

POLYNOMES

PLAN

I : Présentation des polynômes

- 1) Définition
- 2) Lois sur $\mathbb{K}[X]$
- 3) Division euclidienne

II : Zéros d'un polynôme

- 1) Définition
- 2) L'algorithme de Horner
- 3) Polynôme dérivé
- 4) Ordre de multiplicité d'une racine
- 5) Polynôme scindé, relations coefficients–racines
- 6) Théorème de d'Alembert
- 7) Fractions rationnelles
 - a) Définition
 - b) Partie entière
 - c) Partie polaire
 - d) Décomposition d'une fraction rationnelle

Annexe : Nombres algébriques, nombres transcendants, quadrature du cercle

I : *Présentation des polynômes*

1– Définition

On se place sur un corps commutatif \mathbb{K} . Un polynôme (formel) est défini par la donnée de ses coefficients a_0, \dots, a_n éléments de \mathbb{K} . X étant une lettre muette, on note $P(X) = a_0 + a_1X + \dots + a_nX^n$ ou $\sum_{k \geq 0} a_k X^k$, étant entendu que la somme ne comporte qu'un nombre fini de a_k non nuls.

On distingue parfois le polynôme $P(X)$ (qui, par construction, est nul si et seulement si tous ses coefficients sont nuls (*)) de la fonction polynomiale associée :

$$P : \mathbb{K} \rightarrow \mathbb{K}$$

$$x \mapsto a_0 + a_1x + \dots + a_nx^n = P(x)$$

Celle-ci est nulle si et seulement si : $\forall x \in \mathbb{K}, P(x) = 0$ (**)

D'ailleurs, on peut fort bien faire jouer à X d'autres rôles que des valeurs dans \mathbb{K} . X peut aussi être remplacé par exemple par une matrice, ou un endomorphisme d'un espace vectoriel sur \mathbb{K} .

On a bien évidemment l'implication :

$$P(X) = 0 \Rightarrow \forall x \in \mathbb{K}, P(x) = 0.$$

Mais la réciproque est loin d'être évidente. Nous allons montrer que, lorsque \mathbb{K} est égal à \mathbb{R} ou \mathbb{C} , il y a équivalence, ce qui permet de confondre polynôme et fonction polynomiale. La phrase $P = 0$ gardera cependant de préférence le sens (*).

PROPOSITION

i) Soit P un polynôme à coefficients dans \mathbb{R} ou \mathbb{C} . Alors, si la fonction polynomiale associée à P est identiquement nulle, P a tous ses coefficients nuls.

ii) Soient P et Q deux polynômes dans \mathbb{R} ou \mathbb{C} . Alors, si les fonctions polynomiales associées sont égales (prennent les mêmes valeurs), les deux polynômes sont égaux (ont leurs coefficients égaux).

Démonstration :

i) \mathbb{K} contenant \mathbb{R} , nous supposons que la variable x ne prend que des valeurs dans \mathbb{R} . Soit $P = \sum_{k \geq 0} a_k X^k$ tel que $\forall x \in \mathbb{R}, P(x) = 0$.

Alors, pour $x = 0$, on obtient $a_0 = 0$. Donc :

$$\forall x \in \mathbb{R}, a_1 x + \dots + a_n x^n = 0$$

$$\Rightarrow \forall x \neq 0, a_1 + \dots + a_n x^{n-1} = 0.$$

On ne peut plus prendre $x = 0$, cependant, on peut prendre la limite lorsque x tend vers 0, ce qui donne $a_1 = 0$. etc...

ii) se prouve en appliquant i) à $P-Q$

Si $P \neq 0$, on appelle degré de P le maximum des k tels que $a_k \neq 0$. Si $P = 0$, on pose $\text{deg}(P) = -\infty$. Cette convention a été choisie de façon à rendre cohérents certains résultats et est compatible avec d'autres conventions telles $\text{Inf } \emptyset = +\infty$ et $\text{Sup } \emptyset = -\infty$.

Si P est de degré n , $a_n X^n$ est le terme (ou monôme) dominant. Si $a_n = 1$, le polynôme est dit unitaire ou normalisé.

On note $\mathbb{K}[X]$ l'ensemble des polynômes sur le corps \mathbb{K} .

2- Lois sur $\mathbb{K}[X]$

On peut définir sur $\mathbb{K}[X]$

a) Une somme :

$$\text{Si } P = \sum_{k \geq 0} a_k X^k \text{ et } Q = \sum_{k \geq 0} b_k X^k, \text{ alors } P+Q = \sum_{k \geq 0} (a_k + b_k) X^k$$

On vérifie facilement que $(\mathbb{K}[X], +)$ est un groupe commutatif. Le neutre est le polynôme nul, et

$$-P = \sum_{k \geq 0} -a_k X^k$$

$\text{deg}(P+Q) \leq \text{Max}(\text{deg}(P), \text{deg}(Q))$ avec égalité si les polynômes sont de degrés différents, ou s'ils sont de même degré et que les termes de plus haut degré ne s'éliminent pas.

b) Un produit interne :

$$\text{Si } P = \sum_{k \geq 0} a_k X^k \text{ et } Q = \sum_{k \geq 0} b_k X^k, \text{ alors } PQ = \sum_{k \geq 0} \sum_{i=0}^k a_i b_{k-i} X^k$$

On vérifie facilement que $(\mathbb{K}[X], +, \times)$ est un anneau commutatif (l'élément neutre pour le produit est le polynôme 1). Les éléments inversibles sont les polynômes constants non nuls.

Si $PQ = 0$ alors $P = 0$ ou $Q = 0$. On dit que l'anneau est intègre.

c) Produit par un scalaire (produit externe) :

$$\text{Si } P = \sum_{k \geq 0} a_k X^k, \text{ alors } \lambda P = \sum_{k \geq 0} \lambda a_k X^k$$

On vérifie facilement que $(\mathbb{K}[X], +, \cdot)$ est un espace vectoriel sur \mathbb{K} .

On note $\mathbb{K}_n[X] = \{P \in \mathbb{K}[X] \mid \deg(P) \leq n\}$. $\mathbb{K}_n[X]$ est un sous-espace vectoriel de $\mathbb{K}[X]$ dont une base est $(1, X, \dots, X^n)$, de dimension $n+1$.

Montrons le résultat suivant :

Soit $(P_n)_{n \in \mathbb{N}}$ une famille de polynômes telle que P_n soit de degré n . Alors, pour tout n , (P_0, P_1, \dots, P_n) forme une base de $\mathbb{K}_n[X]$.

Démonstration :

En raisonnant sur les termes de plus haut degré d'une combinaison linéaire nulle, il n'est pas difficile de montrer que la famille (P_0, P_1, \dots, P_n) est libre. Comme elle comporte $n+1$ éléments et que $\mathbb{K}_n[X]$ est de dimension $n+1$, il s'agit d'une base de $\mathbb{K}_n[X]$.

Soit (P_0, \dots, P_n) telle que le coefficient non nul de plus bas degré de P_i soit de degré i et $\deg P_i \leq n$. Alors cette famille forme une base de $\mathbb{K}_n[X]$.

Comportant $n+1$ éléments, et $n+1$ étant la dimension de $\mathbb{K}_n[X]$, il suffit de montrer que la famille est libre, ce qui se fait en raisonnant sur les termes de plus bas degré d'une combinaison linéaire nulle.

3- Division euclidienne

ou division suivant les puissances décroissantes :

Donnons un exemple :

$$\begin{array}{r|l}
2X^4 + X^3 - X^2 + X + 1 & 2X^2 - X - 2 \\
2X^4 - X^3 - 2X^2 & \hline
\hline
2X^3 + X^2 + X + 1 & X^2 + X + 1 \\
2X^3 - X^2 - 2X & \\
\hline
2X^2 + 3X + 1 & \\
2X^2 - X - 2 & \\
\hline
4X + 3 &
\end{array}$$

Nous affirmons alors que :

$$\underbrace{2X^4 + X^3 - X^2 + X + 1}_{\text{Dividende}} = \underbrace{(2X^2 - X - 2)}_{\text{Diviseur}} \underbrace{(X^2 + X + 1)}_{\text{Quotient}} + \underbrace{4X + 3}_{\text{Reste}}$$

Ce résultat est général :

DIVISION EUCLIDIENNE :

Soient A et B deux polynômes tel que B ≠ 0. Alors il existe un unique couple (Q,R) tels que :

$$A = BQ + R, \text{ deg}(R) < \text{deg}(B)$$

Q est le quotient, R est le reste.

Lorsque le reste est nul, on dit que B divise A. Un polynôme qui n'est divisible que par lui-même (à une constante multiplicative près) ou par les constantes est dit irréductible. Par exemple, X - 3 dans C, ou X² + 1 dans R.

On notera l'analogie dans l'énoncé avec la division euclidienne dans Z. Les démonstrations, en ce qui concerne l'unicité, sont également analogues.

Démonstration :

Montrons l'unicité :

Si A = BQ+R = BQ'+R' avec deg(R) < deg(B) et deg(R') < deg(B), on a B(Q-Q') = R'-R, avec deg(B(Q-Q')) = deg(B) + deg(Q-Q') et deg(R-R') ≤ Max(deg(R),deg(R')) < deg(B).

Il ne peut y avoir égalité que si Q-Q' = 0 et alors R-R' = 0

Montrons l'existence. Pour cela, nous donneront un algorithme fournissant les valeurs de Q et R.

C'est la généralisation de celui qui a été donné en exemple. Soit A = ∑_{k≥0} a_kX^k et B = ∑_{k≥0} b_kX^k, avec

deg(B) = n et b_n ≠ 0. L'algorithme est le suivant

Q := 0 { valeur initiale du quotient : 0 }

R := A { valeur initiale du reste : A. On appellera r_p le coefficient du terme de plus haut

degré de R de degré p. On a : A = BQ + R }

Tant que deg(R) ≥ deg(B) faire

$$Q := Q + \frac{r_p}{b_n} X^{p-n}$$

$$\{ A = BQ + R - B * \frac{r_p}{b_n} X^{p-n} \}$$

$$R := R - B * \frac{r_p}{b_n} X^{p-n}$$

$$\{ A = BQ + R \text{ et } \deg(R) \text{ a diminué} \}$$

fin tant que

Le prédicat $A = BQ + R$ est conservé après chaque boucle. Il sera donc toujours vérifié à l'issue de l'itération. Celle-ci se termine certainement, puisque $\deg(R)$ décroît strictement. Il deviendra donc nécessairement inférieur à $\deg(B)$.

Si $R = 0$, de sorte que $A = BQ$, on dit que B divise A , ou que A est un multiple de B .

II : Zéros d'un polynôme

1- Définition

On dit que a , élément de \mathbb{K} , est un zéro ou une racine du polynôme P si a annule la fonction polynomiale associée à P , c'est-à-dire si $P(a) = 0$. On a alors le résultat suivant :

PROPOSITION :

a est un zéro de P si et seulement si P est divisible par $X - a$.

Démonstration :

Si P est divisible par $X - a$, alors il existe Q tel que $P(X) = (X - a)Q(X)$. On a alors $P(a) = 0$.

Réciproquement, si $P(a) = 0$, considérons la division euclidienne de P par $X - a$. On a :

$P(X) = (X - a)Q(X) + R(X)$ avec $\deg(R) < \deg(X - a) = 1$, donc R est une constante. On obtient alors $0 = P(a) = R(a) = R$ donc $R = 0$ et P est divisible par $X - a$.

Une autre démonstration consiste à écrire que, si $P(X) = \sum_{k \geq 0} a_k X^k$, et si $P(a) = 0$ alors :

$$P(X) - P(a) = \sum_{k \geq 0} a_k (X^k - a^k)$$

dont chaque terme se factorise par $X - a$.

Il se peut que P se factorise par une puissance de $X - a$. Si k est la puissance maximale de $X - a$ par laquelle le polynôme P se factorise (de sorte que $P = (X - a)^k Q$ avec $Q(a) \neq 0$), on dit que k est l'ordre de multiplicité de la racine a .

2- L'algorithme de Horner

Début de partie réservée aux MPSI

Soit a un scalaire et $P = \sum_{k=0}^n \lambda_k X^k$ un polynôme. La programmation par la méthode de Horner du

calcul de $P(a) = \sum_{k=0}^n \lambda_k a^k$ consiste à écrire :

$$P(X) = (((...((a_n X + a_{n-1})X + a_{n-2})X + \dots)X + a_1)X + a_0.$$

L'algorithme est le suivant, en notant p la variable dont la valeur finale sera $P(a)$:

$p := \lambda_n$ { valeur initiale de p }
 Pour i décroissant de $n-1$ à 0 faire
 { au début de la boucle, $p = \lambda_n a^{n-i-1} + \lambda_{n-1} a^{n-i-2} + \dots + \lambda_{i+1}$ }
 $P := P * a + \lambda_i$
 { $P = \lambda_n a^{n-i} + \lambda_{n-1} a^{n-i-1} + \dots + \lambda_i$ }

A l'issue de la boucle, on a bien le résultat cherché. L'intérêt de l'algorithme de Horner réside en fait dans sa rapidité. Le calcul de produit est très coûteux en machine (et encore plus s'il s'agit de matrices et non de réels), et l'algorithme de Horner n'utilise que n produits, alors que la méthode usuelle en utilise $\frac{n(n+1)}{2}$.

De plus, les valeurs successives prises par p au cours du calcul ne sont autres que les coefficients du polynôme Q , quotient de P par $X - a$, la valeur finale de p étant $P(a) = R$ reste de cette division. En effet, si on indice les valeurs de p par les valeurs de l'indice de boucle i , on a :

$$p_n = \lambda_n$$

$$\forall i \in \{0, \dots, n-1\}, p_i = p_{i+1}a + \lambda_i$$

Si on pose $Q = p_n X^{n-1} + \dots + p_1$ et $R = p_0$, on constatera que les relations vérifiées par les p_i sont précisément celles qui permettent d'écrire :

$$(X - a)Q + R = (X - a)(p_n X^{n-1} + \dots + p_1 X^{i-1} + \dots + p_1) + p_0$$

$$= \sum_{k=0}^n \lambda_k X^k = P$$

Fin de la partie réservée aux MPSI. Retour à la partie commune MPSI, PCSI, PTSI.

3- Polynôme dérivé

Début de partie réservée aux MPSI

On définit le polynôme dérivé de $P = \sum_{k \geq 0} a_k X^k$ comme étant égal à $P' = \sum_{k \geq 1} k a_k X^{k-1}$. On peut définir de

même les dérivées successives. Si P est de degré n et de terme de plus haut degré $a_n X^n$, alors $a_n n! = P^{(n)}(X)$

FORMULE DE TAYLOR :

Soit P un polynôme de degré n et a un élément de \mathbb{K} . Alors :

$$P(X) = \sum_{k \geq 0} \frac{P^{(k)}(a)}{k!} (X-a)^k$$

Démonstration :

$1, X-a, \dots, (X-a)^n$ étant une famille de $n+1$ polynômes de degrés $0, 1, \dots, n$, ils forment une base de $\mathbb{K}_n[X]$. Il existe donc des coefficients $\alpha_0, \dots, \alpha_n$ tels que $P = \sum_{k \geq 0} \alpha_k (X-a)^k$. On vérifie alors que :

$$P^{(k)}(a) = k! \times \alpha_k$$

En effet, les termes $(X-a)^p$ avec $p < k$ ont une dérivée $k^{\text{ème}}$ nulle, le terme $(X-a)^k$ a une dérivée $k^{\text{ème}}$ égale à $k!$, et les termes $(X-a)^p$ avec $p > k$ ont une dérivée $k^{\text{ème}}$ égale à $p(p-1)\dots(p-k+1)(X-a)^{p-k}$ qui s'annule en $X = a$.

4- Ordre de multiplicité d'une racine

PROPOSITION

Il y a équivalence entre :

i) P est divisible par $(X-a)^k$ et pas par $(X-a)^{k+1}$

ii) il existe Q tel que $Q(a) \neq 0$ et $P = (X-a)^k Q$

iii) $P(a) = P'(a) = \dots = P^{(k-1)}(a) = 0$ et $P^{(k)}(a) \neq 0$

On dit que a est une racine de multiplicité k du polynôme P .

Démonstration :

i) \Rightarrow ii)

Si P est divisible par $(X-a)^k$, il existe Q tel que $P = (X-a)^k Q$. Si on avait $Q(a) = 0$, alors Q pourrait se factoriser par $X-a$ et P serait divisible par $(X-a)^{k+1}$.

ii) \Rightarrow iii)

Si $P = (X-a)^k Q$ avec $Q(a) \neq 0$, alors, on a, pour i compris entre 0 et k :

$$P^{(i)}(X) = (X-a)^{k-i} Q_i(X) \text{ avec } Q_i(a) \neq 0$$

Ce résultat se montre aisément par récurrence. Il est vrai pour $i = 0$, et s'il est vrai pour $i < k$, alors :

$$\begin{aligned} P^{(i+1)}(X) &= (k-i)(X-a)^{k-i-1} Q_i(X) + (X-a)^i Q_i'(X) \\ &= (X-a)^{k-i-1} Q_{i+1}(X) \text{ avec } Q_{i+1}(X) = (k-i)Q_i(X) + (X-a)Q_i'(X) \end{aligned}$$

On a bien $P^{(i)}(a) = 0$ pour $0 \leq i \leq k-1$, et $P^{(k)}(a) = Q_k(a)$ différent de 0.

iii) \Rightarrow i)

On applique la formule de Taylor et on factorise par $(X-a)^k$.

Fin de la partie réservée aux MPSI. Retour à la partie commune MPSI, PCSI, PTSI.

5- Polynôme scindé, relations coefficients-racines

On suppose que le polynôme $P = a_0 + a_1 X + \dots + a_n X^n$ se factorise en n facteurs $a_n(X-x_1)(X-x_2)\dots(X-x_n)$. On dit que le polynôme est scindé. On cherche les relations entre les coefficients a_i et les racines x_i . Il suffit de développer la factorisation. On note :

$$\sigma_1 = \sum_{i=1}^n x_i$$

$$\sigma_2 = \sum_{1 \leq i < j \leq n} x_i x_j$$

...

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \dots x_{i_k}$$

...

$$\sigma_n = x_1 x_2 \dots x_n$$

On a alors $P = a_n (X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \dots + (-1)^k \sigma_k X^{n-k} + \dots + (-1)^n \sigma_n)$, d'où :

$$\sigma_1 = -\frac{a_{n-1}}{a_n}$$

$$\sigma_2 = \frac{a_{n-2}}{a_n}$$

...

$$\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$$

...

$$\sigma_n = (-1)^n \frac{a_0}{a_n}$$

Pour $n = 2$, on retrouve les relations classiques des racines du trinôme $ax^2 + bx + c$:

$$S = -\frac{b}{a} \text{ et } P = \frac{c}{a}.$$

Voici un exemple d'utilisation des relations coefficients–racines. Trouver une condition nécessaire et suffisante pour que $X^3 + pX + q$ admette dans $\mathbb{C}[X]$ trois racines a, b et c telles que $a = bc$. On a :

$$\begin{aligned} \begin{cases} a + b + c = 0 \\ ab + bc + ac = p \\ abc = -q \\ a = bc \end{cases} &\Leftrightarrow \begin{cases} b + c = -a \\ a(b+c) + bc = -a^2 + a \\ a^2 = -q \\ a = bc \end{cases} &\Leftrightarrow \begin{cases} b + c = -a \\ -a^2 + a = p \\ a^2 = -q \\ a = bc \end{cases} \\ \Leftrightarrow \begin{cases} a = p - q \\ b + c = q - p \\ a^2 = -q \\ bc = p - q \end{cases} &\Leftrightarrow \begin{cases} a = p - q \\ b + c = q - p \\ bc = p - q \\ -q = (p-q)^2 \end{cases} \end{aligned}$$

La CNS cherchée est $(p-q)^2 + q = 0$. En effet, dans ce cas, on peut trouver a , puis $b+c$ et bc , donc b et c .

EXEMPLE : $q = -1$ et $p = -2$

On a alors $a = -1$, $b+c = 1$ et $bc = -1$ donc b et c sont solutions de :

$$X^2 - X - 1 = 0 \text{ d'où } b = \frac{1+\sqrt{5}}{2} \text{ et } c = \frac{1-\sqrt{5}}{2}.$$

Ce type de relations peut donc servir à résoudre des équations algébriques de la forme $P(X) = 0$ avec condition. En ce qui concerne les équations générales, signalons que l'on sait, depuis la plus haute antiquité, résoudre les équations du 2^o degré, que depuis le XVI^{ème} siècle, on sait résoudre les équations du 3^o et du 4^o degré (Tartaglia 1499–1557, Cardan 1501–1576 ...), que l'impossibilité de la résolution générale des équations du 5^o degré résulte des travaux d'Abel (1802–1829), et que ceux de Galois permettent de savoir quelles équations sont résolubles. Les travaux de Galois (1811–1832) ont en grande partie été à l'origine de l'introduction de notion de groupe.

6– Théorème de d'Alembert

THEOREME (admis)

Tout polynôme non constant admet au moins une racine sur \mathbb{C} .

Il en résulte que les polynômes irréductibles sont tous de degré 1, et que tout polynôme à coefficients complexes peut se factoriser sous la forme $\lambda \prod_{i \geq 0} (X - a_i)^{k_i}$.

Si $P = \sum_{i \geq 0} a_i X^i$, notons $\bar{P} = \sum_{i \geq 0} \bar{a}_i X^i$. Si z est complexe, on a alors : $\overline{P(z)} = \bar{P}(\bar{z})$ de sorte que si z est

racine de P , alors \bar{z} est racine de \bar{P} , avec le même ordre de multiplicité. Si P est à coefficients réels, alors $P = \bar{P}$, et si z est racine de P , alors \bar{z} aussi. Les polynômes P à coefficients réels se décomposent alors sur \mathbb{C} sous la forme :

$$P = \lambda \prod_{i \geq 0} (X - a_i)^{k_i} \prod_{i \geq 0} (X - z_i)^{m_i} (X - \bar{z}_i)^{m_i}$$

et sur \mathbb{R} , en regroupant les parties conjuguées :

$$P = \lambda \prod_{i \geq 0} (X - a_i)^{k_i} \prod_{i \geq 0} (X^2 - \alpha_i X + \beta_i)^{m_i} \text{ avec } \alpha_i = 2\operatorname{Re}(z_i) \text{ et } \beta_i = |z_i|^2$$

Les polynômes irréductibles sur \mathbb{R} sont donc de degré 1 ou 2.

Exemple : $X^4 + 1$ se factorise sur \mathbb{R} sous la forme :

$$(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

Les propriétés arithmétiques des polynômes, spécifiques au programme de MPSI, se trouvent dans le chapitre Arithmétique, dans le fichier ARITHMTQ.PDF

7- Fractions rationnelles

Début de partie réservée aux MPSI

a) Définition :

Une fraction rationnelle est le quotient de deux polynômes $\frac{A}{B}$ avec $B \neq 0$. On dit que deux fractions rationnelles $\frac{A}{B}$ et $\frac{C}{D}$ sont égales si et seulement si $AD = BC$ (comme dans \mathbb{Q} pour les entiers). On dit que la fraction est irréductible si les deux polynômes A et B n'ont pas de diviseurs communs autres que les constantes.

On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles de polynômes à coefficients dans \mathbb{K} . Il n'est pas difficile de vérifier qu'il s'agit d'un corps.

Si a est un zéro d'ordre p de A et d'ordre q de B , notons $A = (X-a)^p C$ et $B = (X-a)^q D$. Alors :

Si $p = q$, $\frac{A}{B} = \frac{C}{D}$ sans que a n'apparaisse plus comme zéro ni de C ni de D .

Si $p > q$, $\frac{A}{B} = (X-a)^{p-q} \frac{C}{D}$ avec $C(a) \neq 0$ et $D(a) \neq 0$. On dit que a est un zéro d'ordre $p-q$ de la fraction rationnelle.

Si $p < q$, $\frac{A}{B} = \frac{1}{(X-a)^{q-p}} \frac{C}{D}$ avec $C(a) \neq 0$ et $D(a) \neq 0$. On dit que a est un pôle d'ordre $q-p$ de la fraction rationnelle.

b) Partie entière :

PROPOSITION

Soit $\frac{A}{B}$ une fraction rationnelle. Il existe un unique polynôme E , appelé partie entière, et une fraction rationnelle $\frac{C}{B}$ telle que :

$$\frac{A}{B} = E + \frac{C}{B} \text{ avec } \deg C < \deg B$$

Cette proposition est équivalente à :

$$A = BE + C \text{ avec } \deg C < \deg B.$$

On reconnaît l'expression de la division euclidienne de A par B . E est le quotient de cette division et C le reste. On notera l'analogie avec ce qui se passe dans \mathbb{Q}^+ , où une fraction $\frac{a}{b}$ s'écrit sous la forme $q + \frac{c}{b}$ avec c et q entiers, et $c < b$. Là aussi, q est le quotient entier de la division euclidienne de a par b .

c) Partie polaire :

PROPOSITION

Soit $\frac{A}{B}$ une fraction irréductible et soit a un pôle de multiplicité n . Ecrivons $B = (X-a)^n P$ avec $P(a) \neq 0$. Il existe une unique décomposition sous la forme :

$$\frac{A}{B} = \frac{Q}{(X-a)^n} + \frac{C}{P}$$

avec C et Q deux polynômes, Q étant tel que $\deg Q < n$. $\frac{Q}{(X-a)^n}$ s'appelle la partie polaire de la fraction rationnelle.

Démonstration

La décomposition est équivalente à :

$$A = PQ + C(X-a)^n \text{ avec } \deg Q < n$$

Quitte à faire le changement de variable $X-a = Y$, nous pouvons supposer que a est nul et que $P(0) \neq 0$. Il s'agit donc de décomposer $A = PQ + CX^n$ avec $\deg Q < n$. Nous allons montrer qu'une telle décomposition existe non seulement pour le n égal à l'ordre de multiplicité du pôle, mais en fait pour tout entier n . La seule hypothèse à utiliser est $P(0) \neq 0$.

□ La décomposition est unique : Si $A = PQ + CX^n = PQ' + C'X^n$ avec $\deg Q < n$ et $\deg Q' < n$, alors on a : $P(Q - Q') = X^n(C' - C)$ donc X^n divise $P(Q - Q')$, mais X^n est premier avec P car $P(0) \neq 0$, donc X^n divise $Q - Q'$. mais $\deg(Q - Q') < n$, donc $Q - Q' = 0$, et par suite, $C' - C$ aussi.

□ La décomposition existe : par récurrence sur n .

Si $n = 1$, on cherche à écrire $A = PQ + CX$. Il suffit de choisir le coefficient constant de Q constant égal à $Q(0)$ de telle façon que $A(0) = P(0)Q(0)$, ce qui est possible car $P(0) \neq 0$. On a alors $A - PQ$ qui s'annule en 0, donc qui se factorise par X .

Supposons ensuite que la décomposition existe au rang $n-1$, c'est-à-dire qu'il existe Q_1 de degré inférieur à $n-1$ et C_1 tel que $A = PQ_1 + C_1X^{n-1}$. On cherche Q et C tel que $\deg Q < n$ et que :

$$A = PQ_1 + C_1X^{n-1} = PQ + CX^n$$

Puisque Q_1 est de degré au plus $n-2$ et Q de degré au plus $n-1$, cherchons Q sous la forme

$$Q = \lambda X^{n-1} + Q_1$$

λ et C doivent alors être tels que :

$$A = PQ_1 + C_1X^{n-1} = \lambda PX^{n-1} + PQ_1 + CX^n$$

$$\Leftrightarrow C_1X^{n-1} = \lambda PX^{n-1} + CX^n$$

$$\Leftrightarrow C_1 = \lambda P + CX$$

Donc λ doit être choisi de façon que $\lambda P(0) = C_1(0)$. λ (et donc Q) étant ainsi défini, il suffit alors de remarquer que $\lambda P - C_1$ s'annule en 0 pour pouvoir factoriser ce polynôme par X, le quotient étant $-C$.

METHODE PRATIQUE :

Dans la pratique, on a souvent $n = 1$ ou 2 et il convient de connaître un moyen rapide de trouver la partie polaire.

Si $n = 1$, on a $\frac{A}{B} = \frac{A}{(X-a)P}$ qui se décompose sous la forme $\frac{A}{(X-a)P} = \frac{q_0}{X-a} + \frac{C}{P}$. On trouve facilement

la valeur de q_0 en multipliant par $X-a$ puis en donnant à X la valeur a . On obtient ainsi $q_0 = \frac{A(a)}{P(a)}$, ce qui serait la valeur donnée par la démonstration dans le cas où a est quelconque. On notera que $P(a)$ n'est autre que $B'(a)$, de sorte que l'on a aussi $q_0 = \frac{A(a)}{B'(a)}$

Si $n = 2$, on a $\frac{A}{B} = \frac{A}{(X-a)^2P} = \frac{q_0 + q_1(X-a)}{(X-a)^2} + \frac{C}{P} = \frac{q_0}{(X-a)^2} + \frac{q_1}{X-a} + \frac{C}{P}$. La valeur q_0 se trouve d'une manière comparable à la précédente, mais en multipliant par $(X-a)^2$ et en donnant à X la valeur A, de sorte que $q_0 = \frac{A(a)}{P(a)}$.

$$\text{Par ailleurs, } A = (q_0 + q_1(X-a))P + C(X-a)^2 = \left(\frac{A(a)}{P(a)} + q_1(X-a)\right)P + C(X-a)^2$$

$$\Rightarrow A - \frac{A(a)}{P(a)}P = q_1(X-a)P + C(X-a)^2$$

Or, en utilisant la formule de Taylor :

$$A = A(a) + (X-a)A'(a) + (X-a)^2U$$

$$P = P(a) + (X-a)P'(a) + (X-a)^2V$$

$$\Rightarrow A - \frac{A(a)}{P(a)}P = (X-a)A'(a) + (X-a)^2U - (X-a)\frac{P'(a)A(a)}{P(a)} - (X-a)^2\frac{VA(a)}{P(a)} = q_1(X-a)P + C(X-a)^2$$

$$\Rightarrow A'(a) + (X-a)U - \frac{P'(a)A(a)}{P(a)} - (X-a)\frac{VA(a)}{P(a)} = q_1P + C(X-a)$$

$$\text{En faisant } X = a, \text{ on obtient } A'(a) - \frac{P'(a)A(a)}{P(a)} = q_1P(a), \text{ soit } q_1 = \frac{P(a)A'(a) - P'(a)A(a)}{P(a)^2} = \left(\frac{A}{P}\right)'(a).$$

$$\text{Finalement, } \frac{A}{(X-a)^2P} = \frac{A(a)}{P(a)} \frac{1}{(X-a)^2} + \left(\frac{A}{P}\right)'(a) \frac{1}{X-a} + \frac{C}{P}.$$

Ce n'est qu'une formule de Taylor appliquée en a à $\frac{A}{P}$.

d) Décomposition d'une fraction rationnelle :

On factorise B sur le corps \mathbb{C} , de sorte que la fraction s'écrit :

$$\frac{A}{(X-a_1)^{k_1}(X-a_2)^{k_2}\dots(X-a_n)^{k_n}}$$

On peut supposer que les a_i ne sont pas racines du numérateur A, sinon, on simplifie les facteurs correspondants $(X-a_i)$ de façon à obtenir une fraction irréductible. Alors $\frac{A}{B}$ est égal à la somme de la partie entière E et de chacune des parties polaires $\frac{Q_i}{(X-a_i)^{k_i}}$ et cette décomposition est unique. En effet, $\frac{A}{B} - (E + \sum_{i=1}^n \frac{Q_i}{(X-a_i)^{k_i}})$ a une partie entière nulle et toutes ses parties polaires sont nulles. La fraction réduite au même dénominateur est alors nulle.

Si on écrit Q_i sous la forme $\sum_{j=1}^{k_i} \lambda_{ij}(X-a_i)^{k_i-j}$, on obtient la décomposition finale dite décomposition en éléments simples :

$$\frac{A}{B} = E + \underbrace{\sum_{i=1}^n \sum_{j=1}^{k_i} \frac{\lambda_{ij}}{(X-a_i)^j}}_{\text{parties polaires}}$$

$\underbrace{\hspace{10em}}_{\text{partie entière}}$

EXEMPLE :

Décomposer en éléments simples $\frac{P'}{P}$ avec $P = (X-a_1)^{k_1}(X-a_2)^{k_2} \dots (X-a_n)^{k_n}$.

$$\text{On a } P' = \sum_{i=1}^n k_i (X-a_1)^{k_1} (X-a_2)^{k_2} \dots (X-a_i)^{k_i-1} \dots (X-a_n)^{k_n} \Rightarrow \frac{P'}{P} = \sum_{i=1}^n \frac{k_i}{X-a_i}$$

Ce n'est rien d'autre que la dérivée logarithmique de P, sauf que la formule s'applique également aux polynômes à coefficients complexes.

Fin de la partie réservée aux MPSI. Retour à la partie commune MPSI, PCSI, PTSI.

Annexe : Nombres algébriques, nombres transcendants, quadrature du cercle

La classification usuelle des nombres est la suivantes : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, à savoir les entiers naturels, les entiers relatifs, les rationnels, les réels, les complexes. Nous allons définir une nouvelle catégorie, comprise entre \mathbb{Q} et \mathbb{C} , les nombres algébriques, et son complémentaire, les nombres transcendants.

u étant un élément de \mathbb{C} , on note $\mathbb{Q}[u]$ le plus petit anneau contenant \mathbb{Q} et u . Il s'agit de l'ensemble

$$\mathbb{Q}[u] = \{a_0 + a_1u + \dots + a_mu^m \mid m \in \mathbb{N}, a_i \in \mathbb{Q}\}$$

autrement dit c'est l'ensemble des valeurs de la forme $P(u)$, où P est un polynôme à coefficients rationnels. De même, u et v étant des éléments de \mathbb{C} , on note $\mathbb{Q}[u,v]$, le plus petit anneau contenant \mathbb{Q} , u et v . On a :

$$\mathbb{Q}[u,v] = \{ \sum a_{ij}u^i v^j \mid a_{ij} \in \mathbb{Q} \}$$

Un élément u de \mathbb{C} est dit **algébrique** s'il existe un polynôme P non nul à coefficient dans \mathbb{Q} tel que $P(u) = 0$. Un nombre qui n'est pas algébrique est dit **transcendant**.

• **EXEMPLES :**

$\sqrt{2}$ est algébrique, racine de $X^2 - 2$

$\sqrt{2} + \sqrt{3}$ est algébrique, racine de $X^4 - 10X^2 + 1$. (Question comment a-t-on trouvé ce polynôme ?)

$\frac{1 + i\sqrt{3}}{2}$ est algébrique, racine de $X^3 - 1$ ou de $X^2 + X + 1$

• **POLYNOME MINIMAL D'UN NOMBRE ALGEBRIQUE**

Si u est algébrique, plusieurs polynômes peuvent s'annuler sur u . Soit P_u polynôme unitaire s'annulant sur u et de degré minimal. Alors tout autre polynôme s'annulant sur u est un multiple de P_u . En effet, soit P tel que $P(u) = 0$. Effectuons la division euclidienne de P par P_u . On a :

$$P = P_u Q + R \text{ avec } \deg R < \deg P_u$$

$$\Rightarrow P(u) = P_u(u)Q(u) + R(u)$$

mais $P(u) = P_u(u) = 0$ donc $R(u) = 0$. Mais P_u est un polynôme non nul de degré minimal s'annulant sur u et $\deg R < \deg P_u$. On a donc nécessairement $R = 0$.

P_u s'appelle polynôme minimal associé à u . Par exemple, pour $u = \frac{1 + i\sqrt{3}}{2}$, le polynôme minimal P_u est $X^2 + X + 1$, alors que $P = X^3 - 1$ est un polynôme s'annulant sur u , multiple de P_u .

Il en résulte que P_u est irréductible sur \mathbb{Q} , car si $P_u = AB$ avec $0 < \deg A < \deg P_u$, $0 < \deg B < \deg P_u$, alors ou bien $A(u) = 0$, ou bien $B(u) = 0$, mais dans les deux cas, on aurait trouvé un polynôme s'annulant sur u de degré inférieur à celui de P_u .

Supposons P_u de degré n , et considérons une combinaison de la forme $a_0 + a_1u + \dots + a_{n-1}u^{n-1} = 0$. Le membre de gauche est un polynôme de degré $n-1$, strictement inférieur au degré de P_u , et s'annulant sur u . Il s'agit donc du polynôme nul et tous les coefficients sont nuls. Autrement dit, les nombres $(1, u, u^2, \dots, u^{n-1})$ forme un système libre dans \mathbb{C} considéré comme espace vectoriel sur \mathbb{Q} . Il s'agit d'une base de $\mathbb{Q}[u]$ en tant qu'espace vectoriel, car toute puissance u^k peut s'exprimer comme combinaison linéaire des $(1, u, u^2, \dots, u^{n-1})$. Il suffit en effet d'effectuer la division euclidienne de X^k par P_u pour obtenir :

$$X^k = P_u Q + R \text{ avec } \deg R \leq n-1$$

et comme $P_u(u) = 0$, on a $u^k = R(u)$.

Ainsi, toute puissance de $\sqrt{2} + \sqrt{3}$ peut s'exprimer comme combinaison linéaire à coefficients rationnels de 1, de $\sqrt{2} + \sqrt{3}$, de $(\sqrt{2} + \sqrt{3})^2$ et de $(\sqrt{2} + \sqrt{3})^3$.

Inversement, soit A un anneau contenant \mathbb{Q} , de dimension finie n en tant qu'espace vectoriel sur \mathbb{Q} . Alors tout élément u de A est algébrique. En effet, $(1, u, u^2, \dots, u^n)$ est un système contenant $n+1$ vecteurs dans A qui est de dimension n , donc est un système lié, ce qui exprime qu'il existe un polynôme à coefficients rationnels s'annulant sur ce nombre.

• **L'ENSEMBLE DES NOMBRES ALGEBRIQUES EST UN CORPS**

□ Soit u algébrique, non nul. alors $\frac{1}{u}$ est algébrique.

En effet, si $a_0 + a_1u + \dots + a_mu^m = 0$, alors $\frac{a_0}{u^m} + \frac{a_1}{u^{m-1}} + \dots + a_m = 0$.

□ Soient u et v deux éléments algébriques. On pose $p = \deg(P_u)$ et $q = \deg(P_v)$. Alors $\mathbb{Q}[u, v]$ est de dimension finie. En effet, nous avons vu que toute puissance u^k est combinaison linéaire de $1, u, \dots, u^{p-1}$. De même, toute puissance v^l est combinaison linéaire de $1, v, \dots, v^{q-1}$. Donc tout terme de la forme $u^k v^l$ peut s'exprimer comme combinaison linéaire des $u^i v^j, 0 \leq i < p, 0 \leq j < q$. Il en est a fortiori de même des combinaison linéaire des $u^k v^l$. Ainsi, les $\{u^i v^j, 0 \leq i < p, 0 \leq j < q\}$ forment un système générateur de $\mathbb{Q}[u, v]$ qui est au plus de dimension pq .

Il en résulte que, uv et $u+v$ étant éléments de $A = \mathbb{Q}[u, v]$ qui est de dimension finie, sont algébriques.

• NOMBRES TRANSCENDANTS

C'est Legendre (1752-1833) qui distingua nombres algébriques (racines d'un polynôme à coefficients entiers) et nombres transcendants (qui ne sont racines d'aucun tel polynôme). Cette définition est d'autant plus remarquable qu'à l'époque, aucun nombre transcendant n'est connu et il faut attendre Liouville qui donne en 1844 la première preuve de l'existence de nombres transcendants, par exemple de :

$$10^{-1!} + 10^{-2!} + 10^{-3!} + \dots = 0,1100010000\dots$$

En 1873, Hermite prouva la transcendance de e , et en 1882, Lindemann prouva la transcendance de π . Pour P et Q à coefficients rationnels, il y a donc équivalence entre

i) $P(\pi) = Q(\pi)$

ii) $P(e) = Q(e)$

iii) $P = Q$

En 1929, Gelfond prouva la transcendance de e^π . On ignore aujourd'hui si $e+\pi, e\pi$ et π^e sont transcendants ou non.

A noter que la découverte de Lindemann mit fin au problème de la quadrature du cercle, posé depuis l'antiquité et qui consiste à trouver comment construire un carré d'aire égal à un cercle donné, uniquement avec une règle et un compas. Le problème est ancien et semble suffisamment connu du grand public au Vème siècle avant JC pour qu'Aristophane s'en moque dans sa pièce *Les Oiseaux* (414 avant JC). Après avoir fondé la cité des Oiseaux, Pisthétairos voit défiler un certain nombre de fâcheux, et parmi eux, Méton, astronome et arpenteur [Aristophane, Théâtre complet, Garnier-Flammarion] :

Méton : Avançant une règle toute droite, je mesurerai de façon que ton cercle devienne un carré, avec au centre l'Agora, où aboutiront en plein milieu des rues droites et que, comme du soleil, qui est rond lui-même, s'élancent droits, de tous côtés, des rayons brillants.

Pisthétairos : C'est un Thalès, Méton.

Méton : Qu'est-ce que c'est ?

Pisthétairos : Sache que je t'aime ; aussi écoute-moi et retire-toi d'ici.

Méton : Quel danger y a-t-il ?

Pisthétairos : Comme à Lacédémone, on chasse d'ici les étrangers et ce sont des grêles de coups qui tombent sur eux par toute la ville.

Méton : Est-ce que par hasard vous êtes en révolution ?

Pisthétairos : Non par Zeus, non certes !

Méton : Qu'est-ce à dire alors ?

Pisthétairos : Nous avons unanimement décidé de pulvériser tous les imposteurs.

Certaines quadratures ont été réalisées dans l'Antiquité, par exemple, la quadrature de la parabole par Archimède ou la quadrature de certaines lunules par Hippocrate de Chios. Le problème de la quadrature du cercle est impossible, car, une fois donné une unité de longueur, la règle et le compas ne permettent de ne construire que certaines quantités algébriques. Il faudrait que $\sqrt{\pi}$ soit algébrique pour pouvoir construire un carré de même aire qu'un cercle de rayon 1, mais π aussi serait algébrique. Le résultat de Lindeman en 1882 met donc fin à ce problème.

A noter que, en 1775 déjà, l'Académie Royale des Sciences prit la résolution *de ne plus examiner aucune solution des problèmes de la duplication du cube, de la trisection de l'angle, ou de la quadrature du cercle, ni aucune machine annoncée comme un mouvement perpétuel*. Contrairement aux trois autres problèmes, l'impossibilité de la quadrature du cercle n'avait pas été démontrée à l'époque, mais il est intéressant de noter les raisons qui ont conduit l'Académie à refuser toute nouvelle solution.

Le problème de la quadrature du cercle est d'un ordre différent (des trois autres) : la quadrature de la parabole trouvée par Archimède, celles des lunules d'Hippocrate de Chio, donnèrent des espérances de quarrer le cercle, c'est-à-dire de connaître la mesure de la surface. [...] Une expérience de plus de soixante-dix ans a montré à l'Académie qu'aucun de ceux qui lui envoyaient des solutions de ces problèmes n'en connaissaient ni la nature ni les difficultés, qu'aucune des méthodes qu'ils employaient n'auraient pu les conduire à la solution, quand même elle serait possible. Cette longue expérience a suffi pour convaincre l'Académie du peu d'utilité qui résulterait pour les Sciences, de l'examen de toutes ces prétendues solutions.

D'autres considérations ont encore déterminé l'Académie. Il existe un bruit populaire que les Gouvernements ont promis des récompenses considérables à celui qui parviendrait à résoudre le Problème de la quadrature du cercle, que ce Problème est l'objet des recherches des Géomètres les plus célèbres ; sur la foi de ces bruits, une foule d'hommes beaucoup plus grande qu'on ne le croit renonce à des occupations utiles pour se livrer à la recherche de ce Problème, souvent sans l'entendre, et toujours sans avoir les connaissances nécessaires pour en tenter la solution avec succès : rien n'était plus propre à les désabuser que la déclaration que l'Académie a jugé de devoir faire. Plusieurs avaient le malheur de croire avoir réussi, ils se refusaient aux raisons avec lesquelles les géomètres attaquaient leurs solutions, souvent ils ne pouvaient les entendre et ils finissaient par les accuser d'envie ou de mauvaise foi. Quelquefois leur opiniâtreté a dégénéré en une véritable folie. Tout attachement opiniâtre à une opinion démontrée fautive, s'il s'y joint une occupation perpétuelle du même objet, une impatience violente de la contradiction, est sans doute une véritable folie ; mais on ne la regarde point comme telle, si l'opinion qui forme cette folie ne choque pas les idées connues des hommes, si elle n'influe pas sur la conduite de la vie, si elle ne trouble pas l'ordre de la Société. La folie des quadrateurs n'auraient donc pour eux aucun autre inconvénient que la perte d'un temps souvent utile à leur famille ; mais malheureusement la folie se borne rarement à un seul objet, et l'habitude de déraisonner se contracte et s'étend comme celle de raisonner juste ; c'est ce qui est arrivé plus d'une fois aux quadrateurs. D'ailleurs ne pouvant se dissimuler combien il serait singulier qu'ils fussent parvenus sans étude à des vérités, que les hommes les plus célèbres ont inutilement cherchées, ils se persuadent presque tous que c'est par une protection particulière de la Providence qu'ils y sont parvenus, et il n'y a qu'un pas de cette idée à croire que toutes les combinaisons bizarres d'idées qui se présentent à eux, sont autant d'inspirations. L'humanité exigeait donc que l'Académie, persuadée de l'inutilité absolue de l'examen qu'elle aurait pu faire des solutions de la quadrature du

cercle, cherchât à détruire, par une déclaration publique, des opinions populaires qui ont été funestes à plusieurs familles.