TP2 : Algèbre linéaire sur un anneau principal

Résumé du TP

Bertrand Meyer

29 novembre 2023

Les modules sur un anneau principal

Passer d'un corps à un anneau

Caveat

Dans des problèmes d'algèbre linéaire sur un anneau A, on ne peut pas diviser par des constantes

$\to$ pas de pivot de Gauß,

$\to$ pas d'algèbre linéaire classique.

Exemple

Le système

$$\begin{cases} 40x & + & 70y & + & 20z & = & -60 \\ 20x & + & 50y & + & 60z & = & 40 \end{cases}$$

a pour solution dans $\mathbb{Q}$

$$(-29/3, 14/3, 0) + \mathbb{Q}(1, -5/8, 3/16).$$

Quelles sont les solutions entières ?

Définition
Un module M sur un anneau A est « l'équivalent d'un espace vectoriel » sur A lorsque A est un anneau.

Définition
Un module M sur un anneau A est « l'équivalent d'un espace vectoriel » sur A lorsque A est un anneau.

Exemples

- (avec $A = \mathbb{Z}$) $\mathbb{Z}^n$ ou $\mathbb{Z}/d\mathbb{Z}$ sont des $\mathbb{Z}$-modules .
- (avec $A = \mathbb{F}_p[x]$) $\mathbb{F}_p[x]/\langle f(x) \rangle$ est un $\mathbb{F}_p[x]$-modules .
- (avec $A = \mathbb{K}[x]$) Soient **K** un corps et $\mathbf{M} \in \mathbb{K}^{n\times n}$ une matrice fixée. L'ensemble des vecteurs $\mathbb{K}^n$ est un $\mathbb{K}[x]$ module (cf. **TP 10**)

$$\cdot : \ (p, \mathbf{x}) \in \mathbb{K}[x] \times \mathbb{K}^n \mapsto p(\mathbf{M})\mathbf{x} \in \mathbb{K}^n$$

- (avec $A = \mathbb{Z}$) Points d'une courbe elliptique (cf. **TP13**)

Pourquoi se restreindre aux anneaux principaux ?

Une droite vectorielle est toujours de la forme $\mathbb{K}\mathbf{v}$ (engendrée par 1 seul élément).

Un sous-module de A (en tant que A-module) est en fait un idéal de A. Si A n'est pas principal, les idéaux ne sont pas forcément monogènes (i.e. de la forme Aa).

Exemple
L'ensemble $\mathfrak{I} = \langle x, y\rangle \subseteq \mathbb{K}[x, y]$ est un idéal (donc un sous-module) de $A = \mathbb{K}[x, y]$. Cependant, il n'existe pas de polynôme a tel que $\mathfrak{I} = Aa$.

Engendrement et bases

On dispose de notion de famille libre, de famille génératrice, de base.

Définition
Un module qui possède

- une famille génératrice finie est dit de type fini.
- une base est dit libre.

Engendrement et bases

On dispose de notion de famille libre, de famille génératrice, de base.

Définition
Un module qui possède

- une famille génératrice finie est dit de type fini.
- une base est dit libre.

Exemples

- $\mathbb{Z}^n$ admet comme $\mathbb{Z}$-base l'ensemble des n vecteurs

$$(0, \ldots, 0, 1, 0, \ldots, 0)\,.$$

- $\mathbb{Z}/d\mathbb{Z}$ est un $\mathbb{Z}$-module de type fini engendré par 1, mais n'admet pas de base, ni même de famille libre.

Rappel : classification des e.v. en dim. finie
Un $\mathbb{K}$-espace vectoriel de dimension fini est forcément une copie de $\mathbb{K}^n$.

Rappel : classification des e.v. en dim. finie
Un $\mathbb{K}$-espace vectoriel de dimension fini est forcément une copie de $\mathbb{K}^n$.

Théorème (Structure des A-modules)
Tout module sur A de type fini est isomorphe à

$$\underbrace{A^r}_{\text{partie libre}} \oplus \underbrace{A/d_1A \oplus A/d_2A \oplus \cdots \oplus A/d_sA}_{\text{partie de torsion}}$$

où r est un unique entier appelé rang et les constantes $d_i \in A$ vérifient $d_1|d_2$, $d_2|d_3$, ..., $d_{s-1}|d_s$, sont uniques modulo $A^\times$ et s'appellent les facteurs invariants.

Base adaptée

Rappel : théorème de la base incomplète
Si $F \subseteq E$ sont deux $\mathbb{K}$ espaces vectoriels, alors il existe une base $(e_1, \ldots, e_m)$ de E telle que $(e_1, \ldots, e_n)$, avec $n \leq m$, est une base de F.

Rappel : théorème de la base incomplète
Si $F \subseteq E$ sont deux $\mathbb{K}$ espaces vectoriels, alors il existe une base $(e_1, \dots, e_m)$ de E telle que $(e_1, \dots, e_n)$, avec $n \leq m$, est une base de F.

Théorème (Base adaptée)
Si $N \subseteq M$ sont deux A-modules et si M est libre, alors il existe une famille de vecteurs $(\mathbf{e}_i)_{i \leq m}$ et des scalaires $(d_j)_{j \leq n}$vérifiant $d_1 | d_2$, $d_2 | d_3$, ..., $d_{n-1} | d_n$ tels que

1. $M = A\mathbf{e}_1 \oplus A\mathbf{e}_2 \oplus \cdots \oplus A\mathbf{e}_m$
2. $N = Ad_1\mathbf{e}_1 \oplus Ad_2\mathbf{e}_2 \oplus \cdots \oplus Ad_n\mathbf{e}_n$

Exemple
Avec $M = \mathbb{Z}^2$, $N = \mathbb{Z}\begin{pmatrix} 3 \\ 6 \end{pmatrix}$, la base $\left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ est adaptée (et d_1 vaut 3).

Réduction des matrices

Opérations élémentaires

Une opération élémentaire sur les lignes (ou les colonnes) est

- une transposition $C_i \leftrightarrow C_j$,
- ou une dilatation de rapport inversible $C_i \leftarrow \lambda C_i$ avec $\lambda \in A^\times$,
- ou une transvection de rapport quelconque $C_i \leftarrow C_i + \mu C_j$ avec $\mu \in A$,
- ou une opération de Bezout :

$$\begin{cases} C_i & \leftarrow & sC_i & + & tC_j \\ C_j & \leftarrow & uC_i & + & vC_j \end{cases} \quad \text{avec} \quad \begin{vmatrix} s & u \\ t & v \end{vmatrix} \in A^\times.$$

Ces opérations sont toutes **inversibles** dans A ($\det \in A^\times$).

Annuler un coefficient avec un autre

Soient $ua + vb = d$ une relation de Bezout, alors

$$\begin{pmatrix} * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & * \\ * & a & * & b & * \\ * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & * \end{pmatrix} \text{ devient } \begin{pmatrix} * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & * \\ * & d & * & 0 & * \\ * & * & * & * & * \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ * & * & * & * & * \end{pmatrix}$$

avec l'opération de Bezout

$$\begin{cases} C_i & \leftarrow & uC_i & + & vC_j \\ C_j & \leftarrow & -(b/d)C_i & + & (a/d)C_j \end{cases}$$

Forme normale d'Hermite

Définition

Une matrice est sous forme normale d'Hermite si

i. toutes les colonnes nulles sont regroupées à gauche de la matrice
ii. le dernier élément non-nul d'une colonne est réduit multiplicativement modulo $A^\times$, on l'appelle directeur,
iii. entre deux colonnes successives, le directeur de la colonne de droite se trouve strictement plus bas que le directeur de la colonne de gauche
iv. dans toute ligne contenant un directeur, les coefficients à droite d'un directeur sont réduits additivement modulo celui-ci.

Forme normale d'Hermite

Exemple

$$\begin{pmatrix} 0 & 0 & 0 & 1 & -10 & 9 \\ 0 & 0 & 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 0 & -5 & 18 \\ 0 & 0 & 0 & 0 & 7 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

Les directeurs, 3, 7 et 4, appartiennent à $\mathbb{Z}^+$. La ligne 2 est réduite modulo 3, la ligne 4 est réduite modulo 7.

Algorithme de mise sous forme HNF

Le pivot p est initialement dans le coin inférieur droit.

1. Amener par une transposition un coefficient non nul en position de pivot (sinon remonter le pivot d'une ligne)
2. Annuler tout coefficient à gauche du pivot par une opération de Bezout
3. Réduire multiplicativement le pivot par une dilatation
4. Réduire additivement modulo p tout coefficient à droite du pivot par une transvection.
5. Remonter le pivot d'une ligne et d'une colonne et recommencer.

À la main sur un exemple (HNF)

$$\mathsf{A} = \begin{pmatrix} -2 & 3 & 3 & 1 \\ 2 & -1 & 1 & -3 \\ -4 & 0 & -1 & -4 \end{pmatrix} \in \mathbb{Z}^{3\times 4}.$$

À la main sur un exemple (HNF)

On commence par ramener 1 en position de pivot par $C_3 \leftrightarrow C_4$, puis $C_4 \leftarrow -C_4$.

$$\begin{pmatrix} -2 & 3 & 3 & 1 \\ 2 & -1 & 1 & -3 \\ -4 & 0 & -1 & \mathbf{-4} \end{pmatrix} \rightarrow \begin{pmatrix} -2 & 3 & 1 & -3 \\ 2 & -1 & -3 & -1 \\ -4 & 0 & -4 & \mathbf{1} \end{pmatrix}$$

À la main sur un exemple (HNF)

À présent on nettoye la dernière ligne par $C_1 \leftarrow C_1 + 4C_4$ et $C_3 \leftarrow C_3 + 4C_4$.

$$\begin{pmatrix} -2 & 3 & 1 & -3 \\ 2 & -1 & -3 & -1 \\ -4 & 0 & -4 & \mathbf{1} \end{pmatrix} \to \begin{pmatrix} -14 & 3 & -11 & -3 \\ -2 & -1 & -7 & -1 \\ 0 & 0 & 0 & \mathbf{1} \end{pmatrix}.$$

On constate par ailleurs que le pivot **1** est > 0 (c-à-d réduit multiplicativement dans $\mathbb{Z}/\{\pm 1\}$ comme souhaité).

À la main sur un exemple (HNF)

Puis $C_2 \leftrightarrow C_3$ et $C_3 \leftarrow -C_3$.

$$\begin{pmatrix} -14 & 3 & -11 & -3 \\ -2 & -1 & \mathbf{-7} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} -14 & -11 & -3 & -3 \\ -2 & -7 & \mathbf{1} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

On réduit le début de la ligne 2 par $C_1 \leftarrow C_1 + 2C_3$ et $C_2 \leftarrow C_2 + 7C_3$

$$\begin{pmatrix} -14 & -11 & -3 & -3 \\ -2 & -7 & \mathbf{1} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} -20 & -32 & -3 & -3 \\ 0 & 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

On constate par ailleurs que le pivot **1** est > 0 (c-à-d réduit multiplicativement dans $\mathbb{Z}/\{\pm 1\}$ comme souhaité).

À la main sur un exemple (HNF)

On peut maintenant réduire additivement modulo 1 la fin de la ligne 2 par $C_4 \leftarrow C_4 + C_3$

$$\begin{pmatrix} -20 & -32 & -3 & -3 \\ 0 & 0 & \mathbf{1} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} -20 & -32 & -3 & -6 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

Version directe : on calcule une relation de Bezout entre -20 et -32 et on applique une opération de Bezout.
Sinon, à la main on peut préférer réduire successivement un coefficient par rapport à l'autre : on ramène le coefficient le plus petit en position de pivot $C_1 \leftrightarrow C_2$, puis $C_2 \leftarrow -C_2$.

$$\begin{pmatrix} -20 & -32 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} -32 & 20 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

On réduit

$$\begin{pmatrix} -32 & 20 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 8 & 20 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

On ramène le coefficient le plus petit en position de pivot $C_1 \leftrightarrow C_2$

$$\begin{pmatrix} 8 & 20 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 20 & 8 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

On réduit

$$\begin{pmatrix} 20 & 8 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 4 & 8 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

On ramène le coefficient le plus petit en position de pivot $C_1 \leftrightarrow C_2$

$$\begin{pmatrix} 4 & 8 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 8 & 4 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (HNF)

On réduit

$$\begin{pmatrix} 8 & 4 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 0 & 4 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

On constate par ailleurs que le pivot 4 est > 0 (c-à-d réduit multiplicativement dans $\mathbb{Z}/\{\pm 1\}$ comme souhaité).

À la main sur un exemple (HNF)

On réduit dans $\mathbb{Z}/4\mathbb{Z}$ la fin de la ligne par $C_3 \leftarrow C_3 + C_2$ et $C_4 \leftarrow C_4 + 2C_2$. On obtient

$$\begin{pmatrix} 0 & 4 & -3 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 4 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

qui est la forme normale d'Hermite que nous cherchions.

Applications de la forme normale d'Hermite

- Forme réduite unique d'une base d'un sous-module de A^m

  $\rightarrow$ Test d'égalité entre deux modules

  $\rightarrow$ Base d'une somme de deux modules

  $\rightarrow$ Test d'inclusion de deux modules.

- Détermination du noyau d'une matrice ou système linéaire homogène

  Les zéros du systèmes correspondent aux colonnes nulles à gauche de la forme HNF.

Forme normale de Smith

Définition
Une matrice est sous forme normale de Smith si

i. les coefficients non-diagonaux sont nuls
ii. tout coefficient diagonal divise le suivant.

Exemple

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 10 & 0 & 0 & 0 \\ 0 & 0 & 30 & 0 & 0 \\ 0 & 0 & 0 & 120 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Algorithme de mise sous forme normale de Smith

Le pivot p est initialement dans le coin supérieur gauche

1. Amener par une transposition de ligne et colonne un coefficient non nul en position de pivot
2. Annuler tout coefficient à droite ou en dessous du pivot par une opération de Bezout
3. Si le pivot ne divise pas un des coefficients restants, ajouter sa colonne à celle du pivot (transvection) et recommencer les annulations
4. Décaler le pivot d'une ligne et d'une colonne. Recommencer.

À la main sur un exemple (SNF)

Cherchons la forme normale de Smith de la matrice

$$X = \begin{pmatrix} 40 & 70 & 20 \\ 20 & 50 & 60 \end{pmatrix}$$

On appliquons l'algorithme **sans** les relations de Bezout.

À la main sur un exemple (SNF)

Avec $C_2 \leftarrow C_2 - 2C_1$,

$$\begin{pmatrix} \mathbf{40} & 70 & 20 \\ 20 & 50 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 40 & \mathbf{-10} & 20 \\ 20 & 10 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_2 \leftarrow -C_2$,

$$\begin{pmatrix} 40 & -10 & 20 \\ 20 & 10 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 40 & 10 & 20 \\ 20 & -10 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_2 \leftrightarrow C_1$,

$$\begin{pmatrix} 40 & 10 & 20 \\ 20 & -10 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 10 & 40 & 20 \\ -10 & 20 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $L_2 \leftarrow L_2 + L_1$,

$$\begin{pmatrix} \mathbf{10} & 40 & 20 \\ -10 & 20 & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} \mathbf{10} & 40 & 20 \\ 0 & 60 & 80 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_2 \leftarrow C_2 - 4C_1$ et $C_3 \leftarrow C_3 - 2C_1$

$$\begin{pmatrix} 10 & 40 & 20 \\ 0 & 60 & 80 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & 60 & 80 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & -7 & -4 \\ -1 & 4 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_3 \leftarrow C_3 - C_2$

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & \mathbf{60} & 80 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & -7 & -4 \\ -1 & 4 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & 60 & \mathbf{20} \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & -7 & 3 \\ -1 & 4 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_3 \leftrightarrow C_2$

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & 60 & \mathbf{20} \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & -7 & 3 \\ -1 & 4 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

devient

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & \mathbf{20} & 60 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \begin{pmatrix} 2 & 3 & -7 \\ -1 & -2 & 4 \\ 0 & 1 & 0 \end{pmatrix}$$

À la main sur un exemple (SNF)

Avec $C_3 \leftarrow C_3 - 3C_2$

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & \mathbf{20} & 60 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 3 & -7 \\ -1 & -2 & 4 \\ 0 & 1 & 0 \end{pmatrix}$$

devient

$$\begin{pmatrix} 10 & 0 & 0 \\ 0 & \mathbf{20} & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 3 & -16 \\ -1 & -2 & 10 \\ 0 & 1 & -3 \end{pmatrix}$$

À la main sur un exemple (SNF)

La matrice

$$\mathsf{X} = \begin{pmatrix} 40 & 70 & 20 \\ 20 & 50 & 60 \end{pmatrix} \in \mathbb{Z}^{2\times 3}$$

a pour forme normale de Smith

$$\mathsf{D} = \begin{pmatrix} 10 & 0 & 0 \\ 0 & 20 & 0 \end{pmatrix}$$

car D est diagonale, positive et 10 divise 20.

En posant

$$\mathsf{L} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \mathsf{C} = \begin{pmatrix} 2 & 3 & -16 \\ -1 & -2 & 10 \\ 0 & 1 & -3 \end{pmatrix},$$

on a

$$\mathsf{L}\,\mathsf{X}\,\mathsf{C} = \mathsf{D}.$$

Applications de la forme normale de Smith

- Solution d'un système linéaire non-homogène

  Le système est diagonalisé.
- Base adaptée à A^n et $\operatorname{im} M$.
- Structure d'un quotient $A^n / \operatorname{im} M$.

  Le quotient se calcule composante par composante dans la base adaptée.

Système linéaire non-homogène dans A

Exemple

Le système $\mathbf{X}\mathbf{z} = \mathbf{b}$ avec $\mathbf{X} = \begin{pmatrix} 40 & 70 & 20 \\ 20 & 50 & 60 \end{pmatrix}$ et $\mathbf{b} = \begin{pmatrix} -60 \\ 40 \end{pmatrix}$

équivaut à $\mathbf{D}\mathbf{z}' = \mathbf{b}$ avec $\mathbf{z} = \mathbf{C}\mathbf{z}'$ et $\mathbf{b}' = \mathbf{L}\mathbf{b}$ soit simplement

$$\begin{cases} 10z_1' & = & -60 & \Leftrightarrow & z_1' & = & -6 \\ 20z_2' & = & -20 & \Leftrightarrow & z_2' & = & -1 \\ & & & & z_3' & \in & \mathbb{Z} \end{cases}.$$

Les solutions sont

$$z_1' \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix} + z_2' \begin{pmatrix} 3 \\ -2 \\ 1 \end{pmatrix} + z_3' \begin{pmatrix} -16 \\ 10 \\ -3 \end{pmatrix} = \begin{pmatrix} -15 \\ 8 \\ -1 \end{pmatrix} + t \begin{pmatrix} -16 \\ 10 \\ -3 \end{pmatrix}, \; t \in \mathbb{Z}.$$