Vincent Beck

Théorème de Cayley

Le (ou plutôt un des nombreux) théorème(s) de Cayley assure que tout groupe G s'identifie de façon naturelle à un sous-groupe du groupe $\mathfrak{S}_{\mathrm{G}}$ des bijections de G. En particulier, lorsque G est fini, G est isomorphe à un sous-groupe d'un $\mathfrak{S}_n$, par exemple pour $n = |\mathrm{G}|$. Ce théorème de Cayley est un résultat abstrait : un peu affaibli, il dit simplement que tout groupe est un sous-groupe du groupe des permutations d'un ensemble. Ainsi le théorème de Cayley ne permet d'obtenir que quelques résultats généraux de théorie des groupes : par exemple, les théorèmes de Sylow (voir [PER, I.5]) ou quelques propriétés liées à la simplicité (voir le corollaire 6). Cependant, il n'est d'aucune utilité pour obtenir des informations sur la structure d'un groupe particulier : ordres des éléments, nombre de sous-groupes, classes de conjugaison, etc. Par exemple, lorsqu'on veut étudier les groupes d'ordre 12, on n'est pas très avancé de savoir qu'ils peuvent s'injecter dans $\mathfrak{S}_{12}$ puisqu'on est passé de l'étude des groupes d'ordre 12 à celle d'un groupe (certes un seul mais) d'ordre 479001600 (voir aussi la remarque 4).

Cette note consacrée au théorème de Cayley est divisée en quatre parties. Dans la première partie, on construit le « morphisme de Cayley » c qui permet d'identifier G à un sous-groupe de $\mathfrak{S}_{\mathrm{G}}$ (voir la preuve du lemme 1). Toujours dans la première partie, on étudie ensuite quelques propriétés, liées au fait qu'on arrive dans un groupe symétrique, de l'image d'un élément de G par ce morphisme c (décomposition en cycles à support disjoint et signature). Cette étude mène à la non-cyclicité du 2-Sylow d'un groupe simple (voir le corollaire 6). Les trois parties qui suivent sont consacrées à la problématique suivante : « le théorème de Cayley affirme qu'un groupe fini G donné s'injecte dans un des $\mathfrak{S}_n$; quel est, pour le groupe G, le plus petit entier n qui convient ? » La deuxième partie étudie le cas des groupes d'ordre 1 à 11. Dans la troisième partie, on étudie le cas des groupes cycliques. Enfin dans la quatrième et dernière partie, on traite le cas des groupes diédraux comme conséquence de l'étude des groupes cycliques.

Étude du morphisme de Cayley.

Commençons par donner la construction du morphisme qui permet l'identification d'un groupe à un sous-groupe d'un groupe de permutations.

Lemme 1 — Théorème de Cayley. Soit G un groupe. Il existe un morphisme injectif $c : \mathrm{G} \to \mathfrak{S}_{\mathrm{G}}$.

Preuve. On fait agir G sur lui-même par translation à gauche : l'application qui définit cette action est (avec $\mathrm{X} = \mathrm{G}$)

$$\begin{cases} \mathrm{G} \times \mathrm{X} \longrightarrow \mathrm{X} \\ (g, h) \longmapsto gh\,. \end{cases}$$

À chaque action de groupes est associé un morphisme de groupes issu du groupe qui agit et à valeurs dans le groupe des permutations de l'ensemble sur lequel G agit (pour de plus amples détails à ce sujet, voir la note « action de groupe »). Le morphisme associé à notre action est

$$c\colon \begin{cases} \mathrm{G} \longrightarrow \mathfrak{S}_{\mathrm{X}} = \mathfrak{S}_{\mathrm{G}} \\ g \longmapsto (h \mapsto gh)\,. \end{cases}$$

On dit que c est le *morphisme de Cayley de* G. Montrons que c est injectif. Pour cela, on considère $g \in \operatorname{Ker} c$. L'application $h \mapsto gh$ est donc l'identité de G. Autrement dit, $gh = h$ pour tout $h \in \mathrm{G}$. En particulier avec $h = 1_{\mathrm{G}}$, on obtient $g = 1_{\mathrm{G}}$ et c est injective. Ainsi $c(\mathrm{G})$ est un sous-groupe de $\mathfrak{S}_{\mathrm{G}}$ isomorphe à G. ■

Remarque 2 — Principe de Cayley. Le principe développé dans le théorème 1 s'étend à d'autres situations. Par exemple, soit k un corps (commutatif), toute k-algèbre (associative unitaire) A de dimension finie sur k « est » une sous-algèbre d'une algèbre de matrices. Il suffit pour cela de montrer que l'application

$$\varphi\colon \begin{cases} \mathrm{A} \longrightarrow \operatorname{End}_k(\mathrm{A}) = \mathrm{M}_{\dim \mathrm{A}}(k) \\ x \longmapsto (y \mapsto xy) \end{cases}$$

est un morphisme injectif de k-algèbres unitaires. L'injectivité de φ résulte du fait que A est unitaire : si les applications $y \mapsto xy$ et $y \mapsto x'y$ sont égales, leur valeur en 1_{A} le sont aussi et donc $x = x'$. Le fait que φ soit un morphisme de k-algèbres unitaires résulte des axiomes de définition des k-algèbres unitaires : par exemple le fait que $\varphi(xx') = \varphi(x)\varphi(x')$ s'obtient par l'associativité du produit de A, le fait que $\varphi(1_{\mathrm{A}}) = \mathrm{id}_{\mathrm{A}}$ résulte de la définition de 1_{A}, enfin la k-linéarité de φ résulte de la distributivité du produit. ■

Étudions, à présent, de plus près l'image $c(g)$ d'un élément g du groupe G.

Proposition 3 — Décomposition en cycles à support disjoint. Soient G un groupe fini, $g \in \mathrm{G}$ et $c : \mathrm{G} \to \mathfrak{S}_{\mathrm{G}}$ le morphisme de Cayley de G. La décomposition en cycles à support disjoint de $c(g)$ est formée par $|\langle g \rangle \backslash \mathrm{G}|$ cycles de longueurs $|\langle g \rangle|$.

Preuve. Par définition, pour déterminer la décomposition en cycles à support disjoint de $c(g)$, il s'agit de trouver les orbites du sous-groupe $\langle c(g) \rangle$ de $\mathfrak{S}_{\mathrm{G}}$ dans son action naturelle sur G (voir []). Toujours par définition, pour $h \in \mathrm{G}$, l'orbite de h sous $\langle c(g) \rangle$ est

$$\left\{ c(g)^k(h), \quad k \in \mathbb{Z} \right\}.$$

Comme c est un morphisme de groupes, on a $c(g)^k = c(g^k)$. De plus, $c(g^k)(h) = g^k h$. Ainsi l'orbite de h sous $\langle c(g) \rangle$ est $\left\{ g^k h, \ k \in \mathbb{Z} \right\} = \langle g \rangle h$. Ainsi l'orbite de $h \in \mathrm{G}$ sous $\langle c(g) \rangle$ n'est rien d'autre que la classe à droite de h modulo $\langle g \rangle$ (voir []). En particulier, elle a $|\langle g \rangle|$ éléments. On en déduit alors qu'il y a $|\langle g \rangle \backslash \mathrm{G}| = |\mathrm{G}|/|\langle g \rangle|$ orbites. ■

Remarque 4 — Décomposition en cycles à support disjoint et ordre des éléments. La décomposition en cycles à support disjoint de $c(g)$ ne dépend que de l'ordre de g. Ainsi deux éléments g, g' de G qui ont même ordre vont avoir le même type de décomposition en cycles à support disjoint c'est-à-dire que pour toutes les longueurs (en fait il n'y en a qu'une qui intervient), $c(g)$ et $c(g')$ ont autant de cycles de cette longueur dans leur décomposition en cycles à support disjoint. En particulier, les éléments $c(g)$ et $c(g')$ se retrouvent conjugués dans $\mathfrak{S}_{\mathrm{G}}$ (voir [BPM, exercice 6.7 questions a et b]).

On voit ici un exemple d'informations qu'on perd en plongeant G dans un groupe plus grand : deux éléments qui ont même ordre mais qui ne sont pas conjugué dans le groupe G ont leur image qui sont conjuguées dans le groupe $\mathfrak{S}_{\mathrm{G}}$. Ainsi, on ne peut plus différentier les deux éléments dans le grand groupe $\mathfrak{S}_{\mathrm{G}}$.

Par exemple, dans le groupe quaternionique $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$, les éléments i et j ne sont pas conjugués mais sont tous les deux d'ordre 4. ■

Corollaire 5 — Signature, groupe alterné et morphisme de Cayley. Soient G un groupe fini, $g \in \mathrm{G}$ et $c : \mathrm{G} \to \mathfrak{S}_{\mathrm{G}}$ le morphisme de Cayley de G. La signature $\varepsilon(c(g))$ de $c(g)$ est donnée par

$$\varepsilon(c(g)) = (-1)^{|\mathrm{G}| - |\langle g \rangle \backslash \mathrm{G}|} = (-1)^{(|\langle g \rangle| + 1)|\langle g \rangle \backslash \mathrm{G}|}.$$

En particulier, le morphisme de Cayley de G est en fait à valeurs dans $\mathfrak{A}_{\mathrm{G}}$ sauf si les 2-Sylow de G sont cycliques et non réduits à $\{1_{\mathrm{G}}\}$.

Preuve. La première écriture résulte de l'expression de la signature d'un élément σ de $\mathfrak{S}_n$ sous la forme $(-1)^{n-m}$ où m est le nombre d'orbite de σ (voir [RDO1, 2.4.3] et la remarque 6 de la note « Signature et corps fini »). La deuxième écriture résulte de la décomposition en cycles à support disjoint : la signature d'un cycle de longueur ℓ est $(-1)^{\ell+1}$.

Supposons que les 2-Sylow de G sont triviaux c'est-à-dire réduits à $\{1_{\mathrm{G}}\}$. Les théorèmes de Sylow assurent que $|\mathrm{G}|$ est impair. Le théorème de Lagrange (voir [PER, I.0.1]) assure que $|\langle g \rangle|$ est impair et donc $|\langle g \rangle| + 1$ est pair. Ainsi

$$\varepsilon(c(g)) = (-1)^{(|\langle g \rangle| + 1)|\langle g \rangle \backslash \mathrm{G}|} = 1$$

pour tout $g \in \mathrm{G}$ c'est-à-dire que c est à valeurs dans $\mathfrak{A}_{\mathrm{G}}$.

Supposons que les 2-Sylow de G sont non triviaux mais non cycliques. Pour $g \in \mathrm{G}$, montrons que le groupe $\langle g \rangle$ ne contient pas de 2-Sylow de G (en particulier, n'est pas un 2-Sylow de G). En effet, si $\langle g \rangle$ contient un 2-Sylow de G alors ce 2-Sylow de G est un sous-groupe d'un groupe cyclique (le groupe $\langle g \rangle$) et donc est cyclique ce qui contredit l'hypothèse (voir []). Un 2-Sylow de $\langle g \rangle$ a donc strictement moins d'éléments qu'un 2-Sylow de G (si ce n'était pas le cas, un 2-Sylow de $\langle g \rangle$ serait aussi un 2-Sylow de G et on a vu que c'était impossible). Ainsi, $|\langle g \rangle \backslash \mathrm{G}|$ est pair et

$$\varepsilon(c(g)) = (-1)^{(|\langle g \rangle| + 1)|\langle g \rangle \backslash \mathrm{G}|} = 1$$

pour tout $g \in \mathrm{G}$ c'est-à-dire que c est à valeurs dans $\mathfrak{A}_{\mathrm{G}}$.

Supposons que les 2-Sylow de G sont cycliques et non triviaux. On considère g tel que $\langle g \rangle$ soit un 2-Sylow de G. Comme le 2-Sylow n'est pas trivial, $|\langle g \rangle| + 1$ est impair. Comme $\langle g \rangle$ est un 2-Sylow, $|\langle g \rangle \backslash \mathrm{G}|$ est impair. Finalement,

$$\varepsilon(c(g)) = (-1)^{(|\langle g \rangle| + 1)|\langle g \rangle \backslash \mathrm{G}|} = -1.$$

et $c(g) \notin \mathfrak{A}_{\mathrm{G}}$. ■

Corollaire 6 — Simplicité et morphisme de Cayley. Soit G un groupe fini simple non isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Les 2-Sylow de G (s'ils sont non triviaux) ne sont pas cycliques.

En particulier, un groupe d'ordre $2n$ avec $n \neq 1$ impair n'est pas simple.

Preuve. Montrons pour commencer que $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ est un sous-groupe distingué de $c(\mathrm{G})$ d'indice 1 ou 2. Comme $\mathfrak{A}_{\mathrm{G}}$ est un sous-groupe distingué de $\mathfrak{S}_{\mathrm{G}}$, on en déduit que $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ est un sous-groupe distingué de $c(\mathrm{G})$ (c'est l'image réciproque du sous-groupe distingué $\mathfrak{A}_{\mathrm{G}}$ de $\mathfrak{S}_{\mathrm{G}}$ par l'inclusion de $c(\mathrm{G})$ dans $\mathfrak{S}_{\mathrm{G}}$ et l'image réciproque d'un sous-groupe distingué par un morphisme de groupes est toujours un sous-groupe distingué ; voir [CAL]). Intéressons-nous maintenant à l'indice de $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ dans $c(\mathrm{G})$. On note $\pi : \mathfrak{S}_{\mathrm{G}} \to \mathfrak{S}_{\mathrm{G}}/\mathfrak{A}_{\mathrm{G}}$ la surjection canonique et on considère le morphisme $\pi_1 : c(\mathrm{G}) \to \mathfrak{S}_{\mathrm{G}}/\mathfrak{A}_{\mathrm{G}}$ la restriction de π à $c(\mathrm{G})$. Bien sûr, $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ est contenu dans $\operatorname{Ker} \pi_1$. Ainsi par la propriété universelle du quotient (voir [CAL, Théorème 4.25 Chapitre 4.4.A]), on obtient, par factorisation, un morphisme de groupes $i : c(\mathrm{G})/\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G}) \to \mathfrak{S}_{\mathrm{G}}/\mathfrak{A}_{\mathrm{G}}$. Mais $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ n'est pas seulement contenu dans le noyau π_1, c'est exactement le noyau de π_1, on en déduit que i est injectif (le noyau de i est $\operatorname{Ker} \pi_1/\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$). Ainsi $c(\mathrm{G})/\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ s'identifie à un sous-groupe du groupe à deux éléments $\mathfrak{S}_{\mathrm{G}}/\mathfrak{A}_{\mathrm{G}}$.

Supposons que les 2-Sylow de G sont cycliques et non triviaux. On en déduit, grâce au corollaire 5 que $c(\mathrm{G})$ n'est pas contenu dans $\mathfrak{A}_{\mathrm{G}}$. Ainsi $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G}) \neq c(\mathrm{G})$ et donc $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G})$ est un sous-groupe distingué d'indice 2 de $c(\mathrm{G})$. Or $c(\mathrm{G})$ est simple puisqu'isomorphe (via c) à G. Ainsi $\mathfrak{A}_{\mathrm{G}} \cap c(\mathrm{G}) = \{1\}$ et $c(\mathrm{G})$ et G sont de cardinal 2 ce qui contredit l'hypothèse.

Supposons que G soit un groupe vérifiant $|\mathrm{G}| = 2n$ avec $n \neq 1$ et n impair. Comme $n \neq 1$ et n impair, G a strictement plus que 2 éléments et n'est donc pas isomorphe $\mathbb{Z}/2\mathbb{Z}$. Par ailleurs, puisque n est impair, un 2-Sylow de G a pour cardinal 2 et est donc cyclique. Le premier résultat du corollaire montre que G n'est pas simple. ■

Application 7 — Groupe d'ordre 150. Le corollaire 6 assure qu'un groupe d'ordre $150 = 2 \cdot 3 \cdot 5^2 = 2 \cdot 75$ n'est pas simple ce qui n'est pas si évident à obtenir en utilisant uniquement les méthodes classiques reposant sur les théorèmes de Sylow. ■

Remarque 8 — Simplicité, résolubilité et 2-Sylow. Soit G un groupe (non nécessairement fini). Pour H, K deux sous-groupes de G, on note $[\mathrm{H}, \mathrm{K}]$ le sous-groupe engendré par les éléments de la forme $hkh^{-1}k^{-1}$ pour $h \in \mathrm{H}$ et $k \in \mathrm{K}$. On définit ensuite par récurrence la suite dérivée de G en posant $\mathrm{D}^0(\mathrm{G}) = \mathrm{G}$ et $\mathrm{D}^{i+1}(\mathrm{G}) = [\mathrm{D}^i\mathrm{G}, \mathrm{D}^i\mathrm{G}]$ pour $i \geqslant 0$ (voir []).

La suite $(\mathrm{D}^i(\mathrm{G}))_{i \in \mathbb{N}}$ est une suite décroissante de sous-groupe de G. On montre par récurrence que $\mathrm{D}^i(\mathrm{G})$ est un sous-groupe distingué (et même caractéristique c'est-à-dire stable par tout automorphisme de G et pas seulement par les automorphismes intérieurs) de G (voir []).

Le groupe G est dit *résoluble* s'il existe $n \in \mathbb{N}$ tel que $\mathrm{D}^n(\mathrm{G}) = 1_{\mathrm{G}}$ (voir []). Un groupe abélien est résoluble puisque $\mathrm{D}^1(\mathrm{G}) = \{1_{\mathrm{G}}\}$. En fait, on a l'équivalence $\mathrm{D}^1(\mathrm{G}) = \{1_{\mathrm{G}}\}$ si et seulement si G est abélien. Bien entendu, il existe des groupes résolubles qui ne sont pas abéliens. Par exemple, le groupe $\mathfrak{S}_3$ est résoluble mais n'est pas abélien : on a $\mathrm{D}^1(\mathrm{G}) = \mathfrak{A}_3 \neq \left\{\mathrm{id}_{\{1,2,3\}}\right\}$ et $\mathrm{D}^2(\mathrm{G}) = \left\{\mathrm{id}_{\{1,2,3\}}\right\}$ puisque $\mathfrak{A}_3$ est abélien.

Pour un groupe simple, montrons l'équivalence entre G est abélien et G est résoluble. On a vu qu'un groupe abélien est toujours résoluble. Montrons qu'un groupe résoluble simple G est abélien. Comme G est résoluble, on a $\mathrm{D}^1(\mathrm{G}) \neq \mathrm{G}$. En effet, si $\mathrm{D}^1(\mathrm{G}) = \mathrm{G}$ alors, par récurrence, on obtient que $\mathrm{D}^i(\mathrm{G}) = \mathrm{G}$ pour tout $i \in \mathbb{N}$ et donc $\mathrm{G} = \{1_{\mathrm{G}}\}$ par résolubilité. Ceci contredit la simplicité : par convention, le groupe $\{1\}$ n'est pas simple. Ainsi $\mathrm{D}^1(\mathrm{G})$ est un sous-groupe distingué et strict du groupe simple G. On a donc $\mathrm{D}^1(\mathrm{G}) = \{1_{\mathrm{G}}\}$ par simplicité. Finalement G est abélien.

Étudions à présent les groupes abéliens simples et montrons qu'il s'agit des (groupes isomorphes à) $\mathbb{Z}/p\mathbb{Z}$ pour $p \in \mathscr{P}$ où $\mathscr{P}$ désigne l'ensemble des nombres premiers. Considérons donc un groupe simple abélien G. Comme G est abélien, tous les sous-groupes de G sont distingués. Ainsi G n'a que deux sous-groupes $\{1_{\mathrm{G}}\}$ et G. Finalement, pour $x \in \mathrm{G} \smallsetminus \{1_{\mathrm{G}}\}$, le sous-groupe $\langle x \rangle$ engendré par x est égal à G. On en déduit que G est monogène. Si x est d'ordre infini alors $\mathrm{G} \overset{\text{gr.}}{\simeq} \mathbb{Z}$ et n'est pas simple puisque $2\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Z}$ distinct de $\{0\}$ et $\mathbb{Z}$. Si x est d'ordre fini alors G est un groupe cyclique (fini). On note n son ordre. Les sous-groupes de G sont alors en bijection avec les diviseurs de n (voir []). Ainsi, puisque G est simple, n ne doit avoir que deux diviseurs : 1 et lui-même c'est-à-dire que n est premier. Les groupes simples abéliens sont appelés les *groupes simples triviaux* (bien que ce ne soit pas des groupes triviaux c'est-à-dire réduit à un élément).

Des deux paragraphes précédents, on en déduit que les groupes simples résolubles sont les (groupes isomorphes à) $\mathbb{Z}/p\mathbb{Z}$ pour $p \in \mathscr{P}$. Par ailleurs, un très difficile théorème de Feit et Thompson (voir [F-T]) montre que les groupes d'ordre impairs sont tous résolubles. Ainsi un groupe simple d'ordre impair est nécessairement isomorphe à $\mathbb{Z}/p\mathbb{Z}$ pour $p \in \mathscr{P} \smallsetminus \{2\}$. On en déduit aussi qu'un groupe simple non abélien n'est pas résoluble et donc d'ordre pair. En particulier, son 2-Sylow n'est pas trivial et donc, grâce au corollaire 6, n'est pas cyclique.

Pour illustrer ces propriétés sur les 2-Sylow des groupes simples, on peut calculer les 2-Sylow de $\mathfrak{A}_5$ qui sont au nombre de 5 et de cardinal 4. Ce sont les groupes suivants

$$\mathrm{S}_5 = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}, \qquad \mathrm{S}_4 = \{\mathrm{id},\ (1,2)(3,5),\ (1,3)(2,5),\ (1,5)(2,3)\},$$

$$\mathrm{S}_3 = \{\mathrm{id},\ (1,2)(5,4),\ (1,5)(2,4),\ (1,4)(2,5)\}, \qquad \mathrm{S}_2 = \{\mathrm{id},\ (1,5)(3,4),\ (1,3)(5,4),\ (1,4)(5,3)\}$$

et $$\mathrm{S}_1 = \{\mathrm{id},\ (5,2)(3,4),\ (5,3)(2,4),\ (5,4)(2,3)\}\ .$$
On constate bien qu'ils ne sont pas cycliques : ils ne contiennent pas d'élément d'ordre 4 mais sont isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$. ■

Inclusion minimale : exemples

Le théorème 1 de Cayley dit qu'un groupe d'ordre n s'injecte dans $\mathfrak{S}_n$. Dans cette partie et les deux qui suivent, on se pose la question de savoir, étant donné un groupe G, quel est le plus petit m tel que G s'injecte dans $\mathfrak{S}_m$. Cette partie est consacrée à l'étude d'exemples concrets : les groupes d'ordre 1 à 11. Pour ces exemples concrets de groupes G, on détermine non seulement le plus petit entier m tel que $\mathfrak{S}_m$ contienne G mais aussi le nombre d'injections de G dans $\mathfrak{S}_{m_{\min}}$. Pour mener cette étude, on utilise les propriétés des groupes symétriques (essentiellement $\mathfrak{S}_3$, $\mathfrak{S}_4$ et $\mathfrak{S}_5$), les théorèmes de Sylow et la classification des groupes d'ordre 1 à 11.

Exemple 9 — Groupe d'ordre 1. Un groupe d'ordre 1 est réduit à l'élément neutre. Il s'injecte donc dans $\mathfrak{S}_0 = \mathfrak{S}_1 = \{1\}$. Il n'y a qu'une seule telle inclusion et c'est un isomorphisme. ■

Exemple 10 — Groupe d'ordre 2. Un groupe d'ordre 2 est cyclique, isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (car 2 est premier). Il est donc isomorphe à $\mathfrak{S}_2$ qui a aussi 2 éléments. De plus, il n'y a qu'une seule inclusion d'un groupe d'ordre 2 dans $\mathfrak{S}_2$ et c'est un isomorphisme. Bien entendu, un groupe d'ordre 2 ne s'injecte pas dans $\mathfrak{S}_1 = \mathfrak{S}_0$ puisque $|\mathfrak{S}_0| = |\mathfrak{S}_1| = 1 < 2$. ■

Exemple 11 — Groupe d'ordre 3. Un groupe d'ordre 3 est cyclique, isomorphe à $\mathbb{Z}/3\mathbb{Z}$ (car 3 est premier). D'après le théorème 1 de Cayley, il s'injecte dans $\mathfrak{S}_3$. Il y a deux telles inclusions. On fixe un générateur du groupe G d'ordre 3 et on l'envoie au choix sur l'un des deux cycles d'ordre 3 de $\mathfrak{S}_3$: $(1,2,3)$ ou $(1,3,2)$ (voir le lemme 25). Comme les 3-cycles sont conjugués dans $\mathfrak{S}_3$, ces deux inclusions diffèrent d'un automorphisme intérieur de $\mathfrak{S}_3$: si i et j sont les deux inclusions, on a $i = c \circ j$ où c est un automorphisme intérieur de $\mathfrak{S}_3$ (c'est-à-dire que, quitte à effectuer une renumérotation, c'est la même inclusion). Comme pour $i < 3$, on a $|\mathfrak{S}_i| < 3$, un groupe d'ordre 3 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 3$. ■

Exemple 12 — Groupe d'ordre 4. D'après le théorème 1 de Cayley, un groupe d'ordre 4 s'injecte dans $\mathfrak{S}_4$. De plus, comme pour $i < 4$, on a $4 \nmid |\mathfrak{S}_i|$, le théorème de Lagrange assure qu'un groupe d'ordre 4 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 4$.

Soit G un groupe d'ordre 4. Le groupe G est cyclique ou isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

Considérons dans un premier temps le cas d'un groupe cyclique G d'ordre 4. Le nombre d'inclusion de G dans $\mathfrak{S}_4$ est alors le nombre d'élément d'ordre 4 dans $\mathfrak{S}_4$ (voir le lemme 25). Or la description des éléments d'ordre 4 de $\mathfrak{S}_4$ assure qu'un élément d'ordre 4 est un 4-cycle et qu'il y en a 6 qui sont conjugués. Ainsi il y a 6 injections de G dans $\mathfrak{S}_4$ qui ne diffèrent que d'un automorphisme intérieur de $\mathfrak{S}_4$.

Étudions à présent le cas où $\mathrm{G} \overset{\text{gr.}}{\simeq} (\mathbb{Z}/2\mathbb{Z})^2$. La description des sous-groupes d'ordre 4 de $\mathfrak{S}_4$ montre que G s'identifie à l'un des sous-groupes
$$\{\mathrm{id},\ (1,2),\ (3,4),\ (1,2)(3,4)\}\,,\qquad \{\mathrm{id},\ (1,3),\ (2,4),\ (1,3)(2,4)\}\,,\qquad \{\mathrm{id},\ (1,4),\ (2,3),\ (1,4)(2,3)\}$$
ou $$\mathrm{V}_4 = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}\,.$$
Les trois premiers sous-groupes sont conjugués et le dernier est distingué dans $\mathfrak{S}_4$.

Par ailleurs, le nombre d'isomorphismes de G dans $(\mathbb{Z}/2\mathbb{Z})^2$ est le nombre d'automorphismes de $(\mathbb{Z}/2\mathbb{Z})^2$ c'est-à-dire 6 (voir la remarque 11 de la note « Action de groupes »). On a donc 24 inclusions. De plus, d'après la proposition 3, le morphisme de Cayley correspond à l'une des 6 inclusions dans V_4. ■

Exemple 13 — Groupe d'ordre 5. Un groupe d'ordre 5 est cyclique isomorphe à $\mathbb{Z}/5\mathbb{Z}$ (car 5 est premier). D'après le théorème 1 de Cayley, il s'injecte dans $\mathfrak{S}_5$. D'après le lemme 25, il y a autant d'injections d'un groupe d'ordre 5 dans $\mathfrak{S}_5$ que d'éléments d'ordre 5 dans $\mathfrak{S}_5$. Or les éléments d'ordre 5 de $\mathfrak{S}_5$ sont les 5-cycles qui sont au nombre de 24. Ainsi, il y a 24 injections d'un groupe d'ordre 5 dans $\mathfrak{S}_5$. De plus, comme les 5-cycles sont conjugués dans $\mathfrak{S}_5$, ces deux inclusions diffèrent d'un automorphisme intérieur de $\mathfrak{S}_5$. Par ailleurs, comme pour $i < 5$, on a $5 \nmid |\mathfrak{S}_i|$, un groupe d'ordre 5 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 5$ (voir aussi la proposition 26). ■

Exemple 14 — Groupe d'ordre 6. Un groupe d'ordre 6 est cyclique ou isomorphe à $\mathfrak{S}_3$.

Commençons par le cas d'un groupe cyclique d'ordre 6. L'élément $(1,2,3)(4,5)$ de $\mathfrak{S}_5$ est un élément d'ordre 6. Ainsi un groupe cyclique d'ordre 6 s'injecte dans $\mathfrak{S}_5$ (voir le lemme 25). Les éléments d'ordre 6 de $\mathfrak{S}_5$ ont tous le même type de décomposition en cycles à support disjoint : ce sont des produits d'un 3-cycle et d'une transposition. Il y en a 20. On a ainsi 20 injections d'un groupe cyclique d'ordre 6 dans $\mathfrak{S}_5$. Par ailleurs, un groupe cyclique d'ordre 6 ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 5$ puisque $\mathfrak{S}_i$ n'a pas d'élément d'ordre 6 (les

éléments de $\mathfrak{S}_2$ sont d'ordre 1 ou 2 ; les éléments de $\mathfrak{S}_3$ sont d'ordre 1, 2 ou 3 ; les éléments de $\mathfrak{S}_3$ sont d'ordre 1, 2, 3 ou 4). Ce résultat découle aussi de la proposition 26.

Le groupe $\mathfrak{S}_3$ s'injecte dans $\mathfrak{S}_3$. Le nombre d'injections de $\mathfrak{S}_3$ dans lui-même est le nombre d'automorphismes de $\mathfrak{S}_3$ c'est-à-dire 6 (voir []). Bien entendu, $\mathfrak{S}_3$ ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 3$ puisque $6 > |\mathfrak{S}_i|$. Comme le groupe diédral D_3 et $\mathfrak{S}_3$ sont isomorphes, ce résultat découle aussi du corollaire 28. ■

Exemple 15 — Groupe d'ordre 7. Un groupe d'ordre 7 est cyclique isomorphe à $\mathbb{Z}/7\mathbb{Z}$ (car 7 est premier). D'après le théorème 1 de Cayley, il s'injecte dans $\mathfrak{S}_7$. D'après le lemme 25, il y a autant d'injections d'un groupe d'ordre 7 dans $\mathfrak{S}_7$ que d'éléments d'ordre 7 dans $\mathfrak{S}_7$. Or les éléments d'ordre 7 de $\mathfrak{S}_7$ sont les 7-cycles qui sont au nombre de $(7-1)! = 6! = 720$. Ainsi, il y a 720 injections d'un groupe d'ordre 7 dans $\mathfrak{S}_7$. De plus, comme les 7-cycles sont conjugués dans $\mathfrak{S}_7$, ces deux inclusions diffèrent d'un automorphisme intérieur de $\mathfrak{S}_7$. Par ailleurs, comme pour $i < 7$, on a $7 \nmid |\mathfrak{S}_i|$, un groupe d'ordre 7 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 7$ (voir aussi la proposition 26). ■

Exemple 16 — Groupe d'ordre 8. Un groupe d'ordre 8 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$, $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, D_4 ou $\mathbb{H}_8$.

Pour étudier, le cas des groupes d'ordre 8, on va utiliser un point de vue différent de celui des exemples précédents. Comme 8 est une puissance de 2, un sous-groupe d'ordre 8 d'un $\mathfrak{S}_m$ est nécessairement contenu dans un 2-Sylow de $\mathfrak{S}_m$ (voir []). Il s'agit donc d'étudier les 2-Sylow des groupes symétriques de 1 à 8 (le théorème 1 de Cayley assure qu'il suffit d'aller jusqu'à 8).

Pour $i < 4$, on a $8 \nmid |\mathfrak{S}_i|$. Ainsi, un groupe d'ordre 8 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 4$.

Pour $i = 4$, on a $|\mathfrak{S}_4| = 8 \cdot 3$. Ainsi, les 2-Sylow de $\mathfrak{S}_4$ sont d'ordre 8. En particulier, il existe des sous-groupes d'ordre 8 dans $\mathfrak{S}_4$. De plus, ils sont tous conjugués (dans $\mathfrak{S}_4$) et donc isomorphes. Les groupes d'ordre 8 qui s'injectent dans $\mathfrak{S}_4$ sont donc nécessairement isomorphes à l'un des 2-Sylow de $\mathfrak{S}_4$. Il s'agit à présent de déterminer duquel des 5 groupes ci-dessus il s'agit. On va montrer que c'est D_4 en faisant agir D_4 sur un ensemble à 4 éléments. Par définition D_4 est le groupe des isométries du carré. Ainsi D_4 agit donc de façon naturelle sur les 4 sommets du carré $(1, i, -1, -i)$ (qu'on numérote $\{1, 2, 3, 4\}$). On en déduit (voir la note « Action de groupe ») un morphisme de groupes φ de D_4 dans $\mathfrak{S}_4$. Montrons que φ est injectif. On considère donc $g \in \mathrm{D}_4$ tel que $\varphi(g)(\ell) = \ell$ pour tout $\ell \in [\![1\,,\, 4]\!]$. Comme les isométries sont affines (voir []), elles conservent le barycentre des 4 sommets, c'est-à-dire l'origine. Ainsi, g est $\mathbb{R}$-linéaire. De plus, par construction de φ, on a $\varphi(g)(\ell) = g(i^{\ell-1})$. Ainsi g est $\mathbb{R}$-linéaire et envoie 1 sur 1 et i sur i. On en déduit que $g = \mathrm{id}_{\mathbb{R}^2}$ et φ est injective. Les 2-Sylow de $\mathfrak{S}_4$ sont donc isomorphes à D_4. La description géométrique donnée par l'action sur le carré permet alors de décrire immédiatement les éléments d'un 2-Sylow de $\mathfrak{S}_4$:

$$\mathrm{S} = \{\mathrm{id},\ (1,3),\ (2,4),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,2,3,4),\ (1,3)(2,4),\ (1,4,3,2)\}$$

qui sont respectivement, l'identité, les réflexions par rapport aux droites passant par les sommets opposés, les réflexions par rapport aux droites passant par les milieux des cotés opposés, les rotations d'angles $\pi/2$, π et $3\pi/2$. Par ailleurs, en changeant la numérotation des sommets du carré, on obtient deux autres 2-Sylow

$$\mathrm{S}' = \{\mathrm{id},\ (1,2),\ (3,4),\ (1,3)(2,4),\ (1,4)(2,3),\ (1,3,2,4),\ (1,2)(3,4),\ (1,4,2,3)\}$$

et

$$\mathrm{S}'' = \{\mathrm{id},\ (1,4),\ (2,3),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,2,4,3),\ (1,4)(2,3),\ (1,3,4,2)\}\,.$$

De plus, les théorèmes de Sylow assurent qu'il y a 1 ou 3 2-Sylow dans $\mathfrak{S}_4$. Il y en a donc 3 et on les a entièrement décrits.

Remarques autour des 2-Sylow de $\mathfrak{S}_4$. Les théorèmes de Sylow assurent que tout 2-sous-groupe de $\mathfrak{S}_4$ est contenu dans un 2-Sylow. En particulier, on vérifie bien que tous les éléments d'ordre 2 (les 6 transpositions et les 3 double-transpositions) ou 4 (les 6 4-cycles) de $\mathfrak{S}_4$ sont contenus dans un des 2-Sylow de $\mathfrak{S}_4$. De plus, le fait que les p-Sylow d'un groupe G soient conjugués et qu'un p-sous-groupe de G soit toujours contenu dans un des p-Sylow de G assurent qu'un p-sous-groupe de G qui est distingué dans G est contenu dans tous les p-Sylow de G. Ici, le groupe $\mathrm{V}_4 = \{\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\}$ est distingué dans $\mathfrak{S}_4$ et est bien contenu dans les 3 2-Sylow de $\mathfrak{S}_4$.

Pour $i = 5$, on a $|\mathfrak{S}_5| = 8 \cdot 15$. Ainsi, les 2-Sylow de $\mathfrak{S}_5$ sont d'ordre 8. En particulier, il existe des sous-groupes d'ordre 8 dans $\mathfrak{S}_5$. De plus, ils sont tous conjugués (dans $\mathfrak{S}_5$) et donc isomorphes. Les groupes d'ordre 8 qui s'injectent dans $\mathfrak{S}_5$ sont donc nécessairement isomorphes à l'un des 2-Sylow de $\mathfrak{S}_5$. De plus, $\mathfrak{S}_4$ est contenu dans $\mathfrak{S}_5$. Ainsi, par cardinalité un 2-Sylow de $\mathfrak{S}_4$ est aussi un 2-Sylow de $\mathfrak{S}_5$. Les 2-Sylow de $\mathfrak{S}_5$ sont donc, comme ceux de $\mathfrak{S}_4$ isomorphes à D_4. Ainsi aucun des 4 autres groupes d'ordre 8 n'est contenu dans $\mathfrak{S}_5$.

Remarques autour des 2-Sylow de $\mathfrak{S}_5$. Les théorèmes de Sylow assurent qu'il y a 1, 3, 5 ou 15 2-Sylow dans $\mathfrak{S}_5$. On sait qu'il y en a 3 dans $\mathfrak{S}_4$ qui est contenu $\mathfrak{S}_5$. Ainsi, il y a au moins 3 2-Sylow dans $\mathfrak{S}_5$. En considérant alors les sous-groupes $\mathfrak{S}_{\{2,3,4,5\}}$, $\mathfrak{S}_{\{1,3,4,5\}}$, $\mathfrak{S}_{\{1,2,4,5\}}$ et $\mathfrak{S}_{\{1,2,3,5\}}$ de $\mathfrak{S}_5$, on obtient les 15 2-Sylow de $\mathfrak{S}_5$.

Pour $i = 6$, on a $|\mathfrak{S}_5| = 16 \cdot 45$. Ainsi, les 2-Sylow de $\mathfrak{S}_6$ sont d'ordre 16. De plus, $\mathfrak{S}_4$ est contenu dans $\mathfrak{S}_6$. On considère alors S un 2-Sylow de $\mathfrak{S}_4$; comme $\{5, 6\} \cap \{1, 2, 3, 4\} = \varnothing$, l'ensemble $\mathrm{G} = \mathrm{S} \cup \mathrm{S}(5, 6)$ est

un sous-groupe de $\mathfrak{S}_6$ d'ordre 16 c'est-à-dire un 2-Sylow de $\mathfrak{S}_6$. De plus, G est isomorphe à $\mathrm{D}_4 \times \mathbb{Z}/2\mathbb{Z}$. En particulier, G ne contient pas d'élément d'ordre 8 et G contient 4 éléments d'ordre 4 (et 11 éléments d'ordre 2). Ainsi G et donc $\mathfrak{S}_6$ ne peut contenir $\mathbb{Z}/8\mathbb{Z}$ qui a un élément d'ordre 8 ni $\mathbb{H}_8$ qui contient 6 éléments d'ordre 4.

Par ailleurs, le groupe

$$\{\mathrm{id},\ (1,2),\ (3,4),\ (1,2)(3,4),\ (5,6),\ (1,2)(5,6),\ (3,4)(5,6),\ (1,2)(3,4)(5,6)\}$$

est un sous-groupe de $\mathfrak{S}_6$ d'ordre 8 isomorphe $(\mathbb{Z}/2\mathbb{Z})^3$ et le groupe

$$\{\mathrm{id},\ (1,2,3,4),\ (1,3)(2,4),\ (1,4,2,3),\ (5,6),\ (1,2,3,4)(5,6),\ (1,3)(2,4)(5,6),\ (1,4,2,3)(5,6)\}$$

est un sous-groupe de $\mathfrak{S}_6$ d'ordre 8 isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$.

Pour $i = 7$, on a $|\mathfrak{S}_5| = 16 \cdot 45 \cdot 7$. Ainsi, les 2-Sylow de $\mathfrak{S}_7$ sont d'ordre 16. De plus, $\mathfrak{S}_6$ est contenu dans $\mathfrak{S}_7$. Les 2-Sylow de $\mathfrak{S}_6$ sont donc aussi des 2-Sylow pour $\mathfrak{S}_7$. Ainsi, les 2-Sylow de $\mathfrak{S}_7$ sont isomorphes à $\mathrm{D}_4 \times \mathbb{Z}/2\mathbb{Z}$ et ne peuvent contenir ni $\mathbb{Z}/8\mathbb{Z}$ ni $\mathbb{H}_8$.

Bilan. Le groupe $(\mathbb{Z}/2\mathbb{Z})^3$ s'injecte dans $\mathfrak{S}_6$ mais pas dans $\mathfrak{S}_i$ pour $i < 6$. Le groupe $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$ s'injecte dans $\mathfrak{S}_6$ mais pas dans $\mathfrak{S}_i$ pour $i < 6$. Le groupe $\mathbb{Z}/8\mathbb{Z}$ s'injecte dans $\mathfrak{S}_8$ mais pas dans $\mathfrak{S}_i$ pour $i < 8$ (voir aussi la proposition 26). Le groupe D_4 s'injecte dans $\mathfrak{S}_4$ mais pas dans $\mathfrak{S}_i$ pour $i < 4$. Le groupe $\mathbb{H}_8$ s'injecte dans $\mathfrak{S}_8$ mais pas dans $\mathfrak{S}_i$ pour $i < 8$. ■

Exemple 17 — Groupe d'ordre 9. Les groupes d'ordre 9 sont isomorphes à $\mathbb{Z}/9\mathbb{Z}$ ou $(\mathbb{Z}/3\mathbb{Z})^2$.

Pour étudier, le cas des groupes d'ordre 9, on va utiliser le même point de vue que celui de l'exemple 16. Comme 9 est une puissance de 3, un sous-groupe d'ordre 9 d'un $\mathfrak{S}_m$ est nécessairement contenu dans un 3-Sylow de $\mathfrak{S}_m$ (voir []). Il s'agit donc d'étudier les 3-Sylow des groupes symétriques de 1 à 9 (le théorème 1 de Cayley assure qu'il suffit d'aller jusqu'à 9).

Pour $i < 6$, on a $9 \nmid |\mathfrak{S}_i|$. Ainsi, un groupe d'ordre 9 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 6$. Pour $i = 6$, on a $|\mathfrak{S}_6| = 9 \cdot 80$ avec $3 \nmid 80$. Ainsi les 3-Sylow de $\mathfrak{S}_6$ sont d'ordre 9. Il s'agit à présent de savoir s'ils sont isomorphes à $\mathbb{Z}/9\mathbb{Z}$ ou à $(\mathbb{Z}/3\mathbb{Z})^2$. Or, à l'aide de 3-cycles à support disjoint, il est facile de construire un groupe d'ordre 9 : par exemple, l'ensemble

$$\mathrm{S} = \{\mathrm{id},\ (1,2,3),\ (1,3,2),\ (4,5,6),\ (4,6,5),\ (1,2,3)(4,5,6),\ (1,2,3)(4,6,5),\ (1,3,2)(4,5,6),\ (1,3,2)(4,6,5)\}$$

est un sous-groupe d'ordre 9 de $\mathfrak{S}_6$ isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$. Ainsi les 3-Sylow de $\mathfrak{S}_6$ sont isomorphes à $(\mathbb{Z}/3\mathbb{Z})^2$.

Déterminons à présent le nombre s de 3-Sylow de $\mathfrak{S}_6$. D'après les théorèmes de Sylow, s est un diviseur de 80. Ainsi $s \in \{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$. De plus, s est congru à 1 modulo 3. Ainsi $s \in \{1, 4, 10, 16, 40\}$. Or le conjugué d'un 3-cycle est un 3-cycle, le conjugué d'un produit de 2 3-cycles à support disjoint est un produit de 2 3-cycles à support disjoint et tous les 3-Sylow de $\mathfrak{S}_6$ sont conjugués, on en déduit que tous les 3-Sylow contiennent exactement 4 3-cycles et 4 produits de 2 3-cycles à support disjoint. Comme il y a 40 3-cycles, on en déduit qu'il y a au moins 10 3-Sylow dans $\mathfrak{S}_6$. On va montrer à présent qu'un 3-cycle appartient à un unique 3-Sylow et obtenir ainsi le fait qu'il y a exactement 10 3-Sylow dans $\mathfrak{S}_6$. Soit (a, b, c) un 3-cycle. Comme tout p-sous-groupe d'un groupe G est contenu dans un p-Sylow de G, (a, b, c) est contenu dans un 3-Sylow de $\mathfrak{S}_6$. Considérons à présent S un 3-Sylow de $\mathfrak{S}_6$ contenant (a, b, c). Comme un 3-Sylow de $\mathfrak{S}_6$ est isomorphe à $(\mathbb{Z}/3\mathbb{Z})^2$, il existe dans S un élément d'ordre 3 qui commute avec (a, b, c) et qui n'est pas dans le sous-groupe $\langle (a, b, c) \rangle$. On note $\{d, e, f\}$ le complémentaire de $\{a, b, c\}$ dans $\{1, 2, 3, 4, 5, 6\}$. Les éléments de $\mathfrak{S}_6$ qui commutent avec (a, b, c) sont les éléments appartenant à

$$\mathfrak{S}_{\{d,e,f\}} \sqcup (a, b, c)\mathfrak{S}_{\{d,e,f\}} \sqcup (a, c, b)\mathfrak{S}_{\{d,e,f\}}\,.$$

Les éléments d'ordre 3 qui commutent avec (a, b, c) sont donc

$$(d, e, f),\ (d, f, e),\ (a, b, c),\ (a, b, c)(d, e, f),\ (a, b, c)(d, f, e),\ (a, c, b),\ (a, c, b)(d, e, f) \ \text{ et } \ (a, c, b)(d, f, e).$$

Finalement, S contient l'un des éléments (d, e, f), (d, f, e), $(a, b, c)(d, e, f)$, $(a, b, c)(d, f, e)$, $(a, c, b)(d, e, f)$ et $(a, c, b)(d, f, e)$. Quitte à multiplier par $(a, b, c) \in \mathrm{S}$ ou $(a, c, b) = (a, b, c)^2 \in \mathrm{S}$, on en déduit que (d, e, f) ou (d, f, e) sont dans S. Quitte à élever (d, f, e) au carré, on en déduit que $(d, e, f) \in \mathrm{S}$. Ainsi $\mathrm{S} = \langle (a, b, c), (d, e, f) \rangle$ est entièrement déterminé par (a, b, c). On en déduit que $\mathfrak{S}_6$ contient 10 3-Sylow. Par ailleurs, fixons S un 3-Sylow de $\mathfrak{S}_6$, le nombre d'injections de $(\mathbb{Z}/3\mathbb{Z})^2$ dans S est égal au nombre d'automorphismes de $(\mathbb{Z}/3\mathbb{Z})^2$. Or le groupe des automorphismes de $(\mathbb{Z}/3\mathbb{Z})^2$ n'est autre que $\mathrm{GL}_2(\mathbb{F}_3)$ (voir [BPM, Proposition 6.31 (*iii*) et (*iv*)] avec $\mathrm{A} = \mathbb{Z}$ et $\mathrm{I} = 3\mathbb{Z}$) qui est de cardinal $(3^2 - 1)(3^2 - 3) = 48$. Ainsi le nombre d'injections de $(\mathbb{Z}/3\mathbb{Z})^2$ dans $\mathfrak{S}_6$ est égal à 480.

Pour $i = 7$ (resp. $i = 8$), on a $|\mathfrak{S}_6| = 9 \cdot 560$ (resp. $|\mathfrak{S}_7| = 9 \cdot 3920$) et $3 \nmid 560$ (resp. $3 \nmid 3920$). Ainsi les 3-Sylow de $\mathfrak{S}_7$ (resp. $\mathfrak{S}_8$) sont d'ordre 9. De plus, $\mathfrak{S}_6$ est contenu dans $\mathfrak{S}_7$ (resp. $\mathfrak{S}_8$). Ainsi, par cardinalité un 3-Sylow de $\mathfrak{S}_6$ est aussi un 3-Sylow de $\mathfrak{S}_7$ (resp. $\mathfrak{S}_8$). Les 3-Sylow de $\mathfrak{S}_7$ (resp. $\mathfrak{S}_8$) sont donc, comme ceux de $\mathfrak{S}_6$ isomorphes à $(\mathbb{Z}/3\mathbb{Z})^2$ et donc ne sont pas isomorphes à $\mathbb{Z}/9\mathbb{Z}$.

Le groupe $\mathbb{Z}/9\mathbb{Z}$ s'injecte dans $\mathfrak{S}_9$ (grâce au théorème 1 de Cayley). Les calculs ci-dessus montrent que $\mathbb{Z}/9\mathbb{Z}$ ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 9$ (voir aussi la proposition 26). Par ailleurs, montrons qu'un élément d'ordre 9

de $\mathfrak{S}_9$ est nécessairement un 9-cycle. Le ppcm des longueurs des cycles de la décomposition en cycles à support disjoint d'un élément d'ordre 9 de $\mathfrak{S}_9$ est 9, la longueur des cycles qui interviennent sont donc des diviseurs de 9, c'est-à-dire $1, 3$ et 9. S'il n'y a que des cycles d'ordre 1 et 3 alors l'élément n'est pas d'ordre 9 (il est d'ordre 3 ou 1 (s'il n'y a que des cycles de longueur 1)). Il y a donc au moins un cycle de longueur 9. Comme la somme des longueurs des cycles est 9, on en déduit qu'un élément d'ordre 9 de $\mathfrak{S}_9$ est un 9-cycle. Il y a donc 8! éléments d'ordre 9 dans $\mathfrak{S}_9$. Ainsi, grâce au lemme 25, il y a 8! morphismes injectifs de $\mathbb{Z}/9\mathbb{Z}$ dans $\mathfrak{S}_9$ (voir aussi la proposition 26).

Bilan. Le groupe $(\mathbb{Z}/3\mathbb{Z})^2$ s'injecte dans $\mathfrak{S}_6$ de 480 façons différentes mais pas dans $\mathfrak{S}_i$ pour $i < 6$. Le groupe $\mathbb{Z}/9\mathbb{Z}$ s'injecte dans $\mathfrak{S}_9$ de 8! façons différentes mais ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 9$. ■

Exemple 18 — Groupe d'ordre 10. Les groupes d'ordre 10 sont isomorphes à $\mathbb{Z}/10\mathbb{Z}$ ou D_5.

Commençons par le groupe D_5. Par définition, D_5 est le groupe des isométries du pentagone. Ainsi D_5 agit donc de façon naturelle sur les 5 sommets du pentagone $(1, \exp(2i\pi/5), \exp(4i\pi/5), \exp(6i\pi/5), \exp(8i\pi/5))$ (qu'on numérote $\{1, 2, 3, 4, 5\}$). On en déduit (voir la note « Action de groupe ») un morphisme de groupes φ de D_5 dans $\mathfrak{S}_5$. Montrons que φ est injectif. On considère donc $g \in \mathrm{D}_5$ tel que $\varphi(g)(\ell) = \ell$ pour tout $\ell \in [\![1\,,\, 5]\!]$. Comme les isométries sont affines (voir []), elles conservent le barycentre des 5 sommets, c'est-à-dire l'origine. Ainsi, g est $\mathbb{R}$-linéaire. De plus, par construction de φ, on a $\varphi(g)(\ell) = g(\exp(2i\pi/5)^{\ell-1})$. Finalement, g est $\mathbb{R}$-linéaire et envoie 1 sur 1 et $\exp(2i\pi/5)$ sur $\exp(2i\pi/5)$. On en déduit que $g = \mathrm{id}_{\mathbb{R}^2}$ et φ est injective. Ainsi $\mathfrak{S}_5$ contient un sous-groupe isomorphe à D_5. Par ailleurs, la description géométrique donnée par l'action sur le pentagone permet de décrire les éléments de $\varphi(\mathrm{D}_5)$

$$\{\mathrm{id},\ (2,5)(3,4),\ (1,3)(4,5),\ (1,5)(2,4),\ (1,2)(3,5),\ (1,4)(2,3),\\ (1,2,3,4,5),\ (1,3,5,2,4),\ (1,4,2,5,3),\ (1,5,4,3,2)\}$$

qui sont respectivement, l'identité, les 5 réflexions, les rotations d'angles $2\pi/5$, $4\pi/5$, $6\pi/5$ et $8\pi/5$. Par ailleurs, comme $10 \nmid |\mathfrak{S}_i|$ pour $i < 5$, D_5 ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 5$.

Passons au cas de $\mathbb{Z}/10\mathbb{Z}$. L'élément $(1, 2, 3, 4, 5)(6, 7)$ est un élément d'ordre 10 de $\mathfrak{S}_7$. Ainsi le groupe $\langle (1, 2, 3, 4, 5)(6, 7) \rangle$ est un groupe cyclique d'ordre 10 et $\mathbb{Z}/10\mathbb{Z}$ s'injecte dans $\mathfrak{S}_7$ (voir le lemme 25). Les éléments d'ordre 10 de $\mathfrak{S}_7$ ont tous la même décomposition en cycles à support disjoint : ce sont les produits d'un 5-cycle et d'une transposition à support disjoint (voir l'étude des éléments d'ordre 10 dans $\mathfrak{S}_i$ pour $i < 7$ dans le paragraphe suivant). Il y en $7!/10 = 21 \cdot 24 = 504$. On a ainsi 504 injections de $\mathbb{Z}/10\mathbb{Z}$ dans $\mathfrak{S}_7$. De plus ces injections diffèrent d'un automorphisme intérieur de $\mathfrak{S}_7$ puisque les éléments d'ordre 10 de $\mathfrak{S}_7$ sont conjugués (ils ont le même type de décomposition en cycles à support disjoint).

Montrons à présent que $\mathbb{Z}/10\mathbb{Z}$ ne s'injecte pas dans $\mathfrak{S}_i$ pour $i < 7$. Soit σ est un élément d'ordre 10 de $\mathfrak{S}_i$ avec $i < 7$. La décomposition en cycles à support disjoint de σ ne fait intervenir que des cycles d'ordre $1, 2, 5$ ou 10 (un diviseur de l'ordre de σ). Comme la somme des longueurs des cycles est $i < 7$, les longueurs des cycles qui interviennent sont $1, 2$ ou 5. Comme le ppcm des longueurs des cycles est 10, il y a nécessairement un cycle de longueur 2 et un cycle de longueur 5. Ainsi $i \geqslant 7$. Finalement, pour $i < 7$, il n'y a pas d'élément d'ordre 10 dans $\mathfrak{S}_i$ pour $i < 7$ (voir aussi la proposition 26). ■

Exemple 19 — Groupe d'ordre 11. Un groupe d'ordre 11 est cyclique isomorphe à $\mathbb{Z}/11\mathbb{Z}$ (car 11 est premier). D'après le théorème 1 de Cayley, il s'injecte dans $\mathfrak{S}_{11}$. D'après le lemme 25, il y a autant d'injections d'un groupe d'ordre 11 dans $\mathfrak{S}_{11}$ que d'éléments d'ordre 11 dans $\mathfrak{S}_{11}$. Or les éléments d'ordre 11 de $\mathfrak{S}_{11}$ sont les 11-cycles qui sont au nombre de $(11-1)! = 10!$. Ainsi, il y a 10! injections d'un groupe d'ordre 11 dans $\mathfrak{S}_{11}$. De plus, comme les 11-cycles sont conjugués dans $\mathfrak{S}_{11}$, ces deux inclusions diffèrent d'un automorphisme intérieur de $\mathfrak{S}_{11}$. Par ailleurs, comme pour $i < 11$, on a $11 \nmid |\mathfrak{S}_i|$, un groupe d'ordre 11 ne peut s'injecter dans $\mathfrak{S}_i$ pour $i < 11$ (voir aussi la proposition 26). ■

Remarque 20 — Théorie de Galois inverse. Savoir quel est le plus petit entier m tel que $\mathfrak{S}_m$ contient un groupe G donné peut être utile en théorie de Galois inverse. La théorie de Galois inverse pose le problème suivant : le groupe G est-il le groupe de Galois d'une extension galoisienne de $\mathbb{Q}$ (si oui lesquelles ?) ou d'un polynôme à coefficients dans $\mathbb{Q}$ (si oui lesquels ?) ? Or le groupe de Galois d'un polynôme à coefficients dans $\mathbb{Q}$ de degré m s'identifie naturellement à un sous-groupe de $\mathfrak{S}_m$ (le groupe de Galois permute les racines du polynôme). L'exemple 16 montre alors que $\mathbb{H}_8$ ne peut être le groupe de Galois d'un polynôme de degré inférieur ou égal à 7. ■

Inclusion minimale : le cas des groupes cycliques

L'objectif de cette partie est de donner la réponse à la question suivante : étant donné un groupe cyclique G d'ordre n, quel est le plus petit entier m tel que $\mathfrak{S}_m$ qui contienne G ? La réponse (voir la proposition 26) fait intervenir la décomposition de n en facteurs premiers et repose donc sur de l'arithmétique élémentaire

(essentiellement le calcul du ppcm). L'argument arithmétique central est exposé dans le lemme 23. Les inégalités des lemmes 21 et 22 sont des préparatifs pour le lemme 23. La décomposition en cycles à support disjoint permet alors de nous ramener au groupe symétrique (voir la proposition 24). Enfin, le lemme 25 qui fait le lien entre éléments d'ordre n et morphismes injectifs issus de $\mathbb{Z}/n\mathbb{Z}$ nous permet de conclure.

Lemme 21 — Inégalité entre somme et produit. Soient $n \in \mathbb{N}^*$ et $(x_1, \ldots, x_n) \in \mathbb{R}^n$ avec $x_i \geqslant 2$ pour tout $i \in [\![1 , n]\!]$. On a

$$\sum_{i=1}^{n} x_i \leqslant \prod_{i=1}^{n} x_i \tag{$*$}$$

avec égalité si et seulement si $n = 2$ et $x_1 = x_2 = 2$ ou $n = 1$.

Preuve. On procède par récurrence sur n. Le cas $n = 1$ est trivial. Pour le cas $n = 2$, on considère $x, y \in \mathbb{R}$ avec $x \geqslant 2$ et $y \geqslant 2$. On a $(x - 1) \geqslant 1$ et $(y - 1) \geqslant 1$. Ainsi $(x - 1)(y - 1) \geqslant 1$ et donc $xy \geqslant x + y$. De plus l'égalité dans la dernière inégalité, impose $(x - 1)(y - 1) = 1$ et donc $x - 1 = y - 1 = 1$.

Soient $n \geqslant 1$. Supposons que l'inégalité $(*)$ soient vrai pour tout $(x_1, \ldots, x_n) \in \mathbb{R}^n$ avec $x_i \geqslant 2$ pour tout $i \in [\![1 , n]\!]$. On considère alors $(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1}$ tel que $x_i \geqslant 2$ pour tout $i \in [\![1 , n + 1]\!]$. On a

$$\prod_{i=1}^{n} x_i \geqslant 2^n \geqslant 2 ,$$

on peut donc appliquer le cas $n = 2$ pour obtenir

$$\prod_{i=1}^{n+1} x_i \geqslant \prod_{i=1}^{n} x_i + x_{n+1} . \tag{$**$}$$

L'hypothèse de récurrence donne alors

$$\prod_{i=1}^{n} x_i + x_{n+1} \geqslant \sum_{i=1}^{n} x_i + x_{n+1} = \sum_{i=1}^{n+1} x_i .$$

ce qui donne l'inégalité souhaité au rang $n + 1$.

Traitons à présent le cas d'égalité. Il va résulter du cas d'égalité pour $n = 2$ et de l'inégalité $(**)$. Soient $n \geqslant 2$ et $(x_1, \ldots, x_n) \in \mathbb{R}^n$ avec $x_i \geqslant 2$ pour tout $i \in [\![1 , n]\!]$ tel que

$$\sum_{i=1}^{n} x_i = \prod_{i=1}^{n} x_i .$$

Comme $n - 1 \geqslant 1$, on peut appliquer la preuve de l'hérédité s'applique, on a donc

$$\prod_{i=1}^{n} x_i \geqslant \prod_{i=1}^{n-1} x_i + x_n \geqslant \sum_{i=1}^{n} x_i .$$

On a donc égalité dans l'inégalité $$\prod_{i=1}^{n} x_i \geqslant \prod_{i=1}^{n-1} x_i + x_n ,$$

ce qui donne d'après le cas d'égalité au rang 2,

$$\prod_{i=1}^{n-1} x_i = 2 \qquad \text{et} \qquad x_n = 2 .$$

Or $$\prod_{i=1}^{n-1} x_i \geqslant 2^{n-1} \geqslant 2 .$$

Donc $$n - 1 = 1 \qquad \text{et} \qquad x_1 = 2 .$$ ■

Le lemme précédent se généralise de la façon suivante.

Lemme 22 — Inégalités et partitions. Soient $n \in \mathbb{N}^*$ et $(x_1, \ldots, x_n) \in \mathbb{R}^n$ avec $x_i \geqslant 2$ pour tout i. Alors pour toute partition $[\![1 , n]\!] = \mathrm{I}_1 \sqcup \cdots \sqcup \mathrm{I}_r$ de $[\![1 , n]\!]$, on a

$$\sum_{i=1}^{n} x_i \leqslant \sum_{k=1}^{r} \left(\prod_{i \in \mathrm{I}_k} x_i \right) \leqslant \prod_{i=1}^{n} x_i .$$

De plus, on a $$\sum_{i=1}^{n} x_i = \sum_{k=1}^{r} \left(\prod_{i \in \mathrm{I}_k} x_i \right)$$

si et seulement si la partition $\mathrm{I}_1 \sqcup \cdots \sqcup \mathrm{I}_r$ n'est constituée que de parties à un ou deux éléments et dont les parties à deux éléments ne contient que des indices i tels que $x_i = 2$.

De plus, on a
$$\sum_{k=1}^{r} \left(\prod_{i \in \mathrm{I}_k} x_i \right) = \prod_{i=1}^{n} x_i$$
si et seulement si la partition $\mathrm{I}_1 \sqcup \cdots \sqcup \mathrm{I}_r$ est la partition triviale en une partie à n éléments ou $n = 2$ et $x_1 = x_2 = 2$.

Preuve. Soit $k \in [\![1 , r]\!]$. Comme $\mathrm{I}_k \neq \varnothing$, on a, grâce au lemme 21,
$$\prod_{i \in \mathrm{I}_k} x_i \geqslant \sum_{i \in \mathrm{I}_k} x_i \,.$$

Ainsi
$$\sum_{k=1}^{r} \left(\prod_{i \in \mathrm{I}_k} x_i \right) \geqslant \sum_{k=1}^{r} \left(\sum_{i \in \mathrm{I}_k} x_i \right) = \sum_{i=1}^{n} x_i \,.$$

L'égalité dans l'inégalité précédente a lieu si et seulement si pour tout $k \in [\![1 , r]\!]$
$$\prod_{i \in \mathrm{I}_k} x_i = \sum_{i \in \mathrm{I}_k} x_i \,.$$
En vertu du lemme 21, on en déduit que $|\mathrm{I}_k| = 1$ ou $|\mathrm{I}_k| = 2$ et $x_i = 2$ pour tout $i \in \mathrm{I}_k$. On en déduit le cas d'égalité.

Pour $k \in [\![1 , r]\!]$, posons $y_k = \prod_{i \in \mathrm{I}_k} x_i$. Comme $\mathrm{I}_k \neq \varnothing$, on a
$$y_k = \prod_{i \in \mathrm{I}_k} x_i \geqslant 2^{|\mathrm{I}_k|} \geqslant 2 \,.$$
Le lemme 21 appliqué à la famille $(y_1, \ldots, y_r)$ montre que
$$\sum_{k=1}^{r} \left(\prod_{i \in \mathrm{I}_k} x_i \right) = \sum_{k=1}^{r} y_i \quad \leqslant \quad \prod_{k=1}^{r} y_i = \prod_{i=1}^{n} x_i \,.$$

D'après le lemme 21, l'égalité dans l'inégalité précédente a lieu si et seulement si $r = 1$ ou $r = 2$ et $y_1 = y_2 = 2$. Le cas $r = 1$ correspond au cas de la partition triviale de $[\![1 , n]\!]$ en une partie à n éléments. Si $r = 2$ et $y_1 = y_2 = 2$. On a $2^{|\mathrm{I}_1|} = 2$ et $2^{|\mathrm{I}_2|} = 2$. Ainsi $|\mathrm{I}_1| = |\mathrm{I}_2| = 1$ et donc $n = 2$. De plus, $y_k = x_j = 2$ avec $\{j\} = \mathrm{I}_k$. ■

Le lemme qui suit est l'argument central du raisonnement. Il s'agit de minimiser la somme des éléments d'une famille dont le ppcm est donné.

Lemme 23 – Minimisation de somme et ppcm. Soient $n \in \mathbb{N}^*$ et $\mathscr{P}$ l'ensemble des nombres premiers. On définit
$$\mathrm{J}_n = \big\{ (x_1, \ldots, x_\ell) \in \mathbb{N}^\ell, \qquad \ell \in \mathbb{N}, \quad \mathrm{ppcm}\,(x_1, \ldots, x_\ell) = n \big\},$$
l'ensemble des familles finies d'entiers dont le ppcm est n. On considère alors la décomposition de n en facteurs premiers
$$n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$$
avec $p_i \in \mathscr{P}$, $\alpha_i \in \mathbb{N}^*$ et $p_i \neq p_j$ si $i \neq j$. On a
$$\min_{(x_1, \ldots, x_\ell) \in \mathrm{J}_n} \sum_{i=1}^{\ell} x_i \quad = \quad \sum_{i=1}^{r} {p_i}^{\alpha_i} \,.$$

Preuve. *Rappel : calcul du* ppcm . Considérons une famille $(x_1, \ldots, x_\ell) \in {\mathbb{N}^*}^\ell$. Pour $i \in [\![1 , \ell]\!]$, on considère la décomposition de x_i en facteurs premiers
$$x_i = \prod_{p \in \mathscr{P}} p^{\nu_p(x_i)} \qquad \text{avec} \quad \nu_p(x_i) \in \mathbb{N} \tag{$**$}$$
et seulement un nombre fini de $\nu_p(x_i)$ non nul. On a alors
$$\mathrm{ppcm}\,(x_1, \ldots, x_\ell) = \prod_{p \in \mathscr{P}} p^{\max_i \nu_p(x_i)} \,.$$
On en déduit que la famille $({p_1}^{\alpha_1}, \ldots, {p_r}^{\alpha_r}) \in \mathrm{J}_n$ et donc

$$\min_{(x_1,\dots,x_\ell)\in \mathrm{J}_n} \sum_{i=1}^{\ell} x_i \quad \leqslant \quad \sum_{i=1}^{r} {p_i}^{\alpha_i}\,.$$

Remarques sur les éléments de J_n.

a. Soit $(x_1,\dots,x_\ell)\in \mathrm{J}_n$. La remarque $(**)$ montre que, pour tout $j\in [\![1\,,\,\ell]\!]$, on a $\nu_p(x_j)=0$ si $p\notin\{p_1,\dots,p_r\}$ et $\nu_{p_i}(x_j)\leqslant \alpha_i$ pour tout $i\in[\![1\,,\,r]\!]$ et tout $j\in[\![1\,,\,\ell]\!]$. Autrement dit,

$$x_j=\prod_{i=1}^{r} {p_i}^{\beta_{ij}} \qquad \text{avec} \quad 0\leqslant \beta_{ij}\leqslant \alpha_i\,.$$

b. De plus, toujours d'après $(**)$, pour tout $j\in[\![1\,,\,r]\!]$, il existe i tel que $\beta_{ij}=\alpha_i$.

Considérons à présent une famille $(y_1,\dots,y_m)\in \mathrm{J}_n$ telle que

$$\sum_{i=1}^{m} y_i \quad = \min_{(x_1,\dots,x_\ell)\in \mathrm{J}_n} \sum_{i=1}^{\ell} x_i.$$

(i) Montrons que pour $i\in[\![1\,,\,m]\!]$, on a $y_i\geqslant 2$. S'il existe i tel que $y_i=1$ alors la famille $(y_1,\dots,\widehat{y_i},\dots,y_m)$ obtenue en omettant y_i appartient à J_n et a une somme strictement inférieure à la famille $(y_1,\dots,y_m)$ ce qui contredit sa minimalité.

(ii) Montrons que pour $i\neq j$, les entiers y_i et y_j sont premiers entre eux. Posons $d=\operatorname{pgcd}(y_i,y_j)$ et $y_j=dy'$. Comme $\operatorname{ppcm}(y_i,y_j)=\operatorname{ppcm}(y_i,y')$, la famille $(y_1,\dots,y_{j-1},y',y_{j+1},\dots,y_m)$ appartient à J_n. Si $d\neq 1$ alors $y'<y_j$ ce qui contredit la minimalité de $(y_1,\dots,y_m)$.

(iii) Montrons qu'il existe une partition $[\![1\,,\,r]\!]=\mathrm{I}_1\sqcup\cdots\sqcup \mathrm{I}_m$ de $[\![1\,,\,r]\!]$ telle que

$$y_k=\prod_{i\in \mathrm{I}_k} {p_i}^{\alpha_i}\,.$$

On définit $\mathrm{I}_k=\{i\in[\![1\,,\,r]\!],\ p_i\mid y_k\}$. Le point (ii) montre que $\mathrm{I}_i\cap\mathrm{I}_j=\varnothing$ si $i\neq j$. Par ailleurs, le point b de la remarque montre que, pour tout $i\in[\![1\,,\,r]\!]$, ${p_i}^{\alpha_i}$ et donc p_i divise l'un des y_j. Ainsi $[\![1\,,\,r]\!]=\mathrm{I}_1\cup\cdots\cup\mathrm{I}_m$. Calculons à présent y_k. Pour $i\in\mathrm{I}_k$, y_k est divisible par p_i et y_q n'est pas divisible par p_i si $q\neq k$. On en déduit alors du point b de la remarque que y_k est divisible par ${p_i}^{\alpha_i}$. Ainsi y_k est divisible par

$$\prod_{i\in \mathrm{I}_k} {p_i}^{\alpha_i}\,.$$

La construction de l'ensemble I_k montre y_k n'est divisible par aucun des p_i pour $i\notin\mathrm{I}_k$. Le point a de la remarque assure que y_k n'est divisible par aucun nombre premier distinct des p_i. Ainsi

$$y_k=\prod_{i\in \mathrm{I}_k} {p_i}^{\beta_i} \qquad \text{avec} \quad \beta_i\geqslant\alpha_i$$

Le point a de la remarque montre que $\beta_i\leqslant\alpha_i$. Finalement

$$y_k=\prod_{i\in \mathrm{I}_k} {p_i}^{\alpha_i}\,.$$

(iv) Le lemme 22 montre que

$$\min_{(x_1,\dots,x_\ell)\in \mathrm{J}_n} \sum_{i=1}^{\ell} x_i \;=\; \sum_{k=1}^{m} y_k \;=\; \sum_{k=1}^{m}\prod_{i\in\mathrm{I}_k} {p_i}^{\alpha_i} \quad\geqslant\quad \sum_{i=1}^{r} {p_i}^{\alpha_i}\,.$$

De plus, le cas d'égalité du lemme 22 montre que $|\mathrm{I}_k|=1$ pour tout k (puisqu'il n'y a pas deux y_i égaux à 2). Ainsi à l'ordre près, la seule famille réalisant le minimum est $({p_1}^{\alpha_1},\dots,{p_r}^{\alpha_r})$. ■

La proposition qui suit est un premier pas vers la réponse à notre question. C'est la décomposition en cycles à support disjoint qui va permettre de faire le lien entre la minimisation de la somme d'une famille dont le ppcm est donné (lemme 23) et le groupe symétrique.

Proposition 24 — Élement d'ordre n dans un groupe symétrique. Soient $n\in\mathbb{N}^*$ et $\mathscr{P}$ l'ensemble des nombres premiers. On considère la décomposition en facteurs premiers de n :

$$n=\prod_{i=1}^{r} {p_i}^{\alpha_i}$$

avec $p_i\in\mathscr{P}$, $\alpha_i\in\mathbb{N}^*$ et $p_i\neq p_j$ si $i\neq j$. Le plus petit entier m tel que $\mathfrak{S}_m$ contient un élément d'ordre n est $m_{\min}={p_1}^{\alpha_1}+\cdots+{p_r}^{\alpha_r}$.

De plus, la décomposition en cycles à support disjoint d'un élément de $\mathfrak{S}_{m_{\min}}$ d'ordre n est formé d'un ${p_1}^{\alpha_1}$-cycle, d'un ${p_2}^{\alpha_2}$-cycle... Les éléments d'ordre n de $\mathfrak{S}_{m_{\min}}$ sont au nombre de $m_{\min}!/n$.

Preuve. Soit $m\in\mathbb{N}^*$ tel que $\mathfrak{S}_m$ contient σ un élément d'ordre n. On considère la décomposition de σ en cycles à support disjoint :

$$\sigma = \prod_{i=1}^{s} \sigma_i \qquad \text{avec} \qquad \operatorname{supp} \sigma_i \cap \operatorname{supp} \sigma_j = \varnothing \quad \text{si} \quad i \neq j$$

et σ_i est un cycle de longueur ℓ_i. L'ordre de σ est $\operatorname{ppcm}(\ell_i,\ i \in [\![1\,,\, s]\!]) = n$. Ainsi la famille $(\ell_1, \ldots, \ell_s) \in \mathrm{J}_n$. De plus, on a

$$\sum_{i=1}^{s} \ell_i = m. \tag{1}$$

Réciproquement, si $(\ell_1, \ldots, \ell_s) \in \mathrm{J}_n$ alors il existe un élément d'ordre n dans $\mathfrak{S}_m$ avec

$$m = \sum_{i=1}^{s} \ell_i.$$

Il suffit de considérer un produit de cycles à support disjoint de longueur respective ℓ_i.

Ainsi l'ensemble

$$\mathrm{D}_n = \{m \in \mathbb{N}, \quad \exists\, \sigma \in \mathfrak{S}_m \text{ d'ordre } n\} = \left\{ \sum_{i=1}^{r} \ell_i, \quad (\ell_1, \ldots, \ell_r) \in \mathrm{J}_n \right\}$$

dont le plus petit élément est, d'après le lemme 23,

$$\sum_{i=1}^{r} {p_i}^{\alpha_i}.$$

En fait, on a
$$\mathrm{D}_n = \left\{ n \in \mathbb{N}, \quad n \geqslant \sum_{i=1}^{r} {p_i}^{\alpha_i} \right\}$$

puisque si $x = (\ell_1, \ldots, \ell_s) \in \mathrm{J}_n$ alors $y = (\ell_1, \ldots, \ell_s, 1) \in \mathrm{J}_n$ et la somme des composantes de y est égale à la somme des composantes de x à laquelle on a ajouté 1. Ainsi D_n est bien une demi-droite.

Soit $\sigma \in \mathfrak{S}_{m_{\min}}$ d'ordre n. D'après le calcul (**1**) et le lemme 23, on obtient la décomposition en cycles à support disjoint souhaitée. En particulier, les éléments d'ordre n de $\mathfrak{S}_{m_{\min}}$ forment une seule classe de conjugaison (voir [BPM, exercice 6.7 questions a et b]). Le nombre d'éléments de cette classe de conjugaison est alors le quotient de $m_{\min}! = |\mathfrak{S}_{m_{\min}}|$ par le nombre d'éléments de $\mathfrak{S}_{m_{\min}}$ qui commutent avec un élément d'ordre n fixé (on utilise ici la bijection entre l'orbite d'un élément de $\mathfrak{S}_m$ (sous l'action par conjugaison) et le quotient du groupe qui agit (ici $\mathfrak{S}_{m_{\min}}$) par le stabilisateur de l'élément considéré). Soient σ un élément d'ordre n de $\mathfrak{S}_{m_{\min}}$ et $\tau \in \mathfrak{S}_{m_{\min}}$ qui commute avec σ. On considère la décomposition de σ en cycles à support disjoint :

$$\sigma = \prod_{i=1}^{r} \sigma_i \qquad \text{avec} \qquad \operatorname{supp} \sigma_i \cap \operatorname{supp} \sigma_j = \varnothing \quad \text{si} \quad i \neq j$$

et σ_i est un cycle de longueur ${p_i}^{\alpha_i}$. Comme τ commute avec σ, τ stabilise les supports des σ_i (car ils sont de longueur deux à deux distinctes). Ainsi, pour tout $i \in [\![1\,,\, r]\!]$, la bijection τ induit par restriction une bijection τ_i du support de σ_i. De plus, chacune des bijections τ_i commute avec le cycle induit par σ_i. Réciproquement, en choisissant, pour tout $i \in [\![1\,,\, r]\!]$, une bijection du support de σ_i qui commute avec σ_i, on construit une bijection $\tau \in \mathfrak{S}_{m_{\min}}$ qui commute avec σ. Il s'agit donc de déterminer les éléments de $\mathfrak{S}_{\operatorname{supp} \sigma_i}$ qui commutent avec σ_i. Or un élément de $\mathfrak{S}_\ell$ qui commute avec un cycle de longueur ℓ est nécessairement une puissance de ce cycle. Ainsi, il y a ${p_i}^{\alpha_i}$ bijections τ_i qui commutent avec σ_i et donc

$$\prod_{i=1}^{r} {p_i}^{\alpha_i} = n$$

bijections qui commutent avec σ. On obtient ainsi le cardinal souhaité. ■

Le lemme qui suit fait le lien entre les éléments d'ordre n dans un groupe et les injections de $\mathbb{Z}/n\mathbb{Z}$ dans ce groupe.

Lemme 25 — Morphisme issu d'un groupe cyclique. Soit G un groupe. On note $\mathrm{G}_n = \{g \in \mathrm{G},\ g^n = 1\}$ l'ensemble des éléments de G dont l'ordre est un diviseur de n et ${}_n\mathrm{G} = \{g \in \mathrm{G},\ \operatorname{ordre}(g) = n\}$ l'ensemble des éléments de G d'ordre n.

Les applications

$$\Delta\colon \begin{cases} \operatorname{Hom}_{\mathrm{gr}}(\mathbb{Z}, \mathrm{G}) \longrightarrow \mathrm{G} \\ \gamma \longmapsto \gamma(1) \end{cases} \qquad \text{et} \qquad \nabla\colon \begin{cases} \mathrm{G} \longrightarrow \operatorname{Hom}_{\mathrm{gr}}(\mathbb{Z}, \mathrm{G}) \\ g \longmapsto (k \mapsto g^k)\,. \end{cases}$$

sont des bijections réciproques l'une de l'autre.

Pour $k \in \mathbb{Z}$, on note $\overline{k}$ la classe de k modulo n. Les applications

$$\Delta_n\colon \begin{cases} \operatorname{Hom}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \longrightarrow \mathrm{G}_n \\ \gamma \longmapsto \gamma(\overline{1}) \end{cases} \qquad \text{et} \qquad \nabla_n\colon \begin{cases} \mathrm{G}_n \longrightarrow \operatorname{Hom}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \\ g \longmapsto (\overline{k} \mapsto g^k)\,. \end{cases}$$

sont des bijections réciproques l'une de l'autre.

Enfin, on note $\mathrm{Inj}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G})$ l'ensemble des morphismes injectifs de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans G. Les applications

$$\Delta'_n : \begin{cases} \mathrm{Inj}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \longrightarrow {}_n\mathrm{G} \\ \gamma \longmapsto \gamma(\overline{1}) \end{cases} \quad \text{et} \quad \nabla'_n : \begin{cases} {}_n\mathrm{G} \longrightarrow \mathrm{Inj}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}) \\ g \longmapsto (\overline{k} \mapsto g^k)\,. \end{cases}$$

sont des bijections réciproques l'une de l'autre.

Preuve. Pour tout $g \in \mathrm{G}$, l'application $k \mapsto g^k$ est bien un morphisme de groupes : par définition des puissances d'un élément dans un groupe, on a bien $g^{k+k'} = g^k g^{k'}$ pour tous $k, k' \in \mathbb{Z}$. L'application ∇ est donc bien définie.

Par ailleurs, on a bien sûr, $\Delta\nabla = \mathrm{id}_{\mathrm{G}}$. De plus, pour $\sigma \in \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}, \mathrm{G})$ et $k \in \mathbb{Z}$, on a

$$\nabla\Delta(\sigma)(k) = \sigma(1)^k\,.$$

Comme σ est un morphisme de groupes, on a $\sigma(1)^k = \sigma(k)$ et donc $\nabla\Delta(\sigma) = \sigma$. Finalement, $\nabla\Delta = \mathrm{id}_{\mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z},\mathrm{G})}$.

Passons à l'étude de Δ_n et ∇_n. Montrons que Δ_n est bien définie. Soit $\gamma \in \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G})$. Comme γ est un morphisme de groupes, on a $\gamma(\overline{1})^n = \gamma(\overline{n}) = \gamma(0) = 1_{\mathrm{G}}$. Ainsi $\gamma(\overline{1}) \in \mathrm{G}_n$ et Δ_n est bien définie. Montrons à présent que ∇_n est bien définie. Soit $g \in \mathrm{G}_n$. Comme on l'a vu ci-dessus, l'application $\nabla(g) : k \mapsto g^k$ est un morphisme de groupes de $\mathbb{Z}$ dans G. Comme $g \in \mathrm{G}_n$, on a $n\mathbb{Z} \subset \mathrm{Ker}\,\nabla(g)$. Ainsi, grâce à la propriété universelle du quotient (voir [CAL, Théorème 4.25 Chapitre 4.4.A]), on obtient par passage au quotient, un morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans G donné par $\overline{k} \mapsto g^k$. Finalement, ∇_n est bien définie. Montrons pour finir que Δ_n et ∇_n sont deux bijections réciproques l'une de l'autre. On a clairement $\Delta_n\nabla_n = \mathrm{id}_{\mathrm{G}_n}$. De plus, pour $\sigma \in \mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G})$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, on a

$$\nabla_n\Delta_n(\sigma)(\overline{k}) = \sigma(1)^k\,.$$

Comme σ est un morphisme de groupes, on a $\sigma(1)^k = \sigma(\overline{k})$ et donc $\nabla_n\Delta_n(\sigma) = \sigma$. Finalement, on obtient $\nabla_n\Delta_n = \mathrm{id}_{\mathrm{Hom}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z},\mathrm{G})}$.

Passons à l'étude de Δ'_n et ∇'_n. Si $\gamma \in \mathrm{Inj}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G})$ alors $\Delta_n(\gamma) = \gamma(\overline{1})$ est un élément d'ordre n de G (car un morphisme injectif de groupes conserve l'ordre des éléments). Réciproquement, si g est un élément d'ordre exactement n de G, alors $\nabla_n(g)$ est injectif puisque

$$\mathrm{Ker}\,\nabla_n(g) = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z}, \quad g^k = 1_{\mathrm{G}}\right\} = \left\{\overline{k} \in \mathbb{Z}/n\mathbb{Z}, \quad k \in n\mathbb{Z}\right\}.$$

Ainsi Δ_n et ∇_n induisent des bijections Δ'_n et ∇'_n entre $\mathrm{Inj}_{\mathrm{gr}}(\mathbb{Z}/n\mathbb{Z}, \mathrm{G})$ et ${}_n\mathrm{G}$. ■

Il ne reste plus qu'à assembler la proposition 24 et le lemme 25 pour obtenir la réponse à notre question initiale.

Proposition 26 – Retour sur le lemme de Cayley. Soient $n \in \mathbb{N}^*$ et $\mathscr{P}$ l'ensemble des nombres premiers. On considère la décomposition en facteurs premiers de n :

$$n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$$

avec $p_i \in \mathscr{P}$, $\alpha_i \in \mathbb{N}^*$ et $p_i \neq p_j$ si $i \neq j$. Le plus petit entier m tel que $\mathbb{Z}/n\mathbb{Z}$ s'injecte dans $\mathfrak{S}_m$ est $m_{\min} = {p_1}^{\alpha_1} + \cdots + {p_r}^{\alpha_r}$. Le nombre d'injections de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathfrak{S}_{m_{\min}}$ est $m!/n$. Elles diffèrent 2 à 2 d'un automorphisme intérieur.

Preuve. Le groupe $\mathbb{Z}/n\mathbb{Z}$ s'injecte dans $\mathfrak{S}_m$ si et seulement si $\mathrm{Inj}_{\mathrm{Gr}}(\mathbb{Z}/n\mathbb{Z}, \mathfrak{S}_m) \neq \varnothing$ c'est-à-dire, en vertu du lemme 25, si et seulement si le groupe $\mathfrak{S}_m$ contient un élément d'ordre n. La proposition 24 donne alors le résultat souhaité. ■

Inclusion minimale : le cas des groupes diédraux

Dans cette partie, on donne la réponse (corollaire 28) à la question suivante : étant donné le groupe diédral D_n des isométries d'un polygone régulier à n cotés, quel est le plus petit entier m tel que $\mathfrak{S}_m$ qui contienne G ? Comme le groupe diédral D_n a une présentation de la forme $\langle r, s, \quad r^n = s^2 = 1,\ srs^{-1} = r^{-1}\rangle$, il s'agit de déterminer le plus petit groupe symétrique contenant un élément r d'ordre n et un élément s d'ordre 2 vérifiant la relation $srs^{-1} = r^{-1}$. Pour l'élément d'ordre n, la réponse est donnée par la proposition 24. Le lemme 27 apporte la réponse pour l'élément d'ordre 2.

Lemme 27 – Conjugaison, inverse et élément d'ordre 2. Soient $n \in \mathbb{N} \smallsetminus \{0, 1\}$ et $\sigma \in \mathfrak{S}_n$. Il existe un élément τ d'ordre 2 tel que $\sigma^{-1} = \tau\sigma\tau^{-1} = \tau\sigma\tau$.

Preuve. Commençons par quelques cas particulier, si $\sigma = \mathrm{id}_{\{1,\ldots,n\}}$ alors on choisit $\tau = (1, 2)$ (on a $n \geqslant 2$). Si σ est une transposition, on prend $\tau = \sigma$. Considérons à présent le cas où σ est un cycle de longueur $m \geqslant 3$.

Ainsi, on a $\sigma = (i_1, \dots, i_m)$ et $\sigma^{-1} = (i_1, i_m, i_{m-1}, \dots, i_2)$. On suppose tout d'abord $m = 2k+1$ impair (avec donc $k \geqslant 1$). En considérant le produit de k transpositions $\tau = (i_m, i_2)(i_{m-1}, i_3) \cdots (i_{k+2}, i_{k+1})$, on a

$$\tau\sigma\tau^{-1} = (\tau(i_1), \dots, \tau(i_m)) = (i_1, i_m, i_{m-1}, \dots, i_2) = \sigma^{-1}\,.$$

On suppose à présent $m = 2k$ pair (avec donc $k \geqslant 2$). En considérant le produit de $k-1$ transpositions $\tau = (i_m, i_2)(i_{m-1}, i_3) \cdots (i_{k+2}, i_k)$, on a

$$\tau\sigma\tau^{-1} = (\tau(i_1), \dots, \tau(i_m)) = (i_1, i_m, i_{m-1}, \dots, i_2) = \sigma^{-1}\,.$$

Passons au cas général. La décomposition de σ en cycles à support disjoint admet au moins un cycle de longueur supérieure ou égal à 2 : on a

$$\sigma = \prod_{i=1}^{s} \sigma_i \qquad \text{avec} \qquad \operatorname{supp} \sigma_i \cap \operatorname{supp} \sigma_j = \varnothing \quad \text{si} \quad i \neq j$$

et σ_i est un cycle de longueur $\ell_i \geqslant 2$ et $s \geqslant 1$ (on ne prend pas en compte dans cette écriture les cycles de longueur 1). D'après l'étude du cas des cycles, pour tout $i \in [\![1\,,\, s]\!]$, il existe un élément $\tau_i \in \mathfrak{S}_{\operatorname{supp} \sigma_i}$ d'ordre 2 tel que ${\sigma_i}^{-1} = \tau_i \sigma_i {\tau_i}^{-1}$. Comme les τ_i sont à support deux à deux disjoints, l'élément

$$\tau = \prod_{i=1}^{s} \tau_i \in \mathfrak{S}_n$$

est d'ordre 2. De plus, par construction, il vérifie

$$\tau\sigma\tau^{-1} = \prod_{i=1}^{s} \tau_i \sigma_i {\tau_i}^{-1} = \prod_{i=1}^{s} {\sigma_i}^{-1} = \sigma^{-1}\,. \qquad \blacksquare$$

Corollaire 28 — Inclusion et groupe diédral. Soient n un entier naturel supérieur ou égal à 3. On considère la décomposition en facteurs premiers de n :

$$n = \prod_{i=1}^{r} {p_i}^{\alpha_i}$$

avec $p_i \in \mathscr{P}$, $\alpha_i \in \mathbb{N}^*$ et $p_i \neq p_j$ si $i \neq j$. Le plus petit entier m tel que le groupe D_n s'injecte dans $\mathfrak{S}_m$ est $m_{\min} = {p_1}^{\alpha_1} + \cdots + {p_r}^{\alpha_r}$.

Preuve. Soit m_0 le plus petit entier m tel que D_n s'injecte dans $\mathfrak{S}_m$. Comme $\mathbb{Z}/n\mathbb{Z}$ s'injecte dans D_n (puisque D_n contient un élément d'ordre n), la proposition 26 assure que $m_0 \geqslant m_{\min}$. Par ailleurs, d'après la proposition 26 et le lemme 27, il existe dans $\mathfrak{S}_{m_{\min}}$ un élément σ d'ordre n et un élément τ d'ordre 2 vérifiant $\tau\sigma\tau^{-1} = \sigma^{-1}$. Autrement dit, le groupe $\langle \sigma, \tau \rangle$ est isomorphe au groupe diédral D_n et donc $m_0 \leqslant m_{\min}$. Ainsi, on a bien $m_0 = m_{\min}$. $\blacksquare$

Références

[BPM] V. Beck, J. Malick, et G.Peyré. *Objectif Agrégation.* H & K, 2004.

[CAL] J. Calais. *Éléments de théorie des groupes.* PUF, 1998.

[F-T] W. Feit et J.G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13 :p.775–1029, 1963.

[PER] D. Perrin. *Cours d'algèbre.* Ellipses, 1996.

[RDO1] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques 1, Algèbre.* Dunod, 1998.