Chapitre 5

Polynômes

Dans tout ce chapitre, $\mathbb{K}$ désigne un corps quelconque (on pourra en général penser que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$). On note $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

5.1 Définitions

5.1.1 Quand les polynômes deviennent un objet compliqué (mais en fait pas tant que ça)

Un polynôme à coefficients dans $\mathbb{K}$ s'écrit

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{ou encore} \quad \sum_{k=0}^{n} a_k X^k, \tag{5.1}$$

avec $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{K}$. Mais qui est ce X ? Ce n'est pas une variable. C'est une indéterminée. Une variable intervient dans l'expression d'une fonction et on ne peut lui substituer qu'un élément du domaine de définition de la fonction en question. Par exemple si on considère les fonctions

$$f : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^3 + 4x + 2 \end{array} \right. \quad \text{ou} \quad g : \left\{ \begin{array}{ccc} \mathbb{R}_+ & \to & \mathbb{R} \\ y & \mapsto & \cos(\sqrt{y}) \end{array} \right.$$

la lettre x désigne une variable qu'on peut remplacer par n'importe quel réel, mais rien d'autre, tandis que y est une variable que l'on peut remplacer par n'importe quel réel positif, mais rien d'autre.

L'expression définissant f a également un sens sur $\mathbb{C}$. On peut définir une autre fonction $\tilde{f}$ qui à $z \in \mathbb{C}$ associe $\tilde{f}(z) = z^3 + 4z + 2 \in \mathbb{C}$. En fait, cette expression définit une fonction sur n'importe quel espace dans lequel on a défini une addition, une multiplication, et une muliplication par les réels.

Considérons l'ensemble E des fonctions du plan $\mathbb{R}^2$ dans lui-même, muni de l'addition et de la multiplication par les réels usuelles, ainsi que de la composition. Ainsi $u^2 = u \circ u$, $u^3 = u^2 \circ u$, etc. Par convention on note $u^0 = \mathrm{Id}_{\mathbb{R}^2}$. On peut alors définir la fonction F qui à $u \in E$ associe

$$F(u) = u^3 + 4u + 2 = u \circ u \circ u + 4u + 2\,\mathrm{Id}_{\mathbb{R}^2}\,.$$

$F(u)$ est alors une fonction de $\mathbb{R}^2$ dans $\mathbb{R}^2$. Enfin on peut également considérer l'application qui à toute matrice carrée A de taille n fixée et à coefficients dans $\mathbb{R}$ associe la matrice $A^3 + 4A + 2I_n$. Les polynômes de matrices s'avèreront très utiles un peu plus tard...

L'interêt de l'indéterminée X est justement d'étudier ce genre de fonctions sans préciser la nature de la variable. L'intérêt est d'une part de traiter d'un seul coup tous les cas, et d'autre part de mettre en valeur le fait que dans tous les résultats de ce chapitre on n'utilisera que peu de propriétés sur la variable, simplement le fait qu'on sait en définir les puissances, les multiplier par un élément du corps $\mathbb{K}$, et les additionner.

Ainsi on a intérêt à voir un polynôme comme un nouvel objet et pas comme une fonction. Pour satisfaire notre soif de rigueur, il faut donc définir proprement ce nouvel objet, comme il avait fallu définir ce nombre i dont le carré vaut -1. Ici il faut donner un sens à l'indéterminée X. En fait, ce X n'est qu'une notation. L'information importante dans l'expression (5.1) est la famille de coefficients $a_0, \dots, a_n \in \mathbb{K}$. Ainsi on pourrait simplement voir un polynôme comme un élément de $\mathbb{K}^{n+1}$. Le problème est que l'entier n dépend lui aussi du polynôme. En effet, un polynôme est donné par un nombre fini mais quelconque de coefficients non nuls. Ainsi on voit plutôt un polynôme comme une suite d'éléments de $\mathbb{K}$ dont seul un nombre fini de coefficients sont non nuls :

Définition. On note $\mathbb{K}[X]$ l'ensemble des suites $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulles à partir d'un certain rang (il existe $N \in \mathbb{N}$ tel que $a_k = 0$ pour tout $k \geqslant N$). Les éléments de $\mathbb{K}[X]$ sont appelés polynômes à une indéterminée sur le corps $\mathbb{K}$.

5.1.2 Structure de l'ensemble des polynômes

Définition. On définit sur $\mathbb{K}[X]$ les opérations suivantes :

- Addition : Pour $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ dans $\mathbb{K}[X]$ on pose $P+Q = (a_k+b_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$.
- Multiplication externe : Pour $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ on pose $\lambda\cdot P = (\lambda a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$.
- Multiplication interne : Pour $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ dans $\mathbb{K}[X]$ on pose $PQ = (c_k)_{k\in\mathbb{N}}$ où pour tout $k \in \mathbb{N}$ on a
$$c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

On peut vérifier que ces trois définitions définissent bien des fonctions de $\mathbb{K}[X] \times \mathbb{K}[X]$ dans $\mathbb{K}[X]$, de $\mathbb{K} \times \mathbb{K}[X]$ dans $\mathbb{K}[X]$ et de $\mathbb{K}[X] \times \mathbb{K}[X]$ dans $\mathbb{K}[X]$, respectivement.

On peut vérifier que l'ensemble $\mathbb{K}[X]$ muni de l'addition précédente est un groupe commutatif, dont l'élément neutre est le polynôme $(0, 0, 0, 0, \dots)$. La multiplication est associative et commutative, et le polynôme $(1, 0, 0, 0, \dots)$ est élément neutre. En outre on a la distributivité du produit par rapport à l'addition :

$$\forall P, Q, R \in \mathbb{K}[X], \quad P(Q + R) = PQ + PR.$$

⚠ $\mathbb{K}[X]$ muni de son addition et de sa multiplication interne n'est pas un corps, car tout élément non nul n'admet pas d'inverse pour la multiplication (voir la proposition 5.11). Par contre, les propriétés déjà évoquées assurent que c'est ce qu'on appelle un *anneau commutatif*.

Outre ces propriétés concernant l'addition et la multiplication interne, la multiplication externe se comporte également comme on pouvait espérer :

- Pour tout $P \in \mathbb{K}[X]$ on a $1_{\mathbb{K}}P = P$ (où on a noté $1_{\mathbb{K}}$ l'élément unité du corps $\mathbb{K}$).
- Pour $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ on a $\lambda(P + Q) = \lambda P + \lambda Q$.
- Pour $P \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$ on a $(\lambda + \mu)P = \lambda P + \mu P$.
- Pour $P \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$ on a $\lambda(\mu P) = (\lambda\mu)P$.
- Pour $P, Q \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$ on a $\lambda(PQ) = (\lambda P)Q + (\lambda Q)P$.

Toutes les propriétés évoquées font de $\mathbb{K}[X]$ muni de ses trois opérations une $\mathbb{K}$-*algèbre commutative*. À ce stade il n'est pas nécessaire de connaître tout ce vocabulaire, on peut simplement retenir que les calculs se passent bien comme pense, sans oublier qu'un polynôme n'a pas d'inverse en général.

Pour $\lambda \in \mathbb{K}$ on note $\lambda \in \mathbb{K}[X]$ le polynôme $(\lambda, 0, 0, 0, \dots)$. On note également $X \in \mathbb{K}[X]$ le polynôme $(0, 1, 0, 0, \dots)$. Pour tout $n \in \mathbb{N}$ on a alors

$$X^n = (0, \dots, 0, 1, 0, 0, \dots)$$

(où le 1 est le coefficient d'indice n, en $(n+1)^{\text{ième}}$ position). Ainsi pour tout $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$ on a

$$(a_0, \dots, a_n, 0, 0, \dots) = \sum_{k=0}^{n} a_k X^k.$$

En outre pour $n, m \in \mathbb{N}$ on a $X^n X^m = X^{n+m}$, donc tous les calculs vont bien se passer conformément à ce que la notation suggère. Ouf !

✎ ***Exercice* 5.36** On considère $P = 4X^3 + 2X^2 - X + 3$ et $Q = X^2 + X + 1$. Calculer $P + Q$ et PQ.

Une fois cette construction rigoureuse effectuée, on n'utilisera quasiment plus jamais la notation sous forme de suite pour un polynôme, mais toujours la notation (5.1).

Définition 5.1. On appelle monôme un polynôme de la forme $a_n X^n$ avec $n \in \mathbb{N}$ et $a_n \in \mathbb{K}^*$.

5.1.3 Fonctions polynômiales

On a vu qu'un polynôme n'est pas une fonction, et que l'indéterminée n'est pas une variable. Ceci dit, le but est tout de même de remplacer cette indéterminée par quelque chose de plus « concret ». Et même si on a tout fait pour pouvoir remplacer l'indéterminée par des objets de natures diverses, le premier cas que l'on veut englober est celui où on remplace l'indéterminée par un élément de $\mathbb{K}$ (un réel si on considère un polynôme à coefficients réels, un complexe si on considère un polynôme à coefficients complexes, etc.).

Définition 5.2. Soit $P = \sum_{k=0}^{n} a_k X_k \in \mathbb{K}[X]$, avec $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$. Alors on associe à P la *fonction polynômiale*

$$\left\{ \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & P(x) = \sum_{k=0}^{n} a_k x^k \end{array} \right.$$

On peut vérifier que l'application qui à un polynôme associe la fonction polynômiale associée est un morphisme de $\mathbb{K}$-algèbre, dans le sens où toutes la structure est bien préservée (la fonction associée à la somme de deux polynômes est la somme des deux fonctions associées à chacun des deux polynômes, etc.). On ne s'attarde pas sur ces considérations ici.

Bien entendu l'intérêt de l'abstraction est, comme on l'a dit, de définir des fonctions sur tout espace dans lequel une expression polynômiale à coefficients dans $\mathbb{K}$ a un sens. Par exemple à un polynôme dans $\mathbb{K}[X]$ on peut associer une fonction sur $\mathbb{K}$ mais aussi sur l'espaces des fonctions de $\mathbb{K}$ dans $\mathbb{K}$ (ou de $\mathbb{K}^n$ dans $\mathbb{K}^n$), mais aussi sur les matrices $n \times n$ à coefficients dans $\mathbb{K}$ ou … sur $\mathbb{K}[X]$.

Exemple 5.3. On considère le polynôme $P(X) = X^3 + 4X + 2 \in \mathbb{R}[X]$. On considère sur $\mathbb{R}$ la fonction f qui à x associe $\cos(x)$. Enfin on considère le polynôme $Q(X) = X + 1 \in \mathbb{R}[X]$. Alors on a

- $P(5) = 5^3 + 4 \times 5 + 2 = 147$,
- $P(f) : x \mapsto \cos(\cos(\cos(x))) + 4\cos(x) + 2$ (c'est, comme f, une fonction de $\mathbb{R}$ dans $\mathbb{R}$),
- $P(Q) = P \circ Q = Q^3 + 4Q + 2 = (X+1)^3 + 4(X+1) + 2 = X^3 + 3X^2 + 7X + 7$ (c'est, comme Q, un polynôme de $\mathbb{R}[X]$).

5.2 Degré d'un polynôme et premières applications

Définition 5.4. Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Il existe $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$ tels que $a_n \neq 0$ et $P = \sum_{k=0}^{n} a_k X^k$.

(i) On appelle alors *degré* de P et on note $\deg(P)$ l'entier n (par convention, le degré du polynôme nul est $-\infty$).

(ii) Le coefficient a_n est appelé *coefficient dominant* de P.

(iii) Le terme $a_n X^n$ est appelé *terme dominant* de P.

Exemples 5.5. On a $\deg(2) = 0$, $\deg(1 + X + X^3) = 3$, $\deg(X^4 + X^6 - X^2) = 6$.

Définition 5.6. Soit $n \in \mathbb{N}$. On note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degrés au plus n. Les éléments de $\mathbb{K}_0[X]$ sont appelés polynômes constants.

On commence par étudier les propriétés du degré vis-à-vis des opérations sur les polynômes.

Proposition 5.7. *Soit $(P, Q) \in \mathbb{K}[X]^2$.*

(i) On a

$$\deg(P+Q) \leqslant \max\big(\deg(P), \deg(Q)\big).$$

En outre l'inégalité est stricte si et seulement si P et Q ont même degré et des coefficients dominants opposés.

(ii) On a

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

Plus précisément, si P et Q sont non nuls alors le terme dominant de PQ est le produit des termes dominants de P et Q.

(iii) Si $Q \neq 0$ on a

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

Exemples 5.8. On note $P(X) = -X^3 + 2X - 1$ et $Q(X) = 2X^2 + X$. On a $\deg(P) = 3$ et $\deg(Q) = 2$. On a alors

$$\deg(P+Q) = \deg(-X^3 + 2X^2 + 3X - 1) = 3 = \max(\deg(P), \deg(Q)),$$

$$\deg(PQ) = \deg(-2X^5 - X^4 + 4X^3 - X) = 5 = \deg(P) + \deg(Q),$$

$$\begin{aligned}\deg(P(Q)) &= \deg(-(2X^2+X)^3 + 2(X^2+X) - 1)\\ &= \deg(-8X^6 - 12X^5 - 6X^4 - X^3 + 4X^2 + 2X - 1)\\ &= 6 = \deg(P)\deg(Q),\end{aligned}$$

$$\begin{aligned}\deg(Q(P)) &= \deg(2(-X^3 + 2X - 1)^2 - X^3 + 2X - 1)\\ &= \deg(2X^6 - 8X^4 + 3X^3 + 8X^2 - 6X + 1)\\ &= 6 = \deg(Q)\deg(P).\end{aligned}$$

Démonstration. On note $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{m} b_k X^k$, avec $a_0, \dots, a_n \in \mathbb{K}$, $a_n \neq 0$, $b_0, \dots, b_m \in \mathbb{K}$ et $b_m \neq 0$. En particulier $\det(P) = n$ et $\det(Q) = m$.

On a

$$(P+Q) = \sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{m} b_k X^k.$$

Si $n > m$ le terme de plus haut degré est $a_n X^n$ et $\deg(P+Q) = n$. De même, si $n < m$ alors le terme de plus haut degré est $b_m X^m$ donc $\deg(P+Q) = m$. Si $n = m$ et $a_n + b_m \neq 0$ alors le terme de plus haut degré est $(a_n + b_m)X^n$ et $\deg(P+Q) = n = m$. Si $n = m$ et $a_n + b_m = 0$ alors tous les termes sont des monomes de degrés strictement inférieurs à $n = m$, donc $\deg(P+Q) < n = m$.

Soit $\lambda \in \mathbb{K}$. On a

$$\lambda P = \sum_{k=0}^{n} \lambda a_k X^k,$$

donc $\deg(\lambda P) = \deg(P)$ (c'est le cas particulier de la propriété sur le produit dans le cas où l'un des deux polynômes est constant non nul). On a alors

$$PQ = \sum_{\substack{0 \leqslant j \leqslant n \\ 0 \leqslant k \leqslant m}} a_j b_k X^{j+k}.$$

En particulier, puisque $a_n b_m \neq 0$, le terme dominant de PQ est $a_n b_m X^{n+m}$ et donc PQ est de degré $n+m$. Enfin

$$P(Q) = \sum_{k=0}^{m} b_k P^k$$

Puisque $b_m P^m$ est de degré nm et que les autres termes sont de degrés strictement inférieurs, on obtient bien que $\deg(P(Q)) = nm$. □

L'analyse du produit de deux polynômes assure en particulier que le produit de deux polynômes non nuls est non nul. Par contraposée, on a aussi le résultat suivant :

Proposition 5.9. *Soient $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$. Alors $P = 0$ ou $Q = 0$.*

Cette propriété est usuelle pour le produit de réels ou de complexes, mais on rappelle qu'elle n'est pas automatique (la composée de deux fonctions non nulles peut être nulle, le produit de deux matrices non nulles peut être nul, etc.).

Corollaire 5.10. *Soit $(P_1, P_2, Q) \in \mathbb{K}[X]^3$. On suppose que $P_1 Q = P_2 Q$ avec $Q \neq 0$. Alors $P_1 = P_2$.*

Démonstration. On a $(P_1 - P_2)Q = 0$ et $Q \neq 0$, donc d'après la proposition 5.9 on a $P_1 - P_2 = 0$. □

On peut voir la proposition 5.9 comme conséquence du fait que si Q est non nul, alors le degré du produit PQ est supérieur ou égal à celui de P. On utilise encore cette propriété pour étudier les éléments inversibles de $K[X]$ ($P \in \mathbb{K}[X]$ est inversible s'il existe $Q \in \mathbb{K}[X]$ tel que $PQ = 1$).

Proposition 5.11. *L'ensemble des polynômes qui admettent un inverse est l'ensemble des polynômes constants non nuls (c'est-à-dire les polynômes de degré 0).*

Démonstration. Si $P = 0$ alors P n'a pas d'inverse. Si $P = \lambda$ avec $\lambda \in \mathbb{K}^*$ alors P est inversible d'inverse $\frac{1}{\lambda}$. Enfin si $\deg(P) \geqslant 1$ et $Q \in \mathbb{K}[X]$ on a $PQ = 0$ si $Q = 0$ et $\deg(PQ) = \deg(P) + \deg(Q) \geqslant 1$ sinon. Ainsi P n'est pas inversible. □

5.3 Division euclidienne dans $\mathbb{K}[X]$

Définition 5.12. Soient $P, Q \in \mathbb{K}[X]$. On dit que Q divise P et on note $Q|P$ s'il existe $R \in \mathbb{K}[X]$ tel que $P = QR$.

Remarque 5.13. Si $Q|P$ alors $\deg(Q) \leqslant \deg(P)$.

Remarque 5.14. Soient $(P, Q) \in \mathbb{K}[X]^2$ et $(\lambda, \mu) \in (\mathbb{K}^*)^2$. Alors Q divise P si et seulement si μQ divise λP.

On a vu que, comme dans $\mathbb{Z}$, tous les éléments de $\mathbb{K}[X]$ ne sont pas inversibles. De même qu'on ne peut pas « diviser dans $\mathbb{Z}$ », on ne peut donc pas « diviser dans $\mathbb{K}[X]$ ». Mais, comme dans $\mathbb{Z}$, on peut faire dans $\mathbb{K}[X]$ des divisions euclidiennes.

La division euclidienne dans $\mathbb{Z}$ est la « division du CM2 ». Par exemple, 13 n'est pas divisible par 3 (autrement dit, il n'existe pas d'entier q tel que $3q$ vaut 13), mais on peut dire que que dans 13 il y a 4 fois 3, et qu'il reste 1. Soit $13 = 4 \times 3 + 1$. On peut aussi écrire que $13 = 3 \times 3 + 4$, ou encore que $13 = 5 \times 3 - 2$. Le critère pour le reste de la division par 3 est d'être compris entre 0 et 2.

Le théorème de division euclidienne dans $\mathbb{Z}$ est le suivant :

Théorème 5.15. *Soit $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que*

$$a = bq + r \quad et \quad 0 \leqslant r < |b|\,.$$

Le quotient q et le reste r peuvent être calculés par l'algorithme étudié à l'école primaire. On effectue par exemple la division euclidienne de 4096 par 23.

```
 4096 | 23
-23   | 178
 179
-161
  186
 -184
    2
```

La première étape consiste à voir combien de fois on peut retrancher 23 à 40 (on fait la division euclidienne de 40 par 23). On obtient 1, et il reste 17. Plus précisémment, on regarde combien de fois on peut retrancher 23×100 à 4096 (on fait la division euclidienne de 4096 par 2300). On retranche 2300, ce qui revient à écrire :

$$4096 = 23 \times 100 + 1796.$$

Selon la terminologie du CM2, on « abaisse le 9, et on se demande combien de fois on peut retrancher 23 à 179. On trouve 7, et il reste 18. On abaisse le 6, on voit qu'on peut retrancher 8 fois 23 à 186 et il reste 2. Finalement, le quotient et le reste de la division euclidienne de 4096 par 23 sont respectivement 178 et 2 (qui est bien compris entre 0 et 22). Les étapes du calculs pourraient s'écrire de la façon suivante :

$$\begin{aligned} 4096 &= 23 \times 100 + 1796 \\ &= 23 \times 170 + 186 \\ &= 23 \times 178 + 2. \end{aligned}$$

On fait exactement la même chose pour les polynômes. Faute de pouvoir diviser n'importe quel polynôme par n'importe quel autre, on le fait à un reste près, ce reste étant le plus « petit » possible. On n'a pas introduit de comparaison entre les polynômes. Le critère sur le reste pour être le plus simple possible est d'avoir le plus petit degré possible. Le théorème est le suivant :

Théorème 5.16. *Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$. Alors il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ tel que*

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

L'algorithme pour trouver le quotient et le reste est analogue à celui dans $\mathbb{Z}$. On effectue par exemple dans $\mathbb{R}[X]$ la division euclidienne de $A(X) = X^5 + X^4 - X^3 + X^2 - 2X + 1$ par $B(X) = 2X^2 - X + 1$.

$$\begin{array}{r|l}
X^5 + X^4 - X^3 + X^2 - 2X + 1 & 2X^2 - X + 1 \\
\cline{2-2}
-(X^5 - \frac{1}{2}X^4 + \frac{1}{2}X^3) & \frac{1}{2}X^3 + \frac{3}{4}X^2 - \frac{3}{8}X - \frac{1}{16} \\
\cline{1-1}
\frac{3}{2}X^4 - \frac{3}{2}X^3 + X^2 & \\
-(\frac{3}{2}X^4 - \frac{3}{4}X^3 + \frac{3}{4}X^2) & \\
\cline{1-1}
-\frac{3}{4}X^3 + \frac{1}{4}X^2 - 2X & \\
-(-\frac{3}{4}X^3 + \frac{3}{8}X^2 - \frac{3}{8}X) & \\
\cline{1-1}
-\frac{1}{8}X^2 - \frac{13}{8}X + 1 & \\
-(-\frac{1}{8}X^2 + \frac{1}{16}X - \frac{1}{16}) & \\
\cline{1-1}
-\frac{37}{16}X + \frac{17}{16} &
\end{array}$$

La première étape consiste à retrancher à A le produit de B avec un monôme de sorte que le reste soit de degré strictement inférieur à celui de A. Pour déterminer ce monôme, il suffit de regarder les termes dominants (grosso modo, on « divise » le terme dominant de A par celui de B). On obtient alors

$$A(X) = B(X)\frac{X^3}{2} + \left(\frac{3X^4}{2} - \frac{3X^3}{2} + X^2 - 2X + 1\right).$$

On procède de même avec ce reste :

$$A(X) = B(X)\frac{X^3}{2} + B(X)\frac{3X^2}{4} + \left(-\frac{3X^3}{4} + \frac{X^2}{4} - 2X + 1\right).$$

Et ainsi de suite, jusqu'à ce que le reste ait un degré strictement inférieur à celui de B. On obtient finalement :

$$A(X) = B(X)\left(\frac{X^3}{2} + \frac{3X^2}{4} - \frac{3X}{8} - \frac{1}{16}\right) + \left(-\frac{37}{16}X + \frac{17}{16}\right).$$

La démonstration du théorème 5.16 suit cet algorithme de calcul pour obtenir l'existence du couple (Q,R).

Démonstration du théorème 5.16. • On commence par prouver l'existence. On montre par récurrence sur $m \in \mathbb{N}$ qu'un tel couple (Q,R) existe si

$$\deg(A) < \deg(B) + m$$

(on rappelle que $\deg(A)$ peut être $-\infty$). Pour $m = 0$, on prend simplement $(Q,R) = (0,A)$. On suppose maintenant l'existence acquise si $\deg(A) < \deg(B) + m$ pour un certain $m \in \mathbb{N}$, et on considère A et B tels que $\deg(A) = \deg(B) + m$. On note

$$A = \sum_{k=0}^{n} a_k X^k \quad \text{et} \quad B = \sum_{k=0}^{n-m} b_k X^k,$$

avec $n = \deg(A) \in \mathbb{N}$, $a_0, \dots, a_n, b_0, \dots, b_{n-m} \in \mathbb{K}$, $a_n \neq 0$, $b_{n-m} \neq 0$. On considère

$$\tilde{A} = A - \frac{a_n}{b_{n-m}} X^m B.$$

On a alors $\deg(\tilde{A}) < \deg(A)$, donc par hypothèse de récurrence il existe $\tilde{Q}, \tilde{R} \in \mathbb{K}[X]$ tels que $\deg(\tilde{R}) < \deg(B)$ et $\tilde{A} = B\tilde{Q} + \tilde{R}$. On a alors

$$A = B\left(\frac{a_n}{b_{n-m}} X^m + \tilde{Q}\right) + \tilde{R}.$$

Il suffit alors de poser $Q = \frac{a_n}{b_{n-m}} X^m + \tilde{Q}$ et $R = \tilde{R}$.

• On montre maintenant l'unicité du couple (Q, R). On suppose que $Q_1, Q_2, R_1, R_2 \in \mathbb{K}[X]$ sont tels que d'une part

$$A = BQ_1 + R_1 \quad \text{et} \quad \deg(R_1) < \deg(B),$$

et d'autre part

$$A = BQ_2 + R_2 \quad \text{et} \quad \deg(R_2) < \deg(B).$$

On a alors

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

donc

$$\deg(B) + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg(B)$$

Cela prouve que $\deg(Q_1 - Q_2) < 0$, donc $Q_1 = Q_2$, et par suite que $R_1 = R_2$. □

5.4 Racines d'un polynôme

5.4.1 Racines distinctes

Définition 5.17. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. On dit que a est une racine de P si $P(a) = 0$.

Proposition 5.18. *Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. Alors a est une racine de P si et seulement si $X - a$ divise P.*

Démonstration. • On suppose que $X - a$ divise P. Cela signifie qu'il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)Q$. On a alors

$$P(a) = (a - a)Q(a) = 0,$$

donc a est une racine de P.

• On suppose maintenant que a est racine de P. On effectue la division euclidienne de P par $X - a$. Il existe $Q, R \in \mathbb{K}[X]$ tels que $P = (X - a)Q + R$ avec $\deg(R) < \deg(X - a) = 1$. Cela implique que R est constant, donc il existe $\lambda \in \mathbb{K}$ tel que $R = \lambda$. On a alors

$$0 = P(a) = (a - a)Q(a) + \lambda,$$

donc $\lambda = 0$. Ainsi $P = (X - a)Q$, ce qui signifie que $X - a$ divise P. □

Proposition 5.19. *Soit $P \in \mathbb{K}[X]$. Soient $a_1, \dots, a_n$ des éléments de $\mathbb{K}$ deux à deux disjoints (avec $n \in \mathbb{N}^*$). Alors on a*

$$\big(\forall j \in [\![1, n]\!],\ a_j \text{ est racine de } P\big) \iff \prod_{j=1}^{n} (X - a_j) \text{ divise } P.$$

Démonstration. On suppose que $\prod_{j=1}^{n}(X-a_j)$ divise P. Il existe $Q \in \mathbb{K}[X]$ tel que $P(X) = Q(X)\prod_{j=1}^{n}(X-a_j)$. En particulier pour tout $k \in [\![1,n]\!]$ on a

$$P(a_k) = Q(a_k)\prod_{j=1}^{n}(a_k-a_j) = 0,$$

donc a_k est racine de P. Inversement on montre par récurrence sur $n \in \mathbb{N}^*$ que si $a_1,\dots,a_n$ sont deux à deux distincts et tels que $P(a_1) = \cdots = P(a_n) = 0$ alors $\prod_{j=1}^{n}(X-a_j)$ divise P. Pour $n=1$, c'est la proposition précédente. On suppose maintenant le résultat acquis jusqu'au rang $n-1$ ($n \geqslant 2$) et on le montre au rang n. Par hypothèse de récurrence il existe $\tilde{Q} \in \mathbb{K}[X]$ tel que

$$P(X) = \tilde{Q}(X)\prod_{j=1}^{n-1}(X-a_j).$$

Puisque a_n est également racine de P on a

$$0 = P(a_n) = \tilde{Q}(a_n)\underbrace{\prod_{j=1}^{n-1}(a_n-a_j)}_{\neq 0},$$

donc $\tilde{Q}(a_n) = 0$. Il existe donc $Q \in \mathbb{K}[X]$ tel que $\tilde{Q} = (X-a_n)Q(X)$. On a alors

$$P(X) = Q(X)\prod_{j=1}^{n}(X-a_j).$$

D'où le résultat. □

Proposition 5.20. *Si $P \in \mathbb{K}[X]$ est de degré $n \in \mathbb{N}$, alors P admet au plus n racines distinctes. De façon équivalente, si $P \in \mathbb{K}[X]\setminus\{0\}$ admet au moins n racines distinctes alors* $\deg(P) \geqslant n$.

Démonstration. On suppose que P admet n racines distinctes $a_1,\dots,a_n \in \mathbb{K}$. D'après la proposition précédente il existe $Q \in \mathbb{K}[X]$ tel que

$$P = Q\prod_{j=1}^{n}(X-a_j).$$

Comme $P \neq 0$ on a $Q \neq 0$ donc

$$\deg(P) = \underbrace{\deg(Q)}_{\geqslant 0} + \underbrace{\deg\left(\prod_{j=1}^{n}(X-a_j)\right)}_{=n} \geqslant n.$$

□

Corollaire 5.21. *Soit $n \in \mathbb{N}$.*

(i) Si $P \in \mathbb{K}_n[X]$ admet au moins $n+1$ racines distinctes alors $P = 0$.

(ii) Soient $P_1, P_2 \in \mathbb{K}_n[X]$. Si les fonctions polynomiales associées prennent des valeurs égales en au moins $n+1$ points distincts alors $P_1 = P_2$.

Corollaire 5.22. *(i) Si $P \in \mathbb{K}[X]$ admet une infinité de racines distinctes alors $P = 0$.*

(ii) Soient $P_1, P_2 \in \mathbb{K}[X]$. Si les fonctions polynomiales associées prennent des valeurs égales en une infinité de points distincts alors $P_1 = P_2$.

L'intérêt du corollaire 5.22 par rapport au corollaire 5.21 est qu'on n'a pas besoin d'information sur les degrés des polynômes pour conclure. Le prix à payer est qu'on a besoin d'une infinité de racines. Mais une infinité de racines ce n'est pas tant que ça, et cela reste un résultat très important. Par exemple, il suffit de savoir que deux polynômes complexes coïncident sur les réels (ou même seulement sur les entiers) par savoir qu'ils sont égaux.

Définition 5.23. On dit d'un polynôme qu'il est scindé s'il peut s'écrire comme produit de polynômes de degré 1. Autrement dit, $P \in \mathbb{K}[X]$ si et seulement s'il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$ et $a_1, \dots, a_n \in \mathbb{K}$ tels que

$$P = \lambda \prod_{j=1}^{n} (X - a_j).$$

Remarque 5.24. Avec les notations précédentes, les racines de P (éventuellement répétées) sont $a_1, \dots, a_n$.

Proposition 5.25. *Si P est de degré $n \in \mathbb{N}^*$ et admet n racines distinctes, alors P est scindé.*

Démonstration. On note $a_1, \dots, a_n$ les racines de P. Alors $\prod_{j=1}^{n}(X - a_j)$ divise P. Ainsi il existe $Q \in \mathbb{K}[X]$ tel que

$$P = Q \prod_{j=1}^{n} (X - a_j).$$

On a nécessairement $\deg(Q) = 0$, donc il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda$. □

Remarque 5.26. Attention la réciproque n'est pas vraie. Le polynôme $(X-1)^4$ est scindé mais n'admet qu'une seule racine

Exemple 5.27. Pour tout $n \in \mathbb{N}^*$, $X^n - 1$ est scindé. Plus précisément on a

$$X^n - 1 = \prod_{k=1}^{n} \left(X - e^{\frac{2ik\pi}{n}}\right).$$

5.4.2 Dérivées d'un polynômes

Dans ce paragraphe, on suppose que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Définition 5.28. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ (avec $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$). On appelle polynôme dérivée de P le polynôme

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

On note alors $P^{(k)}$ les dérivées successives de P

Proposition 5.29. *(i) Si $\mathbb{K} = \mathbb{R}$ et f est la fonction polynômiale associée à P, alors f' est la fonction polynomiale associée à P'.*

(ii) Si $\deg(P) \in \mathbb{N}^*$ alors $\deg(P') = \deg(P) - 1$.

(iii) *Si* $\deg(P) = n \in \mathbb{N}$ *alors* $P^{(n+1)} = 0$.

(iv) *Si* $P = X^n$ *avec* $n \in \mathbb{N}$, *alors* $P^{(n)} = n!$.

(v) *Pour* $P, Q \in \mathbb{K}[X]$ *on a* $(P+Q)' = P' + Q'$.

(vi) *Pour* $P \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$ *on a* $(\lambda P)' = \lambda P'$.

(vii) *Pour* $P, Q \in \mathbb{K}[X]$ *on a* $(PQ)' = P'Q + PQ'$.

(viii) *Pour* $P, Q \in \mathbb{K}[X]$ *et* $n \in \mathbb{N}^*$ *on a* $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$.

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. Pour $m \in \mathbb{N}$ on a

$$P^{(m)}(0) = \begin{cases} 0 & \text{si } m > n, \\ a_m m! & \text{si } m \in [\![0, n]\!]. \end{cases}$$

En particulier pour tout $k \in [\![0, n]\!]$ on a

$$a_k = \frac{P^{(k)}(0)}{k!}.$$

On peut donc écrire

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k. \tag{5.2}$$

Soit $a \in \mathbb{K}$. En appliquant cette formule au polynôme $Q(X) = P(X + a)$ on obtient

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

En composant avec le polynôme $X - a$ on obtient le résultat suivant :

Proposition 5.30 (Formule de Taylor)**.** *Soit* $P \in \mathbb{K}[X]$ *un polynôme de degré* $n \in \mathbb{N}$ *et* $a \in \mathbb{K}$. *Alors on a*

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

5.4.3 Ordres de multiplicité des racines d'un polynôme

Définition 5.31. Soient $K \in \mathbb{K}[X] \setminus \{0\}$ et $a \in \mathbb{K}$. On suppose que a est racine de P. On appelle ordre de multiplicité de la racine a dans P le plus grand entier $k \in \mathbb{N}^*$ tel que $(X - a)^k$ divise P.

Une racine d'ordre 1 est appelée racine simple, une racine d'ordre 2 est appelé racine double et une racine d'ordre $\geqslant 2$ est appelée racine multiple.

Proposition 5.32. *Soient* $P \in \mathbb{K}[X] \setminus \{0\}$, $a \in \mathbb{K}$ *et* $k \in \mathbb{N}^*$. *Alors* a *est une racine d'ordre de multiplicité* k *dans* P *si et seulement si*

$$P(a) = P'(a) = \cdots = P^{(k-1)}(a) = 0 \quad et \quad P^{(k)}(a) \neq 0.$$

Démonstration. On suppose que a est racine d'ordre de multiplicité k. Alors il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)^k Q$ et $Q(a) \neq 0$. D'après la règle de Leibniz on a pour $j \in [\![0, k]\!]$

$$P^{(j)} = \sum_{i=1}^{j} C_j^i k(k-1)\dots(k-i+1)(X-a)^{k-i} Q^{(j-i)}$$

Pour $j \in [\![0, k-1]\!]$ on a donc $P^{(j)}(a) = 0$, tandis que pour $j = k$ on obtient $P^{(k)}(a) = k!Q(a) \neq 0$.

Inversement on suppose que $P^{(j)}(a) = 0$ pour tout $j \in [\![0, k-1]\!]$ et que $P^{(k)}(a) \neq 0$. On note $n = \deg(P)$. D'après la formule de Taylor en a on a

$$P = \sum_{j=0}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^j = \sum_{j=k}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^j = (X-a)^k \underbrace{\sum_{j=k}^{n} \frac{P^{(j)}(a)}{j!}(X-a)^{j-k}}_{=Q}.$$

On a $Q(a) = \frac{P^{(k)}(a)}{k!} \neq 0$ donc $(X-a)^k$ divise P mais pas $(X-a)^{k+1}$. □

Proposition 5.33. *Soit $P \in \mathbb{K}[X]$. On suppose que $a_1, \dots, a_k$ sont des racines deux à deux distinctes de P, d'ordres de multiplicité $\alpha_1, \dots, \alpha_k$ respectivement. Alors $\prod_{j=1}^{k}(X-a_j)^{\alpha_j}$ divise P. En particulier P est au moins de degré $\alpha_1 + \cdots + \alpha_k$. Ainsi, si P est de degré $n \in \mathbb{N}$, alors P admet au plus n racines comptées avec multiplicités.*

Démonstration. Montrons par récurrence sur $m \in [\![1, k]\!]$ que

$$\prod_{j=1}^{m}(X-a_j)^{\alpha_j} \mid P. \tag{5.3}$$

Pour $m = 1$ c'est vrai par définition. Supposons donc le résultat acquis jusqu'au rang $m-1$ (pour $m \in [\![2, k]\!]$). Il existe $Q \in \mathbb{K}[X]$ tel que

$$P = \prod_{j=1}^{m-1}(X-a_j)^{\alpha_j} Q.$$

Notons β l'ordre de multiplicité de la racine a_m dans Q (on note $\beta = 0$ si a_m n'est pas racine de Q). Alors il existe $\tilde{Q} \in \mathbb{K}[X]$ tel que $\tilde{Q}(a_m) \neq 0$ et

$$P = (X-a_1)^{\alpha_1} \dots (X-a_{m-1})^{\alpha_{m-1}}(X-a_m)^{\beta}\tilde{Q}.$$

Supposons par l'absurde que $\beta < \alpha_m$. On note

$$R_1 = (X-a_m)^{\beta} \quad \text{et} \quad R_2 = (X-a_1)^{\alpha_1} \dots (X-a_{m-1})^{\alpha_{m-1}}\tilde{Q}.$$

On a alors

$$0 = P^{(\beta)}(a_m) = (R_1R_2)^{(\beta)}(a_m) = \sum_{i=0}^{\beta} C_{\beta}^{i} R_1^{(i)}(a_m) R_2^{(\beta-i)}(a_m) = \beta! R_2(a_m) \neq 0.$$

D'où la contradiction. D'où (5.3) par récurrence. Les autres assertions s'obtiennent en analysant les degrés. □

5.5 Arithmétique dans $\mathbb{K}[X]$

5.5.1 PGCD, PPCM, théorème de Bézout

Définition 5.34. On dit que deux polynômes P et Q sont premiers entre eux si les seuls diviseurs communs à P et Q sont les polynômes constants non nuls.

***Exercice* 5.37** Montrer que les polynômes X^2-4X+4 et X^2-4X+3 sont premiers entre eux dans $\mathbb{R}[X]$.

Proposition-Définition 5.35. Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. Alors il existe un unique polynôme unitaire D dans $\mathbb{K}[X]$ tel que

$$\begin{cases} D|A \text{ et } D|B, \\ \forall P \in \mathbb{K}[X], \quad \big(P|A \text{ et } P|B\big) \implies P|D. \end{cases} \tag{5.4}$$

D est appelé plus grand commun diviseur de A et B et est noté $\mathsf{pgcd}(A,B)$.

En outre il existe $(U,V) \in \mathbb{K}[X]^2$ tel que

$$D = AU + BV. \tag{5.5}$$

Démonstration. On note $\mathcal{D}$ l'ensemble des polynômes de $\mathbb{K}[X]$ qui s'écrive sous la forme $AU+BV$ avec $(U,V) \in \mathbb{K}[X]^2$. Cet ensemble n'est pas réduit à 0 car il contient A et B. On note alors

$$n = \min\left\{\deg(P), P \in \mathcal{D} \setminus \{0\}\right\}.$$

On considère un polynôme D de $\mathcal{D}$ de degré n. Quitte à le diviser par son coefficient dominant (il reste bien dans $\mathcal{D}$), on peut supposer qu'il est unitaire. Comme D est dans $\mathcal{D}$, il existe $(U,V) \in \mathbb{K}[X]^2$ tel que (5.5) est vérifiée.

Montrons que D vérifie (5.4). On commence par vérifier que D divise A. On note Q et R le quotient et le reste de la division euclidienne de A par D. On suppose par l'absurde que $R \neq 0$. On a

$$R = A - DQ = (1-U)A - VB,$$

ce qui prouve que R appartient à $\mathcal{D}$. Mais son degré est strictement inférieur à celui de D, ce qui est absurde. Ainsi $A = QD$, ce qui signifie que D divise A. On montre de la même façon que D divise B.

Soit $P \in \mathbb{K}[X]$ un diviseur commun de A et B. Il existe $(Q_A, Q_B) \in \mathbb{K}[X]^2$ tel que $A = PQ_A$ et $B = PQ_B$. On a alors

$$D = AU + BV = P(Q_A U + Q_B V),$$

donc P divise D. Ainsi on a montré que D vérifie (5.4).

Il reste à montrer que D est l'unique polynôme unitaire vérifiant (5.4). Pour cela, supposons que $\tilde{D}$ est également un polynôme unitaire vérifiant (5.4). Comme $\tilde{D}$ divise A et B, on obtient par propriété de D que $\tilde{D}$ divise D. On obtient de la même façon que D divise $\tilde{D}$. Comme D et $\tilde{D}$ sont unitaires, on a nécessairement $D = \tilde{D}$, ce qui conclut la démonstration. □

On note que l'unicité de D assure qu'il n'y a qu'un seul polynôme unitaire de $\mathcal{D}$ de degré n.

Remarque 5.36. Soit $(A,B) \in (\mathbb{K}[X] \setminus \{0\})^2$. Alors A et B sont premiers entre eux si et seulement si $\mathsf{pgdc}(A,B) = 1$.

Proposition 5.37 (Lemme de Gauss)**.** *Soient $(A,B,C) \in \mathbb{K}[X]^3$. Si A et B sont premiers entre eux et A divise BC, alors A divise C.*

Démonstration. Il existe $(U,V) \in \mathbb{K}[X]^2$ tel que

$$AU + BV = 1.$$

En multipliant par C on obtient

$$ACU + BCV = C.$$

Sachant que A divise ACU, s'il divise BC il divise aussi BCV et donc C. □

Pour calculer explicitement le pgcd de deux polynômes A et B non nuls, on utilise l'algorithme d'Euclide. On commence par observer que si on note Q et R le quotient et le reste de la division euclidienne de A par B, alors on a

$$\mathsf{pgcd}(A, B) = \mathsf{pgcd}(B, R).$$

En effet, si P divise B et R, alors il divise $A = BQ + R$, et si P divise à la fois A et B, alors il divise $R = A - BQ$. On remarque également que si B divise A alors $\mathsf{pgcd}(A, B) = A$.

Étant donnés deux polynômes non nuls A et B de $\mathbb{K}[X]$, on obtient alors le pgcd de A et B de la façon suivante. On effectue la division euclidienne de A par B :

$$A = BQ_1 + R_1, \quad \deg(R_1) < \deg(B).$$

On effectue alors la division euclidienne de B par le reste R_1 :

$$B = Q_2R_1 + R_2, \quad \deg(R_2) < \deg(R_1).$$

Puis la division euclidienne de R_1 par R_2, et ainsi de suite :

$$R_{k-1} = Q_{k+1}R_k + R_{k+1}, \quad \deg(R_{k+1}) < \deg(R_k).$$

Jusqu'au moment où on obtient un reste nul :

$$R_{p-1} = QR_p.$$

Cela arrive nécessairement. En effet, si ce n'est pas le cas, on obtient une suite de restes $(R_m)_{m\in\mathbb{N}}$, et la suite des degrés correspondants est une suite d'entiers positifs strictement décroissante, ce qui est absurde. Une fois ces calculs effectués, on observe que

$$\mathsf{pgcd}(A, B) = \mathsf{pgcd}(B, R_1) = \mathsf{pgcd}(R_1, R_2) = \cdots = \mathsf{pgcd}(R_{p-1}, R_p) = R_p.$$

Ainsi, le pgcd de A et de B est le dernier reste non nul obtenu par l'algorithme d'Euclide.

Proposition-Définition 5.38. Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$. Alors il existe un unique polynôme unitaire M dans $\mathbb{K}[X]$ tel que

$$\begin{cases} A|M \text{ et } B|M, \\ \forall P \in \mathbb{K}[X], \quad \big(A|P \text{ et } B|P\big) \implies M|P. \end{cases}$$

D est appelé plus petit commun multiple de A et B et est noté $\mathsf{ppcm}(A, B)$.

5.5.2 Factorisation en polynômes irréductibles

On sait que tout entier s'écrit de façon unique comme produit de nombres premiers. On rappelle qu'un nombre premier est un entier supérieur ou égal à 2 dont les seuls diviseurs positifs sont 1 et lui-même. En utilisant le lemme de Gauss, on montre alors que si un nombre premier p divise le produit ab de deux entiers, alors il divise a ou b. Le résultats de décomposition en facteurs premiers est le suivant :

Théorème 5.39. *Soit $n \in \mathbb{Z}$. Alors il existe $\varepsilon \in \{-1, 1\}$, $k \in \mathbb{N}$, $p_1, \ldots, p_k$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_k$ des entiers non nuls tels que*

$$n = \varepsilon p_1^{\alpha_1} \ldots p_k^{\alpha_k}.$$

En outre cette écriture est unique à l'ordre des facteurs près.

Tous ces résultats ont des analogues dans $\mathbb{K}[X]$.

Définition 5.40. On dit qu'un polynôme $P \in \mathbb{K}[X]$ est irréductible s'il est de degré supérieur ou égal à 1 et si ses seuls diviseurs unitaires sont 1 et lui-même.

Remarque 5.41. Si P n'est pas irréductible, on peut donc écrire $P = Q_1Q_2$ avec $\deg(Q_1) \geqslant 1$ et $\deg(Q_2) \geqslant 1$.

Proposition 5.42. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Soit $(A, B) \in \mathbb{K}[X]^2$. Si P divise AB alors P divise A ou P divise B.*

Démonstration. On suppose que P divise AB mais ne divise pas A. Comme P n'est pas un diviseur de A, P et A sont premiers entre eux. Par le lemme de Gauss on obtient que P divise B. □

Corollaire 5.43. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Soient $n \in \mathbb{N}^*$ et $(A_1, \dots, A_n) \in \mathbb{K}[X]^n$. Si P divise le produit $A_1 \dots A_n$ alors P divise l'un des facteurs A_j, $j \in [\![1, n]\!]$.*

Théorème 5.44. *Soit $P \in \mathbb{K}[X] \setminus \{0\}$. Alors il existe $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$, $P_1, \dots, P_n$ des polynômes irréductibes et $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ tels que*

$$P = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n}.$$

En outre cette écriture est unique à l'ordre des facteurs près.

L'idée de la démonstration est la suivante. Pour l'existence, si P est irréductible le résultat est clair. Sinon on l'écrit comme produit de deux polynômes de degrés strictement inférieurs, puis on procède de même avec ces deux facteurs, jusqu'à ce qu'on n'ait plus que des facteurs irréductibles. Cela arrive à un moment, sinon on construirait une suite de diviseurs non nuls de P de degrés de plus en plus petits, ce qui n'est pas possible.

Pour l'unicité, on suppose qu'on a une égalité entre produits de polynômes irréductibles de la forme suivante

$$\lambda P_1^{\alpha_1} \dots P_n^{\alpha_n} = \mu Q_1^{\beta_1} \dots Q_m^{\beta_m}.$$

Par identification des coefficients dominants on a $\lambda = \mu$. P_1 est irréductible. Comme il divise le produit $Q_1^{\beta_1} \dots Q_m^{\beta_m}$, il divise l'un des Q_j. Q_j étant lui même irréductible et unitaire, on a $P_1 = Q_j$. D'après le corollaire 5.10 on peut « simplifier » l'égalité par $P_1 = Q_j$. On obtient une nouvelle égalité avec un facteur de moins, et on procède de la même façon pour prouver que les facteurs sont en fait exactement les mêmes de chaque côté de l'égalité.

5.5.3 Factorisation dans $\mathbb{C}[X]$

La factorisation dans $\mathbb{C}[X]$ est particulièrement simple. C'est d'ailleurs l'intérêt de travailler dans les complexes plutôt que dans les réels. Le résultat assurant que tout polynôme complexe non constant admet une racine est admis ici :

Théorème 5.45 (d'Alembert)**.** *Tout polynôme non constant de $\mathbb{C}[X]$ admet une racine.*

À partir de ce résultat, il est facile de voir que tout polynôme de degré supérieur ou égal à 2 est réductible :

Proposition 5.46. *Les polynômes irreductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Démonstration. Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \geqslant 2$. D'après le théorème de d'Alembert, il existe $a \in \mathbb{C}$ tel que $P(a) = 0$. D'après la proposition 5.18, $(X - a)$ divise P. Comme $P \neq (X - a)$ (ces deux polynômes n'ont pas le même degré), P est donc réductible. □

Le résultat du théorème 5.44 prend alors une forme particulièrement simple dans $\mathbb{C}[X]$:

Proposition 5.47. *Soit $P \in \mathbb{C}[X]$. Alors P est scindé. Autrement dit, il existe $\lambda \in \mathbb{C}$, $k \in \mathbb{N}$, $a_1, \dots, a_k$ deux à deux distincts et $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que*

$$P = \lambda \prod_{j=1}^{k} (X - a_j)^{\alpha_j}.$$

En outre cette écriture est unique à l'ordre des facteurs près.

5.5.4 Factorisation dans $\mathbb{R}[X]$

La factorisation d'un polynôme dans $\mathbb{R}[X]$ est moins évidente, car il existe des polynômes irréductibles dans $\mathbb{R}[X]$ qui ne sont pas de degré 1 (par exemple $X^2 + 1$). C'est l'intérêt de plutôt travailler dans $\mathbb{C}$ et, d'ailleurs, pour montrer des résultats dans $\mathbb{R}[X]$ on va en fait repasser par des calculs dans $\mathbb{C}[X]$.

On a donné comme exemple de polynôme irréductible de degré supérieur à 1 le cas d'un polynôme de degré 2 sans racine réelle. C'est en fait le seul problème que l'on peut rencontrer :

Proposition 5.48. *Tout polynôme de degré supérieur ou égal à 3 dans $\mathbb{R}[X]$ est réductible.*

Démonstration. Soit $P \in \mathbb{R}[X]$ un polynôme de degré supérieur ou égal à 3. Si P admet une racine $a \in \mathbb{R}$, alors il est réductible d'après la proposition 5.18.

On suppose maintenant que P n'a pas de racine réelle. On peut voir P comme un polynôme de $\mathbb{C}[X]$. D'après le théorème 5.45, il admet alors une racine complexe $z \in \mathbb{C}$. Puisque les coefficients de P sont réels, on a alors

$$P(\overline{z}) = \overline{P(z)} = 0,$$

donc $\overline{z}$ est également racine de P. Puisque $z \neq \overline{z}$, on obtient par la proposition 5.19 qu'il existe $Q_2 \in \mathbb{C}[X]$ tel que

$$P = (X - z)(X - \overline{z})Q_2.$$

On note

$$Q_1 = (X - z)(X - \overline{z}) = X^2 - 2\operatorname{Re}(z)X + |z|^2$$

(notons que le discriminant $\Delta = 4\operatorname{Re}(z)^2 - 4|z|^2$ est strictement négatif puisque z n'est pas réel). Alors $Q_1 \in \mathbb{R}[X]$ et $\deg(Q_1) = 2$. Il reste à montrer que $Q_2 \in \mathbb{R}[X]$. On effectue la division euclidienne de P par Q_1 dans $\mathbb{R}[X]$. Il existe $\tilde{Q}_2, R \in \mathbb{R}[X]$ tels que $\deg(R) \leqslant 1$ et $P = Q_1\tilde{Q}_2 + R$. Ces deux propriétés sont encore valables dans $\mathbb{C}[X]$. Dans $\mathbb{C}[X]$ on a alors les deux divisions euclidiennes

$$Q_1Q_2 + 0 = P = Q_1\tilde{Q}_2 + R.$$

Par unicité de la division euclidienne, on obtient que $R = 0$ et $Q_2 = \tilde{Q}_2 \in \mathbb{R}[X]$. □

On remarque par ailleurs qu'un polynôme de degré 2 dans $\mathbb{R}[X]$ est irréductible si et seulement s'il n'a pas de racine réelle. Le théorème de factorisation dans $\mathbb{R}[X]$ peut alors s'écrire de la façon suivante :

Proposition 5.49. *Tout polynôme $P \in \mathbb{R}[X]$ s'écrit sous la forme*

$$P = \lambda \prod_{i=1}^{r} (X - a_i)^{\alpha_i} \prod_{j=1}^{s} Q_j^{\beta_j}$$

avec $\lambda \in \mathbb{R}^*$ $r, s \in \mathbb{N}$, les a_i pour $i \in [\![1, r]\!]$ sont des réels deux à deux distincts, $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$, les Q_j pour $j \in [\![1, s]\!]$ sont des polynômes unitaires de degré 2 sans racine réelle et deux à deux distincts, et enfin $\beta_1, \dots, \beta_s \in \mathbb{N}^*$. En outre cette écriture est unique à l'ordre des facteurs près.

Exemple 5.50. On considère

$$P = X^4 + 6X^2 + 25$$

Les racines complexes de P sont $1+2i$, $1-2i$, $-1+2i$ et $-1-2i$ (étudier les racines du polynôme $Y^2+6Y+25$). On obtient

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

5.6 Fractions rationnelles - Décomposition en éléments simples

Formellement, une fraction rationnelle à coefficients dans $\mathbb{K}$ est une expression de la forme

$$\frac{P(X)}{Q(X)},$$

où P et Q sont des polynômes à coefficients dans $\mathbb{K}$ et $Q \neq 0$. Plus précisément, l'ensemble $\mathbb{K}(X)$ des fractions rationnelles à coefficients dans $\mathbb{K}$ peut être vu comme l'ensemble $\mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ dans lequel on a identifié les couples (P_1, Q_1) et (P_2, Q_2) tels que $P_1Q_2 = P_2Q_1$. Cela s'écrit alors

$$\frac{P_1}{Q_1} = \frac{P_2}{Q_2}.$$

On peut vérifier rigoureusement que les règles de calculs sont alors "celles qu'on imagine". Rien de compliqué, mais on n'entre pas dans les détails ici.

Remarque 5.51. Tout fraction rationnelle $F = \frac{A}{B}$ (avec $A, B \in \mathbb{K}[X] \setminus \{0\}$) s'écrit de façon unique sous forme irréductible, c'est-à-dire sous la forme $F = \frac{P}{Q}$ où $P, Q \in \mathbb{K}[X] \setminus \{0\}$ sont premiers entre eux. Pour l'existence, il suffit de diviser A et B par leur pgcd.

Définition 5.52. Soit $F = \frac{P}{Q} \in \mathbb{K}(X) \setminus \{0\}$ écrite sous forme irréductible. Soit $k \in \mathbb{N}^*$.

- On dit que $a \in \mathbb{K}(X)$ est un zéro de F (d'ordre de multiplicité k) si a est une racine de P (d'ordre de multiplicité k).
- On dit que $a \in \mathbb{K}(X)$ est un pôle de F (d'ordre de multiplicité k) si a est une racine de Q (d'ordre de multiplicité k).

Remarque 5.53. a ne peut pas être à la fois zéro et pôle de F.

Le but de ce petit paragraphe est de donner un aperçu de la décomposition en éléments simples, qui permet d'écrire une fraction rationnelle « compliquée » comme somme de fractions rationnelles « plus simples ». Une première motivation est de pouvoir calculer une primitive d'une fonction rationnelle à coefficients dans $\mathbb{R}$.

Exemple 5.54. On cherche une primitive sur son domaine de définition de la fonction

$$f : x \mapsto \frac{1}{x^2 - 11x + 30}$$

Les racines du polynôme $X^2 - 11X + 30$ sont 5 et 6. On a alors

$$X^2 - 11X + 30 = (X-5)(X-6).$$

On cherche a et b tels que

$$\forall x \in \mathbb{R} \setminus \{5, 6\}, \quad \frac{1}{x^2 - 11x + 30} = \frac{1}{(x-5)(x-6)} = \frac{a}{x-5} + \frac{b}{x-6}. \tag{5.6}$$

En multipliant par $(x-5)$ on obtient

$$\forall x \in \mathbb{R} \setminus \{5,6\}, \quad \frac{1}{x-6} = a + \frac{b(x-5)}{x-6}.$$

La limite en 5 donne $a = -1$. De même en multipliant par $(x-6)$ on obtient $b = 1$, et donc

$$\frac{1}{x^2-11x+30} = -\frac{1}{x-5} + \frac{1}{x-6}. \tag{5.7}$$

On peut aussi calculer a et b en remettant les deux fractions au même dénominateur à droite de (5.6) :

$$\forall x \in \mathbb{R} \setminus \{5,6\}, \frac{1}{x^2-11x+30} = \frac{ax-6a+bx-5x}{x^2-11x+30} \iff \begin{cases} a+b=0 \\ -6a-5b=1 \end{cases} \iff (a,b) = (-1,1).$$

Une fois que l'on a écrit (5.7), il est facile de calculer les primitives de f sur un intervalle de $\mathbb{R} \setminus \{5,6\}$. Ce sont les fonctions sont de la forme

$$x \mapsto -\ln(x-5) + \ln(x-6) + c,$$

avec $c \in \mathbb{R}$.

Le passage qui n'est pas évident dans cet exemple est de deviner qu'il existe a et b pour lesquels on peut écrire (5.6). Le but du théorème suivant est de décrire a priori la forme la plus simple sous laquelle on peut écrire une fraction rationnelle.

Théorème 5.55 (Théorème de décomposition en éléments simples)**.** *Soit $F = \frac{P}{Q} \in \mathbb{K}(X) \setminus \{0\}$ écrite sous forme irréductible. On écrit*

$$Q = \lambda \prod_{i=1}^{r} Q_i^{\alpha_i}$$

où $Q_1, \dots, Q_r$ sont des polynômes irréductibles de $\mathbb{K}[X]$ deux à deux distincts et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$. Alors F s'écrit de façon unique sous la forme

$$F = E + \sum_{i=1}^{r} \sum_{j=1}^{\alpha_i} \frac{P_{i,j}}{Q_i^j}$$

où $E \in \mathbb{K}[X]$, et $P_{i,j} \in \mathbb{K}[X]$ est tel que $\deg(P_{i,j}) < \deg(Q_i)$ pour tous $i \in [\![1,r]\!]$ et $j \in [\![1,\alpha_i]\!]$.

Cette décomposition en éléments simples ne paraît en fait pas si simple. Il convient tout de même de dédramatiser. Dans $\mathbb{C}[X]$, tous les facteurs Q_i sont de degré 1, donc tous les polynômes $P_{i,j}$ sont en fait constants. Dans $\mathbb{R}[X]$, les facteurs Q_i sont de degré 1 ou 2, et les numérateurs $P_{i,j}$ sont donc au pire de degré 1. Il se trouve que dans $\mathbb{R}[X]$ on est capable de calculer une primitive de n'importe lequel des termes apparaissant dans cette décomposition, ce qui signifie que l'on est capable de calculer les primitives de n'importe quelle fonction rationnelle à coefficients dans $\mathbb{R}$. Au prix, parfois, de quelques gouttes de sueur tout de même si on veut le faire à la main. Nous verrons quelques exemples de tels calculs en TD...