R$ et on utilise la condition sur le degré pour en déduire $\deg(R-R') \leq \deg B$, donc nécessairement $Q = Q'$ et donc $R = R'$.

Pour l'existence on le prouve par récurrence forte sur le degré de A sachant que le cas $\deg(B) < \deg(A)$ est évident. Soit donc X^n avec $n > \deg(B)$. Définissons C par $C = X^n - 1/aX^{n-\deg(B)}B$ avec

a coefficient dominant de B. Le terme de C d'ordre n vaut 0 donc $\deg(C) \leq n-1$ et on applique l'hypothèse de récurrence. ■

Exemple: On effectue la division de X^5 par $3X^2+4$. On trouve

$$X^5 = (3X^2+4)(1/3X^3 - 4/9X) + 16/9X.$$

Remarques: Remarquons les faits suivants :
- Toute constante non nulle divise un polynôme.
- P divise toujours P.
- La division dépend de l'ensemble où vivent les coefficients. X^2+1 n'admet comme diviseur dans $\mathbb{R}[X]$ que les constantes, or dans $\mathbb{C}[X]$ $X-i$ le divise car $X^2+1 = (X-i)(X+i)$.

II. Racines d'un polynôme

1. Définition

Définition 3.9

On dit que $a \in \mathbb{K}$ est une **racine** de $P \in \mathbb{K}[X]$ si la fonction polynôme associée à P vérifie $P(a) = 0$.

Remarque: Tout dépend quel ensemble on considère : le polynôme X^2+1 n'a pas de racine réelle, mais il a deux racines complexes. De même X^2-2 a deux racines réelles mais pas de racine rationnelle.

Lemme 3.10

Soit P un polynôme, a est une racine de P si et seulement si $X-a$ divise P.

Démonstration : On effectue la division de P par $X-a$. Alors $P = Q.(X-a)+R$ mais $\deg(R) < 1$ donc R est une constante et en prenant la fonction polynôme en a, on a $P(a) = R(a) \in \mathbb{K}$ donc $P = Q.(X-a) + P(a)$. On a donc $(X-a)$ divise P si et seulement si $P(a) = 0$ c'est à dire ssi a est racine de P. ■

Corollaire 3.11

Si $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{K}$ sont des racines distinctes de $P \in \mathbb{K}[X]$, alors $\prod_{i=1}^{k} X - \alpha_i$ divise P.

Démonstration : Comme α_1 est racine de P, il existe $Q_1 \in \mathbb{K}[X]$ tel que $P = Q_1.(X-\alpha_1)$. On a donc $P(\alpha_2) = 0 = Q_1(\alpha_2)(\alpha_2 - \alpha_1)$. Comme $\alpha_2 \neq \alpha_1$, α_2 est nécessairement racine de Q_1 donc il existe $Q_2 \in \mathbb{K}[X]$ tel que $P = Q_2.(X-\alpha_2)(X-\alpha_1)$. On recommence en calculant $P(\alpha_3)$ et comme $\alpha_3 \neq \alpha_1, \alpha_2$, α_3 est racine de Q_2. Ainsi de suite. A la fin, on a $P = Q_k \prod_{i=1}^{k} X - \alpha_i$ d'où le résultat. ■

Corollaire 3.12

Un polynôme de degré n a au plus n racines.

Démonstration : On utilise le lemme précédent, et le fait que le produit de $(X-a_i), 1 \leq i \leq n$ est de degré n. ■

Proposition 3.13

Soit $P \in \mathbb{R}[X]$. Si $\alpha \in \mathbb{C}$ est racine de P, alors $\bar{\alpha}$ est aussi racine de P

Démonstration : On pose $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{R}[X]$.Comme α est racine, on a $P(\alpha) = \sum_{k=0}^{n} a_k \alpha^k = 0$ mais en prenant le conjugué, on a

$$\overline{P(\alpha)} = 0 = \overline{\sum_{k=0}^{n} a_k \alpha^k} = \sum_{k=0}^{n} a_k \bar{\alpha}^k = P(\bar{\alpha})$$

d'après les règles de sommation et multiplication du conjugué et puisque $\bar{a}_k = a_k$. Donc $\bar{\alpha}$ est racine de P. ■

2. Relations coefficients-racines

Proposition 3.14

Soit $P = X^2 + pX + q$. Soient α et β ses racines. Alors $\alpha\beta = q$ et $\alpha + \beta = -p$.

Démonstration : On développe l'égalité $P = X^2 + pX + q = (X - \alpha)(X - \beta)$ et on identifie les coefficients. ■

Proposition 3.15

Soit $n \geq 2$. Les n racines n-ième de l'unité $w_0, w_1, \ldots, w_{n-1}$ sont les racines complexes du polynôme $X^n - 1$. On a donc

$$\sum_{k=0}^{n-1} w_k = 0 \quad et \quad \prod_{k=0}^{n-1} w_k = (-1)^{n+1}$$

Démonstration : Comme les w_k sont les racines, on a $X^n - 1 = \prod_{k=0}^{n-1}(X - w_k)$. Il suffit alors de développer et d'identifier les coefficients en X^{n-1} et les termes constants pour obtenir les formules. ■

Remarque: L'autre formule classique avec les racines n-ème vient de la formule de la somme géométrique

$$X^n - 1 = (X - 1)\sum_{k=0}^{n-1} X^k.$$

D'autre part, en factorisant $X^n - 1$ par ses racines, on a

$$X^n - 1 = \prod_{k=0}^{n-1}(X - w_k) \text{ avec } w_k = e^{i\frac{2k\pi}{n}}.$$

Donc en divisant par $X - 1$ et en identifiant, on obtient $\displaystyle\sum_{k=0}^{n-1} X^k = \prod_{k=1}^{n-1}(X - w_k)$.

3. Multiplicité

Définition 3.16

On dit que α est une **racine de multiplicité** k si $(X-\alpha)^k$ divise P et que $(X-\alpha)^{k+1}$ ne divise pas P. Si la multiplicité vaut 1 on parle de **racine simple**, sinon on parle de **racine multiple**.

Théorème 3.17

Soient $P \in \mathbb{C}[X]$ de degré n et $a \in \mathbb{C}$. On a

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

où $P^{(k)}(a)$ désigne la dérivée k-ème de la fonction polynôme prise en a.

Démonstration : Pour $P = \sum_{k=0}^{n} a_k X^k$, on écrit la dérivée j^{e} de P :

$$P^{(j)} = \sum_{k=j}^{n} a_k k(k-1)\cdots(k-j+1)X^{k-j}.$$

Donc $P^{(j)}(0) = a_j j!$ d'où le résultat pour $a = 0$. Ensuite on considère le polynôme $P(X+a)$ auquel on applique la formule en 0 et on obtient bien la formule. ■

Corollaire 3.18

Soit P un polynôme complexe, α un nombre complexe et k un entier. On a équivalence entre

i) α est racine de P de multiplicité k.

ii) $P(\alpha) = \cdots = P^{(k-1)}(\alpha) = 0, \quad P^{(k)}(\alpha) \neq 0.$

Démonstration : Conséquence du théorème précédent pour une implication. L'autre sens vient du calcul des dérivées de $(X-\alpha)^k R(X)$. ■

Exemple: Soit $P = X^3 - 5X^2 + 7X - 3$.
Montrer que 1 et 3 sont racines doubles et simples de P.

III. Polynômes irréductibles

Définition 3.19

Un polynôme à coefficients dans $\mathbb{K}$ est **irréductible** s'il ne peut s'écrire comme produit de polynômes non constants à coefficients dans $\mathbb{K}$.

Remarque: Ainsi les polynômes de degré un sont toujours irréductibles, de même pour le polynôme $X^2 - 2$ sur $\mathbb{Q}$.

Lemme 3.20

Soit P un polynôme de degré au moins deux.

- *Si P est irréductible, alors il n'a pas de racine (dans $\mathbb{K}$).*
- *S'il est de degré deux ou trois, alors il est irréductible si et seulement s'il n'a pas de racine.*

Démonstration : C'est un corollaire du lemme précédent pour le premier point. Pour le deuxième, on calcule. ■

Remarque: Le deuxième point du lemme est faux si le degré vaut quatre comme le montre l'exemple : $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ sur $\mathbb{R}$.

Théorème 3.21

Tout polynôme non constant se décompose comme produit de polynômes irréductibles.

Démonstration : Par récurrence forte sur le degré du polynôme. ■

Exemple: On a $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. On calcule les racines cinquièmes de l'unité et on voit qu'il existe a réel tel que.

$$X^5 - 1 = (X - 1)(X^2 - 2aX + 1)(X^2 + 2aX + 1).$$

Remarque: Il existe sur $\mathbb{Q}$ des polynômes irréductibles de tout degré non nul.

Cette décomposition n'est pas unique puisqu'il suffit de multiplier un des polynômes par une constante, et de diviser un autre par la même constante.

Théorème 3.22 (*de d'Alembert*)

Tout polynôme non constant admet une racine complexe.

Démonstration : Admis car dur. ■

Corollaire 3.23

Les polynômes irréductibles sur $\mathbb{C}$, non constant, sont les polynômes de degré un.

Les polynômes irréductibles sur $\mathbb{R}$, non constant, sont de degré un, ou de degré deux sans racine réelle.

Démonstration : Conséquence du théorème précédent.

Et si $P \in \mathbb{R}[X]$, on a $P = \prod(X - \alpha_i)$ avec $\alpha_i \in \mathbb{C}$ mais $\bar{P} = P$ donc $\bar{\alpha}_i = \alpha_j$ d'où $\alpha_i \in \mathbb{R}$ ou il existe $i \neq j$ tel que $\bar{\alpha}_i = \alpha_j$. Bref on peut récrire P sous la forme

$$P = \prod(X - \alpha_k) \prod(X - \beta_i)(X - \bar{\beta}_i) = \prod(X - \alpha_k) \prod(X^2 - 2\,\mathrm{Re}(\beta_i)X + |\beta_j|^2).$$

■