Ag3 : Polynômes

I Structure de K[X]

I.1 Résumé

Voir chapitre Al1 : $(\mathbf{K}[X], +, ., \times)$ est une **K**-algèbre commutative intègre.

I.2 L'espace vectoriel $\mathbf{K}[X]$

L'espace vectoriel $\mathbf{K}[X]$ est un espace vectoriel simple qui n'est pas de dimension finie, on l'utilise par exemple pour montrer que l'équivalence entre surjectivité, injectivité et bijectivité est fausse pour un endomorphisme en dimension quelconque. Mais $\mathbf{K}[X]$ est réunion croissante des espaces vectoriels

$$\mathbf{K}_m[X] = \{P \ ; \ \deg(P) \leq m\}$$

qui eux sont de dimension finie ($\dim(\mathbf{K}_m[X]) = m+1$). Cette particularité fait que certains résultats de dimension finie sont utilisables dans $\mathbf{K}[X]$ qui pourtant n'est pas de dimension finie.

II Division euclidienne

II.1 Divisibilité, polynômes associés

Un polynôme A divise un polynôme B si et seulement s'il existe Q tel que
$B = AQ$.
On dit aussi que B est multiple de A.
Deux polynômes qui se divisent mutuellement (A divise B et B divise A) sont « associés », c'est-à-dire égaux à un coefficient multiplicatif près : il existe un scalaire (c'est-à-dire, un élément de **K**) non nul λ tel que $A = \lambda B$ (ou encore $B = (1/\lambda)A$). En résumé,

$$\Big[\ A|B \quad \text{et} \quad B|A \ \Big] \iff \Big[\ \exists \lambda \in \mathbf{K} \setminus \{0\} \quad A = \lambda B \ \Big]$$

II.2 Division euclidienne

Proposition : Etant donnés deux polynômes A et B, B non nul, il existe un unique couple Q, R de polynômes vérifiant

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

Démonstration : On fixe B, on fait une récurrence (à hypothèse forte) sur le degré de A.

Remarque : Quelques exercice posés parfois à l'oral demandent de déterminer le reste dans une division euclidienne. En général, si on ne demande pas le quotient, inutile de le chercher.

Exercice : Déterminer le reste de la division de X^n par $(X-1)(X-2)(X-3)$. Déterminer le reste de la division de X^n par $(X-1)^2(X-2)$.

Utilisation : On trouve ce problème de reste de la division de X^n par un polynôme dans certains exercices d'oral sur l'exponentielle de matrice, par exemple : déterminer $\exp(A)$, où A est une matrice telle que $A^2 - A = 6I_n$.

Signalons enfin ce genre d'exercice :

Exercice : Déterminer le reste de la division de $X^n - nX + 1$ par $(X-1)^3$.
Une idée : appliquer la formule de Taylor.

III Fonction polynôme, zéros d'un polynôme

III.1 Fonction polynôme associée

La fonction polynôme associée au polynôme $P = \sum_{k=0}^{+\infty} a_k X^k$ est l'application

$$\begin{array}{rccc} \tilde{P}: & \mathbf{K} & \longrightarrow & \mathbf{K} \\ & x & \longmapsto & \sum_{k=0}^{+\infty} a_k x^k \end{array}$$

(Rappelons qu'il n'est surtout pas question de séries ici : les sommes écrites sont finies).
On appelle équation algébrique une équation du type $f(x) = 0$ où f est une fonction polynômiale.

III.2 Méthode de Horner

A connaître…

III.3 Zéros d'un polynôme ; multiplicité

Définition Les zéros (on dit aussi racines) du polynôme P sont les solutions (éventuelles) de l'équation algébrique $\tilde{P}(x) = 0$.

Le reste de la division de P par $X - a$ ($a \in \mathbf{K}$) étant ,
on obtient une caractérisation des zéros à l'aide de la divisibilité :

Proposition : a est un zéro de P si et seulement si $X - a$ divise P.

Définition : On dit que la racine a de P est de multiplicité m losque $(X-a)^m$ divise P et $(X-a)^{m+1}$ ne divise pas P. Une racine simple est une racine d'ordre 1, une racine double est une racine d'ordre 2, etc...

Il est commode, et on le fera parfois, de s'autoriser à dire que a est racine de multiplicité 0 de P pour signifier que a n'est pas racine de P ($\widetilde{P}(a) \neq 0$). D'ailleurs, cela équivaut bien à dire que $(X-a)^0$ divise P et $(X-a)^1$ ne divise pas P.

IV Idéaux

IV.1 Idéaux d'un anneau commutatif

a. Définition :

Soit $(A, +, \times)$ un anneau commutatif. On appelle idéal de A toute partie I de A vérifiant :

1. I est un sous-groupe de $(A, +)$
2. $\forall a \in A \quad \forall x \in I \quad a \times x \in I$

On dit parfois qu'un idéal est un sous-groupe pour + absorbant pour $\times$.

Pour un anneau non commutatif, la notion d'idéal se décline en trois versions : idéal à gauche, idéal à droite, idéal bilatère. Nous ne nous en occupons pas, ce n'est pas au programme.

b. Caractérisation pratique :

Une partie I d'un anneau commutatif $(A, +, \times)$ est un idéal de A si et seulement si

1. $I \neq \emptyset$
2. $\forall (x, y) \in I^2 \quad x - y \in I$
3. $\forall a \in A \quad \forall x \in I \quad a \times x \in I$

c. Idéal des multiples d'un élément

Si x et y sont deux éléments de l'anneau commutatif $(A,+,\times)$, on dit que x divise y, et on note $x|y$, lorsqu'il existe $z \in A$ tel que $y = x \times z$. On dit que y est un multiple de x.

Proposition-Définition Soit $(A,+,\times)$ un anneau commutatif. Si $x \in A$, considérons l'ensemble des multiples de x : c'est $A \times x = \{z \times x \ ; \ z \in A\}$. C'est un idéal de l'anneau A. On le note souvent (a). Autrement dit,

$$A \times x = x \times A = (a)$$

d. Divisibilité et inclusion d'idéaux

On remarque que

$$x|y \iff y \in Ax \iff Ay \subset Ax$$

IV.2 Idéaux de K[X]

Théorème

Si I un idéal de $\mathbf{K}[X]$, il existe un unique polynôme nul ou unitaire P tel que

$$I = P\mathbf{K}[X] = (P)$$

Théorème très utile. La démonstration est intéressante (on en retrouve le mécanisme à d'autres endroits, et on peut avoir à l'écrire pour un exercice ou un problème). L'idée est d'utiliser la division euclidienne.

Eléments associés : Lorsque deux éléments d'un anneau se divisent mutuellement, ils sont dits associés. Deux éléments a et b sont donc associés si et seulement si $(a) = (b)$ (i.e. les multiples de l'un sont les multiples de l'autre). Dans $\mathbf{K}[X]$, deux

polynômes A et B sont associés (i.e. $(A) = (B)$) si et seulement si
Et donc, si $I = (P)$, les polynômes Q tels que $I = (Q)$ sont les $Q = \lambda P$ avec $\lambda \neq 0$.

V PGCD, PPCM

V.1 Définition du pgcd par les idéaux

Proposition - Définition On considère A, B deux éléments de $\mathbf{K}[X]$, $(A,B) \neq (0,0)$. Alors

$$I = \{AU + BV \ ; \ (U,V) \in (\mathbf{K}[X])^2\}$$

est un idéal non nul (i.e. différent de (0)) de $(\mathbf{K}[X],+,\times)$. Il existe un unique D unitaire tel que $I=(D)$; D est appelé PGCD (plus grand commun diviseur) de A et B, et parfois noté $A\wedge B$ (même si la seule notation au programme est $\text{pgcd}(A,B)$).

Autrement dit,
le pgcd de A et de B est l'unique polynôme unitaire D tel que

$$\{AU+BV\ ;\ (U,V)\in\mathbf{K}[X]^2\}\ =\ \{DW\ ;\ W\in\mathbf{K}[X]\}$$

V.2 Equivalence avec la définition habituelle

Définissons $A\wedge B$ comme ci-dessus. Alors les diviseurs communs à A et B sont les diviseurs de $A\wedge B$. Autrement dit :

$$\Big[\ D|A\quad\text{et}\quad D|B\ \Big]\iff\Big[\ D\mid A\wedge B\ \Big]$$

$A\wedge B$ est donc le polynôme unitaire de plus grand degré qui divise à la fois A et B (définition du programme de mpsi).

V.3 Détermination pratique (algorithme d'Euclide)

a. Evocation de l'algorithme

Si $B=0$, c'est fini (avant d'avoir commencé) : le pgcd est A (supposé non nul, car $\text{pgcd}(0,0)$ n'est pas défini).
Si $B\neq 0$, on remarque que

$$A\wedge B\ =\ B\wedge(A-BQ)$$

pour tout polynôme Q. C'est d'ailleurs, quoique facile, très intéressant à montrer car on utilise une technique importante : la « double divisibilité ». Interprétée en termes d'idéaux, ce n'est d'ailleurs rien d'autre que la double inclusion.
On en déduit que, si R_1 est le reste de la division de A par B, $A\wedge B=B\wedge R_1$. On peut alors continuer, et dire que $A\wedge B=R_1\wedge R_2$, R_2 étant le reste de la division de B par R_1. C'est le point de départ de l'algorithme d'Euclide, ou algorithme des divisions successives. Le pgcd est le dernier reste non nul obtenu dans l'algorithme.

V.4 Polynômes premiers entre eux, théorème de Bezout

a. Polynômes premiers entre eux

On dit que A et B sont premiers entre eux lorsque $A\wedge B=1$. Cela signifie que les seuls diviseurs communs à A et B sont les polynômes constants.

b. Théorème de Bézout

Théorème de Bézout A et B sont premiers entre eux si et seulement si il existe des polynômes U et V tels que $AU+BV=1$.

c. Une évidence

Si $A \wedge B = 1$, si $A_1|A$ et $B_1|B$, alors $A_1|B_1 = 1$.
Cela se montre en utilisant la définition du pgcd ou le théorème de Bezout. C'est un résultat rarement énoncé car considéré comme évident, mais qui sert.

d. Obtention de coefficients de Bézout par l'algorithme d'Euclide

L'algorithme d'Euclide permet non seulement d'obtenir le pgcd de deux éléments A et B, mais aussi de déterminer U, V tels que

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

V.5 Une caractérisation utile du pgcd

Proposition : Soit $(A, B) \neq (0, 0)$, et D unitaire, alors D est le PGCD de A et B si et seulement si les deux conditions suivantes sont réalisées :

(i) D divise A et B

(ii) les quotients de A et B par D sont premiers entre eux.

Autrement dit, D est le PGCD de A et B si et seulement s'il existe A_1 et B_1 tels que

$$A = DA_1 \quad , \quad B = DB_1 \quad , \quad A_1 \wedge B_1 = 1$$

Ce résultat s'utilise souvent de la manière suivante : on veut appliquer le théorème de Bezout ou le théorème de Gauss, pour cela on a besoin de l'hypothèse $A \wedge B = 1$, or ce n'est pas le cas. Qu'à cela ne tienne : on divise A et B par leur pgcd, les quotients A_1 et B_1 sont premiers entre eux, et c'est à eux qu'on applique Bezout ou Gauss.

V.6 Théorème (ou lemme...) de Gauss

a. Le lemme de Gauss

Théorème : Soit A, B, C trois polynômes ; si A divise BC et est premier avec B, alors A divise C. Ou :

$$(A|BC \quad \text{et} \quad A \wedge B = 1) \Longrightarrow (A|C)$$

Démonstration : On utilise le théorème de Bezout : il existe U et V tels que

$$UA + VB = 1$$

On multiplie tout par C...

Corollaire 1 : Si $A|C$ et $B|C$ et $A \wedge B = 1$, alors $AB|C$.

Corollaire 2 : $(A \wedge BC = 1) \iff (A \wedge B = A \wedge C = 1)$.

Corollaire 2 bis : $\big(A \wedge B_1 \dots B_p = 1\big) \iff \big(A \wedge B_1 = A \wedge B_2 = \dots = A \wedge B_p = 1\big)$.

Corollaire 2 ter : Si $A \wedge B = 1$, si $(m,n) \in \mathbf{N}^2$, alors $A^m \wedge B^n = 1$.

Corollaire 3 : Si $A \wedge B = 1$, alors $A \wedge BC = A \wedge C$.

Corollaire 4 : Si $A_1, \dots, A_p$ sont deux à deux premiers entre eux, alors
$\Big[A_1 \dots A_p \mid C \Big] \iff \Big[\forall i \in [\![1,p]\!] \quad A_i \mid C \Big]$

La démonstration de ces corollaires en utilisant le théorème de Bézout et le théorème de Gauss est un bon entraînement à l'arithmétique. Il n'est pas nécessaire de les connaître par cœur. La décomposition en facteurs irréductibles (voir plus loin) est un bon moyen de les voir un peu moins astucieusement.

V.7 Nombre de zéros (ou racines) d'un polynôme

a. Majoration du nombre de racines d'un polynôme

Proposition Soit P un polynôme de $\mathbf{K}[X]$, et $\alpha_1, \dots, \alpha_r$ des éléments de $\mathbf{K}$, supposés deux à deux distincts. Alors $\alpha_1, \dots, \alpha_r$ sont racines de P de multiplicités respectives au moins $m_1, \dots, m_r$ si et seulement si le polynôme $\prod_{i=1}^{m} (X - \alpha_i)^{m_i}$ divise P.

Démonstration Où intervient le théorème de Gauss ?

Corollaire Le nombre de racines d'un polynôme non nul, comptées autant de fois que leur multiplicité, est au plus égal à son degré.

Reformulation Soit P un polynôme non nul. Si les racines de P sont $\alpha_1, \dots, \alpha_r$ (supposés distincts) de multiplicités respectives $m_1, \dots, m_r$, alors

$$m_1 + \cdots + m_r \leq \deg(P)$$

Théorème (D'Alembert-Gauss) Lorsque $\mathbf{K} = \mathbf{C}$, l'inégalité précédente est une égalité.

b. Conséquences

La fait qu'un polynôme non nul ait un nombre de racines au plus égal à son degré (en comptant les racines autant de fois que leur multiplicité) a des conséquences importantes, et on utilise fréquemment les résultats suivants :

Proposition : Si deux polynômes de degré au plus n coïncident (ou plutôt si leurs fonctions polynomiales associées coïncident) en au moins $n+1$ points, ils sont égaux.

Autrement dit, si P et Q sont dans $\mathbf{K}_n[X]$ et s'il existe $a_1, \dots, a_n$ deux à deux distincts dans $\mathbf{K}$ tels que

$$\forall i \in [\![1,n]\!] \qquad \widetilde{P}(a_i) = \widetilde{Q}(a_i)$$

alors $P = Q$.

Proposition bis : Quand deux polynômes coïncident en un nombre infini de points, ils sont égaux.

Corollaire : Lorsque le corps **K** est infini, deux polynômes ayant la même fonction polynôme associée sont égaux.

Considérons l'application

$$\begin{array}{rccc} u : & \mathbf{K}[X] & \longrightarrow & \mathscr{A}(\mathbf{K},\mathbf{K}) \\ & P & \longmapsto & \widetilde{P} \end{array}$$

(on note $\mathscr{A}(\mathbf{K},\mathbf{K})$ l'espace vectoriel des applications de **K** dans **K**). Le corollaire dit que u est injective lorsque **K** est infini. Mais d'autre part, on a

$\forall (P,Q) \in (\mathbf{K}[X])^2 \ \forall (\lambda,\mu) \in \mathbf{K}^2 \qquad u(\lambda P + \mu Q) = \lambda u(P) + \mu u(Q)$

[ce qui signifie simplement que, si P et Q sont des polynômes et λ et μ des scalaires,

$\widetilde{\lambda P + \mu Q} = \lambda \widetilde{P} + \mu \widetilde{Q}$

ce qui se vérifie sans difficulté. Faisons-le :

Si $P = \sum_{k=0}^{+\infty} a_k X^k$ et $Q = \sum_{k=0}^{+\infty} b_k X^k$,

$$\begin{aligned} \forall x \in \mathbf{K} \qquad \widetilde{\lambda P + \mu Q}(x) &= \sum_{k=0}^{+\infty} (\lambda a_k + \mu b_k) x^k \\ &= \lambda \sum_{k=0}^{+\infty} a_k x^k \ + \ \mu \sum_{k=0}^{+\infty} b_k x^k \\ &= \lambda \widetilde{P}(x) + \mu \widetilde{Q}(x) \end{aligned}$$

Donc u est linéaire et injective. C'est donc un isomorphisme de $\mathbf{K}[X]$ sur $u(\mathbf{K}[X])$, ce qui explique qu'il y ait peu d'inconvénient à confondre poynôme et fonction polynôme dans le cas d'un corps infini. Ce n'est pas du tout la même chose sur les corps finis (on verra plus tard des corps finis très simples).

Remarquons qu'on a aussi

$\forall (P,Q) \in (\mathbf{K}[X])^2 \ \forall (\lambda,\mu) \in \mathbf{K}^2 \qquad u(P \times Q) = u(P) \times u(Q)$

(même genre de démonstration que pour la linéarité) et

$u(1) = \widetilde{1}$

ce qui fait de u un isomorphisme d'algèbres (on verra plus tard ce que cela signifie précisément).

Finissons par un résultat moins utile, mais de la même famille :

Proposition ter : Si deux polynômes non nuls de degré $\leq n$ ont n zéros communs, ils sont

V.8 Equations $AU + BV = C$ (h.p. mais classique)

L'étude de ces équations est assez classique, et permet de manipuler les pgcd et le théorème de Gauss

Soit $(A,B) \in \mathbf{K}[X]^2 \setminus \{(0,0)\}$, $D = A \wedge B$, $C \in \mathbf{K}[X]$. On considère l'équation

$$AU + BV = C \qquad (E)$$

1. Donner une condition nécessaire et sufffisante (portant sur C et D) pour que cette équation ait au moins une solution.
2. On suppose $A \wedge B = 1$. Soit (U_0, V_0) une solution de (E). Décrire l'ensemble des solutions de (E).
3. On suppose que $D|C$. Comment ramener simplement l'étude de (E) au cas précédent?

V.9 PPCM

Les idéaux sont plus naturels lorsqu'on définit le ppcm que lorsqu'on définit le pgcd. Mais le ppcm est une notion beaucoup moins importante que le pgcd.

Définition : Supposons A **et** B non nuls; $I = (A) \cap (B)$ est un idéal non nul. Il existe donc un unique M unitaire tel que

$$(A) \cap (B) = (M)$$

On appelle M le PPCM de A et B. On peut le noter $A \vee B$.

Proposition Supposons A et B non nuls : soit D leur PGCD, M leur PPCM. Alors AB et MD sont associés (i.e. égaux à un coefficient multiplicatif non nul près).

V.10 PGCD de plus de deux éléments

a. Définition

Définition Soit $(A_1, \ldots, A_p) \in (\mathbf{K}[X] \setminus \{0\})^p$. Considérons

$$I = \{U_1 A_1 + U_2 A_2 + \cdots + U_p A_p \ ; \ (U_1, \ldots, U_p) \in (\mathbf{K}[X])^p\}$$

Alors I est un idéal non nul (non $\{0\}$) de A. Il existe donc un unique D unitaire tel que $I = (D)$; on appelle D le PGCD de $(A_1, \ldots, A_p)$.

Remarque I est le plus petit idéal contenant les A_i ; on dit parfois que c'est l'idéal engendré par $(A_1, \ldots, A_p)$.

b. Caractérisation

Proposition

$$\Big(\forall i \in \{1, \ldots, p\} \quad D|A_i\Big) \Leftrightarrow \Big(D|\operatorname{pgcd}(A_1, \ldots, A_p)\Big)$$

Ou encore : les diviseurs communs à tous les A_i sont les diviseurs de leur pgcd. Ce qui est assez cohérent avec l'appellation pgcd.

c. Associativité du pgcd

Proposition

$$\text{pgcd}(A_1,\dots,A_{p+1}) = \text{pgcd}\big(\text{pgcd}(A_1,\dots,A_p),A_{p+1}\big)$$

($A_1,\dots A_p$ n'étant pas tous nuls)

Extension Plus généralement, avec des hypothèses évidentes :

$$\text{pgcd}(A_1,\dots,A_p,B_1,\dots,B_q) = \text{pgcd}\big(\text{pgcd}(A_1,\dots,A_p),\text{pgcd}(B_1,\dots,B_q)\big)$$

Intérêt Ceci permet de calculer un pgcd de p éléments en se ramenant à des calculs successifs de pgcd de deux éléments.

d. Polynômes premiers entre eux (dans leur ensemble)

Définition On dit que $A_1,\dots,A_p$ sont premiers entre eux (dans leur ensemble) lorsque leur PGCD est égal à 1.

Théorème de Bezout $A_1,\dots,A_p$ sont premiers entre eux dans leur ensemble si et seulement s'il existe $U_1,\dots,U_p$ dans A tels que

$$U_1A_1 + U_2A_2 + \cdots + U_pA_p = 1$$

Remarque Il ne faut pas confondre « premiers entre eux » (dans leur ensemble) et « premiers entre eux deux à deux ».
L'exemple du pgcd de $((X-2)(X-3)$; $(X-2)(X-5)$; $(X-3)(X-5))$ peut être instructif.

VI Polynômes irréductibles

VI.1 Définition

Définition On dit qu'un polynôme P non constant est irréductible lorsque ses seuls diviseurs sont les polynômes constants et les polynômes λP avec $\lambda \in \mathbf{K}\setminus\{0\}$).

Caractérisation P est irréductible si et seulement s'il n'existe pas de factorisation $P = AB$ avec $0 < \deg(A) < \deg(P)$.

Analogie Les polynômes irréductibles sont aux polynômes ce que les nombres premiers sont aux entiers. De même que l'on ne considère pas 1 comme premier, on ne considère pas un polynôme constant comme irréductible.

VI.2 Exemples

On sait que la répartition des nombres premiers est un problème arithmétique fascinant. La recherche des polynômes irréductibles dans $\mathbf{K}[X]$ dépend beaucoup de **K**. Deux cas (deux **K**, donc...) sont au programme :

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

Proposition Dans $\mathbf{R}[X]$, les polynômes irréductibles sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant < 0

La deuxième proposition se déduit assez simplement de la première. La première est une des formulations du célèbre théorème de D'Alembert-Gauss, elle équivaut à dire que tout polynôme non constant de $\mathbf{C}[X]$ a au moins une racine comples.
Dans $\mathbf{Q}[X]$, les choses sont beaucoup plus compliquées...et totalement hors-programme.

Attention aux fausses idées : ne pas avoir de racine ne signifie pas être irréductible. Par exemple, dans $\mathbf{R}[X]$, X^4+1 n'est pas irréductible. Pourtant, il n'a pas de racine réelle.

VI.3 Décomposition en facteurs irréductibles

Théorème Tout polynôme P non constant se décompose de manière unique (à l'ordre des facteurs près sous la forme : $P = a\prod_{i=1}^{n} P_i^{\alpha_i}$ où les P_i sont irréductibles unitaires, les α_i des entiers naturels non nuls, a le coefficient dominant de P.

C'est l'analogue du théorème de décomposition en facteurs premiers dans **Z**.

Sur C :

Proposition Soit $P \in \mathbf{C}[X]$ non constant. Il existe $a_1,\dots,a_p$ nombres complexes deux à deux distincts, $m_1,\dots,m_p$ entiers naturels non nuls, tels que

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

où k est le coefficient directeur de P.

Proposition Soit $P \in \mathbf{C}[X]$ non constant, définissons $d = \deg(P)$. Il existe alors des nombres complexes $a_1,\dots,a_d$ tels que

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

où k est le coefficient directeur de P.

(bien voir la différence des deux formulations, c'est évidemment la même proposition mais écrite de deux manières, qu'on utilisera l'une et l'autre).

Sur R :

Proposition Soit $P \in \mathbf{R}[X]$ non constant. P peut se décomposer sous la forme

$$P = k\left(\prod_{i=1}^{p}(X-a_i)^{m_i}\right)\left(\prod_{i=1}^{q}(X^2+b_iX+c_i)^{n_i}\right)$$

où k est le coefficient directeur de P et, pour tout i, $b_i^2 - 4c_i < 0$.

Le cas réel est (beaucoup) moins souvent utilisé que le cas complexe.

VI.4 Deux résultats utiles

Proposition Si P est irréductible unitaire, si Q est un polynôme quelconque, alors $P \wedge Q = 1$ ou $P|Q$ (un polynôme irréductible est premier avec un polynôme, ou alors il le divise).

Proposition Un polynôme irréductible P divise un produit de polynômes $Q_1 \dots Q_m$ si et seulement si il divise l'un des facteurs Q_i.

VI.5 Utilisation pour le calcul du pgcd et du ppcm

Soit P, Q deux entiers non nuls. On écrit

$$P = \alpha\prod_{i=1}^{d}P_i^{m_i} \qquad Q = \beta\prod_{i=1}^{d}P_i^{n_i}$$

où les P_i sont des polynômes irréductibles unitaires deux à deux distincts, les n_i et les m_i des entiers naturels (qui peuvent être nuls, pour avoir la même liste de polynômes dans les deux membres). Alors

$$\text{pgcd}(P,Q) = \prod_{i=1}^{d}P_i^{\min(m_i,n_i)} \qquad \text{ppcm}(P,Q) = \prod_{i=1}^{d}P_i^{\max(m_i,n_i)}$$

On a de plus

$$P \wedge Q = 1 \iff$$

VI.6 Retour sur le théorème de Gauss

Rappelons le théorème de Gauss :

$$(A|BC \quad \text{et} \quad A \wedge B = 1) \Longrightarrow (A|C)$$

Décomposons les trois polynômes A, B, C en facteurs irréductibles :

$$A = \prod_{i=1}^{m}P_i^{\alpha_i} \quad , \quad B = \prod_{i=1}^{m}P_i^{\beta_i} \quad , \quad C = \prod_{i=1}^{m}P_i^{\gamma_i}$$

Ce faisant, on suppose A, B, C unitaires : aucune importance, les relations de divisibilté entre polynômes ne changent pas si on multiplie ces polynômes par des constantes non nulles. Les trois produits sont indexés de la même manière : aucun problème, cela signifie que $\{P_1, \dots, P_m\}$ contient tous les polynômes qui interviennent dans au moins une des trois décompositions. Et, bien sûr, on autorise les exposants nuls. Par exemple, si

$$A = (X-1)(X-2) \quad , \quad B = (X-2)(X-3) \quad , \quad C = (X-3)(X-4)$$

on réécrit ces décompositions sous la forme

$$A = (X-1)^1 (X-2)^1 (X-3)^0 \dots$$

Si on préfère, on peut aussi écrire

$$A = \prod_{i \in I} P_i^{\alpha_i} \quad , \quad B = \prod_{i \in I} P_i^{\beta_i} \quad , \quad C = \prod_{i \in I} P_i^{\gamma_i}$$

où I est un ensemble fini « convenable ».

1. Traduire les hypothèses du théorème de Gauss ($A|BC$ et $A \wedge B = 1$) en conditions sur les α_i, β_i, γ_i.
2. En déduire que $A|C$.

Le théorème de Gauss peut donc être vu à l'aide de la décomposition en polynômes irréductibles.

VII Polynômes de polynômes

Définition Soit $P = \sum_{k=0}^{d} p_k X^k \in \mathbf{K}[X]$; si $Q \in \mathbf{K}[X]$, on définit naturellement :

$$P(Q) = \sum_{k=0}^{d} p_k Q^k$$

On a : $P(Q) \in \mathbf{K}[X]$.

VIII Polynôme dérivé ; formules de Leibniz et Taylor

VIII.1 Polynôme dérivé

a. Définition

Si $P = \sum_{n=0}^{+\infty} a_n X^n$, on définit

$$D(P) = \sum_{n=1}^{+\infty} n a_n X^{n-1} = \sum_{n=0}^{+\infty} (n+1) a_{n+1} X^n$$

On utilise plus souvent la notation P' que $D(P)$. Rappelons donc qu'il est fort déconseillé de dire « on considère deux polynômes P et P' »…

b. L'endomorphisme dérivation

La dérivation est un endomorphisme de $\mathbf{K}[X]$ très utilisé dans les exemples et contre-exemples concernant les endomorphismes en dimension infinie.
Par exemple,

$$P \longrightarrow P'$$

est un endomorphisme de $\mathbf{K}[X]$ surjectif et non injectif, ce qui ne peut pas arriver pour un endomorphisme en dimension finie.

VIII.2 Formule de Leibniz

Proposition $\forall (P,Q) \in \mathbf{K}[X]^2 \qquad \mathrm{D}(PQ) = P\,\mathrm{D}(Q) + Q\,\mathrm{D}(P)$

ou encore $(PQ)' = PQ' + QP'$

Proposition (formule de Leibniz) On a, pour tous polynômes P et Q, pour tout $n \in \mathbf{N}$,

$$\mathrm{D}^n(PQ) = \sum_{k=0}^{n} \binom{n}{k} \mathrm{D}^k(P)\,\mathrm{D}^{n-k}(Q)$$

ou encore : $(PQ)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} P^{(k)} Q^{(n-k)}$

VIII.3 Formule de Taylor

a. La formule

Proposition Si **K** est un sous-corps de **C**, si $P \in \mathbf{K}[X]$, alors

$$P(X) = \sum_{n=0}^{+\infty} \frac{\widetilde{\mathrm{D}^n P}(a)}{n!}(X-a)^n = \sum_{n=0}^{+\infty} \frac{\widetilde{P^{(n)}}(a)}{n!}(X-a)^n$$

que l'on peut aussi écrire :

$$P(X+a) = \sum_{n=0}^{+\infty} \frac{\widetilde{\mathrm{D}^n P}(a)}{n!} X^n$$

Démonstration Il faut savoir calculer, si m et n sont deux entiers naturels,

$$(X^n)^{(m)} =$$

ou, aussi bien,

$$\left((X-a)^n\right)^{(m)} =$$

Définissons alors

$$\phi \,:\, P \longmapsto \sum_{n=0}^{+\infty} \frac{\widetilde{P^{(n)}}(a)}{n!}(X-a)^n$$

L'application ϕ est linéaire, et coïncide avec l'identité sur la base $\left((X-a)^n\right)_{n\in\mathbf{N}}$ de $\mathbf{K}[X]$. Donc $\phi = \mathrm{Id}_{\mathbf{K}[X]}$ et on conclut.

b. Une caractérisation de la multiplicité d'une racine

Proposition $a \in \mathbf{K}$ est racine de multiplicité m du polynôme P si et seulement si

$$\widetilde{P}(a) = \widetilde{P}'(a) = \ldots = \widetilde{P^{(m-1)}}(a) = 0 \quad \text{et} \quad \widetilde{P^{(m)}}(a) \neq 0$$

Démonstration On remarque que la formule de Taylor donne le reste de la division de P par $(X-a)^m$: c'est

Donc $(X-a)^m$ divise P si et seulement si

ce qui permet de conclure.

Exemple : Soit $n \geq 2$. Montrer que toutes les racines complexes du polynôme $X^n - nX^{n-1} - 1$ sont simples.

IX Polynômes scindés, relations entre coefficients et racines

Ces relations sont très importantes. La formule générale est souvent jugée effrayante alors qu'elle est parfaitement sympathique. Seules les relations avec la somme des racines (formule de Viète) et le produit sont exigibles. Les autres sont à savoir retrouver.

IX.1 Polynômes scindés

On considère un polynôme P non constant.

Définition : On dit que le polynôme P est scindé lorsque tous les polynômes irréductibles qui figurent dans sa décomposition sont de degré 1, i.e. lorsque P s'écrit

$$P = p\prod_{i=1}^{n}(X-\lambda_i)^{\alpha_i}$$

(où p est le coefficient dominant de P)

Caractérisation Le polynôme P est scindé si et seulement si le nombre de racines de P, comptées avec leur ordre de multiplicité, est égal au degré de P.

Rappel Si P est un polynôme quelconque, le nombre de racines de P comptées avec leur ordre de multiplicité est inférieur ou égal au degré de P.

IX.2 Polynômes réels et complexes

Le **théorème de d'Alembert-Gauss** dit que tout polynôme à coefficients complexes a au moins une racine (complexe, bien sûr). Cela équivaut à dire que

Proposition : tout polynôme de $\mathbf{C}[X]$ est scindé

ou encore que

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

Connaître la décomposition en produit de facteurs irréductibles d'un polynôme complexe, c'est donc connaître ses racines et leurs ordres de multiplicité.
On dit aussi que **C** est « algébriquement clos ».
On déduit aussi du théorème de D'Alembert-Gauss le critère de divisibilité suivant :

Critère : Dans $\mathbf{C}[X]$, A divise B si et seulement si pour toute racine α de A, de multiplicité m, α est racine de B avec une multiplicité $\geq m$.

Qu'en est-il sur **R**? certes **R** n'est pas algébriquement clos, mais on a un lemme bien utile :

Lemme important Soit $P \in \mathbf{R}[X]$, $z \in \mathbf{C}\setminus\mathbf{R}$. Alors z est racine de P si et seulement si $\overline{z}$ l'est. Et z et $\overline{z}$ ont même multiplicité en tant que racines de P.

Corollaire : Les polynômes irréductibles de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle, i.e. de discriminant strictement négatif.

Tout polynôme de $\mathbf{R}[X]$ se décompose donc de manière unique, à l'ordre des facteurs près, sous la forme

$$P = p\prod_{i=1}^{n}(X-\alpha_i)^{s_i}\prod_{i=1}^{m}(X^2+\beta_i X+\gamma_i)^{t_i}$$

où tous les $\beta_i^2 - 4\gamma_i$ sont strictement négatifs, l'un des produits pouvant être « vide » (i.e. égal à 1).
L'irréductibilité des polynômes de $\mathbf{K}[X]$ n'est pas toujours facile à étudier. Par exemple, il y a des polynômes irréductibles de tous degrés dans $\mathbf{Q}[X]$.

IX.3 Relations coefficients-racines pour un polynôme scindé

a. Le degré 2

Soit $P = aX^2+bX+c$ scindé, avec $a \neq 2$. Si x_1 et x_2 sont les racines de P (éventuellement $x_1 = x_2$) on peut écrire

$$aX^2+bX+c = a(X-x_1)(X-x_2)$$

En développant le membre de droite, retrouver les formules (à connaître) :

$$x_1+x_2 = \qquad , \qquad x_1x_2 =$$

b. Fonctions symétriques élémentaires

Soit $P = \sum_{i=0}^{n} p_i X^i$ un polynôme scindé de degré n ; on nomme $x_1, \ldots, x_n$ ses racines : il y en a bien n, à condition d'écrire chacune autant de fois que son ordre de multiplicité (les x_i ne sont donc pas supposés distincts). On définit les n fonctions symétriques élémentaires de $x_1, \ldots, x_n$ de la manière suivante :

$\sigma_1(x_1, \ldots, x_n) = x_1 + \cdots + x_n$

$\sigma_2(x_1, \ldots, x_n) = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$

$\ldots \quad \ldots \quad \ldots$

$\sigma_{n-1}(x_1, \ldots, x_n) = x_1 \ldots x_{n-1} + x_1 \ldots x_{n-2}x_n + \cdots + x_2 \ldots x_n$

$\sigma_n(x_1, \ldots, x_n) = x_1 \ldots x_n$

ou, plus généralement,

$$\sigma_k(x_1, \ldots, x_n) = \sum_{J \subset \{1,\ldots,n\}, \mathrm{Card}(J)=k} \left(\prod_{i \in J} x_i \right)$$

(dans un langage plus familier, $\sigma_k(x_1, \ldots, x_n)$ est la somme de tous les produits de k x_i possibles).

On peut aussi préférer l'indexation suivante (moins explicite, mais couramment utilisée) :

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k}$$

c. Les relations

Proposition : On appelle relations coefficients-racines les égalités (valables pour un polynôme P scindé !)

$$\forall j \in \{1, \ldots, n\} \qquad \sigma_j = (-1)^j \frac{p_{n-j}}{p_n}$$

où les σ_j sont les fonctions symétriques élémentaires associées aux racines de $P = p_n X^n + \cdots + p_1 X + p_0$ ($p_n \neq 0$), chaque racine étant répétée autant de fois que sa mutliplicité.

En particulier :

$$\sigma_1 = -\frac{p_{n-1}}{p_n} \qquad ; \qquad \sigma_n = (-1)^n \frac{p_0}{p_n}$$

Dans la pratique, sont surtout à connaître la valeur de la somme et du produit des racines ; pour le produit, c'est particulièrement simple, puisqu'on remarque qu'il suffit de considérer la valeur de P en :

$$\widetilde{P}(\quad) =$$

L'examen du cas $n = 3$ suffit en général pour retrouver ces formules, si on a un doute. Et on a presque toujours $p_n = 1$.

X Interpolation de Lagrange

X.1 Le théorème

Théorème Soit $(\alpha_0,\dots,\alpha_n)\in\mathbf{K}^{n+1}$, supposés deux à deux distincts.
Soit $(y_0,\dots,y_n)\in\mathbf{K}^{n+1}$.
Il existe un unique polynôme P de $\mathbf{K}_n[X]$ tel que

$$\forall i\in[\![0,n]\!]\qquad \widetilde{P}(\alpha_i)=y_i$$

(il existe un unique polynôme de degré $\leq n$ qui prend des valeurs données en $n+1$ points donnés. Si on a un doute, on se rappelle du cas $n=1$.)

X.2 Polynômes interpolateurs de Lagrange

On considère toujours $(\alpha_0,\dots,\alpha_n)\in\mathbf{K}^{n+1}$, avec $i\neq j\ \Rightarrow \alpha_i\neq\alpha_j$.

1. Pour tout $i\in[\![0,n]\!]$, déterminer l'unique polynôme $L_i\in\mathbf{K}_n[X]$ tel que

$$\widetilde{L_i}(\alpha_i)=1\qquad,\qquad \widetilde{L_i}(\alpha_j)=0\quad\text{si } i\neq j$$

2. Démontrer que la famille $(L_0,\dots,L_n)$ est une base de $\mathbf{K}_n[X]$.
3. Calculer les composantes d'un polynôme P de $\mathbf{K}_n[X]$ dans la base $(L_0,\dots,L_n)$ (on les exprimera en fonction des valeurs de $\widetilde{P}$ en les points α_i).
4. En déduire une nouvelle démonstration du théorème énoncé au paragraphe précédent.

Table des matières