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)*

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

- *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:* $\forall g, g', g'' \in G,\ (g \star g') \star g'' = g \star (g' \star g'')$.
- *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 elements* g, g' *commutent si*

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

Un groupe G *est abelien (ou commutatif) si toutes les paires d'elements de* G *commutent:*

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

DÉFINITION 2.3. *Soit* $(G, \star, e_G, \bullet^{-1})$ *un groupe, le cardinal* $|G|$ *de l'ensemble sous-jacent s'appelle egalement l'ordre du groupe* 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:*

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

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

Classification des ss gpes de $\mathbb{Z}$

THÉORÈME 2.2. *Les sous-groupes de $\mathbb{Z}$ sont exactement les sous-ensembles de la forme*

$$q\mathbb{Z} = \{qk,\ k \in \mathbb{Z}\} = 0 \pmod{q} \subset \mathbb{Z}$$

pour $q \in \mathbb{Z}$ un entier.

(Lagrange)

THÉORÈME 2.5. *Soit G un groupe fini et $H \subset G$ un sous-groupe alors l'ordre de H divise l'ordre de G:*

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

COROLLAIRE 2.1. *Si $|G|$ est un nombre premier, ses seuls sous-groupes sont $\{e_G\}$ et G et pour tout $g \in G - \{e\}$, on a*

$$g^{\mathbb{Z}} = G.$$

En particulier G est commutatif.

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*

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

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

$$\operatorname{ord}(g) \mid |G|$$

Sous-groupe Engendré

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*).*

Ex: si $A = \{g\}$ $\langle g \rangle = g^{\mathbb{Z}}$

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.

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

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

l'ensemble des morphismes de G *vers* H.

Notation/Terminologie. On notera

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

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

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

$$\mathrm{End}_{Gr}(G):=\mathrm{Hom}_{Gr}(G,G).$$

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

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

  est est appele l'ensemble des automorphismes de G.

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

<u>Exemples</u> : $\underline{e}_H : g \in G \to e_H \in H$

$h \in H \quad h^{\bullet} : k \in \mathbb{Z} \to h^k \in H$

$\exp_h(\cdot)$

est un morphisme de groupes $\left(h^{m+n} = h^m * h^n \right)$

Contre-exemple (translation)

$(G, \cdot)$ grpe $\quad g \in G$

$$t_g : \begin{array}{ccc} G & \longrightarrow & G \\ h & \longmapsto & g \cdot h \end{array}$$

t_g = translation a gauche par g

$t_g(\cdot)$ n'est un morphisme que si $g = e_G$

si t_g = morphisme alors

$$t_g(e_G) = e_G = g.e_G = g.$$

Conjugaison $(G, \cdot)$ $g \in G$

$$Ad_g : h \in G \longrightarrow g.h.g^{-1} \in G$$

est un morphisme $\forall g$: Conjugaison par g

Preuve : soit $h, h' \in G$

on veut mq $Ad_g(h.h') \overset{?}{=} Ad_g(h).Ad_g(h')$

$$Ad_g(h).Ad_g(h') = g.h.\underbrace{g^{-1}.g}_{e_G}.h'.g^{-1}$$

$$= g\,h.e_G.h'.g^{-1}$$

$$= g\,h.h'g^{-1}$$

$$= Ad_g(h.h')$$

Ad_g est un morphisme de G vers G

$\Rightarrow$ un endomorphisme de G

$$Ad_g \in End_{Gr}(G).$$

Noyau - Image

Proposition 2.4. *(Invariance des sous-groupes par morphismes) Soit $\varphi \in \mathrm{Hom}_{Gr}(G, H)$ 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,*
$$\mathrm{Im}(\varphi) = \varphi(G) \subset H$$
est un sous-groupe de H.
2. *Soit $L \subset H$ un sous-groupe de H, alors la preimage*
$$\varphi^{(-1)}(L) = \{g \in G,\ \varphi(g) \in L\} \subset G$$
est un sous-groupe de G. En particulier $\varphi^{(-1)}(\{e_H\})$ est un sous-groupe de G.

le noyau de φ
$\ker(\varphi)$

<u>Preuve</u> : soit $K < G$ un ssgpe

$$\varphi(K) = \{ \varphi(k) \ \ k \in K \}$$

soient $k, k' \in K$ on veut mq

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

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

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

Comme K est un ssgpe on a

$$k.k'^{-1} \in K \text{ et donc}$$

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

- Soit $L \subset H$ un ssgpe on veut mq

$$\varphi^{(-1)}(L) = \{g \in G \text{ tq } \varphi(g) \in L\} \text{ est un ssgpe}$$

soient $g, g' \in \varphi^{(-1)}(L)$ on veut mq

$$g \cdot g'^{-1} \in \varphi^{(-1)}(L) \,?$$

$$\Longleftrightarrow \varphi(g \cdot g'^{-1}) \in L \,?$$

$\varphi(g \cdot g'^{-1}) = \varphi(g) * \varphi(g')^{-1}$ et comme

$\varphi(g), \varphi(g') \in L$ et que L est un ssgpe de H

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

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

$$\square$$

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

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

THÉORÈME 2.8 (Critere d'injectivite). *Soit* $\varphi \in \mathrm{Hom}_{Gr}(G, H)$ *un morphisme de groupes alors les proprietes suivantes sont equivalentes*

(1) φ *est injectif,*
(2) $\ker(\varphi) = \{e_G\}$.

<u>Preuve</u> : (1) $\to$ (2)

si φ et injectif : $\forall h \in H$ $\varphi^{(-1)}(\{h\})$ a au + un elt.

en particulier si $h = e_H$

$\varphi^{(-1)}(\{e_H\})$ a au + un elt

$\varphi^{(-1)}(\{e_H\}) \ni e_G \Rightarrow \underbrace{\varphi^{(-1)}(\{e_H\})}_{= \ker(\varphi)} = \{e_G\}$

- (2) $\Rightarrow$ (1) : on suppose $\ker \varphi = \{e_G\}$
  et on vmq $\varphi \hookrightarrow$.

  soit $h \in H$ tq $\varphi^{(-1)}(\{h\}) \neq \emptyset$

on rmq on a un seul elt.

soient $g_1, g_2 \in \varphi^{(-1)}(\{h\})$ ovmq $g_1 = g_2$.

on $\varphi(g_1) = \varphi(g_2) = h$

$$\Longrightarrow \underbrace{\varphi(g_1) * \varphi(g_2)^{-1}}_{\varphi(g_1 \cdot g_2^{-1})} = e_H$$

φ morph

$$\Longrightarrow \varphi(g_1 \cdot g_2^{-1}) = e_H$$

$g_1 \cdot g_2^{-1} \in \ker\varphi$ $\qquad$ $g_1 \cdot g_2^{-1} = e_G$

$$\Longrightarrow \quad g_1 = g_2$$

$\square$

<u>Exemple</u> : ordre d'un elt.

$g \in G$ gpe

$\operatorname{ord} g := |g^{\mathbb{Z}}| = |$ Image du gpe $\mathbb{Z}$ par le morphisme $g^{\bullet}|$

$$g^{\bullet} : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & g^k \end{array}$$

$\ker g^{\bullet} \subset \mathbb{Z}$ est un ssgpe

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

<u>Thm</u> : soit $g \in G$ $\operatorname{ord} g = |g^{\mathbb{Z}}| \in \mathbb{N}_{>0} \cup \infty$

soit $q \geq 0$ tq $\ker g^{\bullet} = q\mathbb{Z}$

alors on a

- si $q=0$ $\ker g^{\bullet} = \{0\}$ et donc

$g^{\bullet} : \mathbb{Z} \hookrightarrow G$ et $g^{\mathbb{Z}} \simeq \mathbb{Z}$

et $\operatorname{ord} g = |g^{\mathbb{Z}}| = \infty$

- si $q>0$ alors

$\operatorname{ord} g = |g^{\mathbb{Z}}| = q$

et $\operatorname{ord} g = q$ est le + petit entier >0 solution de l'équation $g^k = e_G$

Exemple (Conjugaison)

$g \in G$

$Ad_g : h \in G \to ghg^{-1} \in G$

$\ker Ad_g = \{ h \in G \text{ tq } ghg^{-1} = e_G \}$

si $ghg^{-1} = e_G \Longrightarrow gh = g$ (on x a dte par g)

$\Longrightarrow h = e_G$

Ad_g est injective.

En fait elle est bijective : et sa reciproque

est $(Ad_g)^{-1} = Ad_{g^{-1}} : h \to g^{-1}hg$

$$Ad_g \circ Ad_{g^{-1}} : h \to gg^{-1}hgg^{-1} = h = Id(h)$$

$$Ad_{g^{-1}} \circ Ad_g : h \to g^{-1}ghg^{-1}g = h = Id_G(h)$$

Théorème 2.10. *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)*

$$\mathbb{Z} \simeq g^{\mathbb{Z}};$$

  On a alors

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

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

$$g^q = e_G$$

  et on a

$$\operatorname{ord}(g) = |g^{\mathbb{Z}}| = q.$$

THÉORÈME 2.9. *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' egalite suivante entre ensembles*

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

<u>Preuve</u>: soit $k \in \ker\varphi$ on rmq

$$Ad_g(k) = gkg^{-1} \in \ker\varphi$$

on calcule $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1}$

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

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

$$g k g^{-1} \in \ker \varphi \implies$$

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

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

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

en prenant $g' = g^{-1}$ on obtient

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

$$\forall g \in G \quad g.\ker\varphi.g^{-1} = \ker\varphi \qquad \square$$

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

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

est dit normal ou distingue et on le note

$$K \lhd G.$$

<u>Rmq</u>: pour mq $\forall g \in G$ $gKg^{-1} = K$

il suffit de mq $\forall g \in G$ $gKg^{-1} \subset K$.

Rmq: On a vu que tout noyau est distingué

et réciproquement si $K \lhd G$ alors il exist un gpe H un morphisme $\varphi : G \to H$ tq

$\ker \varphi = K$.

<u>Opérations sur les morphismes</u>
<u>de Gpes</u>

Notation/Terminologie. On notera

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

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

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

$$\mathrm{End}_{Gr}(G) := \mathrm{Hom}_{Gr}(G, G).$$

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

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

est est appele l'ensemble des automorphismes de G.

Proposition 2.6. *(Invariance des morphismes 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.*

De plus on rappelle que

- *si* φ *et* ψ *sont injectives alors* $\psi \circ \varphi$ *est injective,*
- *et si* φ *et* ψ *sont surjectives alors* $\psi \circ \varphi$ *est surjective,*
-
- *et si* φ *et* ψ *sont bijectives alors* $\psi \circ \varphi$ *est bijective.*

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

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

Preuve: Supposons φ et ψ sont de morphismes de gpes et mq $\psi \circ \varphi$ est un morphisme de gpe il suffit de mq $\forall g, g' \in G$

$$\psi \circ \varphi(g * g') \overset{?}{=} \psi \circ \varphi(g) \otimes \psi \circ \varphi(g')$$

$$\psi(\varphi(g * g')) = \psi(\varphi(g) * \varphi(g'))$$

$$= \psi(\varphi(g)) \otimes \psi(\varphi(g'))$$

$\psi \circ \varphi =$ morphisme.

$\varphi : G \to H$ est un morphisme bijectif

et soit $\varphi^{-1} : H \to G$ sa réciproque

On v mq $\forall h, h' \in H$

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

pour cela on calcule le φ de part et d'autre

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

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

$$= h * h'$$

Donc $\varphi^{-1}(h * h')$ et $\varphi^{-1}(h) \star \varphi^{-1}(h')$

on m̂ image par φ et comme φ est bijective

ils sont egaux.

$h * h'$ $\square$

COROLLAIRE 2.3. *L'ensemble des automorphismes de G*

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

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

Preuve : $\mathrm{Aut}_{Gr}(G)$ = morphisme de G vers G qui sont bijectif

$\subset \mathfrak{S}_G = (\mathrm{Bij}(G), \circ)$

– il suffit de mq $\mathrm{Aut}_{Gr}(G)$ est non vide

non ~~$\emptyset$~~ : $\mathrm{Id}_G \in \mathrm{Aut}_{Gr}(G)$

$\forall\, \varphi, \psi \in \mathrm{Aut}_{Gr}(G)$

$\varphi \circ \psi^{-1} \in \mathrm{Aut}_{Gr}(G)$?

- si $\psi \in \mathrm{Aut}_{Gr}(G) \Rightarrow \psi^{-1} \in \mathrm{Aut}_{Gr}(G)$

et comme φ et $\psi^{-1} \in \mathrm{Aut}_{Gr}(G)$

$\Rightarrow \varphi \circ \psi^{-1} \in \mathrm{Aut}_{Gr}(G)$

on a vérifié le critère des ss gpe. $\square$

Rmq: <u>Gpes Isomorphes</u>

G et H sont isomorphes ssi

$\exists \psi \in Hom_{Gr}(G,H)$ ψ bijectif

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

$\Longleftrightarrow Isom_{Gr}(G,H) \neq \emptyset$

la relation "être isomorphe" $G \simeq H$ \simeq
est une relation d'equivalente

- reflexive : $Id_G ; G \xrightarrow{\simeq} G$
- symetrique $G \underset{\varphi}{\simeq} H \Longleftrightarrow H \underset{\varphi^{-1}}{\simeq} G$
- transitive $G \underset{\varphi}{\simeq} H \quad H \underset{\psi}{\simeq} K$

$\Longrightarrow G \underset{\psi \circ \varphi}{\simeq} K$

2 Grpes isomorphe ont exactment les
m̂ propriétées en tant que gpe
et sont indistingable en tant que gpes

Exemples :

$$(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \times)$$

$$x \longrightarrow e^{x}$$

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

Fourier $\longleftrightarrow$ Mellin

$$\mathbb{Z}/q\mathbb{Z} \simeq \mu_q(\mathbb{C}) = \{ z \in \mathbb{C} \;\; z^q = 1 \}$$

$$= \text{racines } q\text{-ièmes de l'unité}$$

$$e^{2\pi i \,\bullet} = \exp(2\pi i \,\bullet)$$

$$a(q) = a + q\mathbb{Z} \longmapsto e^{2\pi i \frac{a}{q}}$$

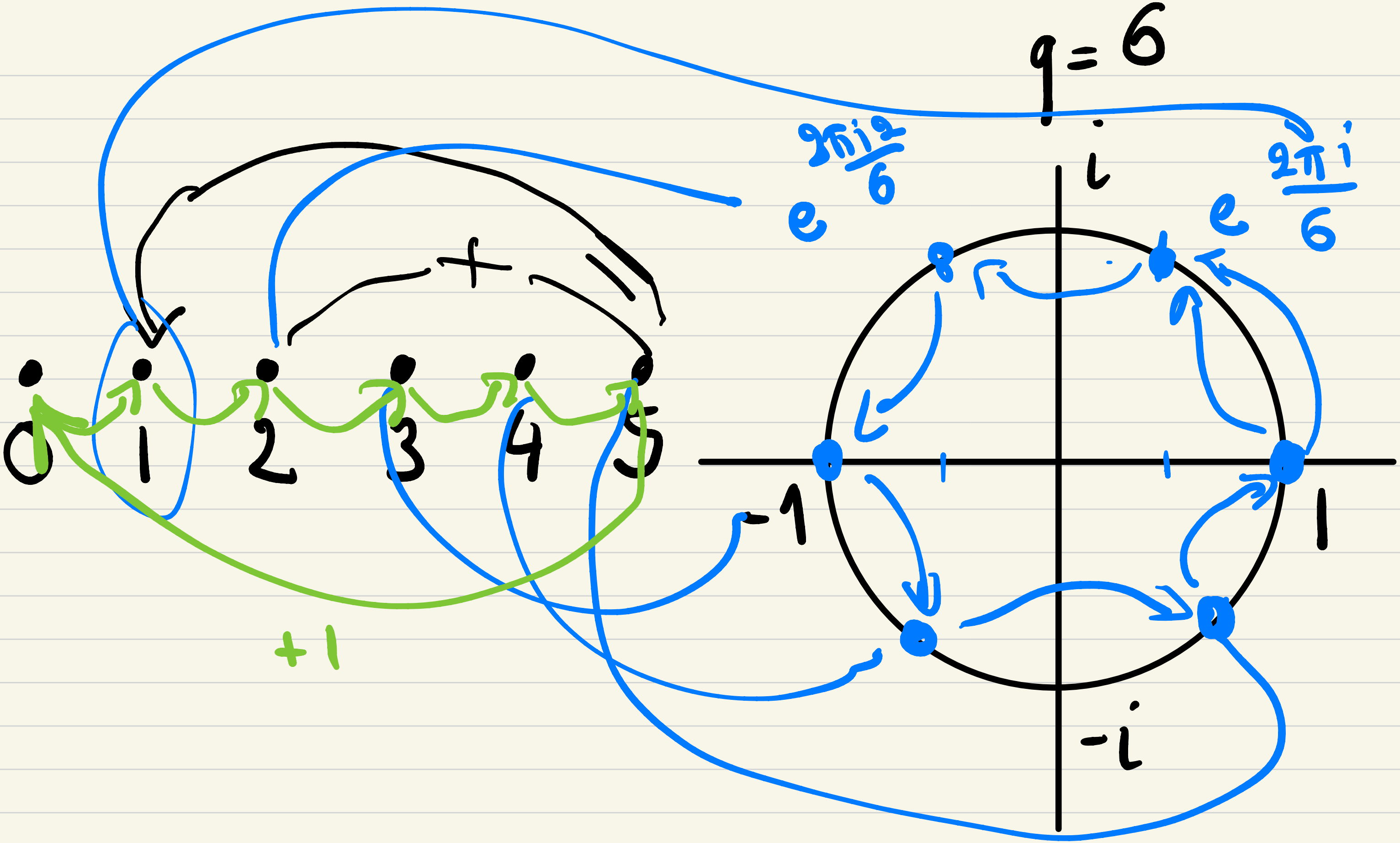
si $a' \equiv a(q) \iff a'+q\mathbb{Z} = a+q\mathbb{Z}$

$$e^{2\pi i \frac{a'}{q}} = e^{2\pi i \frac{a}{q}}$$

si $a' \equiv a(r$ $\quad a' = a+qk \quad k \in \mathbb{Z}$

$$e^{2\pi i \frac{a'}{q}} = e^{2\pi i\left(\frac{a}{q}+k\right)} = e^{2\pi i \frac{a}{q}} \cdot \underbrace{e^{2\pi i k}}_{=1}$$

$$= e^{2\pi i \frac{a}{q}}$$



0 1 2 3 4 5
+
+1
q = 6
i
-i
1
-1
$e^{\frac{2\pi i}{6}}$
$e^{\frac{2\pi i 2}{6}}$

Action d'un Gpe sur un ensemble

DÉFINITION 2.11. *Soit* $(G, \star)$ *un groupe,* X *un ensemble et* $(\mathrm{Bij}(X), \circ)$ *le groupe symetrique de* X *(des bijections de* X *sur lui-meme). Une action (a gauche) de* G *sur* X *est la donnee d'un morphisme*

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

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

\circlerightarrow

Exemple : $X \neq \emptyset$ $\quad \sigma \in \mathrm{Bij}(X)$

$$\sigma^{\bullet} : k \in \mathbb{Z} \longrightarrow \sigma^k \in \mathrm{Bij}(X)$$

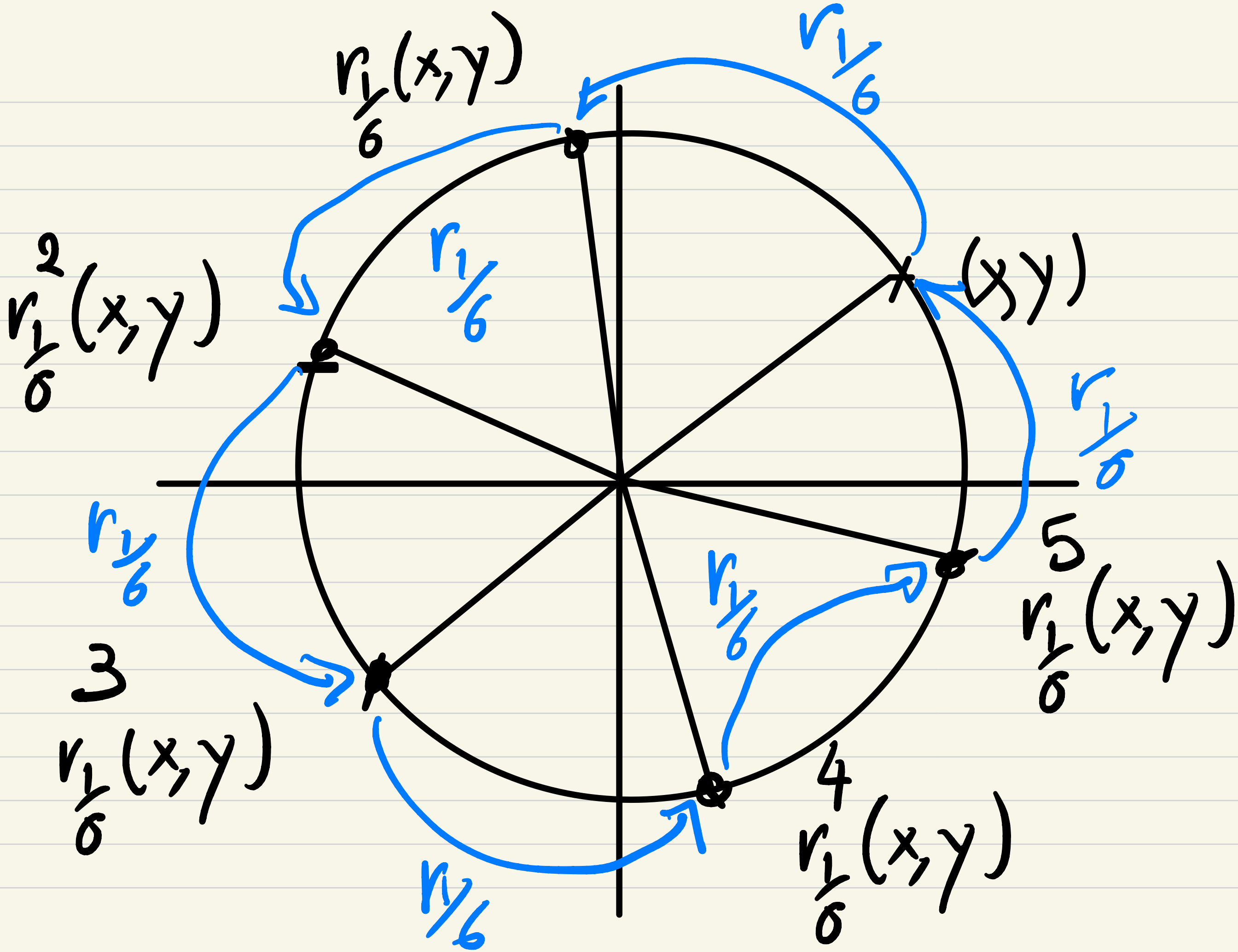
$$\sigma^{\bullet} \in \mathrm{Hom}_{Gr}(\mathbb{Z}, \mathrm{Bij}(X))$$

$\sigma^{\bullet}$ défini une action de $(\mathbb{Z}, +) \underset{\sigma^{\bullet}}{\curvearrowright} X$

Ex: $\mathbb{Z} \curvearrowright \mathbb{R}^2 = X$

$r_{1/6}$ = rotation sur $\mathbb{R}^2$ de centre O et d'angle $\frac{2\pi}{6}\ (2\pi)$

l'action de $\mathbb{Z}$ associe à $k \in \mathbb{Z}$ la rotation d'angle $\frac{2\pi}{6}k\ (2\pi)$



$r_{\frac{1}{6}}(x,y)$
$r_{\frac{1}{6}}$
(x,y)
$r^{2}_{\frac{1}{6}}(x,y)$
$r_{\frac{1}{6}}$
$r_{\frac{1}{6}}$
$r_{\frac{1}{6}}$
$r_{\frac{1}{6}}$
$r^{5}_{\frac{1}{6}}(x,y)$
$r^{3}_{\frac{1}{6}}(x,y)$
$r_{\frac{1}{6}}$
$r^{4}_{\frac{1}{6}}(x,y)$

Proposition 2.7. *La donnee d'une action $G \curvearrowright_\varphi X$ est equivalente a la donnee d'une application (appellee loi de composition externe)*

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

verifiant

(1) *neutralite de l'element neutre:*

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

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

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

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

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

$$(g \star g^{-1}) \odot x \qquad (g^{-1} \star g) \odot x$$

Preuve : Soit $\varphi : G \longrightarrow \mathrm{Bij}(X)$

on défini $g \odot x := \varphi(g)(x)$

- si $g = e_G$ $\quad e_G \odot x = \underbrace{\varphi(e_G)}_{\| \atop \mathrm{Id}_X}(x)$

$$\mathrm{Id}_X(x) = x$$

- $g \odot (g' \odot x) = \varphi(g)\big(\varphi(g')(x)\big)$

$$\forall_{x \in X}\ \varphi(g)\big(\varphi(g')(x)\big) = \big(\varphi(g)\circ\varphi(g')\big)(x)$$

$$= \varphi(g \star g')(x)$$

$$\Longrightarrow \varphi(g)\circ\varphi(g') = \varphi(g\star g')$$

$$-(3) \quad g \odot (g^{-1} \odot x) = (g \star g^{-1}) \odot x$$

$$= e_G \odot x = x \qquad \square$$

Ex:

- $r_{1/6} = \varphi \qquad \varphi(k) = r_{1/6}^{k} : \mathbb{R}^2 \to \mathbb{R}^2$

$$r_{1/6}^{k}(x,y) = k \odot_{\varphi} (x,y)$$

Action du Gpe sur lui-meme par translations

Soit G un gpe alors G agit sur lui-meme par translations a gauche.

$$t_\bullet : G \longrightarrow Bij(G)$$
$$g \longrightarrow t_g : h \in G \to g.h \in G$$

$\forall_g$ t_g est une bijection de G sur G

$$t_g : h \to gh$$

- t_g surj : soit $h' \in G$ alors on cherche

$h \in G$ tq $t_g(h) \overset{?}{=} h'$

$$g . h \overset{?}{=} h'$$

on prend $h = g^{-1} . h'$ $\quad t_g(g^{-1} . h') = h'$

$t_g \hookrightarrow$: si $t_g(h_1) = t_g(h_2)$

$$\Longrightarrow g \cdot h_1 = g \cdot h_2$$

$$\Longrightarrow \times g^{-1} \cdot \quad g^{-1} \cdot g \cdot h_1 = g^{-1} \cdot g \cdot h_2$$

$$\Longrightarrow \quad h_1 = h_2$$

$$t_g \in Bij(G)$$

$$t_\bullet : G \longrightarrow Bij(G)$$

Théorème 2.11. *L'application translation a gauche*

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

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

Preuve : on vmq $\forall g, g' \in G$

$$t_{g.g'} = t_g \circ t_{g'} \; ?$$

$$\forall h \in G \quad t_{g.g'}(h) \overset{?}{=} (t_g \circ t_{g'})(h) \quad \underset{\parallel}{(t_g \circ t_{g'})(h)}$$

$$t_{g.g'}(h) = (g.g').h = g.(g'.h) = t_g(t_{g'}(h))$$

Rmq: la loi de composition "externe"

$$\odot : G \times G \to G$$
$$(g, h) \mapsto g \odot h = g \cdot h.$$

Rmq: $\ker(t_\bullet) = \{g \in G \text{ tq } \underset{\{e_G\}}{\underset{\parallel}{t_g = Id_G}}\}$

si g est tq $t_g = Id_G$

$$\Rightarrow \quad t_g(e_G) = e_G$$

$$\begin{aligned} &\parallel \\ g&\cdot e_G = e_G \\ &\parallel \\ g& = e_G \end{aligned}$$

$$\Longrightarrow \quad t_\cdot : G \hookrightarrow \mathrm{Bij}(G)$$

injective

On dit que l'action est "fidèle".

Action de G sur G par Conjugaison

$$\mathrm{Ad}_g : h \in G \longrightarrow g.h.g^{-1} \in G$$

Ad_g est un morphisme de groupes

$$\mathrm{Ad}_g(h.h') = \mathrm{Ad}_g(h).\mathrm{Ad}_g(h')$$

$$\mathrm{Ad}_\bullet : g \in G \longrightarrow \mathrm{End}_{Gr}(G)$$

Théorème 2.12. *Pour tout g, l'application $\mathrm{Ad}_g : G \mapsto G$ est un isomorphisme de groupes (ie $\mathrm{Ad}_g \in \mathrm{Aut}_{Gr}(G)$) dont l'application reciproque vaut*

$$\mathrm{Ad}_g^{-1} = \mathrm{Ad}_{g^{-1}} : G \xrightarrow{\sim} G.$$

De plus l'application

$$\mathrm{Ad}_\bullet : \begin{array}{ccc} G & \mapsto & \mathrm{Bij}(G) \\ g & \mapsto & \mathrm{Ad}_g \end{array}$$

est un morphisme de groupes.

Preuve: pour mq Ad_g et bijective il suffit d'exhiber sa reciproque.

On a $\mathrm{Ad}_g \circ \mathrm{Ad}_{g^{-1}} = \mathrm{Id}_G$, $\mathrm{Ad}_{g^{-1}} \circ \mathrm{Ad}_g = \mathrm{Id}_G$

Quand on aura verifie cela on saura que Ad_g bij et $(Ad_g)^{-1} = Ad_{g^{-1}}$

- $Ad_g \circ Ad_{g^{-1}} = Id_G$,

soit $h \in G$ $\quad Ad_g \circ Ad_{g^{-1}}(h) = g.g^{-1}.h.g.g^{-1}$

$$= e_G.h.e_G$$

$$= h = Id_G(h)$$

On vmq : $\forall g, g' \in G$ et $h \in G$

$$Ad_{g.g'}(h) = Ad_g \circ Ad_{g'}(h) \ ?$$

$$\begin{aligned}
(g.g').h.(g.g')^{-1} &= g.g'.h.g'^{-1}.g^{-1} \\
&= g.Ad_{g'}(h).g^{-1} \\
&= Ad_g(Ad_{g'}(h)) = Ad_g \circ Ad_{g'}(h) \quad \square
\end{aligned}$$

Rmq : $\ker(Ad_{\bullet}) = \{ g \in G \text{ tq } Ad_g = Id_G \}$

soit $g \in \ker(Ad_{\bullet})$:

$\forall h \in G$ on a $Ad_g(h) = g.h.g^{-1} = h$

$\iff \forall h \in G \quad g.h = h.g$

$\iff g \in Z(G)$

$\ker(\mathrm{Ad}_\bullet) = Z(G) =$ centre de G.

En general $Z(G) \neq \{e_G\}$

Ex: si G est commutatif $Z(G) = G$

et $\forall g \quad g.h.g^{-1} = h \quad \forall g \ \mathrm{Ad}_g = \mathrm{Id}_G$

$\mathrm{Ad}_\bullet = \underline{\mathrm{Id}}_G$

Action à droite

Translation à dte

$$td_g : h \in G \longrightarrow h.g \in G$$

si $g, g' \in G$

$$td_{g.g'}(h) = h.g.g' = td_{g'}(td_g(h))$$

$$= td_{g'} \circ td_g (h)$$

$$td_{g \cdot g'} = td_{g'} \circ td_g$$

Définition 2.13. *Soient* $(G, \star)$ *et* $(H, *)$ *deux groupes, un anti-morphisme de groupes* $\varphi : G \mapsto H$ *est une application telle que*

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

Proposition 2.8. *Une application entre groupes* $\varphi : G \to H$ *est un anti-morphisme de groupes ssi*

$$\varphi \circ \bullet^{-1} : g \mapsto \varphi(g^{-1})$$

est un morphisme de groupes ou bien ssi

$$\bullet^{-1} \circ \varphi : g \mapsto \varphi(g)^{-1}$$

est un morphisme de groupes.

Preuve : soit φ un antimorphisme et $\psi = \varphi \circ \bullet^{-1}$: $\psi(g \star g') = \varphi((g \star g')^{-1})$

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

$$= \psi(g)^* \psi(g')$$

$\vdots$

$\square$

Définition 2.14. *Soit* $(G, \star)$ *un groupe,* X *un ensemble et* $(\mathrm{Bij}(X), \circ)$ *le groupe symetrique de* X *(des bijections de* X *sur lui-meme). Une action a droite de* G *sur* X *est la donnee d'un antimorphisme de groupes*

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

On dit alors que G *agit sur* X *a droite a travers* φ *et one le note* $X \curvearrowleft_\varphi G$.

Proposition 2.9. *La donnee d'une action a droite* $X \curvearrowleft_\varphi G$ *est equivalente a la donnee d'une application*

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

verifiant

(1) *neutralite de l'element neutre:* $\forall x \in X,\ x \odot e_G = x,$
(2) *associativite:* $\forall x \in X,\ g, g' \in G,\ x \odot (g \star g') = (x \odot g) \odot g'.$
(3) *simplification: en combinant les deux proprietes precedentes on a* $\forall x \in X,\ g \in G,$

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

- Gauche $\longrightarrow$ Dte

- Dte $\longrightarrow$ Gauche

Si $G \curvearrowright X$ $\quad \varphi : G \longrightarrow Bij(X)$
morphisme

alors $g \mapsto \varphi(g^{-1})$ est un antimorphisme

et definit une action a dte

$$\varphi(g^{-1})(x) = g^{-1} \odot x =: x \boxdot g$$

Exemple d'action à dte

$G \curvearrowright X \quad Y = \text{Ens}$ (eg. $Y = \mathbb{R}$)

$\mathcal{F}(X,Y) = \{ f : X \to Y \}$

On définit une action à dte

$\mathcal{F}(X,Y) \curvearrowleft G$ induite par l'action $G \curvearrowright X$ en posant soit $f : X \to Y$

$$f|_g : x \in X \to f(g \circ x)$$

alors $f|_{g \cdot g'} = (f|_g)|_{g'}$

et on peut obtenir une action à gauche $G \curvearrowright \mathcal{F}(X,Y)$ en posant

$$g \odot f : x \longrightarrow f(g^{-1} \odot x)$$