Diviseurs élémentaires d'une matrice entière

Yannick Henrio

29 janvier 2017

Vous avez vu dans le cours d'algèbre linéaire la méthode du pivot de Gauss. On peut vérifier qu'effectuer une opération élémentaire sur les lignes revient à multiplier à gauche par une matrice inversible. Par exemple,

$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c+\lambda a & d+\lambda b \end{pmatrix}$$

et ainsi multiplier à gauche par la matrice inversible $\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$, d'inverse (vérifiez !) $\begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$, revient à effectuer l'opération élémentaire $L_2 \leftarrow L_2 + \lambda L_1$. On peut donc déduire de la méthode du pivot de Gauss l'énoncé suivant :

Théorème 1: Pivot de Gauss

Si $\boldsymbol{A} \in \mathcal{M}_{n,p}(\mathbb{R})$ est une matrice réelle de taille (n,p), il existe une matrice réelle inversible $\boldsymbol{P}$ de taille n et une unique matrice échelonnée réduite $\boldsymbol{B}$ tels que $\boldsymbol{B} = \boldsymbol{PA}$.

Le but du projet est d'établir un résultat analogue pour les matrices entières, c'est-à-dire à coefficients entiers. On notera $M_{n,p}(\mathbb{Z})$ l'ensemble des matrices entières de taille (n,p). Dans la suite, toutes les matrices seront supposées entières. De plus, une matrice entière inversible sera une matrice inversible dont la matrice inverse est entière. On notera $GL_n(\mathbb{Z})$ l'ensemble des matrices entières inversibles. On va programmer une variante arithmétique du pivot de Gauss qui se traduit par l'énoncé suivant :

Théorème 2: Base adaptée

Si $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$ est une matrice entière de taille (n,p) et de rang r, il existe des matrices entières inversibles $\boldsymbol{P} \in GL_n(\mathbb{Z})$ et $\boldsymbol{Q} \in GL_p(\mathbb{Z})$ et une unique suite d'entiers strictement positifs $(d_1,\dots,d_r)$ satisfaisant $d_1|d_2|\dots|d_r$ et

$$\boldsymbol{PAQ} = \begin{pmatrix} d_1 & 0 & & \dots & 0 \\ 0 & \ddots & & & \\ & & d_r & & \\ \vdots & & & 0 & \vdots \\ 0 & & & \dots & 0 \end{pmatrix} \tag{1}$$

*La suite $(d_1,\dots,d_r)$ est appelée suite des **diviseurs élémentaires** de $\boldsymbol{A}$.*

1 Ce que devra contenir votre projet

1.1 Rapport et soutenance

Ce projet devra s'achever par la remise d'un rapport écrit contenant au minimum d'une part les réponses aux questions posées dans ce sujet, d'autre part les listings commentés de vos programmes. Une soutenance orale aura ensuite lieu, pendant laquelle vous devrez présenter votre projet, en mettant en lumière les ressources que vous avez pu utilisé, les difficultés rencontrées, et tout commentaire pertinent. Vos programmes seront testés lors de la soutenance, il serait utile de produire une interface graphique. A tout le moins, une méthode de saisie d'une matrice entière est vivement conseillée. Il est toujours gênant pour un examinateur de voir un étudiant être contraint d'entrer des lignes de code en plein milieu de la soutenance...

1.2 Programmation

La seule requête concernant le langage de programmation est qu'il doit être orienté objet. Typiquement, JAVA ou C...

Le programme devra au moins contenir une classe **Matrice** permettant de travailler sur les matrices entières. Typiquement, on aura comme variables d'instance le nombre de lignes, le nombre de colonnes, et les coefficients de la matrice. On doit au minimum avoir un constructeur **Matrice**($int\ n$, $int\ p$) produisant un objet correspondant à la matrice nulle de taille (n, p).

Les méthodes exigées au grand minimum sont :

— Une procédure de calcul du produit de deux matrices entières.
— Une méthode effectuant l'échange de deux lignes de la matrice.
— Une méthode effectuant l'opération $L_i \leftarrow -L_i$.
— Une méthode effectuant l'opération $L_i \leftarrow L_i + \lambda L_j$, où λ est un paramètre entier.
— Une méthode statique d'Euclide-Bezout (algorithme 1).
— Les trois méthodes de réduction d'une matrice (algorithmes 2 à 4).
— Une méthode de calcul des diviseurs élémentaires (algorithme 5, à compléter).

Il sera toutefois nécessaire d'en ajouter à cette liste pour aérer le code !

1.3 Un dernier conseil

Pour justifier la validité des divers algorithmes de réduction, il peut être judicieux de les programmer et de les tester sur des matrices aléatoires en insérant dans le code des méthodes d'affichage pour observer l'évolution de la matrice.

2 L'algorithme d'Euclide-Bezout

Théorème 3

*Soient a et b des entiers relatifs. Soit $d =$ **pgcd**(a, b). Alors, il existe des entiers relatifs u et v tels que $d = au + bv$. On dira que le triplet d'entiers (d, u, v) est un triplet d'Euclide-Bezout associé à (a, b).*

L'algorithme ci-dessous construit un tel triplet d'Euclide-Bezout :

Algorithme 1: Euclide-Bezout

```
Entier[]   euclideBezout( Entier a , Entier b ) {
               Entier x = |a|, y = |b| ;
               Entier[] triplet = new Entier[3] ;
               if( y = 0 ){
                    triplet[0] = x ;
                    triplet[1] = 1 ;
                    triplet[2] = 0 ;
               }
               else {
                    triplet = euclideBezout(y, x%y) ;
                    Entier u = triplet [2] ;
                    Entier v = triplet [1] − (x/y)∗ triplet [2] ;
                    triplet[1] = u ;
                    triplet[2] = v ;
               }
               if( a < 0 ) triplet[1] = −triplet[1] ;
               if( b < 0 ) triplet[2] = −triplet[2] ;
               return triplet ;
           }
```

Cet algorithme renvoie un tableau de trois entiers (d,u,v) satisfaisant $\mathbf{pgcd}(a,b) = d = au + bv$.

Questions 1

Vérifier que cet algorithme accomplit bien la tâche indiquée.

3 Conventions matricielles

Toutes les matrices considérées sont à coefficients entiers relatifs.

Notation 1

1. *Dire qu'une matrice est de taille (n,p) signifie qu'elle a n lignes et p colonnes. On note $M_{n,p}(\mathbb{Z})$ l'ensemble des matrices entières de taille (n,p).*
2. *Les matrices sont notées en caractère gras.*
3. *La matrice nulle de taille (n,p) est notée $\mathbf{0}_{n,p}$ ou simplement $\mathbf{0}$ s'il n'y a pas d'ambigüité sur la taille.*
4. *La matrice unité de taille n est notée* $\boldsymbol{I}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

4 Construction de matrices inversibles

Définition 1

Soit $\boldsymbol{P} \in M_{n,n}(\mathbb{Z})$ une matrice carrée de taille n. On dit que $\boldsymbol{P}$ est inversible s'il existe $\boldsymbol{P}^{-1} \in M_{n,n}(\mathbb{Z})$ satisfaisant $\boldsymbol{P}\boldsymbol{P}^{-1} = \boldsymbol{P}^{-1}\boldsymbol{P} = \boldsymbol{I}_n$. Par exemple, $\boldsymbol{I}_n$ est inversible et $\boldsymbol{I}_n^{-1} = \boldsymbol{I}_n$.
On notera $GL_n(\mathbb{Z})$ l'ensemble des matrices inversibles de taille n.

4.1 Matrices entières inversibles de taille 2

Proposition 1

Considérons une matrice entière $\boldsymbol{P} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfaisant $ad - bc = 1$.
Alors, $\boldsymbol{P}$ est inversible d'inverse $\boldsymbol{P}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Proposition 2

Soit $(a,b) \in \mathbb{Z}^2$ et (d,u,v) un triplet d'Euclide-Bezout associé. Remarquons que $d = \textbf{pgcd}(a,b)$ divise a et b, de sorte que $\frac{a}{d} \in \mathbb{Z}$ et $\frac{b}{d} \in \mathbb{Z}$.

1. *La matrice entière $\boldsymbol{P} = \begin{pmatrix} u & v \\ -b/d & a/d \end{pmatrix}$ est inversible.*
2. *On a la formule $\boldsymbol{P}.\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$.*

Questions 2

Prouver ces deux propositions.

4.2 Obtenir des matrices inversibles de taille quelconque

L'idée est de "plonger" une matrice inversible de taille 2 dans une matrice de taille n.

Notation 2

On rappelle que le symbole de Kronecker est l'application $\delta : \mathbb{N}^2 \to \{0;1\}$ *qui envoie* $(p,q) \in \mathbb{N}^2$ *sur* $\delta_{p,q}$ *défini par* $\delta_{p,q} = 1$ *si* $p = q$ *et* $\delta_{p,q} = 0$ *sinon.*

Soit $\boldsymbol{A} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ *une matrice de taille* 2. *Si* $1 \leqslant k < l \leqslant n$, *on note* $\boldsymbol{B} = \rho_{k,l,n}(\boldsymbol{A})$ *la matrice carrée de taille* n *définie comme suit :*

$$\begin{array}{rcll} b_{i,j} & = & a_{1,1} & \text{si } (i,j) = (k,k) \\ & = & a_{1,2} & \text{si } (i,j) = (k,l) \\ & = & a_{2,1} & \text{si } (i,j) = (l,k) \\ & = & a_{2,2} & \text{si } (i,j) = (l,l) \\ & = & \delta_{i,j} & \text{sinon} \end{array} \tag{2}$$

Par exemple,

$$\rho_{1,3,4}\begin{pmatrix} 3 & 2 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 5 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Propriétés 1

Supposons $1 \leqslant k < l \leqslant n$. *Alors,*

1. *Le plongement* $\rho_{k,l,n} : M_{2,2}(\mathbb{Z}) \to M_{n,n}(\mathbb{Z})$ *préserve les matrices unités :*
$$\rho_{k,l,n}(\boldsymbol{I}_2) = \boldsymbol{I}_n \tag{3}$$
2. *Le plongement* $\rho_{k,l,n} : M_{2,2}(\mathbb{Z}) \to M_{n,n}(\mathbb{Z})$ *préserve le produit de deux matrices :*
$$\forall \boldsymbol{A} \in M_{2,2}(\mathbb{Z})\ \forall \boldsymbol{B} \in M_{2,2}(\mathbb{Z}) \qquad \rho_{k,l,n}(\boldsymbol{A}.\boldsymbol{B}) = \rho_{k,l,n}(\boldsymbol{A})\rho_{k,l,n}(\boldsymbol{B}) \tag{4}$$
3. *Le plongement* $\rho_{k,l,n} : M_{2,2}(\mathbb{Z}) \to M_{n,n}(\mathbb{Z})$ *préserve les matrices inversibles :*
$$\forall \boldsymbol{P} \in GL_2(\mathbb{Z}) \qquad \rho_{k,l,n}(\boldsymbol{P}) \in GL_n(\mathbb{Z}) \tag{5}$$

Questions 3

Prouver ces propriétés.

5 Une relation d'équivalence dans $M_{n,p}(\mathbb{Z})$

Définition 2

On définit une relation notée $\sim$ dans $M_{n,p}(\mathbb{Z})$ par la formule :

$$\forall \boldsymbol{A} \in M_{n,p}(\mathbb{Z})\ \forall \boldsymbol{B} \in M_{n,p}(\mathbb{Z})$$

$$\boldsymbol{A} \sim \boldsymbol{B} \quad \Leftrightarrow \quad \exists \boldsymbol{P} \in GL_n(\mathbb{Z})\ \exists \boldsymbol{Q} \in GL_p(\mathbb{Z}) \quad \boldsymbol{B} = \boldsymbol{PAQ} \tag{6}$$

Questions 4

1. *Si $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$, calculer $\boldsymbol{I}_n \boldsymbol{A} \boldsymbol{I}_p$. En déduire que la relation $\sim$ est réflexive.*
2. *Soit $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$, $\boldsymbol{B} \in M_{n,p}(\mathbb{Z})$, $\boldsymbol{P} \in GL_n(\mathbb{Z})$ et $\boldsymbol{Q} \in GL_p(\mathbb{Z})$, vérifier que $\boldsymbol{B} = \boldsymbol{PAQ} \Rightarrow \boldsymbol{A} = \boldsymbol{P}^{-1}\boldsymbol{B}\boldsymbol{Q}^{-1}$. En déduire que la relation $\sim$ est symétrique.*
3. *Vérifier que le produit de deux matrices entières inversibles est une matrice entière inversible. En déduire que la relation $\sim$ est transitive.*
4. *Conclure.*

6 Une première réduction de la matrice.

Définition 3

On note $\mathrm{Fil}^1(n,p)$ l'ensemble des $\mathbb{Z}$-matrices $\boldsymbol{A}$ de taille (n,p) satisfaisant :

$$a_{1,1} \geq 0 \qquad \text{et} \qquad \forall j \in \{2,\dots,p\}\ a_{1,j} = 0$$

Autrement dit, la première ligne de $\boldsymbol{A}$ est de la forme $(d,0,\dots,0)$, avec $d \geqslant 0$.

Théorème 4

$$\forall \boldsymbol{A} \in M_{n,p}(\mathbb{Z})\ \exists \boldsymbol{B} \in \mathrm{Fil}^1(n,p) \qquad \boldsymbol{A} \sim \boldsymbol{B} \tag{7}$$

L'algorithme suivant construit une telle matrice $\boldsymbol{B}$.

Algorithme 2: Première réduction

```
Matrice réduction1( Matrice A ){
    Matrice B = copie( A ) ;
    Entier n = nombreLignes(A) ;
    Entier p = nombreColonnes(A) ;
    Entier i = 1 ;
    while( L_i(B) = 0 ) i = i + 1 ;
    if( i ⩽ n ){
        if( i ⩾ 2 ) Echanger L_1(B) et L_i(B) ;
        if( b_{1,1} < 0 ) Effectuer L_1 ← −L_1 sur B ;
        for( Entier j = 2 to p ){
            Entier[] (d, u, v) = euclideBezout( b_{1,1} , b_{1,j} ) ;
            if( d ≠ 0 ){
                Matrice Q = ρ_{1,j,p} ( u   −b_{1,j}/d )
                                      ( v    b_{1,1}/d ) ;
                B = BQ ;
            }
        }
    }
    return B ;
}
```

Si $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$, cet algorithme retourne une matrice $\boldsymbol{B} \in \mathrm{Fil}^1(n,p)$ telle que $\boldsymbol{A} \sim \boldsymbol{B}$. Si de plus $\boldsymbol{A} \neq \boldsymbol{0}$, on aura $b_{1,1} > 0$.

Questions 5

Vérifier que cet algorithme accomplit bien la tâche indiquée.

7 Une deuxième réduction de la matrice.

Définition 4

On note $\mathrm{Fil}^2(n,p)$ l'ensemble des $\mathbb{Z}$-matrices $\boldsymbol{A}$ de taille (n,p) satisfaisant :

$$\boldsymbol{A} \in \mathrm{Fil}^1(n,p) \qquad \text{et} \qquad \forall i \in \{2,\dots,n\} \qquad a_{i,1} = 0$$

Autrement dit, $\boldsymbol{A} \in \mathrm{Fil}^2(n,p)$ lorsqu'elle est de la forme suivante :

$$\boldsymbol{A} = \left(\begin{array}{c|ccc} d & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) \qquad \text{avec } d \geqslant 0$$

Remarquons que $\mathrm{Fil}^2(n,p) \subseteq \mathrm{Fil}^1(n,p)$.

Théorème 5

$$\forall \boldsymbol{A} \in \mathrm{Fil}^1(n,p)\ \exists \boldsymbol{B} \in \mathrm{Fil}^2(n,p) \qquad \boldsymbol{A} \sim \boldsymbol{B} \tag{8}$$

Une telle matrice $\boldsymbol{B}$ s'obtient grâce à l'algorithme suivant :

Algorithme 3: Seconde réduction

```
Matrice  réduction2( Matrice A ){
    Matrice B = copie( A ) ;
    Entier n = nombreLignes(A) ;
    if( b_{1,1} ≠ 0 ){
        while( b_{1,1} ∤ C_1(B) ){
            Entier i = 2 ;
            while( b_{1,1} | b_{i,1} ) i = i + 1 ;
            Entier[] (d, u, v) = euclideBezout( b_{1,1} , b_{i,1} ) ;
            Matrice P = ρ_{1,i,n} ( u        v       ) ;
                                  ( -b_{i,1}/d  b_{1,1}/d )
            B = PB ;
            B = réduction1(B) ;
        }
        for( Entier i = 2 to n ){
            Effectuer L_i ← L_i - (b_{i,1}/b_{1,1}) L_1 sur B ;
        }
    }
    return B ;
}
```

Si $\boldsymbol{A} \in \mathrm{Fil}^1(n,p)$, cet algorithme retourne une matrice $\boldsymbol{B} \in \mathrm{Fil}^2(n,p)$ telle que $\boldsymbol{A} \sim \boldsymbol{B}$.

Questions 6

Vérifier que cet algorithme accomplit bien la tâche indiquée.

8 Une troisième réduction de la matrice.

Définition 5

On note $\mathrm{Fil}^3(n,p)$ *l'ensemble des* $\mathbb{Z}$*-matrices* $\boldsymbol{A}$ *de taille* (n,p) *satisfaisant :*

$$A \in \mathrm{Fil}^2(n,p) \qquad \text{et} \qquad a_{1,1} \mid A$$

Autrement dit, $A \in \mathrm{Fil}^3(n,p)$ *lorsqu'elle est de la forme suivante :*

$$A = \left(\begin{array}{c|ccc} d & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right) \qquad \text{avec } d \geqslant 0 \text{ et } d \mid A$$

Remarquons que $\mathrm{Fil}^3(n,p) \subseteq \mathrm{Fil}^2(n,p)$.

Théorème 6

$$\forall \boldsymbol{A} \in \mathrm{Fil}^2(n,p)\ \exists \boldsymbol{B} \in \mathrm{Fil}^3(n,p) \qquad \boldsymbol{A} \sim \boldsymbol{B} \tag{9}$$

Une telle matrice $\boldsymbol{B}$ s'obtient grâce à l'algorithme suivant :

Algorithme 4: Troisième réduction

```
Matrice réduction3( Matrice A ){
    Matrice B = copie( A ) ;
    Entier n = nombreLignes(A) ;
    Entier p = nombreColonnes(A) ;
    if( b_{1,1} ≠ 0 ){
        while( b_{1,1} ∤ B ){
            Entier i = 2 ;
            while( b_{1,1} | L_i(B) ) i = i + 1 ;
            Effectuer L_1 ← L_1 + L_i sur B ;
            B = réduction1(B) ;
            B = réduction2(B) ;
        }
    }
    return B ;
}
```

Si $\boldsymbol{A} \in \mathrm{Fil}^2(n,p)$*, cet algorithme retourne une matrice* $\boldsymbol{B} \in \mathrm{Fil}^3(n,p)$ *telle que* $\boldsymbol{A} \sim \boldsymbol{B}$.

Questions 7

Vérifier que cet algorithme accomplit bien la tâche indiquée.

9 Calcul des diviseurs élémentaires de la matrice

On considère une matrice $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$ de rang r.

Notation 3

Soient $n \geqslant 1$, $p \geqslant 1$ et r des entiers satisfaisant $0 \leqslant r \leqslant \min(n,p)$. Si de plus $d_\bullet = (d_1, \ldots, d_r)$ est une suite d'entiers strictement positifs satisfaisant $d_1 \mid \ldots \mid d_r$, on note

$$\boldsymbol{D}(n,p,r,d_\bullet) = \left(\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & \boldsymbol{0}_{r,p-r} \\ 0 & & d_r & \\ \hline & \boldsymbol{0}_{n-r,r} & & \boldsymbol{0}_{n-r,p-r} \end{array}\right) \tag{10}$$

Théorème 7

Soit $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$ de rang r. Alors, il existe une suite d'entiers strictement positifs $d_\bullet = (d_1, \ldots, d_r)$ satisfaisant $d_1 \mid \ldots \mid d_r$ tel que

$$\boldsymbol{A} \sim \boldsymbol{D}(n,p,r,d_\bullet) \tag{11}$$

Démonstration. Si $\boldsymbol{A} = \boldsymbol{0}_{n,p}$, alors $\boldsymbol{A} = \boldsymbol{D}(n,p,0,\emptyset)$. Le résultat est donc immédiat dans ce cas. Dans le cas où $\boldsymbol{A} \neq \boldsymbol{0}_{n,p}$, on va raisonner par récurrence sur $k = \min(n,p)$. Précisément, on note pour tout entier $k \geqslant 1$, la proposition :

> $\mathscr{P}_k$: Soient n et p des entiers tels que $\min(n,p) = k$, et soit $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$ une matrice non nulle de rang r. Alors, il existe une suite d'entiers strictement positifs $d_\bullet = (d_1, \ldots, d_r)$ satisfaisant $d_1 \mid \ldots \mid d_r$ tel que $\boldsymbol{A} \sim \boldsymbol{D}(n,p,r,d_\bullet)$.

Preuve de la proposition $\mathscr{P}_1$. On considère des entiers n et p des entiers tels que $\min(n,p) = 1$. On a donc soit $n = 1$, soit $p = 1$. Soit $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$ une matrice non nulle de rang r. Remarquons qu'alors $1 \leqslant r \leqslant \min(n,p) = 1$ et ainsi $r = 1$.

Traitons tout d'abord le cas $n = 1$: Posons $\boldsymbol{A}_1 = \textbf{réduction1}(\boldsymbol{A})$. On a donc $\boldsymbol{A}_1 \in \mathrm{Fil}^1(n,p)$ et $\boldsymbol{A} \sim \boldsymbol{A}_1$. Comme $n = 1$ et $\boldsymbol{A}_1 \in \mathrm{Fil}^1(n,p)$, il existe un entier $d > 0$ tel que $\boldsymbol{A}_1 = (d, 0, \ldots, 0) = \boldsymbol{D}(1,p,1,(d))$. Ainsi, $\boldsymbol{A} \sim \boldsymbol{D}(1,p,1,(d))$.

Il reste à traiter le cas $p = 1$. Posons $\boldsymbol{A}_1 = \textbf{réduction1}(\boldsymbol{A})$ et $\boldsymbol{A}_2 = \textbf{réduction1}(\boldsymbol{A}_1)$. On a $\boldsymbol{A} \sim \boldsymbol{A}_1 \sim \boldsymbol{A}_2$ et donc $\boldsymbol{A} \sim \boldsymbol{A}_2$ par transitivité de la relation $\sim$. Comme $p = 1$ et $\boldsymbol{A}_2 \in \mathrm{Fil}^2(n,p)$, il existe un entier $d > 0$ tel que

$$\boldsymbol{A}_2 = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \boldsymbol{D}(n,1,1,(d))$$

Ainsi, $\boldsymbol{A} \sim \boldsymbol{D}(n,1,1,(d))$.

□

Preuve de l'implication $\mathscr{P}_k \Rightarrow \mathscr{P}_{k+1}$ pour tout entier $k \geqslant 1$. On suppose la proposition $\mathscr{P}_k$ vraie. Il faut donc vérifier que $\mathscr{P}_{k+1}$ l'est également sous cette hypothèse. Considérons une matrice non nulle $\boldsymbol{A} \in M_{n,p}(\mathbb{Z})$, avec $\min(n,p) = k+1$. On pose $\boldsymbol{A}_1 = \textbf{réduction1}(\boldsymbol{A})$, $\boldsymbol{A}_2 = \textbf{réduction2}(\boldsymbol{A}_1)$

et $\boldsymbol{A}_3 = \textbf{réduction3}(\boldsymbol{A}_2)$. On a $\boldsymbol{A}_i \in \text{Fil}^i(n,p)$ pour $1 \leqslant i \leqslant 3$ et $\boldsymbol{A} \sim \boldsymbol{A}_1 \sim \boldsymbol{A}_2 \sim \boldsymbol{A}_3$. La transitivité de la relation $\sim$ entraîne $\boldsymbol{A} \sim \boldsymbol{A}_3$. Comme $\boldsymbol{A}_3 \in \text{Fil}^3(n,p)$, il existe un entier $d > 0$ et une matrice $\boldsymbol{B} \in M_{n-1,p-1}(\mathbb{Z})$ tels que

$$\boldsymbol{A}_3 = \left(\begin{array}{c|c} d & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{B} \end{array}\right) \qquad \text{et} \qquad d \mid \boldsymbol{B}$$

Si $\boldsymbol{B} = \boldsymbol{0}$, alors $\boldsymbol{A}_3 = \boldsymbol{D}(n-1,p-1,1,(d))$ et ainsi $\boldsymbol{A} \sim \boldsymbol{D}(n-1,p-1,1,(d))$.

Supposons désormais $\boldsymbol{B} \neq \boldsymbol{0}$. On remarque que $r = \text{rg}\,(\boldsymbol{A}) = \text{rg}\,(\boldsymbol{A}_3) = \text{rg}\,(\boldsymbol{B}) + 1$, et ainsi $\text{rg}\,(\boldsymbol{B}) = r-1$. De plus, $\min(n-1,p-1) = \min(n,p) - 1 = (k+1) - 1 = k$. D'après la proposition $\mathscr{P}_k$, il existe une suite d'entiers strictement positifs $d'_\bullet = (d'_1,\ldots,d'_{r-1})$ satisfaisant $d'_1 \mid \ldots \mid d'_{r-1}$ et $\boldsymbol{B} \sim \boldsymbol{D}(n-1,p-1,r-1,d'_\bullet)$. Autrement dit, il existe des matrices $\boldsymbol{P} \in GL_{n-1}(\mathbb{Z})$ et $\boldsymbol{Q} \in GL_{p-1}(\mathbb{Z})$ telles que $\boldsymbol{PBQ} = \boldsymbol{D}(n-1,p-1,r-1,d'_\bullet)$.

On remarque alors l'égalité matricielle :

$$\begin{array}{rl} & \left(\begin{array}{c|c} 1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{P} \end{array}\right)\left(\begin{array}{c|c} d & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{B} \end{array}\right)\left(\begin{array}{c|c} 1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{Q} \end{array}\right) \\ = & \left(\begin{array}{c|c} 1*d*1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{PBQ} \end{array}\right) \\ = & \left(\begin{array}{c|c} d & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{D}(n-1,p-1,r-1,d'_\bullet) \end{array}\right) \\ = & \boldsymbol{D}(n,p,r,(d,d'_\bullet)) \end{array}$$

Comme $d \mid \boldsymbol{B}$, on a à fortiori $d \mid \boldsymbol{PBQ} = \boldsymbol{D}(n-1,p-1,r-1,d'_\bullet)$, et en particulier d divise le coefficient en haut à gauche d'_1 de $\boldsymbol{D}(n-1,p-1,r-1,d'_\bullet)$. Ainsi,

$$d \mid d'_1 \mid \ldots \mid d'_{r-1}$$

La liste $(d,d'_\bullet) = (d,d'_1,\ldots,d'_{r-1})$ remplit donc toutes les conditions demandées. On a bien vérifié la véracité de $\mathscr{P}_{k+1}$ sous l'hypothèse $\mathscr{P}_k$. □

En conclusion, le principe de récurrence entraîne que la proposition $\mathscr{P}_k$ est vraie pour tout entier $k \geqslant 1$, ce qui signifie que le théorème est vrai pour toute matrice non nulle. Comme le cas d'une matrice nulle a déjà été traité, on a terminé la preuve. □

Questions 8

En s'inspirant de la preuve ci-dessus, compléter l'algorithme ci-dessous en un algorithme récursif calculant les diviseurs élémentaires d'une matrice.

Algorithme 5: Calcul des diviseurs élémentaires, à compléter

```
ListeEntiers   diviseurs ( Matrice A ){
                   Matrice B = copie( A ) ;
                   Entier n = nombreLignes(A) ;
                   Entier p = nombreColonnes(A) ;
                   ListeEntiers diviseurs = ∅ ;
                   if( B ≠ 0 and n = 1 ){ ... }
                   if( B ≠ 0 and n ⩾ 2 and p = 1 ){ ... }
                   if( B ≠ 0 and n ⩾ 2 and p ⩾ 2 ){ ... }
                   return diviseurs ;
               }
```