Notes de cours de M305-Algèbre 2

20 janvier 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 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 $\displaystyle\bigcap_{H \in \mathcal{E}} H$ 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 1. 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 $\{e_1, \dots, e_r\}$i

Lemme 1. 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 1. 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.
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 1. 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. 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 à la sujection canonique $\pi : G \to G/H$. □

Proposition 2. 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 3. 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 1). 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, on a donc que H est de type fini.

□

Définition 2.

→ 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. 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 1 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 3. 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 :

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

f est donc de la forme du lemme 1 et de par la proposition-définition 2, 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 1 associé. Alors d'après la proposition-définition 2, f est injectif et d'après la preuve du corollaire 1, f est surjectif, i.e. f est un isomorphisme de groupes. □

Proposition 4. 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 $\varphi : \left\{ \begin{array}{ccc} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} & \longrightarrow & G \\ (\overline{a_1}, \ldots, \overline{a_r}) & \longmapsto & \sum_{i=1}^{r} a_i x_i \end{array} \right.$.

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. □