

À rédiger pour le 7^{oo}

240.29, 240.30, 110.12, 110.13[*]

Compléments sur les groupes

→ cf PP2:

Je me souviens

Loi de composition interne

1. Qu'est-ce qu'une loi de composition interne?
2. Comment noter une loi de composition interne?
3. Que signifient :
 - associatif?
 - commutatif?
 - élément neutre?
 - symétrique?
4. Soit E un ensemble, muni d'une loi de composition interne $*$. On suppose l'existence d'un élément neutre noté e . Soit a et b deux éléments de E qui admettent un symétrique. Est-ce que $(a*b)$ admet un symétrique?
5. Pour un élément a et un entier n , qu'est-ce que a^n ?
6. Qu'est-ce qu'une **partie stable** de E pour $*$?

2 notations

"additive"

"multiplicative"

↑

réservée aux
groupes commutatifs

$(G, +)$

$(G, \cdot)$

Structure de groupe

7. C'est quoi, un groupe ?
8. C'est quoi, un groupe abélien ?
9. Donner des exemples de groupes.
10. Comment définir le **groupe produit** de deux groupes ?
11. C'est quoi, un sous-groupe ?
12. Quels sont les deux sous-groupes triviaux de $(G, *)$?

$\hookrightarrow \{e\} \quad G$

$(G, \cdot)$ groupe

H sous-groupe de G signifie :

- $H \subset G$

- $e_G \in H$ (i.e. $H \neq \emptyset$)

- ~~$\forall x, y \in H, x \cdot y^{-1} \in H$~~

- H stable par $\cdot$ $\forall x, y \in H \quad x \cdot y \in H$

- H stable par $^{-1}$ $\forall x \in H \quad x^{-1} \in H$

13. Qu'est-ce qu'un morphisme de groupe ?
14. Donner des exemples de morphismes de groupes.

On considère $f : (G, *) \rightarrow (H, \cdot)$ un morphisme de groupe.

15. Quelle est l'image du neutre, du symétrique, par f ?
16. Que dire de l'image (directe) d'un sous-groupe par f ?
17. Que dire de l'image réciproque d'un sous-groupe par f ?
18. C'est quoi, le noyau de f ? Quel lien avec l'injectivité de f ?
19. C'est quoi, l'image de f ? Quel lien avec la surjectivité de f ?
20. Qu'est-ce qu'un **isomorphisme** de groupes.
21. Comment montrer qu'une application est un isomorphisme ?

On note e_H le neutre de e_G $\underline{\hspace{2cm}}$ *

$$\begin{aligned} \text{Ker } f &= f^{-1}(\{e_H\}) \\ &= \{x \in G \mid f(x) = e_H\} \end{aligned}$$

$\Rightarrow$. Bspw. mit $f(e_a) = e_H$ dann $e_a \in \text{Ker } f$.

• Somit $x \in \text{Kern } f$ ist $f(x) = e_H$
" $f(e_G)$

per injectivitate de f , $n = e_G$

⊆ On suppose $\ker f = \{e_G\}$

Sei $x, y \in G$ tq $f(x) = f(y)$

da $f(n) \cdot (f(g))^{-1} = e_H$

$$f(x) \cdot f(y^{-1})$$

$$= f(xy^{-1})$$

$$\text{donc } xy^{-1} \in \text{Ker } f$$

$$\text{Donc } xy^{-1} = e_G$$

$$\text{donc } xy^{-1} \cdot y = e_G \cdot y$$

$$\text{ie } x = y$$

Reprenons avec des notations additives.

$$f: (G, +) \longrightarrow (H, +)$$

$$\text{Soit } x, y \in G \text{ tq } f(x) = f(y)$$

$$\text{donc } f(x) - f(y) = 0_H$$

$$= f(x - y)$$

$$\text{donc } x - y = 0_G \quad \text{ie } x = y$$

Les entiers

- 22. Que désigne $\mathbb{Z}$? $7\mathbb{Z}$?
- 23. Énoncer le théorème de la division euclidienne dans $\mathbb{Z}$.

1 Sous-groupe engendré par une partie

Proposition. Une intersection de sous-groupes est un sous-groupe : si $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$, alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Preuve: • $\forall i, H_i \subset G$

donc $\bigcap_{i \in I} H_i \subset G$

• $\forall i, e_G \in H_i$

donc $e_G \in \bigcap_{i \in I} H_i$

• Soit $x, y \in \bigcap_{i \in I} H_i$

alors $\forall i, x, y \in H_i$ donc $x * y^{-1} \in H_i$

donc $x * y^{-1} \in \bigcap_{i \in I} H_i$

Définition. Soit $(G, *)$ un groupe et A une partie de G . On appelle **sous-groupe engendré par A** le plus petit sous-groupe H de $(G, *)$ qui contient A .

Remarque. On note $\langle A \rangle$ le sous-groupe engendré par A , mais cette notation n'est pas dans le programme officiel.

Remarque. La définition signifie que H est le sous-groupe de $(G, *)$ engendré par A si et seulement si :

- H est un sous-groupe de $(G, *)$
- $A \subset H$
- Pour tout sous-groupe K de $(G, *)$, $A \subset K \implies H \subset K$

Proposition. Avec les notations précédentes :

$$\langle A \rangle = \bigcap_{\substack{A \subset H \\ H \text{ sous-groupe de } G}} H$$

On note $B = \bigcap_{\substack{A \subset H \\ H \text{ sous-groupe de } G}} H$ est un sous-groupe de G

B contient tout sous-groupe de G contenant A .
 B est l'un des H indexant l'intersection.

Définition. La partie A de $(G, *)$ est dite **génératrice** de G lorsque le sous-groupe de $(G, *)$ engendré par A est G .

Description du sous-groupe engendré par A . Soit G un groupe noté multiplicativement. $\langle A \rangle$ est l'ensemble des éléments de G qui s'écrivent sous la forme :

$$a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$$

où $n \in \mathbb{N}$, $a_1, \dots, a_n \in A$, $\varepsilon_1, \dots, \varepsilon_n = \pm 1$.

Remarque. Lorsque G est commutatif et noté additivement, le sous-groupe engendré par A est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1 a_1 + \dots + k_p a_p$$

où $p \in \mathbb{N}$, $a_1, \dots, a_p \in A$ sont distincts, et $k_1, \dots, k_p \in \mathbb{Z}$. Ce ne sont pas tout à fait des combinaisons linéaires, puisque les « scalaires » sont ici entiers.

Exemple: $(G, \cdot)$ $A = \{a, b\} \subset G$

Dans $H = \langle A \rangle$, il y a a, b car $A \subset H$

$a \cdot a$ car H stable par $\cdot$.

a^{-1}, b^{-1} car H stable par passage au sym.

$a a a \cdot b \cdot a^{-1} b a^{-1} b^{-1}$

donc $H \supset \underbrace{\{ \text{produits de } a \text{ et } b \text{ et } a^{-1} \text{ et } b^{-1} \dots \}}$

c'est un sous-groupe de G
qui contient A

donc contient $\langle A \rangle = H$

$$\exists a \in \mathbb{N} \setminus \{0\} \text{ s.t. } a\mathbb{Z} = \langle a \rangle$$

Proposition. Les sous-groupes de $\mathbb{Z}$ sont les $a\mathbb{Z} = \langle a \rangle$, où $a \in \mathbb{N}$.

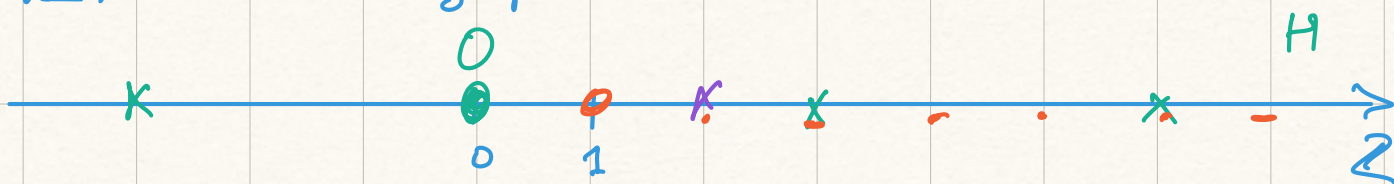
$\Leftarrow$ Soit $a \in \mathbb{N}$.

$$a\mathbb{Z} = \{ ak, k \in \mathbb{Z} \}$$

$$= \langle a \rangle \text{ c'est un sous-groupe de } \mathbb{Z}$$

comme groupe engendré par...

$\Rightarrow$ Soit H sous-groupe de $\mathbb{Z}$.



1^{er} cas: $H = \{0\}$, or $H = 0\mathbb{Z}$

2^e cas on suppose $H \neq \{0\}$

donc $H \cap \mathbb{Z}^+ \neq \emptyset$ donc $H \cap \mathbb{N}^* \neq \emptyset$

$\hookrightarrow$ car H stable opposé.

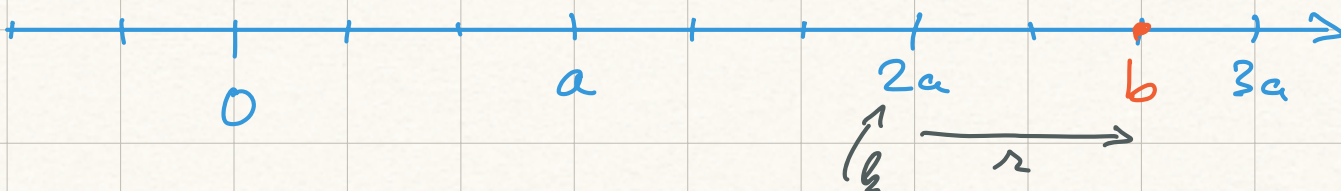
On définit $a = \min(H \cap \mathbb{N}^*)$

Montrons que $H = a\mathbb{Z}$

$\supseteq$ $a \in H$ donc $a\mathbb{Z} \subset H$

car H est un groupe

$\subseteq$ Soit $b \in H$



On effectue la div. euclidienne de b par a :

$$\exists k \in \mathbb{Z}, \exists r \in [0, a[\quad (\text{unique})$$

$$\text{tg} \quad b = ak + r$$

$$\text{donc} \quad r = b - ak$$

$$\in \mathbb{N} \cap \mathbb{N} \quad \text{et} \quad r < a$$

$$\text{donc} \quad r = 0$$

$$\text{donc} \quad b = ak \in a\mathbb{Z}.$$

