Groupes et morphismes

Antoine Ducros

23 octobre 2016

1 Exemples de sous-groupes

1 Sous-groupes de $\mathfrak{S}_4$

1. Soit K le sous-ensemble $\{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$. C'est un sous-groupe de $(\mathfrak{S}_4, \circ)$:

   Non vide et élément neutre $\mathrm{Id} \in K$

   Loi interne K est stable par produit, en effet

$$\begin{gathered}\forall \sigma \in K, \sigma^2 = \mathrm{Id} \\ (12)(34) \circ (13)(24) = (13)(24) \circ (12)(34) = (14)(23) \\ (12)(34) \circ (14)(23) = (14)(23) \circ (12)(34) = (13)(24) \\ (13)(24) \circ (14)(23) = (14)(23) \circ (13)(24) = (12)(34)\end{gathered}$$

2. Le sous-groupe engendré par (12) est $\{(12)^n / n \in \mathbb{N}\}$. Or $(12)^2 = \mathrm{Id}$ donc
$$\langle (12) \rangle \ = \{\mathrm{Id}, (12)\}$$

3. On sait que $(1234)^4 = \mathrm{Id}$, donc

$$\begin{gathered}\langle (1234) \rangle = \{\mathrm{Id}, (1234), (1234)^2, (1234)^3\} \\ (1234)^3 = (1234)^{-1} = (4321) \\ (1234)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)\end{gathered}$$

   Le groupe est donc :

$$\langle (1234) \rangle = \{\mathrm{Id}, (1234), (13)(24), (4321)\}$$

2 Sous-groupes de $\mathbb{Z}$

Soit $d \in \mathbb{Z}, \langle d \rangle = \{nd | n \in \mathbb{Z}\}$ (notation additive) On le note $d\mathbb{Z}$

Théoreme 1. *Tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$, pour un unique $d \in \mathbb{N}$*

Démonstration. Soit G un sous-groupe de $\mathbb{Z}$. Montrons qu'il existe $d \in \mathbb{N}$, tel que $G = d\mathbb{Z}$.

Existence On distingue deux cas

- Si $G = \{0\}, G = 0\mathbb{Z}$: $d \leftarrow 0$ convient.
- Si G est non trivial, il existe $g \neq 0$ dans G, avec $-g \in G$. G contient donc au moins un élément strictement positif, d'où $G \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$, donc elle admet un plus petit élément d. $d \in G \Rightarrow \langle d \rangle \subset G$. Nous allons établir l'inclusion réciproque.
  Soit $g \in G$, effectuons la division euclidienne de g par d :

$$\exists (q, r) \in \mathbb{Z} \times \mathbb{N}, \begin{cases} g = dq + r \\ 0 \leqslant r < d \end{cases}$$

$$\Rightarrow r = \underbrace{dq}_{\in d\mathbb{Z} \subset G} \underbrace{-g}_{\in G} \in G$$

$$\left.\begin{array}{c} 0 \leqslant r < d \\ r \in G \\ d = \min(G \cap \mathbb{N}^*) \end{array}\right\} \Rightarrow r = 0 \Rightarrow g = dq$$

  Ainsi $G \subset d\mathbb{Z}$.
  On a donc bien $G = d\mathbb{Z}$

Unicité Soit $d, d' \in \mathbb{N}$, tels que $d\mathbb{Z} = d'\mathbb{Z}$ Si $d = 0$ alors $d\mathbb{Z} = 0$ donc $d'\mathbb{Z} = 0$ donc $d' = 0$ car $d' = d' \times 1 \in d'\mathbb{Z}$

$\square$