Algèbre et Arithmétique Effectives — 26/11/24

cours 11

TD 6

Exercice 2

Rappel : Soit $(G, \cdot)$ un groupe et $H \subseteq G$, $H \neq \emptyset$. Alors $(H, \cdot)$ est un sous-groupe de G si $\forall\, a, b \in H$, $a \cdot b^{-1} \in H$.

$$GL_2(\mathbb{R}) = \{ A \in \mathcal{M}_2(\mathbb{R}) : \det(A) \neq 0 \}$$

(a) Montrer que

$$\varphi : (GL_2(\mathbb{R}), \cdot) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$$
$$A \longmapsto \det(A)$$

est un homomorphisme de groupes.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in GL_2(\mathbb{R})$.

Alors on a :

$$\varphi(AB) = \varphi \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} =$$

$$= (aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc')$$

$$= \cancel{aa'cb'} + aa'dd' + bc'cb' - \cancel{bc'dd'} +$$
$$- \cancel{ab'ca'} - ab'dc' - bd'ca' - \cancel{bd'dc'}$$

$$\varphi(A)\varphi(B) = (ad - bc)(a'd' - b'c') =$$
$$= ada'd' - adb'c' - bca'd' + bcb'c'$$

(b) $\mathrm{Ker}(\varphi) = \{ A \in \mathcal{M}_2(\mathbb{R}) : \det(A) = 1 \} \subseteq GL_2(\mathbb{R})$

$= SL_2(\mathbb{R})$

$\mathrm{Im}(\varphi) = \mathbb{R}\setminus\{0\}$, car $\forall\ x \in \mathbb{R}\setminus\{0\}$
la matrice $A_x = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ est telle que

$\det(A_x) = x$

D'après le premier théorème d'isomorphisme

$$\frac{GL_2(\mathbb{R})}{\mathrm{Ker}(\varphi)} \cong \mathrm{Im}(\varphi)$$

$$\Downarrow$$

$$\frac{GL_2(\mathbb{R})}{SL_2(\mathbb{R})} \cong \mathbb{R}\setminus\{0\}$$

$$[A]_{SL_2(\mathbb{R})} \longmapsto \det(A) \quad \text{(isomorphisme canonique)}$$

(c) $H_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R},\ (a,b) \neq (0,0) \right\}$

On remarque que $H_1 \subseteq GL_2(\mathbb{R})$, car

$$\det\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 \underset{(a,b)\neq(0,0)}{\neq} 0 \Rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in GL_2(\mathbb{R})$$

Montrons que $\forall\ A, B \in H_1$, $AB^{-1} \in H_1$

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in H_1$$

$$B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in H_1$$

Déterminons l'inverse de B dans $GL_2(\mathbb{R})$:

$$\begin{pmatrix} c & d \\ -d & c \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} ca' + dc' & cb' + dd' \\ -a'd + cc' & -db' + cd' \end{pmatrix}$$

$$\Longrightarrow \begin{cases} ca' + dc' = 1 \\ cb' + dd' = 0 \\ -a'd + cc' = 0 \\ -db' + cd' = 1 \end{cases}$$ ---- On peut résoudre le système (en supposant c ou $d \neq 0$)

Ou on se rappelle de la formule :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \Longrightarrow B^{-1} = \frac{1}{c^2+d^2} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in H_1$$

Donc :

$$AB^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \frac{1}{c^2+d^2} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} =$$

$$= \frac{1}{c^2+d^2} \begin{pmatrix} ac+bd & -ad+bc \\ -bc+ad & bd+ac \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{ac+bd}{c^2+d^2} & \frac{bc-ad}{c^2+d^2} \\ -\frac{bc-ad}{c^2+d^2} & \frac{ac+bd}{c^2+d^2} \end{pmatrix} \in H_1 .$$

iii) $H_3 = \left\{ \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} : a, b \in \mathbb{R}, \ a > 0 \right\}$

n'est pas un sous-groupe car $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin H_3$

d) Montrer que H_1 est isomorphe à $(\mathbb{C} \setminus \{0\}, \cdot)$

$$\varphi : \mathbb{H}_1 \longrightarrow \mathbb{C}\setminus\{0\}$$
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \longmapsto a+ib$$

- φ est un homomorphisme de groupes :
$$\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \varphi\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$
Laissé par exercice.

- φ est injective :

élément neutre de $\mathbb{C}\setminus\{0\}$

$$\mathrm{Ker}(\varphi) = \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{H}_1 : \varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = 1\right\} =$$
$$= \left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{H}_1 : a+ib = 1\right\} \quad \begin{matrix} a=1 \\ b=0 \end{matrix}$$
$$= \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \Rightarrow \varphi \text{ est injective}$$

- φ est surjective :

Soit $a+ib \in \mathbb{C}\setminus\{0\} \Rightarrow (a,b) \neq (0,0)$

Alors $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathbb{H}_1$ et $\varphi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+ib$.

Donc φ est un isomorphisme.

Cours

$$C = \begin{pmatrix} 2 & -3 & 1 & 0 \\ 3 & 0 & 5 & 6 \\ 5 & 1 & 1 & -2 \end{pmatrix} \in \mathcal{M}_{3,4}\left(\mathbb{Z}/7\mathbb{Z} \right)$$

$$\begin{pmatrix} 2 & -3 & 1 & 0 \\ 3 & 0 & 5 & 6 \\ 5 & 1 & 1 & -2 \end{pmatrix} \xrightarrow[\substack{L_2 \leftarrow L_2 + 2L_1 \\ L_3 \leftarrow L_3 + L_1}]{} \begin{pmatrix} 2 & -3 & 1 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 5 & 2 & 5 \end{pmatrix}$$

$$\xrightarrow[L_3 \leftarrow L_3 - 5L_2]{} \begin{pmatrix} 2 & -3 & 1 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 2 & 3 \end{pmatrix}$$ échelonné

Remarque : Une matrice ne possède pas une unique forme échelonnée à elle équivalente.

Algorithme : Gauss(A,b)

Entrée : Un système (A,b) à m équations et n inconnues

Sortie : Un système (A',b') équivalent à (A,b) sous forme échelonnée.

$(i,j) \leftarrow (1,1)$

Tant que $i \leq m$ et $j \leq n$:

on cherche un pivot

$i' \leftarrow \min\{k \geq i : A_{kj} \neq 0\}$ ou $i \leftarrow +\infty$ si $A_{kj} = 0, \forall k$

Si $i' = +\infty$: $j \leftarrow j+1$

Sinon :

Échanger les lignes i et i' de A et de b.

Pour $k = i+1, \ldots, m$:

$$\lambda = \frac{A_{kj}}{A_{i'j}}$$

transvection

$L_k \leftarrow L_k - \lambda L_i$

Pour $\ell = j, \ldots, n$:

$A_{k\ell} \leftarrow A_{k\ell} - \lambda A_{i\ell}$

$b_k \leftarrow b_k - \lambda b_i$

$(i,j) \leftarrow (i+1, j+1)$

Renvoyer (A,b)

Complexité : $\mathcal{O}(mn \cdot \overbrace{\min(n,m)}^{\text{nombre maximum de pivots}})$

Clairement cet algorithme est déterministe, c'est-à-dire que étant donné (A, b) il produira toujours la même forme échelonnée. Toutefois celle-ci n'est pas unique.

<u>Par l'unicité</u> : forme échelonnée réduite

<u>Déf</u> : Un système linéaire (une matrice) est sous forme échelonnée réduite si le système (la matrice) est échelonné, chaque pivot vaut 1 et c'est le seul élément non nul de sa colonne :

<u>Exemple</u> : $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

échelonnée, mais pas échelonnée réduite

$$\begin{pmatrix} 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$ échelonnée réduite.

<u>Exercice</u> : Utiliser des opérations élémentaires pour trouver <u>la</u> forme échelonnée réduite.

1. $\begin{pmatrix} 1 & -1 & 2 & -1 \\ 2 & 1 & -2 & -2 \\ -1 & 2 & -4 & 1 \\ 3 & 0 & 0 & -3 \end{pmatrix}$ sur $\mathbb{Q}$

2. $\begin{pmatrix} 2 & -3 & 1 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 0 & 2 & 3 \end{pmatrix}$ sur $\mathbb{Z}/7\mathbb{Z}$

1. $$\begin{pmatrix} 1 & -1 & 2 & -1 \\ 2 & 1 & -2 & -2 \\ -1 & 2 & -4 & 1 \\ 3 & 0 & 0 & -3 \end{pmatrix} \xrightarrow[\substack{L_2 \leftarrow L_2 - 2L_1 \\ L_3 \leftarrow L_3 + L_1 \\ L_4 \leftarrow L_4 - 3L_1}]{} \begin{pmatrix} 1 & -1 & 2 & -1 \\ 0 & 3 & -6 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 3 & -6 & 0 \end{pmatrix}$$

$$\xrightarrow[L_2 \leftrightarrow L_3]{} \begin{pmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -2 & 0 \\ 0 & 3 & -6 & 0 \\ 0 & 3 & -6 & 0 \end{pmatrix} \xrightarrow[\substack{L_3 \leftarrow L_3 - 3L_2 \\ L_4 \leftarrow L_4 - 3L_2}]{}$$

$$\begin{pmatrix} 1 & -1 & 2 & -1 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow[L_1 \leftarrow L_1 + L_2]{} \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

échelonnée réduite

Algorithme de Gauss-Jordan

L'algorithme de Gauss-Jordan est une suite d'opérations élémentaires qui permet de calculer la forme échelonnée réduite d'un système (d'une matrice)

I PARTIE : Algorithme de Gauss → forme échelonnée

II PARTIE : "transformer" les pivots en 1 et "effacer" les éléments non nuls au dessus de chaque pivot.

Gauss Jordan (A, b)

<u>Entrée</u> : un système (A,b) à m équation et n inconnues

<u>Sortie</u> : un système (A',b') équivalent à (A,b), sous forme échelonnée réduite.

$(A',b') \longleftarrow$ Gauss (A,b)

Pour $i = 1, \dots, m$

$j \leftarrow$ indice de colonne du pivot de la ligne i de A'

pivot $= 1$

Pour $l = j, \dots, n$.

$A'_{i,l} \longleftarrow A'_{i,l} / A'_{i,j}$

$b'_l \leftarrow b'_l / A'_{i,j}$

Pour $k=1, \dots, i-1$:

$\lambda = A'_{k,j}$

Pour $l = j$ à n :

$A'_{k,l} \leftarrow A'_{k,l} - \lambda A'_{i,l}$

$b'_k \leftarrow b'_k - \lambda b'_i$

Renvoyer (A', b').

<u>Notre but</u> : résoudre un système linéaire $AX = b$

$(A \mid b)$: matrice augmentée

$\downarrow$ Algorithme de Gauss Jordan

$(A' \mid b')$ matrice échelonnée réduite

Le système $A'X = b'$ est équivalent au système de départ. Quelles sont les solutions ?

<u>Exemple</u> : Exemple de matrice augmentée 3×5 échelonnée réduite dont le système correspondant est incompatible

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & -4 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \Rightarrow 0 = 1$$

Pour les solutions on a trois possibilités :

1) 0 solution (système incompatible)

$\Updownarrow$

Le dernier pivot de $(A'|b')$ appartient à la dernière colonne.

(la ligne du dernier pivot correspond à l'équation $0 = 1$)

Sinon, si le dernier pivot n'appartient pas à la dernière colonne :

2) 1 solution

$\Updownarrow$

A' n'a pas de colonnes sans pivots

$$\left(\begin{array}{c|c} I_n & \begin{matrix} b_1' \\ \vdots \\ b_n' \end{matrix} \\ 0 & 0 \end{array}\right) \Rightarrow (b_1', \ldots, b_n') \text{ est la solution du système}$$

3) ∞ solutions

$\Updownarrow$

A' a des colonnes sans pivots.

Les t colonnes qui ne contiennent pas de pivot correspondent à des variables libres et les solutions s'écrivent sous la forme

$$\left\{ s + \sum_{k=1}^{t} \lambda_i v_i,\ \lambda_1, \dots, \lambda_t \in K \right\} \quad \text{où} \quad v_1, \dots, v_t \in K^n.$$

s : solution particulière

Vision matricielle

$$A \in M_{m\times n}(K) \xrightarrow{\hspace{3cm}} A' \in M_{m\times n}(K)$$

A' : échelonnée réduite

opérations élémentaires

(Algorithme de Gauss-Jordan)

Est-ce qu'on peut interpréter ces opérations autrement ?

Exemple

$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{3\times 3} \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}}_{3\times 4} = \underbrace{\begin{pmatrix} 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 \\ 9 & 10 & 11 & 12 \end{pmatrix}}_{3\times 4}$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -5 & 0 & 1 \end{pmatrix}}_{3\times 3} \underbrace{\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}}_{3\times 2} \underset{L_3 \leftarrow L_3 - 5L_1}{=} \underbrace{\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 0 & -4 \end{pmatrix}}_{3\times 2}$$

Donc chaque opération élémentaire sur une matrice $\in \mathcal{M}_{m,n}(\mathbb{K})$ correspondant à la multiplication à gauche par la matrice obtenue de I_m en effectuant la même opération :

<u>Donc</u> : Algorithme de Gauss ou Gauss-Jordan

$\Updownarrow$

Multiplier à gauche par des matrices inversibles jusqu'à obtenir une matrice échelonnée ou échelonnée réduite

$$\underbrace{E_r \cdots E_2 E_1}_{\substack{\text{inversible,} \\ \text{car produit} \\ \text{de matrices} \\ \text{inversibles}}} A = \underset{\substack{\uparrow \\ \text{échelonnée} \\ \text{(réduite)}}}{A'}$$

<u>Déf</u> : Deux matrices $A, B \in \mathcal{M}_{m,n}(\mathbb{K})$ sont dites équivalentes par lignes s'il existe une matrice inversible $M \in \mathcal{M}_m(\mathbb{K})$ telle que

$$B = MA$$

<u>Théorème</u> : Soit $A \in \mathcal{M}_{m,n}(\mathbb{K})$. Alors il existe trois matrices P, L, E telles que

$$A = PLE$$

où

- $P \in \mathcal{M}_m(\mathbb{K})$ est une matrice de permut.
- $L \in \mathcal{M}_m(\mathbb{K})$ est une matrice triangulaire inférieure avec que des 1 sur la diagonale
- $E \in \mathcal{M}_{m \times n}(\mathbb{K})$ est une matrice échelonnée.