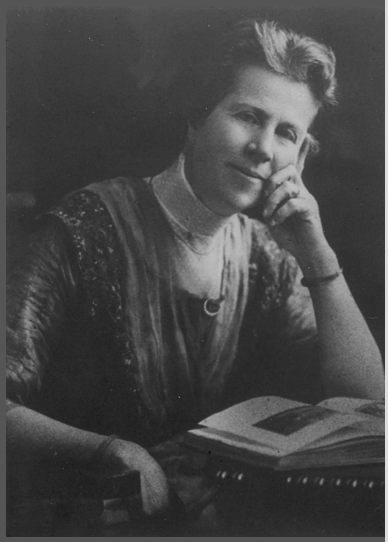
CHAPITRE 5

Polynômes



Grace Chisholm fut l'élève de Felix Klein, à Göttingen, et la première femme à soutenir et obtenir un doctorat en Allemagne. Avant elle, Sofia Kovaleskaïa avait obtenu un doctorat *in absentia*.

Grace Chisholm, née près de Londres, réussit les examens de Cambridge (mathematical Tripos) et d'Oxford (final honours), sans obtenir le droit d'y poursuivre ses études du fait de son sexe. Après avoir obtenu son doctorat en Allemagne, elle est rentrée en Angleterre et s'est mariée avec William Young. En 1896 ils partirent habiter en Suisse et, en suivant une suggestion de Felix Klein, s'intéressèrent à la théorie des ensembles et eurent des contributions majeures dans le domaine de la théorie des fonctions (dont la formule de Taylor-Young).

Grace est connue pour le théorème de Denjoy-Young-Saks dont elle a donné l'extension au cas des fonctions mesurables. Par ailleurs la plupart des articles attribués à William Young sont en fait des collaborations. Grace tapait ses articles, complétait les démonstrations et corrigeait les erreurs.

En sus de ses travaux mathématiques, elle accomplit des études de médecine (qu'elle arrêta juste avant l'internat), maîtrisa six langues, apprit la musique à ses six enfants et écrivit l'un des premiers livres pour enfants à être reproduit.

Introduction

Programme

Dans ce paragraphe, $\mathbf{K}$ est un sous-corps de $\mathbf{C}$.

— Idéaux de $\mathbf{K}[X]$, PGCD de deux polynômes, extension au cas d'une famille finie, relation de Bézout, lemme de Gauss. Irréductibles de $\mathbf{K}[X]$, existence et unicité de la décomposition en facteurs irréductibles. Les étudiant(e)s doivent connaître les irréductibles de $\mathbf{C}[X]$ et $\mathbf{R}[X]$. L'étude des polynômes sur un corps fini est hors programme.

— Exemples de suites de polynômes orthogonaux. Calcul explicite des polynômes d'une telle suite ; application à l'approximation des fonctions.

— Théorème de Weierstrass : toute fonction continue sur un segment y est limite uniforme de fonctions polynomiales. (Démonstration non exigible.)

— Pour u dans $\mathscr{L}(E)$, le noyau du morphisme d'algèbres $P \mapsto P(u)$ de $\mathbf{K}[X]$ dans $\mathscr{L}(E)$ est l'idéal annulateur de u et son image est la sous-algèbre commutative $\mathbf{K}[u]$ de $\mathscr{L}(E)$.

— Pour M dans $\mathscr{M}_n(\mathbf{K})$, le noyau du morphisme d'algèbres $P \mapsto P(M)$ de $\mathbf{K}[X]$ dans $\mathscr{M}_n(\mathbf{K})$ est l'idéal annulateur de M et son image est la sous-algèbre commutative $\mathbf{K}[M]$ de $\mathscr{M}_n(\mathbf{K})$.

— Polynôme minimal d'un endomorphisme d'un espace de dimension finie, d'une matrice carrée. Le polynôme minimal est unitaire. Si d est le degré du polynôme minimal de u, alors la famille $(u^k)_{0\leqslant k\leqslant d-1}$ est une base de $\mathbf{K}[u]$.

Une fonction polynomiale (réelle et d'une variable réelle) définie sur une partie I de $\mathbf{R}$ est une combinaison linéaire de fonctions puissances, i.e. de la forme

$$x \mapsto a_0 + a_1 x + \cdots + a_d x^d = \sum_{i=0}^{d} a_i x^i = \sum_{i\in\mathbf{N}} a_i x^i$$

où $(a_i)_{i\in\mathbf{N}}$ est une suite de réels nulle pour $i > d$ (où d est un entier naturel). On dit aussi que (a_i) est une suite presque nulle. La notation $\sum_{i\in\mathbf{N}}$ ne doit pas cacher le fait qu'il s'agit en réalité d'une somme finie et qu'il n'y a derrière aucune question de convergence.

Bien entendu (a_i) et x pourraient être à valeurs dans tout ensemble acceptant l'addition et la multiplication (un bi-magma donc), i.e. acceptant d'y faire de l'algèbre. Le mot « algèbre » provient du titre d'un ouvrage de Muhammad Ibn Mūsā al-Khuwārizmī (ca. 780-ca. 850) : *Kitāb al-mukhtaar fī isāb al-jabr wa-l-muqābala* (abrégé du calcul par la restauration et la comparaison). Le mot al-jabr signifie *réduction d'une fracture, réunion des morceaux, reconstruction, connexion, restauration.* En espagnol, le mot *algebrista* désigne aussi bien celui qui pratique le calcul algébrique que le rebouteux (celui qui sait réduire les fractures).

La notion de développement limité et les travaux de Grace et William Young permettent de voir localement une fonction f suffisamment régulière comme une fonction polynomiale. En 1797, Joseph-Louis Lagrange pense avoir démontré que toute fonction est somme de sa série de Taylor, ce qui lui permet d'écrire un traité d'analyse entièrement dégagé de toute considération d'infiniment petit, de limite et de fluxion (nom attribué par Newton aux dérivées). Mais en 1823 Cauchy montre que la formule de Taylor ne peut pas être acceptée en général. Toutefois, même si le caractère

local empêche d'obtenir une quelconque formule explicite pour f, valable sur son domaine de définition, elle permet de tracer la tangente à la courbe représentative de f, d'en trouver des éléments caractéristiques comme la courbure, la convexité etc.

Le rêve de LAGRANGE était donc d'écrire toute fonction f sous la forme de la somme de sa série de TAYLOR en un point, disons a, i.e.

$$\forall x \in I \qquad f(x) = \lim_{n\to+\infty} \sum_{k=0}^{n} a_k (x-a)^k$$

où, de plus, $a_k = \dfrac{f^{(k)}(a)}{k!}$. On peut l'écrire

$$\forall x \in I \qquad f(x) = \lim_{n\to+\infty} P_n(x)$$

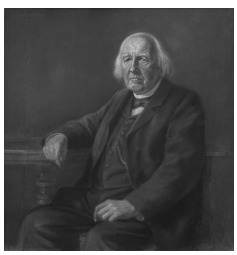
où P_n est une suite de fonctions polynomiales très particulière. En élargissant les suites de polynômes acceptables, Karl WEIERSTRASS a obtenu un résultat très puissant :

Théorème 5 - 1

Théorème d'approximation de WEIERSTRASS

Toute fonction f continue sur un segment I et à valeurs dans $\mathbf{R}$ est limite uniforme de fonctions polynomiales, i.e. pour tout ε strictement positif, il existe une fonction polynomiale P sur I telle que

$$\sup_{x\in I} |f - P| \leq \varepsilon \ .$$



Karl Weierstrass

Comme on le voit il ne s'agit pas seulement d'une convergence ponctuelle : non seulement on peut construire une suite de fonctions polynomiales (P_n) tendant vers f en chaque point, par exemple en prenant $\varepsilon = 2^{-n}$ et P_n associé à cet ε, mais la proximité de f et P_n est indépendante du point x (appartenant toutefois à un segment). On a en effet

$$\forall \varepsilon \in \mathbf{R}_+^* \quad \exists N \in \mathbf{N} \quad \forall n \in \mathbf{N} \quad \forall x \in I \qquad (n \geq N) \Longrightarrow |f(x) - P_n(x)| \leq \varepsilon$$

alors que la convergence ponctuelle se contenterait de choisir N après avoir pris connaissance de x, i.e. N pourrait dépendre de x, ce qui s'écrirait :

$$\forall \varepsilon \in \mathbf{R}_+^* \quad \forall x \in I \quad \exists N \in \mathbf{N} \quad \forall n \in \mathbf{N} \qquad (n \geq N) \Longrightarrow |f(x) - P_n(x)| \leq \varepsilon \ .$$

La démonstration de WEIERSTRASS, que nous étudierons dans un chapitre ultérieur, se fonde sur la notion de masse de DIRAC, un concept très important en physique, en théorie des distributions etc. Une démonstration plus constructive est donnée en exercice. Elle est due à Sergeï Natanovitch BERNSTEIN (1880-1968), mathématicien né dans la partie russophone de l'Ukraine et qui, après avoir étudié à Paris et été élève de Supélec, a résolu dans sa thèse, en français, le 19e problème que David HILBERT avait énoncé, à Paris aussi, en 1900.

On peut interpréter la démonstration de BERNSTEIN grâce à l'intervention de variables aléatoires binomiales et en utilisant l'inégalité de BIENAYMÉ-TCHEBICHEV. Il n'est pas rare que les probabilités permettent de donner des résultats qui semblent hors de leur champ d'action. Le plus spectaculaire, à mon goût, est la démonstration du théorème fondamental de l'algèbre ! Bien souvent c'est au prix d'avancées conceptuelles importantes et d'unification du langage entre des branches des mathématiques qui semblent éloignées. On n'est pas trop surpris de l'intervention de la loi binomiale pour étudier des fonctions polynomiales, mais pour l'autre résultat cité, il faut avoir

digéré un peu de théorie de la variable complexe et des fonctions harmoniques, et donc avoir rencontré le Laplacien et le mouvement Brownien.

Une fois qu'on est convaincu de l'importance des fonctions polynomiales, il faut en mener l'étude. Il s'agit d'objets profondément algébriques, ne serait que parce que leur ensemble forme un espace vectoriel. On peut donc en chercher des bases adaptées aux questions que l'on étudie. On a déjà rencontré les polynômes interpolateurs de Lagrange en MPSI et ceux de Newton ou Hilbert dans le premier chapitre. On vient d'évoquer ceux de Taylor. Tous se réfèrent à des bases différentes. Dans une autre direction les polynômes interviennent aussi en relation avec des questions d'intégration, ce qui mène bien souvent à des questions liées à des produits scalaires et à ce qu'on appelle des suites de polynômes orthogonaux.

Enfin, pour des questions d'analyse, on s'intéresse souvent à des problèmes de seuil, donc à des inéquations, qui passent souvent par la factorisation et donc la recherche des zéros de fonctions polynomiales. La question des racines des polynômes est très féconde et oscille entre l'algèbre et l'analyse. La résolution d'équations a amené à la création ou à la compréhension des nombres. La théorie algébrique des nombres rend compte de leur complexité, et on ne fera que l'effleurer : c'est leur utilisation qui nous occupera le plus. Ce qui n'empêchera pas d'appeler nombre des objets qui en paraissent éloignés : matrices, quaternions etc. Leur point commun ? Être solutions d'équations polynomiales ! Ces nombres interviennent en géométrie, et donc aussi en physique.

1 Polynômes à une indéterminée

Programme

Dans le cadre du programme seuls les polynômes sur un sous-corps de $\mathbf{C}$ sont étudiés et leur construction est hors-programme. Nous étudions néanmoins la construction sur un anneau $\mathbf{A}$ commutatif quelconque, afin de permettre de parler de polynômes à coefficients dans $\mathbf{Z}$ et aussi, à terme, d'évoquer la notion de polynôme à plusieurs indéterminées.

Définition 5 - 1

Un anneau intègre est un anneau commutatif ne possédant pas de diviseur de 0, i.e. dans lequel tout élément est régulier : $\forall (a,b) \in \mathbf{A}^2,\ ab = 0 \Longrightarrow (a = 0 \vee b = 0)$ ou encore $\forall (a,b,c) \in \mathbf{A}^3,\ (a \neq 0 \wedge ab = ac) \Longrightarrow b = c$.

Exemple 5 - 1

L'anneau des matrices carrées de taille n, avec $n > 1$, et à coefficients dans un corps, i.e. $\mathscr{M}_n(\mathbf{K})$, n'est pas intègre. Par exemple il existe des matrices nilpotentes comme celles de la dérivation relativement à une base quelconque de $\mathbf{R}_n[X]$, ou encore des projecteurs dont la composition est nulle, par exemple relativement à des espaces supplémentaires : $p_F^G \circ p_G^F = 0$.

Définition 5 - 2

Soit $\mathbf{A}$ un anneau commutatif. L'ensemble $\mathbf{A}^{(\mathbf{N})}$ des suites presque nulles à valeurs dans $\mathbf{A}$ est un anneau pour l'addition terme à terme et la multiplication définie par

$$(a_i)_{i\in\mathbf{N}}(b_j)_{j\in\mathbf{N}} = (c_k)_{k\in\mathbf{N}} \qquad \text{où } \forall k \in \mathbf{N},\ c_k = \sum_{i=0}^{k} a_i b_{k-i}\ .$$

On note X la suite nulle à l'exception de son terme d'ordre 1 égal à 1, i.e. $X = (\delta_{i,1})_{i\in\mathbf{N}}$. On a alors $X^n = (\delta_{i,n})_{i\in\mathbf{N}}$ et donc $\mathbf{A}^{(\mathbf{N})} \cong \mathbf{A}[X]$ où, par définition,

$$\mathbf{A}[X] = \left\{ \sum_{i\in\mathbf{N}} a_i X^i \;\middle|\; (a_i)_{i\in\mathbf{N}} \in \mathbf{A}^{(\mathbf{N})} \right\} .$$

On dit que X est une **indéterminée** sur $\mathbf{A}$ et si $P \in \mathbf{A}[X]$ avec $P = \sum_{i\in\mathbf{N}} a_i X^i$, on appelle **degré** de P, et on note $\deg(P)$, la quantité (entière naturelle ou égale à $-\infty$) définie par

Définition 5 - 3

$$\deg(P) = \sup \{ i \in \mathbf{N} \,|\, a_i \neq 0 \} ,$$

le supremum étant égal à $-\infty$ si l'ensemble précédent est vide, i.e. si $P = 0$.

Le coefficient du terme de plus haut degré, i.e. $a_{\deg(P)}$ lorsque $\deg(P) \geq 0$, est appelé **coefficient dominant** de P et on dit que P est **unitaire** (ou **normalisé**) quand ce coefficient est égal à 1.

Enfin on appelle **valuation** de P, et on note $\mathrm{val}(P)$, la quantité (entière naturelle ou égale à $+\infty$) définie par

$$\mathrm{val}(P) = \inf \{ i \in \mathbf{N} \,|\, a_i \neq 0 \} ,$$

l'infimum étant égal à $+\infty$ si l'ensemble précédent est vide, i.e. si $P = 0$.

Degré et valuation d'un produit ou d'une somme

Pour P et Q dans $\mathbf{A}[X]$, on a

Propriété 5 - 1

1. $\deg(PQ) \leq \deg(P) + \deg(Q)$ et $\mathrm{val}(PQ) \geq \mathrm{val}(P) + \mathrm{val}(Q)$ avec égalités si $\mathbf{A}$ est intègre,
2. $\deg(P+Q) \leq \max(\deg(P), \deg(Q))$ avec égalité si $\deg(P) \neq \deg(Q)$,
3. $\mathrm{val}(P+Q) \geq \min(\mathrm{val}(P), \mathrm{val}(Q))$ avec égalité si $\mathrm{val}(P) \neq \mathrm{val}(Q)$.

Par ailleurs $\mathbf{A}$ se plonge dans $\mathbf{A}[X]$ en identifiant les scalaires aux polynômes constants, i.e. il s'agit d'un morphisme d'anneaux injectif de $\mathbf{A}$ dans $\mathbf{A}[X]$.

Remarque 5 - 1

En ce qui concerne la somme, plus précisément il y a inégalité stricte dans les inégalités données si et seulement si P et Q ont même degré et coefficients dominants opposés (pour le degré de la somme) ou si P et Q ont même valuation et termes de degré minimal opposés (pour la valuation de la somme).

Intégrité de l'anneau des polynômes

Théorème 5 - 2

L'anneau $\mathbf{A}[X]$ est intègre (et donc en particulier commutatif) si et seulement si $\mathbf{A}$ l'est et alors les polynômes inversibles dans $\mathbf{A}[X]$ sont les polynômes constants égaux à un élément inversible de $\mathbf{A}$. C'est en particulier le cas si $\mathbf{A}$ est un corps.

Démonstration. Si $\mathbf{A}$ est commutatif, $\mathbf{A}[X]$ l'est par construction au vu de la formule donnant c_k, et réciproquement $\mathbf{A}$ s'identifie à un sous-anneau de l'anneau commutatif $\mathbf{A}[X]$ et l'est donc également.

D'après la propriété précédente sur la valuation d'un produit dans $\mathbf{A}[X]$ avec $\mathbf{A}$ intègre, il vient qu'alors $\mathbf{A}[X]$ est intègre puisque $+\infty$ ne peut pas être la somme de deux quantités finies ou encore ($\mathrm{val}(P)$ et $\mathrm{val}(Q)$ finies) $\Rightarrow \mathrm{val}(PQ)$ finie.

La réciproque est immédiate puisque $\mathbf{A}$ se plonge dans $\mathbf{A}[X]$ et donc un diviseur de 0 dans $\mathbf{A}$ est aussi un diviseur de 0 dans $\mathbf{A}[X]$: si $ab = 0$ dans $\mathbf{A}$, alors $ab = 0$ dans $\mathbf{A}[X]$.

Comme $\deg(1) = 0$, un produit de deux polynômes ne peut être égal à 1 que si les deux polynômes sont de degré 0, et sont donc constants égaux à un inversible de $\mathbf{A}$. La réciproque est immédiate. □

Danger

L'hypothèse d'intégrité de $\mathbf{A}$ est essentielle. Par exemple $(1-pX)(1+pX) = 1$ dans $\mathbf{Z}/p^2\mathbf{Z}[X]$.

Théorème 5 - 3

Division euclidienne dans $\mathbf{A}[X]$

Soit A et B dans $\mathbf{A}[X]$ avec $B \neq 0$ et tel que le **coefficient dominant de B soit inversible** dans $\mathbf{A}$. Alors il existe un unique couple (Q, R) dans $\mathbf{A}[X]^2$ tel que

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

Le polynôme Q est appelé quotient de la division euclidienne de A par B et R en est le reste. L'application degré est appelé stathme pour la division euclidienne dans $\mathbf{A}[X]$.

Démonstration. On démontre l'existence par récurrence sur le degré de A, à B fixé. Si $\deg(A) < \deg(B)$, alors $(0, A)$ convient. Sinon, en notant $n = \deg(A)$, $m = \deg(B)$, $A = \sum a_i X^i$ et $B = \sum b_j X^j$, alors $A - a_n(b_m)^{-1}X^{n-m}B$ est un polynôme de degré strictement inférieur à celui de A et ceci montre que la propriété est héréditaire :

$$A - a_n(b_m)^{-1}X^{n-m}B = BQ + R \Longrightarrow A = B(Q + a_n(b_m)^{-1}X^{n-m}) + R \ .$$

Soit maintenant (Q_1, R_1) et (Q_2, R_2) dans $\mathbf{A}[X]^2$ tels que $\deg(R_1) < \deg(B)$, $\deg(R_2) < \deg(B)$ et $A = BQ_1 + R_1 = BQ_2 + R_2$. Alors on a $B(Q_1 - Q_2) = R_2 - R_1$ et le terme de droite est un polynôme de degré strictement inférieur à celui de B alors que celui de gauche est soit nul, soit de degré au moins $\deg(B)$ par inversibilité de b_m. C'est donc que $R_2 - R_1$ et $Q_1 - Q_2$ sont nuls. On en déduit l'unicité de la division euclidienne. □

Remarque 5 - 2

Division euclidienne dans $\mathbf{K}[X]$

En particulier la division euclidienne d'un polynôme A par un polynôme B, à coefficients dans un corps, est définie dès que B est non nul.

Exemple 5 - 2

Si A et B sont deux polynômes à coefficients entiers et si B est unitaire, alors le quotient et le reste de la division euclidienne de A par B (dans $\mathbf{R}[X]$) sont en fait à coefficients entiers : il s'agit en fait d'une division euclidienne dans $\mathbf{Z}[X]$, avec coefficient dominant unitaire pour le dénominateur.

On peut l'illustrer en divisant $5X^2+1$ par $X-1$ et par $5X-1$ respectivement.

Aparté

La récurrence sur le degré de A peut aussi s'écrire comme une récurrence noethérienne sur $\mathbf{A}[X]$ muni de l'ordre noethérien donné par $A\mathcal{R}B \equiv \deg(A) \leq \deg(B)$. Voir l'exercice 1 - 13 pour ces notions.

2 Arithmétique dans $\mathrm{K}[X]$

Programme

Dans le cadre du programme **K** est un sous-corps de **C**, i.e. il vérifie $\mathbf{Q} \subset \mathbf{K} \subset \mathbf{C}$. Ce n'est pas une restriction nécessaire, mais il faut en tout cas s'intéresser de près aux cas particuliers **C**, **R** et **Q**. Comme on le verra pour bien comprendre $\mathbf{Q}[X]$, il faut en fait s'intéresser à $\mathbf{Z}[X]$ et $\mathbf{Z}/n\mathbf{Z}[X]$, au moins en filigranes et, de facto, de nombreux sujets de concours y font appel sans les nommer.

On s'intéresse maintenant à l'anneau $\mathbf{K}[X]$ pour **K** un corps. La division euclidienne y est donc possible par tout polynôme non nul. Cet outil fondamental permet de démontrer que $\mathbf{K}[X]$ ressemble comme deux gouttes d'eau à l'anneau **Z** des entiers. On y retrouve en particulier une décomposition en facteurs premiers. Pour cela on va introduire un peu de vocabulaire.

Définition 5 - 4

Soit **A** un anneau commutatif et I une partie de **A**. On dit que I est un idéal de **A** si c'en est un sous-groupe additif et qu'il est stable par multiplication externe par **A**, i.e.

$$\forall x \in I\,,\ \forall a \in A\,,\quad ax \in I\,.$$

On note (x) ou xA l'idéal engendré par un élément x de A, à savoir

$$xA = \{xa \,|\, a \in \mathbf{A}\}\ .$$

Remarque 5 - 3

La multiplication étant distributive, l'application multiplication (à droite ou à gauche) est un morphisme du groupe multiplicatif $(\mathbf{A}, +)$ et donc xA en est l'image, donc un sous-groupe de **A**. Par construction il est stable par multiplication, ce qui explique pourquoi xA est un idéal. C'est aussi le plus petit idéal de **A** contenant x. Un idéal de la forme xA est dit principal et x en est appelé un générateur. Un tel générateur n'est en général pas unique : $1\mathbf{Z} = (-1)\mathbf{Z}$ par exemple.

Théorème 5 - 4

Idéaux de $\mathbf{K}[X]$

Soit I un idéal de $\mathbf{K}[X]$, non réduit à $\{0\}$. Il existe P dans I tel que

1. $\forall Q \in I$, $\deg(Q) < \deg(P) \Rightarrow Q = 0$,
2. $I = (P)$, i.e. $I = \{PQ \,|\, Q \in \mathbf{K}[X]\} = P\mathbf{K}[X]$.

Démonstration. Soit I un idéal non nul. L'ensemble $\{\deg(Q) \,|\, Q \in I\,,\ Q \neq 0\}$ est donc une partie non vide de **N** et si d est son minimum, on peut choisir P dans I tel que $\deg(P) = d$. Ce polynôme vérifie la première propriété et il est non nul.

Soit maintenant B dans I. Comme $P \neq 0$, on peut effectuer la division euclidienne de Q par P. Il vient $B = PQ + R$ avec Q et R dans $\mathbf{K}[X]$. Comme I est un idéal $B - PQ$ appartient à I puisque c'est le cas pour B et P. Mézalor R appartient à I. La propriété $\deg(R) < \deg(P)$ entraîne alors que R est nul, i.e. $B \in P\mathbf{K}[X]$. D'où $I \subset P\mathbf{K}[X]$.

La réciproque est une conséquence de la définition de $P\mathbf{K}[X]$. □

♠

On dit que $\mathbf{K}[X]$ est un anneau principal, ce qui signifie qu'il est intègre et que tous ses idéaux sont de la forme $P\mathbf{K}[X]$ (avec $P = 0$ on trouve l'idéal nul).

Remarque 5 - 4

Pour P et Q dans $\mathbf{K}[X]$, P **divise** Q si et seulement si Q appartient à l'idéal $P\mathbf{K}[X]$. On a $P \mid Q \iff Q\mathbf{K}[X] \subset P\mathbf{K}[X]$.

Proposition 5 - 1

PPCM

Soit P, Q, R dans $\mathbf{K}[X]$. Alors R est un multiple commun à P et Q si et seulement si

$$R\mathbf{K}[X] \subset P\mathbf{K}[X] \cap Q\mathbf{K}[X] \ .$$

Dans le cas d'égalité R est un plus petit commun multiple, ou ppcm. Si, de plus, R est nul ou unitaire on dit que R est **le ppcm** de P et Q, et on note $R = \mathrm{ppcm}(P, Q)$ ou encore $R = P \vee Q$. Le ppcm est unique et, de plus, si P et Q sont non nuls, tout ppcm de P et Q est non nul.

Démonstration. La première partie est une reformulation puisque les multiples de P sont exactement les éléments de $P\mathbf{K}[X]$ et donc les multiples communs à P et Q sont les éléments de $P\mathbf{K}[X] \cap Q\mathbf{K}[X]$. De plus, par stabilité par multiplication par des éléments de $\mathbf{K}[X]$,

$$R \in P\mathbf{K}[X] \cap Q\mathbf{K}[X] \iff R\mathbf{K}[X] \subset P\mathbf{K}[X] \cap Q\mathbf{K}[X] \ .$$

L'ensemble $P\mathbf{K}[X] \cap Q\mathbf{K}[X]$ est stable par multiplication par $\mathbf{K}[X]$ et c'est un sous-groupe de $\mathbf{K}[X]$, en tant qu'intersection de deux sous-groupes. C'est donc un idéal de $\mathbf{K}[X]$ et la proposition précédente, ainsi que sa démonstration, montre que si cette intersection n'est pas réduite à $\{0\}$, il est égal à $R\mathbf{K}[X]$ pour tout polynôme R de degré minimal parmi les polynômes non nuls de $P\mathbf{K}[X] \cap Q\mathbf{K}[X]$. Par définition un tel polynôme est un ppcm de P et Q, et réciproquement. Par ailleurs l'intersection contient PQ et est donc réduite à $\{0\}$ seulement si $P = 0$ ou $Q = 0$, la réciproque étant directe.

Par conséquent, si $P = 0$ ou $Q = 0$, on a $P\mathbf{K}[X] \cap Q\mathbf{K}[X] = \{0\}$ et tout ppcm de P et Q est nul, et donc **le ppcm** aussi. Dans le cas contraire $P\mathbf{K}[X] \cap Q\mathbf{K}[X] \neq \{0\}$ et donc les ppcm de P et Q sont non nuls. Si R et S sont deux tels ppcm, on a $R\mathbf{K}[X] = S\mathbf{K}[X] = P\mathbf{K}[X] \cap Q\mathbf{K}[X]$ et on dispose de U et V dans $\mathbf{K}[X]$ tels que $R = SU$ et $S = RV$. Il vient $R = RVU$. Comme R est non nul, $VU = 1$ et donc V et U sont des polynômes inversibles, donc constants non nuls. Si r est le coefficient dominant de R et s celui de S, alors en notant $T = \dfrac{1}{r}R$, T est unitaire et on a $R = rT$ et $S = sT$. Comme $T\mathbf{K}[X] = R\mathbf{K}[X] = S\mathbf{K}[X] = P\mathbf{K}[X] \cap Q\mathbf{K}[X]$, on en déduit que T est un ppcm unitaire de P et Q et qu'un tel polynôme est unique, i.e. **le ppcm** existe et est unique. Il est non nul dès que P et Q le sont. □

PGCD

Soit P, Q, R dans $\mathbf{K}[X]$. On note

$$P\mathbf{K}[X]+Q\mathbf{K}[X]=\left\{PU+QV \mid (U,V)\in\mathbf{K}[X]^2\right\}\ .$$

Proposition 5 - 2

Alors R est un diviseur commun à P et Q si et seulement si $P\mathbf{K}[X]+Q\mathbf{K}[X]\subset R\mathbf{K}[X]$ et R est un plus grand commun diviseur, ou pgcd, dans le cas d'égalité.

Dans le cas d'égalité, si R est nul ou unitaire on dit que R est **le pgcd** de P et Q, et on note $R=\text{pgcd}(P,Q)$ ou encore $R=P\wedge Q$. Le pgcd est unique et, de plus, si P ou Q est non nul, tout pgcd de P et Q est non nul.

Démonstration. Si R est un diviseur commun à P et Q, alors P et Q appartiennent à $R\mathbf{K}[X]$ et donc, comme ce dernier est stable par multiplication par $\mathbf{K}[X]$ et par addition il vient successivement $P\mathbf{K}[X]\subset R\mathbf{K}[X]$ et $Q\mathbf{K}[X]\subset R\mathbf{K}[X]$, puis $P\mathbf{K}[X]+Q\mathbf{K}[X]\subset R\mathbf{K}[X]$. Réciproquement si R vérifie l'inclusion précédente, en particulier comme $P=P\times 1+Q\times 0\in P\mathbf{K}[X]+Q\mathbf{K}[X]$, on a $P\in R\mathbf{K}[X]$ et donc R divise P. De même Q divise R et donc R est un diviseur commun de P et Q.

Remarquons que $P\mathbf{K}[X]+Q\mathbf{K}[X]$ est un idéal de $\mathbf{K}[X]$. En effet il est stable par multiplication par $\mathbf{K}[X]$ et c'en est un sous-groupe puisqu'il contient 0, est stable par addition et passage à l'opposé $((PU_1+QV_1)-(PU_2+QV_2)=P(U_1-U_2)+Q(V_1-V_2))$. S'il est non nul on en déduit qu'il s'écrit $R\mathbf{K}[X]$ pour tout polynôme R de degré minimal parmi les polynômes non nuls de $P\mathbf{K}[X]+Q\mathbf{K}[X]$. Si S est un autre diviseur commun à P et Q, on a

$$R\mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]\subset S\mathbf{K}[X]$$

et donc $S\mid R$. Autrement dit R est un pgcd de P et Q, et si S est un pgcd de P et Q on a $R\mid S$ d'après ce qui précède et $R\mid S$ par définition d'un pgcd, donc $R\mathbf{K}[X]=S\mathbf{K}[X]$ et ainsi les pgcd de P et Q sont exactement les polynômes R vérifiant $R\mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]$, i.e. les générateurs de l'idéal principal $P\mathbf{K}[X]+Q\mathbf{K}[X]$.

Par ailleurs $P\mathbf{K}[X]+Q\mathbf{K}[X]$ contient P et Q et est donc réduit à $\{0\}$ seulement si $P=0$ et $Q=0$, la réciproque étant directe.

Par conséquent, si $P=Q=0$, on a $P\mathbf{K}[X]+Q\mathbf{K}[X]=\{0\}$ et tout pgcd de P et Q est nul, et donc **le pgcd** aussi. Dans le cas contraire $P\mathbf{K}[X]+Q\mathbf{K}[X]\neq\{0\}$ et donc les pgcd de P et Q sont non nuls. Si R et S sont deux tels pgcd, on a $R\mathbf{K}[X]=S\mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]$ et on conclut comme dans la proposition précédente, en notant r et s les coefficients dominants de R et S et $T=\dfrac{1}{r}R$, que T est unitaire, qu'on a $R=rT$ et $S=sT$, puis que T est un pgcd unitaire de P et Q et qu'un tel polynôme est unique, i.e. **le pgcd** existe et est unique. Il est non nul dès que P ou Q l'est. □

Remarque 5 - 5

La notion de ppcm est donc plus élémentaire que celle de pgcd. Elle est aussi beaucoup moins utile car nettement moins profonde. Le ppcm sert au mieux à mettre au mettre au même dénominateur des fractions, et encore car c'est conceptuellement inutile, c'est au regard de l'efficacité des calculs que la notion entre en jeu. A contrario le pgcd est la pierre angulaire de l'arithmétique et permet de construire la décomposition en facteurs premiers et la relation de Bézout est un outil incontournable qu'il convient d'avoir toujours disponible, tel un réflexe pavlovien on traduit instantanément la notion de pgcd en relation de Bézout !

Définition 5 - 5

On dit que deux éléments P et Q de $\mathbf{K}[X]$ sont premiers entre eux si $P\wedge Q=1$, i.e. si $P\mathbf{K}[X]+Q\mathbf{K}[X]=\mathbf{K}[X]$.

Théorème 5 - 5

Théorème de Bézout

Soit P et Q deux éléments de $\mathbf{K}[X]$. Ils sont premiers entre eux si et seulement si

$$\exists (U,V) \in \mathbf{K}[X]^2\,, \quad UP+VQ=1\,.$$

Une telle relation est appelée relation de Bézout.

Plus généralement, pour R dans $\mathbf{K}[X]$, on a

$$\big(\exists (U,V) \in \mathbf{K}[X]^2\,, \quad UP+VQ=R\big) \iff (P\wedge Q) \mid R$$

et si R est un pgcd de P et Q, une relation $UP+VQ=R$ est appelée relation de Bézout entre P et Q.

Démonstration. Si $P\wedge Q=1$, on a $1\in \mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]$ et l'existence d'une relation de Bézout en découle.

Réciproquement si une telle relation existe, on a en particulier $1\in P\mathbf{K}[X]+Q\mathbf{K}[X]$ et donc, par stabilité par multiplication par $\mathbf{K}[X]$, $\mathbf{K}[X]\subset P\mathbf{K}[X]+Q\mathbf{K}[X]$ et donc par double inclusion $\mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]$. Le polynôme unitaire de degré minimal de $\mathbf{K}[X]$ étant 1, il vient $P\wedge Q=1$.

Pour la seconde partie, l'équivalence résulte de la définition de $P\mathbf{K}[X]+Q\mathbf{K}[X]$ et de la proposition précédente. □

Remarque 5 - 6

Étienne Bézout (1730–1783) porte un nom dans lequel le « é » se prononce non accentué, on dit donc « Bezout », à l'inverse de Georges Clemenceau qui se prononce accentué mais s'écrit non accentué (on prononce « Clémenceau »).

Théorème 5 - 6

Lemme de Gauss

Soit P, Q, R dans $\mathbf{K}[X]$ tels que $P\mid QR$ et $P\wedge Q=1$, alors $P\mid R$.

Démonstration. À la vue de $P\wedge Q=1$, on applique le réflexe pavlovien

$$\mathbf{K}[X]=P\mathbf{K}[X]+Q\mathbf{K}[X]$$

et donc en multipliant par R, il vient

$$R\mathbf{K}[X]=PR\mathbf{K}[X]+QR\mathbf{K}[X]\,.$$

Comme les deux ensembles de droite sont inclus dans $P\mathbf{K}[X]$ puisque P divise PR et QR, il en va de même pour leur somme puisque $P\mathbf{K}[X]$ est un idéal et donc

$$R\mathbf{K}[X]\subset P\mathbf{K}[X]\,,$$

ce qui signifie $P\mid R$. □

Remarque 5 - 7

Magique, non ?! Le lemme de Gauss est souvent interprété à l'aune de la décomposition en facteurs premiers : si P n'a pas de facteur commun avec Q et qu'il divise QR, c'est qu'il divise R ou plutôt que ses facteurs premiers sont parmi ceux de R. Mais on voit ici que la déduction se fait en sens inverse : c'est grâce au lemme de Gauss que l'on peut accéder à la décomposition en facteurs premiers et ce dernier n'a besoin que de la relation de Bézout.

Exemple 5 - 3

Soit P et Q premiers entre eux dans $\mathbf{K}[X]$, alors $P+Q$ et Q sont premiers entre eux. En effet il suffit de partir d'une relation de Bézout $UP+VQ=1$:

$$U(P+Q)+(V-U)Q=1 \quad \text{et donc } (P+Q)\wedge Q=1\,.$$

Remarque 5 - 8

Faire apparaître une somme, un 0 dans une somme ou un 1 dans un produit peut paraître magique, mais c'est un réflexe à avoir. En ce qui concerne cette première astuce, elle peut se dire en termes de déterminants :

$$UP+VQ=\begin{vmatrix} P & Q \\ -V & U \end{vmatrix}=\begin{vmatrix} P+Q & Q \\ U-V & U \end{vmatrix}=U(P+Q)+(V-U)Q$$

en ajoutant la seconde colonne à la première.

Exemple 5 - 4

Soit P et Q premiers entre eux dans $\mathbf{K}[X]$, alors $P+Q$ et PQ sont premiers entre eux.

On part d'une relation de Bézout $UP+VQ=1$. Il vient $U(P+Q)+(V-U)Q=1$ et $(U-V)P+V(P+Q)=1$, et donc en multiplicant ces deux relations, il vient

$$\begin{aligned} 1=U(P+Q)+(V-U)Q&=U(P+Q)+(V-U)Q\times 1\\ &=(U+(V-U)QV)(P+Q)-(U-V)^2PQ=1\,, \end{aligned}$$

ce qui assure $(P+Q)\wedge(PQ)=1$.

Exemple 5 - 5

Soit P et Q premiers entre eux dans $\mathbf{K}[X]$ alors, pour n et m dans $\mathbf{N}$, P^n et Q^m sont premiers entre eux.

On part d'une relation de Bézout $UP+VQ=1$ et en développant par le binôme $(UP+VQ)^{n+m}=1$ on obtient une relation entre P^n et Q^m (à dire vrai élever à la puissance $n+m-1$ suffit !).

Définition 5 - 6

On appelle polynôme irréductible de $\mathbf{K}[X]$ tout polynôme P qui ne peut s'écrire comme produit de deux polynômes de degrés strictement inférieurs au sien.

En particulier P n'est pas constant.

Lemme 5 - 1

Soit P et Q deux polynômes irréductibles unitaires et distincts. Alors ils sont premiers entre eux.

Démonstration. Un diviseur de P est de degré inférieur ou égal à celui de P et est donc, du fait de son irréductibilité, de degré égal ou bien constant. On en déduit que pour tout polynôme R on a $P\wedge R=1$ ou $P\wedge R=P$. Le second cas équivaut à $P\mid R$. Or $P\mid Q$ entraîne que P et Q ont même degré, par irréductibilité de Q, puis qu'ils sont égaux car ils sont unitaires. □

Le théorème de Gauss permet d'obtenir

Théorème 5 - 7

Existence et unicité de la décomposition en facteurs irréductibles

Soit A un polynôme dans $\mathbf{K}[X]$ non nul et $\mathcal{I}$ l'ensemble des polynômes unitaires irréductibles dans $\mathbf{K}[X]$.

Il existe un unique couple formé d'une suite presque nulle $(v_P(A))_{P\in\mathcal{I}}$ et d'un scalaire non nul a dans $\mathbf{K}^*$ tels que

$$A = a\prod_{P\in\mathcal{I}} P^{v_P(A)} \ .$$

Les produits sont donc finis.

Démonstration. L'existence se démontre par récurrence sur $\deg(A)$ dans $\mathbf{N}$.

— Si $\deg(A) = 0$, alors on pose $v_P(A) = 0$ pour tout P dans $\mathcal{I}$ et $a = A$.

— Si A est irréductible, alors on pose $v_P(A) = \delta_P(A)$ pour tout P dans $\mathcal{I}$ et a le coefficient dominant de A.

— Si A n'est pas irréductible, on dispose de A_1 et A_2 dans $\mathbf{K}[X]$ tels que $A = A_1A_2$ et $\deg(A_1)$ et $\deg(A_2)$ strictement inférieurs à $\deg(P)$. Deux décompositions de A_1 et A_2 fournissent par produit une décomposition de A.

L'unicité est une conséquence du théorème de Gauss. Soit a et b deux unités scalaires non nuls dans $\mathbf{K}^\times$, (a_p) et (b_p) deux suites presque nulles dans $\mathbf{N}^{(\mathcal{I})}$ tels que

$$a\prod_{P\in\mathcal{I}} P^{a_p} = b\prod_{P\in\mathcal{I}} P^{b_p} \ .$$

Si les suites (a_p) et (b_p) sont distinctes, on dispose de P dans $\mathcal{I}$ que $a_p \neq b_p$ et en divisant les deux membres de l'égalité par $P^{\min(a_p,b_p)}$, on obtient deux polynômes. L'un est divisible par P puisque $\min(a_p, b_p) < \max(a_p, b_p)$ et donc l'autre aussi. Mais ceci contredit le théorème de Gauss puisque ce second polynôme est un produit (fini) de polynômes irréductibles distincts de, et donc premiers à, P. On en déduit $(a_p) = (b_p)$ et donc aussi $a = b$. □

Aparté

On pourrait faire une récurrence noethérienne en utilisant la relation d'ordre donnée par la divisibilité.

Définition 5 - 7

Valuation P-adique

On reprend les notations du théorème précédent. L'entier $v_P(A)$ est appelé **valuation P-adique** de A. On étend cette valuation à $\mathbf{K}[X]$ en posant $v_P(0) = +\infty$.

On a donc $\mathrm{val}(A) = v_X(A)$ et d'une façon générale

$$v_P(A) = \max\left\{k\in\mathbf{N} \;\middle|\; P^k \mid A\right\} \ .$$

Remarque 5 - 9

Développement de Taylor

Si P est un polynôme unitaire du premier degré (donc nécessairement irréductible), disons $P = X - a$, on peut écrire le développement de Taylor de A au voisinage de a et obtenir

$$A = \sum_{i\in\mathbf{N}} a_i P^i$$

et alors

$$\mathrm{val}_P(A) = \inf\{i\in\mathbf{N} \,|\, a_i \neq 0\} \ .$$

Développement en base P

L'écriture

$$A = \sum_{i \in \mathbf{N}} a_i P^i$$

Remarque 5 - 10

est une écriture « en base P » de A et peut être définie pour un polynôme non nul P quelconque : c'est une simple conséquence de la division euclidienne puisqu'on a

$$A = B_0 + PQ_0 = B_0 + P(B_1 + PQ_1) = \cdots ,$$

i.e. $A = \sum_{i \in \mathbf{N}} B_i P^i$ avec $\deg(B_i) < \deg(P)$.

On a alors $\mathrm{val}_P(A) = \inf \{i \in \mathbf{N} \mid B_i \neq 0\}$.

Aparté

L'écriture $A = B_0 + P(B_1 + P(B_2 + \cdots))$ s'appelle un schéma de Horner.

Valuation et PPCM/PGCD

Si A et B sont deux polynômes dans $\mathbf{K}[X]$, on a $A \mid B \Leftrightarrow \forall P \in \mathcal{I},\ v_P(A) \leq v_P(B)$. De plus

Théorème 5 - 8

$$A \vee B = \prod_{P \in \mathcal{I}} P^{\max(v_P(A), v_P(B))} \text{ et } A \wedge B = \prod_{P \in \mathcal{I}} P^{\min(v_P(A), v_P(B))} .$$

Il en résulte $AB = c(A \vee B) \cdot (A \wedge B)$ pour un certain c dans $\mathbf{K}^\times$ (unique si $AB \neq 0$).

Démonstration. Soit A, B et C trois polynômes non nuls vérifiant $B = AC$. D'après le théorème précédent, on a, pour tout P dans $\mathcal{I}$, $v_P(B) = v_P(A) + v_P(C)$ et donc $v_P(B) \geq v_P(A)$.

Réciproquement si pour tout P dans $\mathcal{I}$ on a $v_P(B) \geq v_P(A)$, alors en posant $C = \prod_{P \in \mathcal{I}} P^{v_P(B) - v_P(A)}$ et c le quotient du coefficient dominant de B par celui de A, on a $B = cCA$ et donc $A \mid B$. La première assertion en résulte puisqu'elle est directe dans le cas $A = 0$ ou $B = 0$.

Les deux suivantes sur le pgcd et le ppcm s'ensuivent puisque, pour tous entiers naturels a, b et c (interprétés comme des valuations P-adiques), on a

$$(c \leq a \text{ et } c \leq b) \Longleftrightarrow c \leq \min(a, b) \quad \text{et} \quad (a \leq c \text{ et } b \leq c) \Leftrightarrow \max(a, b) \leq c .$$

La dernière résulte du fait qu'on a $\min(a, b) + \max(a, b) = a + b$ et en prenant c le coefficient dominant de AB s'il est non nul et c quelconque sinon, car alors $A \vee B = 0$. □

3 Irréductibles de $\mathrm{K}[X]$

Définition 5 - 8

Soit P dans $\mathbf{K}[X]$ avec $P = \sum_i a_i X^i$. Le morphisme de substitution $x \mapsto \sum_i a_i x^i$ est un morphisme d'anneaux appelé spécialisation en x. La fonction, définie sur $\mathbf{K}$, est appelée fonction polynôme associée à P. On la note $\widetilde{P}$.

On appelle zéro de $\widetilde{P}$ un élément x de $\mathbf{K}$ tel que $\widetilde{P}(x) = 0$.

On appelle racine de P un élément a de $\mathbf{K}$ tel que $(X - a) \mid P$.

Théorème 5 - 9

Si P est dans $\mathbf{K}[X]$ et a dans $\mathbf{K}$. Alors a est un zéro de $\widetilde{P}$ si et seulement si a est racine de P. En particulier si P est de degré n, avec $n \geq 0$, P admet au plus n racines. Dit autrement $\widetilde{P}$ admet au plus n zéros.

Démonstration. On écrit la division euclidienne de P par $X - a$: $P = (X - a)Q + R$ et on remarque que R est constant. Par conséquent, par spécialisation en a,

$$P(a) = 0 \iff R(a) = 0 \iff R = 0 \,.$$

De plus pour a et b distincts, $X - a$ et $X - b$ sont premiers entre eux puisque

$$\frac{1}{b-a}(X - a) - \frac{1}{b-a}(X - b) = 1$$

et donc par récurrence immédiate et en utilisant le lemme de Gauss, si $a_1, \ldots, a_k$ sont k racines distinctes de P, $(X - a_1) \cdots (X - a_k)$ divise P et donc $k \leq \deg(P)$. □

Les résultats suivants permettent de décrire les polynômes irréductibles de $\mathbf{K}[X]$ lorsque $\mathbf{K}$ est $\mathbf{R}$ ou $\mathbf{C}$.

Théorème 5 - 10

Théorème de d'Alembert-Gauss - Théorème fondamental de l'algèbre

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

Démonstration. Ce théorème est admis. C'est en fait un théorème d'analyse (malgré son surnom). □

Pour aller plus loin

On peut le démontrer en admettant uniquement le point suivant : toute fonction polynomiale de degré impair admet un zéro, ce qui résulte du théorème des valeurs intermédiaires (théorème de Bolzano). La démonstration se fait alors par récurrence sur la valuation 2-adique du degré du polynôme, soit grâce à l'algèbre linéaire, soit grâce aux polynômes symétriques élémentaires. Cette démonstration remonte à Joseph-Louis Lagrange (1736 – 1813).

Irréductibles de $\mathbf{C}[X]$

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

Soit P dans $\mathbf{C}[X]$ de degré n avec $n \geq 1$. Il admet une écriture (unique à l'ordre des facteurs près) de la forme

Théorème 5 - 11

$$P = \alpha \prod_{i=1}^{k} (X - a_i)^{n_i}$$

où $k \in \mathbf{N}^*$, $(a_i)_{1 \leq i \leq k}$ des nombres complexes distincts deux à deux, $(n_i)_{1 \leq i \leq k}$ des entiers naturels non nuls de somme n et α un nombre complexe non nul. De plus α est le coefficient dominant de P.

Démonstration. La classification des irréductibles de $\mathbf{C}[X]$ résulte directement du théorème fondamental de l'algèbre puisque tout polynôme non constant P de $\mathbf{C}[X]$ est divisible par $X - a$ où a est une de ses racines, et en est donc un multiple scalaire par irréductibilité. Par existence et unicité de la décomposition en facteurs irréductibles, l'écriture de P comme produit s'ensuit. □

Irréductibles de $\mathbf{R}[X]$

Dans $\mathbf{R}[X]$ les polynômes irréductibles sont les polynômes de degré 1 ainsi que les polynômes de degré 2 sans racine réelle, i.e. de la forme $a(X-u)(X-\overline{u})$ avec a réel non nul et u complexe non réel, ou encore de la forme $aX^2 + bX + c$ avec a, b et c réels vérifiant $b^2 < 4ac$.

Soit P dans $\mathbf{R}[X]$ de degré n avec $n \geq 1$. Il admet une écriture (unique à l'ordre des facteurs près) de la forme

Théorème 5 - 12

$$P = \alpha \prod_{i=1}^{k} (X - a_i)^{n_i} \prod_{j=1}^{\ell} (X^2 + b_j X + c_j)^{m_j}$$

où $(k, \ell) \in \mathbf{N}^2$ avec $(k, \ell) \neq (0, 0)$, $(a_i)_{1 \leq i \leq k}$ des nombres réels distincts deux à deux, $((b_j, c_j))_{1 \leq j \leq \ell}$ des couples distincts deux à deux de réels vérifiant $b_j^2 < 4c_j$, $(n_i)_{1 \leq i \leq k}$ et $(m_j)_{1 \leq j \leq \ell}$ des entiers naturels non nuls vérifiant $\sum_{i=1}^{k} a_i + 2\sum_{j=1}^{\ell} b_j = n$, et α un nombre réel non nul. De plus α est le coefficient dominant de P.

Démonstration. Soit P un polynôme irréductible dans $\mathbf{R}[X]$. Si P admet une racine réelle, il est divisible par un polynôme de degré 1 et donc $\deg(P) = 1$. Sinon, on considère u une racine complexe de P. Puisque P est à coefficients réels, on a $P(\overline{u}) = \overline{P(u)}$ et donc $\overline{u}$ est une racine complexe de P. Comme u n'est pas réel, $X - u$ et $X - \overline{u}$ sont premiers entre eux dans $\mathbf{C}[X]$ et donc $(X-u)(X-\overline{u})$ divise P dans $\mathbf{C}[X]$. Or ce produit est un polynôme à coefficients réels puisqu'il est égal à $X^2 - 2\operatorname{Re}(u)X + |u|^2$ et donc il divise P également dans $\mathbf{R}[X]$ puisque le quotient et le reste dans la division euclidienne ne dépendent pas du corps de base. Puisque P est irréductible, on en déduit que c'est un multiple scalaire de $X^2 - 2\operatorname{Re}(u)X + |u|^2$.

Réciproquement si P est de degré 1, il est irréductible puisque le degré d'un produit est la somme des degrés et si P est de degré 2 sans racine réelle, alors il ne peut être produit de deux polynômes de degré 1 dans $\mathbf{R}[X]$ et est donc irréductible pour la même raison que précédemment.

Par existence et unicité de la décomposition en facteurs irréductibles, l'écriture de P comme produit s'en déduit. □

4 Équations polynomiales

Dans le domaine des équations polynomiales en nombres entiers, rationnels, réels ou complexes, on a longtemps cherché des solutions données par des formules n'autorisant que les quatre opérations élémentaires et la prise de radicaux. Si l'équation du deuxième degré est facilement résolue, il n'en est pas de même pour les équations de degré supérieur. C'est Gerolamo Cardano (1501-1576) qui publie une solution pour le degré trois dans son *Ars magna sive de regulis algebraicis*, solution empruntée à Nicolo Tartaglia (1499-1557) et probablement connue de Scipio del Ferro (1465-1526). Comme on le comprendra plus tard, il est obligé de sortir du champ réel même (et surtout) pour résoudre les équations à coefficients réels et trois racines réelles. Puis c'est son disciple, Ludivico Ferrari (1522-1565) qui obtient la solution du degré quatre. Il faut attendre Niels Henrik Abel (1802-1829) pour que naisse la notion de nombre algébrique et que l'impossibilité de résolution par radicaux des équations de degré supérieur à cinq soit démontrée. C'est Évariste Galois qui donnera le critère général de résolubilité des équations par radicaux. La théorie de Galois est au cœur des recherches mathématiques actuelles (géométrie algébrique, travaux d'Alexander Grothendieck, programme de Robert P. Langlands etc.).

Mais tout ceci ne résout pas tout. En effet, numériquement, encore faut-il savoir extraire des radicaux et, surtout, ce n'est pas nécessairement la meilleure méthode, notamment pour les équations de degré au moins cinq, comme on vient de le souligner. Le premier problème numérique est d'isoler les racines. Si la méthode de dichotomie marche très bien pour les polynômes, il en existe d'autres plus spécifiques inventées par René Descartes (*La géométrie* 1638), Isaac Newton (*L'aritmétique universelle* 1685), Michel Rolle (1652-1719), James Stirling (1692-1770), Joseph Fourier (1768-1830), Augustin-Louis Cauchy (1789-1857), Charles Sturm (1803-1855) et Charles Hermite (1822-1901).

Théorème 5 - 13

Bornes de Lagrange et de Cauchy (♠)

Soit P un polynôme à coefficients complexes, unitaire, donné par $P = \sum_{k=0}^{n} a_k X^k$, et z une racine complexe de P, alors

$$|z| \leq \max\left(1, \sum_{0\leq k\leq n-1} |a_k|\right) \qquad \text{et} \qquad |z| \leq 1 + \max_{0\leq k\leq n-1} |a_k| \ .$$

Démonstration. Soit z une racine de P. Si on a $|z| \leq 1$ le résultat est immédiat. Sinon il vient

$$|z|^n = \left|\sum_{k=0}^{n-1} a_k z^k\right| \leq \sum_{k=0}^{n-1} |a_k|\,|z|^k$$

par inégalité triangulaire. Pour obtenir la borne de Lagrange on majore $|z|^k$ par $|z|^{n-1}$ (par positivité et puisque $|z| \geq 1$) et le résultat s'ensuit en divisant par $|z|^{n-1}$, qui est strictement positif. Quant à la borne de Cauchy, en posant $M = \max_{0\leq k\leq n-1} |a_k|$, il vient par positivité des termes

$$|z|^n \leq M \sum_{k=0}^{n-1} |z|^k = M\frac{|z|^n - 1}{|z| - 1} \leq M\frac{|z|^n}{|z| - 1}$$

et le résultat s'ensuit après division par $|z|^n$ et multiplication par $|z|-1$, deux quantités strictement positives. □

Algorithme 5 - 1

Méthode de Lagrange (♠)

Si P est un polynôme à coefficients réels et à racines simples $(x_i)_{1\leq i\leq n}$, il existe un polynôme unitaire Q dont les racines sont les nombres $\big((x_i-x_j)^2\big)_{1\leq i<j\leq n}$. Si δ est un majorant des racines de $X^{n(n-1)/2}Q(1/X)$ (obtenu avec l'une des bornes précédentes par exemples), alors les racines de P sont espacées d'au moins $\delta^{-1/2}$. Ceci permet de donner un critère de terminaison pour des algorithmes de recherche de racines.

Exemple 5 - 6

Soit $P=aX^2+bX+c$ avec $a\neq 0$ et x_1 et x_2 les racines de P (éventuellement confondues). Alors $(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=\frac{b^2-4ac}{a^2}$ et donc $Q=X-\frac{b^2-4ac}{a^2}$.

Remarque 5 - 11

Lorsque P est unitaire, le terme constant de Q est au signe près le discriminant de P. Ce dernier s'annule si et seulement si P admet une racine double.

Théorème 5 - 14

Relations de Viète

Si P est un polynôme non constant, noté $P=\sum_{k=0}^{n}a_kX^k$ et si $(x_i)_{1\leq i\leq n}$ sont ses racines (complexes) éventuellement confondues, on a

$$\sum_{1\leq i_1<\cdots<i_k\leq n} x_{i_1}\dots x_{i_k}=(-1)^k\frac{a_{n-k}}{a_n}\,.$$

Aparté

Les polynômes (en n variables) σ_k donnés par

$$\sigma_k=\sum_{1\leq i_1<\cdots<i_k\leq n} X_{i_1}\dots X_{i_k}$$

sont appelés polynômes symétriques élémentaires en n variables. Tout polynôme symétrique, i.e. vérifiant $P(X_1,\dots,X_n)=P(X_{\sigma(1)},\dots,X_{\sigma(n)})$ pour toute permutation σ dans S_n, est un polynôme en les σ_k.

Démonstration. On obtient $a_n\prod_{i=1}^{n}(X-x_i)=\sum_{k=0}^{n}(-1)^k\sigma_k(x_1,\dots,x_n)X^{n-k}$ en développant le produit, et le résultat s'ensuit. □

Remarque 5 - 12

Les coefficients du polynôme Q, dont les racines sont les nombres $\big((x_i-x_j)^2\big)_{1\leq i<j\leq n}$, s'expriment donc de façon rationnelle en fonction des coefficients de P puisque ce sont des quantités symétriques des racines de P.

Pour aller plus loin

Sommes de Newton

Les polynômes (en n variables) Σ_k donnés par $\Sigma_k = \sum_{i=1}^{n} X_i^k$ sont appelés sommes de Newton. Tout polynôme symétrique est également un polynôme en les Σ_k.

On peut montrer les identités de Girard (obtenues par Albert Girard en 1629 et par Isaac Newton en 1666) :

$$k\sigma_k + \sum_{i=1}^{k}(-1)^i \sigma_{k-i}\Sigma_i = 0 \quad \text{et} \quad ka_{n-k} + \sum_{i=1}^{k} a_{n-k+i}\Sigma_i = 0 \ .$$

Théorème 5 - 15

Règle des signes de Descartes - 1637 (♠)

Soit P dans $\mathbf{R}[X]$ somme de $n+1$ monômes non nuls (avec $n \in \mathbf{N}$). On écrit $P(X) = \sum_{k=0}^{n} a_k X^{b_k}$ avec $0 = b_0 < b_1 < \cdots < b_n$ et les a_k des réels tous non nuls. On note $V(P)$ le nombre de variations de signes des coefficients de P. Autrement dit

$$V(P) = \text{Card}\left\{k \in [\![1;n]\!] \,|\, a_k a_{k-1} < 0\right\} \ .$$

Le nombre de racines réelles (comptées avec multiplicité) strictement positives de P, noté $n_+(P)$ est majoré par $V(P)$.

Plus précisément $V(P) - n_+(P)$ est un entier naturel pair et $n_+(P) = V(P)$ si P est scindé sur $\mathbf{R}$.

Démonstration. Si P n'a aucune racine réelle strictement positive, on a $n_+(P) = 0 \leq V(P)$. Sinon on l'écrit

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

avec les (α_i) réels strictement positifs et on montre d'une façon générale $V(R(X-\alpha)) \geq V(R) + 1$ pour R dans $\mathbf{R}[X]$ et $\alpha \in \mathbf{R}_+^*$, ce qui permet de conclure car on aura alors $V(P) \geq V(Q) + k = V(Q) + n_+(P) \geq n_+(P)$, par une récurrence immédiate.

Soit alors R et α comme précédemment. On écrit $R = r\sum_{k=0}^{p}(-1)^k R_k$ avec r le coefficient dominant de R, $V(R) = p$ et des polynômes (R_k) à coefficients positifs de degrés d_k et valuations v_k vérifiant

$$v_0 > d_1 \geq v_1 > \cdots > d_p \geq v_p \ .$$

On remarque que le terme de degré v_k dans $(-1)^k(X-\alpha)R_k$ est de signe opposé à celui de degré $d_k + 1$ du même polynôme et, si $k < p$, du même signe que celui de degré $d_{k+1} + 1$ dans $(-1)^{k+1}(X-\alpha)R_{k+1}$. Au vu de l'hypothèse sur les valuations et degrés on en déduit que les signes des coeficients de $(X-\alpha)R$ sont ceux des coefficients non nuls parmi ceux des $(-1)^k(X-\alpha)R_k$. D'où un nombre impair de changements de signes entre les degrés $d_{k+1}+1$ et d_k+1 ainsi qu'entre les degrés d_p+1 et v_p. On a donc $V((X-\alpha)R) \geq p+1$, avec la précision sur la parité également.

Enfin on remarque $V(P) + V(P(-X)) \leq \deg(P)$. En effet si $a_k a_{k-1} < 0$ et $(-1)^{b_k} a_k (-1)^{b_{k-1}} a_{k-1} < 0$, alors $b_k - b_{k-1}$ est pair, donc supérieur à 2, et ainsi $b_n - b_0 = \sum_{k=1}^{n}(b_k - b_{k-1}) \geq V(P) + V(P(-X))$. Il vient $n_+(P) + n_+(P(-X)) \leq$

$V(P)+V(P(-X))\leq \deg(P)$. Or $n_+(P)+n_+(P(-X))$ est le nombre de racines de P puisque $b_0=0$ et donc $P(0)\neq 0$. Si P est scindé, il y a donc égalité dans toutes les inégalités et en particulier $n_+(P)=V(P)$. □

Exemple 5 - 7

Si $P=X^8-3X^7-4X^6+7X^5+3X^4-X^2-X-1$, la suite des signes s'écrit (+,-,-,+,+,-,-,-) et donc il y a au plus trois racines positives. Pour $P(-X)$ la suite devient (+,+,-,-,+,-,+,-) et il y a au plus cinq racines négatives. Il y a de plus un nombre impair de racines dans $\mathbf{R}_+^*$ et $\mathbf{R}_-^*$.

Remarque 5 - 13

Pour a et b réels, $V(P(X+a))$ et $V(P(b-X))$ fournissent des majorants du nombre de racines strictement supérieures à a et strictement inférieures à b respectivement.

Pour être plus précis et obtenir un majorant ou le nombre exact de racines d'un polynôme sur un intervalle donné on peut adapter les idées de DESCARTES. On construit divers suites associées à un polynôme et dépendant d'un réel x.

Fourier-Budan On considère la suite des dérivées $(P(x),P'(x),\dots,P^{(n)}(x))$.

Sturm Soit $(P_k)_{0\leq k\leq n}$ la suite de polynômes définie par $P_0=P$, $P_1=-P'$ et, pour $1\leq k\leq n-1$, P_{k+1} est l'opposé du reste dans la division euclidienne de P_{k-1} par P_k. On note m le plus grand indice tel que P_m ne soit pas le polynôme nul, Q_k le polynôme P_k/P_m pour $k\leq m$. On considère alors la suite $(Q_k(x))_{0\leq k\leq m}$.

On appelle nombre de changements de signes d'une suite $(u_k)_{0\leq k\leq n}$, le nombre de ses changements de signe sans tenir compte des termes nuls, i.e.

$$\text{Card}\left\{k\in[\![0;n-1]\!]\,|\,\exists \ell\in[\![k+1;n]\!]\ u_ku_\ell<0 \text{ et } u_{k+1}=\cdots=u_{\ell-1}=0\right\}\ .$$

Soit alors $v_x(P)$ et $w_x(P)$ le nombre de variations de signes respectifs des suites précédentes.

On admet alors les théorèmes suivants (démontrés en exercice).

Théorème 5 - 16

FOURIER-BUDAN (♠)

Soit $I=[a;b]$ un intervalle de $\mathbf{R}$. Si a et b ne sont pas racines de P, le nombre de racines (comptées avec multiplicité) de P dans I est majoré par $v_a(P)-v_b(P)$, et a même parité. Si de plus P n'a que des racines réelles, il y a en fait égalité.

Théorème 5 - 17

STURM (♠)

Soit $I=[a;b[$ un intervalle de $\mathbf{R}$. Le nombre de racines (comptées sans multiplicité) de P dans I est égal à $w_b(P)-w_a(P)$.

Pour aller plus loin

Isaac NEWTON a énoncé en 1707 une règle plus précise que celle de DESCARTES, mettant en jeu la suite $\alpha_k^2-\alpha_{k+1}\alpha_{k-1}$, où $a_k=\binom{n}{k}\alpha_k$. Par exemple avec $2X^4-13X^2+10X-49$ la règle de DESCARTES donne au plus trois racines positives et au plus une racine négative (et donc exactement une puisque le polynôme est pair et négatif en 0). NEWTON écrit les suites $(-49,5/2,-13/6,0,2)$ et $(2401,-1199/12,169/36,13/3,4)$ et en conclut qu'il y a au plus une racine positive et une racine négative. Il ne compte que les variations de la première suite qui ne correspondent pas à une variation dans la seconde. Ainsi il ne retient que la variation de signe entre $-13/6$ et 2. Cette règle a été démontrée en 1864 par James Joseph SYLVESTER (1814-1897).

5 Nombres – Au delà du rationnel

Le nombre entier naturel semble directement accessible mais formaliser sa définition n'est pas si simple. Que ce soit pour les besoins de l'addition ou de la multiplication, et surtout de leurs applications réciproques, on a besoin des entiers relatifs et des rationnels. Leur construction a lieu au collège et leur absence dans la vie quotidienne montre qu'ils sont d'un abord ardu. Le nombre rationnel, sous forme de fraction, est souvent caché derrière son développement décimal et celui-ci est tronqué à ses deux premiers chiffres faute de donner un sens aux décimales suivantes. Pourtant des questions ou observations simples comme la diagonale d'un carré, le format A4, un cercle etc. font appel à des nombres qui ne sont ni entiers, ni rationnels. Ceci n'empêche pas de les définir à partir de nombres rationnels et même à partir d'équations polynomiales à coefficients enters : $x^2+y^2=1$, $x^2=2$ etc. Le nombre entier naturel s'additionne, se multiplie. Correctement étendu le nombre devient un élément d'un corps, d'une algèbre. Il ne paraît pas facile d'additionner des nombres via les équations qui les définissent. La route la plus évidente semble de les calculer mais pour aller plus loin, il faudra trouver d'autres méthodes, algébriques.

Les méthodes précédentes permettent de localiser les racines d'un polynôme et donc de les calculer de façon aussi précise que l'on veut. Même s'il n'est pas clair que l'on en ait une meilleure compréhension. Pour cela il faudrait en créer une image plus forte qu'une suite de chiffres dont il n'est pas clair de savoir ce qui se trouve après les points de suspension.

Exemple 5 - 8

Lagrange a mis au point une méthode qui permet de calculer sur des nombres entiers, plus porteuse de sens et moins entâchée d'erreurs. En voici un exemple. On cherche à calculer la racine positive de X^2-X-1, i.e. le nombre d'or (souvent noté φ). La règle de Descartes assure en effet qu'il y a au plus une racine positive, et donc exactement une seule par parité. Un calcul direct donne $P(1)=-1<0<1=P(2)$ et donc $1<\varphi<2$. On pourrait continuer par dichotomie mais les calculs seront vite pénibles. Plutôt que cela on pose $x=1+\dfrac{1}{y}$, avec $y>0$, de sorte que $P(x)=-1+\dfrac{1}{y}+\dfrac{1}{y^2}$ d'après la formule de Taylor avec $P(1)=-1$, $P'(1)=1$ et $P''(1)=2$. Ainsi x est racine de P si et seulement si $-y^2+y+1=0$, en remettant au même dénominateur. Autrement dit x est racine de P si et seulement si y l'est et donc y est alors compris entre 1 et 2. En itérant le processus, on en déduit

$$\varphi=1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}.$$

Cela permet d'avoir des approximations successives : 1, 2, $\dfrac{3}{2}$, $\dfrac{5}{3}$ en arrêtant le processus à la n^{e} barre de fraction et, d'autre part, en utilisant la positivité des termes, de préciser l'écart avec la valeur réelle.

Dans le cas d'une équation du second degré, il n'y a pas besoin de tant de théorie pour arriver à ce résultat. C'est différent avec une équation de degré plus grand. Par exemple avec X^3-2X-5. La règle des signes donne une unique racine positive et

comme $P(2) = -1$ et $P(3) = 16$, elle est comprise entre 2 et 3. En posant $x = 2 + \dfrac{1}{y}$ et en utilisant la formule de TAYLOR on trouve que x est racine de P si et seulement si y l'est de $X^3 - 10X^2 - 6X - 1$. Ici la valeur en 10 est négative et celle en 11 positive et on pose donc $y = 10 + \dfrac{1}{z}$. On trouve que z est racine de $61X^3 - 94X^2 - 20X - 1$, donc compris entre 1 et 2 etc. Au final la racine positive de P est donnée par

$$x = 2 + \cfrac{1}{10 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}.$$

On en déduit les approximations 2, $\dfrac{21}{10}$, $\dfrac{23}{11}$, $\dfrac{44}{21}$ et on peut préciser par exemple, en utilisant la théorie des fractions continues

$$\left| x - \frac{44}{21} \right| \leq \frac{1}{21(21+11)} = \frac{1}{672}.$$

Pour aller plus loin

La formule de TAYLOR peut se calculer rapidement grâce au schéma de William George HORNER (1786-1837), n'utilisant que des multiplications simples et des additions. En voici une illustration pour calculer $P(a + y^{-1})$:

a	X^3	X^2	X	1
2	**1**	**0**	**-2**	**-5**
+		2	4	4
$\times a$	1	**2**	**2**	**-1**
+		2	8	
$\times a$	1	4	**10**	
+		2		
$\times a$	1	**6**		
+				
	1			

Le résultat de la multiplication par 2 est écrit dans la case en diagonale vers le haut et la droite par rapport au terme de départ. On lit 1, 6, 10, -1, i.e. $P(2 + X) = X^3 + 6X^2 + 10X - 1$.

Ces nombres ne sont pas très manipulables : ce sont des valeurs, mais pas des objets que l'on peut additionner, multiplier etc. Le comble pour des nombres ! Il serait plus convaincant de créer une algèbre dans laquelle ces nombres existent clairement et c'est ce que rendent possible, par exemple, les matrices. Ainsi, si $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, on a

$$A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = A + I_2$$

et donc A est une racine de $X^2 - X - 1$! D'après les formules de VIÈTE, l'autre racine est $I_2 - A$, puisque la somme des racines fait 1, ou encore $-A^{-1}$ puisque leur produit

fait -1. On peut le vérifier :

$$I_2 - A = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -I_2 \ .$$

On peut maintenant calculer avec φ. Par exemple pour calculer $(\varphi^2+2\varphi+1)(2\varphi^2-3)$, il suffit de calculer

$$\left(\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} + 2\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + I_2\right) \cdot \left(2\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} - 3I_2\right) = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 7 & 11 \end{pmatrix}$$

et comme la dernière matrice s'écrit aussi $7\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + 4I_2$, le résultat est $7\varphi + 4$.

On peut voir que tous les calculs se font dans l'algèbre $\mathscr{M}_2(\mathbf{R})$, bien entendu, mais comme celle-ci n'est pas commutative, ils se font plutôt dans une sous-algèbre. On vérifie directement qu'il s'agit de $\left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \;\middle|\; (a,b) \in \mathbf{R}^2 \right\}$. Pour s'assurer qu'on a affaire à une algèbre on peut bien sûr le faire à la main, mais il est plus commode de remarquer qu'il s'agit des matrices de la forme $aI_2 + bA$. On a alors directement

$$\begin{cases} (aI_2 + bA) + (cI_2 + dA) = (a+c)I_2 + (b+d)A \\ (aI_2 + bA)(cI_2 + dA) = acI_2 + (ad+bc)A + adA^2 = (ac+ad)I_2 + (ad+bc+ad)A \end{cases}$$

car $A^2 = A + I_2$.

Remarque 5 - 14

Comme on le voit les matrices permettent de créer des nombres. Un détail cependant : nulle part on a écrit que A est un réel positif ! En fait A contient les deux racines de X^2-X-1 à la fois en ce sens que l'endomorphisme canoniquement associé admet une matrice plus simple, diagonale, formée des deux réels φ et $1-\varphi$. Comme on l'a vu, il en va de même pour $I_2 - A$. Plus précisément $A\begin{pmatrix} 1 \\ \varphi \end{pmatrix} = \begin{pmatrix} \varphi \\ 1+\varphi \end{pmatrix} = \varphi\begin{pmatrix} 1 \\ \varphi \end{pmatrix}$ et $A\begin{pmatrix} 1 \\ 1-\varphi \end{pmatrix} = \begin{pmatrix} 1-\varphi \\ 2-\varphi \end{pmatrix} = (1-\varphi)\begin{pmatrix} 1 \\ 1-\varphi \end{pmatrix}$, car $(1-\varphi)^2 = 1 - 2\varphi + \varphi^2 = 2 - \varphi$, et il vient

$$\begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix}^{-1} A \begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix} = \begin{pmatrix} \varphi & 0 \\ 0 & 1-\varphi \end{pmatrix} \ .$$

En notant P la matrice $\begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix}$, on a $P^{-1}AP = D$ avec D diagonale. Et alors $P^{-1}(I_2 - A)P = P^{-1}I_2P - P^{-1}AP = I_2 - D$, de sorte que $P^{-1}(I_2 - A)P$ est également diagonale. Mieux : ses éléments diagonaux sont ceux de D, mais permutés.

De la même façon on peut créer

$$\sqrt{2} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \ .$$

Le deuxième exemple fournit $\mathbf{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; (a,b) \in \mathbf{R}^2 \right\}$, ce qui permet de voir les complexes comme des applications linéaires du plan, et plus précisément la composée d'une homothétie de rapport $\sqrt{a^2+b^2}$ et d'une rotation, ce qui revient à décomposer un complexe sous forme polaire. Ainsi i n'est rien d'autre que la rotation d'un quart de tour, ce qui est évident si on songe que i^2 est un demi-tour et i^4 l'identité.

Pour les équations de degré supérieur, une matrice apparaît naturellement, la matrice compagnon du polynôme $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ est donnée par

$$\begin{pmatrix} 0 & & & (0) & -a_0 \\ 1 & 0 & & & \vdots \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ (0) & & & 1 & -a_{n-1} \end{pmatrix}$$

puisque par construction l'image de e_1 est e_2, celle de e_2 est e_3, etc. et donc en notant A cette matrice on a $Ae_1 = e_2$, $A^2e_1 = Ae_2 = e_3$, …, $A^{n-1}e_1 = e_n$ et $A^ne_1 = Ae_n = -a_0e_1 - a_1e_2 - \cdots - a_{n-1}e_n$ et donc $\left(A^n + a_{n-1}A^{n-1} + \cdots + a_0I_2\right)e_1 = 0$ et pour k entre 2 et n, on a $e_k = A^{k-1}e_1$ et comme A^{k-1} commute avec I_2, A, etc. il vient

$$\left(A^n + a_{n-1}A^{n-1} + \cdots + a_0I_2\right)e_k = A^k\left(A^n + a_{n-1}A^{n-1} + \cdots + a_0I_2\right)e_1 = 0$$

et donc $A^n + a_{n-1}A^{n-1} + \cdots + a_0I_2$ est la matrice nulle.

6 Polynômes d'endomorphismes

On est amené à considérer des polynômes (ou plutôt des fonctions polynomiales) dont la variable est une matrice. C'est ainsi que l'on peut construire les nombres complexes, les quaternions de Sir William Rowan Hamilton (1805-1865) ou les octonions de Sir Arthur Cayley (1821-1895). Comme une matrice est, ou représente c'est selon, une application linéaire, on est aussi amené aux polynômes d'endomorphismes.

Définition 5 - 9

Soit E un espace vectoriel sur un corps $\mathbf{K}$, u dans $\mathrm{End}(E)$ et P dans $\mathbf{K}[X]$. L'endomorphisme $P(u)$ de E est l'application donnée par

$$x \mapsto a_0x + a_1u(x) + a_2u(u(x)) + \cdots + a_nu^n(x)$$

avec $P = \sum_{k=0}^{n} a_kX^k$ et u^k désigne la composé de u avec lui-même k fois : $u^0 = \mathrm{Id}_E$ et $u^{k+1} = u \circ u^k$.

Un des théorèmes fondamentaux pour l'étude des endomorphismes linéaires est le théorème suivant.

Théorème 5 - 18

Cayley-Hamilton – Georg Frobenius (1878)

Soit A dans $\mathscr{M}_n(\mathbf{K})$. L'application $x \mapsto \det(xI_n - A)$ est polynomiale de degré n. Si on note χ_A le polynôme associé, appelé polynôme caractéristique de A, on a $\chi_A(A) = 0$.

Nous démontrerons ce théorème dans le cadre du chapitre sur la réduction.

Exemple 5 - 9

Si A est la matrice compagnon du polynôme P, alors $\chi_A = P$ et nous avons donc déjà démontré le théorème de Cayley-Hamilton dans ce cas.

À u on peut associer φ_u le morphisme d'algèbres de $\mathbf{K}[X]$ dans $\mathrm{End}(E)$ donné par $\varphi_u(P) = P(u)$. En effet φ_u est un morphisme de $\mathbf{K}$-espaces vectoriels et il suffit donc de vérifier que φ_u préserve la multiplication sur les éléments de la base canonique de $\mathbf{K}[X]$, i.e. $u^{p+q} = u^p \circ u^q$ pour p et q entiers naturels, ce qui est la définition.

Définition 5 - 10

On note $\mathbf{K}[u]$ l'image de φ_u. Ce sont les polynômes en l'endomorphisme u.

Puisque $\mathbf{K}[X]$ est une algèbre commutative, il en est de même pour son image par le morphisme d'algèbres φ_u.

Propriété 5 - 2

L'algèbre $\mathbf{K}[u]$ est une sous-algèbre commutative de $\mathrm{End}(E)$. En particulier pour P et Q dans $\mathbf{K}[X]$, on a $P(u) \circ Q(u) = Q(u) \circ P(u)$.

Définition 5 - 11

Un polynôme P de $\mathbf{K}[X]$ est appelé polynôme annulateur de u si $P \in \mathrm{Ker}(\varphi_u)$, i.e. si $P(u)$ est l'endomorphisme nul.

Pour des raisons de dimension, si celle de E est finie alors φ_u n'est pas injectif. Remarquons aussi que si P appartient à $\mathrm{Ker}(\varphi_u)$ il en va de même pour tout multiple de P, que ce soit un multiple scalaire ou un multiple polynomial. On peut alors considérer $\{\deg(P) \,|\, P \in \mathrm{Ker}(\varphi_u), P \neq 0\}$. C'est une partie non vide de $\mathbf{N}$, et même de $\mathbf{N}^*$, et on peut en considérer le plus petit élément, noté d, ainsi qu'un élément de $\mathrm{Ker}(\varphi_u)$ de degré d. Quitte à le multiplier par un scalaire, on peut considérer un tel polynôme qui soit de surcroît unitaire. On le note P. La remarque précédente montre que tous les multiples de P sont dans $\mathrm{Ker}(\varphi_u)$. Réciproquement si $Q(u) = 0$, on écrit la division euclidienne $P = BQ + R$ et on a $R(u) = P(u) - B(u) \circ Q(u) = 0$ avec $\deg(R) < \deg(P)$. Il vient $R = 0$ et donc $Q \in P\mathbf{K}[X]$.

Définition 5 - 12

Si E est de dimension finie, on appelle polynôme minimal de u l'unique polynôme unitaire π_u tel que $\mathrm{Ker}(\varphi_u) = \pi_u \mathbf{K}[X]$.

Autrement dit π_u est le polynôme unitaire de degré minimal annulant u et si P est un polynôme annulateur de u, alors $\pi_u \mid P$.

Propriété 5 - 3

Si E est de dimension finie, on a $\deg(\pi_u) \geq 1$ et en fait $\deg(\pi_u) = \dim(\mathbf{K}[u])$.

En effet la division euclidienne par π_u donne

$$\mathbf{K}[X] = \pi_u \mathbf{K}[X] \oplus \mathbf{K}_{\deg(\pi_u)-1}[X] = \mathrm{Ker}(\varphi_u) \oplus \mathbf{K}_{\deg(\pi_u)-1}[X]$$

et donc, d'après le théorème du rang

$$\mathbf{K}[u] = \mathrm{Im}(u) \simeq \mathbf{K}_{\deg(\pi_u)-1}[X] \,.$$

Exemples 5 - 10

— Si u est une homothétie de rapport λ, $\pi_u = X - \lambda$.
— Si u est un projecteur distinct de 0 et Id_E, $\pi_u = X^2 - X$.
— Si u est une symétrie distincte de $\pm\mathrm{Id}_E$, $\pi_u = X^2 - 1$.
— Si $E = \mathbf{K}_n[X]$ et u est donnée par $u(P) = P'$, alors $\pi_u = X^{n+1}$.

Remarque 5 - 15

Matrice compagnon

L'application linéaire définie par $u(e_i) = e_{i+1}$ pour $1 \leq i \leq n-1$ et

$$u(e_n) = -\sum_{i=1}^{n} a_{i-1} e_i \,,$$

où $(e_i)_{1\leq i\leq n}$ est une base de E, admet $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ comme polynôme minimal et on a donc $\chi_u = \pi_u$.

On peut interpréter les résultats sur les suites récurrentes linéaires et les équations différentielles linéaires à coefficients constants avec cette application linéaire.

Exercices

Généralités

5 - 1 Ⓢ ★

Soit u l'endomorphisme de $\mathbf{K}_n[X]$ défini par $u(P) = P(1-X)$, avec $\mathbf{K}$ un sous-corps de $\mathbf{C}$.

a. Calculer u^2.

b. Déterminer une base (P_k) échelonnée en degré de $\mathbf{K}_n[X]$ telle que pour tout entier k on ait $u(P_k)$ colinéaire à P_k.

5 - 2 Ⓢ ★★ Jeu de Passe-dix

a. Soit p un entier supérieur à 3 et T_n le polynôme de Hilbert, i.e. $T_n = \binom{X}{n}$. Montrer

$$\deg\left(X^p - (X-1)^3 \sum_{k=3}^{p} T_2(k-1) X^{p-k}\right) < 3 .$$

b. Quelle est la probabilité que la somme des faces d'un lancer de trois dés soit supérieure à 10 ?

Indication : On pourra considérer le polynôme $(X+X^2+\cdots+X^6)^3$.

5 - 3 Ⓢ M 2017 ★★ ♥

a. Soit A et B dans $\mathscr{M}_n(\mathbf{K})$ avec B la matrice dont tous les éléments sont égaux à 1. Soit f l'application de $\mathbf{K}$ dans lui-même définie par $f(x) = \det(A+xB)$. Montrer que f est affine.

b. Calculer, pour $\lambda_1, \ldots, \lambda_n$, a, b réels, le déterminant d'ordre n

$$D_n = \begin{vmatrix} \lambda_1 & a & \cdots & a \\ b & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a \\ b & \cdots & b & \lambda_n \end{vmatrix} .$$

5 - 4 Ⓢ ★★ Théorèmes de Bolzano & Rolle

Michel Rolle conspuait l'analyse, à laquelle il ne croyait pas. Son théorème est donc un théorème d'algèbre, même si Pierre-Ossian Bonnet en a fait, des années plus tard, un des piliers de l'analyse moderne ! Soit P un polynôme non constant de $\mathbf{R}[X]$. On écrit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_n \neq 0$. On note $x_1 < x_2 < \cdots < x_n$ ses racines réelles, n_i l'ordre de multiplicité de x_i et on **définit** $P' = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i$. Il s'agit de montrer qu'entre deux racines successives de P s'en trouve une de P'. On peut vérifier qu'avec cette définition on a encore $(PQ)' = P'Q + PQ'$ ainsi que la formule plus générale, dite de Leibniz.

a. Soit $a < b$ deux réels et Q un polynôme irréductible de $\mathbf{R}[X]$ ne s'annulant pas sur le segment $[\,a;b\,]$. Montrer, sans utiliser le théorème de Bolzano mais en utilisant la classification des irréductibles dans $\mathbf{R}[X]$, $Q(a)Q(b) > 0$.

b. Montrer que, pour tout $1 \leq i \leq n-1$, on peut écrire $P = (X-x_i)^{n_i}(X-x_{i+1})^{n_{i+1}} Q_i$ avec $Q_i(x_i)Q_i(x_{i+1}) > 0$.

c. Avec les notations précédentes, montrer qu'il existe un polynôme R_i dans $\mathbf{R}[X]$ tel que $P' = (X-x_i)^{n_i-1}(X-x_{i+1})^{n_{i+1}-1} R_i$ avec $R_i(x_i)R_i(x_{i+1}) < 0$.

d. En déduire, toujours sans utiliser le théorème de Bolzano, qu'il existe c dans $]x_i;x_{i+1}[$ tel que $P'(c) = 0$.

Arithmétique des polynômes

5 - 5 Ⓢ ★ Contenu

Soit P dans $\mathbf{Z}[X]$. On appelle contenu de P, noté $c(P)$, le pgcd de ses coefficients. Montrer que pour P et Q dans $\mathbf{Z}[X]$, on a $c(PQ) = c(P)c(Q)$.

5 - 6 Ⓢ ★ Contenu

Soit P dans $\mathbf{Q}[X]$, non nul. Montrer qu'il existe un unique polynôme Q dans $\mathbf{Z}[X]$ et un unique rationnel a tels que $P = aQ$ et $c(Q) = 1$. En notant $a = c(P)$, montrer que c est multiplicative, i.e. que la propriété de l'exercice 5 - 5 s'étend à $\mathbf{Q}[X]$.

5 - 7 Ⓢ ★ Lemme de Gauss

Soit P dans $\mathbf{Z}[X]$. On dit que P est primitif si $c(P) = 1$ (voir exercice 5 - 5).

Montrer que P est irréductible dans $\mathbf{Z}[X]$ si et seulement s'il l'est dans $\mathbf{Q}[X]$ et s'il est primitif. On pourra utiliser l'exercice 5 - 6.

5 - 8 Ⓢ ★ Caractérisation d'un polynôme

Soit a et b deux nombres complexes distincts et P et Q unitaires non constants dans $\mathbf{C}[X]$ vérifiant $P^{-1}(a) = Q^{-1}(a)$ et $P^{-1}(b) = Q^{-1}(b)$. On pose $R = (P-a)(P-b)$. Enfin, quitte à échanger P et Q, on suppose que P est de degré supérieur à celui de Q.

a. Montrer que les racines de R sont également des racines de $P-Q$.

b. Montrer que $P-a$ et $P-b$ sont premiers entre eux.

c. Soit x une racine multiple de R d'ordre k (avec $k > 1$). Montrer que c'est une racine d'ordre k de $P-a$ ou de $P-b$, et d'ordre au moins k de $P'(P-Q)$.

d. En déduire que R divise $P'(P-Q)$.

e. En considérant les degrés de ces polynômes, montrer $P = Q$.

f. Montrer que la conclusion ne tient pas si on suppose seulement $P^{-1}(a) = Q^{-1}(a)$.

5 - 9 Ⓢ ★★ **Cristère d'Eisenstein**

Soit p un nombre premier et P dans $\mathbf{Z}[X]$. On note $P = \sum_{k=0}^{n} a_k X^k$ avec $a_n \neq 0$. On suppose que p divise tous les coefficients de P sauf a_n et que p^2 ne divise pas a_0. Montrer que P est irréductible sur $\mathbf{Q}[X]$. Gotthold Eisenstein, 1823–1852, un des brillant-e-s mathématicien-ne-s du XIX$^{\text{e}}$ siècle mort-e-s avant 30 ans.

5 - 10 Ⓢ ★★ **Polynômes cyclotomiques - p premier**

Soit n dans $\mathbf{N}^*$. On note Φ_n le polynôme unitaire de $\mathbf{C}[X]$ dont les racines (simples) sont exactement les racines primitives n^{e} de l'unité.

a. Soit p un nombre premier. Montrer $\Phi_p = \sum_{k=0}^{p-1} X^k$ et déduire de l'exercice 5 - 9 que Φ_p est un polynôme irréductible de $\mathbf{Z}[X]$.

b. Soit k dans $\mathbf{N}^*$. Montrer $\Phi_{p^k} = \Phi_p(X^{p^{k-1}})$ et en déduire que Φ_{p^k} est également un polynôme irréductible de $\mathbf{Z}[X]$.

5 - 11 Ⓢ ★★★ **Décomposition dans $\mathbf{Z}[X]$**

Soit P dans $\mathbf{Z}[X]$. Montrer que si P est non nul, il peut s'écrire sous la forme

$$P = \pm p_1^{k_1} \cdots p_r^{k_r} A_1^{n_1} \cdots A_s^{n_s}$$

où les p_i sont des nombres premiers distincts, A_i des polynômes dans $\mathbf{Z}[X]$ irréductibles et distincts, k_i et n_i des entiers naturels non nuls, r et s des entiers naturels.

Discuter l'unicité de cette écriture.

5 - 12 ★★★ **Polynômes cyclotomiques**

On reprend l'exercice 5 - 9. Soit α une racine primitive n^{e} de l'unité, avec $n \geq 2$ non nécessairement premier.

a. Montrer que l'ensemble des polynômes dans $\mathbf{Q}[X]$ annulant α forme un idéal non nul de $\mathbf{Q}[X]$. On note P le générateur unitaire de cet idéal et $d+1$ son degré.

b. Montrer que P est dans $\mathbf{Z}[X]$.

c. Montrer que, pour tout entier k, il existe un unique P_k dans $\mathbf{Z}_d[X]$ tel que $P(\alpha^k) = P_k(\alpha)$.

d. Soit p un nombre premier et Q et R dans $\mathbf{Z}[X]$, montrer que $(Q+R)^p - Q^p - R^p$ est un polynôme à coefficients entiers tous divisibles par p. On pourra commencer par montrer que si on a $0 < k < p$, alors $p \mid \binom{p}{k}$.

e. En déduire que P_p est à coefficients divisibles par p.

f. On écrit $P_k = \sum_{i=0}^{d-1} a_i^{(k)} X^i$ et on pose $A = \max_{1\leq k\leq n} \max_{0\leq i<d} \left|a_i^{(k)}\right|$. Montrer que pour p premier vérifiant $p > A$, on a $P_p = 0$.

g. En déduire que pour m n'ayant que des facteurs premiers strictement supérieurs à A, on a $P_m = 0$.

h. Soit maintenant k un entier quelconque premier à n, q le produit de tous les nombres premiers inférieurs à A et ne divisant par k. Montrer que $k + nq$ n'a aucun facteur premier inférieur à A et en déduire $P_k = 0$ puis $P = \Phi_n$.

Équations polynomiales

5 - 13 ★ **Règle de Descartes**

Donner le nombre de racines réelles du polynôme $X^4 + 3X^2 + 5X - 7$ et préciser leurs signes.

5 - 14 Ⓢ ★ **Racines toutes strictement positives**

Soit n un entier supérieur à 2 et x_1, x_2, …, x_n des nombres réels. On note σ_1, σ_2, …, σ_n leurs fonctions symétriques élémentaires, i.e.

$$\sigma_k = \sum_{1\leq i_1<i_2<\ldots<i_k\leq n} x_{i_1} x_{i_2} \cdots x_{i_k} = \sum_{\substack{I\subset[\![1;n]\!] \\ \text{Card}(I)=k}} \prod_{i\in I} x_i \ .$$

a. Donner en fonction de $(\sigma_k)_{1\leq k\leq n}$ les coefficients du polynôme unitaire admettant x_1, x_2, …, x_n comme racines (formules de Newton).

b. Donner les racines du polynôme P donné par $P = X^n + \sigma_1 X^{n-1} + \cdots + \sigma_{n-1} X + \sigma_n$.

c. On suppose σ_1, σ_2, …, σ_n strictement positifs. Montrer $u \in \mathbf{R}_+^* \Longrightarrow P(u) \in \mathbf{R}_+^*$.

d. Montrer que x_1, x_2, …, x_n sont strictement positifs si et seulement si σ_1, σ_2, …, σ_n le sont.

5 - 15 Ⓢ ★ **Polynômes hyperboliques**

On appelle hyperbolique un polynôme dans $\mathbf{R}[X]$ scindé sur $\mathbf{R}$, i.e. admettant toutes ses racines réelles. Montrer que P dans $\mathbf{R}[X]$, unitaire, est hyperbolique si et seulement si

$$\forall z \in \mathbf{C} \qquad |\text{Im}(z)|^n \leq |P(z)| \ .$$

Indication : pour tout nombre complexe u, on a $|\text{Im}(u)| \leq |u|$.

5 - 16 Ⓢ ★★ **Minoration des racines**

À partir des bornes de Lagrange ou de Cauchy, donner une minoration de la valeur absolue des racines d'un polynôme de valuation nulle.

5 - 17 Ⓢ ★★ **Homogénéisation des bornes**

Soit P dans $\mathbf{C}[X]$ non nul et non nécessairement unitaire et z une racine de P.

a. Montrer $|z| \leq \max\left(1, \sum_{0\leq k\leq n-1} \frac{|a_k|}{|a_n|}\right)$ et $|z| \leq 1 + \max_{0\leq k\leq n-1} \frac{|a_k|}{|a_n|}$.

b. En déduire

$$|z| \leq \min_{s>0} \max\left(s, \sum_{0\leq k\leq n-1} \frac{|a_k|}{|a_n|} s^{k-n+1}\right)$$

et

$$|z| \leq \min_{s>0}\left(s + \max_{0\leq k\leq n-1} \frac{|a_k|}{|a_n|} s^{k-n+1}\right).$$

5 - 18 Ⓢ ★★ Borne de Zassenhauss

Soit P dans $\mathbf{C}[X]$ non constant, avec $P = \sum_{k=0}^{n} a_k X^k$ et $a_n \neq 0$, et z une racine de P. Montrer

$$|z| \leq 2 \max_{0\leq k\leq n-1}\left(\left|\frac{a_k}{a_n}\right|^{\frac{1}{n-k}}\right).$$

5 - 19 Ⓢ ★★ Règle des signes de Descartes

On veut démontrer la règle des signes de façon directe, en utilisant le théorème de Rolle et celui de Bolzano, ce qui ne veut pas nécessairement dire qu'on utilise de l'analyse ! On procède par récurrence sur le nombre de monômes dans P, noté $n+1$. On suppose P de valuation nulle et on écrit $P = \sum_{k=0}^{n} a_k X^{b_k}$.

a. Traiter le cas $n = 0$ et celui où P n'a pas de racine réelle strictement positive.

b. On suppose $n \geq 1$ et que P a au moins une racine réelle strictement positive. On note $(x_1, \ldots, x_j)$ les zéros de P sur $\mathbf{R}_+^*$ et $(m_1, \ldots, m_j)$ leurs multiplicités.

i. On écrit $P' = X^a Q$ où $a = \mathrm{val}(P')$. Montrer que $V(Q)$ est bien défini et appartient à $\{V(P), V(P)-1\}$ et préciser les cas.

ii. En supposant $n_+(Q) \leq V(Q)$ et $V(Q) = V(P) - 1$, établir $n_+(P) \leq V(P)$. On pourra commencer par supposer les racines de P simples, puis tenir compte des multiplicités.

iii. En supposant $n_+(Q) \leq V(Q)$ et $V(Q) = V(P)$, établir $n_+(P) \leq V(P)$. On pourra montrer que P' admet une racine sur $]0; x_1[$.

c. Conclure $n_+(P) \leq V(P)$ en toute généralité et montrer qu'il y a égalité si P a toutes ses racines réelles.

d. Où a-t-on utilisé que les (b_k) sont entiers ? En déduire le théorème de Laguerre, à savoir $n_+(P) \leq V(P)$ mais en prenant les (b_k) réels.

5 - 20 Ⓢ ★★ Borne de Cauchy

Soit P un polynôme à coefficients complexes, unitaire et valuation nulle, donné par $P = \sum_{k=0}^{n} a_k X^k$, et z une racine complexe de P. On considère Q le polynôme donné par $Q = X^n - \sum_{k=0}^{n-1} |a_k| X^k$.

a. Montrer que Q admet une unique racine strictement positive. On la note ρ.

b. Montrer $|z| \leq \rho$.

c. En déduire les bornes de Lagrange et Cauchy. (En fait la borne donnée par Cauchy est ρ.)

5 - 21 Ⓢ ★★★ †

On cherche à factoriser, pour a, b et c dans $\mathbf{K}$, le polynôme P donné par

$$P = \begin{vmatrix} X & a & b & c \\ a & X & b & c \\ b & c & X & a \\ c & b & a & X \end{vmatrix}.$$

a. Montrer que a et $-(a+b+c)$ sont racines de P.

b. Factoriser P par $(X-a)(X+a+b+c)$ par opérations élémentaires.

c. Conclure.

5 - 22 Ⓢ M 2017 ★★★ Déterminant de Vandermonde à trous

Soit $(\lambda_i)_{1\leq i\leq n}$ des réels tous distincts.

a. Factoriser $\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_1^{n-2} & \lambda_2^{n-2} & \cdots & \lambda_n^{n-2} \\ \lambda_1^{n} & \lambda_2^{n} & \cdots & \lambda_n^{n} \end{vmatrix}$.

b. Plus généralement soit $(k_i)_{1\leq i\leq n}$ des entiers naturels tels que $k_1 < k_2 < \cdots < k_n$. On suppose $0 < \lambda_1 < \lambda_2 < \cdots < \lambda_n$. Montrer $\begin{vmatrix} \lambda_1^{k_1} & \lambda_2^{k_1} & \cdots & \lambda_n^{k_1} \\ \lambda_1^{k_2} & \lambda_2^{k_2} & \cdots & \lambda_n^{k_2} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_1^{k_n} & \lambda_2^{k_n} & \cdots & \lambda_n^{k_n} \end{vmatrix} > 0$.

5 - 23 Ⓢ ★★★ Règle de Fourier-Budan

Soit P un polynôme à coefficients réels de degré n et Z l'ensemble de tous les zéros de P et de ses polynômes dérivés. On reprend les notations du théorème de Fourier-Budan.

a. Montrer que Z est fini et que $v_x(P)$ est constante sur tout intervalle contenu dans $\mathbf{R} \setminus Z$.

b. On note $z_1 < z_2 < \ldots < z_p$ les éléments de Z. Montrer $v_x(x) = 0$ si $x > z_p$ et $v_x = n$ si $x < z_1$.

c. Soit c de Z, et k et ℓ deux indices tels que $P^{(k)}(c) = a_k \neq 0$, $P^{(\ell)}(c) = a_l \neq 0$ et, si $k < j < \ell$, $P^{(j)}(c) = 0$. Montrer que le nombre de changements de signes dans la suite $(P^{(j)}(x))_{k\leq j\leq \ell}$ est plus grand pour $x > c$ que pour $x < c$, au moins pour x dans un certain intervalle ouvert contenant c que l'on précisera. On distinguera le cas $\ell > k+1$ et le cas $\ell = k+1$.

d. En déduire que si c n'est pas un zéro de P, on a

$$\lim_{x\to c, x<c} v_x(P) - \lim_{x\to c, x>c} v_x(P) \geq 0 \ .$$

e. Montrer que si c est un zéro de P on a $\lim\limits_{x\to c, x<c} v_x(P) - \lim\limits_{x\to c, x>c} v_x(P) \geq m$, en notant m sa multiplicité dans P.

f. En déduire que si a et b sont deux réels tel que $a < b$ et a et b ne soient pas racines de P, alors le nombre de racines de P contenues dans $[\,a;b\,]$ est majoré par $v_a(P) - v_b(P)$.

g. Montrer que si P est scindé, il y a en fait égalité.

5 - 24 Ⓢ ★★★ Théorème de Sturm

Soit P un polynôme à coefficients réels de degré n et Z l'ensemble de tous les zéros des polynômes Q_k, en reprenant les notations du théorème de Sturm.

a. Montrer que P_m est le pgcd de P et P' et qu'il divise tous les termes de la suite $(P_k)_{0\leq k\leq m}$.

b. On suppose tout d'abord P à racines simples.

i. Montrer que Q_m ne s'annule pas.

ii. Si c est une racine réelle de P, montrer $Q_0'(c)Q_1(c) < 0$.

iii. Si c est une racine réelle de Q_k, pour $1 \leq k \leq m-1$, montrer $Q_{k-1}(c)Q_{k+1}(c) < 0$.

iv. Conclure dans ce cas en s'inspirant de l'exercice 5 - 23.

c. Conclure dans le cas général.

Nombres

5 - 25 Ⓢ ★ Polynômes de Lagrange

Pour n dans $\mathbf{N}$, et x dans $\mathbf{C}^{n+1}$ avec $x = (x_0, \ldots, x_n)$ où les x_k sont des nombres complexes distincts, on pose pour k dans $[\![0;n]\!]$,

$$L_{k,x} = \prod_{\substack{0\leq i\leq n\\ i\neq k}} \frac{X - x_i}{x_k - x_i} \ .$$

On note e_k l'application qui à P associe $P(x_k)$.

a. Montrer que $(L_{k,x})_{0\leq k\leq n}$ est une base de $\mathbf{C}_n[X]$. Que dire par rapport à $\mathbf{R}_n[X]$ et $\mathbf{Q}_n[X]$?

b. Montrer que e_k est une application linéaire sur $\mathbf{C}_n[X]$. Donner une base de son noyau.

c. Déduire de la question précédente que, pour tout P dans $\mathbf{C}_n[X]$ on a $P = \sum\limits_{k=0}^{n} e_k(P)L_{k,x}$.

d. Soit $\mathbf{K}$ un sous-corps de $\mathbf{C}$ et P dans $\mathbf{C}[X]$. Montrer $P(\mathbf{K}) \subset \mathbf{K} \iff P \in \mathbf{K}[X]$.

5 - 26 Ⓢ ★ Polynômes de Hilbert

Pour n dans $\mathbf{N}$, on pose

$$T_n = \binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!} \ .$$

Si P est un polynôme (à coefficients dans un anneau quelconque), on note $\Delta(P) = P(X+1) - P$.

a. Montrer que $(T_n)_{n\in\mathbf{N}}$ est une base de $\mathbf{Q}[X]$. Que dire par rapport à $\mathbf{R}[X]$ et $\mathbf{C}[X]$?

b. Montrer que Δ est une application linéaire sur $\mathbf{Q}[X]$. En préciser le noyau.

c. Montrer que pour tout n dans $\mathbf{N}^*$ on a $\Delta(T_n) = T_{n-1}$ et en déduire que Δ est surjective.

d. Déduire de la question précédente que, pour tout P dans $\mathbf{Q}[X]$ on a $P = \sum\limits_{k=0}^{+\infty} \Delta^n(P)(0)T_n$ où Δ^n est la composée de Δ n fois avec lui-même.

5 - 27 Ⓢ ★ Interpolation de Newton

a. Former le polynôme d'interpolation (méthode des différences de Newton correspondant à

x	0	1	2	3	4	5
$f(x)$	1	4	27	112	325	756

.

b. Donner les valeurs des approximations à l'ordre 1 et 5 de $f(3,2)$.

5 - 28 Ⓢ ★★ Correction d'erreur †

Trouver et corriger la faute de frappe dans la suite : 1, 3, 11, 31, 69, 113, 223, 351, 521, 739, 1011.

5 - 29 Ⓢ ★★ Calculs approchés de logarithmes

On note log le logarithme en base 10 et on fournit les approximations $\log(2) \simeq 0,3010$, $\log(3) \simeq 0,4771$ et $\log(11) \simeq 1,0414$.

a. Montrer que l'on peut, à partir de ces trois données, calculer $\log(n)$ avec une erreur inférieure à 0,001 pour tous les entiers n compris entre 1 et 20, sauf 7, 13, 14, 17 et 19.

b. Donner l'interpolation linéaire de log entre 1 et 1,1 obtenue par la méthode de Newton.

c. Montrer que l'approximation $\log\left(1 + x.10^{-3}\right) \simeq 4x.10^{-4}$ est valide à 0,001 près pour $0 \leq x < 10$.

d. Donner la formule d'interpolation de NEWTON pour le choix : $y(1) = 0,001$ et $y(1,1) = 0,041$. Justifier ce choix d'arrondis empiriquement. On admettra que cette formule permet de calculer $\log\left(1 + x.10^{-3}\right)$ à 0,001 près pour $10 \leq x < 100$.

e. Justifier le calcul suivant : $\log(63,37) \simeq 1+0,3010+0,4771+0,0234 \simeq 1,801$.

f. Donner une approximation de $\log(183,1)$ et de $\log(2783)$ par cette méthode.

5 - 30 Ⓢ ★★ Polynômes à valeurs entières

Soit P dans $\mathbf{C}_n[X]$. En utilisant l'exercice 5 - 26, montrer que les propriétés suivantes sont équivalentes :

1. $P(\mathbf{Z}) \subset \mathbf{Z}$;
2. P est une combinaison entière (relative) des polynômes de HILBERT ;
3. P prend des valeurs entières sur $[\![0; n]\!]$;
4. P prend des valeurs entières sur $n+1$ entiers consécutifs.

5 - 31 Ⓢ M 2019 ★★★ Polynômes surjectifs

Déterminer tous les polynômes P dans $\mathbf{C}[X]$ vérifiant

a. $P(\mathbf{C}) = \mathbf{C}$.

b. $P(\mathbf{R}) = \mathbf{R}$.

c. $P(\mathbf{U}) = \mathbf{U}$ où $\mathbf{U} = \{z \in \mathbf{C} \,|\, |z| = 1\}$.

d. $P(\mathbf{Q}) = \mathbf{Q}$.

Polynômes d'endomorphismes

5 - 32 Ⓢ X 1988 ★ Puissances d'une matrice

Soit M dans $\mathscr{M}_n(\mathbf{R})$, avec $M = \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & 2 \end{pmatrix}$.

Calculer M^k pour $k \in \mathbf{Z}$.

5 - 33 Ⓢ ★ Δ ♥

Soit u l'endomorphisme de $\mathbf{K}_n[X]$ défini par $u(P) = P(X+1)$. En déterminer le polynôme minimal. On pourra se ramener à l'opérateur Δ, où $\Delta = u - \mathrm{Id}$.

5 - 34 Ⓢ ★

Soit $A \in \mathscr{M}_n(\mathbf{R})$. Montrer que le polynôme minimal de A est le même qu'on la considère comme élément de $\mathscr{M}_n(\mathbf{R})$ ou de $\mathscr{M}_n(\mathbf{C})$.

5 - 35 Ⓢ ★★ Opérateurs différentiels

Soit E l'espace vectoriel $\mathbf{C}_n[X]$ des polynômes à coefficients complexes de degré inférieur ou égal à n. On désigne par Id l'identité de E et par d l'opérateur de dérivation.

a. Soit $\varphi = \mathrm{Id} - \lambda d$ avec $\lambda \in \mathbf{C}$. Montrer que φ est inversible et déterminer φ^{-1} à l'aide des puissances de d. On pourra commencer par remarquer $\mathrm{Id} = \mathrm{Id} - \lambda^{n+1} d^{n+1}$.

b. Soit $\lambda_1, \lambda_2, \ldots, \lambda_p$ des nombres complexes deux à deux distincts. On pose $\psi = \prod_{k=1}^{p} (\mathrm{Id} - \lambda_i d)$. Montrer que ψ est inversible et déterminer son inverse à l'aide des puissances de d. On pourra commencer par utiliser une décomposition en éléments simples.

Compléments

5 - 36 Ⓢ ★ Polynômes de BERNOULLI

On définit une suite de polynômes B_n par les conditions : $B_0 = 1$ et pour $n \geq 1$, $B_n' = nB_{n-1}$ et $\int_0^1 B_n(t)\,\mathrm{d}t = 0$. On note $b_n = B_n(0)$ (nombre de Jakob BERNOULLI).

a. Montrer que ces formules définissent effectivement une suite de polynômes, qu'ils sont unitaires avec $\deg(B_n) = n$ et qu'on a, pour $n \geq 2$, $B_n(0) = B_n(1)$.

b. Montrer, pour tout entier n, $B_n(1-X) = (-1)^n B_n$ et en déduire que b_n est nul si n est impair supérieur à 3. On pourra démontrer et utiliser l'unicité de la suite (B_n).

c. Montrer, pour tout entier n,

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

et en déduire que pour n impair $B_n(1/2) = 0$ et pour n pair $B_n(1/2) = (2^{1-n} - 1)b_n$.

5 - 37 Ⓢ ★ Équation symétrique

On cherche les racines du polynôme $X^4 + 5X^3 + 8X^2 + 5X + 1$.

a. Donner r et s tels qu'il se récrive $(X^2+rX+1)(X^2+sX+1)$ et conclure.

b. Poser $Y = X + \dfrac{1}{X}$ et conclure.

5 - 38 Ⓢ ★ Polynômes de BERNSTEIN

On note, pour $0 \leq k \leq n$, $B_{n,k} = \binom{n}{k} X^k (1-X)^{n-k}$. Soit P un polynôme dans $\mathbf{R}[X]$. On note $B_n(P)$ le polynôme $\sum_{k=0}^{n} P\left(\frac{k}{n}\right) B_{n,k}$.

a. Montrer $B_n(1) = 1$ et en déduire que les $B_{n,k}$ définissent des fonctions polynomiales de $[\,0; 1\,]$ dans lui-même.

b. Soit, pour x dans $[\,0; 1\,]$, la fonction g sur $[\,0; 1\,]$ donnée par $g(t) = \sum_{k=0}^{n} \binom{n}{k} t^k (1-x)^{n-k}$. Montrer $g'(x) = n$ et en déduire, pour $n > 0$, $B_n(X) = X$.

c. En considérant $g''(x)$, montrer, pour $n > 0$, $B_n(X^2) = X^2 + \dfrac{X(1-X)}{n}$.

5 - 39 Ⓢ ★★ **Théorème de Weierstrass**

On reprend les notations de l'exercice 5 - 38. Soit f une fonction continue sur $[0;1]$. On note P_n le polynôme $\displaystyle\sum_{k=0}^{n} f\left(\frac{k}{n}\right) B_{n,k}$. Soit ε dans $\mathbf{R}_+^*$. On lui associe, par théorème de Heine et donc par uniforme continuité de f sur $[0;1]$, un réel strictement positif η tel que

$$\forall (u,v) \in [0;1]^2 \quad |u-v| < \eta \Longrightarrow |f(u) - f(v)| < \varepsilon \ .$$

Par théorème de Weierstrass dit des bornes (atteintes), on dispose de $M = \max_{[0;1]} |f|$ et on choisit n non nul supérieur à $\dfrac{2M}{\varepsilon\eta^2}$. Soit alors x dans $[0;1]$.

a. On pose $P_x = B_n((X-x)^2)$. En utilisant l'exercice 5 - 38 montrer $P_x = (X-x)^2 + \dfrac{X(1-X)}{n}$ et en déduire $|P_x(x)| \leq \dfrac{1}{4n}$.

b. Montrer $P_n - f(x) = B_n(f - f(x))$ et, en évaluant ce polynôme en x, en déduire en coupant la somme en deux et en utilisant l'exercice 5 - 38

$$|P_n(x) - f(x)| \leq \varepsilon + 2M \sum_{\substack{0\leq k\leq n \\ |\frac{k}{n}-x|\geq\eta}} B_{n,k}(x) \ .$$

c. En déduire $|P_n(x) - f(x)| \leq \varepsilon + 2M \dfrac{1}{\eta^2} |P_x(x)|$ et conclure $\sup_{[0;1]} |P_n - f| \leq 2\varepsilon$.

5 - 40 Ⓢ ★★ **Moments ♥♥**

Soit f continue de $[a;b]$ dans $\mathbf{R}$ et, pour n dans $\mathbf{N}$, $I_n = \displaystyle\int_a^b f(t)t^n \,\mathrm{d}t$. Montrer, en utilisant le théorème de Weierstrass (i.e. l'exercice 5 - 39) que si tous les I_n sont nuls, alors f est nulle.

5 - 41 Ⓢ ★★ **Polynômes de Hermite**

En liaison avec la loi Gaussienne, Charles Hermite a introduit une famille (H_n) vérifiant : $\forall n \in \mathbf{N}$, $\forall x \in \mathbf{R}$

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}(e^{-x^2/2}) = (-1)^n H_n(x) e^{-x^2/2} \ .$$

a. Montrer que l'on définit ainsi une (unique) famille de polynômes unitaires de degrés donnés par $\deg(H_n) = n$.

b. Montrer, pour tout entier n, $H_{n+1} = XH_n - nH_{n-1}$.

c. En déduire, pour tout entier n, $H'_{n+1} = (n+1)H_n$ et $H''_n - XH'_n + nH_n = 0$.

5 - 42 Ⓢ ★★ **Résolution de l'équation de degré 3**

On souhaite résoudre l'équation $x^3 + 6x = 20$. Selon les consignes laissées à Girolamo Cardano par Nicolo Tartaglia, on représente x^3 comme un cube de coté x, $6x$ comme le volume de six prismes carrés (parallélépipèdes rectangles à bases carrées) : trois de volume x^2v et trois autres de volume xv^2. Enfin 20 est la différence de deux cubes de côtés respectifs u et v. Plus algébriquement ...

a. Poser $x = u - v$. Quelle relation doivent satisfaire u et v pour que l'équation $x^3 + 6x = 20$ se simplifie en $u^3 - v^3 = 20$?

b. Trouver tous les réels a et b vérifiant $a + b = 20$ et $-ab = 8$.

c. En déduire u^3, $-v^3$ puis x.

d. Peut-on adapter cette méthode à toute équation de degré 3 ?

5 - 43 ★★★ **Racines réelles d'un polynôme cubique**

Soit a, b, c les racines (éventuellement confondues) du polynôme $X^3 + pX + q$. Montrer que $(b-a)^2$, $(c-b)^2$ et $(a-c)^2$ sont les racines (éventuellement confondues) du polynôme $X^3 + 6pX^2 + 9p^2X + 4p^3 + 27q^2$.

En déduire le nombre de racines réelles de $X^3 - 3X + r$ lorsque r est un réel positif, et préciser leurs signes.

5 - 44 ★★★ **Résolution de l'équation de degré 4**

a. Méthode de Ludovico Ferrari. On étudie $X^4 + 2aX^2 = bX + c$. Montrer que l'ensemble des y tels que l'équation se ramène à $(X^2 + a + y)^2 = (\alpha X + \beta)^2$, pour certains α et β, forment les solutions d'une équation de degré 3. En déduire une méthode pour résoudre les équations de degré 4.

b. Méthode de Leonhard Euler. On étudie $X^4 + aX^2 + bX + c$. Montrer que l'ensemble des u tels que l'équation se ramène à $(X^2 + uX + \alpha)(X^2 - uX + \beta)$, pour certains α et β, forment les solutions d'une équation de degré 3. En déduire une méthode pour résoudre les équations de degré 4.