

POLYNOMES

PLAN

I : Présentation des polynômes

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

II : Zéros d'un polynôme

- 1) Définition
- 2) Polynôme dérivé
- 3) Ordre de multiplicité d'une racine
- 4) Polynôme scindé, relations coefficients-racines
- 5) Théorème de d'Alembert
- 6) Fractions rationnelles
- 7) Polynômes interpolateurs de Lagrange

Annexe : Nombres algébriques, nombres transcendants, quadrature du cercle

- 1) Définition
- 2) Polynôme minimal d'un nombre algébrique
- 3) L'ensemble des nombres algébriques est un corps
- 4) Nombres transcendants

Exercices

- 1) Énoncés
- 2) Solutions

I : Présentation des polynômes

1- Définition

On se place sur $\mathbf{K} = \mathbf{R}$ ou \mathbf{C} . Un **polynôme formel** est défini par la donnée d'une suite finie (a_0, \dots, a_n) éléments de \mathbf{K} et appelés coefficients de \mathbf{K} . X étant une lettre muette, on note :

$$P(X) = a_0 + a_1X + \dots + a_nX^n = \sum_{k \geq 0} a_k X^k$$

étant entendu que, dans la dernière notation, 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 :

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

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

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

On a bien évidemment l'implication :

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

Mais la réciproque ne va pas de soi. Nous allons montrer que, lorsque \mathbf{K} est égal à \mathbf{R} ou \mathbf{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 \mathbf{R} ou \mathbf{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 \mathbf{R} ou \mathbf{C} . Alors, si les fonctions polynomiales associées sont égales (prennent les mêmes valeurs), les deux polynômes sont égaux (ont leurs coefficients égaux).

Démonstration :

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

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

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

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

On ne peut plus prendre $x = 0$, cependant, on peut prendre la limite lorsque x tend vers 0, ce qui donne $a_1 = 0$. Il suffit ensuite d'itérer le raisonnement.

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

Si $P \neq 0$, on appelle **degré** de P le maximum des k tels que $a_k \neq 0$, noté $\deg(P)$. On appelle **valuation** de P le minimum des k tels que $a_k \neq 0$, noté $\text{val}(P)$. Si $P = 0$, on pose $\deg(P) = -\infty$ et $\text{val}(P) = +\infty$. 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 $\mathbf{K}[X]$ l'ensemble des polynômes sur le corps \mathbf{K} .

La raison pour laquelle on introduit les polynômes formels et non les fonctions polynomiales provient du fait qu'on peut fort bien faire jouer à X d'autres rôles que des valeurs dans \mathbf{K} . X peut aussi être remplacé par exemple par une matrice carrée, ou un endomorphisme d'un espace vectoriel sur \mathbf{K} .

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

On peut définir sur $\mathbf{K}[X]$ les opérations suivantes.

a) Une somme :

Si $P = \sum_{k \geq 0} a_k X^k$ et $Q = \sum_{k \geq 0} b_k X^k$, 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 l'opposé de P est le polynôme $-P = \sum_{k \geq 0} -a_k X^k$.

On a $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ (y compris si P ou $Q = 0$, avec la convention $\deg(0) = -\infty$.) 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 :

Si $P = \sum_{k \geq 0} a_k X^k$ et $Q = \sum_{k \geq 0} b_k X^k$, alors $P \times Q$ ou $PQ = \sum_{k \geq 0} \sum_{i=0}^k a_i b_{k-i} X^k$. PQ est obtenu en multipliant tous

les termes de P par ceux de Q et en regroupant les monômes du même degré.

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

On a $\deg(PQ) = \deg(P) + \deg(Q)$, y compris si P ou Q est nul, avec la convention $\deg(0) = -\infty$.
Si $PQ = 0$ alors $P = 0$ ou $Q = 0$.

c) Produit par un scalaire (produit externe) :

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

On vérifie que $(\mathbb{K}[X], +, \cdot)$ est un **espace vectoriel** sur \mathbb{K} . Le produit par un scalaire est compatible avec le produit interne dans le sens où $(\lambda \cdot P) \times Q = P \times (\lambda \cdot Q) = \lambda \cdot (P \times Q)$ noté λPQ . $(\mathbb{K}[X], +, \times, \cdot)$ est une **algèbre**.

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 $n + 1$.

PROPOSITION

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 $\mathbb{K}_n[X]$.

On dit que les P_n sont **étagés**.

Démonstration :

□ Montrons par récurrence sur n que la famille (P_0, P_1, \dots, P_n) est libre.

Pour $n = 0$, si λ_0 est tel que $\lambda_0 P_0 = 0$, alors $\lambda_0 = 0$ car P_0 est un coefficient constant non nul (car $\deg(P_0) = 0$). Supposons la propriété vraie au rang $n - 1$. Soient $\lambda_0, \dots, \lambda_n$ des coefficients tels que :

$$\lambda_0 P_0 + \lambda_1 P_1 + \dots + \lambda_n P_n = 0$$

Le coefficient de degré n du membre de gauche est le produit de λ_n par le coefficient de degré n de P_n , et ce produit est nul car le membre de droite est nul. Or le coefficient de degré n de P_n est non nul car $\deg(P_n) = n$, donc c'est λ_n qui est nul. Il reste donc $\lambda_0 P_0 + \lambda_1 P_1 + \dots + \lambda_{n-1} P_{n-1} = 0$ et on applique l'hypothèse de récurrence pour conclure à la nullité de tous les coefficients.

□ Comme la famille libre (P_0, P_1, \dots, P_n) comporte $n + 1$ éléments et que $\mathbf{K}_n[X]$ est de dimension $n + 1$, il s'agit d'une base de $\mathbf{K}_n[X]$.

3- Division euclidienne

Donnons d'abord un exemple. Divisons $2X^4 + X^3 - X^2 + X + 1$ par $2X^2 - X - 2$. Pour cela, on cherche un monôme qui, multiplié par $2X^2 - X - 2$ fait apparaître le terme dominant $2X^4$. Il s'agit de X^2 . On multiplie $2X^2 - X - 2$ par X^2 et on fait la différence avec $2X^4 + X^3 - X^2 + X + 1$. On itère le procédé pour faire disparaître les uns après les autres les termes dominants. On notera que la démarche est ressemblante à celle effectuée pour diviser un entier par un autre.

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

A la fin du calcul, 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 $B \neq 0$. Alors il existe un unique couple (Q, R) de polynômes tels que :

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

Q est le **quotient**, R est le **reste**.

Si $R = 0$, de sorte que $A = BQ$, on dit que B **divise** A , ou que A est un **multiple** de B . 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 $\mathbf{C}[X]$, ou $X^2 + 1$ dans $\mathbf{R}[X]$ sont irréductibles

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

Démonstration :

□ Montrons l'unicité :

Si $A = BQ + R = BQ_1 + R_1$ avec $\deg(R) < \deg(B)$ et $\deg(R_1) < \deg(B)$, on a $B(Q - Q_1) = R_1 - R$, avec :

$$\deg(B(Q - Q_1)) = \deg(B) + \deg(Q - Q_1)$$

et $\deg(R - R_1) \leq \max(\deg(R), \deg(R_1)) < \deg(B)$.

Il ne peut y avoir égalité entre les degrés que si $Q - Q_1 = 0$ et dans ce cas, $R - R_1 = 0$

□ Montrons l'existence. Pour cela, nous donnons un algorithme fournissant les valeurs de Q et R et nous prouvons la validité de l'algorithme. C'est la généralisation de celui qui a été donné en exemple. Soit $A = \sum_{k \geq 0} a_k X^k$ et $B = \sum_{k \geq 0} b_k X^k$, avec $\deg(B) = n$ et $b_n \neq 0$. L'algorithme formel est le

suivant :

| | |
|--|---|
| $Q \leftarrow 0$ | # valeur initiale du quotient : 0 |
| $R \leftarrow A$ | # valeur initiale du reste : A. |
| | # Notons r_p le coefficient dominant de R, de degré p . |
| | # On a : $A = BQ + R$ |
| Tant que $\deg(R) \geq \deg(B)$ faire | |
| $Q \leftarrow Q + \frac{r_p}{b_n} X^{p-n}$ | # $A = BQ + R - B \frac{r_p}{b_n} X^{p-n}$ |
| $R \leftarrow R - B * \frac{r_p}{b_n} X^{p-n}$ | # $A = BQ + R$ et $\deg(R)$ 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 strictement inférieur à $\deg(B)$.

On pourra consulter dans le chapitre L1/ALGO1.PDF l'algorithme de Horner, traitant du cas où $B = X - a$. Cet algorithme numérique donne les coefficients de Q et la valeur de R en un temps de calcul proportionnel au degré de A .

On admettra dans le présent chapitre que la décomposition d'un polynôme en le produit d'un scalaire et de facteurs irréductibles unitaires est unique. Pour une démonstration, voir L1/ARITHMTQ.PDF, où les propriétés arithmétiques des polynômes sont exposées. Dans ce même chapitre, on montre que, si P est de degré n et que la fonction polynomiale associée à P s'annule en au moins $n + 1$ points, alors P est le polynôme nul.

II : Zéros d'un polynôme

1- Définition

On dit que a , élément de \mathbf{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 :

Soit P un polynôme et a un scalaire. 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 $X - a$, puisque :

$$X^k - a^k = (X - a)(X^{k-1} + aX^{k-2} + a^2X^{k-3} + \dots + a^{k-1})$$

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 .

EXEMPLE :

Vérifier que $X^3 - X^2 - 8X + 12$ possède 1 comme racine double.

2- Polynôme dérivé

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 dominant $a_n X^n$, alors $P^{(n)}(X) = a_n n!$.

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

3- Ordre de multiplicité d'une racine

PROPOSITION

Soit P un polynôme et a un scalaire. 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 élément de $\llbracket 1, k \rrbracket$:

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

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

$$\begin{aligned} P^{(i+1)}(X) &= (k-i)(X-a)^{k-i-1} Q_i(X) + (X-a)^{k-i} Q_i'(X) \\ &= (X-a)^{k-i-1} Q_{i+1}(X) \text{ avec } Q_{i+1}(X) = (k-i)Q_i(X) + (X-a)Q_i'(X) \\ &\quad \text{et } Q_{i+1}(a) = (k-i)Q_i(a) \neq 0 \end{aligned}$$

Il en résulte qu'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 $(X - a)^k$.

4- 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 $a_n(X - x_1)(X - x_2)\dots(X - x_n)$, les x_i étant distincts ou non. 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 :

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

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

...

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

...

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

Les σ_i sont les **fonctions symétriques élémentaires** des racines. 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 $ax^2 + bx + c$:

$$S = x_1 + x_2 = -\frac{b}{a} \text{ et } P = x_1 x_2 = \frac{c}{a}$$

EXEMPLE :

□ 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 :

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

La CNS cherchée est $(p - q)^2 + q = 0$. Sous cette condition, on peut trouver a , puis $b + c$ et bc , donc b et c .

□ Dans le cas particulier où $q = -1$ et $p = -2$, on a $a = -1$, $b + c = 1$ et $bc = -1$ donc b et c sont solutions de :

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

Les relations coefficients-racines peuvent donc servir à résoudre des équations algébriques de la forme $P(X) = 0$ avec condition. En ce qui concerne les équations générales, on sait, depuis la plus haute antiquité, résoudre les équations du deuxième degré. Depuis le XVI^{ème} siècle, on sait résoudre les équations du troisième et du quatrième degré (Tartaglia 1499-1557, Cardan 1501-1576). L'impossibilité de la résolution générale des équations du cinquième degré ou plus résulte des travaux d'Abel (1802-1829), et ceux de Galois (1811-1832) permettent de savoir quelles équations sont résolubles.

On peut montrer que toute fonction algébrique de x_1, \dots, x_n et symétrique en ces variables peut s'exprimer algébriquement en fonction de $\sigma_1, \sigma_2, \dots, \sigma_n$. Contentons-nous de montrer ce résultat

pour les quantités $S_k = \sum_{i=1}^n x_i^k$. On a $S_0 = n$, $S_1 = \sum_{i=1}^n x_i = \sigma_1$, puis, pour $n \geq 2$:

$$S_2 = \sum_{i=1}^n x_i^2 = \left(\sum_{i=1}^n x_i\right)^2 - 2 \sum_{i < j} x_i x_j = \sigma_1^2 - 2\sigma_2$$

Le cas général est donné par le théorème suivant :

PROPOSITION (FORMULES DE NEWTON)

Avec les notations précédentes, on a :

- (i) $\forall p \geq n, S_p = \sigma_1 S_{p-1} - \sigma_2 S_{p-2} + \dots + (-1)^{n-1} \sigma_n S_{p-n}$
- (ii) $\forall p \in \llbracket 1, n \rrbracket, S_p = \sigma_1 S_{p-1} - \sigma_2 S_{p-2} + \dots + (-1)^{p-2} \sigma_{p-1} S_1 + (-1)^{p-1} p \sigma_p$

Ces relations de récurrence permettent de calculer les S_p en fonction des σ_i .

La formule (i) est un cas particulier de la formule (ii) si on rajoute des racines fictives x_{n+1}, \dots, x_p toutes nulles.

Démonstration :

□ Les relations peuvent se vérifier en remplaçant dans le second membre les σ_k et les S_{p-k} par leurs expressions et en s'apercevant que les produits de ces expressions se simplifient de proche en proche mais c'est assez fastidieux. On propose une démarche plus rapide, utilisant les développements limités (voir le chapitre L1/DLTAYLOR.PDF). On utilise le fait que, pour z variable réelle (ou complexe) :

$$\frac{z}{1-z} = z + z^2 + \dots + z^p + \frac{z^{p+1}}{1-z} = z + z^2 + \dots + z^p + o(z^p) \text{ quand } z \text{ tend vers } 0$$

Considérons le polynôme $Q(z) = (1 - x_1z)(1 - x_2z)\dots(1 - x_nz)$. Nous affirmons alors, qu'à tout ordre p :

$$-\frac{zQ'(z)}{Q(z)} = S_1z + S_2z^2 + \dots + S_pz^p + o(z^p)$$

En effet :

$$Q'(z) = \sum_{k=1}^n -x_k (1 - x_1z)\dots(1 - x_{k-1}z)(1 - x_{k+1}z)\dots(1 - x_nz) = \sum_{k=1}^n -x_k \frac{Q(z)}{1 - x_kz}$$

$$\text{donc } -\frac{zQ'(z)}{Q(z)} = \sum_{k=1}^n \frac{x_kz}{1 - x_kz} = \sum_{k=1}^n (x_kz + x_k^2z^2 + \dots + x_k^pz^p + o(z^p))$$

$$= S_1z + S_2z^2 + \dots + S_pz^p + o(z^p)$$

comme annoncé. Par ailleurs, si on développe le polynôme Q , on a aussi :

$$Q(z) = 1 - \sigma_1z + \sigma_2z^2 - \sigma_3z^3 + \dots + (-1)^n\sigma_nz^n$$

$$\text{donc } -zQ'(z) = \sigma_1z - 2\sigma_2z^2 + 3\sigma_3z^3 + \dots + (-1)^{n-1}n\sigma_nz^n$$

Il suffit alors d'écrire que :

$$-zQ'(z) = Q(z)(S_1z + S_2z^2 + \dots + S_pz^p + o(z^p))$$

$$\text{ou } \sigma_1z - 2\sigma_2z^2 + \dots + (-1)^{n-1}n\sigma_nz^n = (1 - \sigma_1z + \sigma_2z^2 + \dots + (-1)^n\sigma_nz^n) \times (S_1z + S_2z^2 + \dots + S_pz^p + o(z^p))$$

et d'égaliser les coefficients du terme z^p dans les deux membres pour obtenir les relations voulues.

$$\text{Si } p > n \quad 0 = S_p - \sigma_1S_{p-1} + \sigma_2S_{p-2} - \dots + (-1)^{n-1}\sigma_{n-1}S_{p-n+1} + (-1)^n\sigma_nS_{p-n}$$

$$\text{Si } p \leq n \quad (-1)^{p-1}p\sigma_p = S_p - \sigma_1S_{p-1} + \sigma_2S_{p-2} - \dots + (-1)^{p-1}\sigma_{p-1}S_1$$

A noter que la première égalité est également vraie pour $p = n$ car, dans ce cas, $S_{p-n} = S_0 = n$ et on retrouve une expression commune avec la deuxième égalité.

EXEMPLE :

□ On retrouve, pour $p = 2 \leq n$:

$$S_2 = \sigma_1S_1 - 2\sigma_2 = \sigma_1^2 - 2\sigma_2$$

puis, de proche en proche :

$$S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

$$S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_4$$

$$S_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1^2\sigma_3 + 5\sigma_1\sigma_2^2 - 5\sigma_1\sigma_4 - 5\sigma_2\sigma_3 + 5\sigma_5$$

5- Théorème de d'Alembert

THEOREME (admis)

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

Il en résulte que, sur \mathbf{C} , 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 \mathbf{C} sous la forme :

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

ou les a_i sont réels et les z_i non réels. Sur \mathbf{R} , on obtient, 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 \mathbf{R} sont donc de degré 1 ou 2.

EXEMPLE :

□ $X^4 + 1$, bien que n'ayant aucune racine réelle, se factorise sur \mathbf{R} sous la forme :

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$$

6- Fractions rationnelles

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 \mathbf{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 $\mathbf{K}(X)$ l'ensemble des fractions rationnelles de polynômes à coefficients dans \mathbf{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 :

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

Démonstration :

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 \mathbf{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 $A = PQ + CX^n = PQ_1 + C_1X^n$ avec $\deg(Q) < n$ et $\deg(Q_1) < n$, alors on a : $P(Q - Q_1) = X^n(C_1 - C)$ donc X^n divise $P(Q - Q_1)$, mais P ne comprend aucun facteur irréductible X car $P(0) \neq 0$, donc c'est $Q - Q_1$ qui se factorise par X^n . Mais $\deg(Q - Q_1) < n$, donc $Q - Q_1 = 0$, et par suite, $C_1 - C$ aussi.

□ Montrons l'existence de la décomposition par récurrence sur n .

Si $n = 1$, on cherche à écrire $A = PQ + CX$. Il suffit de choisir 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 strictement 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, le pôle a est simple (i.e. $n = 1$) et il suffit de connaître un moyen rapide de trouver la partie polaire. Dans ce cas $\frac{A}{B} = \frac{A}{(X-a)P}$ 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 $q_0 = \frac{A(a)}{P(a)}$. On notera que $P(a)$ n'est autre que $B'(a)$, de sorte que l'on a aussi $q_0 = \frac{A(a)}{B'(a)}$.

d) Décomposition d'une fraction rationnelle :

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

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

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** :

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

$\underbrace{E}_{\text{partie entière}}$

Nous admettrons que, sur \mathbf{R} , les fractions rationnelles se réduisent en éléments simples sous la forme d'une somme de termes de la forme suivante :

une partie entière

des parties polaires $\frac{\lambda}{(X - a)^j}$, j variant de 1 à l'ordre du pôle réel a de la fraction rationnelle.

des termes $\frac{\lambda X + \mu}{(X^2 + aX + b)^j}$, où $X^2 + aX + b$ est un polynôme irréductible sur \mathbf{R} , j variant de 1 à la plus grande puissance de $X^2 + aX + b$ apparaissant en dénominateur de la fraction rationnelle (correspondant à l'ordre des racines de $X^2 + aX + b$ comme pôles non réels de la fraction rationnelle).

EXEMPLES :

□ Décomposer sur \mathbf{C} la fraction rationnelle $\frac{1}{X^4 + 1}$, puis en déduire une décomposition sur \mathbf{R} .

Les racines de $X^4 + 1$ sont $\exp(\pm \frac{i\pi}{4})$ et $\exp(\pm \frac{3i\pi}{4})$. En appliquant la méthode pratique donnée plus haut, on a :

$$\begin{aligned} \frac{1}{X^4 + 1} &= \frac{1}{4\exp(\frac{3i\pi}{4})(X - \exp(\frac{i\pi}{4}))} + \frac{1}{4\exp(-\frac{3i\pi}{4})(X - \exp(-\frac{i\pi}{4}))} \\ &\quad + \frac{1}{4\exp(\frac{i\pi}{4})(X - \exp(\frac{3i\pi}{4}))} + \frac{1}{4\exp(-\frac{i\pi}{4})(X - \exp(-\frac{3i\pi}{4}))} \\ &= \frac{\cos(\frac{3\pi}{4})X + 1}{2(X^2 - 2\cos(\frac{\pi}{4}) + 1)} + \frac{\cos(\frac{\pi}{4})X + 1}{2(X^2 - 2\cos(\frac{3\pi}{4}) + 1)} \\ &= \frac{-\sqrt{2}X + 2}{4(X^2 - \sqrt{2} + 1)} + \frac{\sqrt{2}X + 2}{4(X^2 + \sqrt{2} + 1)} \end{aligned}$$

□ Décomposer en éléments simples $\frac{P'}{P}$ avec $P = (X - a_1)^{k_1}(X - a_2)^{k_2} \dots (X - a_n)^{k_n}$, les a_i étant des complexes distincts.

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

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

Dans les exercices de L1/GEOMAFF.PDF, on montre que les zéros de P' sont dans l'enveloppe convexe des zéros de P .

□ Soit $P = (X - a_1)(X - a_2) \dots (X - a_n)$, les a_i étant distincts. On a $\frac{1}{P} = \sum_{i=1}^n \frac{1}{P'(a_i)} \frac{1}{X - a_i}$. On applique en effet la méthode pratique donnée plus haut pour trouver les pôles simples d'une fraction rationnelle.

De même, si Q est un polynôme de degré $n - 2$, alors $\sum_{i=1}^n \frac{Q(a_i)}{P'(a_i)} = 0$. En effet, $\frac{Q}{P} = \sum_{i=1}^n \frac{Q(a_i)}{P'(a_i)} \frac{1}{X - a_i}$ et il suffit de multiplier les deux membres par X et de faire tendre X vers l'infini. Comme $\deg(Q) = \deg(P) - 2$, on a $\lim_{X \rightarrow \infty} \frac{XQ}{P} = 0$.

□ Toujours avec $P = (X - a_1)(X - a_2) \dots (X - a_n)$, cherchons la décomposition en éléments simples de $\frac{1}{P^2}$. Les pôles étant doubles, il existe des coefficients α_i et β_i tels que :

$$\frac{1}{P^2} = \sum_{i=1}^n \frac{\alpha_i}{X - a_i} + \sum_{i=1}^n \frac{\beta_i}{(X - a_i)^2}$$

Pour tout i , $\frac{(X - a_i)^2}{P^2}$ est égal à la somme de β_i et de termes ayant tous $X - a_i$ en facteur au numérateur. Par conséquent, si on donne à X une valeur réelle x et que l'on fait tendre x vers a_i , on obtient :

$$\beta_i = \lim_{x \rightarrow a_i} \frac{(x - a_i)^2}{P(x)^2}$$

et, puisque $P(a_i) = 0$, $\lim_{x \rightarrow a_i} \frac{x - a_i}{P(x)} = \lim_{x \rightarrow a_i} \frac{x - a_i}{P(x) - P(a_i)} = \frac{1}{P'(a_i)}$ donc $\beta_i = \frac{1}{P'(a_i)^2}$.

On aura de même :

$$\begin{aligned} \alpha_i &= \lim_{x \rightarrow a_i} (x - a_i) \left(\frac{1}{P(x)^2} - \frac{\beta_i}{(x - a_i)^2} \right) \\ &= \lim_{x \rightarrow a_i} (x - a_i) \left(\frac{1}{P(x)^2} - \frac{1}{P'(a_i)^2 (x - a_i)^2} \right) \end{aligned}$$

Si on effectue un développement limité de $P(x)$ à l'ordre 2 au voisinage de a_i (voir L1/DLTAYLOR.PDF), on obtient :

$$\begin{aligned} P(x) &= P(a_i) + (x - a_i)P'(a_i) + \frac{(x - a_i)^2}{2} P''(a_i) + o((x - a_i)^2) \\ &= (x - a_i)P'(a_i) + \frac{(x - a_i)^2}{2} P''(a_i) + o((x - a_i)^2) \quad \text{car } P(a_i) = 0 \end{aligned}$$

$$\Rightarrow P(x)^2 = (x - a_i)^2 P'(a_i)^2 + (x - a_i)^3 P'(a_i)P''(a_i) + o((x - a_i)^3)$$

$$\begin{aligned} \Rightarrow \frac{1}{P(x)^2} &= \frac{1}{(x - a_i)^2 P'(a_i)^2 + (x - a_i)^3 P'(a_i)P''(a_i) + o((x - a_i)^3)} \\ &= \frac{1}{(x - a_i)^2 P'(a_i)^2} \frac{1}{1 + \frac{(x - a_i)P''(a_i)}{P'(a_i)} + o(x - a_i)} \end{aligned}$$

remarquer que $P'(a_i) \neq 0$ car les pôles sont simples

$$= \frac{1}{(x-a_i)^2 P'(a_i)^2} \left(1 - \frac{(x-a_i)P''(a_i)}{P'(a_i)} + o(x-a_i)\right)$$

$$\Rightarrow \frac{1}{P(x)^2} - \frac{1}{P'(a_i)^2 (x-a_i)^2} = -\frac{P''(a_i)}{(x-a_i)P'(a_i)^3} + o\left(\frac{1}{x-a_i}\right)$$

donc $\alpha_i = -\frac{P''(a_i)}{P'(a_i)^3}$

Ainsi $\frac{1}{P^2} = -\sum_{i=1}^n \frac{P''(a_i)}{P'(a_i)^3} \frac{1}{X-a_i} + \sum_{i=1}^n \frac{1}{P'(a_i)^2} \frac{1}{(X-a_i)^2}$

7- Polynômes interpolateurs de Lagrange

Soient $a_0 < a_1 < \dots < a_n$ $n+1$ réels distincts. On appelle **polynômes interpolateurs de Lagrange** les $n+1$ polynômes L_0, \dots, L_n de degré au plus n tels que, pour tout i , L_i s'annule en $a_0, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$ et $L_i(a_i) = 1$. Montrons que ces polynômes existent en les déterminant explicitement. Les a_k étant distincts, et $a_0, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$ étant racines de L_i , il existe nécessairement un polynôme Q_i tel que $L_i = (X-a_0)\dots(X-a_{i-1})(X-a_{i+1})\dots(X-a_n)Q_i$. L_i étant de degré inférieur ou égal à n et le membre de droite étant de degré $n + \deg(Q)$, on a nécessairement $\deg(L_i) = n$ et $\deg(Q) = 0$. Donc Q est un polynôme constant. Sa valeur est déterminée par la condition $L_i(a_i) = 1$, ce qui donne :

$$L_i = \frac{(X-a_0)\dots(X-a_{i-1})(X-a_{i+1})\dots(X-a_n)}{(a_i-a_0)\dots(a_i-a_{i-1})(a_i-a_{i+1})\dots(a_i-a_n)}$$

APPLICATIONS :

Voici deux utilisations possibles de ces polynômes.

□ Soit f une fonction dont on connaît les valeurs prises en a_0, \dots, a_n (obtenues par exemple par échantillonnage) : $\forall i, f(a_i) = y_i$. Pour x différent des a_i , on souhaiterait attribuer une valeur à $f(x)$ par

interpolation. On peut prendre le polynôme P défini par : $P = \sum_{i=0}^n y_i L_i$. Ce polynôme présente l'intérêt

que, pour tout k , $P(a_k) = f(a_k)$. En effet :

$$P(a_k) = \sum_{i=0}^n y_i L_i(a_k) = y_k \quad \text{puisque } L_i(a_k) = \begin{cases} 0 & \text{si } i \neq k \\ 1 & \text{si } i = k \end{cases}$$

$$= f(a_k)$$

En particulier, si f est lui-même un polynôme de degré n au plus, alors P et f coïncident en $n+1$ points. Etant tous deux de degré inférieurs ou égal à n , cela impose que $P = f$. On a ici une détermination exacte du polynôme f à partir de la connaissance des valeurs qu'il prend en $n+1$ points. Algébriquement, on a montré que les polynômes de Lagrange constituent une base de l'espace vectoriel $\mathbb{R}_n[X]$.

Il convient de signaler cependant que l'interpolation peut ne pas être très bonne en dehors des a_i si f n'est pas un polynôme.

□ L'interpolation précédente peut être utilisé dans le calcul intégral. Soient des points :

$$a < a_0 < a_1 < \dots < a_n < b$$

Si f est un polynôme de degré inférieur ou égal à n , nous venons de voir que :

$$f = \sum_{i=0}^n f(a_i) L_i$$

$$\Rightarrow \int_a^b f(t) dt = \sum_{i=0}^n \alpha_i f(a_i) \text{ où } \alpha_i = \int_a^b L_i(t) dt$$

Si on se fixe les valeurs de a_i , on peut calculer une fois pour toutes les valeurs α_i . On peut alors utiliser l'expression $\sum_{i=0}^n \alpha_i f(a_i)$ pour calculer de manière exacte la valeur de l'intégrale de f , uniquement à partir des valeurs que prend ce polynôme en les a_i . Si f n'est pas un polynôme, on peut également prendre l'expression $\sum_{i=0}^n \alpha_i f(a_i)$ comme valeur approchée de l'intégrale de f . Cela est intéressant dans le cas où le calcul d'une primitive est difficile ou impossible, ou bien dans le cas où f n'est connue qu'en un nombre fini de points (résultant d'une mesure d'un échantillonnage par exemple).

Dans le cas particulier où l'on prend $n = 1$, $a = a_0 < a_1 = b$, on retrouve la méthode des trapèzes :

$$\int_a^b f(t) dt \text{ est approximé par } (b-a) \frac{f(a) + f(b)}{2}$$

$$\text{On a en effet } L_0 = -\frac{x-b}{b-a}, L_1 = \frac{x-a}{b-a}, \alpha_0 = \int_a^b L_0(t) dt = \frac{b-a}{2} = \int_a^b L_1(t) dt = \alpha_1.$$

Annexe : Nombres algébriques, nombres transcendants, quadrature du cercle

1- Définition

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

u étant un élément de \mathbf{C} , on note $\mathbf{Q}[u]$ l'ensemble :

$$\mathbf{Q}[u] = \{a_0 + a_1 u + \dots + a_m u^m \mid m \in \mathbf{N}, a_i \in \mathbf{Q}\}$$

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 \mathbf{C} , on note $\mathbf{Q}[u, v]$, l'ensemble :

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

Un élément u de \mathbf{C} est dit **algébrique** s'il existe un polynôme P non nul à coefficient dans \mathbf{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 $X^2 + X + 1$.

□ $\cos(\frac{2\pi}{7})$, $\cos(\frac{4\pi}{7})$ et $\cos(\frac{6\pi}{7})$ sont tous les trois algébriques. En effet, posons $\theta = \frac{2\pi}{7}$, $\frac{4\pi}{7}$ ou $\frac{6\pi}{7}$, $e^{i\theta}$ est racine du polynôme $X^7 - 1$, ou mieux encore, après avoir divisé $X^7 - 1$ par $X - 1$, de $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$. Si on divise par X^3 et qu'on remplace X par $e^{i\theta}$, on obtient :

$$e^{3i\theta} + e^{2i\theta} + e^{i\theta} + 1 + e^{-i\theta} + e^{-2i\theta} + e^{-3i\theta} = 0$$

$$\Leftrightarrow 2\cos(3\theta) + 2\cos(2\theta) + 2\cos(\theta) + 1 = 0$$

On développe $\cos(2\theta) = 2\cos^2(\theta) - 1$ et $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ et on obtient :

$$8\cos^3(\theta) + 4\cos^2(\theta) - 4\cos(\theta) - 1 = 0$$

Ainsi, $\cos(\frac{2\pi}{7})$, $\cos(\frac{4\pi}{7})$ et $\cos(\frac{6\pi}{7})$ sont racines de $8X^3 + 4X^2 - 4X - 1$.

2- Polynôme minimal d'un nombre algébrique

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 \mathbf{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 l'un ou l'autre 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 $(1, u, u^2, \dots, u^{n-1})$ forment un système libre dans \mathbf{C} considéré comme espace vectoriel sur \mathbf{Q} . Il s'agit d'une base de $\mathbf{Q}[u]$ 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 une partie de \mathbf{C} qui soit un espace vectoriel de dimension finie n sur \mathbf{Q} et stable pour le produit (on dit que A est une **sous-algèbre** de \mathbf{C} de dimension finie). 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.

3- L'ensemble des nombres algébriques est un corps

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

En effet, si $a_0 + a_1u + \dots + a_mu^m = 0$ avec les a_i rationnels, 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 $\mathbf{Q}[u, v]$ est une sous-algèbre 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 $\mathbf{Q}[u, v]$ qui est au plus de dimension pq .

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

4- Nombres transcendants

C'est Legendre (1752-1833) qui distingua nombres algébriques (racines d'un polynôme à coefficients entiers ou rationnels) 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.

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 disque 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 1966, traduction de Marc-Jean Alfonsi] :

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.

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*. 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 fausse, 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 quadratureurs. 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.

Exercices

1- Enoncés

Exo.1) Soit $A = X^4 + 6X^3 + 10X^2 + 3X - 6$ et $B = X^2 + 3X$.

- Effectuer la division euclidienne de A par B.
- Factoriser A.

Exo.2) Soit $P(X) = \prod_{i=1}^n (X - a_i)$ et $Q(X) = \prod_{i=1}^n (X - a_i^2)$

Montrer que P s'écrit de manière unique sous la forme $F(X^2) + XG(X^2)$, où F et G sont deux polynômes, et qu'alors, $Q(X) = (-1)^n(F(X)^2 - XG(X)^2)$.

Exo.3) Montrer que les polynômes suivants forment une base de l'espace vectoriel $\mathbf{R}_n[X]$:

- $1, X, X(X+1), X(X+1)(X+2), \dots, X(X+1)\dots(X-n+1)$
- $X^n, X^{n-1}(X-1), X^{n-2}(X-1)(X-2), \dots, X^{n-p}(X-1)\dots(X-p), \dots, (X-1)\dots(X-n)$

Exo.4) Soit (P_n) la suite de polynômes définis par :

$P_0 = 2, P_1 = X$, et $\forall n \in \mathbf{N}, P_{n+2} = XP_{n+1} - P_n$

- Exprimer pour z complexe non nul $P_n(z + \frac{1}{z})$.
- Factoriser P_n .

Exo.5) Soit n un entier strictement positif.

- Montrer que 1 est racine triple de $P(X) = nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n$.
- Donner le quotient de $P(X)$ par $(X-1)^3$.

Exo.6) Pour quelles valeurs de n le polynôme $X^{4n} - X^{3n} + X^{2n} - X^n + 1$ est-il divisible par $X^4 - X^3 + X^2 - X + 1$?

Exo.7) Soit P un polynôme de degré $n \geq 2$. Montrer l'équivalence entre :

- P est divisible par sa dérivée P'
- $\exists \lambda, \exists a, P = \lambda(X-a)^n$
- $PP'' = \frac{n-1}{n} P'^2$

Exo.8) Montrer l'équivalence entre :

i) $\forall x \in \mathbf{R}, P(x) \geq 0$

ii) $\exists A \in \mathbf{R}[X], \exists B \in \mathbf{R}[X], P = A^2 + B^2$.

Exemple : $P = X^4 + 6X^2 + 24X + 37$.

Exo.9) Soit P un polynôme non nul, à coefficients réels de degré n . Soit a un réel tel que :

$$\forall k, P^{(k)}(a) \geq 0.$$

Montrer qu'alors toute racine réelle x de P vérifie $x \leq a$.

Exo.10) Soit P un polynôme de degré n sur \mathbf{R} ou \mathbf{C} . Montrer que $P(X+1) = \sum_{k=0}^n \frac{P^{(k)}(X)}{k!}$.

Exo.11) Soient a, b, c les racines complexes de $X^3 + X + 1$. Calculer : $\frac{a^3}{a^2+1} + \frac{b^3}{b^2+1} + \frac{c^3}{c^2+1}$.

Exo.12) Résoudre dans \mathbf{C}
$$\begin{cases} x + y + z = 0 \\ x^2 + y^2 + z^2 = 14 \\ x^3 + y^3 + z^3 = 18 \end{cases}$$
.

Exo.13) Calculer $\sum i_1 i_2 \dots i_k$ pour $1 \leq k \leq n$ et $1 \leq i_1 < i_2 < \dots < i_k \leq n$.

Exo.14) Décomposer en éléments simples :

a) $\frac{X^3}{(X^2-1)^2}$

b) $\frac{n!}{X(X+1)\dots(X+n)}$

Exo.15) Soit a, b, c distincts non nuls.

a) Réduire en éléments simples la fraction $\frac{X^3}{(X-a)(X-b)(X-c)}$.

b) En déduire une expression simplifiée de $\frac{a^2}{(b-a)(c-a)} + \frac{b^2}{(a-b)(c-b)} + \frac{c^2}{(a-c)(b-c)}$.

c) et de $\frac{a^3}{(b-a)(c-a)} + \frac{b^3}{(a-b)(c-b)} + \frac{c^3}{(a-c)(b-c)}$

Exo.16) Soit P un polynôme unitaire de degré n et $Q = X(X-1)(X-2)\dots(X-n)$.

a) Montrer que $\frac{P}{Q} = \sum_{k=0}^n \frac{P(k)}{Q'(k)} \frac{1}{X-k}$. Que vaut $Q'(k)$?

b) En considérant $\sum_{k=0}^n \frac{P(k)}{Q'(k)}$, montrer que $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} P(k) = n!$.

c) En déduire en particulier que :

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^n = n!$$

et pour $0 \leq p < n$, $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^p = 0$

d) En déduire également que : $\exists k \in \llbracket 0, n \rrbracket, 2^n | P(k)| \geq n!$.

Exo.17) Construire un polynôme P qui coïncide avec e^x en $0, 1, 2, \dots, n$ et tel que $\deg P \leq n$. Que vaut $P(n+1) - e^{n+1}$?

Exo.18) Soit E l'espace vectoriel des polynômes de degré inférieur ou égal à $2n$. Soit F le sous-ensemble des polynômes qui s'annulent en 0 , et G le sous-ensemble des polynômes qui s'annulent en tous les points $\pm 1, \pm 2, \dots, \pm n$.

a) Montrer que F et G sont des sous-espaces vectoriels supplémentaires.

b) Donner l'expression explicite du projeté d'un polynôme sur G parallèlement à F .

(Voir L1/ESPVECT.PDF pour la notion de supplémentaire et de projecteur).

2- Solutions

Sol.1) a) On devra trouver $A = BQ + R$ avec $Q = X^2 + 3X + 1$ et $R = -6$.

b) On remarque que $Q = B + 1$, donc :

$$\begin{aligned} A &= B^2 + B - 6 = (B + 3)(B - 2) \\ &= (X^2 + 3X + 3)(X^2 + 3X - 2) \\ &= \left(X + \frac{3 - i\sqrt{3}}{2}\right) \left(X + \frac{3 + i\sqrt{3}}{2}\right) \left(X + \frac{3 - \sqrt{17}}{2}\right) \left(X + \frac{3 + \sqrt{17}}{2}\right) \end{aligned}$$

Sol.2) Regrouper dans $F(X^2)$ les termes de degré pair de P et dans $XG(X^2)$ les termes de degré impair. On a alors :

$$\begin{aligned} Q(X^2) &= \prod_{i=1}^n (X^2 - a_i^2) = \prod_{i=1}^n (X - a_i)(X + a_i) = P(X) \times (-1)^n P(-X) \\ &= (-1)^n (F(X^2) + XG(X^2))(F(X^2) - XG(X^2)) \\ &= (-1)^n (F(X^2)^2 - X^2 G(X^2)^2) \end{aligned}$$

Pour conclure, il suffit de remarquer que, si deux polynômes A et B sont tels que $A(X^2) = B(X^2)$, alors $A(X) = B(X)$.

Sol.3) a) La famille de degré étagé.

b) Remarquer que les polynômes ont des valuations étagées et prouver leur indépendance en adaptant la démonstration de l'indépendance d'une famille de polynômes de degré étagé. Conclure en constatant que le nombre de polynômes proposés est égal à la dimension de $\mathbf{R}_n[X]$.

Sol.4) a) Par récurrence, $P_n(z + \frac{1}{z}) = z^n + \frac{1}{z^n}$.

b) On résout $P_n(z + \frac{1}{z}) = 0$ ce qui est équivalent à $z^{2n} = -1$ dont les racines sont :

$$z_k = \exp\left(\frac{i\pi}{2n} + \frac{ik\pi}{n}\right), 0 \leq k \leq 2n-1.$$

Les $z_k + \frac{1}{z_k}$ sont des racines de P_n et valent $2\cos\left(\frac{(2k+1)\pi}{2n}\right)$. Il y a n valeurs distinctes en faisant varier k de 0 à $n-1$. Pour k variant de n à $2n-1$, on retrouve ces valeurs :

$$\begin{aligned} 2\cos\left(\frac{(2k+1)\pi}{2n}\right) &= 2\cos\left(\frac{(2k-2n+1)\pi}{2n} + \pi\right) = -2\cos\left(\frac{(2k-2n+1)\pi}{2n}\right) \\ &= -2\cos\left(-\frac{(2k-2n+1)\pi}{2n}\right) = 2\cos\left(\pi - \frac{(2k-2n+1)\pi}{2n}\right) \\ &= 2\cos\left(\frac{(2(2n-k-1)+1)\pi}{2n}\right) \text{ avec } 2n-k-1 \text{ variant de } 0 \text{ à } n-1. \end{aligned}$$

Comme P_n est de degré n (par récurrence), on a trouvé les n racines de P_n . Etant unitaire (par récurrence), on a :

$$P_n = \prod_{k=0}^{n-1} (X - 2\cos\left(\frac{(2k+1)\pi}{2n}\right))$$

Sol.5) a) On a $P(1) = 0$

$$\begin{aligned} P'(X) &= n(n+2)X^{n+1} - (n+1)(n+2)X^n + (n+2) & \text{donc } P'(1) &= 0 \\ P''(X) &= n(n+1)(n+2)X^n - n(n+1)(n+2)X^{n-1} & \text{donc } P''(1) &= 0 \\ P^{(3)}(X) &= n^2(n+1)(n+2)X^{n-1} - (n-1)n(n+1)(n+2)X^{n-2} & \text{donc } P^{(3)}(1) &\neq 0 \end{aligned}$$

Comme $P(1) = P'(1) = P''(1) = 0$ et $P^{(3)}(1) \neq 0$, 1 est racine triple.

$$\begin{aligned} \text{b) } nX^{n+2} - (n+2)X^{n+1} + (n+2)X - n &= (X-1)(nX^{n+1} - 2X^n - 2X^{n-1} - \dots - 2X^2 - 2X + n) \\ &= (X-1)^2(nX^n + (n-2)X^{n-1} + (n-4)X^{n-2} + \dots + (n-2k)X^{n-k} + \dots + (2-n)X - n) \end{aligned}$$

$$= (X-1)^2 \sum_{k=0}^n (2k-n)X^k$$

$$= (X-1)^2 \sum_{k=0}^n (2k-n)(X^k - 1) \text{ car } \sum_{k=0}^n (2k-n) = 0$$

$$= (X-1)^3 \sum_{k=0}^n (2k-n) \sum_{j=0}^{k-1} X^j$$

Le quotient est :

$$\begin{aligned} Q &= \sum_{k=0}^n (2k-n) \sum_{j=0}^{k-1} X^j = \sum_{0 \leq j < k < n} (2k-n) X^j = \sum_{j=0}^{n-1} \sum_{k=j+1}^n (2k-n) X^j \\ &= \sum_{j=0}^{n-1} (n-j)(j+1) X^j \end{aligned}$$

car $\sum_{k=j+1}^n (2k-n) = (n-j)(j+1)$, somme d'une suite arithmétique de raison 2.

Sol.6) Le polynôme diviseur s'écrit $\frac{X^5 + 1}{X + 1}$ et admet pour quatre des cinq racines cinquième de -1 , $\omega_k = \exp(\frac{(2k+1)i\pi}{5})$, $1 \leq k \leq 4$. Il doit en être de même du polynôme initial $\frac{X^{5n} + 1}{X^n + 1}$. On doit donc avoir $\omega_k^{5n} = -1$ mais $\omega_k^n \neq -1$. Comme $\omega_k^5 = -1$, il est nécessaire et suffisant que n soit impair, mais non multiple de 5.

Sol.7) (ii) \Rightarrow (i) Si $P = \lambda(X - a)^n$, alors $P' = \lambda n(X - a)^{n-1}$ qui divise bien $\lambda(X - a)^n$, de quotient $\frac{X - a}{n}$

(ii) \Rightarrow (iii) est de même de vérification facile.

(i) \Rightarrow (ii) Supposons P de degré n divisible par P' . P' étant de degré $n - 1$, le quotient est de degré 1. Soit a sa racine. En comparant les coefficients dominants de P et P' , on vérifie que le coefficient dominant du quotient est $\frac{1}{n}$. Donc $P = \frac{X - a}{n} P'$. Par récurrence, vérifions que, pour tout k strictement

inférieur à n , $P^{(k)} = \frac{X - a}{n - k} P^{(k+1)}$. C'est vrai pour $n = 0$ (avec $P^{(0)} = P$), et si c'est vrai au rang k , alors,

en dérivant la relation $P^{(k)} = \frac{X - a}{n - k} P^{(k+1)}$, on obtient :

$$P^{(k+1)} = \frac{1}{n - k} P^{(k+1)} + \frac{X - a}{n - k} P^{(k+2)}$$

$$\text{donc } P^{(k+1)} = \frac{X - a}{n - k - 1} P^{(k+2)}.$$

On en déduit par récurrence que, pour tout k inférieur ou égal à n , $P = \frac{(X - a)^k}{n(n - 1) \dots (n - k + 1)} P^{(k)}$. Pour

$k = n$, on obtient $P = \frac{(X - a)^n}{n!} P^{(n)}$, avec $P^{(n)}$ polynôme constant car P est de degré n .

(iii) \Rightarrow (i) Soit Q et R le quotient et le reste de la division euclidienne de P par P' . Comme $\deg(P') = \deg(P) - 1$, Q est de degré 1 et R est constant. En considérant les coefficients dominants de P et P' , on voit que le coefficient dominant de Q est $\frac{1}{n}$. Il existe donc a tel que :

$$P = \frac{1}{n} (X - a)P' + R$$

donc, en dérivant cette expression :

$$P' = \frac{1}{n} (X - a)P'' + \frac{1}{n} P'$$

$$\text{donc } P' = \frac{1}{n - 1} (X - a)P''$$

Par conséquent, si $PP'' = \frac{n - 1}{n} P'^2$, on a, en remplaçant l'un des P' par $\frac{1}{n - 1} (X - a)P''$:

$$PP'' = \frac{1}{n} (X - a)P'P''$$

$$\text{donc } P = \frac{1}{n} (X - a)P' \text{ et } P' \text{ divise } P.$$

Sol.8) ii) \Rightarrow i) évident

i) \Rightarrow ii) Si on considère la décomposition de P en facteurs irréductibles, pour que la fonction polynomiale associée à P soit positive ou nulle, il est nécessaire que P soit produit de facteurs de la forme $(X - a)^{2k}$, de $X^2 + bX + c$ irréductibles et d'une constante λ positive ou nulle. Les facteurs $X^2 + bX + c$ se factorisent sur \mathbb{C} sous la forme $(X - z)(X - \bar{z})$ avec z complexe non réel. Soit Q le produit des $(X - a)^k$, des $(X - z)$ et de $\sqrt{\lambda}$. Alors $P = Q\bar{Q}$. Si on décompose le développement de Q en $Q = A + iB$ en les polynômes A et B , partie réelle et imaginaire de Q , alors $\bar{Q} = A - iB$ et $P = (A + iB)(A - iB) = A^2 + B^2$.
Exemple : $P = (X^2 + 1)^2 + (2X + 6)^2$

Sol.9) D'après la formule de Taylor, $P(a + t) = \sum_{k=0}^n \frac{P^{(k)}(a)}{k!} t^k > 0$ pour tout $t > 0$. Donc les racines réelles de P sont inférieures ou égales à a .

Sol.10) C'est la formule de Taylor où X est la constante et $Y = 1$ la variable !

$$P(X + Y) = \sum_{k=0}^n \frac{P^{(k)}(X)}{k!} Y^k$$

Sol.11) On utilise les relations coefficients-racines $\sigma_1 = 0$, $\sigma_2 = 1$, $\sigma_3 = -1$. On a :

$$a^3 + a + 1 = 0 \Rightarrow a^2 + 1 = -\frac{1}{a}$$

donc $\frac{a^3}{a^2 + 1} = -a^4 = a^2 + a$. De même pour b et c . Il s'agit donc de calculer :

$$a^2 + b^2 + c^2 + a + b + c = \sigma_1^2 - 2\sigma_2 + \sigma_1 = -2$$

Sol.12) x , y et z sont les racines d'un polynôme de degré 3. Les coefficients σ_1 , σ_2 , σ_3 de ce polynôme vérifient :

$$0 = x + y + z = \sigma_1$$

$$14 = x^2 + y^2 + z^2 = (x + y + z)^2 - 2(xy + yz + xz) = \sigma_1^2 - 2\sigma_2 \quad \text{donc } \sigma_2 = -7$$

$$18 = x^3 + y^3 + z^3 = (x + y + z)^3 - 3(x^2y + y^2x + x^2z + xz^2 + yz^2 + y^2z) - 6xyz$$

$$= \sigma_1^3 - 3(xy + yz + xz)(x + y + z) + 3xyz$$

$$= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

$$\text{donc } \sigma_3 = 6$$

Ainsi, le polynôme cherché vaut :

$$X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3 = X^3 - 7X - 6 = (X + 1)(X^2 - X - 6) = (X + 1)(X + 2)(X - 3)$$

et les valeurs de x , y , z , à permutation près, sont -1 , -2 , 3 .

Sol.13) Soit S_n la somme. On a par exemple :

$$S_1 = 1$$

$$S_2 = 1 + 2 + 1 \times 2 = 5$$

$$S_3 = 1 + 2 + 3 + 1 \times 2 + 2 \times 3 + 1 \times 3 + 1 \times 2 \times 3 = 23$$

Montrons que, pour tout n , $S_n = (n + 1)! - 1$. En voici deux démonstrations :

□ Par récurrence :

S_n est la somme des quantités

$\sum i_1 i_2 \dots i_k$ pour $k \leq n-1$ et $i_k \leq n-1$, ce qui donne S_{n-1}

$$\begin{array}{ll} n & \text{pour } k=1 \text{ et } i_1 = n \\ nS_{n-1} & \text{pour } k \geq 2 \text{ et } i_k = n \end{array}$$

Donc $S_n = S_{n-1} + n + nS_{n-1}$ etc...

□ Posons $P = (X+1)(X+2)\dots(X+n) = X^n + \sigma_1 X^{n-1} + \sigma_2 X^{n-2} + \dots + \sigma_{n-1} X + \sigma_n$ avec ici

$$\sigma_k = \sum i_1 i_2 \dots i_k, \quad 1 \leq i_1 < i_2 < \dots < i_k \leq n, \text{ et } S_n = \sum_{k=1}^n \sigma_k = P(1) - 1 = (n+1)! - 1.$$

Sol.14) a) $\frac{X^3}{(X^2-1)^2} = \frac{1}{4(X-1)^2} - \frac{1}{4(X+1)^2} + \frac{1}{2(X-1)} + \frac{1}{2(X+1)}$

b) $\sum_{k=0}^n (-1)^k \binom{n}{k} \frac{1}{X+k}$

Sol.15) a) On a :

$$\frac{X^3}{(X-a)(X-b)(X-c)} = 1 + \frac{a^3}{(a-b)(a-c)(X-a)} + \frac{b^3}{(b-a)(b-c)(X-b)} + \frac{c^3}{(c-a)(c-b)(X-c)}$$

b) Pour $X=0$, $\frac{a^2}{(b-a)(c-a)} + \frac{b^2}{(a-b)(c-b)} + \frac{c^2}{(a-c)(b-c)} = 1.$

c) En passant le 1 dans le membre de gauche, en multipliant par X et en faisant tendre X vers l'infini, on obtient

$$\frac{a^3}{(b-a)(c-a)} + \frac{b^3}{(a-b)(c-b)} + \frac{c^3}{(a-c)(b-c)} = a + b + c$$

Sol.16) a) Multiplier $\frac{P}{Q}$ par $X-k$ et faire tendre X vers k ou appliquer la méthode partielles donnée

dans le cours pour déterminer le coefficient relatif à un pôle simple. On vérifiera que :

$$Q'(k) = k! (n-k)! (-1)^{n-k}$$

b) Multiplier $\frac{P}{Q}$ par X et faire tendre X vers l'infini. On obtient :

$$1 = \sum_{k=0}^n \frac{P(k)}{Q'(k)} = \frac{1}{n!} \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} P(k)$$

c) En particulier pour $P = X^n$, on obtient $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^n = n!$, puis en retranchant membre à

membre les deux égalités $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^n = n!$ et $\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} P(k) = n!$, on obtient

$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} R(k) = 0$ pour tout polynôme $R = P - X^n$ de degré inférieur ou égal à n . En prenant

$R = X^p$, on obtient les résultats demandés.

d) Par l'absurde, si : $\forall k \in \llbracket 0, n \rrbracket, |P(k)| < \frac{n!}{2^n}$, alors :

$$1 = \left| \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} \frac{P(k)}{n!} \right| \leq \sum_{k=0}^n \binom{n}{k} \frac{|P(k)|}{n!} < \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} = 1$$

ce qui est absurde.

Sol.17) On utilise les polynômes interpolateurs de Lagrange.

$$P = \sum_{i=0}^n e^i \frac{X(X-1)(X-2)\dots(X-i+1)(X-i-1)\dots(X-n)}{i(i-1)(i-2)\dots(i-i+1)(i-i-1)\dots(i-n)}$$

$$\begin{aligned} \Rightarrow P(n+1) &= \sum_{i=0}^n e^i \frac{(n+1)!}{(n+1-i) i! (-1)^{n-i} (n-i)!} = \sum_{i=0}^n e^i (-1)^{n-i} \frac{(n+1)!}{i! (n-i+1)!} \\ &= \sum_{i=0}^n e^i (-1)^{n-i} \binom{n+1}{i} = - \sum_{i=0}^{n+1} e^i (-1)^{n+1-i} \binom{n+1}{i} + e^{n+1} = e^{n+1} - (e-1)^{n+1} \end{aligned}$$

$$\Rightarrow P(n+1) - e^{n+1} = -(e-1)^{n+1}$$

Autre méthode :

$$P = 1 + (e-1)X + (e-1)^2 \frac{X(X-1)}{2} + (e-1)^3 \frac{X(X-1)(X-2)}{6} + \dots + (e-1)^n \frac{X(X-1)\dots(X-n)}{n!}$$

car ce polynôme vérifie bien $P(i) = \sum_{k=0}^i (e-1)^k \binom{i}{k} = e^i$ et $\deg(P) \leq n$.

$$\text{On a ensuite } P(n+1) = \sum_{k=0}^n (e-1)^k \binom{n+1}{k} = \sum_{k=0}^{n+1} (e-1)^k \binom{n+1}{k} - (e-1)^{n+1} = e^{n+1} - (e-1)^{n+1}$$

Sol.18) a) On vérifie facilement que ce sont des sous-espaces vectoriels. Par ailleurs, une base de F est X, X^2, \dots, X^{2n} , et une base de G est $(X^2-1)(X^2-4)\dots(X^2-n^2)$. $F \cap G = \{0\}$ car un élément de $F \cap G$ est un polynôme de degré inférieur ou égal à n mais qui admet les $n+1$ racines $0, \pm 1, \pm 2, \dots, \pm n$. Il est donc nul. On a par ailleurs $\dim(F) = 2n$, $\dim(G) = 1$ et :

$$\dim(F \oplus G) = \dim(F) + \dim(G) = 2n + 1 = \dim(E)$$

donc $E = F \oplus G$.

b) Si P est un polynôme écrit sous la forme :

$$P = a_1 X + a_2 X^2 + \dots + a_n X^n + \lambda (X^2-1)(X^2-4)\dots(X^2-n^2)$$

alors $\lambda = \frac{P(0)}{(-1)^n (n!)^2}$. Donc le projeté de P sur G parallèlement à F est :

$$\frac{P(0)}{(-1)^n (n!)^2} (X^2-1)(X^2-4)\dots(X^2-n^2)$$

