Opération d'un groupe sur un ensemble

1 Définitions et exemples

1.1 Opération d'un groupe sur un ensemble

Soit G un groupe et X un ensemble. Une *opération à gauche*[1] de G sur X est une application

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g.x \end{array}$$

vérifiant les propriétés suivantes :

1. $\forall g, g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x$,
2. $\forall x \in X,\ 1.x = x$.

On peut aussi voir une opération à gauche de G sur X comme un morphisme φ de G dans le groupe $\mathbf{S}(X)$ des bijections de X ; on pose alors

$$g.x \overset{\text{déf}}{=} \varphi(g)(x).$$

Opération à gauche ou à droite ?

On définit de la même façon une *opération à droite* de G sur X comme une application

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & x.g \end{array}$$

vérifiant cette fois :

1. $\forall g, g' \in G,\ \forall x \in X,\ (x.g).g' = x.(gg')$,
2. $\forall x \in X,\ x.1 = x$.

La différence avec l'opération à gauche tient dans le fait que l'action du produit gg' sur un point x consiste ici à appliquer d'abord g puis g', ce qui est cohérent avec la notation $x.g$. Pour une opération à droite de G sur X, l'application $g \longmapsto (x \longmapsto x.g)$ n'est cette fois plus un morphisme. On obtient un morphisme de G dans $\mathbf{S}(X)$ en considérant $g \longmapsto (x \longmapsto x.g^{-1})$.

Lorsqu'un groupe G opère à gauche sur un ensemble X, on peut définir naturellement une opération à droite de G sur l'ensemble des applications de X dans un ensemble Y en posant, pour tout $f : X \longrightarrow Y$ et tout $g \in G$: $f.g \overset{\text{déf}}{=} f \circ g$.

Dans la suite, les opérations considérées seront par défaut des opérations à gauche. Toutes les propriétés démontrées dans ce cadre se traduisent sans problème en termes d'opérations à droite.

[1] On dit aussi une *action* de G sur X

1.2 Quelques exemples

Pour tout ensemble X, le groupe $\mathbf{S}(X)$ des bijections de X opère naturellement sur X : il suffit de poser $\sigma.x \stackrel{\text{déf}}{=} \sigma(x)$ pour $\sigma \in \mathbf{S}(X)$ et $x \in X$. En particulier le groupe symétrique $\mathbf{S}_n$ opère naturellement sur $\{1, \ldots, n\}$.

Une fois donnée une opération d'un groupe G sur un ensemble X, tout sous-groupe H de G opère lui-aussi sur X par restriction. Or, bon nombre de groupes classiques sont construits comme des sous-groupes du groupe des bijections d'un ensemble donné, et à ce titre opèrent eux aussi “naturellement” sur cet ensemble. Ceci permet de trouver une multitude d'exemples, parmi lesquels on peut citer :

- Si E est un espace vectoriel, le groupe $GL(E)$ des automorphismes linéaires de E opère sur E.
- Le groupe des isométries du plan conservant une figure donnée opère sur le plan (et aussi sur l'ensemble des points de la figure conservée).
- [...]

Une bijection σ d'un ensemble X sur lui-même permet de définir une opération de $\mathbb{Z}$ sur X, en posant

$$\forall p \in \mathbb{Z},\ \forall x \in X,\ p.x \stackrel{\text{déf}}{=} \sigma^p(x).$$

Cette opération correspond au morphisme de $\mathbb{Z}$ dans $\mathbf{S}(X)$ défini par $p \longmapsto \sigma^p$.

1.3 Vocabulaire

On considère ici une opération d'un groupe G sur un ensemble X.

Orbite d'un point

On définit sur X une relation d'équivalence $\mathscr{R}$ par

$$x \mathscr{R} y \stackrel{\text{déf}}{\iff} \exists g \in G,\ y = g.x.$$

(Vérifier qu'il s'agit bien d'une relation d'équivalence...) L'*orbite* d'un point x de X est alors la classe d'équivalence de x pour cette relation. On la note $\mathrm{Orb}(x)$. Ainsi,

$$\mathrm{Orb}(x) \;=\; \{y \in X \;/\; \exists g \in G,\ g.x = y\}$$

Les orbites forment une partition de X.

Stabilisateur d'un point

Pour $x \in X$, on appelle *stabilisateur de x* le sous-ensemble $\mathrm{Stab}(x)$ défini par

$$\mathrm{Stab}(x) \stackrel{\text{déf}}{=} \{g \in G \;/\; g.x = x\}.$$

Le stabilisateur de x est toujours un sous-groupe de G, mais qui n'est pas en général distingué.

Théorème 1.1 *L'indice de $Stab(x)$ dans G est égal au cardinal de l'orbite de x. En conséquence, si G est un groupe fini, le cardinal d'une orbite quelconque sous l'action de G divise toujours l'ordre de G, et on a*

$$|Orb(x)| \;=\; |G|/|Stab(x)|.$$

Points fixes

Pour $g \in G$, on appelle *point fixe de* g tout point x de X tel que $g.x = x$. On note $\mathrm{Fix}(g)$ l'ensemble des points fixes de g.

Fidèlement (opérer)

On dit que G opère *fidèlement* sur X si le morphisme φ de G dans $\mathbf{S}(X)$ défini par l'opération est injectif, autrement dit si

$$(\forall x \in X,\ g.x = x) \implies g = 1.$$

Si on se place dans l'exemple de l'opération de $\mathbb{Z}$ sur X définie à partir de $\sigma \in \mathbf{S}(X)$ (voir plus haut), cette opération est fidèle lorsque pour tout p, $\sigma^p \neq \mathrm{Id}_X$. En particulier, elle ne peut pas être fidèle si X est fini [...]. Dans le cas où σ est d'ordre p fini, on peut à l'aide de σ définir une opération fidèle de $\mathbb{Z}/p\mathbb{Z}$ sur X [...].

Plus généralement, une opération quelconque de G sur X permet toujours de définir une opération fidèle de $G/\mathrm{Ker}\,\varphi$ sur X [...].

Transitivement (opérer)

On dit que G opère *transitivement* sur X lorsqu'il n'y a qu'une seule orbite pour l'opération considérée, c'est-à-dire si

$$\forall x, y \in X,\ \exists g \in G,\ y = g.x.$$

Exercice 1.1 *Soit G un groupe opérant transitivement sur un ensemble E, et H un sous-groupe normal de G, agissant par restriction sur le même ensemble E. Montrer que toutes les H-orbites ont même cardinal. Que peut-on dire si E est fini de cardinal premier ?*

1.4 Opérations d'un groupe sur lui-même

G étant un groupe quelconque, on peut définir plusieurs opérations de G sur lui-même.

Opération par translation à gauche

L'opération de G sur lui-même par *translation à gauche* est simplement définie par la formule

$$g.h \overset{\text{déf}}{=} gh.$$

Cette opération est mieux que transitive : si on prend deux éléments quelconques h et h', il existe un *unique* $g \in G$ tel que $g.h = h'$. En particulier, le morphisme de G dans $\mathbf{S}(G)$ défini par cette opération est injectif : G opère fidèlement par translation à gauche sur lui-même. On en déduit le théorème important qui suit [...].

Théorème 1.2 (Théorème de Cayley) *Si G est un groupe fini d'ordre n, G est isomorphe à un sous-groupe du groupe symétrique $\mathbf{S}_n$.*

Exercice 1.2 Un résultat de Frobénius (1895)

Soit G un groupe fini, et H un sous-groupe de G tel que tout diviseur premier de $|H|$ soit supérieur ou égal à $|G/H|$. Montrer que H est distingué dans G.

(Indication : *considérer l'opération de H sur G/H par translation à gauche.*)

Opération de conjugaison

On peut aussi faire opérer G sur lui-même par *conjugaison*, en posant

$$g.h \stackrel{\text{déf}}{=} ghg^{-1}.$$

Pour $g \in G$, l'application $i_g \ : \ h \longmapsto ghg^{-1}$ est un automorphisme du groupe G, appelé *automorphisme intérieur*. Les orbites pour cette opération s'appellent les *classes de conjugaison*, et deux éléments d'une même orbite sont dits *conjugués*. Le stabilisateur de $h \in G$ s'appelle aussi dans ce cas le *centralisateur* de h, il est constitué des éléments de G qui commutent avec h. L'opération de conjugaison n'est en général ni fidèle ni transitive (trouver des contre-exemples).

Exercice 1.3 *Montrer que si H est un sous-groupe de G, tout conjugué de H (i.e. toute partie de G de la forme gHg^{-1}, où $g \in G$) est encore un sous-groupe de G. En déduire que G agit par conjugaison sur l'ensemble de ses sous-groupes.*

Lorsque l'on considère en même temps l'action de G sur un ensemble X, on peut identifier chaque élément du groupe G à une bijection de X sur lui-même, et l'opération de conjugaison s'interprète de façon naturelle. En effet, dire que $h' = i_g(h) = ghg^{-1}$, c'est dire que le diagramme suivant commute.

$$\begin{tikzcd} X \arrow[r, "h"] \arrow[d, "g"'] & X \arrow[d, "g"'] \\ X \arrow[r, "h'"] & X \end{tikzcd}$$

Autrement dit, l'action de h' sur les éléments $g(x),\ x \in X$ est identique à l'action de h sur les éléments $x \in X$. On en déduit ce que l'on peut appeler le *principe de conjugaison*, se résumant en deux idées essentielles :

- Beaucoup de propriétés *géométriques*[2] des éléments de G sont invariantes par conjugaison.
- Si un élément h de G est lié à une certaine partie Y de l'ensemble sur lequel opère G (par exemple Y est l'ensemble des points fixes de h), alors l'ensemble correspondant pour le conjugué $h' = ghg^{-1}$ est $g(Y)$.

Voici deux exemples classiques pour illustrer ces idées.

Exercice 1.4 *Soit $\sigma \in \mathbf{S}_n$ un cycle de longueur p : $\sigma = (a_1, \dots, a_p)$, et soit $\tau \in \mathbf{S}_n$. Montrer que $i_\tau(\sigma) = \Big(\tau(a_1), \dots, \tau(a_p)\Big)$. En déduire que l'ensemble des cycles de longueur p constitue une classe de conjugaison.*

Exercice 1.5 *Dans un groupe G, vérifier que deux éléments conjugués sont toujours de même ordre. La réciproque est-elle vraie en général ? Trouver tous les groupes abéliens dans lesquels deux éléments de même ordre sont toujours conjugués. Trouver aussi un exemple de groupe non abélien dans lequel cette propriété est vraie.*

[2] On peut appeler "géométriques" les propriétés des éléments du groupe relatives à une opération donnée (le nombre de points fixes, les valeurs propres...)

Exercice 1.6 *Soit G un groupe fini, et H un sous-groupe strict de G. Prouver que*

$$E \stackrel{\text{déf}}{=} \bigcup_{x \in G} xHx^{-1}$$

ne recouvre pas G tout entier.

2 Opération d'un groupe fini

2.1 Équation aux classes

On considère ici un groupe fini G opérant sur lui-même par conjugaison. Le centre $Z(G)$ du groupe G est exactement l'ensemble des $g \in G$ dont l'orbite (*i.e.* la classe de conjugaison) est réduite à un seul point. Pour $g \in G \setminus Z(G)$, on définit le sous-groupe $Z(g)$ de G constitué des éléments qui commutent avec g. Il est immédiat que $Z(g)$ coïncide avec le stabilisateur de g sous l'opération de conjugaison. On sait alors d'après le théorème 1.1 que le cardinal de la classe de conjugaison de g est égal à l'indice de $Z(g)$ dans G. Choisissons maintenant un système $(g_i)_{1 \leq i \leq k}$ de représentants des classes de conjugaison distinctes et non ponctuelles de G. Comme les classes de conjugaison forment une partition de G, on a immédiatement l'égalité suivante, appelée *équation aux classes*, ou *formule des classes*.

$$|G| \;=\; |Z(G)| + \sum_{i=1}^{k} (G : Z(g_i)).$$

Soit p un entier premier. Un *p-groupe* est un groupe fini dont l'ordre est une puissance de p. L'exercice suivant présente une propriété importante des p-groupes, conséquence de la formule des classes.

Exercice 2.1 *Soit p un entier premier. Montrer que si G est un p-groupe non réduit à $\{1\}$, son centre n'est pas non plus réduit à $\{1\}$.*

Plus généralement, on montre en utilisant les mêmes arguments le résultat qui suit.

Exercice 2.2 *Soit p un entier premier, G un p-groupe opérant sur un ensemble fini X. Notons X^G l'ensemble des points de X fixes par cette opération, i.e.*

$$X^G \stackrel{\text{déf}}{=} \{x \in X \;/\; \forall g \in G,\; g.x = x\}.$$

Montrer que

$$|X^G| \;\equiv\; |X| \quad (mod\ p).$$

Exercice 2.3 *Soit G un groupe d'ordre p^2, où p est un entier premier. Montrer que G est abélien.*

2.2 Formule de Burnside

Théorème 2.1 *Soit G un groupe fini opérant sur un ensemble fini X. Le nombre N d'orbites est donné par la formule*

$$N \;=\; \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Preuve — Le nombre N d'orbites vaut

$$N = \sum_{x\in X} \frac{1}{|\mathrm{Orb}(x)|}.$$

Or, pour chaque $x \in X$, on a vu (voir le théorème 1.1) que le cardinal de l'orbite de x est égal à l'indice du stabilisateur de x dans G, et donc $1/|\mathrm{Orb}(x)| = |\mathrm{Stab}(x)|/|G|$. On en déduit

$$N = \frac{1}{|G|} \sum_{x\in X} |\mathrm{Stab}(x)|.$$

Mais par ailleurs, on peut remarquer que

$$\begin{aligned} \sum_{x\in X} |\mathrm{Stab}(x)| &= |\{(g,x) \in G \times X \ / \ g.x = x\}| \\ &= \sum_{g\in G} |\mathrm{Fix}(g)|. \end{aligned}$$

❏

Exercice 2.4 *G étant un groupe fini agissant* transitivement *sur un ensemble fini X de cardinal $|X| \geq 2$, prouver qu'il existe un élément de G sans point fixe pour cette action. (Lemme de Jordan)*

Application au dénombrement

La formule de Burnside exposée ci-dessus peut être utilisée dans des problèmes de dénombrement, lorsqu'il s'agit de compter des objets *modulo* un certain groupe de transformations (c'est-à-dire sans distinguer deux objets qui se déduisent l'un de l'autre par une transformation du groupe donné). Cela revient donc exactement à compter le nombre d'orbites de l'action du groupe sur l'ensemble des objets considérés.

Voici un exemple d'un tel problème. On veut colorier les 6 faces d'un cube ; il y a q couleurs disponibles. Combien y a-t-il de façons différentes de le faire, sachant qu'on ne distingue pas deux coloriages qui se déduisent l'un de l'autre par un déplacement du cube ?

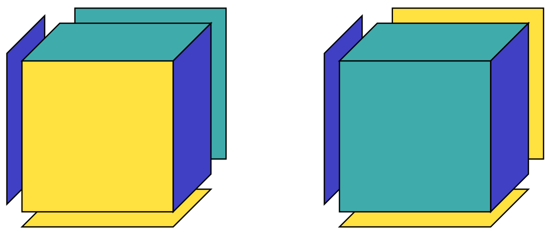

FIG. 1 – Deux coloriages identiques du cube

Notons $\mathscr{F}$ l'ensemble des 6 faces du cube, et $\mathscr{C}$ l'ensemble des q couleurs. On considère l'ensemble X des applications φ de $\mathscr{F}$ dans $\mathscr{C}$, sur lequel agit (à droite !) le groupe G des isométries directes du cube par la formule $g.\varphi \stackrel{\text{déf}}{=} \varphi \circ g$. Deux applications φ et φ' de X

correspondent au même coloriage du cube si et seulement si on peut passer de l'une à l'autre par l'action d'un élément de G ; autrement dit, il y a autant de coloriages différents que d'orbites pour l'action de G sur X. Il reste donc à dénombrer ces orbites, et la formule de Burnside est l'outil idéal pour cela. Le groupe G des isométries directes du cube comprend 24 éléments que l'on peut répartir en 5 types :

- l'identité,
- 3 symétries axiales d'axe passant par les centres de deux faces opposées (type 2),
- 6 rotations d'angle $\pm\pi/2$, d'axe passant par les centres de deux faces opposées (type 3),
- 6 symétries axiales d'axe passant par les milieux de deux arêtes opposées (type 4),
- 8 rotations d'angle $\pm 2\pi/3$, d'axe passant par deux sommets opposés (type 5).

On doit maintenant compter le nombre de points fixes dans X pour chacun de ces éléments. Chaque $g \in G$ agit comme une permutation sur $\mathscr{F}$, qui se décompose en cycles disjoints ; une application $\varphi : \mathscr{F} \longrightarrow \mathscr{C}$ est fixe par g si et seulement si elle est constante sur chacun de ces cycles. Le nombre de points fixes de g est donc $q^{\gamma(g)}$, où $\gamma(g)$ est le nombre de cycles de l'action de g sur $\mathscr{F}$. On a

- $\gamma(\mathrm{Id}) = 6$,
- pour g de type 2, $\gamma(g) = 4$,
- pour g de type 3, $\gamma(g) = 3$,
- pour g de type 4, $\gamma(g) = 3$,
- pour g de type 5, $\gamma(g) = 2$,

Le nombre de coloriages différents possibles du cube avec q couleurs vaut donc

$$\frac{1}{24}\left(q^6 + 3q^4 + 12q^3 + 8q^2\right).$$

Exercice 2.5 *Le petit théorème de Fermat par les perles...*

Soit p un entier premier, et $n \geq 2$ un entier. On dispose de perles de n couleurs possibles, avec lesquelles on fabrique des colliers circulaires comportant chacun p perles. Pour chaque collier, on veut utiliser au moins deux couleurs. En utilisant la formule de Burnside, calculer le nombre de colliers réalisables sachant que l'on ne distingue pas deux colliers qui se déduisent l'un de l'autre par une rotation.

En déduire que $n^p \equiv n \pmod{p}$.

2.3 Un lemme de Cauchy sur les groupes finis

Le théorème de Lagrange affirme que l'ordre de tout sous-groupe d'un groupe fini G doit diviser l'ordre de G. Réciproquement, étant donné un diviseur d de l'ordre de G, on peut se demander s'il existe forcément un sous-groupe de G d'ordre d. Ce n'est pas vrai en général (trouver un contre-exemple !), mais certains résultats célèbres sur les groupes finis vont dans ce sens. C'est le cas notamment des théorèmes de Sylow exposés plus loin, ainsi que du lemme de Cauchy qui suit.

Théorème 2.2 (Lemme de Cauchy) *Soit G un groupe fini d'ordre n, et p un entier premier divisant n. Alors*

1. *le nombre de solutions dans G de l'équation $x^p = 1$ est un multiple de p,*
2. *il y a au moins un sous-groupe de G d'ordre p.*

Pour la preuve laissée en exercice, voici quelques indications.

- Expliquer comment déduire la seconde affirmation de la première.
  On considère $S \stackrel{\text{déf}}{=} \{(x_1, x_2, \ldots, x_p) \in G^p \;/\; x_1 x_2 \cdots x_p = 1\}$.
- Montrer que $|S| = n^{p-1}$.
- Soit $\gamma \stackrel{\text{déf}}{=} (1, \ldots, p) \in \mathbf{S}_p$ (cycle d'ordre p). Expliquer pourquoi la formule

$$\gamma^k.(x_1, x_2, \ldots, x_p) \stackrel{\text{déf}}{=} (x_{\gamma^k(1)}, x_{\gamma^k(2)}, \ldots, x_{\gamma^k(p)})$$

  permet de définir une action du sous-groupe $<\gamma>$ engendré par γ sur l'ensemble S.
- Montrer qu'une orbite pour cette action est de cardinal 1 ou p.
- Conclure.

2.4 Les théorèmes de Sylow

Soit G est un groupe fini d'ordre n, et p un entier premier. On écrit $n = mp^\alpha$, où m n'est pas divisible par p. On appelle *p-sous-groupe de Sylow de G* (ou *p-Sylow de G*) tout sous-groupe de G d'ordre p^α. Ainsi, un p-sous-groupe de Sylow de G est un sous-groupe qui est un p-groupe, et dont l'indice dans G est premier avec p. Notons que si n n'est pas divisible par p, la notion de p-Sylow de G n'a pas grand intérêt ; on requiert donc parfois dans la définition de p-sous-groupe de Sylow que l'entier premier p divise l'ordre du groupe. Mais il est commode de considérer la définition la plus large.

L'existence, le nombre de p-Sylow dans un groupe fini G, et les relations entre ces sous-groupes sont étudiés par les théorèmes de Sylow.

L'exercice qui suit donne un exemple de p-sous-groupe de Sylow, qui sera utilisé dans la preuve du premier théorème de Sylow.

Exercice 2.6 *Soit p un entier premier, et $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. On fixe un entier $n \in \mathbb{N}^*$, et on note G le groupe $GL(n, \mathbb{F}_p)$.*

Calculer l'ordre de G, et montrer que l'ensemble S des matrices triangulaires supérieures dont les coefficients diagonaux sont égaux à 1 constitue un p-sous-groupe de Sylow de G.

Théorème 2.3 (Premier théorème de Sylow) *Si G est un groupe fini et p un entier premier, il existe au moins un p-sous-groupe de Sylow de G.*

Le lemme suivant sera utilisé pour prouver ce théorème. Il montre l'existence d'un p-Sylow dans tout sous-groupe d'un groupe dont on connaît un p-Sylow.

Lemme 2.4 *Soit G un groupe fini, S un p-Sylow de G, et H un sous-groupe de G. Alors il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H.*

Preuve — Faisons opérer H sur G/S par translation à gauche : pour $h \in H$ et $g \in G$, $h.gS \stackrel{\text{déf}}{=} (hg)S$. On vérifie facilement [...] que pour tout $g \in G$, $\mathrm{Stab}(gS) = gSg^{-1} \cap H$. On en déduit

$$|\mathrm{Orb}(gS)| = |H|/|gSg^{-1} \cap H|.$$

Or, les orbites formant une partition de G/S, dont le cardinal n'est pas divisible par p, il existe au moins une orbite dont le cardinal n'est pas multiple de p. On peut donc trouver $g \in G$ tel que le sous-groupe $gSg^{-1} \cap H$ de H soit d'indice premier avec p. Mais par ailleurs, ce sous-groupe est aussi un p-groupe [...]. C'est donc un p-Sylow de H. ❑

Preuve du théorème 2.3 — Si G est un groupe fini d'ordre n, le théorème de Cayley (théorème 1.2) montre que G peut être vu comme un sous-groupe du groupe symétrique $\mathbf{S}_n$. Puis, $\mathbf{S}_n$ est lui-même isomorphe à un sous-groupe de $GL(n, \mathbb{F}_p)$: le sous-groupe des matrices de permutations. G est donc toujours plongeable dans le groupe $GL(n, \mathbb{F}_p)$, dont on sait d'après le résultat de l'exercice 2.6 qu'il admet toujours un p-sous-groupe de Sylow. Le lemme précédent permet alors d'en déduire l'existence d'au moins un p-Sylow dans G. ❏

Théorème 2.5 (Second théorème de Sylow) *Les p-Sylow de G sont deux à deux conjugués, et donc leur nombre k divise n.*

Preuve — Soient S et H deux p-Sylow de G. D'après le lemme 2.4, il existe $g \in G$ tel que $H \cap gSg^{-1}$ soit un p-Sylow de H. Mais comme H est un p-groupe, le seul p-Sylow de H est évidemment H lui-même, donc $H \cap gSg^{-1} = H$, autrement dit $H \subset gSg^{-1}$. Mais H, S, et donc gSg^{-1} ont même cardinal, d'où $H = gSg^{-1}$. H et S sont donc conjugués. Pour montrer que k divise n, il suffit ensuite de remarquer que l'ensemble des p-Sylow de G constitue une orbite pour l'opération de conjugaison de G sur l'ensemble de ses sous-groupes. ❏

Corollaire 2.6 *Un p-Sylow de G est normal dans G si et seulement si il est l'*unique *p-Sylow de G.*

Théorème 2.7 (Troisième théorème de Sylow) *Le nombre k de p-Sylow de G vérifie $k \equiv 1 \pmod p$, et donc k divise m.*

Preuve — Fixons un p-Sylow S de G. S opère par conjugaison sur l'ensemble X de tous les p-Sylow de G. Considérons l'ensemble X^S des p-Sylow de G qui sont fixes par cette opération, *i.e.*

$$X^S \overset{\text{déf}}{=} \left\{T \in X \ / \ \forall s \in S,\ sTs^{-1} = T\right\},$$

et montrons que X^S est réduit à $\{S\}$. Pour cela, prenons $T \in X^S$, et appelons N le sous-groupe de G engendré par S et T. Il est facile de voir que T est normal dans N, puisque les $g \in G$ tels que $gTg^{-1} = G$ constituent un sous-groupe de G qui contient S et T, donc qui contient N. Mais par ailleurs, S et T étant des p-Sylow de G, ce sont *a fortiori* des p-Sylow de N. Le corollaire 2.6 prouve alors que T est l'unique p-Sylow de N, d'où $S = T$.

S est donc l'unique point de X fixe sous l'action de S par conjugaison. Or, comme S est un p-groupe, on sait (voir l'exercice 2.2) que le cardinal de X est congru au nombre de points fixes modulo p, c'est-à-dire

$$k \equiv 1 \pmod p.$$

❏

Une application classique des théorèmes de Sylow consiste à pouvoir affirmer que certains groupes finis ne sont pas simples, rien qu'en voyant leur cardinal.

Exercice 2.7 *Soit G un groupe fini d'ordre n. Montrer que si n est de la forme pq avec p et q premiers distincts, alors G n'est pas simple. Trouver d'autres conditions sur n entraînant qu'aucun groupe d'ordre n ne soit simple.*

Exercice 2.8 *Montrer qu'un groupe d'ordre 300 n'est jamais simple.*

(Indication : *montrer que s'il y a plusieurs 5-Sylow, il y en a exactement 6, et considérer alors l'action de G par conjugaison sur l'ensemble de ces 5-Sylow ; cette action définit un morphisme φ de G dans $\mathbf{S}_6$ et on vérifie alors que $\operatorname{Ker}\varphi$ est un sous-groupe normal non trivial de G.)*

Références

[1] Alain Bouvier et Denis Richard. *Groupes – observation, théorie, pratique.* Hermann, 1994.

[2] Josette Calais. *Éléments de Théorie des Groupes.* Puf, 1998.

[3] Daniel Perrin. *Cours d'Algèbre.* Ellipses, 1996.

[4] J.J. Rotman. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer-Verlag, 1995.