Groupe quotient

Soit G un groupe et H un sous-groupe de G

On définit sur G une relation d'équiv. en posant $x \equiv_H y \iff x^{-1}y \in H$

$\iff y \in xH = \{xh \mid h \in H\}$.

Lemme : $\equiv_H$ est une relation d'équivalence.

Preuve : exercice.

Def : $G/H = G/\equiv_H$ = ensemble des classes à droite modulo H.

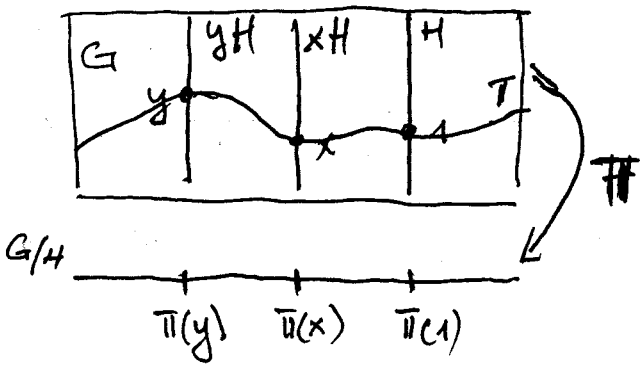
$\pi : G \longrightarrow G/H$ projection canonique

$x \longmapsto xH$

Les classes ~~sont~~ toutes la même cardinalité :

$H \longrightarrow xH$ est une bijection.

$h \longmapsto xh$



T - transversale.

$T = s(G/H)$ où

$s : G/H \longrightarrow G$ est une section de π

(à chaque classe on choisit un représentant)

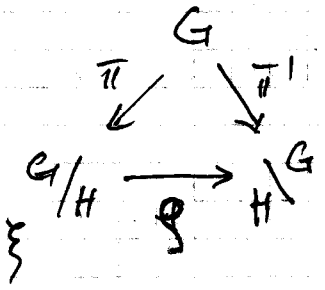
il y a une bijection $T \longrightarrow G/H$

$t \longmapsto \pi(t)$.

De même on définit une relation d'équivalence $\equiv_H$

$x \equiv_H y \iff xy^{-1} \in H$; $H\backslash G = G/\equiv_H$ = ensemble de classes à gauche.

En général $G/H \neq {}_H\backslash G$. Cependant il existe une bijection $G/H \simeq {}_H\backslash G$ donnée par



$$\varphi(\xi) = \pi'\left(s(\xi)^{-1}\right)$$

où $\pi' : G \to {}_H\backslash G$ est la projection canonique.

Preuve :

1) démontrer que φ ne dépend pas du choix de s.

2) démontrer que φ est bijective.

1) Supposons que $s_1 : G/H \to G$ est un autre choix de section de π. Alors $s(\xi) = s_1(\xi)\, h$, $h \in H$.

$$\pi'\left(s(\xi)^{-1}\right) = \pi'\left(h^{-1} s_1(\xi)^{-1}\right) = \pi'\left((s_1(\xi)\, h)^{-1}\right).$$

2) a) φ est injective : $\pi'\left(s(\xi)^{-1}\right) = \pi'\left(s(\eta)^{-1}\right)$

$\Leftrightarrow s(\xi)^{-1} = h\, (s(\eta))^{-1} \Leftrightarrow s(\xi) = s(\eta)\, h^{-1}$

$\Leftrightarrow \xi = \eta$.

b) φ est surjective : Soit $\eta' \in {}_H\backslash G$ et $x \in \eta'$

Alors $\varphi(\pi(x^{-1})) = \pi'\left(\left(s \circ \pi(x^{-1})\right)^{-1}\right) = \pi'(x) = \eta'$.

Exemple : $S_3 = \{1 ; (1,2) ; (1,3) ; (2,3) ; (1,2,3) ; (1,3,2)\}$.

$H = \{1 , (1,2)\}$.

$$S_3/H = \{H , (1,3)H , (2,3)H\} = \{H ; \{(1,3) ; (1,2,3)\} ; \{(2,3) ; (1,3,2)\}\}$$

$${}_H\backslash S_3 = \{H ; \{(1,3) ; (1,3,2)\} ; \{(2,3) ; (1,2,3)\}\}.$$

Définition

Soit G un groupe et $H \leq G$, tel que $\#(G/H) < \infty$.

$[G:H] = |G/H| = \#\, G/H$ = l'indice de H dans G.

Théorème (Formule d'indices)

Soit G un groupe fini et $H \leq G$. Alors on a $|G| = [G:H] \cdot |H|$.

Preuve : On choisi une transversale T : $G = \coprod_{x \in T} xH$

$$\#G = \sum_{x \in T} \#(xH) = \sum_{x \in T} \#H =$$

$$= \#T \#H = \#G/H \cdot \#H \qquad \square$$

Corollaires

1) (Théorème de Lagrange) Soit G un groupe fini et $H \leq G$. Alors $|H|$ divise $|G|$.

2) Soit G un groupe fini et $g \in G$. alors l'ordre de g divise $|G|$. En particulier, $g^{|G|} = 1$. (ordre$(g) = |\langle g \rangle|$)

Problème Mettre sur G/H une structure de groupe telle que $\pi : G \longrightarrow G/H$ soit un morphisme de groupe : $\pi(xy) = \pi(x) \cdot \pi(y)$ à définir.

Si $x = x' h_1$ et $y = y' h_2$ avec $h_1, h_2 \in H$ il faut, pour pouvoir définir la multiplication dans G/H, que $x' h_1 y' h_2 = x' y' h_3$ pour un $h_3 \in H$.

En particulier pour tout $y' \in G$ $h_1, h_2 \in H$ on doit avoir $y'^{-1} h_1 y' = h_3 h_1^{-1} \in H$

Donc on obtient la condition :

$x H x^{-1} = H$ pour tout $x \in G$.

Définition Soit G un groupe et $H \leq G$.
On dit que H est un sous-groupe **normal** (ou **distingué**) de G si $xHx^{-1} = H$. Notation: $H \trianglelefteq G$

Construction de la loi de G/H

Si G est un groupe et $H \trianglelefteq G$ alors G/H avec la multiplication $\overline{\pi}(x)\cdot\overline{\pi}(y) := \overline{\pi}(xy)$ est un groupe, appelé le **groupe quotient** de G par H

Exemples

1) $G \trianglelefteq G$ et $\{1\} \trianglelefteq G$; $G/G \simeq \{1\}$, $G/\{1\} \simeq G$.

2) $f : G \to H$ un morphisme de groupe.
Alors $\ker f \trianglelefteq G$.

3) $A_n \trianglelefteq S_n$ car $A_n = \ker(\text{sign})$ pour
$\text{sign} : S_n \longrightarrow \{\pm 1\}$.
$\sigma \longmapsto +1$ si σ est paire
-1 si σ est impaire

4) $\{\text{id}, (1,2)\} \not\trianglelefteq S_3$

Remarques

1) $H \trianglelefteq G$ si et seulement si $xH = Hx \ \forall x \in G$.

2) "Etre normal" n'est pas une relation transitive :

$\{1, (1,2)(3,4)\} \trianglelefteq \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq A_4$

mais $\{1, (12)(3,4)\} \not\trianglelefteq A_4$.

Lemme : Soit $f : G \to H$ un morphisme de groupes. Alors $G/\ker f \simeq \operatorname{Im} f$.

Preuve

On a que

$$1 \to \ker f \to G \xrightarrow{f} \operatorname{Im} f \to 1 \quad \text{et}$$
$$1 \to \ker f \to G \xrightarrow{\pi} G/\ker f \to 1$$

sont des suites exactes courtes

On construit une application.

$\varphi : G/\ker f \to \operatorname{Im} f$ définie par

$$\varphi(\bar{\pi}(g)) := f(g).$$

C'est un exercice simple de voir que φ est un morphisme de groupe. De plus.

$$\begin{array}{ccccccccc} 1 & \to & \ker f & \to & G & \to & \operatorname{Im} f & \to & 1 \\ & & \| & & \| & & \uparrow \varphi & & \\ 1 & \to & \ker f & \to & G & \to & G/\ker f & \to & 1 \end{array}$$

est un diagramme commutatif par construction de φ. Donc par le petit lemme de cinq (voir exercices) φ est un isomorphisme. □

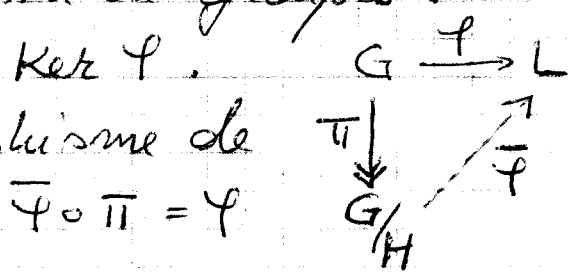
En fait la construction de $\varphi : G/\ker f \to \operatorname{Im} f$ est le cas particulier d'une propriété générale du quotient, appelée la propriété universelle du quotient.

Théorème (propriété universelle du quotient)

Soit G un groupe, $H \trianglelefteq G$. Alors pour tout groupe L et tout morphisme de groupes :

$\varphi : G \to L$ t.q. $H \subseteq \ker \varphi$.

Il existe un unique morphisme de groupes $\overline{\varphi} : G/H \to L$ t.q. $\overline{\varphi} \circ \pi = \varphi$



Preuve a) Unicité : supposons qu'il existe

φ' et $\varphi'' : G/H \to L$ t.q. $\varphi' \circ \pi = \varphi$ et $\varphi'' \circ \pi = \varphi$

Comme π est surjective on a que $\varphi' = \varphi''$.

b) Existence Soit $\xi \in G/H$ avec $\pi(x) = \xi$ pour un $x \in G$

Posons $\overline{\varphi}(\xi) := \varphi(x)$. Par définition on a $\overline{\varphi} \circ \pi = \varphi$.

Reste à voir :

1) $\overline{\varphi}$ est bien défini : si $\pi(x) = \pi(x')$ alors $x' = xh$, $h \in H$. Mais ceci entraine $\varphi(x) = \varphi(x')$ car $H \leq \ker \varphi$.

2) $\overline{\varphi}$ est un morphisme de groupe

Soit $\xi = \pi(x)$ $\eta = \pi(y)$. Donc $\xi\eta = \pi(xy)$

Alors $\overline{\varphi}(\xi \cdot \eta) = \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = \overline{\varphi}(\xi) \cdot \overline{\varphi}(\eta)$

□

Lemme Avec les notations du théorème on a :

1) $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$

2) $\ker(\overline{\varphi}) \simeq (\ker \varphi)/H$

Preuve : 1) $a \in \mathrm{Im}(\overline{\varphi}) \Leftrightarrow \exists\, \eta \in G/H$, $\overline{\varphi}(\eta) = a$

$\Leftrightarrow \exists\, x \in G$, $\varphi(x) = a \Leftrightarrow a \in \mathrm{Im}\,\varphi$.

2) Etant donné que $H \trianglelefteq G$ on a que $H \trianglelefteq \ker \varphi$.
Par la propriété universelle du quotient, il existe $\bar{\varphi} : \ker \varphi / H \to G/H$ tel que

$$\begin{array}{ccc} \ker(\varphi) & \xrightarrow{\pi_H \circ i} & \\ \downarrow \pi_H & & \\ \ker(\varphi)/H & \xrightarrow{j} & G/H \end{array}$$

car $\ker \pi \circ i = H \leq \ker \varphi$.

On voit que j est injectif $\left(1 = j(\pi_H(x)) = \pi \circ i(x) \iff i(x) \in H \iff x \in H\right)$

De plus $\bar{\varphi} \circ j(\pi(x)) = \bar{\varphi} \circ \pi_H \circ i(x) =$
$= \varphi(x) = 1$ si $x \in \ker \varphi$

Donc $1 \to \ker(\varphi)/H \xrightarrow{j} G/H \xrightarrow{\bar{\varphi}} \mathrm{Im}(\bar{\varphi}) \to 1$ est une s.e.c.

Comme j est un isomorphisme sur son image et $\mathrm{Im}\, j = \ker \bar{\varphi}$ par exactitude de la suite, on obtient que $\ker(\varphi)/H \simeq \ker(\bar{\varphi})$. □

Centre et centralisateur d'un groupe

Def : Soit G un groupe et A un sous-ensemble non-vide de G. Alors le **centralisateur de A dans G** est $C_G(A) = \{x \in G \mid xa = ax, \forall a \in A\}$.

Cas particuliers

1) $A = \{x\} \Rightarrow C_G(x) =$ centralisateur de x dans G.
2) $A = G \Rightarrow C_G(G) = Z(G)$ est le **centre de G**.

Lemme :

1) $Z(G) \trianglelefteq G$

2) G est abélien ssi $G = Z(G)$

Preuve : exercice

Automorphismes de groupe

Def Soit G un groupe. Un automorphisme de G est un morphisme de groupe bijectif de G dans G.

Rem : $(Aut(G), \circ)$ est un groupe, où $Aut(G)$ est l'ensemble de tous les automorphismes de G.

Def Soit $g \in G$. L'application $\alpha_g : G \longrightarrow G$, $x \longmapsto gxg^{-1}$ est appelée la conjugaison par g.

Rem : $\alpha_g \in Aut(G)$ (à vérifier).

Lemma 1) $Inn(G) := \{\alpha_g \mid g \in G\}$ est un sous-groupe de G. $Inn\, G$ est appelé le groupe d'automorphismes intérieures de G.

2) $Inn(G) \trianglelefteq G$. $Out(G) := Aut(G)/Inn(G)$ est appelé le groupe des automorphismes extérieures.

Preuve 1) $\alpha_g \circ (\alpha_h)^{-1} = \alpha_{gh^{-1}}$

2) $\varphi \circ \alpha_g \circ \varphi^{-1} = \alpha_{\varphi(g)}$ $\varphi \in Aut(G)$. □

Proposition : $Inn(G) = G/Z(G)$.

Preuve : L'application $\beta : G \longrightarrow Inn(G)$

définie par $\beta(x) = \alpha_x$ est un morphisme de groupes surjectif, de noyau $Z(G)$ $\square$.

L'équation des classes

Soit G un groupe. On définit la relation $\sim$ dans G par

$x \sim y$ si il existe $g \in G$, $\alpha_g(x) = y$.

Il est facile à voir que $\sim$ est une relation d'équivalence.

On note avec $S \subseteq G$ un ensemble de représentants des classes de conjugaison dans G, où $C(x) = \{y \in G \mid x \sim y\}$ est la classe de conjugaison de x dans G.

Remarque : $C(x) = \{gxg^{-1} \mid g \in G\}$.

Lemme :

1) $C(x) = \{x\}$ ssi $x \in Z(G)$
2) On a une bijection entre $C(x)$ et $G/C_G(x)$.

Preuve :

1) "$\Rightarrow$" On a que $\forall g \in G$ $gxg^{-1} \in C(x)$.
Mais $C(x) = \{x\}$ donc $gxg^{-1} = x$.
Comme ceci est vrai $\forall g \in G$ on a que $x \in Z(G)$
"$\Leftarrow$" $x \in Z(G)$ implique $gxg^{-1} = x$, $\forall g \in G$
Donc $C(x) = \{gxg^{-1} \mid g \in G\} = \{x\}$

2) On considère l'application :

$$\theta : G \longrightarrow C(x)$$
$$g \longmapsto \alpha_g(x) = g x g^{-1}$$

On définit ensuite :

$$\bar{\theta} : G/C_G(x) \longrightarrow C(x)$$
$$\bar{g} \longmapsto \alpha_g(x).$$

où $\pi : G \longrightarrow G/C_G(x)$ est la projection canonique

$$g \longmapsto \bar{g}$$

On vérifie :

- $\bar{\theta}$ est bien définie :

$\bar{g} = \bar{h} \iff \exists\, c \in C_G(x)$ $g = hc$

Donc $\alpha_g(x) = g x g^{-1} = h \underbrace{c x c^{-1}}_{=x} h^{-1}$

$= h x h^{-1} = \alpha_h(x)$

- $\bar{\theta}$ est surjective :

facile car θ est surjective

- $\bar{\theta}$ est injective :

Si $\alpha_h(x) = \alpha_g(x) \iff h x h^{-1} = g x g^{-1}$

$\iff (g^{-1}h) x (h^{-1}g) = x$

$\iff g^{-1}h \in C_G(x)$

$\iff \bar{g} = \bar{h}$ dans $G/C_G(x)$

□

On décompose S en union disjointe :

$$S = S' \amalg S'' \quad \text{où} \quad S' = \{x \in S \mid C(x) = \{x\}\}$$
$$= \{x \in S \mid x \in Z(G)\}$$
$$= Z(G).$$

Donc $$G = \coprod_{x \in S} C(x) = \coprod_{x \in Z(G)} \{x\} \amalg \coprod_{x \in S''} C(x)$$

On obtient l'équation des classes :

$$|G| = \sum_{x \in Z(G)} 1 + \sum_{x \in S''} |C(x)|$$
$$= |Z(G)| + \sum_{x \in S''} \frac{|G|}{|C_G(x)|}$$

Corollaire : Soit G un groupe fini, avec $|G| = p^\alpha$, p un nombre premier, $\alpha \in \mathbb{Z}_{>0}$. Alors $Z(G)$ n'est pas le groupe trivial (i.e. $Z(G) \neq \{e\}$).

Preuve :

On utilise l'équation des classes :

$$|G| = |Z(G)| + \sum_{x \in S''} \frac{|G|}{|C_G(x)|}$$

Comme $p \mid |G|$ et $p \mid \frac{|G|}{|C_G(x)|}$ on obtient $p \mid |Z(G)|$, donc $|Z(G)| > 1$.

□