- Q : M inversible de $M_n(\mathbb{Z})$ signifie $\exists N \in M_n(\mathbb{Z}),\ NM = MN = I_n$

1 Ex 1 a) $h([2,6]) = h([2,-4]) = h([2,-2]) = h([0,-2]) = h([-2]) = 2$

1 h : {liste de nombres} $\longrightarrow$ {nombres} de sorte que abs($\ell[i]$) est bien défini

1 D_h : on a besoin de b. [illegible]

1+1 justif b) • Ad hoc : $\ell < \ell'$ si ℓ est extraite de ℓ' en enlevant les 0 ou si $len(\ell) = len(\ell') \geq 2$ et $\ell = [\,|\ell'_0| - |\ell'_1|, \ell'_1, \dots]$ ou $[\ell'_0, |\ell'_0| - |\ell'_1|, \ell'_2 \dots]$ suivant $|\ell'_0| \geq |\ell'_1|$.
Mais reste alors à montrer que $<$ est bien fondé
On utilise pour cela $\ell \mapsto len(\ell) + \sum |\ell_i|$

• $\ell < \ell'$ si $len(\ell) < len(\ell')$ ou si ~~[illegible]~~ $len(\ell) = len(\ell')$ et $\sum_i |\ell[i]| < \sum_i |\ell'[i]|$

alors $h(\ell)$ est une fonction explicite de ℓ et de $(h(\ell'))_{\ell' < \ell}$ donc h est récursive relativt à $<$

$<$ est bien fondée s'il n'y a pas de suite décroissante infinie. C'est le cas sur les listes de nbres entiers : ~~[illegible]~~

$\{\text{listes d'entiers}\} \longrightarrow \mathbb{N}\times\mathbb{N},\ \ell \mapsto \left(len(\ell), \sum_i |\ell[i]|\right)$ est strictt décroissante pour l'ordre lexicographique sur $\mathbb{N}\times\mathbb{N}$

• Alternative $\ell < \ell'$ si $len(\ell) + \sum |\ell[i]| < len(\ell') + \sum |\ell[i]|$ bien fondé sur les listes de nbres entiers

et h est récursive relativt à $<$

((Rq $h(\ell)$ termine si ℓ est à valeurs ds $\mathbb{Q}$: relation bien fondée : $\ell < \ell'$ si $\forall n \in \mathbb{N}^*$, $n\ell'$ à valeurs ds $\mathbb{Z} \Rightarrow n\ell$ à valeurs ds $\mathbb{Z}$

et si $len(\ell) + \sum |\ell[i]| < len(\ell') + \sum |\ell[i]|$

$\ell([1, \sqrt{2}])$ ne termine pas : $\mathbb{Z}\{1, \sqrt{2}\} \subset \mathbb{R}$ n'est pas isomorphe à $\mathbb{Z}$

c) On observe pgcd(ℓ) est inchangé ds les appels récursifs à h

1 $h(\ell) = pgcd(\ell)$ si $len(\ell) \leq 1$

1 just. les élts minimaux de l'ordre ad hoc sont les ℓ de longueur ≤ 1 Donc par récurrence relativt à l'ordre ad hoc $h(\ell) = pgcd(\ell)$

Ex2 a) $A = \begin{pmatrix} 2 & 5 & 9 \\ 5 & 11 & 21 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$ via $c_2 - 2c_1 \to c_2$, $c_1 - 2c_2 \to c_1$, $c_3 - 9c_2 \to c_3$

2

$L_2 - L_1 \to L_2$

$c_1 \leftrightarrow c_2$ $\quad c_3 - 4c_2 \to c_3$ par ex.

cf locale - L3 algèbre effective - script forme smith

b) $P = \text{transf}(I_2, \text{op. lignes})$, $Q = \text{transf.}(I_3, \text{op. col})$ alors $PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$

$\text{Im}(PAQ) = \langle (1,0), (0,3) \rangle \subset \mathbb{Z}^2$

$=$

2 $\quad P\,\text{Im}\,A$ donc $\text{Im}\,A = \langle P^{-1}(1,0), P^{-1}(0,3) \rangle = \langle$ 1ère col de P^{-1}, $3\times$ 2ème col. de $P^{-1} \rangle$

$P^{-1} = \text{transf}(I_2, \text{op} \underbrace{\text{inv}(\text{op. lignes})}_{L_2 + L_1 \to L_2}) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

concl. $(1,1), (0,3)$ base de $\text{Im}\,A$

concrètement $\begin{pmatrix} 1 \\ 1 \end{pmatrix} = P^{-1} PAQ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = AQ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = A$ (1ère col. Q)

$\begin{pmatrix} 0 \\ 3 \end{pmatrix} = AQ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = A$ (2ème col. Q)

ici c'est moins long de calculer P^{-1} que de calculer Q

c) eq de $\text{Im}(PAQ)$: $y = 0 \cancel{[3]}$ mod 3

$\begin{pmatrix} x \\ y \end{pmatrix} \in \text{Im}\,A \iff \cancel{P\begin{pmatrix} x \\ y \end{pmatrix} \in \text{Im}} \quad \underbrace{(0,1)\,P}_{} \begin{pmatrix} x \\ y \end{pmatrix} = 0$ mod 3

2 $\quad \underbrace{P[1,:]}_{(-1\ 1)} \begin{pmatrix} x \\ y \end{pmatrix}$ $\quad$ or $P = \text{transf.}(I_2, \text{op lignes}) = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$

Eq. de $\text{Im}\,A$: $x - y = 0$ mod 3

Ex3 $\quad P = X^3 + X^2 + X + 1 \in \mathbb{F}_3[X]$

1 $\quad$ a) $(1, X, X^2)$ base de $\mathbb{F}_3[X]/_P$

$\varphi : y \mapsto y^3 \quad \varphi(1) = 1$; $\varphi(X) = X^3 \overset{\text{mod } P}{=} -X^2 - X - 1$, $\varphi(X^2) = X^6$ mod P $= X^2$

division euclidienne de X^6 par P :

$$\begin{array}{l|l} X^6 & P \\ X^6 + X^5 + X^4 + X^3 & X^3 - X^2 \\ \hline -X^5 - X^4 - X^3 & \\ -X^5 - X^4 - X^3 - X^2 & \\ \hline X^2 & \end{array}$$

2 $\quad \text{Mat}\,\varphi = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$

b) $\text{Mat}(\varphi - \text{id}) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -2 & 0 \\ 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}$ de rang 1 $\quad \text{Ker}(\varphi - \text{id}) = \langle (1,0,0), (0,0,1) \rangle$

si P était irréductible, $\text{Ker}(\varphi - \text{id})$ serait de dim 1 donc P n'est pas irréd.

c) racines de P : 0 ou 1 ou $2 = -1$ $\quad P(0) = 1 \neq 0$, $P(1) = 4 = 1 \neq 0$, $P(-1) = -1 + 1 - 1 + 1 = 0$ $\leadsto$ $P(X) = (X+1)(X^2+1)$

(Ex3 c) X^2+1 est irréductible car sinon il aurait un facteur de degré 1 donc une racine.

Le lemme chinois donne un isomorphisme d'anneaux $\mathbb{F}_3[X]/_P \to \mathbb{F}_3[X]/_{X+1} \times \mathbb{F}_3[X]/_{X^2+1}$

$$R \bmod P \mapsto (R \bmod X+1,\ R \bmod X^2+1)$$

$\mathbb{F}_3[X]/_{X+1} \simeq \mathbb{F}_3$, $\mathbb{F}_3[X]/_{X^2+1}$ est un corps $\simeq \mathbb{F}_9$

On cherche l'expression de l'iso réciproque

relation de Bezout $\quad X^2+1 = X(X+1) - X+1 = X(X+1) - (X+1) + 2 = (X+1)(X-1) + \underbrace{2}_{-1}$

$$-(X^2+1) + (X-1)(X+1) = 1$$

$$-(X^2+1)R + (X-1)(X+1)R = R$$

$$R \bmod X+1 = -(X^2+1)R \bmod X+1$$

$$R \bmod X^2+1 = (X^2-1)R \bmod X^2+1$$

$$R \bmod P = -(X^2+1)R_1 + (X^2-1)R \bmod R$$

Expression $(A,B) \mapsto -(X^2+1)A + (X^2-1)B \bmod P$

via l'iso

$$\mathrm{Ker}(\varphi - id) \simeq \underbrace{\mathrm{Ker}\left(x \mapsto x^3 - x : \mathbb{F}_3[X]/_{X+1} \circlearrowleft\right)}_{= \mathbb{F}_3[X]/_{X+1} = \mathbb{F}_3[X]/_{X+1}} \times \underbrace{\mathrm{Ker}\left(x \mapsto x^3 - x : \mathbb{F}_3[X]/_{X^2+1} \circlearrowleft\right)}_{= \mathbb{F}_3} = \mathbb{F}_3 \langle (1,0), (0,1) \rangle$$

d'où la $\mathbb{F}_3$-base de $\mathrm{Ker}(\varphi - id)$: $\left(-(X^2+1),\ (X^2-1)\right) \in \mathbb{F}_3[X]/_{(P)}{}^2$