

Chapitre 10

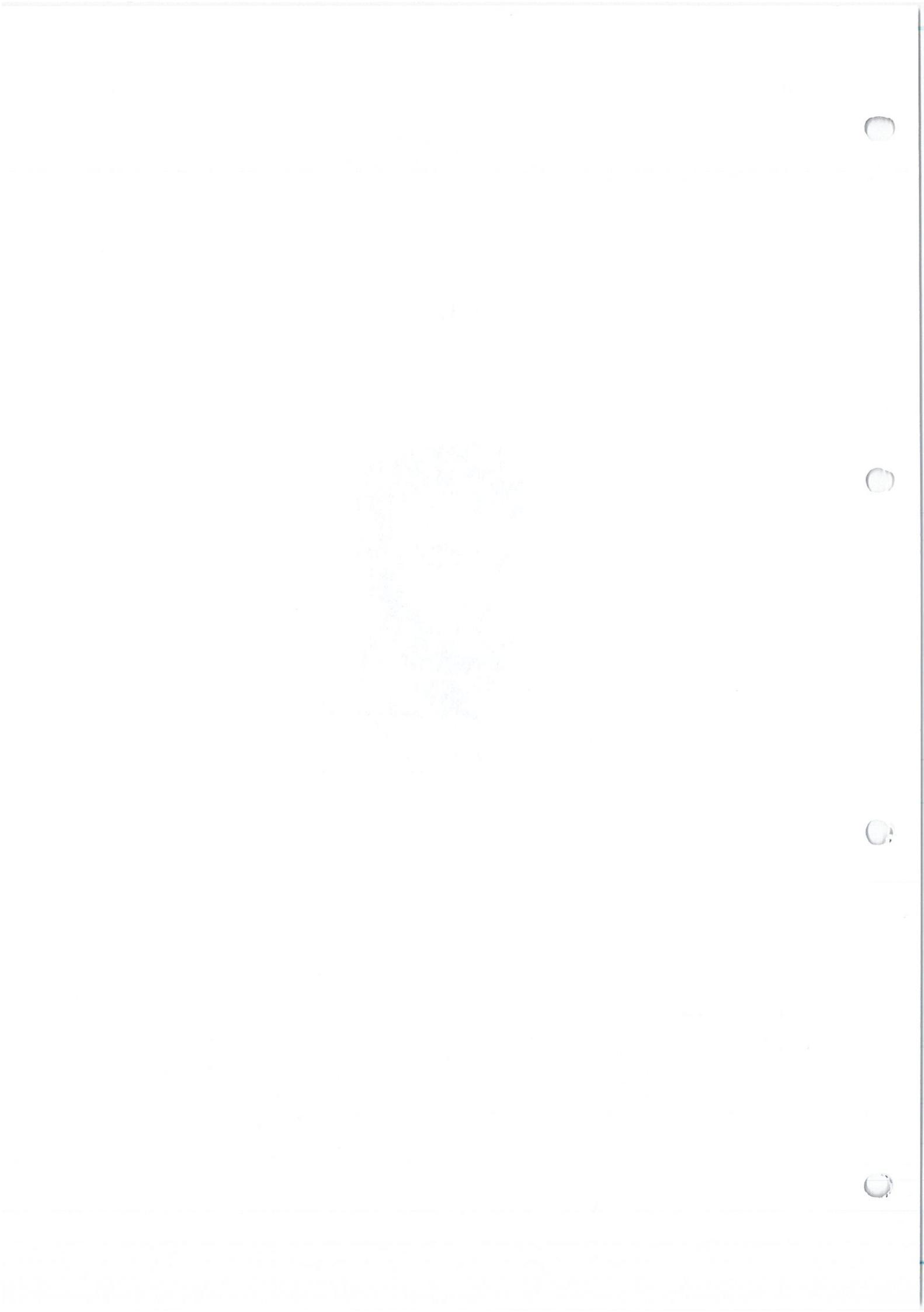
Groupes



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.



CHAPITRE 10

Groupeo.I) Lois de composition internes.1) Lois de composition internes.a) Définition.Définition:

Soit E un ensemble. Une loi de composition interne (LCI) sur E est une application de E^2 dans E .

!!!

remarque:

Si $m: E^2 \rightarrow E$ est une loi sur E et si $x, y \in E$ on notera en général $x \cdot y := m(x, y)$

On a alors $\forall x, y \in E$, $x \cdot y \in E$

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

remarque:

S'il y a ambiguïté, on notera $x * y$ ou $x \star y$ ou $x \otimes y$, etc.

exemples de loi:

- l'addition sur \mathbb{R} (c'est $\mathbb{R}^2 \rightarrow \mathbb{R}$)

$$(x, y) \mapsto x + y$$

- De même, l'addition sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$.

- Si E un ensemble, on considère $E^2 \rightarrow E$

$$(x, y) \mapsto x$$

- Sur $\mathcal{P}(E)$: l'intersection ie $\mathcal{P}(E)^2 \rightarrow \mathcal{P}(E)$

$$(A, B) \mapsto A \cap B$$

de même, l'union.

- sur $\mathcal{F}(E, E)$, la composition. C'est $\mathcal{F}(E, E)^2 \rightarrow \mathcal{F}(E, E)$

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

- Sur $M_{n,p}(\mathbb{R})$, j'ai l'addition. C'est

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

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

D'" n lignes, p colonnes"

$$\text{Dans } M_{2,3}(\mathbb{R}): \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} + \begin{pmatrix} 6 & 5 & 4 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 7 & 7 \\ 7 & 7 & 7 \end{pmatrix}$$

- Sur $M_n(\mathbb{R})$, le produit

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

$$\text{Dans } M_3(\mathbb{R}): \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 5 & 2 & 1 \\ 11 & 5 & 4 \\ 17 & 8 & 9 \end{pmatrix}$$

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

$$(\alpha, \gamma) \longmapsto \alpha^\gamma$$

- Sur \mathbb{C} : $\mathbb{C}^2 \longrightarrow \mathbb{C}$

$$(z, z') \longmapsto |z + z'|$$

- la soustraction dans \mathbb{Z}

remarque:

- une loi c'est $E^2 \rightarrow E$

- une relation c'est $E^2 \rightarrow \{\text{oui}, \text{non}\}$

(or oui, non) $\approx \{0, 1\}$ et $\mathcal{F}(E, \{0, 1\}) \cong \mathcal{P}(E)$ cf 9.4)

b) Magmas.

Définition:

Un magma est un couple (E, \cdot) où \cdot est une loi sur E .

2) Associativité:

a) Définition:

Soit E un ensemble.

Définition:

Soit \cdot une loi sur E . On dit que \cdot est associative si

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

exemples :

- l'addit° (dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}, M_{n,p}(\mathbb{R}) \dots$) l'est

- Dans $F^*(E, E)$, la composition est associative :

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

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

- d'exponentiation ne l'est pas

- \circledast On note $e(x, y) := x^y$; mieux $x \otimes y$

$$\text{On calcule } e(2, e(1, 2)) = 2 * (1 \otimes 2) = 2 \otimes (1^2) = 2 \otimes 1 = 2^1 = 2$$

$$\text{Et } (2 * 1) * 2 = (2^1) \otimes 2 = 2 \otimes 2 = 2^2 = 4$$

- La soustraction ne l'est pas :

$$(1 - (1 - 1)) = 1 \quad \text{et} \quad (1 - 1) - 1 = -1$$

b) Semi-groupes

Définition:

Soit (E, \cdot) un magma. On dit que c'est un semi-groupe si \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 cet élément x^3

On note aussi $x^2 := x \cdot x$

On a $(x \cdot x) \cdot (x \cdot x) = x \cdot (x \cdot (x \cdot x)) = x \cdot ((x \cdot x) \cdot x) = \dots$

tous les parenthèses possibles donnent le même résultat, qui on note x^4 .

De façon générale, on définit α^n . Comme tous les parenthèses donnent le même résultat, on écrit

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdot \dots \cdot \alpha}_{n \text{ fois}}$$

Fait:

Soit (E, \cdot) un semi-groupe

Soit $\alpha \in E$

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

3) Commutativité.

Définition:

Soit \cdot une loi sur E .

On dit que \cdot est commutative \Leftrightarrow

$$\forall \alpha, \gamma \in E, \alpha \cdot \gamma = \gamma \cdot \alpha$$

exemples:

- le produit matriciel n'est pas commutatif.

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

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

$$\therefore \text{ donc } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

- la composition n'est pas commutative !

4) Exemples.

Voir ci-dessous

5) Newton.

a) Définition:

CHAPITRE 10)

3

Définition:

Soit (E, \cdot) un semi-groupe, i.e soit E un ensemble muni d'une loi associative.

Soit $e \in E$. On dit que e est un neutre de E par " \cdot " si " $\forall \alpha \in E, \begin{cases} \alpha \cdot e = \alpha \\ e \cdot \alpha = \alpha \end{cases}$ "

Proposition:

Le neutre s'il existe est unique.

démonstration:

Soit E un ensemble muni de une loi (\cdot ici associative)

Soient $e_1, e_2 \in E$ des neutres de E pour " \cdot ". Alors, on a:

$$\begin{cases} e_1 \cdot e_2 = e_2 \text{ car } e_1 \text{ est un neutre} \\ e_1 \cdot e_2 = e_1 \text{ car } e_2 \text{ est un neutre} \end{cases}$$

Donc $e_1 = e_2$ \square

exemple de semi-groupe sans neutre:

- $(\mathbb{N}^*, +)$

- On munit \mathbb{R} de la loi $\alpha \otimes y = \max(\alpha, y)$. La loi \otimes est associative (\otimes max($\alpha, \max(y, z)$) = max(max(α, y), z) et \otimes est aussi commutative.

mais \mathbb{R} n'admet pas de neutre pour \otimes

démonstration:

ORPQ et on fixe $e \in \mathbb{R}$ un neutre de \mathbb{R} pour \otimes . On a

$$\forall \alpha \in \mathbb{R}, \max(\alpha, e) = \alpha$$

Donc $\max(e-1, e) = e-1$. Donc $e-1 > e$: Absurde \square

exemples de neutres:

- 1 pour (\mathbb{R}, \times)

- $O_{n,p}$ pour $(M_{n,p}(\mathbb{R}), +)$ $O_{n,p}$: matrice avec que des 0

- Id_E pour $(\mathcal{F}(E, E), \circ)$

- I_n pour $(M_n(\mathbb{R}), \times)$

- \emptyset pour $(\mathcal{P}(E), \cup)$

- E pour $(P(E), \cap)$
- O pour $(N, +)$

b) Monoïdes.

Définition:

Un monoïde est un triplet (M, \cdot, e) où M est un ensemble, où \cdot est une loi sur M et où e est un neutre de M pour " \cdot ".

exemples:

- $(N, +, 0)$
- $(\mathcal{F}(E, E), \circ, \text{Id}_E)$
- $(M_{n,p}(IR), +, O_{n,p})$
- $(\mathcal{D}(E), \cap, E)$, $(P(E), \cup, \emptyset)$
- $(M_n(IR), \times, I_n)$
- $(IR, \times, 1)$

c) Inverse.

Soit (M, \cdot, e) un monoïde.

Définition:

Soit $x \in M$. On dit que x est inversible (dans M pour " \cdot ".)

$$\text{soit } \begin{cases} \exists y_d \in M : x \cdot y_d = e & (1) \\ \exists y_g \in M : y_g \cdot x = e & (2) \end{cases}$$

remarque:

Si on a uniquement (1), on dit que x est inversible à droite.

Si on a uniquement (2), on dit que x est inversible à gauche.

Proposition:

$$\text{Soit } x \in M. \text{ Soient } y_d, y_g \in M \text{ tq } \begin{cases} x \cdot y_d = e \\ y_g \cdot x = e \end{cases}$$

CHAPITRE 10

4

Alors $y_d = y_g$

démonstration: pas de parenthèseage car la loi est associative.

$$\text{On a } y_g \cdot \alpha \cdot y_d = (y_g \cdot \alpha) \cdot y_d = e \cdot y_d = y_d$$

$$= y_g \cdot (\alpha \cdot y_d) = y_g \cdot e = y_g \quad \square$$

Proposition: ①

$$\alpha \text{ est inversible} \Leftrightarrow \exists y \in M : \begin{cases} \alpha \cdot y = e \\ y \cdot \alpha = e \end{cases}$$

démonstration:

OK ③

remarque:

On se place dans $(\mathcal{F}(E, E), \circ, \text{Id}_E)$

Soit $f: E \rightarrow E$. Alors, on a:

- f inversible à droite $\Leftrightarrow f \circ g = \text{Id}_E$
- f inversible à gauche $\Leftrightarrow f$ injective
- f inversible $\Leftrightarrow f$ bijective.

exercice: démontrer 2 premières.

Proposition:

unicité de "l'inverse".

Soit $\alpha \in M$. Soient $y_1, y_2 \in M$ tq

$$\begin{cases} \alpha \cdot y_1 = e \\ y_1 \cdot \alpha = e \end{cases} \quad \text{et} \quad \begin{cases} \alpha \cdot y_2 = e \\ y_2 \cdot \alpha = e \end{cases}$$

Alors $y_1 = y_2$.

démonstration:

(AF) + cf plus haut ③

Définition:

Soit $\alpha \in M$ inversible

L'inverse de α (dans M pour ".") est l'unique $y \in M$ tq

$$\begin{cases} \alpha \cdot y = e \\ y \cdot \alpha = e \end{cases}$$

On le note α^{-1}

exemples:

- Dans $(\mathbb{N}, +, 0)$

Soit $a \in \mathbb{N}$. Est-il inversible? A-t-on $\exists b \in \mathbb{N} \text{ tq } \begin{cases} a+b=0 \\ b+a=0 \end{cases}$?

La réponse est non sauf si $a=0$

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

Tous le monde est inversible et l'inverse de 8 pour + dans \mathbb{Z} est -8 car $\begin{cases} 8+(-8)=0 \\ -8+8=0 \end{cases}$

- Dans $(\mathbb{R}, \times, 1)$:

Soit $\alpha \in \mathbb{R}$. A-t-on un $y \in \mathbb{R}$ tq $\alpha y = y \alpha = 1$?

On a α inversible (dans \mathbb{R} pour \times) $\Leftrightarrow \alpha \neq 0$

- Dans $(\mathcal{P}(E), \cap, E)$:

Soit $A \in \mathcal{P}(E)$. A-t-on $B \in \mathcal{P}(E)$ tq $A \cap B = B \cap A = E$?

On a A inversible (pour \cap dans E) $\Leftrightarrow A = E$

- Très intéressant, les matrices $M \in M_n(\mathbb{R})$ qui sont inversibles pour la multiplication.

ex1: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 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

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

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

Conclusion: dans $(M_2(\mathbb{R}), \times, I_2)$, la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est inversible.

ex 2: la matrice $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est non inversible dans $(M_2(\mathbb{R}), \times, I_2)$

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

$$O_2 \cdot M = M \cdot O_2 = I_2 \text{ donc } O_2 = I_2. \text{ Absurde!}$$

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

$$(dem: on a \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix})$$

CHAPITRE 10

Q'astuce: $\begin{pmatrix} a_1 & a_2 & \dots & (0) \\ (0) & \ddots & \ddots & a_n \end{pmatrix} \times \begin{pmatrix} b_1 & b_2 & \dots & (0) \\ (0) & \ddots & \ddots & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & a_2 b_2 & \dots & (0) \\ (0) & \ddots & \ddots & a_n b_n \end{pmatrix}$

$$\text{ex: } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \times \begin{pmatrix} 5 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 15 \end{pmatrix}$$

ORPA et $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 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 $M \times \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

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

!!!

Remarque: 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 $\begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} = O_2 \\ \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = O_2 \end{cases}$

Proposition:

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

En effet: $e \cdot e = e \quad \square$

exemples:

- $0 + 0 = 0$
- $1 \times 1 = 1$
- $\text{Id}_E \circ \text{Id}_E = \text{Id}_E$
- $O_{n,p} + O_{n,p} = O_{n,p}$
- $I_n \times I_n = I_n$
- $E \cap E = E$
- $\emptyset \cup \emptyset = \emptyset$

d) Inverse du produitProposition:

Soit (M, \cdot, e) un monoïde.

Soient $a, b \in M$. Alors:

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

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

démonstration:

Où a, b inversibles.

. On calcule

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

. De même :

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

Ainsi par définition : (ab) est inversible et son inverse est $b^{-1}a^{-1}$

I.e. 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 $\alpha \in M$ est inversible, son inverse est alors noté $-\alpha$

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

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

g) Remarque finale.

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

II) Groupes.

1) Définition.

Définition:

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

21 Exemples.

a) Exemples.

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

b) Groupe des permutations d'un ensemble.

Soit E un ensemble. "S" gothique

On note S_E ou \mathcal{S}_E l'ensemble des bijections de E dans E .

Proposition / Définition:

Le triplet $(S_E, \circ, \text{Id}_E)$ est un groupe appelé groupe des permutations de E .

démonstration:

• Déjà, on a bien $S_E \times S_E \rightarrow S_E$
 $(f, g) \mapsto f \circ g$

car la composition de 2 bijections est bijective.

• Ensuite, on a $\text{Id}_E \in S_E$ et $\forall f \in S_E, f \circ \text{Id}_E = f$
 $\text{Id}_E \circ f = f$

• Donc Id_E est un neutre de S_E pour \circ .

• Enfin, si $f \in S_E$, il existe $g \in S_E$ tq $g \circ f = \text{Id}_E$ et
 $f \circ g = \text{Id}_E$

• Ie: toute $f \in S_E$ est inversible dans $(S_E, \circ, \text{Id}_E)$

c) Groupe produit

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

On considère $G_1 \times G_2$ qui en munir d'une loi \oplus en posant

$$(\alpha_1, \alpha_2) \oplus (y_1, y_2) := (\alpha_1 \cdot y_1, \alpha_2 * y_2)$$

$$\begin{matrix} \downarrow & \downarrow \\ EG_1 & EG_2 \end{matrix} \quad \begin{matrix} \uparrow & \uparrow \\ EG_1 & EG_2 \end{matrix}$$

Propriétés / Définition:

- 1) le triplet $(G_1 \times G_2, \otimes, (e_1, e_2))$ est un groupe
- 2) Si $(x, y) \in G_1 \times G_2$, l'inverse de (x, y) pour \otimes est (x^{-1}, y^{-1})
- 3) C'est le groupe produit de (G_1, \cdot, e_1) et (G_2, \times, e_2)

!!! Remarque:

Au lieu de noter (G, \cdot, e) , on note souvent (G, \cdot) voire même G .

3) Sous-groupes.

a) Définition.

Définition:

Soit (G, \cdot, e) un groupe

Soit $H \subseteq G$

On dit que H est un sous-groupe de G si

$$\forall x, y \in H, xy \in H$$

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

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

remarque:

Soit G un groupe et soit $H \text{ sgr } G$.

Alors, l'application $\cdot : G \times G \rightarrow G$ peut être

restreinte à $H \times H$; on obtient $\cdot|_{H \times H} : H \times H \rightarrow G$

Comme $H \text{ sgr } G$, on a $\forall x, y \in H, xy \in H$

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

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

Fait:

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

démonstration:

ok \square

CCL: $H \text{ sgr } G \Rightarrow H \text{ groupe}$.

b) Caractérisation.

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

Proposition:

$$H \text{ogr } G \iff \forall \alpha, y \in H, \alpha y^{-1} \in H$$

démonstration:

\Leftarrow C'est plutôt facile. Soient $\alpha, y \in H$

Je sais que $y^{-1} \in H$. Comme aussi $\alpha \in H$, on a $\alpha y^{-1} \in H$

(Or H est non vide : fixons donc $\alpha_0 \in H$)
 $\left(\begin{array}{l} \text{On a } \alpha_0 \cdot \alpha_0^{-1} \in H \text{ i.e. } e \in H \\ \end{array} \right)$ HS

\Leftarrow Opp $\forall \alpha, y \in H, \alpha y^{-1} \in H$

On a $e \in H$. En effet, comme $H \neq \emptyset$, fixons $\alpha_0 \in H$. On a $\alpha_0 \cdot \alpha_0^{-1} \in H$ i.e. $e \in H$.

Soient $\alpha, y \in H$

- Comme $e \in H$, on a $ey^{-1} \in H$ i.e. $y^{-1} \in H$

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

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

- Donc, $\alpha y \in H$ ■

remarque:

On avait oublié de dire que $\forall \alpha \in G, (\alpha^{-1})^{-1} = \alpha$
 si G groupe.

démonstration:

exercice + généralisat°

c) Exemples.

- $\mathbb{R}_+^* \text{ogr } (\mathbb{R}^*, \times, 1)$

- $\mathbb{Q}^* \text{ogr } (\mathbb{R}^*, \times, 1)$

démonstration:

• $1 \in \mathbb{Q}^*$

• $\forall \alpha, y \in \mathbb{Q}^*, \alpha y \in \mathbb{Q}^*$

• $\forall \alpha \in \mathbb{Q}^*, \frac{1}{\alpha} \in \mathbb{Q}^*$ ■

- \mathbb{Q}_+^* agr \mathbb{Q}^* agr \mathbb{R}^*

exercice: Soit G groupe. Soient H, K agr G . Alors

HK agr G

(\oplus généralement: si $(H_i)_{i \in I}$ est une famille de sous-groupes de G , alors $\bigcap_{i \in I} H_i$ agr G) (\oplus 16.16: l'union n'est pas à considérer)

- $\{1\}, 1 \nmid \text{agr}(\mathbb{R}^*, \times, 1)$

- $\{1\} \nmid \text{agr}(\mathbb{R}^*, \times, 1)$

Fait \oplus :

$\{e\}$ agr G et G agr G

- \mathbb{R}^* agr $(\mathbb{C}^*, \times, 1)$

- \mathbb{U}_n agr $(\mathbb{C}^*, \times, 1)$

démontrons:

$$\bullet 1 \in \mathbb{U}_n$$

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

$$\bullet w \in \mathbb{U}_n \Rightarrow w^{-1} \in \mathbb{U}_n \quad \text{B}$$

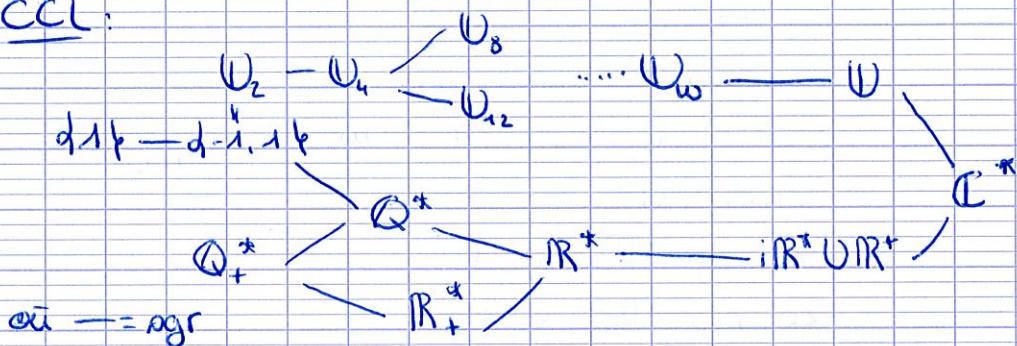
- \mathbb{U} agr $(\mathbb{C}^*, \times, 1)$

exercice \star/\star : On note $\mathbb{U}_w := \bigcup_{n \geq 1} \mathbb{U}_n$

Mq \mathbb{U}_w agr \mathbb{U} .

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

- CCL:



Li Sous-groupe engendré *

Soit G un groupe et soit $X \subset G$

But: Trouver le sous-groupe de G engendré par X .

a) Point de vue interne *

On pose $\langle X \rangle := \{ \alpha_1^{e_1} \alpha_2^{e_2} \dots \alpha_n^{e_n} ; \begin{array}{l} n \in \mathbb{N} \\ \alpha_1, \dots, \alpha_n \in X \\ e_1, \dots, e_n \in \mathbb{Z}^{\pm 1} \} \}$

Proposition: $\langle X \rangle$ est un sous-groupe de G .
 $\{ (\pm \alpha_1) + (\pm \alpha_2) + \dots + (\pm \alpha_n) ; \begin{array}{l} n \in \mathbb{N} \\ \alpha_1, \dots, \alpha_n \in X \end{array} \}$

$\langle X \rangle$ est un sous-groupe de G .

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

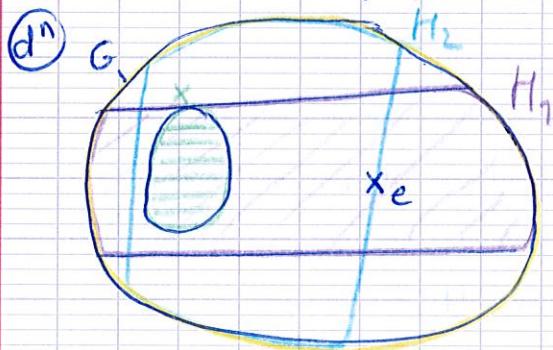
À l'oral. \square

remarque:

$$\langle \emptyset \rangle = \text{def}$$

b) Point de vue externe *

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



Proposition 1:

$\{ X \}$ est le plus petit sgr de G qui contient X .

démonstration:

- Déjà, $\{ X \}$ sgr de G : cf exercice $\bigcap_{i \in I} H_i$

- Soit H_0 sgr G tel que $X \subset H_0$

On a $\bigcap_{\substack{H \text{ sgr } G \\ X \subset H}} H \subset H_0$ donc $\{ X \} \subset H_0$. \square

H_0 figure dans cette liste

Proposition 2:

$$\langle X \rangle = \{ X \}$$

démonstration:

(AC*) \square

c) Groupes monogènes

Définition:

Soit G un groupe. On dit que G est monogène si :

$$\exists \alpha_0 \in G : G = \langle d\alpha_0, k \rangle$$

exemples:

- $(d\{1\}, x, 1)$ est monogène. "groupe nul"
- $(d\{-1, 1\}, x, 1)$ i.e \mathbb{W}_2 est monogène, engendré par -1
- \mathbb{U}_3 est monogène, engendré par j
- \mathbb{U}_n est monogène, engendré par $e^{\frac{2i\pi}{n}}$
- $(\mathbb{Z}, +, 0)$ est monogène, engendré par 1 .

Si G est monogène engendré par a , on a

$$G = \langle d a^n : n \in \mathbb{Z} \rangle$$

exemple:

- \mathbb{U}_n n'est pas monogène car $\mathbb{U} \neq \mathbb{N}$
- De même $(\mathbb{R}, +, 0)$ n'est pas monogène.

III) Morphismes de groupes.

1) Définitions

a) Morphismes

Définition:

Soient $(G, ., e_G)$ et $(H, *, e_H)$ deux groupes.

Soit $\Psi: G \rightarrow H$.

On dit que Ψ est un morphisme de groupes si

$$\forall x, y \in G, \Psi(x \cdot y) = \Psi(x) * \Psi(y)$$

\uparrow loi de G \uparrow loi de H

remarque:

- On note $\text{Hom}_{(G,H)}(G, H)$ l'ensemble des morphismes de G dans H (ancien nom: homomorphisme)
- Si $\Psi: G \rightarrow G$ morphisme, on dit que Ψ est un endomorphisme. On note $\text{End}_{(G,G)}(G)$.

II) Groupes.

a) Groupes cycliques

On dit que G est cyclique si G est monogène et fini.

Remarque:

Un groupe abélien est un groupe commutatif.

b) Diagrammes.

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



On dit qu'il commute si le diagramme d'ensembles sous-jacents commute.

c) Propriétés.

Soient G, H deux groupes.

Soit $\Psi: G \rightarrow H$ un morphisme.

Proposition:

On a $\forall \alpha \in G, \Psi(\alpha^{-1}) = \Psi(\alpha)^{-1}$

Proposition 2:

On a $\Psi(e_G) = e_H$

démonstration:

2) On a $\Psi(e_G \cdot e_G) = \Psi(e_G) * \Psi(e_G)$

D'où $\Psi(e_G) = \Psi(e_G) * \Psi(e_G)$

On a $\Psi(e_G) \in H$. Notons $y_0 := \Psi(e_G)$. On a $y_0 * y_0 = y_0$

Or, H est un groupe donc H est inversible : on dispose de y_0^{-1} .

On a alors

$$\begin{aligned} (y_0 * y_0) * y_0^{-1} &= y_0 * y_0^{-1} \\ &= y_0 * (e_H) \\ &= y_0 \end{aligned}$$

Donc $y_0 = e_H$

Donc $\Psi(e_G) = e_H$

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

Je passe $(\ast\ast)$ à $\Psi(\cdot)$. On obtient

$$\begin{cases} \Psi(\alpha) * \Psi(\alpha^{-1}) = \Psi(e_G) = e_H \\ \Psi(\alpha^{-1}) * \Psi(\alpha) = e_H \end{cases}$$

Donc par définition : $\Psi(\alpha^{-1})$ est l'inverse de $\Psi(\alpha)$ dans H pour *

I.e., on a $\Psi(\alpha)^{-1} = \Psi(\alpha^{-1})$ \square

2) Composition des morphismes.

Soient G, H, K trois groupes.

Soient $\Psi: G \rightarrow H$ et $\Phi: H \rightarrow K$ des applications.

Proposition:

Ψ morphisme $\Rightarrow \Phi \circ \Psi$ morphisme.

Φ morphisme

démonstration: \dagger \ddagger

Je note $*$, \circ et \bowtie les lois de G, H et K .

Montrons que $G \xrightarrow{\Psi} H \xrightarrow{\Phi} K$ est un morphisme.

Soient $x, y \in G$. On calcule : *définit de "o"*

$$\begin{aligned} (\Psi \circ \Phi)(x *_G y) &= \Psi(\Phi(x *_G y)) \\ &= \Psi(\Phi(x) *_H \Phi(y)) = \Psi(\Phi(x)) *_K \Psi(\Phi(y)) \\ &= (\Psi \circ \Phi)(x) *_K (\Psi \circ \Phi)(y) \end{aligned}$$

définit de "o"

3 | Exemples.

- $\exp : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_+^*, \times, 1)$
qui on peut noter $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \times)$
- $\frac{1}{\cdot} : (\mathbb{R}^*, \times) \longrightarrow (\mathbb{R}^*, \times)$

démonstration:

$$1) \exp(a+b) = \exp(a) \cdot \exp(b) \quad \square$$

$$2) \frac{1}{a \times b} = \frac{1}{a} \times \frac{1}{b} \quad \square$$

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

dém^①:

$$\ln(ab) = \ln(a) + \ln(b) \quad \square$$

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

dém^①:

$$\sqrt{ab} = \sqrt{a} \cdot \sqrt{b} \quad \square$$

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

ce^① $(a+b)^2 \neq a^2 + b^2$

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

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

dém^①:

$$I(f+g) = I(f) + I(g). \text{ On dit que } I \text{ est additive.}$$

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

$$n \longmapsto 2^n$$

dem^T:

$$2^{n+m} = 2^n \times 2^m \quad \text{□}$$

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

$$n \longmapsto a^n$$

!!!

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

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

dem^T:

$$e^{i(\theta+\theta')} = e^{i\theta} \cdot e^{i\theta'} \quad \text{□}$$

- Soit E un ensemble.

$(\mathcal{P}(E), \cap, E) \xrightarrow{\quad A \quad} (\mathcal{F}(E, \{0, 1\}), \times, \lambda)$ est un morphisme de monoïdes.

dem^P:

$$\mathbb{M}_{A \cap B} = \mathbb{M}_A \times \mathbb{M}_B \quad \text{□}$$

4.1 Tirer en arrière et pousser en avant des sous-groupes

On considère $G \xrightarrow{\varphi} H$
 $G' \xrightarrow{\text{ogr}} H'$

avec G, H des groupes et φ un morphisme.

Proposition:

1) $\varphi^{-1}[H']$ sgr G .

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

démonstration:

1) Mq. $e_G \in \varphi^{-1}[H']$

Ie, $\varphi(e_G) = e_{H'}$

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

De plus, comme $H' \text{ sgr } H$, on a $e_H \in H'$

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

Donc $\varphi^{-1}[H'] \neq \emptyset$

Mq. $\forall x, y \in \varphi^{-1}[H']$, $x \circ y^{-1} \in \varphi^{-1}[H']$ (d'après la

CHAPITRE 10

9 9

caractérisat° des sgr).

Soient $\alpha, y \in \Psi^{<-1}[H']$

Mq $\alpha y^{-1} \in \Psi^{<-1}[H']$

| On a $\alpha \in \Psi^{<-1}[H']$. Donc $\Psi(\alpha) \in H'$

De même, $\Psi(y) \in H'$

Comme $H' \text{ sgr } H$, on a $\Psi(y)^{-1} \in H'$

Or $\Psi(y)^{-1} = \Psi(y^{-1})$

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

Or $H' \text{ sgr } H$. Donc

$\Psi(\alpha) \cdot \Psi(y^{-1}) \in H'$

Ie $\Psi(\alpha y^{-1}) \in H'$

D'où $\alpha y^{-1} \in \Psi^{<-1}[H']$ \square

2) Mq $\Psi[G']$ sgr H .

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

| Comme $G' \text{ sgr } G$, on a $e_G \in G'$

Done $\Psi(e_G) \in \Psi[G']$

or $\Psi(e_G) = e_H$

Donc $e_H \in \Psi[G']$

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

| Soient $\alpha, \beta \in \Psi[G']$ qui on écrit $\alpha = \Psi(\alpha)$ et $\beta = \Psi(\beta)$
avec $\alpha, \beta \in G'$ (R)

Comme $G' \text{ sgr } G$, on a $\alpha \beta^{-1} \in G'$

Done $\Psi(\alpha \beta^{-1}) \in \Psi[G']$

Or, $\Psi(\alpha \beta^{-1}) = \Psi(\alpha) \cdot \Psi(\beta^{-1}) = \Psi(\alpha) \Psi(\beta)^{-1} = \alpha \beta^{-1}$

On a bien montré que $\alpha \beta^{-1} \in \Psi[G']$ \square

S/ Noyau d'un morphisme

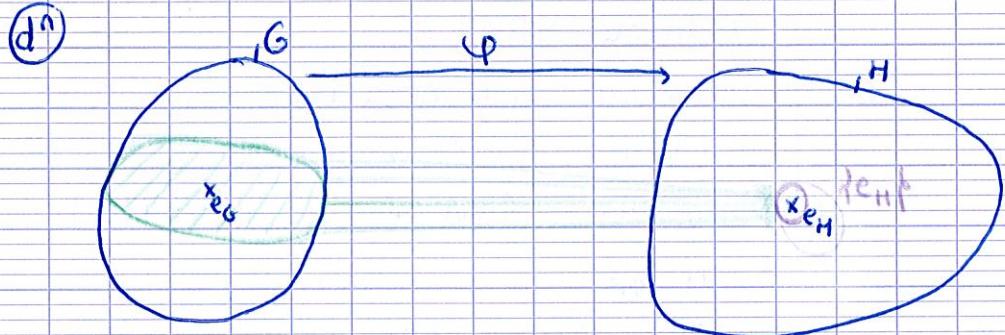
M

a Définition

Définition:

Soient G, H deux groupes. Soit $\varphi: G \rightarrow H$ un morphisme. Le noyau de φ est le sous-groupe de G , noté $\text{Ker } \varphi$, défini par

$$\text{Ker } \varphi = \varphi^{-1}[e_H]$$



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

b) Caractérisation de l'injectivité d'un morphisme.

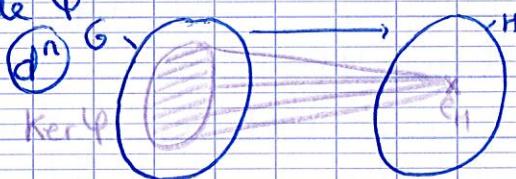
Soit $\varphi: G \rightarrow H$ morphisme entre 2 groupes.

Proposition:

$$\varphi \text{ injective} \Leftrightarrow \text{Ker } \varphi = \{e_G\}$$

remarques:

- On a $\text{Ker } \varphi \trianglelefteq G$. En effet, $\text{Ker } \varphi$ est le tiré-en-arrière d'un sous-groupe de H (cf III, 41).
- Donc on a toujours $e_G \in \text{Ker } \varphi$
- En quelques sortes, "Ker φ mesure le défaut d'injectivité de φ "



démonstration:

\Rightarrow On suppose φ injective. Montrons $\text{Ker } \varphi = \{e_G\}$

Déjà, on a toujours $\{e_G\} \subseteq \text{Ker } \varphi$

Soit $x \in \text{Ker } \varphi$. On a $\varphi(x) = e_H$

Or $e_H = \varphi(e_G)$ Donc $\varphi(x) = \varphi(e_G)$

Or \varPhi inj donc $\alpha = e_G$

\Leftarrow Onq $\text{Ker } \varPhi = \{e_H\}$

Mq \varPhi inj.

Soient $\alpha, \gamma \in G$ tq $\varPhi(\alpha) = \varPhi(\gamma)$

Mq $\alpha = \gamma$

D'après $\alpha := \varPhi(\alpha) = \varPhi(\gamma)$

On a $\varPhi(\alpha\gamma^{-1}) = \varPhi(\alpha)\varPhi(\gamma^{-1}) = \alpha\alpha^{-1} = e_H$

Donc $\alpha\gamma^{-1} \in \text{Ker } \varPhi$

Or $\text{Ker } \varPhi = \{e_H\}$. Donc $\alpha\gamma^{-1} = e_H$

Donc $\alpha\gamma^{-1}\gamma = e_H\gamma$

D'où $\alpha = \gamma$ \square

6) Image d'un morphisme.

Définition: \circledast

Soit $\varPhi: G \rightarrow H$ un morphisme.

L'image de \varPhi , noté $\text{Im}(\varPhi)$, est le sgr de H défini par

$$\text{Im}(\varPhi) := \varPhi[G]$$

!!! 7) Isomorphismes.

a) Isomorphismes.

Définition: \circledast

Soit $\varPhi: G \rightarrow H$ un morphisme.

On dit que \varPhi est un isomorphisme si \varPhi bijectif.

Proposition:

\varPhi isomorphisme $\Rightarrow \varPhi^{-1}: H \rightarrow G$ morphisme.

démonstration:

Mq $\forall \alpha, \beta \in H$, $\varPhi^{-1}(\alpha\beta) = \varPhi^{-1}(\alpha) \cdot \varPhi^{-1}(\beta)$

| Soient $\alpha, \beta \in H$ (R^x) Je les écris $\alpha := \varPhi(x)$, $\beta = \varPhi(y)$

avec $\alpha, \gamma \in G$

$$\text{On a } \Psi(\alpha\beta) \cdot \Psi(\gamma) = \Psi(\alpha\gamma\beta)$$

$$\text{i.e. } \alpha\beta = \Psi(\alpha\gamma\beta)$$

$$\text{Donc } \Psi^{-1}(\alpha\beta) = \Psi^{-1}(\Psi(\alpha\gamma\beta))$$

$$\text{i.e. } \Psi^{-1}(\alpha\beta) = \alpha\gamma$$

$$\text{Comme } \alpha = \Psi(\gamma), \text{ on a } \Psi^{-1}(\alpha) = \Psi^{-1}(\Psi(\gamma)) \text{ i.e. } \Psi^{-1}(\alpha) = \gamma$$

$$\text{De même, } \gamma = \Psi^{-1}(\beta)$$

$$\underline{\text{CCL: }} \Psi^{-1}(\alpha\beta) = \Psi^{-1}(\alpha) \cdot \Psi^{-1}(\beta)$$

b) Automorphismes de groupes.

Définition:

Un automorphisme Ψ de G est un isomorphisme de G dans G .

On note $\text{Aut}_{(Gr)}(G)$ l'ensemble des automorphismes de G .

c) Groupes isomorphes.

!!! Définition:

Soient G, H deux groupes.

On dit que G et H sont isomorphes et on note $G \cong H$

s'il $\exists \Psi: G \rightarrow H$ i.o.

remarque:

• Si $\Psi: G \rightarrow H$ est un i.o., on note $G \xrightarrow{\Psi} H$

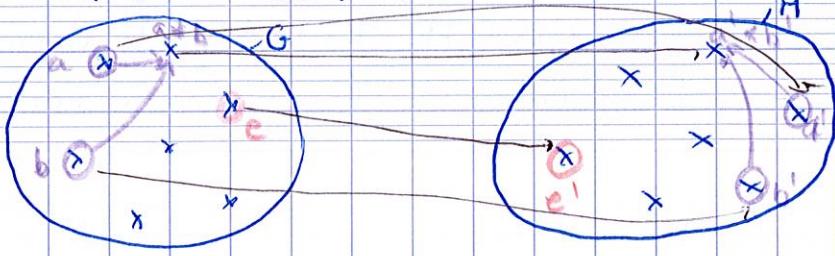
• On considère d'un côté $(\mathbb{Z}, +, 0)$ et on définit un ensemble $\tilde{\mathbb{Z}} := \{ \dots, \tilde{-3}, \tilde{-2}, \tilde{-1}, \tilde{0}, \tilde{1}, \tilde{2}, \tilde{3}, \dots \}$ où \tilde{m} est l'entier m avec un tilde au-dessus.

On munit $\tilde{\mathbb{Z}}$ d'une loi $\tilde{+}$ définie par $\tilde{n} + \tilde{m} = \tilde{n+m}$

$$\text{ex: } \tilde{8} + \tilde{3} = \tilde{11}$$

$$\text{Alors } (\mathbb{Z}, +, 0) \cong (\tilde{\mathbb{Z}}, \tilde{+}, 0)$$

d)



CHAPITRE 10

43

exemple surprenant:

$$(\mathbb{R}_+^*, \times) \cong (\mathbb{R}_+^*, +)$$

démonstration:

• $\ln : \mathbb{R}_+^* \rightarrow \mathbb{R}$ est un iso de groupes.

• En effet, $\ln(\cdot)$ est bijective (• $\ln(\cdot)$ est continue,

• $\ln(\cdot) \neq$

• $\ln(x) \xrightarrow{x \rightarrow 0^+} -\infty$ et $\ln(x) \xrightarrow{x \rightarrow +\infty} +\infty$

• $\circledast \quad \ln(ab) = \ln(a) + \ln(b)$. ■

Complément:

Soit G un groupe; soit $g \in G$

• RDC: Soit $x \in G$. On dispose de $gxg^{-1} \in G$

C'est le conjugué de x par g .

notations: $\text{conj}_g(x)$ ou $\text{conj}_g^{[G]}(x)$

• 1^{er} étage: On dispose de $\text{conj}_g : G \longrightarrow G$

$$x \mapsto gxg^{-1}$$

On a $\text{conj}_g \in \mathcal{F}(G, G)$

Fait: • $\text{conj}_g(\cdot)$ est un morphisme

• Ie: $\text{conj}_g \in \text{End}_{(\text{corp})}(G)$.

• 2^{ème} étage: On dispose de $\text{conj} : G \longrightarrow \text{End}_{(\text{corp})}(G)$

$$g \mapsto \text{conj}_g$$

Fait: • conj_g est bijectif

• Ie: $\text{conj}_g \in \text{Aut}_{(\text{corp})}(G)$

• 2^{ème} étage rénové:

On sait que $\text{Aut}_{(\text{corp})}(G)$ est un groupe

- 1) composé de 2 auto est un auto
- 2) l'inverse d'un auto est un auto
- 3) Id_G est un auto

Plus précisement: $(\text{Aut}_{(\text{corp})}(G), \circ, \text{Id}_G)$

Proposition: • $\text{conj}^{[G]} : G \longrightarrow \text{Aut}_{(\text{corp})}(G)$ est un morphisme

• Ie: $\text{conj}^{[G]} \in \text{Hom}_{(\text{corp})}(G, \text{Aut}_{(\text{corp})}(G))$

