2. Sous-groupes

1. Définition, caractérisation
2. Diagramme de Hasse
3. Théorème de Lagrange
4. Morphisme : noyau et image
5. Sous-groupe engendré par une partie
6. Sous-groupes monogènes d'un groupe fini
7. Sous-groupes de $\mathbb{Z}$ et arithmétique

1. Définition, caractérisation

Soit $(G, *, e)$ un groupe.

Définition (Sous-groupe)

Soit $H \subset G$. Si la loi de G restreinte à H en fait un groupe $(H, *, e)$, on dit que H est un sous-groupe de G.
Autrement dit, H est un sous-groupe de G si et seulement si l'inclusion

$$H \hookrightarrow G$$

est un morphisme de groupe.

Exemples :

1. **sous-groupes triviaux** : G et $\{e\}$.
2. les entiers pairs forment un sous-groupe de $\mathbb{Z}$

caractérisation des sous-groupes

Soit $(G, *, e)$ un groupe.

Proposition (Sous-groupe)

Soit $(G, *, e)$ un groupe. $H \subset G$ est un sous-groupe de G si et seulement si

$$H \neq \emptyset \quad \textit{et} \quad \left((\forall x, y \in H) \quad x * y^{-1} \in H\right)$$

Démonstration : exercice (de TD) □

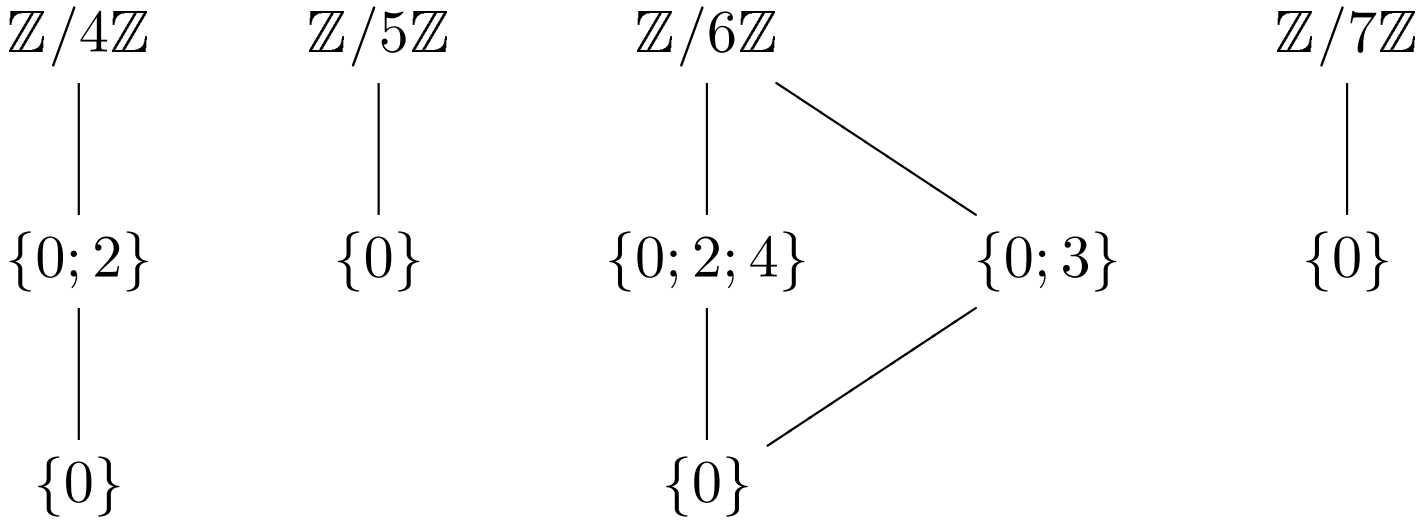
Remarque : Si $\mathrm{card}(G) = n$, il existe $\mathrm{card}\left(\mathcal{P}(G)\right) = 2^n$ parties de G. Il se peut que seules 2 parmi celles-ci soient des sous-groupes. (ex : $\mathbb{Z}/5\mathbb{Z}$, voir plus loin)

2. Diagramme de Hasse

Pour un groupe G, c'est le treillis de l'ensemble de ses sous-groupes, ordonné par l'inclusion. L'ensemble des sous-groupes de G admet toujours :

1. un plus grand élément : G, placé "en haut" ;
2. un plus petit élément : $\{e\}$, placé "en bas".

Exemples :



3. Théorème de Lagrange

Soit $(G, *, e)$ un groupe. Pour tout sous-groupe $H \hookrightarrow G$, on définit deux relations

$$\forall x, x' \in G, \qquad x \mathcal{R}_d x' \overset{\text{déf}}{\iff} x * x'^{-1} \in H \quad \text{et} \quad x \mathcal{R}_g x' \overset{\text{déf}}{\iff} x'^{-1} * x \in H$$

Exercices :

1. $\mathcal{R}_d$ et $\mathcal{R}_g$ sont des relations d'équivalences, dont les classes d'équivalence de $x \in G$ sont respectivement :

   $$\mathcal{R}_d(x) = Hx \quad (\text{classe à droite}) \quad \text{et} \quad \mathcal{R}_g(x) = xH \quad (\text{classe à gauche})$$

2. $\forall x \in G, \qquad \text{card}(Hx) = \text{card}(xH) = \text{card}(H)$

Pour les groupes finis, le théorème de Lagrange . . .

Définitions (ordre, indice)

Soit $(G, *, e)$ un groupe fini, *i.e.* $\mathrm{card}(G) \in \mathbb{N}$.

1. Son cardinal s'appelle l'ordre de G, et se note $\mathrm{ord}(G) \overset{\text{déf}}{=} \mathrm{card}(G)$.
2. L'indice d'un sous-groupe H de G est le nombre de classe d'équivalence de $\mathcal{R}_g$ (ou de $\mathcal{R}_d$, associée à H), et se note $[G : H]$.

Théorème (Lagrange)

L'ordre d'un sous-groupe divise l'ordre du groupe.

$$ord(G) = [G : H] ord(H)$$

Démonstration : G est la réunion disjointe des $[G : H]$ classes d'équivalence pour $\mathcal{R}_g$ (par exemple), qui ont chacune $\mathrm{ord}(H)$ éléments. □

4. Morphisme : noyau et image

Soit $f : G \to G'$ un morphisme de groupes.

Lemme

1. $H \hookrightarrow G \quad \Longrightarrow \quad f(H) \hookrightarrow G'$
2. $H' \hookrightarrow G' \quad \Longrightarrow \quad f^{-1}(H') \hookrightarrow G$

Démonstration : (exercices) □

Définitions

1. Noyau de f : $\mathrm{Ker}(f) \overset{\text{déf}}{=} f^{-1}(\{e'\}) = \{x \in G \ : f(x) = e'\} \hookrightarrow G$
2. Image de f : $\mathrm{Im}(f) \overset{\text{déf}}{=} f(G) = \{f(x) \ : x \in G\} \hookrightarrow G'$

noyau, image, morphisme injectif, surjectif

Soit $f : G \to G'$ un morphisme de groupes.

Proposition

1. f *injectif* $\iff$ $Ker(f) = \{e\}$
2. f *surjectif* $\iff$ $Im(f) = G'$

Démonstration : (exercices) □

5. Sous-groupe engendré par une partie

Soient $(G, *, e)$ un groupe et $A \subset G$, $A \neq \emptyset$.

Définition-proposition

On appelle sous-groupe engendré par A, et on note $< A >$, le plus petit sous-groupe de G contenant A.

1. *construction "par l'extérieur"*

$$< A > = \bigcap_{A \subset H \hookrightarrow G} H$$

2. *construction "par l'intérieur" (en notation multiplicative)*

$$< A > = \left\{ \prod_{k=1}^{n} x_k \ : n \in \mathbb{N},\ x_k \in A \ \ ou\ x_k^{-1} \in A \right\}$$

Sous-groupe engendré par une partie (2)

Démonstration :

1. la construction "par l'extérieur" découle du lemme ci-après.
2. la construction "par l'intérieur" se voit par double inclusion.

□

Lemme

Toute intersection de sous-groupes de $(G, *, e)$ est un sous-groupe de G.

Démonstration : (exercice) □

Exemple : Soit $x \in G$. On désigne par $< x >$ le sous-groupe de G engendré par $\{x\}$. Si $< x >= G$, on dit que G est un groupe monogène, ou que x est un générateur de G.
Si G est un groupe fini, on définira l'ordre de $x \in G$ par :

$$\mathrm{ord}(x) \overset{\text{déf}}{=} \mathrm{ord}(< x >)$$

6. Sous-groupes monogènes d'un groupe fini

Soit $(G, *, e)$ un groupe fini, $\mathrm{ord}(G) = n$.

Proposition

1. $\forall x \in G, \quad ord(x) | n.$
2. $\forall x \in G, \quad ord(x)$ *est le plus petit entier* $m \in \mathbb{N}$ *non nul tel que* $x^m = e.$
3. $\forall x \in G, \quad x^m = e \iff ord(x) | m$
4. $\forall x \in G, \quad x^n = e$

Démonstration :

1. Lagrange.
2. par la construction "par l'intérieur" de $< x >$.
3. par une division euclidienne de m par $\mathrm{ord}(x)$.
4. découle des 1 et 3 ci-dessus.

□

7. Sous-groupes de $\mathbb{Z}$ et arithmétique

Lemme (détermination des sous-groupes de $\mathbb{Z}$)

1. *Pour tout $n \in \mathbb{Z}$, $\quad n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +, 0)$.*
2. *Si H est un sous-groupe de $(\mathbb{Z}, +, 0)$, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.*

Démonstration :

1. On remarque : $n\mathbb{Z} = < n >$.
2. Si $H = \{0\}$ alors $n = 0$. Sinon, $H \cap \mathbb{N} \setminus \{0\}$ est non vide, donc admet un plus petit élément $n \in \mathbb{N}$, $n \neq 0$. Evidemment $n\mathbb{Z} \subset H$. L'inclusion inverse se montre par division euclidienne (exercice).

□

Sous-groupes de $\mathbb{Z}$ et arithmétique

Proposition (divisibilité, pgcd, ppcm)

Soient $a, b \in \mathbb{Z} \setminus \{0\}$.

1. $b|a \iff a\mathbb{Z} \subset b\mathbb{Z}$
2. $d = pgcd(a,b) \iff d \in \mathbb{N}$ *et* $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
3. $m = ppcm(a,b) \iff m \in \mathbb{N}$ *et* $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

Démonstration :

1. exercice.
2. $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. (d'où Bézout !)
3. $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. □

Remarque : les membres de droite de (1) et (2) de cette proposition ont encore un sens si $a = 0$ ou $b = 0$. Ceci conduit à poser :

$$\mathrm{pgcd}(0,0) \overset{\text{déf}}{=} 0$$