Leçon 103: Exemples et applications des notions de sous-groupes distingués et de groupe quotient

Adrien Fontaine

21 décembre 2013

Table des matières

Cadre : Dans toute la leçon, $(G, ., e)$ désigne un groupe et H un sous-groupe de G.

1 Introduction

Le passage au quotient est une notion majeure en mathématiques. Sa vocation est de regrouper des éléments ayant la même propriété et de changer d'espace pour ne plus les distinguer. Ainsi, des espaces aussi usuels que l'anneau $\mathbb{Z}/n\mathbb{Z}$, les espaces L^p ou le groupe $\mathbb{R}/2\pi\mathbb{Z}$ reposent sur cette construction. Dès lors, en théorie des groupes, la notion de sous-groupe distingué est centrale pour "passer au quotient".

2 Généralités

2.1 Notion de classe

Définition 1

On appelle classe à gauche de l'élément $a \in G$ relativement à H, le sous-ensemble

$$aH = \{g \in G / g = ah, h \in H\}$$

et on définit de même les classes à droite Ha.
Les classes à gauche forment une partition de G. Leur ensemble est noté G/H.

Remarque 1

Attention ! G/H n'est pas un groupe en général !

Définition 2

On définit l'indice de H dans G, et on note $(G : H)$ comme le cardinal de G/H, i.e

$$(G : H) = \mid G/H \mid$$

Lorsque le groupe est fini, la considération des classes à gauche conduit au théorème suivant :

Théorème 1 (*Lagrange*)

Si G est fini, l'ordre de H et l'indice de H dans G divisent l'ordre de G. Précisément, on a :

$$\mid G \mid = \mid H \mid \times \mid G/H \mid = \mid H \mid \times (G : H)$$

En particulier, l'ordre d'un élément $g \in G$ divise l'ordre de G.

2.2 Sous-groupes distingués

Définition 3

On dit que H est distingué dans G, et on note $H \triangleright G$, si on a :

$$\forall a \in G, \forall h \in H, aha^{-1} \in H$$

Exemple 1

1. *$\{e\}$ et G sont toujours des sous-groupes distingués, dits triviaux.*
2. *Dans un groupe abélien, tout sous-groupe est distingué.* [1]
3. *Si $f : G \to G'$ est un homomorphisme de groupe, son noyau $Ker(f)$ est un sous-groupe distingué de G.*
4. *L'ensemble des automorphismes intérieurs de G ($Int(G)$) est distingué dans l'ensemble des automorphisme de G.*
   $Int(G)$ est l'ensemble des automorphismes de G de la forme :
   $$\begin{array}{rccc} \sigma_g & : & G & \to & G \\ & & x & \mapsto & gxg^{-1} \end{array}$$
   et on vérifie facilement que pour tout $\alpha \in Aut(G)$, on a $\alpha \circ \sigma_g \circ \alpha = \sigma_{\alpha(g)}$.
5. *contre-exemple : $Gl_n(\mathbb{Z}) \not\triangleright GL_n(\mathbb{R})$. En effet, le contre-exemple suivant s'étend à toutes les tailles :*
   $$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} = \begin{bmatrix} 1 & 1/2 \\ 0 & 1 \end{bmatrix} \notin GL_2(\mathbb{Z})$$

Remarque 2

Pour montrer qu'un sous-groupe est distingué, il suffit de montrer $xhx^{-1} \in H$ seulement sur une partie génératrice de H.

Proposition 1

On a équivalence entre :

1. *$H \triangleleft G$*
2. *$\forall g \in G, gH = Hg$*

Application : Tout sous-groupe d'indice 2 est distingué.
En effet, si H est un sous-groupe d'indice 2 de G. Soit $a \in G$. Si $a \in H$, on a $Ha = H = aH$. Si $a \notin H$, alors H étant d'indice 2, la partition de G en classes à gauches (resp. à droite) est $G = H \cup aH$ (resp. $G = h \cup Ha$). On a donc $Ha = H^c = aH$. Donc, H est distingué dans G.

Théorème 2 (*Froebenius*)

[2] *Si G est fini. Soit p le plus petit diviseur premier de $|\ G\ |$. Alors tout sous groupe de G d'indice p est distingué dans G.*

Démonstration : Soit H un sous-groupe d'indice p de G. Considérons l'ensemble G/H des classes à gauche de G suivant H. Sur cet ensemble à p éléments, H agit par translation :

$$\begin{array}{ccc} H \times G/H & \to & G/H \\ (h, gH) & \mapsto & (hg)H \end{array}$$

avec au moins un point fixe, la classe $eH = H$. L'orbite de tout point non fixe a pour cardinal un diviseur de l'ordre de H strictement supérieur à 1 ($|\ \omega(gH)\ ||\ Stab(gH)\ |=|\ H\ |$), donc supérieur ou égal à p (on peut pas avoir un diviseur de $|\ H\ |$plus petit que p car sinon ça serait aussi un diviseur de $|\ G\ |$. Ce qui est incompatible avec ce qui précède (car $G/H = \bigcup_{g \in G} \omega(gH)$). Ainsi, tous les points sont fixes donc $\forall g \in G, \forall h \in H, hgH = gH$, *i.e* $g^{-1}hg \in H$. ■

2.3 Groupes quotients

On cherche les relations d'équivalence $\mathcal{R}$ sur G telles que $G/\mathcal{R}$ soit un groupe. On dispose alors du résultat suivant :

Proposition 2

Si $H \triangleleft G$, l'ensemble G/H peut être muni d'une structure de groupe via $(xH)(x'H) = (xx')H$ et est appelé groupe quotient de G par H.
De plus, on dispose d'un morphisme de groupe surjectif

$$\begin{array}{rccc} \Pi & : & G & \to & G/H \\ & & x & \mapsto & xH \end{array}$$

de noyau H.

Remarque 3

On a donc une réciproque à l'exemple 3 de sous-groupe distingué.

Exemple 2

1. *$SL_n(\mathbb{K}) \triangleleft GL_n(\mathbb{K})$ car $SL_n(\mathbb{K}) = Ker(det)$*
2. *$A_n \triangleleft S_n$ car $A_n = Ker(\varepsilon)$ où ε est la signature d'une permutation.*

3

2.4 Théorèmes d'isomorphismes

Dans ce paragraphe, on suppose $H \triangleleft G$. [4]

Théorème 3 (*Propriété universelle du groupe quotient*)

Soit Γ un groupe et $\varphi : G \to \Gamma$ un morphisme de groupe tel que $H \subset Ker(\varphi)$. Alors, il existe un unique $\tilde{\varphi} G/H \to \Gamma$ tel que $\varphi = \tilde{\varphi} \circ \pi$.

Corollaire 1 (*Premier théorème d'isomorphisme*)

Avec les mêmes notations, $G/Ker(\varphi) \simeq Im(\varphi)$.

5

Proposition 3 (*Deuxième théorème d'isomorphisme*)

[6] *Soit $H \triangleleft G$ et K un sous-groupe de G. Alors, les groupes quotients $K/K \cap H$ et HK/H existent et on a $K/K \cap H \simeq HK/H$.*

Proposition 4 (*Deuxième théorème d'isomorphisme*)

Soit K un sous-groupe de G tel que $K \subset H$, $K \triangleleft G$, $H \triangleleft G$. Alors,

$$G/H \simeq (G/K)/(H/K)$$

3. mettre les deux propriétés du plan de Alex et Lison
4. besoin du calais p147
5. mettre des exemples d'application, peut être dans OA

3 Groupes et sous-groupes remarquables

3.1 Groupes simples

Définition 4

Si $G \neq \{e\}$, on dit que G si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Exemple 3

1. *$\mathbb{Z}/p\mathbb{Z}$ est simple, si et seulement si, p est premier.*[7]
2. DÉVELOPPEMENT *$\mathfrak{A}_n$ est simple pour $n \geq 5$ [2]*

On utilise pour démontrer ce résultat, quelques propriétés des p-sous-groupes de Sylow, notamment le fait qu'ils soient tous conjugués entre eux. Ce théorème et bien d'autres seront rappelés dans la partie 4 de cette leçon qui y est consacrée.
On aura besoin dans la démonstration du résultat suivant :

Proposition 5

Les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$.

Démonstration : Ceci découle du résultat suivant :

Lemme 1

Soient $n \geq 3$, $(a_1, ..., a_{n-2}) \in \{1, ..., n\}$ deux à deux distincts, et $(b_1, ..., b_{n-2}) \in \{1, ..., n\}$ deux à deux distincts. Alors il existe $\sigma \in \mathfrak{A}_n$ telle que

$$\forall i \in \{1, ..., n-2\}, \sigma(a_i) = b_i$$

Démonstration : Soit $(a_{n-1}, a_n) \in \{1, ..., n\}$ et $(b_{n-1}, b_n) \in \{1, ..., n\}$ tels que $\{a_1, ..., a_n\} = \{1, ..., n\}$ et $\{b_1, ..., b_n\} = \{1, ..., n\}$. On considère alors $\sigma \in \mathfrak{S}_n$ tel que $\forall i \in \{1, ..., n\}, \sigma(a_i) = b_i$. Si, $\varepsilon(\sigma) = 1$ alors c'est terminé. Sinon, on compose σ par (a_{n-1}, a_n) (ce qui ne change pas les images des $(a_i)_{1 \leq i \leq n-2}$ mais multiplie la signature par -1). ■

On a également besoin de la proposition suivante :

Proposition 6

Si $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre p, $\sigma = (a_1...a_p)$ et si $\tau \in \mathfrak{S}_n$, on a :

$$\tau\sigma\tau^{-1} = (\tau(a_1)...\tau(a_p))$$

Démonstration : Si $x \notin \{\tau(a_1), ..., \tau(a_p)\}$, $\tau^{-1}(x) \notin \{a_1, ..., a_p\}$ et donc :

$$\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$$

Et si $x = \tau(a_i)$, $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$, d'où,

$$\tau\sigma\tau^{-1} = (\tau(a_1)...\tau(a_p))$$

■

On peut maintenant montrer que les $3-cycles$ sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$. Soient $\rho = (a_1a_2a_3)$ et $\tau = (b_1b_2b_3)$ deux 3-cycles dans $\mathfrak{A}_n$. Comme $n - 2 \geq 3$, il existe une permutation $\sigma \in \mathfrak{A}_n$ telle que $\forall 1 \leq i \leq 3, \sigma(a_i) = b_i$, et donc $\tau = \sigma\rho\sigma^{-1}$ d'après la proposition. ■

Enfin, on utilise également le résultat suivant :

Proposition 7

Les cycles d'ordre 3 engendrent $\mathfrak{A}_n$ pour $n \geq 3$

Démonstration : En effet, $\mathfrak{A}_n$ est engendré par les produits pairs de transpositions et on a les formules :

$$(a,b)(b,c) = (a,b,c)$$
$$(a,b)(a,c) = (a,c,b)$$
$$(a,b)(c,d) = (a,b)(a,c)(a,c)(c,d) = (a,c,b)(a,c,d)$$

■

On est maintenant en mesure de démontrer le théorème :

Théorème 4

Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

Démonstration : La démonstration se fait en 2 étapes. D'abord pour $n = 5$ puis pour $n > 5$ par réduction au cas $n = 5$.

1. Le théorème pour n=5
   Décrivons les éléments de $\mathfrak{A}_5$:
   - Tout d'abord il y a le neutre, soit 1 élément.
   - Ensuite il y a les éléments d'ordre 3, ce sont les 3-cycles. Pour déterminer un 3-cycle, il faut choisir les deux points fixes, ce qui nous fait $\binom{2}{5} = 10$ possibilités, puis on détermine l'image des 3 points qui ne sont pas fixes par la permutation. Or une fois fixée l'image d'un élément, les images des deux autres sont automatiquement déterminées. On a donc deux possibilités pour les images des points du 3-cycle qui ne sont pas fixes. Soit au total, $10 \times 2 = 20$ 3-cycles.
   - Ensuite il y a les éléments d'ordre 5, ce sont les 5-cycles. Cette fois-ci, il n'y a pas de point fixe et il suffit de déterminer les images des points de la permutation. Pour 1, on a 4 possibilités $(2, 3, 4, 5)$ puis pour 2, on a 3 possibilités (tout sauf 2 lui même et l'image de 1 qui est déjà prise, et ainsi de suite. Au total, on a donc $4 \times 3 \times 2 = 24$ 5-cycles
   - Enfin, on a les produits de deux transpositions à supports disjoints. Ce sont les éléments d'ordre 2. Pour déterminer, une telle permutation, il faut se donner un point fixe (5 possibilités) et un choix de 2 éléments parmi les 4 restants qui correspondent à une des deux permutations (l'autre étant alors automatiquement déterminée), soit $\binom{2}{4} = 6$ possibilités. Mais attention, en procédant ainsi, on compte deux fois certains éléments : en effet, si on choisit par exemple 1 et 2 dans $\{1, 2, 3, 4\}$ et qu'ensuite on choisit 3 et 4, on considère en fait la même permutation qui est : $(12)(34) = (34)(12)$. Il faut donc penser à diviser par 2 pour obtenir le nombre de permutations d'ordre 2. Finalement, on a donc $5 \times 6/2 = 15$ possibilités.

   On a donc dénombrer $1 + 20 + 24 + 15 = 60$ éléments de $\mathfrak{A}_5$ et $| \mathfrak{A}_5 | = 60$ donc on a bien décrit tous les éléments de $\mathfrak{A}_5$.
   De plus, les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_5$ d'après la proposition 5. Les éléments d'ordre 2 le sont aussi : si $\tau = (ab)(cd)(e)$ et $\tau' = (a'b')(c'd')(e')$, il existe $\sigma \in \mathfrak{A}_5$ tel que

$\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ d'après le lemme 1. Alors :

$$\begin{aligned}\sigma\tau\sigma^{-1} &= \sigma(ab)(cd)(e)\sigma^{-1}\\ &= \sigma(ab)\sigma^{-1}\sigma(cd)\sigma^{-1}\sigma(e)\sigma^{-1}\\ &= (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))(\sigma(e))\\ &= (a'b')(\sigma(c)\sigma(d))(e')\\ &= (a'b')(c'd')(e')\\ &= \tau'\end{aligned}$$

Soit alors $H \triangleleft \mathfrak{A}_5$, $H \neq \{1\}$. Si H contient un élément d'ordre 3 (resp. 2), alors H étant distingué, il les contient tous puisqu'ils sont tous conjugués. Si il contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc tous les 5-sous-groupes de Sylow puisqu'ils sont tous conjugués, donc H contient tous les éléments d'ordre 5.
Mais H ne peut contenir un seul des trois types d'éléments précédents (en plus du neutre) car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ divisent 60 (le cardinale de H divise $\mid \mathfrak{A}_5 \mid = 60$ d'après le théorème de Lagrange 1). Donc, H contient au moins un des trois types, d'où $\mid H \mid \geq 15 + 20 + 1 = 36$. D'où, $\mid H \mid = 60$ et $H = \mathfrak{A}_5$.

2. Le théorème pour $n > 5$
Posons $E = \{1, ..., n\}$. Soit $H \triangleleft \mathfrak{A}_n$, $H \neq 1$ et soit $\sigma \in H, \sigma \neq 1$. On va se ramener au cas $n = 5$ et, pour ceci fabriquer à partir de σ, un élément non trivial de H, qui n'agisse en fait, que sur un ensemble à 5 éléments, donc qui ait $n - 5$ points fixes.
Comme $\sigma \neq 1$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$, et soit τ le 3-cycle $\tau = (a, c, b)$, de sorte que $\tau^{-1} = (a, b, c)$ et soit $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. On a :

$$\rho = \underbrace{(\tau\sigma\tau^{-1})}_{\in H}\sigma^{-1} \in H$$

Et $\rho = (a, c, b)(\sigma(a), \sigma(b), \sigma(c))$.
Comme $b = \sigma(a)$, l'ensemble $F = \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et on a $\rho(F) = F$ et $\rho_{|E\setminus F} = Id_{E\setminus F}$.
Quitte à rajouter des éléments à F, on peut supposer $\mid F \mid = 5$. Enfin, $\rho \neq 1$ car $\rho(b) = \tau(\sigma(b)) \neq b$ car $\sigma(b) \neq \tau^{-1}(b) = c$.
Soit alors $\mathfrak{A}(F)$ l'ensemble des permutations paires de F. $\mathfrak{A}(F)$ est isomorphe à $\mathfrak{A}_5$ et $\mathfrak{A}(F)$ se plonge dans $\mathfrak{A}_n$ par :

$$\begin{array}{rccc}\Phi & : & \mathfrak{A}(F) & \to & \mathfrak{A}_n\\ & & u & \mapsto & \bar{u}\end{array}$$

où $\bar{u}_{|F} = u$ et $\bar{u}_{|E\setminus F} = Id_{E\setminus F}$.
Posons, $H_0 = \{u \in \mathfrak{A}(F)/\bar{u} \in H\} = H \cap \mathfrak{A}(F)$.
Il est clair que $H_0 \triangleleft \mathfrak{A}(F)$ et on a $\rho_{|F} \in H_0$ et $\rho_{|F} \neq Id_F$. Comme $\mathfrak{A}(F) \cong \mathfrak{A}_5$ est simple, on a $H_0 = \mathfrak{A}(F)$. Ainsi, si u est un cycle d'ordre 3 de $\mathfrak{A}(F)$, $\bar{u} \in H$ et $\bar{u}$ est encore un cycle d'ordre 3. Mais comme les 3 cycles sont tous conjugués dans $\mathfrak{A}_n$, H contient tous les 3-cycles, et comme ils engendrent $\mathfrak{A}_n$, on a $H = \mathfrak{A}_n$.
Ce qui achève la démonstration. ■

Citons enfin d'autres exemples de groupes simples :

Exemple 4

1. *$SO_3(\mathbb{R})$ est simple*
2. *$PSO_n(\mathbb{R})$ est simple pour $n \geq 5$*

Application :
Soit $f : G \to \Gamma$ un morphisme. Si G est simple, $Ker(f)$ étant un sous-groupe distingué de G, on a $Ker(f) = \{e\}$ ou $Ker(f) = G$, c'est à dire, f est injectif ou trivial.

Proposition 8

Les seuls groupes simples abéliens sont les groupes cycliques d'ordre premier. [8]

Démonstration : Un groupe cyclique est abélien. De plus, si son ordre est premier, alors il n'a pas d'autres sous-groupes que $\{e\}$ et G, donc il est nécessairement simple.
Réciproquement, supposons que G soit un groupe abélien simple. Cette hypothèse implique $G \neq \{e\}$ donc il existe $x \neq e$ dans G. Le sous-groupe $< x >$ étant distingué dans le groupe abélien G, nécessairement $< x >= G$. Le groupe G est donc monogène et puisqu'il est simple, il ne peut être que cyclique d'ordre premier. ■

3.2 Groupe dérivé d'un groupe

Définition 5

Le groupe dérivé $D(G)$ est le sous-groupe engendré par les commutateurs de G, i.e *les éléments de la forme $[x, y] = xyx^{-1}y^{-1}$ avec $x, y \in G$.*

Remarque 4

G est abélien $\Leftrightarrow D(G) = \{e\}$

Application :

1. $D(G)$ est distingué dans G
2. $D(S_n) = A_n$ pour $n \geq 2$
3. $D(GL_n(\mathbb{K}) = SL_n(\mathbb{K})$ pour tout $n \geq 2$ et pour tout corps $\mathbb{K}$ ayant au moins 3 éléments. En effet, notons tout d'abord que pour tout $(A, B) \in GL_n(\mathbb{K})^2$, on a $det([A, B]) = 1$ par multiplicativité du déterminant. Le groupe dérivé de $GL_n(\mathbb{K})$ est donc inclus dans $SL_n(\mathbb{K})$. Or, $SL_n(\mathbb{K})$ est engendré par les matrices de transvections [9]. On va donc essayer de voir si toute matrice de transvection est un commutateur (puisque le groupe dérivé est le plus petit groupe contenant les commutateurs, si on arrive à montrer que les transvections sont des commutateurs, alors le groupe dérivé contient le groupe engendré par les transvections *i.e* $SL_n(\mathbb{K})$. Pour $i \neq j$, on pose $T_{i,j}(\lambda) = I_n + E_{i,j}$. On a alors $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$. Calculons le commutateur défini par une matrice de dilatation $D_i(a)$ avec $a \notin \{0, 1\}$ (il en existe car $\mathbb{K}$ contient au moins 3 éléments) et une matrice de transvection $T_{i,j}(b) = I_n + bE_{i,j}$. On a :

$$D_i(a)(I_n + bE_{i,j})D_i(a)^{-1} = I_n + D_i(a)bE_{i,j}D_i(a)^{-1} = I_n + abE_{i,j} = T_{i,j}(ab)$$

et donc,

$$D_i(a)T_{i,j}(b)D_i(a)^{-1}T_{i,j}(b)^{-1} = T_{i,j}(ab)T_{i,j}(-b) = T_{i,j}((a-1)b)$$

Lorsque b varie dans $\mathbb{K}$, la scalaire $(a-1)b$ décrit aussi $\mathbb{K}$. Donc, toute matrice de transvection est un commutateur. Par suite, le groupe engendré par les commutateurs de $GL_n(\mathbb{K})$ est égal à $SL_n(\mathbb{K})$.

Proposition 9

On a :

9. XENS 2 p165

1. $D(G) \triangleleft G$

2. si $N \triangleleft G$, alors G/N est un groupe abélien, si et seulement si, $D(G) \subset N$.

Autrement dit, $D(G)$ est le plus petit sous-groupe distingué de G tel que $G/D(G)$ soit abélien.

Démonstration : 1. Soient $x, y, z \in G$. On a :

$$z[x,y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = [zxz^{-1}, zyz^{-1}]$$

2.

$$\begin{aligned} G/N \text{ abélien} &\Leftrightarrow \forall \bar{x}, \bar{y} \in G/N, \bar{x}\bar{y} = \bar{y}\bar{x} \\ &\Leftrightarrow \forall x, y \in G, xy(yx)^{-1} \in N \\ &\Leftrightarrow \forall x, y \in G, [x,y] \in N \\ &D(G) \subset N \end{aligned}$$

■

Application : Tout morphisme de G dans un groupe abélien se factorise par $D(G)$.

3.3 Produit direct

Définition 6

Soient N et H deux groupes. Le produit direct $G = N \times H$ est le produit cartésien de N et H muni de la loi produit :

$$(n,h)(n',h') = (nn', hh')$$

On a alors une projection $p : G \to H$ définie par $p(n,h) = h$. C'est un homomorphisme de groupes, surjectif, de noyau le sous-groupe distingué $\bar{N} = \{(n,1)/n \in \mathbb{N}\}$ et on a donc une suite exacte :

$$1 \to N \xrightarrow{i} N \times H \xrightarrow{p} H \to 1$$

avec $i(n) = (n,1)$, de sorte que $N \times H$ est bien une extension de N par H. Bien entendu, ici N et H jouent des rôles symétriques et on a aussi un sous-groupe $\bar{H}$ (défini de manière symétrique) noyau de la projection sur N.

Proposition 10

Soient G un groupe et H, K deux sous-groupes. On suppose que $H \triangleleft G$, $K \triangleleft G$, $HK = G$ et $H \cap K = 1$. Alors, $f : (h,k) \mapsto hk$ est un isomorphisme de groupes de $H \times K$ sur G.

Démonstration : En utilisant le fait que $G = HK$ et $H \cap K = 1$, on montre facilement que f est une bijection de $H \times K$ sur G.

Comme H et K sont distingués, pour tout $h \in H$ et pour tout $k \in K$, on a :

$$h(h^{-1}kh) = kh = (khk^{-1})k \text{ avec } khk^{-1} \in H \text{ et } h^{-1}kh \in K$$

L'unicité de l'expression de $kh \in G = HK$ impose $h = khk^{-1}$ soit $hk = kh$ et ce pour tout $h \in H$ et $k \in K$. Pour tous $h, h' \in$ et $k, k' \in K$, on en déduit :

$$f((h,k)(h',k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h,k)f(h',k')$$

Donc, f est un homomorphisme de groupes. C'est un isomorphisme de $H \times K$ sur G. ■

Voici un exemple bien classique de produit direct :

Lemme 2 (*Lemme chinois*)

Si p et q sont des entiers premiers entre eux, on a un isomorphisme

$$\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Démonstration : Si on désigne par $\bar{n}$ (resp. $\hat{n}$, $\dot{n}$) les classes de n modulo pq (resp. p, q), on a un homomorphisme $\bar{n} \mapsto (\hat{n}, \dot{n})$ injectif car $(p, q) = 1$ et on conclut grâce à l'égalité des cardinaux. ■

Théorème 5 (*Structure des groupes abéliens finis*)

Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers q_1 supérieur ou égal à deux, q_2 multiple de q_1, ..., q_k multiple de q_{k-1}, uniques, tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times ... \times (\mathbb{Z}/q_k\mathbb{Z})$.

4 p-groupes et théorèmes de Sylow

[2] Le théorème de Lagrange affirme que si H est un sous-groupe du groupe fini G, son cardinal divise le cardinal de G. On peut se demander à l'inverse si, dans un groupe de cardinal n, il existe, pour tout diviseur d de n, un (ou plusieurs) sous-groupes d'ordre d.
Il n'en est rien en général, comme le montre l'exemple de $\mathfrak{A}_5$: on a $\mid \mathfrak{A}_5 \mid = 24$ et on voit aisément que $\mathfrak{A}_5$ n'a pas de sous-groupe d'ordre 12 (sinon, il serait d'indice 2 et donc distingué dans $\mathfrak{A}_5$ qui est simple, ce qui est absurde). Il est cependant un cas très important où la propriété est vraie, celui des sous-groupes de Sylow. Dans tout ce paragraphe, p désigne un nombre premier.

Définition 7

Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous groupe de Sylow de G un sous-groupe de cardinal p^{alpha}.

Exemple 5

Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier) et soit $G = GL_n(\mathbb{F}_p), n \in \mathbb{N}^*$. Alors G est un groupe fini de cardinal

$$\begin{aligned} \mid G \mid &= (p^n - 1)(p^n - p)...(p^n - p^{n-1}) \\ &= p^{n(n-1)/2}(p^n - 1)(p^{n-1} - 1)...(p - 1) \\ &= mp^{n(n-1)/2} \text{ avec } p \nmid m \end{aligned}$$

On exhibe alors aisément un p-sous groupe de Sylow P de G :

$$P = \{A = (a_{i,j}) / a_{i,j} = 0 \text{ pour } i > j \text{ et } a_{i,i} = 1\}$$

Lemme 3

Soit G un groupe de cardinal $\mid G \mid = p^\alpha m$ avec $p \nmid m$, et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Démonstration : Le groupe G opère sur G/S par translation à gauche :

$$\begin{array}{rccc} \Phi & : & G \times G/S & \to & G/S \\ & & (g, aS) & \mapsto & (ga)S \end{array}$$

Il est alors facile de voir que le stabilisateur de aS est le sous-groupe aSa^{-1}, conjugué de S. (attention S n'est pas nécessairement distingué, donc G/S n'est pas nécessairement un groupe, cela désigne simplement l'ensemble des classes à gauche modulo S). Mais H opère lui aussi sur G/S par restriction, avec comme stabilisateur de aS, $aSa^{-1} \cap H$.
Il reste à voir que l'un de ces groupes est un p-Sylow de H. Or, S est un p-Sylow donc aSa^{-1} aussi, donc les $aSa^{-1} \cap H$ sont des p-groupes. Il suffit donc de montrer qu'il existe $a \in G$ tel que $\mid H/(aSa^{-1} \cap H) \mid$ soit premier à p (on a $\mid H \mid = p^\beta n$ avec $\beta \leq \alpha$ et $p \nmid n$ et $\mid aSa^{-1} \cap H$ est une puissance de p).
Par ailleurs,

$$\begin{array}{rccc} \Psi & : & H/(aSa^{-1} \cap H) & \to & \omega(aS) \\ & & \bar{g} & \mapsto & g.aS \end{array}$$

où $\omega(aS)$ est l'orbite de aS sous l'action de H sur G/S est une bijection (on quotiente par la relation d'équivalence

$$\begin{aligned} g \sim g' &\Leftrightarrow g.aS = g'.aS \\ &\Leftrightarrow (gg'^{-1}).aS = aS \\ &\Leftrightarrow gg'^{-1} \in Stab(aS) \\ &\Leftrightarrow gg'^{-1} \in aSa^{-1} \cap H) \end{aligned}$$

Donc, $\mid H/(aSa^{-1} \cap H) \mid = \mid \omega(aS) \mid$.
Si tous ces nombres étaient divisibles par p, il en serait de même de $\mid G/S \mid$ car G/S est réunion des orbites $\omega(aS)$. Mais, ceci contredit le fait que S est un p-Sylow de G. D'où le résultat. ■

On est maintenant en mesure de démontrer les théorèmes de Sylow suivants :

Théorème 6

Soit G un groupe fini, de cardinal $\mid G \mid = p^\alpha m$ avec $p \nmid m$. Alors :

1. *Il existe un p-sous groupe de Sylow de G*
2. *Tous les p-Sylow de G sont conjugués entre eux*
3. *Si H est un sous groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$*

Démonstration : 1. D'après le théorème de Cayley (si G est fini de cardinal n, G est isomorphe à un sous-groupe de $\mathfrak{S}_n$), on peut plonger G dans $\mathfrak{S}_n$. On peut ensuite plonger $\mathfrak{S}_n$ dans $GL_n(\mathbb{F}_p)$ via :

$$\begin{array}{rccc} \Phi & : & \mathfrak{S}_n & \to & GL_n(\mathbb{F}_p) \\ & & \sigma & \mapsto & u_\sigma : e_i \mapsto e_{\sigma(i)} \end{array}$$

(où (e_i) est la base canonique de $\mathbb{F}_p^n$)
Finalement, on a donc réalisé G comme un sous-groupe de $GL_n(\mathbb{F}_p)$.or, $GL_n(\mathbb{F}_p)$ possède un p-Sylow comme on l'a vu dans l'exemple ci-dessus. Donc, G aussi d'après le lemme précédent.

2. On prouve 2. et 3. ensemble. Si H est un p-sous-groupe et S un p-Sylow de G, il existe d'après le lemme précédent, $a \in G$, tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. Mais comme H est un p-groupe, on a $aSa^{-1} \cap H = H$. Donc, H est inclus dans aSa^{-1} qui est un p-Sylow. Si de plus, H est un p-Sylow, on a exactement $H = aSa^{-1}$. ■

Corollaire 2

Un p-Sylow de G est unique, si et seulement si, il est distingué.

5 Résolubilité

Références

[1] Josette Calais, *Éléments de théorie des groupes*. Presses Universitaires de France, 1984.

[2] Daniel Perrin, *Cours d'algèbre*. Ellipses, 1996.

[3] Serge Francinou, Hervé Gianella, Serge Nicolas, *Exercices de mathématiques, oraux X-ENS, algèbre 2*. Cassini, 2006.

[4] François Combes, *Algèbre et géométrie*. Bréal, 2003.