Représentations

Soit X un ensemble non-vide. Notons par S_X le groupe de bijections de X dans X avec multiplication donnée par la composition.

Une bijection $f : X \to Y$ induit un isomorphisme $\tilde{f} : S_X \to S_Y$ en prenant $\tilde{f}(\sigma) := f \circ \sigma \circ f^{-1}$.

En particulier, si $\# X = n < \infty$ alors on a une bijection $X \xrightarrow{f} \{1, 2, \ldots, n\}$, donc un isomorphisme $S_X \xrightarrow{\tilde{f}} S_{\{1,2,\ldots,n\}} \cong S_n$

Définition S_X s'appelle le groupe de permutations de X.

Le groupes S_X sont plus facile a visualiser, donc on espère qu'un morphisme d'un groupe donné G dans un groupe de permutation S_X nous donnera plus d'information sur G. D'où la définition suivante.

Définition Soit G un groupe. Une représentation par permutations de G consiste en la donnée d'un couple (X, ρ) où X est un ensemble et ρ est un morphisme de groupes $\rho : G \to S_X$.
On dit que la représentation est fidèle si ρ est un monomorphisme.

Exemples 1) (X, τ) représentation triviale :

$$\tau : G \longrightarrow S_X$$
$$g \longmapsto \mathrm{id}_X$$

2) (G, α) représentation par conjugaison.

$$\alpha : G \longrightarrow S_G$$
$$g \longmapsto (x \mapsto gxg^{-1})$$

Remarque : τ et α ne sont pas fidèles.

Théorème (Cayley, 1878). Tout groupe admet une représentation par permutations fidèle.

Preuve Soit G un groupe. On définit la représentation (G, λ) par $\lambda : G \longrightarrow S_G$

$$g \longmapsto (x \mapsto gx)$$

Il est clair que $\lambda(g)$ est une bijection pour tout $g \in G$ et que λ est une application injective.

On vérifie que λ est un morphisme de groupes :

$$\lambda(g \cdot h) = \begin{pmatrix} G & \longrightarrow & G \\ x & \longmapsto & g \cdot h \cdot x \end{pmatrix} = \begin{pmatrix} G & \longrightarrow & G & \longrightarrow & G \\ x & \longmapsto & h \cdot x & \longmapsto & ghx \end{pmatrix}$$
$$y \longmapsto g \cdot y$$
$$= \left(x \mapsto \lambda(g)\left(\lambda(h)(x)\right)\right) = \lambda(g) \circ \lambda(h).$$

□

Remarques.

1) Donc tout groupe est isomorphe à un sous-groupe du groupe des permutations sur soi-même.
2) (G, λ) s'appelle la représentation régulière gauche.
3) Il existe aussi la représentation régulière droite (G, ρ), $\rho : G \longrightarrow S_G$

$$g \longmapsto (x \mapsto xg^{-1})$$

Théorème Soit G un groupe et H un sous-groupe de G d'indice n. Alors il existe une représentation par permutations $\varphi : G \longrightarrow S_n$ telle que $\ker \varphi = \bigcap_{x \in G} xHx^{-1}$.

Corollaire

Soit G un groupe simple (i.e. il n'a pas de sous-groupe propre non-trivial qui soit normal) et H un sous-groupe d'indice $n \neq 1$. Alors G admet une représentation par permutations fidèle:

$$\rho : G \longrightarrow S_n.$$

Preuve du corollaire

$\ker \rho$ est un sous-groupe normal de G. Comme G est simple, il n'en reste que $\ker \rho = \{1\}$ ou $\ker \rho = G$.
Mais $\ker \rho = \bigcap_{g \in G} gHg^{-1} \leq H \lneq G$. Donc $\ker \rho = \{1\}$ et ρ est une représentation fidèle.

Preuve du théorème

On pose $X = G/H$ et donc $\#X = n$ et $S_X \simeq S_n$

On considère l'application $\rho : G \longrightarrow S_X$

$$g \longmapsto (aH \longmapsto gaH)$$

ρ est bien définie car $aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow$
$b^{-1}g^{-1}ga \in H \Leftrightarrow (gb)^{-1}ga \in H \Leftrightarrow gaH = gbH$
(utiliser l'autre sens pour voir l'injectivité)
Il est facile à voir que ρ est un homomorphisme de groupes (preuve analogue à celle pour la représentation régulière gauche).
De plus $g \in \ker \rho \Leftrightarrow \rho(g) = id_X \Leftrightarrow aH = gaH, \forall a$
$\Leftrightarrow a^{-1}ga \in H, \forall a \in G \Leftrightarrow g \in aHa^{-1}, \forall a \in G$
$\Leftrightarrow g \in \bigcap_{a \in G} aHa^{-1}$. Donc

$$\ker \rho = \bigcap_{a \in G} aHa^{-1}$$

(le plus grand sous-groupe normal de G contenu dans H) □

Action d'un groupe sur un ensemble

Soit X un ensemble et soit G un groupe

Définition : Une **action à gauche de G sur X** est la donnée d'une application

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

qui satisfait : 1) $1 \cdot x = x \quad \forall\, x \in X$

2) $(g_1 \cdot g_2)\, x = g_1 \cdot (g_2 \cdot x) \quad \forall\, g_1, g_2 \in G,\ x \in X$

($\cdot$ à gauche : dans G ; $\cdot$ à droite : actions.)

On dit que X est un **G-ensemble**.

Si X et Y sont des G-ensembles alors une application des G-ensembles de X dans Y est une application $f : X \longrightarrow Y$ telle que $f(g \cdot x) = g \cdot f(x)$, $\forall x \in X$, $\forall g \in G$.

Remarque 1) De même, on peut définir une action à droite de G sur X : $(G, X) \longrightarrow X$ avec les propriétés

$$(g, x) \longmapsto g * x$$

1') $x * 1 = x \quad \forall\, x \in X$

2') $x * (g_1 g_2) = (x * g_1) * g_2$

2) Toute action à gauche de G sur X donne une action à droite et vice-versa en posant :

$$x * g = g^{-1} \cdot x .$$

Exercice : vérifier

Théorème : La donnée d'un G-ensemble à gauche X est equivalente à la donnée d'une représentation par permutations de G. Plus précisement, on a une bijection :

$$\left\{\begin{array}{l}\text{Actions à gauche}\\ \text{de } G \text{ sur } X\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Représentations par}\\ \text{permutations de } G\end{array}\right\}$$

$$\begin{pmatrix} G\times X \longrightarrow X \\ (g,x) \longmapsto g\cdot x \end{pmatrix} \longmapsto \begin{pmatrix} G \longrightarrow S_X \\ g \longmapsto (x \mapsto g\cdot x) \end{pmatrix}$$

$$\begin{pmatrix} G\times X \longrightarrow X \\ (g,x) \longmapsto \rho(g)(x) \end{pmatrix} \longleftarrow \rho : G \longrightarrow S_X$$

Exercice vérifier que ces applications sont bien définies et sont l'inverse l'une de l'autre.

Exemple :

1) $S_X \times X \longrightarrow X$
$(\sigma, x) \longmapsto \sigma(x)$

2) $G \times G \longrightarrow G$
$(g, a) \longmapsto gag^{-1}$ (conjugaison)
$\longmapsto ga$ (translation)
$\longmapsto a$ (triviale)

3) $\varphi : H \longrightarrow G$ homomorphisme de groupes
$H \times G \longrightarrow G$ G devient un H-ensemble
$(h, g) \longmapsto \varphi(h)\cdot g$

4) $\theta : K \longrightarrow Aut(H)$ On dit que H
$K \times H \longmapsto H$ est un **K-groupe**
$(k, h) \longmapsto \theta(k)(h)$

Définitions / Notations

Soit X un G-ensemble à gauche

1) $\mathrm{Stab}_G(x) = G_x = \{g \in G \mid g \cdot x = x\}$.

2) G_x aussi appelé le sous-groupe d'isotropie de x ($1 \in G_x$, $h, g \in G_x \Rightarrow h^{-1} g x = x \Rightarrow h^{-1} g \in G_x$)

3) On dit que x est un point fixe de l'action si $G_x = G$ ($\forall g \in G \quad g \cdot x = x$)

4) On dit que G agit librement sur X si $\forall x \in X$, $G_x = \{1\}$.

5) On dit que l'action de G sur X est fidèle si $(g \cdot x = x \quad \forall x \in X) \Rightarrow g = 1$.

Rem : action libre $\Rightarrow$ action fidèle.

6) On dit que G agit transitivement sur X si $(\forall x, y \in X, \exists g \in G, y = g \cdot x)$.

7) $\mathcal{O}_x = \{g \cdot x \mid g \in G\}$ s'appelle l'orbite de x.

Remarque On a une relation d'équivalence sur X, dont les classes d'equivalence sont les orbites de l'action de G, en posant $x \sim y$ si $y \in \mathcal{O}_x$.

Donc on a une décomposition de X en union disjointe des classes d'equivalence ;

$$X = \coprod_{x \in S} \mathcal{O}_x$$

où S est un ensemble de représentants d'orbites pour l'action de G sur X.

Proposition Soit G un groupe fini et soit X un G-ensemble. On prend $x \in X$. Alors $\#\mathcal{O}_x = [G : G_x]$.

Preuve

On construit une application surjective $f : G \longrightarrow \mathcal{O}_x$ en prenant $f(g) = g \cdot x$

On définit une application $\overline{f} : G/G_x \longrightarrow \mathcal{O}$ par $\overline{f}(\pi(g)) = f(g)$ où $\pi : G \longrightarrow G/G_x$ est la projection canonique.

- $\overline{f}$ est bien défini car
$\pi(g) = \pi(h) \iff g^{-1}h \in G_x \iff g^{-1}h\,x = x$
$\iff gx = hx \iff f(g) = f(h)$.
- en parcourant les équivalences dans l'autre sens on démontre que $\overline{f}$ est injective.
- de plus $\overline{f}$ est clairement surjective.

Donc $\overline{f} : G/G_x \longrightarrow \mathcal{O}_x$ est une bijection et
$\#\mathcal{O}_x = [G : G_x]$. □

Produit semi-direct

Déf : Une suite exacte $1 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C \longrightarrow 1$ des groupes est dite scindée s'il existe un morphisme $s : C \to B$ tel que $v \circ s = id_C$.

Question Peut-on construire un groupe G tel que la suite
$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

soit une suite exacte scindée des groupes (K et H sont des groupes finis).
Une réponse positive est donnée par $G \simeq K \times H$.
Mais peut-on construire d'autres groupes G.
La construction suivante va dans cette direction.

Construction de $K \times_\theta H$

Soit K un H-groupe donné par $\theta : H \to Aut(K)$.
Sur l'ensemble $K \times H$ on définit une multiplication tordue par θ :

$$(k, h) \cdot_\theta (k', h') := (k\,\theta(h)(k'),\ h\,h')$$

Lemme $(K \times H, \cdot_\theta)$ est un groupe.

Preuve

- exercice : montrer l'associativité
- $(1, 1)$ est l'élément neutre.
- $(k, h)^{-1} = (\theta(h^{-1})(k^{-1})\ ;\ h^{-1})$ (à vérifier) □

Définition Le groupe $(K \times H, \cdot_\theta)$ est appelé le produit semi-direct de K et H par θ et se note $K \times_\theta H$, $K \rtimes_\theta H$ ou $K \rtimes H$

Remarque : Si θ est l'action triviale, alors le produit semi-direct par θ est isomorphe au produit direct :

$$\theta = id_K \Rightarrow K \rtimes_\theta H \cong K \times H .$$

Lemme Soit K un H-groupe par θ. On a une suite exacte scindée donnée par :

$$1 \longrightarrow K \xrightarrow{i} K \rtimes_\theta H \xrightarrow{p} H \longrightarrow 1$$

où $i(k) = (k, 1)$ et $p((k, h)) = h$.

Preuve :

- i est clairement injectif

$$i(k \cdot k') = (k \cdot k', 1) = (k, 1) \cdot (k', 1) = i(k) \cdot i(k')$$

donc un homomorphisme de groupes.

- p est clairement surjectif.

$$p((k, h) \cdot (k', h')) = p((k\,\theta(h)(k'), h\,h')) = h\,h' = p((k, h)) \cdot p((k', h'))$$

donc un homomorphisme de groupes.

- $\operatorname{Im} i = \{(k, 1) \mid k \in K\} = \operatorname{Ker} p$

Donc la suite est exacte.

On définit $\tau : H \longrightarrow K \rtimes_\theta H$ par $\tau(h) := (1, h)$

- $\tau(h\,h') = (1, h\,h') = (1, h) \cdot (1, h') = \tau(h) \cdot \tau(h')$ donc un homomorphisme de groupes.
- $p \circ \tau(h) = p((1, h)) = h$, donc τ est une section de p. □

Remarques Du lemme précédent on obtient

- $K \simeq \{(k, 1) \mid k \in K\}$ est un sous-groupe normal de $K \rtimes_\theta H$
- $H \simeq \{(1, h) \mid h \in H\}$ est un sous-groupe de $K \rtimes_\theta H$
- $(1, h)(k, 1)(1, h^{-1}) = (\theta(k), 1)$ la conjugaison correspond à θ.

Théorème Soit K, H deux groupes. Un groupe G est isomorphe à un produit semi-direct de K et H si et seulement si on a une suite exacte scindée :

$$1 \longrightarrow K \xrightarrow{u} G \underset{s}{\overset{v}{\rightleftarrows}} H \longrightarrow 1$$

Preuve

"$\Longrightarrow$" c'est le lemme précédent.

"$\Longleftarrow$" on suppose que la suite est exacte scindée.

On a :

1) $u(K) \trianglelefteq G$
2) $u(K) = \ker v$
3) $v \circ s = id_H$
4) $s(H) \cap u(K) = \{1\}$.

On met une structure de H-groupe sur K par :

$$\theta : H \longrightarrow \mathrm{Aut}(K)$$
$$h \longmapsto u^{-1}\big(\underbrace{s(h)\, u(k)\, s(h^{-1})}_{\in u(K) \text{ car } u(K) \trianglelefteq G}\big)$$

- $\theta(h)$ est une bijection d'inverse $\theta(h^{-1})$.
- $\theta(h_1 h_2)(k) = u^{-1}\big(s(h_1 h_2)\, u(k)\, s((h_1 h_2)^{-1})\big)$
$$= u^{-1}\big(s(h_1)\, \underbrace{s(h_2)\, u(k)\, s(h_2^{-1})}_{u(\theta(h_2)(k))}\, s(h_1)\big)$$
$$= \theta(h_1)\big(\theta(h_2)(k)\big)$$

Donc $\theta(h_1, h_2) = \theta(h_1) \circ \theta(h_2)$ et θ est un homomorphisme de groupes.

Il s'en suit qu'on peut construire $K \rtimes_\theta H$.

On peut voir que $K \rtimes_\theta H \cong G$

On essaye d'utiliser le petit lemme des cinq :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{i} & K \times_\theta H & \underset{\sigma}{\overset{p}{\rightleftarrows}} & H & \longrightarrow & 1 \\ & & \| & & \downarrow \varphi & & \| & & \\ 1 & \longrightarrow & K & \xrightarrow{u} & G & \underset{s}{\overset{v}{\rightleftarrows}} & H & \longrightarrow & 1 \end{array}$$

Donc si on construit un homomorphisme de groupes $\varphi : K \times_\theta H \longrightarrow G$ qui fait commuter le diagramme, φ sera forcement un isomorphisme

On pose $\varphi((k,h)) = u(k) \cdot s(h)$

Et on vérifie que c'est un morphisme

$$\begin{aligned} \varphi((k,h)(k',h')) &= \varphi((k\theta(h)(k'), hh') = \\ &= u(k\theta(h)(k')) \cdot s(hh') \\ &= u(k)\, u(\theta(h)(k'))\, s(h)\, s(h') \\ &= u(k)\, s(h)\, u(k')\underbrace{s(h^{-1})\, s(h)}_{=1}\, s(h') \\ &= u(k)\, s(h)\, u(k')\, s(h') \\ &= \varphi((k,h))\, \varphi((k',h')) \end{aligned}$$

□

Remarques

1) $\varphi \circ \sigma = s$

2) φ est l'unique morphisme qui fait commuter le diagramme et qui satisfait $\varphi \circ \sigma = s$.

En effet soit ψ un morphisme avec mêmes propriétés.

$$\begin{aligned} \psi((k,h)) &= \psi(i(k)\,\sigma(h)) = \psi \circ i(k) \cdot \psi \circ \sigma(h) \\ &= u(k) \cdot s(h) \\ &= \varphi((k,h)) \quad \text{Donc } \psi = \varphi \end{aligned}$$

Application

Soit $C_n = \langle x \rangle$ et $C_m = \langle y \rangle$ deux groupes cycliques d'ordre n, respectivement m.

On définit $\theta : C_m \to Aut(C_n)$ t.q.

$(\theta(y))^m = id_{C_n}$

Donc $\theta(y)(x) = x^k$ $\quad 1 \leq k \leq n-1$ et $(k,n) = 1$

$(\theta(y))^m(x) = x^{k^m} = x \Rightarrow k^m \equiv 1 \pmod{n}$

Ainsi, pour tout k, $1 \leq k \leq n-1$, $(k,n) = 1$ et $k^m \equiv 1 \pmod{n}$ on définit

$$\theta_k : C_m \longrightarrow Aut(C_n)$$
$$y \longmapsto (x \longmapsto x^k)$$

Définition

Un groupe <u>métacyclique de paramètres (n, m, k)</u> avec $1 \leq k \leq n-1$, $(k,n) = 1$, $k^m \equiv 1 \pmod{n}$ est $M(n,m,k) = C_n \rtimes_{\theta_k} C_m$.

Remarques

1) $M(n,m,1) = C_n \times C_m$

2) $M(n,m,k)$ est engendré par $(x,1)$ et $(1,y)$ avec les relations :

$(x,1)^n = (1,1)$

$(1,y)^m = (1,1)$

$(1,y)(x,1)(1,y) = (x,1)^k$.

Exercice Montrer que les relations plus haut sont vérifiées.

Pour voir que $(x,1)$ et $(1,y)$ sont des générateurs

On utilise que
$(x^\alpha, 1) = (x,1)^\alpha$ et $(u,v) = (u,1)(1,v)$
$(1, y^\beta) = (1,y)^\beta$

Proposition
$M = \langle a, b \mid a^n = 1, b^m = 1, a^k b a^{-1} b^{-1} = 1 \rangle$
est une présentation du groupe $M(n,m,k)$.

Preuve
On a une bijection $\{a, b\} \longrightarrow \{x, y\}$ qui envoie les relations dans M sur des relations dans $M(n,m,k)$. Par le théorème de Van Dyk, on a une surjection

$$f : M \longrightarrow M(n,m,k)$$

Mais, étant donné que $ba = a^k b$ dans M, tout élément de M s'écrit $a^r b^s$ avec $0 \leq r \leq n-1$ et $0 \leq s \leq m-1$,
Donc $|M| \leq n \cdot m = |M(n,m,k)|$.
Il s'en suit que f est un isomorphisme.

Sous-groupe dérivé

Définition Soit G un groupe $[a,b] := aba^{-1}b^{-1}$ est appelé le commutateur de a et b.

Remarques
1) $[b,a]ab = ba$ donc a et b commutent si et seulement si $[b,a] = 1$.
2) $[a,1] = [1,a] = 1$; $[a,b]^{-1} = [b,a]$.
3) $f : G \to H$ homomorphisme $f([a,b]) = [f(a), f(b)]$.

en particulier
$$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}].$$

4) G est abélien si et seulement si $\forall\, g,h \in G$ on a $[g,h] = 1$

Définition

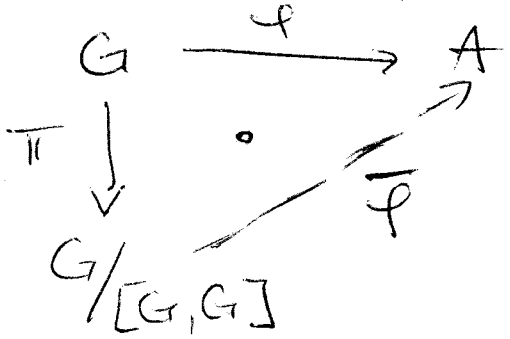
On appelle sous-groupe dérivé de G le sous-groupe de G engendré par les commutateurs.
Notation : $[G,G]$, G', $\mathcal{D}G$.

Remarque A priori $[G,G]$ est plus grand que l'ensemble de commutateurs de G.

Théorème Soit G un groupe. Alors

1) $[G,G] \trianglelefteq G$
2) $G/[G,G]$ est abélien.
3) on a la propriété universelle suivante :

Pour tout groupe abélien A et tout morphisme de groupes $\varphi : G \to A$, il existe un unique morphisme $\overline{\varphi} : G/[G,G] \to A$ tel que $\overline{\varphi} \circ \pi = \varphi$, où $\pi : G \to G/[G,G]$ est la projection canonique.



Déf : Le groupe $G/[G,G]$ s'appelle l'abélianisé de G et se note G_{ab}.

Preuve (du théorème)

1) $x \in [G,G] \Rightarrow x = \prod_{i=1}^{u} [a_i, b_i]$

$$g x g^{-1} = g\left(\prod_{i=1}^{u} [a_i,b_i]\right) g^{-1} = \prod_{i=1}^{u} \left(g [a_i,b_i] g^{-1}\right)$$
$$= \prod_{i=1}^{u} [g a_i g^{-1}, g b_i g^{-1}] \in [G,G].$$

2) Soit $\pi : G \to G/[G,G]$

Alors $[\pi(g), \pi(h)] = \pi([g,h]) = 1$
Donc $G/[G,G]$ est abélien.

3) Il suffit de voir que $[G,G] \subseteq \ker f$.
et appliquer la propriété universelle du quotient.

tout commutateur dans A est trivial.

$$f([g,h]) = [f(g), f(h)] = 1$$
donc $[g,h] \in \ker f$, $\forall g, h \in G$. □

Corollaire Soit G un groupe et H un sous-groupe normal de G. Alors G/H est abélien ssi $[G,G] \leq H$.

Preuve

"$\Rightarrow$" $\pi : G \to G/H$ morphisme. Par 3) de la preuve du théorème $[G,G] \leq \ker \pi = H$

"$\Leftarrow$"
$$[\pi(g), \pi(h)] = \pi(\underbrace{[g,h]}_{\in H}) = 1$$

Donc G/H est abélien □