

Cryptographie post quantique : TD1 - Rappel d'algèbre linéaire

Ressources utilisées:

- Cours et exercices - Pascal Lainé, Université Lyon 1,
- Cours de préparation à l'agrégation interne - Arnaud Jehanne, Université de Bordeaux,
- Cours de cryptanalyse - Christine Bachoc, Université de Bordeaux.

Ce premier TD a pour objectif de vous faire les rappels nécessaires pour le cours de cryptographie post-quantique. Le TD est à faire en semi-autonomie: c'est-à-dire que vous pouvez avancer à votre rythme. Les exercices 1 et 2 sont des rappels d'algèbre linéaire tandis que les exercices 3 et + sont une introduction aux réseaux euclidiens, une des bases mathématiques utilisées pour la cryptographie post-quantique.

1 Rappel d'algèbre linéaire

Matrices et vecteurs

Definition 1 (Matrices). Soit R un anneau commutatif. Soit deux entiers naturels non nuls m et n . Une matrice A de taille (m, n) est un tableau rectangulaire dans R i.e. une famille d'éléments de R indexée par les éléments de $\{1, \dots, m\} \times \{1, \dots, n\}$:

$$A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

On dit que $a_{i,j}$ est l'élément de la i -ème ligne et de la j -ème colonne de A . On note $\mathcal{M}_{m,n}(R)$ l'ensemble des matrices de taille (m, n) à coefficients dans R .

On définit l'addition des matrices et la multiplication par un scalaire de la manière suivante :

- Soient $M, N \in \mathcal{M}_{m,n}(R)$, alors $M + N$ est la matrice dont chaque élément $a_{i,j}$ est $m_{i,j} + n_{i,j}$.
 $A = M + N$.
- Soient $M \in \mathcal{M}_{m,n}(R)$ et $\lambda \in R$, alors λM est la matrice dont chaque élément $a_{i,j}$ est $\lambda m_{i,j}$.
 $A = \lambda M$.

On définit également la multiplication de matrices. Soient $M \in \mathcal{M}_{m,n}(R)$ et $N \in \mathcal{M}_{n,p}(R)$, alors MN est la matrice de taille (m, p) dont chaque élément $a_{i,j} = \sum_{k=1}^n m_{i,k} n_{k,j}$. $A = M \cdot N$.

$$\begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{m,1} & m_{m,2} & \cdots & m_{m,n} \end{bmatrix} \cdot \begin{bmatrix} n_{1,1} & n_{1,2} & \cdots & n_{1,p} \\ n_{2,1} & n_{2,2} & \cdots & n_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n,1} & n_{n,2} & \cdots & n_{n,p} \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,p} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,p} \end{bmatrix}$$

Definition 2. Un vecteur est une matrice de taille $(m, 1)$ pour un certain entier naturel non nul m .

Résolution de systèmes linéaires - Pivot de Gauss

Definition 3 (Pivot de Gauss). Le pivot de Gauss est une méthode pour résoudre les systèmes d'équations linéaires en transformant la matrice augmentée du système en une matrice triangulaire supérieure.

Exercice 1.*Résolution de systèmes linéaires*

Considérer le système d'équations linéaires suivant :

$$\begin{cases} 2x + y + z = 1 \\ 4x + y + 3z = 4 \\ 6x + 5y + 2z = 2 \end{cases}$$

1. Résoudre le système d'équations dans $\mathbb{R}$ puis dans $\mathbb{Z}$.

2. Mettre sous forme matricielle: $A \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = b$.

Considérer le système d'équations linéaires suivant :

$$\begin{cases} 2x + 3y - z = 2 \\ x + 2y - z = 4 \\ -x + y + z = -1 \\ -3x + y + 2z = 0 \end{cases}$$

3. Sans résoudre, que pouvez-vous dire du nombre de solutions de ce système ?

4. Mettre sous forme matricielle: $A \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = b$.

5. Résoudre le système en utilisant la forme matricielle dans $\mathbb{R}$ puis dans $\mathbb{Z}$.

6. Donner l'expression de $A^\top$ la matrice transposée de A .

7. Estimer le nombre de solutions puis résoudre $A^\top \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 2 \\ -7 \\ -2 \end{bmatrix}$ dans $\mathbb{R}$, dans $\mathbb{Z}$ puis dans $\mathbb{Z}/7\mathbb{Z}$.

Considérer le système d'équations linéaires suivant :

$$\begin{cases} -x + 2y + z \approx -1 \\ -3x + y + 2z \approx 4 \\ -x + y + z \approx 0 \\ 3y + 2z \approx -7 \end{cases}$$

Chacune des équations est approximative, c'est-à-dire qu'il existe un ε tel que l'équation soit vérifiée à $\{-1, 0, 1\}$ près.

8. Résoudre le système d'équations approximatives dans $\mathbb{Z}$.

Exercice 2.*Bases et espaces vectoriels*

1. Soient les vecteurs $v_1 = (1, 1, 0)$, $v_2 = (4, 1, 4)$ et $v_3 = (2, -1, 4)$. La famille (v_1, v_2, v_3) est-elle libre ?

2. Soit E un espace vectoriel de $\mathbb{R}$ et soit (v_1, v_2, v_3) une famille libre d'éléments de E , les familles suivantes sont-elles libres ?

1. $(v_1, v_3),$
 2. $(3v_1 + v_3, v_3, v_2 + v_3),$
 3. $(v_1, 2v_1 + v_3, -v_3).$
3. En considérant la même famille précédente (v_1, v_2, v_3) et en supposant que c'est une base de $\mathbb{R}^3$, les familles précédentes sont-elles des bases de $\mathbb{R}^3$?

Cours

Definition 4 (Espaces Vectoriels). Une *espace vectoriel* E sur un corps K est un ensemble muni de deux opérations : l'addition et la multiplication par un scalaire, qui satisfont les axiomes suivants :

- $(E, +)$ est un groupe abélien.
- Pour tout $\lambda, \mu \in K$ et pour tout $\mathbf{u}, \mathbf{v} \in E$:
 - $\lambda(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}$ (distributivité de la multiplication par un scalaire par rapport à l'addition dans E)
 - $(\lambda + \mu)\mathbf{u} = \lambda\mathbf{u} + \mu\mathbf{u}$ (distributivité de la multiplication par un scalaire par rapport à l'addition dans K)
 - $(\lambda\mu)\mathbf{u} = \lambda(\mu\mathbf{u})$ (associativité de la multiplication par un scalaire)
 - $1\mathbf{u} = \mathbf{u}$ (élément neutre de la multiplication par un scalaire)

Definition 5 (Famille libre). Une *famille libre* d'élément de E est une famille $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ telle que pour tout $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$, si $\sum_{i=1}^n \lambda_i \mathbf{v}_i = 0$ alors $\lambda_i = 0$ pour tout i . (On dit que les vecteurs sont linéairement indépendants.)

Definition 6 (Famille génératrice). Une *famille génératrice* d'élément de E est une famille $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ telle que tout élément de E peut s'exprimer comme combinaison linéaire des vecteurs de la famille i.e. pour tout $\mathbf{v} \in E$, il existe $(\lambda_1, \dots, \lambda_n) \in \mathbb{R}^n$ tel que $\mathbf{v} = \sum_{i=1}^n \lambda_i \mathbf{v}_i$.

Exemple : La famille $(\mathbf{e}_1, \dots, \mathbf{e}_n)$ est une base de $\mathbb{R}^n$. ($\mathbf{e}_i$ est le vecteur dont la i -ème coordonnée est 1 et les autres sont 0.)

Definition 7 (Base d'un espace vectoriel). Une *base* est une famille libre et génératrice d'un espace vectoriel.

Definition 8 (Application linéaire). Soient E et F deux espaces vectoriels sur un corps K . Une application $f : E \rightarrow F$ est dite *linéaire* si pour tout $\mathbf{u}, \mathbf{v} \in E$ et pour tout $\alpha, \beta \in K$, on a :

$$f(\alpha\mathbf{u} + \beta\mathbf{v}) = \alpha f(\mathbf{u}) + \beta f(\mathbf{v}).$$

On peut représenter une application linéaire par une matrice. Soit $f : K^n \rightarrow K^m$ une application linéaire, alors il existe une matrice $A \in \mathcal{M}_{m,n}(K)$ telle que pour tout $\mathbf{x} \in K^n$, on a :

$$f(\mathbf{x}) = A\mathbf{x}.$$

Réciproquement, toute matrice $A \in \mathcal{M}_{m,n}(K)$ définit une application linéaire $f : K^n \rightarrow K^m$ par la formule ci-dessus.

2 Introduction aux réseaux euclidiens

Cours

Definition 9 (Réseaux euclidiens). Un réseau euclidien Λ de dimension m est un sous-groupe discret (additif) de $\mathbb{R}^m$ i.e. $\mathbf{0} \in \Lambda, \forall \mathbf{x}, \mathbf{y} \in \Lambda, \mathbf{x} + \mathbf{y} \in \Lambda$.

Definition 10 (Base d'un réseau). Un réseau Λ peut être défini par une base $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ où $\mathbf{b}_i \in \mathbb{R}^m$. Le réseau est alors l'ensemble des combinaisons linéaires entières de ces vecteurs :

$$\Lambda(\mathbf{B}) = \left\{ \sum_{i=1}^m z_i \mathbf{b}_i \mid z_i \in \mathbb{Z} \right\}.$$

Exercice 3.

Problèmes calculatoires faciles

Montrer que les problèmes suivants sont faciles à résoudre (pour $m \geq n$) :

1. Etant donné une base d'un réseau $\mathbf{B} \in \mathbb{Z}^{m \times n}$ et un vecteur $v \in \mathbb{Z}^m$, décider si $v \in \Lambda(\mathbf{B})$.
2. Etant donné $\mathbf{B}_1, \mathbf{B}_2 \in \mathbb{Z}^{m \times n}$, décider si $\Lambda(\mathbf{B}_1) = \Lambda(\mathbf{B}_2)$.
3. Etant donnée une matrice d'entiers $\mathbf{A} \in \mathbb{Z}^{m \times n}$, calculer une base du réseau $\{x \in \mathbb{Z}^m : x^T \mathbf{A} = 0\}$.
4. Etant donnée une base $\mathbf{C}$, vérifier si $\Lambda(\mathbf{C})$ est cyclique (i.e., pour tous les vecteurs $x \in \Lambda(\mathbf{C})$, tous les vecteurs obtenus par une rotation cyclique des coordonnées de x sont aussi des vecteurs du réseau).

Cours

Definition 11 (Parallépipède fondamental). Le parallépipède fondamental d'un réseau Λ de base $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ est défini comme l'ensemble :

$$\mathcal{P}(\mathbf{B}) = \left\{ \sum_{i=1}^m \alpha_i \mathbf{b}_i \mid -\frac{1}{2} \leq \alpha_i < \frac{1}{2} \right\}.$$

Definition 12 (Rang d'un réseau). Le **rang** d'un réseau est la dimension de l'espace engendré par ses éléments, ici n , s'il est égal à la dimension on dit qu'un réseau est de **rang plein**.

Definition 13 (Déterminants d'un réseau). Le déterminant d'un réseau Λ de base $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ est défini comme le déterminant de la matrice $\mathbf{B}$:

$$\det(\Lambda(\mathbf{B})) = \sqrt{\det(\mathbf{B}^T \mathbf{B})}.$$

Exercice 4.

Bases

1. Soit Λ un réseau de rang n , et soient $b_1, \dots, b_n \in \Lambda$ n vecteurs linéairement indépendants. Montrer que $b_1, \dots, b_n$ forme une base de Λ si et seulement si $\mathcal{P}(b_1, \dots, b_n) \cap \Lambda = \{0\}$.
2. Montrer que deux bases d'un réseau $B_1, B_2 \in \mathbb{R}^{m \times n}$ sont équivalentes si et seulement si il existe une matrice unimodulaire $U \in \mathbb{R}^{n \times n}$ telle que $B_2 = B_1 U$.
3. Montrer que le déterminant d'un réseau est bien indépendant du choix de sa base.