Joachim / Léo 16.09.14

103

Exemples de sous-groupes distingués et de groupes quotient. Applications

I) Motivations

~~la notion de groupe distingué et de groupe quotient est une notion naturelle~~ due mais ne pas écrire / à dire mais ne pas écrire

Ex: le cercle $\mathbb{R}/\mathbb{Z}$ fournit un premier exemple de groupe quotient. Il formalise très bien la notion d'angle et les calculs d'angles.

On fixe G un groupe, H un sous-groupe de G et π la projection $\pi : G \to G/H$ (classe à gauche)

Prop: π est un morphisme de groupes si et seulement si la relation d'équivalence $g_1 \sim g_2 \Leftrightarrow g_1 g_2^{-1} \in H$ est compatible avec la loi de groupe de G.
Si $g_1 \sim g_2$ et $g_3 \sim g_4$ alors $g_1 g_3 \sim g_2 g_4$

Déf: H est un sous-groupe distingué si:
$\forall g \in G\ \forall h \in H \quad ghg^{-1} \in H$

Prop: π est un morphisme si et seulement si H est un sous-groupe distingué.

Si G est commutatif, π est toujours un morphisme.

Ex: · $\mathbb{Z}/n\mathbb{Z}$

· $A_3 \lhd \mathfrak{S}_3$, $\mathfrak{S}_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$

· $\langle (12345) \rangle$ n'est pas distingué dans $\mathfrak{S}_5$

· Tout sous-groupe de Q_8 est distingué, même si Q_8 n'est pas abélien.

II) Comment les construit-on ?

Prop: H est un sous-groupe distingué de G si et seulement si H est le noyau d'un morphisme du groupe G dans un groupe G'.

Appli: Si G est simple, tout morphisme non trivial de G dans G' est injectif.

Ex: · $SO_3(\mathbb{R})$ est simple à mettre dans une autre partie) DVP
· A_n est simple pour $n \geq 5$

Prop: Soit G un groupe. Tout sous-groupe d'indice 2 de G est distingué.

Ex: · $SO_3(\mathbb{R}) \lhd O_3(\mathbb{R})$ $\quad (SO_3(\mathbb{R}) = \mathrm{Ker}(\det_{|O_3(\mathbb{R})}))$

· $A_n \lhd \mathfrak{S}_n$ $\left(\#A_n = \frac{\#\mathfrak{S}_n}{2},\ A_n = \mathrm{Ker}(\varepsilon)\right)$

· $\langle i \rangle \lhd Q_8$ car $[\langle i \rangle : Q_8] = 2$.

· $O_3(\mathbb{R})/SO_3(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$

Prop: Soit G un groupe, $\mathrm{Aut}(G)$ le groupe de ses automorphismes et $\mathrm{Int}(G)$ le groupe de ses automorphismes intérieurs.
Alors $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$

Ex: · $\mathrm{Int}(\mathfrak{S}_6) \lhd \mathrm{Aut}(\mathfrak{S}_6)$ avec:
$\mathrm{Aut}(\mathfrak{S}_6) \simeq \langle \varphi \rangle \mathrm{Int}(\mathfrak{S}_6)$ avec $\varphi \in \mathrm{Aut}(\mathfrak{S}_6) \setminus \mathrm{Int}$, $\varphi^2 = id$) DVP

· $\mathrm{Int}(\mathfrak{S}_3) \simeq \mathrm{Aut}(\mathfrak{S}_3)$

· $\mathrm{Int}(G) = \{id\}$ si G est commutatif

Prop: Soit G un groupe et H un sous-groupe de G. Alors le normalisateur de H est le plus grand sous-groupe de G dans lequel H est distingué. On le note $N_G(H)$

Ex:
- Si H est distingué, $N_G(H) = G$
- $N_{O_3}(\langle s\rangle) = \langle s\rangle$
- $N_{\mathfrak{S}_4}(A_3) = \mathfrak{S}_3$

Les sous-groupes caractéristiques

Déf: Soit G un groupe et H un sous-groupe de G. H est un sous-groupe caractéristique si il est stable par les automorphismes de G.
$\forall \varphi \in Aut(G) \quad \varphi(H) \subset H$.

Prop: Si H est caractéristique, il est distingué.
Ex: $\mathbb{Z}/2\mathbb{Z} \times \{0\}$ est distingué, mais non caractéristique dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Prop: Soit G un groupe et H un sous-groupe de G et K un sous-groupe de H.
Si $K \triangleleft_{car} H \triangleleft G$ alors $K \triangleleft G$

Déf: Soit G un groupe.
$Z(G) = \{g \in G \ / \ \forall h \in G \quad gh = hg\}$ est le centre de G

Ex:
- $Z(\mathfrak{S}_3) = \{id\}$
- $Z(G) = G$ si G est commutatif
- $Z(SO_n(\mathbb{R})) = \{\lambda I_n \ / \ \lambda \in \mathbb{R}\}$

Déf: Soit G un groupe. Le groupe dérivée de G, $\mathcal{D}(G)$, est le sous-groupe de G engendré par les commutateurs.

Ex:
- $\mathcal{D}(O_3(\mathbb{R})) = SO_3(\mathbb{R})$
- $\mathcal{D}(Q_8) = \{1; -1\}$

$Z(G)$ et $\mathcal{D}(G)$ sont des sous-groupes caractéristiques de G.

Déf: Soit G un groupe. $G/\mathcal{D}(G)$ est l'abélianisé de G. C'est le plus grand quotient abélien de G : $\mathcal{D}(G) < H \iff H \triangleleft G$ et G/H abélien

Ex: $Q_8/\mathcal{D}(Q_8) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (groupe de Klein).

Appli: Soit G un groupe. G est résoluble si et seulement si il existe une suite de sous-groupe de G (H_i) vérifiant $G = H_0 \supset H_1 \dots \supset H_n = \{e\}$ avec :
$H_i \triangleleft G$ et H_i/H_{i+1} est abélien.

Ex: $\mathfrak{S}_4$ est résoluble.

III Les théorèmes d'isomorphismes : Comment manipuler les groupes distingués et les groupes quotients

1 Le premier théorème d'isomorphisme.

Théorème: Soit G un groupe et φ un morphisme du groupe G dans un autre groupe G'. Alors :

$$G/\ker\varphi \cong Im\,\varphi.$$

En particulier si G est fini : $|G| = |Ker\varphi| \cdot |Im\varphi|$.

Ex: $Int(G) \cong G/Z(G)$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & Im\,\varphi \\ G/\ker\varphi \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

On a la factorisation $\varphi = \bar{\varphi} \circ \pi$ avec :
- $\bar{\varphi}$ injective
- π surjective

Réf: Felix Ulmer
Théorie des groupes

VP

Réf: Felix Ulmer
Théorie des groupes

(2) Deuxième théorème d'isomorphisme

Théorème : Soit G un groupe, H et K deux sous-groupes de G avec $K \subset N_G(H)$. Alors $HK = KH$ est un sous-groupe de G, $H \lhd HK \lhd G$, $K \cap H \lhd$ et :

$$KH/H \simeq K/K\cap H$$

Appli : Théorème de Sylow : Soit G un groupe d'ordre $p^a m$ avec p premier et $p \nmid m$. Si n_p désigne le nombre de p-Sylow de G on a :

- Les p-Sylow sont tous conjugués
- $n_p \equiv 1[p]$ et $n_p | m$

Le théorème de Sylow permet de trouver des sous groupes distingués : Un groupe d'ordre $3 \times 5 \times 17$ a un unique 17-Sylow

(3) Troisième théorème d'isomorphisme

Théorème : Soit G un groupe, K et H deux sous-groupes distingués de G tels que $K \supset H$.

Alors $$\left(G/H\right) / \left(K/H\right) \simeq G/K$$

Ex : • $\left(\mathbb{Z}/10\mathbb{Z}\right) / \left(2\mathbb{Z}/10\mathbb{Z}\right) \simeq \mathbb{Z}/2\mathbb{Z}$

• $\left(\mathfrak{S}_4/V\right) / \left(A_4/V\right) \simeq \mathbb{Z}/2\mathbb{Z}$ (V : groupe de Klein)

(IV) À quoi servent-ils ?

ne pas écrire mais le dire

▷ ~~Passer au quotient~~ permet de rendre les choses intrinsèques en ne ~~considérant les objets qu'au travers de leurs propriétés communes~~.

Ex : O le sous-groupe de $\mathcal{L}^p(I)$ ($p \in [1;+\infty]$, I un intervalle de $\mathbb{R}$) constitué des fonctions nulles presque partout. $\mathcal{L}^p(I)/O = L^p(I)$

▷ Rendre la structure d'un groupe plus explicite en la décomposant.

Ex : $D_n = \langle e^{in\cdot}, \overline{\cdot} \rangle$

▷ Modéliser plus facilement certaines propriétés ou étendre un groupe.

Ex : construire $PSL_n(\mathbb{R})$ en travaillant dans $\mathbb{R}^{n+1}$. On étend les fonctions affines.

▷ Mettre en évidence des propriétés de certains objets, souvent algébriques ou géométriques. On les "code" dans le langage des groupes.

Ex : Le groupe des isométries d'une figure code sa régularité.

Application : **le groupe des** isométries d'un triangle admet un sous groupe distingué non trivial si et seulement si le triangle est équilatéral.

Développement : Simplicité de $SO_3(\mathbb{R})$
Binome : Léo Bigorgne et Joackim Bernier
Référence : Philippe Caldero et Jérôme Germoni, *Histoires hédonistes de groupes et de géométries* page 237
Prérequis :

— Réduction de $O_n(\mathbb{R})$: Si $M \in O_n(\mathbb{R})$ alors il existe $P \in O_n\mathbb{R}$ tel que $P^{-1}MP$ soit diagonale par blocs, chacun des blocs étant d'une des trois formes suivantes : $-1, 1, \begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$ pour $\theta \in \mathbb{R}$.
— corollaire : $SO_n(\mathbb{R})$ est connexe par arcs.
— $SO_n(\mathbb{R})$ est compact.
— Si $M \in O_n(\mathbb{R})$ stabilise un sous espace H alors il stabilise aussi son orthogonal.
— $O_n(\mathbb{R})$ est engendré par les reflexions.
— Le centre de $SO_n(\mathbb{R})$ ne contient que des matrices scalaires.

Idée des preuves :

— Par récurrence totale sur la dimension à initialiser pour $n = 2$. Puis montrer qu'il existe soit un plan soit une droite stable.
— Par récurrence sur la dimension. On prend $x \neq u(x)$ on compose à gauche par la réflexion d'hyperplan $(x - u(x))^\perp$.
— Un endomorphime qui commute avec un autre laisse stable ses sous espaces propres.

La démonstration :

— **Définition : Retournement orthogonal** élément de $SO_n(\mathbb{R})$ dont la réduction ne contient que des 1 et deux -1.
— **Étape 1 : Pour $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les retournements orthogononaux.** Si $u \in SO_n(\mathbb{R})$ alors $u = \prod_{i=1}^{2k} R_{H_i}$. On montre donc qu'un produit de deux réflexions R_H et $R_{H'}$ et un produit de deux retournements orthogononaux.
Soit F un sous espace de dimension 1 dans $H \cap H'$, on pose alors :

$$\begin{cases} r|F = -I_1, \\ r|F^\perp = R_H|F^\perp, \\ r'|F = -I_1, \\ r'|F^\perp = R_{H'}|F^\perp. \end{cases}$$

r est un retournement car $r|F^\perp$ est une réflexion.
Attention dans la référence il y a une erreur.
— Soit H un sous groupe distingué non trivial de $SO_3(\mathbb{R})$.
— **Étape 2 : Si H contient un retournement, il les contient tous.** Soit $r_D \in H$ un retournement d'axe D. Soit D' une autre droite. Alors il existe $s \in SO_3(\mathbb{R})$ envoyant D sur D'. Alors $r_{D'} = srs^{-1} \in H$.
— **Étape 3 : H contient au moins un retournement.**
Soit $h \in H$ non trivial. On pose alors : $\begin{array}{cccc} \phi & : & SO_3(\mathbb{R}) & \to & \mathbb{R} \\ & & g & \mapsto & tr(ghg^{-1}h^{-1}) \end{array}$ Si $g \in SO_3(\mathbb{R})$ alors $ghg^{-1}h^{-1} \in H$ puisque H est distingué. Si θ est l'angle associé au bloc de taille deux de $ghg^{-1}h^{-1}$ alors $\phi(g) = 1 + 2cos(\theta) \leq 3$ et il y a égalité pour $g = h$.
Puisque $SO_3(\mathbb{R})$ *est connexe* et ϕ est continue alors $\phi(SO_3(\mathbb{R})) := [a; 3]$.
Par l'absurde si a=3 alors, pour tout $g \in SO_3(\mathbb{R})$, $tr(ghg^{-1}h^{-1}) = 3$, donc $ghg^{-1}h^{-1} = I_3$ $(\theta = 0)$. Mais alors $h = I_3$ ce qui est exclu.
Donc $a < 3$, donc il existe $n \in \mathbb{N}$ tel que $a < 1 + 2cos(\frac{\pi}{n}) < 3$. Soit g l'antécédent d'un tel élément, alors $ghg^{-1}h^{-1}$ est une rotation d'angle $\frac{\pi}{n}$. Ainsi, $(ghg^{-1}h^{-1})^n$ est un retournement qui est dans H.

Théorème de Sylow

Joackim Bernier et Léo Bigorgne

15 septembre 2014

Soit G un groupe fini d'ordre $p^a m$ avec $p \nmid m$.

Théorème 0.1 *Tous les p-Sylow de G sont conjugués et si n_p désigne leur nombre on a*

$$n_p \equiv 1[p]$$

$$n_p \mid m$$

Démonstration 0.1 *Soit P et H deux p-Slylow de G. On fait agir G par conjugaison sur ses p-Sylow. Notons n le nombre de conjugués de P et $\omega(P)$ son orbite sous l'action de G. H en tant que sous groupe de G agit par restriction et si L désigne un p-Sylow de G on note $\omega_H(L)$ son orbite pour l'action restreinte à H. $\omega(P)$ se partitionne en k sous orbites pour l'action de H sur $\omega(P)$.*

On a la relation

$$n = \sum_{i=1}^{k} |\omega_H(P_i)|$$

Où P_i est un représentant de la i-ème sous orbite.

On a pour tout $i \in \{1; ...; k\}$, $|\omega_H(P_i)| \mid |H|$ donc $|\omega_H(P_i)| = 1$ ou $p \mid |\omega_H(P_i)|$.

Si $|\omega_H(P_i)| = 1$ alors $P_i = H$. En effet dans ce cas $H \subset N(P_i)$ donc HP_i est un sous groupe de G dans lequel P_i est distingué. Donc, par le deuxième théoréme d'isomorphisme on a

$$HP_i/P_i \simeq H/H \cap P_i$$

Et HP_i est un p-groupe et donc par maximalité de H et P_i on a $H = HP_i = P_i$.

Si on applique ce résultat à $H = P$ on obtient

$$n \equiv 1[p]$$

Si H est quelconque on déduit de ce qui précède qu'il existe i tel que $p \nmid |\omega_H(P_i)|$. Alors $H = P_i$ et H et P sont conjugés. On en déduit $n = n_p$.

De plus $n \mid |G|$ et $n \wedge p^a = 1$ donc par le théorème de Gauss :

$$n \mid m$$

Références

[1] Felix Ulmer, Théorie des groupes.

Automorphismes de Σ_6

Joackim Bernier et Léo Bigorgne

16 septembre 2014

Théorème 0.1 $\exists \varphi \in \mathfrak{S}_6 \setminus Int(\mathfrak{S}_6), \varphi^2 = id$ *et*

$$Aut(\mathfrak{S}_6) =< \varphi > Int(\mathfrak{S}_6)$$

On utilisera dans la démonstration les résultats suivants :

Si un automorphisme de $\mathfrak{S}_6$ envoie une transposition sur une transposition, il est intérieur.

A_6 est simple.

Démonstration 0.1 *Montrons tout d'abord que $\mathfrak{S}_6$ contient un sous-groupe d'indice 6 ne stabilisant aucun point de $\{1; ...; 6\}$.*

$PGL(2;5)$ agit transitivement sur $\mathbb{P}^1(\mathbb{F}_5)$ (qui a 6 éléments). D'où une injection de $PGL(2;5)$ (de cardinal 120) dans $\mathfrak{S}_6$ dont l'image est un sous-groupe d'indice 6 de $\mathfrak{S}_6$ agissant transitivement sur $\{1; ...; 6\}$.

Construisons maintenant un automorphisme non intérieur de $\mathfrak{S}_6$.

L'action de $\mathfrak{S}_6$ par translation à gauche sur $\mathfrak{S}_6/_N$ (de cardinal 6) donne un morphisme de groupe

$$\varphi : \mathfrak{S}_6 \to \mathfrak{S}_6$$

C'est un isomorphisme car son noyau est inclus dans N (le stabilisateur de la classe N) et comme le seul sous-groupe distingué non trivial de $\mathfrak{S}_6$ est A_6, de cardinal 360, on en déduit que $Ker(\varphi) = \{id\}$. Si dans la bijection entre $\{1; ...; 6\}$ et $\mathfrak{S}_6/_N$ on associe la classe de N à 6 alors $\varphi(N)$ laisse stable 6. Par conséquent, φ ne peut être intérieur. En effet si $\varphi = \sigma.\sigma^{-1}$ on a pour tout $\gamma \in N$, $\sigma\gamma\sigma^{-1}(6) = 6$ et donc

$$\gamma(\sigma^{-1}(6)) = \sigma^{-1}(6)$$

Ce qui est impossible car N agissant transitivement sur $\{1; ...; 6\}$ ne peut laisser stable $\sigma^{-1}(6)$. Ainsi φ est un automorphisme non intérieur de $\mathfrak{S}_6$. Montrons maintenant que $Int(\mathfrak{S}_6)$ est d'indice 2 dans $Aut(\mathfrak{S}_6)$.

Tout d'abord si $\phi \in \mathfrak{S}_6 \setminus Int(\mathfrak{S}_6)$, ϕ envoie une transposition sur une triple transposition (et réciproquement). En effet, soit $\tau \in \mathfrak{S}_6$ une transposition. Alors $\phi(\tau)$ est d'ordre 2 et est donc une transposition simple, double ou triple. Comme φ est un isomorphisme

$\varphi(A_6)$ *est un sous-groupe distingué non trivial et est donc* A_6*. Par conséquent* $\varphi(\tau)$ *ne peut être une double transposition. Si toute transposition était envoyé sur une transposition,* ϕ *serait intérieur donc il existe* τ *un transposition telle que* $\phi(\tau)$ *soit une triple transposition. Si* γ *est une transposition,* γ *et* τ *sont conjuguées, donc* $\phi(\gamma)$ *et* $\phi(\tau)$ *aussi. Par conséquent* $\phi(\gamma)$ *et* $\phi(\tau)$ *ont même type et* $\phi(\gamma)$ *est aussi une triple transposition.*

Soit ϕ *et* $\psi \in \mathfrak{S}_6 \setminus Int(\mathfrak{S}_6)$ *et* τ *une transposition.* $\psi(\tau)$ *est une triple transposition donc* $\phi^{-1}(\psi(\tau))$ *est une transposition et* $\phi^{-1}\psi \in Int(\mathfrak{S}_6)$*. Et* $Int(\mathfrak{S}_6)$ *est d'indice 2 dans* $Aut(\mathfrak{S}_6)$*.*

Il nous reste maintenant à montrer qu'il existe $\varphi \in \mathfrak{S}_6 \setminus Int(\mathfrak{S}_6)$ *d'ordre* 2.

Soit $\varphi \in \mathfrak{S}_6 \setminus Int(\mathfrak{S}_6)$*. Quitte à composer à gauche par un automorphisme intérieur bien choisi on peut supposer que* $\varphi(12345) = (12345)$ *car* $\varphi(12345)$ *est un 5-cycle (il est d'ordre 5) et tous les 5-cycles sont conjugués. On a de plus* $\varphi^2 \in Int(\mathfrak{S}_6)$ *donc* $\exists \sigma \in \mathfrak{S}_6$, $\varphi^2 = int_\sigma$ *et* σ *commute avec* (12345)*, dont le commutant est* $< (12345) >$ *donc* $\sigma = (12345)^k$ *et* φ^5 *convient.*

Références

[1] Daniel Perrin, cours d'algèbre.