Polynômes

Christophe Antonini[1], Olivier Teytaud[2], Pierre Borgnat[3], Annie Chateau[4], and Edouard Lebeau[5]

[1]Enseignant en CPGE, Institut Stanislas, Cannes
[2]Chargé de rechercher INRIA, Université d'Orsay, Orsay
[3]Chargé de recherche CNRS, ENS Lyon, Lyon
[4]Maitre de conférence, Université Montpellier-2, Montpellier
[5]Enseignant en CPGE, Lycée Henri Poincaré, Nancy

22 septembre 2021

Généralités sur les polynômes et zoologie.

1 Polynômes

Après quelques généralités (1.1), on présentera la division euclidienne (1.2) et la fonction naturellement associée à un polynôme (1.3), avec le concept notamment de racine d'un polynôme.

On plongera alors dans l'important cas d'un corps (1.4), avant de se concentrer sur quelques cas importants (1.5).

1.1 Généralités

DÉFINITION 0.1 **polynômes**
Soit A un anneau commutatif unitaire (resp. $\mathbb{K}$ un corps). L'ensemble des suites d'éléments de A nulles à partir d'un certain rang, noté $A^{(\mathbb{N})}$, est un A-module (resp. un $\mathbb{K}$-espace vectoriel) pour l'addition et la multiplication par un scalaire usuelles. En le munissant en outre du produit suivant :

$$\times : (u, v) \mapsto w \text{ avec } w_n = \sum_{i+j=n} u_i.v_j$$

On obtient une A-algèbre (resp. $\mathbb{K}$-algèbre), notée $A[X]$ (resp. $\mathbb{K}[X]$).

Les éléments de $A[X]$ sont appelés **polynômes**.

Deux polynômes P et Q non nuls sont dits **associés** s'il existe λ inversible tel que $P = \lambda.Q$.

On identifie A (resp. $\mathbb{K}$) et l'ensemble des suites $(u_n)_{n\in\mathbb{N}}$ avec $u_n = 0$ pour tout $n > 0$, par l'isomorphisme canonique $x \mapsto (u_n)_{n\in\mathbb{N}}$ avec $u_0 = x$ et $u_n = 0$ pour tout $n > 0$.

On note X l'élément $(u_n)_{n\in\mathbb{N}}$ avec $u_0 = 0$, $u_1 = 1$, et $u_n = 0$ pour $n > 1$.

La famille des X^i pour $i \in \mathbb{N}$ constitue la base canonique du module libre $A^{(\mathbb{N})}$ (resp. du $\mathbb{K}$-espace vectoriel $\mathbb{K}^{(\mathbb{N})}$).

Étant donné P un polynôme, on appelle **degré de** P et on note $\deg P$ le plus grand n tel que P_n est non nul. On appelle **coefficient dominant de** P le coefficient de $X^{\deg P}$ (que l'on peut voir comme $X^{deg(P)^*}(P)$ si l'on travaille avec un corps, voir la partie **??**) ; on le note $coef(P)$.

Un polynôme non nul est dit **unitaire** si son coefficient dominant est 1.

On appelle **support d'un polynôme** P l'ensemble des $n \in \mathbb{N}$ tels que $X^{n*}(P) \neq 0$. Par définition d'un polynôme, son support est fini.

Le degré d'un polynôme P est donc aussi le sup de son support.

On appelle **valuation de** P et on note $val(P)$ l'inf du support de P.

On appelle **composé de deux polynômes** P **et** Q et on note $P \circ Q$ le polynôme $\sum P_n Q^n$ (que l'on peut aussi voir comme $\sum_{n\in\mathbb{N}} X^{n*}(P).Q^n$ si l'on travaille avec un corps).

PROPOSITION 0.1 **Propriétés basiques des anneaux de polynômes**

•1 est élément neutre pour la multiplication, X élément neutre pour $\circ$, 0 élément neutre pour l'addition.

•Les éléments inversibles de $\mathbb{K}[X]$ sont les éléments identifiés aux éléments de $\mathbb{K} \setminus \{0\}$.

•$deg(0) = -\infty$ et $val(0) = +\infty$.

•$deg(1) = 0$.

•$deg(X^i) = i$ et $val(X^i) = i$.

•$deg(P.Q) = deg(P) + deg(Q)$ et $val(P.Q) = val(P) + val(Q)$.

•$deg(P + Q) \leq \sup(deg(P), deg(Q))$ avec égalité si $deg(P) \neq deg(Q)$ ou si les coefficients dominants de P et Q ne sont pas opposés.

•$val(P + Q) \geq \inf(val(P), val(Q))$ avec égalité si $val(P) \neq val(Q)$ ou si $P_{val(P)}$ et $Q_{val(Q)}$ ne sont pas opposés.

•si A est intègre alors $A[X]$ est un anneau intègre ; c'est-à-dire que le produit de deux polynômes est nul si et seulement si l'un des deux polynômes est nul.

•$(P + Q) \circ R = P \circ R + Q \circ R$ mais en général $P \circ (Q + R) \neq P \circ Q + P \circ R$.

1.2 Division euclidienne

THÉORÈME 0.2 **Division euclidienne**
Soient A et B deux polynômes, avec $coef(B)$ inversible. Alors

$$\exists (Q, R) \text{ polynômes } / A = B.Q + R$$

$$\text{avec } deg\ R < deg\ B$$

Démonstration

•*Unicité :*

Supposons $B.Q + R = B.Q' + R'$ avec les conditions données sur le degré.

$$\text{Alors } B.(Q - Q') = R' - R$$

$$deg(B) + deg(Q - Q') = deg(R' - R)$$

$$\text{donc } deg(Q - Q') = -\infty$$

et $Q = Q'$ et $R = R'$.

•*Existence :*

On distingue deux cas.

– *Si le degré de A est inférieur strictement au degré de B, le résultat est clair avec $Q = 0$ et $R = A$.*

– *Sinon on procède par récurrence sur le degré de A, en considérant $A - \frac{coef(A)}{coef(B)}.X^{deg(A)-deg(B)}$...*

DÉFINITION 0.2 **quotient**
Q est appelé **quotient** de A par B, et R est appelé **reste** de A par B.

Un exemple en Maple :

Exemple Maple

```
> rem(x^4 + x^3 + x^2 + x + 1, x^3, x); 1 + x^2 + x
> quo(x^4 + x^3 + x^2 + x + 1, x^3, x);
x + 1
```

COROLLAIRE 0.3

Soit $\mathbb{K}$ un corps commutatif. $\mathbb{K}[X]$ est un anneau euclidien, donc un anneau principal.

Démonstration *La division euclidienne en est la preuve ; dans un corps, tout polynôme non nul a son coefficient dominant inversible.*

1.3 Fonction associée, racines d'un polynôme

DÉFINITION 0.3 **application polynômiale associée à A**
Étant donnée B une A-algèbre associative commutative et unitaire, on peut identifier P à une application de A dans A, dite **application polynômiale associée à A**, noté $\tilde{P}$, et définie par

$$\tilde{P}(x) = \sum_{n \in \mathbb{N}} P_n \ x^n.$$

Cela est notamment valable pour $B = A$; implicitement $\tilde{P}$ désignera généralement une fonction de A dans A.

PROPOSITION 0.4
Soit a dans A et P un polynôme appartenant à $A[X]$.
Le reste de la division euclidienne de P par $(X-a)$ est $P(a)$.

En considérant la division euclidienne de P par $(x-a)^n$, on peut énoncer la définition suivante :

DÉFINITION - PROPOSITION 0.4 **1**
Soit P un polynôme, a un élément de A et n un entier naturel.
Les conditions suivantes sont équivalentes :
– $(X-a)^n | P$ et $(X-a)^{n+1} \not| P$
– Il existe un polynôme Q tel que $P = (X-a)^n Q$ et $\tilde{Q}(a)$ non nul.
On dit alors que a est **racine** de P d'**ordre de multiplicité** n.

1.4 Cas où $A = \mathbb{K}$ est un corps

THÉORÈME 0.5
Si $\mathbb{K}$ est un corps commutatif alors $\mathbb{K}[X]$ est un anneau euclidien, donc un anneau principal, donc un anneau factoriel.

Démonstration *Le fait que $\mathbb{K}[X]$ est un anneau euclidien a été prouvé dans le corollaire 0.3.*

DÉFINITION - PROPOSITION 0.5 **1**
On dit qu'un corps $\mathbb{K}$ est **algébriquement clos** si et seulement si l'une des trois propositions équivalentes suivantes est vérifiée :
– tout polynôme de $\mathbb{K}[X]$ est **scindé**, c'est-à-dire produit de polynômes de degré 1.
– tout polynôme non constant a une racine dans $\mathbb{K}$.
– tout polynôme irréductible est de degré 1.

Intuition Dans $\mathbb{K}[X]$ avec $\mathbb{K}$ corps algébriquement clos, tout polynôme de degré n s'écrit de manière unique à l'ordre près des facteurs sous la forme :

$$c(X-k_1)(X-k_2)\dots(X-k_n)$$

avec c inversible, et les k_i les racines (pas forcément distinctes !) du polynôme.

Intuition $\mathbb{C}$ est algébriquement clos, d'après le corollaire **??**.
Un exemple en Maple :

Exemple Maple

$>\ P := X->x\hat{}4-1;$
$P := X^4 - 1$
$>\ factor(P);$
$(x-1)(x+1)(x^2+1)$
$>\ factor(P, complex);$
$(x+1.)(x+1.\,I)(x-1.I)(x-1.000000000)$

1.5 Zoologie des polynômes à une indéterminée

En dehors des paragraphes ci-dessous, on pourra consulter le §**??**, page **??** sur l'interpolation par les polynômes de Lagrange, d'ailleurs généralisable à un cadre plus vaste que les polynômes réels, et le théorème **??**, d'approximation par les polynômes de Bernstein.

1.5.1 Relations entre les racines et les coefficients d'un polynôme - localisation des racines d'un polynôme

On se donne pour l'ensemble de cette partie un polynôme $P \in \mathbb{C}[X]$, de degré n, P non nul. On définit $P = \sum_{i=0}^{n} p_i X^i$.

⊡ **Relations entre les racines et les coefficients d'un polynôme** On utilisera ici les polynômes symétriques élémentaires $\Sigma_i = \Sigma_{i,n}$ définis en partie 1.6.3.

THÉORÈME 0.6 **Relations entre racines et coefficients d'un polynôme**

Notons $\sigma_i = \Sigma_i(r_1, ..., r_n)$, avec r_1,...,r_n des complexes. On a $P = \lambda \Pi_{i=1}^{n}(X - r_i)$ pour un certain λ si et seulement si pour tout $i \in \{1, \ldots, n\}$, on a $\sigma_i = (-1)^i \frac{p_{n-i}}{p_n}$.

Démonstration *On écrit simplement l'égalité*

$$\sum_{i=0}^{n} p_i X^i = \lambda \prod_{i=1}^{n}(x - r_i).$$

On en déduit que $\lambda = p_n$, et les relations souhaitées en développant d'un côté et de l'autre du signe $=$.

⊡ **Localisation des racines d'un polynôme**

◇ **Premières informations** Le théorème de Rolle **??** permet de montrer que le polynôme dérivé d'un polynôme scindé est scindé.

◇ **Méthode itérative** On peut par exemple utiliser la méthode de Newton, trouvable dans tout bon ouvrage d'analyse numérique et en **??**. On pourra par exemple consulter [1], et la méthode est brièvement résumée en Partie **??**.

◇ **Méthode algébrique** La théorie du résultant donne quelques résultats intéressants sur la localisation de racines ; voir théorème 0.8.

1.5.2 Polynômes irréductibles

DÉFINITION 0.6 **polynôme irréductible**
Un polynôme P appartenant à $\mathbb{K}[X]$ est dit **polynôme irréductible** si il est irréductible en tant qu'élément de l'anneau $\mathbb{K}[X]$, c'est-à-dire s'il n'est pas inversible et si tout diviseur de P est une unité ou est produit de P par une unité.

Pour plus d'informations sur la recherche de facteurs irréductibles communs à deux polynômes, on consultera le théorème 0.8.

THÉORÈME 0.7
•Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
•Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes $aX^2 + bX + c$, avec $a \neq 0$ et $b^2 - 4ac < 0$.

Démonstration *Il est évident que les polynômes considérés sont bel et bien irréductibles, dans les deux cas réel et complexe. Réciproquement, le théorème de D'Alembert-Gauss (**??**) donne le résultat dans le cas complexe. Dans le cas réel, on procède comme suit :*
•*Supposons $P \in \mathbb{R}[X]$ irréductible dans $\mathbb{R}[X]$.*
•*Par simplicité et sans perte de généralité, on va supposer P unitaire.*
•*Si x est racine de P dans $\mathbb{C}$, alors $\overline{x}$ l'est aussi, avec le même ordre de multiplicité.*
•*P n'a pas de racine réelle r, sinon $X - r$ diviserait P et P ne serait pas irréductible.*
•*P peut donc s'écrire $P = \prod_{i=1}^{r} (X - r_i)^{n_i} (X - \overline{r}_i)^{n_i}$.*
•*$(X - r_i)(X - \overline{r}_i)$ est alors un polynôme réel (on le voit simplement en le développant), donc P est un produit de polynômes de discriminants négatifs strictement (là aussi il suffit de développer pour le voir). Il n'est irréductible que s'il contient un et un seul tel terme.*
D'où le résultat.

1.5.3 Résultant. Discriminant

DÉFINITION 0.7 **discriminant**
Étant donnés P et Q deux polynômes de $\mathbb{K}[X]$, on appelle **résultant de P et Q** le déterminant de la matrice carré suivante de type $p + q \times p + q$ avec p et q les degrés de P et Q :

$$\begin{pmatrix}
P_0 & 0 & 0 & 0 & \dots & 0 & Q_0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\
P_1 & P_0 & 0 & 0 & \dots & 0 & Q_1 & Q_0 & 0 & 0 & \dots & 0 & 0 & 0 \\
P_2 & \dots & P_0 & 0 & \dots & 0 & Q_2 & Q_1 & Q_0 & 0 \dots & 0 & 0 & 0 & \\
 & & \ddots & \ddots & \ddots & & & & \ddots & \ddots & \ddots & \ddots & & \\
P_3 & \dots & \ddots & \ddots & \ddots & 0 & Q_3 & \dots & \ddots & \ddots & \ddots & \ddots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & Q_{q-2} & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & Q_{q-1} & Q_{q-2} & & \vdots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & Q_q & Q_{q-1} & Q_{q-2} & & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & 0 & Q_q & Q_{q-1} & Q_{q-2} & & \vdots & \vdots & \vdots \\
P_p & P_{p-1} & \ddots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots \\
0 & P_p & \ddots & \ddots & \ddots & \ddots & 0 & \ddots & 0 & Q_q & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & P_p & \ddots & \ddots & \ddots & 0 & \ddots & 0 & 0 & \ddots & \ddots & \ddots & \ddots \\
0 & \dots & 0 & P_p & \ddots & \ddots & 0 & \ddots & 0 & 0 & \ddots & \ddots & \ddots & \ddots \\
0 & \dots & 0 & 0 & P_p & \ddots & \ddots & 0 & \ddots & 0 & \ddots & \ddots & Q_q & Q_{q-1}{}^0 \\
\dots & \dots & \dots & \dots & P_p & 0 & \dots & \dots & \dots & \dots & \dots & 0 & Q_q &
\end{pmatrix}$$

avec $P = \sum_{k=0}^{p} P_p X^k$ et $Q = \sum_{k=0}^{q} Q_q X^k$.

On appelle **discriminant** d'un polynôme P le résultant de P et de P' son polynôme dérivé. [1]

Intuition Il est à noter que le discriminant coïncide avec le classique $b^2 - 4ac$ pour un polynôme $ax^2 + bx + c$ si l'on fait l'aménagement cité dans la note de bas de page ci-dessus.

THÉORÈME 0.8

Le résultant de P et Q est nul si et seulement si P et Q ont au moins un facteur irréductible en commun. Le discriminant d'un polynôme P est nul si et seulement si il a au moins un facteur irréductible en commun avec son polynôme dérivé.

Démonstration

La deuxième affirmation n'est naturellement qu'une spécialisation de la première. On se contentera donc de prouver la première.

•*Supposons tout d'abord que P et Q aient un facteur irréductible commun R.*

– Alors $P = RS$ et $Q = RT$, avec deg T = deg Q − deg R et deg S = deg P − deg R, T et S non nuls.

– $PT = QS$, ou $PT - QS = 0$. Ceci exprime très exactement l'existence d'un vecteur X tel que la matrice M donnée dans l'énoncé vérifie $MX = 0$, avec X non nul ; donc la matrice n'est pas la matrice d'une bijection, donc son déterminant est nul.

•*Supposons maintenant qu'il existe un vecteur X tel que MX soit nul et X soit $\neq 0$. Alors, il existe T et S vérifiant $PT = QS$, avec deg T = deg Q − deg R et deg S = deg P − deg R.*

*– Supposons alors que P et Q n'aient pas de facteur irréductible en commun. Alors, par le Théorème de Gauss (**??**), P divise S, ce qui est impossible car deg $S <$ deg P.*

En particulier, si les polynômes sont scindés, ils ont une racine commune si et seulement si leur résultant est nul. Si P est scindé, son discriminant est nul si et seulement si P admet une racine double.

1.5.4 Division suivant les puissances croissantes

THÉORÈME 0.9 **Division suivant les puissances croissantes**

Soit $n \in \mathbb{N}$, C et D des polynômes à une indéterminée sur un même anneau A commutatif et unitaire. On suppose que $D(0)$ (en tant qu'élément de A), est inversible. Alors il existe deux polynômes Q et R vérifiant

— $C = DQ + X^{n+1}R$,

— $\deg Q \leq n$,

où Q et R sont appelés respectivement **quotient et reste de la division suivant les puissances croissantes de C par D à l'ordre n.**

Démonstration *La preuve se fait par récurrence inverse sur la valuation de C. Si cette valuation est supérieure ou égale à $n+1$, le résultat est clair. La suite est facile.*

Application 0.1 Cela servira notamment pour les développements limités de quotients (voir Proposition **??**, ou pour la décomposition de fractions rationnelles en éléments simples ci-dessous :

Voyons un exemple concret, la division suivant les puissances croissantes de $X^3 + 2X^2 + 2$ par $X + 2$:

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

Donc

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

c'est la division suivant les puissances croissantes à l'ordre 0. Continuons :

$$\begin{array}{rr|l} & X^3+2X^2+2 & X+2 \\ \cline{3-3} - & X+2 & 1-\frac{X}{2} \\ \cline{1-2} & 1X^3+2X^2-X & \\ - & -\frac{X^2}{2}-X & \\ \cline{1-2} & 1X^3+\frac{5}{2}X^2 & \end{array}$$

Donc

$$X^3 + 2X^2 + 2 = (X + 2)(1 - \frac{X}{2}) + (X + \frac{5}{2})X^2,$$

c'est la division suivant les puissances croissantes à l'ordre 1. Continuons encore :

$$\begin{array}{rr|l} & X^3+2X^2+2 & X+2 \\ \hline - & X+2 & 1-\frac{X}{2}+\frac{5}{4}X^2 \\ \hline & 1X^3+2X^2-X & \\ - & -\frac{X^2}{2}-X & \\ \hline & X^3+\frac{5}{2}X^2 & \\ - & \frac{5}{4}X^3+\frac{5}{2}X^2 & [2pt] \\ \hline & -\frac{1}{4}X^3 & \end{array}$$

Donc, division suivant les puissances croissantes à l'ordre 2,

$$X^3+2X^2+2=(X+2)(1-\frac{X}{2}+\frac{5}{4}X^2)-\frac{1}{4}X^3.$$

DÉFINITION 0.8 **corps des fractions rationnelles**
On appelle **corps des fractions rationnelles** pour un corps $\mathbb{K}$ le corps des fractions de $\mathbb{K}[X]$. Intuitivement, il s'agit des quotients de polynômes formels.

THÉORÈME 0.10 **Décomposition en éléments simples**

Soit $\mathbb{K}$ un corps clos (par exemple $\mathbb{C}$). Alors toute fraction rationnelle peut s'écrire de manière unique sous la forme suivante : $P+\sum_{i=1}^{n}(\sum_{j=1}^{n_i}\frac{\lambda_{i,j}}{(X-p_i)^j})$, avec P un polynôme dans $\mathbb{K}$, avec les n_i non nuls, avec les $\lambda_{i,j}\in\mathbb{K}$, et les p_i (les **pôles**) sont des éléments de $\mathbb{K}$ deux à deux disjoints.

Toute fraction rationnelle sur le corps des réels peut s'écrire de manière unique sous la forme suivante : $P+\sum_{i=1}^{n}(\sum_{j=1}^{n_i}\frac{\lambda_{i,j}}{(X-p_i)^j})+\sum_{i=1}^{m}(\sum_{j=1}^{m_i}\frac{\alpha_i X+\beta_i}{X^2+\gamma X+\delta})$ avec les p_i des réels distincts, les λ_i, α_i, β_i des réels, les $X^2+\gamma X+\delta$ des polynômes irréductibles 2 à 2 disjoints.

Ces formes uniques sont appelées **décompositions en éléments simples**.

Ces preuves ici admises se trouvent dans [2]. La décomposition en éléments simples peut s'obtenir à partir des divisions en puissances croissantes (et euclidiennes pour trouver le polynôme P de la décomposition). Mais des techniques pratiques plus efficaces existent :

- S'il y a plusieurs fractions rationnelles ajoutées, on peut étudier chacune d'elles séparément.
- Factoriser le dénominateur de la fraction rationnelle.
- Écrire la forme générale de la décomposition en éléments simples, comme dans le théorème 0.10.
- On utilise alors diverses heuristiques pour obtenir les éléments manquants :
  - Multiplier la fraction rationnelle et la décomposition en éléments simples par $(X-a)^d$, avec a une racine et d son degré. Spécialiser en $X=a$. On obtient ainsi les λ_{i,n_i}.
  - Regarder l'équivalent en $+\infty$ de la fraction rationnelle multipliée par X.
  - Enfin, spécialiser sur certaines valeurs $X=v$.

1.5.5 Polynômes orthogonaux

DÉFINITION 0.9 **polynôme à n indéterminées à coefficients dans A**
On suppose donné $(a,b) \in \overline{\mathbb{R}}^2$, $a < b$. On suppose donnée une fonction w de $]a,b[$ dans $\mathbb{R}_+^*$ continue. Enfin on suppose que pour tout n, $\int_a^b x^n w(x)dx$ est convergente [2]. On note alors E l'ensemble des fonctions de $]a,b[$ dans $\mathbb{R}$ telles que

$$\|f\|_2 := \sqrt{\int_a^b |f(x)|^2 w(x)dx} < \infty$$

L'ensemble des polynômes est inclus dans E, E muni du produit scalaire suivant :

$$< f,g >= \int_a^b f(x)g(x)w(x)dx$$

est un espace de Hilbert.

Il existe alors une suite de polynômes $(P_n)_{n\in\mathbb{N}}$, telle que $degP_n = n$, et telle que les P_n forment une famille orthogonale.

Démonstration *Le résultat découle simplement de l'orthogonalisation de Schmidt (Proposition* **??***) appliquée à $1, X, X^2, X^3, ...$ Le fait que le degré de P_n est $\leq n$ provient simplement des propriétés de l'orthogonalisation de Schmidt, i.e. le fait que P_n appartient à l'espace engendré par $1, X, ..., X^n$. Le fait que ce degré est $\geq n$ provient simplement du fait que s'il existait un P_n de degré $< n$, alors la famille $P_0, ..., P_n$ serait une famille libre (puisqu'orthogonale) et située dans un espace de dimension n ; ce qui contredit le lemme de Steinitz (***??***).*

Les polynômes orthogonaux ont de multiples applications, que l'on pourra trouver par exemple dans le livre [1].

On pourra consulter l'exemple Maple qui suit l'orthogonalisation de Schmidt (voir Proposition **??**).

1.5.6 Polynômes de Tchebycheff de première espèce

THÉORÈME 0.11

$$\forall n \in \mathbb{N}\ \exists T_n \in \mathbb{R}[X]\ \deg\ T_n \leq n \wedge (\forall t \cos(nt) = T_n(\cos(t))).$$

Démonstration

•*Soit $n \in N$. On a*

$$e^{inx} = \cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n = \sum_{k=0}^{n} C_n^k \cos(x)^{n-k} \sin(x)^k (i)^k$$

•*En prenant les parties réelles :*

$$\cos(nx) = \sum_{k=0}^{k\leq n/2} C_n^{2k} \cos(x)^{n-2k} (-1)^k (1-\cos(x)^2)^k$$

D'où le résultat.

PROPOSITION 0.12

$$T_n = 2^{n-1} \prod_{k=0}^{n-1} (X - \cos(\frac{2k+1}{2n}\pi))$$

Démonstration *Il suffit de vérifier que le coefficient dominant est le bon, que le degré est le bon, et que les* $\cos(\frac{2k+1}{2n}\pi)$ *sont bien des racines.*

1.5.7 Tout polynôme positif est somme de deux carrés

THÉORÈME 0.13

Soit P un polynôme appartenant à $\mathbb{R}[X]$. On suppose en outre que P est positif sur $\mathbb{R}$. Alors P est somme de deux carrés.

Démonstration *•Soit* $\mathcal{C}$ *l'ensemble des polynômes qui s'expriment comme somme de deux carrés.*

•Alors $\mathcal{C}$ *contient tous les polynômes de la forme* $(x-a)^n$*, pour* n *pair.*

•Tout polynôme irréductible unitaire de degré 2 est dans $\mathcal{C}$*. En effet,* $X^2 + b.X + c$ *est égal à* $(X - \frac{b}{2})^2 + (c - \frac{b^2}{4})$*, qui est bien une somme de deux carrés si* $c - \frac{b^2}{4} > 0$*.*

•Du coup, tout polynôme irréductible de degré 2 à coefficient dominant > 0 *est dans* $\mathcal{C}$*.*

•Si P *et* Q *sont dans* $\mathcal{C}$*, alors* PQ *est dans* $\mathcal{C}$ *(*$\mathcal{C}$ *est stable par multiplication). En effet, avec* $P = A^2 + B^2$ *et* $Q = C^2 + D^2$ *:*

$$(A^2 + B^2).(C^2 + D^2) = (AD + BC)^2 + (AC - BD)^2.$$

•$\mathcal{C}$ *contient les polynômes positifs dépourvus de racine. En effet, soit* P *sans racine ; il est produit de polynômes irréductibles. Le coefficient dominant est positif, au vu de l'équivalent en* $\pm\infty$*, donc on peut l'exprimer comme produit de polynômes irréductibles de degré 2 à coefficients dominants positifs.*

•Soit P *un polynôme positif. On a déjà vu que s'il n'admet pas de racine il est dans* $\mathcal{C}$*. On suppose maintenant qu'il admet des racines, par exemple une racine* a*. Soit* n *maximal tel que* $(X-a)^n$ *divise* P*.* $P = (X-a)^n Q$ *est équivalent en* a *à* $Q(a)(X-a)^n$ *; donc* n *doit être pair pour que le signe de* P *puisse être positif. En supposant par récurrence que pour les degrés inférieurs à celui de* P *le résultat est acquis, on conclut que* Q *et* $X - a$ *sont dans* $\mathcal{C}$*, et donc que* P *est dans* $\mathcal{C}$*.*

1.6 Polynômes à plusieurs indéterminées

Cette partie sera délibérément très peu détaillée ; beaucoup de démonstrations sont calquées sur le cas des polynômes à une indéterminée. On peut en première lecture se limiter à la partie 1, ou l'on travaillera avec des polynômes à une seule indéterminée, et fournissant les méthodes permettant de s'attaquer à cette partie plus abstraite.

1.6.1 Généralités

Définition 0.10
Soit A un anneau commutatif unitaire.

On appelle **polynôme à n indéterminées à coefficients dans** A l'ensemble des applications presque nulles de $\mathbb{N}^n$ dans A. On note $A[X_1, \ldots, X_n]$ l'ensemble des polynômes à n indéterminées à coefficients dans A. Par la suite, on dira souvent simplement, pour gagner en concision, polynôme.

On dit que $P \in \mathbb{K}[X_1, \ldots, X_n]$ est **de degré** d si d est le max des $|\nu|$ tels que P_ν est non nul (voir Définition **??** pour les rappels sur les opérations dans $\mathbb{N}^n$).

Si $i \in [[1, n]]$, on dit que P est de degré d en X_i si le sup des ν_i tels que $P_\nu \neq 0$ est d.

On note X_i l'élément de $A[X_1, \ldots, X_n]$ nul partout sauf en $\nu = (\delta_{i,j})_{j \in [1,n]}$, avec $X_\nu = 1$.

Étant donnés P et Q deux polynômes, on note $R = P \times Q$ le **produit de P et Q** avec

$$R_\nu = \sum_{\alpha+\beta=\nu} P_\alpha Q_\beta$$

(pour les opérations dans N^n, voir Définition **??**).

On appelle **monôme** un polynôme dont un seul élément est non nul.

On appelle **dérivé formel** d'un polynôme P par D^ν pour $\nu \in \mathbb{N}^n$ le polynôme

$$\sum_{\alpha \in \mathbb{N}^n} \frac{(\nu+\alpha)!}{\alpha!} P_{\alpha+\nu}.$$

On note parfois $\frac{\delta}{\delta X_i}\ D^\nu$ avec $\nu_j = (\delta_{i,j})_{j \in [1,n]}$.

Proposition 0.14
On identifie $A[X_1, \ldots, X_n]$ à $A[X_1, \ldots, X_{n-1}][X_n]$.

On identifie $A[X_1, \ldots, X_p][X_{p+1}, \ldots, X_n]$ à $A[X_1, \ldots, X_n]$.

$A[X_1, \ldots, X_n]$ est intègre si et seulement si A est intègre.

$A[X_1, \ldots, X_n]$ est muni naturellement d'une structure de A-module. Muni de la multiplication définie plus haut, il s'agit d'une A-algèbre.

L'ensemble des monômes unitaires est une base de $A[X_1, \ldots, X_n]$.

Étant donnée B une A-algèbre associative commutative unitaire, $P \in A[X_1, \ldots, X_n]$ et $x_1, ..., x_n$ n éléments de B, on appelle **valeur de P en** $(x_1, \ldots, x_n)$ l'élément de B $\sum_{\nu \in \mathbb{N}^n} P_\nu x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}$. On note cet élément $\tilde{P}(x_1, \ldots, x_n)$. On constate ainsi qu'un polynôme P s'identifie naturellement à une application $\tilde{P}$ de B^n dans B. On note $A[x_1, \ldots, x_n]$ l'ensemble des $\tilde{P}(x_1, \ldots, x_n)$ pour $P \in A[x_1, \ldots, x_n]$.

Si $(x_1, \ldots, x_n)$ vérifie $\tilde{P}(x_1, \ldots, x_n) = 0$, on dit que $(x_1, \ldots, x_n)$ est un zéro de P.

Étant donné $(x_1, \ldots, x_n)$ n éléments de B, l'ensemble des polynômes P vérifiant $P(x_1, \ldots, x_n) = 0$ est un idéal de $A[X_1, \ldots, X_n]$, engendré par les $(X_i - a_i)$ pour $i \in [1, n]$.

1.6.2 Si A est un corps $\mathbb{K}$

Proposition 0.15
Si $\mathbb{K}$ est un corps, $\mathbb{K}[X_1, \ldots, X_n]$ est naturellement muni d'une structure de $\mathbb{K}$-espace vectoriel .

Formule de Taylor, si $\mathbb{K}$ est un corps de caractéristique nulle : soit $P \in \mathbb{K}[X]$, alors

$$P = \sum_{\nu \in \mathbb{N}^n} \frac{1}{\nu!}(D^\nu P)(0)X^\nu.$$

1.6.3 Zoologie des polynômes à plusieurs indéterminées : les polynômes symétriques

⚠ *Attention 0.2* A est supposé ici anneau commutatif et unitaire.

DÉFINITION 0.11 **polynôme symétrique**
Soit $P \in A[X_1, \ldots, X_n]$. P est dit **polynôme symétrique** si et seulement si pour tout σ permutation de $[1, ..., n]$, $P(X_1, ..., X_n) = P(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)})$.

On appelle **polynômes symétriques élémentaires** les polynômes de la forme

$$\Sigma_{k,n} = \sum_{1 \leq a_1 \leq a_2 \leq \ldots \leq a_k \leq n} X_{a_1} X_{a_2} ... X_{a_k} \text{ pour } 1 \leq k \leq n$$

On appelle **k-ième polynôme de Newton** le polynôme $N_k = \sum_{i=1}^{n} X_i^k$.

Les polynômes symétriques élémentaires sont de la forme suivante, dans le cas $n = 3$:

$$\begin{aligned} \Sigma_{1,3} = &\quad X_1 + X_2 + X_3 \\ \Sigma_{2,3} = &\quad X_1X_2 + X_2X_3 + X_1X_3 \Sigma_{3,3} = \quad X_1X_2X_3 \end{aligned}$$

Application 0.3 On verra en section **??** une application des polynômes symétriques en géométrie et en section 1.5 une application aux polynômes à une indéterminée.

On ne donnera pas ici de preuve des résultats énoncés ; on pourra se référer à [2]. On a les propriétés suivantes :

•Les polynômes symétriques élémentaires sont symétriques (évident).

•Les polynômes de Newton sont symétriques (évident).

•Si Q est un polynôme à n indéterminées, alors $P = Q(\Sigma_{1,n}, \Sigma_{2,n}, ..., \Sigma_{n,n})$ est un polynôme symétrique (facile).

•Si $P \in A[X_1, ..., X_n]$ est symétrique, alors il existe un polynôme Q tel que $P = Q(\Sigma_{1,n}, \Sigma_{2,n}, ..., \Sigma_{n,n})$ (pas évident du tout, récurrence sur le nombre d'indéterminées et sur le degré du polynôme).

• **Relations de Newton** : Si $1 \leq k \leq n$ on a

$$N_k = \sum_{i=1}^{k-1} (-1)^i N_{k-i} \Sigma_{i,n} + (-1)^k k \Sigma_{k,n}.$$

Si $n \leq k$, on a $N_k = \sum_{i=1}^{n} (-1)^i N_{k-i} \Sigma_{i,n}$.

Références

[1] J.-P. Demailly, *Analyse numérique et équations différentielles*, Presses Universitaires de Grenoble, 1996.

[2] P. Tauvel, *Mathématiques générales pour l'agrégation*, Masson, 1997.