Notes de cours de M305-Algèbre 2

5 février 2015

Table des matières

1 Rappels de théorie des groupes

À compléter

2 Groupes abéliens de type fini

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

Remarque 1. Tout groupe abélien $(G, +, 0_G)$ peut s'identifier à un $\mathbb{Z}$-module en posant :

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

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 2.1. Soient G un groupe abélien et S une partie de G. Alors il existe un unique sous-groupe H de G qui contient S 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 $\bigcap\limits_{H \in \mathcal{E}} H$ est un sous-groupe de G contenant S qui contenu dans tout autre élément de $\mathcal{E}$. □

Remarque 2. Soit G un groupe abélien, soit S une partie de G. Alors $\langle S \rangle$ contient l'élément neutre, et 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. :

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

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

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

Définition 2.2. Soit G un groupe abélien, soit S une partie de G.

- On dit que S est u*ne 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 $e = (e_i)_{1 \leqslant i \leqslant r} \in (\mathbb{Z}^r)^r$ 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 $\{e_1, \ldots, e_r\}$i

Lemme 2.3. Soit G un groupe abélien, soit $r \in \mathbb{N}^*$, soit $(x_1, \ldots, x_r) \in G^r$. Alors il *existe un unique morphisme* de groupes f du groupe $\mathbb{Z}^r$ dans le groupe G qui, pour tout $i \in [\![1, r]\!]$, *envoie* e_i *sur* x_i $(\star)$, donné par $f : \left\{ \begin{array}{ccc} \mathbb{Z}^r & \longrightarrow & G \\ (a_i)_{1 \leqslant i \leqslant r} & \longmapsto & \displaystyle\sum_{i=1}^{r} a_i x_i \end{array} \right.$.
De plus, $\operatorname{Im} f = \langle \{x_1, \ldots, x_r\} \rangle$.

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 la décomposition unique d'un vecteur de $\mathbb{Z}^r$ dans cette base et la linéarité du morphisme. □

Corollaire 2.4. 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 2.3.
Soit G un groupe abélien de type fini. Alors G possède une partie génératrice finie $S = \{x_1, \ldots, x_r\}$ (où $r \in \mathbb{N}$), d'où $\operatorname{Im} f = \langle S \rangle = G$, 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 $S = \{f(e_1), \ldots, f(e_r)\}$ 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, donc son image, i.e. g, s'écrit comme combinaison linéaire d'éléments de S). □

Proposition 2.5. 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 $\operatorname{Im} f$ est de type fini.

Démonstration. Soit S une partie génératrice de G. Alors $f(S)$ est une partie génératrice de $\operatorname{Im} f$. □

Corollaire 2.6. 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 2.5 à la sujection canonique $\pi : G \to G/H$. □

Proposition 2.7. Soient G et H deux groupes abéliens. Soit f un morphisme de groupes de G dans H. On suppose que les groupes abéliens $\operatorname{Im} f$ et $\operatorname{Ker} f$ sont de *type fini*. Alors G est un groupe abélien de type fini.

Démonstration. Par hypothèse, il existe $(x_1, \ldots, x_r) \in G^r$ tel que la partie finie $\{f(x_1), \ldots, f(x_r)\}$ engendre $\operatorname{Im} f$ et il existe $(y_1, \ldots, y_r) \in (\operatorname{Ker} f)^s$ tel que la partie finie $\{y_1, \ldots, y_s\}$ engendre $\operatorname{Ker} f$. Soit $g \in G$. Alors il existe $(n_1, \ldots, n_r) \in \mathbb{Z}^r$ tel que $f(g) = \displaystyle\sum_{i=1}^{r} n_i f(x_i) = f\left(\sum_{i=1}^{r} n_i x_i\right)$.
On conclut en décomposant l'élément $g - \displaystyle\sum_{i=1}^{r} n_i x_i \in \operatorname{Ker} f$ selon la famille $\{y_1, \ldots, y_s\}$. □

Proposition 2.8. 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 $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & ng \end{array} \right.$ 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 $f : \mathbb{Z}^r \to G$ surjectif, où $r \in \mathbb{N}^*$ désigne le cardinal de la partie génératrice de G (cf preuve du corollaire 2.4). 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 $r-1$ ($r \in \mathbb{N}^*$). Considèrons 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 $\psi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G/K \\ a & \longmapsto & \overline{f(0,\dots,0,a)} \end{array} \right.$. Soit $\overline{g} \in G/K$. 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 $g = \underbrace{f(a_1,\dots,a_{r-1},0)}_{\in K} + f(0,\dots,0,a_r)$, i.e. $\overline{g} = \overline{f(0,\dots,0,a_r)} = \psi(a_r)$. Ainsi, ψ est surjectif, et donc G/K est monogène d'après ce qui a été montré au premier point de cette preuve.
  Soit H un sous-groupe de G. Considèrons $\pi_H : H \to G/K$ la restriction à H de la surjection canonique. $\operatorname{Im}\pi_H$ est un sous-groupe de G/K monogène, donc $\operatorname{Im}\pi_H$ est monogène.
  $\operatorname{Ker}\pi_H = K \cap H \subset K$ est de type fini par hypothèse de récurrence. D'après la proposition 2.7, on a donc que H est de type fini.

□

Définition 2.9.

→ 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 :

- Soit $(x_1,\dots,x_r) \in G^r$. On dit que les éléments $x_1,\dots,x_r$ forment une famille libre, ou encore sont linéairement indépendants, si :

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

- On dit que les éléments $x_1,\dots,x_r$ forment une base de G si ils forment une famille libre et génératrice de G.

Définition-proposition 2.10. 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_{tor}.
- Le groupe quotient G/G_{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 $f : \mathbb{Z}^r \to G$ du lemme 2.3 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 $\overline{g} \in G/G_{\text{tor}}$ de torsion : il existe $n \in \mathbb{N}^*$ tel que $n\overline{g} = \overline{ng} = \overline{0}$, 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. $\overline{g} = \overline{0}$. Donc G/G_{tor} est sans torsion.
- f est injectif si et seulement si $\operatorname{Ker} f = \left\{ (a_i)_{1 \leqslant i \leqslant r} \in \mathbb{Z}^r \mid \sum_{i=1}^{r} a_i x_i = 0 \right\} = \{0_{\mathbb{Z}^r}\}$.

□

Corollaire 2.11. Soit G un groupe abélien de type fini. Alors G est libre de type fini si et seulement si il admet une base.

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

$$f(z) = f\Big(\sum_{i=1}^{r} a_i e_i\Big) \overset{f \text{ morphisme}}{=} \sum_{i=1}^{r} a_i f(e_i) = \sum_{i=1}^{r} a_i x_i$$

f est donc de la forme du lemme 2.3 et de par la proposition-définition 2.10, on a que $(x_1, \ldots, x_r)$ est libre. De plus par isomorphisme on a que $\{x_1, \ldots, x_r\}$ est génératrice de G. $(x_1, \ldots, x_r)$ est donc une base de G.
$\underline{\Leftarrow}$ Soit $(x_1, \ldots, x_r)$ une base de G et soit f le morphisme du lemme 2.3 associé. Alors d'après la proposition-définition 2.10, f est injectif et d'après la preuve du corollaire 2.4, f est surjectif, i.e. f est un isomorphisme de groupes. □

Proposition 2.12. Soit G un groupe abélien de type fini, alors le groupe de torsion G_{tor} est fini.

Démonstration. Soit $\{x_1, \ldots, x_r\}$ une partie génératrice de G_{tor} (licite car G_{tor} est de type fini comme sous-groupe d'un groupe de type fini). Pour tout $i \in [\![1, r]\!]$, on note n_i l'ordre de l'élément x_i. On considère le morphisme de groupes $\varphi : \begin{cases} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} & \longrightarrow & G \\ (\overline{a_1}, \ldots, \overline{a_r}) & \longmapsto & \sum_{i=1}^{r} a_i x_i \end{cases}$.

φ est bien défini car pour tout $(\overline{a_1}, \ldots, \overline{a_r}) = (\overline{b_1}, \ldots, \overline{b_r}) \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, $(a_i - b_i) \in n_i\mathbb{Z}$, donc $n_i = ordre(x_i) \mid (a_i - b_i)$ et donc $\sum_{i=1}^{r} \underbrace{(a_i - b_i)x_i}_{=0} = 0$.

De plus φ est surjectif par construction donc $|G| \leqslant \prod_{i=1}^{r} n_i \in \mathbb{N}^*$ i.e. G est fini. □

2.1 Théorèmes de structure

Remarque 3. Soit $\mathbb{K}$ un corps. Soit E un $\mathbb{K}$-espace vectoriel sur le corps $\mathbb{K}$ de dimension finie. Soit F un sous-espace vectoriel de E. Alors F admet un supplémentaire S dans E. On considère l'application linéaire f de projection de E dans E/F restreint à S. Alors f est injectif (car $\operatorname{Ker} f = F \cap S = \{0\}$ et surjective (car tout élément de E/F admet un représentant appartenant à S en utilisant la décomposition de E), ie S et E/F sont isomorphes.

Soit G un groupe abélien de type fini.

Soit H un sous-groupe de G.On cherche à déterminer, quand il existe, l'analogue d'un supplémentaire pour H, ie un sous-groupe H' de G tel que $H \times H'$ soit isomorphe à G, ou de manière équivalente, un isomorphisme de groupes de H' dans G/H. Par exemple, tout sous-groupe H' de $\mathbb{Z}$ isomorphe à $\mathbb{Z}/2\mathbb{Z}$ serait immédiatement de torsion, ce qui n'est pas possible puisque $\mathbb{Z}$ est sans torsion. On peut également se demander si tout groupe abélien G de type fini admet une base. Ce n'est jamais le cas si G_{tor} n'est pas réduit à l'élément nul. Par exemple, l'élément $\overline{1} \in \mathbb{Z}/2\mathbb{Z}$ (de torsion puisque d'ordre 2) ne forme pas une base de $\mathbb{Z}/2\mathbb{Z}$.

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

On note $\mathrm{GL}_n(\mathbb{Z})$ 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 2.13. Soit $A \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathcal{M}_n(\mathbb{Z})$. Alors $A \in \mathrm{GL}_n(\mathbb{Z})$ si et seulement si $|\det A| = 1$.

Démonstration. On suppose $A \in \mathrm{GL}_n(\mathbb{Z})$. Alors $(A, A^{-1}) \in \mathcal{M}_n(\mathbb{Z})^2$. Comme $\underbrace{(\det A)}_{\in\mathbb{Z}}\underbrace{(\det A^{-1})}_{\in\mathbb{Z}} = 1$, $\det A$ est un élément inversible du groupe $\mathbb{Z}$, donc égal à 1 ou -1. La réciproque vient de la formule de la comatrice. □

Théorème 2.14. Soit $A \in \mathcal{M}_{mn}(\mathbb{Z})$. Alors il existe $P \in \mathrm{GL}_n(\mathbb{Z})$ et $Q \in \mathrm{GL}_m(\mathbb{Z})$ tels que
$$PAQ^{-1} = \begin{pmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ & 0 & & 0 \end{pmatrix},$$ où $r \in \mathbb{N}$ et la famille $(d_i)_{1\leqslant i\leqslant r} \in (\mathbb{Z}^*)^r$ vérifie $d_1|\dots|d_r$.

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

Remarque 4. Ce théorème est l'équivalent de la forme réduite standard à équivalence près d'une matrice à coefficients dans le corps $\mathbb{C}$.

Proposition 2.15. 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 $n \in \mathbb{N}$ 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 (quitte à multiplier une combinaison linéaire par un dénominateur commun) donc forme une famille libre du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$. Donc $|\mathcal{F}| \leqslant n$. □

Remarque 5. Il n'y a pas d'analogue du théorèmes de la base incomplète pour les groupes abéliens : exemple ?

Théorème 2.16 (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 $e = (e_1, \ldots, e_n)$ de G et une famille d'entiers $(d_i)_{1\leqslant i\leqslant r} \in (\mathbb{Z}^*)^r$ où $r \leqslant n$ vérifiant $d_1| \ldots |d_r$ tels que la famille d'éléments de G $(d_1e_1, \ldots, d_re_r)$ forme une base de H. De plus, l'entier r et les coefficients $(d_i)_{1\leqslant i\leqslant r}$ sont uniquement déterminés par la base e de départ, appelés respectivement le rang et les facteurs du groupe G.

Démonstration. Soit $(x_1, \ldots, x_n)$ une base de G. Soit $(y_1, \ldots, y_m)$ une famille génératrice de H (licite car H est un sous-groupe abélien de type fini). ☐

Théorème 2.17 (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 $(d_i)_{1\leqslant i\leqslant r}$ vérifiant $d_1| \ldots |d_r$ tels que le groupe G soit isomorphe au groupe produit $\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_r\mathbb{Z}$.

Remarque 6. $G_{\text{tor}} = \{0\}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$ et $G_{\text{sans torsion}} = \mathbb{Z}^r \times \{0\}^s$

Démonstration. On se donne un morphisme de groupes surjectif f de $\mathbb{Z}^n$ dans G. On pose $H = \operatorname{Ker} f$. 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 $e = (e_1, \ldots, e_n)$ de $\mathbb{Z}^n$ et une famille d'entiers $(d_i)_{1\leqslant i\leqslant s} \in (\mathbb{Z}^*)^s$ où $s \leqslant n$ vérifiant $d_1| \ldots |d_s$ tels que la famille $(d_1e_1, \ldots, d_re_s)$ d'éléments de G forme une base de H, ie $H = \left\{ \sum_{i=1}^{s} a_i d_i e_i \mid (a_i)_{1\leqslant i\leqslant s} \in \mathbb{Z}^s \right\} = \left\{ \sum_{i=1}^{n} a_i e_i \mid (a_i)_{1\leqslant i\leqslant n} \in (d_i\mathbb{Z})^s \times \{0\}^{n-s} \right\}$ $(\star')$.

On considère le morphisme de groupes surjectif $\pi : \left\{ \begin{array}{ccc} \mathbb{Z}^n & \longrightarrow & \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{n-r} \\ \sum_{i=1}^{n} a_i e_i & \longmapsto & (\overline{a_1}, \ldots, \overline{a_s}, a_{s+1}, \ldots, a_n) \end{array} \right.$ de noyau $\operatorname{Ker} \pi = (d_1\mathbb{Z})e_1 \times \ldots \times (d_s\mathbb{Z})e_s \times \{0\}^{n-s}$ isomorphe à H (cf $(\star')$). Ainsi, d'après $(\star)$, G est isomorphe à $\mathbb{Z}^n/\operatorname{Ker} \pi$, lui-même isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}^r$ où $r = n - s \in [\![0, n]\!]$ (d'après le théorème de factorisation). D'où l'existence. ☐

Remarque 7. —

— Variante du théorème :

Corollaire 2.18. Soit G un *groupe abélien de type fini.* On suppose G *sans torsion.* Alors le groupe abélien de type fini G est *libre.*

Démonstration. ☐

2.2 Anneaux

Sot A un anneau.

Définition 2.19. Un A-module est par définition un groupe M additif muni d'une application $. : \left\{ \begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & am \end{array} \right.$ vérifiant : pour tout $(a, b) \in A^2$, pour tout $m \in M$:

— $0m = 0$ et $1m = m$

— $(a+b)m = am + bm$
— $(ab)m = a(bm)$

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

Lemme 2.20. Soit I un idéal de l'anneau A contenant l'élément 1 (neutre de la multiplication). Alors $I = A$.

Définition 2.21. • 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 I 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 2.22. 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 $x \in I\backslash\{0\}$. Alors x est inversible, ie il existe $y \in \mathbb{K}$ tel que $xy = 1$. Donc $1 \in I$. D'après le lemme précédent, $\mathbb{K} = I$. □

Définition 2.23. 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 2.24 (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 π 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 π) 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 $x \in A/I\backslash\{0\}$. 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. $\square$