Cours 1

Théorie de groupe

Déf Un groupe est un ensemble G muni d'une opération

$$\cdot : G \times G \longrightarrow G$$
$$(x, y) \longmapsto x \cdot y$$

tq (i) (associativité) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\forall x, y, z \in G$

(ii) (unité) $\exists\, e \in G$ tq $e \cdot x = x \cdot e = x$, $\forall x \in G$.

(iii) (inverse) $\forall x \in G$, $\exists\, y \in G$ tq $x \cdot y = y \cdot x = e$.

notation : $y =: x^{-1}$

(Rq : (iii) $\Rightarrow$ l'inverse à gauche = l'inverse à droite.)

Rq : La notion de monoïde est comme gp mais sans (iii).

Déf : Un gp G est abélien si $\forall x, y \in G$, $x \cdot y = y \cdot x$.

Question : Si G admet une structure supplémentaire compatibles (e.g. variété différentielle, variété algébrique, espace topologique ---)

(e.g. $GL_n(\mathbb{C})$, $SO_n(\mathbb{R})$, S_{3n}, $\mathbb{Z}_p$, ---)

Définition de groupe "sans élément"

Déf. Un groupe est un ensemble G muni des applications

- $\mu : G \times G \longrightarrow G$,
- $e : \{*\} \longrightarrow G$
- $\iota : G \longrightarrow G$

tq (i) (Associativité) le diagramme suivant commute :

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mu\times id_G} & G\times G \\ {\scriptstyle id_G\times\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ G\times G & \xrightarrow[\mu]{} & G \end{array}$$

$(x,y,z) \longmapsto (xy,z)$

$(x,yz) \longmapsto x\cdot(yz)$ $\quad (xy)\cdot z$

(ii) (unité) le diagramme suivant commute :

$$\begin{array}{ccc} G & \xrightarrow{(id_G,e)} & G\times G \\ & \searrow^{id_G} & \downarrow{\scriptstyle \mu} \\ {\scriptstyle (e,id_G)}\downarrow & & G \\ G\times G & \xrightarrow[\mu]{} & \end{array}$$

$x \longmapsto (x,e)$

$(e,x) \longmapsto e\cdot x$ $\quad x = x\cdot e$

(iii) (Inverse) le diagramme suivant commute :

$$\begin{array}{ccc} G & \xrightarrow{(id_G,\iota)} & G\times G \\ & \searrow & \downarrow{\scriptstyle \mu} \\ {\scriptstyle (\iota,id_G)}\downarrow & \{*\} \xrightarrow{e} & G \\ G\times G & \xrightarrow[\mu]{} & \end{array}$$

$x \longmapsto (x, \iota(x))$

$(\iota(x),x) \longmapsto e = x\cdot\iota(x)$

Exercice : Vérifier que cette Déf est équiv. à la Déf usuelle.

Rq : L'avantage de cette définition abstraite est qu'elle marche dans n'importe quelle "catégorie".

e.g. pour définir un groupe | topologique / de Lie / alg..

On fait comme ci-dessus

en remplaçant ensemble par | espace topologique / variété diff. / variété alg.

et demandant les flèches soient | continues / C^∞ / algébriques.

Si de plus le diagramme suivant commute :

(iv)

$$\begin{array}{ccc} G\times G & \xrightarrow{\mu} & G \\ {\scriptstyle (pr_2,pr_1)=:i}\searrow & & \nearrow{\scriptstyle \mu} \\ & G\times G & \end{array}$$

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

$\downarrow$ $\qquad\qquad =$

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

alors on dit que G est un groupe abélien.

Exemples de gp

- Gp trivial
- G gp. $\rightsquigarrow$ $G^{op} := (G, \bullet^{op})$ où $x \bullet^{op} y := y \cdot x$; $G \simeq G^{op}$, $g \mapsto g^{-1}$
- groupe cyclique libre (toujours $\cong \mathbb{Z}$)

(:= un groupe engendré par un élément σ tq $\sigma^n = e \Leftrightarrow n = 0$ avec $n \in \mathbb{Z}$)

e.g. $\left(\{3^n \mid n \in \mathbb{Z}\}, \cdot\right) \xrightarrow{\cong} \mathbb{Z}$

$\frac{1}{3} \longmapsto 1$

$\left(\left\{\begin{pmatrix} 1 & 0 \\ 2025 & 2 \end{pmatrix}^n \middle| n \in \mathbb{Z}\right\}, \cdot\right)$

$\forall n \neq 0$, $(n\mathbb{Z}, +)$

- Fix $n \in \mathbb{Z}_{\neq 0}$, groupe cyclique d'ordre n ($\cong \mathbb{Z}/n\mathbb{Z}$)

:= un gp engendré par un élément σ tq $\{m \mid \sigma^m = e\} = n\mathbb{Z}$ i.e. $\mathrm{ord}(\sigma) = n$.

e.g. $\mu_n(\mathbb{C}) := \{z \in \mathbb{C} \mid z^n = 1\}$

- $\mathfrak{S}_n$: groupe symétrique

{ les permutations de $\{1, \dots, n\}$ }

plus généralement $\mathfrak{S}_X$ pour X un ensemble.

$\mathfrak{S}_X$ = { bijections de X vers X }.

[Exemple important / universel car tout groupe (fini) G admet un plongement $L_g : G \hookrightarrow \mathfrak{S}_G$
$g \mapsto \begin{pmatrix} G \to G \\ h \mapsto g.h \end{pmatrix}$]

- Soit $G_1 \xrightarrow{\varphi} G_2$ un morphisme

Alors. $\ker(\varphi) := \{ g \in G_1 \mid \varphi(g) = e_{G_2} \}$ est un sous-gp distingué.

(Rappel Un sous-gp H de G est distingué
si $\forall g \in G \quad gHg^{-1} \subset H$
i.e. H est stable par conjugaison d'élément de G.)

- $\mathrm{Im}(\varphi)$ est un sous-groupe de G_2.

e.g. $\mathfrak{S}_n \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ est un morphisme

$\rightsquigarrow A_n := \ker(\mathrm{sgn})$ le groupe alterné.

- $GL_n(\mathbb{K}) = \{$ matrices inversibles $n \times n$ à coeff. dans un corps $\mathbb{K} \}$

$GL_n(\mathbb{K}) \xrightarrow{\det} G_m(\mathbb{K}) := \mathbb{K}^\times$ est un morphisme [Notation : $G_m := GL_1$]

$\rightsquigarrow$ $SL_n(\mathbb{K}) := \ker(\det)$

- **Groupes classiques :**

$SO_n(\mathbb{R})$, $SO_n(\mathbb{C})$, $O_n(\mathbb{R})$, $O_n(\mathbb{C})$

$$SO(p,q) = \left\{ M \in GL_{p+q}(\mathbb{K}) \;\middle|\; {}^tM \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} M = \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix} \right\}$$

$Sp_{2n}(\mathbb{R})$, $Sp_{2n}(\mathbb{C})$, ---

$PGL_n(\mathbb{K}) := GL_n(\mathbb{K}) / G_m(\mathbb{K})$ où $G_m(\mathbb{K}) = \mathbb{K}^\times \cong \{\lambda \cdot I_n \mid \lambda \in \mathbb{K}^\times\} \cap GL_n(\mathbb{K})$

$PSL_n(\mathbb{K}) := SL_n(\mathbb{K}) / G_m(\mathbb{K}) \cap SL_n(\mathbb{K}) = SL_n(\mathbb{K}) / \mu_n(\mathbb{K})$

$U_n := \{ M \in GL_n(\mathbb{C}) \mid \overline{{}^tM} \cdot M = I_n \}$

- **Automorphismes**

philosophie : X un "ensemble structuré"

(e.g. - ensemble
- groupe, anneau, corps, module...
- espace top., var. diff./alg., ---
- espace affines, espaces projectifs
- espaces vectoriels, avec forme bil. ---)

alors $Aut(X) := \{ \varphi : X \to X \mid \varphi \text{ préserve la structure} \}$

est un groupe

De plus $Aut(X)$ agit sur X et aussi des espaces naturellement liés à X.

sous-exemples

- X ensemble, $\mathrm{Aut}(X) = \mathfrak{S}_X$
- G groupe. $\mathrm{Aut}(G)$ est un groupe
- $X = V$ un $\mathbb{K}$-espace vectoriel (de dim $n < \infty$)

$$\mathrm{Aut}(V) = GL(V) \underset{\text{choix d'une base}}{\cong} GL_n(\mathbb{K})$$

- (V, q) un espace vectoriel muni d'une forme bilinéaire symétrique

$$\mathrm{Aut}(V,q) = O(V,q) \text{ ou même } O(V)$$

si $q : V \times V \longrightarrow \mathbb{K}$, $(e_i, e_j) \longmapsto \delta_{ij}$

alors $O(V,q) \cong O_n(\mathbb{K})$.

– si $q : V \times V \longrightarrow \mathbb{K}$ est donnée dans la base canonique par Gram :

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

alors $O(V,q) \cong O(p,q)$.

– De même pour forme symplectique $\rightsquigarrow Sp_{2n}$.

- Espace affine $\mathbb{A}^n_{\mathbb{K}}$

  $\rightsquigarrow \mathrm{Aut}(\mathbb{A}^n_{\mathbb{K}}) \cong \mathbb{A}^n \rtimes GL_n(\mathbb{K}) \curvearrowright \mathbb{A}^n$.

  Espace projectif $\mathbb{P}^n_{\mathbb{K}}$

  $\rightsquigarrow \mathrm{Aut}(\mathbb{P}^n_{\mathbb{K}}) \cong PGL_{n+1}(\mathbb{K}) := \dfrac{GL_{n+1}(\mathbb{K})}{G_m(\mathbb{K})}$.

  $\curvearrowright \mathbb{P}^n(\mathbb{K})$

- X un espace top., variété diff, variété alg, ---

  $\mathrm{Homeo}(X)$, $\mathrm{Diff}(X)$, $\mathrm{Aut}(X)$.

- Si $\mathbb{L}/\mathbb{K}$ est une extension de corps

  alors $\mathrm{Aut}(\mathbb{L}/\mathbb{K}) := \{ \mathbb{L} \xrightarrow{\varphi \cong} \mathbb{L} \mid \varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}} \}$

  (voir S2 Théorie de Galois).

⋮

Déf. G un groupe.

- $\mathrm{Aut}(G)$: le gp des auto. de G

- On a un morphisme de groupes (exercice).

$$G \xrightarrow{\phi} Aut(G)$$

$$g \longmapsto \left(\phi_g : \begin{array}{ccc} G & \longrightarrow & G \\ h & \longmapsto & ghg^{-1} \end{array}\right)$$

- $Z(G) := \ker(\phi) = \{ g \in G \mid gh = hg \ \forall h \}$

(centre de G)

- $Int(G) := Im(\phi) \triangleleft Aut(G)$

(exercice : $Int(G) \triangleleft Aut(G)$ distingué)

(le gp des auto. intérieurs de G)

- $Out(G) := \dfrac{Aut(G)}{Int(G)}$

le groupe des "auto. extérieurs".

- Si $H < G$ est un sous-groupe

le normalisateur de H dans G =

$$N_G(H) := \{ g \in G \mid gHg^{-1} \subset H \}.$$

le <u>centralisateur</u> de H dans G

$$Z_G(H) := \{ g \in G \mid ghg^{-1} = h, \ \forall h \in H \}.$$

Rq par construction

$$N_G(H) \curvearrowright H \quad \text{par conjugaison.}$$

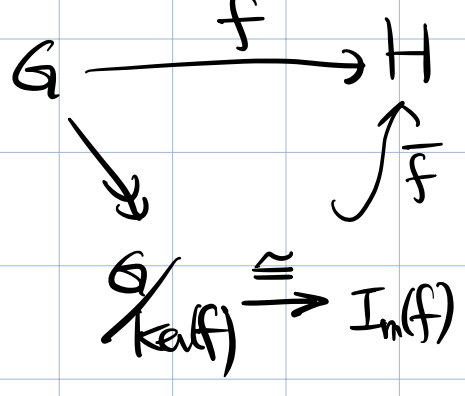
et $Z_G(H)$ est le noyau de cette action.

e.g. si $H = G$, $N_G(G) = G$; $Z_G(G) = Z(G)$

si $H = \langle g \rangle$, $N_G(H) = N_G(g)$; $Z_G(H) =: Z_G(g)$

Soit $G \xrightarrow{f} H$ un morphisme

- On a une <u>factorisation canonique</u> : "1er thm. fond. de gp".



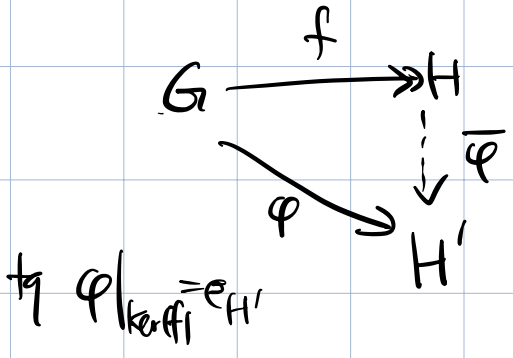
- <u>Propriété universelle de noyau</u> :

Si $G \xrightarrow{f} H$ est un morph. de gp surjectif

Alors $\forall$ groupe H', on a une bijection

$$\mathrm{Hom}(H, H') \simeq \left\{ \varphi \in \mathrm{Hom}(G, H') \;\middle|\; \varphi|_{\ker(f)} = e_{H'} \right\}$$

i.e. $\ker(f) \subset \ker(\varphi)$.



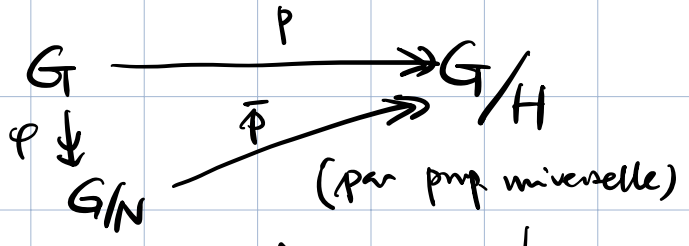
tq $\varphi|_{\ker f} = e_{H'}$

- <u>Exemple</u> $N < H < G$ sous-gp distingués.

alors on a un isom. canonique

$$\frac{G/N}{H/N} \xrightarrow{\sim} G/H$$

"3ème thm fond. de gp"



$N \subset \ker(p) = H$

$$\ker(\varphi) = \left\{ [g] \in G/N \;\middle|\; [g] = [e] \in G/H \right\} = H/N$$

$\Updownarrow$

$g \in H$

$\Rightarrow$ (1er thm fond.)

$$\frac{G/N}{H/N} \xrightarrow{\simeq} G/H$$

Rappel. $H < G$ sous-groupe

$[G:H] := \#\, G/H = \#\, {}_H\backslash G$ où $G/H := \{\text{les classes à gauches}\}$

${}_H\backslash G = \{\text{droite}\}$

- $N < H < G$, alors $[G:N] = [G:H] \cdot [H:N]$.

Déf (Suite de composition) Soit G un groupe fini.

Une **Suite de Composition** de G est

$$\{e\} = G_n \lhd \cdots \lhd G_2 \lhd G_1 \lhd G_0 = G$$

où $\forall\, 1 \le i \le n$, $G_i \lhd G_{i-1}$ est un sous-groupe distingué

(⚠ on ne demande pas que G_i est distingué dans G)

tq $\forall\, 1 \le i \le n$ G_{i-1}/G_i est un groupe simple.

($i^{\text{ème}}$ facteur)

Rappel Un groupe fini G est dit **simple** si $\{e\}$ et G sont les **seuls** sous-gp. distingués de G.

("atome" dans la théorie de groupe)

Exemples

- groupe cyclique d'ordre p, où p premier
- A_n $(n \geq 5)$.
- $PSL_2(\mathbb{F}_7)$ etc.
- Bonne nouvelle : les groupes simples (finis) sont classifiés.

(mauvaise nouvelle : assez compliqués).

Thm (Jordan-Hölder) Pour un groupe fini G.

(Existence) $\exists$ une suite de composition $\{e\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G$

(unicité) n et $\{\{ G_i/G_{i+1} \mid 1 \leq i \leq n \}\}$ sont indépendants de la suite.

c'est-à-dire, si on a deux suites de composition
$$\begin{cases} \{e\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G \\ \{e\} = G'_{n'} \triangleleft G'_{n'-1} \triangleleft \cdots \triangleleft G'_1 \triangleleft G'_0 = G \end{cases}$$

Alors $n = n'$ et $\exists$ une permutation $\sigma \in \mathfrak{S}_n$

tq $G_{i-1}/G_i \cong G_{\sigma(i)-1}/G_{\sigma(i)}$

Exemple (non-unicité) : $G = \underbrace{\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \triangleright \underbrace{3\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}} \triangleright \{1\}$; $G = \underbrace{\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/2\mathbb{Z}} \triangleright \underbrace{2\mathbb{Z}/6\mathbb{Z}}_{\mathbb{Z}/3\mathbb{Z}} \triangleright \{1\}$.

Déf Un groupe (fini) G est <u>résoluble</u> si il admet une suite de composition dont tous les facteurs sont cyclique d'ordre p (p premier)

Déf : $DG := [G,G] :=$ le sous-gp. distingué de G engendré par les éléments de la forme $g_1 g_2 g_1^{-1} g_2^{-1}$ avec $g_1, g_2 \in G$.

<u>Exercice</u> : • $G/[G,G] = G^{ab}$ est un groupe abélien

• $\forall A$ gp. abélien, $\mathrm{Hom}(G, A) \cong \mathrm{Hom}(G^{ab}, A)$.