Groupe abélien de type fini

Marc Abboud

20 Janvier 2021

1 Définition et théorème de structure

On rappelle brièvement ce qu'est un groupe abélien, le sous-groupe engendré par une partie et la notion de groupe de type fini avant de passer au théorème de structure des groupes abéliens de type fini.

Definition 1.1. Un groupe $(G, +)$ est un ensemble muni d'une loi de composition $+ : G \times G \to G$ tel que G admet un neutre, chaque élément a un inverse et l'ordre des opérations n'a pas d'importance, c'est à dire $(x + y) + z = x + (y + z)$ pour tout x, y, z dans G.

On dit que le groupe est *abélien* ou *commutatif* si $x + y = y + x$ pour tout élément x, y de G.

Definition 1.2. Soit S une partie d'un groupe G, on dit que S engendre G si tout élément de G s'écrit comme produit d'éléments de S et de leur inverse.

Un groupe est de *type fini* s'il est engendré par une partie finie. Un exemple particulier de groupe de type fini sont les groupes cycliques.

Exercice 1 : Montrer que $\mathbf{Q}$ et $\mathbf{Q}/\mathbf{Z}$ ne sont pas de type fini.

Exercice 2 : Montrer que tout sous-groupe de $\mathbf{Z}^r$ est de type fini. En déduire que pour tout groupe abélien de type fini, tout sous-groupe est de type fini.

Definition 1.3. Un groupe est *cyclique* s'il est engendré par un seul élément.

Proposition 1.4. *Un groupe cyclique G est abélien. Il y a en fait deux possibilités : G est infini et isomorphe à $\mathbf{Z}$ ou bien G est fini de cardinal n et G est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.*

Démonstration. Soit g un générateur de G. On a un morphisme de groupes surjectif

$$\varphi : a \in \mathbf{Z} \twoheadrightarrow g^a \in G$$

Il y a alors deux possibilités : 1) le morphisme φ est injectif et c'est alors un isomorphisme, donc $G \simeq \mathbf{Z}$.

2) Le noyau de φ n'est pas trivial et est alors de la forme $n\mathbf{Z}$ avec n un entier, car c'est un sous groupe de $\mathbf{Z}$. On a alors par propriété universelle du quotient $G \simeq \mathbf{Z}/n\mathbf{Z}$. □

Exercice 3 : Donner les générateurs de $\mathbf{Z}/n\mathbf{Z}$ et montrer qu'ils forment un groupe isomorphe à $(\mathbf{Z}/n\mathbf{Z})^\times$.

Théorème 1.5. *Soit G un groupe abélien de type fini, il existe une décomposition de G sous la forme*

$$G \simeq \mathbf{Z}^r \times \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z}$$

avec la propriété que pour tout $i = 1, \cdots, s-1, d_i$ divise d_{i+1} et cette décomposition est unique.

On appelle r le rang *de G et les d_i sont les* facteurs invariants.

Ce théorème est plus général que le théorème de structure des groupes abéliens finis (auquel cas évidemment $r = 0$).

2 Étude de $\mathbf{Z}/n\mathbf{Z}$

Exercice 4 : Soit G un groupe et H, K des sous groupes tels que

1. H et K sont distingués dans G.
2. $G = HK$.
3. $H \cap K = \{e\}$.

Montrer que G est isomorphe à $H \times K$. Montrer que le résultat est aussi vrai si on suppose G fini et qu'on remplace l'hypothèse 3 par $|G| = |H|\,|K|$.

Exercice 5 : Soit $\mathbf{k}$ un corps fini, on cherche à montrer que le groupe abélien $\mathbf{k}^\times$ est cyclique. Si on utilise le théorème de structure des groupes abéliens, le résultat est assez rapide à démontrer. Voici une preuve qui ne l'utilise pas. On note N le cardinal de $\mathbf{k}^\times$.

1. Soit d un entier divisant N et x un élément d'ordre d. Montrer que le sous groupe engendré par x est de cardinal d.
2. Quel est le nombre maximal de solutions de l'équation $t^d - 1 = 0$ dans $\mathbf{k}^\times$?
3. En déduire que si y est un autre élément d'ordre d, alors $y \in < x >$.
4. Soit $N(d)$ le nombre d'élément d'ordre d dans $\mathbf{k}^\times$, montrer que l'on a $N(d) = 0$ ou bien $N(d) = \varphi(d)$ avec φ l'indicatrice d'Euler.
5. Montrer que $N = \sum_{d/N} N(d)$ et conclure.
6. En déduire que $(\mathbf{Z}/p\mathbf{Z})^\times$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$.

Exercice 6 :

1. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
2. Soit n un entier naturel et d divisant n. Montrer que $\mathbf{Z}/n\mathbf{Z}$ possède un unique sous-groupe de taille d.

On rappelle le thèorème chinois

Théorème 2.1. *Soient n, m des entiers premiers entre eux, alors il y a un isomorphisme d'anneaux*

$$\mathbf{Z}/(nm)\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}.$$

En particullier, $(\mathbf{Z}/nm\mathbf{Z})^\times \simeq (\mathbf{Z}/n\mathbf{Z})^\times \times (\mathbf{Z}/m\mathbf{Z})^\times$.

Exercice 7 : Montrer que $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$.

Exercice 8 : Le but de cet exercice est de décrire les groupes $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ pour p premier et α un entier.

1. On suppose d'abord que p est impair. On sait que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cylique par l'exercice 5. Soit $\alpha \geq 2$, montrer par récurrence que pour tout $k \geq 1$ il existe λ_k premier à p tel que $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. En déduire que $1 + p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^{\alpha-1}\mathbf{Z})^\times$.
2. En considérant la projection $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$ montrer qu'il existe un élément v d'ordre $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$.
3. En déduire que $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$.
4. On suppose maintenant $p = 2$, traiter le cas $\alpha = 1, 2$.
5. Soit $\alpha \geq 3$, montrer que 5 est d'ordre $2^{\alpha-2}$, en déduire que le noyau de la projection $\pi : (\mathbf{Z}/2^\alpha\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/4\mathbf{Z})^\times$ est le sous-groupe engendré par 5.
6. Montrer que $\pi(-1) = -1$ et que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times$ est isomorphe au produit $< 5 > \times < -1 >$. En déduire que $(\mathbf{Z}/2^\alpha\mathbf{Z})^\times \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$.

Exercice 9 : Trouver les entiers n tels que $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.

3 Exercices sur les groupes abéliens finis

Exercice 10 : Soit G un groupe et $x, y \in G$ d'ordre m et n respectivement. Si m et n sont premiers entre eux et que x et y commutent, alors xy est d'ordre mn.

Soit G un groupe fini, on définit *l'exposant* de G comme le ppcm des ordres des éléments de G.

Proposition 3.1. *Soit G un groupe fini abélien et N le maximum des ordres des éléments de G. Alors, tous les éléments de g ont un ordre divisant N et l'exposant de G est égal à N.*

Exercice 11 : Retrouver le fait que pour $\mathbf{k}$ un corps fini, le groupe $\mathbf{k}^\times$ est cyclique.

Exercice 12 : Montrer qu'un produit de groupe $G_1 \times \cdots \times G_S$ est cyclique si et seulement si chaque G_i est cyclique et les cardinaux des G_i sont deux à deux premiers entre eux.

Exercice 13 : Soit G un groupe et Z son centre. On suppose que le quotient G/Z est cyclique. Montrer que G est abélien. En utilisant ce résultat, classifier tous les groupes de cardinal p^2 pour p premier.

Exercice 14 : Donner le plus petit entier n tel qu'il existe un groupe de taille n non commutatif.

Exercice 15 : Soit G un groupe abélien fini non cyclique. Montrer qu'il existe un nombre premier p tel que G possède un sous-groupe H isomorphe à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Exercice 16 : Donner tous les groupes abéliens de cardinal 360 à isomorphisme près. Plus généralement, combien y'a t'il de groupes abéliens de taille n à isomorphisme près ?