

# Notes de cours de M305-Algèbre 2

25 février 2015

# Table des matières

|          |                                            |          |
|----------|--------------------------------------------|----------|
| <b>1</b> | <b>Classification des groupes abéliens</b> | <b>3</b> |
| 1.1      | Groupes abéliens de type fini . . . . .    | 3        |
| 1.2      | Théorèmes de structure . . . . .           | 7        |
| 1.2.1    | Sous-groupes de $\mathbb{Z}^r$ . . . . .   | 8        |
| 1.2.2    | Anneaux . . . . .                          | 11       |

# Remarques préliminaires

On supposera connu les résultats de théorie des groupes vus au S5. Pour plus d'informations, se référer aux notes de cours de Nicolas Ratazzi.

# Chapitre 1

## Classification des groupes abéliens

Le but de ce chapitre est de donner une classification des groupes abéliens. On va s'intéresser pour cela à une sous-catégorie de groupes abéliens : les groupes abéliens de type fini. Dans toutes ce chapitre la loi des groupes considérés sera  $+$  sauf mention contraire explicite.

### 1.1 Groupes abéliens de type fini

**Remarque 1.1.** Tout groupe abélien  $(G, +, 0_G)$  peut s'identifier à un  $\mathbb{Z}$ -module en posant :

$$\forall (n, g) \in \mathbb{Z} \times G, n \cdot g := \begin{cases} 0_G & \text{si } n = 0 \\ ((n-1) \cdot g) + g & \text{si } n > 0 \\ ((n+1) \cdot g) + (-g) & \text{si } n < 0 \end{cases}$$

On vérifie aisément que  $\cdot$  est bien définie et vérifie :

$$\forall n \in \mathbb{Z}, \forall (h, g) \in G \times G, n \cdot (h + g) = (n \cdot g) + (n \cdot h)$$

**Définition-proposition 1.2.** Soient  $G$  un groupe abélien et  $S$  une partie de  $G$ . Alors il existe un unique sous-groupe  $H$  de  $G$  qui contient  $S$  et qui soit minimal (pour l'inclusion).  $H$  est appelé le *sous-groupe de  $G$  engendré par la partie  $S$* , et noté  $\langle S \rangle$ .

*Démonstration.* On note  $\mathcal{E}$  l'ensemble des sous-groupes de  $G$  contenant  $S$ .  $\mathcal{E}$  est non vide (car  $G \in \mathcal{E}$ ). Alors  $\bigcap_{H \in \mathcal{E}} H$  est un sous-groupe de  $G$  contenant  $S$  qui est contenu dans tout autre élément de  $\mathcal{E}$ . □

**Remarque 1.3.** Soit  $G$  un groupe abélien, soit  $S$  une partie de  $G$ . Alors  $\langle S \rangle$  contient l'élément neutre et est stable par additivité et passage à l'inverse. Comme  $G$  est abélien,  $\langle S \rangle$  contient donc toutes les combinaisons linéaires d'éléments de  $S$ , i.e. :

$$\left\{ \sum_{i=1}^r n_i s_i \mid (s_i)_{1 \leq i \leq r} \in S^r, (n_i)_{1 \leq i \leq r} \in \mathbb{Z}^r, r \in \mathbb{N} \right\} \subset \langle S \rangle$$


On constate qu'un tel ensemble est de plus un sous-groupe de  $G$  et donc, par unicité, on a même :

$$\langle S \rangle = \left\{ \sum_{i=1}^r n_i s_i \mid (s_i)_{1 \leq i \leq r} \in S^r, (n_i)_{1 \leq i \leq r} \in \mathbb{Z}^r, r \in \mathbb{N} \right\}$$

**Définition 1.4.** Soit  $G$  un groupe abélien, soit  $S$  une partie de  $G$ .

- On dit que  $S$  est une *partie génératrice* de  $G$ , ou encore que  $S$  engendre  $G$ , si  $G = \langle S \rangle$ .
- On dit que le *groupe abélien*  $G$  est de *type fini* s'il admet une *partie génératrice finie*.

Pour tout  $r \in \mathbb{N}^*$ , on note  $e = (e_i)_{1 \leq i \leq r} \in (\mathbb{Z}^r)^r$  la base canonique de  $\mathbb{Z}^r$  (chaque vecteur a pour  $i^{\text{ème}}$  coordonnée 1 et 0 ailleurs).

 **Exemple :**

- Un groupe  $G$  abélien fini est de type fini (engendré par la partie  $G$  finie).
- Soit  $r \in \mathbb{N}^*$ . Alors  $\mathbb{Z}^r$  est un groupe abélien de type fini (engendré par la partie  $\{e_1, \dots, e_r\}$ ).

**Lemme 1.5.** Soit  $G$  un groupe abélien, soit  $r \in \mathbb{N}^*$ , soit  $(x_1, \dots, x_r) \in G^r$ . Alors il *existe un unique morphisme* de groupes  $f$  du groupe  $\mathbb{Z}^r$  dans le groupe  $G$  qui, pour tout  $i \in \llbracket 1, r \rrbracket$ , envoie

$$e_i \text{ sur } x_i \text{ } (\star), \text{ donné par } f : \begin{cases} \mathbb{Z}^r & \longrightarrow G \\ (a_i)_{1 \leq i \leq r} & \longmapsto \sum_{i=1}^r a_i x_i \end{cases}.$$

De plus,  $\text{Im } f = \langle \{x_1, \dots, x_r\} \rangle$ .

*Démonstration.* Un morphisme de groupes de  $\mathbb{Z}^r$  dans  $G$  vérifiant  $(\star)$  est uniquement déterminé par l'image de la base canonique  $e$ , de par l'unicité de la décomposition d'un vecteur de  $\mathbb{Z}^r$  dans cette base et linéarité du morphisme.  $\square$

**Corollaire 1.6.** Un groupe abélien est de type fini si et seulement si il existe un morphisme de groupes *surjectif* du groupe  $\mathbb{Z}^r$  dans le groupe  $G$  (où  $r \in \mathbb{N}$ ).

*Démonstration.* On conserve les notations du lemme 1.5.

Soit  $G$  un groupe abélien de type fini. Alors  $G$  possède une partie génératrice finie  $S = \{x_1, \dots, x_r\}$  (où  $r \in \mathbb{N}$ ), d'où  $\text{Im } f = \langle S \rangle = G$ , i.e. le morphisme de groupes  $f$  de  $\mathbb{Z}^r$  dans  $G$  est surjectif.

Réciproquement, soit  $g$  un morphisme de groupes surjectif de  $\mathbb{Z}^r$  (où  $r \in \mathbb{N}$ ) dans  $G$ , alors  $S = \{f(e_1), \dots, f(e_r)\}$  est une partie génératrice de  $G$  (car tout élément de  $G$  possède un antécédent dans  $\mathbb{Z}^r$  qui se décompose dans la base canonique  $e$ , et donc son image, i.e.  $G$ , s'écrit comme combinaison linéaire d'éléments de  $S$ ).  $\square$

**Proposition 1.7.** Soient  $G$  et  $H$  deux groupes abéliens. Soit  $f$  un morphisme de groupes de  $G$  dans  $H$ . On suppose que le groupe abélien  $G$  est de type fini. Alors le groupe abélien  $\text{Im } f$  est de type fini.

*Démonstration.* Soit  $S$  une partie génératrice de  $G$ . Alors  $f(S)$  est une partie génératrice de  $\text{Im } f$ .  $\square$

**Corollaire 1.8.** Soit  $G$  un groupe abélien de type fini et  $H$  un sous-groupe de  $G$ . Alors le quotient  $G/H$  est de type fini.

*Démonstration.* Il suffit d'appliquer la proposition 1.7 à la surjection canonique  $\pi : G \rightarrow G/H$ .  $\square$

**Proposition 1.9.** Soient  $G$  et  $H$  deux groupes abéliens. Soit  $f$  un morphisme de groupes de  $G$  dans  $H$ . On suppose que les groupes abéliens  $\text{Im } f$  et  $\text{Ker } f$  sont de *type fini*. Alors  $G$  est un groupe abélien de type fini.

*Démonstration.* Par hypothèse, il existe  $(x_1, \dots, x_r) \in G^r$  tel que la partie finie  $\{f(x_1), \dots, f(x_r)\}$  engendre  $\text{Im } f$  et il existe  $(y_1, \dots, y_r) \in (\text{Ker } f)^s$  tel que la partie finie  $\{y_1, \dots, y_r\}$  engendre  $\text{Ker } f$ . Soit  $g \in G$ . Alors il existe  $(n_1, \dots, n_r) \in \mathbb{Z}^r$  tel que  $f(g) = \sum_{i=1}^r n_i f(x_i) = f\left(\sum_{i=1}^r n_i x_i\right)$ .

On conclut en décomposant l'élément  $g - \sum_{i=1}^r n_i x_i \in \text{Ker } f$  selon la famille  $\{y_1, \dots, y_s\}$ .  $\square$

**Proposition 1.10.** Soit  $G$  un groupe abélien de type fini. Soit  $H$  un sous-groupe de  $G$ . Alors le groupe abélien  $H$  est de type fini.

*Démonstration.*

→ Supposons le groupe  $G$  monogène. Si  $G$  est cyclique, on sait alors que  $H$  est cyclique. Sinon, on se donne un générateur  $g$  de  $G$  (qui est donc d'ordre infini). On sait que l'application  $\varphi : \begin{cases} \mathbb{Z} & \longrightarrow G \\ n & \longmapsto ng \end{cases}$  est un isomorphisme de groupes.  $H$  est isomorphe au sous-groupe  $\varphi^{-1}(H)$  de  $\mathbb{Z}$  qui s'écrit donc  $\varphi^{-1}(H) = m\mathbb{Z}$  (où  $m \in \mathbb{N}$ ), i.e.  $H = \varphi(m\mathbb{Z}) = \{ng \mid n \in m\mathbb{Z}\} = \langle mg \rangle$  i.e.  $H$  est monogène.

→ Dans le cas contraire, on considère un morphisme de groupes  $f : \mathbb{Z}^r \rightarrow G$  surjectif, où  $r \in \mathbb{N}^*$  désigne le cardinal de la partie génératrice de  $G$  (cf. preuve du corollaire 1.6). Montrons par récurrence sur  $r \in \mathbb{N}^*$  que  $H$  est de type fini :

\* Initialisation  $r = 1$  : C'est le cas où  $G$  est monogène et a donc déjà été traité dans le premier point de cette preuve.

\* Hérédité : Supposons le résultat vrai pour  $r - 1$  ( $r \in \mathbb{N}^*$ ). Considérons le groupe  $\mathbb{Z}^{r-1}$  comme sous-groupe de  $\mathbb{Z}^r$  (via l'injection de  $\mathbb{Z}^{r-1} \times \{0\}$  dans  $\mathbb{Z}^r$ ). Par hypothèse de récurrence, tout sous-groupe de  $K = f(\mathbb{Z}^{r-1})$  est de type fini. Montrons que  $G/K$  est monogène : considérons le morphisme de groupes  $\psi : \begin{cases} \mathbb{Z} & \longrightarrow G/K \\ a & \longmapsto \overline{f(0, \dots, 0, a)} \end{cases}$ . Soit  $\bar{g} \in G/K$ . Par surjectivité de  $f$ , il existe  $(a_1, \dots, a_r) \in \mathbb{Z}^r$  tel que  $g = f(a_1, \dots, a_r)$ . Donc  $\bar{g} = \overline{f(a_1, \dots, a_r)} = \overline{f(\underbrace{(a_1, \dots, a_{r-1}, 0)}_{\in K} + f(0, \dots, 0, a_r))} = \overline{f(0, \dots, 0, a_r)} = \psi(a_r)$ . Ainsi,  $\psi$

est surjectif, et donc  $G/K$  est isomorphe à  $\mathbb{Z}/\text{Ker } \psi$  monogène ( $\text{Ker } \psi = n\mathbb{Z}$ ,  $n \in \mathbb{N}$  comme sous-groupe de  $\mathbb{Z}$ ) et donc  $G/K$  est monogène d'après le premier point de cette preuve.

Soit  $H$  un sous-groupe de  $G$ . Considérons  $\pi_H : H \rightarrow G/K$  la restriction à  $H$  de la surjection canonique.  $\text{Im } \pi_H$  est un sous-groupe de  $G/K$  monogène, donc  $\text{Im } \pi_H$  est monogène.

$\text{Ker } \pi_H = K \cap H \subset K$  est de type fini par hypothèse de récurrence. D'après la proposition 1.9, on a donc que  $H$  est de type fini.  $\square$

**Définition 1.11.**

→ Soit  $G$  un groupe quelconque :

- \* Soit  $g \in G$ . On dit que l'élément  $g$  est de torsion si  $g$  est d'ordre fini.
- \* On dit que le groupe  $G$  est de torsion si tout élément de  $G$  est de torsion.
- \* On dit que le groupe  $G$  est sans torsion si tout élément de  $G$  non nul est d'ordre infini.

→ Si  $G$  est de plus abélien, on dit que  $G$  est libre de type fini s'il existe  $r \in \mathbb{N}$  tel que  $G$  soit isomorphe à  $\mathbb{Z}^r$ .

Dans ce cas, on a que :

- \*  $(x_1, \dots, x_r) \in G^r$  forment une famille libre, ou encore sont linéairement indépendants, si :

$$\forall (n_1, \dots, n_r) \in \mathbb{Z}^r, \left( \sum_{i=1}^r n_i x_i = 0 \implies \forall i \in \llbracket 1, r \rrbracket, n_i = 0 \right)$$

- \*  $(x_1, \dots, x_r) \in G^r$  forment une base de  $G$  si ils forment une famille libre et génératrice de  $G$ .

**Définition-proposition 1.12.** Soit  $G$  un groupe abélien.

- Il existe un unique sous-groupe  $H$  de  $G$  de torsion qui contient tout sous-groupe de  $G$  de torsion.  $H$  est appelé le sous-groupe de torsion de  $G$ , et est noté  $G_{\text{tor}}$ .
- Le groupe quotient  $G/G_{\text{tor}}$  est sans torsion.
- Soit  $(x_1, \dots, x_r) \in G^r$ . Alors la famille  $(x_1, \dots, x_r)$  est libre si et seulement si le morphisme de groupes  $f : \mathbb{Z}^r \rightarrow G$  du lemme 1.5 est injectif.

*Démonstration.*

- Le sous-ensemble  $H$  de  $G$  constitué de l'ensemble des éléments de torsion de  $G$  est un sous-groupe de torsion de  $G$  (l'élément nul est d'ordre 1, la somme de deux éléments de torsion est d'ordre le ppcm des ordres, et l'ordre de l'inverse d'un élément de torsion est inchangé) et contient tout sous-groupe de torsion par construction.
- Soit  $\bar{g} \in G/G_{\text{tor}}$  de torsion : il existe  $n \in \mathbb{N}^*$  tel que  $n\bar{g} = \bar{0}$ , i.e.  $ng \in G_{\text{tor}}$  : il existe  $m \in \mathbb{N}^*$  tel que  $mng = 0$  d'où  $g$  est de torsion, i.e.  $\bar{g} = \bar{0}$ . Donc  $G/G_{\text{tor}}$  est sans torsion.
- $f$  est injectif si et seulement si  $\text{Ker } f = \left\{ (a_i)_{1 \leq i \leq r} \in \mathbb{Z}^r \mid \sum_{i=1}^r a_i x_i = 0 \right\} = \{0_{\mathbb{Z}^r}\}$ .

□

**Corollaire 1.13.** Soit  $G$  un groupe abélien de type fini. Alors  $G$  est libre de type fini si et seulement si il admet une base.

*Démonstration.*  $\ominus$  Supposons  $G$  libre de type fini et soit  $r \in \mathbb{N}$  tel que  $f : \mathbb{Z}^r \rightarrow G$  soit un isomorphisme de groupes. Soit  $(x_1, \dots, x_r) = (f(e_1), \dots, f(e_r))$  les images de la base canonique  $e = (e_i)_{1 \leq i \leq r}$  de  $\mathbb{Z}^r$  par  $f$ . Soit  $z \in \mathbb{Z}^r$  et  $(a_1, \dots, a_r) \in \mathbb{Z}^r$  tel que  $z = \sum_{i=1}^r a_i e_i$ . On a donc :

$$f(z) = f\left(\sum_{i=1}^r a_i e_i\right) \stackrel{f \text{ morphisme}}{=} \sum_{i=1}^r a_i f(e_i) = \sum_{i=1}^r a_i x_i$$

$f$  est donc de la forme du lemme 1.5 et de par la proposition-définition 1.12, on a que  $(x_1, \dots, x_r)$  est libre. De plus par isomorphisme on a que  $\{x_1, \dots, x_r\}$  est génératrice de  $G$ .  $(x_1, \dots, x_r)$  est donc une base de  $G$ .

$\ominus$  Soit  $(x_1, \dots, x_r)$  une base de  $G$  et soit  $f$  le morphisme du lemme 1.5 associé. Alors d'après la proposition-définition 1.12,  $f$  est injectif et d'après la preuve du corollaire 1.6,  $f$  est surjectif, i.e.  $f$  est un isomorphisme de groupes. □

**Proposition 1.14.** Soit  $G$  un groupe abélien de type fini, alors le groupe de torsion  $G_{\text{tor}}$  est fini.

*Démonstration.* Soit  $\{x_1, \dots, x_r\}$  une partie génératrice de  $G_{\text{tor}}$  (licite car  $G_{\text{tor}}$  est de type fini comme sous-groupe d'un groupe de type fini). Pour tout  $i \in \llbracket 1, r \rrbracket$ , on note  $n_i$  l'ordre de l'élément

$x_i$ . On considère le morphisme de groupes  $\varphi : \begin{cases} \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z} & \longrightarrow G_{\text{tor}} \\ (\overline{a_1}, \dots, \overline{a_r}) & \longmapsto \sum_{i=1}^r a_i x_i \end{cases}$ .  
 $\varphi$  est bien défini car pour tout  $(\overline{a_1}, \dots, \overline{a_r}) = (\overline{b_1}, \dots, \overline{b_r}) \in \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ ,  $(a_i - b_i) \in n_i\mathbb{Z}$ , donc  $n_i = \text{ordre}(x_i) \mid (a_i - b_i)$  et donc  $\sum_{i=1}^r \underbrace{(a_i - b_i)}_{=0} x_i = 0$ .

De plus  $\varphi$  est surjectif par construction donc  $|G_{\text{tor}}| \leq \prod_{i=1}^r n_i \in \mathbb{N}^*$  i.e.  $G_{\text{tor}}$  est fini.  $\square$

**Remarque 1.15.** Si  $G$  est de type fini, alors  $G/G_{\text{tor}}$  est de type fini (l'image de la famille génératrice de  $G$  par la projection canonique  $\pi : G \rightarrow G/G_{\text{tor}}$  est génératrice de  $G/G_{\text{tor}}$ ).

## 1.2 Théorèmes de structure

**Remarque 1.16.** Soit  $E$  un  $\mathbb{K}$ -espace vectoriel sur le corps  $\mathbb{K}$  de dimension finie et  $F$  un sous-espace vectoriel de  $E$ . Alors  $F$  admet un supplémentaire  $S$  dans  $E$  qui est isomorphe à  $E/F$  (considérer l'application linéaire  $\pi$  de projection de  $E$  dans  $E/F$  restreinte à  $S$ . Alors  $\pi$  est injective, car  $\text{Ker } \pi = F \cap S = \{0\}$  et surjective, car tout élément de  $E/F$  admet un représentant appartenant à  $S$  en utilisant que  $E = F \oplus S$ ).

Question: Un concept analogue existe-t-il pour les groupes abéliens de type fini ?

Plus précisément, existe-t-il, pour  $G$  un groupe abélien de type fini et  $H \subset G$  un sous-groupe,  $H'$  un sous-groupe de  $G$  tel que  $H \times H'$  soit isomorphe à  $G$  ou, de manière équivalente, un isomorphisme de groupes entre  $H'$  et  $G/H$  ?

Nous pouvons d'ores et déjà affirmer que cela ne sera pas le cas en toute généralité : En effet, tout sous-groupe  $H' \subset \mathbb{Z}$  isomorphe à  $\mathbb{Z}/2\mathbb{Z}$  serait immédiatement de torsion, ce qui n'est pas possible puisque  $\mathbb{Z}$  est sans torsion.

Autre question: Tout groupe abélien  $G$  de type fini admet-t-il une base ?

**Proposition 1.17.** Soit  $G$  un groupe abélien de type fini. Alors  $G$  admet une base si et seulement si  $G_{\text{tor}} = \{0\}$ .

**Remarque 1.18.** D'après le corollaire 1.13, cela revient à montrer que  $G$  est isomorphe à  $\mathbb{Z}^r$ ,  $r \in \mathbb{N}$  si et seulement si  $G_{\text{tor}} = \{0\}$ .

*Démonstration.*  $\oplus$  Soit  $f$  un isomorphisme entre  $G$  et  $\mathbb{Z}^r$  et  $g_t \in G_{\text{tor}}$ .

Alors  $\exists! (n_1, \dots, n_r) \in \mathbb{Z}^r$  tel que  $f(n_1, \dots, n_r) = g_t$ .

Soit  $m := \text{ordre}(g_t) > 0$ . Alors  $mg_t = 0 = mf(n_1, \dots, n_r) = f(mn_1, \dots, mn_r)$ , donc  $(mn_1, \dots, mn_r) \in \text{Ker } f = \{0\}$  i.e.  $\forall i \in \llbracket 1, r \rrbracket$ ,  $mn_i = 0$  et donc par intégrité de  $\mathbb{Z}^r$  :

$$m = 0 \text{ ou } \forall i \in \llbracket 1, r \rrbracket, n_i = 0$$

Or  $m > 0$ , donc  $\forall i \in \llbracket 1, r \rrbracket$ ,  $n_i = 0$ , et donc  $g_t = f(n_1, \dots, n_r) = f(0) = 0$ .

On en déduit que  $G_{\text{tor}} = \{0\}$



⊖ Raisonnons par contraposée :

Comme  $G$  est de type fini, la proposition 1.6 nous assure que il existe  $r \in \mathbb{N}$  et  $f : \mathbb{Z}^r \rightarrow G$  tel que  $f$  soit un morphisme de groupes surjectif.

Montrons alors que si  $G_{\text{tor}} \neq \{0\}$ , un tel morphisme  $f$  n'est pas injectif i.e.  $\text{Ker } f \neq \{0\}$ .

Comme  $0 \in G_{\text{tor}}$ ,  $G_{\text{tor}} \neq \{0\} \implies \exists g_t \in G_{\text{tor}} \setminus \{0\}$ . Soit alors  $(n_1, \dots, n_r) \in \mathbb{Z}^r$  tel que  $f(n_1, \dots, n_r) = g_t$ . Comme  $f(0) = 0$ ,  $g_t \neq 0 \implies (n_1, \dots, n_r) \neq 0$ .

Soit  $m := \text{ordre}(g_t) > 0$ . Alors par intégrité de  $\mathbb{Z}$ ,  $m(n_1, \dots, n_r) = (mn_1, \dots, mn_r) \neq 0$ .

Or  $mg_t = 0 = mf(n_1, \dots, n_r) = f(m(n_1, \dots, n_r)) = f(mn_1, \dots, mn_r)$ , donc

$(mn_1, \dots, mn_r) \in \text{Ker } f$  et  $(mn_1, \dots, mn_r) \neq 0$  et donc  $\text{Ker } f \neq \{0\}$ .  $\square$

📌 **Exemple :** La famille  $(\bar{1}) \in \mathbb{Z}/2\mathbb{Z}$  ne forme pas une base de  $\mathbb{Z}/2\mathbb{Z}$  (car  $2\bar{1} = \overline{2 \cdot 1} = \bar{0}$ , donc  $(\bar{1})$  n'est pas libre)

Par l'existence d'une surjection de  $\mathbb{Z}^r$  dans  $G$  (proposition 1.6) et par le théorème de factorisation,  $G$  est isomorphe au groupe quotient  $\mathbb{Z}^r / \text{Ker } f$ . Nous allons donc dans un premier temps chercher à comprendre la structure des sous-groupes de  $\mathbb{Z}^r$ .

### 1.2.1 Sous-groupes de $\mathbb{Z}^r$

**Définition 1.19** ( $\text{GL}_n(\mathbb{Z})$ ). On note  $\text{GL}_n(\mathbb{Z})$  le groupe des matrices carrées de taille  $n$  inversibles à coefficients dans l'anneau  $\mathbb{Z}$  telles que l'inverse soit aussi à coefficients dans  $\mathbb{Z}$ .

**Lemme 1.20.** Soit  $A \in \text{GL}_n(\mathbb{Q}) \cap \mathcal{M}_n(\mathbb{Z})$ . Alors  $A \in \text{GL}_n(\mathbb{Z})$  si et seulement si  $|\det A| = 1$ .

*Démonstration.* ⊖ On suppose  $A \in \text{GL}_n(\mathbb{Z})$ . Alors  $(A, A^{-1}) \in \mathcal{M}_n(\mathbb{Z})^2$ .

Comme  $\underbrace{(\det A)}_{\in \mathbb{Z}} \underbrace{(\det A^{-1})}_{\in \mathbb{Z}} = 1$ ,  $\det A \in \mathbb{Z}^\times$ , et donc  $\det A = \pm 1$ .

⊖ Découle de la formule de la comatrice :  $A^{-1} = \frac{{}^t \text{com} A}{\det A}$  ( $\det A = \pm 1$  et les coefficients de  ${}^t \text{com} A$  s'expriment comme sommes et produits des coefficients de  $A \in \mathcal{M}_n(\mathbb{Z})$ , donc sont tous dans  $\mathbb{Z}$ ).  $\square$

**Lemme 1.21** (Lemme clef). Soit  $A \in \mathcal{M}_{n,m}(\mathbb{Z})$ . Alors  $\exists (P, Q) \in \text{GL}_n(\mathbb{Z}) \times \text{GL}_m(\mathbb{Z})$  tels que

$$PAQ^{-1} = \begin{pmatrix} \overbrace{\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \end{pmatrix}}^r & 0 \\ 0 & 0 \end{pmatrix}, \text{ où } r \in \mathbb{N} \text{ et la famille } (d_i)_{1 \leq i \leq r} \in (\mathbb{Z}^*)^r \text{ vérifie } d_1 \mid \dots \mid d_r.$$

De plus, ces coefficients sont uniquement déterminés par la matrice  $A$ , et appelés les *facteurs invariants* de  $A$ .

*Démonstration.* Plus tard.  $\square$

**Remarque 1.22.** Ce théorème est l'équivalent de la forme réduite standard à équivalence près d'une matrice à coefficients dans un corps  $\mathbb{K}$  :

$$\text{Si } A \in \mathcal{M}_{n,m}(\mathbb{K}), \text{ alors } \exists (P, Q) \in \text{GL}_n(\mathbb{K}) \times \text{GL}_m(\mathbb{K}) \text{ tel que } PAQ^{-1} = \begin{pmatrix} \overbrace{1 \dots 1}^r & & 0 \\ & \ddots & \\ 0 & & 1 & & 0 \\ & & & 0 & 0 \end{pmatrix}$$

où  $r = \text{rg}(A)$ .


**Proposition 1.23.** Soit  $G$  un *groupe abélien libre de type fini*. On note  $n$  le cardinal d'une base de  $G$ . Alors toute famille d'éléments linéairement indépendants de  $G$  admet au plus  $n$  éléments.

*Démonstration.*  $G$  étant isomorphe à  $\mathbb{Z}^n$  pour un certain  $n \in \mathbb{N}$  (définition-proposition 1.12) et comme un isomorphisme de groupe échange les familles libres, il suffit de raisonner sur une famille  $\mathcal{F}$  libre d'éléments de  $\mathbb{Z}^n$ .

$\mathcal{F}$  est alors  $\mathbb{Q}$ -libre (il suffit de multiplier une combinaison linéaire dans  $\mathbb{Q}$  par un dénominateur commun et de conclure par liberté de la famille dans  $\mathbb{Z}^n$ ), donc forme une famille libre du  $\mathbb{Q}$ -espace vectoriel  $\mathbb{Q}^n$ . De par les résultats généraux sur les espaces vectoriels, on a donc  $|\mathcal{F}| \leq n$ .  $\square$

**Remarque 1.24.**  $\triangle$  En général, une famille libre d'un *groupe abélien libre de type fini* ne peut se prolonger en une base de  $G$  !

En d'autres termes, il n'y a pas d'analogue du théorème de la base incomplète pour les groupes abéliens.

 **Exemple :** Dans  $\mathbb{Z}^2$ ,  $\mathcal{F} = ((1, 0), (0, 2))$  est une famille libre de  $\mathbb{Z}^2$ , mais non génératrice ((0, 1) ne peut se décomposer dans  $\mathcal{F}$ ) qui de plus ne peut se prolonger en une base  $\mathcal{B}$  de  $\mathbb{Z}^2$  (sinon on aurait  $|\mathcal{B}| \geq 3$  ce qui, en vertu de la proposition 1.23, est absurde)

**Exercice 1.25.** Redémontrer la proposition 1.23 en utilisant le lemme clef 1.21.

**Théorème 1.26** (de la base adaptée). Soit  $G$  un *groupe abélien libre de type fini*. Soit  $H$  un sous-groupe de  $G$ . Alors  $H$  est également un *groupe abélien libre de type fini*. De plus, il existe une base  $e = (e_1, \dots, e_n)$  de  $G$  et une famille d'entiers  $(d_i)_{1 \leq i \leq r} \in (\mathbb{Z}^*)^r$  où  $r \leq n$  vérifiant  $d_1 | \dots | d_r$  tels que la famille d'éléments de  $G$   $(d_1 e_1, \dots, d_r e_r)$  forme une base de  $H$ .

De plus, l'entier  $r$  et les coefficients  $(d_i)_{1 \leq i \leq r}$  sont uniquement déterminés par la base  $e$  de départ, appelés respectivement le *rang* et les *facteurs* du groupe  $G$ .

*Démonstration.* Existence : Soit  $(x_1, \dots, x_n)$  une base de  $G$  qui identifie canoniquement  $G$  à  $\mathbb{Z}^n$ . Soit  $(y_1, \dots, y_m)$  une famille génératrice de  $H$  (licite car  $H$  est un sous-groupe abélien de type fini).

Comme les  $(x_1, \dots, x_n)$  forme une base de  $G$ , on peut écrire de manière unique :

$$\forall j \in \llbracket 1; m \rrbracket, y_j = \sum_{i=1}^n a_{ij} x_i, a_{ij} \in \mathbb{Z}$$

Soit  $A := (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ . Alors le lemme clef 1.21 nous donne  $(P, Q) \in \text{GL}_m(\mathbb{Z}) \times \text{GL}_n(\mathbb{Z})$  tels que

$$PAQ^{-1} = \begin{pmatrix} d_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & d_r & \\ & 0 & & 0 \end{pmatrix} \text{ et } d_1 | \dots | d_r. \text{ Posons } \forall i \in \llbracket 1; n \rrbracket, e_i := Qx_i = \sum_{j=1}^n q_{ij}x_j \text{ et}$$

$\forall j \in \llbracket 1; m \rrbracket, f_j := P^{-1}y_j$  i.e.  $\forall i \in \llbracket 1; m \rrbracket, y_i = Pf_i = \sum_{j=1}^m p_{ij}f_j$ .

Autrement dit, on change :

- la base  $(x_1, \dots, x_n)$  par son image par  $Q$ .
- la famille génératrice  $(y_1, \dots, y_m)$  par son image par  $P^{-1}$ .

Par inversibilité de  $P$  et  $Q$ , on a que :

- $(e_1, \dots, e_n)$  est une base de  $G$ .
- $(f_1, \dots, f_m)$  est une famille génératrice de  $H$ .

Par construction, on a  $f_1 = d_1e_1, \dots, f_r = d_re_r, f_j = 0$  ( $r < j \leq m$ ). Alors  $(f_1, \dots, f_r)$  est une famille génératrice de  $H$ , libre par liberté de  $(e_1, \dots, e_r)$ , i.e.  $(f_1, \dots, f_r) = (d_1e_1, \dots, d_re_r)$  est une base de  $H$ .

Unicité : Plus tard. □

**Théorème 1.27** (de structure des groupes abéliens de type fini). Soit  $G$  un *groupe abélien de type fini*. Alors il existe un unique entier  $r \in \mathbb{N}$  et une unique famille d'entiers  $(d_i)_{1 \leq i \leq r}$  vérifiant  $d_1 | \dots | d_r$  tels que le groupe  $G$  soit isomorphe au groupe produit  $\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$ .

**Remarque 1.28.**  $G_{\text{tor}} = \{0\}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$  et  $G_{\text{sans torsion}} = \mathbb{Z}^r \times \{0\}^s$ .

Ces deux groupes vérifient bien  $G_{\text{sans torsion}} \simeq G/G_{\text{tor}}$ .

*Démonstration.* On se donne un morphisme de groupes surjectif  $f$  de  $\mathbb{Z}^n$  dans  $G$ . On pose  $H = \text{Ker } f$ . Alors, d'après le théorème de factorisation,  $G$  est isomorphe à  $\mathbb{Z}^n/H$  ( $\star$ ). Par application du théorème de la base adaptée à  $\mathbb{Z}^n$ , il existe une base  $e = (e_1, \dots, e_n)$  de  $\mathbb{Z}^n$  et une famille d'entiers  $(d_i)_{1 \leq i \leq s} \in (\mathbb{Z}^*)^s$  où  $s \leq n$  vérifiant  $d_1 | \dots | d_s$  tels que la famille

$$(d_1e_1, \dots, d_se_s) \text{ d'éléments de } G \text{ forme une base de } H, \text{ ie } H = \left\{ \sum_{i=1}^s a_i d_i e_i \mid (a_i)_{1 \leq i \leq s} \in \mathbb{Z}^s \right\} =$$

$$\left\{ \sum_{i=1}^n a_i e_i \mid (a_i)_{1 \leq i \leq n} \in (d_i \mathbb{Z})^s \times \{0\}^{n-s} \right\} (\star').$$

$$\text{On considère le morphisme de groupes surjectif } \pi : \begin{cases} \mathbb{Z}^n & \longrightarrow \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{n-r} \\ \sum_{i=1}^n a_i e_i & \longmapsto (\overline{a_1}, \dots, \overline{a_s}, a_{s+1}, \dots, a_n) \end{cases}$$

de noyau  $\text{Ker } \pi = (d_1\mathbb{Z})e_1 \times \dots \times (d_s\mathbb{Z})e_s \times \{0\}^{n-s}$  isomorphe à  $H$  (cf ( $\star'$ )). Ainsi, d'après ( $\star$ ),  $G$  est isomorphe à  $\mathbb{Z}^n / \text{Ker } \pi$ , lui-même isomorphe à  $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^r$  où  $r = n - s \in \llbracket 0, n \rrbracket$  (d'après le théorème de factorisation). D'où l'existence. □

**Corollaire 1.29.** Soit  $G$  un *groupe abélien de type fini*. On suppose  $G$  sans torsion. Alors  $G$  est libre.


*Démonstration.* □

### 1.2.2 Anneaux

Soit  $A$  un anneau.

**Définition 1.30.** Un  $A$ -module est par définition un groupe  $M$  additif muni d'une application

$$\cdot : \begin{cases} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & am \end{cases} \text{ vérifiant : pour tout } (a, b) \in A^2, \text{ pour tout } m \in M : \\ \begin{aligned} &— 0m = 0 \text{ et } 1m = m \\ &— (a + b)m = am + bm \\ &— (ab)m = a(bm) \end{aligned}$$


 **Exemple :** L'anneau  $A$  est un  $A$ -module. Un idéal de l'anneau  $A$  est un sous-module de  $A$ .

**Lemme 1.31.** Soit  $I$  un idéal de l'anneau  $A$  contenant l'élément 1 (neutre de la multiplication). Alors  $I = A$ .

**Définition 1.32.** • Soit  $(a_j)_{j \in J} \in A^J$ . On note alors également  $(a_j)_{j \in J}$  le plus petit idéal de  $A$  contenant cette famille :

$$(a_j)_{j \in J} = \left\{ \sum_{j \in J} \lambda_j a_j \mid (\lambda_j)_{j \in J} \in A^{(J)} \right\}$$

- Soit  $I$  un idéal de l'anneau  $A$ .
  - On dit que l'idéal  $I$  est principal si il existe  $a \in A$  tel que  $I = (a)$ .
  - On dit que l'anneau  $A$  est principal si  $A$  est intègre et tout idéal de l'anneau  $A$  est principal.

 **Exemple :**


- L'anneau  $\mathbb{Z}$  est principal (car  $\mathbb{Z}$  est intègre et tout idéal de  $\mathbb{Z}$  est un sous-groupe additif de  $\mathbb{Z}$ , ie de la forme  $a\mathbb{Z} = (a)$  où  $a \in \mathbb{Z}$ ).
- On considère l'anneau  $A = \mathbb{C}[X, Y]$ . Alors l'idéal  $(X, Y)$  n'est pas principal. En effet,  $I = (X, Y) = \{PX + QY \mid (P, Q) \in \mathbb{C}[X, Y]^2\} = \{P \in \mathbb{C}[X, Y] \mid P(0, 0) = 0\}$ . Supposons par l'absurde qu'il existe  $P_I \in A$  tel que  $I = (P_I) = \{PP_I \mid P \in \mathbb{C}[X, Y]\}$ . Alors en particulier,  $X \in I$  et  $Y \in I$  sont des multiples de  $P_I$ . Donc  $P_I$  est constant. Comme  $P_I \in I$ ,  $P_I(0, 0) = 0$ , d'où  $P_I = 0$ . Contradiction.

**Proposition 1.33.** Soit  $\mathbb{K}$  un corps. Alors les idéaux de l'anneau  $\mathbb{K}$  sont exactement  $\mathbb{K}$  et l'idéal trivial 0.

*Démonstration.* Soit  $I$  un idéal non nul de l'anneau  $\mathbb{K}$ . Soit  $x \in I \setminus \{0\}$ . Alors  $x$  est inversible, ie il existe  $y \in \mathbb{K}$  tel que  $xy = 1$ . Donc  $1 \in I$ . D'après le lemme précédent,  $\mathbb{K} = I$ .  $\square$

**Définition 1.34.** Soit  $I$  un idéal strict de l'anneau  $A$ .

- On dit que l'idéal  $I$  est premier si l'anneau quotient  $A/I$  est intègre.
- On dit que l'idéal  $I$  est maximal si l'anneau quotient  $A/I$  est un corps.

 **Exemple :**

- Soit  $n \in \mathbb{N}^*$ . Alors l'idéal  $n\mathbb{Z} = (n)$  de l'anneau  $\mathbb{Z}$  est premier et maximal si et seulement si l'entier  $n$  est premier.

— L'idéal  $(0)$  de l'anneau  $\mathbb{Z}$  est premier mais pas maximal.

**Proposition 1.35** (correspondance des deux définitions de maximalité). Soit  $I$  un idéal strict de l'anneau  $A$ . Alors l'idéal  $I$  est maximal si et seulement si pour tout idéal  $J$  de l'anneau  $A$  contenant strictement  $I$ , on a :  $J = A$  (ie l'idéal  $I$  est maximal pour l'inclusion).

*Démonstration.* On suppose que le quotient  $A/I$  est un corps. Soit  $J$  un idéal de l'anneau  $A$  contenant strictement  $I$ . On considère le morphisme d'anneaux de projection  $\pi$  de  $A$  dans  $A/I$ . Alors,  $\pi(J)$  est un idéal de l'anneau  $A/I$  (car  $\pi(J)$  est un sous-groupe additif du groupe  $J$  comme image d'un groupe par un morphisme de groupes et pour tout  $(x, b) \in \pi(J) \times A/I$ , il existe  $(a, a') \in J \times A$  tel que  $x = \pi(a)$  (par surjectivité de  $\pi$ ) et  $b = \pi(a')$ , d'où  $ax = \pi(a)\pi(a') = \pi(\underbrace{aa'}_{\in J}) \in \pi(J)$ ). Comme l'idéal  $J$  n'est pas l'idéal trivial,  $\pi(J) = A/I$  (cf proposition précédente).

Soit  $a \in A$ . Comme  $\pi(a) \in \pi(J)$ , il existe  $a' \in J$  tel que  $\pi(a) = \pi(a')$ , ie  $a - a' \in I \subset J$ . D'où  $a \in J$ . Ainsi,  $A \subset J$ , donc  $J = A$ .

Réciproquement, on suppose l'idéal  $I$  maximal pour l'inclusion. Alors l'anneau quotient  $A/I$  est non trivial. Soit  $x \in A/I \setminus \{0\}$ . Il existe alors  $a \in A$  tel que  $x = \pi(a)$ . On considère l'ensemble  $J = (a) + I = \{\lambda a + i \mid (\lambda, i) \in A \times I\}$ . Alors  $J$  est un idéal de l'anneau  $A$  contenant l'élément  $a$  et l'ensemble  $I$ . Donc  $I$  est un idéal strict de l'idéal  $J$ . Par maximalité  $I$ , il vient  $A = J$ . Or,  $1 \in J$  donc il existe  $(\lambda, i) \in A \times I$  tel que  $1 = \lambda a + i$ . D'où  $\pi(1) = \pi(\lambda a) + \underbrace{\pi(i)}_{=0} = \pi(\lambda)x = 1_{A/I}$ .

D'où l'élément  $x$  est inversible. Ainsi,  $A/I$  est un corps. □