Cours groupe C : Polynômes

Noé Fisher

8 Décembre 2024

Définition : Loi de composition interne

On considère un ensemble quelconque E. On dit alors que $*$ est une **loi de composition interne** (lci) sur E si $*$ est une application de $E \times E$ (l'ensemble des couples d'éléments de E) dans E.
Pour $(x, y) \in E \times E$, on notera par la suite $x * y$ l'image du couple (x, y) par $*$.

Exemples

Pour $E = \mathbb{N}$ (l'ensemble des entiers naturels).

- l'addition $(+)$ est bien une lci sur $\mathbb{N}$, car pour tout $(n, m) \in \mathbb{N}^2, n+m \in \mathbb{N}$.
- la soustraction $(-)$ n'est pas une lci sur $\mathbb{N}$. Par exemple, avec le couple $(0, 1)$, on a $0 - 1 \notin \mathbb{N}$. En revanche, c'est une lci sur $\mathbb{Z}$ (entiers relatifs).

Vocabulaire

Une lci $*$ sur E est dite

- **associative** si pour tout $(x, y, z) \in E^3, (x * y) * z = x * (y * z)$.
- **commutative** si pour tout $(x, y) \in E^2, x * y = y * x$.
- **unifère** s'il existe un **élément neutre** $e \in E$ tel que pour tout $x \in E$, $e * x = x * e = x$.
  (Remarque : si $*$ est associative, il y a au plus un élément neutre.)
- **inversible** si elle possède un élément neutre et que pour tout $x \in E$, x possède un **inverse** $x^{-1} \in E$ tel que $x * x^{-1} = x^{-1} * x = e$.

Définition : Anneau

Un ensemble $\mathbb{A}$ muni de deux lci $+$ et $\cdot$ est un **anneau** si

- $+$ est associative, commutative, et inversible (on note $0_{\mathbb{A}}$ son unique élément neutre).
- $\cdot$ est associative et unifère (on note $1_{\mathbb{A}}$ l'unique élément neutre).
- . est **associative** sur $+$, c'est-à-dire que :
  $\forall (a,b,c) \in \mathbb{A}^3 : a \cdot (b+c) = a \cdot b + a \cdot c$ et
  $\forall (x,y,z) \in \mathbb{A}^3, (x+y) \cdot z = x \cdot z + y \cdot z$

Si $\cdot$ est commutative, on dit que $(\mathbb{A}, +, \cdot)$ est un **anneau commutatif**.
Si tout élément autre que $0_{\mathbb{A}}$ possède un inverse pour $\cdot$, on dit que $(\mathbb{A}, +, \cdot)$ est un **corps (commutatif)**.

Exemples

- $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif.
- l'ensemble des nombres rationnels $(\mathbb{Q}, +, \cdot)$, celui des nombres réels $(\mathbb{R}, +, \cdot)$ et celui des nombres complexes $(\mathbb{C}, +\cdot)$ sont tous trois des corps commutatifs.
- $(\mathbb{N}, +, \cdot)$ n'est pas un anneau (1 n'a pas d'inverse pour $+$ par exemple)
- soit $n \in \mathbb{N}$ avec $n \geq 2$, l'ensemble des entiers modulo n $\mathbb{Z}/n\mathbb{Z}$ peut-être muni d'une structure d'anneau commutatif.
  $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est un nombre premier.

Définition : Polynôme

On considère un anneau commutatif $(\mathbb{A}, +, \cdot)$ formellement, un polynôme à coefficients dans $\mathbb{A}$ est une suite à valeurs dans $\mathbb{A}$ qui est nulle à partir d'un certain rang : $P = (a_0, a_1, \ldots, a_d, 0, 0, 0, \ldots)$.

Si le polynôme est non-nul, l'indice du dernier terme non-nul est le **degré** du polynôme. On le note $\deg(P)$.
(On considère parfois par convention que le degré du polynôme nul est $-\infty$).

Le dernier terme non-nul (a_d) est appelé **coefficient dominant** de P, et son premier terme (a_0) est appelé **terme indépendant**.
Si le coefficient dominant vaut $1_{\mathbb{A}}$, P est dit **unitaire**.

Sommme et produit de convolution

Pour deux polynômes $P = (a_0, a_1, \ldots, a_d, 0, 0, 0, \ldots)$ et $Q = (b_0, b_1, \ldots, b_m, 0, 0, 0, \ldots)$, avec sans perte de généralité, $m \geq d$, on définit le polynôme $P + Q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots a_m + b_m, 0, \ldots)$.
On obtient $\boxed{\deg(P+Q) \leq \max(\deg(P), \deg(Q))}$.

On définit aussi le polynôme $P \cdot Q = (c_0, c_1, \ldots)$ tel que

$$\forall n \in \mathbb{N}, c_n = \sum_{k=0}^{n} a_k b_{n-k} = a_n b_0 + a_{n-1} b_1 + \ldots + a_1 b_{n-1} + a_0 b_n.$$

On obtient $\boxed{\deg(P+Q) = \deg(P) + \deg(Q)}$

Notations

À partir de maintenant on va noter un polynôme $P = (a_0, a_1, \ldots, a_d, 0, 0, 0, \ldots)$ ainsi : $P = a_d X^d + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$, où X est une indéterminée formelle.
On note dès lors $\mathbb{A}[X]$ l'ensemble des polynômes à coefficients dans un anneau $\mathbb{A}$, et on a que $(\mathbb{A}[X], +, \cdot)$ est un anneau commutatif.

Remarque

On peut donc définir des polynômes à coefficients dans $\mathbb{A}[X]$, et l'on obtient $\mathbb{A}[X][Y] = \mathbb{A}[X, Y]$ l'anneau des polynômes à deux indéterminées et à coefficients dans $\mathbb{A}$.

Évaluation

On considère $(\mathbb{B}, \tilde{+}, \tilde{\cdot})$ un anneau non-nécessairement commutatif et qui contient $\mathbb{A}$ (toujours le même anneau commutatif). Soit $x \in \mathbb{B}$. On définit l'évaluation d'un polynôme en x :

$$\delta_x : \begin{cases} \mathbb{A}[X] & \to & \mathbb{B} \\ P = a_d X^d + \ldots + a_0 & \mapsto P(x) = a_d \tilde{\cdot} x^d \tilde{+} \ldots \tilde{+} a_0 \end{cases}$$

On a les propriétés suivantes :
$\forall P, Q \in \mathbb{A}[X], \delta_x(P+Q) = \delta_x(P) \tilde{+} \delta_x(Q)$, ie $(P+Q)(x) = P(x) \tilde{+} Q(x)$

$\forall P, Q \in \mathbb{A}[X], \delta_x(P \cdot Q) = \delta_x(P) \tilde{\cdot} \delta_x(Q) = \delta_x(Q) \tilde{\cdot} \delta_x(P)$, ie
$(P \cdot Q)(x) = P(x) \tilde{\cdot} Q(x) = Q(x) \tilde{\cdot} P(x)$

Fonctions polynomiales

Avec $\mathbb{B} = \mathbb{A}$, on peut définir la **fonction polynomiale** $\tilde{P}$ associée à P.

$$\tilde{P} : \begin{cases} \mathbb{A} & \to \mathbb{A} \\ x & \mapsto P(x) \end{cases}$$

Généralement, on va avoir tendance à confondre fonctions polynomiales et polynômes associés, et noter P la fonction $\tilde{P}$.

Remarque : Attention, dans certains anneaux, une même fonction polynomiale peut être obtenue à partir de plusieurs polynômes différents. Par exemple, dans $\mathbb{Z}/n\mathbb{Z}$, le polynôme $P = (X-1)(X-2)\dots(X-n)$ a la même fonction polynomiale que le polynôme nul.

Composition de polynômes

En prenant $\mathbb{B} = \mathbb{A}[X]$, on peut évaluer un polynôme P en un autre polynôme R, et obtenir un polynôme $P(R)$.
On remarque alors que la fonction polynomiale associée à $P(R)$ va coïncider avec $\tilde{P} \circ \tilde{R}$ (la composée des deux fonctions polynomiales).
Cela signifie que l'on peut écrire pour tout $x \in \mathbb{A}$: $(P(R))(x) = P(R(x))$

Exemple

On peut donc considérer à partir d'un polynôme P des polynômes tels que $P(X^2), P(X+1), P(2X)$, etc.

Définition : diviseurs et multiples

• Comme dans $\mathbb{Z}$, on peut dire pour $P, Q \in \mathbb{A}[X]$ que Q divise P (noté $Q \mid P$), ou que Q est un diviseur de P, ou encore que P est un multiple de Q s'il existe $R \in \mathbb{A}[X]$ tel que $P = Q \cdot R = R \cdot Q$.

• la notion de nombres premiers peut aussi se généraliser : on dit qu'un polynôme P de degré $d \geq 1$ est **irréductible** si tous ses diviseurs sont de degrés 0 ou d.

On considère à présent un corps commutatif $\mathbb{K}$.

Division euclidienne

Soit $P, Q \in \mathbb{K}[X]$, avec Q **différent du polynôme nul**.
Il existe alors un unique couple de polynômes (D, R) tels que

- $\deg(R) < \deg(Q)$, et
- $P = D \cdot Q + R$

Démonstration

Existence :

Avec $m = \deg(Q)$, on fait une récurrence sur $n = \deg(P)$.

• si $n < m$, on prend $(D, R) = (0, P)$

• Soit $n \geq m$, on suppose la propriété vérifiée pour tout polynôme de degré strictement inférieur à n.

Soit a_n le coefficient dominant de P, et $b_m \neq 0$ celui de Q, comme on est dans un corps, on peut diviser par b_m.

On pose alors $Z = P - a_n X^{n-m} \cdot b_m^{-1} Q$, on remarque que $\deg(Z) < n$ (Z peut être nul), alors par hypothèse de récurrence, il existe U, V avec $\deg(V) < m$ tels que $Z = UQ + V$.

Enfin, $P = a_n X^{n-m} \cdot b_m^{-1} Q + Z = (a_n \cdot b_m^{-1} X^{n-m} + U)Q + V$, ce qui conclut.

Démonstration

Unicité :

Si $P = D_1Q + R_1 = D_2Q + R_2$, alors $(D_1 - D_2)Q = (R_2 - R_1)$.

Si $D_1 - D_2 \neq 0$, il vient

$\deg(Q) \leq \deg(D_1 - D_2) + \deg(Q) = \deg(R_1 - R_2) < \deg(Q)$.

C'est absurde, donc $D_1 - D_2 = 0$ puis $R_1 - R_2 = 0$

Exemple

Division de $X^4 - 3X^3 + X + 1$ par $X^2 - 2$

$$
\begin{array}{rrrrr|l}
X^4 & -3X^3 & & +X & +1 & X^2 - 2 \\
\cline{6-6}
X^4 & & -2X^2 & & & X^2 - 3X + 2 \\
\cline{1-5}
 & -3X^3 & +2X^2 & +X & +1 & \\
 & -3X^3 & & +6X & & \\
\cline{1-4}
 & & 2X^2 & -5X & +1 & \\
 & & 2X^2 & & -4 & \\
\cline{1-5}
 & & & -5X & +5 &
\end{array}
$$

Cela permet de généraliser énormément de résultats d'arithmétiques :

Propriétés

- Existence d'une décomposition en facteurs irréductibles dans $\mathbb{K}[X]$, et unicité à l'ordre des facteurs près.
- Existence d'un plus grand commun diviseur (PGCD) pour deux polynômes $P, Q \in \mathbb{K}[X]$. Afin d'assurer l'unicité, on impose que le PGCD soit unitaire, et on le note $P \wedge Q$.
- Théorème de Bézout : Soit $P, Q \in \mathbb{K}[X]$, on a $P \wedge Q = 1$ si et seulement si il existe $U, V \in \mathbb{K}[X]$ tels que $PU + QV = 1_{\mathbb{K}[X]}$

Racines et multiplicité

Un élément α de $\mathbb{A}$ est appelé **racine** de P si et seulement si $P(\alpha) = 0_{\mathbb{A}}$. On a l'équivalence suivante : (démonstration laissée en exercice)

a est une racine de P si et seulement si le polynôme $X - \alpha$ divise P.

Si P n'est pas le polynôme nul, on appelle **multiplicité** de la racine α le plus grand entier m tel que $(X - \alpha)^m \mid P$.
Cet entier m est caractérisé par l'existence d'un polynôme Q tel que $P(X) = (X - \alpha)^m Q(X)$ et $Q(\alpha) \neq 0$
On dit qu'une racine est **simple** si elle est de multiplicité 1 et **multiple** sinon.

Remarque

On en déduit les deux corollaires suivants :

- Si P est non-nul, la somme des multiplicités des racines de P est inférieure ou égale à $\deg(P)$
- En particulier, un polynôme de degré au plus n et qui admet au moins $n+1$ racines distinctes est obligatoirement le polynôme nul.

Polynôme dérivé

En partant de $P = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_1 X + c_0 \in \mathbb{A}[X]$, on peut définir le polynôme dérivé $P' = n c_n X^{n-1} + (n-1) c_{n-1} X^{n-2} + \ldots + c_1$. (Si $\mathbb{A} = \mathbb{R}$, on remarque que la fonction polynomiale associée au polynôme dérivé coïncide avec la dérivée de la fonction polynomiale de P.)

Proposition

On se place à nouveau dans un corps $\mathbb{K}$. Alors $\alpha \in \mathbb{K}$ est une racine de multiplicité m de $P \in \mathbb{K}[X]$ si et seulement si

$$\boxed{P(\alpha) = P'(\alpha) = \ldots = P^{(m-1)}(\alpha) = 0_{\mathbb{K}} \text{ mais } P^{(m)}(\alpha) \neq 0_{\mathbb{K}}.}$$

Définition

Le polynôme $P \in \mathbb{K}[X]$ est dit **scindé sur le corps** $\mathbb{K}$ si et seulement s'il se décompose en produits de polynômes de degré 1 dans $\mathbb{K}[X]$:

$$P(X) = c_n(X - r_1) \cdot (X - r_2) \cdot \ldots \cdot (X - r_n)$$

Exemple

- Le polynôme $X^2 - 1 = (X - 1)(X + 1)$ est scindé sur les corps $\mathbb{Q}$ et $\mathbb{R}$
- $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ est aussi scindé sur $\mathbb{R}$ mais pas sur $\mathbb{Q}$, car $\sqrt{2} \notin \mathbb{Q}$.
- $X^2 + 1 = (X - i)(X + i)$ est scindé sur $\mathbb{C}$ mais pas sur $\mathbb{R}$ (ni $\mathbb{Q}$).

Corps algébriquement clos

Un **corps algébriquement clos** est un corps $\mathbb{K}$ vérifiant l'une des trois propriétés équivalentes suivantes :

- tout polynôme non-constant de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$.
- tout polynôme non-constant de $\mathbb{K}[X]$ possède au moins une racine dans $\mathbb{K}$.
- les seuls polynômes irréductibles de $\mathbb{K}[X]$ sont ceux de degré 1.

Théorème de D'Alembert-Gauss/Théorème fondamental de l'algèbre

$\mathbb{C}$, le corps des nombres complexes est algébriquement clos.

Proposition

À l'aide du théorème précédent on peut caractériser les irréductibles de $\mathbb{R}[X]$. Il s'agit des polynômes de degré 1 et de ceux de degré 2 ne possédant pas de racines réelles (c'est-à-dire) ceux dont le discriminant est < 0).

On en déduit : Soit $P \in \mathbb{R}[X]$ un polynôme de degré n. Il existe k nombres réels $r_1, \ldots, r_k$ et l polynômes $Q_1, \ldots Q_l \in \mathbb{R}[X]$ unitaires irréductibles du second degré avec $k + 2l = n$ tels que

$$P(X) = c_n(X - r_1) \ldots (X - r_k)Q_1(X) \ldots, Q_l(X),$$

où c_n est le coefficient dominant de P.

Polynôme interpolateur de Lagrange

On considère un entier $n \geq 1$ et un corps (commutatif) $\mathbb{K}$. On se donne n éléments deux à deux distincts $a_1, \ldots, a_n \in \mathbb{K}$, et n autres éléments (non-nécessairement distincts) $b_1, \ldots, b_n \in \mathbb{K}$. Il existe alors un unique polynôme $P \in K_{n-1}[X]$ (ie de degré inférieur ou égal à n) tel que $\forall k \in [\![1, n]\!], P(a_k) = b_k$.
Il s'agit du polynôme

$$P(X) = \sum_{i=1}^{n} \left(b_i \cdot \prod_{j \neq i} \frac{X - a_j}{a_i - a_j} \right).$$

Soit $\mathbb{K}$ un corps algébriquement clos (par exemple $\mathbb{C}$), et $P(X) = c_n X^n + c_{n-1}X^{n-1} + \ldots + c_1 X + c_0 \in \mathbb{K}[X]$.
En notant $r_1, r_2, \ldots, r_n$ les racines de P dans $\mathbb{K}$, on trouve :

$$\begin{cases} r_1 + r_2 + \ldots + r_n = -\frac{c_{n-1}}{c_n} \\ r_1r_2 + r_1r_3 + \ldots + r_1r_n + r_2r_3 + \ldots + r_{n-1}r_n = \frac{c_{n-2}}{c_n} \\ r_1r_2r_3 + r_1r_2r_4 + \ldots + r_1r_2r_n + r_1r_3r_4 + \ldots + r_{n-2}r_{n-1}r_n = -\frac{c_{n-3}}{c_n} \\ \quad \vdots \\ r_1r_2 \ldots r_n = (-1)^n \cdot \frac{c_0}{c_n} \end{cases}$$

ce qui peut aussi s'écrire :

$$\forall k \in [\![1, n]\!], \sum_{i_1 < \ \ldots \ < i_k} r_{i_1} r_{i_2} \ldots r_{i_k} = (-1)^k \cdot \frac{c_{n-k}}{c_n}.$$