103

EXEMPLES ET APPLICATIONS DES NOTIONS DE SOUS-GROUPES DISTINGUÉS ET DE GROUPES QUOTIENTS.

Notation: Notons G, G' deux groupes, de neutres e et e', H un sous-groupe de G, H' un sous-groupe de G'.

I Sous-groupes distingués et groupes quotients

1) Sous-groupes distingués [U], [P], [C], ([OA])

def: • H est dit distingué dans G, noté $H \triangleleft G$, si $\forall g \in G, \forall h \in H, ghg^{-1} \in H$

• On appelle automorphisme intérieur tout morphisme $\sigma_g : \begin{cases} G \to G \\ h \mapsto ghg^{-1} \end{cases}$ où $g \in G$. On note $Int(G)$ leur ensemble.

Rq: $H \triangleleft G$ ssi H est stable par automorphisme intérieur.

ex: * $\{e\} \triangleleft G$, $G \triangleleft G$
* $Int(G) \triangleleft Aut(G)$
* G abélien $\Rightarrow$ tout sous-groupe est distingué dans G.

[OA] → * $GL_n(\mathbb{Z})$ n'est pas distingué dans $GL_n(\mathbb{R})$, en effet: $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix} \notin GL_n(\mathbb{Z})$.

prop: Soit $f \in Hom(G, G')$, alors $f^{-1}(H')$ est un sous-groupe de G, distingué si H' l'est.

↳ prop: Soit $f \in Hom(G, G')$, alors $\ker(f) \triangleleft G$.

ex: * $SL_n(k) = \ker(\det)$ donc $SL_n(k) \triangleleft GL_n(k)$.
* $A_n = \ker(\varepsilon)$ donc $A_n \triangleleft \mathfrak{S}_n$.

↳ prop: Soit $f \in Hom(G, G')$, si $H \triangleleft G$, alors $f(H) \triangleleft f(G)$. De plus, si f est surjectif, $f(H) \triangleleft G'$.

Rq: • Soit K un sous-groupe de H, si $K \triangleleft G$ alors $K \triangleleft H$ mais $K \triangleleft H \triangleleft G \not\Rightarrow K \triangleleft G$.

2) Notion de classes [U], [C], [P]

def/prop: La relation définie sur G par $x R_H y$ ssi $y^{-1}x \in H$ est une relation d'équivalence sur G. La classe d'équivalence de $y \in G$ est $yH = \{yh, h \in H\}$ appelée classe à gauche.

On note G/H l'ensemble des classes à gauche. Son cardinal s'appelle indice de H dans G, noté $[G:H]$.

Rq: On peut également définir les classes à droite avec $x R'_H y$ ssi $x^{-1}y \in H$, qui donne $Hy = \{hy, h \in H\}$, l'ensemble des classes à droite $G\backslash H$ a même cardinal que G/H. Si G est abélien, alors $R_H = R_H'$.

↳ Thm (Lagrange): Si G est fini, $|G| = |H| \cdot |G/H|$.

↳ soit $g \in G$, alors ordre$(g) \mid |G|$.

App°: $[G:H] = 2 \Rightarrow H \triangleleft G$.

ex: * $G = \mathbb{Z}$, $H = n\mathbb{Z}$ alors $x R_H y \Leftrightarrow x \equiv y \Leftrightarrow x - y \in n\mathbb{Z}$.
* $D_n := \langle r, s \mid r^n = s^2 = srsr = e \rangle$ $[D_n : \langle r \rangle] = 2$ donc $\langle r \rangle \triangleleft D_n$.

3) Groupe quotient

def/prop: Si $H \triangleleft G$ alors G/H est muni d'une structure de groupe, via $(gH)(g'H) = (gg')H$, on l'appelle groupe quotient de G par H.
L'application canonique $\pi : \begin{cases} G \to G/H \\ g \mapsto gH \end{cases}$ est un morphisme surjectif de noyau H.

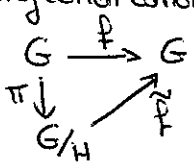
ex: * $n\mathbb{Z} \triangleleft \mathbb{Z}$ donc $\mathbb{Z}/n\mathbb{Z}$ est un groupe
* $\mathbb{Z} \triangleleft \mathbb{R}$ donc $\mathbb{R}/\mathbb{Z}$ est un groupe

↳ prop: $H \triangleleft G \Rightarrow \exists \varphi : G \to G/H$ tel que $\ker \varphi = H$.

4) Théorèmes d'isomorphismes [U], [C], ([OA])

prop (Propriété universelle): Soit $f \in \mathrm{Hom}(G, G')$, si $H \lhd G$, et si $H \subset \ker(f)$ alors $\exists ! \tilde{f} \in \mathrm{Hom}(G/H, G')$ tel que $f = \tilde{f} \circ \pi$ (où $\pi : G \to G/H$ est la projection canonique)

De plus, on a : $\begin{cases} \ker(\tilde{f}) = \pi(\ker(f)) \\ \mathrm{Im}(\tilde{f}) = \mathrm{Im}(f) \end{cases}$



cor (1er Thm d'isomorphisme): Avec les mêmes notations on a $\mathrm{Im}(f) \simeq G/\ker(f)$.

App: Tout groupe cyclique G d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

ex:
* $GL_n(\mathbb{C})/SL_n(\mathbb{C}) \simeq \mathbb{C}^*$
* $\mathfrak{S}_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$
* $\mathbb{R}/\mathbb{Z} \simeq \mathbb{U}$ où $\mathbb{U} = \{z \in \mathbb{C} / |z| = 1\}$

[CON] → **App**: Thm (Frobenius-Zolotarev): Soit $p \geq 3$ premier, $n \in \mathbb{N}^*$ alors $\forall u \in GL_n(\mathbb{F}_p)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$ (symbole de Legendre)

prop (3e thm isomorphisme): Soit $k < H < G$ des sous-groupes de G. Si $K \lhd G$ et $H \lhd G$ alors : $(G/k)/(H/k) \simeq G/H$.

II Groupes et sous-groupes importants

1) Groupes simples [U], [CAL]

def: G est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

[OVT] **prop**: A_n est simple pour tout entier $n \geq 5$.

[OVT] **prop**: $SO_3(\mathbb{R})$ est simple.

Rq: G simple et $\varphi \in \mathrm{Hom}(G, G') \Rightarrow \varphi$ est injectif ou trivial

App: Si $H \lhd G$, l'étude de G peut être ramenée à l'étude de H et de G/H par "dévissage". Les groupes simples sont indévissables.

prop: Les groupes simples abéliens sont les groupes cycliques d'ordre premier. ← [CAL]

2) Sous-groupe caractéristique [U]

def: H est dit caractéristique dans G si H est stable par automorphisme de G, on note $H \mathrm{car} G$.

prop: $H \mathrm{car} G \Rightarrow H \lhd G$

prop: $K < H < G$ des sous-groupes de G.
i) $K \mathrm{car} H \mathrm{car} G \Rightarrow K \mathrm{car} G$
ii) $K \mathrm{car} H \lhd G \Rightarrow K \lhd G$

3) Deux sous-groupes importants

a) Le centre $Z(G)$ [U], [P], [C]

def: Le centre de G est le groupe $Z(G) = \{x \in G / \forall y \in G, xy = yx\}$

prop: On note $\sigma : \begin{cases} G \to \mathrm{Int}G \\ g \mapsto \sigma_g \end{cases}$ alors $Z(G) = \ker(\sigma)$ et $Z(G)$ car G.

ex:
* $Z(\mathfrak{S}_n) = \{\mathrm{id}\}$ par $n \geq 3$
* $Z(\mathbb{H}_8) = \{\pm \mathrm{id}\}$ ($\mathbb{H}_8$: groupe des quaternions)

b) Le groupe dérivé $D(G)$ [P]

def: On appelle groupe dérivé de G le groupe engendré par les commutateurs : $D(G) = \langle \{[x,y] := xyx^{-1}y^{-1},\ x, y \in G\} \rangle$

prop: $D(G)$ car G

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

ex:
* $D(\mathfrak{S}_n) = A_n$ et $D(A_n) = A_n$ $\forall n \geq 2$
* $D(\mathbb{H}_8) = \{\pm \mathrm{id}\}$
* $D(GL_n(k)) = SL_n(k)$ sauf si $n = 2$, $k = \mathbb{F}_2$ et $D(SL_n(k)) = SL_n(k)$ sauf si $n = 2$ et ($k = \mathbb{F}_2$ ou $\mathbb{F}_3$)

thm: i) $G/D(G)$ est le plus grand quotient abélien de G.
ii) $D(G) \subset H$ ssi $H \triangleleft G$ et G/H abélien

III Notion de p-groupes et théorèmes de Sylow

Soit p un nombre premier

1) Les p-groupes [Li]

def: Un p-groupe est un groupe d'ordre une puissance de p.

ex: $\mathbb{Z}/p^\alpha\mathbb{Z}$ est un p-groupe $\forall \alpha \in \mathbb{N}^*$

prop: Soit X un G-ensemble, on note X^G l'ensemble des points fixes de X sous l'action de G, alors $|X^G| = |X| \bmod p$

↳ prop: Si G est un p-groupe alors $Z(G) \neq \{e\}$
En particulier, un p-groupe d'ordre non premier n'est jamais simple.

App: Un groupe d'ordre p^2 est toujours abélien.

2) Autour des théorèmes de Sylow [Li], [Cc], [Ph], [Sz]

Dans un groupe d'ordre n existe-t-il pour tout diviseur d de n, un ou plusieurs sous-groupes d'ordre d ?

def: Si G est fini d'ordre $n = p^\alpha m$ ($\alpha \in \mathbb{N}^*$, $m \in \mathbb{N}^* / p \nmid m$) on appelle alors p-sylow de G un sous-groupe de G d'ordre p^α.

Rq: P est un p-sylow de G signifie que P est un p-groupe tel que $p \wedge [G:P] = 1$.

DVT thm (Sylow): Soit G un groupe fini d'ordre $p^\alpha m$ ($\alpha \in \mathbb{N}^*$, $m \in \mathbb{N}^* / p \nmid m$), alors :
i) G contient au moins un p-sylow
ii) Si H est un sous-groupe de G, alors il existe au moins un p-sylow S de G tel que $H \subset S$
iii) Les p-sylow de G sont conjugués.
iv) Si on note n_p le nombre de p-Sylow de G, alors on a $n_p \mid m$ et $n_p \equiv 1 \bmod p$

Cor: Soit S un p-sylow de G alors :
$S \triangleleft G \iff S$ est l'unique p-sylow de G

⊛ ex: L'ensemble des matrices unipotentes de $T_n(\mathbb{F}_p)$ est un p-sylow de $GL_n(\mathbb{F}_p)$ d'ordre $p^{n(n-1)/2}$ ← [Sz]

App: Permet parfois de déterminer si un groupe fini est simple ou non.
ex: Un groupe d'ordre 56 n'est pas simple. ← [Cc]

IV Produit direct de groupes [Cc]

def/prop: Soit H et K deux groupes. $\forall (h,k), (h',k') \in H \times K$, on pose : $(h,k)(h',k') = (hh', kk')$. Alors $G := H \times K$ est un groupe muni de cette opération, appelé produit direct de H et K.

Rq: $H \times \{e\} \triangleleft G$, $K \times \{e\} \triangleleft G$,

prop (Caractérisation): Soit H et K deux sous-groupes de G. Si $H \triangleleft G$, $K \triangleleft G$, $HK = G$ et $H \cap K = \{e\}$ alors $H \times K \simeq G$ via l'isomorphisme $(h,k) \mapsto hk$.

ex: $U_6 \simeq U_3 \times U_2$.

prop (thm chinois): Soit $p, q \in \mathbb{N}^*$ tels que $p \wedge q = 1$
Alors : $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Références :

[U] : Felix Ulmer, Théorie des groupes

[P] : Daniel Perrin, Cours d'algèbre

[C] : François Combes, Algèbre et géométrie

[OA] : Beck, Malick & Peyré, Objectif agrégation

[SZ] : Aviva Szpirglas, Mathématiques L3 : algèbre

[CAL] : Josette Calais, Théorie des groupes

Simplicité de $\mathfrak{A}_n$

Antoine Louazel & Fanny Remoué

Théorème : Pour tout entier $n \geq 5$, le groupe alterné $\mathfrak{A}_n$ est simple.

Preuve : Soit N un sous-groupe distingué de $\mathfrak{A}_n$. Il s'agit de montrer que N est un sous-groupe trivial. Supposons que $N \neq \{\mathrm{id}\}$ et prouvons alors que $N = \mathfrak{A}_n$. Raisonnons par l'absurde en supposant que $N \neq \mathfrak{A}_n$. Dans la suite de cette démonstration, nous écrirons toute décomposition d'une permutation de N en produit de cycles à supports disjoints.

Si N contient un 3-cycle (i_1, i_2, i_3), alors tout autre 3-cycle (i'_1, i'_2, i'_3) de $\mathfrak{S}_n$ serait dans la même classe de conjugaison (dans $\mathfrak{S}_n$) que (i_1, i_2, i_3) ; il existerait donc un élément ρ de $\mathfrak{S}_n$ tel que $\rho(i_1, i_2, i_3)\rho^{-1} = \big(\rho(i_1), \rho(i_2), \rho(i_3)\big) = (i'_1, i'_2, i'_3)$.

- Si $\varepsilon(\rho) = 1$, $\rho \in \mathfrak{A}_n$ et donc $(i'_1, i'_2, i'_3) \in N$ car N est distingué
- Sinon, puisque $n \geq 5$, il existe alors $i_4 \neq i_5 \in [\![1\,;n]\!]\backslash\{i'_1, i'_2, i'_3\}$. La permutation $\tilde{\rho} := (i_4, i_5)\rho \in \mathfrak{A}_n$ vérifie $\tilde{\rho}(i_1, i_2, i_3)\tilde{\rho}^{-1} = (i_4, i_5)\rho(i_1, i_2, i_3)\big((i_4, i_5)\rho\big)^{-1} = (i'_1, i'_2, i'_3)$.

N contiendrait dans ce cas tous les 3-cycles, ce qui impliquerait le fait que $N = \mathfrak{A}_n$ (ce dernier étant engendré par les 3-cycles), d'où la contradiction ! Le groupe N ne contient donc pas de 3-cycles.

Supposons à présent que la décomposition de $\sigma \in N$ contienne un cycle de longueur supérieure à 4, disons $\sigma = (i_1, i_2, i_3, i_4, \dots)$ .... Comme N est distingué, $\sigma' := (i_1, i_2, i_3)\sigma(i_1, i_2, i_3)^{-1} = (i_2, i_3, i_1, i_4, \dots)$ ... $\in N$ dans lequel les autres cycles restent identiques à ceux de σ. Dans $\sigma'\sigma^{-1}$, ces autres cycles s'annulent et $\sigma'\sigma^{-1} = (i_2, i_3, i_1, i_4)(i_1, i_4, i_3, i_2) = (i_1, i_2, i_4)$ est un 3-cycle (les éventuels i_j avec $j \geq 5$ du premier cycle de σ sont fixes), d'où la contradiction avec le premier point.

Si la décomposition de $\sigma \in N$ contient un unique 3-cycle, alors les autres cycles seraient des transpositions et σ^2 serait dans ce cas un 3-cycle, ce qui – toujours par la premier point – est impossible.

Si la décomposition de $\sigma \in N$ contient (au moins) deux 3-cycle, disons $\sigma = (i_1, i_2, i_3)(i'_1, i'_2, i'_3)$ ..., alors $\sigma' := (i'_1, i'_2, i_3)\sigma(i'_1, i'_2, i_3)^{-1} = (i_1, i_2, i'_1)(i'_2, i_3, i'_3)$ ... $\in N$ puisque N est distingué. Par suite, $\sigma'\sigma = (i_1, i'_1, i_3, i_2, i'_3)$ ... $\in N$ et cela nous donne une contradiction avec le second point. La décomposition de toute permutation de N ne contient par conséquent aucun 3-cycle et est donc produit d'un nombre pair de transpositions.

Si la décomposition de $\sigma \in N$ est $\sigma := (i_1, i_2)(i_3, i_4)$, alors pour $i_5 \in [\![1\,;n]\!]\backslash\{i_1, \dots, i_4\}$, on aurait $\sigma' := (i_1, i_5, i_2)\ \sigma(i_1, i_5, i_2)^{-1} = (i_1, i_5)(i_3, i_4) \in N$. Comme $\sigma'\sigma = (i_1, i_2, i_5) \in N$, on obtient à nouveau une contradiction avec le premier point.

La décomposition de $\sigma \in N$ est donc de la forme $\sigma := (i_1, i_2)(i_3, i_4)(i_5, i_6)(i_7, i_8)$ .... Dans ce cas, $\sigma' := (i_5, i_4)(i_3, i_2)\sigma(i_5, i_4)(i_3, i_2) = (i_1, i_3)(i_2, i_5)(i_4, i_6)(i_7, i_8)$ ... $\in N$ et du coup $\sigma'\sigma = (i_1, i_5, i_4)(i_2, i_3, i_6) \in N$, ce qui contredit le quatrième point.

Conclusion : Il est impossible d'avoir $N \lhd \mathfrak{A}_n$ avec $\notin \{\mathrm{id}, \mathfrak{A}_n\}$ pour $n \geq 5$. ■

Théorème de Sylow

Arnaud GIRAND

11 décembre 2011

Référence :
- [Per96] ; p. 18–20

Leçons :
- 101 - Groupe opérant sur un ensemble. Exemples et applications.
- 104 - Groupes finis. Exemples et applications.
- 110 - Nombres premiers. Applications.

Prérequis :
- formule des classes.

Soit G un groupe fini de cardinal $n \geq 1$. On suppose qu'il existe un nombre premier p et deux entiers $\alpha, m \geq 1$ tels que $n = p^\alpha m$, avec $p \nmid m$.

Lemme 1
Soit $H \leq G$.
Soit S un p–Sylow de G.
Alors il existe $a \in G$ tel que $H_a := aSa^{-1} \cap H$ soit un p–Sylow de H.

DÉMONSTRATION : G agit sur G/S par translation à gauche et :

$$\begin{aligned} \forall a, g \in G,\ g.(aS) = as &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ gas = as' \\ &\Leftrightarrow \forall s \in S,\ \exists s' \in S,\ g = as's^{-1}a^{-1} \\ &\Leftrightarrow g \in aSa^{-1} \end{aligned}$$

On a donc $\forall a, g \in G$, $\mathrm{Stab}_G(aS) = aSa^{-1}$. Or H agit sur G/S par restriction et $\mathrm{Stab}_H(aS) = \mathrm{Stab}_G(aS) \cap H = H_a$ est un sous-groupe de $\mathrm{Stab}_G(aS)$, d'où $|H_a| \,|\, |aSa^{-1}| = |S| = p^\alpha$. De fait, par primalité, $p \,|\, |H_a|$.
Or $|H_a| = \dfrac{|H|}{(H : H_a)}$ donc il nous suffit de trouver $a \in G$ tel que $(H : H_a) \wedge p = 1$.

Si on note $\omega(aS)$ l'orbite d'un élément aS de G/S sous l'action de H, l'application $g \mapsto g.aS$ et la propriété universelle du quotient nous indiquent que $(H : H_a) = |H/H_a| = |\omega(aS)|$. De fait, si p divisait tous les indices $(H : H_a)$, on aurait par la formule des classes que p divise $m = |G/S|$, ce qui est impossible, d'où le résultat.

Proposition 1 (Sylow)
On note $c_p \geq 0$ le nombre de p–Sylow de G.
Alors :

(i) pour tout p–groupe $H \leq G$, il existe un p–Sylow de G contenant H (et donc $c_p \geq 1$) ;

(ii) les p–Sylow de G sont tous conjugués (et donc $c_p | n$), en particulier si S est un p–Sylow de G et si $S \lhd G$ alors S est l'unique p–Sylow de G ;

(iii) $c_p \equiv 1[p]$ (et donc $c_p | m$).

DÉMONSTRATION :

(*i*) On a l'injection suivante (où $(e_1, \ldots, e_n)$ désigne la base canonique de $\mathbb{F}_p^n$) :

$$\begin{aligned} \mathfrak{S}_n &\hookrightarrow GL_n(\mathbb{F}_p) \\ \sigma &\mapsto (u_\sigma : e_i \mapsto e_{\sigma(i)}) \end{aligned}$$

Ainsi, d'après le théorème de Cayley (proposition 2) et la propriété universelle du quotient, on peut identifier G à un sous groupe de $GL_n(\mathbb{F}_p)$. Or $GL_n(\mathbb{F}_p)$ possède un p–Sylow (les

matrices triangulaires supérieures "strictes", cf. infra) donc d'après le lemme 1, G aussi : notons le S.

Toujours d'après le lemme 1, comme H est un sous-groupe de G, il existe $a \in G$ tel que H_a soit un p-Sylow de H. Or H est également un p-groupe et donc son unique p-Sylow est lui-même, ergo $H_a = H$, ce qui implique que $H \subset aSa^{-1}$, qui est un p-Sylow [1].

(ii) On procède comme pour le point *(i)* en imposant à H d'être un p-Sylow. On obtient bien alors que pour tout p-Sylow S de G, il existe $a \in G$ tel que $H \subset aSa^{-1}$. Or $|H| = p^\alpha = |S| = |aSa^{-1}|$ donc $H = aSa^{-1}$ est conjugué à S.

(iii) Notons X l'ensemble des p-Sylow de G. On sait que G agit sur X par conjugaison et si $S \in X$, cette action en induit une de S sur X. D'après le lemme 2 on a donc $|X| \equiv |X^S|[p]$. Il est de plus clair que $S \in X^S$.

Soit $T \in X^S$, i.e $\forall s \in S,\ sTs^{-1} = T$. On considère le sous-groupe N de G engendré par S et T ; alors $S \leq N$ et $T \leq N$ sont deux p-Sylow de N. Cependant il est clair que $T \lhd N$ et donc par le point *(ii)* $T = S$. In fine $X^S = \{S\}$ et donc $c_p = |X| \equiv 1[p]$.

Détails supplémentaires :

- *$GL_n(\mathbb{F}_p)$ admet un p-Sylow* (cf. [Per96], p.15). Commençons par remarquer que :

$$\forall A \in \mathcal{M}_n(\mathbb{F}_p),\quad A \in GL_n(\mathbb{F}_p) \Leftrightarrow (Ae_1, \dots, Ae_n) \text{ est une base de } \mathbb{F}_p^n$$

$GL_n(\mathbb{F}_p)$ est de facto équipotent à l'ensemble des bases de $\mathbb{F}_p^n$. Or pour se donner une telle base $(a_1, \dots, a_n)$, on dispose de $p^n - 1$ choix pour a_1 (on choisit $a_1 \in \mathbb{F}_p^n \setminus \{0\}$, de $p^n - p$ choix pour a_2 (on choisit $a_2 \notin \langle a_1 \rangle$) et de manière générale de $p^n - p^{i-1}$ choix pour a_i, $i \in [n]$ (on choisit $a_i \notin \langle a_1, \dots, a_{i-1} \rangle$). In fine :

$$|GL_n(\mathbb{F}_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$$

On a donc $|GL_n(\mathbb{F}_p)| = p^{n(n-1)/2} m$, avec $p \nmid m$. On considère alors le sous-groupe de $GL_n(\mathbb{F}_p)$ constitué des matrices triangulaires supérieures "strictes" :

$$P := \{A \in GL_n(\mathbb{F}_p) \mid \forall i, j \in [n],\ a_{i,j} = 0 \text{ si } i > j,\ a_{i,i} = n\} \leq GL_n(\mathbb{F}_p)$$

Alors $|P| = p^{n(n-1)/2}$ (on "choisit" exactement $\frac{n(n-1)}{2}$ coefficients de chaque matrice) donc P est un p-Sylow de $GL_n(\mathbb{F}_p)$.

- On trouve le résultat suivant dans [Per96], p.15 :

Proposition 2 (Cayley)
Soit G un groupe fini de cardinal $n \geq 1$.
Alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.
DÉMONSTRATION : G agit sur lui-même par translation à gauche donc il existe un morphisme de groupes de G dans $\mathfrak{S}(G) \cong \mathfrak{S}_n$. Ce morphisme est de plus injectif car si $g, h \in G$ $(\forall x \in G,\ g.x = h.x) \Rightarrow (g = h)$. On conclut par propriété universelle du quotient.

- Le lemme suivant est démontré dans [Per96], p.17 :

Lemme 2
Soit G un p-groupe.
Soit X un G-ensemble fini.
Alors :

$$|X| \equiv |X^G|[p]$$

DÉMONSTRATION : D'après la formule des classes :

$$|X| = |X^G| + \sum |\omega(x)|$$

Où la somme compte une fois chaque orbite non triviale. De fait, chacun de ces $|\omega(x)|$ est strictement supérieur à 1 et divise $|G|$ donc $p||\omega(x)|$, d'où le résultat.

- *Une application classique : il n'existe pas de groupe simple d'ordre 63.* Soit G un groupe d'ordre $63 = 3^2 \times 7$. Alors $c_7 \equiv 1[7]$ et $c_7|9$ donc $c_7 = 1$: G admet un unique 7-Sylow qui est donc distingué.

1. La conjugaison conservant les cardinaux, le conjugué d'un p-Sylow est un p-Sylow de G.

Simplicité de $SO(3)$

On montre que le groupe des rotations de l'espace à trois dimensions $SO(3)$ est un groupe simple, c'est-à-dire que ses seuls sous-groupes distingués sont $\{Id\}$ et $SO(3)$.

Le principe de la démonstration est issu du livre *Oraux X-ENS, algèbre, tome 3.* Il existe d'autres démonstrations de ce résultat dans les livres *Cours d'algèbre* de Perrin, et *Calcul différentiel. Thèmes d'analyse pour l'agrégation* de Gonnord et Tosel.

1. Soit G un sous-groupe de $SO(3)$, et soit G_0 la composante connexe dans G de l'identité. Montrons que G_0 est un sous-groupe de $SO(3)$, et que $G_0 \lhd SO(3)$ dés que $G \lhd SO(3)$.

   Par définition G_0 contient l'identité. L'application

   $$\begin{aligned} \varphi : \ G_0 \times G_0 &\longrightarrow G \\ (x, y) &\longmapsto xy^{-1} \end{aligned}$$

   est continue, et $G_0 \times G_0$ étant connexe, on en déduit que l'image de φ est un connexe de G. De plus elle contient l'identité, donc est incluse dans G_0, ce qui montre que G_0 est un sous-groupe de G.
   Si on suppose désormais que $G \lhd SO(3)$ et si $h \in SO(3)$, alors l'application

   $$\begin{aligned} \mathrm{Int}_h : \ G &\longrightarrow G \\ g &\longmapsto hgh^{-1} \end{aligned}$$

   est bien définie. Le même argument que plus haut montre que Int_h envoie G_0 dans G_0, et ce pour tout $h \in SO(3)$, ce qui siginifie que G_0 est un sous-groupe distigué de $SO(3)$.

2. Soit désormais G un sous-groupe connexe de $SO(3)$, distingué et non réduit à l'identité. Montrons que G contient un retournement, c'est-à-dire une rotation d'angle π. On en déduira alors que $G = SO(3)$.

   Soit $r \in SO(3)$. Il existe une base orthonormée de $\mathbb{R}^3$ telle que la matrice de l'application linéaire canoniquement associée à r dans cette base soit

   $$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

   On a $Tr(r) = 1 + 2\cos\theta$, donc la fonction

   $$\begin{aligned} \varphi : G &\longrightarrow [-1, 1] \\ g &\longmapsto \frac{Tr(g) - 1}{2} \end{aligned}$$

est bien définie.
Cherchons un élément $s \in G$ tel que $\varphi(s) \leq 0$. Soit g un élément de G distinct de l'identité. On a

$$\frac{Tr(g)-1}{2} = \cos\theta$$

où θ est défini au signe près. Quitte à changer g en g^{-1} on peut supposer que $\theta \in]0,\pi]$. Si $\theta \in [\pi/2,\pi]$ alors $s = g$ convient. Sinon, soit $N = E\left(\frac{\pi}{2\theta}\right)$. On a

$$N\theta \leq \frac{\pi}{2} < (N+1)\theta \leq \frac{\pi}{2} + \theta \leq \pi,$$

donc $s = g^{N+1}$ convient.
Par hypothèse G est connexe, et φ est clairement continue, donc $\varphi(G)$ est un connexe de $[-1,1]$ contenant $\varphi(s) \leq 0$ et $\varphi(Id) = 1$. Or, les connexes de $\mathbb{R}$ sont les intervalles, donc il existe $g \in G$ tel que $\varphi(g) = 0$, c'est-à-dire G contient une rotation d'angle $\pm\frac{\pi}{2}$. L'élément $R = g^2 \in G$ est donc un retournement.
Montrons qu'alors $G = SO(3)$. Pour tout $g \in SO(3)$, l'élément gRg^{-1} est dans G car G est distingué par hypothèse, et est un retournement d'axe $g(\Delta)$ où Δ est l'axe de R. Le fait que $SO(3)$ agisse transitivement sur l'ensemble des droites de $\mathbb{R}^3$ montre que G contient tous les retournements. Or tout élément de $SO(3)$ est produit de deux retournements, ce qui conclut.

3. Soit maintenant G un sous-groupe distingué de $SO(3)$. Montrons que $G = \{Id\}$ ou $G = SO(3)$. Si $G_0 \neq \{Id\}$ alors 1 et 2 montrent que $G_0 = SO(3)$, donc a fortiori $G = SO(3)$. Si $G_0 = \{Id\}$ alors montrons que $G = \{Id\}$, ce qui terminera la preuve. Remarquons que dans ce cas toutes les composantes connexes de G sont des singletons. Soit $g \in G$. L'application continue

$$\begin{aligned} \varphi : SO(3) &\longrightarrow G \\ h &\longmapsto hgh^{-1} \end{aligned}$$

est bien définie car $G \lhd SO(3)$. Le groupe $SO(3)$ est connexe donc l'image de φ est un connexe contenant g, donc est égale à $\{g\}$ d'après la remarque sur les composantes connexes de G. Cela signifie que g commute avec toutes les rotations de l'espace. En particulier g est une rotation qui fixe toutes les droites de $\mathbb{R}^3$, ce qui montre que $g = Id$.