
THEORIE DES GROUPES

DÉFINITION 2.1. *Un groupe $(G, \star, e_G, \cdot^{-1})$ est la donnee d'un quadruple forme de*

- *d'un ensemble G non-vide,*
- *d'une application (appelee loi de composition interne)*

$$\star : \begin{array}{ccc} G \times G & \mapsto & G \\ (g, g') & \mapsto & \star(g, g') =: g \star g' \end{array}$$

$g \star g' \neq g' \star g$ (en general)

- *d'un element $e_G \in G$ (appele element neutre),*
- *d'une application (appele inversion)*

$$\bullet^{-1} : \begin{array}{ccc} G & \mapsto & G \\ g & \mapsto & g^{-1} \end{array}$$

ayant les proprietes suivantes:

- *Associativite:* $\forall g, g', g'' \in G,\ (g \star g') \star g'' = g \star (g' \star g'')$ $= g * g' * g''$
- *Neutralite de e_G:* $\forall g \in G,\ g \star e_G = e_G \star g = g.$
- *Inversibilite:* $\forall g \in G,\ g^{-1} \star g = g \star g^{-1} = e_G.$

Exemples : $\mathfrak{S}_X$ $X \neq \emptyset$.

$(\mathfrak{S}_X = Bij(X;X), \circ, Id_X, \bullet^{-1})$

forme un groupe (le gp symetrique)

$X = \{1,2,3\}$

$G_3 = G_{\{1,2,3\}}$ a 6 elts

$Id_{\{1,2,3\}} = 1 \to 1 \quad 2 \to 2 \quad 3 \to 3$

(12) : $1 \to 2 \quad 2 \to 1 \quad 3 \to 3$

(23) : $1 \to 1 \quad 2 \to 3 \quad 3 \to 2$

(13) : $1 \to 3 \quad 2 \to 2 \quad 3 \to 1$

(123) : $1 \to 2 \quad 2 \to 3 \quad 3 \to 1$

(132) : $1 \to 3 \quad 2 \to 1 \quad 3 \to 2$

$(12)^{-1} = (12)$

$(123)^{-1} = (132)$

$(12) \circ (23)$: $1 \to 2$, $2 \to 3$, $3 \to 1$

$= (123)$

$(\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}, +, 0, n \to -n)$

$(\mathbb{N}, +, 0, n \to -n)$ pas un gpe : pas d'inversion

$(\mathbb{Q}, +, 0, n \to -n)$ gp

$(\mathbb{R}, +, 0, n \to -n)$ gp

$(\mathbb{Q}^* = \mathbb{Q} - \{0\}, \times, 1, x \to \frac{1}{x})$ et un gpe

$(\mathbb{Z} - \{0\}, \times, 1, \cdot^{-1})$ pas un gpe

$2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

$(\mathbb{Z}^\times = \{-1, +1\}, \times, 1, \cdot^{-1})$ est un gpe

Groupe trivial : $(\{e\}, *, e, \bullet^{-1} = Id_{\{e\}})$

Astérisque ou RHCP

$* : (e, e) \to e$

Groupe trivial

Gpe produit : $(G, \times)$ $(H, \cdot)$ des gpes

le produit $G \times H = \{(g,h) \quad g \in G \quad h \in H\}$

a une structure naturelle de gpe (gpe produit)

$$(g,h) \otimes (g',h') = (g \times g', h.h')$$

$\otimes$ est une loi associative

$$e_{G\times H} = (e_G, e_H)$$

$$(g,h)^{-1} = (g^{-1}, h^{-1})$$

$$(G\times H, \otimes, (e_G, e_H), (\bullet,\bullet)^{-1} = (\bullet^{-1}, \bullet^{-1}))$$

forme un gpe

Ex : $F(X, G) = G^X$

$G^X = \prod_{x \in X} G$ si $(G, \times)$ est notre gpe

$f_1, f_2 \in G^X$ $\quad f_1 = (f_1(x))_{x \in X}$ $\quad f_2 = (f_2(x))_{x \in X}$

$f_i(x) \in G$

$f_1 \otimes f_2 = (f_1(x) \times f_2(x))_{x \in X}$

Alternativement en voyant G^X comme un espace de fcts

$$f_1 \otimes f_2 : x \in X \to f_1(x) \times f_2(x)$$

La loi $\otimes$ est associative.

$$e_{F(X,G)} = \underline{e_G} : x \to e_G$$

$$f_1^{-1} : x \to f_1(x)^{-1}$$

1 eres Proprietes

PROPOSITION 2.1. *(Proprietes de base de la loi de groupe) Soit G un groupe. On a*

(1) Involutivite de l'inversion:

$$\forall g,\ (g^{-1})^{-1} = g,\ g^{-1} \star g = e_G.$$

(2) Unicite de l'element neutre: soit $e'_G \in G$ tel qu'il existe $g \in G$ verifiant $g \star e'_G = g$ alors $e'_G = e_G$. On a la meme conclusion si il existe g' tel que $e'_G \star g' = e'_G$.

(3) Unicite de l'inverse: si $g' \in G$ verifie $g \star g' = e_G$ alors $g' = g^{-1}$ et on a donc egalement $g' \star g = e_G$. De meme si $g' \in G$ verifie $g' \star g = e_G$ alors $g' = g^{-1}$ et on a donc egalement $g \star g' = e_G$.

(4) Inverse d'un produit: on a

$$(g \star g')^{-1} = g'^{-1} \star g^{-1}.$$

Preuve : ② e_G est unique : soit e'_G tq

$g * e'_G = g$ on multiplie les 2 termes de l'= par g^{-1} à gauche

$$g^{-1} * g * e'_G = g^{-1} * g = e_G$$

$$e'_G = e_G * e'_G = e_G .$$

③ soit g' tq $g * g' = e_G$

$$g^{-1} * g * g' = g^{-1} * e_G$$

$$= e_G * g' = g^{-1}$$

$$= g' = g^{-1} \bullet$$

① on a

$$(g^{-1})^{-1} * g^{-1} = e_G$$

d'autre part $g * g^{-1} = e_G$

$\Rightarrow$ g est l'inverse de g^{-1}

$\Rightarrow$ $(g^{-1})^{-1} = g$

④ pour mq

$$(g*g')^{-1} = g'^{-1} * g^{-1}$$

il suffit de mq

$$g'^{-1} * g^{-1} * (g*g') = e_G$$

car alors on aura $g'^{-1} * g^{-1}$ est l'inverse de $g*g'$

$$(g')^{-1} * g^{-1} * g * g' = (g')^{-1} * e_G * g'$$

$$= (g')^{-1} * g'$$

$$= e_G .$$

Abelien

Gpes Commutatif : Soit $(G, \cdot)$ un gpe

on dit que G est commutatif ssi

$$\forall g, g' \in G \quad g \cdot g' = g' \cdot g$$

Rmq: en particulier $(g \cdot g')^{-1} = (g')^{-1} \cdot g^{-1} = g^{-1} \cdot (g')^{-1}$

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

$(\mathbb{Q}^\times = \mathbb{Q} - \{0\}, \times, 1, \cdot^{-1})$

Si G est commutatif le gpe

$\mathcal{F}(X, G) = G^X$ est commutatif

$$\mathfrak{S}_3 = Bij(\{1,2,3\})$$

$$(12)\circ(23) = (123)$$

$$(23)\circ(12) = (132)$$

$\mathfrak{S}_3$ n'est pas commutatif.

$$\mathfrak{S}_2 = Bij(\{1,2\}) = \{Id_{\{1,2,3\}}, (12)\}$$

- Si p est premier et $(G, \cdot)$ est fini de cardinal $|G| = p$ alors G est commutatif.

$|X| \geq 3$ $\mathfrak{S}_X$ n'est pas commutatif

il existe $x_1, x_2, x_3 \in \mathfrak{S}_X$ tous distincts

soit $\sigma_{(12)} : x_1 \to x_2$ $x_2 \to 1$ et $x \to x$ si $x \neq x_1, x_2$

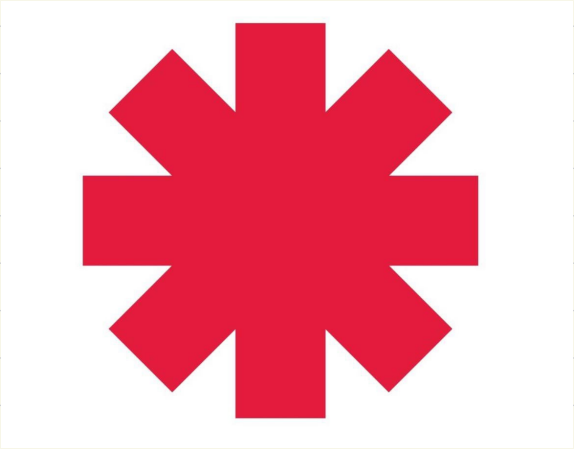
soit $\sigma_{(23)} : x_1 \to x_1$, $x_2 \to x_3$ $x_3 \to x_2$ et $x \to x$ si $x \neq x_2, x_3$

alors $\sigma_{(12)} \circ \sigma_{(23)} \neq \sigma_{(23)} \circ \sigma_{(12)}$

Ordre d'un Gpe: $(G, \cdot)$ = gpe

son ordre est $|G|$.

Exemple de Notation de lois de gpes



Notation Exponentielle

$(G, \cdot) = gpe \quad g \in G$

$g = g^1 \quad g \cdot g = g^2 \quad \underbrace{g \cdot \dots \cdot g}_{k \text{ fois}} = g^k$

$g^0 = e_G \quad g^{-1} = \text{l'inverse de } g \quad (g^{-1})^2 = g^{-1} \cdot g^{-1}$

$= (g^2)^{-1} = g$

si $k \geq 0$ $\quad g^{-k} = (g^k)^{-1} = (g^{-1})^k$

on définit pour tout $k \in \mathbb{Z}$ on définit

g^k

et on note $\quad g^{\mathbb{Z}} = \{ g^k \ k \in \mathbb{Z} \} = \{ \ldots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \ldots \}$

On a donc une application

$$g^{\bullet}, \exp_g(\bullet) : \mathbb{Z} \longrightarrow G$$
$$k \longrightarrow g^k$$

Prop : $\forall m, n \in \mathbb{Z}$
$g^{m+n} = g^m \cdot g^n$ | On dit que $g^{\bullet}$ est un morphisme de groupes entre $\mathbb{Z}$ et G

Notation Multiple

$(G,+)$ Commutatif. 0_G = elt neutre

$g \in G$ $\quad g+g = 2.g \quad g+g+g = 3.g$

$\underbrace{g+\dots+g}_{k \text{ fois } k \geq 1} = k.g$

$0.g = 0_G$

$-(2g) = (-g)+(-g)$

$= (-2).g$

$-(k.g) = k.(-g)$

$$\mathbb{Z}.g = \{ k.g \quad k \in \mathbb{Z} \}$$

On a $\mathbb{Z} \longrightarrow G$

$k \longrightarrow k.g$

Prop : $\forall m, n \in \mathbb{Z} \quad (m+n).g = m.g + n.g$

Sous-groupe :

Définition 2.4. *Soit $(G, \star, e_G, \bullet^{-1})$ un groupe. Un sous-groupe $H \subset G$ est un sous-ensemble de G tel que*

(1) $e_G \in H$.

(2) H *est stable pour la loi de composition interne* $\star$*:*

$$\forall h, h' \in H,\ h \star h' \in H.$$

(3) H *est stable par l'inversion:*

$$\forall h \in H,\ h^{-1} \in H.$$

Du coup $(H, \star, e_G, \bullet^{-1})$ est un gpe.

Exemples Bêtes:

- $H = G$ est un ssgpe de G
- $\{e_G\} \subset G$ est un ssgpe de G

ssgpe "trivial".

- $g \in G$ $\quad g^{\mathbb{Z}} = \{ g^k \mid k \in \mathbb{Z} \}$ est un ssgpe de G, $g = e_G$, $g^m \cdot g^n = g^{m+n}$, $(g^m)^{-1} = g^{-m}$

$g^{\mathbb{Z}}$ = le sous-gpe engendré par g

$:=: \langle g \rangle$

Exemples : $(\mathbb{Z}, +)$ $(\mathbb{N}, +)$ n'est pas un ssgpe

$2\mathbb{Z} = \{2k \ k \in \mathbb{Z}\}$ = ensemble des entiers pairs

= ensemble de multiples de .

est un ssgpe.

- $2\mathbb{Z}+1 = \{2k+1 \quad k \in \mathbb{Z}\}$ = ensemble des entiers impairs

= pas un ssgpe.

Classification des ssgpes de $\mathbb{Z}$

Thm : soit $q \in \mathbb{Z}$ et $q\mathbb{Z} = \{qk \ k \in \mathbb{Z}\}$ est un ssgpe de $\mathbb{Z}$ et tout ssgpe de $\mathbb{Z}$ est de la forme $q\mathbb{Z}$

Preuve : $q\mathbb{Z}$ est un ssgpe : pas trop dur.

Preuve : Soit $H \subset \mathbb{Z}$ un ssgpe

mq $H = q\mathbb{Z}$ pour $q \in \mathbb{Z}$

si $H = \{0\}$ on a fini.

sinon il existe $m \in H - \{0\}$

quitte à changer m en $-m$ ops que

$m > 0$

Donc H possede des elt > 0.

Soit $q \in H$ $q > 0$ et q le plus petit possible avec ces proprietes

Alors $H \overset{?}{=} q\mathbb{Z}$.

Soit $n \in H$ par division Euclidienne par q il existe $k \in \mathbb{Z}$ et $0 \leq r < q$ tq

$$n = q.k + r.$$

Je dis que $r \in H$: $n \in H$ $q.k \in H$

$\Rightarrow -qk \in H$ $n + (-qk) = n - qk \in H$

$\| \; r$

on sait que $0 \leq r < q$ et $r \in H$

$\Longrightarrow r = 0$ si $r > 0$ cela contredirait le fait que q st le + petit elt de $H > 0$.

$n - qk = 0 \Longleftrightarrow n = qk \in q\mathbb{Z}$

□

l'ensemble des ss gpes de $\mathbb{Z}$
est en bij avec $\mathbb{N}$

$q \in \mathbb{N} \longrightarrow q\mathbb{Z} \subset \mathbb{Z}$

$0.\mathbb{Z} = \{0\}$ $1.\mathbb{Z} = \mathbb{Z}$ $|<q$ $q\mathbb{Z}$ est un
ssgpe nontrivial
strict de $\mathbb{Z}$
$q\mathbb{Z} \subsetneq \mathbb{Z}$.

Sous-gpes engendré par un elt $(G, .)$

$g \in G \quad g^{\mathbb{Z}} = \{ g^k \ k \in \mathbb{Z} \} \subset G$

est un ssgpe de G appelé le ssgpe engendré par g

$$g^0 = e_G \cdot (g^k)^{-1} = g^{-k} \in g^{\mathbb{Z}}$$

$m \quad n \quad m+n$

$$g \cdot g = g$$

$$g^{\mathbb{Z}} = \langle g \rangle = \text{le + petit ssgpe contenant } g$$

Exemple: Les gpes symetriques sont universels:

Thm: to gpe $(G, .)$ peut-être identifié a un ssgpe d'un gp symetrique plus precisement un ssgp. de $\mathfrak{S}_G = Bij(G)$

PROPOSITION 2.2 (Critere de sous-groupe). *Pour montrer qu'un sous-ensemble non-vide*

$$\emptyset \neq H \subset G$$

est un sous-groupe il suffit de verifier que

(1) (a) $\forall h, h' \in H,\ h \star h' \in H,$
(b) $\forall h \in H,\ h^{-1} \in H.$

Alternativement il suffit de verifier que

(2) $\forall h, h' \in H,\ h \star h'^{-1} \in H.$

Preuve : de (2). $H \neq \emptyset$ soit $h \in H$

alors $h * h^{-1} \in H$

$\| e_G$

Comme $e_G \in H$ on sait $e_G * h^{-1} \in H$

$e_G * h^{-1} = h^{-1} \in H$

$\Rightarrow$ H est stable par $\bullet^{-1}$

H stable par $*$: $h, h' \in H$

$\Rightarrow (h')^{-1} \in H$ et donc

$h * h' = h * (h'^{-1})^{-1} \in H$

Thm (Lagrange) Soit $(G, \cdot)$ un gpe fini et $H \subset G$ un ssgpe alors

$|H|$ divise $|G|$

Preuve: plus tard quand on aurait fait les actions de gpes.

Cor: Si $|G| = p$ est premier alors

- tout ssgpe de G est soit $\{e_G\}$ soit G.
- G est commutatif ($g \cdot g' = g' \cdot g$)

Preuve : Soit $H \subset G$ un ssgpe

alors $|H| \mid |G| = p$ premier

$\Rightarrow |H| = 1$ ou $p = |G|$

si $|H| = 1 \Rightarrow H = \{e_G\}$

si $|H| = |G| \Rightarrow H = G$

G est commutatif : comme $|G| = p > 1$

il existe $g \in G$ $g \neq e_G$ soit

$g^{\mathbb{Z}}$ le ssgpe engendré par g

$g^{\mathbb{Z}} \neq \{e_G\} \Rightarrow g^{\mathbb{Z}} = G$

mais $g^{\mathbb{Z}}$ est commutatif :

$$g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$$

$\Rightarrow G$ est commutatif.

et $\forall g \in G - \{e_G\}$ $G = g^{\mathbb{Z}}$ $\square$

Définition 2.5. *Soit G un groupe et $g \in G$ un element de G. L'ordre de g est l'ordre du sous-groupe $g^{\mathbb{Z}} \subset G$ (ou $\mathbb{Z}.g$ si la notation est additive). On le note*

$$\mathrm{ord}(g) = |g^{\mathbb{Z}}| \ (= |\mathbb{Z}.g| \ \textit{en notation additive}).$$

Corollaire 2.2. *Soit G une groupe fini. Pour tout $g \in G$, l'ordre de g divise l'ordre de G:*

$$\mathrm{ord}(g) || G|$$

Ex: $G = G_3$ $Id_{\{1,2,3\}}$ est d'ordre 1

(12) est d'ordre 2

$(12)^{\mathbb{Z}} = \{Id, (12)\}$: $(12)^2 = (12)(12) = Id$

$(23)^{\mathbb{Z}} = \{Id, (2,3)\}$ ⇝ d'ordre 2

$(123)^{\mathbb{Z}} = \{Id, (123)(123)^2\}$

$(123)^0 = Id$ $(123)^1 = (123)$ $(123)^2 = (123)(123)$

$= (132)$

$(123)^3 = (123)^2 (123)$

$= (132)(123) = (1)(2)(3) = Id$

les elts de G_3 (qui est d'ordre 6)
sont d'ordre 1, 2 ou 3.

Ss Gpe engendré par un ensemble

$(G, .)$ $g \in G$ $g^{\mathbb{Z}} = \langle g \rangle$

Soit $A \subset G$ un ensemble on se demande si il existe un + petit ssgpe contenant A

Un tel ssgpe existe et on l'appelle le ssgpe engendré par A et on le note $\langle A \rangle \subset G$

PROPOSITION 2.3. *(Invariance par intersection) Soit G un groupe et $H_1, H_2 \subset G$ deux sous-groupes alors $H_1 \cap H_2$ est un sous-groupe. Plus generalement soit $H_i, i \in I$, $H_i \in G$ une collection de sous-groupes de G indexes par I alors*

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

est un sous-groupe de G.

Preuve: $I = \{1, 2\}$. Soient $H_1, H_2 \subset G$ des ssgpes on veut mq $H_1 \cap H_2$ est un ssgpe

Il suffit de mq $\forall\ h, h' \in H_1 \cap H_2$

$$h \cdot (h')^{-1} \in H_1 \cap H_2$$

$h, h' \in H_1 \Rightarrow h \cdot (h')^{-1} \in H_1$

$h, h' \in H_2 \Rightarrow h \cdot (h')^{-1} \in H_2$

$\Rightarrow h \cdot (h')^{-1} \in H_1 \cap H_2$

$H_1 \cap H_2 \neq \emptyset$ $\quad e_G \in H_1$ $e_G \in H_2$

$\Rightarrow e_G \in H_1 \cap H_2$

□

Exo: Redigez la preuve que

$\bigcap_{i \in I} H_i \subset G$ est un ssgpe.

Soit $A \subset G$ un ss ens de G

et soit $\mathcal{SG}_A = \{$ ssgpes de G contenant $A\}$

alors

$\bigcap_{H \in \mathcal{SG}_A} H$ est un ssgpe qui contient A

C'est le + petit ssgpe contenant A :

si $H' \subset G$ sg tq $A \subset H'$

alors $\bigcap_{H \in Sg_A} H \subset H'$

Définition 2.6. *Soit*

$$\mathcal{G}_A = \{H \subset G \text{ sous-groupe } | A \subset H\}$$

l'ensemble de tous les sous-groupes de G contenant A (cet ensemble est non-vide car G est dedans). Alors l'intersection de ses sous-groupes

$$\bigcap_{H \in \mathcal{G}_A} H \subset G$$

est un sous-groupe contenant A et c'est le plus petit (si H est un sous-groupe contenant A alors $\langle A \rangle \subset H$.) Ce sous-groupe

$$\langle A \rangle := \bigcap_{H \in \mathcal{G}_A} H$$

s' appelle le sous-groupe engendre par A.

Si $\langle A \rangle = G$ on dit que G est engendre par A (ou que A est un systeme de generateurs de G).

Rmq: si $A = \emptyset$ $\langle A \rangle = \langle \emptyset \rangle = \{e_G\}$

THÉORÈME 2.6 (Caracterisation linguistique du groupe engendre par un ensemble). *Soit $A \subset G$ un ensemble, si $A = \emptyset$ alors $\langle A \rangle = \{e_G\}$, sinon on pose*

$$A^{-1} = \{g^{-1},\ g \in A\} \subset G$$

l'image de A par l'inversion, alors

$$\langle A \rangle = \{g_1 \star \cdots \star g_n,\ n \geqslant 1,\ g_i \in A \cup A^{-1}\}.$$

En d'autres termes, $\langle A \rangle$ est l'ensemble des elements de G qu'on peut former en multipliant ensemble des elements de A et de son inverse A^{-1} de toutes les manieres possibles.

Preuve : Il suffit de mq

$M(A) = \{g_1 \star \cdots \star g_n,\ n \geqslant 1\ g_i \in A \cup A^{-1}\}$ est un

ssgr contenant A et que

tout ssgpe contenant A
contient $M(A)$.

① $M(A)$ contient A et est un ssgpe

$$A = \{g_i \ g_i \in A\} \subset M(A)$$

soient $h = g_1 * \dots * g_m \in M(A)$

$h' = g'_1 * \dots * g'_n \in M(A)$

$g_i, g'_j \in A \cup A^{-1}$ on veut montrer que

$h * (h')^{-1} \in M(A)$

$$h * (h')^{-1} = (g_1 * \cdots * g_m) * (g_1' * \cdots * g_n')^{-1}$$

$$= g_1 * \cdots * g_m * (g_n')^{-1} * \cdots * (g_1')^{-1}$$

$g_1 \in A \cup A^{-1}$, $g_m \in A \cup A^{-1}$

$(g_n')^{-1} * \cdots * (g_1')^{-1} \in A \cup A^{-1} = A \cup A^{-1}$

$\in M(A)$.

- Soit H ssgpe tq $A \subset H$

alors $A^{-1} \subset H^{-1} = H$

$A \cup A^{-1} \subset H$ si $g \in M(A)$

$g = g_1 * \dots * g_n$ $n \geq 1$ $g_i \in A \cup A^{-1} \subset H$

$\Rightarrow g \in H$ car H est stable par $*$ □

Ex: $\langle 2 \rangle = \mathbb{Z}.2$ $\langle 3 \rangle = \mathbb{Z}.3 \subset (\mathbb{Z}, +)$

$\langle 2, 3 \rangle =$ l'ensemble des sommes de multiples de 2 et de multiples de 3

$= \mathbb{Z}2 + \mathbb{Z}3$

$= \{ 2a + 3b \quad a, b \in \mathbb{Z} \}$

en particulier $(-2)+3 = 1 \in \langle 2,3 \rangle$

donc $\langle 2,3 \rangle \supset 1.\mathbb{Z} = \mathbb{Z}$

$$\langle 2,3 \rangle = \mathbb{Z}.$$

Plus généralement si m et n sont premiers entre eux alors $\langle m,n \rangle = \mathbb{Z}.m + \mathbb{Z}n$

$$= \mathbb{Z}$$

Si m et n sont premiers entre eux

Bezout dit que $\exists\, a, b \in \mathbb{Z}$ tq

$$am + bn = 1$$

$$\Rightarrow 1 \in \langle m, n \rangle$$

$$\Rightarrow \mathbb{Z} \cdot 1 = \mathbb{Z} \subset \langle m, n \rangle$$

$$\langle m, n \rangle = \mathbb{Z}.$$

En general si m, n sont qques

$$\langle m, n \rangle = \mathbb{Z}\, \text{pgcd}(m, n).$$

Morphisme de Gpes

Définition 2.8. *Soient $(G, \star)$ et $(H, *)$ deux groupes, un morphisme de groupes $\varphi : G \mapsto H$ est une application telle que*

$$\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g').$$

On notera

$$\mathrm{Hom}_{Gr}(G, H)$$

l'ensemble des morphismes de G vers H.

Terminologie : $\mathrm{Isom}_{Gr}(G,H)$ les morphismes bijectifs

↑ isomorphismes

si $H = G$ $\mathrm{Hom}_{Gr}(G,G) = \mathrm{End}_{Gr}(G)$

↑ Endomorphismes de Groupes

et $\mathrm{Isom}_{Gr}(G,G) = \mathrm{Aut}_{Gr}(G) \subset \mathrm{Bij}(G)$

↑ automorphismes de Groupes

THÉORÈME 2.7 (Propriete fonctionnelle d'un morphisme). *Soit $\varphi : G \mapsto H$ un morphisme de groupes alors*

(1) $\varphi(e_G) = e_H$,
(2) $\forall g \in G,\ \varphi(g^{-1}) = \varphi(g)^{-1}$,
(3) $\forall g, g' \in G,\ \varphi(g \star g') = \varphi(g) * \varphi(g')$.

Preuve : (1) soit $g \in G$ on a

$$g * e_G = g$$

$$\varphi(g * e_G) = \varphi(g)$$

$$\varphi(g) * \varphi(e_G) = \varphi(g) \Rightarrow \varphi(e_G) = e_H$$

② on calcule

$$\varphi(g) * \varphi(g^{-1}) = \varphi(g \star g^{-1})$$

$$= \varphi(e_G) = e_H$$

$$\Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$$

□

Exemples: $e_H : G \to H$

$g \to e_H$

- $g \in G$

$g^{\bullet} : k \in \mathbb{Z} \to g^k \in G$

$g^{m+n} = g^m \cdot g^n$

$$\cdot^{g} = \exp_g(\cdot) \in \mathrm{Hom}_{Gr}(\mathbb{Z}, G)$$

Cas particulier :

$$[\times q] : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ k & \to & q.k \end{array} \in \mathrm{End}_{Gr}(\mathbb{Z})$$

et un morphisme de $\mathbb{Z}$ vers $\mathbb{Z}$