

# HAI820I Calcul Formel — TDs et TPs

Ivan Lejeune

30 janvier 2026

## Table des matières

1	Structures mathématiques . . . . .	2
2	Arithmétique des polynomes . . . . .	4
2.1	Multiplication et addition naïve . . . . .	4
2.2	Multiplication de Karatsuba . . . . .	4
2.3	Evaluation et Interpolation . . . . .	4
2.4	Racines de l'unité et FFT . . . . .	4
2.5	Division euclidienne . . . . .	5
2.6	Produit de matrices . . . . .	6
2.7	Algèbre linéaire rapide : réduction au produit de matrices . . . . .	6

# 1 Structures mathématiques

**Exercice 1.1 Objectif.** Identifier les propriétés d'un groupe (neutre, inverses, commutativité) à partir d'une table d'opérations symbolique.

Soit  $G = \{\alpha, \beta, \gamma, \delta\}$  un ensemble muni d'une loi de composition interne  $*$ . La table de l'opération est donnée ci-dessous (où l'entrée à la ligne  $i$  et la colonne  $j$  correspond à  $i * j$ ) :

*	$\alpha$	$\beta$	$\gamma$	$\delta$
$\alpha$	$\alpha$	$\beta$	$\gamma$	$\delta$
$\beta$	$\beta$	$\alpha$	$\delta$	$\gamma$
$\gamma$	$\gamma$	$\delta$	$\alpha$	$\beta$
$\delta$	$\delta$	$\gamma$	$\beta$	$\alpha$

- Identification de l'élément neutre :** Quel est l'élément neutre  $e$  de ce groupe ? Justifiez votre réponse en observant les lignes et colonnes du tableau.
- Recherche d'inverses :** Pour chaque élément  $x$  de  $G$ , trouver son inverse  $x^{-1}$  (l'unique élément tel que  $x * x^{-1} = e$ ). Que remarquez-vous sur l'inverse de  $\gamma$  ?
- Commutativité :** Le groupe  $(G, *)$  est-il abélien (commutatif) ?
- Résolution d'équation :** A l'aide de la table, résoudre l'équation suivante d'inconnue  $x$  :

$$\gamma * x = \delta$$

## Solution.

- La seule ligne (et colonne) qui ne modifie aucun élément est celle de  $\alpha$  donc  $e = \alpha$ .

- On a

$$\begin{cases} \alpha^{-1} = \alpha \\ \beta^{-1} = \beta \\ \gamma^{-1} = \gamma \\ \delta^{-1} = \delta \end{cases}$$

On remarque que  $\gamma$  est son propre inverse.

- On a bien  $\forall x, y \in G, x * y = y * x$  car le tableau est symétrique par rapport à la diagonale. Donc  $(G, *)$  est abélien.
- On cherche dans le tableau l'élément  $x$  tel que  $\gamma * x = \delta$ . On trouve  $x = \beta$ .

## Exercice 1.2.

On se place dans l'anneau  $(M_2(\mathbb{R}), +, \cdot)$ . On considère les matrices suivantes :

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

- Calculer le produit  $A \cdot B$  puis le produit  $B \cdot A$ .
- L'anneau  $M_2(\mathbb{R})$  est-il commutatif ?
- Calculer  $A^2$ .
- Pourquoi cela empêche-t-il  $M_2(\mathbb{R})$  d'être un anneau intègre même s'il ne contient que des coefficients réels ?

## Solution.

1. On a

$$\begin{aligned} A \cdot B &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

et

$$\begin{aligned} B \cdot A &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

2. L'anneau  $M_2(\mathbb{R})$  n'est pas commutatif parce qu'on a trouvé deux éléments ( $A$  et  $B$ ) de  $M_2(\mathbb{R})$  tels que  $A \cdot B \neq B \cdot A$ .

3. On a

$$\begin{aligned} A^2 &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

4. On vient de trouver deux éléments de  $M_2(\mathbb{R})$  ( $A$ ) non nuls tels que  $A \cdot A = 0$ . Alors l'anneau  $M_2(\mathbb{R})$  n'est pas intègre.

### Exercice 1.3.

On travaille dans l'anneau de polynomes  $(\mathbb{Z}/6\mathbb{Z})[x]$ . Les coefficients sont calculés modulo 6. Soient  $P(x) = 2x^2 + 3$  et  $Q(x) = 3x + 1$

#### 1. Anomalie du degré

- Quels sont les degrés de  $P$  et  $Q$ ?
- Calculer le produit  $P(x) \cdot Q(x)$  en réduisant les coefficients modulo 6.
- Quel est le degré du polynôme résultant ? La propriété  $\deg(P \cdot Q) = \deg(P) + \deg(Q)$  est-elle vérifiée ? Expliquez pourquoi.

2. Echec de la division euclidienne standard. On considère les polynomes  $F(x) = x^2 + 1$  et  $G(x) = 2x$ . Essayez de poser la division euclidienne de  $F$  par  $G$ .

*Indice :* Pour éliminer le terme en  $x^2$ , vous devez multiplier  $2x$  par un coefficient  $k$  tel que  $2 \cdot k = 1 \pmod{6}$ . Un tel entier existe-t-il dans  $\mathbb{Z}/6\mathbb{Z}$ ? Conclure.

#### Solution.

1. Sur les degrés :

- $P$  est de degré 2 et  $Q$  de degré 1.
- On a

$$\begin{aligned} P \cdot Q &= (2x^2 + 3) \cdot (3x + 1) \pmod{6} \\ &= 6x^3 + 2x^2 + 9x + 3 \pmod{6} \\ &= 2x^2 + 3x + 3 \pmod{6} \end{aligned}$$

- Le degré du polynôme résultant est 2. La propriété  $\deg(P \cdot Q) = \deg(P) + \deg(Q)$  n'est pas vérifiée car l'anneau n'est pas intègre (par exemple  $2 \cdot 3 = 0 \pmod{6}$ ).

2.  $2$  ne possède pas d'inverse dans  $\mathbb{Z}/6\mathbb{Z}$  car  $2 \wedge 6 = 2$ . On ne peut donc pas poser la division euclidienne de  $F$  par  $G$  ici.

## 2 Arithmétique des polynomes

### 2.1 Multiplication et addition naive

#### Exercice 2.1.

Coder dans Sagemath les opérations d'addition et de multiplication de deux polynomes qui sont donnés par la liste de leurs coefficients. Le premier élément de la liste correspondra à l'élément constant du polynome. Vous testerez vos fonctions sur des polynomes aléatoires de degrés dans  $\{10, 100, 1000\}$  avec les domaines de coefficients suivants :  $\text{GF}(17)$ ,  $\mathbb{Z}$ ,  $\mathbb{Z}/100\mathbb{Z}$ . A chaque fois vous prendrez soin de faire des opérations impliquant aussi bien des polynomes de degrés identiques que des polynomes de degrés différents. Vous devrez comparer les résultats de vos calculs avec celui fait par les opérations natives d'addition et de multiplication de polynomes dans Sage.

**Solution.** On utilise le code suivant :

```
def poly_add(A, B, R):
    n = max(len(A), len(B))
    res = [R(0)] * n
    for i in range(n):
        a = A[i] if i < len(A) else 0
        b = B[i] if i < len(B) else 0
        res[i] += a + b
    res = normalise(res, R)
    return res
```

Code 1 – Fonction d'addition de polynomes

### 2.2 Multiplication de Karatsuba

#### Exercice 2.2 title.

#### Solution.

#### Exercice 2.3 title.

#### Solution.

#### Exercice 2.4 title.

#### Solution.

### 2.3 Evaluation et Interpolation

#### Exercice 2.5 title.

#### Solution.

### 2.4 Racines de l'unité et FFT

#### Exercice 2.6 title.

#### Solution.

 Exercice 2.7 title.

 Solution.

 Exercice 2.8 title.

 Solution.

 Exercice 2.9 title.

 Solution.

 Exercice 2.10 title.

 Solution.

 Exercice 2.11 title.

 Solution.

## 2.5 Division euclidienne

 Exercice 2.12 title.

 Solution.

 Exercice 2.13 title.

 Solution.

 Exercice 2.14 title.

 Solution.

 Exercice 2.15 title.

 Solution.

 Exercice 2.16 title.

 Solution.

 Exercice 2.17 title.

 Solution.

 Exercice 2.18 title.

 Solution.

 Exercice 2.19 title.

 Solution.

## 2.6 Produit de matrices

 Exercice 2.20 title.

 Solution.

## 2.7 Algèbre linéaire rapide : réduction au produit de matrices

 Exercice 2.21 title.

 Solution.

 Exercice 2.22 title.

 Solution.

 Exercice 2.23 title.

 Solution.

 Exercice 2.24 title.

 Solution.

 Exercice 2.25 title.

 Solution.

 Exercice 2.26 title.

 Solution.