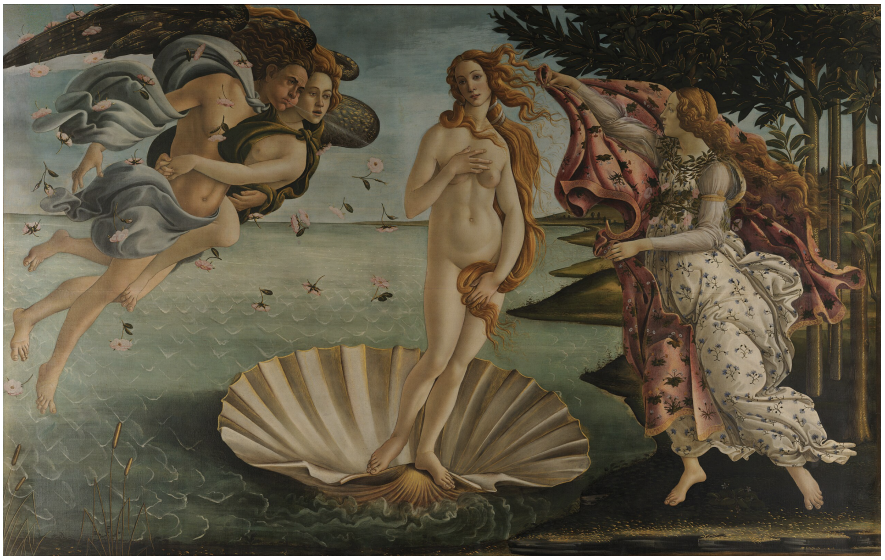
ALG 11 | Polynômes à coefficients dans $\mathbb{K}$

On fonde une théorie des polynômes indépendemment de celle des fonctions. Cette version formelle des polynômes se généralise à d'autres corps que $\mathbb{R}$ et $\mathbb{C}$, comme par exemple les corps finis.



Naissance de Vénus, Sandro Botticelli

L'héritage mathématique grec se résume à l'arithmétique et à la géométrie. Certes, quelques savants (cf. **Diophante**) ont abordé la résolution des équations mais sans aucun recours au symbolisme et en reposant systématiquement leurs travaux sur des considérations géométriques.

Lagrange

La naissance de l'Algèbre date du Moyen-Age arabe, période où les mathématiques se sont progressivement détachées de l'influence de la géométrie : le savant **Al-Khwarizmi** jette les bases de cette nouvelle branche des mathématiques dans son *Abrégé du calcul par restauration et comparaison*, à l'origine du mot *Al-jabr*[1], algèbre. Il fallut cependant attendre l'époque de **Claude Viète** et de **René Descartes** pour que se développe le calcul littéral sur les inconnues x, y, etc. Dès cette époque les savants recherchent les relations existant entre les cœfficients d'un polynômes et ses racines.

Ces développements aboutirent à l'invention des nombres complexes (cf. **Bombelli**, **Gauss**, etc.), au théorème fondamental de l'algèbre (cf. **D'Alembert**, **Gauss**) et aux travaux d'**Evariste Galois** sur les groupes de permutation et la résolubilité des équations algébriques.

Seule figure au programme la résolution *générale* des équations de degré deux. Il faut cependant savoir qu'il existe des méthodes *générales* de résolution des équations de degré trois (cf. les travaux de **Scipion del Ferro**) et quatre (cf. **Ferrari** et plus tardivement **Lagrange**). Après de nombreux échecs concernant l'ordre cinq, **Evariste Galois** prouva au début du XIX$^{\text{e}}$ siècle qu'au-delà de l'ordre quatre, il n'existe aucune *formule générale* permettant de calculer les racines d'un polynôme à l'aide de radicaux.

1. Algèbre $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$

Une expression de la forme $p_0 + p_1 x + p_2 x^2 + \cdots + p_n x^n$ où $n \in \mathbb{N}$ a un sens lorsque les variables p_k $(0 \leqslant k \leqslant n)$ et x appartiennent à un anneau $(A, +, \times)$. Mais quel sens précis faut-il donner au mot « *expression* » ? La réponse la plus immédiate est de définir cette « *expression* » comme l'application φ de $\mathbb{A}$ dans $\mathbb{A}$ telle que, pour tout élément x de $\mathbb{A}$, $\varphi(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_n x^n$; ce type de fonction est appelée *une fonction polynomiale* à coefficients dans A de la variable x. Cette première approche s'avère en fait incomplète.

Plaçons-nous un instant dans le cas où l'anneau $\mathbb{A}$ est le corps $\mathbb{F}_2 := \{0, 1\}$. Les opérations + et × sont définies par :

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Considérons les fonctions polynomiales de $\mathbb{F}_2$ dans $\mathbb{F}_2$ définies par $f(x) = x^2 + x$ et $g(x) = x^3 + x$. Puisque $0^n = 0$ et $1^n = 1$ pour tout entier naturel non nul n, ces deux fonctions coïncident sur $\mathbb{F}_2$. Une affirmation telle que f *est de degré* 2 *et* g *de degré* 3 n'a donc aucun sens puisque $f = g$. Cependant, les *formules* définissant f et g sont effectivement différentes. La définition d'une expression du type

1. Ce mot signifie littéralement « *remplissage ou réduction d'une fracture* ». Chez Cervantès, le mot *algebrista* désigne un rebouteux.

précédent comme une *fonction de* $\mathbb{F}_2$ *dans* $\mathbb{F}_2$ est donc insuffisante car elle ne permet pas de distinguer entre les deux *formules*. Cette remarque permet de cerner l'intérêt de la notion de polynôme : différencier une *expression* du type précédent de la fonction qu'elle définit.

Nous allons introduire dans ce chapitre la notion générale de polynôme à coefficients dans le corps $\mathbb{R}$ ou $\mathbb{C}$, et verrons que dans ce cas, il est possible d'identifier un polynôme à la fonction polynomiale qui lui est associée. L'ensemble des définitions de cette partie sont cependant généralisables à n'importe quel corps $(\mathbb{k},+,\times)$ et l'exemple précédent prouve qu'il faut alors distinguer les notions de polynôme et de fonction polynomiale.

Les développements récents de la cryptologie[2] utilisent les propriétés des polynômes à coefficients dans un corps $\mathbb{K}$ fini, cadre dans lequel cette distinction n'est pas gratuite.

Dans tout ce qui suit, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$. Dans l'esprit du *mécano* de la théorie des ensembles, nous allons construire l'ensemble des polynômes à coefficients dans $\mathbb{K}$ à partir des ensembles dont nous disposons. L'objectif de ce premier paragraphe est de définir un polynôme comme une suite $(p_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ nulle à partir d'un certain rang[3] : $\exists n_0\in\mathbb{N}$, $\forall n\geqslant n_0$, $p_n=0$. Le polynôme correspondant à l'expression x^3+x sera $(0,1,1,0,\ldots)$ et celui correspondant à x^4-2x+1 sera $(1,-2,0,1,0,\ldots)$, les points de suspension signifiant que la suite stationne à la valeur 0. Il restera alors à définir trois opérations sur les polynômes, celles correspondant aux calculs suivants :

$$(x^3+x)+(x^4-2x+1)=x^4+x^3-x+1,\ (x^3+x)\times(x^4-2x+1)=x^7+x^5-2x^4+x^3-2x^2+x$$

et $3(x^3+x)=3x^3+3x$.

1.1. Polynômes à coefficients dans $\mathbb{K}$

Définition 11.0. Polynômes formels à coefficients dans $\mathbb{K}$

On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite $P=(p_n)_{n\in\mathbb{N}}$ nulle à partir d'un certain rang. On note $\mathbb{K}^{(\mathbb{N})}$ l'ensemble de ces suites.

Une suite nulle à partir d'un certain rang est également appelée une suite *presque nulle*.

Définition 11.0. Opérations sur les polynômes

Pour tous $P=(p_n)_{n\in\mathbb{N}}\in\mathbb{K}^{(\mathbb{N})}$, $Q=(q_n)_{n\in\mathbb{N}}\in\mathbb{K}^{(\mathbb{N})}$ et $\lambda\in\mathbb{K}$, on pose

$$P+Q=(p_n+q_n)_{n\in\mathbb{N}},\ \lambda P=(\lambda p_n)_{n\in\mathbb{N}}\quad\text{et}\quad PQ=(c_n)_{n\in\mathbb{N}}\quad\text{où}\quad\forall n\in\mathbb{N},\ c_n=\sum_{k=0}^{n}p_kq_{n-k}$$

Ces opérations définissent respectivement une loi interne, externe à domaine d'opérateurs $\mathbb{K}$ et une loi interne sur $\mathbb{K}^{(\mathbb{N})}$.

Cette définition du produit peut paraître déroutante au premier regard... En fait, elle est tout à fait naturelle quand on se pose la question suivante : quel est le coefficient de x^n dans le produit

$$\left(\sum_{k\in\mathbb{N}}p_kx^k\right)\left(\sum_{k\in\mathbb{N}}q_kx^k\right)\ ?$$

2. Étymologiquement *science du secret*, la cryptologie est la science du codage et du décodage de données, une discipline à mi-chemin entre les mathématiques et l'informatique. Les cryptologues sont nos amis : c'est grâce à eux que nous pouvons effectuer en toute sécurité des transactions bancaires sur internet.

3. Rappelons que l'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites d'éléments de $\mathbb{K}$ a été défini dans le chapitre sur les structures algébriques.

Ce produit fait apparaître après développement des expressions de la forme $p_k x^k q_\ell x^\ell = p_k q_\ell x^{k+\ell}$. Pour trouver le coefficient de x^n il faut donc sommer tous les $p_k q_\ell$ tels que $k+\ell = n$, d'où la définition choisie.
Nous regroupons dans la proposition suivante l'ensemble des règles de calcul sur les polynômes. Toutes les vérifications sont élémentaires et laissées au lecteur.

Proposition 11.1. Structure d'algèbre de $\mathbb{K}[X]$

$(\mathbb{K}^{(\mathbb{N})}, +, \cdot, \times)$ est une $\mathbb{K}$-algèbre associative et commutative.

Ajoutons que les éléments neutres pour les lois + et × sont respectivement égaux à $(0,\dots)$ et $(1,0,\dots)$. L'anneau $(\mathbb{K}[X], +, \times)$ étant commutatif, la formule du binôme de Newton y est valable. Comme dans tout anneau commutatif, les formules du binôme et de factorisation de $A^n - B^n$ sont appliquables dans $\mathbb{K}[X]$.

1.2. Base canonique de l'algèbre $\mathbb{K}[X]$

L'écriture sous forme de suite presque nulle d'un polynôme est très lourde à manipuler. Le recours à l'indéterminée X, qui n'est autre qu'un polynôme particulier, permet d'alléger à la fois les raisonnements et les calculs.

Définition 11.2. L'indéterminée X

On note X l'unique élément de $\mathbb{K}^{(\mathbb{N})}$ dont le seul terme non nul est celui d'indice 1 et vaut 1, c'est-à-dire $X = (0,1,0,\dots)$.

Attention, il ne faut pas confondre le polynôme X avec une variable. Dès que le contexte fait intervenir l'anneau $\mathbb{K}[X]$, la lettre majuscule X est une notation réservée (au même titre que la lettre i des nombres complexes). On n'écrira donc JAMAIS des phrases du type « *en posant* $X = \dots$ » qui n'ont aucun sens !

Définition 11.3. L'algèbre $\mathbb{K}[X]$ (↯ 11.1)

On rassemble ici quelques propriétés usuelles.

- ⇛ On prouve par récurrence que, pour tout $k \in \mathbb{N}^*$, $X^k = (0,\dots,0,1,0,\dots)$ (k zéros au début).
- ⇛ Les polynômes de la forme λX^k où $k \in \mathbb{N}$ et $\lambda \in \mathbb{K}$ sont appelés des monômes.
- ⇛ Soit $(p_n)_{n\in\mathbb{N}} \in \mathbb{K}^{(\mathbb{N})}$. Il existe un entier naturel n_0 tel que $\forall n > n_0\ ,\ p_n = 0$. On pose

$$\sum_{k\in\mathbb{N}} p_k X^k = \sum_{k=0}^{n_0} p_k X^k$$

  Cette notation a l'avantage d'éviter le recours à l'entier n_0 et d'alléger en conséquence les démonstrations.
- ⇛ La notation $\mathbb{K}^{(\mathbb{N})}$ de l'ensemble des polynômes sur le corps $\mathbb{K}$ est désormais caduque. Nous noterons désormais $\mathbb{K}[X]$ cet ensemble.

On prendra garde à la notation $\sum_{n\in\mathbb{N}} p_n X^n$: il ne s'agit pas d'une limite mais en fait d'une somme finie car les p_k sont nuls APCR. Toutes les sommes de ce chapitre seront finies !

Proposition 11.4. Base canonique de $\mathbb{K}[X]$

L'algèbre $\mathbb{K}[X]$ est de dimension infinie et $(X^n)_{n\in\mathbb{N}}$ en est une base, appelée base canonique de $\mathbb{K}[X]$. Ainsi, pour tout $P \in \mathbb{K}[X]$, il existe une unique $(p_n) \in \mathbb{K}^{(\mathbb{N})}$ telle que $P = \sum_{k\in\mathbb{N}} p_k X^k$. Les p_k sont appelés coefficients du polynôme P.

Les polynômes $(a, 0, \ldots)$ sont appelés *polynômes constants*. L'application $\phi : \mathbb{K} \to \mathbb{K}[X]$ définie par

$$a \mapsto aX^0 = (a, 0, \ldots)$$

vérifie les propriétés $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ et $\phi(1) = 1$ (ce dernier « 1 » désignant le neutre de $\mathbb{K}[X]$). C'est un morphisme d'anneaux injectif dont l'image est l'ensemble des polynômes constants. Par cette propriété de morphisme, $\phi(\mathbb{K})$ (ensemble des polynômes constants) est donc un corps isomorphe à $\mathbb{K}$. On fera l'abus suivant d'écriture : on notera a le polynôme aX^0, i.e. on identifie le scalaire a et le polynôme constant aX^0. Via cette identification, on a donc $\mathbb{K} \subset \mathbb{K}[X]$. En particulier, l'élément neutre $X^0 = (1, 0, \ldots)$ pour la loi $\times$ est égal à 1 et l'élément neutre $(0, \ldots)$ pour la loi $+$ est égal à 0.

Identification des coefficients

On déduit de la proposition précédente un résultat bien connu : deux polynômes sont égaux *si et seulement si* ils ont les mêmes coefficients, c'est-à-dire, pour toutes suites presque nulles (p_n) et (q_n)

$$\sum_{k\in\mathbb{N}} p_k X^k = \sum_{k\in\mathbb{N}} q_k X^k \iff \forall k \in \mathbb{N},\ p_k = q_k$$

On formalise ici en particulier la notion bien connue de degré.

Soit un polynôme $P = (p_n)$ non nul ; de manière équivalente

$$P = \sum_{k\in\mathbb{N}} p_k X^k \neq 0$$

Posons $E = \{k \in \mathbb{N} ;\ p_k \neq 0\}$. Puisque la suite (p_n) est non nulle, E est non vide. Comme cette suite est presque nulle, E est une partie majorée[4] de $\mathbb{N}$. E admet donc un plus grand élément (noté n) en tant que partie non vide et majorée de $\mathbb{N}$. On a donc

$$P = p_0 + \cdots + p_n X^n$$

Définition 11.5. Degré

Soit $P \in \mathbb{K}[X]$.

⇛ Si $P = 0$, on pose

$$\deg(P) = -\infty$$

⇛ Si

$$P = \sum_{n\in\mathbb{N}} p_n X^n \neq 0$$

on note $\deg(P)$ le plus grand entier naturel n tel que $p_n \neq 0$. L'entier $\deg(P)$ est appelé degré du polynôme P.

✕ Par exemple, $P := (X+1)^5 - 1 - X^5 = 5X^4 + 10X^3 + 10X^2 + 5X$ par la formule du binôme donc $\deg P = 4$.

Le choix de la convention $\deg 0 = -\infty$ est loin d'être arbitraire. Il permet d'éviter les cas particuliers dans les théorèmes qui suivent, moyennant quelques conventions. On posera désormais $-\infty + (-\infty) = -\infty$ et, pour tout $n \in \mathbb{N}$, $n + (-\infty) = (-\infty) + n = -\infty$.

4. En effet, si $p_n = 0$ dès que $n \geqslant n_0$, l'entier n_0 est un majorant de E.

Définition 11.6. Coefficient dominant, polynôme unitaire (↯ 11.2)

Soit P un polynôme non nul, de degré $n \geqslant 0$. Il s'écrit de manière unique $P = p_0 + \cdots + p_n X^n$ avec $p_n \neq 0$.

⇛ Le coefficient p_n est appelé coefficient dominant de P.

⇛ Un polynôme est dit unitaire lorsque son coefficient dominant vaut 1.

La proposition suivante rassemble les principales propriétés du degré.

Proposition 11.7. Propriétés du degré

Soit P et Q dans $\mathbb{K}[X]$.

a. $\deg(PQ) = \deg P + \deg Q$ et $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$.

b. Si $\deg P \neq \deg Q$, on a $\deg(P+Q) = \max(\deg P, \deg Q)$; c) $\forall \lambda \in \mathbb{K}^*$, $\deg(\lambda P) = \deg P$.

Par une récurrence facile, on étend ces formules à m polynômes :

$$\deg \prod_{i=1}^{m} P_i = \sum_{i=1}^{m} \deg P_i \quad \text{et} \quad \deg \sum_{i=1}^{m} P_i \leqslant \max_{i \in [\![1,m]\!]} \deg P_i$$

On retiendra facilement la formule exprimant $\deg(PQ)$ en visualisant le produit PQ de la manière suivante,

$$\text{si } P = \sum_{k=0}^{n} p_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{n'} q_k X^k, \quad \text{alors} \quad PQ = p_0 q_0 + \cdots + p_n q_{n'} X^{n+n'}$$

où les pointillés désignent une somme de monômes de degré compris strictement entre 0 et $n+n'$.

L'anneau $\mathbb{K}[X]$ est intégre, ie pour tous polynômes P et Q, $PQ = 0$ *si et seulement si* $P = 0$ ou $Q = 0$. Ceci découle de la formule du degré de $\deg PQ$, qui justifie les équivalences suivantes : $PQ = 0$ *si et seulement si* $\deg PQ = -\infty$, *si et seulement si* $\deg P = -\infty$ ou $\deg Q = -\infty$.

Attention au polynôme nul!

Il faut toujours faire attention quand on parle du degré d'un polynôme P : c'est un entier si $P \neq 0$, sinon il vaut $-\infty$. Il faut donc mettre de côté de cas de $P = 0$, au moyen d'une disjonction de cas.

Proposition 11.8. Sev des polynômes de degré inférieur à n

Soit $n \in \mathbb{N}$. L'ensemble des polynômes de degré inférieur ou égal à n, noté $\mathbb{K}_n[X]$, est un sev de dimension finie de $\mathbb{K}[X]$. La famille $(1, X, \ldots, X^n)$ est une base de $\mathbb{K}_n[X]$, dite base canonique de $\mathbb{K}_n[X]$. En particulier, $\dim \mathbb{K}_n[X] = n+1$.

Définition 11.9. Famille de polynômes de degrés étagés

Une famille $(P_0, \ldots, P_n)$ de polynômes est dite de degrés étagés si $0 \leqslant \deg P_0 < \deg P_1 < \cdots < \deg P_n$.

On notera que la condition $\deg(P_0) \geqslant 0$ impose que $P_0 \neq 0$. Plus généralement, le caractère étagé des degrés est une condition suffisante de liberté.

Proposition 11.10. Familles de polynômes de degrés étagés

Toute famille de polynômes de degrés étagés est libre.

✘ On pose $H_0 = 1$ et, pour $k \in \mathbb{N}^*$, $H_k = X(X-1)\cdots(X-k+1)$. Pour tout $n \in \mathbb{N}$, la famille $(H_0, \dots, H_n)$ est une base de $\mathbb{K}_n[X]$, appelée base de Hilbert. En effet, pour tout $k \in [\![0, n]\!]$, $\deg H_k = k$ (produit de k polynômes de degré un, en utilisant l'extension des formules du 1.2) : $(H_0, \dots, H_n)$ est donc une famille de polynômes de degrés étagés.

2. Substitution dans une $\mathbb{K}$-algèbre

La notation X symbolise la capacité de l'indéterminée à être *remplacée* dans un polynôme par n'importe quel élément a d'une $\mathbb{K}$-algèbre $\mathbb{A}$. Par exemple, pour $M \in \mathscr{M}_n(\mathbb{K})$, on pourra donner un sens à $P(M)$ (on dit que l'on *substitue* M à X), utiliser la notation $\mathbb{K}[M]$, etc.

Définition 11.11. Substitution dans une $\mathbb{K}$-algèbre

Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre d'élément neutre $1_{\mathbb{A}}$ et $a \in \mathbb{A}$.

⇛ Pour $P = p_0 + p_1 X + \ldots + p_n X^n \in \mathbb{K}[X]$, on pose $P(a) = p_0 1_{\mathbb{A}} + p_1 a + \cdots + p_n a^n$.

⇛ On note $\mathbb{K}[a] := \{P(a) ; P \in \mathbb{K}[X]\}$.

La notion de substitution permet donc d'unifier différents cadres (fonctions polynomiales, composition des polynômes, polynômes de matrices, etc).

✘ Soit $P := X^3 - X + 1$.

- ✔ Substitution dans $\mathbb{A} := \mathbb{K}$: $P(2) = 2^3 - 2 + 1 = 7$.
- ✔ Substitution dans $\mathbb{A} := \mathbb{K}[X]$: $P(X^2) = (X^2)^3 - (X^2) + 1 = X^6 - X^2 + 1$.
- ✔ Substitution dans $\mathbb{A} := \mathscr{M}_2(\mathbb{K})$: On a $P(A) = A^3 - A + I_2$ pour $A \in \mathscr{M}_2(\mathbb{K})$.

✘ Lorsque $Q = X$, on a $P(Q) = p_0 + p_1 X + \ldots + p_n X^n = P$ et on peut donc écrire que $P(X) = P$. Attention, il ne faudra en revanche pas confondre f et $f(x)$ pour des fonctions polynomiales.

- ✔ Plus généralement, pour deux polynômes P et Q, on note également $P \circ Q$ la substitution $P(Q)$. Ce polynôme est appelé polynôme composé de P et Q.
- ✔ Déterminons les polynômes P de $\mathbb{K}[X]$ vérifiant $P(X+1) = P(X)$. On va établir que $P(X+1) = P(X)$ *si et seulement si* P est de degré nul. Si P est de degré nul, alors $P(X+1) = P(X)$. Montrons la réciproque par contraposition. Supposons que $\deg P \geqslant 1$, notons n ce degré et $P = \sum_{k=0}^{n} p_k X^k$. On a
$$P(X+1) - P(X) = \sum_{k=0}^{n} p_k \left((X+1)^k - X^k\right) = \sum_{k=1}^{n} p_k \left((X+1)^k - X^k\right)$$
Pour k dans $\mathbb{N}^*$, on a $(X+1)^k - X^k = \sum_{\ell=0}^{k-1} \binom{k}{\ell} X^\ell$, polynôme de degré $k-1$. Comme $p_n \neq 0$, on en déduit que $\deg(P(X+1) - P(X)) = n-1$ donc $P(X+1) - P(X) \neq 0$.

Les propriétés de la substitution sont générales. En particulier, le c) est équivalent à la linéarité de l'application $P \mapsto P(a)$.

Proposition 11.12. Propriétés de la substitution

Pour tout $a \in \mathbb{K}$, tout $(P,Q) \in \mathbb{K}[X]^2$ et tout $\lambda \in \mathbb{K}$, on a :

a. $(P+\lambda Q)(a) = P(a) + \lambda Q(a)$; **b.** $(PQ)(a) = P(a)Q(a)$; **c.** $(P \circ Q)(a) = P(Q(a))$.

Par exemple, si $P = (X-a)(X-b) + X^3$, $z \in \mathbb{K}$ et $A \in \mathscr{M}_2(\mathbb{K})$, on peut donc écrire $P(A) = (A - aI_2)(A - bI_2) + A^3$ et $P(z) = (z-a)(z-b) + z^3$ par les propriétés a. et b.

On a jusqu'à ici considéré des propriétés de l'application de substitution $P \mapsto P(a)$. Nous retournons à présent le point de vue en nous intéressant à l'application d'évaluation $a \mapsto P(a)$.

Définition 11.13. Fonction polynomiale associée à un polynôme

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$. L'application $\widetilde{P} : \mathbb{K} \to \mathbb{K}$ définie par $\widetilde{P}(x) = P(x)$ est appelée fonction polynomiale associée à P.

On dit également que le nombre $P(a)$ est la valeur du polynôme P en a. Évaluer un polynôme P en a, c'est calculer le scalaire $P(a)$.

3. Dérivation sur $\mathbb{K}[X]$

Comme pour la composition, il s'agit de définir formellement la dérivée d'un polynôme, sans recourir à la notion de limite.

Définition 11.14. Dérivée d'un polynôme (↯ 11.3)

On note $D : \mathbb{K}[X] \to \mathbb{K}[X]$ l'unique application linéaire telle que $D(1) = 0$ et $\forall n \in \mathbb{N}^*$, $D(X^n) = nX^{n-1}$. Pour tout P dans $\mathbb{K}[X]$, on note $P' := D(P)$ (ce polynôme est appelé polynôme dérivé de P).

Le lecteur est familier avec ces calculs :

- On a donc pour tout $P = \sum_{k=0}^{n} p_k X^k \in \mathbb{K}[X]$, $P' = \sum_{k=1}^{n} k p_k X^{k-1}$ (convention 0 si $n = 0$).
- Le polynôme dérivé de $P = X^4 - 6X^3 + 2$ vaut $P' = 4X^3 - 18X^2$.
- Il est clair qu'un polynôme $P \in \mathbb{K}[X]$ vérifie $P' = 0$ *si et seulement si* P est constant, c'est-à-dire $P \in \mathbb{K}_0[X] = \mathbb{K}$.

Proposition 11.15. Propriétés de la dérivation

En reprenant les notations de la définition ci-dessus :

a. $\forall (P,Q) \in \mathbb{K}[X]^2$, $(PQ)' = P'Q + PQ'$;

b. Pour tous $n \in \mathbb{N}^*$ et $P \in \mathbb{K}[X]$, $(P^n)' = nP'P^{n-1}$;

c. Pour tous polynômes P et Q dans $\mathbb{K}[X]$, on a $(P \circ Q)' = Q' \times (P' \circ Q)$.

Nous venons de construire une notion de dérivation *formelle et purement algébrique* des polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$, c'est-à-dire sans faire appel à des passages à la limite, à des taux d'accroissement, etc. Cependant, dans le cas où $P \in \mathbb{R}[X]$, la dérivée de la fonction polynomiale $\widetilde{P}$ associée à

P est bien définie et notée $(\widetilde{P})'$. Il est clair que cette *fonction* est la fonction polynomiale associée au polynôme dérivé $D(P) = P'$ de P. Ainsi, pour tout $P \in \mathbb{R}[X]$, on a $\widetilde{D(P)} = \widetilde{P'} = (\widetilde{P})'$. Nous ne savons pas encore dériver des fonctions de la variable complexe. Dans tout ce qui suit, seule la *dérivée formelle* de $P \in \mathbb{C}[X]$ aura un sens.

L'itération de l'opération de dérivation permet de définir des polynômes dérivés de tout ordre entier.

Définition 11.16. Dérivées successives

Pour tout $k \in \mathbb{N}^*$, la composée $D^k = D \circ \dots D$ (k fois) est bien définie et pour tout polynôme $P \in \mathbb{K}[X]$, on note $P^{(k)} = D^k(P)$ et on l'appelle polynôme dérivé d'ordre k de P.

On adoptera la convention usuelle $D^0 = \mathrm{id}_{\mathbb{K}[X]}$. Ainsi, $\forall P \in \mathbb{K}[X],\ P^{(0)} = P$. On notera souvent P'' au lieu de $P^{(2)}$.

- Posons par exemple $P := X^4 - 5X^3 + 4X + 1$. On a $P' = 4X^3 - 15X^2 + 4$, $P'' = 12X^2 - 30X$, $P^{(3)} = 24X - 30$, $P^{(4)} = 24$ et, pour tout entier $k \geqslant 5$, $P^{(k)} = 0$.
- Plus généralement, pour tout $n \in \mathbb{N}^*$, on a $\operatorname{Ker} D^n = \mathbb{K}_{n-1}[X]$.

Le lecteur pourra aborder le test (↯ 11.4). Par une récurrence facile, on prouve la formule suivante.

Proposition 11.17. Dérivées successives d'un monôme (↯ 11.5)

Soit $n \in \mathbb{N}$, $a \in \mathbb{K}$ et $P = (X - a)^n$. On a alors

$$\forall k > n,\ P^{(k)} = 0 \quad \text{et} \quad \forall k \leqslant n,\ P^{(k)} = \frac{n!}{(n-k)!}(X-a)^{n-k}$$

L'identité de Leibniz $(PQ)' = P'Q + PQ'$ se généralise à un ordre n quelconque de la manière suivante.

Proposition 11.18. Formule de Leibniz

$$\forall (P,Q) \in \mathbb{K}[X]^2,\ \forall n \in \mathbb{N},\ (PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}.$$

Le lecteur aura remarqué que la preuve de la formule de Leibniz est en tout point similaire à la démonstration de la formule du binôme.

Proposition 11.19. Formule de Taylor

$$\forall n \in \mathbb{N},\ \forall P \in \mathbb{K}_n[X],\ \forall a \in \mathbb{K},\ P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k.$$

Ce théorème montre que la formule de Taylor-Young, démontrée dans le cours d'asymptotique AN 6, est *exacte* pour les polynômes, ie le reste en o est nul si on applique la formule à un ordre supérieur ou égal au degré du polynôme.

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

Nous allons définir sur $\mathbb{K}[X]$ une arithmétique analogue à celle des entiers relatifs. Le point de départ sera bien sûr la définition de la notion de divisibilité et la mise en évidence d'une division euclidienne sur $\mathbb{K}[X]$.

Définition 11.20. Divisibilité dans $\mathbb{K}[X]$

Soit A et B dans $\mathbb{K}[X]$.

⇛ On dit que A est divisible par B, que B divise A ou encore que A est un multiple de B lorsqu'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$. On note alors $B \mid A$.

⇛ L'ensemble des multiples de A est noté $A\mathbb{K}[X] = \{AP\,;\, P \in \mathbb{K}[X]\}$.

✗ Par exemple, le polynôme $X^4 + X$ est divisible par les polynômes X et $X^3 + 1$, mais également par le polynôme $X + 1$ puisque $X^4 + X = (X+1)(X^3 - X^2 + X)$.

✗ Plus généralement, pour tout $n \in \mathbb{N}$, $X^{2n+1} + 1$ est divisible par $X + 1$ car

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

Il existe sur l'anneau $\mathbb{K}[X]$ *une division euclidienne* analogue à celle de $(\mathbb{Z}, +, \times)$. Elle est au fondement de l'arithmétique des polynômes. Effectuer la division d'un polynôme A par un autre polynôme B non nul revient à écrire A sous la forme $A = BQ + R$ avec $(Q, R) \in \mathbb{K}[X]^2$ et $\deg(R) < \deg(B)$. La proposition suivante établit l'existence et l'unicité de ce couple (Q, R).

✗ Effectuons, avant une preuve générale, la division euclidienne de $A = X^2 - 2X + 1$ par $B = X - 3$.

On recherche un monôme Q_1 tel que $\deg(A - Q_1 B) < \deg A$: $Q_1 = X$ convient. Puis on détermine un monôme Q_2 tel que

$$\deg(A - Q_1 B - Q_2 B) < \deg(A - Q_1 B)$$

$Q_2 = 1$ convient. Puisque $\deg(A - Q_1 B - Q_2 B) < \deg B$, la division est terminée.

$X^2 - 2X + 1$	$X - 3$
$-(X^2 - 3X)$	$X + 1$
$= X + 1$	
$-(X - 3)$	
$= 4$	

Ainsi $X^2 - 2X + 1 = (X+1)(X-3) + 4$. On *pose* la division euclidienne sur $\mathbb{K}[X]$ comme ci-dessus.

Proposition 11.21. Division euclidienne dans $\mathbb{K}[X]$ (↯ 11.6)

Soit A et B dans $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un unique couple de polynômes (Q, R) de $\mathbb{K}[X]$ tel que

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B)$$

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

L'unicité dans la division euclidienne sur $\mathbb{K}[X]$ permet d'affirmer qu'un polynôme $B \neq 0$ divise A *si et seulement si* le reste dans la division euclidienne de A par B est nul.

✗ Effectuons la division euclidienne de $A = X^4 + X^2 + 2$ par $B = X^2 - 3$. En adoptant la notation décrite ci-dessus :

$$\begin{array}{r|l} X^4+X^2+X+2 & X^2-3 \\ \hline -(X^4-3X^2) & X^2+4 \\ \hline = 4X^2+X+2 & \\ -(4X^2-12) & \\ \hline = X+14 & \end{array} \qquad \text{ainsi } A=(X^2+4)B+(X+14)$$

✗ Déterminons le reste dans la division euclidienne de $P\in\mathbb{K}[X]$ par $X-a$ puis $(X-a)^2$ où $a\in\mathbb{K}$.

✔ Comme $\deg(X-a)=1$, le reste dans la division euclidienne de P par $X-a$ est un polynôme constant λ. En notant Q le quotient, on a $P=(X-a)Q+\lambda$. En substituant a à X dans cette relation, on a $P(a)=\lambda$.

✔ Passons à la division euclidienne par $(X-a)^2$. On peut procéder de même : le reste dans la division euclidienne de P par $(X-a)^2$ est de la forme $uX+v$. En notant Q le quotient, on a $P=(X-a)^2Q+uX+v$. On en tire $P(a)=ua+v$ et $P'(a)=u$ d'où $uX+v=P(a)+P'(a)(X-a)$. On peut retrouver ce résultat en appliquant la formule de Taylor :

$$P(X)=\sum_{k\in\mathbb{N}}\frac{P^{(k)}(a)}{k!}(X-a)^k=P(a)+P'(a)(X-a)+(X-a)^2\sum_{k\geqslant 2}\frac{P^{(k)}(a)}{k!}(X-a)^{k-2}$$

qui donne directement la division euclidienne de P par $(X-a)^2$.

5. Racines d'un polynôme

On commence par une définition bien connue.

Définition 11.22. Racine(s) d'un polynôme (↯ 11.7)

Soit $P\in\mathbb{K}[X]$ et α dans $\mathbb{K}$. On dit que α est une racine[5] de P lorsque $P(\alpha)=0$, autrement dit lorsque α est un zéro de la fonction $\widetilde{P}:\mathbb{K}\to\mathbb{K}$.

Une équation de la forme $P(\alpha)=0$ où $P\in\mathbb{K}[X]$ est appelée une équation algébrique sur $\mathbb{K}$. Elle est dite de degré $n\in\mathbb{N}$ lorsque $\deg(P)=n$. Le lecteur est renvoyé au chapitre sur les nombres complexes où il trouvera la méthode générale de résolution des équations algébriques de degré deux sur $\mathbb{C}$.

Le lecteur peut ici aborder le test (↯ 11.8).

5.1. Majoration du nombre de racines

Nous allons faire le lien entre la notion de racine et l'arithmétique des polynômes.

Proposition 11.23.

Soit $P\in\mathbb{K}[X]$ et $a\in\mathbb{K}$. Alors a est une racine de P *si et seulement si* $(X-a)\mid P$.

Ce résultat se généralise au cas de $m\geqslant 1$ racines par des arguments d'arithmétique.

5. Le terme « racine » provient d'une analogie avec un arbre : les cœfficients sont les branches de l'arbre, les racines sont la partie souterraine, cachée du polynôme.

Proposition 11.24.

Si $a_1, \dots, a_m$ sont des racines deux à deux distinctes de $P \in \mathbb{K}[X]$, alors $(X - a_1) \dots (X - a_m) \mid P$.

Nous sommes maintenant en mesure d'établir le résultat central de ce paragraphe : le degré d'un polynôme non nul P de $\mathbb{K}[X]$ est un majorant du nombre de ses racines dans $\mathbb{K}$.

Proposition 11.25.

Tout polynôme $P \in \mathbb{K}[X]$ non nul admet au plus $\deg P$ racines dans $\mathbb{K}$.

On en déduit immédiatement que le seul polynôme admettant une infinité de racines dans $\mathbb{K}$ est le polynôme nul.

Comment montrer qu'un polynôme est nul ?

Un polynôme $P \in \mathbb{K}[X]$ est nul *si et seulement si* il admet une infinité de racines dans $\mathbb{K}$.

✗ Déterminons les polynômes $P \in \mathbb{K}[X]$ tels que $P(X+1) = P(X)$. Considérons un tel polynôme et posons $Q := P - P(0)$. On a $Q(X+1) = Q(X)$ et $Q(0) = 0$. Pour $n \in \mathbb{N}$, on a $Q(n+1) = Q(n)$ et on en déduit par une récurrence facile que $Q(n) = 0$ pour tout $n \in \mathbb{N}$. Comme Q est admet une infinité de racines, Q est nul. Ainsi Q est constant. Il est clair que, réciproquement, tout polynôme constant P vérifie $P(X+1) = P(X)$.

Nous avons maintenant les outils pour mieux comprendre les liens entre *polynômes* et *fonctions polynomiales* dans le cas où le corps de base est $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Proposition 11.26.

L'application $F : \mathbb{K}[X] \to \mathbb{K}^{\mathbb{K}}$ définie par $F(P) = \widetilde{P}$ est injective.

Autrement dit, deux polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$ sont égaux *si et seulement si* leurs fonctions polynomiales associées sont égales. Le lecteur aura remarqué que le caractère infini du corps $\mathbb{K}$ joue un rôle central dans cette démonstration. Comme nous l'avons vu en introduction de ce chapitre, les polynômes $P_1 = X^3 + X$ et $P_2 = X^2 + X$ sur $\Bbbk := \mathbb{F}_2 = \{0, 1\}$ sont distincts bien que $\widetilde{P_1} = \widetilde{P_2}$.

5.2. Le théorème de D'Alembert-Gauss

Nous avons démontré dans le chapitre consacré aux nombres complexes que tout polynôme de degré deux à coefficients dans $\mathbb{C}$ admet une racine dans $\mathbb{C}$. Ce résultat est généralisable à un polynôme de degré quelconque mais non constant.

Theoreme 11.27. D'Alembert-Gauss

Tout $P \in \mathbb{C}[X]$ non constant admet une racine dans $\mathbb{C}$.

Ce théorème est admis. Il existe de nombreuses démonstrations de ce théorème, reposant sur des considérations analytiques.

Corollaire 11.28.

Pour tout $P \in \mathbb{C}[X]$ non constant de degré n, $\exists (z_1, \dots, z_n, \lambda) \in \mathbb{C}^{n+1}$, $P = \lambda \prod_{k=1}^{n} (X - z_k)$.

✗ Pour tout polynôme P non constant de $\mathbb{C}[X]$, la fonction $\widetilde{P} : \mathbb{C} \to \mathbb{C}$ est surjective.

✔ Soit $\omega \in \mathbb{C}$. Comme $P - \omega$ n'est pas constant, on déduit du théorème de D'Alembert-Gauss que $P - \omega$ admet au moins une racine z_0 dans $\mathbb{C}$. Ainsi, $\omega = \widetilde{P}(z_0)$.

✔ On en déduit que $\widetilde{P}$ est surjective.

Définition 11.29. Polynôme scindé

Un polynôme $P \in \mathbb{K}[X]$ est dit scindé sur $\mathbb{K}$ s'il existe $n \in \mathbb{N}^*$, $(x_1, \dots, x_n) \in \mathbb{K}^n$ et $\lambda \in \mathbb{K}^*$ tels que

$$P = \lambda \prod_{k=1}^{n} (X - x_k)$$

Autrement dit, un polynôme est scindé sur $\mathbb{K}$ *si et seulement si* il est le produit de polynômes de $\mathbb{K}[X]$ de degré un. On peut donc reformuler le théorème de d'Alembert-Gauss : tout polynôme de $\mathbb{C}[X]$ non constant est scindé sur $\mathbb{C}$.

5.3. Multiplicité d'une racine

À toute racine d'un polynôme non nul est associée une multiplicité.

Définition 11.30. Multiplicité ou ordre d'une racine

Soit $P \in \mathbb{K}[X] \setminus \{0\}$ et $a \in \mathbb{K}$.

⇛ Il existe un plus grand entier naturel n tel que $(X-a)^n \mid P$. Cet entier est appelé la multiplicité (ou encore l'ordre) de a dans le polynôme P. On notera $\mu_a(P)$ cette multiplicité. En particulier, a est racine de P si et seulement si $\mu_a(P) \neq 0$.

⇛ Une racine de multiplicité un est dite simple. Une racine est dite multiple si elle n'est pas simple.

⇛ On a $n = \mu_a(P)$ si et seulement si il existe $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^n Q$ et $Q(a) \neq 0$.

La multiplicité n de a dans P est donc la plus grande puissance de $X - a$ factorisable dans P. Cette notion généralise les valuations p-adiques de l'arithmétique entière.

lemme 11.31. Multiplicativité de la multiplicité

Pour tout P et Q dans $\mathbb{K}[X]$ non nuls et a dans $\mathbb{K}$, on a $\mu_a(PQ) = \mu_a(P) + \mu_a(Q)$.

Cette proposition s'étant par une récurrence facile à un produit fini de polynômes.

Proposition 11.32.

Si $a_1, \dots, a_m$ sont des racines deux à deux distinctes de multiplicités respectives $\mu_1, \dots, \mu_m$ de $P \in \mathbb{K}[X]$ non nul, alors $(X-a_1)^{\mu_1} \dots (X-a_m)^{\mu_m} \mid P$.

On en déduit immédiatement le corallaire suivant.

Corollaire 11.33.

Tout $P \in \mathbb{K}[X]$ de degré n admet au plus n racines dans $\mathbb{K}$ comptées avec leurs multiplicités.

Dans la pratique, le calcul de la multiplicité d'une racine a de $P \in \mathbb{K}[X]$ s'effectue rarement en recherchant la plus grande puissance de $X-a$ divisant P. La proposition suivante montre que l'on peut déterminer cette multiplicité en calculant les nombres $P^{(k)}(a)$, pour $k \in \mathbb{N}$.

Proposition 11.34. Caractérisation de la multiplicité par les dérivées (↯ 11.9)

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $n \in \mathbb{N}^*$. Il y a équivalence entre les propriétés suivantes :

a. le nombre a est une racine de multiplicité n de P ;

b. $\forall k \in [\![0, n-1]\!],\ P^{(k)}(a) = 0$ et $P^{(n)}(a) \neq 0$.

Les racines appartenant à $\mathbb{C} \setminus \mathbb{R}$ d'un polynôme à coefficients réels vont toujours par deux : on peut les regrouper par paires de racines conjuguées. Ce résultat repose sur le lemme suivant.

Lemme 11.35.

Pour tous $Q \in \mathbb{R}[X]$ et $a \in \mathbb{C}$, $\overline{Q(a)} = Q(\overline{a})$.

Appliquons ce lemme aux couples de racines conjuguées d'un polynôme à coefficients réels.

Proposition 11.36. Conjugué d'une racine (↯ 11.10)

Soit $P \in \mathbb{R}[X]$, $n \in \mathbb{N}^*$ et $a \in \mathbb{C}$. Le nombre a est une racine de P de multiplicité n *si et seulement si* le nombre $\overline{a}$ est une racine de P de multiplicité n.

✘ Déterminons les racines du polynôme $P = X^6 + X^5 + 3X^4 + 2X^3 + 3X^2 + X + 1$ sachant que i est une racine multiple de P.

✔ On a $P(i) = 0$ (les termes s'annulent deux à deux symétriquement par rapport au milieu).

✔ Le nombre i est racine double de P car

$$\begin{cases} P'(i) &= 6i^5 + 5i^4 + 12i^3 + 6i^2 + 6i + 1 = 6i + 5 - 12i - 6 + 6i + 1 = 0 \\ P''(i) &= 30i^4 + 20i^3 + 36i^2 + 12i + 6 = 30 - 20i - 36 + 12i + 6 = -8i \neq 0 \end{cases}$$

✔ Comme P est réel, son conjugué $-i$ est aussi racine double de P. On en déduit que le polynôme $(X-i)^2(X+i)^2 = (X^2+1)^2$ divise P dans $\mathbb{C}[X]$.

✔ En posant la division euclidienne de P par $\left(X^2+1\right)^2 = X^4+2X^2+1$, on trouve

$$P = \left(X^2+1\right)^2\left(X^2+X+1\right)$$

Comme $X^2+X+1 = (X-j)\left(X-j^2\right)$, les racines de P sont i (de multiplicité deux), $-i$ (de multiplicité deux), j et j^2.

6. Polynômes irréductibles sur $\mathbb{K}$

L'objectif de cette partie est de définir une classe de polynômes qui joueraient le même rôle que les nombres premiers sur $\mathbb{Z}$, puis d'en déduire l'analogue polynomial du théorème fondamental de l'arithmétique des nombres entiers.

Définition 11.37. Irréductibilité (↯ 11.11)

Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible sur $\mathbb{K}$ si P n'est pas constant et ses seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes constants et ceux de la forme λP, où $\lambda \in \mathbb{K}^*$. Un polynôme non irréductible sur $\mathbb{K}$ est dit réductible sur $\mathbb{K}$. Ainsi :

$$P \text{ est réductible sur } \mathbb{K} \iff \exists Q \in \mathbb{K}[X],\ Q \mid P \ \text{ et } \ 0 < \deg Q < \deg P$$

Un polynôme irréductible sur $\mathbb{K}$ est donc « *incassable* » par division dans $\mathbb{K}[X]$.

La précision « sur $\mathbb{K}$ » dans la définition précédente est essentielle.

✘ Le polynôme X^2+1 n'est pas irréductible sur $\mathbb{C}$ car il se factorise en $X^2+1 = (X-i)(X+i)$ dans $\mathbb{C}[X]$. En revanche, X^2+1 est irréductible sur $\mathbb{R}$. Prouvons cette dernière affirmation par l'absurde : si X^2+1 n'était pas irréductible sur $\mathbb{R}$, il admettrait un diviseur $Q \in \mathbb{R}[X]$ de degré 1. Ce dernier admettant nécessairement une racine réelle a, on aurait $a^2+1=0$, ce qui absurde car a est réel.

✘ Les polynômes X^3+1 et X^4+1 sont réductibles sur $\mathbb{R}$ et sur $\mathbb{C}$. Le polynôme X^2+X+1 est irréductible sur $\mathbb{R}$ mais pas sur $\mathbb{C}$. En effet :

- ✔ On a $X^3+1 = X^3-(-1)^3 = (X+1)\left(X^2-X+1\right)$ donc X^3+1 est réductible sur $\mathbb{R}$ et $\mathbb{C}$.
- ✔ On a $X^4+1 = \left(X^2+1\right)^2-2X^2 = \left(X^2-\sqrt{2}X+1\right)\left(X^2+\sqrt{2}X+1\right)$ d'où la même conclusion.
- ✔ On a $X^2+X+1 = (X-j)(X-j^2)$ donc X^2+X+1 est réductible sur $\mathbb{C}$.
- ✔ Raisonnons par l'absurde en supposant X^2+X+1 réductible sur $\mathbb{K}$. Il existe donc $Q \in \mathbb{R}[X]$ diviseur non trivial de X^2+X+1. Ainsi, nécessairement $\deg Q = 1$. Or, un polynôme de degré un de $\mathbb{R}[X]$ admet une racine réelle. Ainsi X^2+X+1 admet une racine réelle ce qui est absurde car son discriminant est strictement négatif.

Proposition 11.38. Irréductibles sur $\mathbb{C}$ et sur $\mathbb{R}$ (↯ 11.12)

On note $\mathscr{I}_{\mathbb{K}}$ l'ensemble des polynômes irréductibles sur $\mathbb{K}$.

a. $\mathscr{I}_{\mathbb{C}} = \left\{P \in \mathbb{C}[X],\ \deg P = 1\right\}$.

b. Un polynôme P appartient à $\mathscr{I}_{\mathbb{R}}$ si et seulement si il est de degré un ou s'il est de degré deux et de discriminant strictement négatif.

Le théorème fondamental de l'arithmétique affirme qu'il est possible de factoriser un polynôme quelconque $P \in \mathbb{K}[X]$ à l'aide des constantes non nulles (qui sont les éléments inversibles de l'anneau $\mathbb{K}[X]$) et des polynômes irréductibles sur $\mathbb{K}$.

Théorème 11.39. fondamental de l'arithmétique

Soit $P \in \mathbb{K}[X]$ un polynôme non constant. Il existe un unique entier $m \in \mathbb{N}$, un unique nombre $\lambda \in \mathbb{K}$, un unique m-uplet (à permutation près) de couples $(P_1, \alpha_1), \dots, (P_m, \alpha_m)$, où les P_i sont polynômes unitaires irréductibles sur $\mathbb{K}$ deux à deux distincts et les α_i sont des entiers naturels non nuls tels que

$$P = \lambda \prod_{k=1}^{m} P_k^{\alpha_k}$$

Cette décomposition est appelée décomposition de P en produit de facteurs irréductibles sur $\mathbb{K}$.

✘ Décomposons en produit d'irréductibles sur $\mathbb{R}$ et sur $\mathbb{C}$ le polynôme $P = X^3 - 1$. On a

$$P = (X-1)\left(X^2 + X + 1\right) \text{ (les deux facteurs sont irréductibles sur } \mathbb{R})$$

Sur $\mathbb{C}$, on a classiquement $P = (X-1)(X-j)\left(X-j^2\right)$.

On peut bien-sûr généraliser aux racines n-ème de l'unité.

Proposition 11.40. Racines n-ème de l'unité

Soit $n \in \mathbb{N}^*$. On a

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

✘ On peut en déduire une expression simplifiée de $\pi := \prod_{k=1}^{n-1} \sin\frac{k\pi}{n}$ où $n \in \mathbb{N}$ vérifie $n \geqslant 2$.

✔ Pour $k \in [\![1, n-1]\!]$, on a $\sin\frac{k\pi}{n} = \frac{e^{\frac{-ik\pi}{n}}}{2i}\left(e^{\frac{2ik\pi}{n}} - 1\right)$ d'où

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

Comment passer de $\mathbb{C}$ à $\mathbb{R}$? (↯ 11.13)

Pour trouver la factorisation de $P \in \mathbb{R}[X]$ en produit de polynômes irréductibles sur $\mathbb{R}$ à partir de sa factorisation en produit de polynômes irréductibles sur $\mathbb{C}$, on regroupe les racines non réelles du polynôme P par paires de conjugués $(a, \overline{a})$ afin d'obtenir un polynôme à coefficients réels. En effet, on a $(X-a)(X-\overline{a}) = X^2 - 2\mathrm{Re}(a)X + |a|^2$.

- Déterminons la décomposition en produit de facteurs irréductibles sur $\mathbb{R}$ de $P = (X+1)^7 - X^7 - 1$ sachant que j est une racine multiple de P. Nous ferons un usage intensif des relations $1 + j + j^2 = 0$ et $j^3 = 1$ dans ce qui suit. De plus on remarque par la formule du binôme que $\deg P = 6$ avec un coefficient dominant qui vaut 7.
  - On a $P(j) = (1+j)^7 - j^7 - 1 = -j^{14} - j^7 - 1 = -\left(j^2 + j + 1\right) = 0$. De même, $P'(j) = 7j^{12} - 7j^6 = 0$ et $P''(j) = -42j^{10} - 42j^5 = 42$. Ainsi j est racine double de P.
  - Comme P est réel, on en déduit que son conjugué j^2 est également racine double de P. Par d'Alembert-Gauss, P admet 6 racines (comptées avec multiplicité). Nous en avons pour l'instant 4, il en manque deux.
  - Avant de se lancer dans des calculs, on regarde s'il y a des racines évidentes. On s'aperçoit facilement que 0 et -1 sont racines de P.
  - Nous avons donc toutes les racines complexes de P, ainsi que son coefficient dominant d'où

$$P = 7X(X+1)(X-j)^2\left(X-j^2\right) = 7X(X+1)\left(X^2+X+1\right)^2$$

- Dans certains cas, on peut décomposer en produit d'irréductibles sur $\mathbb{R}$ sans passer sur $\mathbb{C}$, en utilisant des identités remarquables. Considérons par exemple $P = X^4 + 1$. On remarque que

$$P = \left(X^2+1\right)^2 - 2X^2 = \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right)$$

  La décomposition sur $\mathbb{R}$ est terminée car ces deux trinômes sont de discriminants strictement négatifs. C'est bien plus rapide que de calculer les racines complexes de P !

7. Relations entre les coefficients et les racines

Nous allons généraliser les relations bien connues suivantes :

$$(z-z_1)(z-z_2) = z^2 - \sigma_1 z + \sigma_2, \quad \text{où} \quad \begin{cases} \sigma_1 &= z_1 + z_2 \\ \sigma_2 &= z_1 z_2 \end{cases}$$

exprimant les coefficients d'un polynôme complexe en fonction de ses racines.

Définition 11.41. Fonctions symétriques élémentaires (↯ 11.14)

Soit $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in \mathbb{K}^n$. On note, pour tout entier $k \in [\![1, n]\!]$,

$$\sigma_k(x_1, \dots, x_n) = \sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} x_{i_1} \dots x_{i_k}$$

Les $\sigma_k : \mathbb{K}^n \to \mathbb{K}$ pour $k \in [\![1, n]\!]$ sont appelées fonctions symétriques élémentaires d'ordre n.

La notation σ_k est ambigüe : cette fonction dépend également de l'entier naturel non nul n. On écrira souvent σ_k au lieu de $\sigma_k(x_1, \dots, x_n)$ afin d'alléger les notations.

Par exemple, pour $n = 2$, on a $\sigma_1 = x_1 + x_2$ et $\sigma_2 = x_1 x_2$; pour $n = 3$, on a

$$\sigma_1 = x_1 + x_2 + x_3\,,\ \sigma_2 = x_1x_2 + x_2x_3 + x_3x_1 \ \text{ et } \ \sigma_3 = x_1x_2x_3$$

L'adjectif « *symétrique* » signifie que les fonctions σ_k sont invariantes par permutation *quelconque* de leurs n variables : pour tout $\tau \in \mathfrak{S}_n$, $(x_1, x_2, \dots, x_n) \in \mathbb{K}^n$, on a $\sigma_k(x_{\tau(1)}, \dots, x_{\tau(n)}) = \sigma_k(x_1, \dots, x_n)$. On pourra aborder avec profit le test (↯ 11.15).

On rencontre les fonctions symétriques élémentaires lorsque l'on cherche à développer des expressions du type $\prod_{k=1}^{n} (X - x_k)$.

✗ Par exemple, $(X - x_1)(X - x_2) = X^2 - (x_1 + x_2)X + x_1 x_2 = X^2 - \sigma_1 X + \sigma_2$.

✗ Dans le cas de trois racines x_1, x_2 et x_3, on a

$$\begin{aligned} P &= \lambda(X - x_1)(X - x_2)(X - x_3) = \lambda\left(X^3 - (x_1 + x_2 + x_3)X^2 + (x_1x_2 + x_2x_3 + x_3x_1)X - x_1x_2x_3\right) \\ &= \lambda\left(X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3\right) \end{aligned}$$

On calcule donc les coefficients d'un polynôme dont on connaît les racines au moyen des fonctions symétriques élémentaires. La proposition suivante généralise nos calculs à un nombre $n \geqslant 1$ quelconque de racines.

Proposition 11.42. Relations coefficients-racines (↯ 11.16)

Pour $n \in \mathbb{N}^*$ et $(x_1, \dots, x_n) \in \mathbb{K}^n$, on a $P = \prod_{k=1}^{n} (X - x_k) = X^n + \sum_{i=0}^{n-1} (-1)^{n-k} \sigma_{n-k} X^k$.

✗ Soit a, b et c les racines du polynôme $P = X^3 + 2X + 2$. Calculons $S = a^4 + b^4 + c^4$. Soit z une racine de P. On a $z^3 = -2z - 2$ d'où $z^4 = -2z^2 - 2z$. On en déduit que

$$S = -2\left(a^2 + b^2 + c^2\right) - 2(a + b + c)$$

Notons σ_1, σ_2 et σ_3 les fonctions symétriques élémentaires de a, b et c. On a $P = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ d'où $\sigma_1 = 0$, $\sigma_2 = 2$ et $\sigma_3' = -2$. Ainsi $a + b + c = 0$ et $ab + bc + ca = 2$ d'où $a^2 + b^2 + c^2 = \sigma_1^2 - 2\sigma_2 = -4$ d'où $S = 8$.

✗ Explicitons un polynôme de degré trois à coefficients entiers dont a^2, b^2 et c^2 sont les racines. Il s'agit de déterminer $Q := \left(X - a^2\right)\left(X - b^2\right)\left(X - c^2\right) = X^3 - \sigma_1' X^2 + \sigma_2' X - \sigma_3'$ où σ_1', σ_2' et σ_3' les fonctions symétriques élémentaires de a^2, b^2 et c^2. Ainsi

$$\sigma_1' = a^2 + b^2 + c^2 = -4\,,\ \sigma_2' = a^2b^2 + b^2c^2 + c^2a^2 = \sigma_2^2 - 2abc(a + b + c) = 4\,,\ \sigma_3' = a^2b^2c^2 = \sigma_3^2 = 4$$

Ainsi $Q = X^3 + 4X^2 + 4X - 4$.

✗ Calculons, pour $n \in \mathbb{N}$ tel que $n \geqslant 2$, $\pi := \prod_{k=1}^{n-1} \dfrac{1}{1 - e^{\frac{2ik\pi}{n}}}$. Posons $z_k := \frac{1}{1 - e^{\frac{2ik\pi}{n}}}$ pour $k \in [\![1, n-1]\!]$.

✔ L'idée est de trouver un polynôme dont les z_k sont les racines.

✔ Fixons k dans $[\![1, n-1]\!]$. On a $e^{\frac{2ik\pi}{n}} = 1 - \frac{1}{z_k} = \frac{z_k - 1}{z_k}$ d'où

$$\left(\frac{z_k - 1}{z_k}\right)^n - 1 = 0 \quad \text{c'est-à-dire} \quad (z_k + 1)^n - z_k^n = 0$$

✔ Le polynôme $Q := (X + 1)^n - X^n$ est de degré $n - 1$, admet $z_1, \dots, z_{n-1}$ pour racines distinctes (par injectivité de $z \mapsto \frac{1}{1 - z}$) et l'on déduit de la formule du binôme que son coefficient dominant vaut n et sont terme constant vaut 1. Ainsi, par les relations coefficients-racines :

$$n(-1)^n \pi = 1 \quad \text{d'où} \quad \pi = \frac{(-1)^n}{n}$$

Le lecteur est renvoyé au test (↯ 11.17) afin de s'entraîner.

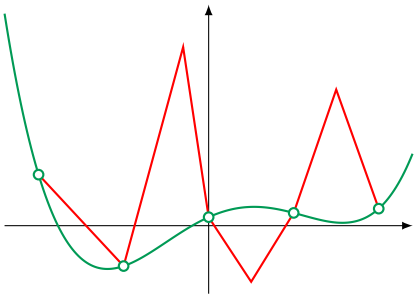
8. Introduction aux polynômes interpolateurs de Lagrange

On s'intéresse dans cette section à des polynômes prenant des valeurs fixées en des points donnés.

La problématique est la suivante : étant donnée une fonction $f : [a,b] \to \mathbb{R}$, $n \in \mathbb{N}$ et $a_0 < \cdots < a_n$ des éléments de $[a,b]$. On recherche les polynômes $P \in \mathbb{R}[X]$ qui interpolent f aux points a_0, …, a_n, i.e. tels que

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

Ci-contre une interpolation polynomiale P (en vert) d'une fonction f affine par morceaux (en rouge) aux points -1, $-\frac{1}{2}$, 0 $\frac{1}{2}$ et 1.



Proposition 11.43. Interpolation de Lagrange

Soit $n \in \mathbb{N}$, a_0, …, a_n deux à deux distincts dans $\mathbb{K}$ et $(y_0,\dots,y_n) \in \mathbb{K}^{n+1}$.

$$\exists! P \in \mathbb{K}_n[X]\ ,\ \forall i \in [\![0,n]\!]\ ,\ P(a_i) = y_i \qquad (\star)$$

On peut aborder la démonstration de deux façons : en reconnaissant un isomorphisme ou de manière plus constructive, en explicitant une solution.

Définition 11.44. Polynômes d'interpolation de Lagrange aux a_i

Soit $n \in \mathbb{N}$ et a_0, …, a_n deux à deux distincts dans $\mathbb{K}$. On appelle polynômes d'interpolation de Lagrange aux points a_0, …, a_n les éléments de l'unique famille $(L_0,\dots,L_n)$ de polynômes de $\mathbb{K}_n[X]$ définie par $\forall (i,j) \in [\![0,n]\!]^2$, $L_i(a_j) = \delta_{i,j}$. On peut l'expliciter :

$$\forall i \in [\![0,n]\!],\ L_i = \prod_{\substack{j \in [\![0,n]\!] \\ j \neq i}} \frac{X - a_j}{a_i - a_j}$$

Proposition 11.45. Interpolation de Lagrange, suite et fin

La famille $(L_0,\dots,L_n)$ est une base de $\mathbb{K}_n[X]$ et pour tout $P \in \mathbb{K}_n[X]$, $P = \sum_{k=0}^{n} P(a_k) L_k$.

- En appliquant ce résultat à $P := 1$, on obtient que $1 = L_0 + \cdots + L_n$.
- On en déduit également que l'unique solution de $(\star)$ dans $\mathbb{K}_n[X]$ est $\sum_{i=0}^{n} y_i L_i$.

Intérêt des polynômes interpolateurs de Lagrange

Outre la problématique originelle, on retiendra que ces polynômes apparaissent souvent lorsque l'on fait des hypothèses sur les valeurs que prend un polynôme sur un ensemble de points fixé.

✘ Déterminons les polynômes $P \in \mathbb{C}[X]$ vérifiant $P\langle\mathbb{C}\rangle \subset \mathbb{R}$.

✔ Soit P un tel polynôme. Fixons $n \in \mathbb{N}$ tel que $n \geqslant \deg P$. Notons $(L_0, \dots, L_n)$ les polynômes d'interpolation de Lagrange aux points $0, \dots, n$. Puisque $P \in \mathbb{C}_n[X]$, on a

$$P = \sum_{k=0}^{n} P(k) L_k \qquad (\star)$$

D'après l'expression des L_k (cf. ci-dessus), $L_k \in \mathbb{R}[X]$ pour tout $k \in [\![0, n]\!]$. Puisque $P\langle\mathbb{C}\rangle \subset \mathbb{R}$, les nombres $P(0), \dots, P(n)$ sont réels. On déduit donc de la formule $(\star)$ que $P \in \mathbb{R}[X]$.

9. Quelques résultats sur les fractions rationnelles

Les fractions rationnelles sont aux polynômes ce que les rationnels sont aux entiers relatifs. La construction de l'ensemble $\mathbb{Q}$ esquissée dans le cours ALG 1 peut être adaptée pour construire le corps des fractions rationnelles $\mathbb{K}(X)$ à coefficients dans $\mathbb{K}$ à partir de l'anneau $\mathbb{K}[X]$. Nous nous contenterons d'une approche informelle : une fraction rationnelle est une fonction qui est le quotient de deux fonctions polynomiales P et Q telles que $Q \neq 0$.

Le seul résultat figurant au programme est le suivant, qui décrit la décomposition en éléments simples de *certaines* fractions rationnelles :

Proposition 11.46. Décomposition en éléments simples

Pour tout $n\mathbb{N}^*$, $P \in \mathbb{K}_{n-1}[X]$, $x_1, \dots, x_n$ des éléments distincts de $\mathbb{K}$:

$$\exists!\,(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n,\ \forall x \in \mathbb{K} \setminus \{x_1, \dots, x_n\},\ \frac{P(x)}{(x - x_1) \times \cdots \times (x - x_m)} = \sum_{k=1}^{m} \frac{\lambda_k}{x - x_k}$$

✘ Considérons la fraction rationnelle $f : x \mapsto \dfrac{x^2+1}{x^3+3x^2+2x}$.

Comme

$$X^3 + 3X^2 + 2X = X\big(X^2 + 3X + 2\big) = X(X+1)(X+2) \quad \text{et} \quad \deg\big(X^2+1\big) < \deg\big(X^3 + 3X^2 + 2X\big)$$

le théorème précédent s'applique : il existe $(a, b, c) \in \mathbb{R}^3$ tel que

$$\forall x \in \mathbb{R} \setminus \{-2, -1, 0\},\ f(x) = \frac{x^2+1}{x(x+1)(x+2)} = \frac{a}{x} + \frac{b}{x+1} + \frac{c}{x+2}$$

On peut déterminer le triplet (a, b, c) en mettant au même dénominateur la fraction puis en identifiant les coefficients. Ceci aboutit à un système linéaire d'inconnue (a, b, c), facile à résoudre. Nous allons procéder différemment. L'existence de (a, b, c) est assurée.

✔ En multipliant par x la décomposition précédente, on obtient :

$$\forall x \in \mathbb{R} \setminus \{-2, -1, 0\},\ xf(x) = \frac{x^2+1}{x^2+3x+2} = a + b\frac{x}{x+1} + c\frac{x}{x+2}$$

En passant à la limite $x \to 0$, on obtient $\frac{1}{2} = a$.

✔ De même, en multipliant par $x+1$:

$$\forall x \in \mathbb{R}\setminus\{-2,-1,0\},\ (x+1)f(x) = \frac{x^2+1}{x(x+2)} = a\frac{x+1}{x} + b + c\frac{x+1}{x+2}$$

En passant à la limite $x \to -1$, on obtient $-2 = b$.

✔ De même, en multipliant par $x+2$:

$$\forall x \in \mathbb{R}\setminus\{-2,-1,0\},\ (x+2)f(x) = \frac{x^2+1}{x(x+1)} = a\frac{x+2}{x} + b\frac{x+2}{x+1} + c$$

En passant à la limite $x \to -2$, on obtient $\frac{5}{2} = c$.

✘ Considérons à présent la fraction rationnelle $g : x \mapsto \dfrac{x^5+2}{x^3+1}$.

Comme $\deg\left(X^5+2\right) > \deg\left(X^3+1\right)$, le théorème ne s'applique pas. On peut cependant s'y ramener au moyen d'une division euclidienne :

$$X^5+2 = \left(X^3+1\right)X^2 + 2 - X^2$$

Comme $X^3+1 = (X+1)(X+j)\left(X+j^2\right)$, il existe (a,b,c) dans $\mathbb{C}^3$ tel que

$$\forall x \in \mathbb{C}\setminus\left\{-1,-j,-j^2\right\},\ g(x) = x^2 + \frac{2-x^2}{(x+1)(x+j)\left(x+j^2\right)} = x^2 + \frac{a}{x+1} + \frac{b}{x+j} + \frac{c}{x+j^2}$$

On peut accélérer les calculs en remarquant qu'il existe (α,β,γ) dans $\mathbb{C}^3$ tel que

$$\forall x \in \mathbb{C}\setminus\left\{-1,-j,-j^2\right\},\ g(x) - x^2 = \frac{2-x^2}{(x+1)\left(x^2-x+1\right)} = \frac{\alpha}{x+1} + \frac{\beta x+\gamma}{x^2-x+1}$$

Il suffit pour cela de mettre au même dénominateur les deux derniers termes. On procède ensuite partiellement comme ci-dessus :

✔ Comme $(x+1)g(x) \xrightarrow[x\to-1]{} 0$, on en déduit que $\alpha = \dfrac{1}{3}$.

✔ En passant à la limite $x \to +\infty$ dans $x\left(g(x)-x^2\right)$, on en déduit que $-1 = \alpha+\beta$, i.e. $\beta = -\dfrac{4}{3}$.

✔ Puisque $g(0) = 2$, on a $2 = \alpha+\gamma$, d'où $\gamma = \dfrac{5}{3}$.

✘ Le cas où le dénominateur admet au moins une racine complexe multiple est hors programme. Dans cette situation, la forme de la décomposition n'est plus celle proposée dans le théorème ci-dessus. Par exemple,

$$\forall x \in \mathbb{R}\setminus\{0,-1\},\ \frac{1}{x^2(x+1)^3} = -\frac{3}{x} + \frac{1}{x^2} + \frac{3}{x+1} + \frac{2}{(x+1)^2} + \frac{1}{(x+1)^3}$$

10. Énoncés des tests

11.1.

Montrer que $X+3 \mid X^3+27$.

11.2.

Que dire du produit de deux polynômes unitaires ? De la somme de deux polynômes unitaires ? Que dire de leur différence ?

11.3.

L'application $D : \mathbb{K}[X] \to \mathbb{K}[X]$ est-elle injective ? surjective ?

11.4.

Déterminer $D^{-1}\Big\langle \{X\} \Big\rangle$.

11.5.

Soit $n \geqslant 1$. Quel est le polynôme dérivé d'ordre $(n-1)$ de X^{n+1} ?

11.6.

Effectuer la division euclidienne du polynôme $A = X^4+X^3+X^2+X+1$ par $B = X^2+X+1$.

11.7.

Montrer que, pour tout $n \in \mathbb{N}^*$, $\exists P \in \mathbb{R}[X]$ de degré $2n$ n'admettant aucune racine dans $\mathbb{R}$.

11.8.

Exprimer les racines complexes de $P = X^6-1$ à l'aide de $j = e^{2i\pi/3}$.

11.9.

Soit un polynôme $P \in \mathbb{K}[X]$ non nul et $a \in \mathbb{K}$ tels que $P(a) = P'(a) = P''(a) = 0$. Que dire de la racine a de P ?

11.10.

Existe-t-il un polynôme $P \in \mathbb{R}[X]$ dont les racines sont exactement i, $-i$, j et $-j$?

11.11.

Que pensez-vous de l'affirmation suivante : *un polynôme irréductible sur $\mathbb{K}$ n'admet aucune racine sur $\mathbb{K}$* ?

11.12.

Que pensez-vous de l'affirmation suivante : *un polynôme n'admettant aucune racine sur $\mathbb{R}$ est irréductible sur $\mathbb{R}$* ?

11.13.

Décomposer $P = X^4-1$ puis $Q = X^3+1$ sur $\mathbb{C}$ puis sur $\mathbb{R}$.

11.14.

Combien de termes dénombre-t-on dans σ_k ?

11.15.

Écrire les fonctions symétriques élémentaires d'ordre 4.

11.16.

On note $P = 2X^4 - 5X^2 + 1$. Calculer les fonctions symétriques élémentaires associées aux racines complexes de P.

11.17.

Exprimer $x_1^2 + x_2^2 + x_3^2$ en fonctions des σ_k des x_i.

11. Solutions

11.1.

On a

$$X^3 + 27 = (X+3)(X^2 - 3X + 9)$$

11.2.

Soit P et Q deux polynômes unitaires.

- ⇛ Le produit PQ est unitaire car, d'une manière général, le coefficient dominant de PQ est le produit des coefficients dominants de P et Q.
- ⇛ La somme de deux polynômes unitaires est unitaire *si et seulement si* les degrés des deux polynômes sont différents.
- ⇛ Pas d'équivalence aussi simple pour une différence : la différence de deux polynômes unitaires n'est pas toujours unitaire : cf. $X - X^2$ et $X^2 - (X^2 + 3X)$.

11.3.

Comme $\operatorname{Ker} D = \mathbb{K}_0[X] \neq \{0\}$, D n'est pas injective. En revanche, pour tout $n \in \mathbb{N}$, $D(X^{n+1}/(n+1)!) = X^n$ donc D est surjective.

11.4.

Il s'agit de résoudre l'équation linéaire $D(P) = X$. Comme $\operatorname{Ker}(D) = \mathbb{K}_0[X]$ et $D(X^2/2) = X$, on a

$$D^{-1}(\{X\}) = \left\{ \frac{X^2}{2} + \lambda \,;\, \lambda \in \mathbb{K} \right\}$$

11.5.

On trouve

$$\left(X^{n+1}\right)^{(n-1)} = \frac{(n+1)!}{2} X^2$$

11.6.

On trouve

$$Q = X^2$$
$$R = X + 1$$

11.7.

Considérer $(1 + X^2)^n$.

11.8.

Comme $X^6 - 1 = (X^3 - 1)(X^3 + 1)$, les racines de P sont les racines cubiques de ± 1, ie ± 1, $\pm j$, $\pm j^2$.

11.9.

On peut dire que a est racine de P avec une multiplicité au moins égale à trois.

11.10.

Non, par l'absurde : si $P \in \mathbb{R}[X]$ vérifie $P(j) = 0$, alors $P(\bar{j}) = P(j^2) = 0$. Or, $j^2 \notin \{-i, i, -j, j\}$.

11.11.

C'est faux : les polynômes de degré un sont tous irréductibles sur $\mathbb{K}$ et admettent une racine. En revanche, tout polynôme de degré supérieur ou égal à deux admettant une racine dans $\mathbb{K}$ est réductible.

11.12.

C'est faux : $(X^2 + 1)^2$ n'admet aucune racine réelle mais n'est pas irréductible sur $\mathbb{R}$.

11.13.

- ⇛ Les racines de P sont les racines quatrièmes de l'unité, ie ± 1 et $\pm i$. Ainsi,

  $$X^4 - 1 = (X+1)(X-1)(X+i)(X-i)$$

  et donc

  $$X^4 - 1 = (X+1)(X-1)(X^2+1)$$

- ⇛ Les racines de P sont les racines cubiques de -1, ie -1, $-j$ et $-j^2$. Ainsi,

  $$X^3 + 1 = (X+1)(X+j)(X+j^2)$$

  et donc

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

11.14.

La fonction σ_k comporte $\binom{n}{k}$ termes car

$$\#\left\{(i_1,\dots,i_k)\in[\![1,n]\!]^k\,;\,i_1<i_2<\cdots<i_k\right\}=\binom{n}{k}$$

11.15.

On a

$$\begin{aligned}
\sigma_1 &= x_1+x_2+x_3+x_4\\
\sigma_2 &= x_1x_2+x_1x_3+x_1x_4\\
&\quad +x_2x_3+x_2x_4+x_3+x_4\\
\sigma_3 &= x_1x_2x_3+x_1x_2x_4\\
&\quad +x_1x_3x_4+x_2x_3x_4\\
\sigma_4 &= x_1x_2x_3x_4
\end{aligned}$$

11.16.

On retrouve les relations coefficients-racines :

$$P(X)=2(X^4-\sigma_1X^3+\sigma_2X^2-\sigma_3X+\sigma_4)$$

ainsi

$$\sigma_1=0\sigma_2 \qquad =-5/2\sigma_3=0\sigma_4 \qquad =1/2$$

11.17.

On a clairement

$$x_1^2+x_2^2+x_3^2=\sigma_1^2-2\sigma_2$$