On a vu qu'un quotient d'un groupe abélien de type fini est de type fini.
Aujourd'hui on verra qu'un sous-groupe d'un groupe abélien de type fini est de type fini.

<u>Proposition</u>. Soit $n \in \mathbb{N}$ et $G \leq \mathbb{Z}^n$ sous-groupe. Alors il existe $g_1, \dots, g_m \in G$ tels que

$$G = \langle g_1, \dots, g_m \rangle$$

où $m \in \mathbb{N}$ avec $m \leq n$. En particulier, tout sous-groupe de $\mathbb{Z}^n$ est de type fini.

<u>Démo</u> : Par récurrence sur n.
Si $n = 0$, $\mathbb{Z}^n = \mathbb{Z}^0 = \{0\}$ et $G = \{0\}$
or $\{0\} = \langle \emptyset \rangle$ i.e. $m = 0$
Supposons que l'énoncé est vrai au rang n. On le démontre au rang $n+1$. Soit $G \leq \mathbb{Z}^{n+1}$ un sous-groupe. Soit

$$p : \mathbb{Z}^{n+1} \to \mathbb{Z}^n$$

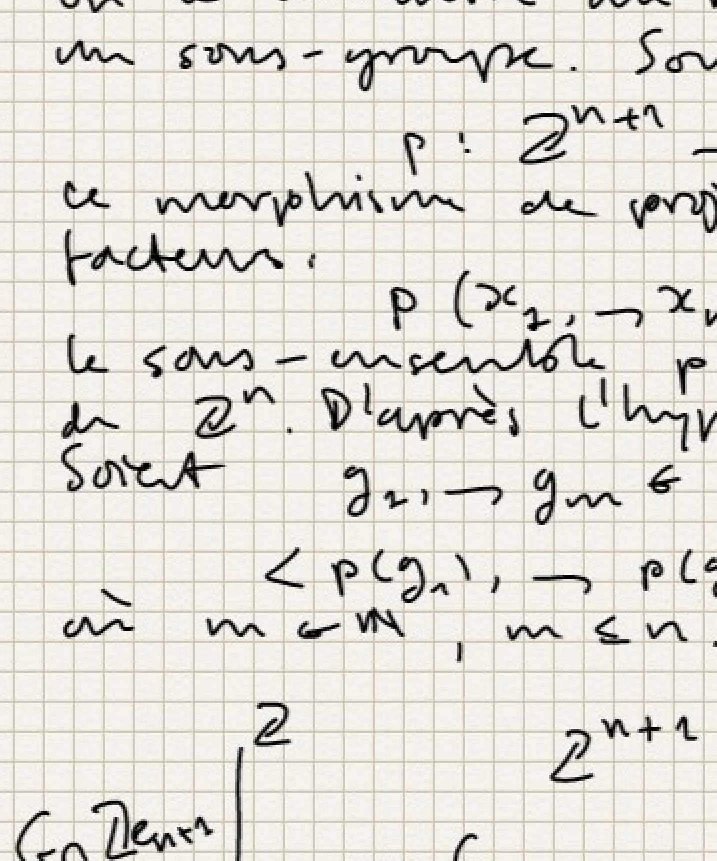
le morphisme de projection sur les n premiers facteurs.

$$p(x_1, \dots, x_{n+1}) = (x_1, \dots, x_n)$$

Le sous-ensemble $p(G)$ est un sous-groupe de $\mathbb{Z}^n$. D'après l'hypothèse récurrence.
Soient $g_1, \dots, g_m \in G$ tels que

$$\langle p(g_1), \dots, p(g_m) \rangle = p(G)$$

où $m \in \mathbb{N}$, $m \leq n$.



Considérons le sous-groupe $G \cap \mathbb{Z}e_{n+1}$ de $\mathbb{Z}e_{n+1} \cong \mathbb{Z}$.
Or, tout sous-groupe de $\mathbb{Z}$ est monogène.
Donc il existe

$$g_{m+1} \in G \cap \mathbb{Z}e_{n+1}$$

tq

$$\langle g_{m+1} \rangle = G \cap \mathbb{Z}e_{n+1}$$

Mq $\langle g_1, \dots, g_{m+1} \rangle = G$

$\leq$ Par construction $g_1, \dots, g_{m+1} \in G$
D'où $\langle g_1, \dots, g_{m+1} \rangle \leq G$

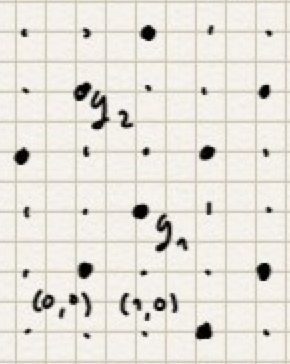
$\supseteq$: Soit $x \in G$. Comme
$$p(x) \in p(G) = \langle p(g_1), \dots, p(g_m) \rangle,$$
il existe $a_1, \dots, a_m \in \mathbb{Z}$ tels que
$$p(x) = a_1 p(g_1) + \dots + a_m p(g_m)$$
Du coup,
$$p(x - a_1 g_1 - \dots - a_m g_m) =$$
$$= p(x) - a_1 p(g_1) - \dots - a_m p(g_m) = 0$$
i.e.
$$x - a_1 g_1 - \dots - a_m g_m \in \mathbb{Z} e_{n+1} \cap G$$
$$= \langle g_{m+1} \rangle$$
D'où il existe $a_{m+1} \in \mathbb{Z}$ tq
$$x - a_1 g_1 - \dots - a_m g_m = a_{m+1} g_{m+1}$$
Donc
$$x = a_1 g_1 + a_2 g_2 + \dots + a_m g_m + a_{m+1} g_{m+1}$$
Par conséquent
$$x \in \langle g_1, \dots, g_{m+1} \rangle.$$
Cela montre bien que
$$G = \langle g_1, \dots, g_{m+1} \rangle$$ $\square$

Remarque. La démonstration est constructive. i.e. elle permet de construire effectivement une famille génératrice d'un sous-groupe de $\mathbb{Z}^n$

Exemple Soit
$$G = \{ (x,y) \in \mathbb{Z}^2 \mid 2x + y \equiv 0 \mod 3 \}$$
G est un sous-groupe de $\mathbb{Z}^2$ car G est le noyau du morphisme de groupes composé :
$$\begin{array}{ccccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/3 \\ (x,y) & \longmapsto & 2x+y & & \\ & & z & \longmapsto & \bar{z} \mod 3 \end{array}$$
Soit $p : \mathbb{Z}^2 \to \mathbb{Z}$ la projection $p(x,y) = x$.
$$p(G) = \{ x \in \mathbb{Z} \mid \exists y \in \mathbb{Z} \text{ avec } 2x + y \equiv 0 \mod 3 \}$$
$$= \mathbb{Z} = \langle 1 \rangle$$
On prend donc $g_1 = (1,1) \in G$
On a bien $\langle p(g_1) \rangle = \langle 1 \rangle = p(G)$
Puis
$$G \cap \mathbb{Z} e_2 = \{ (x,y) \in \mathbb{Z}^2 \mid 2x + y \equiv 0 \ (3) \text{ et } x = 0 \} = \langle 3 e_2 \rangle$$

On pose donc $g_2 = 3e_2$
D'après la démo de la proposition

$$\langle g_1, g_2 \rangle = G \qquad g_1 = (1,1), \quad g_2 = (0,3)$$



$\mathbb{Z}^2 = \{\cdot\}$
$G = \{\bullet\}$

<u>Corollaire</u>. Tout sous-groupe d'un groupe abélien de type fini est de type fini.
<u>Démo</u>. Soit G un groupe abélien de type fini et $H \subseteq G$ un sous-groupe. D'après ce qu'on a vu la semaine dernière, il existe un morphisme surjectif

$$f : \mathbb{Z}^n \to G$$

pour un certain entier naturel n.
On cons., $f^{-1}(H) \subseteq \mathbb{Z}^n$ sous-groupe.
D'après la proposition précédente, il existe $h_1, \dots, h_m \in f^{-1}(H)$ tq

$$\langle h_1, \dots, h_m \rangle = f^{-1}(H).$$

Prendre l'image par f:

$$\langle f(h_1), \dots, f(h_m) \rangle = f(f^{-1}H) \underset{\substack{\uparrow \\ \text{car } f \\ \text{surjectif}}}{=} H$$

□

<u>Déf</u>. Soit $f : G \to G'$ un morphisme de groupes abéliens. Le <u>conoyau</u> de f est le groupe quotient $G'/\mathrm{im}(f)$.
<u>Corollaire</u>: Tout groupe abélien de type fini est isomorphe au conoyau d'un morphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$, pour certains $m, n \in \mathbb{N}$.
<u>Démo</u>: Soit G un groupe abélien de type fini. D'après ce qu'on a vu, il existe un morphisme surjectif

$$f : \mathbb{Z}^n \to G$$

D'après la proposition précédente, $\ker(f)$ est de type fini. Il existe donc un

morphisme surjectif
$$g : \mathbb{Z}^m \longrightarrow \ker(f) \subseteq \mathbb{Z}^n$$
On a donc,
$$\operatorname{coker}(g) = \mathbb{Z}^n/_{\operatorname{im}(g)} = \mathbb{Z}^n/_{\ker(f)} \cong \operatorname{im}(f)$$
$$= G$$
☑

On va donc étudier les morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$ afin de démontrer le théorème de classification des groupes abéliens de type fini.

Rappelons que si G et G' sont des groupes abéliens, l'ensemble
$$\operatorname{Hom}(G, G') = \{ f : G \to G' \mid f \text{ morphisme} \}$$
est un groupe abélien sous la lci
$$(f+g)(x) = f(x) + g(x) \qquad (x \in G)$$
En particulier,
$$\operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$$
est un groupe abélien.
Soit $M_{n\times m}(\mathbb{Z})$ l'ensemble des matrices $n\times m$ à coefficients dans $\mathbb{Z}$. $M_{n\times m}(\mathbb{Z})$ est un groupe abélien sous l'addition matricielle.
Soit
$$\Phi : M_{n\times m}(\mathbb{Z}) \longrightarrow \operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$$
définie par
$$(\Phi(a))(x) = ax \qquad (a \in M_{n\times m}(\mathbb{Z}),\ x \in \mathbb{Z}^m)$$
où ax est le produit matriciel.
$\Phi(a)$ est bien un morphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$, i.e, $\Phi(a) \in \operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$
De plus, $\Phi(a+b) = \Phi(a) + \Phi(b)$
i.e, Φ est un morphisme de groupes.
Observons que $\ker \Phi = \{0\}$. Montrons que $\operatorname{im}(\Phi) = \operatorname{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$. Soit $f : \mathbb{Z}^m \to \mathbb{Z}^n$ un morphisme. Soit $a_{ij} \in \mathbb{Z}$ définis par
$$f(e_j) = \sum_{i=1}^{n} a_{ij}\, e_i$$
Soit $a = (a_{ij})_{\substack{i=1,\dots,n \\ j=1,\dots,m}} \in M_{n\times m}(\mathbb{Z})$
On a bien $\Phi(a) = f$.

Par conséquent Φ est un isomorphisme de $M_{n\times m}(\mathbb{Z})$ sur $\mathrm{Hom}(\mathbb{Z}^m, \mathbb{Z}^n)$

De manière générale, on peut définir la matrice d'un morphisme de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$ dans des bases quelconques, pas forcément standard.

Déf. Soit $x_1, \dots, x_m$ une famille d'éléments de $\mathbb{Z}^n$.

1) $x_1 \dots x_m$ est libre si
$a_1 x_1 + \dots + a_m x_m = 0 \Rightarrow a_1 = \dots = a_m = 0$
quels que soient $a_1, \dots, a_m \in \mathbb{Z}$

2) $x_1 \dots x_m$ est génératrice de $\mathbb{Z}^n$
quel que soit $x \in \mathbb{Z}^n$, il existe
$a_1, \dots, a_m \in \mathbb{Z}$ tq $x = a_1 x_1 + \dots + a_m x_m$
Autrement dit, si $\langle x_1, \dots, x_m \rangle = \mathbb{Z}^n$.

3) $x_1 \dots x_m$ est une base de $\mathbb{Z}^n$
si $x_1, \dots, x_m$ est libre et génératrice de $\mathbb{Z}^n$.

Attention les théorèmes de l'algèbre linéaire ne sont pas forcément valables dans ce cadre. Par exemple, le théorème de la base extraite n'est pas valable pour $\mathbb{Z}^n$: la famille $2, 3$ dans $\mathbb{Z}$ est génératrice : tout élément n de $\mathbb{Z}$ s'écrit $n = (-n)\times 2 + n \times 3$
Pourtant on ne peut en extraire une base de $\mathbb{Z}$: ni 2 ni 3 n'est génératrice de $\mathbb{Z}$. De même le Théorème de la base incomplète n'est pas valable pour les familles d'éléments de $\mathbb{Z}^n$ (exemple : la famille 2 dans $\mathbb{Z}$)

La matrice a définie ci-dessus associée à un morphisme $f : \mathbb{Z}^m \to \mathbb{Z}^n$, est la matrice de f dans les bases standard de $\mathbb{Z}^m$ et $\mathbb{Z}^n$ respectivement.

Plus généralement

<u>Déf.</u> Soit $\mathcal{B}$ une base de $\mathbb{Z}^m$ et C une base de $\mathbb{Z}^n$. Écrivons $\mathcal{B} = (x_1, \dots, x_m)$ et $C = (y_1, \dots, y_n)$. Soit $f : \mathbb{Z}^m \to \mathbb{Z}^n$ un morphisme. La <u>matrice</u> de f dans les bases $\mathcal{B}$ et C est la matrice $a = (a_{ij}) \in M_{n\times m}(\mathbb{Z})$ définie par
$$f(x_j) = \sum_{i=1}^{n} a_{ij}\, y_i$$

<u>Prop</u> Avec les mêmes notations, l'application
$$\Psi : \mathrm{Hom}(\mathbb{Z}^m, \mathbb{Z}^n) \longrightarrow M_{n\times m}(\mathbb{Z})$$
qui associe à f sa matrice dans les bases $\mathcal{B}$ et C est un isomorphisme de groupes

<u>Remarque</u> : On l'a vu lorsque $\mathcal{B}$ et C sont les bases standards de $\mathbb{Z}^m$ et $\mathbb{Z}^n$ respectivement, auquel cas $\Psi = \Phi^{-1}$.

On démontrera un énoncé de classification de morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$:

<u>Théorème.</u> Soit $f : \mathbb{Z}^m \to \mathbb{Z}^n$ un morphisme de groupes. Alors, il existe des bases $\mathcal{B}$ et C de $\mathbb{Z}^m$ et $\mathbb{Z}^n$ respectivement, dans lesquelles la matrice de f est
$$\begin{pmatrix} d_1 & 0 & 0 & \cdots & & 0 \\ 0 & d_2 & 0 & & & \vdots \\ 0 & 0 & d_3 & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ \vdots & & & & d_l & \\ \vdots & & & & & 0 \\ & & & & & \ddots \\ 0 & & \cdots & & & 0 \end{pmatrix}$$
où $d_1 \mid d_2,\ d_2 \mid d_3, \dots, d_{l-1} \mid d_l$ et $d_i \in \mathbb{N} \setminus \{0\}$

<u>Remarque</u> On peut comparer cet énoncé avec l'énoncé suivant en algèbre linéaire : Soit K un corps et $f : K^m \to K^n$ une application linéaire. Alors, il existe

des bases $\mathcal{B}$ et $\mathcal{C}$ de K^m et K^n, respectivement, dans lesquelles la matrice de f est la matrice $n \times m$

$$\underbrace{\phantom{\begin{matrix}1 & & \\ & \ddots & \\ & & 1\end{matrix}}}_{\substack{\text{ce qu'on}\\ \text{rajoute}\\ \text{pour obtenir}\\ \text{une base de } K^m}} \underbrace{\phantom{\begin{matrix}0 & & \\ & \ddots & \\ & & 0\end{matrix}}}_{\text{base de ker } f}$$

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & 0 & \\ & & 1 & & & \\ & & & 0 & & \\ & 0 & & & \ddots & \\ & & & & & 0 \end{pmatrix} \begin{array}{l} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} \text{images des éléments rajoutés} \\ \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} \text{qu'on complète en une base de } K^n \end{array}$$

Notons que le nombre de "1" dans cette matrice est égal au rang de l'application linéaire f. En pratique, on obtient les bases $\mathcal{B}$ et $\mathcal{C}$ en faisant des opérations élémentaires sur la matrice de f dans les bases standards :

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \underset{L_2' = L_2 - 3L_1}{\rightsquigarrow} \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix} \underset{L_1 = L_1 + L_2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \underset{L_2' = L_2 / -2}{\rightsquigarrow} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

C'est exactement ce qu'on fera pour démontrer le théorème de classification des morphismes de $\mathbb{Z}^m$ dans $\mathbb{Z}^n$.

<u>Déf.</u> Soient $n \in \mathbb{N}$, $i, j \in \{1, \dots, n\}$.
La <u>matrice standard</u> $e_{ij} \in M_{n \times n}(\mathbb{Z})$ est la matrice dont tous les coefficients sont nuls sauf l'élément (i,j) qui vaut 1.

<u>Ex.</u> $(n = 2)$ $\quad e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $\quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

<u>Déf.</u> Soit $n \in \mathbb{N}$. Une <u>matrice de transvection</u> à coefficients dans $\mathbb{Z}$ est une matrice de la forme

$$I_n + q e_{ij} =: e_{ij}(q)$$

où $q \in \mathbb{Z}$, $i, j \in \{1, \dots, n\}$, $i \neq j$.

Exemples $n=2$

$$e_{1,2}(3) = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \qquad e_{2,1}(-36) = \begin{pmatrix} 1 & 0 \\ -36 & 1 \end{pmatrix}$$

Prop. Soit $a \in M_{n\times m}(\mathbb{Z})$ et $q \in \mathbb{Z}$

1) Soient $i,j \in \{1, \dots, n\}$ $i \neq j$.
la matrice $e_{ij}(q)\,a$ est la matrice obtenue à partir de la matrice a en remplaçant la i-ième ligne de a par la somme de la i-ième ligne de a et q fois la j-ième ligne de a

2) Soient $i,j \in \{1, \dots, m\}$, $i \neq j$
la matrice $a\,e_{ij}(q)$ est obtenue à partir de a en rajoutant q fois la i-ième colonne de a à la j-ième colonne de a.

Corollaire. Les matrice de transvection $e_{ij}(q)$ est inversible en tant que matrice à coefficients dans $\mathbb{Z}$ et

$$e_{ij}(q)^{-1} = e_{ij}(-q).$$