Polynômes
(version chantier)

Marc SAGE

<2015

Table des matières

1 Introduction **3**

2 L'algèbre $K[X]$ **4**
2.1 Degré valuation 4
2.2 Composition 5
2.3 Evaluation ou spécialisation 5
2.4 Fonction polynomiale 5

3 Divisibilité, généralité **5**

4 Irréductibilité **6**

5 Racines **7**

6 Dérivation **9**

7 Changement corps de base **10**

8 Congruence modulo P, scission de polynômes, clôture algébrique **10**

9 Clôture algébrique **11**

10 Plusieurs variables **11**

11 POur aller plus loin **11**

sur les transcendants

le temre apparait début mars 1675 (Leibniz à Oldenbourg). Plus tard, à Tchirnhauss (mais 1678) :

1. *transcendant* = non-analytique
2. archétype de transcendant est équation où inconnue entre dans l'exposant.

Aisnsi, la *transcendance* (litt. qui dépasse tout degré fixé, phil. qui dépasse le champ de l'expérience seimple) vient de la variabilité non borné de l'exposant. Plus généralement il parle à Bernoulli de *parcourantes* (mais cela n'a pas pris) qui nous semble n'être autre que le terme moderne de *varaible*.

(source M. Serfati, *de la méthode*, p. 281)

sur les nômes

Hervé Lehning, *À la recherche de la preuve en mathématiques*

Selon certains linguistes comme ALbert Dauzat (1877-1955), "nôme" viendrait de "onoma", qui signifie "nom". Cette interprétation colle à la réalité mathématique : un monôme se nomme par son degré (la puissance) et un monôme a un seul degré [ET LE SCALAIRE ? ? ?]. [...]

Il existe une autre étymologie : "nomos" signifie "loi". On peut alors penser à la fonction mathématique, donc à la "loi" de calcul. Ces deux étymologies éclairent la différence subtile entre polynôme et fonction polynomiale [outre le ^ :-)] D'un côté, les polynômes sont des "êtres" formels, de l'autre des lois de calculs.

EXO : *soit a racine simple de P mais $P''(a)=0$. Mq $\sum_{\lambda \text{ raine}} \frac{1}{a-\lambda}=0$. En déduire, pour un poly cubique, que ses racines sont en progression arihmétique ssi celle du milieu anule la dérviees seconde.*

DEM : $P=(X-a)Q$, $P''=2Q'+(X-a)Q''$, donc $P''(a)=0$ se réécrit $Q'(a)=0$. Or, $\sum_{\lambda \text{ raine}} \frac{1}{a-\lambda} = \frac{Q'}{Q}(a)$

Soient b et c les autres zéros, alors $P''(a)=0$ ssi $\frac{1}{a-b}+\frac{1}{a-c}=0$ ssi $(a-c)+(a-b)=0$ ssi $a=\frac{b+c}{2}$s

EXO : *soit a zéro somple de P, λ les autrs racines de P, μ celles de P'. Mq $\sum \frac{1}{a-\lambda}=\frac{1}{2}\sum \frac{1}{a-\mu}$.*

DEM : on veut $\frac{Q'}{Q}(a)=\frac{P''}{P'}(a)$ où $Q:=\frac{P}{X-a}$; mais on a $P'=Q+(X-a)Q'$ et $P''=2Q'+(X-a)Q''$, d'où le résultat.

EXO *Mq $P:=X^n-X^{n-1}-2X^{n-2}-3X^{n-3}-...-n$ a une unique racine >0, qui est irrationnelle pour $n\geq 3$. Quid si $n<3$?*

DEM : pour $n=1$, le polynome Pvaut $X-1$, ok. Pour $n=2$, il vaut $X^2-X-2=(X-1)(X+2)$.

On voit appaitre des dérivées $\frac{P(x)}{x^{n-1}}=\underbrace{\left(\frac{1}{T}-\left[\sum_{i=0}^{n}T^i\right]'\right)}_{\text{décroit stttt}}\left(\frac{1}{x}\right)$, avec valeur <0 en 1 et limite >0 en ∞, d'où une unique racine >1.

Puisque P unitaire, toute racine rationnelle est entière. Pour se débarasser du nombre "dépendant de n" de termes du polynômes, on utilse (poser $N:=n+1$)

$$\left(\sum_{i=0}^{N-1}T^i\right)'=\left(\frac{1-T^N}{1-T}\right)'=\frac{-NT^{N-1}(1-T)+\left(1-T^N\right)}{(1-T)^2}=\frac{(N-1)T^N-NT^{N-1}+1}{(1-T)^2},$$

d'où pour toute racine $\lambda\neq 0$ de P : $\lambda:=\frac{1}{\mu}=\left[\sum_{i=0}^{N-1}T^i\right]'(\mu)=\frac{(N-1)\mu^N-N\mu^{N-1}+1}{(1-\mu)^2}$, ie $1-2\mu+\mu^2=(N-1)\mu^{N+1}-N\mu^N+\mu$, ie $\mu^2-3\mu+1=(N-1)\mu^{N+1}-N\mu$, ie

$$\lambda^{N+1}-3\lambda^N+\lambda^{N-1}+N\lambda-(N-1)=0.$$

(on s'est donc ramené à un quadrinome, dont 1 est racine). Pour $\lambda>1$, les deux deniers termes sont $>1N-(N-1)>0$, donc les trois premiers divisés par λ^{N-1} restent <0, ie $\lambda^2-3\lambda+1<0$, ie $(\lambda-1)(\lambda-2)<1$, impossible pour λ entier >2. On obtient donc $\lambda=2$ et $0=2^{N-1}\left(2^2-3\cdot 2+1\right)+2N-(N-1)=-2^n+n+2$, d'où $2^n=n+2$, ordre de grandeu impossible pour $n>2$

EXO : *Mq les zéros d'un polynôme de la forme $\sum_{i\geq 0}X^{n_i}$ avec $0=n_0<n_1<\cdots$ sont hors d'un disque de rayon $\frac{\sqrt{5}-1}{2}$*

DEM : noter que rayon donné est racine de X^2+X-1.Pour λ raince de P, on a $0=1+\lambda^{n_1}+\lambda^{n_2}+\cdots$, d'où $1\leq\sum_{i\geq 1}|\lambda|^{n_i}$. Si $n_1\geq 2$, on obtient $1<|\lambda|^2\frac{1}{1-|\lambda|}$, impossible. Donc $n_1=1$, mais alors $(1-X)P$ est de la forme P avec $n_1=2$ (et des $\pm$ devant les coef), d'où même raisonmen et même conclusion.

EXO : *mq les racines de* $X^{n+1}-aX^n+aX-1$ *sont toutes unitaire (pour* $a\in[-1,1]$*).*

DEM : pour $a=\pm 1$, le polyn se factoriser gentil $X^n(X-a)+a(X-a)=(X^n+a)(X-a)$, terminée. OPS $|a|<1$.

Soit λ racine $\lambda^n(\lambda-a)=1-a\lambda$, d'où $\left|\lambda^{2n}\right||\lambda-a|^2=|1-a\lambda|$. Rq : aucun des facteurs n'est nul, car λ n'est pas racine et car l'égalité $|\lambda-a|=0=|1-a\lambda|$ implique $a^2=1$, auquel cas le polyn . Ainsi, on a les équivalences (absurdes)

$$|\lambda|<1 \iff |\lambda-a|^2>|1-a\lambda| \iff |\lambda|^2-2a\operatorname{Re}\lambda+a^2>1-2a\operatorname{Re}\lambda+a^2|\lambda|^2 \iff \left(|\lambda|^2-1\right)\left(a^2-1\right)<0 \iff |\lambda|^2-1>0.$$

1 Introduction

Comment faire du calcul dans une algèbre ? Plus précisément, quelles expressions peut-on former à partir d'une famille (x_i) d'éléments de cette algèbre et de ses trois lois de calculs ?

Commençons par un seul élément x. On peut déjà former ses itérés x^n où n est un entier positif, on peut multiplier ces itérés par un scalaire pour former un *monôme* a_nx^n (l'expression x^n est un monôme dit *unitaire* ou *normalisé*) et l'on peut enfin sommer de telles expressions pour obtenir une somme finie de la forme

$$\sum_{n\geq 0}a_nx^n, \text{ appelée } \textit{polynôme} \text{ en } x.$$

Il est aisé de voir qu'une combinaison linéaire de polynômes est encore un polynôme :

$$\sum_{n\geq 0}a_nx^n+\lambda\sum_{n\geq 0}b_nx^n=\sum_{n\geq 0}(a_n+\lambda b_n)x^n.$$

Un (tout) petit calcul montre, en regroupant les mêmes puissances de x, qu'il en est de même pour le produit :

$$\left(\sum_{p\geq 0}a_px^p\right)\left(\sum_{q\geq 0}b_qx^q\right)=\sum_{p\geq 0}\sum_{q\geq 0}a_px^pb_qx^q=\sum_{n\geq 0}\sum_{p+q=n}a_pb_qx^{p+q}=\sum_{n\geq 0}\left(\sum_{p+q=n}a_pb_q\right)x^n.$$

Nous avons donc montré que toutes les expressions formables à partir d'un élément x d'une algèbre (et de ses trois lois de calcul) sont *exactement* les polynômes en x.

On montrerait de la même façon que les expressions formables à partir d'un nombre fini d'éléments $x_1,...,x_k$ sont exactement les combinaisons linéaires des monômes unitaires $x_1^{n_1}x_2^{n_2}...x_k^{n_k}$, aussi appelées polynômes en $x_1,...,x_k$, qui sont de la forme

$$\sum_{n_1,...,n_k\geq 0}a_{n_1,...,n_k}x_1^{n_1}x_2^{n_2}...x_k^{n_k} \text{ où les } a_{n_1,...,n_k} \text{ sont des scalaires.}$$

Si nous partons d'une famille (x_i) éventuellement infinie, nous ne pouvons former des expressions qu'en appliquant un nombre **fini** de fois les lois de notre algèbre[1] ; ces dernières ne prenant en argument qu'un nombre **fini** d'éléments, il n'apparaît à la fin de notre calcul qu'un nombre fini de x_i, ce qui nous ramène au cas ci-dessus.

Ainsi, les polynômes ne sont rien d'autres que des fonctions de calcul universelles dans une algèbre, ce qui motive leur étude[2].

Nous nous bornerons à étudier les polynômes à une variable. Deux raisons à cela : d'une part, la formule

$$\sum_{p,q\geq 0}a_{p,q}x^py^q=\sum_{q\geq 0}\left(\sum_{p\geq 0}a_{p,q}x^p\right)y^q=\sum_{p\geq 0}\left(\sum_{q\geq 0}a_{p,q}y^q\right)x^p$$

[1] À ce stade, pas de questions de séries ou produits infinis, lesquels nécessiteraient de toute façon une topologie pour parler de convergence.

[2] On parle ici d'algèbres, objet d'étude récurrent des algèbristes, mais il suffit de considérer les trinômes du second degré pour se rendre compte que les polynôme ont également leur mot à dire en analyse.

montre (par une récurrence immédiate) qu'un polynôme en $x_0, ..., x_k$ (sur un anneau A) n'est autre qu'un polynôme en x_0 sur l'anneau des polynômes en $x_1, ..., x_k$; d'autre part, malgré notre enthousiasme motivé par l'observation précèdente, les polynômes à plusieurs variables sont beaucoup plus difficiles à étudier – et c'est bien normal : les connaître parfaitement reviendrait à connaître toutes les algèbres, quête (probablement) sans fin dans laquelle (se) sont engagés des algébristes chevronnés.

Pour étudier les polynômes $\sum a_n x^n$ en une variable x, nous coderons ce dernier par la liste ordonnée de ses coefficients, ce qui a l'avantage de se libérer de la variable x et par là même de l'algèbre sous-jacente.

Plus généralement, on va mettre une structure d'algèbre sur les suites de scalaires —> séries formelles dont les polynômes (support fini) en sont un sous-anneau

les coef d'un polynôme peuvent être vus de cinq façons :

définition formelle : écriture $\sum a_n X^n$ code une suite finie de coef

forme factorisée : $a \prod_{i=1}^{p} (X - \lambda_i)^{\omega_i}$ code un p-uplet pondéré avec un coefficient dominant : ou un multi-ensemble à n élément plus un coef dom $a \prod (X - \lambda_i)$

par les racines : Viète : $a_{d-n} = (-1)^n \sigma_n$

fonctionnelle : Taylor - Mac Laurin : $a_n = \frac{P^{(n)}(0)}{n!}$

analytique : Cauchy : $a_n z^n = \int P\left(ze^{i\theta}\right) e^{-in\theta} \frac{d\theta}{2\pi}$ (planter un compas en 0, le crayon en z, et décrire un cercle), d'où $a_n \leq \frac{1}{r^n} \sup_{r\mathbb{U}} |P|$.

un peu de combi : (exo FGN) un poly code une suite finie, intro vers séries entières ?

2 L'algèbre $K[X]$

L'adjectif "polynomial" *ne prend pas* d'accent circonflexe, contrairement au nom associé...

Un polynôme est une corde à linge surlaquelle on accroche un étiquette marquée a_n (unique information codée)

On met un structure d'algèbre pour pouvoir travailler.

$K \hookrightarrow K[X]$ est une algèbre intègre de dimension infinie, de base canonique $(X^n)_{n\geq 0}$.

On peut remplacer K par un anneau A : mêmes lois. eg : $Z[X] \hookrightarrow Q[X]$, $F_2[X] \hookrightarrow F_4[X]$.

Si A intègre, on garde l'intégritié, mais on la perd sinon, tout comme $\partial AB \leq \partial A + \partial B$: $2X \cdot 2X = 4X^2 = 0$ dans $Z/4Z[X]$

2.1 Degré valuation

deg, d°, ou ∂ si pas de confusion avec dérivation.

$\deg \sum \leq \max\{\deg\}$

$\deg \prod = \sum \deg$

$\dim K_n[X] = n + 1$

EXO : $\{(X-a)^p (X-b)^q\}_{p+q=n}$ libre (base duale ? ?) (idée : $b = 0$, voire $b = -a$!)

EXO : soit $a \in R^n$: mq $\exists! \lambda \in R, \forall P \in R_n[X] : \int_{-1}^{1} P = \sum \lambda_i P(a_i)$ ($\int$ est une fl, donc se décompose dans la base des évala_i)

EXO : soit $a \in R^n$: mq $\exists! \lambda \in R, \forall P \in R_n[X] : P = \sum \lambda_i P(a_i + X)$ (analyse : $P = 0 \Rightarrow \lambda$ sont les coef de eval0 dans la base des eval$_{a_i}$)

2.2 Composition

EXO : *endo de $K[X]$? Auto ?* *Quels endo commutetn à la dérivatio ?*

MOrphisme : si φ endo d'lagèbre, alors $\varphi(P) = \varphi(P(X)) = P(\varphi(X))$, donc φ composition à droite par un certain polynôme.

Auto ? Il faut surj, donc $\varphi(X)$ non cst. notons $\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \varphi(X) \\ \varphi^{-1}(X) \end{pmatrix}$. Alors $X = \varphi\left(\varphi^{-1}(X)\right) = \varphi(B) = \varphi(B(X)) = B(\varphi(X)) = B(A) = B \circ A$, d'où en prenant les degés A et B affines (non cst), qui conviennt.

2.3 Evaluation ou spécialisation

Soit $\mathcal{A}$ une K-algèbre. On a un morphisme d'algèbres $\left\{ \begin{array}{ccc} K[X] & \longrightarrow & \mathcal{A} \\ P & \longmapsto & P(a) \end{array} \right.$.

En particulier, $P(a)Q(a) = PQ(a) = QP(a) = Q(a)P(a)$: si a est un endo, deux poly d'un même endo commutent (donc noyaux stables...)

eg :
$P(X) = P = X \circ P$: on a trouvé le neutre du monoïde $(K[X], \circ)$
$P(Q) = P \circ Q$
$P(u) = a_0 \mathrm{Id} + a_1 u + ... + a_n u^n$
$P(X - \lambda)$: translation –> tous les automorphismes de $K[X]$

Algo de Horner-Ruffini

!! Si A anneau, alors l'éval $\left\{ \begin{array}{ccc} A[X] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array} \right.$ est un morphisme de groupe additif mais pas forcément multiplicatif (ok si a commute avec les coef des polynômes), induit morphisme d'algèbres sur $Z[X]$ où Z centre de A!! (rq utile pour une démo de Caly hamilton utilisant l'isom $M_n(K[X]) \cong (M_n(K))[X]$)

2.4 Fonction polynomiale

$K[X] \longrightarrow K^K$
noyau $\left(X^{|K|} - X\right)$

Sur R et C, polynomiales sont continue !
EXO : images des $P(\mathbb{R})$ pour $P \in \mathbb{R}[X]$? Image continue d'un intervalle, donc intervalle. Non borné car limite infinie, selon degré. Tous les intervalles fermé (car extr atteint) sont atteints par des $a \pm X^2$ ou par X.
EXO : images des $P\left(\mathbb{R}^2\right)$ pour $P \in \mathbb{R}[X, Y]$? Image continue d'un connexe, donc intervalle. Non borné car limite infinie, selon degré. Mais peut-être ouvert : $X^2 + (XY + 1)^2$.

EG : poly de tchybychev T_n.
EXO : mq $-2\sum_{n \geq 1} T_n\left(\frac{a}{2}\right) T_n\left(\frac{b}{2}\right) = \ln|a - b|$ pour $a \neq b$ de module ≤ 2.

3 Divisibilité, généralité

division euclidienne : c'ets dire $K[X] = (B) \oplus K_{\deg B - 1}[X]$
EG : $(\cos\theta + X \sin\theta)^n$ par $X^2 + 1$? terme cst, on le trouve en passant dans $\mathbb{C}$
EG : $P - X \mid P^{\circ n} - X$: par réc et télescopage, il suffit de mq pour $n = 2$, or

$$P(P(X)) - P(X) = \sum_{i \geq 1} a_i \underbrace{\left(P^i - X^i\right)}_{\text{multiple de } P - X}$$, ce qu conclut.

division selon puissance croissante (renverser les roles deg/val) c'est dire $K[X] = (P) \oplus \left(X^{n+1}\right)$ où $P(0) \neq 0$

Faire avec A intègre (Z quoi) juste après : même démo. Il faut juste pour inverser le coef dom

EXO : soit P entier unitaire prenant quatre fois sur Z la valeur 12. Montrer que 25 n'edst pas atteint sur Z.

DEM : $P - 12$ a quatre racine distcintes, donc $P - 12 = Q \prod (X - a)$ avec $a, b, c, d \neq$. Si 25 attient, alors $Q \prod (X - a)$ atteint $25 - 12 = 13$ qui est premier, d'où quatre diviseurs distincts $\{X - a\} = \{\pm 1, \pm 13\}$, mais le produit de ces qautre divisues contient 13, ce qui est une contradction !

lemme : reste de P par $X - \lambda$ est $P(\lambda)$.

cor : $P(\lambda) = 0$ ssi $X - \lambda \mid P$.

$A \mid B \implies \deg A \leq \deg B$, sinon $B = 0$.

$\deg A \circ B = \deg A \deg B$, sinon B constant

divisibilité est un ordre sur les unitaires, quasi ordre sinon (être associée est l'égalité modulo un scalaire), donc ordre sur quotient.

idéaux de $K[X]$, $A \mid B \iff (B) \subset (A)$.

pgcd/ppcm –> représentants de inf et sup (on le prend unitaire)

caractérisation : $D = \bigwedge A_i$ ssi D divise tous les A_i et si tout diviseur commun aux A_i divise D, idem pour M.

Existence : le générateur unitaire de $\sum (A_i)$ est un pgcd et de $\bigcap A_i$ un ppcm.

Cor : Bézout (ave accent !)

$\sum_{\emptyset} = (0)$, donc $\text{pgcd}(\emptyset) = 0$ (cohérenta avec $0 = \max K[X]$

$\bigcap_{\emptyset} = (1)$, donc $\text{ppcm}(\emptyset) = 1$ (cohérenta avec $1 = \min K[X]$

prop usuelles : les même que pour Z (pour les démos on passe aux normalisés), croissance de $I \mapsto \bigwedge_I A_i$, décroissance de $A_i \mapsto \bigwedge_I A_i$, idem pour $\vee$, puis associativité, homogénéité, ppcm×pgcd=produit

Algo d'Euclide

algorithe de Horner :division de $\sum a_i X^i$ par $X - \lambda$: la relation $b_{n-1} - \lambda b_n = a_n$ se lit sur

$$\begin{array}{ccccccc} a_n & & a_{n-1} & & & a_0 & \\ \uparrow \times\lambda & \searrow^+ & \uparrow \times\lambda & \searrow^+ & & \uparrow \times\lambda & \searrow^+ \\ 0 & & b_{n-1} & & b_{n-2} & b_0 & P(\lambda) \end{array}$$

eg : $2X^3 - X^2 - 5X + 1$ par $X - 2$: $\begin{array}{cccccc} 2 & -1 & -5 & 1 & \\ & 2 & 3 & 1 & 3 \end{array}$, d'où quotient $= 2X^2 + 3X + 1$ et reste=3.

Mieux : donne changement de variables. Pour composer par $X - a$, on itère la division par $Y := X + a$: $P(X) = Y(Y(...+_{b_2}) + b_1) + b_0$, d'où $P(X - a) = b_0 + b_1 X + ...$ Exemple : si $P = 4X^3 - 7X^2 + 3X - 5$, on veut $P(X + 2)$: $\begin{array}{ccccc} 4 & -7 & 3 & 5 & \\ & 4 & 1 & 5 & 0 \\ & & 4 & 9 & 23 \\ & & & 4 & 17 \\ & & & & 4 \end{array}$, doù $P(X + 2) = 4X^3 + 17X^2 + 23X$.

On aurait aussi pu appliquer Taylor MacLaurin.

4 Irréductibilité

P irred si les diviseurs de P sont associés à 1 ou P, exlusivement (un nombre premier a deux diviseurs, 1 et lui-même), ie si P ne peut pas s'écrire comme produit de deux poly (tous deux) non constants

Ainisi, pas irréductible ssi $P = AB$ avec $1 \leq \deg A, \deg B < \deg P$ (ou si P constant !)

ex : poly de degré 1

si $\deg P = 2$ ou 3, P est irréd ssi pas de racine : mais généralis fausses.

$X^2 - 2$ sur Q ou R

X^2+1 sur R ou C

EXO X^n-2 irreduc sur Q.

rq : un polynôme de degré premier a le droit d'etre réductible : le deg du produit 'nest pas le produit des degés

Démo $P(\lambda)=0 \implies X-\lambda \mid P$: comme $X-\lambda$ est irréductible, le cas contraire signifierait $X-\lambda \wedge P=1$, d'où par Bézout $(X-\lambda)U+PV=1$, et évalué en λ on aurait $0=1$, pb...

décomposition, on tout démontrer avec ! $A\neq 0$ s'écrit $\lambda\prod P^{v_P}$ où P irred unitaire.

EXO : décompososer $X^{2n}-1$ sur R ?

5 Racines

fonction polynomiale (sans accent) $P\mapsto P(\cdot)$.

INjectfis si K infini, de noyay les multiples de $X^{|K|+1}-X$ sinon.

ordre (de multiplicité : à quel point λ est-elle multiple ?) de λ = valuation de $X-\lambda$

cor : $\sum \omega_\lambda \leq \deg$,

cor : nb racines $\leq$ deg

RQ : vrai sur anneau intègre. Cadre le plus général au sens de l'exo suivant :

EXO : *tout trinome au plus deux racines (donc ssi $\forall n$tout poly de degé n a au plus n racines) ssi* A nul, intègre, ou $Z/4$ ou $F_2\left[X^2\right]/X^2$.

DEM Supp $ab=0$ avec $a,b\neq 0$ Alors $X(X+a-b)$ s'annule en $0,-a,b$, d'où $a=-b$ et $a^2=0=b^2$, donc X^2 s'nulle en $a,b,0$ d'où $a=b$ et par conqséuqne $a^2=0=2a$. Alors ax racine de X^2 pour tout x, donc vaut 0 ou bien a. En choisissant $x\neq 0,a$, on exclut $ax=0$ (sinon même raisonnemnt que pour b mq $x=a$), donc $ax=a$, ie $a(x-1)=0$; en choissant deplus $x\neq 1$, on a $x-1=a$, ce qui montre $A\subset\{0,1,a,a+1\}$ et $|A|\leq 4$. rq $Z/c->A$, donc (Lgrange) $c$divse$|A|$.

Si $|A|=2,3$, alors A est un Z/p donc un corps, donc toujours intgère et on a toujours résultat sur racines, donc équivalence est triviale.

Si $|A|=1$, pas intègre, mais au plus une racine pour tout polyn, donc éuqivalence fausse.

Si $|A|=4$, alors car Adivise4. SI car $=4$, alors $A=Z/4$ –> regarder à la main, tout les trinome au plus deux racines. Si car $=2$, alors A est une F_2-alg et la surjection $Eval_a: F_2[X]\twoheadrightarrow A$ (surj car $a^2=0,1,a$,ou$a+1$) donne un iso $A=F_2[X]/P$ pour $P=X^2,X^2+1,X^2+X$,ouX^2+X+1. REgardons les poly :

$X^2+\lambda X+\mu$ $(\lambda,\mu\neq 0)$ évite 0 et λ

$X^2+(\mu\neq 0,1)$ évite 0 et 1

X^2+1 évite 0 et (a ou $a+1$)

X^2 évite 1 et $a$ou$a+1$

$X^2+\lambda X$ $(\lambda\neq 0,1)$ évite 1 et $\lambda+1$

AInsi, seul peut-être X^2+X a >2racines. Il en a déjà deux 0 et 1.

$a^2=0$: alors a et $a+1$ sont envoyé sur $a\neq 0$

$a^2=1$:alors a et $a+1$ sont envoyé sur $a+1\neq 0$

$a^2=a+1$ (cas intègre ! !) envoyé sur $1\neq 0$

$a^2=a$: alors a et $a+1$ sont envoyé sur 0,d'où problème.

$\forall i$, $(X-\lambda_i)^{\omega_i}\mid P\neq 0 \implies \prod(X-\lambda_i)^{\omega_i}\mid P$

notons α et β deux ordres : alors ordre dans AB est $\alpha+\beta$ et dans $A+B$ est $\geq \min\{\alpha,\beta\}$ avec $=$ si $\alpha\neq\beta$.

EXO *ESt-ce qye P scindé simple => $P+P(0)$ scindé simmple* ? Si oui, P ss => $P+C$ ss où C arbitrairemnt grand, or c'est faux pour parabole $x(x-1)$.

EXO : *si P scindé simple, montrer que pas deux ceof nul conscutifs. Si un coef est nul, il y a chgt de signe*

DEM : les dérivées sont aussi scindées simples, donc si trou de taille ≥ 2 en dérivant on obtient 0 racine double, absurde. Si il a pas de change de signe, dériver donne $\ldots+aX^2+b$ avec $ab>0$, d'où un minimul local >0, impossible vue les vriations d'un scindé simple

Fonctions symétriques élémentaires : méthode de Laurent Deproit pour montrer des inégalités ? ? ?

EXO. *Soit $n \geq 1$ un entier. Montrer qu'il n'y qu'un nombre fini de polynôme à coefficients dans Z dont toutes les racines sont dans le disque unité.*

DEM : Il suffit de borner la valeurs des coefficients puisque ces derniers prennent des valeurs entières. Or, ils s'expriment chacun comme un somme finie de produits de racines, donc sont majorées

COR (lemme de Kronecker) : *On considère un polynôme unitaire à coefficients entiers dont toutes les racines complexes sont dans le disque unité privé de 0. Montrer que ces dernières sont des racines de l'unité.* (On pourra montrer qu'il n'y a qu'un nombre fini de tels polynômes.)

DEm : d'après ce qui précède, l'ensemble $\mathcal{P}$ des polynômes considérés par l'énoncé. est fini. Fixons à présent un élément $P = \prod (X - \lambda_i)$ dans $\mathcal{P}$. Pour tout entier $n \geq 0$, le polynôme $P_n := \prod (X - \lambda_i^n)$ a pour coeffcients des fonctions symétriques en les λ_i, donc des polynômes entiers en les fonctions symétriques élémentaires des λ_i (lesquelles sont les coefficients de P), donc des entiers. Il en résulte que tous les P_n sont dans $\mathcal{P}$.

Par finitude de $\mathcal{P}$, il y a deux entiers $0 < a < b$ tels que $P_a = P_b$, d'où (en identifiant les racines) une permutation σ telle que $\lambda_i^b = \lambda_{\sigma(i)}^a$ pour tout i. En itérant Id^b et σ, on obtient pour tout i l'égalité $\lambda_i^{b^{\ell_i}} = \lambda_i^{a^{\ell_i}}$ où ℓ_i est la longueur du cycle de σ contenant i. Cela permet de conclure.

EXO *Calculer* $\prod \sin\left(\frac{k}{n}\pi\right)$. Tu commences par dire que c'est un nombre positif, donc tu le remplaces par son module. Ensuite tu dis que tu peux calculer le produit des $\left|2i \sin \frac{k\pi}{n}\right| = \left|1 - e^{-2\pi i \frac{k}{n}}\right|$ et ce produit c'est $P(1)$, pour $P = X^{n-1} + X^{n-2} + ... + X + 1$

EXO : *mq* $\prod_{k=1}^{n} \cot \frac{k\pi}{2n+1} = \frac{1}{\sqrt{2n+1}}$ *en considérant* $(X+1)^n - (X-1)^n$

Eq 4e degré : soit λ_i les 4 racines d'un polynoe P de deg 4. Le polynoe $S := \prod_{i<j} (X - \lambda_i - \lambda_j)$ est symétrique, donc polynôme en les coef de P. Si P n'a pas de coef en X^3, $\sum \lambda_i = 0$, donc chaque paire $\{\lambda_i, \lambda_j\}$ est matchée avec sa paire duale, donc S est pair, donc de degré 3 en X^2. Soit s une racine de S. Alors, en regropuant les racines de P deux à deux selon s, on peut factoriser $P = \left(X^2 + sX + \alpha\right)\left(X^2 - sX + \beta\right)$. Développer donne une équation du second degré satisfaitepar α et β (calcul que j'ai fait dans un post)

Lien avec méthode classique ? tuer X^3, puis translater X^2 pour factoriser carré ; cf message Joel

Méthode Lagrange : cf gourdon + notes historiques bourbaki + Dieudonné

Deg 3 : calcul du discrimaint page 79-80 gourdon

recherche de racine raionnelles

EXO : soit $P \in \mathbb{C}[X]$ tel tout rationnel est attien par un rationnnel. Montrer que $P \in \mathbb{Q}_1[X]$.

DEM : soit $r_i \in P^{-1}(i) \cap \mathbb{Q}$. Alors P vaut son lagrange en lesr_i, donc est à ceof rationnels. hyp-conclu invairant par $P \mapsto kP$, donc OPS $P \in Z[X]$.

Cherchons un rationne $\frac{1}{p}$ à atteindre pour une contraiction. SI $\frac{1}{p} = P\left(\frac{u}{v}\right)$, on a $v^n = p \sum a_i u^i v^{n-i}$. Alors p divise v^n, donc p, donc p^n divise v^n, donc (si $n \geq 2$) p divse$\sum a_i u^i v^{n-i} = a_n u^n + v()$, donc p diviser $a_n u^n$. Comme u, v étrangers, p ne peut diviser u, donc il divse a_n. Il suffit de contredire cela pour avoir $n \leq 1$.

Réciproquement, $n = 0$ est à rejeter.

RQ : montrer *tout polynôme complexe non constant est surjectif.*

DEM : $\forall \lambda$, $P - \lambda$ non constant donc s'annule

EXO : *quels polynômes complexes sont d'image $\subset \mathbb{R}$?* Si pas constant, doivent atteindre i, absurde. Donc constants réels.

EXO : *poly réel scindé à ceof dans ± 1 ? (regader $\sum \lambda^2 + \frac{1}{\lambda^2}$)*

DEM on peut chercher poly **unitaires**. on regarde les relations coef racines. La somem (bien def car 0 pas racine) est $\geq 2n$. De plus, $\sum \lambda^2 = \left(\sum \lambda\right)^2 - 2\sum \lambda\mu = 1 \pm 2 \in \{-1, 3\}$, donc vaut 3. De même, $X^n P\left(\frac{1}{X}\right)$ est coef dans ± 1 scndé de racine les $\frac{1}{\lambda}$, d'où $\sum \frac{1}{\lambda^2} = 3$. Ainsi la someme $6 \geq 2n$, d'où $n \leq 3$.

En deg 1, tout sceindé. En deg 2, scndé ssi $\Delta \geq 0$, ie $1 - 4c \geq 0$, ie ssi $c < 0$. En deg 3, il reste $X^3 \pm X^2 - X \pm 1$; mais on égalité dans la somme, donc $\lambda - \frac{1}{\lambda} = 0$, ie $\lambda = \pm 1$, d'où $\lambda \pm 1 - \lambda \pm 1 = 0$, ie les $\pm$ sont opposés. Alors $P = X^2(X + \lambda) - (X + \lambda) = (X + \lambda)\left(X^2 - 1\right)$.

6 Dérivation

commute avec fonctoins polyn
$\operatorname{Ker}\partial = K\left[X^{\operatorname{car} K}\right]$.
En car nulle, $\deg P' = \deg P - 1$ (si $P \neq 0$) et ∂ surj de noyau K, donc $\operatorname{Ker}\partial^n = K_{n-1}[X]$
En car p, eg $\left(X^p + 2\right)' = 0$.

dériver un produit : ok sur C^R par injectivité. Sinon linéiare, donc autant montrer tout de suite Leibniz
cor : dérivée compo

Taylor : donner la géénralisation : $A = \sum \frac{A^{(k)}(\lambda_k)}{k!}\left(X - \lambda_k\right)^k$ (FAUSSE!! tester sur degré 2)

RQ : base duale de (X^n) est donc $A \mapsto \frac{A^{(n)}(0)}{n!}$, et plus généralement de $\left(X - a_n\right)^n$ est $A \mapsto \frac{A^{(n)}(a_n)}{n!}$ (FAUSSE!! tester sur degré 2).

COR : caac des ordres des racines :
$\omega_\lambda = \min\left\{k \geq 0\ ;\ P^{(k)}(\lambda) \neq 0\right\}$, donc si un racine est d'ordre infini, le poly est nul.

Rant forum : Soit X et Y deux indéterminées, $a \in K$ et $P \in K[X]$ où K est un corps de caractéristique nulle.
La formule de Taylor (classique) affirme que : $P(X + a) = \sum \frac{P^{(k)}(a)}{k!}X^k$
On peut même dire que : $P(X + Y) = \sum \frac{P^{(k)}(Y)}{k!}X^k$
On peut en déduire que : $P(X + a) = \sum \frac{P^{(k)}(X)}{k!}a^k$
APP : si je prends P un pylonome de degré n, $\overrightarrow{a}$ $n + 1$des scalaires 2 à 2 distincts, alors la famille des $P(X + a_k)$ est une base de $R_n[X]$. (écrit des Mines PC 2008).
Preuve : P est de degré n, donc la famille des $\frac{P^{(k)}}{k!}$ est une base de $R_n[X]$ (degrés échelonnés en décroissant). La deuxième formule de Taylor dit que la matrice des coordonnées de la famille des $P(X + a_k)$ dans cette base est une matrice Van der Monde. Donc CQFD.

Lagrange : CNS pour l'écriture finale (existence par injec de $P \mapsto (P(a_i))$ de $K_n[X]$ dans K^{n+1}). Noter que base duale sont évalualtion. Pour une solution au pb d'interpolation sans condition de degré, rajouter un multiple de $\prod(X - a_i)$.
RQ : résoudre lagrange, c'est ccehr solution de ssytème de congruence$P = b_i \mod (X - a_i)$, qui a une solution par lemme chinois.
rq : Lagrange est la bijectivité du produit des évalulation en les poles, qui est clairment lininéaire injective, avec les bonnes dimension, ce qui conclut.
si $P = \prod(X - a_i)$, noter que que $P'(a_i) L_i = \frac{P}{X - a_i}$.
app : K fini $\implies K^K = K[X]$
EXO : *soit* $P \in \mathbb{C}[X]$ *tq* $P(\mathbb{N}) \subset \mathbb{Q}$. *Montre que* $P \in \mathbb{Q}[X]$. DEM : on interpole en des points entiers.
Faire mieux avec polynome d'Hermite : on rajoute les valeurs des dérivées aux poles : considérer $A \longmapsto \left(A^{(i)}(a_j)\right)$, on a les équivalences $A \in \operatorname{Ker} \iff \forall j, (X - a_j)^{\omega_j} \mid A \iff \prod(X - a_j)^{\omega_j} \mid A$, pb deg si $A \neq 0$.
Résoudre Hermite, c'est checher solution à ssytème de congruence$P = b_i \mod \left(X - a_i\right)^{n_i}$, qui a une solution par lemme chinois appliqué au $\left(X - a_i\right)^{n_i}$.
Inversion Vandermonde ? Soit $L = \operatorname{Mat}_{b.c.}(L_0, ..., L_n)$ où $L_i := \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}$. Puisque X^k coincient avec $\sum_{i=0}^n a_i^k L_i$ en chaque a_j, L est l'inverse du Vandermonde.

RQ dériver commute avec la translation $X \mapsto X - a$, donc on peut faire $a = 0$ dans certaines démo.
EXO : *ce sont en fait les seuls endo qui commuteny avec la dérivation* (DEM : $\varphi(X)' = \varphi(X') = \varphi(1) = 1$, donc $\varphi(X) = X - \lambda$, qui convient)

EXO : trouver les polynome A tq $A' \mid A$ (en carac nulle). Généraliser à $A'^m \mid A^n$.
DEM : on écrit $nA = PA'$ où $n := \deg A$ (en carac nulle, on a $\deg A' = \deg a - 1$) et où P affine unitaire, d'où en décrivant $nA' = A' + PA''$, ie $(n - 1) A' = PA''$, d'où (fois P) $n^{\downarrow 2} A = P^2 A''$. On recommence : $n^{\downarrow 2} A' = 2PA'' + P^2 A'''$, puis (fois P) $n^{\downarrow 2} nA = 2n^{\downarrow 2} A + P^3 A'''$, ie $n^{\downarrow 3} A = P^3 A'''$. Par rec, on déduit $n^{\downarrow n} A = P^n A^{(n)}$, d'où $A = P^n$. Finalament, A est de la forme $\left(X - \lambda\right)^n$.

implique $A' \mid A^n$. On décompose A en produit d'irred $A = \prod P_i^{a_i}$ Alors

$$A' = \sum P_i' \frac{A}{P_i} = \left(\prod P_i^{a_i - 1}\right) \sum a_i P_i' \prod_{j \neq i} P_j$$

Si P est un facteur irred de $\sum a_i P_i' \prod_{j \neq i} P_j \mid A' \mid A^n$, il en est un de A, donc un P_k, qui divise tous les $\prod_{j \neq i} P_j$ pour $i \neq k$, donc qui divise la différence $a_k P_k' \prod_{j \neq k} P_j$, d'où $P \mid P'$, impossible vu les degrés (P' est non nul car un irred est non cst).Finaleemnt, $A = A' \prod P_i$.

EXO : dans une algèbre, si $[a, b] = 1$, mq $[P(a), b] = P'(b)$ pour tout polynôme P.
DEM : par linéaire, on prend $P = X^n$. Puis exo classique (recurrence) evn 1

7 Changement corps de base

$K \hookrightarrow L \implies K[X] \hookrightarrow L[X]$
Si $\varphi \in \operatorname{Aut} K$, mettons $a \mapsto \overline{a}$, alors φ induit un auto de $K[X]$ donné par $\overline{\sum a_i X^i} = \sum \overline{a_i} X^i$.
Si φ stabilise une partie E, alors l'induit stablise $E[X]$.
Exmple : φ la conjugason complexe
On a $\overline{P(\lambda)} = \overline{P}\left(\overline{\lambda}\right)$, donc $\omega_\lambda = \omega_{\overline{\lambda}}$ **si** P**stable** et idem avec les dérivées.
Vital : dans $R[X]$, les racines complexe (non réelles) sont deux à deux conjuguées et ont même ordre de multiplicité.
App ; un poly réel ≥ 0 est somme de deux carrés.
EG : $X^2 - 2X\cos\theta + 1 = \left(X - e^{i\theta}\right)\left(X - e^{-i\theta}\right)$

EXO : *polynomes complexes qui stabilisent* $\mathbb{R}$? On a $P(x) = \overline{P(x)}$ pour tout réel x, donc $P - \overline{P}$ s'annul sur $\mathbb{R}$, donc est nul, donc P réel, ce qui suffit.

dvision conservé, pgcd et ppcm aussi, irréductibilité NON,

EXO *pour* $P \in R[X]$*, on a* P *stabilise* R^+ *ssi* $P = A^2 + XB^2$
DEM : les racines positives sont paries, donc P est produit de $X + a^2$ par $(X - \lambda)^2$ par $(X - b)^2 + c^2$; or $\left\{A^2 + XB^2\right\}$ stable par praoduit par bramaghuptha (générlaisr lagrange)

EXO (une racine hors du corps de base ne peut être trop multiple) *Si* $K \subset L$ *et* $P \in K[X]$ *alors toute racine hors de* K *est d'ordre* $\leq \frac{1}{2} \deg P$ *(en carc nulle)*
DEM : décomposons $P = \prod P_i^{a_i}$ et soit λ racine hors de K. λ est racine d'un P_i, et d'un seul (sinon les P_i ne serainet pas étragners), et est racine simple (sinon $P_i \wedge P_i' \neq 1$). Ainsi, l'ordre de λ dans P est exactement a_i. Mais $\deg P_i \geq 2$ sinon $\lambda \in k$,d'où $\deg P = \sum a_i \deg P_i \geq 2\omega_\lambda$, cQFD

8 Congruence modulo P, scission de polynômes, clôture algébrique

$K[X]/P$ algère de dim $\deg P$
corps ssi P irréd
COR : construire des corps finis $\mathbb{F}_4$
COR : tout polynôme admet un corps de décomposition

Regardons l'équation $P(x) = 0$: selon inconue (x ou P), on est amenée à deux def relative et une intrinsqè.
Une extention est dit ***algébrique*** *si tout élément ets solution d'une équati algébrique,* ***algébgriquement fermée***[3] *si tout équation algébiaue a une solution. Lorsque ces deux conditions sont réalisées, on parle de* ***clotûre algébrique*** (à penser comme extension algébrique maximale, ou algt fermée minimale).
UN corps est ***algbqt clos*** *(notion intrinsèque) s'il est algébriquement fermé dans lui-mêem, ou encore s'il est une cloture algébrique de lui-même.*

[3] les nombres définissables de manière algébrique restent dedans

Th (Steinitz) *tout corps admet une clôture algébrique.* (dem par ordinaux)

LEmmm *tout corps admet une extension* $k \overset{\text{alg.}}{\hookrightarrow} k^r$ *rompant tout poly de* $k[X]$.

Dem steinitz : en définissant une suite $K_{n+1} := (K_n)^r$ avec $K_0 := k$, l'extension $\bigcup_{n\in\mathbb{N}} K_n$ est algébrique (tout élément tombe dans un K_n qui est algérbique sur k) et algébriqement close (un polynôme à coef dedans a tous ses coef dans un même K_n, donc a une racine dans K_{n+1}), CQFD

Dem lemme (cas fini) : on énumère les poynômes de $k[X]$ en une suite $P_0, P_1, P_2...$ puis on rajoute des racines successivement. On défini $k_0 = k$ et pour $n \geq 1$ k_n =corps de rupture de P_n sur k_{n-1}. Alors $k \hookrightarrow \bigcup_{n\in\mathbb{N}} k_n$ est algèbrique et romp tout polynê de $k[X]$ (en effet, P_n a une racine dans k_n) : mais d'autres polynômes sont apparus

Dem lemme (Cas général) : exactement pareil, sauf que les poynôme de $k[X]$ ne sont plus forécément énumérables. Les ordinaux sont faits pour assoir cette intuition énumérative. Soit $(P_\alpha)_{\alpha<\alpha_0}$, on défini $k_0 = k$, k_σ =corps de rupture de P_σ sur $k_{\sigma-1}$, k_λ =corps de rupture de P_λ sur $\bigcup_{\alpha<\lambda} k_\alpha$. Alors $k \hookrightarrow \bigcup_{\alpha<\alpha_0} k_\alpha$ convient.

9 Clôture algébrique

10 Plusieurs variables

$P(a) = 0$ ssi $P \in (X_i - a_i)$ (réc ?)

Th schwarz et Taylor

poly homogènes : algèbres graduée, d'où $\deg AB = \deg A + \deg B$; en raiosnnant sur le monomes de plus haut degré partiel

TH Euler : P homo degre k ssi $\sum X_i \partial_i P = kP$.
=> regarder les monomes
<= notons $\delta := \sum X_i \partial_i$. On décompose $P = \sum P_i$, doù $\sum kP_i = kP = \delta P = \sum \delta P_i = \sum iP_i$, d'où égalité $\forall i$, donc $P = P_{\max}$.

David, 7 12 05, 18h16⟨⟩
Et maintenant ils s'imaginent en masse que si les F_i sont des polynômes homogènes et les P_i des polynômes tels que $\sum P_i F_i$ soit homogène, alors **forcément** les P_i sont homogènes.
(C'est vachement subtil, parce que si on dit à la place que les P_i peuvent être modifiés pour être homogènes tout en gardant la même valeur de $\sum P_i F_i$, ça devient correct, et c'est ce qu'il faut dire. Certains arrivent à rédiger de façon tellement byzantine qu'on ne sait plus ce qu'ils disent au juste, c'est peut-être l'un et peut-être l'autre.)

11 POur aller plus loin

dans $k[X]$, on peut utliser à la place de X n'importe quel "nb" ξ tq $\sum a_n \xi^n = 0 \implies (a_n) = 0$ (*transceandant*) car on a alors un iso $k[X] \cong k[\xi]$ tq $X \longleftrightarrow \xi$ (c'est la *propriété universelle* de l'algèbr edes polynômes)

transcendance :
le théorème de Gelfond-Schneider, démontré indépendamment et presque simultanément en 1934 par Aleksandr Gelfond et Theodor Schneider, s'énonce de la façon suivante :
Si α est un nombre algébrique différent de 0 et de 1 et si β, est un nombre algébrique irrationnel alors α^β, est un nombre transcendant.
Le théorème de Baker résoud la conjecture de Gelfond. Dû à Alan Baker dans une série d'articles intitulés Linear forms in the logarithms of algebraic numbers parue en 1966 et 1967 dans la revue Mathematika, c'est un résultat de transcendance sur les logarithmes de nombres algébriques, qui généralise à la fois le théorème d'Hermite-Lindemann (1882) (transcendance de e et π) et le théorème de Gelfond-Schneider (1934).
Th Baker : Soit $a_1, ..., a_n$ des nombres complexes $\mathbb{Q}$-libres dont les exponentielles sont algébriques sur $\mathbb{Q}$. Alors $1, a_1, ..., a_n$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$.

Exemple : le théorème de Baker permet de montrer la transcendance de nombres comme x log(2)+y log(3)+z log(5) pour tous nombres algébriques x, y, z non tous nuls.

Bézout entre $\mathbb{Z}$ et $\mathbb{Q}$

Joel, Fri, 2 Dec 2005 20 :03 :01

Sur un anneau A, deux polynômes P et Q admettent une relation du type $UP + VQ = 1$ si et seulement si l'idéal engendré par P et Q est tout. Autrement dit, si l'intersection des deux sous-schémas fermés $V(P) = \mathrm{Sp}\, A[T]/P$ et $V(Q) = \mathrm{Sp}\, A[T]/Q$ de la droite affine sur $\mathrm{Sp}\, A$ est vide.

Ici, $A = \mathbb{Z}$, il y a une relation de Bézout sur $\mathbb{Z}$ si et seulement s'il n'existe pas de corps k et d'élément x de k tel que $P(x) = Q(x) = 0$.

La conclusion, c'est que P et Q admettent une relation de Bézout sur $\mathbb{Z}$ si et seulement si P et Q sont premiers entre eux dans $\mathbb{Q}[X]$ et que pour tout nombre premier p, les réductions modulo p de P et Q sont premières entre elles dans $\mathbb{F}_p[X]$.