Chapitre 20

Polynômes

Compétences attendues.

- ✓ Effectuer la division euclidienne de polynômes, calculer le PGCD de deux polynômes.
- ✓ Déterminer la multiplicité d'une racine à l'aide de l'une des caractérisations.
- ✓ Exploiter les relations coefficients-racines.
- ✓ Décomposer un polynôme en facteurs irréductibles dans $\mathbb{R}[X]$ ou $\mathbb{C}[X]$.
- ✓ Effectuer une décomposition en éléments simples d'une fraction rationnelle dans $\mathbb{R}(X)$ ou $\mathbb{C}(X)$.

Mathieu Mansuy - Professeur en MP2I au Lycée Carnot (Dijon)
Page personnelle : `mathieu-mansuy.fr/`
E-mail : `mathieu.mansuy@ac-dijon.fr`

1 L'algèbre $\mathbb{K}[X]$

Jusqu'ici, nous avons manipulé ce qu'on a appelé des *fonctions polynomiales*, c'est-à-dire des fonctions de la forme $f : x \mapsto a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ définies sur $\mathbb{R}$, où $n \in \mathbb{N}$ et $a_0, a_1, \ldots, a_n$ sont des réels. La lettre x désigne une variable qu'on peut remplacer par n'importe quel réel, mais rien d'autre.

L'expression définissant f a également un sens sur $\mathbb{C}$. On peut donc définir une autre fonction $\tilde{f}$ qui à $z \in \mathbb{C}$ associe $\tilde{f}(z) = a_0 + a_1 z + \cdots + a_n z^n$. En fait, cette expression définit une nouvelle fonction sur n'importe quel anneau dans lequel on sait multiplier par un réel, par exemple $\mathscr{M}_n(\mathbb{R})$ ou $(\mathscr{F}(\mathbb{R}, \mathbb{R}), +, \circ)$.

L'idée ici est de traiter ce genre de fonctions sans préciser la nature de la variable, qu'on remplacera par ce qu'on appellera une indéterminée. L'intérêt est d'une part de traiter d'un seul coup toutes les fonctions associées à f, et d'autre part de mettre en évidence des résultats qui ne dépendent pas des 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. L'information importante dans l'expression de f et des fonctions qui lui sont associées, est la famille de coefficients $a_0, \ldots, a_n$. On va donc définir un polynôme par la suite de ses coefficients.

Dans tout le chapitre, $\mathbb{K}$ désigne un corps quelconque. On pourra prendre $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, mais sauf mention explicite du contraire, les résultats énoncés restent valables pour $\mathbb{K} = \mathbb{Q}$ ou encore $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ avec p premier.

1.1 Définitions

Définition.

- On appelle *polynôme (à une indéterminée) à coefficients dans* $\mathbb{K}$ toute *suite presque nulle* d'éléments de $\mathbb{K}$, c'est-à-dire toute suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang :
$$\exists N \in \mathbb{N},\ \forall k \geq N,\ a_k = 0.$$
- Pour tout $k \in \mathbb{N}$, le coefficient a_k est appelé le *coefficient d'ordre* k du polynôme.
- Le polynôme dont tous les coefficients sont nuls est appelé *polynôme nul*, et on le note 0.

La proposition suivante découle directement de la définition de polynôme.

Propriété 1 (Égalité de deux polynômes)

Soient $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ deux polynômes. Alors :

- $P = Q$ si, et seulement si, pour tout $k \in \mathbb{N}$, $a_k = b_k$.
- $P = 0$ si, et seulement si, pour tout $k \in \mathbb{N}$, $a_k = 0$.

Définition.

Soient $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$ deux polynômes à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. On définit :

- la *somme* $P + Q$ *de* P *et* Q par : $P + Q = (a_k + b_k)_{k\in\mathbb{N}}$;
- le *produit* $\lambda \cdot P$ *de* P *par le scalaire* λ par : $\lambda \cdot P = (\lambda a_k)_{k\in\mathbb{N}}$;
- le *produit* $P \times Q$ *des polynômes* P *et* Q par $P \times Q = (c_k)_{k\in\mathbb{N}}$ où pour tout $k \in \mathbb{N}$:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Propriété 2 (Opérations sur les polynômes)

Soient $P = (a_0, a_1, \dots, a_p, 0, \dots)$ et $Q = (b_0, b_1, \dots, b_q, 0, \dots)$ deux polynômes à coefficients dans $\mathbb{K}$ et $\lambda \in \mathbb{K}$. Alors :

(1) $\lambda \cdot P$ et $P + Q$ sont des polynômes ;

(2) $P \times Q = (c_k)_{k\in\mathbb{N}}$ est un polynôme, et :

(i) $c_k = 0$ pour tout $k > p + q$; (ii) $c_{p+q} = a_p b_q$.

Notation.

On notera X le polynôme $(0, 1, 0, \dots)$, appelé l'indéterminée. Avec le produit définit plus haut, on obtient $X^2 = (0, 0, 1, 0, \dots)$ et plus généralement (en effectuant une récurrente) :

$$\text{pour tout } k \in \mathbb{N},\ X^k = (0, \dots, 0, \underbrace{1}_{\substack{(k+1)^{\text{ème}} \\ \text{position}}}, 0, \dots).$$

Par convention, on pose $X^0 = (1, 0, \dots)$. Avec ces notations, le polynôme $P = (a_0, a_1, \dots, a_p, 0, 0, \dots)$ s'écrit :

$$\begin{aligned} P &= a_0(1, 0, \dots) + a_1(0, 1, 0, \dots) + \cdots + a_p(0, 0, \dots, 1, 0, \dots) \\ &= a_0 \cdot X^0 + a_1 \cdot X + \cdots + a_p \cdot X^p. \end{aligned}$$

On s'autorisera aussi à noter $P = \sum_{k=0}^{+\infty} a_k X^k$ en gardant à l'esprit qu'il ne s'agit pas véritablement d'une somme infinie, puisque tous les termes sont nuls à partir d'un certain rang.
On notera alors $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{K}$ en l'indéterminée X.

Exemple. Considérons les polynômes $P = (1, -2, 0, -1, 0, \cdots)$ et $Q = (1, 0, 1, 0, \cdots)$. Avec les notations introduites précédemment :

$$P = X^0 - 2X - X^3 \quad \text{et} \quad Q = X^0 + X^2.$$

Alors $P + Q = 2X^0 - 2X + X^2 - X^3$ et $P \times Q = X^0 - 2X + X^2 - 3X^3 - X^5$.

Propriété 3

- $(\mathbb{K}[X], +, \times)$ est un anneau commutatif d'éléments neutres $0_{\mathbb{K}[X]} = 0$ pour $+$ et $1_{\mathbb{K}[X]} = X^0$ pour $\times$.
- L'application $j : \lambda \in \mathbb{K} \mapsto \lambda \cdot X^0 \in \mathbb{K}[X]$ est un morphisme d'anneaux injectif, permettant d'identifier $\mathbb{K}$ comme sous-anneau de $\mathbb{K}[X]$.

Notation.

Pour tout $\lambda \in \mathbb{K}$, on notera alors plus simplement λ le polynôme $j(\lambda) = \lambda \cdot X^0$. Un tel polynôme sera dit *constant*. Cette identification permet de simplifier encore un peu l'écriture d'un polynôme $P = (a_0, a_1, \dots, a_p, 0, \dots)$ en :

$$P = a_0 + a_1 X + \cdots + a_p X^p.$$

Propriété 4

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

(1) $\lambda \cdot (P + Q) = \lambda \cdot P + \lambda \cdot Q$;

(2) $(\lambda + \mu) \cdot P = \lambda \cdot P + \mu \cdot P$;

(3) $\lambda \cdot (\mu \cdot P) = (\lambda\mu) \cdot P$;

(4) $(\lambda \cdot P) \times Q = \lambda \cdot (P \times Q) = P \times (\lambda \cdot Q)$.

On dit alors que $(\mathbb{K}[X], +, \times, \cdot)$ est une *algèbre*, appelée *l'algèbre des polynômes à une indéterminée à coefficients dans* $\mathbb{K}$.

Propriété 5 (Formule du binôme de Newton)

Soient $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}$. Alors :

$$(P + Q)^n = \sum_{k=0}^{n} \binom{n}{k} P^k Q^{n-k}.$$

Propriété 6

Soient $(P, Q) \in \mathbb{K}[X]^2$ et $n \in \mathbb{N}^*$. Alors :

$$P^n - Q^n = (P - Q) \times \sum_{k=0}^{n-1} P^k Q^{n-1-k}.$$

Définition.

Soient $P = \sum_{k=0}^{p} a_k X^k$ et $Q = \sum_{i=0}^{q} b_i X^i$ sont deux polynômes. On définit le *polynôme composé* $P \circ Q$ par :

$$P \circ Q = \sum_{k=0}^{p} a_k Q^k = \sum_{k=0}^{p} a_k \left(\sum_{i=0}^{q} b_i X^i \right)^k.$$

Exemples.

- Si $P = X^2 + 1$ et $Q = X - 2$, alors :
$$P \circ Q = (X-2)^2 + 1 = X^2 - 4X + 5 \quad \text{et} \quad Q \circ P = X^2 + 1 - 2 = X^2 - 1$$
- Si $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$, le polynôme $P \circ (X + a)$ sera noté $P(X + a)$. En particulier si $a = 0$, alors $P(X)$ n'est autre que le polynôme P (que nous pourrons donc noter indifféremment P ou $P(X)$).
- Si $P = \lambda \in \mathbb{K}$ et $Q \in \mathbb{K}[X]$, alors $P \circ Q = \lambda$.

Mise en garde.

Ne pas confondre $P(X+1)$, qui désigne le polynôme P composé avec $X+1$, et $P \times (X+1)$, le produit des polynômes P et $(X + 1)$. Partons du principe que si on avait souhaité parler de ce produit, on l'aurait plutôt noté $(X + 1)P$, ou alors carrément $P \times (X + 1)$.

1.2 Degré d'un polynôme

Définition.

Soit $P = \sum_{k=0}^{+\infty} a_k X^k$ un polynôme non nul.

- On appelle *degré de* P, et on note $\deg(P)$, l'entier $\deg(P) = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$.

  Par convention, le degré du polynôme nulle est égal à $-\infty$.
- Si $n = \deg(P)$, le coefficient a_n est appelé *coefficient dominant de* P. On dit que P est *unitaire* si son coefficient dominant a_n vaut 1.

Exemple. Le polynôme $P = -2X^3 + X^2 - 1$ est de degré 3 et son coefficient dominant est -2. P n'est pas unitaire, mais $\frac{P}{-2}$ l'est.

Remarques.

- Si P est un polynôme non nul de degré n et de coefficient a_n, alors $\frac{P}{a_n}$ est un polynôme unitaire proportionnel à P.
- Un polynôme P est constant si, et seulement si, $\deg(P) \leq 0$.

Propriété 7 (Opérations et degré)

Soient P et Q deux polynômes de $\mathbb{K}[X]$. Alors :

(1) pour tout $\lambda \neq 0$, $\deg(\lambda \cdot P) = \deg(P)$.

(2) $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$.
De plus, si $\deg(P) \neq \deg(Q)$, alors $\deg(P + Q) = \max(\deg(P), \deg(Q))$.

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

(4) Si $\deg(Q) \geq 1$, alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$.

Exercice 1 Déterminer tous les polynômes P de $\mathbb{K}[X]$ satisfaisant $P(X^2) = (X^2+1)P(X)$.

Propriété 8 (Intégrité et éléments inversibles de l'anneau des polynômes)

- L'anneau $(\mathbb{K}[X], +, \times)$ est *intègre*. Autrement dit :

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ P \times Q = 0_{\mathbb{K}[X]} \quad \Leftrightarrow \quad P = 0_{\mathbb{K}[X]} \text{ ou } Q = 0_{\mathbb{K}[X]}.$$

- Le groupe $(\mathscr{U}(\mathbb{K}[X]), \times)$ des inversibles de l'anneau $(\mathbb{K}[X], +, \times)$ est $(\mathbb{K}^*, \times)$. Autrement dit, pour tout $P \in \mathbb{K}[X]$:

$$\exists Q \in \mathbb{K}[X],\ P \times Q = 1 \quad \Leftrightarrow \quad P \in \mathbb{K}^*.$$

✎ **Notation.**

Pour tout $n \geq 0$, on note $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré inférieurs ou égaux à n.
Avec cette notation, $\mathbb{K}_0[X]$ désigne en particulier l'ensemble des polynômes constants de $\mathbb{K}[X]$.

Propriété 9

L'ensemble $\mathbb{K}_n[X]$ est stable par combinaison linéaire :

$$\forall (\lambda,\mu) \in \mathbb{K}^2,\ \forall (P,Q) \in \mathbb{K}_n[X]^2,\ \lambda P + \mu Q \in \mathbb{K}_n[X].$$

⚠ **Mise en garde.**

Si $n \geq 1$, $\mathbb{K}_n[X]$ n'est pas stable par produit (et $\mathbb{K}_n[X]$ n'est pas un sous-anneau de $\mathbb{K}[X]$).

2 Arithmétique dans $\mathbb{K}[X]$

2.1 Divisibilité

Définition.

Soient $A, B \in \mathbb{K}[X]$. On dit que A *divise* B ou que B est *un multiple de* A s'il existe $Q \in \mathbb{K}[X]$ tel que: $B = AQ$.

✎ **Notation.**

On désigne par $\mathscr{D}(A)$ l'ensemble des diviseurs d'un polynôme A, et par $A\mathbb{K}[X] = \{AQ,\ Q \in \mathbb{K}[X]\}$ l'ensemble des multiples de A.

Exemples. Dans $\mathbb{K}[X]$, $X-1 \mid X^n - 1$ et $X+1 \mid X^{2n+1}+1$.

Remarque. A divise B si, et seulement si, $B\mathbb{K}[X] \subset A\mathbb{K}[X]$.

Propriété 10 (Caractérisation des polynômes associés)

Soient $A, B \in \mathbb{K}[X]$. Alors :

$$(A \mid B \text{ et } B \mid A) \Leftrightarrow A\mathbb{K}[X] = B\mathbb{K}[X] \Leftrightarrow \exists \lambda \in \mathbb{K}^*,\ A = \lambda B.$$

Si l'une de ces assertions est vérifiée, on dit alors que A et B sont des *polynômes associés*.

Remarque. On notera que deux polynômes unitaires et associés sont égaux.

2.2 Division euclidienne

Théorème 11 (de la division euclidienne)

Soient $(A, B) \in \mathbb{K}[X]^2$ avec $B \neq 0_{\mathbb{K}[X]}$. Alors il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

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

Les polynômes Q et R sont appelés le *quotient* et le *reste* de la *division euclidienne de A par B*.

Exercice 2 Effectuer la division des polynômes suivants :

(1) $X^3 + 2X^2 + X + 1$ par $X^2 + 1$. (2) $X^5 + 3X^4 + 1$ par $X^3 + X + 1$

Propriété 12

Soient $A, B \in \mathbb{K}[X]$, $B \neq 0_{\mathbb{K}[X]}$. Alors :

$$B \text{ divise } A \quad \Leftrightarrow \quad \text{le reste de la division euclidienne de } A \text{ par } B \text{ est nul.}$$

2.3 Algorithme d'Euclide et PGCD de deux polynômes

Définition.

Soit $(A, B) \in \mathbb{K}[X]^2$, $(A, B) \neq (0_{\mathbb{K}[X]}, 0_{\mathbb{K}[X]})$.

On appelle *plus grand commun diviseur* (en abrégé PGCD) de A et B, tout diviseur commun à A et B de degré maximal.

Algorithme d'Euclide. Soient A et B deux polynômes, $B \neq 0_{\mathbb{K}[X]}$. On définit une suite (R_k) de polynômes par :

- $R_0 = A$, $R_1 = B$;
- supposons avoir défini les polynômes R_{k-1} et R_k pour un certain rang $k \geq 1$. Si $R_k \neq 0_{\mathbb{K}[X]}$, on effectue la division euclidienne de R_{k-1} par R_k : il existe (Q_k, R_{k+1}) un couple de polynômes tel que :

$$R_{k-1} = Q_k R_k + R_{k+1} \quad \text{avec} \quad \deg(R_{k+1}) < \deg(R_k).$$

La suite d'entiers naturels $(\deg(R_k))$ étant strictement décroissante, il existe $N \in \mathbb{N}$ tel que $\deg(R_N) \geq 0$ et $R_{N+1} = 0_{\mathbb{K}[X]}$.

Propriété 13

(1) $\mathscr{D}(A) \cap \mathscr{D}(B) = \mathscr{D}(R_N)$.

(2) R_N est un PGCD de A et B. De plus, tout PGCD de A et B est associé à R_N.

(3) A et B admettent un unique PGCD unitaire que l'on notera $A \wedge B$.

Remarque. Par convention, $0_{\mathbb{K}[X]} \wedge 0_{\mathbb{K}[X]} = 0_{\mathbb{K}[X]}$.

En adaptant les démonstrations données dans $\mathbb{Z}$, on obtient les propriétés suivantes du PGCD :

- $(\exists \lambda \in \mathbb{K}^*,\ D = \lambda(A \wedge B)) \Leftrightarrow \begin{cases} D \mid A \text{ et } D \mid B \\ \forall P \in \mathbb{K}[X], (P \mid A \text{ et } P \mid B) \Rightarrow P \mid D \end{cases}$.
- Associativité du PGCD : pour $A, B, C \in \mathbb{K}[X]$, $(A \wedge B) \wedge C = A \wedge (B \wedge C)$.
- Homogénéité du PGCD : pour $A, B, P \in \mathbb{K}[X]$ avec P unitaire, $(PA) \wedge (PB) = P(A \wedge B)$.

À l'aide de l'algorithme d'Euclide étendu (identique à celui pour les entiers), on montre la :

Propriété 14 (*Identité de Bezout*)

Soient $A, B \in \mathbb{K}[X]$. Alors, il existe $U, V \in \mathbb{K}[X]$ tels que :

$$AU + BV = A \wedge B.$$

Exercice 3 Calculer le PGCD et déterminer un couple de Bezout pour les polynômes $P = X^5 + 2X^3 - X^2 + X - 1$ et $Q = X^3 - X^2 + X - 1$.

2.4 Polynômes premiers entre eux

Définition.

On dit que deux polynômes A et B sont *premiers entre eux* si $A \wedge B = 1$.

Théorème 15 (*de Bezout*)

Deux polynômes A et B sont premiers entre eux si, et seulement si, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$.

Comme pour les entiers, on en déduit un certain nombre de corollaires.

Corollaire 16

Soient $n, p, q \geq 1$ et des polynômes $A, B, B_1, \ldots, B_n$.

- Si A est premier avec chacun des B_i pour $i = 1, \ldots, n$, alors A est premier avec $B_1 \times \cdots \times B_n$.
- Si A est premier avec B, alors A^p est premier avec B^q.

Exercice 4 Soient $a, b \in \mathbb{K}$ distincts, et $p, q \geq 1$. Montrer que $(X-a)^p$ et $(X-b)^q$ sont premiers entre eux.

Corollaire 17

Soient A, B, C des polynômes tels que A divise C, B divise C et A et B sont premiers entre eux. Alors AB divise C.

Corollaire 18 (*Théorème de Gauss*)

Soient A, B, C des polynômes tels que A divise BC et A est premier avec B. Alors A divise C.

2.5 PPCM de deux polynômes

Définition.

Soient $A, B \in \mathbb{K}[X]$ non nuls.

On appelle *plus petit commun multiple* (en abrégé PPCM) de A et B, tout multiple commun non nul de A et B de degré minimal.

Propriété 19

Soient A et B deux polynômes non nuls de $\mathbb{K}[X]$.

- Si M et N sont deux PPCM de A et B, alors M et N sont associés : il existe $\lambda \in \mathbb{K}^*$ tel que $M = \lambda N$.
- A et B admettent un unique PPCM unitaire que l'on notera $A \vee B$.

Remarque. Par convention, pour tout polynôme A, $A \vee 0 = 0$.

En adaptant les démonstrations données dans $\mathbb{Z}$, on montre les propriétés suivantes du PGCD :

- $(\exists \lambda \in \mathbb{K}^*,\ M = \lambda(A \vee B)) \Leftrightarrow \begin{cases} A \mid M \text{ et } B \mid M \\ \forall P \in \mathbb{K}[X],\ (A \mid P \text{ et } B \mid P) \Rightarrow M \mid P \end{cases}$.
- Pour deux polynômes unitaires ou nuls A et B, $A \times B = (A \wedge B) \times (A \vee B)$.
- Associativité et homogénéité du PPCM.

2.6 Généralisation au PGCD et PPCM de plusieurs polynômes

Définition.

Soit $n \geq 1$. On considère n polynômes $A_1, \ldots, A_n$ non tous nuls de $\mathbb{K}[X]$.

On appelle *plus grand commun diviseur* de $A_1, \ldots, A_n$, tout diviseur commmun de $A_1, \ldots, A_n$ de degré maximal.

Propriété 20

Soit $n \geq 1$. On considère n polynômes $A_1, \ldots, A_n$ non tous nuls de $\mathbb{K}[X]$. Alors D est un PGCD de $A_1, \ldots, A_n$ si, et seulement si, il vérifie :

- $D \mid A_i$ pour tout $i \in [\![1, n]\!]$;
- Pour tout $P \in \mathbb{K}[X]$, si $P \mid A_i$ pour tout $i \in [\![1, n]\!]$, alors $P \mid D$.

De plus, tous les PGCD de $A_1, \ldots, A_n$ sont associés. On notera $A_1 \wedge \cdots \wedge A_n$ l'unique PGCD unitaire de $A_1, \ldots, A_n$.

Propriété 21

Si $D = A_1 \wedge \cdots \wedge A_n$, alors il existe $U_1, \ldots, U_n \in \mathbb{K}[X]$ tels que $D = \sum_{i=1}^{n} A_i U_i$.

Définition.

Soient $A_1, \ldots, A_n \in \mathbb{K}[X]$, avec $n \geq 1$.

- Les polynômes $A_1, \ldots, A_n$ sont dits *premiers entre eux deux à deux* si $A_i \wedge A_j = 1$ pour tout $i \neq j$.
- Les polynômes $A_1, \ldots, A_n \in \mathbb{K}[X]$ sont dits *premiers dans leur ensemble* si $A_1 \wedge \cdots \wedge A_n = 1$.

Remarque. Si les polynômes $A_1, \ldots, A_n$ sont premiers entre eux deux à deux, alors ils sont premiers dans leur ensemble. La réciproque est fausse en générale.

2.7 Polynômes irréductibles

Définition.

Un polynôme non constant $P \in \mathbb{K}[X]$ est dit *irréductible sur* $\mathbb{K}$ s'il satisfait :

$$\forall A, B \in \mathbb{K}[X],\ P = A \times B \ \Rightarrow\ \deg(A) = 0 \ \text{ ou } \ \deg(B) = 0.$$

Remarques.

- Les polynômes irréductibles sont les analogues dans $\mathbb{K}[X]$ des nombres premiers dans $\mathbb{N}$.
- Les polynômes de degré un sont irréductibles sur $\mathbb{K}$: en effet si $P \in \mathbb{K}[X]$ est de degré 1 et si $A, B \in \mathbb{K}[X]$ sont tels que $P = A \times B$, alors $\deg(P) = 1 = \deg(A) + \deg(B)$. Ainsi, $\deg(A) = 0$ ou $\deg(B) = 0$.
- Le polynôme $X^2 + 1$ n'est pas irréductible sur $\mathbb{C}$ car $X^2 + 1 = (X + i)(X - i)$. Il est cependant irréductible sur $\mathbb{R}$: en effet, s'il existe $a, b, c, d \in \mathbb{R}$ tel que $X^2 + 1 = (aX + b)(cX + d)$, alors en

développant puis en identifiant coefficients par coefficients :

$$\begin{cases} ac = 1 \\ ad + bc = 0 \\ bd = 1 \end{cases} \quad \text{d'où} \quad 1 = abcd = ad(-ad) = -(ad)^2$$

ce qui est contradictoire.

Propriété 22

Soient $P \in \mathbb{K}[X]$ un polynôme irréductible sur $\mathbb{K}$, et $A, A_1, \dots, A_n \in \mathbb{K}[X]$ (avec $n \geq 1$). Alors :

- soit P divise A, soit P est premier avec A ;
- si P divise le produit $A_1 \times A_2 \times \cdots \times A_n$, alors il divise l'un des facteurs $A_1, A_2, \dots, A_n$.

Théorème 23 (*Théorème fondamental de l'arithmétique dans* $\mathbb{K}[X]$)

Tout polynôme non constant A se décompose de manière unique (à l'ordre des facteurs près) comme un produit de polynômes irréductibles unitaires :

$$A = \lambda \prod_{k=1}^{r} P_k^{\alpha_k}$$

où $\lambda \in \mathbb{K}^*$, $r \in \mathbb{N}^*$, $P_1, \dots, P_r$ des polynômes irréductibles et unitaires deux à deux distincts, et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls.

Comme dans $\mathbb{Z}$, on établira que le PGCD et le PPCM de deux ou plusieurs polynômes peuvent être obtenus à partir de leur factorisation en produit de polynômes irréductibles.

3 Racines d'un polynôme

3.1 Fonctions polynomiales

À partir d'un polynôme $P \in \mathbb{K}[X]$, on va associer une fonction définie sur $\mathbb{K}$.

Définition.

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$. On appelle *fonction polynomiale associée à* P, la fonction $\tilde{P} : \mathbb{K} \to \mathbb{K}$ définie par :

$$\forall x \in \mathbb{K},\ \tilde{P}(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

On note $\mathscr{P}_{\mathbb{K}} = \{x \mapsto \tilde{P}(x) \mid P \in \mathbb{K}[X]\}$ le sous-ensemble de $\mathscr{F}(\mathbb{R}, \mathbb{R})$ formé des fonctions polynomiales à coefficients dans $\mathbb{K}$.

Propriété 24

L'application $\Phi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathscr{P}_{\mathbb{K}} \\ P & \mapsto & \widetilde{P}. \end{array}$ satisfait :

(1) $\forall \lambda, \mu \in \mathbb{K}, \forall P, Q \in \mathbb{K}[X], \Phi(\lambda \cdot P + \mu \cdot Q) = \lambda\Phi(P) + \mu\Phi(Q)$;

(2) $\forall P, Q \in \mathbb{K}[X], \Phi(P \times Q) = \Phi(P) \times \Phi(Q)$;

(3) $\Phi(1_{\mathbb{K}[X]}) = 1_{\mathscr{F}(\mathbb{R},\mathbb{R})}$.

En particulier, $\mathscr{P}_{\mathbb{K}}$ est un sous-anneau de $(\mathscr{F}(\mathbb{R},\mathbb{R}), +, \times)$, et Φ est un morphisme d'anneaux surjectif de $\mathbb{K}[X]$ dans $\mathscr{P}_{\mathbb{K}}$.

Pour aller plus loin.

Avec le premier point, on a plus précisément montré que $\mathscr{P}_{\mathbb{K}}$ est une sous-algèbre de $\mathscr{F}(\mathbb{R},\mathbb{R})$ et que Φ est un morphisme d'algèbres surjectif.

Définition.

Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. On appelle *évaluation de P en a* l'élément $\widetilde{P}(a)$ de $\mathbb{K}$. Par abus de notation, on le notera $P(a)$, et on parlera de la *valeur de P en a*.

Algorithme de Hörner. Calculer la valeur d'un polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$ en $x_0 \in \mathbb{K}$ peut se faire de plusieurs manières :

- la méthode naïve : on calcule les puissances de x_0, puis on réalise la combinaison linaire de ces puissances ;
- de manière plus subtile, on utilise l'écriture
$$P(x_0) = ((\cdots((a_n x_0 + a_{n-1})x_0 + a_{n-2})x_0 + \cdots + a_2)x_0 + a_1)x_0 + a_0$$
et on calcule depuis le terme le plus intérieur aux parenthèses. Cette méthode appelée *algorithme de Hörner* (1787-1837) est la plus efficace en terme d'opérations (n additions et n multiplications) pour évaluer un polynôme en un point x_0.

Exercice 5 Évaluer $P = 2X^4 - X^3 + 3X^2 - 1$ en -2 grâce à l'algorithme d'Hörner.

Pour aller plus loin.

Les définitions et propriétés données dans cette section se généralisent au cas d'une algèbre $(A, +, \times, \cdot)$ sur $\mathbb{K}$. En effet, à tout polynôme $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on peut associer une application $\Phi_A(P) : A \to A$ définie par :
$$\Phi_A(P) : x \mapsto a_0 1_A + a_1 x + \cdots + a_n x^n.$$
Ainsi :

- si $A = \mathscr{M}_n(\mathbb{K})$, l'évaluation de P en la matrice $M \in \mathscr{M}_n(\mathbb{K})$, qu'on note simplement $P(M)$,

est :
$$P(M) = a_0 I_n + a_1 M + \cdots + a_n M^n.$$

- si $A = (\mathscr{F}(\mathbb{R},\mathbb{R}), +, \circ, \cdot)$, l'évaluation de P en la fonction $f \in \mathscr{F}(\mathbb{R},\mathbb{R})$, qu'on note simplement $P(f)$, est :
$$P(f) = a_0 \mathrm{id}_{\mathbb{R}} + a_1 f + \cdots + a_n f^n.$$

3.2 Racines

Définition.

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

Remarques.

- Il est bon de préciser dans quel corps on se place lorsqu'on parle de racine. Par exemple, le polynôme X^2+1 n'a pas de racine dans $\mathbb{R}$, mais en a deux dans $\mathbb{C}$. De même, X^3-2 n'a aucune racine dans $\mathbb{Q}$, en a une dans $\mathbb{R}$ et trois dans $\mathbb{C}$.
- Si P divise Q, alors toute racine de P est une racine de Q.

Exemples.

- Tout polynôme $aX+b$ de degré 1 de $\mathbb{K}[X]$ a une racine $-\dfrac{b}{a}$ dans $\mathbb{K}[X]$.
- Si $z \in \mathbb{C}$ est racine de $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{R}[X]$, alors $\bar{z}$ est aussi racine de P, puisque :
$$0 = \overline{\sum_{k=0}^{p} a_k z^k} = \sum_{k=0}^{p} a_k \bar{z}^k = P(\bar{z}).$$

  Cette propriété est **fausse** si $P \in \mathbb{C}[X]$.

Exercice 6 Soit $n \in \mathbb{N}$ et $\theta \not\equiv 0\,[\pi]$. Déterminer le reste de la division euclidienne de X^n par $P = X^2 - 2\cos(\theta)X + 1$.

Propriété 25

Soit $a \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Alors :
$$a \text{ est racine de } P \;\Leftrightarrow\; (X-a) \mid P.$$

Exercice 7 Déterminer une racine évidente α de $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$, puis factoriser P par α.

Exercice 8
1. Montrer que si $P \in \mathbb{K}[X]$ est de degré 2 ou 3 et sans racine dans $\mathbb{K}$, alors P est irréductible sur $\mathbb{K}$.
2. Montrer qu'un polynôme réel de degré 3 n'est pas irréductible sur $\mathbb{R}$.

Propriété 26

Soit $P \in \mathbb{K}[X]$, $n \in \mathbb{N}^*$ et $a_1, \ldots, a_n \in \mathbb{K}$ des scalaires deux à deux distincts. Alors :

$$a_1, a_2, \cdots, a_n \text{ sont racines de } P \Leftrightarrow (X - a_1) \ldots (X - a_n) \mid P.$$

On obtient la conséquence importante suivante de cette proposition.

Théorème 27

- Un polynôme de degré $n \in \mathbb{N}$ admet au plus n racines distinctes.
- Un polynôme de $\mathbb{K}_n[X]$ qui admet au moins $n+1$ racines est le polynôme nul.
- Un polynôme qui admet une infinité de racines est le polynôme nulle.

Comme autre conséquence, on obtient le résultat suivant qui permettra d'identifier les polynômes et le fonctions polynomiales lorsque le corps $\mathbb{K}$ est infini (donc en particulier lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).

Propriété 28

Si $\mathbb{K}$ est infini, alors l'application $\Phi : \begin{array}{ccc} \mathbb{K}[X] & \to & \mathscr{P}_{\mathbb{K}} \\ P & \mapsto & \tilde{P} \end{array}$ est un isomorphisme de $\mathbb{K}$-algèbres.

Remarque. Plus généralement, si A est une partie infinie de $\mathbb{K}$, alors $P \mapsto \tilde{P}_{|A}$ est une bijection de $\mathbb{K}[X]$ sur l'ensemble des fonctions polynomiales sur A, de sorte que pour un polynôme $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}[X]$:

$$\begin{array}{c} P = 0_{\mathbb{K}[X]} \\ \text{(c'est-à-dire } a_k = 0 \text{ pour tout } k \in \mathbb{N}) \end{array} \Leftrightarrow \begin{array}{c} \tilde{P} = 0_{\mathscr{F}(A,\mathbb{K})} \\ \text{(c'est-à-dire } \tilde{P}(t) = 0 \text{ pour tout } t \in A) \end{array}$$

Par exemple, on peut identifier $\mathbb{R}[X]$ à l'ensemble des fonctions polynomiales sur $\mathbb{R}_+$ ou sur $[0, 1]$.

Pour aller plus loin.

Si $\mathbb{K}$ est fini, l'application Φ n'est plus injective : par exemple lorsque $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ avec p premier, tout élément x de $\mathbb{K}$ satisfait $x^p = x$ par le petit théorème de Fermat. Ainsi, la fonction polynomiale associée à $P = X^p - X$ est nulle alors que P n'est pas le polynôme nulle de $\mathbb{K}[X]$. Il sera donc nécessaire dans ce cas de bien distinguer polynômes et fonctions polynomiales.

Exercice 9 Montrer que la fonction racine carrée n'est pas une fonction polynomiale sur $\mathbb{R}$.

3.3 Dérivation dans $\mathbb{K}[X]$

Dans cette section et la suivante, nous supposerons que $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, ou plus généralement un corps qui contient $\mathbb{Q}$.

Définition.

Soit $P = \sum_{k=0}^{p} a_k X^k \in \mathbb{K}_p[X]$ un polynôme. On définit le *polynôme dérivé* de P, noté P', par :

$$P' = \sum_{k=1}^{n} k a_k X^{k-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i \in \mathbb{K}_{p-1}[X].$$

Plus généralement, on note $P^{(0)} = P$ et pour tout $n \in \mathbb{N}$, $P^{(n+1)} = \left(P^{(n)}\right)'$.

Remarque. Cette définition s'inspire des règles bien connues de dérivation des fonctions polynomiales à coefficients réels. Ainsi pour $\mathbb{K} = \mathbb{R}$, $\Phi(P') = \Phi(P)'$ pour tout polynôme P, où la dérivée de droite est celle des fonctions numériques de la variable réelle. On étend ces règles pour définir formellement la notion de polynôme dérivé quel que soit le corps $\mathbb{K}$ (et donc notamment pour $\mathbb{K} = \mathbb{C}$ ou $\mathbb{Q}$ dans lesquels la notion de limite ou de taux d'accroissement n'auraient pas de sens).

Propriété 29

Soient $P, Q \in \mathbb{K}[X]$ des polynômes, et $\lambda, \mu \in \mathbb{K}$. Alors :

(1) $P' = 0 \Leftrightarrow P$ est constant.

(2) si $\deg(P) \geq 1$, alors $\deg(P') = \deg(P) - 1$.

(3) $(\lambda P + \mu Q)' = \lambda P' + \mu Q'$.

(4) $(P \times Q)' = P' \times Q + P \times Q'$.

(5) $(P \circ Q)' = Q' \times (P' \circ Q)$

Pour aller plus loin.

Les points (1) et (2) ne sont plus valables lorsque $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Par exemple dans $\mathbb{Z}/3\mathbb{Z}$, si $P = X^6 + 2X^3 + 1$, alors $P' = 6X^5 + 6X^2 = 0$. Ainsi $P' = 0$ alors que P n'est pas constant. De même, $\deg(P') \neq \deg(P) - 1$. On pourra seulement affirmer dans cette situation que :

- P constant $\Rightarrow P' = 0$;
- $\deg(P') \leq \deg(P) - 1$.

Exemple. Soit $P = (X - a)^n$ où $a \in \mathbb{K}$ et $n \in \mathbb{N}$. Pour tout $k \in [\![0, n]\!]$:

$$P^{(k)} = \begin{cases} n(n-1)\cdots(n-k+1)X^{n-k} = \dfrac{n!}{(n-k)!}(X-a)^{n-k} & \text{si } k \in [\![0,n]\!] \\ 0 & \text{si } k > n \end{cases}.$$

Propriété 30

Soient $n \in \mathbb{N}$, $P, Q \in \mathbb{K}[X]$ et $\lambda, \mu \in \mathbb{K}$.

(1) Si $\deg(P) = n$, alors $\deg(P^{(k)}) = \deg(P) - k$ si $k \leq n$ et $P^{(k)} = 0$ pour tout $k > n$.

(2) $(\lambda P + \mu Q)^{(n)} = \lambda P^{(n)} + \mu Q^{(n)}$.

Propriété 31 (Formule de Leibniz)

Soient $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$. Alors :

$$(P \times Q)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Propriété 32 (Formule de Taylor)

Soient $P \in \mathbb{K}[X]$ de degré $n \in \mathbb{N}$, et $a \in \mathbb{K}$. Alors :

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

Remarque. En particulier pour $a = 0$, on obtient par identification des coefficients :

$$\forall k \in [\![0, n]\!],\ a_k = \frac{P^{(k)}(0)}{k!}.$$

Pour aller plus loin.

La formule de Taylor n'est plus valable dans un corps fini : dans $\mathbb{Z}/p\mathbb{Z}$, $p! = 0$ et n'est donc pas inversible.

3.4 Ordre de multiplicité des racines d'un polynôme

Propriété 33

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $r \in \mathbb{N}^*$. Il y a équivalence entre :

(i) $(X - a)^r$ divise P ;

(ii) il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)^r Q$;

(iii) $P(a) = P'(a) = \cdots = P^{(r-1)}(a) = 0$.

Si l'une de ces conditions est satisfaite, on dit alors que *a est racine de P de multiplicité au moins r*.

Propriété 34

Soient $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Il y a équivalence entre :

(i) $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P ;

(ii) il existe $Q \in \mathbb{K}[X]$, $P = (X-a)^m Q$ et $Q(a) \neq 0$;

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

Si l'une de ces conditions est satisfaite, on dit alors que *a est racine de P de multiplicité m exactement*.

Pour aller plus loin.

Le point (iii) n'est plus valable lorsque $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Par exemple pour $p = 2$, 1 est racine de multiplicité 2 exactement de $P = (X-1)^2$ d'après le point (i), alors que $P^{(k)}(1) = 0$ pour tout $k \geq 0$.

Vocabulaire. Lorsque $m \geq 2$, on parle de racine multiple. Les racines d'ordre 1,2,3 de P sont respectivement appelés racines simples, doubles, triples de P.

Exercice 10 Déterminer l'ordre de multiplicité m de 1 comme racine de $P = X^5 - 7X^4 + 19X^3 - 25X^2 + 16X - 4$, et déterminer $Q \in \mathbb{K}[X]$ tel que $P = (X-1)^m Q$.

Exercice 11 Soit $P \in \mathbb{R}[X]$. Montrer que si $z \in \mathbb{C} \setminus \mathbb{R}$ est racine de P de multiplicité $m \geq 1$, alors $\overline{a}$ est aussi racine de P de multiplicité m.

Propriété 35

Soit $P \in \mathbb{K}[X]$, et soient $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ des scalaires deux à deux distincts (avec $k \geq 1$) et $r_1, \ldots, r_k \in \mathbb{N}^*$. Alors :

$$\alpha_i \text{ racine de } P \text{ de multiplicité au moins } r_i \text{ pour tout } i \in [\![1,k]\!] \quad \Leftrightarrow \quad (X-\alpha_1)^{r_1} \ldots (X-\alpha_k)^{r_k} \mid P.$$

Corollaire 36

Un polynôme de degré n a au plus n racines **comptées avec leurs ordres de multiplicité**.

3.5 Polynômes scindés, relations coefficients-racines

Définition.

On dit qu'un polynôme $P \in \mathbb{K}[X]$ est *scindé sur* $\mathbb{K}$ s'il peut s'écrire comme un produit de polynômes du premier degré de $\mathbb{K}[X]$, c'est-à-dire s'il existe $\lambda \in \mathbb{K}^*$, $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ deux à deux distincts et $m_1, \ldots, m_k \in \mathbb{N}^*$ tels que :

$$P = \lambda (X-\alpha_1)^{m_1} \cdots (X-\alpha_k)^{m_k}.$$

Le scalaire λ est alors le coefficient dominant de P, $\alpha_1, \ldots, \alpha_k$ ses racines distinctes de multiplicités respectives $m_1, \ldots, m_k$.

Remarques.

- La notion de polynôme scindé dépend du corps $\mathbb{K}$ considéré : ainsi $X^2+1=(X-i)(X+i)$ est scindé sur $\mathbb{C}$, mais pas sur $\mathbb{R}$ car $i \notin \mathbb{R}$.
- Un polynôme $P \in \mathbb{K}[X]$ est scindé et irréductible sur $\mathbb{K}$ si, et seulement si, $\deg(P)=1$.

Propriété 37

Un polynôme $P \in \mathbb{K}[X]$ est scindé sur $\mathbb{K}$ si, et seulement si, son degré est égal à la somme des ordres de multiplicité de ses racines dans $\mathbb{K}$.

Exemple. Le polynôme X^n-1 est de degré n et admet n racines distinctes dans $\mathbb{C}$, les racines n-ièmes de l'unité. Donc X^n-1 est scindé sur $\mathbb{C}$. Puisque X^n-1 est de plus unitaire, il s'écrit :

$$X^n-1=\prod_{k=0}^{n-1}\left(X-e^{\frac{2ik\pi}{n}}\right).$$

On étudie à présent les relations entre coefficients et racines des polynômes scindés. Rappelons le résultat suivant.

Propriété 38 (Relations coefficients-racines pour un polynôme de degré 2)

Soit $P=aX^2+bX+c \in \mathbb{K}[X]$. Alors :

$$\alpha_1 \text{ et } \alpha_2 \text{ sont racines de } P \text{ dans } \mathbb{K} \Leftrightarrow \begin{cases} \alpha_1+\alpha_2=-\dfrac{b}{a} \\ \alpha_1\alpha_2=\dfrac{c}{a} \end{cases}.$$

Ce résultat se généralise aux polynômes de degré n de la manière suivante.

Définition.

On considère n scalaires $\alpha_1,\dots,\alpha_n$, distincts ou non, appartenant à $\mathbb{K}$.
Les *fonctions symétriques élémentaires de* $\alpha_1,\dots,\alpha_n$ sont les fonctions définies par :

$$\sigma_k=\sum_{1\leq i_1<i_2<\dots<i_k\leq n}\alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} \quad \text{pour tout } k\in[\![1,n]\!].$$

Exemple. Pour $n=3$, $\sigma_1=\alpha_1+\alpha_2+\alpha_3$, $\sigma_2=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3$ et $\sigma_3=\alpha_1\alpha_2\alpha_3$.

Propriété 39 (Relations entre coefficients et racines d'un polynôme scindé)

On considère un polynôme scindé de degré n de $\mathbb{K}[X]$ s'écrivant :

$$P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = a_n(X-\alpha_1)\dots(X-\alpha_n).$$

Si $\sigma_1, \dots, \sigma_n$ sont les fonctions symétriques élémentaires de $\alpha_1, \dots, \alpha_n$, alors :

$$P = a_n\left(X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \cdots + (-1)^n \sigma_n\right)$$

et par identification :

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n} \text{ pour tout } k \in [\![1, n]\!].$$

Exemple. Le polynôme $P = X^n - 1$ est scindé sur $\mathbb{C}$ et ses racines sont exactement les racines n-ièmes de l'unité. D'après les relations coefficients racines, $\sigma_1 = \sum_{k=0}^{n-1} e^{\frac{2ik\pi}{n}} = 0$, $\sigma_2 = \sum_{0\leq k<\ell\leq n-1} e^{\frac{2i(k+\ell)\pi}{n}} = 0$, puis $\sigma_3 = 0$, etc, jusqu'à

$$\sigma_n = \prod_{\omega\in\mathbb{U}_n} \omega = (-1)^n \frac{-1}{1} = (-1)^{n+1}.$$

Le saviez-vous ?

Penchons nous sur le problème inverse : existe-t-il des formules permettant d'exprimer les racines d'un polynôme P à partir de ses coefficients. Le cas $\deg(P) = 2$ est résolu depuis bien longtemps, puisque les Babyloniens connaissaient déjà les formules que vous avez apprises au lycée. La question s'est alors posée de généraliser ces résultats pour $\deg(P) \geq 3$. Plus précisément, existe-t-il des formules analogues pour des équations polynomiales de degré supérieur, permettant d'exprimer les solutions uniquement avec les coefficients de P et les opérations « $+$ », « $\times$ » et « $\sqrt[n]{\ }$ » avec $n \geq 2$? Si c'est effectivement le cas, l'équation est dite *résoluble par radicaux*.

Il a fallu attendre le 16ème siècle pour que de telles formules soient obtenues pour les équations polynomiales de degré 3. La solution nous vient d'Italie, où les mathématiciens Tartaglia et Scipione del Ferro découvrent à peu près en même temps ce qu'on appelle aujourd'hui la méthode de Cardan. Cardan, quant à lui, a plus ou moins volé le travail de Tartaglia et l'a publié en son nom. Quelques années plus tard, un certain Ferrari, élève de Cardan, résout quant à lui les équations de degré 4. Ces formules étant cependant bien compliquées, on ne les enseigne pas dans nos classes.

Le cas des équations polynomiales de degré $d \geq 5$ sera traité 200 ans plus tard. En 1824, dans un texte qui restera incompris quelques années, le mathématicien norvégien Niels Henrik Abel (1802-1829) montre qu'aucune formule générale de résolution des équations polynomiales de degré supérieur ou égal à 5 n'est possible. Il est donc inutile de s'évertuer à chercher de telles formules, elles n'existent pas !

Le Français Évariste Galois (1811-1832), sans connaître les résultats d'Abel, obtient un résultat plus précis : pour n'importe quelle équation polynomiale donnée, il propose un critère pour déterminer si oui ou non, cette équation est résoluble par radicaux. Ce résultat donne ainsi une réponse complète au problème de la résolubilité d'une équation polynomiale.

Provoqué dans un duel lié à une histoire d'amour malheureuse, Galois meurt à l'âge de 20 ans. À la veille de ce duel, il dresse dans une lettre le bilan de ses recherches et demande à ce que Jacobi ou Gauss donnent leur avis « sur l'importance de (ses) théorèmes ». Le mathématicien français Joseph Liouville (1809-1882) publiera ses oeuvres scientifiques quatorze ans plus tard à titre posthume, ce qui donnera à Galois une renommée internationale. Ses idées ont eu une portée considérable, aboutissant à l'introduction de notions fondamentales, et sont toujours fécondes aujourd'hui[a].

[a] Pour en connaitre davantage sur la vie d'Evariste Galois, je vous conseille cette vidéo.

Évariste Galois (1811 - 1832).

4 Théorème fondamental de l'algèbre

4.1 Le théorème de d'Alembert-Gauss

Théorème 40 (*Théorème de d'Alembert-Gauss*)

Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$.

La preuve est hors programme en MP2I. Nous en proposerons une en complément de cours. Ce résultat, parfois appelé théorème fondamental de l'algèbre a connu une première tentative de démonstration par d'Alembert, mais la première preuve vraiment rigoureuse est due à Gauss, qui en donna au moins quatre preuves différentes.

Corollaire 41

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

On traduit cette propriété en disant que $\mathbb{C}$ est un *corps algébriquement clos*.

Corollaire 42

Soient $P, Q \in \mathbb{C}[X]$, avec P non nul

- P divise Q si, et seulement si, toutes les racines de P sont des racines de Q, avec une multiplicité dans Q supérieure ou égale à la multiplicité dans P.
- P et Q sont premiers entre eux si, et seulement si, ils n'ont pas de racine commune dans $\mathbb{C}$.
- P est à racines simples dans $\mathbb{C}$ si, et seulement si, P est premier avec P'.

4.2 Factorisation dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$

Propriété 43 (Factorisation irréductible sur $\mathbb{C}$)

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

(2) Tout polynôme $P \in \mathbb{C}[X]$ non constant se factorise de manière unique (à l'ordre près des facteurs) en produit de polynômes irréductibles et unitaires de $\mathbb{C}[X]$ sous la forme :

$$P(X) = \lambda \prod_{i=1}^{k} (X - \alpha_i)^{m_i}$$

où λ est le coefficient dominant de P, $\alpha_1, \dots, \alpha_k$ sont les racines distinctes de P de multiplicités respectives $m_1, \dots, m_k \in \mathbb{N}^*$.

Propriété 44 (Factorisation irréductible sur $\mathbb{R}$)

(1) Les polynômes irréductibles de $\mathbb{R}[X]$ sont :

- les polynômes de degré 1 ;
- les polynômes de degré 2 à discriminant strictement négatif.

(2) Tout polynôme P de $\mathbb{R}[X]$ se factorise de manière unique (à l'ordre près des facteurs) en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$ sous la forme :

$$P(X) = \lambda \left(\prod_{i=1}^{p} (X - \alpha_i)^{m_i} \right) \left(\prod_{j=1}^{q} (X^2 - (z_j + \bar{z_j})X + z_j \bar{z_j})^{n_j} \right)$$

où λ est le coefficient dominant de P, $\alpha_1, \dots, \alpha_p$ les racines réelles de P de multiplicités respectives $m_1, \dots, m_p$ et $z_1, \overline{z_1}, \dots, z_q, \overline{z_q}$ les racines complexes non réelles de P de multiplicités $n_1, \dots, n_q$.

Méthode. Comment factoriser un polynôme de $\mathbb{R}[X]$ en produits d'irréductibles ?
Pour factoriser sur $\mathbb{R}$, on peut factoriser sur $\mathbb{C}$, puis regrouper les termes complexes conjugués.

Exercice 12 Factoriser les polynômes $X^4 + 1$ et $X^n - 1$ dans $\mathbb{R}[X]$.

5 Polynômes interpolateurs de Lagrange

Dans cette partie, on considère $\alpha_0, \alpha_1, \dots, \alpha_n$ des éléments de $\mathbb{K}$ **deux à deux distincts**, et $\beta_0, \dots, \beta_n \in \mathbb{K}$. Le problème de l'*interpolation polynomiale* consiste à déterminer un polynôme P de degré minimal tel que $P(\alpha_i) = \beta_i$ pour tout $i \in [\![0, n]\!]$.

Notation.

On définit pour tout $(i,j) \in [\![0,n]\!]^2$ le symbole de Kronecker $\delta_{i,j} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon} \end{cases}$.

Soit $i \in [\![0,n]\!]$. Traitons pour commencer le cas particulier où $b_j = \delta_{i,j}$ pour tout $j \in [\![0,n]\!]$.

Propriété 45

Soient $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{K}$ deux à deux distincts, et soit $i \in [\![0,n]\!]$.
Il existe un unique polynôme L_i dans $\mathbb{K}_n[X]$ satisfaisant $L_i(\alpha_j) = \delta_{i,j}$.

Définition.

Soient $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{K}$ deux à deux distincts. Pour $i \in [\![0,n]\!]$, on appelle *i-ème polynôme de Lagrange associé à $(\alpha_0, \alpha_1, \dots, \alpha_n)$* le polynôme :

$$L_i = \prod_{\substack{k=0 \\ k \neq i}}^{n} \frac{X - \alpha_k}{\alpha_i - \alpha_k} = \frac{X-\alpha_0}{\alpha_i - \alpha_0} \cdots \frac{X-\alpha_{i-1}}{\alpha_i - \alpha_{i-1}} \frac{X-\alpha_{i+1}}{\alpha_i - \alpha_{i+1}} \cdots \frac{X-\alpha_n}{\alpha_i - \alpha_n} \in \mathbb{K}_n[X].$$

Il vérifie $L_i(\alpha_j) = \delta_{i,j}$ pour tout $j \in [\![0,n]\!]$.

Propriété 46

Soient $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{K}$ deux à deux distincts, et $\beta_0, \beta_1, \dots, \beta_n \in \mathbb{K}$.

- Il existe un unique polynôme $P \in \mathbb{K}_n[X]$ satisfaisant $P(\alpha_i) = \beta_i$ pour tout $i \in [\![0,n]\!]$, à savoir :
$$P = \beta_0 L_0 + \beta_1 L_1 + \cdots + \beta_n L_n.$$
- Les polynômes $Q \in \mathbb{K}[X]$ satisfaisant $Q(\alpha_i) = \beta_i$ pour tout $i \in [\![0,n]\!]$ sont exactement ceux de la forme $P + R \prod_{k=0}^{n} (X - \alpha_i)$ où R décrit $\mathbb{K}[X]$.

Pour aller plus loin.

Soit $f : [a,b] \to \mathbb{R}$ une fonction définie sur un segment $[a,b]$ et $\alpha_0, \dots, \alpha_n \in [a,b]$ deux à deux distincts. Par ce qui précède, il existe un unique polynôme dans $\mathbb{R}_n[X]$ tel que :

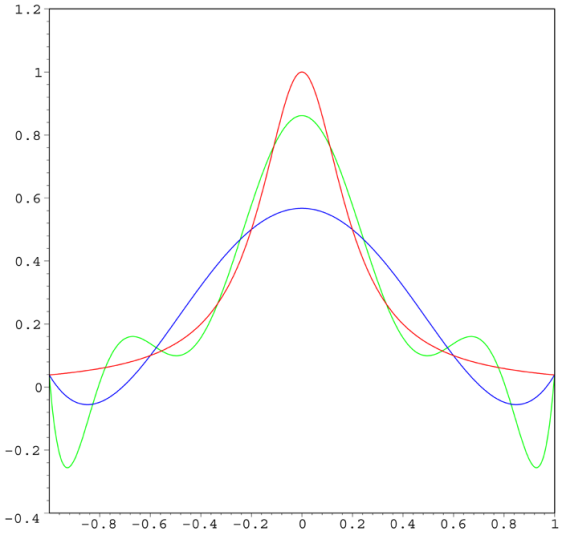
$$\forall i \in [\![0,n]\!],\ P(\alpha_i) = f(\alpha_i).$$

Le polynôme P est appelé *polynôme interpolateur de Lagrange de f aux points $\alpha_0, \dots, \alpha_n$*. La fonction polynomiale associée coïncide avec f en ces points.

Pour « approcher au mieux » f par une fonction polynomiale, une idée naturelle serait d'augmenter le nombre de points d'interpolation. Il semble en effet raisonnable de penser que la courbe représentative du polynôme interpolateur de Lagrange de f va converger (dans un sens qu'il faudrait préciser) vers celle de f si on augmente le nombre de points où ces deux courbes coïncident.

Ce n'est cependant pas le cas en général. Par exemple, si on choisit des points d'interpolation équi-répartis sur $[a,b]$, on peut observer pour certaines fonctions (même de classe $\mathscr{C}^\infty$) qu'au contraire, l'approximation est de plus en plus mauvaise lorsque n augmente, particulièrement sur les extrémités du segment : on parle de *phénomène de Runge*.

Une solution pour corriger ce problème et ainsi obtenir de « bonnes approximations polynomiales » de f est de choisir nos points d'interpolation de manière plus optimale, en concentrant davantage ces points sur les extrémités du segment $[a,b]$ où ce phénomène se produit.



Courbes représentatives d'une fonction f (en rouge) et de ses polynômes interpolateurs de degré 5 (courbe bleue) et de degré 9 (courbe verte).

6 Fractions rationnelles

6.1 Le corps des fractions rationnelles

Donnons les principales étapes de la construction du corps des fractions rationnelles.

On définit sur $\mathscr{F} = \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\})$ une relation binaire $\sim$ par :

$$(P_1, Q_1) \sim (P_2, Q_2) \;\Leftrightarrow\; P_1 Q_2 = P_2 Q_1.$$

On montre sans difficulté (mais en utilisant de manière prépondérante l'intégrité de $\mathbb{K}[X]$) que $\sim$ est une relation d'équivalence sur $\mathscr{F}$.

Définition.

On appelle *fraction rationnelle sur* $\mathbb{K}$ toute classe d'équivalence de $\mathscr{F}$ pour la relation $\sim$.

✎ **Notation.**

On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles sur $\mathbb{K}$, c'est-à-dire l'ensemble $\mathscr{F}/\sim$ des classes d'équivalence pour la relation $\sim$.

Pour tout $(P,Q) \in \mathscr{F}$, on note $\dfrac{P}{Q}$ sa classe d'équivalence.

Remarque. Par définition, $\dfrac{P_1}{Q_1} = \dfrac{P_2}{Q_2}$ si, et seulement si, $P_1 Q_2 = P_2 Q_1$.

Propriété 47

Tout élément F de $\mathbb{K}(X)$ peut s'écrire $F = \dfrac{P}{Q}$ avec $P \wedge Q = 1$.

Une telle écriture est appelée *forme irréductible de* F, et est unique à multiplication près par des scalaires non nuls.

Propriété 48

- On définit deux lois de composition internes $+$ et $\times$ sur $\mathbb{K}(X)$ en posant, pour tout $F = \dfrac{A}{B}$ et $G = \dfrac{C}{D}$:
$$F + G = \frac{AD + BC}{BD} \quad \text{et} \quad F \times G = \frac{AC}{BD}.$$
- L'ensemble $\mathbb{K}(X)$ muni des lois $+$ et $\times$ est un corps, d'éléments neutres $\dfrac{0}{1}$ pour $+$ et $\dfrac{1}{1}$ pour $\times$.
- L'application $j : P \in \mathbb{K}[X] \mapsto \dfrac{P}{1} \in \mathbb{K}(X)$ est un morphisme d'anneaux injectif, permettant d'identifier la fraction rationnelle $\dfrac{P}{1}$ au polynôme P, et donc de voir $\mathbb{K}[X]$ comme un sous-anneau de $\mathbb{K}(X)$.

Définition.

Soit $F \in \mathbb{K}(X)$. Alors la quantité $\deg(A) - \deg(B)$ ne dépend pas du représentant $\dfrac{A}{B}$ de F. On l'appelle le *degré de* F et on le note $\deg(F)$.

Exemple. $\deg\left(\dfrac{X^2+1}{X^3(X^2+2)}\right) = 2 - 5 = -3$.

Remarque. On vérifie que :

- pour tout $F, G \in \mathbb{K}(X)$, $\deg(F+G) \leq \max(\deg(F), \deg(G))$ et $\deg(F \times G) = \deg(F) + \deg(G)$,
- pour tout $P \in \mathbb{K}[X]$, $\deg(P) = \deg\left(\dfrac{P}{1}\right)$.

6.2 Racines et pôles

Définition.

Soit $F = \dfrac{A}{B}$ une fraction rationnelle écrite sous **forme irréductible**.
On appelle *zéro de* F toute racine de A et *pôle de* F toute racine de B. L'*ordre d'un zéro* (resp. *d'un pôle*) de F est alors sa multiplicité en tant que racine de A (resp. de B).

Définition.

Soit $F = \frac{A}{B}$ une fraction rationnelle écrite sous **forme irréductible**, et soit E l'ensemble des pôles de F.
On appelle *fonction rationnelle associée à* F la fonction
$$\widetilde{F} : \begin{array}{ccc} \mathbb{K} \setminus E & \to & \mathbb{K} \\ x & \mapsto & \dfrac{A(x)}{B(x)} \end{array}.$$

Propriété 49

Soit $F \in \mathbb{K}(X)$. Il existe un unique couple $(E, Q) \in \mathbb{K}[X] \times \mathbb{K}(X)$ tel que :

$$F = E + Q \quad \text{et} \quad \deg(Q) < 0.$$

On dit alors que E *est la partie entière de* F.

Méthode. Comment obtenir la partie entière d'une fraction rationnelle ?

Pour obtenir la partie entière d'une fraction rationnelle $F = \dfrac{A}{B}$, *on effectue la division euclidienne de* A *par* B *:* E *est le quotient dans cette division euclidienne.*

6.3 Décomposition en éléments simples

Théorème 50 (Décomposition en éléments simples)

Soit $F = \frac{P}{Q} \in \mathbb{K}(X)$ de degré strictement négatif, et soit $Q = Q_1^{\alpha_1} \cdots Q_n^{\alpha_n}$ la décomposition de Q en produit de facteurs irréductibles.
Il existe une unique famille de polynômes $A_{1,1}, \ldots, A_{1,\alpha_1}, \ldots, A_{n,1}, \ldots A_{n,\alpha_n}$ tels que :

$$\begin{aligned} F &= \frac{A_{1,1}}{Q_1} + \frac{A_{1,2}}{Q_1^2} + \cdots + \frac{A_{1,\alpha_1}}{Q_1^{\alpha_1}} + \frac{A_{2,1}}{Q_2} + \cdots + \frac{A_{2,\alpha_2}}{Q_2^{\alpha_2}} + \cdots + \frac{A_{n,1}}{Q_n} + \cdots + \frac{A_{n,\alpha_n}}{Q_n^{\alpha_n}} \\ &= \sum_{i=1}^{n} \sum_{k=1}^{\alpha_i} \frac{A_{i,k}}{Q_i^k}. \end{aligned}$$

avec pour tout $i \in [\![1, n]\!]$, pour tout $k \in [\![1, \alpha_i]\!]$, $\deg(A_{i,k}) < \deg(Q_i)$.

La démonstration de ce résultat est hors programme. On retiendra les conséquences suivantes.

Corollaire 51 (Décomposition en éléments simples sur $\mathbb{C}$)

Soit $F = \dfrac{A}{B} \in \mathbb{C}(X)$, avec $B = \alpha \displaystyle\prod_{i=1}^{n} (X - \lambda_i)^{m_i}$. Alors il existe un unique polynôme $E \in \mathbb{C}[X]$ et une unique famille de complexes $\alpha_{1,1}, \ldots, \alpha_{1,m_1}, \alpha_{2,1}, \ldots, \alpha_{2,m_2}, \ldots, \alpha_{n,m_n}$ tels que :

$$\begin{aligned} F &= E + \frac{\alpha_{1,1}}{X - \lambda_1} + \cdots + \frac{\alpha_{1,m_1}}{(X - \lambda_1)^{m_1}} + \cdots + \frac{\alpha_{n,1}}{X - \lambda_n} + \cdots + \frac{\alpha_{n,m_n}}{(X - \lambda_n)^{m_n}} \\ &= E + \sum_{i=1}^{n} \sum_{k=1}^{m_t} \frac{\alpha_{i,k}}{(X - \lambda_i)^k}. \end{aligned}$$

Corollaire 52 (Décomposition en éléments simples sur $\mathbb{R}$)

Soit $F = \dfrac{A}{B} \in \mathbb{R}(X)$, où la décomposition en produit de facteurs irréductibles de B est

$$B = \alpha \prod_{i=1}^{n} (X - \lambda_i)^{m_t} \prod_{k=1}^{r} \left(X^2 + b_k X + c_k\right)^{p_k}.$$

Alors il existe un unique polynôme $E \in \mathbb{R}[X]$ et une unique famille de réels $\alpha_{1,1}, \ldots, \alpha_{1,m_1}, \ldots, \alpha_{n,m_n}, \beta_{1,1}, \ldots, \beta_{1,p_1}, \ldots, \beta_{r,p_r}, \gamma_{1,1}, \ldots, \gamma_{r,p_r}$ tels que

$$F = E + \sum_{i=1}^{n} \sum_{j=1}^{m_l} \frac{\alpha_{i,j}}{(X - \lambda_i)^j} + \sum_{k=1}^{r} \sum_{\ell=1}^{p_k} \frac{\beta_{k,\ell} X + \gamma_{k,\ell}}{(X^2 + b_k X + c_k)^\ell}.$$

Les méthodes rencontrées en début d'année pour le calcul de la décomposition en éléments simples restent valables. Ajoutons deux choses :

- Si α est un pôle simple de F, c'est-à-dire si $F = \dfrac{P}{Q} = \dfrac{P}{(X-\alpha)Q_1}$, avec $Q_1(\alpha) \neq 0$, alors la partie polaire de F associée à α est de la forme $\dfrac{\lambda}{X - \alpha}$ et :

  $$\lambda = \left.\frac{P}{Q_1}\right|_{X=\alpha} = \frac{P(\alpha)}{Q_1(\alpha)}.$$

  Par ailleurs, $Q' = ((X-\alpha)Q_1]' = (X-\alpha)Q_1' + Q_1$, et donc $Q'(\alpha) = Q_1(\alpha)$. Donc la partie polaire associée au pôle simple α est $\dfrac{P(\alpha)}{Q'(\alpha)} \dfrac{1}{X - \alpha}$.

- Pour une fraction rationnelle réelle, on pourra la décomposer sur $\mathbb{C}$, puis regrouper les termes conjugués deux à deux afin d'obtenir sa décomposition en éléments simples sur $\mathbb{R}$. On pensera aussi à prendre le conjugué de sa décomposition sur $\mathbb{C}$ et utiliser l'unicité afin d'obtenir des relations sur les coefficients.

Exercice 13 Décomposer en éléments simples les fractions rationnelles suivantes :

- $\dfrac{X^5}{1 - X^4}$ sur $\mathbb{R}$;
- $\dfrac{1}{X^n - 1}$ $(n \in \mathbb{N}^*)$ sur $\mathbb{C}$;
- $\dfrac{P'}{P}$ où P est un polynôme scindé (sur $\mathbb{R}$ ou $\mathbb{C}$).