Pour ve : 11.1, 11.3, 52.24 (a)

Compléments sur les groupes

Je me souviens

1.1 Loi de composition interne

1. Qu'est-ce qu'une loi de composition interne ?
2. Comment noter une loi de composition interne ?

loi de c.i : $E \times E \longrightarrow E$

$(x, y) \longmapsto x * y$

application de $E \times E$ à valeurs dans E

notation : $+$ $\quad x + y$ notation additive

$*$ $\quad xy$ notation multiplicative.

$\times$, $\cdot$, $\top$, $\heartsuit$, $\circ$

3. Que signifient :

- associatif ?
- commutatif ?
- élément neutre ? Comment le note-t-on ?
- inversible ?

$*$ est associative si $(x*y)*z = x*(y*z)$ $\forall x,y,z$

→ peut écrire $x*y*z$

→ non associatif → rare.

$*$ est commutatif si $\forall x,y$ $x*y = y*x$

e est neutre de $*$ signifie $\forall x \in E$ $\underset{\substack{\shortparallel \\ e*x}}{x*e} = x$

x est <u>inversible</u> signifie $\exists y \in E$ tq $x*y = y*x = e$

(on note $y = x^{-1}$

et on dit y <u>inverse</u> de x)

not multiplicative

x admet un <u>opposé</u> si $\exists y \in E$ tq ~~$x*y = y*x = e$~~

$x+y = y+x = e$

not additive

(en général $+$ est commutative)

y est <u>l'opposé</u> de x, noté $-x$

réciproque si la loi est $\circ$

symétrique / symétrisable en général.

$\mathbb{Z}, \times$ 1 3

4. Soit E un ensemble, muni d'une loi de composition interne $*$. On suppose l'existe d'un élément neutre noté e. Soit a et b deux éléments de E, inversibles. Est-ce que $(a * b)$ est inversible ?

si a et b inversibles, alors $(a*b)$ inversible

et $(a*b)^{-1} = b^{-1} * a^{-1}$

Ok! $(a*b)*(b^{-1}*a^{-1}) = e$

$$(b^{-1}*\underbrace{a^{-1})*(a}_{e}*b) = e$$

5. Pour un élément a et un entier n, qu'est-ce que a^n ?

$n \in \mathbb{N}$, $a^n = a*a*\cdots*a$ n fois (récurrence)

$a^0 = e$

n négatif $n = -4$ $(a^{-1})^{-n} = a^{-1}*a^{-1}*a^{-1}*a^{-1}$

notation multiplicative

en notation additive

$n\,a = a+a+\cdots+a$ n fois

$0\,a = 0$

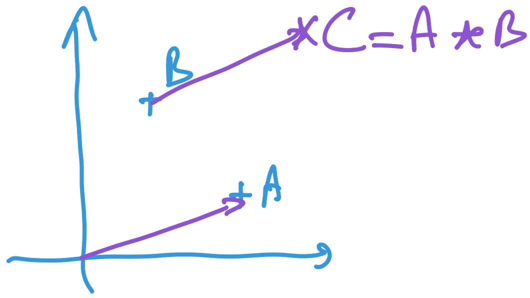
$-7a = -a-a-\cdots-a$

6. Qu'est-ce qu'une **partie stable** de E pour $*$?

$F \subset E$ est stable pour $*$

Signifie : $\forall x, y \in F, \quad x * y \in F$

$\cancel{\forall (x,y) \in F^2}$



Loi de ci sur $\mathbb{R}^2$

$A = (a_1, a_2)$

$B = (b_1, b_2)$

$A * B = (a_1 + b_1, \ a_2 + b_2)$

$* : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$\forall \big((a_1, a_2), (b_1, b_2)\big) \in (\mathbb{R}^2)^2$

$\cancel{\forall A, B \in \mathbb{R}^2}$

$\forall (a_1, a_2), (b_1, b_2) \in \mathbb{R}^2$

$\forall a_1 \ a_2 \ b_1 \ b_2 \in \mathbb{R}$

1.2 Structure de groupe

7. C'est quoi, un groupe ?

G est un groupe si

- il a une loi de ci $*$
- $*$ associative
- $*$ admet un neutre
- tout $x \in G$ est inversible.

8. Donner des exemples de groupes.

$(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$ commutatif (abélien) symétrique = opposé.

$(\mathcal{M}_n(\mathbb{R}),+)$, $(\mathbb{R}^{\mathbb{R}},+)$

$\mathcal{F}(\mathbb{R},\mathbb{R})$

$(\mathbb{N},+)$ pas un groupe

$(\mathbb{R},\times)$ pas un groupe

$(\mathbb{R}^*,\times)$ groupe $(\mathbb{Q}^*,\times)$, $(\mathbb{C}^*,\times)$

$(\mathcal{D}_n(\mathbb{R}),\times)$ ~~groupe~~ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ non inversible.

$(GL_n(\mathbb{R}),\times)$ groupe

$(\mathfrak{S}_n,\circ)$ groupe des permutations.

$(\mathbb{U},\times)$ ensemble des complexes de module 1

$(\mathbb{U}_n,\times)$ ensemble des racines n^e de l'unité.

9. Comment définir le **groupe produit** de deux groupes ?

Soit $(G, \times)$, $(H, \cdot)$ groupes

le groupe produit est le groupe qui est $G \times H$

muni de la loi produit :

$$* : (G \times H) \times (G \times H) \longrightarrow (G \times H)$$

$$((g_1, h_1), (g_2, h_2)) \longmapsto (g_1 \times g_2, h_1 \cdot h_2)$$

$(G \times H, *)$ est un groupe.

(bon exercice)

10. C'est quoi, un sous-groupe ?

11. Quels sont les deux sous-groupes triviaux de $(G, *)$?

H est un sous-groupe de $(G, *)$

déf

signifie : $H \subset G$

$(H, *)$ groupe

$* : G \times G \longrightarrow G$

$*_H : H \times H \longrightarrow H$

<u>Caractérisation</u>

caract utile en pratique

- $H \subset G$
- $e \in H \longleftrightarrow H \neq \emptyset$
- H est stable par $*$
- H est stable par passage à $\begin{cases} \text{l'inverse} \\ \text{symétrique} \\ \text{opposé si } + \end{cases}$

<u>Sous-groupes triviaux :</u> $\{e\}$ et G.

1.3 Morphisme de groupes

12. Qu'est-ce qu'un morphisme de groupe ?

13. Donner des exemples de morphismes de groupes.

application $(G, *) \longrightarrow (H, \circ)$

qui respecte la structure de groupe

$\cos \quad (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$

$\cos(x+y) \neq \cos(x) + \cos(y)$ pas morphisme de groupe.

$$f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto 2x$$

$$f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y)$$

morphisme de groupe.

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$$ et ln
$$x \longmapsto e^x$$

$$\exp(x+y) = \exp(x) \times \exp(y)$$

morphisme de groupe

$$\det : (GL_n(\mathbb{R}), \times) \longrightarrow (\mathbb{R}^*, \times)$$
$$M \longmapsto \det(M)$$

$$\det(M \times N) = \det(M) \times \det(N)$$

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

14. Quelle est l'image du neutre, de l'inverse, par f ?

$$f(e_G) = e_H$$

$$f(x^{-1}) = \left(f(x)\right)^{-1}$$

15. Que dire de l'image (directe) d'un sous-groupe par f ?

16. Que dire de l'image réciproque d'un sous-groupe par f ?

$$f : (G, *) \longrightarrow (H, \cdot)$$

$A \subset G$ A sous-groupe de G

[image directe de A par f] $= f(A)$

est un sous-groupe de $(H, \cdot)$

Si B sous-groupe de $(H, \cdot)$,

alors $f^{-1}(B)$ est un sous-groupe de G.

Cool!

Exemple

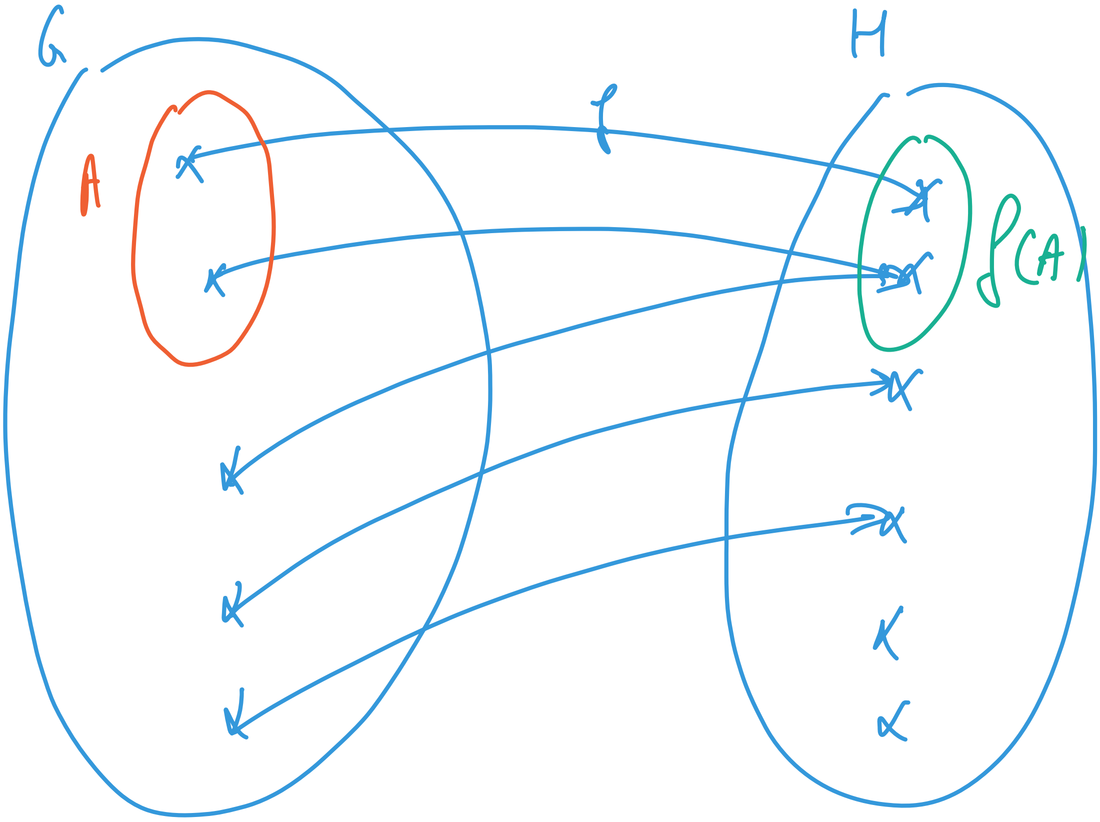
$SL_n(\mathbb{R}) = \{ M \in M_n(\mathbb{R}) \text{ tq } \det(M) = 1 \}$

Mque groupe pour $\times$ $\rightarrow$ déf.

$\rightarrow$ sous-groupe $GL_n(\mathbb{R})$

$\rightarrow$ $SL_n(\mathbb{R}) = \det^{-1}(\{1\})$

$= \operatorname{Ker} \det$



$[\text{image directe de } A \text{ par } f] = f(A)$

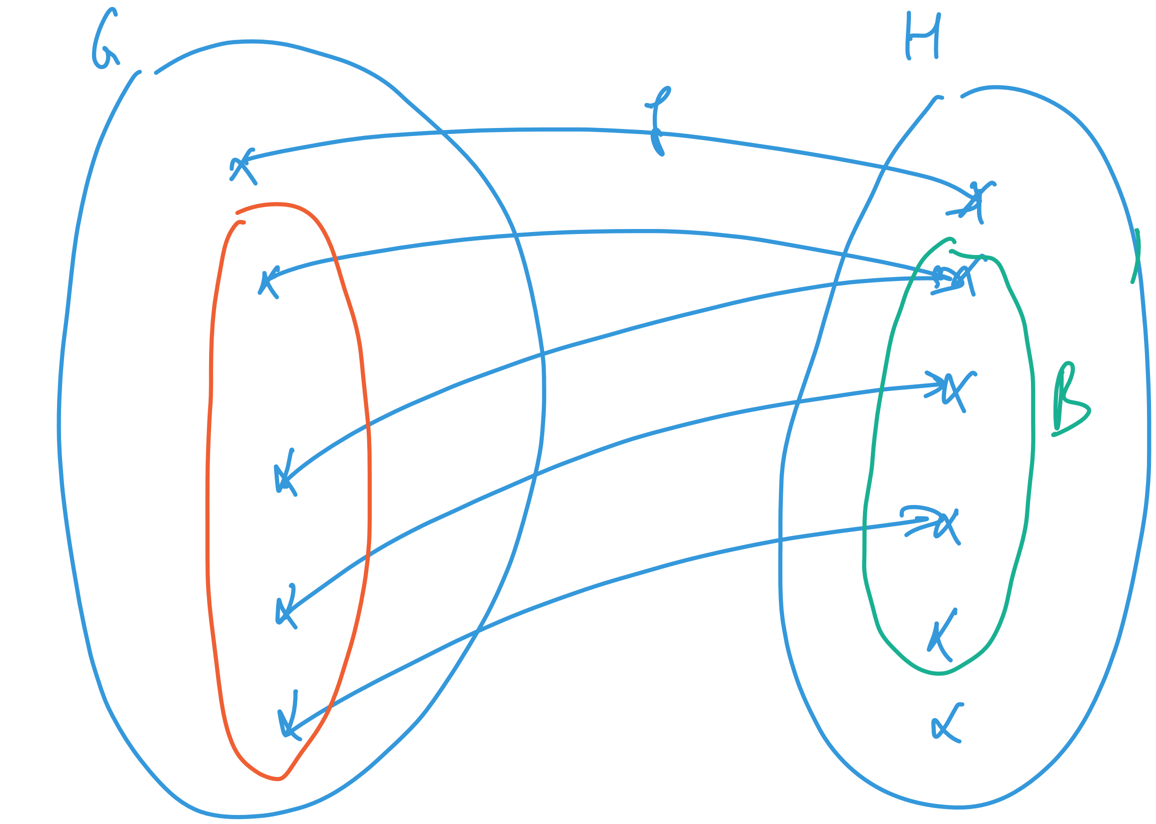
$= \{ f(a),\ a \in A \}$

$b \in f(A) \iff \exists a \in A \text{ tq } b = f(a)$ DUR

$[\text{Image réciproque de } B \text{ par } f] = \cancel{f(B)}^{-1} \quad f^{-1}(B) \quad \overleftarrow{f}(B)$

$= \{ x \in G \text{ tq } f(x) \in B \}$

$x \in f^{-1}(B) \iff f(x) \in B$ FACILE



[Image réciproque de B par f] $= \cancel{f(B)}^{-1}$ $f^{-1}(B)$ $\overleftarrow{f}(B)$

$$= \{x \in G \mid f(x) \in B\}$$

$$x \in f^{-1}(B) \iff f(x) \in B$$

17. C'est quoi, le noyau de f ? Quel lien avec l'injectivité de f ?

18. C'est quoi, l'image de f ? Quel lien avec la surjectivité de f ?

$$f : (G, \times) \longrightarrow (H, \cdot)$$

$$\operatorname{Ker} f = \{ x \in G \text{ tq } f(x) = e_H \}$$
$$= f^{-1}(\{e_H\}) \qquad \text{sous-groupe de } G$$

$\operatorname{Ker} f = \{e_G\} \iff f$ est injective

$$\operatorname{Im} f = f(G)$$
$$= \{ y \in H,\ \exists x \in G \text{ tq } y = f(x) \}$$

$(\operatorname{Im} f = H \iff f$ est surjective$)$

19. Qu'est-ce qu'un **isomorphisme** de groupes.

20. Comment montrer qu'une application est un isomorphisme ?

morphisme injectif et surjectif

$$f : (G, \times) \longrightarrow (H, \cdot)$$

<u>justif</u> : $\operatorname{Ker} f = \{e_G\}$ et f surjective et morphisme

<u>ou</u> Trouver g tq $f \circ g = \mathrm{Id}_H$ et $g \circ f = \mathrm{Id}_G$
et f morphisme

1.4 Les entiers

21. Que désigne $\mathbb{Z}$? $7\mathbb{Z}$?

22. Énoncer le théorème de la division euclidienne dans $\mathbb{Z}$.

$\mathbb{Z}$ entiers relatifs $-1, -2, 10, 0$

$$7\mathbb{Z} = \{ \text{multiples de } 7 \}$$
$$= \{ 7k,\ k \in \mathbb{Z} \} \quad \text{paramétrage}$$

$$n \in 7\mathbb{Z} \iff \exists k \in \mathbb{Z} \text{ tq } n = 7k$$

division eucl de a par b où $a, b \in \mathbb{N}$ $b \neq 0$

$$\exists! (q, r) \text{ tq } \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

$$\begin{array}{r|l} a & b \\ \hline \dots & \\ r & \dots q \end{array}$$

Si $a, b \in \mathbb{Z}$,

$$a = bq + r$$
$$0 \leq r < |b|$$

2 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.

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 $(G,*)$, $A\subset K \implies H\subset K$*

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

Remarque. *On peut décrire le sous-groupe engendré par A : C'est l'ensemble des éléments de G qui s'écrivent sous la forme :*

$$a_1^{\varepsilon_1} * \cdots * a_n^{\varepsilon_n}$$

où $n \in \mathbb{N}$, $a_1, \ldots, a_n \in A$, $\varepsilon_1, \ldots, \varepsilon_n = \pm 1$.
Lorsque G est commutatif et noté additivement, le sous-groupe engendré par A est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1 a_1 + \cdots + k_p a_p$$

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