POLYNOMES

Soit K = ℝ ou ℂ

I) Polynômes à une indéterminée sur K

1) Définition

Définition: Un **polynôme P sur K (ou à coefficients dans K)** est une suite presque nulle d'éléments de K $(a_0, a_1, \ldots, a_p, 0, .., 0,..)$ où les $a_k \in K$ et sont nuls à partir d'un certain rang.

On munit l'ensemble des polynômes de l'addition + et de la loi externe . , restrictions de celles existant pour l'ensemble des suites.

Si $P = (a_0, .., a_p, 0,.., 0, ...)$ et $Q = (b_0, .., b_q, 0,.., 0, ...)$ sont deux polynômes, on définit P×Q, ou PQ, par : $PQ = (c_0, .., c_n, 0,.., 0, ...)$ où $\forall k \in \mathbb{N}$, $c_k = \sum_{j=0}^{k} a_{k-j}\ b_j$

Soit K[X] l'ensemble des polynômes à coefficients dans K. On vérifie aisément que **(K[X],+,×) est un anneau** (l'élément neutre de × étant $I = (1, 0, .. , 0 , ..)$) et qu'il stable par multiplication externe (on dira que (K[X], + , .) est un espace vectoriel sur K)

2) Notation définitive

On note $I = X^0$ et X le polynôme (0, 1, 0, 0, ..., 0, ...).

On vérifie, à l'aide du produit vu précédemment, que $\forall n \in \mathbb{N}$, $X^n = (0,..,0 , 1, 0, .., 0,..)$ où la suite débute par n 0 et ne possède qu'un 1.

Si $P = (a_0, .., a_p, 0,.., 0, ...)$, on a alors : $P = \sum_{k=0}^{+\infty} a_k\ X^k = \sum_{k=0}^{p} a_k\ X^k$

II) Degré d'un polynôme

Définition: Soit $P = \sum_{k=0}^{p} a_k\ X^k$ un polynôme non nul, on appelle **degré de P** le plus grand entier k tel que a_k soit différent de 0. On note deg(P) cet indice.

On convient que le degré du polynôme nul est $-\infty$.

Définition: Si P est un polynôme (non nul) de degré d, le **coefficient dominant** de P est par définition le coefficient du terme de plus haut degré i.e. a_d.

Définition: Un **polynôme unitaire** (ou normalisé) est un polynôme de coefficient dominant 1.

Proposition : Soit $(P,Q) \in (K[X])^2$.

(i) $\deg(P+Q) \leq \max(\deg(P),\deg(Q))$ (ii) $\deg(PQ) = \deg(P) + \deg(Q)$

Dem: **(i)** Si $\deg(P) \neq \deg(Q)$, $\deg(P+Q) = \max(\deg(P),\deg(Q))$
Si $\deg(P) = \deg(Q)$. Si les coefficients dominants ne sont pas opposés alors P+Q a le même degré, sinon il a un degré inférieur.
(ii) Dans la formule donnant les coefficients du produit, on voit que c_{p+q} est le produit des deux coefficients dominants (donc il est non nul). Pour k > p+q, l'un au moins des termes a_{k-j} ou b_j est nul dans la somme donc c_k est nul. Aussi deg(PQ) = p+q. (On prolonge cette formule dans le cas où un (ou les deux) polynôme P et Q est nul.

Proposition : Le produit de deux polynômes non nuls est non nul

Dem: On utilise la formule donnant le degré du produit de deux polynômes

Proposition : L'ensemble $K_n[X]$ des polynômes de degré inférieur ou égal à n est un sous-espace vectoriel de K[X] i.e. il est stable par combinaison linéaire

Dem: On vérifie aisément les stabilités

Définition: Soit $P = \sum_{k=0}^{p} a_k X^k$ et Q deux polynômes. On appelle **composé de P par Q** , le polynôme $P \circ Q = \sum_{k=0}^{p} a_k Q^k$

Proposition : Soit $(P, Q) \in (K[X])^2$ avec Q non constant. Alors $\deg(P \circ Q) = \deg(P) \times \deg(Q)$

Dem: Si P est constant, c'est le cas aussi de P o Q

Sinon, en notant p le degré de P, le degré de P o Q est celui de Q^p c'est-à-dire $p \times \deg(Q)$

III) Divisibilité dans K[X]

Divisibilité dans K[X]

Définition: Soit A et B deux polynômes de K[X].

On dit que B est un **multiple** de A $\Leftrightarrow \exists Q \in K[X] \mid B = AQ$.

Définition: Soit A un polynôme de K[X]. On dit que B $\in$K[K] est un **diviseur** de A $\Leftrightarrow$ A est un multiple de B.

0 étant multiple de tout polynôme, on l'écarte et on cherche si dans K[X] \ {0}, la relation A R B $\Leftrightarrow$ A divise B est une relation d'ordre.

$\rightarrow$ On a bien la réflexivité

$\rightarrow$ On a également la transitivité

$\rightarrow$ Par contre on n'a pas l'antisymétrie (par exemple P et 2P sont multiples l'un de l'autre)

Aussi en se restreignant aux polynômes unitaires, on a bien une relation d'ordre.

Définition: Deux polynômes P et Q sont **associés** $\Leftrightarrow \exists \alpha \in K^* \mid P = \alpha Q$

Division euclidienne dans K[X]

Théorème : Soit $(A,B) \in K[X]^2$, $B \neq 0$. Alors $\exists !(Q,R) \in K[X]^2$ tel que : $A = BQ + R$ et $\deg(R) < \deg(B)$. Q et R s'appellent respectivement les quotient et reste de la division euclidienne de A par B

Dem: **Existence** Soit $B \in K[X]$ non nul fixé. Soit la propriété de récurrence P_n : " $\forall P \in K[X]$ | $\deg(P) \leq n$, $\exists (Q,R) \in K[X]^2$ | $P = BQ + R$ et $\deg(R) < \deg(B)$. "

$\rightarrow$ P_0 est clairement vrai : il suffit, si B non constant, de prendre Q = 0 , et si B constant, $B = \alpha I$, de prendre $Q = (\alpha)^{-1} P$.

$\rightarrow$ Si P_n est vrai. Soit $P \in K[X]$ avec $\deg(P) \leq n + 1$. Si $\deg(P) \leq n$ on a bien le résultat

Si $\deg(P) = n+1$. Si $n+1 < \deg(B)$ alors on prend Q = 0, sinon, on considère $P_1 = P - ({}^a/_b)X^{n+1-\deg(B)} B$ avec a et b les coefficients dominants respectifs de P et B. On vérifie alors que $\deg(P_1) \leq n$ donc on peut lui appliquer l'hypothèse de récurrence et alors le reste R pour P est celui pour P_1 .

Unicité Si $\exists (Q,R)$ et (S,T) tels que $A = BQ + R = BS + T$. On a : $B(Q-S) = T-R$.

Or $\deg(T-R) < \deg(B)$. Donc d'après la formule donnant le degré d'un produit, on en déduit que T-R = 0 = Q-S. CQFD.

Algorithme de la division euclidienne

On utilise l'algorithme proposé par la démonstration : tant que le polynôme P est de degré supérieur au égal à celui de B, on ôte à P le polynôme $({}^a/_b)X^{\deg(P) - \deg(B)} B$: on obtient alors un polynôme qui est de degré strictement inférieur à celui de P. On réitère le procédé au nouveau polynôme jusqu'à obtenir un polynôme de degré strictement inférieur à deg(B). Ce dernier polynôme est alors le reste R. Q est la somme des monômes $({}^a/_b)X^{\deg(P) - \deg(B)}$. La disposition pratique est la même que la disposition pratique de la division euclidienne sur $\mathbb{Z}$.

Exemple : $2X^4 - X^3 + X^2 - X + 3 = (2X^2-3X)(X^2 + X + 2) + 5X + 3$

IV) Fonctions polynomiales

I Définition

Définition: Soit P un polynôme de K[X]. On note $P = \sum_{k=0}^{n} a_k X^k$. On appelle **fonction polynomiale** associée à P la fonction $f : \mathbb{R} \to \mathbb{R}$, $x \to a_0 + a_1x + a_2x^2 + ... + a_nx^n$

On notera souvent f sous la forme $\tilde{P}$ ou **par abus** P.

Définition: Une **équation algébrique** est une équation de la forme : (e) $\tilde{P}(x) = 0$

Définition: Une **solution (ou racine)** de (e) est appelée **zéro** de P.

Théorème : x_0 est un zéro de P $\Leftrightarrow$ $(X - x_0)$ divise P

Dem: Rappel : A divise P ssi le reste de la division euclidienne de P par A est nul.

On effectue donc la division euclidienne de P par $(X - x_0)$. On a : $P = (X - x_0)Q + R$ avec deg(R) ≤ 0 donc avec R constant. $X-x_0$ divise P $\Leftrightarrow$ R est nul $\Leftrightarrow$ $\tilde{R}(x_0) = 0 \Leftrightarrow \tilde{P}(x_0) = 0$

Définition: Soit x_0 un zéro de P. On dit que x_0 est **zéro d'ordre k** de P ssi P est divisible par $(X-x_0)^k$ mais pas par $(X-x_0)^{k+1}$.

Théorème : * Si $(x_0,x_1,...,x_n)$ sont des éléments de K différents. Alors si $(x_0,x_1,...,x_n)$ sont des zéros de P alors soit P est nul soit deg(P) ≥ n+1.

**** Si x_0 est un zéro de P d'ordre k alors deg(P) ≥ k**

***** Si x_0 d'ordre k et x_1 d'ordre m sont des zéros de P alors deg(P) ≥ k+m**

Dem: * On a $P = (X-x_0)Q_0$. x_1 est un zéro de P mais pas de $(X-x_0)$ donc c'est un zéro de Q_0 . D'où $P = (X-x_0)(X-x_1)Q_1$ et on réitère le procédé : $(X-x_0)(X-x_1)...(X-x_n)$ divise P. ** $P = (X-x_0)^kQ$ CQFD

*** $P =(X-x_0)^kQ$. Mais $(X-x_1)^m$ est premier avec $(X-x_0)^k$ et divise P, donc il divise Q : $P = (X-x_0)^k(X-x_1)^mQ_1$ ...

Corollaire : Si P et Q sont deux polynômes de K[X] de degré inférieur ou égal à n et dont les fonctions polynomiales associées coïncident en n+1 points différents alors P=Q

Dem: On applique le premier résultat du théorème au polynôme P – Q .

Caractèrisation d'un poynôme par sa fonction polynomiale

Soit φ : K[X] → F(K,K) , P → φ(P) = $\tilde{P}$.

Théorème : φ est une application injective

Dem: Soit P et Q deux poynômes ayant la même fonction polynomiale. Soit R = P – Q . Soit n un majorant des degrés de P et de Q. R s'annule en 0, 1, 2, …, n et donc en au moins n + 1 points distincts. Or deg(R) ≤ n, donc R est nul… et donc P = Q. Donc φ est injective.

On n'a pas surjectivité : la fonction sinus s'annule une infinité de fois mais n'est pas polynomiale.

Algorithme de Horner

Principe : On écrit $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ I = ((((($a_nX + a_{n-1}$) X + a_{n-2}) ... +a_0).

Intérêt algorithmique : Pour calculer P(x) directement il faut ((n-1) + (n-2) + ... +1) = $O(n^2)$ multiplications et n additions alors qu'avec l'algorithme d'Horner, il ne faut que n additions et n multiplications.

Utilisation pour calculer des valeurs en un point des fonctions polynomiales:

On écrit dans la première ligne d'un tableau les coefficients du polynôme dans l'ordre décroissant des degrés (on met éventuellement des 0 en l'absence d'un terme de degré k).

On prend la valeur du point considéré. Dans la première colonne on note le produit de cette valeur par le premier coefficient. Puis on ajoute le résultat au coefficient suivant qui l'on multiplie par la valeur du point considéré et on réitère le procédé. A la dernière colonne on ne calcule que la somme du dernier résultat obtenu et du coefficient.

Exemple : On veut la valeur en 3 de la fonction associée à $P = 2X^3 – 3X^2 + 4X – 5$

	2	-3	4	-5
3	3 ↓	3 ↓	13 ↓	34
	6 ↗	9 ↗	39 ↗	

Polynômes scindés

Définition: Soit $P \in K[X]$ de degré $n \geq 1$. On dit que P est **scindé sur K** ssi
$\exists (a_1,...,a_p) \in K^p, \exists (\alpha_1,...,\alpha_p) \in (\mathbb{N}^*)^p \mid \forall j \in \{1,..,p\}$, a_j zéro d'ordre α_j et $\alpha_1 + ... + \alpha_p = n$

$$\Leftrightarrow \exists (a_1,...,a_p) \in K^p, \exists (\alpha_1,...,\alpha_p) \in (\mathbb{N}^*)^p , \exists \lambda \in K^* \mid P(X) = \lambda \prod_{k=1}^{p} (X - a_k)^{\alpha_k}$$

Relations entre les coefficients et les racines d'un polynôme scindé

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme scindé , $a_n \neq 0$. On appelle $x_1, x_2, ..., x_n$ ses zéros où on a pris les zéros autant de fois que leur ordre de multiplicité.

On a : $P = a_n (X - x_1)(X - x_2) ... (X - x_n)$

$$= a_n \left(X^n - (x_1+...+x_n)X^{n-1} + ... + (-1)^k \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} x_{i_1} ... x_{i_k} X^{n-k} + ... + (-1)^n x_1 x_2 ... x_n \right)$$

Ainsi : $x_1 + x_2 + ... + x_n = -\frac{a_{n-1}}{a_n}$, $\sum_{1 \leq i < < j \leq n} x_i x_j = \frac{a_{n-2}}{a_n}$, ..., $\sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} x_{i_1} ... x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$ et

$x_1 . x_2 .. . x_n = (-1)^n \frac{a_0}{a_n}$

Exemple : Si $P = aX^2 + b X + c$ avec $a \neq 0$. Si x_1 et x_2 sont les deux racines (dans $\mathbb{C}$) on a

$x_1 + x_2 = -\frac{b}{a}$ et $x_1 . x_2 = \frac{c}{a}$

Exemple : Si $P = aX^3 + b X^2 + c X + d$ avec $a \neq 0$. Si x_1 , x_2 et x_3 sont les trois racines (dans $\mathbb{C}$) on a : $x_1 + x_2 + x_3 = -\frac{b}{a}$, $x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{c}{a}$ et $x_1 x_2 x_3 = -\frac{d}{a}$

Exemple : Si $P = aX^4 + b X^3 + c X^2 + d X + e$ avec $a \neq 0$. Si x_1 , x_2 , $x_3$et x_4 sont les quatre racines (dans $\mathbb{C}$) on a : $x_1 + x_2 + x_3 + x_4 = -\frac{b}{a}$, $x_1 x_2 x_3 x_4 = \frac{e}{a}$,

$x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4 = \frac{c}{a}$ et $x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 = -\frac{d}{a}$

Exercice : Soit (x,y,z) les trois racines de $X^3 + p X + q$ $(q \neq 0)$.

Déterminer : $S_2 = x^2 + y^2 + z^2$, $S_3 = x^3 + y^3 + z^3$ et $S_1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$

Réponse : $S_1 = -\frac{p}{q}$, $S_2 = -2p$ et $S_3 = -3q$

V Dérivation

Dérivation formelle

Définition: Soit $P = \sum_{k=0}^{n} a_k X^k$. Soit $\Delta(P) = P' = \sum_{k=0}^{n} k a_k X^{k-1}$ On l'appelle **polynôme dérivé** de P. On appelle **dérivation** l'application : $\Delta : K[X] \to K[X]$, $P \to \Delta(P)$

Remarque: Dans le cas où $K = \mathbb{R}$, la dérivation formelle correspond à la dérivation usuelle.

Propriété : (i) $\forall (P,Q)\in K[X]^2$, $\forall(\alpha,\beta)\in K[X]$, $\Delta(\alpha P + \beta Q) = \alpha\,\Delta(P) + \beta\,\Delta(Q)$
(ii) $\forall (P,Q)\in K[X]^2$, $\Delta(PQ) = \Delta(P)Q + P\Delta(Q)$
(iii) si $\deg(P) \geq 1$, $\deg(P') = \deg(P) - 1$, si $\deg(P)<1$, $P' = 0$

Dem: **(i)** Soit $(P,Q)\in K[X]^2$, $(\alpha,\beta)\in K^2$. Soit $n = \sup(\deg(P), \deg(Q))$. Quitte à rajouter des coefficients nuls, on a, en posant $P = \sum_{k=0}^{n} a_k X^k$ et $Q = \sum_{k=0}^{n} b_k X^k$: $\Delta(\alpha P+\beta Q) = \Delta\left(\sum_{k=0}^{n} (\alpha\, a_k + \beta\, b_k) X^k\right) =$

$\sum_{k=1}^{n} k(\alpha\, a_k + \beta\, b_k) X^{k-1} = \alpha \sum_{k=1}^{n} k\, a_k\, X^{k-1} + \beta \sum_{k=1}^{n} k\, b_k X^{k-1}$ Donc $\Delta(\alpha P+\beta Q) = \alpha\,\Delta(P) + \beta\,\Delta(Q)$

(ii) On reprend les notations du (i) : On a : $PQ = \Delta\left(\sum_{k=0}^{2n} \left(\sum_{i+j=k} a_i\, b_j\right) X^k\right) = \sum_{k=0}^{2n} \left(\sum_{i+j=k} a_i\, b_j\, (i+j) X^{i+j-1}\right) =$

$\sum_{k=0}^{2n} \left(\sum_{i+j=k} ((i\, a_i\, X^{i-1})\,(b_j X^j) + (a_i X^i)\,(j\, b_j\, X^{j-1}))\right) = \Delta(P)Q + P\Delta(Q)$

(iii) Provient directement de l'expression de $\Delta(P)$

Dérivations successives

$\Delta^2(P) = P''$, $\Delta^3(P) = P'''$,...., $\Delta^n = \Delta(\Delta^{n-1}(P)) = P^{(n)}$

Théorème : Formule de Leibniz $\Delta^n(PQ) = \sum_{k=0}^{n} C_n^k\, \Delta^k(P)\, \Delta^{n-k}(Q)$

Dem: On procède, comme en analyse, par récurrence sur n

Théorème : Formule de Taylor **Soit $a\in K$. Soit $P\in K[X]$ de degré $\deg(P) \leq N$. Alors**

$$P(a+X) = \sum_{k=0}^{N} \frac{P^{(k)}(a)}{k!} X^k \quad \text{ou} \quad P(X) = \sum_{k=0}^{N} \frac{P^{(k)}(a)}{k!} (X - a)^k$$

Dem: Soit $Q(X) = P(a+X)$. On a $\deg(Q) = \deg(P) \leq N$ donc, on peut écrire Q sous la forme $Q = \sum_{k=0}^{n} b_k X^k$
De plus, $\forall k\in\mathbb{N}$, $Q^{(k)}(0) = P^{(k)}(a)$. Or $Q^{(k)}(0) = k!\, b_k$. D'où le résultat

Corollaire : Si $P\in K[X]$ de degré n, $a \in K$ et $q\in\{0,..,n\}$. Alors :
a est un zéro d'ordre q de P ssi $P(a) = 0, P'(a) = 0, ..., P^{(q-1)}(a) = 0$ et $P^{(q)}(a) \neq 0$

Dem: $\Rightarrow$ Si a zéro d'ordre q de P, on a: $P = (X-a)^q R$ avec $R(a) \neq 0$. Par la formule de Leibniz, on sait que si $k \leq q-1$, $P^{(k)}(a) = 0$ et $P^{(q)}(a) = q!\, R(a) \neq 0$
$\Leftarrow$ Si $P(a) = 0, P'(a) = 0, ..., P^{(q-1)}(a) = 0$ et $P^{(q)}(a) \neq 0$, on a d'après la formule de Taylor,

$P(X) = \sum_{k=q}^{N} \frac{P^{(k)}(a)}{k!} (X - a)^k = (X-a)^q \sum_{k=q}^{N} \frac{P^{(k)}(a)}{k!} (X - a)^{k-q} = (X-a)^q R(X)$ avec $R(a) \neq 0$

VI Arithmétique des polynômes

Diviseurs communs de deux polynômes : Algorithme d'Euclide.

Théorème : Soit $(A,B) \in K[X]^2$ tel que $(A,B) \neq (0,0)$. L'ensemble des diviseurs communs de A et de B est l'ensemble des diviseurs d'un unique polynôme unitaire.

Définition: Ce polynôme est appelé **plus grand diviseur commun** de A et B et est noté **PGCD(A,B)** ou **$A \wedge B$**. On convient le PGCD(0,0) = 0 .

Dem: Quitte à échanger A et B, on peut supposer $\deg(A) \leq \deg(B)$. On note D(P) l'ensemble des diviseurs de P.

→ Si B=0, les diviseurs communs de A et de B sont ceux de A (car tout polynôme divise 0). L'ensemble D(A) est alors l'ensemble des diviseurs du polynôme unitaire associé à A.

→ Si $B \neq 0$. On effectue la division euclidienne de A par B : $A = BQ + R$ avec $\deg(R) < \deg(B)$. On vérifie que tout diviseur de A et de B divise R et que réciproquement tout diviseur commun de B et de R divise A. D'où $D(A) \cap D(B) = D(B) \cap D(R)$. On poursuit l'algorithme, appelé algorithme d'Euclide, tant que le reste obtenu est non nul.
On obtient : $D(A) \cap D(B) = D(B) \cap D(R) = D(R) \cap D(R_2) = \ldots = D(R_k) \cap D(R_{k+1})$. On aboutira nécessairement à un reste nul car la suite des degrés $\deg(R_k)$ est strictement décroissante.
On suppose alors que $R_k \neq 0$ et $R_{k+1} = 0$. On a alors $D(A) \cap D(B) = D(R_k)$. On prend alors le polynôme unitaire associé à R_k.

Exemple : $X^4 - 3X^2 - 4 = (X^3 + 2X^2 - X - 2)(X-2) + 2X^2 - 8$
$X^3 + 2X^2 - X - 2 = (X^2 - 4)(X+2) + 3X + 6$ et $X^2 - 4 = (X+2)(X-2)$
D'où : $(X^4 - 3X^2 - 4) \wedge (X^3 + 2X^2 - X - 2) = X + 2$

Polynômes premiers entre eux

Relation de Bézout: Soit $(A,B) \in K[X]^2$. Alors $\exists (U,V) \in K[X]^2$ tels que $A U + B V = A \wedge B$

Dem: Soit $D = A \wedge B$.On reprend l'algorithme d'Euclide mais à l'envers : on a $D = R_k = R_{k-2} - R_{k-1} Q_k$. Ainsi D est la somme d'un multiple de R_{k-2} et d'un multiple de R_{k-1} . On réitère le procédé et de proche en proche on montre que D est la somme d'un multiple de A et d'un multiple de B. A fortiori, tout multiple de D est la somme d'un multiple de A et d'un multiple de B.

Définition: On dit que deux polynômes A et B sont **premiers entre eux** si et seulement si leur PGCD est 1 (ou I).

Théorème de Bezout : Soit $(A,B) \in K[X]^2$. Alors A et B sont premiers entre eux si et seulement si $\exists (U,V) \in K[X]^2$ tels que $A U + B V = I$

Dem: On utilise le théorème précédent : A K[X] + B K[X] = K[X]...

Exemple : Les polynômes de Bezout associés à $A = X^3 + 1$ et $B = X^2 + 1$ sont
$(U,V) = ({}^1/_2(X+1) + (X^2+1)C , {}^1/_2(-X^2-X+1) - (X^3+1)C)$

Corollaire 1 : Lemme de Gauss : Si A divise un produit BC de deux polynômes et qu'il est premier avec l'un des facteurs, il divise l'autre : $(A \mid BC$ et $A \wedge B = I) \Rightarrow A \mid C$

Dem: D'après le théorème de Bezout, $\exists (U,V)$ tels que $I = A U + B V$.
D'où : $A U C + B V C = C$: A divise $A U C$ et $B V C$ donc divise la somme C.

Corollaire 2 : Si un polynôme est divisible par deux polynômes premiers entre eux alors il est divisible par leur produit : $(A|C , B|C$ et $A \wedge B = I) \Rightarrow AB|C$

Dem: D'après le théorème de Bezout, $\exists (U,V)$ tels que $I = A U + B V$.
D'où : $A U C + B V C = C$. Or $C = A C_1 = B C_2$. D'où $C = AB (UC_2 + VC_1)$

Corollaire 3 : Si P est premier avec A et B , il est premier avec AB.

Dem: On multiplie les deux égalités obtenues par le théorème de Bezout.

Exemple : Si un polynôme possède deux racines a et b, $a \neq b$, alors il est divisible par (X-a) et (X-b) qui sont premiers entre eux donc il est divisible par (X-a)(X-b)

PPCM de deux polynômes.

Théorème : Soit $(A,B) \in K[X]^2$ tel que ni A ni B n'est nul. L'ensemble des multiples communs de A et de B est l'ensemble des multiples d'un unique polynôme unitaire.

Définition: Ce polynôme est appelé **plus petit multiple commun** de A et B et est noté **PPCM(A,B)** ou **$A \vee B$**. On convient le PPCM(0,0) = 0 .

Dem: On pose D = PGCD(A,B), $A = D A_1$ et $B = D B_1$. Par définition du PGCD, B_1 et A_1 premiers entre eux. Soit alors P un multiple de A et de B. On écrit $P = A P_1 = B P_2$.
$A_1 \wedge B_1 = I \Rightarrow \exists (U,V) \mid I = A_1 U + B_1 V \Rightarrow P = A_1 U B P_2 + B_1 V A P_1 = A_1B (UP_2 + VP_1)$
car $A_1B = A B_1$. Aussi P est un multiple de A_1B
Réciproquement A_1B est un multiple de B et de A car $A_1B = A B_1$ avec $B = D B_1$. Il ne reste plus qu'à prendre le polynôme unitaire associé à $A_1 B$.

Remarque : On vient de montrer que le produit AB était un polynôme associé au produit du PGCD et du PPCM de A et de B.

PGCD d'un nombre fini de polynômes

Définition: Soit $(P_1, P_2, \ldots, P_n) \in K[X]^n$, n polynômes non tous nuls. On appelle **PGCD de $(P_1, P_2, \ldots, P_n)$** le polynôme unitaire de degré maximal de l'ensemble des diviseurs communs à $P_1, P_2, \ldots$ et P_n . On le note **$PGCD(P_1, P_2, \ldots, P_n)$.**

Remarque : Cet élément existe bien. En effet l'ensemble des degrés des polynômes unitaires diviseurs communs à $(P_1, P_2, \ldots, P_n)$ est une partie de $\mathbb{N}$, non vide (contient 0 = deg(I)), et majorée (par le maximum des degrés des P_k) : cette partie de $\mathbb{N}$ possède donc bien un plus grand élément.

Définition: Soit $(P_1, P_2, \ldots, P_n) \in K[X]^n$. On dit que **$(P_1, P_2, \ldots, P_n)$ sont premiers dans leur ensemble si $PGCD(P_1, P_2, \ldots, P_n) = I$.**

On dit que **$(P_1, P_2, \ldots, P_n)$ sont premiers deux à deux** si pour tout couple (i,j) avec $i \neq j$, $PGCD(P_i, P_j) = I$

Exemple : Les polynômes $X(X-1)$, $X(X+1)$ et $(X-1)(X+1)$ sont premiers dans leur ensemble mais pas premiers 2 à 2.

Relation de Bézout: Soit $(P_1, P_2, \ldots, P_n) \in K[X]^n$. Alors $\exists (U_1, U_2, \ldots, U_n) \in K[X]^n$ tels que $P_1 U_1 + P_2 U_2 + \ldots + P_n U_n = PGCD(P_1, P_2, \ldots, P_n)$

VII Polynômes irréductibles.

Définition: Un polynôme non constant est dit **irréductible** si ses seuls diviseurs sont les polynômes constants et les polynômes qui lui sont associés.

Théorème : Tout polynôme non constant possède au moins un diviseur irréductible.

Dem: Soit P un polynôme non constant. L'ensemble des degrés des diviseurs non constants de P est une partie non vide de $\mathbb{N}^*$ qui possède donc un plus petit élément n_0. Soit D_0 un diviseur de P de degré n_0. D_0 est nécessairement irréductible sinon il posséderait un diviseur non constant et de degré $< n_0$. CQFD

Théorème : Tout polynôme non constant est un produit de facteurs irréductibles. La décomposition est unique (si on prend les facteurs irréductibles unitaires).

Dem: Existence : Soit P un polynôme non constant. Soit D un de ses facteurs irréductibles. De deux choses l'une : soit P/D est constant (et c'est fini) soit il n'est pas constant et on écrit sa décomposition... (récurrence)

Unicité : Si $P = \alpha \prod_{k=1}^{n} D_k^{\alpha_k} = \beta \prod_{j=1}^{p} C_j^{\beta_j}$ D_k et C_j des polynômes irréductibles unitaires. Par comparaison des coefficients dominants, on a $\alpha = \beta$.
Quitte à prendre des puissances égales à 0 et à réordonner les produits, on peut écrire les décompositions avec les mêmes facteurs irréductibles : $P = \alpha \prod_{k=1}^{q} \pi_k^{\alpha_k} = \alpha \prod_{k=1}^{q} \pi_k^{\beta_k}$.
Considérons le facteur irréductible Π. On a $\Pi^{\alpha} A = \Pi^{\beta} B$ avec Π premier à A et à B. Si $\alpha<\beta$ alors $\Pi^{\alpha-B}A = B$ ce qui contredit B et Π premiers entre eux. De même avec $\beta<\alpha$. Aussi on a montré $\alpha=\beta$.

Théorème de D'Alembert-Gauss : Tout polynôme de degré n ≥1 sur ℂ est scindé.

Application à la recherche des polynômes irréductibles sur ℝ et sur ℂ

Théorème : (i) Les polynômes irréductibles sur ℂ sont les polynômes de degré 1
(ii) Les polynômes irréductibles sur ℝ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif

Dem: **(i)** ⇒ Les polynômes de degré 1 sont bien irréductibles sur ℂ
⇐ Soit P un polynôme sur ℂ de degré >1. D'après le théorème de D'Alembert-Gauss, P est divisible par un polynôme de degré 1 donc P n'est pas irréductible.
(ii) ⇒ Les polynômes de degré 1 sont irréductibles.
Si P est un polynôme de degré 2 de discriminant $\Delta<0$. P est irréductible sinon il serait divisible par un polynôme réel de degré 1 qui a une racine réelle ce qui est impossible car P n'a pas de racines réelles
⇐ Soit P un polynôme réel de degré > 1. Comme $P \in \mathbb{R}[X] \subset \mathbb{C}[X]$, P possède une racine $a \in \mathbb{C}$.

- Si $a \in \mathbb{R}$, alors $(X - a)$ divise P donc P non irréductible
- Si $a \in \mathbb{C}\setminus\mathbb{R}$. Alors $\overline{a}$ est aussi racine de P. Or $(X-a)$ et $(X-\overline{a})$ sont premiers entre eux, donc $(X-a)(X-\overline{a})$ divise P (dans $\mathbb{C}[X]$) . Mais $(X-a)(X-\overline{a})$ est réel, donc par unicité des quotient et reste de la division euclidienne de P par $(X-a)(X-\overline{a})$ dans $\mathbb{C}[X]$, le quotient de P par $(X-a)(X-\overline{a})$ est réel . Ainsi $(X-a)(X-\overline{a})$ divise P. Aussi, si P n'est pas de la forme $\lambda(X-a)(X-\overline{a})$, il n'est pas irréductible.

Exemple : La factorisation de $(X^n - 1)$ dans $\mathbb{C}[X]$ est :

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

Propriété : Soit P et Q deux polynômes de ℂ[X]. Alors P divise Q si et seulement si tous les zéros de P sont des zéros de Q et leurs ordres de multiplicité dans Q sont supérieurs à leurs ordres dans P.

Dem: Provient de la décomposition en facteurs irréductibles

VIII Interpolation de Lagrange

Théorème : Soit $(a_1, a_2, \ldots, a_n)$ n éléments distincts deux à deux de K, soit $(y_1, \ldots, y_n) \in K^n$. Alors il existe un unique polynôme P de $K_{n-1}[X]$ tel que : $\forall j \in [\![1, n]\!]$, $P(a_j) = y_j$

Dem: Existence. Pour $k\in[\![1, n]\!]$, on pose $P_k = \prod_{\substack{1\le j\le n\\ j\neq k}} \left(\frac{X - a_j}{a_k - a_j}\right)$. On vérifie aisément que : P_k est de degré $\le n-1$ et $\forall (k,j)\in[\![1, n]\!]^2$, $P_k(a_j) = \delta_{k,j}$ où $\delta_{k,j}$ est le symbole de Kronecker (vaut 1 si j = k, 0 sinon) .

Ainsi le polynôme $P = \sum_{k=1}^{n} y_k P_k$ est un polynôme de degré $\le n-1$ tel que $\forall j\in[\![1, n]\!]$, $P(a_j) = y_j$

Unicité. Si P et Q sont deux polynômes de degré $\le n-1$ tels que $\forall j\in[\![1, n]\!]$, $P(a_j) = y_j = Q(a_j)$
Alors $P - Q$ est un polynôme de degré $\le n-1$ ayant au moins n zéros distincts : donc P – Q est nul.

Remarque : Les polynômes P vérifiant $\forall j\in[\![1, n]\!]$, $P(a_j) = y_j$, sont de la forme $P = P_0 + U\prod_{k=1}^{n}(X - a_k)$ où U est un polynôme quelconque et P_0 est l'unique polynôme de degré $\le n-1$ solution du problème.

Exercice : Trouver tous les polynômes vérifiant : P(– 1) = 1 , P(0) = 1, P(1) = 2 et P(2) = 4

FRACTIONS RATIONNELLES

I) Définition

Définition: Une **fraction rationnelle sur K** est un quotient $\frac{P}{Q}$ où P et Q sont deux polynômes à coefficients dans K et Q non nul.

Egalité de deux fractions rationnelles

Définition: Les deux fractions rationnelles $\frac{P_1}{Q_1}$ et $\frac{P_2}{Q_2}$ sont **égales** ssi $P_1 Q_2 = P_2 Q_1$

Somme de deux fractions rationnelles

Définition: On définit **l'addition** par : $\frac{P_1}{Q_1} + \frac{P_2}{Q_2} = \frac{P_1 Q_2 + P_2 Q_1}{Q_1 Q_2}$

Produit de deux fractions rationnelles

Définition: On définit la **multiplication** par : $\frac{P_1}{Q_1} \times \frac{P_2}{Q_2} = \frac{P_1 P_2}{Q_1 Q_2}$

Propriété admise : L'ensemble K(X) des fractions rationnelles sur K est un corps pour les opérations définies ci-dessus

Forme irréductible d'une fraction rationnelle

Propriété: Pour toute fraction R de K(X), il existe un unique couple (P_0, Q_0) de polynômes avec Q_0 unitaire et P_0 et Q_0 premiers entre eux tel que $R = \frac{P_0}{Q_0}$.

De plus pour toute autre représentation de R sous la forme $\frac{P}{Q}$ on aura l'existence d'un polynôme T tel que $P = T P_0$ et $Q = T Q_0$

Dem: Si R est une fraction rationnelle, en divisant le numérateur et le dénominateur par leur PGCD et le coefficient dominant du dénominateur, on trouve une expression de la forme $\frac{P_0}{Q_0}$ voulue.

Pour toute autre représentation de R sous la forme $\frac{P}{Q}$, l'égalité : (1) : $P_0 Q = Q_0 P$ et le théorème de Gauss permet d'affirmer que P est un multiple de P_0. On a alors $P = T P_0$ avec un certain polynôme T.
En remplaçant dans l'égalité (1), on a aussi $Q = T Q_0$
Ce résultat prouve alors l'unicité du couple (P_0, Q_0) car alors P et Q sont premiers entre eux sssi T est un polynôme constant non nul, et Q est unitaire ssi T est unitaire.

Définition: On appelle cette représentation de R sous la forme $R = \frac{P_0}{Q_0}$ avec P_0 et Q_0 premiers entre eux et Q_0 unitaire la **forme irréductible** de R

Degré d'une fraction rationnelle

Définition: Soit R une fraction rationnelle de forme irréductible $R = \frac{P_0}{Q_0}$. On appelle **degré de R** l'entier relatif : $\deg(R) = \deg(P_0) - \deg(Q_0)$

Remarque : Si R est une fraction dont une représentation est $\frac{P}{Q}$ alors $\deg(R) = \deg(P) - \deg(Q)$

Exercice : Montrer : $\deg(R_1 R_2) = \deg(R_1) + \deg(R_2)$ et $\deg(R_1 + R_2) \leq \max(\deg(R_1), \deg(R_2))$

II) Fonction rationnelle

Définition: Soit R une fraction rationnelle de forme irréductible $R = \frac{P_0}{Q_0}$. On appelle **fonction rationnelle** associée à R la fonction : $K \setminus E \to K$, $x \to \frac{P_0(x)}{Q_0(x)}$ avec E ensemble des zéros de Q_0

Zéro d'une fraction rationnelle

Définition: Soit R de forme irréductible $R = \frac{P_0}{Q_0}$. On appelle **zéro** de R, tout zéro de P_0. Si α est un zéro de R, son ordre de multiplicité est l'ordre de multiplicité qu'il possède en tant que zéro de P_0

Pole d'une fraction rationnelle

Définition: Soit R de forme irréductible $R = \frac{P_0}{Q_0}$. On appelle **pole** de R, tout zéro de Q_0. Si α est un pole de R, son ordre de multiplicité est l'ordre de multiplicité qu'il possède en tant que zéro de Q_0

Exemple : Si $R = \frac{(X-1)^3 (X+2)^2}{(X+2)(X-1)^4}$ 1 est un pole d'ordre 1 et – 2 est un zéro d'ordre 1

III) Etude locale d'une fraction rationnelle

Partie entière d'une fraction rationnelle

Définition: Soit R une fraction rationnelle de forme irréductible $R = \frac{P_0}{Q_0}$. On appelle **partie entière** de R, le quotient de la division euclidienne de P_0 par Q_0.

Remarque : La partie entière de R est l'unique polynôme E tel que R – E soit une fraction rationnelle de degré strictement négatif

Partie polaire d'une fraction rationnelle relative à un pôle donné

Propriété: Soit R une fraction rationnelle de forme irréductible $R = \frac{P_0}{Q_0}$. Soit α un pôle de R d'ordre m. Alors il existe un unique polynôme P_α vérifiant : $\deg(P_\alpha) < m$ et $R - \frac{P_\alpha}{(X-\alpha)^m}$ est une fraction rationnelle n'ayant plus α pour pôle

Définition: On appelle **partie polaire relative au pôle α** de R, la fraction $\frac{P_\alpha}{(X-\alpha)^m}$

Dem: Admis

Remarque : En décomposant P_α à l'aide des $(X-\alpha)^k$ avec $0 \le k \le m-1$ (cf. Taylor) , on pourra écrire la partie polaire relative au pôle α sous la forme : $\sum_{k=1}^{m} \frac{A_k}{(X-\alpha)^k}$ avec A_k constantes

Décomposition en éléments simples sur $\mathbb{C}$

Théorème: Soit R une fraction rationnelle sur $\mathbb{C}$. Alors R est la somme de sa partie entière et de toutes ses parties polaires

Dem: La différence de R et de la somme de toutes ses parties polaires est une fraction n'ayant aucun pole parmi ceux de R ni parmi les autres complexes qui ne sont ni pôle de R ni pôle des parties polaires de R.
Ainsi cette fraction est une fraction sans pôle sur $\mathbb{C}$. Donc c'est un polynôme T. Mais alors R – T est une somme de parties polaires donc est une fraction de degré strictement négatif. Ainsi T est la partie entière de R

Définition: On appelle **élément simple sur K** toute fraction rationnelle de la forme : $\frac{P}{Q^k}$ avec Q un polynôme unitaire irréductible, k un entier naturel non nul et P un polynôme de degré $\deg(P) < \deg(Q)$

Théorème: Soit R une fraction rationnelle sur $\mathbb{C}$. Alors R s'écrit de manière unique comme somme d'éléments simples et d'un polynôme

Dem: L'écriture de R sous forme de somme de sa partie entière et de ses parties polaires fournit une DES.
Si on avait une autre écriture, les pôles des différents éléments sont nécessairement ceux de R. De plus en regroupant tous les éléments simples ayant le même pôle a, on trouve une fraction de pôle a de degré strictement négatif et tel qu'en lui retranchant R on obtient une fraction n'ayant plus a pour pôle : ainsi le regroupement de tous les éléments simples ayant le même pôle a fournit la partie polaire de R relative au pôle a.
On termine la démonstration en constatant que R débarrassée de tous les éléments simples donne un polynôme T tel que R – T soit une fraction de degré strictement négatif.

Remarque : Toute fraction rationnelle sur $\mathbb{R}$ admet également une unique DES sur $\mathbb{R}$ que l'on obtient en regroupant les parties polaires de la décomposition sur $\mathbb{C}$ correspondant à des pôles conjugués

Pratique de la décomposition en éléments simples

On considère une fraction $R = \frac{P_0}{Q_0}$ où on prendra soin de décomposer Q_0 en produit de facteurs irréductibles.

1) On commence par déterminer la partie entière E de R. On obtient alors un polynôme S de degré strictement inférieur à celui de Q_0 vérifiant : $R = E + \frac{S}{Q_0}$

2) Si α est un pôle d'ordre m. On écrit $Q_0 = (X - \alpha)^m T$ avec T un polynôme ne s'annulant pas en α. La partie polaire associée au pôle α de R s'écrit sous la forme : $\sum_{k=1}^{m} \frac{A_k}{(X-\alpha)^k}$ avec A_k constantes.

On multiplie la fraction R par $(X - \alpha)^m$: on obtient : $(X - \alpha)^m R = \frac{P_0}{T} = \sum_{k=1}^{m} A_k (X-\alpha)^{m-k} + (X-\alpha)^m L$

où L est une fraction n'ayant pas α pour pôle . En prenant la valeur en α , on obtient : $A_m = \frac{P_0(\alpha)}{T(\alpha)}$

Remarque 1 : Si le pôle est simple, on a : $Q_0 = (X - \alpha) T$ et donc $T(\alpha) = Q'_0(\alpha)$

Remarque 2 : $R = E + \frac{S}{Q_0}$ donc les parties polaires de R sont les mêmes que celles de $\frac{S}{Q_0}$. Donc le travail précédent peut être fait avec S plutôt qu'avec P.

3) Pour les coefficients qui resteraient à déterminer, on prend des valeurs particulières simples qui ne sont pas des pôles (0, 1, i, .., et aussi "+ ∞")

Exemple : $\frac{4X^3 - 7X^2 + 3X + 2}{(X-1)^2 X (X+1)} = \frac{1}{(X-1)^2} - \frac{1}{X-1} + \frac{2}{X} + \frac{3}{X+1}$

Exemple : Si P est un polynôme scindé dont les n zéros α_k sont d'ordre m_k alors la décomposition en éléments simples de $\frac{P'}{P}$ est $\frac{P'}{P} = \sum_{k=1}^{n} \frac{m_k}{X - \alpha_k}$