Algèbre linéaire sur les entiers

Michel Coste*

Version 1 – Mars 2008

Le but de ces notes n'est pas de donner un exposé de plus sur les modules de type fini sur un anneau principal, mais d'expliquer comment traiter de manière algorithmique quelques problèmes simples d'algèbre linéaire sur les entiers, en particulier le problème de la résolution en entiers d'un système linéaire à coe□cients entiers. Ces notes sont destinées en priorité aux agrégatifs préparant l'option algèbre et calcul formel.

L'accent principal est mis sur l'algorithme d'échelonnement d'une matrice à coe□cients entiers, par opérations inversibles sur les lignes, alors qu'on trouve plus facilement dans les manuels l'algorithme de diagonalisation par opérations inversibles sur les lignes et les colonnes. Je me suis pas mal inspiré du livre de P. Naudin et C. Quitté : *Algorithmique algébrique* (Masson). J'ai aussi utilisé pour certains passages le livre de S. Basu, R. Pollack et M-F. Roy : *Algorithms in Real Algebraic Geometry* (Springer). J'utilise la terminologie de **forme normale de Hermite** et de **forme normale de Smith**. Un certain nombre d'exemples d'utilisation des commandes correspondantes dans Maple sont donnés dans des encadrés au long du texte.

La dernière partie de ces notes est de nature un peu di□érente et tourne autour du calcul du déterminant d'une matrice carrée à coe□cients entiers, notamment du point de vue de la taille des entiers qui interviennent.

Je compte bien améliorer ce texte grâce à vos questions, remarques et critiques.

1 Échelonner

La technique d'échelonnement (ou pivot de Gauss) joue un rôle bien connu pour la résolution des systèmes linéaires, le calcul du rang, le calcul du déterminant sur un corps. Nous allons étudier ici comment on peut mener un échelonnement sur l'anneau des entiers relatifs, et à quoi ceci peut servir. L'étude pourrait se généraliser sans peine à n'importe quel anneau euclidien, en particulier à l'anneau des polynômes en une variable sur un corps.

Commençons par définir le but de la manoeuvre, c'est-à dire ce qu'est une matrice échelonnée suivant les lignes.

Définition 1 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$ une matrice à n lignes et p colonnes à coefficients $a_{i,j}$. Pour i allant de 1 à n, posons $p(i)$ le plus petit indice j tel que $a_{i,j} \neq 0$ (avec la convention $p(i) = \infty$ si la i-ème ligne est nulle). Alors la matrice A est dite* ***échelonnée suivant les lignes*** *quand on a, pour tout $i = 2, \ldots, n$, $p(i) = \infty$ ou $p(i-1) < p(i)$. Autrement dit, le premier coefficient non nul d'une ligne est toujours strictement à droite du premier coefficient non nul de la ligne précédente.*

Le résultat de base pour l'échelonnement est le suivant :

Proposition 2 *Soit $\begin{pmatrix} a \\ b \end{pmatrix}$ un vecteur de $\mathbb{Z}^2$, $d = \mathsf{pgcd}(a,b)$. Alors on peut calculer une matrice $M \in \mathsf{GL}_2(\mathbb{Z})$ telle que $M \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$.*

*michel.coste@univ-rennes1.fr

Démonstration : On suppose a et b non tous les deux nuls (car sinon il su□t de prendre $M = I_2$) ; on a alors $d \neq 0$. Grâce à l'algorithme d'Euclide étendu, on peut calculer des entiers relatifs u et v tels que $ua + vb = d$. Soient a' et b' les entiers relatifs définis par $a = da'$ et $b = db'$. On prend alors

$$M = \begin{pmatrix} u & v \\ -b' & a' \end{pmatrix} .$$

□

On peut appliquer la proposition 2 à des vecteurs de longueur $n > 2$, quand on veut en modifier deux des composantes d'indices i et j. On « gonfle » alors les matrices 2×2 en remplaçant par leurs coe□cients les coe□cients d'indices (i,i), (i,j), (j,i) et (j,j) de la matrice identité I_n. En utilisant plusieurs fois la proposition ainsi étendue, on obtient sans peine le

Corollaire 3 *Soit* $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ *un vecteur de* $\mathbb{Z}^n$, $d = \mathrm{pgcd}(a_1, \ldots, a_n)$. *Alors on peut calculer une matrice* $M \in \mathrm{GL}_n(\mathbb{Z})$ *telle que*

$$M \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} .$$

Le calcul successif d'identités de Bézout entre deux coe□cients n'est sans doute pas le procédé le plus e□cace pour trouver la matrice M du corollaire. On peut plutôt répéter l'opération qui consiste à choisir un coe□cient du vecteur de valeur absolue non nulle minimale, et à faire la division euclidienne des autres coe□cients par celui-ci. Remarquez que chaque division euclidienne se fait par multiplication à gauche par une matrice de transvection élémentaire à coe□cients entiers. A la fin, on peut multiplier à gauche par une matrice de transposition pour amener le pgcd obtenu en première position.

Grâce à cet outil, nous avons un algorithme d'échelonnement de n'importe quelle matrice à coe□cients entiers.

Théorème 4 *Soit A une matrice à n lignes et p colonnes à coefficients dans $\mathbb{Z}$. Alors on peut calculer une matrice $L \in \mathrm{GL}_n(\mathbb{Z})$ telle que LA soit échelonnée suivant les lignes.*

Démonstration : On traite l'une après l'autre les colonnes de la matrice A, de façon à ce qu'à l'issue de l'étape k la sous-matrice formée par les k premières colonnes soit échelonnée suivant les lignes. De façon précise, supposons qu'on ait déjà $L^{(k)} \in \mathrm{GL}_n(\mathbb{Z})$ telle que $L^{(k)}A = (a_{i,j}^{(k)})$ ait ses k premières colonnes échelonnées suivant les lignes. Soit ℓ le plus grand entier tel qu'il existe i entre 1 et k avec $a_{\ell,i}^{(k)} \neq 0$ (on a forcément $\ell \leq k$). Si $\ell = n$, la matrice $L^{(k)}A$ est déjà échelonnée suivant les lignes et on peut s'arrêter là. Supposons donc $\ell < n$. Alors, en appliquant le corollaire 3, on calcule une matrice $T \in \mathrm{GL}_{n-\ell}(\mathbb{Z})$ telle que

$$T \begin{pmatrix} a_{\ell+1,k+1}^{(k)} \\ a_{\ell+2,k+1}^{(k)} \\ \vdots \\ a_{n,k+1}^{(k)} \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} ,$$

où $d = \mathrm{pgcd}(a_{\ell+1,k+1}^{(k)}, \ldots, a_{n,k+1}^{(k)})$. On pose alors

$$L^{(k+1)} = \begin{pmatrix} I_\ell & 0 \\ 0 & T \end{pmatrix} L^{(k)} \in \mathrm{GL}_n(\mathbb{Z}) ,$$

Encadré 1 – Un exemple d'échelonnement suivant les lignes

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 9 & 1 & 4 & 7 \\ 6 & 2 & 5 & 8 \\ 12 & 4 & 8 & 10 \end{pmatrix}$
$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 & -1 & -1 \\ 6 & 2 & 5 & 8 \\ 0 & 0 & -2 & -6 \end{pmatrix}$
$\begin{pmatrix} 1 & -1 & 0 \\ -2 & 3 & 0 \\ 0 & -2 & 1 \end{pmatrix}$	$\begin{pmatrix} 3 & -1 & -1 & -1 \\ 0 & 4 & 7 & 10 \\ 0 & 0 & -2 & -6 \end{pmatrix}$

Chaque matrice de la colonne de droite est le produit de la matrice à sa gauche par la matrice tout en haut à droite.

et on a bien que $L^{(k+1)}A$ a ses k + 1 premières colonnes échelonnées suivant les lignes. □

L'échelonnement permet d'obtenir une base et le rang d'un sous-module de $\mathbb{Z}^p$ donné par un nombre fini de générateurs.

Proposition 5 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$. On échelonne cette matrice suivant les lignes pour obtenir $B = LA$ avec $L \in \mathsf{GL}_n(\mathbb{Z})$. Alors les lignes non nulles de B forment une base du sous-module M de $\mathbb{Z}^p$ engendré par les lignes de A.*

Démonstration : Puisque $B = LA$ avec $L \in \mathsf{GL}_n(\mathbb{Z})$, toute ligne de B est combinaison linéaire à coe□cients entiers de A et, puisque $A = L^{-1}B$, toute ligne de A est combinaison linéaire à coe□cients entiers de lignes de B. Donc le sous-module M est le même que le sous-module engendré par les lignes non nulles de B.

Soient $B_1, \ldots, B_r$ ces lignes. Rappelons que $B_i = (0, \ldots, 0, b_{i,p(i)}, \ldots, b_{i,p})$ avec $b_{i,p(i)} \neq 0$ et $0 \leq p(1) < p(2) < \ldots < p(r) \leq p$. Si les entiers $\lambda_1, \ldots, \lambda_r$ vérifient $\lambda_1 B_1 + \cdots + \lambda_r B_r = 0$, on doit avoir $\lambda_1 b_{1,p(1)} = 0$, d'où $\lambda_1 = 0$, puis $\lambda_2 b_{2,p(2)} = 0$, d'où $\lambda_2 = 0$, etc.. Donc $(v_1, \ldots, v_r)$ est bien une base de M. □

L'échelonnement d'une matrice fournit donc une preuve concrète qu'un sous-module (finiment engendré) de $\mathbb{Z}^p$ est libre. Le rang du sous-module est le nombre de lignes non nulles dans la matrice échelonnée. L'échelonnement permet de tester facilement l'appartenance au sous-module.

Exercice 1 Est-ce que le vecteur $(3, -1, 0, 2)$ appartient au sous-module de $\mathbb{Z}^4$ engendré par les lignes de la matrice de l'encadré 1 ? Appartient-il au sous-espace vecoriel de $\mathbb{Q}^4$ engendré par ces lignes ?

2 Forme normale de Hermite

Nous n'avons pas unicité de la matrice obtenue par échelonnement. Pour obtenir cette unicité, il faut demander un peu plus que l'échelonnement. C'est comme ce qui se passe sur un corps, et nous allons adapter la notion de matrice échelonnée réduite selon les lignes.

Définition 6 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$ à coefficients $a_{i,j}$ une matrice échelonnée suivant les lignes. Soit r le nombre de lignes non nulles de A et soit $a_{i,p(i)}$ le premier coefficient non nul sur la ligne i pour $i = 1, \ldots, r$. Alors la matrice A est dite échelonnée* ***réduite*** *suivant les lignes quand, pour tout $i = 1, \ldots, r$ on a $a_{i,p(i)} > 0$ et $0 \leq a_{k,p(i)} < a_{i,p(i)}$ pour $k = 1, \ldots, i-1$.*

On a alors unicité de la forme échelonnée réduite.

Proposition 7 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$. Alors il existe une unique matrice échelonnée réduite suivant les lignes $B \in \mathsf{M}_{n,p}(\mathbb{Z})$ telle qu'il existe $L \in \mathsf{GL}_n(\mathbb{Z})$ avec $B = LA$. La matrice B s'appelle* ***la forme normale de Hermite*** *de A.*

Démonstration : Nous nous contenterons d'indications. L'existence est en fait constructive : on commence par échelonner la matrice A pour obtenir B. On peut supposer que le premier coe□cient non nul $b_{i,p(i)}$ de chaque ligne non nulle de B est positif, quitte à multiplier cette ligne par -1. On peut ensuite faire $0 \leq b_{k,p(i)} < b_{i,p(i)}$ pour $k < i$ en soustrayant à la k-ème ligne la i-ème multipliée par le quotient de la division euclidienne de $b_{k,p(i)}$ par $b_{i,p(i)}$; on le fait dans l'ordre pour $i = 1, 2, \ldots$ (de gauche à droite).

Supposons qu'on ait deux formes normales de Hermite B et B' pour une même matrice A. Les lignes non nulles de B et B' sont deux bases du même sous-module de $\mathbb{Z}^p$ de rang r. Notons ces lignes $B_1, \ldots, B_r$ et $B'_1, \ldots, B'_r$ respectivement. Par la condition d'échelonnement pour B et B' on a $B'_i = \sum_{\ell=i}^{r} \lambda_{i,\ell} B_\ell$, avec $\lambda_{i,i} = \pm 1$. Le fait que B et B' sont réduites impose d'abord $\lambda_{i,i} = 1$, puis $\lambda_{i,\ell} = 0$ pour $\ell = i+1, \ldots, r$. □

Remarquons que si on a unicité de la forme normale de Hermite B de la matrice A, il n'y a pas nécessairement unicité de la matrice inversible L telle que $B = LA$ (la matrice de transformation).

Encadré 2 – La commande HermiteForm du paquet LinearAlgebra de Maple

---

```
> restart:with(LinearAlgebra):
> A:=Matrix([[9,1,4,7],[6,2,5,8],[12,4,8,10]]);
```

$$A := \begin{bmatrix} 9 & 1 & 4 & 7 \\ 6 & 2 & 5 & 8 \\ 12 & 4 & 8 & 10 \end{bmatrix}$$

```
> HermiteForm(A,method=integer,output=['H','U']);
```

$$\begin{bmatrix} 3 & 3 & 0 & -9 \\ 0 & 4 & 1 & -8 \\ 0 & 0 & 2 & 6 \end{bmatrix}, \begin{bmatrix} -1 & -4 & 3 \\ -2 & -3 & 3 \\ 0 & 2 & -1 \end{bmatrix}$$

La commande HermiteForm (avec method=integer) permet d'avoir la forme normale de Hermite (avec 'H' dans les « outputs ») et une matrice de transformation à cette forme normale (avec 'U').

La preuve de l'unicité dans la proposition 7 n'utilise que le fait que les lignes des deux matrices engendrent le même sous-module. On en tire le corollaire suivant, qui explicite complètement la relation d'équivalence à gauche entre matrices de $\mathsf{M}_{n,p}(\mathbb{Z})$.

Corollaire 8 *Soit A et B des matrices de $\mathsf{M}_{n,p}(\mathbb{Z})$. Les propriétés suivantes sont équivalentes :*

1. *Il existe $L \in \mathsf{GL}_n(\mathbb{Z})$ telle que $B = LA$ (A et B sont équivalentes à gauche).*
2. *Les lignes de A engendrent le même sous-module de $\mathbb{Z}^p$ que les lignes de B.*
3. *A et B ont même forme normale de Hermite.*

3 Utilisations de l'échelonnement

Nous avons déjà vu que l'échelonnement des matrices à coe□cients entiers permet de résoudre le problème de trouver une base d'un sous-module. Nous passons maintenant à d'autres problèmes que l'on peut résoudre par cette technique.

3.1 Résoudre un système linéaire diophantien

Prenons l'exemple du problème suivant : trouver une base du module des solutions entières de l'équation

$$2x + 3y + 5z = 0 .$$

Le mauvais réflexe est de trouver une base de l'espace des solutions sur $\mathbb{Q}$, soit $((-\frac{3}{2}, 1, 0), (-\frac{5}{2}, 0, 1))$ et de chasser les dénominateurs pour prétendre que l'ensemble des solutions entières est $\mathbb{Z}(-3, 2, 0) + \mathbb{Z}(-5, 0, 2)$. En e□et, on n'obtient pas ainsi la solution entière $(0, 5, -3)$.

Pourtant, notre système d'équations est bien échelonné (ce n'est pas trop di□cile quand il y a une seule équation !). La clé du problème est que, contrairement à ce qu'on a l'habitude de faire pour résoudre les systèmes linéaires sur un corps, la bonne tactique est ici d'échelonner la matrice du système **selon les colonnes**. On peut voir la résolution de cette équation sur les entiers dans l'encadré 3.

Encadré 3 – Résolution en entiers de $2x + 3y + 5z = 0$

```
> A:=Matrix([[2,3,5]]);
> (H,U):=HermiteForm(Transpose(A),method=integer,output=['H','U']):
> Transpose(H),Transpose(U);
```

$$A := \begin{bmatrix} 2 & 3 & 5 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} -1 & -3 & -4 \\ 1 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

```
> isolve(2*x+3*y+5*z=0);
```

$$\{x = -4\_Z1 - 3\_Z2, z = \_Z1, y = \_Z1 + 2\_Z2\}$$

Pour calculer la mise en forme normale de Hermite selon les colonnes, on utilise « Transpose ». Les deux dernières colonnes de la matrice de transformation à la forme normale forment une base du module des solutions.

Supposons qu'on ait à résoudre le système linéaire diophantien à n équations et p inconnues $AX = C$, avec $A \in \mathsf{M}_{n,p}(\mathbb{Z})$, X le vecteur colonne des p inconnues et C le vecteur colonne du second membre à n composantes entières. L'échelonnement suivant les colonnes de la matrice A nous donne $B = AR$ avec $R \in \mathsf{GL}_p(\mathbb{Z})$. Le système $BY = C$ est facile à résoudre en entiers. Supposons que B ait r colonnes $B_1, \ldots, B_r$ non nulles. Alors, grâce à l'échelonnement, on peut tester facilement s'il existe des entiers $d_1, \ldots, d_r$ (forcément uniques) tels que $C = d_1B_1 + \cdots + d_rB_r$; ceci revient à dire que C appartient au module engendré par les colonnes de A dont $(B_1, \ldots, B_r)$ est une base. Si cette condition nécessaire et su□sante pour l'existence de solutions entières du système est remplie, alors les solutions entières en Y du système sont les $(d_1, \ldots, d_r, z_{r+1}, \ldots, z_p)$, où $z_{r+1}, \ldots, z_p$ sont des entiers quelconques. Comme la matrice R est inversible sur les entiers, les solutions entières en X de $AX = BR^{-1}X = C$ sont de la forme RY où Y est une solution entière de $BY = C$. Soient $R_1, \ldots, R_p$ les colonnes de R. L'ensemble des solutions entières de $AX = B$ est ainsi

$$d_1 R_1 + \cdots + d_r R_r + \mathbb{Z} R_{r+1} + \cdots + \mathbb{Z} R_p .$$

Encadré 4 – Résolution d'un système linéaire diophantien à l'aide de la forme normale de Hermite

```
> AA:=RandomMatrix(3,5):
> A:=SubMatrix(AA,1..3,1..4):
> C:=convert(SubMatrix(AA,1..3,-1),Vector[column]):
> A,C;
```

$$\begin{bmatrix} 24 & 70 & -13 & 29 \\ -96 & 72 & 42 & 77 \\ -90 & -78 & -95 & 79 \end{bmatrix}, \begin{bmatrix} 47 \\ 22 \\ -53 \end{bmatrix}$$

```
> (HH,UU):=HermiteForm(Transpose(AA),method=integer,output=['H','U']):
> Transpose(HH), Transpose(UU);
```

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} -219827 & -90472 & -322761 & -396488 & -247405 \\ 172094 & 70827 & 252677 & 310395 & 193683 \\ -202787 & -83459 & -297742 & -365754 & -228227 \\ -324378 & -133501 & -476268 & -585060 & -365072 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

```
> SOL:= -SubMatrix(Transpose(UU),1..4,-1): SOL, Multiply(A,SOL);
```

$$\begin{bmatrix} 247405 \\ -193683 \\ 228227 \\ 365072 \end{bmatrix}, \begin{bmatrix} 47 \\ 22 \\ -53 \end{bmatrix}$$

```
> isolve({seq(Multiply(A,Vector([x,y,z,t]))[i]=C[i],i=1..3)});
```

$$\{y = 116712 + 310395\,\_Z1,\ x = -149083 - 396488\,\_Z1,\ t = -219988 - 585060\,\_Z1,\ z = -137527 - 365754\,\_Z1\}$$

```
> subs(_Z1=-1,%);
```

$$\{y = -193683,\ x = 247405,\ t = 365072,\ z = 228227\}$$

On calcule la forme normale de Hermite selon les colonnes de la matrice augmentée AA du système $AX = C$, et une matrice de transformation. Comme la dernière colonne de la forme normale est nulle et que la dernière ligne de la matrice de transformation est $(0, \ldots, 0, 1)$, ce système a une solution entière donnée par l'opposé SOL de la dernière colonne de la matrice de transformation, privée du 1 terminal. L'avant-dernière colonne de la matrice de transformation, privée du 0 terminal, engendre le module des solutions entières du système sans second membre.

On sait bien que la résolution d'un système d'équations linéaires est une histoire d'image et de noyau de la matrice du système : le système admet des solutions si et seulement si le second membre est dans l'image, et l'espace des solutions du système sans second membre est le noyau. Nous avons vu que l'échelonnement suivant les colonnes fournit les informations utiles sur l'image et le noyau : les colonnes non nulles de la matrice échelonnée forment une base de l'image permettant de tester facilement l'appartenance, et une base du noyau peut se lire dans la matrice de passage à la forme échelonnée.

Exercice 2 Vérifiez que le système $AX = C$ admet des solutions entières si et seulement si la forme normale de Hermite suivant les colonnes de la matrice augmentée $\widetilde{A} = (A|C)$ a les mêmes colonnes non nulles que la forme normale de Hermite suivant les colonnes de A. Si c'est le cas, comment trouver une solution particulière de $AX = C$ à partir de matrices de transformations de A et $\widetilde{A}$ à leurs formes normales de Hermite suivant les colonnes ?

Exercice 3 Expliquez le commentaire de l'encadré 4. Y aurait-il eu des solutions entières si le second

membre du système avait été $(46, 22, -53)$?

3.2 Compléter une base

Un vecteur $(a_1, \ldots, a_n)$ de $\mathbb{Z}^n$ est dit **primitif** quand pgcd$(a_1, \ldots, a_n) = 1$.

Proposition 9 *Un vecteur $(a_1, \ldots, a_n)$ de $\mathbb{Z}^n$ peut être complété en une base de $\mathbb{Z}^n$ si et seulement s'il est primitif.*

Avant de lire la démonstration constructive, on peut réfléchir au petit exemple donné dans l'encadré 5.

Encadré 5 – Compléter le vecteur primitif $(6, 10, 15)$ en une base

```
> A:=Matrix([[6,10,15]]);
> (H,U):=HermiteForm(Transpose(A),method=integer,output=['H','U']):
> Transpose(H), Transpose(MatrixInverse(U));
```

$$A := \begin{bmatrix} 6 & 10 & 15 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 6 & 10 & 15 \\ -1 & -1 & -3 \\ 0 & -1 & 1 \end{bmatrix}$$

Les lignes de l'inverse de la matrice de transformation à la forme normale de Hermite suivant les colonnes forment une base complétant le vecteur donné.

Démonstration : Supposons $A = (a_1, \ldots, a_n)$ primitif. Alors sa forme normale de Hermite suivant les colonnes est $(1, 0, \ldots, 0)$ et on peut calculer une matrice $R \in \mathrm{GL}_n(\mathbb{Z})$ telle que $AR = (1, 0, \ldots, 0)$. Mais alors $A = (1, 0, \ldots, 0)\, R^{-1}$ est la première ligne de la matrice R^{-1}, et les lignes de cette matrice forment donc une base de $\mathbb{Z}^n$ qui complète A.

Réciproquement, si A se complète en une base de $\mathbb{Z}^n$, alors A est la première ligne d'une matrice de $\mathrm{GL}_n(\mathbb{Z})$, de déterminant ± 1. Le développement de ce déterminant suivant la première ligne montre que A est primitif. □

Exercice 4 Traitez à la main l'exemple de l'encadré 5. Vous pouvez noter les opérations sur les colonnes faites pour échelonner, puis remonter avec les inverses de ces opérations sur la matrice identité pour obtenir directement la matrice R^{-1} de la démonstration.

Exercice 5 Si on vous donne k vecteurs dans $\mathbb{Z}^n$, comment tester s'ils peuvent être complétés en une base et, le cas échéant, comment les compléter e□ectivement ?

Exercice 6 On sait qu'un sous espace vectoriel d'un espace vectoriel de dimension finie peut être décrit par un système générateur, ou par un système d'équations linéaires (comme image, ou comme noyau). En est-il de même d'un sous-module de $\mathbb{Z}^n$?

4 Forme normale de Smith

On sait que, sur un corps, toute matrice est équivalente à une matrice dont tous les coe□cients en dehors de la diagonale sont nuls et qui n'a que des 1 et des 0 sur la diagonale. On se ramène à une telle forme par des opérations élémentaires sur les lignes et sur les colonnes. On a un résultat analogue sur les entiers. Nous dirons qu'une matrice rectangulaire $A = (a_{i,j})$ est diagonale quand $a_{i,j} = 0$ pour tous $i \neq j$.

Proposition 10 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$. On peut calculer deux matrices inversibles $L \in \mathsf{GL}_n(\mathbb{Z})$ et $R \in \mathsf{GL}_p(\mathbb{Z})$ telles que $L\,A\,R$ soit diagonale.*

Démonstration : La démonstration procède par récurrence. Il su□t de voir comment trouver deux matrices inversibles $L_1 \in \mathsf{GL}_n(\mathbb{Z})$ et $R_1 \in \mathsf{GL}_p(\mathbb{Z})$ telles que $L_1\,A\,R_1$ ait tous ses coe□cients sur la première ligne ou sur la première colonne nuls, à l'exception possible du coe□cient diagonal. Pour cela on applique successivement le corollaire 3 sur la première ligne et sur la première colonne. Bien sûr, quand on réduit la première ligne on peut introduire de nouveaux coe□cients non nuls sur la première colonne (ou vice-versa), mais si c'est le cas c'est que le coe□cient diagonal ne divisait pas les autres coe□cients de la première ligne (resp. colonne), et donc on a strictement diminué sa valeur absolue en le remplaçant par le pgcd des coe□cients de la première ligne (resp. colonne). Le va-et-vient ne peut pas continuer indéfiniment, et on aura au bout d'un nombre fini de réductions uniquement des zéros sur la première ligne et la première colonne en dehors du coe□cient diagonal. □

La forme diagonale à laquelle on s'est ramené au moyen de la proposition précédente n'est pas unique. Pour avoir l'unicité on impose des conditions de positivité et surtout de divisibilité entre les coe□cients diagonaux.

Théorème 11 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$. Alors on peut calculer une matrice diagonale $B \in \mathsf{M}_{n,p}(\mathbb{Z})$ dont les coefficients diagonaux b_i sont positifs ou nuls et vérifient $b_i \mid b_{i+1}$ pour $i = 1, \ldots, \inf(n,p) - 1$ et des matrices inversibles $L \in \mathsf{GL}_n(\mathbb{Z})$ et $R \in \mathsf{GL}_p(\mathbb{Z})$ telles que $B = L\,A\,R$. La matrice B vérifiant ces propriétés est unique. On l"appelle* ***la forme normale de Smith*** *de A.*

Remarquons que si on a unicité de la forme normale de Smith, on n'a pas forcément unicité des matrices de transformation gauche L et droite R.

Démonstration : On sait déjà se ramener à une matrice diagonale. Réaliser la condition de positivité sur la diagonale ne pose pas de problème. Pour réaliser la condition de divisibilité entre coe□cients diagonaux successifs, on peut utiliser l'identité $(*)$ ci-dessous.

Soient a et b des entiers non tous les deux nuls, $\mathrm{pgcd}(a,b) = d = ua + vb$ avec u et v entiers. Définissons les entiers a_1 et b_1 par $a = a_1 d$ et $b = b_1 d$. Posons $m = a_1 b = a b_1$ (m est un ppcm de a et b). Alors

$$(*) \qquad \begin{pmatrix} u & v \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 1 & -vb_1 \\ 1 & ua_1 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & m \end{pmatrix},$$

et on remarque que les deux matrices $\begin{pmatrix} u & v \\ -b_1 & a_1 \end{pmatrix}$ et $\begin{pmatrix} 1 & -vb_1 \\ 1 & ua_1 \end{pmatrix}$ sont inversibles sur les entiers.

Passons maintenant à l'unicité de la forme normale de Smith. Soit B vérifiant les propriétés du théorème, et soient b_i ses coe□cients diagonaux. Il existe un entier r tel que $b_i \neq 0$ pour $i \leq r$ et $b_i = 0$ pour $i > r$. Alors r est égal au rang de la matrice A et, pour $k = 1, \ldots, r$, le produit $b_1 \cdots b_k$ est le pgcd de tous les déterminants $k \times k$ extraits de A. Ceci assure l'unicité des b_i et donc de B.

Vu les conditions de divisibilité entre les b_i, il est vrai que le produit $b_1 \cdots b_k$ est le pgcd de tous les déterminants $k \times k$ extraits de B. Pour justifier l'a□rmation ci-dessus, il su□t donc d'établir que les déterminants $k \times k$ extraits de B et ceux extraits de A engendrent le même idéal de $\mathbb{Z}$. C'est une conséquence de la formule de Cauchy-Binet que nous rappellons ci-dessous. □

Proposition 12 (Formule de Cauchy-Binet) *Soit S une matrice $k \times p$ et T une matrice $p \times k$. Pour tout sous-ensemble $I \subset \{1, \ldots, p\}$ de cardinal $|I| = k$, on désigne par S_I (resp. T^I) la matrice obtenue à partir de S (resp. T) en extrayant les colonnes (resp. lignes) dont les indices sont dans I. Alors*

$$\det(ST) = \sum_{\substack{I \subset \{1,\ldots,p\} \\ |I| = k}} \det(S_I)\,\det(T^I)\,.$$

Encadré 6 – La commande SmithForm du paquet LinearAlgebra de Maple

```
> restart:with(LinearAlgebra):
> A:=Matrix([[9,1,4,7],[6,2,5,8],[12,4,8,10]]);
```

$$A := \begin{bmatrix} 9 & 1 & 4 & 7 \\ 6 & 2 & 5 & 8 \\ 12 & 4 & 8 & 10 \end{bmatrix}$$

```
> SmithForm(A,method=integer,output=['S','U','V']);
```

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ -2 & 0 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 2 & 5 & 1 \\ -2 & 14 & 38 & 11 \\ 1 & -16 & -42 & -12 \\ 0 & 5 & 13 & 4 \end{bmatrix}$$

La commande SmithForm permet d'avoir la forme normale de Smith (S) et des matrices de transformation gauche (U) et droite (V) en cette forme normale.

Démonstration : Soit D_λ la matrice diagonale $p \times p$ de coe□cients diagonaux $\lambda_1, \ldots, \lambda_p$. Puisque chaque coe□cient de la matrice $S\,D_\lambda\,T$ est une forme linéaire en les λ_i, le déterminant $\det(S\,D_\lambda\,T)$ est un polynôme homogène de degré p en les λ_i.

Soit J une partie de $\{1, \ldots, p\}$ de cardinal $< k$. Alors quand on fait $\lambda_i = 0$ pour tout $i \notin J$, on a que la spécialisation de $\det(S\,D_\lambda\,T)$ est identiquement nulle. Ceci montre que tous les monômes apparaissant dans $\det(S\,D_\lambda\,T)$ sont de la forme $\prod_{i\in I} \lambda_i$ avec I partie de $\{1, \ldots, p\}$ de cardinal k. Choisissons une telle partie I, et faisons tous les λ_i avec $i \in I$ égaux à 1, et tous les autres nuls. Alors la valeur trouvée pour $\det(S\,D_\lambda\,T)$ est $\det(S_I)\,\det(T^I)$. Ceci montre que le coe□cient de $\prod_{i\in I} \lambda_i$ dans $\det(S\,D_\lambda\,T)$ est $\det(S_I)\,\det(T^I)$.

Il ne reste plus qu'à faire tous les λ_i égaux à 1 pour établir la formule de Cauchy-Binet. □

En conséquence de la formule de Cauchy-Binet, on a que tout déterminant $k \times k$ extrait d'un produit de matrices $L\,A\,R$ à coe□cients entiers appartient à l'idéal engendré par les déterminants $k \times k$ extraits de A. C'est ce qu'on a utilisé dans la démonstration du théorème 11.

Exercice 7 Inspirez-vous de la formule $(*)$ dans la démonstration du théorème de forme normale de Smith pour exhiber explicitement un isomorphisme entre $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (théorème des restes chinois explicite).

5 Utilisation de la forme normale de Smith

Nous allons voir ici des utilisations qui nécessitent vraiment le calcul de la forme normale de Smith, et pas seulement celui de la forme normale de Hermite

5.1 Base adaptée

Définition 13 *Soit M un sous-module de $\mathbb{Z}^p$. Une base de $\mathbb{Z}^p$* ***adaptée à*** *M est une base $(E_1, \ldots, E_p)$ telle qu'il existe des entiers non nuls $d_1, \ldots, d_r$ ($r \leq p$ est le rang de M) tels que $(d_1E_1, \ldots, d_rE_r)$ soit une base de M.*

Le calcul de la forme normale de Smith permet d'obtenir une base adaptée à un sous-module.

Proposition 14 *Soit M le sous module de $\mathbb{Z}^p$ engendré par les lignes d'une matrice $A \in \mathsf{M}_{n,p}(\mathbb{Z})$. Soient $L \in \mathsf{GL}_n(\mathbb{Z})$ et $R \in \mathsf{GL}_p(\mathbb{Z})$ des matrices inversibles telles que $L\,A\,R$ soit diagonale. Alors les lignes de R^{-1} sont (à permutation près) une base de $\mathbb{Z}^p$ adaptée à M.*

Il est à noter que bien que le résultat final ne dépende que de la matrice R, on ne peut pas résoudre le problème de la base adaptée par un simple échelonnement suivant les colonnes.

Démonstration : Soit $B = L\,A\,R$. La matrice B est diagonale, et les lignes de $B\,R^{-1} = L\,A$ engendrent le même sous-module que les lignes de A. On obtient donc une base adaptée à M en prenant les lignes de R^{-1}, en plaçant d'abord les lignes de numéro i correspondant à un coe□cient diagonal $b_i \neq 0$. □

Dans le cas où B est la forme normale de Smith de A, il n'y a besoin de permuter les lignes de R^{-1} pour avoir une base adaptée.

5.2 Structure d'un module quotient

Une matrice $A \in \mathsf{M}_{n,p}(\mathbb{Z})$ est la matrice d'une application linéaire $\mathbb{Z}^p \to \mathbb{Z}^n$. Comment décrire le quotient de $\mathbb{Z}^n$ par l'image M de cette application linéaire ? En fait, tout $\mathbb{Z}$-module de type fini, c.-à-d. tout groupe abélien de type fini, peut se présenter de cette façon : tout module qui admet un système de n générateurs est un quotient de $\mathbb{Z}^n$. Nous voici donc arrivés au fameux théorème de structure des groupes abéliens de type fini.

Théorème 15 *Soit $A \in \mathsf{M}_{n,p}(\mathbb{Z})$, et soient $b_1, \ldots, b_r$ les coefficients diagonaux non nuls de sa forme normale de Smith (on rappelle que $b_1 \mid b_2 \mid \ldots \mid b_r$). Alors le quotient de $\mathbb{Z}^n$ par l'image de la matrice A est isomorphe en tant que module à $\mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_r\mathbb{Z} \times \mathbb{Z}^{n-r}$.*

Dans le produit, on peut ôter les facteurs avec $b_i = 1$ puisque $\mathbb{Z}/\mathbb{Z}$ est le module nul, et on peut écrire $\mathbb{Z}$ comme $\mathbb{Z}/0\mathbb{Z}$.

Démonstration : Soit $B = L\,A\,R$ la forme normale de Smith de A. Alors L est la matrice d'un isomorphisme $\mathbb{Z}^n \to \mathbb{Z}^n$ qui envoie l'image de A sur l'image de B, qui est $b_1\mathbb{Z} \times \cdots \times b_r\mathbb{Z} \times \{0\}^{n-r}$. Donc L induit un isomorphisme du quotient de $\mathbb{Z}^n$ par l'image de A sur $\mathbb{Z}/b_1\mathbb{Z} \times \cdots \times \mathbb{Z}/b_r\mathbb{Z} \times \mathbb{Z}^{n-r}$. □

Le théorème de structure s'accompagne d'un résultat d'unicité, que nous donnons ici par souci de complétude bien qu'il n'ait au fond rien à voir avec les entiers, ni même avec les anneaux principaux : il est valable pour n'importe quel anneau commutatif $\mathbb{A}$. Pour énoncer et démontrer ce résultat, nous introduisons les notations suivantes : $\rho(M)$ désignera le nombre minimal de générateurs d'un $\mathbb{A}$-module de type fini et, si I est un idéal de $\mathbb{A}$ et a un élément de $\mathbb{A}$, $(I : a)$ désignera l'idéal des $b \in \mathbb{A}$ tels que $ab \in I$.

Proposition 16 *Soit $\mathbb{A}$ un anneau commutatif. Si M est un $\mathbb{A}$-module isomorphe à $\mathbb{A}/I_1 \times \mathbb{A}/I_2 \times \cdots \times \mathbb{A}/I_r$, où $I_1 \supset I_2 \supset \ldots \supset I_r$ est une suite décroissante d'idéaux propres de $\mathbb{A}$, alors $r = \rho(M)$ et $I_k = \{a \in \mathbb{A}\ ;\ \rho(aM) \leq r - k\}$ pour $k = 1, \ldots, r$. En particulier si $\mathbb{A}/J_1 \times \mathbb{A}/J_2 \times \cdots \times \mathbb{A}/J_s$ est aussi isomorphe à M, où $J_1 \supset \ldots \supset J_s$ est une suite décroissante d'idéaux propres de $\mathbb{A}$, alors $s = r$ et $J_k = I_k$ pour $k = 1, \ldots, r$.*

Cette proposition s'applique bien sûr dans le cas $\mathbb{A} = \mathbb{Z}$, avec $I_k = (b_k)$, les b_k étant des entiers di□érents de ± 1 satisfaisant $b_k \mid b_{k+1}$.

Démonstration : Soit $\mathfrak{m}$ un idéal maximal de $\mathbb{A}$ contenant I_1. Le module quotient $M/\mathfrak{m}M$ a une structure induite d'espace vectoriel sur le corps $\mathbb{A}/\mathfrak{m}$, isomorphe à $(\mathbb{A}/\mathfrak{m})^r$. Comme tout système générateur de M induit un système générateur de $M/\mathfrak{m}M$, on en déduit que $\rho(M) \geq r$. Par ailleurs, puisque chaque $\mathbb{A}/I_k$ est monogène, M a un système générateur formé de r éléments. Donc $\rho(M) = r$.

Soit a un élément de $\mathbb{A}$. Le module aM est isomorphe à $a\mathbb{A}/I_1 \times \cdots \times a\mathbb{A}/I_r$, qui est lui-même isomorphe à $\mathbb{A}/(I_1 : a) \times \cdots \times \mathbb{A}/(I_r : a)$. En e□et, $(I_k : a)$ est le noyau du morphisme de $\mathbb{A}$-modules $A \xrightarrow{\times a} A \to A/I_k$ dont l'image est $a\mathbb{A}/I_k$. On a $(I_1 : a) \supset (I_2 : a) \supset \ldots \supset (I_r : a)$, et $(I_k : a) = A$ si et seulement si $a \in I_k$. En appliquant la première partie de la démonstration, on en déduit que $\rho(aM) \leq r - k$ si et seulement si a appartient à I_k, ce qui conclut la démonstration de la proposition. □

6 Quelques variations autour du déterminant

6.1 Borne de Hadamard

La borne de Hadamard pour le déterminant d'une matrice est tout à fait naturelle quand on pense le déterminant comme volume : le volume d'un parallélépipède est majoré par le produit des longueurs de ses côtés.

Proposition 17 *Soit A une matrice $n \times n$ à coefficients réels. Désignons par $A_1, \ldots, A_n$ ses colonnes. Alors $|\det(A)| \leq \|A_1\| \times \cdots \times \|A_n\|$, où $\|.\|$ est la norme euclidienne usuelle sur $\mathbb{R}^n$.*

Démonstration : On peut se restreindre au cas où $(A_1, \ldots, A_n)$ est une base de $\mathbb{R}^n$, car sinon $\det(A)$ est nul. On applique alors le procédé d'orthogonalisation de Gram-Schmidt à cette base pour fabriquer une base orthogonale $(B_1, \ldots, B_n)$ avec $B_i = A_i + \sum_{j<i} \lambda_{j,i} A_j$. Soit B la matrice qui a pour colonnes les B_i. La matrice B est orthogonalement semblable à la matrice diagonale de coefficients diagonaux $\|B_1\|, \ldots, \|B_n\|$; par ailleurs on a $B = AT$ où T est triangulaire supérieure avec uniquement des 1 sur la diagonale. Donc $\det(A) = \|B_1\| \times \cdots \times \|B_n\|$. Comme B_i est orthogonal à $\sum_{j<i} \lambda_{j,i} A_j$, on a $\|B_i\| \leq \|A_i\|$, ce qui conclut la démonstration. □

Si tous les coefficients de A sont majorés en valeur absolue par a, alors son déterminant l'est par $(\sqrt{n}\, a)^n$. Si tous les coefficients sont des entiers à au plus k chiffres et si $n = 10$, le déterminant a au plus $10k + 5$ chiffres.

Encadré 7 – Borne de Hadamard, calcul modulaire

```
> A:=RandomMatrix(10,10,generator=rand(-10^4..10^4)):
> Determinant(A);evalf(%);
```

$$-16432867439433972499768633571214003298870 3$$

$$-0.1643286744\,10^{42}$$

```
> ListP:=[seq(ithprime(i),i=1600..1610)];
```

$ListP$:= [13499, 13513, 13523, 13537, 13553, 13567, 13577, 13591, 13597, 13613, 13619]

```
> P:=mul(ListP[i],i=1..11):evalf(P);
```

$$0.2856048031\,10^{46}$$

```
> seq(Det(A) mod ListP[i], i=1..11);
> mods(chrem([%],ListP),P);
```

1848, 9452, 3943, 9128, 7526, 2254, 8645, 6015, 2000, 11225, 5623

$$-16432867439433972499768633571214003298870 3$$

La borne de Hadamard (10^{45} pour une matrice 10×10 avec des coefficients à 4 chiffres) n'est pas trop loin de l'ordre de grandeur du déterminant d'un matrice prise au hasard. Le même déterminant est ensuite calculé par un calcul modulaire, en utilisant la commande « chrem » (pour chinese remainder).

Exercice 8 Testez l'optimalité de la borne de Hadamard en considérant des matrice $aJ \otimes J \cdots \otimes J$ (produits tensoriels de la matrice $J = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ avec elle même.)

6.2 Méthode de Bareiss

Nous allons revenir ici sur la méthode usuelle du pivot de Gauss (ou décomposition LU), en portant une attention particulière au cas où on part d'une matrice à coefficients entiers. Nous nous intéresserons

à la croissance de la taille des coe□cients au cours de l'algorithme, et à la possibilité de mener les calculs sans fraction.

Soit A une matrice $n \times p$ à coe□cients dans un corps. Désignons par $A = G^{[0]}, G^{[1]}, G^{[2]}, \ldots$ les matrices obtenues dans les étapes successives de l'élimination de Gauss (nous suppososns que celle-ci se passe sans avoir besoin de permuter des lignes). Désignons par $g_{i,j}^{[p]}$ les coe□cients de $G^{[p]}$. On a $g_{i,j}^{[p]} = 0$ pour $j < \min(i, p+1)$, et le passage de l'étape $p-1$ à l'étape p se fait en conservant les p premières lignes et, pour $i > p$, en retranchant à la i-ème ligne la p-ème multipliée par $g_{i,p}^{[p-1]}$ et divisée par $g_{p,p}^{[p-1]}$ (le pivot) ; on pose donc :

$$g_{i,j}^{[p]} = g_{i,j}^{[p-1]} - \frac{g_{i,p}^{[p-1]}}{g_{p,p}^{[p-1]}} g_{p,j}^{[p-1]} \ . \tag{1}$$

Notre hypothèse sur le bon déroulement de l'algorithme de Gauss revient supposer le pivot $g_{p,p}^{[p-1]}$ non nul pour tout p.

Si la matrice A de départ est à coe□cients entiers, les coe□cients obtenus dans les di□érentes étapes de l'algorithme d'élimination sont rationnels. Nous allons expliquer le phénomène constaté expérimentalement (voir encadré 8) sur la taille des coe□cients.

Commençons par introduire une notation. On désignera par $d_{i,j}^{[p]}$ (avec $p < i \leq n$ et $p < j \leq n$ le déterminant de la matrice $(p+1) \times (p+1)$ extraite de la matrice A en prenant ses p premières lignes et la ligne i d'un côté, ses p premières colonnes et la colonne j de l'autre.

Proposition 18 *Avec les notations précédentes, on a*

$$d_{p,p}^{[p-1]} = g_{1,1}^{[0]} g_{2,2}^{[1]} \cdots g_{p,p}^{[p-1]} \qquad et \qquad d_{i,j}^{[p]} = g_{i,j}^{[p]} d_{p,p}^{[p-1]} \ . \tag{2}$$

Démonstration : Puisque la matrice $G^{[p]}$ est obtenue à partir de la matrice A par des opérations élémentaires sur les lignes où on n'a fait qu'ajouter des multiples de lignes d'indice $\leq p$ aux autres lignes, le déterminant $d_{i,j}^{[p]}$ est égal au déterminant de la matrice extraite de $G^{[p]}$ en choisissant les lignes et colonnes de mêmes indices que pour $d_{i,j}^{[p]}$. Les formules en découlent immédiatement. □

Supposons que la matrice A soit à coe□cients entiers d'au plus k chi□res. Alors le coe□cient d'indice (p,j) que l'on trouve à la fin du processus d'élimination est $g_{p,j}^{[p-1]} = d_{p,j}^{[p-1]} / d_{p-1,p-1}^{[p-2]}$, c'est-à-dire le quotient d'un déterminant $p \times p$ extrait de A par un déterminant $(p-1) \times (p-1)$. Au vu de la borne de Hadamard, ceci colle bien avec la constatation expérimentale (en gros kp chi□res au numérateur, $k(p-1)$ au dénominateur).

Voyons maintenant comment calculer les déterminants extraits $d_{i,j}^{[p]}$ et en particulier le déterminant de A par une variante d'élimination de Gauss sans fraction. C'est l'**algorithme de Bareiss**. On calcule par étape des matrices $B^{[0]} = A$, $B^{[1]}$, $B^{[2]}$, etc. ; on désigne par $b_{i,j}^{[p]}$ les coe□cients de la matrice $B^{[p]}$. Le passage de l'étape $p-1$ à l'étape p se fait en conservant les p premières lignes et, pour $i > p$, en multipliant la i-ème ligne par $b_{p,p}^{[p-1]}$ (le pivot), puis en lui retranchant la p-ème multipliée par $b_{i,p}^{[p-1]}$, et enfin en divisant le tout par $b_{p-1,p-1}^{[p-2]}$ (le pivot de l'étape précédente – on convient que $b_{0,0}^{[-1]} = 1$) ; on pose donc :

$$b_{i,j}^{[p]} = \frac{b_{i,j}^{[p-1]} b_{p,p}^{[p-1]} - b_{i,p}^{[p-1]} b_{p,j}^{[p-1]}}{b_{p-1,p-1}^{[p-2]}} \ . \tag{3}$$

Proposition 19 *Avec les notations précédentes, on a $b_{i,j}^{[p]} = d_{i,j}^{[p]}$. En particulier, les $b_{i,j}^{[p]}$ sont entiers, et les calculs de la méthode de Bareiss se font donc sans fraction.*

Exercice 9 Démontrez l'égalité de la proposition 19 en utilisant les formules (1), (2) et (3) ci-dessus.

Encadré 8 – Élimination de Gauss dans le paquet LinearAlgebra de Maple

```
> A:=RandomMatrix(6,6);
```

$$A := \begin{bmatrix} -73 & 47 & 89 & -29 & 8 & -37 \\ -42 & -85 & 32 & 36 & 93 & 21 \\ -10 & 88 & -68 & -44 & 52 & 67 \\ 18 & -70 & -35 & 17 & -99 & -8 \\ 92 & -88 & 27 & -99 & 45 & -22 \\ -33 & -64 & 96 & 32 & -56 & 86 \end{bmatrix}$$

```
> LUDecomposition(A,output=['P','U']);
```

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -73 & 47 & 89 & -29 & 8 & -37 \\ 0 & \frac{-8179}{73} & \frac{-1402}{73} & \frac{3846}{73} & \frac{6453}{73} & \frac{3087}{73} \\ 0 & 0 & \frac{-770238}{8179} & \frac{-13698}{8179} & \frac{942662}{8179} & \frac{841229}{8179} \\ 0 & 0 & 0 & \frac{-751542}{42791} & \frac{-8078440}{55017} & \frac{-32728985}{770238} \\ 0 & 0 & 0 & 0 & \frac{4993425436}{3381939} & \frac{3008303447}{6763878} \\ 0 & 0 & 0 & 0 & 0 & \frac{199815490934}{1248356359} \end{bmatrix}$$

```
> LUDecomposition(A,method=FractionFree,output='U');
```

$$\begin{bmatrix} -73 & 47 & 89 & -29 & 8 & -37 \\ 0 & 8179 & 1402 & -3846 & -6453 & -3087 \\ 0 & 0 & -770238 & -13698 & 942662 & 841229 \\ 0 & 0 & 0 & 13527756 & 113098160 & 32728985 \\ 0 & 0 & 0 & 0 & 19973701744 & 6016606894 \\ 0 & 0 & 0 & 0 & 0 & 3197047854944 \end{bmatrix}$$

```
> seq(Determinant(SubMatrix(A,1..i,1..i)),i=1..6);
```

$$-73,\ 8179,\ -770238,\ 13527756,\ 19973701744,\ 3197047854944$$

La matrice A de départ a des coe□cients à 2 chi□res. On e□ectue une première décomposition LU et on a□che la matrice U (on a□che aussi la matrice de permutation P pour s'assurer qu'il n'y a pas eu permutation de lignes). Le coe□cient non nul typique sur la ligne p de la matrice U est une fraction avec $2p$ chi□res au numérateur et $2(p-1)$ au dénominateur.
On e□ectue ensuite une « décomposition LU sans fraction », c'est à dire l'algorithme de Bareiss. On constate que les coe□cients diagonaux sur la nouvelle matrice U sont les mineurs principaux de A, en particulier le dernier est $\det(A)$.

6.3 Calcul modulaire

Si A est une matrice à coe□cients entiers, on peut faire un calcul modulaire de son déterminant : on choisit des nombres premiers $p_1, \ldots, p_r$, on calcule $\Delta_i = \det(A) \bmod p_i$ dans le corps $\mathbb{Z}/p_i\mathbb{Z}$ pour $i = 1, \ldots, r$, et on reconstitue ensuite $\det(A)$ grâce au théorème des restes chinois. Pour être sûr de bien retrouver le déterminant, il su□t de s'assurer que le produit $P = p_1 \cdots p_r$ est strictement plus grand que 2 fois la valeur absolue du déterminant. En e□et, si Δ est l'entier ≥ 0 et $< P$ congru à chaque δ_i modulo p_i, alors $\det(A) = \Delta$ si $\Delta \leq P/2$ et $\det(A) = -\Delta$ sinon.

Or, la borne de Hadamard fournit un majorant commode de la valeur absolue du déterminant : ainsi, pour un déterminant 10×10 dont les coe□cients ont quatre chi□res au plus, il su□t de choisir des

nombres premiers dont le produit P est supérieur ou égal à 2×10^{45}. Vous pouvez voir un exemple de calcul modulaire dans l'encadré 7.

Le calcul modulaire permet une parallélisation du calcul du déterminant, puisque chaque $\det(A) \bmod p_i$ peut être calculé indépendamment de autres.

Exercice 10 Donnez une variante de la borne de Hadamard pour un déterminant dont les coe□cients sont des polynômes en une indéterminée X, en termes de degré. Décrivez un algorithme de calcul d'un tel déterminant par interpolation.