Anneaux des polynômes

Pour étudier l'équation algébrique $x^3 - 3x^2 + 2 = 0$ il peut être intéressant d'introduire la fonction polynomiale $f : x \mapsto x^3 - 3x^2 + 2$ et d'en étudier les variations. Mais pour aller plus loin nous allons introduire le polynôme $P = x^3 - 3x^2 + 2$ afin de nous intéresser non plus à la variable x mais aux coefficients des puissances de x.

Polynôme

Quelle différence y a-t-il entre fonction polynomiale et polynôme ?

Dans une fonction polynomiale, la lettre x désigne la variable : il s'agit d'un nombre réel ou d'un nombre complexe selon le domaine de définition considéré.

Pour un polynôme, la lettre x ne désigne plus un élément variant dans un ensemble mais sert seulement à repérer les coefficients du polynôme en question, on dit que x est une indéterminée. Dans l'exemple initial, le coefficient de degré 3 du polynôme P vaut 1, celui de degré 2 vaut –3, celui de degré 1 est nul et enfin le coefficient constant vaut 0.

En fait un polynôme n'est rien d'autre que la liste de ses coefficients et deux polynômes sont égaux si et seulement s'ils ont les mêmes coefficients : c'est le principe d'identification des coefficients polynomiaux.

Pour un polynôme non nul, la plus grande puissance de x affectée d'un coefficient non nul est appelée degré de ce polynôme. Ci-dessus le degré du polynôme P est égal à 3. Il est usuel de poser le degré du polynôme nul égal à $-\infty$, c'est une convention.

Il est facile de retourner du polynôme à la fonction polynomiale, il suffit pour cela de savoir évaluer un polynôme P en n'importe quel nombre a. Ceci s'obtient en substituant à chaque puissance de l'indéterminée x la puissance correspondante de a, la valeur ainsi obtenue est notée $P(a)$. Lorsque celle-ci est nulle on dit que a est une racine (ou un zéro) du polynôme P. Désormais, résoudre une équation algébrique revient à déterminer les racines d'un polynôme. Par exemple le théorème de D'Alembert Gauss (cf. article) s'énonce en termes polynomiaux :

Tout polynôme non constant admet au moins une racine complexe.

L'anneau des polynômes

En opérant sur les coefficients des polynômes il est aisé de définir l'addition et la multiplication de deux polynômes. Ainsi pour

$$P = a_0 + a_1x + a_2x^2 + \cdots \text{ et } Q = b_0 + b_1x + b_2x^2 + \cdots,$$

on pose :

$$P + Q = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots \text{ et } PQ = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots$$

Les opérations ainsi définies possèdent les mêmes propriétés que les opérations correspondantes sur les entiers relatifs, cela permet de dire que l'ensemble des polynômes est muni d'une structure d'anneau commutatif. On peut aussi remarquer les propriétés :

$$\deg(P+Q) \le \max(\deg P, \deg Q) \text{ et}$$
$$\deg(PQ) = \deg P + \deg Q .$$

Arithmétique polynomiale

Comme sur les nombres entiers, il est possible de faire de l'arithmétique avec les polynômes. Pour commencer nous disposons d'une division euclidienne : si A et B sont deux polynômes avec B non nul, il existe d'uniques polynômes Q et R tels qu'on ait

$$A = BQ + R \text{ et } \deg R < \deg B .$$

Q et R sont alors appelés quotient et reste de la division euclidienne de A par B.

A partir de cette division euclidienne, on retrouve les notions arithmétiques usuelles, par exemple, on dit que B divise A lorsque le reste de la division euclidienne

Division euclidienne

La division euclidienne d'un polynôme A par un polynôme non nul B se pose comme une division entre entiers. On commence par rechercher le plus grand monôme qui multiplié par le polynôme B permet d'égaler la plus grande puissance du polynôme A. On retranche alors de A le produit obtenu et on recommence cette manipulation jusqu'à obtenir un polynôme de degré strictement inférieur à celui de B. On lit enfin quotient et reste aux places usuelles.

$$\begin{array}{lr|l}
 & x^3 - x^2 + 1 & x^2 + x + 1 \\ \cline{3-3}
- & x^3 + x^2 + x & x - 2 \\ \cline{1-2}
= & -2x^2 - x + 1 & \\
- & -2x^2 - 2x - 2 & \\ \cline{1-2}
= & x + 3 &
\end{array}$$

Ci-dessus $A = x^3 - x^2 + 1, B = x^2 + x + 1, Q = x - 2$ et $R = x + 3$.

correspondante est nul. On peut aussi parler de PGCD et de PPCM de deux polynômes et tout comme avec les nombres entiers, l'algorithme d'Euclide permet de calculer le PGCD de deux polynômes par une succession de divisions euclidiennes diviseur par reste.

Arithmétique et racines

Le reste de la division euclidienne d'un polynôme P par $x-a$ est un polynôme de degré strictement inférieur à 1, c'est donc un polynôme constant et cette division euclidienne s'écrit :

$$P=(x-a)Q+C^{te}$$

En évaluant cette relation en a, on obtient $C^{te}=P(a)$. Ainsi on démontre que le polynôme $x-a$ divise P si et seulement si a est racine de P : on retrouve ainsi la possibilité qu'il y a de factoriser par $(x-a)$ une équation algébrique dont a est racine (cf. article). De plus, en posant la division euclidienne comme ci-dessus, on peut déterminer le facteur correspondant.

Cette caractérisation arithmétique des racines d'une équation algébrique ne s'arrête pas là, on peut aussi définir la multiplicité d'une racine a d'un polynôme P comme étant la plus grande puissance de $(x-a)$ divisant P. Par exemple 1,2 et 3 sont racines respectivement simple, double et triple du polynôme

$$P=(x-1)(x-2)^2(x-3)^3$$

Algorithme de Horner

Lorsque a est racine d'un polynôme P, on peut factoriser P par $x-a$ et le facteur correspondant est obtenu en posant la division euclidienne de P par $x-a$. La méthode de Horner permet de réaliser efficacement cette division sur trois lignes. On dispose en première ligne les coefficients du polynôme P par puissance décroissante. On commence par abaisser sur la dernière ligne le coefficient de la première colonne. On le multiplie par a, on place le résultat sur la deuxième ligne à la colonne suivante. On abaisse ensuite la différence sur cette colonne et on reprend le processus. Sauf erreur de calcul, la dernière valeur doit être nulle. On lit enfin les coefficients du quotient cherché sur la dernière ligne.

1	-1	-5	2
	2	-6	2
1	-3	1	0

Ci-dessus $P=x^3-x^2-5x+2$, $a=2$ et on obtient le facteur x^2-3x+1.

Décomposition en facteurs irréductibles

Si $a,b,\ldots,s$ désignent toutes les racines complexes d'un polynôme non constant et si leurs multiplicités respectives sont $\alpha,\beta,\ldots,\sigma$, on peut factoriser P par $(x-a)^\alpha(x-b)^\beta\ldots(x-s)^\sigma$. Le facteur correspondant n'aura alors plus de racines complexes et d'après le théorème de D'Alembert Gauss il sera constant, égal à un certain complexe λ. Ainsi tout polynôme non constant P à coefficients complexes peut s'écrire sous la forme :

$$P=\lambda(x-a)^\alpha(x-b)^\beta\ldots(x-s)^\sigma$$

avec $\lambda\in\mathbb{C}^*$, $a,b,\ldots,s\in\mathbb{C}$ les racines complexes de P et $\alpha,\beta,\ldots,\sigma\in\mathbb{N}^*$ leurs multiplicités respectives.

De cette factorisation, on tire que la somme des multiplicités des racines d'un polynôme P est égale à son degré. Ainsi les équations de degré 2, ont deux racines, celles de degré 3, ont trois racines, quitte à compter ces dernières avec multiplicité, etc.

La factorisation du polynôme P présentée ci-dessus est appelée la décomposition en facteurs irréductibles du polynôme P, elle est unique. On peut faire un parallèle avec la décomposition d'un nombre entier en produit de nombres premiers : dans le cadre des polynômes, les termes $x-a$ jouent le rôle des nombres premiers.

Relations entre coefficients et racines d'un polynôme

Résoudre une équation algébrique revient à déterminer les racines d'un polynôme à partir de la connaissance de ses coefficients. Le problème inverse, déterminer les coefficients connaissant les racines, est beaucoup plus facile et se résout par simple développement. Introduisons un polynôme P de degré $n\in\mathbb{N}^*$. Par la factorisation présentée ci-dessus, on peut écrire :

$$P=\lambda(x-a_1)(x-a_2)\ldots(x-a_n)$$

en introduisant les n racines $a_1,a_2,\ldots,a_n$ du polynôme P, celles-ci étant comptées avec multiplicité c'est-à-dire chacune apparaissant autant de fois dans la liste qu'elle est racine multiple de P : une racine simple apparaît une fois, une racine double deux fois etc.

Le développement général du produit ci-dessus est un peu lourd et ne nécessite pas de figurer ici, on le trouvera dont tout cours d'algèbre du premier cycle universitaire. Néanmoins une fois celui-ci réalisé, on est capable d'exprimer les coefficients du polynôme en fonction de ses racines. Voyons les cas des degrés 2 et 3.

Cas du degré 2

Un polynôme P de degré 2 possède deux racines a et b (avec éventuellement $a=b$ dans le cas où P serait de discriminant nul). Comme vu ci-dessus, on peut alors factoriser P sous la forme

$$P=\lambda(x-a)(x-b)$$

et en développant :

$$P=\lambda(x^2-(a+b)x+ab)\,.$$

Cette relation détermine les coefficients du polynôme P au coefficient de proportionnalité λ près, on ne peut pas préciser mieux ce dernier sauf si par exemple on connaît le coefficient de la plus grande puissance de x.

La résolution des systèmes somme/produit est une application courante du résultat ci-dessus : si l'on connaît la somme S et le produit P de deux inconnues, on peut affirmer que celles-ci sont les racines de l'équation algébrique :

$$x^2-Sx+P=0$$

En résolvant cette dernière, on résout le système étudié

Un problème électrique

Deux résistances ont une résistance équivalente égale à 20Ω lorsqu'elles sont montées en parallèle et égale à 90Ω lorsqu'elles sont montées en série. Que valent ces résistances ?

Ce problème revient à résoudre le système $\begin{cases}1/x+1/y=1/20\\ x+y=90\end{cases}$ qui est équivalent au système somme/produit $\begin{cases}x+y=90\\ xy=180\end{cases}$ Les solutions de celui-ci sont les racines de l'équation $t^2-90t+180=0$. Les résistances cherchées valent 30Ω et 60Ω.

Cas du degré 3

Etudions maintenant le cas d'un polynôme P de degré 3.
Celui-ci possède trois racines a,b,c comptées avec multiplicité. Par la factorisation de P, on obtient :

$$P=\lambda(x-a)(x-b)(x-c)$$

Pour développer cette expression, il est usuel d'introduire les quantités suivantes appelées expressions symétriques élémentaires :

$$\begin{cases}\sigma_1=a+b+c\\ \sigma_2=ab+bc+ca\\ \sigma_3=abc\end{cases}$$

et on observe

$$P=\lambda(x^3-\sigma_1x^2+\sigma_2x-\sigma_3)\,.$$

En application de ce résultat, nous pouvons résoudre les systèmes à partir desquels il est possible de déterminer la somme σ_1 de trois inconnues, la somme σ_2 des doubles produits et le produit σ_3 de ces inconnus. Cela permet par exemple de résoudre le système suivant :

$$\begin{cases}a+b+c=1\\ a^2+b^2+c^2=9\\ a^3+b^3+c^3=1\end{cases}$$

Si (a,b,c) est un triplet solution alors $\sigma_1=1$. On obtient $\sigma_2=-4$ en observant :

$$(a+b+c)^2=a^2+b^2+c^2+2\sigma_2$$

Enfin on obtient $\sigma_3=-4$, en vérifiant :

$$(a+b+c)^3=3(a+b+c)(a^2+b^2+c^2)-2(a^3+b^3+c^3)+6\sigma_3$$

Ainsi a,b,c sont les racines de l'équation

$$x^3-x^2-4x+4=0$$

Après résolution, on obtient que a,b,c correspondent à l'ordre près à $1,2$ et -2.

La résolution de l'équation du troisième degré par la méthode de Lagrange

Notons a,b,c les trois racines comptées avec multiplicité d'une équation de degré 3. Compte tenu de ce qui précède, nous pouvons calculer les quantités $\sigma_1,\sigma_2,\sigma_3$ à l'aide des coefficients de l'équation étudiée. Introduisons le nombre complexe $j=\mathrm{e}^{2i\pi/3}$ et rappelons que celui-ci vérifie les relation $j^3=1$ et $1+j+j^2=0$. Posons $f=a+jb+j^2c$ et $g=a+j^2b+jc$. Les quantités f et g ne sont pas des expressions symétriques en

a,b,c mais en revanche f^3+g^3 et f^3g^3 le sont. On peut alors montrer qu'il est possible d'exprimer ces quantités en fonction de σ_1, σ_2 et σ_3 puis finalement de déterminer f et g par extraction de racine cubique. On peut alors calculer a,b,c par les formules :

$$a=\frac{\sigma_1+f+g}{3},b=\frac{\sigma_1+jf+j^3g}{3},c=\frac{\sigma_1+j^2f+jg}{3}$$

En observant qu'un principe analogue de réduction du problème pouvait être suivi pour la résolution des équations degré 4, mais pas pour les équations de degré cinq, Lagrange mettait en place les premières étapes qui conduirent, au début du XIX$^{\text{ème}}$ siècle à la démonstration pas les mathématiciens Abel et Galois de l'impossibilité de résolution par radicaux des équations de degrés supérieurs à cinq.