2) Soit $M = A/I$ où $I \subseteq A$ est un idéal non nul. On considère M comme A-module. M est de type fini comme A-module car

$$\langle \bar{1} \rangle = A/_I$$

En effet, $\bar{a} = \overline{a \cdot 1} = a \cdot \bar{1}$ pour tout $a \in A$.
Si A est intègre, M possède un rang et

$$\text{rang}(M) = \dim_K(M_K)$$

où $K = \text{Frac}(A)$. Or,

$$M_K = \{0\}$$

En effet, un élément de M_K s'écrit sous la forme $\frac{m}{s}$ où $m \in M$ et $s \in A^* = A \setminus \{0\}$.
Comme $M = A/_I$, $m = \bar{a}$ avec $a \in A$.
Comme $I \neq \{0\}$, il existe $t \in I \setminus \{0\}$.
On alors

$$\frac{m}{s} = \frac{(\bar{a})}{s} = \frac{t \cdot \bar{a}}{t \cdot s} = \frac{(\overline{ta})}{ts} = \frac{(\bar{0})}{ts} = 0$$

car $ta \in I$. Du coup, $M_K = \{0\}$
Par conséquent,

$$\text{rang}\, M = \dim_K \{0\} = 0$$

3) Si M et N sont des A-modules de type fini, alors la somme directe (externe) $M \oplus N = M \times N$ est encore de type fini et

$$(M \oplus N)_K \cong M_K \oplus N_K \quad \text{(iso de } K\text{-esp vect)}$$

où $K = \text{Frac}(A)$, A intègre. (exo)
En particulier,

$$\text{rang}(M \oplus N) = \text{rang}(M) + \text{rang}(N)$$

4) Soient $d_1, \dots, d_\ell \in A^*$, A intègre.
Alors le A-module

$$A^r \oplus A/_{(d_1)} \oplus \dots \oplus A/_{(d_\ell)}$$

est de type fini et son rang est égal à r.

Théorème de la base adaptée.

Soit A un anneau principal et $M \subseteq A^n$ un sous-A-module. Alors, il existe une base $v_1, \dots, v_n$ de A^n dans laquelle M est diagonal i.e,

$$M = (d_1 v_1, d_2 v_2, \dots, d_n v_n)$$

où $d_1, \dots, d_n \in A$, $d_i \mid d_{i+1}$ $i = 1, \dots, n-1$

De plus, les éléments $d_1, \dots, d_n$ sont uniquement déterminés par M à inversibles près, i.e., si

$$M = (d_1' v_1', d_2' v_2', \dots, d_n' v_n')$$

où $d_1', \dots, d_n' \in A$ avec $d_i' \mid d_{i+1}'$ $i = 1, \dots, n-1$, alors

$$d_i' = u_i d_i \quad \text{où} \quad u_i \in A^\times$$

De manière équivalente, les idéaux $(d_1), (d_2), \dots, (d_n)$ sont uniquement déterminés par M.

On démontrera cet énoncé dans le cas particulier où A est un anneau euclidien. Rappelons qu'un anneau euclidien est un anneau intègre muni d'un stathme euclidien

$$w : A^* = A \setminus \{0\} \longrightarrow \mathbb{N}$$

avec
1) $\forall a, b \in A^* : w(ab) \geq w(a)$
2) $\forall a, b \in A^* : \exists q, r \in A$ tq.

$$a = qb + r \quad \text{et} \quad r = 0 \text{ ou } r \neq 0 \text{ et } w(r) < w(b)$$

Tout anneau euclidien est principal. (ex.)

Exemples : $(\mathbb{Z}, |\cdot|)$, $(K[x], \deg)$, $(\mathbb{Z}[i], |\cdot|^2)$ sont euclidiens

$$\mathbb{Z}\left[\tfrac{1}{2} + \tfrac{1}{2} i\sqrt{19}\right] = \left\{ a + b\left(\tfrac{1}{2} + \tfrac{1}{2} i\sqrt{19}\right) \,\middle|\, a, b \in \mathbb{Z} \right\}$$

est principal non euclidien.

La démonstration du Théorème de la base adaptée repose sur l'algorithme de Smith généralisé à des matrices à coeff^s dans un ann. eucl

Def. Soit A un anneau. On définit la matrice de transvection

$$e_{ij}^{(n)}(q) \in M_{n\times n}(A)$$

par

$$e_{ij}^{(n)}(q)_{k,l} = \begin{cases} 1 & \text{si } k=l \\ q & \text{si } k=i,\ l=j \\ 0 & \text{sinon} \end{cases}$$

où $q \in A$.

L'algorithme de Smith pour un anneau euclidien A :

Soit $a \in M_{n\times m}(A)$

Alors il existe $u \in GL_n(A)$, $v \in GL_m(A)$ produits de matrice de transvection, tels que

$$uav = \mathrm{diag}_{n\times m}(d_1, \dots, d_l)$$

où $d_i \in A^*$ et $d_i \mid d_{i+1}$ dans A

l'entier l est égal au rang de la matrice a vue comme matrice à coeff.s dans $K = \mathrm{Frac}(A)$. En particulier, l est uniquement déterminé par a.

De plus, les éléments $d_1, \dots, d_l$ de A sont uniquement déterminés par a à inversibles près. En fait,

$$(d_1) = (a_{ij})$$

$$(d_1 d_2) = (\text{mineurs } 2\times 2 \text{ de } a)$$

$$\vdots$$

$$(d_1 d_2 \cdots d_l) = (\text{mineurs } l\times l \text{ de } a)$$

On appelle $d_1, \dots, d_l$ les <u>facteurs invariants</u> de la matrice a.

<u>Exemple</u> $A = \mathbb{Q}[X]$

Soit $a = \begin{pmatrix} X-1 & X \\ X^2 & X^2+X \end{pmatrix} \in M_{2\times 2}(\mathbb{Q}[X])$

Déterminer le rang de a et ~~les~~ ses facteurs invariants.

Dérouler l'algorithme de Smith sur a :

$$\begin{pmatrix} X-1 & X \\ X^2 & X^2+X \end{pmatrix}$$

Division euclidienne de X par $X-1$:

$$X = 1 \cdot (X-1) + 1$$

Soustraire 1 fois colonne 1 de colonne 2 :

$$\begin{pmatrix} X-1 & 1 \\ X^2 & X \end{pmatrix}$$

$X-1 = (X-1) \times 1$ Soustraire $(X-1)$ fois colonne 2 de colonne 1 :

$$\begin{pmatrix} 0 & 1 \\ X & X \end{pmatrix} \underset{C_1' = C_1 + C_2}{\rightsquigarrow} \begin{pmatrix} 1 & 1 \\ 2X & X \end{pmatrix} \underset{C_2' = C_2 - C_1}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 2X & -X \end{pmatrix}$$

$$\underset{L_2' = L_2 - 2XL_1}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 0 & -X \end{pmatrix}$$

Comme $1 \mid -X$, on a terminé et les facteurs invariants de a sont 1, $-X$ et le rang de a est égal à 2.

<u>Démo du Th de la base adaptée</u>

$N \subseteq A^n$ sous-A-module, A euclidien. Comme A est euclidien, il est principal et donc noethérien. Comme A^n est de type fini comme A-module N est de type fini. Soient $a_1, \ldots, a_m$ une famille génératrice de N où $m \in \mathbb{N}$. Soit a la matrice $n \times m$ de colonnes $a_1, \ldots, a_m$, i.e. $a \in M_{n \times m}(A)$

D'après l'algorithme de Smith, il existe $u \in Gl_n(A)$, $v \in Gl_m(A)$ telles que

$$uav = \operatorname{diag}_{n \times m}(d_1, \ldots, d_l)$$

où $d_i \in A^*$ et $d_i \mid d_{i+1}$ $i = 1, \ldots, l-1$

Comme $v \in Gl_m(A)$, les colonnes de av engendrent N. Les colonnes de la matrice u^{-1} constituent une base de A^n : $v_1, \ldots, v_n$ dans laquelle M est diagonal :

$$M = (d_1 v_1, d_2 v_2, \ldots, d_\ell v_\ell, 0 v_{\ell+1}, \ldots, 0 v_n)$$

On admettra l'unicité. ☐

<u>Ex.</u> $A = \mathbb{Q}[X]$.

Soit $N \subseteq A^2$ le sous-module engendré par

$$\begin{pmatrix} X-1 \\ X^2 \end{pmatrix}, \begin{pmatrix} X \\ X^2+X \end{pmatrix}$$

Déterminer une base adaptée de A^2.

$a = \begin{pmatrix} X-1 & X \\ X^2 & X^2+X \end{pmatrix}$ est la matrice de l'exemple précédent. On peut vérifier que

$$u = \begin{pmatrix} 1 & 0 \\ -2X & 1 \end{pmatrix} \qquad v = \begin{pmatrix} X-1 & -X \\ -X+2 & X-1 \end{pmatrix}$$

Or $av = \begin{pmatrix} 1 & 0 \\ 2X & -X \end{pmatrix}$

Comme $v \in GL_2(\mathbb{Q}[X])$,

$$\begin{pmatrix} 1 \\ 2X \end{pmatrix}, \begin{pmatrix} 0 \\ -X \end{pmatrix}$$

constitue une famille génératrice de N

$u^{-1} = \begin{pmatrix} 1 & 0 \\ 2X & 1 \end{pmatrix}$

Soient $v_1 = \begin{pmatrix} 1 \\ 2X \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Alors v_1, v_2 est une base de $\mathbb{Q}[X]^2$ et

$$1 \cdot v_1 , \ -X \cdot v_2$$

est une famille génératrice de N.
C'est en fait une base de N.

<u>Remarque.</u> Si $N \subseteq A^n$, A principal, $N = (d_1 v_1, \ldots, d_n v_n)$ comme ci-dessus.
Si $d_1, \ldots, d_\ell \neq 0$ et $d_{\ell+1} = \cdots = d_n = 0$,

alors $d_1 v_1, \dots, d_\ell v_\ell$ est une base de M. Par conséquent :

<u>Corollaire</u>. Soit A un anneau principal. Soit $M \subseteq A^n$ un sous-A-module. Alors M est libre de rang $\leq n$.

<u>Théorème</u> (Classification des modules de type fini sur un anneau principal.)
Soit A un anneau principal et M un A-module de type fini. Alors, il existe $r \in \mathbb{N}$ et $d_1, \dots, d_\ell \in A$, $d_i \notin A^\times$ et $d_i \neq 0$ tels que

$$M \cong A^r \oplus A/(d_1) \oplus A/(d_2) \oplus \dots \oplus A/(d_\ell)$$

(isomorphisme comme A-modules.) où

$$d_1 | d_2,\ d_2 | d_3, \dots, d_{\ell-1} | d_\ell \text{ dans } A$$

De plus, r et $d_1, \dots, d_\ell$ sont uniquement déterminés par M (à inversibles près pour les d_i)

<u>Déf.</u> r est le <u>rang</u> de M (comme vu précédemment) et $d_1, \dots, d_\ell$ sont les <u>facteurs invariants</u> de M

<u>Démo</u> (du Th de classification) :
Comme M est de type fini, il existe un morphisme de A-modules surjectif

$$f : A^n \longrightarrow M$$

$\ker(f)$ est un sous-A-module de A^n.
Soit $v_1, \dots, v_n$ une base de A^n adaptée au sous-module $\ker(f)$ de A^n :

$$\ker(f) = (c_1 v_1, \dots, c_k v_k, d_1 v_{k+1}, \dots, d_\ell v_{k+\ell})$$

où $c_1, \dots, c_k \in A^\times$ et $d_1, \dots, d_\ell \notin A^\times$, $d_i \neq 0$
$d_i | d_{i+1}$ pour $i = 1, \dots, \ell-1$
Du coup

$$M \cong A^n/\ker(f) \cong A^n/(c_1 e_1, \dots, c_k e_k, d_1 e_{k+1}, \dots, d_\ell e_{k+\ell})$$
$$\cong A/(c_1) \oplus \dots \oplus A/(c_k) \oplus A/(d_1) \oplus \dots \oplus A/d_\ell \oplus A^{n-k-\ell}$$

$$\cong A/_{(d_1)} \oplus \dots \oplus A/_{(d_l)} \oplus A^{n-k-l}$$

On pose $r = n-k-l$

On admettra l'unicité de $d_1, \dots, d_l$ $\boxtimes$