L3 Calcul Formel
Université de Lorraine

TP 5 : Pivot de Gauss-Jordan

Clément Dell'Aiera

On travaillera pour ce TP dans l'anneau des entiers $A = \mathbb{Z}$, mais l'algorithme présenté fonctionne correctement dans tout anneau euclidien A. La base canonique de $\mathfrak{M}_{n,m}(A)$ est notée $E_{ij} = (\delta_{l=i,l'=j})_{1\leq l\leq n, 1\leq j\leq m}$. Soit $\mathcal{P}$ un système complet d'éléments irréductibles de A, pour les entiers on peut prendre $\mathcal{P} = \mathbb{P}$ l'ensemble des nombres premiers. Tout élément $n \in A$ s'écrit

$$n = u \prod_{p\in\mathcal{P}} p^{v_p(n)}$$

où u est une unité de A. On définit le poids d'un élément n comme

$$\delta(n) = \sum_{p\in\mathcal{P}} v_p(n) \in \mathbb{N}.$$

- Si $M = (m_{ij}) \in \mathfrak{M}_{n,m}(A)$, $M^{(k)}$ désigne la sous matrice de taille $(n-k+1)\times(m-k+1)$ obtenue en ne gardant que le "coin en bas à gauche" :

$$M^{(k)} = (m_{ij})_{k\leq i\leq n, k\leq j\leq m}.$$

- Si $x \in A$, $i \neq j$, et $l > 0$, on appelle matrices de transvection les matrices

$$T^l_{ij}(x) = I_l + xE_{ij} \in GL(l, A)$$

Lorsqu'une matrice M est fixée, on note L_i sa $i^{\text{ème}}$ ligne et C_j sa $j^{\text{ème}}$ colonne. L'algorithme du pivot de Gauss ramène un système linéaire quelconque à une forme que l'on appelle échelonnée au moyen d'opérations élémentaires sur les lignes et les colonnes. On se servira tout au long du TP des faits suivants :

- l'opération $L_i \leftarrow L_i + xL_j$ est donnée par l'opération matricielle

$$\begin{cases} \mathfrak{M}_{n,m}(A) & \to & \mathfrak{M}_{n,m}(A) \\ M & \mapsto & T^n_{ij}(x)M \end{cases}$$

- l'opération $C_j \leftarrow C_j + xC_i$ est donnée par l'opération matricielle

$$\begin{cases} \mathfrak{M}_{n,m}(A) & \to & \mathfrak{M}_{n,m}(A) \\ M & \mapsto & MT^m_{ij}(x) \end{cases}$$

- l'opération $L_i \leftrightarrow L_j$ est donnée par l'opération matricielle

$$\begin{cases} \mathfrak{M}_{n,m}(A) & \to & \mathfrak{M}_{n,m}(A) \\ M & \mapsto & T_{ij}^n(1)T_{ji}^n(-1)T_{ij}^n(1)M \end{cases}$$

- l'opération $C_i \leftrightarrow C_j$ est donnée par l'opération matricielle

$$\begin{cases} \mathfrak{M}_{n,m}(A) & \to & \mathfrak{M}_{n,m}(A) \\ M & \mapsto & MT_{ij}^m(-1)T_{ji}^m(1)T_{ij}^m(-1) \end{cases}$$

Si $M = (m_{ij}) \in \mathfrak{M}_{n,m}(A)$, on définit $p_M(i) = \inf\{k : m_{ik} \neq 0\}$. On dit que M est sous **forme échelonnée** si la suite $p_M(i)$ est strictement croissante,

$$M = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \quad \text{par exemple.}$$

Le but du pivot de Gauss est, étant donnée une matrice $M \in \mathfrak{M}_{n,m}(A)$, de trouver une suite de transvections telle que, en faisant successivement les multiplications à gauche par ces transvections, la matrice obtenue soit échelonnée. La matrice échelonnée est équivalente à la matrice de départ au sens suivant.

$$M \sim N \text{ si } \exists P \in GL(n, A)/M = PN.$$

L'algorithme est basé sur le lemme suivant :

Lemme 1. Soit $x \in A^n$ un vecteur, et d un pgcd des composantes de x, alors il existe $L \in GL(n, A)$ telle que

$$Lx = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Par récurrence, on en déduit que pour toute matrice $M \in \mathfrak{M}_{n,m}(A)$, il existe une matrice inversible $L \in GL(n, A)$ telle que LM soit échelonnée.

Pivot de Gauss
Entrée : $M \in \mathfrak{M}_{n,m}(A)$ non nulle.
Sortie : $D \in \mathfrak{M}_{n,m}(A)$ matrice échelonnée équivalente à M.
$L := I_n$
$M_0 = M$
Pour j allant de 1 à $k = \min(m, n)$:

1. trouver $P \in GL(n - j + 1, A)$ telle que

$$PC_j = \begin{pmatrix} d_j \\ \vdots \\ 0 \end{pmatrix}$$

où C_j est la $j^{\text{ème}}$ colonne de $M_j^{(j)}$, et d_j le pgcd de ses composantes.

2. $M_{j+1} = P^{(j)}M_j$ où $P^{(j)} = \begin{pmatrix} I_{j-1} & 0 \\ 0 & P \end{pmatrix}$

Retourner M_k

1. Implémenter une fonction T qui prend entrée deux indices i et j, un entier l, et un élément $x \in A$, et renvoie la matrice de transvection $T_{ij}^{l}(x)$.
2. Implémenter une fonction *echange* qui prend en entrée une matrice M et quatres indices i_0, i_1, j_0 et j_1, et renvoie la matrice M ayant subie les permutations $L_{i_0} \leftrightarrow L_{i_1}$ et $C_{j_0} \leftrightarrow C_{j_1}$.
3. Implémenter une fonction *Test* qui prend en entrée un vecteur x de $\mathbb{Z}^k$ et renvoie $True$ si une seule composante de x est non nulle, $False$ sinon.
4. Implémenter une fonction *DE* qui, étant donné un vecteur x de $\mathbb{Z}^k$, renvoie une matrice inversible $P \in GL(j, \mathbb{Z})$ telle que
$$Px = \begin{pmatrix} pgcd(x_1, ...x_k) \\ : \\ 0 \end{pmatrix}.$$
Pour cela, on trouve la composante i_0 de valeur absolue minimale de x, $|x_{i_0}| = \min\{|x_j|\}$ et on fait la division euclidienne de toutes les autres composantes par x_{i_0}. On recommence jusqu'à ce qu'il n'y ait au plus qu'une composante non nulle. Une remarque importante, la division euclidienne de x_j par x_{i_0} se fait grâce à l'opération $L_j \leftarrow L_j - qL_{i_0}$ où $q = x_j//x_{i_0}$, donc grâce à la multiplication à gauche par une transvection bien choisie, i.e. $T_{ji_0}^{n}(-q)$. Une fois qu'il ne reste qu'une composante non nulle, utiliser *echange* pour mettre ce coefficient en première position. Vous pouver utiliser des fonctions auxiliaires.
5. Implémenter une fonction *Pivot* qui prend en entrée une matrice M de taille $n \times m$, et renvoie une matrice inversible $P \in GL(n, \mathbb{Z})$ telle que PM soit échelonnée.
6. Implémenter une fonction *poids* qui calcule le poids d'un entier.
7. Implémenter une fonction *MinimalWeight* qui prend en entrée une matrice M et un entier k, et renvoie la position de l'élément de poids minimal de la première colonne de la sous-matrice $M^{(k)}$.
8. Implémenter une fonction qui effectue le pivot de Gauss, cette fois-ci en remplaçant "valeur absolue" par "poids" dans le choix du pivot. (Dans le premier cas, le pivot était choisi de façon à minimiser la valeur absolue.)

Voici quelques applications de cet algorithme. Elles sont toutes traitées dans le chapitre VIII du livre de Berhuy, *Modules : théorie et pratique...et un peu d'arithmétique*, que je vous conseille vivement.

- **Forme normale de Smith**
En appliquant le lemme sur la première ligne, puis la première colonne, et en affinant un peu, on peut obtenir le théorème suivant. Si $M \in \mathfrak{M}_{n,m}(\mathbb{Z})$, alors il existe des matrices inversibles $L \in GL(n, \mathbb{Z}), R \in GL(m, \mathbb{Z})$ telles que LMR soit diagonales à coefficients positifs, de coefficients diagonaux b_j tels que $b_j | b_{j+1}$. La matrice diagonale obtenue est unique, on l'appelle la forme de Smith de M.
- **Résolution de systèmes d'équations linéaires dipophantiennes.**
Soit A un anneau principal et a_1, a_2, ..., a_k des éléments de A non tous nuls et $b \in A$. Soit d un généateur de $(a_1, ..., a_k)$. L'équation
$$a_1x_1 + ... + a_kx_k = b$$

admet une solution dans A^k ssi $d|b$. Alors toute solution s'écrit de manière unique

$$\alpha C_1 + x_2 C_2 + x_k C_k, x_j \in A,$$

avec $\alpha \in A$ tel que $b = \alpha d$ et les C_j sont les colonnes d'un matrice inversible $C \in GL(k, A)$ telle que

$$(a_1 \ ... \ a_k)C = (d \ 0 \ ... \ 0).$$

Par exemple, vous pouvez résoudre $3x + 4y + 7z = b$ dans $\mathbb{Z}$, un exemple corrigé dans le livre de Berhuy, chp VII, I.22, p 248.

- **Théorème de structure des groupes abéliens de type fini.**
Soit G un groupe abélien admettant un nombre fini de générateurs. Alors il existe deux entiers positifs p et q, et des entiers non nuls $d_1|d_2|...|d_q$, $d_j \geq 2$, tels que

$$G \simeq \mathbb{Z}^p \times \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_q\mathbb{Z}.$$

Ces entiers p et d_j sont uniques et caractérisent la classe d'isomorphisme de G.

- **Décomposition de Frobenius.**
Soit V un k-espace vectoriel et $f \in \mathcal{L}(V)$ un endomorphisme. Alors il existe des polynômes unitaires $P_1|P_2|...|P_r$ de $k[X]$ et une base B de V tels que

$$Mat(f, B) = \begin{pmatrix} C_{P_1} & & \\ & ... & \\ & & C_{P_r} \end{pmatrix}$$

où C_P est la matrice compagnon associée à P, i.e. si $P = X^n + p_{n-1}X^{n-1} + ... + p_0 \in k[X]$,

$$C_P = \begin{pmatrix} 0 & & & & -p_0 \\ 1 & 0 & & & -p_1 \\ & 1 & ... & & ... \\ & & & 0 & -p_{n-2} \\ & & & 1 & -p_{n-1} \end{pmatrix}.$$

Ces polynômes sont appelés les invariants de similitudes de f et la matrice diagonale par bloc ci-dessus est la forme de Frobenius de f ? De plus, 2 endomorphismes sont semblables ssi ils ont la même forme de Frobenius.

- **Théorème de structure des modules de type fini sur un anneau principal.**
Tous ces théorèmes sont des corollaires du théorème de structure des modules de type fini sur un anneau principal, qui est traité dans le livre de Berhuy. Pour les TP précédents, j'ai principalement utilisé les livres *Cours d'Arithmétique* de Michel Demazure et *Arithmétique* de Marc Hindry.