Lycée CHATEAUBRIAND
Colas Bardavid

Chapitre 10

Groupes

Évariste GALOIS (1811 – 1832)

Évariste Galois

Figure romantique des mathématiques par excellence, il meurt à 20 ans dans un duel amoureux. La veille de sa mort, il rédige un testament mathématique où il couche sur le papier certaines de ses idées. Il révolutionne les mathématiques. Ses idées, très profondes, sont encore extrêmement influentes dans les mathématiques contemporaines. Il est à l'origine de la théorie des groupes et de la théories des corps.

Lycée CHATEAUBRIAND
MPSI 3

Colas Bardavid

10
Groupes

plan de cours et principaux résultats

I. Lois de composition internes

16.5 16.6 16.7

1) Lois de composition internes
a) définition
b) magmas

2) Associativité
a) définition
b) semi-groupes
c) puissances

3) Commutativité

4) Exemples

5) Neutre
a) définition
b) monoïdes
c) inverse
d) inverse du produit
e) cas commutatif

II. Groupes

16.9 16.16 16.32

1) Définition

2) Exemples
a) exemples
b) groupe des permutations d'un ensemble
c) groupe produit

3) Sous-groupes
a) définition
b) caractérisation
c) exemples

4) Sous-groupe engendré
a) définition
b) groupes cycliques

III. Morphismes de groupes

16.27 ⚓
16.22 ⚓🔗
16.20 🔗

1) Définitions

a) morphismes
b) diagrammes

2) Composition des morphismes

3) Exemples

4) Tirés-en-arrière et poussés-en-avant des sous-groupes

5) Noyau d'un morphisme

a) définition

Définition 10.1
Soient G et G' deux groupes, dont on note e_G et $e_{G'}$ les neutres respectifs.
Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes.
Le noyau de φ, noté $\mathsf{Ker}(\varphi)$, est le sous-groupe de G défini par

$$\boxed{\mathsf{Ker}(\varphi) := \Big\{ x \in G \;\Big|\; \varphi(x) = e_{G'} \Big\}.}$$

b) caractérisation de l'injectivité d'un morphisme

Proposition 10.2 Ⓣ
Soit $\varphi : G \longrightarrow G'$ un morphisme de groupes. Alors,

$$\varphi \text{ est injectif} \iff \mathsf{Ker}\,\varphi = \{e_G\}.$$

6) Image d'un morphisme

7) Isomorphismes

a) isomorphismes de groupes
b) automorphismes de groupes
c) groupes isomorphes
d) exemples

chapitre 10 :
Groupes

I Lois de composition interne

a) déf :

Soit E un ensemble,
une loi de composition interne sur E est une application de E^2 dans E

Rég : Si $E^2 \longrightarrow E$ est une loi
On notera en général $x*y := m(x,y)$
on dira alors $\forall x,y : x*y \in E$

On notera aussi $xy := x \cdot y$

Rq : s'il y a ambiguité on notera $x \top y$

Exemples de lci :
L'addition sur $\mathbb{R}$ (c'est $\mathbb{R}^2 \longrightarrow \mathbb{R}$, $(x,y) \longrightarrow x+y$)
De même l'addition, on considère $E^2 \to E$, $(x,y) \to x$
De même sur $\mathbb{C}$ sur $[1;n]$

- sur $\mathcal{P}(E)$: $\mathcal{P}(E)^2 \to \mathcal{P}(E)$, $(A,B) \mapsto A \cap B$
- sur $\mathcal{F}(E,E)$, la composée $(f,g) \mapsto f \cdot g$

Sur $M_{n,p}(\mathbb{R})^2 \longrightarrow M_{n,p}(\mathbb{R})$

$(M,N) \longmapsto M+N$

Lincoln

Dans $M_{2,3}(\mathbb{R})$: $\begin{pmatrix}1&2&3\\1&5&6\end{pmatrix} + \begin{pmatrix}6&5&1\\3&2&1\end{pmatrix}$

$= \begin{pmatrix}7&7&7\\7&7&7\end{pmatrix}$

Sur $M_n(\mathbb{R})$

Dans $M_3(\mathbb{R})$ $\begin{matrix}1&2&3\\4&5&6\\2&8&\end{matrix}$ $=$ $\begin{pmatrix}5&2&1\\1&5&4\\7&8&7\end{pmatrix}$

Si $(\mathbb{R}_+^*)^{\mathbb{R}^2} = \mathbb{R}^*$

$(x+y)$ $\quad \mathbb{C}^2$ dans

Rq^* : une

Sur $\mathbb{R}_+^*$: $(\mathbb{R}_+^*)^2 \longrightarrow \mathbb{R}_+^*$

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

sur $\mathbb{C}$ $\quad \mathbb{C}^2 \longrightarrow \mathbb{C}$

$z, z' \quad |z+z'|$

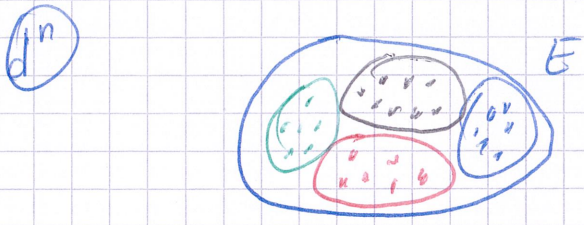
Rq^* une Pcl c'est $E^2 \longrightarrow E$

une relation c'est $E^2 \longrightarrow \{oui, non\}$

5) Une remarque

Soit E muni d'une relation d'équivalence R

Alors les classes d'équivalences de E par R forme une partition de E



Ie : $\forall A \in E/R,\ A \neq \emptyset$

$\forall A, B \in E/R,\ A \neq B \Rightarrow A \cap B = \emptyset$

On a $\bigcup_{A \in E/R} A = E$

b) magmas

Def: On dit que $(E, \cdot)$ est un magma où $\cdot$ est une lci sur E

2 Associativité

a) def

Soit E un ensemble

Def: Soit $\cdot$ une lci sur E on dit que $\cdot$ est associative ssi

$\forall x, y, z \in E,\ x \cdot (y \cdot z)$

Exemple

- L'addition dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathcal{M}_{n,p}(\mathbb{R}\ldots)$

Dans $(\mathcal{F}(E,E), \circ)$, la composition est associative

(T) $f \circ (g \circ h) = (f \circ g) \circ h$

- (AF) $(z, z') \mapsto (z + z')$ n'est pas associative

L'exp. ne tire pas

on a $e(x,y) := x^y$, mieux $x * y$

On calcule $e(2, e(1,2)) = 2 * (1 * 2)$

et $(2*1)*2 = (2^1)*2 = 2*2 = 2^2 = 4$

La soustraction ne l'est pas

(car $1-(1-1) = 1$

et $(1-1)-1 = -1$

h) Semi groupes

Déf° : Soit $(E, \cdot)$ un magma. On dit que c'est un semi-groupe ssi $\cdot$ est associative

c) puissances

Soit $(E, \cdot)$ un semi-groupe

Soit $x \in E$ et soit $n \in \mathbb{N}^*$

Alors, on a $x \cdot (x \cdot x) = (x \cdot x) \cdot x$

On note alors $x^2 = x \cdot x$

(On note $(x \cdot x) \cdot x = x^3$)

Tous les [illegible] par qu'on note x^n

De façon générale, on définit x^n

• Très intéressant : les matrices $M \in M_n(\mathbb{R})$ qui sont inversibles par multiplication

Ex : $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est inversible

On sait que $\forall n \in \mathbb{Z}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

On vérifie que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

<u>ccl</u> : dans $(M_2(\mathbb{R}), \times, I_2)$, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est inversible

<u>Ex 2</u>

• $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est non inversible dans $(M_2(\mathbb{R}), \times, I_2)$

(D/ ORPA et on fixe $M \in M_2(\mathbb{R})$ tq

$$O_2 \cdot M = M \cdot O_2 = I_2$$

Donc $O_2 = I_2$ absurde)

• $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est non inversible

(D/ on a $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Astuce $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \begin{pmatrix} b_1 & 0 & \cdots & 0 \\ 0 & b_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_n \end{pmatrix}$

$$= \begin{pmatrix} a_1 b_1 & 0 & & \\ 0 & a_2 b_2 & & \\ & & \ddots & \\ & & & a_n b_n \end{pmatrix}$$

Ex : $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 3 \\ 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 15 \end{pmatrix}$

ORPA et osq $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est inversible dans $(M_2(\mathbb{R}), \times, I_2)$

Fixons $M \in M_2(\mathbb{R})$ tq $M \times \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = I_2$

Donc $M \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Donc $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$: absurde

Rq ⚠ : Dans $(M_2(\mathbb{R}), \times, I_2)$, certaines Matrices ne sont pas inversibles

Mais ! Dans $(M_2(\mathbb{R}), +, O_2)$, toutes les matrices sont inversibles

Ex : l'inverse de $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ dans $(M_2(\mathbb{R}), +, O_2)$ est $\begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix}$: on a bien $\begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} = O_2 \\ \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = O_2 \end{cases}$

Prop : Dans $(M, *, e)$, l'élément e est inversible et $e^{-1} = e$

D/ En effet : $e \cdot e = e$ ∎

Ex : $\cdot\ 0 \times 0 = 0$ $\quad \cdot\ O_{n,p} + O_{n,p} = O_{n,p}$

$\cdot\ 1 \times 1 = 1$ $\quad \cdot\ I_n \times I_n = I_n$

$\cdot\ \emptyset \cup \emptyset = \emptyset$ $\quad \cdot\ Id_E \circ Id_E = Id_E$ $\quad \cdot\ E \cap E = E$

d) inverse du produit

Prop : Soit $(M, \cdot, e)$ un monoïde

Soient $a, b \in \mathbb{M}$. Alors

1) a, b inversibles $\Rightarrow$ $a \times b$ inversible

2) Dans ce cas, on a $(ab)^{-1} = b^{-1} \cdot a^{-1}$

D/ Osq a, b inversibles

- On calcule

$$(ab) \cdot b^{-1} \cdot a^{-1} = a(bb^{-1})a^{-1} = aea^{-1}$$
$$= aa^{-1} = e$$

- et de même :

$$b^{-1}a^{-1}(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

Ainsi, par déf° : ab est inversible et son inverse est $b^{-1}a^{-1}$.

Ie, on a $(ab)^{-1} = b^{-1}a^{-1}$ ■

e) Cas commutatif !!

Quand on travaille dans un monoïde commutatif au lieu de noter $(M, \cdot, e)$, on note $(M, +, 0)$ ou $(M, +, 0_M)$

Et, si $x \in \mathbb{M}$ est inversible, son inverse est noté $-x$

enfin, si $n \in \mathbb{N}^*$, on note

$$nx := \underbrace{x + x + \dots + x}_{n \text{ fois}}$$

f) Rq finale

Dans $(M, \cdot, e)$, si $x \in M$, on pose $x^0 := e$

II Groupes

1) Définition

déf : Un groupe est un monoïde $(G, \cdot, e)$ où tous les éléments sont inversibles

2) Exemples

a) exemples

- $(\mathbb{Z}, +, 0)$
- $(\mathbb{N}, +, 0)$ n'est pas un groupe
- $(\mathbb{R}^*, \times, 1)$
- $(M_2(\mathbb{R}), +, 0_2)$,
- Plus généralement, $(M_{n,p}(\mathbb{R}), +, 0_{n,p})$

b) groupes des permutations

Soit E un ensemble

On note S_E ou $\mathfrak{S}_E$ l'ensemble des bijections

de E dans E

Prop-def

Le tripet $(\mathfrak{S}, \circ, Id_E)$ est un groupe appelé groupe des permutations de E

D/ · Déjà, on a bien $\mathfrak{S}_E \times \mathfrak{S}_E \longrightarrow \mathfrak{S}_E$

$(f, g) \longmapsto f \circ g$

car la composée ~~de~~ de 2 bij est bij

· Ensuite, on a $Id_E \in \mathfrak{S}$ et $\forall f \in \mathfrak{S}_E$

$$\begin{cases} f \circ Id_E = f \\ Id_E \circ f = f \end{cases}$$

· Donc Id_E est un neutre dans $\mathfrak{S}$ pour $\circ$

· Enfin, si $f \in \mathfrak{S}_E$, il existe $g \in \mathfrak{S}_E$ tq

$$g \circ f = Id_E \quad \text{et} \quad f \circ g = Id_E$$

Ie, toute $f \in \mathfrak{S}_E$ est inversible dans $(\mathfrak{S}_E, \circ, Id_E)$

c) groupe produit

Soient $(G_1, \cdot, e_1)$ et $(G_2, *, e_2)$ deux groupes

On considère $G_1 \times G_2$ qu'on munit d'une loi en posant $(x_1, x_2) \circledast (y_1, y_2) := (x_1 \cdot y_1, x_2 * y_2)$

$\in G_1$ $\in G_2$ $\in G_1$ $\in G_2$ $\in G_1 \times G_2$

Prop-def :

1) Ce triplet $(G_1 \times G_2, \circledast, (e_1, e_2))$ est un groupe

2) Si $(x, y) \in G_1 \times G_2$, l'inverse de (x, y) pour $\circledast$ est (x^{-1}, y^{-1})

3) C'est le groupe produit de $(G_1, \cdot, e_1)$ et $(G_2, *, e_2)$

Rq !! : Au lieu de noter $(G, \cdot, e)$, on note souvent $(G, \cdot)$ voire même G

3) Sous-groupes

a) définition

Déf : Soit $(G, \cdot, e)$ un groupe

Soit $H \subseteq G$

On dit que H est un sous groupe de G $\overset{\Delta}{\text{si}}$

$$\begin{cases} \forall x, y \in H, \ xy \in H \\ \forall x \in H, \ x^{-1} \in H \end{cases} \quad \text{et !} \quad e \in H$$

On note $H \ \text{sgr} \ G$

Rq : Soit G un groupe et soit $H \ \text{sgr} \ G$
Alors, l'application $\cdot : G \times G \longrightarrow G$ peut être restreinte à $H \times H$, on obtient

- $\cdot|_{H\times H} : H\times H \longrightarrow G$

Ĉ Hsgr G, on a $\forall x,y \in H,\ x\cdot y \in H$

Donc $\cdot|_{H\times H}$ est corestreignable à H

On obtient $\cdot|_{H\times H}^{H} : H\times H \longrightarrow H$

Fait : $\left(H, \cdot|_{H\times H}^{H}, e\right)$ est un groupe

D/ ok ■

CCL : H sgr G $\Longrightarrow$ H groupe

b) caractérisation

Soit G groupe et soit $H \subset G$ non vide.

Prop :

$$H \text{ sgr } G \Longleftrightarrow \forall x,y \in H,\ xy^{-1} \in H$$

D/ $\boxed{\Longrightarrow}$ c'est plutôt facile Soient $x,y \in H$

Je sais que $y^{-1} \in H$ Ĉ aussi : $x \in H$, on a $x \in H$, on a $xy^{-1} \in H$

[or H non vide : fixons donc $x_0 \in H$
On a $x_0 \cdot x_0^{-1} \in H$] Hs

($\Leftarrow$) Osq $\forall x, y \in H$, $xy^{-1} \in H$

· Déjà, $e \in H$. En effet, $\hat{C}$ $H \neq \emptyset$, fixons $x_0 \in H$

On a $x_0 \cdot x_0^{-1} \in H$ ie $\boxed{e \in H}$

· Soient $x, y \in H$

* $\hat{C}$ $e \in H$, on a $e y^{-1} \in H$ ie $y^{-1} \in H$

* Donc, on a $x (y^{-1})^{-1} \in H$

* Or $(y^{-1})^{-1} = y$

* Donc: $xy \in H$ ■

Rq: on avait oublié de dire que

$\forall x \in G$, $(x^{-1})^{-1} = x$

si G groupe

(D/ (exo) + généralisable)

c) exemples

· $\mathbb{R}_+^*$ sgr $(\mathbb{R}^*, \times, 1)$

· $\mathbb{Q}$ sgr $(\mathbb{R}^*, \times, 1)$

D/ : $1 \in \mathbb{Q}$

$\forall x, y \in \mathbb{Q}$, $xy \in \mathbb{Q}$

si $x \in \mathbb{Q}$, $x^{-1} \in \mathbb{Q}$

- $\mathbb{Q}_+^*$ sgr $\mathbb{Q}^*$ sgr $\mathbb{R}^*$

exo Soit G un groupe. Soient H et K des sous-groupes de G

Alors $H \cap K$ sgr G.

(+ gén : si $(H_i)_{i \in I}$ est une famille de sgr de G alors $\bigcap_{i \in I} H_i$ sgr G)

- $\{-1, 1\}$ sgr $(\mathbb{R}^*, \cdot, 1)$
- $\{1\}$ sgr $(\mathbb{R}^*, \cdot, 1)$

Fait : $\{e\}$ sgr G, et G sgr G

- $\mathbb{R}^*$ sgr $(\mathbb{C}^*, \cdot, 1)$
- $\mathbb{U}_n$ sgr $(\mathbb{C}^*, \cdot, 1)$

D/ $1 \in \mathbb{U}_n$

$\cdot$ $w, w' \in \mathbb{U}_n \Rightarrow ww' \in \mathbb{U}_n$

$w \in \mathbb{U}_n \Rightarrow w^{-1} \in \mathbb{U}_n$ ■

- $\mathbb{U}$ sgr $(\mathbb{C}^*, \cdot, 1)$

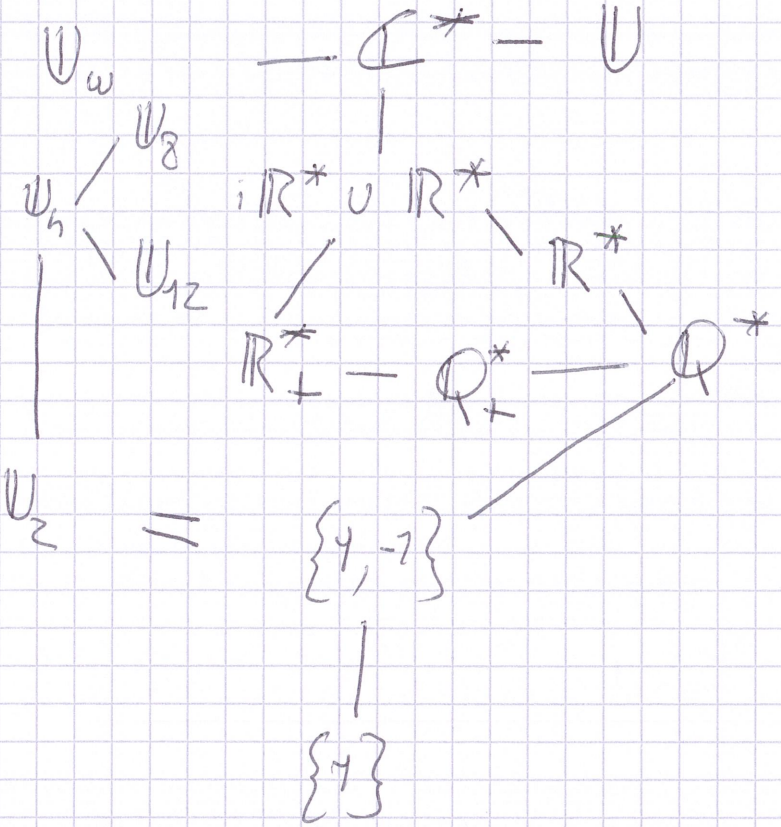
exo $\frac{*}{2}$ on note ~~$\mathbb{U}_\omega$ sgr $\mathbb{U}$~~

$$\mathbb{U}_\omega := \bigcup_{n \geq 1} \mathbb{U}_n$$

Mq $\mathbb{U}_\omega$ sgr $\mathbb{U}$

. $i\mathbb{R}^* \cup \mathbb{R}^*$ sgr $(\mathbb{C}^*, \times, 1)$

ccl



4) Sous groupe engendré

Soit G un groupe

Soit $X \subset G$

But : trouver le sous-groupe de G engendré par X

a) point de vue interne

On pose $\langle X \rangle := \left\{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \,,\, \begin{cases} n \in \mathbb{N} \\ x_1, \dots, x_n \in X \\ \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\} \end{cases} \right\}$

$$\langle X \rangle := \left\{ x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \;\middle/\; \begin{array}{l} n \in \mathbb{N} \\ x_1, \dots, x_n \in X \\ \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\} \end{array} \right\}$$

Prop : $\langle X \rangle$ sgr G

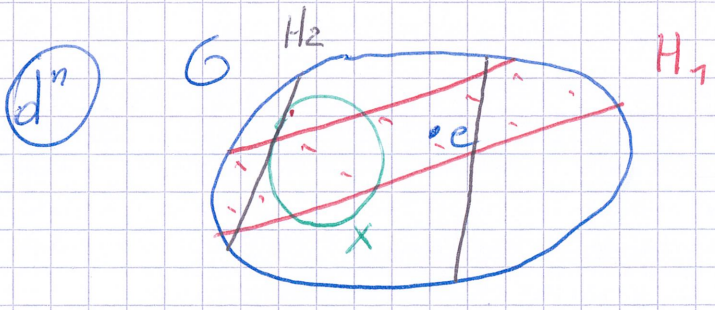
On l'appelle sous-groupe de G engendré par X

D/ À l'oral ■

- pour $n = 0$ $\prod_{i=0}^{0} x_i^{\varepsilon_i} = 1$

b) point de vue externe

On pose $\langle X \rangle := \bigcap_{\substack{H \text{ sgr } G \text{ tq} \\ X \subset H}} H$



Prop 1 : $\langle X \rangle$ est le ④ petit sgr G qui contient X

D/ • Déjà, $\prec X \succ$ sgr G : cf (exo) $\bigcap_{i \in F} H_i$

• Soit H_0 sgr G tq $X \subset H_0$

On a $\bigcap_{H \text{ sgr } G,\ X \subset H} H \subset H_0$ donc $\prec X \succ \subset H_0$ ■

Prop 2 : $\langle X \rangle = \prec X \succ$

D/ (AC) * ■

c) groupe cyclique

Déf : Soit G un groupe. On dit que

G est cyclique $\overset{\Delta}{\text{ssi}}$

$\exists\, x_0 \in G : G = \prec \{x_0\} \succ$

Exemples

• $(\{1\}, \times, 1)$ ← "groupe nul" est cyclique

• $(\{1,-1\}, \times, 1)$ ie $\mathbb{U}_2$ est cyclique, engendré par -1

• $\mathbb{U}_n$ est cyclique par $e^{2i\pi/n}$

• $(\mathbb{Z}, +, 0)$ est cyclique, engendré par 1

Si G est cyclique engendré par a, on a

$$G = \{a^n,\ n \in \mathbb{Z}\}$$

Ex** : $\mathbb{U}$ n'est pas cyclique car $\mathbb{U} \not\cong \mathbb{N}$

de même $(\mathbb{R}, +, 0)$ n'est pas cyclique

III Morphismes de groupes

1) définitions

a) morphismes

Déf : Soient $(G, \cdot, e_G)$ et $(H, *, e_H)$ deux groupes. Soit $\varphi : G \to H$

On dit que φ est un morphisme de groupes

ssi $\forall x, y \in G,\ \varphi(\underbrace{x \cdot y}_{\in G \text{ Pci de } G}) = \underbrace{\varphi(x)}_{\in H} * \underbrace{\varphi(y)}_{\text{Pci de } H}$

Rq : • On note $\mathrm{Hom}_{(Gr)}(G, H)$ l'ensemble des morphismes de G dans H

(ancien nom : Homo morphisme)

• Si $\varphi : G \to G$ morphisme, on dit que φ est un endo morphisme de G

on note $\mathrm{End}_{(Gr)}(G)$

Prop ⓣ : φ iso $\Rightarrow$ φ^{-1} $H \to G$ morphisme

D/ Mq $\forall \alpha, \beta \in H$, $\varphi^{-1}(\alpha\beta) = \varphi^{-1}(\alpha)\varphi^{-1}(\beta)$

Soient $\alpha, \beta \in H$ (R^x) Je les ecris

$\alpha = \varphi(x)$, $\beta = \varphi(y)$ avec $x, y \in G$

On a $\varphi(x) \cdot \varphi(y) = \varphi(xy)$

Ie $\alpha \cdot \beta = \varphi(xy)$

Donc $\varphi^{-1}(\alpha, \beta) = \varphi^{-1}(\varphi(xy))$ ie $\varphi^{-1}(\alpha\beta) = xy$

Ĉ $\alpha = \varphi(x)$, on a $\varphi^{-1}(\alpha) = \varphi^{-1}(\varphi(x))$ donc

$x = \varphi^{-1}(\alpha)$

De m̂ : $y = \varphi^{-1}(\beta)$

<u>ccl</u> : $\varphi^{-1}(\alpha\beta) = \varphi^{-1}(\alpha)\varphi(\beta)$ ■

b) automorphisme

<u>Déf°</u> : un auto morphisme φ de G est un isomorphisme de G dans G

On note $Aut_{(Gr)}(G)$ l'ens des auto morphismes de

c)

<u>Déf</u> : Soient G, H deux groupes

On dit que G et H sont isomorphes et on note $G \cong H$ $\underset{ssi}{\Leftrightarrow}$ $\exists \varphi : G \to H$ iso

d) exemples

b) Caractérisation de l'injectivité d'un morphisme

Soit $\varphi : G \longrightarrow H$ morphisme entre deux groupes

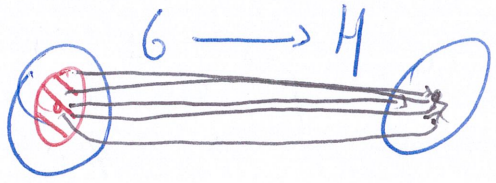
Prop : φ inj $\Longleftrightarrow \ker \varphi = \{e_G\}$

Rqs : On a $\ker \varphi$ sgr G ; en effet, $\ker \varphi$ est le tiré en arrière d'un sous groupe de H et cf § précédent

Donc, on a toujours $e_G \in \ker \varphi$

en gq sorte, "$\ker \varphi$ mesure le défaut d'injectivité de φ"

cf d°



D/ $\Longrightarrow$ Osq φ inj, Mq $\ker \varphi = \{e_G\}$

Déjà, on a $\{e_G\} \subset \ker \varphi$ (toujours)

Soit $x \in \ker \varphi$, on a $\varphi(x) = e_H$

or $e_H = \varphi(e_G)$ donc $\varphi(x) = \varphi(e_G)$

or φ inj, donc $x = e_G$

(⇐) Osq $\ker \varphi = \{e_G\}$

Mq φ inj Soient $x, y \in G$ tq $\varphi(x) = \varphi(y)$

Mq $x = y$

Notons $\alpha := \varphi(x) = \varphi(y)$

On a $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = \alpha\alpha^{-1} = e_H$

Donc $xy^{-1} \in \ker \varphi$

or $\ker \varphi = \{e_G\}$ donc $xy^{-1} = e_G$

Donc $xy^{-1}y = e_G y$ donc $x = y$ ∎

6) Image d'un morphisme

Déf : Soit $\varphi : G \longrightarrow H$ un morphisme

L'image de φ, noté $\mathrm{Im}(\varphi)$, est le sous groupe de H défini par $\mathrm{Im}(\varphi) := \varphi[G]$

7) !! Isomorphismes

a) isomorphismes

Déf : Soit $\varphi : G \longrightarrow H$ un morphisme

On dit que φ est un isomorphisme $\overset{\Delta}{\text{ssi}}$ φ bijectif

Soient $\alpha, \beta \in \varphi[G']$ qu'on écrit

$\alpha = \varphi(x)$ et $\beta = \varphi(y)$ avec $x, y \in G'$

Comme $G' \leq G$, on a $xy^{-1} \in G'$

donc $\varphi(xy^{-1}) \in \varphi[G']$

or $\varphi(xy^{-1}) = \varphi(x) \cdot \varphi(y^{-1}) = \alpha \cdot \beta^{-1}$

on a bien montré que $\alpha\beta^{-1} \in \varphi[G']$ ■

5) Noyau d'un morphisme

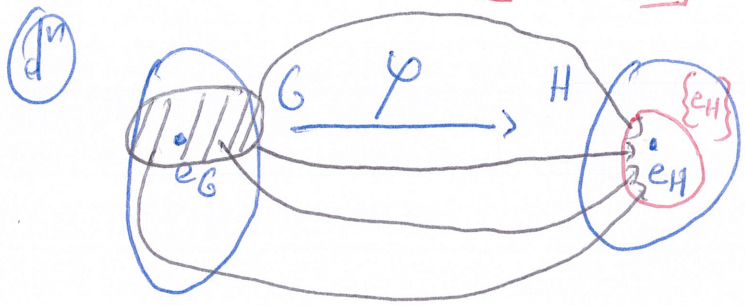
a) def°

Def: Soit G, H deux groupes

Soit $\varphi : G \longrightarrow H$ un morphisme

Le noyau de φ est le sous groupe de G, noté $\ker\varphi$, défini par

$$\ker\varphi = \varphi^{\langle -1 \rangle}[\{e_H\}]$$



Donc $\ker\varphi = \{x \in G \mid \varphi(x) = e_H\}$

Soient $x, y \in \varphi^{\langle -1 \rangle}[H']$

Mq $xy^{-1} \in \varphi^{\langle -1 \rangle}[H']$

On a $x \in \varphi^{\langle -1 \rangle}[H']$ Donc $\varphi(x) \in H'$

De même, $\varphi(y) \in H'$

Donc, $\hat{C}$ $H' \text{ sgr } H$, on a $\varphi(y)^{-1} \in H'$

or $\varphi(y)^{-1} = \varphi(y^{-1})$

Ainsi, on a $\varphi(x), \varphi(y^{-1}) \in H'$

or $H' \text{ sgr } H$ Donc

$\varphi(x) \cdot \varphi(y^{-1}) \in H'$

Ie $\varphi(xy^{-1}) \in H'$

Ie (RM) $xy^{-1} \in \varphi^{\langle -1 \rangle}[H']$ ✓

2) Mq $\varphi[G'] \text{ sgr } H$

Mq $e_H \in \varphi[G']$

$\hat{C}$ $G' \text{ sgr } G$, on a $e_G \in G'$

Donc $\varphi(e_G) \in \varphi[G']$

or $\varphi(e_G) = e_H$

D'où $e_H \in \varphi[G']$

Mq $\forall \alpha, \beta \in \varphi[G']$, $\alpha\beta^{-1} \in \varphi[G']$

Soit E ens

$$(\mathcal{P}(E), \cap, E) \longrightarrow (\mathcal{F}(E, \{0,1\}), \times)$$
$$A \longmapsto \mathbb{1}_A$$

(D/ $\mathbb{1}_{A\cap B} = \mathbb{1}_A \times \mathbb{1}_B$) est un morphisme de monoïdes

4) Tirés en arrière, poussés-en-avant des sgr

On considère $G \xrightarrow{\varphi} H$

G' sgr de G, H' sgr de H

avec G, H groupe et φ morphisme

Prop : 1) $\varphi^{(-1)}[H']$ sgr G

2) $\varphi[G']$ sgr H

D/ : 1) Mq $e_G \in \varphi^{(-1)}[H']$

Ie Mq $\varphi(e_G) \in H'$

Ĉ φ est un morphisme, on a $\varphi(e_G) = e_H$

De plus Ĉ H' sgr H, on a $e_H \in H'$

Donc, on a $\varphi(e_G) \in H'$ ie $e_G \in \varphi^{(-1)}[H']$

donc $\varphi^{(-1)}[H'] \neq \emptyset$

Mq $\forall x, y \in \varphi^{(-1)}[H'], xy^{-1} \in \varphi^{(-1)}[H']$

D/ $\exp(a+b) = \exp(a) \times \exp(b)$

D/ $\frac{1}{a \times b} = \frac{1}{a} \cdot \frac{1}{b}$

- $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$

D/ $\ln(ab) = \ln(a) + \ln(b)$

- $\sqrt{\cdot} : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}_+^*, \times)$

D/ $\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$

$(\cdot)^2 : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ n'est pas un morphisme

ie $(a+b)^2 \neq a^2 + b^2$

- $\left(\mathcal{C}([0;1], \mathbb{R}), +, \tilde{0}\right) \longrightarrow (\mathbb{R}, +, 0)$

$I : f \longmapsto \int_0^1 f(t)\,dt$

D/ $I(f+g) = I(f) + I(g)$

On dit que $I(\cdot)$ est additive

- $(\mathbb{Z}, +, 0) \longrightarrow (\mathbb{R}_+^*, \times, 1)$

$n \longmapsto 2^n$

D/ $2^{n+m} = 2^n 2^m$

Soit $a \in \mathbb{C}^*$, j'ai : $(\mathbb{Z}, +) \longrightarrow (\mathbb{C}^*, \times)$

$n \longmapsto a^n$

$(\mathbb{R}, +) \longrightarrow (\mathbb{U}, \times)$

$\theta \longmapsto e^{i\theta}$

D/ $e^{i(\theta+\theta')} = e^{i\theta} \cdot e^{i\theta'}$

2) Composition des morphismes

Soient G, H, K trois groupes

Soient $\varphi : G \to H$ et $\psi : H \to K$ des applications

Prop : $\left.\begin{array}{l}\varphi \text{ morphisme} \\ \psi \text{ morphisme}\end{array}\right\} \Rightarrow \psi \circ \varphi$ morphisme

D/ ⚓++

Je note $*_G$, $*_H$ et $*_K$ les lois de G, H et K

Mq $G \xrightarrow{\varphi} H \xrightarrow{\psi} K$ (avec $\psi \circ \varphi$) est un morphisme

Soient $x, y \in G$. On calcule :

$(\psi \circ \varphi)(x *_G y)$

def° de "∘" ↘

$= \psi(\varphi(x *_G y)) = \psi(\varphi(x) *_H \varphi(y))$

$= \psi(\varphi(x)) *_K \psi(\varphi(y))$

$= \psi \circ \varphi(x) *_K \psi \circ \varphi(y)$

3) Exemple

- $\exp : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_+^*, \times, 1)$

  Qu'on peut noter $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$

- $\frac{1}{\cdot} : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$

D/. ~~Soit $x \in G$~~

On a $\varphi(e_G \cdot e_G) = \varphi(e_G) * \varphi(e_G)$

d'où $\varphi(e_G) = \varphi(e_G) * \varphi(e_G)$

On a $\varphi(e_G) \in H$ Notons $y_0 := \varphi(e_G)$

on a $y_0 * y_0 = y_0$

Or H est un groupe donc y_0 est inversible :

On dispose de y_0^{-1} On a alors

$$(y_0 * y_0) * y_0^{-1} = y_0 * y_0^{-1}$$

$$y_0 (y_0 * y_0^{-1}) = e_H$$

$$y_0 * e_H = e_H$$

donc $y_0 = e_H$

donc $\varphi(e_G) = e_H$

Soit $x \in G$. On a $\begin{cases} x \cdot x^{-1} = e_G \\ x^{-1} \cdot x = e_G \end{cases}$ $(**)$

je passe $(**)$ à $\varphi(\cdot)$

donc $\begin{cases} \varphi(x) * \varphi(x^{-1}) = \varphi(e_G) = e_H \\ \varphi(x^{-1}) * \varphi(x) = e_H \end{cases}$

- Donc, par déf° : $\varphi(x^{-1})$ est l'inverse de $\varphi(x)$ dans H pour $*$
- Ie, on a $\varphi(x)^{-1} = \varphi(x^{-1})$ ■

erreur def : groupe cyclique à remplacer par groupe monogène

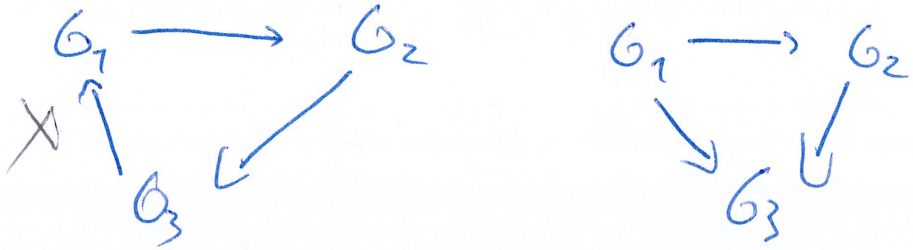
Rq : On dit q G est cyclique $\overset{\Delta}{ssi}$ G est monogène et fini

On dit que G est un groupe abélien $\overset{\Delta}{ssi}$ G est un groupe commutatif

b) diagrammes

Un diagramme de groupe est la donnée de groupes reliés par des morphismes

Ex :



On dit qu'il commute $\overset{\Delta}{ssi}$ le diagramme d'ensemble sous-jacent commute.

c) propriétés

Soient G, H deux groupes

Soit $\varphi : G \to H$ un morphisme.

Prop : on a $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$

Prop 2 : On a $\varphi(e_G) = e_H$

4) exemples → voir ci dessus

5) neutre

a) déf

Def : Soit $(E, \cdot)$ un semi groupe
ie soit E un ens muni d'une LCI associative

Soit $e \in E$. On dit que e est un neutre de E par ! si

$$\forall x \in E, \quad x \cdot e = x \quad \text{et} \quad e \cdot x = x$$

Prop : Le neutre s'il existe, est unique

D/ Soient

(ici associative) E un ens muni d'une LCI

Soient e_1, e_2 deux neutres de E pour $\cdot$. Alors, on a

$e_1 \cdot e_2 = e_1$ car e_2 est neutre

$e_1 \cdot e_2 = e_2$ car e_1 est neutre

donc $e_1 = e_2$

$(\mathbb{N}^*, \perp)$ on note R de la loi x ⊛

La loi ⊛ est associative ie (1)

Fait Soit $(E, \cdot)$ un semi groupe

// $x \in E$

Alors $\forall n, m \in \mathbb{N}^*, x^n \cdot x^m = x^{n+m}$

D/ bon ▨

3) Commutativité

def : Soit une loi sur E

On dit que $\cdot$ est commutative

ssi $\forall x, y \in E, x \cdot y = y \cdot x$

Ex

* Le prod matriciel $=$ ¬ commutatif

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

mais $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

dc : $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$

* compo ¬ commutative

x = inversible ⟺ ∃ y

Pg Ri On se plo Alors

on est tous ⟺

$f \circ g = Id_E$

exo

f inv à droite ⟺

Prq : unicité

Soit x ∈ M Soient Y_1, Y_2 tq

Alors $Y_1 = Y_2$

Def Soit x ∈ A

$\begin{cases} x \cdot y = \\ y \cdot x = \end{cases}$

On

$g \circ f = I$

on le note

Exemples

$(\mathbb{N}, +, 0)$, $(\mathcal{F}(E,E), \circ, Id_E)$

$(M_{pp}(\mathbb{R}), +, 0_M)$, $(\mathcal{P}(E), \cap, E)$

$(\mathcal{P}(E), \cup, \emptyset)$, $(M_n(\mathbb{R}), \times, I_n)$ $(\mathbb{R}, \times, 1)$

c) inverse

Soit $(M, *, e)$ un monoide

Def^{0} : Soit $x \in M$ on dit que x est

inversible donc ssi

$\exists y_d \in M : x y_d = e$

$\exists y \in M : y_g x = e$

Dm $\{ x \overset{?}{=} y$

x ...

y ...

puis ole ...

Prop

Ex

Soit b est inversible

Dans $(\mathbb{Z}, +, 0)$

Il le mot inverse

Cf le mot

On a

l'inverse de 8 par + de $\mathbb{Z}$ est -8 car $8 + (-8) = 0$

$(-8) + 8 = 0$

Dans $(\mathbb{R}, \times, 1)$: Soit $x \in \mathbb{R}$

A-t-on un $y \in \mathbb{R}$ tq $xy = yx = 1$

On a x inversible dans $\mathbb{R}$ par x

$\Leftrightarrow$ $x \neq 0$

Dans $(\mathcal{P}(E), \cap, \subset)$ soit $A \subset E$

Alors on a $B \subset E$ tq $A \cap B = B \cap A = \emptyset$

Alors on a $B \subset E$ tq $A \cap B$