Chapitre 10 : Groupes

I) Lois de composition interne

1) Lois de composition internes

a) def°

Def° : Soit E un ensemble

Une loi de composition interne (lci) sur E est une application

$$\varphi : E^2 \longrightarrow E$$

Important

- Si $\varphi : E^2 \longrightarrow E$ est une lci, et si $x, y \in E$, on note, p. ex,

$x * y := \varphi(x, y)$

On dit alors que $*$ est la loi de composition interne

- Autres symboles : $\bullet$, $\cdot$
- Si la loi est notée "$\cdot$" alors, au lieu de $x \cdot y$, on pourra aussi noter xy, pour $x, y \in E$

Ex : · sur $\mathbb{R}$, on dispose de la loi $\begin{aligned} \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto xy \end{aligned}$

b) magma

Un magma est un couple $(E, \bullet)$ où :

- E est un ensemble
- $\bullet$ est une loi sur E

2) Associativité

a) def°

Soit E un ensemble et $\bullet$ une loi sur E

Def° : on dit que $\bullet$ est associative $\overset{\Delta}{\text{ssi}}$

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

On note $\bullet$ loia

Rq : Si on avait noté $\varphi : E^2 \longrightarrow E$ la loi, la def° de φ loia aurait été :

$$\forall x, y, z \in \mathbb{Z}, \; \varphi(x, \varphi(y, z)) = \varphi(\varphi(x, y), z)$$

Ex :

Ocsd $\varphi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}$; c'est une loi sur $\mathbb{Z}$

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

Mais $x-(y-z) \neq (x-y)-z$ en g^{al}

$(x := 0, y := 0, z := 1)$

Donc cette loi n'est pas associative.

A retenir : on n'étudie pas (ici) les lois non associatives.

b) puissances

Soit E un ensemble et $\cdot$ une lci sur E

Soit $n \in \mathbb{N}^*$ et soient $x_1, x_2, \ldots, x_n \in E$

Ĉ $\cdot$ est associative, tous les parenthésages possibles de

$$x_1 \cdot (x_2 \cdot (x_3 \cdot \ldots \cdot x_n))$$

donnent le m̂ résultat.

On peut donc omettre les parenthésages, on note juste

$$x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n$$

ou $x_1 x_2 x_3 \ldots x_n$

Notation :

Si $n \in \mathbb{N}^*$ et si $x \in E$, on pose

$$x^n := \underbrace{x \cdot x \cdot x \cdot x \cdot \ldots \cdot x}_{n \text{ fois}}$$

On dit que c'est la poissance n-ième de x pour.

Prop

1) $x^{n+m} = x^n \cdot x^m$

2) $(x^n)^m = x^{nm}$

D/ N AC ĝ aux paranthèsages
Soit $n \in \mathbb{N}^*$
2) ORP rec ; on note pour $m \in \mathbb{N}^*$,

$$P(m) = \text{"}(x^n)^m = x^{n \cdot m}\text{"}$$

$m = 1$: ok car $\forall y \in E$, $y^1 = y$

Hérédité : soit $m \in \mathbb{N}^*$ tq $(x^n)^m = x^{n \cdot m}$

On a donc $(x^n)^m \cdot x^n = x^{n \cdot m} \cdot x^n$

D'après 1), on a donc

$$\begin{cases} (x^n)^m \cdot x^n = (x^n)^{m+1} & \text{avec " } x \leftarrow x^n \\ & n \leftarrow m \\ x^{n \cdot m} \cdot x^n = x^{n \cdot m + n} & m \leftarrow 1 \text{ "} \end{cases}$$

Ĉ & $n \times m + n = n(m+1)$, $P(m+1)$ est V

■

3) Commutativité

Def°: Soit E un ens. et soit $\cdot$ une loi sur E

On dit que $\cdot$ est commutative ssi

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

Remarque !

- Les lois commutatives peuvent être notées : $*$, $\bullet$, $\cdot$, ect...
- En revanche il y a une notation qu'on utilise que pour les lois commutatives : c'est "$+$"
- Quand une loi commutative est notée $+$, on note

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

4) Exemples

- L'addition sur $\mathbb{N}$: c'est une loi commutative (lciac)
- ——— $\mathbb{Z}$
- ——— $\mathbb{R}$
- ——— $\mathbb{C}$
- ——— $\mathbb{Q}$

$\}$ Ce sont des lciac

- La multiplication sur $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$

qui est à chaque fois une lcic.

- La division sur $\mathbb{R}^*$: elle n'est pas commutative, ni associative (en general $\frac{\frac{a}{b}}{c} \neq \frac{a}{\frac{b}{c}}$)

$$\frac{a}{bc} \qquad \frac{ac}{b}$$

- <u>Soit E un ens.</u>

Sur $\mathcal{P}(E)$ on dispose de : l'union ($\cup$) et l'intersection ($\cap$) sont des lcic

- <u>La composition</u>

Soit E un ens. Ocsd $\mathcal{F}(E,E)$

On dispose de

$$\mathcal{F}(E,E)^2 \longrightarrow \mathcal{F}(E,E)$$

$$(f,g) \longmapsto \boxed{f \circ g}$$

C'est une lci ; elle est associative. En general, elle n'est pas commutative

- On ne peut pas considerer $E \times F$ comme une lci car il faudrait la definir sur " l'ensemble de tous les ensembles
Or (exo) : la collection de tous les ensembles n'est pas un ensembles.

D) ORPA et on note $\mathcal{U}$ l'ensemble de tous les ensembles

On pose $\mathcal{A} := \{E \in \mathcal{U} \mid E \notin E\}$: c'est un ensemble

On a $\mathcal{A} \notin \mathcal{A}$ (ORPA) et $\mathcal{A} \in \mathcal{A}$ (ORPA) $\blacksquare$

(1). • On note $M_n(\mathbb{R})$ l'ens des matrices carrées de taille n à coeff dans $\mathbb{R}$

Sur $M_n(\mathbb{R})$, on a deux lcia : l'addition qui est commutative ; le produit ⚠ En général $AB \neq BA$.

• ~~Notons~~ Sur $\mathbb{R}^2$: l'addition définit par (1)

$$\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x+x' \\ y+y' \end{pmatrix}$$

(on a posé $\begin{pmatrix} x \\ y \end{pmatrix} := (x, y)$ pour des raisons de clarté)

• De m̂ dans $\mathbb{R}^3$

• De même dans $\mathbb{R}^n$:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1+y_1 \\ x_2+y_2 \\ \vdots \\ x_n+y_n \end{pmatrix}$$

Ce sont des lciac.

• Si X ens, sur $\mathcal{F}(X, \mathbb{R})$, on peut faire $f+g$ et $f \times g$: ce sont des lciac.

• Sur $\mathbb{R}$, ocsd $\begin{array}{ccc} \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & \sin(e^x) \times y \end{array}$

• La concaténation de mots : l.c.i.a

5) Neutres

a) def°

Soit E un ensemble muni d'une l.c.i.a $\bullet$

Def° : Soit $e \in E$ on dit que e est un neutre de E pour l'opération $\bullet$ $\overset{\Delta}{ssi}$ $\forall x \in E, (x \bullet e = x$ et $e \bullet x = x)$

Prop : Soit ~~E,~~ $e_1, e_2 \in E$ des neutres. Alors $e_1 = e_2$.
C'est l'unicité du neutre

D/ ĉ e_1 neutre, on a $e_1 \bullet e_2 = e_2$
ĉ e_2 neutre, on a $e_1 \bullet e_2 = e_1$

Donc $e_1 = e_2$ ▪

Exemple

• Dans $\mathbb{R}$ muni de $\times$: 1 est neutre
• Dans $\mathbb{R}$ muni de $+$: 0 est neutre
• Dans $\mathcal{P}(E)$ muni de $\cap$: E est neutre
• ———————— $\cup$: $\varnothing$ ————
• Dans $\mathcal{F}(E,E)$: Id_E est neutre
• (muni de $\circ$)

• Dans l'ens des mots muni de la concatenation : le mot vide est neutre

b) Monoïdes

<u>Def°</u> : un <u>monoïde</u> est un triplet avec $(E, \bullet, e)$

tq : * E est un ensemble
* $\bullet$ est une lci sur E
* e est neutre

<u>Remarque</u> : Si E est un monoïde et si $x \in E$, on pose

$x^0 := e$

On a encore $\left\{\begin{array}{l} x^{n+m} = x^n x^m \\ (x^n)^m = x^{nm} \end{array}\right.$

c) inverses d'un élt

Soit $(E, \cdot, e)$ un monoïde

<u>Def°</u> : soit $x \in E$
Soit $\alpha \in E$

* On dit que α est un inverse à ~~...~~ gauche de x (pour $\cdot$) $\Leftrightarrow$ ssi

$\alpha \cdot x = e$

* On dit que α est un inverse à droite de x (pour $\cdot$) $\Leftrightarrow$ ssi

$x \cdot \alpha = e$

(*) On dit que α est un inverse de x (pour $\circ$) ssi :

$$x \circ \alpha = e \quad \text{et} \quad \alpha \circ x = e$$

Rq : on definit aussi " x inversible à gauche ssi

$\exists \alpha \in E, \alpha \circ x = e$ " ; " inversible à droite " ; " inversible ".

<u>Prop</u> : Unicité de l'inverse

Soit $x \in E$ - Soient $\alpha, \beta \in E$ des inverses de x
Alors $\alpha = \beta$

D/ On a

$$\alpha \circ x \circ \beta = \alpha \circ \overbrace{(x \circ \beta)}^{=e} = \alpha \circ e = \alpha$$
$$= \underbrace{(\alpha \circ x)}_{=e} \circ \beta = e \circ \beta = \beta$$

■

(Exo) Mq " l'inverse à gauche n'est pas unique en g^{al} "

<u>Notation</u>

Soit $x \in E$

Si x est ~~...~~ inversible (ie $\exists \alpha \in E : \alpha \circ x = x \circ \alpha = e$) alors son inverse est " unique ". On la note x^{-1}

Exemples

- Dans $(\mathbb{R}, +, 0)$: tous les $x \in \mathbb{R}$ sont inversibles

Et, l'inverse (pour $\oplus$) de x est : $-x$

- Dans $(\mathbb{R}, \times, 1)$: tous les $x \in \mathbb{R}^*$ sont inversibles

(en effet : $\nexists \alpha \in \mathbb{R} : 0 \times \alpha = \alpha \times 0 = 1$)

Et l'inverse de $x \neq 0$ est $\frac{1}{x}$

- Dans $\mathcal{F}(E, E)$: les $f : E \longrightarrow E$ inversibles sont les bijections

- Dans $(\mathcal{P}(E), \cup, \emptyset)$: seul $\emptyset$ est inversible

Fait : Soit $(E, \cdot, e)$ un monoïde

Alors e est inversible et $e^{-1} = e$

- Dans $(M_n(\mathbb{R}), \times, I_n)$: on retrouve la notion de matrice inversible

d) inverse du produit

Soit $(E, \cdot, e)$ un monoïde

Prop : Soient $x, y \in E$. Alors :

1) x inversible et y inversible $\Rightarrow$ $x \cdot y$ inversible

2) Dans ce cas on a $(x\circ y)^{-1} = y^{-1}\circ x^{-1}$

D/ Osq x, y inversible. On a :

⊛ $(x\circ y)\circ(y^{-1}\circ x^{-1}) = x\circ(\underbrace{y\circ y^{-1}}_{=e})\circ x^{-1} = (\underbrace{x\circ e}_{=x})\circ x^{-1}$

$= x\circ x^{-1} = e$

⊛ $(y^{-1}\circ x^{-1})\circ(x\circ y) = e$ de m

Ainsi : $x\circ y$ est inversible et son inverse est $y^{-1}\circ x^{-1}$;

d'où $(x\circ y)^{-1} = y^{-1}\circ x^{-1}$ ∎

e) cas commutatif

Dans le cas où la lcia est commutative et est notée $+$:

- le neutre (s'il existe) est noté 0_E ou 0
- l'inverse de x (s'il existe) est noté $-x$

Rq : on note alors $x - y := x + (-y)$

II Groupes

1) Définition

Déf° : Un groupe est un triplet $(G, \cdot, e)$ tq :

- $\circledast$ G est un ens
- $\circledast$ $\cdot$ est une lcia sur G
- $\circledast$ e est neutre pour $\cdot$
- $\circledast$ $\forall x \in G$, x inversible

} monoïde

Rq : au lieu de dire "soit $(G, \cdot, e)$ un groupe", souvent on sous-entend "$\cdot$" et "e" et on dit "Soit G un group"

Prop : (qq $\mathbb{R}^*$)

Soit G un groupe. Alors ①

1) $(x^{-1})^{-1} = x$
2) $e^{-1} = e$
3) $ax = ay \Rightarrow x = y$
4) Soit $a \in G$. O csd

$$\lambda_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & ax \end{array}$$

Alors λ_a est une bijection

D (1)2) ok
3) O sq $ax = ay$. Donc $a^{-1}ax = a^{-1}ay$
Ie $x = y$

4) λ_a est inj d'après 3)

Mq λ_a est surj

Soit $y \in G$. On cherche $x \in G$ tq $\lambda_a(x) = y$

Posons $x := a^{-1} y$ ⚠ J'ai bien le droit d'écrire a^{-1} car je suis de un groupe : tt le monde est inversible

On a $\lambda_a(x) = a \circ (a^{-1} \circ y)$
$= (a \circ a^{-1}) \circ y$
$= e \circ y = y$

DLR

Def°

Soit $(G, \circ, e)$ un groupe

On dit que il est abélien ou commutatif ssi $\circ$ commutative

2) Exemples

a) exemples

- $(\mathbb{R}, +, 0)$ c'est $\mathbb{R}$ additif
- $(\mathbb{R}^*, \times, 1)$ c'est $\mathbb{R}^*$ multiplicatif ou $\mathbb{R}$ multiplicatif

- $(\mathbb{Z}, +, 0)$ c'est $\mathbb{Z}$ additif

- $(\mathbb{N}, +, 0)$ c'est un monoïde qui n'est pas un groupe

- Notons $Bij(E) := \{ f : E \to E \mid f \text{ bij} \}$

Alors $(Bij(E), \circ, Id_E)$ est un groupe

b) groupe des permutations d'un ensemble

Soit ~~x~~ un ensemble

Def°: une permutat° de X est une bijection $f : X \to X$

- On note S_X ou $\mathfrak{S}_X$ l'ensemble des permutations de X

(Rq : $\mathfrak{S}_X = Bij(X)$)

- Si $n \in \mathbb{N}^*$ on note S_n ou $\mathfrak{S}_n$ l'ensemble $Bij(\llbracket 1, n \rrbracket)$

Fait fondamental :

$(\mathfrak{S}_X, \circ, Id_X)$ est un groupe, appelé groupe des permutations de X

Rq : $\mathfrak{S}_n$ est fini et $|\mathfrak{S}_n| = n!$

c) groupe produit

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

Ocsd $G \times H$ qu'on muni de la loi $\blacksquare$ définie par :

$$\underbrace{(x, y)}_{\in G\times H} \blacksquare \underbrace{(x', y')}_{\in G\times H} := (x \cdot x', y * y')$$

Fait fondamental :

$(G \times H, \blacksquare, (e_G, e_H))$ est un groupe appelé groupe produit de G par H.

3) Sous-groupes

a) def°

Def° : soit G un groupe et soit $H \subset G$

On dit que H est un sous groupe de G (pour $\cdot$) ⚠ ssi

(i) ⊛ $\forall x, y \in H, x \cdot y \in H$
("H stable par $\cdot$")

(ii) ⊛ $\forall x \in H, x^{-1} \in H$
("H est stable par passage à l'inverse")

(iii) ⊛ $e \in H$

Rq: en supposant (i) et (ii) on a (iii) $\Leftrightarrow H \neq \emptyset$

On notera H sgr G

Rq*: si H sgr G alors $(H, \circ|_{H\times H}^{H}, e_G)$ est un groupe

b) exemples

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

$(\mathbb{U}_3, \times, 1)$ sgr $(\mathbb{R}^*, x, 1)$

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

On a :

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

$(\mathbb{U}_3, \times, 1)$ sgr $(\mathbb{U}, \times, 1)$

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

Plaçons nous dans $(\mathbb{C}^*, \times, 1)$ et notons — au lieu de sgr et omettons les lois (toutes ×) et les neutres (tous 1)

On a :
$$\begin{tikzcd}
\mathbb{C}^* \arrow[r, dash] \arrow[d, dash] & \mathbb{U} \arrow[r, dash] & \mathbb{U}_{20} \arrow[r, dash] \arrow[dr, dash] & \mathbb{U}_5 & & \\
& & & \mathbb{U}_4 \arrow[r, dash] & \mathbb{U}_2 = \{-1,1\} \arrow[d, dash] & \\
\mathbb{R}^* \arrow[r, dash] \arrow[dr, dash] & \mathbb{R}_+^* \arrow[r, dash] & \mathbb{Q}_*^+ \arrow[urr, dash] & & \{1\} & \\
& \mathbb{Q}^* \arrow[ur, dash] & & & &
\end{tikzcd}$$

4) Sous groupe engendré *

a) déf°

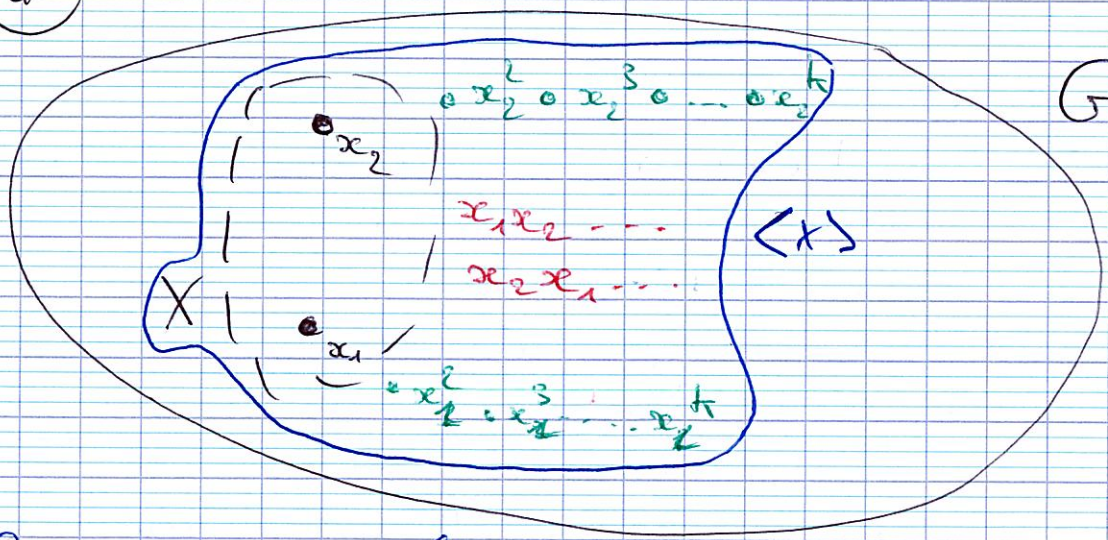
Soit G un groupe
(Rq un grp est tjs nonvide car $e \in G$)

Soit $X \subset G$ une partie qcq

Prop-def :

Il existe une + petite sous groupe de G contenant X.
On l'appelle sous groupe engendré par X et on le note $\langle X \rangle$

d°



AC Mq $\exists H \subset G : \left(H \text{ sgr } G \text{ et } X \subset H \text{ et } \forall K \subset G, \left.\begin{matrix} K \text{ sgr } G \\ X \subset K \end{matrix}\right\} \Rightarrow H \subset$

ie $\exists H \text{ sgr } G : (X \subset H \text{ et } \forall K \text{ sgr } G, X \subset K \Rightarrow H \subset K)$

D/ "par intérieur"

On pose $X' := X \cup \{x^{-1} ; x \in X\}$

On pose $H := \{x_1 x_2 \dots x_n ; n \in \mathbb{N}, x_1 \in X', \dots, x_n \in X'\}$

Alors 1) H sgr G : e+o $\left((x_1 x_2 \dots x_n)^{-1} = x_n^{-1} \dots x_1^{-1}\right)$
2) H convient : e+o

Lemme : Soit G grp
Soit $(H_i)_{i \in I}$ une famille de sgr de G

Alors $\bigcap_{i \in I} H_i$ sgr G

D/ Posons $H := \bigcap_{i \in I} H_i$

- $\hat{C}$ $\forall i$ ~~€~~ H_i sgr G donc $\forall i$, $e \in H_i$ donc $e \in \bigcap_{i \in I} H_i$

donc $e \in H$

- Soit $x \in H$ R* on a donc $\forall i$, $x \in H_i$

Soit $i \in I$; $x \in H_i$ et H_i sgr G donc $x^{-1} \in H_i$ par def.
Ainsi, on a mq $\forall i \in I$, $x^{-1} \in H_i$ ie $x^{-1} \in H$

~~Donc~~ Soient $x, y \in H$
On a donc R* : $\forall i$, $\begin{cases} x \in H_i \\ y \in H_i \end{cases}$

Soit $i \in I$: $\hat{C}$ $\left.\begin{matrix} x \in H_i \\ y \in H_i \end{matrix}\right\}$ $xy \in H_i$

Et ce $\forall i \in I$. Donc $xy \in \bigcap_{i \in I} H_i$ ie $xy \in H$ $\boxtimes$

Cas particulier :

H sgr G et K sgr $G \Rightarrow H \cap K$ sgr G

⚠ C'est complètement faux pour l'union

D/2 "par le haut"

On a G gp et on a $X \subset G$

On pose $\mathcal{E} := \{K \text{ sgr } G \mid X \subset K\}$

__But__ : trouver le + petit élément de $\mathcal{E}$

__Déjà__ : $\mathcal{E} \neq \emptyset$ car $G \in \mathcal{E}$

__Rq__ : G sgr G ; $\{e\}$ sgr G

- On pose $H := \bigcap_{K \in \mathcal{E}} K$; c'est sgr de G DACQP
- Ĉ $\forall K \in \mathcal{E}, X \subset K$, on a $X \subset H$
- De plus $\forall K \in \mathcal{E}, H \subset K$.
- Ainsi tout sgr K de G qui contient X contient H

Ie H convient

b) groupes monogènes et groupes cycliques

Rq : $\langle \emptyset \rangle = \{e\}$

Notation : si $x \in G$ on note aussi $\langle x \rangle$ au lieu de $\langle \{x\} \rangle$

Rq : Ainsi $\langle x \rangle$ est le + sgr de G qui contient x

On a (R*) $\langle x \rangle = \{ x^k ; k \in \mathbb{Z} \}$

Def : Soit G un grp

- On dit que G est monogène ssi

$$\exists x \in G : G = \langle x \rangle$$

- On dit que G est cyclique ssi

G monogène et G fini

exo

- Mq $(\mathbb{Z}, +, 0)$ est monogène
- Mq $\forall n \in \mathbb{N}^*, (\mathbb{U}_n, \times, 1)$ est cyclique

III) Morphismes de groupes

1) Definitions

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

Def :

Un morphisme (de groupe) de G dans H est une application
$$\varphi : G \longrightarrow H \quad tq$$
$$\forall x, y \in G, \quad \varphi(x \cdot y) = \varphi(x) * \varphi(y)$$

Rq : c'est une applications qui est compatible aux structures.

Rq : on dit aussi homomorphisme de groupes

On note $Hom_{(Gr)}(G, H)$ l'ensemble des morphismes de groupes de G dans H.

Fait (T) $Hom_{(Gr)}(G, H) \neq \emptyset$

D/ Ocsd $\varphi : \begin{array}{ccc} G & \longrightarrow & H \\ g & \longmapsto & e_H \end{array}$

avec $\cdot_H$

Soient $x, y \in G$. on a $\varphi(x \cdot y) = e_H$ et $\varphi(x) \cdot \varphi(y) = e_H \cdot e_H = e_H$

avec $\cdot_G$

Prop ⚠ : Soient G, H gp et soit $\varphi : G \to H$ un morphisme.

Alors :

1) On a $\varphi(e_G) = e_H$

2) On a $\forall x \in G,\ \varphi(x^{-1}) = \varphi(x)^{-1}$

Rq : Ainsi, les compatibilités au neutre et à l'inverse sont "gratuites"

D/ 1) On a $\varphi(\underbrace{e_G \cdot e_G}_{= e_G}) = \varphi(e_G) = \varphi(e_G) \cdot \varphi(e_G)$

Donc $\varphi(e_G)^{-1} \cdot \varphi(e_G) = \varphi(e_G)^{-1} \varphi(e_G)\, \varphi(e_G)$

Ie : $e_H = \varphi(e_G)$ ■ 1)

2) Soit $x \in G$

On a $\underbrace{\varphi(\underbrace{x \cdot x^{-1}}_{e_G})}_{= e_H} = \varphi(x) \cdot \varphi(x^{-1})$

ie on a $e_H = \varphi(x) \cdot \varphi(x^{-1})$

Donc $\varphi(x)^{-1} e_H = \varphi(x)^{-1} \varphi(x)\, \varphi(x^{-1})$ DLR ■

2) Composition

Soient G, H, K gp.

On csd ~~le diagramme~~ la situation

$$G \xrightarrow{\varphi} H \xrightarrow{\psi} K$$

__Prop__ :

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

D/ $\mathbb{I}^{++}$ (T)

$$(\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x) \cdot \varphi(y))$$

$$= \psi(\varphi(x)) \cdot \psi(\varphi(y)) = (\psi \circ \varphi)(x) \cdot (\psi \circ \varphi)(y)$$

■

__Def°__ : Un diagramme de groupes est la donnée de gps, reliées par des morphismes.

- Il est dit commutatif ssi le diagramme d'ensembles sous-jacent l'est.

3) Exemples

- $\exp : \mathbb{R} \longrightarrow \mathbb{R}_+^*$ est un morphisme entre

$$(\mathbb{R}, +, 0) \text{ et } (\mathbb{R}_+^*, \times, 1)$$

On a : $\exp(x+y) = \exp(x) \times \exp(y)$

- De m $\ln : \mathbb{R}_+^* \longrightarrow \mathbb{R}$ est un morphisme

- De m $\exp_{\mathbb{C}} : (\mathbb{C}, +, 0) \longrightarrow (\mathbb{C}^*, \times, 1)$

- ~~De m~~ la fonction $\sqrt{\cdot} : (\mathbb{R}_+^*, \times, 1) \longrightarrow (\mathbb{R}_+^*, \times, 1)$ est un morphisme

En effet : $\sqrt{xy} = \sqrt{x}\sqrt{y}$

- L'application $(\mathbb{R}, +, 0) \longrightarrow (\mathbb{U}, \times, 1)$ est un morphisme

$$t \longmapsto e^{it}$$

Def : Soit G g gp

Un endomorphisme (de gp) de G est un morphisme de G dans G

On note $\mathrm{End}_{(Gr)}(G)$, l'ensemble des endos de G

Rq : on a tjrs $\mathrm{Id}_G \in \mathrm{End}_{(Gr)}(G)$ et aussi $\tilde{e}_G \in \mathrm{End}_{(Gr)}(G)$

4) Tiré-en-arrière et poussé-en-avant

On csd le diag. de gp :

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

Et ocsd $G' \subset G$ et ocsd $H' \subset H$

Prop :

1) H' sgr $H \implies \varphi^{\langle -1 \rangle}[H']$ sgr G

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

D/ cf canevas

1. Osq H' sgr H. Mq $\varphi^{\langle -1 \rangle}[H']$ sgr G

- On a $\varphi(e_G) = e_H$; c H' sgr H : on a $e_H \in H'$

Donc $\varphi(e_G) \in H'$ ie $e_G \in \varphi^{\langle -1 \rangle}[H']$

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

On a $\varphi(x) \in H'$ et $\varphi(y) \in H'$

ĉ H' sgr H $\underbrace{\varphi(x) \cdot \varphi(y)} \in H'$

ie $\varphi(xy) \in H'$; ie $xy \in \varphi^{\langle -1 \rangle}[H']$

• On a $\varphi(x^{-1}) = \varphi(x)^{-1}$

$\hat{C}$ $\varphi(x) \in H'$ et $\hat{c}$ H' sgr H : on a $\varphi(x)^{-1} \in H$

Ie $\varphi(x^{-1}) \in H$ ie $x^{-1} \in \varphi^{\langle -1 \rangle}[H']$

■ 1)

2) Osq G' sgr G

• On a $e_G \in G'$ donc $\varphi(e_G) \in \varphi[G']$ R* AC

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

!! R* • Soient $\alpha, \beta \in \varphi[G']$ qu'on écrit $\alpha = \varphi(x)$ et $\beta = \varphi(y)$

avec $x, y \in G'$

Donc $\alpha\beta = \varphi(x)\varphi(y) = \varphi(xy)$

$\hat{C}$ x et $y \in G'$ et $\hat{c}$ G' sgr G, on a $xy \in G'$

Donc $\varphi(xy) \in \varphi[G']$ ie $\alpha\beta \in \varphi[G']$

• $\hat{C}$ G' sgr G et $\hat{c}$ $x \in G'$, on a $x^{-1} \in G'$

Donc $\varphi(x^{-1}) \in \varphi[G']$, or $\varphi(x^{-1}) = \varphi(x)^{-1}$
$= \alpha^{-1}$

Donc $\alpha^{-1} \in \varphi[G']$ ■

5) Noyau d'un morphisme

a) définition

Ocsd le diag. de gp :

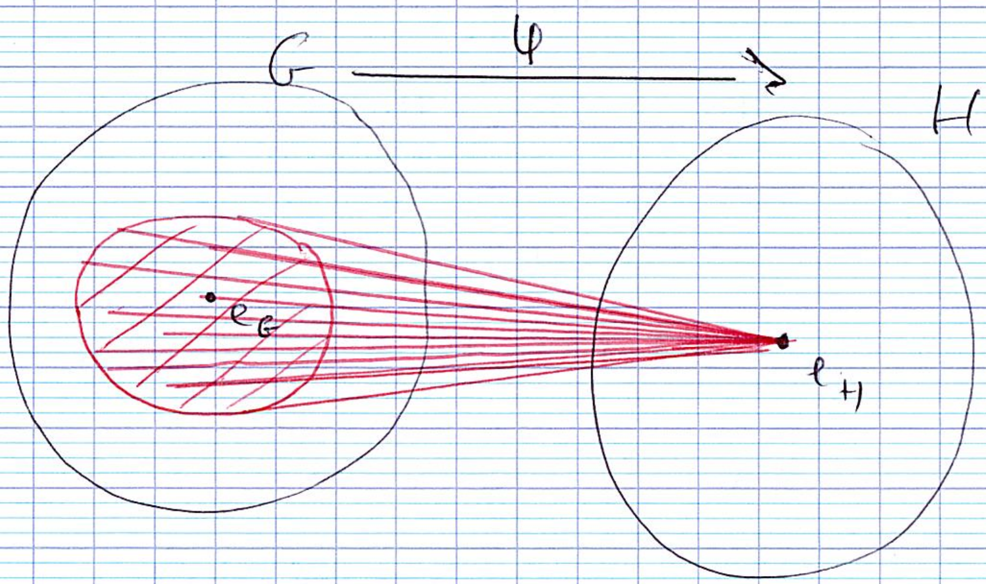
$$G \xrightarrow{\varphi} H$$

Def

Le noyau de φ, noté $\mathrm{Ker}(\varphi)$, est le sgrde$G$ défini par

$$\mathrm{Ker}(\varphi) := \left\{ x \in G \mid \varphi(x) = e_H \right\}$$

dn



sch^a

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \Big| \text{sgr} & & \\ \mathrm{Ker}(\varphi) & & \end{array}$$

D/ R* $\underline{Ker(\varphi) \text{ sgr } G}$

En effet $Ker(\varphi) = \varphi^{<-1>}[\{e_H\}]$

et $\{e_H\}$ sgr H (R_*) et DACQP

Ex :

Ocsd $\varphi : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{U}, \times, 1)$

$$t \longmapsto e^{it}$$

C'est un morphisme

On a $Ker(\varphi) = \{ t \in \mathbb{R} \mid e^{it} = 1 \}$

DALC, on a (T)

$$e^{it} = 1 \iff t \equiv 0 [2\pi]$$

Donc $Ker(\varphi) = \{ t \in \mathbb{R} \mid t \equiv 0 [2\pi] \}$

$= \{ 2\pi k ; k \in \mathbb{Z} \}$ noté $2\pi\mathbb{Z}$

Bilan $Ker(\varphi) = 2\pi\mathbb{Z}$

exo Pour $a \in \mathbb{Z}$, on note $a\mathbb{Z} := \{ ka ; k \in \mathbb{Z} \}$
C'est l'ensemble des multiples de a

Soit H sgr $(\mathbb{Z}, +, \circ)$

2) Alors : $\exists a \in \mathbb{Z} : H = a\mathbb{Z}$

1) Mq $\forall a \in \mathbb{Z}$, $a\mathbb{Z}$ sgr $(\mathbb{Z}, +, \circ)$

b) Caractérisation des morphismes inj

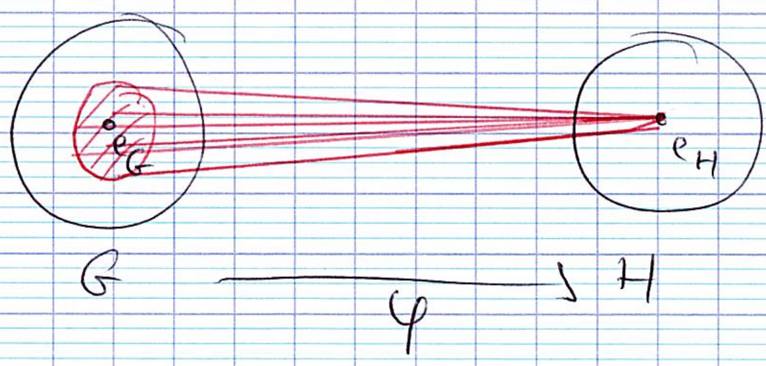
Prop - R^x

Soit $\varphi : G \longrightarrow H$ un morphisme entre deux gp

Alors :

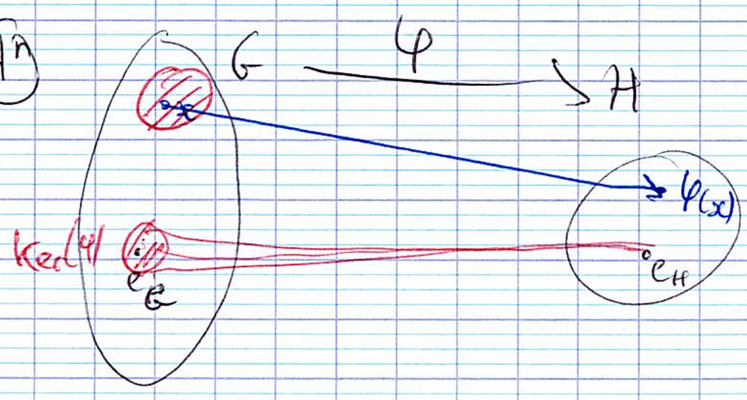
$$\varphi \text{ inj} \iff \operatorname{Ker}(\varphi) = \{e_G\}$$

dⁿ



Fait : $\operatorname{Ker}(\varphi) = G \iff \varphi = \tilde{e}_H$

dⁿ



D/

• Déjà : R^*, on a toujours $e_G \in Ker(\varphi)$ car on a tjrs,

$\varphi(e_G) = e_H$ (ou car $Ker(\varphi)$ sgr R^c)

• ($\Leftarrow$) Osq φ inj ; Mq $Ker(\varphi) = \{e_G\}$

• déjà : on a $\{e_G\} \subset Ker(\varphi)$

• récipqt : soit $x \in Ker(\varphi)$ R^* $\varphi(x) = e_H$

Or $\varphi(e_G) = e_H$ R^* ; donc $\varphi(x) = \varphi(e_G)$

Or φ inj donc $x = e_G$ donc $Ker(\varphi) \subset \{e_G\}$ $\Leftarrow$

• ($\Rightarrow$) Osq $Ker(\varphi) = \{e_G\}$

Mq φ inj

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

Mq $x = y$

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

Ie $\varphi(x)\varphi(y^{-1}) = e_H$ ie $\varphi(xy^{-1}) = e_H$

D'où $xy^{-1} \in Ker(\varphi)$ donc $xy^{-1} = e_G$

Donc $x = y$ ■

6) Image d'un morphisme

Soit $\varphi : G \longrightarrow H$ un morphisme (T)

Def° : L'image de φ, notée $\mathrm{Im}(\varphi)$, est le sgr H défini par

$$\mathrm{Im}(\varphi) := \varphi[G]$$

D/ C'est un sgr car G sgr G et DACQP ■

Prop°

$$\mathrm{Im}(\varphi) = H \iff \varphi \text{ surj}$$

D/ ok

Sch^a

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, dash] & H \arrow[d, dash] \\ \mathrm{Ker}(\varphi) & \mathrm{Im}(\varphi) \end{tikzcd}$$

7/ Isomorphismes

Soient G, H gp et $\varphi : G \to H$ ~~morphisme~~

Osq φ bij

On dispose donc $\underline{R^*}$ de $\varphi^{-1} : H \to G$ la bij réciproque de φ

$$\boxed{\underline{\text{Prop}} : \varphi \text{ morphisme} \Rightarrow \varphi^{-1} \text{ morphisme}}$$

D/ Osq φ morphisme

Mq φ^{-1} morphisme

Ie mq $\forall h, h' \in H$, $\varphi^{-1}(hh') = \varphi^{-1}(h) \cdot \varphi^{-1}(h')$

Soient $h, h' \in H$ (dⁿ) $G \longrightarrow H$

h, h'

__Posons__ $\boxed{g := \varphi^{-1}(h)}$ et $g' := \varphi^{-1}(h')$

(__ou__ $\hat{c}$ φ surj, __fixons__ $g, g' \in G$ tq $h = \varphi(g)$, $h' = \varphi(g')$)

$\vec{c}$ φ morphisme, on a $\varphi(gg') = \varphi(g)\varphi(g')$

Or $\boxed{\varphi(g) = h}$ et $\varphi(g') = h'$. Donc $\varphi(gg') = hh'$

Donc $\underbrace{\varphi^{-1}(\varphi(hh'))}_{1} = \varphi^{-1}(hh')$

Ie $hh' = \varphi^{-1}(hh')$

Ie $\varphi^{-1}(h)\varphi^{-1}(h) = \varphi^{-1}(hh')$ ∎

a) isomorphismes de groupes

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

Déf : On dit que φ est un isomorphisme (de gp) (iso)

$\overset{\Delta}{\text{ssi}}$ φ bij

- On a alors (R×) : $\varphi^{-1} : H \longrightarrow G$ est un (iso)morphisme

Rq : la "vraie" déf° est :

$$\varphi \text{ iso } \overset{\Delta}{\text{ssi}} \exists \psi : H \longrightarrow G \text{ morphisme } \begin{cases} \psi \circ \varphi = Id_G \\ \varphi \circ \psi = Id_H \end{cases}$$

b) automorphismes de groupes

Déf° : Un automorphisme de G est un isomorphisme de G dans G

On note $Aut_{(Gr)}(G)$ l'ensemble des automorphismes de G

Rq : on a tjrs (T) $Id_G \in Aut_{(Gr)}(G)$

Prop : $(Aut_{(Gr)}(G), \circ, Id_G)$ grpe

D/ exo ■

Notation : Si $\varphi : G \longrightarrow H$ iso, on note

$$\varphi : G \xrightarrow{\sim} H$$

Rq ① : $\left.\begin{array}{l}\varphi \text{ iso} \\ \psi \text{ iso}\end{array}\right\} \Rightarrow \psi \circ \varphi$ iso

c) groupes isomorphes

Def° : Soient G, H gp

On dit que G est isomorphe à H ssi ⚠

$\exists\, \varphi : G \longrightarrow H$ isomorphisme

On note $G \xrightarrow{\sim} H$

Rq ① : $G \simeq H \Rightarrow G$ et H equipotents

idée : ce sont les m̃ groupes

Ex :

On prend $\mathbb{Z} : \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

munie de $+$. On obtient le gp $(\mathbb{Z}, +, 0)$

On prend un autre ens. que $\mathbb{Z}$: on prend les $n \in \mathbb{Z}$ et on ajoute un $\sim$ au-dessus d'eux

On pose $\widetilde{\mathbb{Z}} = \{\ldots, \widetilde{-2}, \widetilde{-1}, \tilde{0}, \tilde{1}, \tilde{2}, \ldots\}$

On munit $\widetilde{\mathbb{Z}}$ d'une loi $\tilde{+}$ def par ① $\tilde{x} \,\tilde{+}\, \tilde{y} = \widetilde{x+y}$

Ex : $\tilde{2} \,\tilde{+}\, \tilde{3} = \tilde{5}$

Alors $(\mathbb{Z}, +, \circ) \simeq (\tilde{\mathbb{Z}}, \tilde{+}, \tilde{\circ})$

d/ exemples

Prop : $(\mathbb{R}_+^*, \times, 1) \simeq (\mathbb{R}, +, 0)$

D/ $\exp : \mathbb{R} \to \mathbb{R}_+^*$ est un morphisme de gp bij
ie un isomorphisme

~~Rq : si R est un anneau, on peut aussi de~~