Polynômes

Antoine Louatron

Table des matières

Dans tout le chapitre, $\mathbb{K}$ désignera un corps. Dans la pratique, on appliquera les résultats à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

I Anneau des polynômes à une indéterminée

I.1 Définitions

I.1.1 Définition

1. *On appelle polynôme à une indéterminée à coefficients dans $\mathbb{K}$ toute suite stationnaire en 0 d'éléments de $\mathbb{K}$: $(a_0, \dots, a_n, 0, 0, \dots)$.*
   En pratique, une telle famille est notée sous la forme $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = \sum_{k=0}^{n} a_kX^k = P = P(X)$.
   X n'est pas une quantité réelle ou complexe inconnue, c'est un objet formel que l'on appelle l'indéterminé.
   L'ensemble des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$.
2. *On appelle polynôme constant les polynômes de la forme a_0X^0, $a_0 \in \mathbb{K}$, c'est à dire les polynômes n'ayant que le premier coefficient éventuellement non nul. Plus particulièrement on note* 0 *le polynôme ayant tous ses coefficients nuls.*
3. *On appelle monôme un polynôme n'ayant qu'un coefficient non nul, c'est à dire de la forme a_kX^k.*

I.1.2 Notation

1. On pourra parfois noter $\sum\limits_{k\in\mathbb{N}} a_kX^k$ le polynôme de la définition en convenant que la somme est en fait finie et qu'on a donc $a_{n+1} = a_{n+2} = \cdots = 0$.
2. Si on note une somme finie, on convient que le terme dominant est non nul.

I.1.3 Remarque

1. Un polynôme n'est pas une fonction ni une équation. C'est une suite de coefficients.
2. X n'est pas une variable ni une inconnue. Il marque juste la position des coefficients les uns par rapport aux autres.

I.1.4 Définition

Avec les notations de I.1.1

1. *Si $P \neq 0$, on appelle degré de P et on note $\deg P$ le plus grand entier k pour lequel $a_k \neq 0$.*
2. *Par convention on pose $\deg 0 = -\infty$.*
3. *Pour $n \in \mathbb{N}$ on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de $\mathbb{K}[X]$ de degré inférieur (ou égal) à n.*
4. *Le coefficient de degré $\deg P$ est appelé coefficient du terme de plus haut degré ou coefficient dominant de P. Si ce coefficient est* 1*, le polynôme P est dit unitaire.*

I.1.5 Théorème (Identification des coefficients)
Deux polynômes de $\mathbb{K}[X]$ sont égaux ssi leurs coefficients sont égaux, ie. $\sum a_kX_k$ et $\sum b_kX^k$ sont égaux ssi $\forall k \in \mathbb{N} a_k = b_k$.

Preuve.
Il s'agit de l'égalité de familles. on se souvient du fait que deux familles sont égales si elles ont le même nombres d'éléments et que ces éléments sont égaux deux à deux. ∎

I.1.6 Attention

Ce théorème ne s'applique pour le moment qu'aux polynômes, et pas aux fonctions polynomiales ! C'est justement tout l'intérêt de ces objets formels.

Explication On fait maintenant le lien avec ce que l'on appelait avant polynôme.

I.1.7 Définition

1. *Soit $P \in \mathbb{K}[X]$, $P = \sum\limits_{k\in\mathbb{N}} a_kX^k$ et $\lambda \in \mathbb{K}$. On appelle valeur de P en λ et on note $P(\lambda)$ l'élément de $\mathbb{K}$ défini par $\sum\limits_{k\in\mathbb{N}} a_k\lambda^k$.*
2. *On définit une application $f_P : \left\{ \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & P(x) \end{array} \right.$. C'est la fonction polynomiale associée à P. On pourrait également la noter $\widetilde{P}$.*

I.1.8 Remarque

1. On prendra garde à ne pas parler de la fonction P, mais bien du polynôme P et de la fonction f_P.
2. En particulier P et $P(X)$ représentent le même objet qui est un polynôme mais f_P et $f_P(x)$ sont des objets complètement différents.
3. **Pour l'instant**, on peut associer une fonction à un polynôme mais pas l'inverse.

I.1.9 Exemple
Calculer $P(0)$.

I.2 Opérations sur les polynômes

I.2.1 Exemple
Multiplier et sommer de manière intuitive $P = a_2X^2 + a_1X + a_0$ et $Q = b_3X^3 + b_2X^2 + b_1X + b_0$.

I.2.2 Définition-Proposition
Soient $P, Q \in \mathbb{K}[X]$, $P = \sum_{k\in\mathbb{N}} a_kX_k$ et $Q = \sum_{k\in\mathbb{N}} b_kX^k$.

1. *On appelle somme de P et Q (noté $P + Q$) le polynôme $\sum (a_k + b_k)X^k$.*
2. *On appelle produit de P et Q (noté PQ) le polynôme $\sum c_kX^k$ où $c_k = \sum_{i=0}^{k} a_ib_{k-i} = \sum\limits_{i+j=k} a_ib_j$.*
3. *En particulier si $\lambda \in K$, $\lambda P = \sum \lambda a_kX^k$.*

Preuve.
Comme P, Q sont des polynômes, on peut prendre $N_1, N_2 \in \mathbb{N}$ tels que

$$\forall k > N_1\ a_k = 0 \text{ et } \forall k > N_2\ b_k = 0.$$

1. On pose $N = \max(N_1, N_2)$. Alors $\forall k > N\ a_k + b_k = 0$ et donc la somme $\sum (a_k + b_k)X^k$ est bien une somme finie.
2. Soit $k > N_1 + N_2$. Alors $\forall i \in [\![0, k]\!]\ i > N_1$ ou $k - i > N_2$ donc $\sum_{i=0}^{k} a_ib_{k-i} = 0$ et la somme $\sum \left(\sum_{i=0}^{k} a_ib_{k-i}\right) X^k$ est bien finie.
   On a en particulier $c_{N_1+N_2} = a_{N_1}b_{N_2}$ en tant que dernier coefficient non nul. ∎

I.2.3 Propriétés des opérations

Soient $P, Q, R \in \mathbb{K}[X]$, $\lambda \in \mathbb{R}$.

1. $P + 0 = P$ et $P \times 1 = P$ (neutres)
2. $P \times 0 = 0$
3. $(P + Q) + R = P + (Q + R)$ et $(PQ)R = P(QR)$ (associativité)
4. $P + Q = Q + P$ et $PQ = QP$ (commutativité)
5. Tout polynôme possède un opposé (il suffi d'opposer chaque coefficient).
6. $P(Q + R) = PQ + PR$ (distributivité).
7. $\lambda(P + Q) = \lambda P + \lambda Q$ (distributivité)
8. $PQ = 0 \iff P = 0$ ou $Q = 0$ (intègre). On le prouvera juste après.
9. pour $n \in \mathbb{N}$, $(P + Q)^n = \sum\limits_{k=0}^{n} \binom{n}{k} P^kQ^{n-k}$ car $PQ = QP$.

I.2.4 ATTENTION

A priori on ne peut PAS inverser les polynômes : $\frac{1}{X}$ n'est pas un polynôme par exemple. On ne peut faire intervenir que des puissances positives de X.

I.2.5 Définition
Soit $P, Q \in \mathbb{K}[X]$, $P(X) = \sum_{k\in\mathbb{N}} a_kX^k$. On appelle composé de Q par P et on note $P \circ Q$ ou $P(Q)$ le polynôme $P \circ Q(X) = \sum_{k\in\mathbb{N}} a_kQ^k(X)$..
On a bien sûr posé $Q^0 = 1$.

I.2.6 Exemple
On pose $P = X + 2$. $P(X) = X + 2$ et $P(X^2) = X^2 + 2$ et $P(2X - 1) = 4X$.

I.2.7 Remarque

On a alors $P = X \circ P = P \circ X = P(X)$.

I.2.8 Proposition
Soient $P, Q \in \mathbb{K}[X]$.
$$f_{P\pm Q} = f_P \pm f_Q,\ f_{PQ} = f_P \times f_Q,\ f_{P\circ Q} = f_P \circ f_Q$$

Preuve.
Immédiat, les opérations sur les polynômes ont été construites pour. ∎

I.3 Degrés

I.3.1 Théorème
Soient $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$.

1. $\deg(PQ) = \deg P + \deg Q$. *On remarque que cette formule est vraie même pour le polynôme nul.*
2. $\deg \lambda P = -\infty$ *si* $\lambda = 0$ *et* $\deg \lambda P = \deg P$ *sinon.*
3. $\deg(P \circ Q) = \deg(P) \times \deg(Q)$ *si Q n'est pas le polynôme nul.*

Preuve.
Il suffit de reprendre la preuve de l'existence de PQ en tant que polynôme.
Pour la composition, on a besoin en plus du résultat du prochain théorème. ∎

I.3.2 M-Remarque

Si maintenant on a $PQ = 0$ (un produit de polynômes) alors les degrés de P et Q ne peuvent être tout les deux des entiers naturels, donc l'un des deux est $-\infty$.

I.3.3 Théorème
Soient $P, Q \in \mathbb{K}[X]$. $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$ *avec égalité si ces degrés sont distincts ou si les coefficients dominants sont non-opposés.*

Preuve.
Par contruction, si $\deg P > \deg Q$ (par exemple), alors le terme dominant de $P + Q$ est celui de P.
Si les degrés sont égaux, alors l'éventuel terme dominant est la somme des termes dominants de P et Q. Si ces termes sont opposés, le degré descend d'au moins 1. ∎

I.3.4 Exemple
Exemples sympathique : $(X + 1) + X + 2$. pas sympa : $(X^2 + 1) + (-X^2 - 1)$.

II Arithmétique dans K[X]

II.1 Divisibilité

II.1.1 Définition
Soit $A, B \in \mathbb{K}[X]$. On dit que A divise B ou que B est un multiple de A (noté $A|B$) ssi il existe un polynôme $P \in K[X]$ tel que $AP = B$.

II.1.2 Remarque

Comme pour les entier, il s'agit de pouvoir factoriser ou non.

II.1.3 Exemple
Montrons que $X^2|(X+1)^n - nX - 1$.

On peut appliquer la formule du binôme de Newton :

$$(X+1)^n - nX - 1 = \sum_{k=0}^{n} \binom{n}{k} X^k - nX - 1 = \sum_{k=2}^{n} \binom{n}{k} X^k = X^2 \sum_{k=2}^{n} \binom{n}{k} X^{k-2}.$$

Remarquer que la dernière factorisation est possible car toutes les puissances de X sont positives.

II.1.4 Remarque

Si $A, B \in \mathbb{K}[X]$ et qu'on a $D|A$ et $D|B$ alors $D|(A \pm B)$ et plus généralement $D|AU + BV$ pour tous $U, V \in \mathbb{K}[X]$: en effet, être divisible par D c'est être factorisable par D.

II.2 Division euclidienne

II.2.1 Exemple
Division de $X^4 + 2X^3 - X + 6$ par $X^2 - X + 2$. On trouve $Q = X^2 + 3X + 1$ et $R = -6X + 4$.

II.2.2 Théorème
Soient $(A, B) \in \mathbb{K}[X] \times (\mathbb{K}[X] \backslash \{0\})$. *Il existe un unique couple* $(Q, R) \in (\mathbb{K}[X])^2$ *tel que*

$$\begin{cases} A = BQ + R \\ \deg R < \deg B. \end{cases}$$

Le polynôme Q *est le quotient et* R *le reste dans la division euclidienne de* A *par* B.

Preuve.

1. Unicité.
   Soient (Q_1, R_1) et (Q_2, R_2) des couples convenables. On a en particulier

   $$B(Q_1 - Q_2) = R_2 - R_1.$$

   Ainsi $\deg B + \deg(Q_1 - Q_2) = \deg(R_1 - R_2)$. Mais on sait que $\deg(R_1 - R_2) \leqslant \max(\deg R_1, \deg R_2) < \deg B$, donc $\deg(Q_1 - Q_2) < 0$. Il n'y a qu'un polynôme de degré négatif, c'est 0. Finalement $Q_1 = Q_2$ et donc $R_1 = R_2$.
2. Existence.
   On pose $B = \sum_{k=0}^{n} b_k X^k$ où $n = \deg B \geqslant 0$. Si B divise A, alors on pose $R = 0$ et on a trouvé un couple convenable.
   Supposons maintenant que B ne divise pas A. Alors l'ensemble $D = \{\deg(A - BQ) | Q \in \mathbb{K}[X]\}$ est une partie de $\mathbb{N}$ (car la valeur $-\infty$ est exclue par hypothèse) non vide. Elle admet donc un minimum noté m. Soit $Q \in \mathbb{K}[X]$ tel que $\deg(A - BQ) = m$. On pose $R = A - BQ$ et on va prouver que $\deg R = m < n = \deg B$. Posons $R = \sum_{k=0}^{m} r_k X^k$
   Raisonnons par l'absurde en supposant que $m \geqslant n$. Alors $X^{m-n} \in K[X]$ et on considère $A - BQ - \frac{r_m}{b_n} X^{m-n} B = R - \frac{r_m}{b_n} X^{m-n} B$ qui est de degré $< m$ (car les termes dominant s'annulent dans cette soustraction). Il suffit maintenant de poser $K = Q + \frac{r_m}{b_n} X^{m-n}$ et alors $A - BQ - \frac{r_m}{b_n} X^{m-n} B = A - BK$ et donc $\deg(A - BK) \in D$. On a trouvé un entier dans D strictement plus petit que m. C'est impossible.
   Conclusion : $m < n$ ■

II.2.3 Exercice
Effectuer la division euclidienne de $7X^5 + 4X^4 + 2X^3 - X + 5$ *par* $X^2 + 2$.

Rappel Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On pose $P(\lambda) = f_P(\lambda)$. C'est un nombre dans $\mathbb{K}$.

II.2.4 Théorème
Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Le reste dans la division euclidienne de P par $(X-\lambda)$ est $P(\lambda)$.

Preuve.
On écrit cette division euclidienne $P = (X-\lambda)Q + R$, avec $\deg R < 1$, c'est à dire que R est constant (éventuellement nul). On a maintenant, en évaluant les deux parties de cette égalité en λ

$$P(\lambda) = (\lambda - \lambda)Q(\lambda) + R(\lambda) = R(\lambda).$$

Ainsi $R(\lambda) = P(\lambda)$ et R est constant, donc $R(X) = P(\lambda)$. ■

II.2.5 Méthode

Pour trouver le reste de la division euclidienne dans le cas général ($A = BQ + R$), on évalue cette relation aux racines de B.

II.2.6 Exemple
Diviser euclidiennement $X^3 + 5X - 7$ par $(X-1)(X-2)$.

II.3 Polynômes irréductibles

II.3.1 Définition
Soit $P \in \mathbb{K}[X]$. On dit que P est irréductible dans $\mathbb{K}[X]$ ssi il n'est pas constant et tous ses diviseurs sont soit constant soit de même degré que P. Dans le cas contraire, P est dit réductible.

II.3.2 Remarque

C'est l'équivalent pour les polynômes des nombres premiers : ils n'ont pas de "vrai" diviseur.

II.3.3 Exemple
Tout polynôme de degré 1 est irréductible. Soit $P \in \mathbb{K}[X]$ de degré 1. Si on peut écrire $P = AD$, alors ni A ni D n'est nul, et ils sont donc de degré entier. De plus

$$\deg A + \deg D = \deg P = 1$$

Donc $\deg A = 0$ ou $\deg D = 0$. C'est à dire que soit $D \in \mathbb{K}^*$ soit $A \in \mathbb{K}^*$. Dans tout les cas, l'autre est de même degré que P.

II.3.4 Exemple
Tout polynôme de degré 2 et ne possédant pas de racine dans $\mathbb{K}$ est irréductible. Soit en effet P ne possédant pas de racine dans $\mathbb{K}$. S'il est réductible, il s'écrit $P = P_1P_2$ avec $\deg P_1 = \deg P_2 > 0$, c'est à dire $P = (aX+b)(cX+d)$ et donc P admet deux racines non nécessairement distinctes $-\frac{b}{a}$ et $-\frac{d}{c}$.

$X^2 + 1$ est irréductible dans $\mathbb{R}[X]$.

II.3.5 Remarque

La notion de polynôme irréductible dépend de $\mathbb{K}$. Par exemple X^2+1 est irréductible dans $\mathbb{R}[X]$ mais dans $\mathbb{C}[X]$ on a $X^2 + 1 = (X-i)(X+i)$.

III Zéros des polynômes

III.1 Racines

III.1.1 Définition-Proposition
Soit $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Les deux propositions suivantes sont équivalentes

1. $P(\lambda) = 0$
2. $X - \lambda$ *divise* P

Dans ce cas, on dit que λ est une racine (ou un zéro) de P dans $\mathbb{K}$.

Preuve.
C'est un corollaire direct du théorème II.2.4. ■

III.1.2 Remarque

1. On a donc $P(\lambda) = 0 \iff P$ peut se factoriser par $(X-\lambda)$. On l'utilise souvent. Et dans les deux sens.
2. Les racines d'un polynôme dépendent très fortement du corps $\mathbb{K}$. Par exemple X^2+1 n'a pas de racine dans $\mathbb{R}$ mais en possède deux distinctes dans $\mathbb{C}$.

III.1.3 ATTENTION

Un polynôme peut être réductible sans pour autant posséder de racine : $(X^2+1)^2$ dans $\mathbb{R}[X]$.
On a : P a une racine implique P possède un facteur, mais la réciproque est fausse.

III.1.4 Définition
Soit P un polynôme et $\lambda \in \mathbb{K}$.

1. *L'ordre de multiplicité de λ est la plus grande puissance de $X-\lambda$ divisant P. Si λ n'est pas racine de P, on dit que son ordre de multiplicité est 0.*
   On a donc λ est de multiplicité α ssi $(X-\lambda)^\alpha | P$ et $(X-\lambda)^{\alpha+1} \nmid P$
2. *Une racine de multiplicité 1 est dite simple, et une racine de multiplicité supérieure à 2 est dite multiple (double pour multiplicité 2).*

III.1.5 Exemple
Racines et multiplicité de $P(X) = 4(X-1)^4X^2(X+2)$.

III.1.6 Exemple
Si P possède $\pm i$ comme racine simple et 2 comme racine double alors $P(X) = (X-i)(X+i)(X-2)^2Q(X)$ avec Q un polynôme.

III.1.7 Théorème
Soit $P \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. *Si $\deg P = n$ alors P possède au plus n racines comptées avec multiplicité ie la somme des multiplicités des racines de P est au plus n.*
2. *Un polynôme de degré au plus n et possédant au moins $n+1$ racines (comptées avec multiplicité) est nul.*
3. *Le polynôme nul est le seul polynôme à posséder une infinité de racines.*

Preuve.
Le deuxième point est la contraposée du premier.

On prouve ce théorème par récurrence. Un polynôme de degré 0 est un polynôme constant non nul donc n'a pas de racine.

Supposons que les polynômes de degré n exactement possèdent au maximum n racines.

Soit P de degré $n+1$. Il y a deux cas.

— Si P n'a pas de racine alors il en a au plus n+1...
— Si P possède au moins une racine on peut l'écrire $P = (X-\lambda)Q$ avec $\deg(Q) = n$. Ainsi Q possède au plus n racines et P possède une racine de plus que Q donc P possède au plus n+1 racines.

Par récurrence, le théorème est vrai. ∎

III.1.8 Exemple
Il existe un unique polynôme de degré 2 dont la courbe représentative (de la fonction polynomiale associée) passe par $\begin{pmatrix}-1\\-1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}$. Si on avait P et Q qui conviennent alors $P(-1) = Q(-1), P(0) = Q(0)$ et $P(1) = Q(1)$ donc $P-Q$ possède au moins 3 racines $-1, 0, 1$ et donc $P-Q = 0$ (car il est de degré 2 au maximum).

Montrons l'existence. On pose $P = aX^2+bX+c$. On doit avoir $\begin{cases} a-b+c = -1 \\ c = 1 \\ a+b+c = 2 \end{cases}$ et on trouve directement $a = -\frac{1}{2}$ et $b = \frac{3}{2}$.

III.1.9 Théorème
Deux fonctions polynomiales égales sur un intervalle infini I (ou sur un ensemble infini) ont les même coefficients.

Preuve.
Soient $P, Q \in \mathbb{K}[X]$ tels que $f_P = f_Q$. On a alors d'après la proposition I.2.8 f_{P-Q} est la fonction nulle. On en déduit que pour tout $\lambda \in I$, $(P-Q)(\lambda) = 0$ et donc que $P - Q$ admet une infinité de racines car I est infini. Ainsi $P - Q = 0$. ■

III.1.10 M-Remarque

La boucle est bouclée : à un polynôme on peut associer exactement une fonction et à une fonction polynomiale définie sur un intervalle infini, on peut associer exactement un polynôme.

EN particulier, deux fonctions polynômiales égales sur un ensemble infini ont les mêmes coefficients.

III.2 Dérivation des polynômes

III.2.1 Définition

Soit $P \in \mathbb{K}[X]$, $P = \sum\limits_{k\in\mathbb{N}} a_k X^k$.

1. *Le polynôme dérivé de P est $P' = \sum_{k=1}^{+\infty} k a_k X^{k-1}$.*
2. *On pose $P^{(0)} = P$ et pour tout $n \in \mathbb{N}$, $P^{(n+1)} = \left(P^{(n)}\right)'$. C'est le $(n+1)$ème polynôme dérivé de P ou le polynôme dérivé d'ordre $n+1$.*

III.2.2 Remarque

1. Si $\mathbb{K} = \mathbb{R}$ alors $f_{P'} = (f_P)'$.
2. On a également $P' = \sum\limits_{k=0}^{+\infty} (k+1) a_{k+1} X^k$. Cette façon décrire est pratique quand il s'agit d'identifier les coefficients.
3. $\deg P' = \deg P - 1$ si P est non constant, attention !

III.2.3 Remarque

Encore une fois, tout se passe bien si $\mathbb{K} = \mathbb{R}$ et qu'on compare la dérivée d'un polynôme et celle de sa fonction polynomiale associée.

III.2.4 Exercice

Montrer que tout polynôme est le polynôme dérivé d'au moins un autre polynôme.

III.2.5 Exemple

Soit $k \in \mathbb{N}$ et $i \leqslant n$. Calculons la dérivées $i$ème de X^k.

$$(X^k)^{(i)} = k(X^{k-1})^{(i-1)} = k(k-1)X^{(i-2)} = \cdots = k(k-1)\ldots(k-i+1)X^{k-i} = \frac{k!}{(k-i)!}X^{k-i}.$$

III.2.6 Théorème (Formule de Taylor)

Soit $P \in \mathbb{K}[X]$ un polynôme non nul et $\lambda \in \mathbb{K}$. Notons $n = \deg(P)$.

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k \text{ et } P(X+\lambda) = \sum_{k=0}^{n} \frac{P^{(k)}(\lambda)}{k!} X^k.$$

En particulier $P(X) = \sum\limits_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k = P(0) + P'(0)X + \frac{P''(0)}{2}X^2 + \frac{P^{(3)}(0)}{3!}X^3 + \ldots$.

Preuve.
Commençons par prouver le cas $\lambda = 0$. On suppose P non constant, la formule étant triviale dans ce cas.

On pose $P = \sum\limits_{k=0}^{n} a_k X^k$. Donc $P' = \sum\limits_{k=1}^{n} k a_k X^{k-1}$ et $P'(0) = a_1$. Montrons que $\forall i \leqslant n$ $P^{(i)}(0) = i! a_i$. En effet, soit $i \in [\![1, n]\!]$.

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

et donc $P^{(i)}(0) = i!a_i$. On en déduit immédiatement que

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

appliquons maintenant cette formule au polynôme $Q = P(X + \lambda)$. On a immédiatement par récurrence que $Q^{(k)} = P^{(k)}(X + \lambda)$ pour tout $k \in \mathbb{N}$ et donc

$$P(X + \lambda) = Q(X) = \sum_{k\in\mathbb{N}} \frac{Q^{(k)}(0)}{k!} X^k = \sum_{k\in\mathbb{N}} \frac{P^{(k)}(\lambda)}{k!} X^k$$

∎

III.2.7 Théorème
Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Les assertions suivantes sont équivalentes :

1. *λ est une racine de P multiplicité r exactement (ie $(X - \lambda)^r | P$ mais pas $(X - \lambda)^{r+1}$).*
2. *Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P = (X - \lambda)^r Q$ et $Q(\lambda) \neq 0$.*
3. *$P^{(0)}(\lambda) = P^{(1)}(\lambda) = \cdots = P^{(r-1)}(\lambda) = 0$ et $P^{(r)}(\lambda) \neq 0$ (avec exactement r égalités, en commençant par $k = 0$)*

Preuve.

— (1) ⇒ (2). C'est immédiat par la définition/caractérisation d'une racine : $Q(\lambda) = 0 \iff X - \lambda | Q$. Donc si $Q(\lambda) = 0$ alors $(X - \lambda)^{r+1} | P$.

— (2 ⇒ (3)). On écrit la formule de Taylor en notant n le degré de P.

$$P(X) = \sum_{k=0}^{r-1} \frac{P^{(k)}(\lambda)}{k!} (X - \lambda)^k + (X - \lambda)^r \sum_{k=r}^{n} \frac{P^{(k)}(\lambda)}{k!} (X - \lambda)^{k-r}$$

De plus $P = (X - \lambda)^r Q$, donc par unicité du reste de la division euclidienne par $(X - \lambda)^r$ on a $\sum_{k=0}^{r-1} \frac{P^{(k)}(\lambda)}{k!} (X - \lambda)^k = 0$ et par unicité des coefficients on obtient $\forall i \in [\![0, r]\!]$ $P^i(\lambda) = 0$. De plus $Q(\lambda) \neq 0$ donc $P^{(r)}(\lambda) \neq 0$ (en évaluant en λ et par unicité du quotient).

— (3) ⇒ (1). Ecrivons la formule de Taylor. Alors $(X - \lambda)^r | P$ mais $(X - \lambda)^{r+1} \not| P$ ∎

IV Polynômes réels et complexes

IV.1 Polynômes scindés

IV.1.1 Définition

Soit $P \in \mathbb{K}[X]$. On dit que P est scindé sur $\mathbb{K}$ s'il possède exactement autant de racines que son degré dans $\mathbb{K}$ (comptées avec multiplicité).

Encore une fois, le corps dans lequel on travail est important et notre polynôme fétiche $X^2 + 1$ est là pour nous le rappeler. Il n'a pas de racine dans $\mathbb{R}$ mais scindé est sur $\mathbb{C}$.

IV.1.2 Remarque

On peut alors écrire $P(X) = (X - \lambda_1)^{\alpha_1} \times \cdots \times (X - \lambda_p)^{\alpha_p} Q(X)$ avec Q de degré 0 c'est à dire que Q est une constante non nulle.

IV.1.3 Exemple

$P(X) = 4X(X - 1)(X - 2)$. Développer. Qu'est 4 ?

IV.1.4 Rappels non superflus

Soit $n \in \mathbb{N} \backslash \{0\}$. Le polynôme $X^n - 1$ est scindé sur $\mathbb{C}$ et ses racines sont les racines nièmes de l'unité. On a donc

$$X^n - 1 = \prod_{\omega\in\mathbb{U}_n} (X - \omega) = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}}) \text{ donc } \sum_{k=0}^{n-1} X^k = \prod_{\omega\in\mathbb{U}_n\backslash\{1\}} X - \omega = \prod_{k=1}^{n-1} (X - e^{\frac{2ik\pi}{n}}).$$

Pour obtenir la deuxième égalité, on effectue la division de polynômes de $X^n - 1$ par $X - 1$.

IV.1.5 Exemple

1. $(X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta$.
2. $(X-\alpha)(X-\beta)(X-\gamma) = (X^2-(\alpha+\beta)X+\alpha\beta)(X-\gamma) = X^3 - (\alpha+\beta+\gamma)X^2 + (\alpha\gamma+\beta\gamma+\alpha\beta)X - \alpha\beta\gamma$
3. Que vérifient les racines α et β de X^2-4X+7 ?

IV.1.6 Relation coefficients-racines

Soient $\lambda_1, \dots, \lambda_n \in \mathbb{K}$. On pose $P = (X-\lambda_1)\dots(X-\lambda_n)$. Développons.

— Le coefficient dominant de P est 1.

— Le coefficient du terme de degré $n-1$ est $-\lambda_1 - \dots - \lambda_n$.

— Le terme constant est $(-1)^n \lambda_1 \dots \lambda_n$.

IV.1.7 Méthode

Pour résoudre un système d'équations symétriques on pourra faire apparaître le polynôme ayant les inconnues comme racines puis calculer les fonctions symétriques de ce polynôme à partir des données. Voir le TD.

IV.1.8 Exercice

$(X-\alpha)(X-\beta)(X-\gamma)(X-\delta)(X-\gamma) = ...$

IV.2 Irréductibles de $\mathbb{C}[X]$

IV.2.1 Théorème (D'Alembert-Gauss)

Tout polynôme ***non constant*** *de $\mathbb{C}[X]$ admet au moins une racine complexe.*

Preuve.

Admis ! ■

IV.2.2 Corollaire

Tout polynôme de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Preuve.

Raisonnons sur le degré de P. Les polynômes de degré 0 sont scindés, ainsi que ceux de degré 1 Si maintenant P est de degré $n > 0$ alors P admet une racine $\lambda \in \mathbb{C}$ et $P = (X-\lambda)Q$, avec $\deg Q = n-1$ donc par hypothèse de récurrence Q admet $n-1$ racines et donc P admet n racines. On conclut par récurrence. ■

IV.2.3 Théorème

Soit $P \in \mathbb{C}[X]$ un polynôme non nul. Alors il existe une unique manière d'écrire (à l'ordre des facteurs près) $P = a \times \prod_{k=1}^{p} (X-\lambda_i)^{\alpha_i}$ où

— *a est le coefficient dominant de P*

— *les λ_i sont des complexes deux à deux distincts racines de P de multiplicité α_i exactement.*

Preuve.

On a déjà vu l'existence, on a admet l'unicité. ■

IV.3 Irréductibles de $\mathbb{R}[X]$

IV.3.1 Lemme

Soit $P \in \mathbb{C}[X]$, $P = \sum_{k\in\mathbb{N}} a_k X^k$. On note $\overline{P} = \sum_{k\in\mathbb{N}} \overline{a_k} X^k$. C'est le polynôme conjugué de P. Soit de plus $\lambda \in \mathbb{C}$.

Alors λ est racine de P de multiplicité $r \in \mathbb{N}$ ssi $\overline{\lambda}$ est racine de $\overline{P}$ de multiplicité r. En particulier, si $P \in \mathbb{R}[X]$, alors $P = \overline{P}$ et λ et $\overline{\lambda}$ ont même multiplicité dans P.

Preuve.
Cela provient directement du fait que la conjugaison est un morphisme de corps (ie est "compatible" avec l'addition et la multiplication). En effet on a pour tous $\lambda \in \mathbb{C}$ et $k \in \mathbb{N}$: $\overline{P}^{(k)}(\overline{\lambda}) = \overline{P^{(k)}(\lambda)}$. Soit maintenant $r \in \mathbb{N}$

$$\begin{aligned} \lambda \text{ racine de } P \text{ de multiplicité } r &\iff \forall k \in [\![0, r-1]\!]\ P^{(k)}(\lambda) = 0 \text{ et } P^{(r)}(\lambda) \neq 0 \\ &\iff \forall k \in [\![0, r-1]\!]\ \overline{P}^{(k)}(\overline{\lambda}) = 0 \text{ et } \overline{P}^{(r)}(\overline{\lambda}) \neq 0 \\ &\iff \overline{\lambda} \text{ racine de } \overline{P} \text{ de multiplicité } r \end{aligned}$$

■

IV.3.2 Théorème (Irréductibles de $\mathbb{R}$)
Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et les polynômes de degré 2 n'admettant pas de racine réelle (discriminant < 0).

Preuve.
Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. D'après le théorème de D'Alembert-Gauss il existe $\lambda \in \mathbb{C}$ racine de P.

— Si $\lambda \in \mathbb{R}$ alors on a déjà vu que $X - \lambda | P$ et donc P est de degré 1.

— Sinon, $\overline{\lambda} \neq \lambda$ et ces deux complexes sont racines de P donc leur produit divise P et $\deg P = 2$. De plus

$$(X - \lambda)(X - \overline{\lambda}) = X^2 - 2\Re\lambda + |\lambda|^2 \in \mathbb{R}[X]$$

Comme $P = a(X - \lambda)(X - \overline{\lambda})$ avec $a \in \mathbb{R}^*$, son discriminant est $4a^2((\Re\lambda)^2 - |\lambda|^2) = -4(\operatorname{Im}\lambda)^2 < 0$. ■

IV.3.3 Corollaire
Tout $P \in \mathbb{R}[X]$ s'écrit de manière unique sous la forme

$$a_n \prod_{i=1}^{r} (X - \lambda_i)^{\alpha_i} \prod_{j=1}^{s} (X^2 + b_j X + c_j)^{\beta_j}$$

où a_n est le coefficient dominant de P, $\lambda_1, \ldots, \lambda_r$ les racines réelles de P de multiplicités respectives $\alpha_1, \ldots, \alpha_r$ et les polynômes $X^2 + b_j X + c_j$ sont deux à deux distincts et irréductibles pour $j \in [\![1, s]\!]$.

IV.3.4 En pratique

Pour trouver une telle décomposition, on décompose sur $\mathbb{C}$ puis on développe les facteurs conjugués.

Index général

Index des symboles