



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

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

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

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

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

ayant les proprietes suivantes:

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

DÉFINITION 2.2. Soit $(G, \star)$ un groupe. Deux éléments g, g' commutent si

$$g \star g' = g' \star g.$$

Un groupe G est abélien (ou commutatif) si toutes les paires d'éléments de G commutent:

$$\forall g, g' \in G, \quad g \star g' = g' \star g.$$

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:

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

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 l'un ou l'autre des groupes de proprietes (1) ou (2) ci-dessous:

$$(1) \quad (a) \quad \forall h, h' \in H, h \star h' \in H,$$

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

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

Thm de Lagrange

THÉORÈME 2.4. Soit G un groupe fini et $H \subset G$ un sous-groupe alors l'ordre de H divise l'ordre de G :

$$|H| \mid |G|.$$

Co: Si $|G|$ est premier ses seuls ssgrs sont $\{e_G\}$ et G et $\forall g \in G - \{e_G\}$

$$G = \langle g \rangle.$$

En particulier G est commutatif.

Gpe Engendré

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 généralement soit $H_i, i \in I$, $H_i \in G$ une collection de sous-groupes de G indexés par I alors

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

est un sous-groupe de G .

Preuve: $H_1, H_2 \subset G$ sous-groupes de G

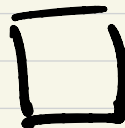
pour mq $H_1 \cap H_2$ est un ssgpe il suffit de mq

$$\forall h, h' \in H_1 \cap H_2 \Rightarrow h * h'^{-1} \in H_1 \cap H_2$$

- $h, h' \in H_1$ et comme H_1 est un sous-groupe
 $h * h'^{-1} \in H_1$

- $h, h' \in H_2$ et comme H_2 est un sous-groupe
 $h * h'^{-1} \in H_2$

$\Rightarrow h * h'^{-1} \in H_1 \cap H_2$



Def : $G = \text{gpe}$. $A \subset G$ un sseensemble.

alors il existe un + petit ssgpe contenant

A : $\bigcap_{\substack{H \subset G \text{ ssgpe} \\ A \subset H}} H$ est un ssgpe de G contenant A et c'est bien le + petit possible.

Rmq : l'intersection n'est pas sur un ensemble vide car G est un ssgpe de G contenant A .

Def: Cette intersection est le
ssgpe engendré par A .

On le note $\langle A \rangle \subset G$

Ex: $A = \emptyset$ $\langle \emptyset \rangle = \{e_G\}$

Exemple: $g^{\mathbb{Z}} = \{ g^n \mid n \in \mathbb{Z} \}$ est un ssgrpe
de G et c'est le + petit ssgrpe contenant
 g .

$$g^{\mathbb{Z}} = \text{ssgrpe} \text{ car } g^m * g^n = g^{m+n}$$

$$\langle g \rangle = g^{\mathbb{Z}}.$$

Example: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

$$\mathbb{Z}/_q \mathbb{Z} = \{a(q) \mid a \in \mathbb{Z}\}$$

$$a(q) := a + q\mathbb{Z}$$

$$\cdot \quad \mathbb{Z}/_q \mathbb{Z} = \{a(q) \mid 0 \leq a \leq q-1\}$$

$$\mathbb{Z}/_q \mathbb{Z} = \langle 1(q) \rangle = \langle a(q) \rangle$$

pour $a \wedge q = 1 = \text{pgcd}(a, q)$

DÉFINITION 2.7. Un groupe G est dit

- monogène si il est engendré par un seul élément:

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

On dit que g est un générateur de G .

- cyclique si il est fini et monogène.

Ex: $\mathbb{Z}$ est monogène

$\mathbb{Z}/q\mathbb{Z}$ est cyclique.

$$\begin{array}{l} A \subset G \quad \langle A \rangle \\ A = \{g\} \quad \langle \{g\} \rangle = \langle g \rangle. \end{array}$$

THÉORÈME 2.4 (Caractérisation linguistique du groupe engendré 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

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

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

Preuve: pour mq que $\{g_1 \star \dots \star g_n \mid g_i \in A \cup A^{-1}\}$ est égal à $\langle A \rangle$ il suffit de mq

- $A \subset \{g_1 \star \dots \star g_n \mid g_i \in A \cup A^{-1}\}$
- $\{g_1 \star \dots \star g_n \mid g_i \in A \cup A^{-1}\}$ est un ssgr

- et que tout ss gpe H contenant A
contient $\{g_1 + \dots + g_n \mid n \geq 1, g_i \in A \cup A^{-1}\}$.

- $A \subset \{g_1 + \dots + g_n \mid n \geq 1, g_i \in A \cup A^{-1}\}$
 $g \in A$ $g =$ un produit d'un seul elt de $A \cup A^{-1}$
 $\in \{g_1 + \dots + g_n \mid n \geq 1, g_i \in A \cup A^{-1}\}$

$\{g_1 * \dots * g_n \mid n \geq 1, g_i \in A \cup A^{-1}\}$ est un ss gpe

on utilise le critere:

$$g = g_1 * \dots * g_n, \quad g' = g'_1 * \dots * g'_m$$

$$g_1, \dots, g_n, g'_1, \dots, g'_m \in A \cup A^{-1}$$

$$g * g'^{-1} = g_1 * \dots * g_n * g_m^{-1} * g_{m-1}^{-1} * \dots * g_1^{-1}$$

= produit de $m+n$ elts de $A \cup A^{-1}$.

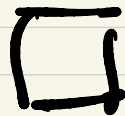
on mq si $A \subset H \subset G$
 $\uparrow$ sspe alors

$$H \supset \{g_1 * \dots * g_n \mid g_i \in A \cup A^{-1}\}$$

$$\text{car si } A \subset H \Rightarrow A^{-1} \subset H^{-1} = H$$

$$\Rightarrow A \cup A^{-1} \subset H$$

et H est stable par $*$...



Ex: $\mathbb{Z} \langle 2 \rangle = 2\mathbb{Z} \subsetneq \mathbb{Z}$

$$\langle 3 \rangle = 3\mathbb{Z} \subsetneq \mathbb{Z}$$

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

Plus généralement si

$$a \wedge b = 1 \quad \langle a, b \rangle = \mathbb{Z}$$

(a', b)



Morphismes de G -pres

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

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

l'ensemble des morphismes de G vers H .

THÉORÈME 2.6 (Propriété 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 calcule de deux manières

$$\begin{aligned} \varphi(g * e_G) &= \varphi(g) \\ &= \varphi(g) * \varphi(e_G) \end{aligned}$$

$$\begin{aligned} \text{on a que } \varphi(g) &= \varphi(g) * \varphi(e_G) \\ \Rightarrow \varphi(e_G) &= e_H \end{aligned}$$

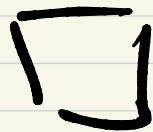
(2) $\forall g \in G$ on calcule de 2 manières

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

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

$$= e_A$$

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



Examples: Morphisme trivial

$$- \forall g \quad \varphi(g) = e_H$$

$$- (G, *) \quad g \in G$$

$$g^\bullet : (\Pi, +) \longrightarrow (G, *)$$

$$\text{C'est morphisme car } g^m \xrightarrow{g^{m+n}} g^{m+n} = g^m * g^n.$$

- $(G, +_G)$ un grpe commutatif
note additive

• $g: \begin{array}{ccc} & g \in G & \\ \mathbb{Z} & \longrightarrow & G \\ m & \longrightarrow & m \cdot g = \underbrace{g +_G g +_G \dots +_G g}_{m \text{ fois.}} \end{array}$

$$(m+n) \cdot g = m \cdot g +_G n \cdot g.$$

$$- \exp: (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \cdot)$$

$$x \longrightarrow e^x = \exp(x)$$

$$e^{x+y} = e^x \cdot e^y$$

$$- \ln: (\mathbb{R}_{>0}, \cdot) \longrightarrow (\mathbb{R}, +)$$

$$\ln(u \cdot v) \longrightarrow \ln(u) + \ln(v)$$

$$\mathbb{Z}/q\mathbb{Z} = \{a(q) \mid a \in \mathbb{Z}\}$$

$$\bullet (q): (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/q\mathbb{Z}, +_q)$$

$$a \longrightarrow a(q) = a + q\mathbb{Z}$$

$$a + b(q) = a(q) +_q b(q)$$

$$= a + b + q\mathbb{Z}$$

Non-morphisme de Gpe.

$$\bullet +): \quad \begin{array}{ccc} (\mathbb{Z}_+, +) & \longrightarrow & (\mathbb{Z}_+, +) \\ n & \longmapsto & n+1 \end{array}$$

pas un morphisme de gpe:

$$0_{\mathbb{Z}+1} = 1 \neq 0_{\mathbb{Z}}$$

Question: trouvez tous le morphisme

$$\varphi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +).$$

Noyau - Image

PROPOSITION 2.4. (Invariance des sous-groupes par morphismes) Soit $\varphi \in \text{Hom}_{\text{Gr}}(G, H)$ un morphisme de groupes.

(1) Soit $K \subset G$ un sous-groupe alors $\varphi(K) \subset H$ est un sous-groupe. En particulier l'image de φ ,

$$\text{Im}(\varphi) = \varphi(G) \subset H$$

est un sous-groupe de H .

(2) Soit $L \subset H$ un sous-groupe de H , alors la preimage

$$\varphi^{(-1)}(L) = \{g \in G, \varphi(g) \in L\} \subseteq G$$

est un sous-groupe de G . En particulier $\varphi^{(-1)}(\{e_H\})$ est un sous-groupe de G .

Preuve: Soit $K \subset G$ un ssgpe pour mq
 $\varphi(K) = \{\varphi(k) \mid k \in K\}$ est un ssgpe !
 suffit de mq $\forall h, h' \in \varphi(K) \quad h * h'^{-1} \in \varphi(K)$

$$h, h' \in \varphi(K) \Rightarrow \begin{aligned} h &= \varphi(k) \\ h' &= \varphi(k') \end{aligned} \quad k, k' \in K$$

$$h * h'^{-1} = \varphi(k) * \varphi(k')^{-1}$$

$$= \varphi(k * k'^{-1}) \in \varphi(K)$$

$k * k'^{-1} \in K$ car K est un ssgpe de G .

- $L \subset H$ un ssgrpe pour mq

$\phi^{(-1)}(L) \subset G$ est un ssgrpe il suffit
de mq si $g, g' \in \phi^{(-1)}(L)$ alors

$$g * g'^{-1} \in \phi^{(-1)}(L) ?$$

$$\phi(g), \phi(g') \in L$$

et comme L est un ssgr

$$\varphi(y) * \varphi(g')^{-1} \in L$$

"

$$\varphi(g * g'^{-1}) \in L$$

$$\Rightarrow g * g'^{-1} \in \varphi^{(-1)}(L)$$



DÉFINITION 2.9. Le sous-groupe $\varphi^{(-1)}(\{e_H\})$ s'appelle le noyau de φ et est noté

$$\ker(\varphi) = \varphi^{(-1)}(\{e_H\}) = \{g \in G, \varphi(g) = e_H\}.$$

THÉORÈME 2.7 (Critère d'injectivité). Soit $\varphi \in \text{Hom}_{Gr}(G, H)$ un morphisme de groupes alors les propriétés suivantes sont équivalentes

(1) φ est injectif,

(2) $\ker(\varphi) = \{e_G\}$.

Preuve: si φ est injectif, $\Leftrightarrow \forall h \in H$
 $\varphi^{(-1)}(\{h\})$ a au plus 1 elt.
- Si on l'applique à $h = e_H$
 $\varphi^{(-1)}(\{e_H\})$ a au plus 1 elt

mais $e_G \in \varphi^{(-1)}(\{e_H\})$ car

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

Donc $\varphi^{(-1)}(\{e_H\}) = \{e_G\}$ si φ inject

— Réciproquement supposons que

$$\varphi^{-1}(\{e_H\}) = \{e_G\}$$

Soit $h \in H$ et $g, g' \in \varphi^{(-1)}(\{h\})$

on veut mq $g = g'$ ou a

$$\varphi(g) = \varphi(g') = h$$

$$\begin{aligned} \Rightarrow \varphi(g) * \varphi(g')^{-1} &= e_H \\ &= \varphi(g * g'^{-1}) = e_H \end{aligned}$$

$\Rightarrow$ donc $g * g'^{-1}$ est un antécédent
de e_H

et il vaut e_G par hypothèse

$$\left(\varphi^{(-1)}(\{e_H\}) \right) = \{e_G\}$$

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

$$\Rightarrow g = g' \quad \square$$

$(G, \cdot)$

THÉORÈME 2.8. Soit $\varphi : G \mapsto H$ un morphisme de groupes et $\ker(\varphi) \subset G$ son noyau. Alors pour tout $g \in G$ on a l'égalité suivante entre ensembles

$$g \cdot \ker(\varphi) \cdot g^{-1} = \{g \cdot k \cdot g^{-1}, k \in \ker(\varphi)\} = \ker(\varphi).$$

Preuve: soit $k \in \ker \varphi$ et
 $g \in G$ on veut montrer $gkg^{-1} \in \ker \varphi$
c'est-à-dire $\varphi(gkg^{-1}) = e_H$.

$$\begin{aligned}\varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g)^{-1} \\ &= \varphi(g)*e_H*\varphi(g)^{-1} \\ &= \varphi(g)*\varphi(g)^{-1} = e_H\end{aligned}$$

$$\Rightarrow \forall g \in G \quad g \cdot \ker \varphi \cdot g^{-1} \subset \ker \varphi$$

$$\Rightarrow g^{-1} \cdot (g \ker \varphi g^{-1}) g \subset g^{-1} \cdot \ker \varphi \cdot g$$

$$\ker \varphi \subset g^{-1} \cdot \ker \varphi \cdot g$$

On a mg $\forall g \in G \quad \ker \varphi \subset g^{-1} \cdot \ker \varphi \cdot g$

on remplace $g \leftrightarrow g^{-1} \Rightarrow \ker \varphi \subset g \cdot \ker \varphi \cdot g^{-1} \quad \square$

DÉFINITION 2.10. Un sous-groupe $K \subset G$ ayant la propriété que pour tout $g \in G$ on a

$$\forall g \in G \quad g.K.g^{-1} = K$$

est dit normal ou distingué et on le note

$$K \triangleleft G.$$

Rmq: G commutatif. Tout sous-groupe est distingué
si G est commutatif

$$g.K.g^{-1} = g.g^{-1}.K = e_G.K = K.$$

Rmq: On a $K \triangleleft G$ ssi

$$\forall g \in G \quad gKg^{-1} \subseteq K.$$

$\Rightarrow$ Cela implique que $\forall g \quad gKg^{-1} = K.$

Rmq ker $\varphi \triangleleft G$. Tout Noyau est distingué

la réciproque est vraie :

si $K \triangleleft G$ est un sous-groupe distingué de G

il existe un morphisme $\varphi: G \rightarrow H$

tg ker $\varphi = K$. Notion gpe quotient.
 $\mathbb{Z}/9\mathbb{Z}$

$$g^\bullet: \mathbb{Z}_m \longrightarrow G$$

THÉORÈME 2.9. Soit G un groupe, $g \in G$ un element et $q \in \mathbb{N}$ un entier naturel tel que

$$q\mathbb{Z} = \ker(g^\bullet).$$

- Si $q = 0$ alors $\ker(g^\bullet) = \{0\}$ et $g^\bullet$ est injectif et ainsi on a un isomorphisme de groupes (un morphisme de groupes bijectif)

$$\mathbb{Z} \simeq g^\bullet = \langle g \rangle$$

On a alors

$$\text{ord}(g) = |\mathbb{Z}| = \infty.$$

- Si $q > 0$, alors q est le plus petit entier strictement positif verifiant

$$g^q = e_G$$

et on a

$$\text{ord}(g) = |g^\bullet| = q.$$

- Si G est fini on a $\text{ord}(g) \mid |G|$ et $g^{|G|} = e_G$.

Preuve : $g^\bullet : (\mathbb{T}, +) \longrightarrow (G, *)$

$$m \longrightarrow g_m^m$$

ker $g^\bullet$ est un ss gpe de $\mathbb{T}$

$$\begin{aligned} \ker g^\bullet &= \{ m \in \mathbb{T} \mid g_m^m = e_G \} \\ &= q\mathbb{T} \quad q \geq 0 \end{aligned}$$

Si $q=0$ $\ker g^\bullet = 0, \mathbb{Z} = \{0\}$

par le critère d'injectivité $g^\bullet: \mathbb{Z} \hookrightarrow G$

en particulier $g^\bullet$ définit une
bijection entre $\mathbb{Z}$ et

$$\text{Im}(g^\bullet) = g^\bullet \mathbb{Z} = \langle g \rangle \subset G$$

G contient un ssgr en bij avec $\mathbb{Z}$

$$|g^{\mathbb{Z}}| = \infty \Rightarrow |G| = \infty.$$

- Si $q \geq 1$.

$$\ker g^{\bullet} = \{ m \in \mathbb{Z} \mid q g^m = e_G \}$$

$$= q\mathbb{Z} \quad q \geq 1$$

la preuve du fait que les ss gpe de $\mathbb{Z}$ sont de la forme $q\mathbb{Z} \quad q \geq 0$

dit que q est le + petit entier > 0
tq $q \in \ker(g^\bullet)$

$$\Leftrightarrow q = \text{le + petit entier } > 0 \text{ tq } g^q = e_G.$$

Je dis alors que $\pi_g = \{e_G, g, g^2, \dots, g^{q-1}\}$

et que tous ces elts $\{e, g, g^2, \dots, g^{q-1}\}$
sont distincts $\Rightarrow |g^{\mathbb{Z}}| = q$.

Preuve de cela; soit $m \in \mathbb{Z}$
on fait la div euclidienne de m par q
$$m = qk + r \quad k \in \mathbb{Z} \quad 0 \leq r \leq q-1$$

$$\begin{aligned}
 g^m &= g^{qk+r} \\
 &= (g^q)^k \cdot g^r \\
 &= e_k \cdot g^r = g^r
 \end{aligned}$$

Done $g^m = g^r$ where $0 \leq r \leq q-1$

$$g^\Pi = \{g^r \mid 0 \leq r \leq q-1\}$$

soient $0 \leq r \leq r' \leq q-1$

$$\text{tq } g^r = g^{r'} \implies g^{r'-r} = e_G$$

$$\implies r' - r = q^m \quad m \geq 0$$

$$\text{mais } 0 \leq r' - r \leq q-1$$

$$\implies m=0 \quad r'=r$$

$$\implies g^\mathbb{F} = \{g^r \mid 0 \leq r \leq q-1\} \quad q \text{ est cardinal}$$

Supposons G est fini par Lagrange

$$q = |g^{\mathbb{Z}}| \text{ divise } |G|$$

$$|G| = q \cdot n \quad n \geq 1$$

$$g^{|G|} = g^{qn} = (g^q)^n = e_6^n = e_6$$



Exo: Soit G un gr, $g \in G$

$$\text{Ad}_g : h \in G \rightarrow ghg^{-1}$$

- $\forall g$ Ad_g est un morphisme de grs

- Ad_g est bijectif et calculer

$$(\text{Ad}_g)^{-1}.$$

Opérations sur les morphismes de G es

Notation/Terminologie. On notera

- $\text{Hom}_{Gr}(G, H)$ l'ensemble des morphismes de groupes de G vers H ,
- $\text{Inj}_{Gr}(G, H)$ l'ensemble des morphisme injectifs (qu'on appelle également *monomorphismes* de groupes),
- $\text{Surj}_{Gr}(G, H)$ l'ensemble des morphisme surjectifs (qu'on appelle également *epimorphismes* de groupes), et
- $\text{Isom}_{Gr}(G, H)$, l'ensemble des morphisme de groupes bijectifs (qu'on appelle lgalement *isomorphismes* de groupes).
- Si $H = G$, on ecrit notera ces ensembles

$$\text{Hom}_{Gr}(G), \text{Inj}_{Gr}(G), \text{Surj}_{Gr}(G), \text{Isom}_{Gr}(G);$$

en particulier l'ensemble des morphismes de G sur lui-meme $\text{Hom}_{Gr}(G)$ est aussi appelle ensemble des *endomorphismes* du groupe G et est egalemt note

$$\text{Hom}_{Gr}(G) = \text{End}_{Gr}(G).$$

L'ensemble des endomorphismes bijectifs (isomorphismes) de G sur lui-meme est note

$$\text{Aut}_{Gr}(G) = \text{Isom}_{Gr}(G, G)$$

est est appele l'ensemble des automorphismes de G .

PROPOSITION 2.5. (Invariance par composition et par reciproque) Soient $(G, \star), (H, *), (K, \otimes)$ des groupes et

$$\varphi : G \mapsto H \text{ et } \psi : H \mapsto K$$

des morphismes de groupes alors la composee $\psi \circ \varphi : G \mapsto K$ est un morphisme de groupes.

Supposons que $\varphi : G \mapsto H$ un morphisme de groupes bijectif alors l'application reciproque

$$\varphi^{-1} \in \text{Hom}_{\text{Gr}}(H, G)$$

est un morphisme de groupe bijectif.

Preuve: $\varphi \in \text{Hom}_{\text{Gr}}(G, H) \quad \psi \in \text{Hom}_{\text{Gr}}(H, K)$

$$\psi \circ \varphi : g \mapsto \psi(\varphi(g))$$

$$\begin{aligned} \psi \circ \varphi (g * g') &= \psi(\varphi(g * g')) = \psi(\varphi(g) * \varphi(g')) \\ &= \psi(\varphi(g)) \otimes \psi(\varphi(g')) \end{aligned}$$

Soit $\varphi \in \text{Isom}_{Gr}(G, H)$ un morphisme

on veut mq $\varphi^{-1}: H \rightarrow G$ est un morphisme

bijectif

? $\forall h, h' \in H \quad \varphi^{-1}(h * h') \stackrel{?}{=} \varphi^{-1}(h) * \varphi^{-1}(h')$

pour mq ces 2 elts de G sont égaux

il suffit de mq leurs image par φ

sont égales : ils seront les antécédents d'un
 $\hat{m}$ elt^o de H et comme φ est bij ils
seront $=$.

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

$$\begin{aligned}\varphi(\varphi^{-1}(h) * \varphi^{-1}(h')) &= \varphi(\varphi^{-1}(h)) * \varphi(\varphi^{-1}(h')) \\ &= h * h' \quad \square\end{aligned}$$

COROLLAIRE 2.4. L'ensemble des automorphismes de G

$$\text{Aut}_{Gr}(G) \subset \text{Bij}(G) = \mathcal{G}_G$$

est un sous-groupe pour la composition $\circ$.

Preuve: on applique le critère de sous-groupe

$$\varphi \in \text{Aut}_{Gr}(G) \quad \psi \in \text{Aut}_{Gr}(G)$$

$$\text{on veut montrer que } \psi^{-1} \circ \varphi \in \text{Aut}_{Gr}(G)$$

$$- \psi^{-1} \circ \varphi \in \text{Bij}(G) \quad (\text{Bij}(G) \text{ est un groupe})$$

- on a vu que $\psi^{-1} \in \text{End}_G(G) = \text{Hom}_G(G, G)$

et que $\text{Hom}_G(G, G)$ est stable par $\circ$

$$\psi^{-1} \circ \varphi \in \text{Hom}_G(G, G) \cap \text{Bij}(G, G)$$

$$\parallel$$
$$\text{Aut}_G(G)$$

$\square$

Grps Isomorphes: Deux Gps sont dit isomorphes si il existe un isomorphisme entre les deux $\varphi: G \xrightarrow{\sim} H$

φ morphisme de gpes.

- Il en resulte que du point de vue de la theorie des gpes G et H ont les m[^]me propriete.

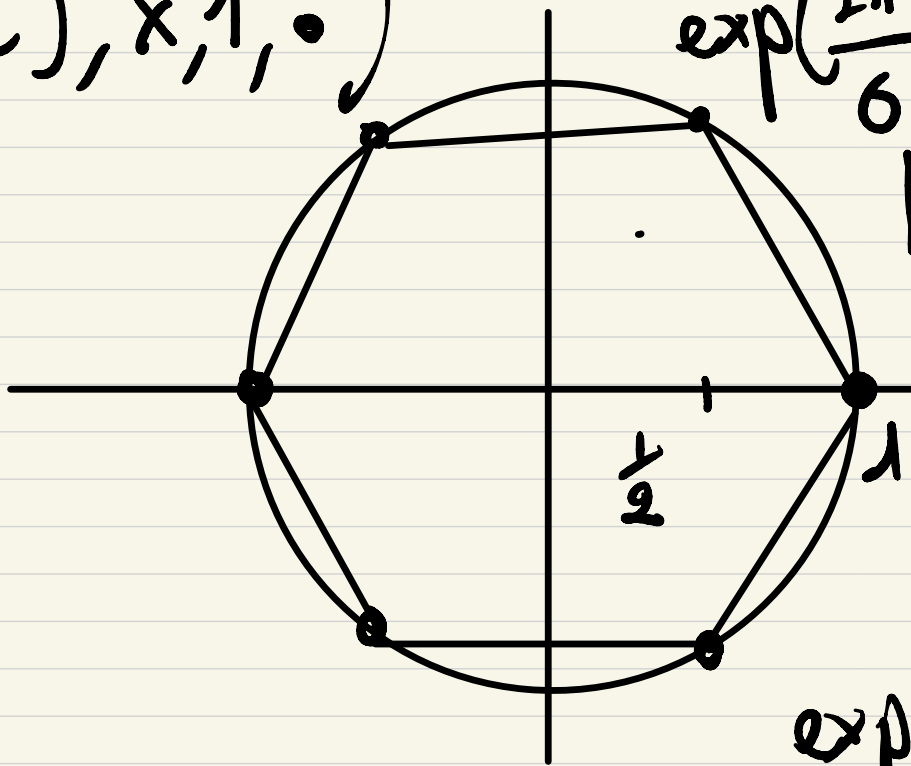
Example: $(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \times)$
 $\exp(\cdot)$

$$(\mathbb{Z}/q\mathbb{Z}, +_q) \simeq \mu_q(\mathbb{C}) = \{z \in \mathbb{C} \mid z^q = 1\}$$

$$= \left\{ \exp\left(\frac{2\pi i k}{q}\right), 0 \leq k \leq q-1 \right\}$$

$$k(q) = k + q\mathbb{Z} \longrightarrow \exp\left(\frac{2\pi i k}{q}\right)$$

$$(p_9(\mathbb{C}), x, 1, \cdot^{-1})$$



$$\exp\left(\frac{2\pi i}{6}\right)$$

$$p_6(\mathbb{C})$$

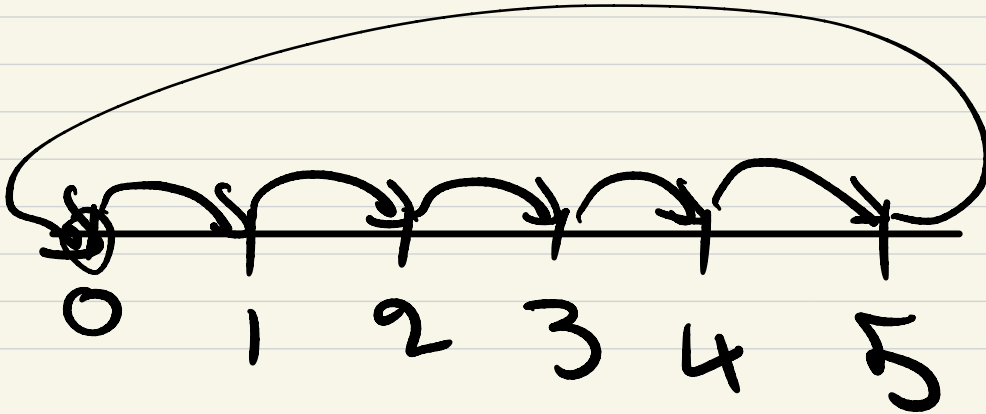
$$\exp\left(\frac{2\pi i}{6}\right)^6 = 1$$

$0(6), 1(6), 2(6), 3(6), 4(6), 5(6)$

$$0(6) + 1(6) = 1(6)$$

$$1(6) + 1(6) = 2(6)$$

$$2(6) + 1(6) = 3(6)$$



Rmq: si $k' \in \mathbb{Z}$ et tel que

$$k'(q) = k(q)$$

alors $\exp\left(\frac{2\pi i k'}{q}\right) = \exp\left(\frac{2\pi i k}{q}\right)$

si $k'(q) = k(q)$ $k' = k + ql$ $l \in \mathbb{Z}$

$$\exp\left(\frac{2\pi i k'}{q}\right) = \exp\left(\frac{2\pi i k}{q} + \frac{2\pi i ql}{q}\right)$$

$$= \exp\left(\frac{2\pi i k}{q}\right) \underbrace{\exp(2\pi i \ell)}_{1} \quad \ell \in \mathbb{Z}$$

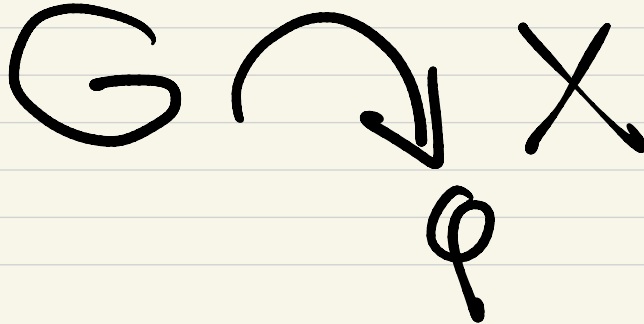
Action d'un gpe sur un
ensemble

$$(G_X, \circ)$$

DÉFINITION 2.11. Soit $(G, \star)$ un groupe, X un ensemble et $(\text{Bij}(X), \circ)$ le groupe symétrique de X (des bijections de X sur lui-même). Une action (à gauche) de G sur X est la donnée d'un morphisme

$$\varphi : G \mapsto \text{Bij}(X).$$

On dit alors que G agit sur X (à gauche) à travers le morphisme φ et on le note $G \curvearrowright_{\varphi} X$.



$$X \text{ ens } \neq \emptyset \quad \sigma \in \text{Bij}(X)$$

On fabrique une action de $\mathbb{Z}$ sur X
en posant

$$\begin{aligned} \bullet & \quad \sigma : (\mathbb{Z}, +) \longrightarrow \text{Bij}(X) \\ & \quad n \longmapsto \sigma^n = \underbrace{\sigma \circ \dots \circ \sigma}_n \text{ } n \text{ fois} \end{aligned}$$

on dit que $(\mathbb{Z}, +)$ agit sur X
car on a associé à tout elt de $\mathbb{Z}$
une permutation compatible
avec l'addition de $\mathbb{Z}$ et la composition
de bij: $\forall n \in \mathbb{Z}$

$$G^n : x \longrightarrow G^n(x) = \underbrace{G(G(\dots G(x)))}_{n \text{ fois}}$$

on a

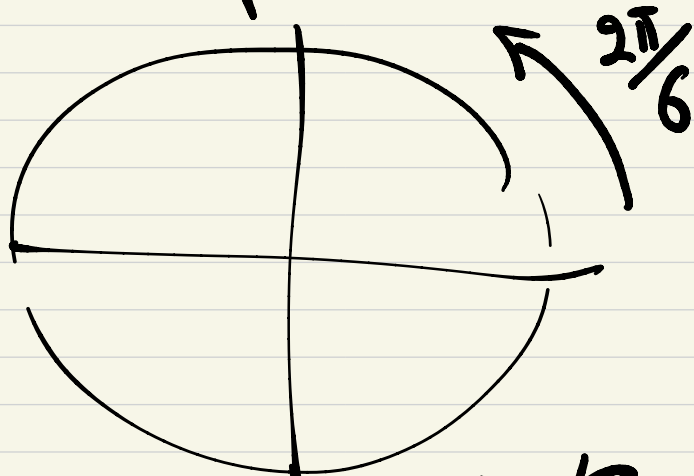
$$\begin{aligned}\sigma^{m+n}(x) &= \sigma^m(\sigma^n(x)) \\ &= \sigma^m \circ \sigma^n(x).\end{aligned}$$

Action de $\mathbb{Z}$ sur $\mathbb{R}^2$:

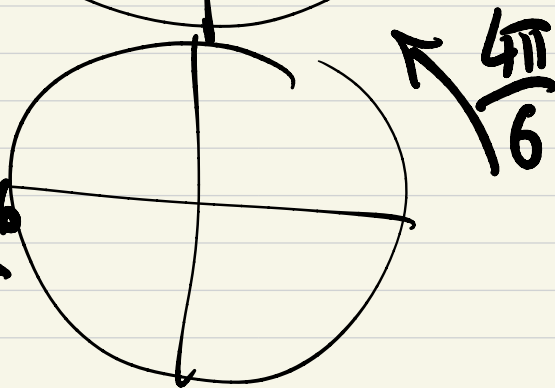
ρ_6 = rotation de centre O
et d'angle $\frac{2\pi}{6}$.

Action: $n \rightarrow p_6^n$

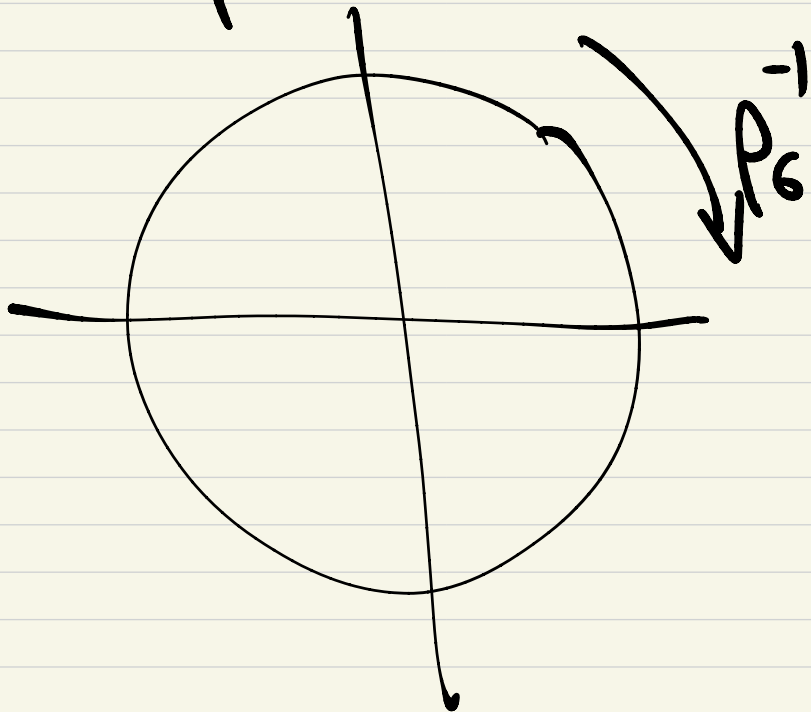
1 $\rightarrow$



2 $\rightarrow p_6^2 = p_6 p_6$



$-1 \longrightarrow P_6^{-1} = \text{rot d'angle } -\frac{2\pi}{6}$



PROPOSITION 2.6. La donnée d'une action $G \curvearrowright_{\varphi} X$ est équivalente à la donnée d'une application (appelée loi de composition externe)

$$\bullet \odot \bullet : \begin{array}{ccc} G \times X & \mapsto & X \\ (g, x) & \mapsto & g \odot x \end{array} \quad (= \varphi(g)(x))$$

verifiant

(1) neutralité de l'élément neutre:

$$\forall x \in X, e_G \odot x = x,$$

(2) associativité: $\forall x \in X, g, g' \in G,$

$$(g \star g') \odot x = g \odot (g' \odot x).$$

(3) simplification: en combinant les deux propriétés précédentes on a $\forall x \in X, g \in G,$

$$g \odot (g^{-1} \odot x) = g^{-1} \odot (g \odot x) = x.$$

"Preuve": on définit pour $\varphi \in \text{Hom}_{\text{Gr}}(G, \text{Bij}(X))$

$$\begin{aligned} - \odot: G \times X &\longrightarrow X \\ (g, x) &\longrightarrow \varphi(g)(x) = g \odot x \end{aligned}$$

Le fait que $\varphi \in \text{Hom}_{\text{Gr}}(G, \text{Bij}(X))$
implique (1), (2), (3)

$$\zeta_1 \quad \odot : G \times X \rightarrow X$$

verifie (1) (2) (3)

on definit pour tout $g \in G$

une application $\varphi(g): X \rightarrow X$

$$\varphi(g)(x) = g \odot x$$

on montre que $\varphi(e_G) = Id_X$ (1)

que $\varphi(g)$ est bijective de réciproque
 $\varphi(g)^{-1} = \varphi(g^{-1})$ (utiliser (2))

— $\varphi: G \rightarrow \text{Bij}(X, X)$ et avec (2)
on a que
 $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$

$\Rightarrow \varphi$ est un morphisme de G vers $\text{Bij}(X)$ $\square$

Translation ds un gpe: $X = (G, *)$

On définit une action $G \curvearrowright G$
par "translation à gauche"

$$\odot : \begin{array}{l} G \times G \longrightarrow G \\ (g, h) \longmapsto g \odot h = g * h \end{array}$$

le morphisme associe

$$G \longrightarrow (\text{Bij}(G), \circ)$$

$$t_{\bullet} : g \longmapsto t_g : h \longmapsto g * h$$

Pour tout $g, g' \in G$ on

$$\begin{aligned} t_{g * g'} : h &\longrightarrow (g * g') * h = g * (g' * h) \\ &= t_g(t_{g'}(h)) \end{aligned}$$

on a bien

$$t_{g * g'} = t_g \circ t_{g'}$$

$$- t_{e_6} : h \mapsto e_6 * h = h$$

$$t_{e_6} = \text{Id}_G$$

$$- t_g \circ t_{g^{-1}} = t_{g * g^{-1}} = t_{e_G} = \text{Id}_G$$

$$- t_{g^{-1}} \circ t_g = t_{g^{-1} * g} = t_{e_G} = \text{Id}_G$$

Ca dit que t_g est une bij de G vers G
de réciproque $(t_g)^{-1} = t_{g^{-1}}$

- $t_\bullet: g \rightarrow t_g$ est une action $G \curvearrowright_t G$

l'application $g \rightarrow t_g$
est un morphisme

mais

$$t_g: \begin{array}{ccc} G & \xrightarrow{\quad} & G \\ h & \xrightarrow{\quad} & gh \end{array}$$

n'est pas général
PAS un morphisme

The war
ning

Ce n'est un morphisme que si $g = e_G$

Si $g \neq e_G$

$$t_g: \begin{array}{ccc} G & \rightarrow & G \\ h & \mapsto & gh \end{array}$$

$$t_g(e_G) = g \cdot e_G = g \neq e_G.$$

THÉORÈME 2.10. *L'application translation à gauche*

$$t_{\bullet} : \begin{array}{ccc} G & \mapsto & \text{Bij}(G) \\ g & \mapsto & t_g : g' \mapsto g.g' \end{array}$$

est un morphisme de groupes de $(G, .)$ vers $(\text{Bij}(G), \circ)$. Le morphisme $t_{\bullet}$ définit donc une action à gauche de G sur G qu'on appellera action par translations à gauche et qu'on notera $G \curvearrowright_t G$.

Une autre action qui est par morphisme
est la conjugaison:

$$g \in G$$

$$\text{Ad}_g: \begin{array}{ccc} G & \longrightarrow & G \\ h & \longrightarrow & ghg^{-1} \end{array}$$

$\forall g \in G$ Ad_g est un morphisme bijectif
(Exo)

et l'application

$$\begin{aligned} \text{Ad}_\bullet: G &\longrightarrow \text{Aut}_G(G) \cong \text{Bij}(G) \\ g &\longmapsto \text{Ad}_g: h \longmapsto ghg^{-1} \end{aligned}$$

est un morphisme de groupes et définit
une action de G sur G (par conjugaison)

EXERCICE 2.6. Soit G un groupe et

$$t_{\bullet} : \begin{array}{ll} G & \mapsto \text{Bij}(G) \\ g & \mapsto t_g : G \mapsto G \end{array}$$

l'action par translation à gauche de G vers G .

(1) Montrer que $t_{\bullet}$ est injective.