Exercices classiques - Groupes finis

Monier MPSI p92

Ex : Montrer que les sous-groupes de $(\mathbb{Z},+)$ sont les $k\mathbb{Z}$, $k \in \mathbb{N}$

preuve : il est clair que les $k\mathbb{Z}$ $(k \in \mathbb{N})$ sont des sous-groupes de $(\mathbb{Z},+)$

Soit G un sous-groupe de $\mathbb{Z}$, supposons $G \neq \{0\}$

$\exists\, a \in G$ tel que $a \neq 0$

Si $a > 0$ alors $G \cap \mathbb{N}^* \neq \emptyset$

Si $a < 0$ alors $-a \in G$ et donc $G \cap \mathbb{N}^* \neq \emptyset$

donc $G \cap \mathbb{N}^+$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément noté k.

Montrons que $G = k\mathbb{Z}$.

1) Comme $k \in G$, on montre par récurrence que $\forall n \in \mathbb{N}$ $kn \in G$

passage à l'opposé $\forall n \in \mathbb{Z}$ $kn \in G$

donc $kn \subset G$

2) Réciproquement, soit $x \in G$. Par division euclidienne de x par k

$\exists (q,r) \in \mathbb{Z}^2$ tq

$x = kq + r$ avec $0 \leq r < k$

$x \in G$, $kq \in G$ donc $r \in G$ (G sous-groupe de $\mathbb{Z}$)

par déf de k (élément minimal) $r = 0$

donc $x = kq \in k\mathbb{Z}$.

Ex : Déterminer les sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ $n \in \mathbb{N}^*$

preuve : soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z},+)$

soit la surjection canonique $s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes.

on a $s^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. D'après l'exo précédent

$$s^{-1}(H) = k\mathbb{Z}$$

Comme s est surjective on a $H = s(s^{-1}(H)) = s(k\mathbb{Z})$

$$= \bar{k}\,\mathbb{Z}/n\mathbb{Z}$$

Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les $\bar{k}\,\mathbb{Z}/n\mathbb{Z}$, $k \in \mathbb{Z}$.

Ex : Soit $(G, \cdot)$ groupe monogène

Montrer que $\begin{cases} G \simeq \mathbb{Z} & \text{si } G \text{ est infini} \\ G \simeq \mathbb{Z}/n\mathbb{Z} & \text{si } G \text{ est fini et } n = \mathrm{card}(G) \end{cases}$

preuve : Notons a un générateur du groupe monogène G.

$G = \langle a \rangle$.

L'application $\varphi : \mathbb{Z} \to G$, $n \mapsto a^n$ est un morphisme de groupes.

car $\forall (m,n) \in \mathbb{Z}^2$ $\varphi(n+m) = a^{n+m} = a^n a^m = \varphi(n)\varphi(m)$

De plus φ est surjective puisque $G = \{a^n, n \in \mathbb{Z}\}$

1er cas, si φ est injective, alors φ est 1 isomorphisme de groupes

et $G \simeq \mathbb{Z}$, en particulier G est infini

2eme cas : φ non injectif.

$\ker \varphi$ est un sous-groupe de $\mathbb{Z}$. D'après exo 1,

$\exists n \in \mathbb{N}$ tq $\ker(\varphi) = n\mathbb{Z}$

Comme $\ker \varphi \neq \{0\}$ on a $n \in \mathbb{N}^*$ (non injectif)

Les éléments $\{e, a, a^2, \dots, a^{n-1}\}$ de G sont 2 à 2 distincts

car si $(k, l) \in \{0, \dots, n-1\}^2$ vérif $a^k = a^l$

alors $k - l \in \ker \varphi$ et $n \mid k - l$

donc $k = l$. Donc $G = \{e, a, a^2, \dots, a^{n-1}\}$

Vérifie que $\psi : G \to \mathbb{Z}/n\mathbb{Z}$, $a^k \mapsto \hat{k}$, $0 \leq k \leq n-1$ est un isomorphisme de groupes.