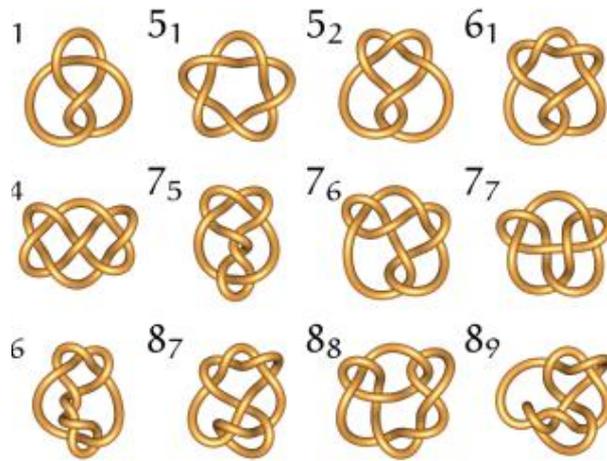


Ag3 : Polynômes

A Knot Zoo



Les polynômes sont très utiles, en tant qu'objets algébriques, mais aussi en tant que fonctions particulièrement simples (n'utilisant que les opérations élémentaires). On les rencontre donc fréquemment, depuis très longtemps, en mathématiques. Une utilisation récente et étonnante en théorie des noeuds : les polynômes de Jones et d'Alexander permettent de classer les noeuds. Des détails et de belles images sont visibles sur le site KnotPlot de Robert Scharein.

I Structure de $\mathbf{K}[X]$

I.1 Résumé

Voir chapitre A11 : $(\mathbf{K}[X], +, \cdot, \times)$ est une \mathbf{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 fautive 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.

Exercice 1 : Montrer que l'application

$$\Delta : P \mapsto P(X + 1) - P(X)$$

est un endomorphisme surjectif de $\mathbf{K}[X]$

(on peut s'intéresser au degré de $P(X + 1) - P(X)$ en fonction du degré de P).

Remarque (voir plus bas) : $P(X)$ et P , c'est la même chose (si on parle de polynômes, pas de fonctions polynômes). Mais écrire $P(X + 1) - P(X)$ est plus naturel qu'écrire $P(X + 1) - P$.

Exercice 2 : Soit $Q \in \mathbf{K}[X]$. Montrer que l'équation

$$P'' + 6XP' - P = Q$$

a une solution unique dans $\mathbf{K}[X]$.

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 \mathbf{K}) non nul λ tel que $A = \lambda B$ (ou encore $B = (1/\lambda)A$). En résumé,

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

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 exercices 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

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

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

(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

Calculer $\tilde{P}(x)$, si $x \in \mathbf{K}$, c'est évaluer P en x . Des raisons d'efficacité numérique alliées à la simplicité algorithmique motivent le calcul de

$\tilde{P}(x) = a_d x^d + \dots + a_0$ par la réécriture

$$\tilde{P}(x) = (((a_d x + a_{d-1}) x + a_{d-2}) x + a_{d-3}) \dots + a_1) x + a_0$$

Par exemple, $3x^6 + 2x^5 - 8x^3 + x^2 + 30x + 11$ sera écrit

$$((((((3x + 2) x + 0) x - 8) x + 1) x + 30) x + 11).$$

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 lorsque $(X-a)^m$ 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 ($\tilde{P}(a) \neq 0$). 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

Ce nom étrange vient de la notion de nombre complexe « idéal » étudiée par Kummer au XIX^{ème} siècle.

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,

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

Parenthèse hors programme

Le programme dispense de la notion d'idéal engendré par une partie. Elle n'est pas plus compliquée que ses analogues (sous-groupe engendré, sous-espace vectoriel engendré. . .) avec les mêmes étapes :

1. L'intersection d'une famille quelconque d'idéaux est un idéal : si, pour tout $k \in K$, I_k est un idéal de $(A, +, \times)$, alors $\bigcap_{k \in K} I_k$ est un idéal de $(A, +, \times)$.
2. Etant donnée une partie X de A , il y a un plus petit idéal (pour l'inclusion) contenant X : c'est l'intersection des idéaux contenant X .
3. Cet idéal s'appelle l'idéal engendré par X

L'idéal des multiples de a , c'est l'idéal engendré par a .

d. Divisibilité et inclusion d'idéaux

On remarque que

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

Autrement dit, la relation de divisibilité s'exprime en termes d'inclusion d'idéaux (mais attention, c'est un peu à l'envers, il faut réfléchir). Grâce à cette remarque assez simple, on peut présenter les idées de base de l'arithmétique (divisibilité, pgcd, ppcm. . .) en termes d'idéaux.

IV.2 Idéaux de $\mathbf{K}[X]$

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.

Éléments 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 $\lambda \neq 0$.

Parenthèse culturelle (h.p) Un anneau sur lequel on peut définir une division euclidienne est dit euclidien. Un anneau tel que tout idéal soit l'ensemble des multiples d'un de ses éléments est dit principal. Un anneau dans lequel tout élément se décompose en produit de facteurs irréductibles est dit factoriel. Et on montre que Euclidien \Rightarrow Principal \Rightarrow Factoriel.

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 (bis)

Pour les amateurs d'ensembles, D est l'unique polynôme unitaire tel que

$$(D) = (A) + (B)$$

On a le droit d'oublier cette écriture, esthétique mais complètement inutile.

V.3 Une propriété

Si $(A, B) \neq (0, 0)$, si $C \neq 0$, alors $(AC) \wedge (BC) = C \times (A \wedge B)$.

V.4 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 :

$$\left[D|A \text{ et } D|B \right] \iff \left[D|A \wedge B \right]$$

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

V.5 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.

b. Un exercice

1. On se place dans l'anneau $(\mathbf{K}[X], +, \times)$ des polynômes à une indéterminée sur un corps commutatif $(\mathbf{K}, +, \times)$.
Soit (a, b) deux entiers naturels non nuls. Montrer que, si le reste de la division de a par b est r , le reste de la division de $X^a - 1$ par $X^b - 1$ est $X^r - 1$ (pour une fois, on peut chercher le quotient de cette division).
2. Sous les mêmes hypothèses que dans la question précédente, écrire le pgcd de $X^a - 1$ et $X^b - 1$ à l'aide de $a \wedge b$.
3. Comment retrouver ce résultat sur $\mathbf{C}[X]$ par une autre méthode?

V.6 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.7 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.8 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 :

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

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 : $(A \wedge B_1 \dots B_p = 1) \iff (A \wedge B_1 = A \wedge B_2 = \dots = A \wedge B_p = 1)$.

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

$$\left[A_1 \dots A_p | C \right] \iff \left[\forall i \in \llbracket 1, p \rrbracket \quad A_i | C \right]$$

La démonstration de ces corollaires en utilisant le théorème de Bézout et le théorème de Gauss est un bon entraînement à l'arithmétique. Seuls les deux premiers sont écrits dans le programme. La décomposition en facteurs irréductibles (voir plus loin) est un bon moyen de les voir un peu moins astucieusement.

V.9 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 On utilise 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

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

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

$$\forall i \in \llbracket 1, n \rrbracket \quad \tilde{P}(a_i) = \tilde{Q}(a_i)$$

alors $P = Q$.

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

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

Considérons l'application

$$\begin{aligned} u : \mathbf{K}[X] &\longrightarrow \mathcal{A}(\mathbf{K}, \mathbf{K}) \\ P &\longmapsto \tilde{P} \end{aligned}$$

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

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

[ce qui signifie simplement que, si P et Q sont des polynômes et λ et μ des scalaires, $\widetilde{\lambda P + \mu Q} = \lambda \tilde{P} + \mu \tilde{Q}$

ce qui se vérifie sans difficulté. Faisons-le :

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

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

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 polynôme 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

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

(même genre de démonstration que pour la linéarité) et

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

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.10 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

$$AU + BV = C \tag{E}$$

1. Donner une condition nécessaire et suffisante (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.11 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.12 PGCD de plus de deux éléments

a. Définition

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

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

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, \dots, 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, \dots, A_p) .

b. Caractérisation

Proposition

$$\left(\forall i \in \{1, \dots, p\} \quad D | A_i \right) \Leftrightarrow \left(D | \text{pgcd}(A_1, \dots, A_p) \right)$$

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**

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

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

Extension Plus généralement, avec des hypothèses évidentes :

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

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

$$U_1 A_1 + U_2 A_2 + \dots + U_p A_p = 1$$

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

La recherche des polynômes irréductibles dans $\mathbf{K}[X]$ dépend beaucoup de \mathbf{K} . Deux cas (deux \mathbf{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 complexe.

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 \mathbf{Z} . Donnons le schéma de la preuve. L'unicité et l'existence peuvent être traitées indépendamment.

Existence : On commence par montrer le

Lemme : Si P est un polynôme non constant, il a au moins un diviseur irréductible.

Preuve du lemme : intéressante et pas trop compliquée!

Preuve de l'existence : Par récurrence (à hypothèse forte) sur le degré de P . Si P est irréductible, il n'y a rien à montrer. Sinon, soit Q un diviseur irréductible de P , on écrit $P = QP_1$, on applique l'hypothèse de récurrence à P_1 . Ne pas oublier d'initialiser.

Preuve de l'unicité : On prend deux décompositions qui conviennent :

$$P = a \prod_{i=1}^n P_i^{\alpha_i} = a \prod_{k=1}^m Q_k^{\beta_k}$$

(les α_k et les β_k étant des exposants non nuls). Si $P_1 \wedge Q_k = 1$ pour tout k , alors P_1 est premier avec P , ce qui est contradictoire (il le divise, et il n'est pas constant). Donc il existe k_0 tel que $P_1 \wedge Q_{k_0} \neq 1$, et comme P_1 et Q_{k_0} sont irréductibles unitaires, cela signifie que $P_1 = Q_{k_0}$. On montre ainsi que chaque P_i est dans $\{Q_k ; k \in \llbracket 1, m \rrbracket\}$. Mais de même, chaque Q_k est dans $\{P_i ; i \in \llbracket 1, n \rrbracket\}$. Et donc, premier résultat,

$$\{P_i ; i \in \llbracket 1, n \rrbracket\} = \{Q_k ; k \in \llbracket 1, m \rrbracket\}$$

Donc, quitte à réindexer, on se ramène à montrer que si

$$P = a \prod_{i=1}^n P_i^{\alpha_i} = a \prod_{i=1}^m P_i^{\gamma_i}$$

alors pour tout i on a $\gamma_i = \alpha_i$. Supposons par exemple $\gamma_1 < \alpha_1$. En simplifiant, on aurait alors

$$P_1^{\alpha_1 - \gamma_1} \times \prod_{i=2}^n P_i^{\alpha_i} = \prod_{i=2}^m P_i^{\gamma_i}$$

et donc P_1 diviserait le second membre, or il est premier avec P_2, \dots, P_n , donc premier avec ce second membre... contradiction.

Plus important que la démonstration, les cas au programme :

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

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

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

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

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

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

On a de plus

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

VI.6 Retour sur le théorème de Gauss

Rappelons le théorème de Gauss :

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

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 divisibilité 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 $\alpha_i, \beta_i, \gamma_i$.
2. En déduire que $A|C$.

Le théorème de Gauss peut donc être vu à l'aide de la décomposition en polynômes irréductibles. Mais cette décomposition est surtout un bon moyen de retrouver les corollaires :

1. Que déduire de l'hypothèse $A|C, B|C$ et $A \wedge B = 1$?
2. Si on suppose seulement $A \wedge B = 1$, comment simplifier $A \wedge BC$ (en l'écrivant comme un autre pgcd)?

Comme signalé plus haut, on a ici une manière sans doute moins astucieuse de voir Gauss et ses corollaires.

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

Plus généralement Si $A \in \mathcal{M}_n(\mathbf{K})$, on ne voit pas bien ce qui empêcherait de définir

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

et effectivement, on le fera, et on l'utilisera abondamment (voir chapitres sur la réduction). On définira donc des polynômes de matrices (ce sont des matrices) et des polynômes d'endomorphismes de la même manière.

Notation Ne pas noter $\tilde{P}(Q) : P(Q)$ n'a rien à voir avec la fonction polynôme associée à P . Ne pas noter non plus $P \circ Q$, qui serait une notation valable pour les fonctions polynômes associées, mais pas judicieuse pour les polynômes (un polynôme n'a rien à voir avec une application).

Remarque Donc $P(X) = P..$ l'habitude de noter un polynôme P ou $P(X)$ suivant les cas est donc irréprochable.

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. Remarque

Cette définition est purement algébrique; mais dans le cas très spécial où $\mathbf{K} = \mathbf{R}$, la fonction polynôme associée au polynôme dérivé (au sens algébrique) est la dérivée (au sens analytique) de la fonction associée au polynôme de départ : $\widetilde{D}(P) = D(\tilde{P})$, ou encore $\tilde{P}' = (\tilde{P})'$.

Dans le cas général, si \mathbf{K} est un corps quelconque sur lequel on ne fait pas d'analyse et sur lequel, donc, la dérivation des fonctions n'est pas définie, on n'a plus ce parallèle entre dérivation « algébrique » et dérivation « analytique ».

c. 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 $\forall (P, Q) \in \mathbf{K}[X]^2 \quad D(PQ) = P D(Q) + Q D(P)$

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

Démonstration Montrons que la linéarité (en fait ici, la bilinéarité) permet d'écrire une démonstration agréable :

Pour $P = X^n$ et $Q = X^m$, la vérification est un calcul sympathique.

Fixons $P = X^n$ ($n \in \mathbf{N}$ fixé). Les applications

$$Q \longmapsto D(PQ)$$

et

$$Q \longmapsto PD(Q) + QD(P)$$

sont linéaires (vérification facile) et coïncident sur la base canonique, donc sont égales.

On a donc, pour tout P de la forme X^n , pour tout $Q \in \mathbf{K}[X]$,

$$D(PQ) = PD(Q) + QD(P)$$

Fixons maintenant Q . Les applications $P \longmapsto D(PQ)$

et

$$P \longmapsto PD(Q) + QD(P)$$

sont linéaires et coïncident sur la base canonique, donc sont égales. C'est fini!

Cette démonstration est intéressante à comprendre. Elle utilise la bilinéarité de

$$(P, Q) \longmapsto D(PQ)$$

et celle de

$$(P, Q) \longmapsto PD(Q) + QD(P)$$

(ces deux applications sont linéaires par rapport à P , à Q fixé, et par rapport à Q , à P fixé). Et on applique deux fois le résultat qui dit que deux applications linéaires qui coïncident sur une base sont égales.

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

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

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

Démonstration Récurrence, formule précédente, réindexation, formule du triangle de Pascal. . . pas inintéressante. Donnons l'étape cruciale (la preuve que la formule est récurrente) :

$$\begin{aligned}
 \left[\sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n-k)} \right]' &= \sum_{k=0}^n \binom{n}{k} \left[P^{(k)} Q^{(n-k)} \right]' \\
 &= \sum_{k=0}^n \binom{n}{k} P^{(k+1)} Q^{(n-k)} + \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\
 &= \sum_{j=1}^{n+1} \binom{n}{j-1} P^{(j)} Q^{(n+1-j)} + \sum_{k=0}^n \binom{n}{k} P^{(k)} Q^{(n+1-k)} \\
 &= P^{(n+1)} + Q^{(n+1)} + \sum_{k=1}^n \left[\binom{n}{k} + \binom{n}{k-1} \right] P^{(k)} Q^{(n+1-k)} \\
 &= \sum_{k=0}^{n+1} \binom{n+1}{k} P^{(k)} Q^{(n+1-k)}
 \end{aligned}$$

VIII.3 Formule de Taylor

a. La formule

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

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

que l'on peut aussi écrire :

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

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

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

ou, aussi bien,

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

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 $((X - a)^n)_{n \in \mathbf{N}}$ de $\mathbf{K}[X]$. Donc $\phi = \text{Id}_{\mathbf{K}[X]}$ 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

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

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.

◇ Il faut penser à la formule de Taylor (souvent oubliée) lorsque dans un problème mettant en jeu des polynômes un point autre que 0 joue un rôle particulier.

◇ Il faut, lorsque se présente un problème d'ordre de multiplicité de racine, penser aux deux caractérisations : par divisibilité ou par annulation des dérivés successives.

◇ La formule de Taylor n'est pas valable sur $\mathbf{K}[X]$ pour n'importe quel corps \mathbf{K} . On verra plus tard des corps finis sur lesquels cette formule est fautive. mais le programme stipule qu'on ne s'occupe pas de $\mathbf{K}[X]$ dans ce cas. On ne rencontre en général que de polynômes à coefficients réels ou complexes, exceptionnellement à coefficients dans \mathbf{Q} ...

IX Polynômes scindés, relations entre coefficients et racines

Ces relations sont très importantes. La formule générale est souvent jugée ef-

frayante alors qu'elle est parfaitement sympathique. Ce qu'on va (re-)voir ici.

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 peut s'écrire

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

(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 Dans le cas général, 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 \mathbf{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 \mathbf{R} ? certes \mathbf{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 \bar{z} l'est. Et z et \bar{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 $a \neq 0$. 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) :

$$x_1 + x_2 = \quad , \quad x_1 x_2 =$$

Exercice : A quelle condition sur a et b (réels) existe-t-il des réels x et y tels que

$$\begin{cases} x + y = a \\ x \times y = b \end{cases} \quad ?$$

b. Quelques calculs préliminaires

Développer :

$$(X - x_1)(X - x_2)(X - x_3) =$$

$$(X - x_1)(X - x_2) \dots (X - x_n) = X^n - (\quad) X^{n-1} + \dots +$$

(on ne cherchera à expliciter que le coefficient de degré $n - 1$ et le coefficient constant).

c. Fonctions symétriques élémentaires

Soit $P = \sum_{i=0}^n p_i X^i$ un polynôme scindé de degré n ; on nomme x_1, \dots, 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, \dots, x_n de la manière suivante :

$$\sigma_1(x_1, \dots, x_n) = x_1 + \dots + x_n$$

$$\sigma_2(x_1, \dots, x_n) = x_1 x_2 + \dots + x_1 x_n + x_2 x_3 + \dots + x_{n-1} x_n$$

... ..

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

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

ou, plus généralement,

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

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

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

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

Ces fonctions sont symétriques : si on mélange les x_i on ne change pas les σ_k .

Plus précisément, si $u \in \mathfrak{S}_n$, pour tout k on a

$$\sigma_k(x_{u(1)}, \dots, x_{u(n)}) = \sigma_k(u_1, \dots, u_n)$$

Elémentaires? essayez d'en trouver des plus simples! on peut montrer que toute fonction polynomiale (à plusieurs variables) en les x_i peut s'écrire comme polynôme en $\sigma_1, \dots, \sigma_n$. Ce résultat est complètement hors-programme.

d. Les relations

On voit alors que

$$(X - x_1)(X - x_2) \dots (X - x_n) = X^n - (x_1 + \dots + x_n)X^{n-1} + (x_1x_2 + x_1x_3 + \dots)X^{n-2} \\ + \dots + (-1)^n x_1x_2 \dots x_n$$

c'est-à-dire

$$(X - x_1)(X - x_2) \dots (X - x_n) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^n \sigma_n$$

Si on sait écrire cette relation, on a tous les résultats qu'on veut, il faut donc se concentrer là-dessus! quand on a pris un bon départ avec le $-\sigma_1 X^{n-1}$, il n'y a plus qu'à continuer : les signes alternent, les puissances de X décroissent comme les indices des σ croissent...

Soit alors P un polynôme scindé, que l'on écrit sous la forme développée :

$$P = p_n X^n + p_{n-1} X^{n-1} + \dots + p_1 X + p_0$$

et sous la forme factorisée :

$$P = p_n (X - x_1)(X - x_2) \dots (X - x_n)$$

Cette dernière se réécrit

$$P = p_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^n \sigma_n)$$

on obtient donc, par unicité de la décomposition sur la base canonique,

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

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

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

En particulier :

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

Au programme, sont à connaître par cœur la valeur de la somme et du produit des racines; pour la somme, le résultat est la formule de Viète; pour le produit, c'est particulièrement simple, puisqu'on remarque qu'il suffit de considérer la valeur de P en :

$$\tilde{P}() =$$

Il faut savoir retrouver les autres formules, ce que permet un peu de pratique. Les apprendre par cœur serait très fastidieux. L'examen du cas $n = 3$ suffit en général pour retrouver les formules, si on a un doute. Et on a presque toujours $p_n = 1$.

Exercice : On note comme d'habitude $\mathbf{U}_n = \{z \in \mathbf{C} ; z^n = 1\}$. Calculer $\sum_{\zeta \in \mathbf{U}_n} \zeta$,

$$\sum_{\zeta \in \mathbf{U}_n} \zeta^2, \quad \prod_{\zeta \in \mathbf{U}_n} \zeta.$$

Exercice : Soit $P = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X \in \mathbf{K}[X]$. On suppose $a_n \neq 0$, $a_1 \neq 0$, P scindé. Calculer le produit des racines non nulles de P .

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

$$\forall i \in \llbracket 0, n \rrbracket \quad \tilde{P}(\alpha_i) = y_i$$

(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 $n = 1$.)

Démonstration : On considère l'application

$$\begin{aligned} \psi : \mathbf{K}_n[X] &\longrightarrow \mathbf{K}^{n+1} \\ P &\longmapsto (\tilde{P}(\alpha_0), \dots, \tilde{P}(\alpha_n)) \end{aligned}$$

dont il est assez clair qu'elle est linéaire. On montre qu'elle est injective, elle est alors surjective d'après le théorème du rang et le fait que

$$\dim(\mathbf{K}_n[X]) = \dim(\mathbf{K}^{n+1})$$

X.2 L'exercice à savoir faire

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 $i \in \llbracket 0, n \rrbracket$, déterminer l'unique polynôme $L_i \in \mathbf{K}_n[X]$ tel que

$$\tilde{L}_i(\alpha_i) = 1 \quad , \quad \tilde{L}_i(\alpha_j) = 0 \quad \text{si } i \neq j$$

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 \tilde{P} en les points α_i).
4. En déduire une nouvelle démonstration du théorème énoncé au paragraphe précédent.

XI Annexe : polynômes de plusieurs variables

La lecture de ce paragraphe, hors-programme, peut être intéressante pour les candidats aux ENS

XI.1 Définition

Le sous-espace vectoriel de $\mathcal{A}(\mathbf{K}^n, \mathbf{K})$ engendré par la famille $(f_{\alpha_1, \dots, \alpha_n})_{(\alpha_1, \dots, \alpha_n) \in \mathbf{N}^n}$, où $f_{\alpha_1, \dots, \alpha_n}$ est l'application

$$(x_1, \dots, x_n) \mapsto x_1^{\alpha_1} \dots x_n^{\alpha_n},$$

est appelé **espace vectoriel des applications polynômiales sur \mathbf{K}^n** (c'est même une **sous-algèbre** de $\mathcal{A}(\mathbf{K}^n, \mathbf{K})$, le produit de deux applications polynomiales étant une application polynomiale).

En particulier, les applications polynomiales sur \mathbf{K}^2 sont les applications

$$(x, y) \mapsto \sum_{(\alpha, \beta) \in \mathbf{N}^2} \lambda_{\alpha, \beta} x^\alpha y^\beta$$

(où, bien sûr, il n'y a dans la somme qu'un nombre fini de termes non nuls, ce qui signifie que $(\lambda_{\alpha, \beta})_{(\alpha, \beta) \in \mathbf{N}^2}$ est à support fini, ou « presque nulle », ou dans $\mathbf{K}^{(\mathbf{N}^2)}$).

XI.2 Base

Proposition Si \mathbf{K} est infini, la famille $(f_{\alpha_1, \dots, \alpha_n})_{(\alpha_1, \dots, \alpha_n) \in \mathbf{N}^n}$ est une base de cette algèbre des fonctions polynomiales sur \mathbf{K}^n .

Démonstration Cette famille étant par définition génératrice, il suffit de prouver l'indépendance linéaire de la famille $(f_{\alpha_1, \dots, \alpha_n})_{(\alpha_1, \dots, \alpha_n) \in \mathbf{N}^n}$. On va le faire par récurrence sur n .

Initialisation : $n = 1$: c'est un résultat classique sur les polynômes : il s'agit ici de montrer que la famille $(f_\alpha)_{\alpha \in \mathbf{N}}$ est libre, avec $f_\alpha : x \mapsto x^\alpha$. Si $\sum_{\alpha \in \mathbf{N}} \lambda_\alpha f_\alpha = 0$ (somme finie : au plus un nombre fini de λ_α non nuls), le polynôme $\sum_{\alpha \in \mathbf{N}} \lambda_\alpha X^\alpha$ a une infinité de racines (tous les éléments de \mathbf{K} , qui

est supposé infini), c'est donc le polynôme nul, ce qui signifie que tous ses coefficients sont nuls. Le résultat s'ensuit.

Etude du cas $n = 2$: Supposons que l'on ait $f = \sum_{(\alpha,\beta) \in \mathbf{N}^2} \lambda_{\alpha,\beta} f_{\alpha,\beta} = 0$ (somme

finie). On aurait alors, pour tout couple (x, y) d'éléments de \mathbf{K} ,

$\sum_{\alpha \in \mathbf{N}} \left(\sum_{\beta \in \mathbf{N}} \lambda_{\alpha,\beta} y^\beta \right) x^\alpha = 0$ (on peut réordonner les termes comme on le sou-

haite : la somme est finie). En utilisant le cas $n = 1$, on en tire que, pour tout y , pour tout α ,

$\sum_{\beta \in \mathbf{N}} \lambda_{\alpha,\beta} y^\beta = 0$. Et donc, pour tout α , en appliquant de nouveau le résultat

pour $n = 1$, on obtient que tous les $\lambda_{\alpha,\beta}$ ($\beta \in \mathbf{N}$) sont nuls. Finalement, tous les coefficients $\lambda_{\alpha,\beta}$ sont nuls.

Récurrence : La proposition à l'ordre $n = p+1$ se déduit de la proposition à l'ordre $n = p$ comme le cas $n = 2$ se déduit du cas $n = 1$.

Table des matières

I	Structure de $K[X]$	2
I.1	Résumé	2
I.2	L'espace vectoriel $K[X]$	2
II	Division euclidienne	3
II.1	Divisibilité, polynômes associés	3
II.2	Division euclidienne	3
III	Fonction polynôme, zéros d'un polynôme	4
III.1	Fonction polynôme associée	4
III.2	Méthode de Horner	4
III.3	Zéros d'un polynôme; multiplicité	4
IV	Idéaux	6
IV.1	Idéaux d'un anneau commutatif	6
a.	Définition :	6
b.	Caractérisation pratique :	6
c.	Idéal des multiples d'un élément	6
d.	Divisibilité et inclusion d'idéaux	7
IV.2	Idéaux de $K[X]$	8
V	PGCD, PPCM	9
V.1	Définition du pgcd par les idéaux	9
V.2	(bis)	9
V.3	Une propriété	9
V.4	Equivalence avec la définition habituelle	9
V.5	Détermination pratique (algorithme d'Euclide)	10
a.	Evocation de l'algorithme	10
b.	Un exercice	10
V.6	Polynômes premiers entre eux, théorème de Bezout	11
a.	Polynômes premiers entre eux	11
b.	Théorème de Bézout	11
c.	Une évidence	11

d.	Obtention de coefficients de Bézout par l'algorithme d'Euclide	11
V.7	Une caractérisation utile du pgcd	11
V.8	Théorème (ou lemme. . .) de Gauss	12
a.	Le lemme de Gauss	12
V.9	Nombre de zéros (ou racines) d'un polynôme	13
a.	Majoration du nombre de racines d'un polynôme	13
b.	Conséquences	13
V.10	Equations $AU + BV = C$ (h.p. mais classique)	15
V.11	PPCM	16
V.12	PGCD de plus de deux éléments	16
a.	Définition	16
b.	Caractérisation	16
c.	Associativité du pgcd	17
d.	Polynômes premiers entre eux (dans leur ensemble)	17
VI Polynômes irréductibles		18
VI.1	Définition	18
VI.2	Exemples	18
VI.3	Décomposition en facteurs irréductibles	19
VI.4	Deux résultats utiles	20
VI.5	Utilisation pour le calcul du pgcd et du ppcm	21
VI.6	Retour sur le théorème de Gauss	21
VII Polynômes de polynômes		23
VIII Polynôme dérivé; formules de Leibniz et Taylor		24
VIII.1	Polynôme dérivé	24
a.	Définition	24
b.	Remarque	24
c.	L'endomorphisme dérivation	24
VIII.2	Formule de Leibniz	24
VIII.3	Formule de Taylor	26
a.	La formule	26
b.	Une caractérisation de la multiplicité d'une racine	27

IX Polynômes scindés, relations entre coefficients et racines	27
IX.1 Polynômes scindés	28
IX.2 Polynômes réels et complexes	28
IX.3 Relations coefficients-racines pour un polynôme scindé	29
a. Le degré 2	29
b. Quelques calculs préliminaires	30
c. Fonctions symétriques élémentaires	30
d. Les relations	31
X Interpolation de Lagrange	33
X.1 Le théorème	33
X.2 L'exercice à savoir faire	33
XI Annexe : polynômes de plusieurs variables	34
XI.1 Définition	34
XI.2 Base	34