Leçon 101 : Groupe opérant sur un ensemble. Exemples et applications.

Table des matières

1. Dernier rapport du Jury (2019) 1
2. Remarques 2
3. Questions 4
4. Éléments de réponses 6
5. Développements possibles 11
5.1. Classification des groupes d'ordre p^2 11
5.2. Isomorphismes exceptionnels 12
5.3. Générateurs de $\mathcal{S}_n$ 18
5.4. Théorèmes de Sylow 21
5.5. Sous-groupes finis de $\mathrm{SO}(3,\mathbb{R})$ 25
5.6. Automorphismes de $\mathcal{S}_n$ 27
5.7. Théorème de Wedderburn 32
5.8. Détermination des groupes d'isométries du cube et du tétraèdre 34
5.9. Dénombrement des colorations du cube 38
Références 41

1. Dernier rapport du Jury (2019)

Dans cette leçon, au-delà de la présentation du matériel théorique indispensable, le choix, l'organisation et la pertinence des illustrations sont des éléments forts de l'appréciation. Les deux facettes de l'action d'un groupe G sur un ensemble X doivent être maîtriséées : l'application de $\mathrm{G} \times X$ vers X et le morphisme de G vers $\mathcal{S}_X$. La relation entre orbite et stabilisateur qui en découle est incontournable ainsi que des exemples de son utilisation. Il faut savoir utiliser des actions bien choisies pour obtenir des informations soit sur un ensemble donné, soit sur un groupe G donné et faire apparaître des sous-groupes intéressants de G comme stabilisateurs. Par ailleurs, la présentation doit illustrer comment l'étude des orbites de certaines actions revient à classifier certains objets, soit en trouvant un représentant simple de chaque orbite, soit en dégageant des invariants caractérisant les orbites. Les actions de groupes interviennent aussi

efficacement dans des problèmes de dénombrements, notamment via la formule de Burnside. Les exemples peuvent être internes à la théorie des groupes (action naturelle de $\mathcal{S}_n$ sur $\{1, 2, \ldots, n\}$, action par translation ou par conjugaison, etc). Mais il est souhaitable d'emprunter aussi à d'autres domaines (action sur des anneaux, des espaces de matrices ou des espaces de polynômes, représentations de groupes, groupes d'isométries, etc). La géométrie fournit aussi de nombreux exemples pertinents (groupes d'isométries d'un solide ou d'un polygone régulier). Pour aller plus loin, on peut aborder l'action de $\mathrm{PGL}(2, \Bbbk)$ sur la droite projective menant au birapport ou celle de $\mathrm{SL}(2, \mathbb{Z})$ sur le demi-plan de Poincaré ou les preuves par actions de groupes des théorèmes de Sylow ou encore d'autres actions donnant lieu à des isomorphismes exceptionnels. Il est aussi possible de s'intéresser aux aspects topologiques ou différentiels liés à certaines actions.

2. Remarques

- Généralités :
  - on dit qu'un groupe G opère sur un ensemble G s'il existe un morphisme de groupes $\mathrm{G} \to \mathcal{S}_E$;
  - l'orbite d'un élément $e \in E$ est par définition le sous-ensemble $\mathcal{O}_\mathrm{G}(e) = \big\{g \cdot e \,|\, g \in \mathrm{G}\big\}$; bien sûr si e' appartient à $\mathcal{O}_\mathrm{G}(e)$, alors $\mathcal{O}_\mathrm{G}(e) = \mathcal{O}_\mathrm{G}(e')$;
  - le stabilisateur de $e \in E$ est par définition le sous-groupe
  $$\mathrm{Stab}_\mathrm{G}(e) = \big\{g \in \mathrm{G} \,|\, g \cdot e = e\big\};$$
  si $e' = g \cdot e$, alors $\mathrm{Stab}_\mathrm{G}(e') = g\,\mathrm{Stab}_\mathrm{G}(e)\,g^{-1}$;
  - on a $|\mathcal{O}_\mathrm{G}(e)| = [\mathrm{G} : \mathrm{Stab}_\mathrm{G}(e)]$;
  - équation aux classes :
  $$|E| = |E^\mathrm{G}| + \sum_{\substack{\mathcal{O}_\mathrm{G}(e) \in \mathcal{O} \\ |\mathcal{O}_\mathrm{G}(e)| \neq 1}} |\mathcal{O}_\mathrm{G}(e)|$$
  où $\mathcal{O}$ est l'ensemble des orbites ;
  - formule de Burnside : $\displaystyle\sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)| = |\mathcal{O}| \cdot |\mathrm{G}|$;
  - l'action est fidèle si $\mathrm{G} \to \mathcal{S}_E$ est injective ;
  - l'action est transitive s'il n'y a qu'une seule orbite ; notion d'action n-transitive.
- Cas où E est un groupe :
  - $E = \mathrm{G}$: il y a trois actions classiques, translation à gauche, à droite par g^{-1} et par conjugaison ;
    - on s'intéresse en particulier aux classes de conjugaison (par exemple le groupe symétrique avec la décomposition en cycles à supports disjoints),
    - le centre d'un p-groupe n'est pas réduit à l'élément neutre,
    - tout corps fini est commutatif.
  - E est un sous-groupe de G :

    - ∗ s'il est distingué on peut faire opérer G par conjugaison (par exemple soit H un sous-groupe distingué de cardinal p dans un p-groupe, montrer que H est contenu dans le centre),
    - ∗ les classes de similitude, d'équivalence, de congruence avec les matrices.
  - — E est un quotient de G :
    - ∗ soit H un sous-groupe de $\mathcal{S}_n$ d'indice $1 < k < n$ (resp. $k = n$), montrer que $k = 2$ et $\mathrm{H} = \mathcal{A}_n$ (resp. $\mathrm{H} \simeq \mathcal{S}_{n-1}$) ;
    - ∗ soit H un sous-groupe d'indice p de G où p est le plus petit premier divisant $|\mathrm{G}|$, en déduire que $\mathrm{H} \triangleleft \mathrm{G}$.
  - — E est un ensemble de sous-groupes de G :
    - ∗ théorème de Sylow,
    - ∗ si G possède un 2-Sylow cyclique, alors G n'est pas simple.
  - — E est un autre groupe : on demande que $\mathrm{G} \to \mathcal{S}_E$ s'envoie sur $\mathrm{Aut}(E)$ ce qui permet de définir la notion de produit semi-direct :
    - ∗ groupe diédral,
    - ∗ trouver tous les groupes d'ordre 30.
- De la géométrie :
  - — opération transitive de $\mathrm{GL}(n, \Bbbk)$ sur les bases de $\Bbbk^n$ ce qui dans le cas réel nous amène à la notion d'orientation ;
  - — les différentes géométries : affines (rapport de proportionnalité), projectives (birapport), semblables (angles), hyperboliques (angles hyperboliques)...
  - — sous-groupes finis de $\mathrm{SO}(3, \mathbb{R})$ et polyèdres réguliers ;
  - — lemme du ping-pong ;
  - — classification des quadriques projectives ;
  - — décomposition de Bruhat : $\mathrm{T}(n, \mathbb{C}) \setminus \mathrm{GL}(n, \mathbb{C}) / \mathrm{T}(n, \mathbb{C}) \simeq \mathcal{S}_n$ où $\mathrm{T}(n, \mathbb{C})$ désigne l'ensemble des matrices triangulaires supérieures. On interprète ce résultat en termes de drapeaux : l'ensemble des classes de paires de drapeaux complets sous l'action de $\mathrm{GL}(n, \mathbb{C})$ est en bijection avec $\mathcal{S}_n$;
  - — groupe circulaire ;
  - — un groupe libre de rang 2 dans $\mathrm{SO}(3, \mathbb{R})$ et paradoxe de Banach-Tarski ;
  - — groupes de pavages (euclidiens, sphériques ou hyperboliques) ;
  - — $\mathrm{PGL}(n, \Bbbk)$ agit sur $\mathbb{P}^{n-1}(\Bbbk)$: applications à $n = 2$, 3 et $\Bbbk = \mathbb{F}_2$, $\mathbb{F}_3$;
  - — action d'un groupe topologique : si G est un groupe topologique compact agissant sur un espace séparé X alors pour tout $x \in X$, $\mathrm{G} / \mathrm{Stab}_{\mathrm{G}}(X) \to \mathcal{O}_{\mathrm{G}}(x)$ est un homéomorphisme (par exemple $\mathrm{SO}(n) / \mathrm{SO}(n-1)$ et $\mathbb{S}^{n-1}$ sont homéomorphes de sorte qu'en particulier $\mathrm{SO}(n)$ est connexe) ;
  - — quaternions et groupe orthogonal.
- De la combinatoire :
  - — soit G un groupe d'ordre pq qui opère sur un ensemble E de cardinal $n = pq - p - q$; montrer qu'il existe au moins un point fixe et que n est le plus grand cardinal tel que cet énoncé soit vrai ;

— nombre de coloriages du cube avec c couleurs ;
— colliers de perles avec 4 bleues, 3 rouges et 2 vertes.

- Théorie des représentations des groupes finis : exemple du groupe symétrique.
- Polynômes symétriques et antisymétriques.

3. Questions

(1) Soit G un groupe fini. Soit p le plus petit nombre premier divisant $|\mathrm{G}|$. Soit H un sous-groupe de G d'indice p. On se propose de montrer que H est distingué dans G.

a) Montrer que H opère sur l'ensemble des classes à gauche G/H par $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ pour tout $h \in \mathrm{H}$ et pour tout $a \in \mathrm{G}$.

Quel est le stabilisateur de $a\mathrm{H}$?

Quelle est l'orbite de la classe H ?

b) Montrer que si H n'était pas distingué dans G, alors au moins une des orbites aurait un cardinal $\geq p$.

c) Conclure.

(2) Soit E un espace vectoriel de dimension finie n sur un corps $\Bbbk$.

a) Faisons opérer le groupe linéaire $\mathrm{G} = \mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par $g \cdot F := g(F)$ pour tout $g \in \mathrm{G}$ et tout sous-espace F de E. Quelles sont les orbites pour cette action ?

b) On prend $\Bbbk = \mathbb{Z}/7\mathbb{Z}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

(3) a) Combien y a-t-il d'opérations du groupe $\mathbb{Z}/4\mathbb{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?

b) Soient G et X deux groupes. On dit que G *opère par automorphismes sur* X si on s'est donné une opération $(g, x) \mapsto g \cdot x$ de G sur X telle que pour tout $g \in \mathrm{G}$ l'application $x \mapsto g \cdot x$ soit un automorphisme de X.

L'opération de G sur lui-même par translation est-elle une opération par automorphismes ?

L'opération de G sur lui-même par conjugaison est-elle une opération par automorphismes ?

c) Si $\mathrm{G} = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathbb{Z}/13\mathbb{Z}, +\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

d) Si $\mathrm{G} = \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathcal{S}_3, \circ\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

(4) Soit E un espace euclidien. On fait opérer le groupe orthogonal $\mathrm{O}(E)$ de E sur l'ensemble des sous-espaces vectoriels de E.

a) Quelles sont les orbites pour cette action ?

b) Donner un énoncé analogue pour les espaces hermitiens.

c) Y a-t-il un énoncé analogue pour le groupe orthogonal $\mathrm{O}(q)$ d'un espace vectoriel de dimension finie muni d'une forme quadratique non dégénérée q ?

(5) Soit G un groupe. Soit g un élément de G. On appelle *centralisateur* de g l'ensemble G_g des éléments h de G tels que $hg = gh$.

a) Montrer que G_g est un sous-groupe de G. Est-il toujours distingué dans G ?

b) Supposons que G soit fini. Soit C la classe de conjugaison de g. Trouver une relation entre $|\mathrm{G}|$, $|C|$ et $|\mathrm{G}_g|$.

(6) Soit G un groupe opérant sur un ensemble X. Si (g, x) appartient à $\mathrm{G} \times X$ quelle relation peut-on écrire entre $\mathrm{Stab}(x)$ et $\mathrm{Stab}(g \cdot x)$?

(7) Soit G un groupe d'ordre 33 agissant sur un ensemble X de cardinal 19. Montrer qu'il existe une orbite de cardinal 1.

(8) Pour chaque polyèdre régulier et convexe $\mathcal{P}$ d'un espace euclidien $\mathcal{E}$ de dimension 3 déterminer le nombre d'isométries de $\mathcal{E}$ préservant $\mathcal{P}$.

(9) Combien de colliers de 9 perles différents peut-on faire avec 4 perles bleues, 3 perles blanches et 2 perles oranges ?

(10) Montrer que nous avons les isomorphismes suivants

$$\mathrm{PGL}(2, \mathbb{F}_2) \simeq \mathcal{S}_3, \qquad \mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4, \qquad \mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4, \qquad \mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5.$$

(11) Soit $\Bbbk$ un corps commutatif. Considérons l'action du groupe $\mathrm{GL}(m, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$ sur $\mathrm{M}_{m,n}(\Bbbk)$ définie par $\big((P, Q), M\big) \mapsto PMQ^{-1}$.

Déterminer le nombre d'orbites de cette action.

(12) Soit $\Bbbk$ un corps commutatif. Considérons l'action de $\mathrm{GL}(n, \Bbbk)$ sur $\mathrm{Sym}(n, \Bbbk)$ définie par

$$(P, S) \mapsto PS{}^{\mathrm{t}}P$$

a) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{C}$.

b) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{R}$.

c) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk = \mathbb{F}_p$ lorsque p désigne un nombre premier impair.

(13) Soit G un groupe d'ordre $n \in \mathbb{N}^*$ et soit $\Bbbk$ un corps commutatif. Montrer qu'il existe un morphisme de groupes injectif de G dans $\mathrm{GL}(n, \Bbbk)$.

(14) Soit G un groupe d'ordre $2m$ avec $m \in \mathbb{N}^*$ impair. Montrer que G admet un sous-groupe d'indice 2.

(15) Déterminer les groupes finis admettant exactement deux classes de conjugaison.

(16) Déterminer les groupes finis admettant exactement trois classes de conjugaison.

(17) Construire un morphisme surjectif de $\mathcal{S}_4$ sur $\mathcal{S}_3$.

(18) Soit G un groupe d'ordre p^n où n appartient à $\mathbb{N}^*$ et p est un nombre premier. Montrer que le centre de G n'est pas trivial.

(19) Soit G un groupe d'ordre infini. Supposons que G admette un sous-groupe propre H d'indice fini. Montrer que G n'est pas simple.

(20) Soit G un groupe fini d'ordre $n \geq 2$. Soit p le plus petit facteur premier de n. Montrer que si H est un sous-groupe distingué de G d'ordre p alors H est central.

(21) Soit $n \geq 5$.

a) Montrer qu'un sous-groupe H d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

b) En utilisant les théorèmes de Sylow sur les 5-Sylow de $\mathcal{S}_5$ construire un sous-groupe de $\mathcal{S}_6$ d'indice 6 qui n'est pas de la forme

$$\mathcal{S}_6(i) = \left\{\sigma \in \mathcal{S}_6 \,|\, \sigma(i) = i\right\}$$

avec $1 \leq i \leq 6$.

(22) Groupes et propriétés géométriques de l'orbite.

Soit E un espace affine euclidien. Soit f un élément du groupe $\mathrm{Isom}(E)$ des isométries de E. Soit G le sous-groupe de $\mathrm{Isom}(E)$ engendré par f. Soit p un point de E. Montrer que les assertions suivantes sont équivalentes :

(a) L'orbite de p sous G est bornée ;

(b) Toute orbite sous G d'un point de E est bornée ;

(c) f a un point fixe.

(23) Quelles sont les classes de conjugaison de $\mathcal{S}_n$?

(24) Réaliser $\mathcal{S}_3$ comme un sous-groupe de $\mathrm{GL}(2, \mathbb{R})$.

(25) A-t-on $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right) \simeq \mathcal{S}_3$?

(26) Combien y a-t-il de matrices nilpotentes 5×5 à coefficients réels à conjugaison près ?

(27) Combien y a-t-il de matrices nilpotentes à coefficients dans $\mathbb{F}_q$?

4. Éléments de réponses

(1) a) On peut vérifier que $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ est bien définie : si $a\mathrm{H} = b\mathrm{H}$, alors $(ha)\mathrm{H} = (hb)\mathrm{H}$ donc $h \cdot (a\mathrm{H})$ ne dépend pas du représentant a choisi dans une même classe à gauhe), et que ceci définit une opération de groupe.
Le stabilisateur de $a\mathrm{H}$ est $\mathrm{H} \cap a\mathrm{H}a^{-1}$ car dire que $h \in \mathrm{H}$ vérifie $h \cdot (a\mathrm{H}) = a\mathrm{H}$ signifie que $a^{-1}(ha)$ appartient à H ou encore que h appartient à $a\mathrm{H}a^{-1}$.
L'orbite de H est réduite à H.

b) Si H n'est pas distingué dans G, alors il y a au moins une orbite dont le cardinal n'est pas 1 puisque cela signifie qu'il existe $a \in \mathrm{G}$ et $h \in \mathrm{H}$ tel que $a^{-1}(ha)$ n'appartient pas à H. Puisque le cardinal de cette orbite divise celui de H (donc aussi celui de G par le théorème de Lagrange) ce cardinal est au moins p étant donné que p est le plus petit diviseur ≥ 2 de $|\mathrm{G}|$.

c) Si G n'est pas distingué dans G, alors il y a au moins une orbite de cardinal au moins p mais il y a aussi une orbite de cardinal 1 (celle de H). L'équation aux classes assure alors que $\left|\mathrm{G}/\mathrm{H}\right| \geq p + 1$: contradiction avec le fait que $[\mathrm{G} : \mathrm{H}] = p$.

(2) a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement si F et G sont des sous-espaces de dimension d, on choisit une base $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \ldots, n$.

b) Fixons un sous-espace F de dimension 3 (on sait qu'il y en a au moins 1). D'après a) le nombre cherché est le cardinal de l'orbite de F sous l'action de $\mathrm{GL}(E)$ ou encore l'ordre de $\mathrm{GL}(E)$ divisé par celui du stabilisateur S de F. Le cardinal de $\mathrm{GL}(E)$ est obtenu en comptant le nombre de bases de E, il vaut

$$(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4).$$

En prenant une base de F que l'on complète en une base de E on voit que S est isomorphe au groupe des matrices-bloc de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où $A \in \mathrm{GL}(3, \mathbb{F}_7)$, $B \in \mathrm{M}_{3,2}(\mathbb{F}_7)$ et $C \in \mathrm{GL}(2, \mathbb{F}_7)$. Ainsi

$$|S| = (7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6.$$

Par suite le cardinal cherché est

$$\begin{aligned}
&\frac{(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4)}{(7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6} \\
&\quad = \frac{7 \times 7^2 \times 7^3 \times 7^4 \times (7^5-1)(7^4-1)(7^3-1)(7^2-1)(7-1)}{7 \times 7^2 \times 7 \times 7^6 \times (7^3-1)(7^2-1)(7-1)(7^2-1)(7-1)} \\
&\quad = \frac{(7^5-1)(7^4-1)}{(7^2-1)(7-1)} \\
&\quad = 140050
\end{aligned}$$

(3) a) On cherche le nombre de morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans le groupe des permutations $\mathcal{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\overline{1})$) dans $\mathcal{S}_5$. Or $\mathcal{S}_5$ contient

— un élément d'ordre 1 (l'identité),
— $\binom{5}{2} = 10$ transpositions,
— $5 \cdot 3 = 15$ doubles transpositions (cinq façons de choisir le point fixe puis trois double transpositions avec les quatre éléments restants),
— $5 \cdot 6 = 30$ 4-cycles (cinq façons de choisir le point fixe et six 4-cycles dans le groupe des permutations des quatre éléments restants).

Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.

b) L'opération de G sur lui-même par translation n'est pas une opération par automorphismes.

L'opération de G sur lui-même par conjugaison est une opération par automorphismes.

c) Le groupe des automorphismes de X est isomorphe au groupe multiplicatif de l'anneau $\mathbb{Z}/13\mathbb{Z}$ (en effet si on pose $\varphi_a(x) = ax$ on peut vérifier que $a \mapsto \varphi_a$ est un isomorphisme de $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ sur $\mathrm{Aut}(X)$) lequel est isomorphe au groupe additif $\mathbb{Z}/12\mathbb{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ou encore le nombre d'éléments de $\mathbb{Z}/12\mathbb{Z}$ d'ordre divisant 3. Il y a ainsi 3 possibilités.

d) Les seuls automorphismes de $\mathcal{S}_3$ sont intérieurs. Le groupe des automorphismes de $\mathcal{S}_3$ est donc isomorphe à $\mathcal{S}_3$ quotienté par son centre, c'est-à-dire à $\mathcal{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathcal{S}_3$ et il y a 3 possibilités.

(4) a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement si F et G sont des sous-espaces de dimension d, on choisit une base orthonormée $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base orthonormée $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base orthonormée $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base orthonormée $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \ldots, n$.

b) Idem en remplaçant le groupe orthogonal de E par le groupe unitaire de E.

c) Il est clair que si F est un sous-espace une condition nécessaire pour qu'un autre sous-espace G soit dans l'orbite de F est que les restrictions de q à F et G soient des formes quadratiques isomorphes (ce qui entraîne en particulier $\dim F = \dim G$ mais n'est pas équivalent à cette condition. Cette condition est en fait suffisante mais c'est un énoncé difficile, le théorème de Witt ([Per82]).

(5) a) Il est immédiat que G_g est un sous-groupe de G mais il n'est pas toujours distingué dans G : par exemple dans $\mathcal{S}_3$ le centralisateur d'une transposition τ n'est pas distingué dans $\mathcal{S}_3$.

b) La groupe G opère par conjugaison sur lui-même. Par définition C est l'orbite de g et G_{g_0} son stabilisateur d'où

$$|\mathrm{G}| = |C| \cdot |\mathrm{G}_g|.$$

(6) Nous avons $\mathrm{Stab}(g \cdot x) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

(7) Utiliser la formule des classes.

(8) Le groupe $\mathrm{Isom}(\mathcal{P})$ agit transitivement sur $\mathcal{P}$; il suffit donc de déterminer l'ordre du stabilisateur d'un sommet de $\mathcal{P}$.

(9) Il faut compter le nombre d'orbites en considérant l'action du groupe diédral D_9 sur un polygone régulier à 9 côtés dont on a coloré les sommets en suivant l'énoncé. En utilisant la formule de Burnside on trouve que l'on peut réaliser 76 colliers distincts.

(10) Le groupe $\mathrm{PGL}(n, \mathbb{F}_q)$ agit fidèlement sur les droites de $\mathbb{F}_q^n$.

(11) Il s'agit de classer les matrices à équivalence près. On en déduit qu'il y a $\min(m, n) + 1$ orbites.

(12) Il s'agit de classer les formes bilinéaires sur $\Bbbk^n$.
— Si $\Bbbk = \mathbb{C}$, alors il y a $n + 1$ orbites.
— Si $\Bbbk = \mathbb{R}$, alors il y a $\frac{(n+2)(n+1)}{2}$ orbites.
— Si $\Bbbk = \mathbb{F}_p$, alors il y a $2n + 1$ orbites.

(13) Utiliser le théorème de Cayley.

(14) Utiliser le théorème de Cayley.

(15) Avec la formule des classes on trouve $\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z}$.

(16) La formule des classes assure qu'il existe un couple (a, b) dans $\mathbb{N}^2$ tel que $1 \leq b \leq a \leq |\mathrm{G}|$ et

$$1 = \frac{1}{|\mathrm{G}|} + \frac{1}{a} + \frac{1}{b}.$$

Nous en déduisons que $1 \leq b \leq 3$ puis en étudiant les différents cas nous obtenons que $\mathrm{Card}(\mathrm{G}) \leq 6$. Finalement nous obtenons que $\mathrm{G} \simeq \mathbb{Z}/3\mathbb{Z}$ ou $\mathrm{G} \simeq \mathcal{S}_3$.

(17) Faire agir $\mathcal{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathcal{S}_4$ qui ne sont pas des transpositions.

(18) Faire agir G sur lui-même et utiliser la formule des classes.

(19) Faire agir G sur G/H par translation des classes.

(20) Faire agir G sur H par conjugaison. Étudier le cardinal de chaque orbite pour obtenir qu'elles sont des singletons.

(21) a) Faire agir $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ par translation. Comme nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que le morphisme

$$\varphi \colon \mathrm{H} \to \mathrm{Bij}\left(\mathcal{S}_n/\mathrm{H}\right)$$

est injectif. De plus les éléments de $\varphi(\mathrm{H})$ fixent la classe H d'où le résultat.

b) Le troisième théorème de Sylow assure que $\mathcal{S}_5$ compte six 5-Sylow. Faisons agir $\mathcal{S}_5$ par conjugaison sur l'ensemble X des 5-Sylow. On obtient un morphisme de groupes

$$\varphi \colon \mathcal{S}_5 \to \mathrm{Bij}(X).$$

Le premier théorème de Sylow assure que cette action est transitive. Puisque nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que φ est injective. Finalement l'image de φ répond à la question.

(22) Montrons que (c) implique (a).

Par hypothèse il existe $m \in E$ tel que $f(m) = m$. Pour tout $k \in \mathbb{N}$ nous avons

$$d(m, f^k(p)) = d(f^k(m), f^k(p)) = d(m, p)$$

ainsi l'orbite de p sous G est bornée.

Montrons que (a) implique (b).

Il existe $r > 0$ tel que $d(p, f^k(p)) \leq r$ pour tout $k \in \mathbb{N}$. Soit m un point de E alors $d(f^k(p), f^k(m)) = d(p, m)$. Par conséquent

$$d(p, f^k(m)) \leq d(p, f^k(p)) + d(f^k(p), f^k(m)) \leq r + d(p, m).$$

Montrons que (b) implique (c).

Le théorème de la forme réduite des isométries de E implique l'existence de $g \in \mathrm{Isom}(E)$ avec un point fixe p et $\overrightarrow{v} \in \ker(f - \mathrm{id}_E)$ tel que $f = t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$. Ainsi $f^k(A) = A + k\overrightarrow{v}$ et donc $d(A, f^k(A)) = k||\overrightarrow{v}|| \to +\infty$ si $\overrightarrow{v} \neq \overrightarrow{0}$. Puisque la suite $(f^k(A))_k$ est bornée nous obtenons que $\overrightarrow{v} = \overrightarrow{0}$ ainsi $f = g$ a un point fixe.

(23) Le groupe $\mathcal{S}_3$ agit (linéairement) sur le sous-espace de dimension 2

$$E = \left\{(x, y, z) \in \mathbb{R}^3 \,|\, x + y + z = 0\right\}$$

par permutation des coordonnées. On obtient un morphisme de groupes

$$\mathcal{S}_3 \to \mathrm{GL}(E) \simeq \mathrm{GL}(2, \mathbb{R})$$

qui est clairement injectif ! Si on prend pour base de E les vecteurs $v_1 = (1, -1, 0)$ et $v_2 = (0, 1, -1)$ on obtient le morphisme suivant

$$(1\ 2) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \qquad\qquad (2\ 3) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$$

(24) On peut par exemple faire agir $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ sur les trois éléments non nuls de $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

(25) D'après la forme réduite de Jordan des matrices nilpotentes il y en a autant que de partitions de 5, *i.e.* 7.

(26) Une matrice nilpotente non nulle est conjuguée à la matrice

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Pour l'action de $\mathrm{GL}(2, \mathbb{F}_q)$ par conjugaison le stabilisateur de cette matrice est le sous-groupe des matrices de la forme

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

où $a \in \mathbb{F}_q^\times$ et $b \in \mathbb{F}_q$ ce qui fait un groupe d'ordre $q(q-1)$. Il y a donc $\frac{|\mathrm{GL}(2, \mathbb{F}_q)|}{q(q-1)} = q^2 - 1$ matrices nilpotentens non nulles...

5. Développements possibles

- ◇ Classification des groupes d'ordre p^2, [Szp08, Chapitre 3, exercice 3].
- ◇ Des isomorphismes exceptionnels des groupes linéaires projectifs d'un corps fini, [Per82, p. 106].
- ◇ Générateurs de $\mathcal{S}_n$, [Com98, p. 79-81].
- ◇ Théorème de Sylow (version opération de groupes), [Per82, p. 18-20].
- ◇ Les sous-groupes finis de $\mathrm{SO}(3,\mathbb{R})$, [CG17, chap. 12], [CG15, chap. 9], [Szp09, p. 434-437].
- ◇ Automorphismes de $\mathcal{S}_n$, [Per82, p. 30].
- ◇ Théorème de Wedderburn, [Per82, p. 82].
- ◇ Détermination des groupes d'isométries du cube et du tétraèdre, [CG17, CG15, CP19].
- ◇ Dénombrement des colorations du cube, [CP19, p. 141-142].
- ◇ Théorème de Brauer, [FGN09].
- ◇ $\mathcal{A}_5$ est l'unique groupe simple d'ordre 60, [Szp08, p. 99, 126-127].
- ◇ Nombre de matrices sur un corps finis de polynôme caractéristique donné, [FGN09, CG17].

5.1. Classification des groupes d'ordre p^2.

Référence : [Szp08, Chapitre 3, exercice 3]

Exercice 1

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

(1) Supposons G non abélien. Soit g un élément de $\mathrm{G}\setminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.

Montrer que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).

(2) En déduire que si G n'est pas abélien, alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier divisant l'ordre $|\mathrm{G}|$ de G.

(3) Soit p un nombre premier. Soit n un entier.

Quelles sont les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n ?

Quel est le centre d'un groupe d'ordre p^2 ?

Quel est le centre d'un groupe non abélien d'ordre p^3 ?

(4) Donner un exemple de groupe d'ordre p^3 non abélien.

(5) Montrer que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Éléments de réponse 1

Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

(1) Supposons G non abélien. Soit g un élément de $\mathrm{G}\setminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.

Montrons que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).

L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{Stab}(g)$ est claire.

Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{Stab}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{Stab}(g)$.

Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Puisque $g \notin Z(\mathrm{G})$ il existe un élément $h \in \mathrm{G}$ qui ne commute pas avec g donc qui n'appartient pas à $\mathrm{Stab}(g)$. Il en résulte que $\mathrm{Stab}(g)$ est un sous-groupe propre de G.

(2) Supposons que G ne soit pas abélien, montrons qu'alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier p divisant l'ordre $|\mathrm{G}|$ de G.

D'après 1. si G n'est pas abélien et si g appartient à $\mathrm{G} \setminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{Stab}(g)|$. Mais $|\mathrm{G} : \mathrm{Stab}(g)| \geq p$ car $|\mathrm{G} : \mathrm{Stab}(g)|$ divise $|\mathrm{G}|$. Par suite $|\mathrm{G} : Z(\mathrm{G})| > p$.

(3) Soit p un nombre premier. Soit n un entier.

Donnons les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n.

Si G est abélien, alors $|Z(\mathrm{G})| = p^n$.

Si G n'est pas abélien, alors $|\mathrm{G} : Z(\mathrm{G})| > p$ donc $|Z(\mathrm{G})| < p^{n-1}$. L'exercice précédent assure que $Z(\mathrm{G})$ n'est pas réduit à l'élément neutre donc $|Z(\mathrm{G})| \geq p$. Finalement lorsque G n'est pas abélien, nous avons

$$|Z(\mathrm{G})| \in \left\{p,\, p^2,\, \ldots,\, p^{n-2}\right\}$$

Si $n = 2$, le groupe G est nécessairement abélien.

Déterminons le centre d'un groupe d'ordre p^2. Le centre d'un groupe G d'ordre p^2 est donc G tout entier.

Déterminons le centre d'un groupe non abélien d'ordre p^3. Le centre d'un groupe non abélien d'ordre p^3 est d'ordre p.

(4) Donnons un exemple de groupe d'ordre p^3 non abélien.

Le groupe des quaternions est un groupe d'ordre 2^3 (ici $p = 2$) et n'est pas abélien.

(5) Montrons que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Soit G un groupe d'ordre p^2. Il est abélien. Nous avons l'alternative suivante :

— ou bien G contient un élément d'ordre p^2 auquel cas G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;

— ou bien tous les éléments de $\mathrm{G} \setminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \setminus \{e\}$ tels que $y \notin \langle x \rangle$. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$. En effet le sous-groupe $\langle x \rangle \cap \langle y \rangle$ est d'ordre strictement inférieur à p et d'ordre divisant p donc d'ordre 1. Puisque tout sous-groupe du groupe abélien G est distingué G est isomorphe à $\langle x \rangle \times \langle y \rangle$ (Exercice 10). Or $\langle x \rangle \simeq \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

5.2. **Isomorphismes exceptionnels.**

Référence : [Per82, p. 106]

Leçons possibles :

101 : Groupe opérant sur un ensemble. Exemples et applications.

103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

104 : Groupes abéliens et non abéliens finis. Exemples et applications.

105 : Groupe des permutations d'un ensemble fini. Applications.

106 : Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.

Quelques rappels

Définitions 1. Soit E un plan vectoriel (*i.e.* un espace vectoriel de dimension 2) sur $\mathbb{k}$.

On appelle *droite projective associée à* E l'ensemble des droites vectorielles de E. Cet ensemble est noté $\mathbb{P}(E)$.

On appelle *droite projective* tout ensemble de la forme $\mathbb{P}(E)$ (pour un certain plan vectoriel E).

La droite projective associée au plan $\mathbb{k}^2$ est notée $\mathbb{P}^1(\mathbb{k})$; elle est appelée *droite projective standard sur* $\mathbb{k}$.

Soit E un plan vectoriel. A tout vecteur $x \in E \setminus \{0\}$ associons la droite vectorielle $\mathbb{k}x$. On définit ainsi une application canonique

$$p\colon E \setminus \{0\} \to \mathbb{P}(E) \qquad\qquad x \mapsto [x].$$

Elle est surjective : si D est une droite vectorielle de E et x un vecteur non nul de D, nous avons $D = \mathbb{k}x = [x]$. La relation d'équivalence $\mathcal{R}$ sur $E \setminus \{0\}$ associée à p est la *relation de colinéarité* : si x et y appartiennent à $E \setminus \{0\}$, alors $x\mathcal{R}y$ équivaut à $\mathbb{k}x = \mathbb{k}y$. Les classes modulo $\mathcal{R}$ sont donc les $D \setminus \{0\}$ où D appartient à $\mathbb{P}(E)$. Nous identifions donc, via p, l'ensemble $\mathbb{P}(E)$ à l'ensemble quotient $E \setminus \{0\}/_{\mathcal{R}}$.

Bien que les éléments de $\mathbb{P}(E)$ soient des droites vectorielles de E nous les appelons aussi des points de la droite projective $\mathbb{P}(E)$.

Définition 1. Soient E et E' deux plans vectoriels. Soit u un isomorphisme linéaire de E sur E'. Notons $[u]$ la bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ définie ainsi : si D appartient à $\mathbb{P}(E)$, alors $[u](D)$ est la droite vectorielle $u(D)$ de E'.

On appelle *homographie* de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ toute bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ de la forme $[u]$ pour un certain isomorphisme u de E sur E'.

Lemme 1. *Soient E et E' deux plans vectoriels. Soient u et v deux isomorphismes de E sur E'. Pour que les homographies $[u]$ et $[v]$ soient égales il faut et il suffit que u et v soient colinéaires.*

Démonstration. Si $v = \lambda u$ pour un certain $\lambda \in \mathbb{k}^*$, alors $v(D) = \lambda(u(D)) = u(D)$ pour toute droite vectorielle D de E donc $[v] = [u]$.

Réciproquement supposons que $[v] = [u]$. Pour tout $x \in E$ non nul il existe alors un scalaire $\lambda_x \in \mathbb{k}^*$ tel que $v(x) = \lambda_x u(x)$. Montrons que l'application

$$E \setminus \{0\} \to \mathbb{k}^*, \qquad\qquad x \mapsto \lambda_x$$

est constante. Soient donc x, y dans $E \setminus \{0\}$. Supposons d'abord que x et y soient linéairement indépendants. Nous avons

$$\lambda_{x+y}u(x) + \lambda_{x+y}u(y) = \lambda_{x+y}u(x+y) = v(x+y) = v(x) + v(y) = \lambda_x u(x) + \lambda_y u(y).$$

Puisque $(u(x), u(y))$ est une famille libre de E' nous obtenons que $\lambda_x = \lambda_{x+y} = \lambda_y$. Si x et y sont liés, considérons un vecteur $z \in E \smallsetminus \Bbbk x$; alors les familles (x, z) et (y, z) sont libres donc d'après ce qui précède $\lambda_x = \lambda_z = \lambda_y$. □

Voici un énoncé essentiel sur les homographies.

Théorème 2. *Soient Δ et Δ' deux droites projectives et t_1, t_2, t_3 (respectivement t'_1, t'_2, t'_3) trois points de Δ (respectivement Δ') distincts. Il existe une unique homographie h de Δ sur Δ' telle que $h(t_i) = t'_i$ pour $i = 1, 2, 3$.*

Démonstration. Il existe deux plans vectoriels E et E' tels que $\Delta = \mathbb{P}(E)$ et $\Delta' = \mathbb{P}(E')$. Pour $i = 1, 2, 3$ le point t_i de Δ est une droite vectorielle D_i de E_i de même le point t'_i de Δ' est une droite vectorielle D'_i de E'. Pour tout i choisissons un vecteur non nul x_i de D_i (respectivement x'_i de D'_i).

Puisque $D_1 \neq D_2$, (x_1, x_2) est une base de E. Il existe donc des scalaires α_1 et $\alpha_2 \in \Bbbk$ uniques tels que $x_3 = \alpha_1 x_1 + \alpha_2 x_2$. En outre D_3 étant distincte de D_1 et D_2, α_1 et α_2 sont non nuls. De même (x'_1, x'_2) est une base de E' et il existe α'_1, $\alpha'_2 \in \Bbbk^*$ tels que $x'_3 = \alpha'_1 x'_1 + \alpha'_2 x'_2$. Posons $\lambda_1 = \frac{\alpha'_1}{\alpha_1}$ et $\lambda_2 = \frac{\alpha'_2}{\alpha_2}$. Soit $u\colon E \to E'$ l'isomorphisme linéaire appliquant x_1 sur $\lambda_1 x'_1$ et x_2 sur $\lambda_2 x'_2$. Ainsi $u(D_i) = D'_i$ pour $i = 1, 2$. De plus

$$u(x_3) = u(\alpha_1 x_2 + \alpha_2 x_2) = \alpha_1 \lambda_1 x'_1 + \alpha_2 \lambda_2 x'_2 = \alpha'_1 x'_1 + \alpha'_2 x'_2 = x'_3$$

d'où $u(D_3) = D'_3$. L'homographie $[u]$ de Δ sur Δ' envoie bien t_i sur t'_i pour $i = 1, 2, 3$.

Soit v un isomorphisme de E sur E' distinct de u et tel que $v(D_i) = D'_i$ pour $i = 1, 2, 3$. Il existe donc β_1, β_2, $\beta_3 \in \Bbbk^*$ tels que $v(x_i) = \beta_i x'_i$ pour $i = 1, 2, 3$. Alors

$$\beta_3(\alpha'_1 x'_1 + \alpha'_2 x'_2) = \beta_3 x'_3 = v(x_3) = v(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 \beta_1 x'_1 + \alpha_2 \beta_2 x'_2$$

d'où $\beta_3 \alpha'_1 = \alpha_1 \beta_1$ et $\beta_3 \alpha'_2 = \alpha_2 \beta_2$. Ainsi $\beta_1 = \lambda_1 \beta_3$ et $\beta_2 = \lambda_2 \beta_3$. Par conséquent $v = \beta_3 u$ car nous avons pour $i = 1, 2$

$$v(x_i) = \beta_i x'_i = \lambda_i \beta_3 x'_i = \beta_3 u(x_i).$$

Il en résulte que $[v] = [u]$. □

Remarque 3. Soit E un plan vectoriel. Si u appartient à $\mathrm{GL}(E)$, l'homographie $[u]$ est en particulier une permutation de $\mathbb{P}(E)$. De plus $u \mapsto [u]$ est un morphisme de $\mathrm{GL}(E)$ dans le groupe $\mathcal{S}_{\mathbb{P}(E)}$ des permutations de $\mathbb{P}(E)$.

Proposition 4. *Soit E un plan vectoriel.*

(1) L'ensemble des homographies de la droite projective $\mathbb{P}(E)$ sur elle-même est un sous-groupe de $\mathcal{S}_{\mathbb{P}(E)}$, nous le notons $\mathrm{PGL}(E)$. Lorsque $E = \Bbbk^2$, le groupe $\mathrm{PGL}(\Bbbk^2)$ est aussi noté $\mathrm{PGL}(2, \Bbbk)$.

(2) L'application

$$\mathrm{GL}(E) \to \mathrm{PGL}(E) \qquad\qquad u \mapsto [u]$$

est un morphisme surjectif dont le noyau est le groupe des homothéties $\left\{\lambda \mathrm{id}_E \,|\, \lambda \in \Bbbk^*\right\}$.

Démonstration. La première assertion résulte de la définition d'une homographie et de la Remarque 3.

Concernant la seconde assertion : la surjectivité résulte de la définition d'une homographie et la description du noyau du Lemme 1 □

L'énoncé suivant est une simple traduction du Théorème 2 lorsque $E = E'$:

Théorème 5. *Soit E un plan vectoriel. L'opération naturelle de $\mathrm{PGL}(E)$, qui est un sous-groupe de $\mathcal{S}_{\mathbb{P}(E)}$, sur $\mathbb{P}(E)$ est simplement 3 fois transitif*[1]*. Autrement dit étant donnés trois points distincts t_1, t_2, t_3 (respectivement t'_1, t'_2, t'_3) de $\mathbb{P}(E)$, il existe une unique homographie h de $\mathrm{PGL}(E)$ telle que $h(t_i) = t'_i$ pour $i = 1, 2, 3$.*

Donnons une interprétation de la droite projective standard $\mathbb{P}^1(\Bbbk)$ et du groupe $\mathrm{PGL}(2, \Bbbk)$ des homographies de cette droite projective. Considérons l'ensemble $\widehat{\Bbbk} = \Bbbk \cup \{\infty\}$ où ∞ est un symbole arbitraire n'appartenant pas à $\Bbbk$.

Lemme 6. *Considérons l'application*

$$\varphi\colon \Bbbk^2 \smallsetminus \{0\} \to \widehat{\Bbbk} \qquad\qquad (x, y) \mapsto \begin{cases} \frac{x}{y} \text{ si } y \neq 0 \\ \infty \text{ si } y = 0 \end{cases}$$

Alors φ induit une bijection Φ de $\mathbb{P}^1(\Bbbk) = {}^{(\Bbbk^2 \smallsetminus \{0\})}\!/_{\mathcal{R}}$ sur $\widehat{\Bbbk}$.

Démonstration. Tout d'abord φ est surjective. En effet $\infty = \varphi((1, 0))$ et $t = \varphi((t, 1))$ pour tout $t \in \Bbbk$.

Soient (x, y) et (x', y') deux éléments de $\Bbbk^2 \smallsetminus \{0\}$. Ces deux couples ont même image par φ si et seulement si $y = y' = 0$ ou $y \neq 0$, $y' \neq 0$ et $\frac{x}{y} = \frac{x'}{y'}$ ce qui équivaut à dire que (x, y) et (x', y') sont colinéaires. La relation d'équivalence associée à l'application φ est donc $\mathcal{R}$ d'où la conclusion par passage au quotient. □

Identifions le groupe $\mathrm{GL}(\Bbbk^2)$ au groupe $\mathrm{GL}(2, \Bbbk)$ des matrices carrées inversibles 2×2 à coefficients dans $\Bbbk$: toute transformation linéaire u de $\Bbbk^2$ est identifiée à sa matrice dans la base canonique de $\Bbbk^2$.

Proposition 7. *Soient $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \Bbbk)$ et h l'homographie de $\mathbb{P}^1(\Bbbk)$ associée à M. La permutation $\widetilde{h} = \Phi \circ h \circ \Phi^{-1}$ de $\widehat{\Bbbk}$ s'obtient ainsi :*

$$\widetilde{h}(z) = \begin{cases} \frac{az+b}{cz+d} \text{ si } z \in \Bbbk \text{ et } cz + d \neq 0 \\ \infty \text{ si } c \neq 0 \text{ et } z = -\frac{d}{c} \end{cases} \qquad\qquad \widetilde{h}(\infty) = \begin{cases} \infty \text{ si } c = 0 \\ \frac{a}{c} \text{ si } c \neq 0 \end{cases}$$

1. Rappelons qu'une action d'un groupe G sur un ensemble E est *simplement transitive* si elle est à la fois transitive et libre, *i.e.* si pour tous x, y dans E il existe un unique $g \in$ G tel que $gx = y$.

Une action d'un groupe G sur un ensemble E (d'au moins n éléments) est dite *n-transitive* si l'action correspondante sur l'ensemble des n-uplets d'éléments distincts est transitive, *i.e.* si pour n points distincts x_1, x_2, …, x_n et n points distincts y_1, y_2, …, y_n quelconques dans E, il existe toujours au moins un élément g de G tel que $g \cdot x_1 = y_1$, $g \cdot x_2 = y_2$, …, $g \cdot x_n = y_n$

Démonstration. Soient $z \in \widehat{\Bbbk}$ et $(x,y) \in \Bbbk^2 \smallsetminus \{0\}$ tels que $z = \varphi((x,y))$ de sorte que $\Phi^{-1}(z)$ est la droite vectorielle $\Bbbk(x,y)$. L'image (x',y') de (x,y) par M est donnée par

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Par définition $\widetilde{h}(z) = \varphi((x',y'))$ c'est-à-dire

$$\widetilde{h}(z) = \varphi((ax+by, cx+dy)).$$

(1) Supposons dans un premier temps que $z \neq \infty$, soit $y \neq 0$. Dans ce cas $z = \frac{x}{y}$ donc $x = zy$ d'où

$$\widetilde{h}(z) = \varphi(y(az+b, cz+d)) = \varphi((az+b, cz+d)).$$

◇ Si $cz + d \neq 0$, alors $\widetilde{h}(z) \in \Bbbk$ est donnée par la formule

$$\widetilde{h}(z) = \frac{az+b}{cz+d}.$$

◇ Supposons que $cz + d = 0$. Comme $(c,d) \neq (0,0)$ nous avons $c \neq 0$ et $z = -\frac{d}{c}$. Alors $\widetilde{h}(z) = \varphi((az+b, 0)) = \infty$.

(2) Supposons que $z = \infty$, *i.e.* que $y = 0$. Alors $x \neq 0$ et

$$\widetilde{h}(\infty) = \varphi(x(a,c)) = \varphi((a,c)).$$

Nous en déduisons que

$$\widetilde{h}(\infty) = \begin{cases} \infty \text{ si } c = 0 \\ \frac{a}{c} \text{ si } c \neq 0 \end{cases}$$

□

Désormais nous identifions via la bijection Φ définie dans le Lemme 6 la droite projective $\mathbb{P}^1(\Bbbk)$ et $\widehat{\Bbbk}$. Cette identification étant faite le groupe $\mathrm{PGL}(2,\Bbbk)$ apparaît comme sous-groupe de $\mathcal{S}_{\widehat{\Bbbk}}$. Plus précisément $\mathrm{PGL}(2,\Bbbk)$ est formé des *transformations homographiques* de $\widehat{\Bbbk}$, *i.e.* des transformations de

$$[M] \colon z \mapsto \frac{az+b}{cz+d} \qquad\qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\Bbbk)$$

avec les trois conventions particulières concernant ∞ données par la Proposition 7. Rappelons que

$$\mathrm{GL}(2,\Bbbk) \to \mathrm{PGL}(2,\Bbbk) \qquad\qquad M \mapsto [M]$$

est un morphisme surjectif dont le noyau est $\{\lambda \mathrm{id} \mid \lambda \in \Bbbk^*\}$. Par ailleurs l'opération naturelle de $\mathrm{PGL}(2,\Bbbk)$ sur $\widehat{\Bbbk}$ est simplement 3 fois transitive comme dans le Théorème 5. L'énoncé suivant donne la description du stabilisateur de ∞ :

Lemme 8. *Le stabilisateur de ∞ dans l'opération naturelle de $\mathrm{PGL}(2,\Bbbk)$ sur $\widehat{\Bbbk}$ est formé des transformations affines de la droite affine $\Bbbk$, i.e. des transformations $f \colon z \mapsto az+b$ où $a \in \Bbbk^*$ et $b \in \Bbbk$, f étant prolongée par $f(\infty) = \infty$.*

Démonstration. La Proposition 7 assure que ce stabilisateur est formé des transformations $[M]$ où $M \in \mathrm{GL}(2,\Bbbk)$ est du type $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ avec a, $d \in \Bbbk^*$ et $b \in \Bbbk$. Si M est de ce type, alors $M = dN$ donc $[M] = [N]$ en posant

$$N = \begin{pmatrix} \frac{a}{d} & \frac{b}{d} \\ 0 & 1 \end{pmatrix}$$

d'où l'énoncé. □

Remarque 9 (Le cas d'un corps de base fini)**.** Supposons que $\Bbbk$ soit un corps fini à q éléments. Nous écrivons aussi $\Bbbk = \mathbb{F}_q$ en désignant par $\mathbb{F}_q$ un corps à q éléments fixé (un tel corps existe et est unique à isomorphisme près). Observons que la droite projective standard $\mathbb{P}^1(\Bbbk)$, identifiée à $\widehat{\Bbbk}$, est de cardinal $q+1$. Il en résulte que toute droite projective $\mathbb{P}(E)$ est de cardinal $q+1$ (considérer une homographie de $\mathbb{P}(E)$ sur $\widehat{\Bbbk}$). Le Théorème 5 assure que $\mathrm{PGL}(E)$ opère simplement 3 fois transitivement sur $\mathbb{P}(E)$, *i.e.* il opère transitivement sur l'ensemble des triplets injectifs (a,b,c) de points de $\mathbb{P}(E)$. Il est clair que cet ensemble est de cardinal $(q+1)q(q-1) = q(q^2-1)$. Il en résulte que

$$|\mathrm{PGL}(E)| = q(q^2-1).$$

À l'opération naturelle et fidèle de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$ est associé un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathcal{S}_{\mathbb{P}(E)}$. En numérotant les points de $\mathbb{P}(E)$ on obtient donc un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathcal{S}_{q+1}$, *i.e.* $\mathrm{PGL}(E)$ est isomorphe à un sous-groupe de $\mathcal{S}_{q+1}$.

Théorème 10. *On a les isomorphismes suivants*

(1) $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{PSL}(2,\mathbb{F}_2) \simeq \mathcal{S}_3$ *;*

(2) $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathcal{S}_4$ *et* $\mathrm{PSL}(2,\mathbb{F}_3) \simeq \mathcal{A}_4$ *;*

(3) $\mathrm{PGL}(2,\mathbb{F}_4) = \mathrm{PSL}(2,\mathbb{F}_4) \simeq \mathcal{A}_5$ *;*

(4) $\mathrm{PGL}(2,\mathbb{F}_5) \simeq \mathcal{S}_5$ *et* $\mathrm{PSL}(2,\mathbb{F}_5) \simeq \mathcal{A}_5$.

Lemme 11. *Tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.*

Démonstration. Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \leq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors : si $\mathrm{H} \not\simeq \mathcal{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q-1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = {}^{\mathcal{S}_n}\!/_{\mathrm{H}}$ d'où un homomorphisme

$$\varphi \colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$. □

Démonstration du Théorème 10. Soit E un $\Bbbk$-espace vectoriel. On introduit l'espace projectif $\mathbb{P}(E)$ associé à E ; c'est l'ensemble des droites vectorielles de E. Le groupe $\mathrm{GL}(E)$ opère sur $\mathbb{P}(E)$ et les homothéties opérant trivialement $\mathrm{PGL}(E)$ opère aussi sur $\mathbb{P}(E)$. De plus $\mathrm{PGL}(E)$ opère fidèlement sur $\mathbb{P}(E)$.

Nous faisons agir $\mathrm{PGL}(2, \mathbb{F}_q)$ sur les droites vectorielles de $(\mathbb{F}_q)^2$. Il y a $q+1$ telles droites de sorte que l'on a un morphisme injectif

$$\varphi \colon \mathrm{PGL}(2, \mathbb{F}_q) \hookrightarrow \mathcal{S}_{q+1}.$$

Par ailleurs le cardinal de $\mathrm{PGL}(2, \mathbb{F}_q)$ est $\frac{(q^2-1)(q^2-q)}{q-1} = q(q^2-1)$; c'est aussi le cardinal de $\mathrm{SL}(2, \mathbb{F}_q)$. Notons aussi que si la caractéristique de $\mathbb{F}_q$ n'est pas 2, alors $\mathrm{PSL}(2, \mathbb{F}_q)$ est d'indice 2 dans $\mathrm{PGL}(2, \mathbb{F}_q)$.

(1) On a $\mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2)$.

(2) Comme $|\mathrm{PGL}(2, \mathbb{F}_3)| = 24$, on a $\mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4$. Puisque $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 dans $\mathcal{S}_4$ on a $\mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4$.

(3) On a $|\mathrm{PGL}(2, \mathbb{F}_4)| = |\mathrm{PSL}(2, \mathbb{F}_4)| = 60$. Puisque $\mathcal{A}_5$ est l'unique sous-groupe d'indice 2 dans $\mathcal{S}_5$ on a $\mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5$.

(4) On a $|\mathrm{PGL}(2, \mathbb{F}_5)| = 120$ donc $\mathrm{PGL}(2, \mathbb{F}_5)$ s'identifie à un sous-groupe d'indice 6 de $\mathcal{S}_6$. Ainsi, d'après le Lemme 11, le groupe $\mathrm{PGL}(2, \mathbb{F}_5)$ est isomorphe à $\mathcal{S}_5$. Il en résulte que

$$\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathcal{A}_5.$$

□

5.3. **Générateurs de $\mathcal{S}_n$.**

Référence : [Com98, p. 79-81]

Leçons possibles :

101 : Groupe opérant sur un ensemble. Exemples et applications.

104 : Groupes abéliens et non abéliens finis. Exemples et applications.

105 : Groupe des permutations d'un ensemble fini. Applications.

108 : Exemples de parties génératrices D'un groupe. Applications.

Théorème 12. *Toute permutation $s \in \mathcal{S}_n$ est un produit de transpositions.*

Proposition 13. *Toute permutation $s \in \mathcal{S}_n$ s'écrit de manière unique (modulo l'ordre des termes) comme un produit de cycles disjoints*

$$s = c_1 c_2 \dots c_p.$$

L'ordre de s est le ppcm des ordres de c_1, c_2, …, c_p.

Proposition 14. *Soient* G *un groupe et $g \in \mathrm{G}$. L'application $f \colon k \mapsto a^k$ est un morphisme de $\mathbb{Z}$ sur le sous-groupe $\langle a \rangle$ engendré par a.*

Si f est injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}$.

Si f n'est pas injectif, alors $\langle a\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ est le plus petit entier non nul tel que $a^n = e$. Dans ce cas, les entiers k tels que $a^k = e$ sont les multiples de n et $\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$.

Proposition 15. *Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. Notons que $0 \in n\mathbb{Z}$. Soient g, g' dans $n\mathbb{Z}$, *i.e.* $g = nk$ et $g' = nk'$ avec k et k dans $\mathbb{Z}$. Ainsi $g - g' = n(k - k')$ appartient à $n\mathbb{Z}$. Il en résulte que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement soit G un sous-groupe de $\mathbb{Z}$. Si G est réduit à $\{0\}$, alors $\mathrm{G} = 0\mathbb{Z}$. Supposons désormais que $\mathrm{G} \neq \{0\}$; alors il existe $g \neq 0$ dans G. Remarquons que $-g \in \mathrm{G}$ donc $\mathrm{G} \cap \mathbb{N}^* \neq \emptyset$. Soit n le plus petit élément de $\mathrm{G} \cap \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$ on a

$$nk = \underbrace{n + n + \ldots + n}_{k \text{ fois}} \in G$$

et $n(-k) = -(nk) \in \mathrm{G}$. Ainsi $n\mathbb{Z} \subset \mathrm{G}$. Soit $g \in \mathrm{G}$ positif. La division de g par n conduit à $g = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{N}$. Il en résulte que

$$r = g - \underbrace{n + n + \ldots + n}_{q \text{ fois}}$$

appartient à G. Supposons r non nul : alors n n'est pas le plus petit élément de $\mathrm{G} \cap \mathbb{N}$: contradiction. Par suite $r = 0$ et $g = nq \in n\mathbb{Z}$. Si $g \in \mathrm{G}$ est négatif, alors $-g \in \mathrm{G}$ est positif et appartient donc à $n\mathbb{Z}$. Il s'en suit que $\mathrm{G} \subset n\mathbb{Z}$ et donc $\mathrm{G} = n\mathbb{Z}$. □

Démonstration de la Proposition 14. L'application $f_0 \colon \mathbb{N} \to \langle a\rangle$, $k \mapsto a^k$ vérifie

$$\forall\, k \in \mathbb{N} \qquad \forall\, k' \in \mathbb{N} \qquad f_0(k + k') = a^{k+k'} = a^k a^{k'} = f_0(k) f_0(k').$$

La propriété universelle du symétrisé $\mathbb{Z}$ de $\mathbb{N}$ permet de prolonger f_0 en un morphisme f de $\mathbb{Z}$ dans $\langle a\rangle$. Pour $k = -|k| < 0$, on a $f(-|k|) = f(|k|)^{-1} = (a^{|k|})^{-1} = a^k$. Par suite $\mathrm{im} f = \{a^k \,|\, k \in \mathbb{Z}\} = \langle a\rangle$.

D'après la Proposition 15 il existe $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. Si $n = 0$, alors f est injective ; c'est un isomorphisme f de $\mathbb{Z}$ dans $\langle a\rangle$. Si n est non nul, le théorème d'isomorphisme assure l'existence d'un isomorphisme $\overline{f}$ entre $\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$ et $\langle a\rangle$. Par définition le noyau de f est l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = e$, c'est-à-dire l'ensemble $n\mathbb{Z}$ des multiples de n. Puisque 0, 1, …, $n-1$ sont des représentants des n classes modulo $n\mathbb{Z}$ leurs images $e = a^0$, a, a^2, …, a^{n-1} par $\overline{f}$ sont les éléments de $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f) = \langle a\rangle$. □

Proposition 16. *Soit E un ensemble. Soit* G *un groupe. Considérons une action à gauche de* G *sur E.*

(i) La relation

$$x \mathcal{R} y \iff (\exists\, g \in \mathrm{G} \quad g \cdot x = y)$$

est une relation d'équivalence sur E.

(ii) Soit $x \in E$; alors

$$\mathrm{G}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$

est un sous-groupe de G.

(iii) Soit $x \in E$, soit $g_0 \in \mathrm{G}$ et soit $y = g_0 \cdot x$. Alors

$$\mathrm{G}_y = g_0 \mathrm{G}_x g_0^{-1} \qquad \big\{g \in \mathrm{G} \,|\, g \cdot x = y\big\} = g_0 \mathrm{G}_x$$

Démonstration. (i) Pour tout $x \in E$ on a $x \mathcal{R} x$ car $e \cdot x = x$; la relation $\mathcal{R}$ est donc réflexive. Si $x \mathcal{R} y$ alors il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ d'où $x = g^{-1} \cdot y$, *i.e.* $y \mathcal{R} x$. Ainsi $\mathcal{R}$ est symétrique. Enfin elle est transitive car

$$(g \cdot x = y \text{ et } g' \cdot y = z) \Rightarrow g'g \cdot x = z$$

(ii) Direct.

(iii) Pour tout g dans G on a d'une part

$$\begin{aligned} g \in \mathrm{G}_y &\iff g \cdot (g_0 \cdot x) = g_0 \cdot x \\ &\iff (g_0^{-1} g g_0) \cdot x = x \\ &\iff g_0^{-1} g g_0 \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x g_0^{-1} \end{aligned}$$

d'autre part

$$\begin{aligned} g \in \big\{g \in \mathrm{G} \,|\, g \cdot x = y\big\} &\iff g \cdot x = y \\ &\iff g \cdot x = g_0 \cdot x \\ &\iff g_0^{-1} g \cdot x = x \\ &\iff g_0^{-1} g \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x \end{aligned}$$

□

Démonstration de la Proposition 13. La Proposition 15 assure que $k \mapsto s^k$ est un morphisme du groupe additif $\mathbb{Z}$ dans $\mathcal{S}_n$. C'est une action de $\mathbb{Z}$ sur l'ensemble $E = \{1, 2, \ldots, n\}$. Soient $\mathcal{O}_1$, $\mathcal{O}_2$, …, $\mathcal{O}_p$ les orbites qui ne sont pas réduites à un point, *i.e.* les orbites des éléments du support de s. Soit i_1 dans $\mathcal{O}_1$. Son stabilisateur est un sous-groupe de $\mathbb{Z}$ donc de la forme $k\mathbb{Z}$ (Proposition 15). Les éléments de $\mathcal{O}_1$ sont

$$i_1,\ i_2 = s(i_1),\ i_3 = s(i_2) = s^2(i_1),\ \ldots,\ i_k = s(i_{k-1}) = s^{k-1}(i_1).$$

D'après la Proposition 16 (iii) ces éléments sont bijectivement associés aux classes de $\mathbb{Z}$ modulo le stabilisateur $k\mathbb{Z}$ et sont donc distincts. On a $s^k(i_1) = i_1$. L'action de s sur l'orbite $\mathcal{O}_1$ est la même que celle du cycle $c_1 = (i_1\ i_2\ \ldots\ i_k)$. De même il existe des cycles c_2, c_3, …, c_p ayant pour supports les orbites $\mathcal{O}_2$, $\mathcal{O}_3$, …, $\mathcal{O}_p$ ayant la même action que s sur ces orbites. Les cycles c_1, c_2, …, c_p commutent car ils sont disjoints et $(c_1 c_2 \ldots c_p)(i) = s(i)$ pour tout point i du support $\bigcup_{m=1}^{p} \mathcal{O}_m$ de s. Les autres éléments de E sont fixes par s et $c_1 c_2 \ldots c_p$ donc $s = c_1 c_2 \ldots c_p$.

Montrons l'unicité (modulo l'ordre des cycles) de l'expression $s = c_1 c_2 \ldots c_p$ par récurrence sur p. Si $p = 0$, *i.e.* si $s = \mathrm{id}$, l'unicité est évidente. Soit $p \geq 1$. Supposons que les permutations pouvant s'exprimer comme produit de moins de p cycles disjoints ont une écriture unique

(modulo l'ordre des cycles). Considérons une permutation s qui est le produit de p cycles disjoints :

$$s = c_1 c_2 \dots c_p$$

Soit $s = c'_1 c'_2 \dots c'_q$ une autre décomposition de s en cycles disjoints. Soit i un élément du support $\mathcal{O}_1$ de c_1. Il appartient au support d'un des cycles c'_j et à un seul. Quitte à réindicer les c'_j on peut supposer que i appartient au support de c'_1. Pour tout r dans $\mathbb{Z}$ on a

$$s^{r(i)} = c_1^{r(i)} = (c'_1)^{r(i)}.$$

Ainsi $c_1 = c'_1$. Par conséquent $c_1 c_2 \dots c_p = c'_1 c'_2 \dots c'_q$ entraîne $c_2 c_3 \dots c_p = c'_2 c'_3 \dots c'_q$. D'après l'hypothèse de récurrence on obtient $p = q$ et $\{c_2, c_3, \dots, c_p\} = \{c'_2, c'_3, \dots, c'_p\}$.

Comme les cycles commutent on a pour tout entier n

$$s^n = c_1^n c_2^n \dots c_p^n$$

Les supports des c_i étant disjoints, $s^n = \mathrm{id}$ si et seulement si $(c_1^n, c_2^n, \dots, c_p^n) = (\mathrm{id}, \mathrm{id}, \dots, \mathrm{id})$, *i.e.* si et seulement si n est multiple commun des ordres $k_1, k_2, \dots, k_p$ de $c_1, c_2, \dots, c_p$. Le plus petit entier strictement positif n tel que $s^n = \mathrm{id}$ est donc $\mathrm{ppcm}(k_1, k_2, \dots, k_p)$. □

Démonstration du Théorème 12. D'après la Proposition 13 il suffit de montrer que tout cycle $(i_1\ i_2\ \dots\ i_p)$ est un produit de transpositions. Montrons par récurrence sur la longueur p du cycle que

$$(i_1\ i_2\ \dots\ i_p) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p).$$

La formule est vraie pour $p = 2$.

Supposons que $p > 2$ et que la formule soit vraie pour $p-1$, *i.e.*

$$(i_1\ i_2\ \dots\ i_{p-1}) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_{p-1});$$

alors

$$(i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_{p-1})(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_p).$$

□

5.4. **Théorèmes de Sylow.**

Référence : [Per82, p. 18-20]

Leçons possibles :

101 : Groupe opérant sur un ensemble. Exemples et applications.

104 : Groupes abéliens et non abéliens finis. Exemples et applications.

103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

D'après le théorème de Lagrange si G est un groupe fini et H un sous-groupe de G, alors |H| divise |G|. Réciproquement on peut se demander si dans un groupe de cardinal n il existe pour tout diviseur d de n un (ou plusieurs) sous-groupe d'ordre d. La réponse est non en général ; par exemple $\mathcal{A}_4$ est un sous-groupe de cardinal 12 qui ne contient pas de sous-groupe d'ordre 6. Néanmoins il y a toute une classe de groupes où cette propriété est vraie, ce sont les sous-groupes de Sylow.

Dans ce paragraphe p désigne un nombre premier.

Définition 2. Un groupe G est un *p-groupe* si tout élément de G a pour ordre une puissance de p.

Exemples 1. Un groupe d'ordre p^α, $\alpha \geq 1$, est un p-groupe.

Un sous-groupe d'ordre p^α d'un groupe G est un p-sous-groupe de G.

Définition 3. Soit G un groupe d'ordre $p^\alpha m$ avec m et p premiers entre eux. Un sous-groupe de G d'ordre p^α est un *p-sous-groupe de Sylow* de G ou un *p-Sylow* de G.

Exemple 1. Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$. Le groupe G est un fini de cardinal

$$|\mathrm{G}| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$

en effet se donner une matrice de G revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. En particulier

$$|\mathrm{G}| = p^{n(n-1)/2} \underbrace{(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1) \dots (p - 1)}_{m}$$

et m est premier à p.

L'ensemble des matrices triangulaires supérieures strictes

$$\mathrm{P} = \left\{ A = (a_{ij}) \,|\, a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1 \right\}$$

est un p-sous-groupe de Sylow de G. En effet comme les a_{ij}, pour $i < j$, sont quelconques on a

$$|\mathrm{P}| = p \times p^2 \times \ldots \times p^{n-1} = p^{n(n-1)/2}.$$

L'énoncé suivant atteste l'existence des sous-groupes de Sylow :

Théorème 17 (Premier théorème de Sylow)**.** *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Il existe au moins un p-Sylow dans G*, c'est-à-dire un sous-groupe d'ordre p^α.*

Remarque 18. Notons que nous n'avons pas supposé $\alpha \geq 1$; si $\alpha = 0$, c'est-à-dire si p ne divise pas $|\mathrm{G}|$, le groupe G admet un unique p-Sylow, à savoir $\{e\}$.

Avant de démontrer ce résultat donnons un lemme qui permet, connaissant un Sylow d'un groupe G d'en trouver un pour un sous-groupe H :

Lemme 19. *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Soient H *un sous-groupe de* G *et soit* S *un p-Sylow de* G*. Alors il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}a^{-1} \cap \mathrm{H}$ soit un p-Sylow de* H*.*

Démonstration. Notons G/S l'ensemble des classes à gauche modulo S (*i.e.* l'ensemble des parties $a\mathrm{S}$ pour $a \in \mathrm{G}$). Le groupe G opère sur G/S par translation à gauche (en posant $g \cdot (a\mathrm{S}) = (ga)\mathrm{S}$). Le stabilisateur

$$\mathrm{Stab}(a\mathrm{S}) = \left\{ g \in \mathrm{G} \,|\, g \cdot a\mathrm{S} = a\mathrm{S} \right\}$$

de $a\mathrm{S}$ est $a\mathrm{S}a^{-1}$. Mais H opère lui aussi sur ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ par restriction avec $a\mathrm{S}a^{-1} \cap \mathrm{H}$ comme stabilisateur de $a\mathrm{S}$.

Montrons qu'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes. Il suffit donc que pour un $a \in \mathrm{G}$, $\left|{}^{\mathrm{H}}\!/_{(a\mathrm{S}a^{-1} \cap \mathrm{H})}\right|$ soit premier à p.

Rappelons que l'application

$$ {}^{\mathrm{G}}\!/_{\mathrm{Stab}(x)} \to \mathcal{O}(x) \qquad\qquad \overline{g} \mapsto g \cdot x $$

de l'ensemble des classes à gauche dans l'orbite de x est bien définie et est une bijection.

Ainsi $\left|{}^{\mathrm{H}}\!/_{(a\mathrm{S}a^{-1} \cap \mathrm{H})}\right| = |\mathcal{O}(a\mathrm{S})|$ où $|\mathcal{O}(a\mathrm{S})|$ désigne le cardinal de l'orbite de $a\mathrm{S}$ dans ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $\left|{}^{\mathrm{G}}\!/_{\mathrm{S}}\right|$ car ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ est réunion des orbites $\mathcal{O}(a\mathrm{S})$: contradiction avec le fait que S est un p-Sylow de G. □

Démonstration du Théorème 17. Soit G un groupe d'ordre fini n. Soit p un diviseur de n. On plonge G dans $\mathcal{S}_n$ (théorème de Cayley). Puis on plonge $\mathcal{S}_n$ dans $\mathrm{GL}(n, \mathbb{F}_p)$: l'élément σ de $\mathcal{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par : $u_\sigma(e_i) = e_{\sigma(i)}$.

On a donc réalisé G comme un sous-groupe de $\mathrm{GL}(n, \mathbb{F}_p)$ qui possède un p-Sylow (Exemple 1), donc G aussi par le Lemme 19. □

Le deuxième théorème de Sylow étudie la conjugaison des p-sous-groupes de Sylow.

Théorème 20 (Second et troisième théorèmes de Sylow)**.** *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Soit n_p le nombre de p-Sylow de G*.*

- ◇ *Si* H *est un p-Sylow de* G *et* K *est un p-sous-groupe de* G*, alors* K *est contenu dans un conjugué de* H *: il existe $g \in \mathrm{G}$ tel que* K *est un sous-groupe de $g\mathrm{H}g^{-1}$, ou encore $g^{-1}\mathrm{K}g \subset \mathrm{H}$.*
- ◇ *Les p-Sylow de* G *sont conjugués deux à deux.*
- ◇ *$n_p \equiv 1$ (mod p) et n_p divise m.*

Remarque 21. Soit G un groupe fini. Soit φ un automorphisme de G.

Si S est un p-Sylow de G, alors $|\varphi(\mathrm{S})| = |\mathrm{S}| = p^\alpha$; ainsi $\varphi(\mathrm{S})$ est un p-Sylow de G.

Si de plus S est l'unique p-Sylow de G, alors $\varphi(\mathrm{S}) = \mathrm{S}$, *i.e.* S est un sous-groupe caractéristique de G.

Corollaire 22. *Si* S *est un p-Sylow de* G*, alors*

$$ \mathrm{S} \triangleleft \mathrm{G} \Leftrightarrow \mathrm{S} \text{ est l'unique } p\text{-Sylow de } \mathrm{G} \Leftrightarrow n_p = 1. $$

Lemme 23. *Soit* G *un p-groupe opérant sur un ensemble E. Soit*

$$ E^{\mathrm{G}} = \left\{ x \in E \,|\, \forall\, g \in \mathrm{G} \quad g \cdot x = x \right\} $$

l'ensemble des points fixes sous G*, alors $|E| \equiv |E^{\mathrm{G}}|$ mod p.*

Démonstration. Écrivons E comme réunion disjointe de ses orbites sous G en remarquant que $x \in E^{\mathrm{G}}$ si et seulement si $\mathcal{O}(x) = \{x\}$. Si x n'appartient pas à E^{G}, alors $|\mathcal{O}(x)| > 1$ et comme

$|\mathcal{O}(x)|$ divise $|\mathrm{G}| = p^n$, p divise $|\mathcal{O}(x)|$. Le résultat provient alors de l'égalité

$$|E| = |E^{\mathrm{G}}| + \sum_{x \notin E^{\mathrm{G}}} |\mathcal{O}(x)|.$$

□

Démonstration du Théorème 20. Si H est un p-sous-groupe de G et si S est un p-Sylow de G, alors d'après le Lemme 19 il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}a^{-1} \cap \mathrm{H}$ soit un p-Sylow de H. Mais comme H est un p-groupe, $a\mathrm{S}a^{-1} \cap \mathrm{H} = \mathrm{H}$. Par suite H est inclus dans $a\mathrm{S}a^{-1}$ qui est un Sylow. Si de plus H est un Sylow on a $\mathrm{H} = a\mathrm{S}a^{-1}$. On a donc montré les deux premières assertions.

Montrons maintenant la troisième assertion.

Faisons opérer G par conjugaison sur l'ensemble E de ses p-Sylow [2] Soit S un p-Sylow, S opère lui aussi sur E et on a (Lemme 23)

$$|E| \equiv |E^{\mathrm{S}}| \bmod p$$

Montrons que $|E^{\mathrm{S}}| = 1$. Bien sûr si $s \in \mathrm{S}$, on a $s\mathrm{S}s^{-1} = \mathrm{S}$, autrement dit $\mathrm{S} \in E^{\mathrm{S}}$. Montrer que $|E^{\mathrm{S}}| = 1$ revient donc à montrer que S est l'unique élément de E^{S}. Soit T un élément de E^{S}, *i.e* T est un p-Sylow tel que :

$$\forall\, s \in \mathrm{S} \quad s\mathrm{T}s^{-1} = \mathrm{T}$$

Considérons le sous-groupe N de G engendré par S et T. On a $\mathrm{S} \subset \mathrm{N}$, $\mathrm{T} \subset \mathrm{N}$ et ce sont a fortiori des p-Sylow de N. Mais comme S normalise T on a $\mathrm{T} \triangleleft \mathrm{N}$. Le Corollaire 22 assure que T est l'unique Sylow de N. Ainsi $\mathrm{S} = \mathrm{T}$.

Les p-Sylow forment une orbite sous G donc n_p divise m (en effet les p-Sylow forment une orbite sous G donc n_p divise $|\mathrm{G}| = p^\alpha m$ et $n_p \equiv 1 \bmod p$). □

Corollaire 24 (Théorème de Cauchy)**.** *Soit* G *un groupe.*

Si p est un nombre premier qui divise l'ordre de G*, alors* G *contient un élément d'ordre p.*

Démonstration. Écrivons $|\mathrm{G}|$ sous la forme $p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.

Raisonnons par l'absurde, *i.e.* supposons qu'aucun élément de G soit d'ordre p. Alors l'ordre de tout élément de G n'est pas divisible par p ; en effet si $|\langle g \rangle| = ap$, alors g^a est d'ordre p. En particulier tout élément du p-Sylow de G (l'existence de ce p-Sylow est assurée par le Premier Théorème de Sylow) est d'ordre non divisible par p et par ailleurs cet ordre divise p^a : contradiction. □

Corollaire 25. *Si* G *est un groupe tel que $|\mathrm{G}| = p^\alpha m$ avec $p \not| m$, alors* G *contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.*

Démonstration. Soit S un p-Sylow de G ; alors $|\mathrm{S}| = p^\alpha$. Puisque S est un p-groupe, $Z(\mathrm{S}) \neq \{e\}$. Le théorème de Cauchy (Corollaire 24) assure l'existence d'un élément g d'ordre p dans $Z(\mathrm{S})$.

Le groupe $\langle g \rangle$ est un sous-groupe de $\mathrm{S} \subset \mathrm{G}$ d'ordre p, nous avons donc montré l'énoncé pour $i = 1$.

Supposons que tout sous-groupe de S d'ordre p^i, $i < \alpha$, contient un sous-groupe d'ordre p^j pour tout entier $j \leq i$. L'hypothèse de récurrence assure l'existence d'un sous-groupe H_{i-1}

2. Si G est un groupe et E l'ensemble de ses sous-groupes, alors G opère sur E par automorphisme intérieur : $g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$.

d'ordre p^{i-1} dans ${}^{\mathrm{S}}\!/_{\langle g\rangle}$. Désignons par $\pi\colon \mathrm{S} \to {}^{\mathrm{S}}\!/_{\langle g\rangle}$. Le groupe $\pi^{-1}(\mathrm{H}_{i-1})$ est un sous-groupe de S et donc de G d'ordre p^i. □

Le cas de $\mathrm{GL}(n, \mathbb{F}_p)$

Soit $\mathbb{F}_p = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ le corps fini à p éléments (p premier). Soit $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$. Nous avons vu dans l'Exemple 1 que l'ensemble des matrices triangulaires supérieures strictes

$$\mathrm{P} = \left\{A = (a_{ij}) \,|\, a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\right\}$$

est un p-sous-groupe de Sylow de G. Le Théorème 20 assure que les p-Sylow de G sont les sous-groupes de la forme $M\mathrm{P}M^{-1}$ où M appartient à $\mathrm{GL}(n, \mathbb{F}_p)$.

5.5. **Sous-groupes finis de** $\mathrm{SO}(3, \mathbb{R})$**.**

Références : [CG17, chap. 12], [CG15, chap. 9], [Szp09, p. 434-437]
Leçons possibles :
101 : Groupe opérant sur un ensemble. Exemples et applications.
104 : Groupes abéliens et non abéliens finis. Exemples et applications.
191 : Exemples d'utilisation des techniques d'algèbre en géométrie.

Théorème 26. *Tout sous-groupe fini de* $\mathrm{SO}(3, \mathbb{R})$ *est isomorphe à* ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, D_{2n}, $\mathcal{A}_4$, $\mathcal{S}_4$ *ou* $\mathcal{A}_5$.

Plus précisément si G *est un sous-groupe fini de* $\mathrm{SO}(3, \mathbb{R})$*, alors* G *est conjugué au groupe des rotations préservant l'un des polyèdres suivants* (*les cas* $n = 1$, 2 *mis à part*)

— $\mathrm{Isom}^+($ *pyramide de base un polygone régulier à* n *côtés* $) \simeq {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$;
— $\mathrm{Isom}^+($ *double pyramide de base un polygone régulier à* n *côtés* $) \simeq \mathrm{D}_{2n}$;
— $\mathrm{Isom}^+($ *tétraèdre régulier* $) \simeq \mathcal{A}_4$;
— $\mathrm{Isom}^+($ *cube* $) \simeq \mathcal{S}_4$;
— $\mathrm{Isom}^+($ *icosaèdre régulier* $) \simeq \mathcal{A}_5$.

Lemme 27 (formule de Burnside)**.** *Soit* G *un groupe fini agissant sur un ensemble fini* E*. Désignons par* $\mathrm{G}\backslash E$ *l'ensemble des orbites et par* $\mathrm{Fix}(g) = \{x \in E \,|\, g \cdot x = x\}$ *l'ensemble des points fixes de* g *dans* E*. Alors*

$$|\mathrm{G}\backslash E| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

Démonstration. Soit $S = \{(x, g) \in E \times \mathrm{G} \,|\, g \cdot x = x\}$. On calcule le cardinal de S de deux façons différentes. D'une part

$$|S| = \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

et d'autre part

$$\begin{aligned}
|S| &= \sum_{x\in E} |\mathrm{Stab}_{\mathrm{G}}(x)| = \sum_{\mathcal{O}\in \mathrm{G}\backslash E} \sum_{x\in\mathcal{O}} |\mathrm{Stab}_{\mathrm{G}}(x)| \\
&= \sum_{\mathcal{O}\in \mathrm{G}\backslash E} \sum_{x\in\mathcal{O}} \frac{|\mathrm{G}|}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O}\in \mathrm{G}\backslash E} \sum_{x\in\mathcal{O}} \frac{1}{|\mathcal{O}|} \\
&= |\mathrm{G}| \sum_{\mathcal{O}\in \mathrm{G}\backslash E} |\mathcal{O}| \cdot \frac{1}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O}\in \mathrm{G}\backslash E} 1 \\
&= |\mathrm{G}| \cdot |\mathrm{G}\backslash E|.
\end{aligned}$$

□

Lemme 28. *Tout sous-groupe fini* G *de* $\mathrm{SO}(2,\mathbb{R})$ *est monogène, engendré par la rotation d'angle* $\frac{2\pi}{n}$ *où* $n = |\mathrm{G}|$.

Démonstration. Si n est un entier, nous notons H_n le sous-groupe de $\mathrm{SO}(2,\mathbb{R})$ formé des rotations d'angle multiple de $\frac{2\pi}{n}$. C'est un sous-groupe d'ordre n engendré par la rotation d'angle $\frac{2\pi}{n}$.

Soit G un sous-groupe de $\mathrm{SO}(2,\mathbb{R})$ d'ordre n. Pour tout g dans G nous avons $g^n = \mathrm{id}$; en particulier tout élément g de G est une rotation d'angle multiple de $\frac{2\pi}{n}$. Autrement dit $\mathrm{G} \subset \mathrm{H}_n$. Par ailleurs $|\mathrm{H}_n| = n$ donc $\mathrm{G} = \mathrm{H}_n$.

□

Esquisse de démonstration du Théorème 26. Soit G un sous-groupe fini d'ordre n de $\mathrm{SO}(3,\mathbb{R})$. À tout élément de $\mathrm{G} \smallsetminus \{\mathrm{id}\}$ on associe deux pôles qui sont l'intersection de l'axe de la rotation avec la sphère unité de $\mathbb{R}^3$. Le groupe G agit sur l'ensemble E des pôles des éléments de G qui est fini et par définition on a l'inégalité suivante

$$|E| \leq 2(n-1).$$

Toute rotation non triviale de G fixe exactement deux pôles et l'identité fixe tous les éléments de G. Par conséquent la formule de Burnside (Lemme 27) assure que le nombre k d'orbites de cette action est

$$k = \frac{2(n-1)+|E|}{n} = 2 + \frac{|E|-2}{n}$$

À partir de $|E| \leq 2(n-1)$ et $k = 2 + \frac{|E|-2}{n}$ on obtient

$$k \leq 2 + \frac{2(n-1)-2}{n} = \frac{4(n-1)}{n} < 4.$$

Ainsi k appartient à $\{2, 3\}$.

a. Si $k = 2$, alors G est cyclique. En effet puisque

$$k = 2 + \frac{|E|-2}{n}$$

on a $k = 2$ si et seulement si $|E| = 2$. Dans ce cas toutes les rotations de G ont le même axe et G peut être vu comme un sous-groupe fini de rotations du plan orthogonal à cet unique axe. Le Lemme 28 implique que G est cyclique.

b. Supposons que $k = 3$. Notons ω_1, ω_2 et ω_3 les orbites ; désignons par n_1, n_2 et n_3 les cardinaux des stabilisateurs correspondants. Quitte à réindicer les n_i on peut supposer que $n_1 \leq n_2 \leq n_3$.

Alors

b.1. si $n_1 = n_2 = 2$, alors $|\mathrm{G}| = |\mathrm{D}_{2n_3}| = 2n_3$;

b.2. sinon on est dans l'une des situations suivantes :
- $\diamond$ $(n_1, n_2, n_3) = (2, 3, 3)$ et $|\mathrm{G}| = |\mathcal{A}_4| = 12$;
- $\diamond$ $(n_1, n_2, n_3) = (2, 3, 4)$ et $|\mathrm{G}| = |\mathcal{S}_4| = 24$;
- $\diamond$ $(n_1, n_2, n_3) = (2, 3, 5)$ et $|\mathrm{G}| = |\mathcal{A}_5| = 60$.

Commençons par déterminer les triplets possibles. La formule de Burnside assure que $3 = 2 + \frac{|E|-2}{n}$. Par ailleurs $|\omega_i| = \frac{n}{n_i}$ donc

$$\frac{|E|}{n} = \frac{|\omega_1| + |\omega_2| + |\omega_3|}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}.$$

Finalement on obtient la condition

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n} \tag{1}$$

Par définition un pôle est fixé par au moins l'identité et une autre rotation donc $n_1 \geq 2$. La condition (1) assure que $n_1 = 2$. Un argument analogue assure que $2 \leq n_2 \leq n_3$. Si $n_2 = 2$ alors n_3 est arbitraire et $n = 2n_3$. Si $n_2 = 3$, alors $3 \leq n_3 \leq 5$ ce qui d'où les trois cas ci-dessus. De plus $n = \frac{12n_3}{6-n_3}$, soit $n = 12$ (resp. $n = 24$, resp. $n = 60$) si $n_3 = 3$ (resp. $n_3 = 4$, resp. $n_3 = 5$).

Traitons par exemple le cas $|\mathrm{G}| = 12$, *i.e.* $(n_1, n_2, n_3) = (2, 3, 3)$. L'orbite ω_3 est de cardinal $\frac{12}{3} = 4$; désignons par x_1, x_2, x_3 et x_4 ses éléments. On peut supposer que x_1 et x_2 ne sont pas symétriques par rapport à l'origine. Puisque $|\mathrm{Stab}(x_1)|\,|\mathrm{Orb}(x_1)| = 12$ il existe une rotation $r \in \mathrm{Stab}(x_1)$ d'ordre 3 ; quitte à réindicer les x_i on a $x_3 = r(x_2)$, $x_4 = r^{-1}(x_2)$. En particulier les points x_2, x_3 et x_4 sont équidistants de x_1. On peut bien entendu faire le même raisonnement pour tout x_i ; on obtient donc que x_1, x_2, x_3 et x_4 sont les sommets d'un tétraèdre régulier préservé par G. Or le groupe des rotations qui préservent un tétraèdre est d'ordre 12 et G est d'ordre 12. Le groupe G coïncide donc avec le groupe des rotations préservant un tétraèdre (isomorphe à $\mathcal{A}_4$ qui est l'unique sous-groupe d'indice 2 dans $\mathcal{S}_4$).

□

Remarque 29. Le groupe $\mathcal{S}_4$ intervient à la fois comme $\mathrm{Isom}^+(\text{cube})$ et comme $\mathrm{Isom}(\text{tétraèdre})$. On peut transposer dans chacun de ces trois points de vue tout ce que l'on sait sur ce groupe (classe de conjugaison, sous-groupes d'ordre donné, etc)

5.6. **Automorphismes de $\mathcal{S}_n$.**

Référence : [Per82, p. 30]

Leçons possibles :

101 : Groupe opérant sur un ensemble. Exemples et applications.

104 : Groupes abéliens et non abéliens finis. Exemples et applications.

105 : Groupe des permutations d'un ensemble fini. Applications.
108 : Exemples de parties génératrices D'un groupe. Applications.

Puisque $n \geq 3$ le centre $Z(\mathcal{S}_n)$ de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$ (Lemme 31). Par suite $\mathcal{S}_n$ agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(\mathcal{S}_n)$ des automorphismes intérieurs de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_n$.

L'énoncé suivant assure que sauf dans le cas exceptionnel $n = 6$ les automorphismes intérieurs sont les seuls automorphismes.

On donne ensuite un automorphisme non intérieur de $\mathcal{S}_6$.

Automorphismes de $\mathcal{S}_n$, $n \neq 6$

Lemme 30. *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

Lemme 31. *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 30)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Théorème 32. *Soit $n \geq 3$. Supposons que $n \neq 6$; alors*

$$\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Int}(\mathcal{S}_n) \simeq \mathcal{S}_n.$$

Lemme 33. *Soit φ un automorphisme de $\mathcal{S}_n$ qui envoie transpositions sur transpositions. Alors φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.*

Démonstration. Les transpositions de la forme $(1\ i)$ où $2 \leq i \leq n$ engendrent $\mathcal{S}_n$. Posons $\tau_i = \varphi(1\ i)$. Remarquons que pour i et j distincts τ_i et τ_j ne commutent pas car $(1\ i)$ et $(1\ j)$ ne commutent pas. Il en résulte que les transpositions τ_i et τ_j ont exactement un élément en commun dans leur support. On peut donc écrire τ_2 et τ_3 sous la forme

$$\tau_2 = (\alpha_1\ \alpha_2) \qquad\qquad \tau_3 = (\alpha_1\ \alpha_3)$$

avec $\alpha_2 \neq \alpha_3$. Montrons que pour tout $k \geq 4$ on a $\tau_k = (\alpha_1\ \alpha_k)$ pour un certain $\alpha_k \in \{1, 2, \ldots, n\}$. En effet si α_1 n'était pas dans le support de τ_k on aurait $\tau_k = (\alpha_2\ \alpha_3)$ et

$$\tau_2 \circ \tau_k = (\alpha_1\ \alpha_2\ \alpha_3) \qquad\qquad \tau_3 \circ \tau_k = (\alpha_1\ \alpha_3\ \alpha_2)$$

seraient inverses l'un de l'autre. Mais

$$(1\ 2)(1\ k) = (2\ 1\ k)$$

n'est pas l'inverse de

$$(1\ 3)(1\ k) = (3\ 1\ k)$$

contradiction.

Notons que $\alpha\colon k \mapsto \alpha_k$ est un élément de $\mathcal{S}_n$.

L'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\ j)$ de $\mathcal{S}_n$; ils coïncident donc sur $\mathcal{S}_n$ tout entier. □

Démonstration du Théorème 32. Soit φ un automorphisme non intérieur de $\mathcal{S}_n$. Montrons que $n = 6$.

D'après le Lemme 33 il existe une transposition τ telle que $\varphi(\tau)$ ne soit pas une transposition. Puisque $(\varphi(\tau))^2 = \mathrm{id}$, $\varphi(\tau)$ est un produit de $k \geq 2$ transpositions à supports disjoints. Désignons par $\mathrm{C}(\tau)$ le centralisateur de τ

$$\mathrm{C}(\tau) = \big\{ f \in \mathcal{S}_n \,|\, f \circ \tau = \tau \circ f \big\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathcal{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi\colon \mathrm{C}(\tau) \to \mathcal{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.

Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \big\{ f \in \mathcal{S}_n \,|\, f \circ \varphi(\tau) = \varphi(\tau) \circ f \big\}$. Les groupes H et $\mathrm{C}(\tau)$ sont isomorphes via φ. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$ donc H contient un sous-groupe N isomorphe à $\big(\mathbb{Z}/2\mathbb{Z}\big)^k$. De plus N est le noyau du morphisme

$$\begin{array}{ccl} \mathrm{H} & \to & \mathcal{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

donc $\mathrm{N} \lhd \mathrm{H}$.

Ainsi comme $\mathrm{C}(\tau) \simeq \mathrm{H}$, $\mathrm{C}(\tau)$ contient un sous-groupe N' avec les deux propriétés suivantes :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq \big(\mathbb{Z}/2\mathbb{Z}\big)^k \end{cases}$$

Via ψ on obtient que $\mathcal{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $\big(\mathbb{Z}/2\mathbb{Z}\big)^k$ ou $\big(\mathbb{Z}/2\mathbb{Z}\big)^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.

Or les sous-groupes distingués de $\mathcal{S}_n$ sont

- ◇ $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathcal{S}_n$ si $n \neq 4$;
- ◇ $\{\mathrm{id}\}$, $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathcal{S}_4$.

On en déduit les deux possibilités suivantes

- ◇ $n = 4$ car $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $\big(\mathbb{Z}/2\mathbb{Z}\big)^{k-1}$ avec $k = 2$;
- ◇ $n = 6$ car $\mathcal{S}_4$ contient $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathcal{S}_4$ est de cardinal 4 (c'est le groupe $\mathcal{K}$) alors que le centralisateur d'une double transposition est de cardinal 8 (en effet il divise strictement 24, est multiple strict de 4 car contient $\mathcal{K}$ mais aussi au moins un 4-cycle) : contradiction.

Ainsi $n = 6$. □

Automorphismes extérieurs de $\mathcal{S}_6$, version 1

Étudions désormais les automorphismes extérieurs de $\mathcal{S}_6$.

Rappelons l'énoncé suivant :

Théorème 34. *Soit $n \geq 5$. Les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Lemme 35. *L'ensemble $\mathrm{Syl}_5(\mathcal{S}_5)$ des 5-sous-groupes de Sylow de $\mathcal{S}_5$ est de cardinal 6.*

Lemme 36. *Numérotons arbitrairement de 1 à 6 les éléments de $\mathrm{Syl}_5(\mathcal{S}_5)$. Faisons opérer $\mathcal{S}_5$ sur $\mathrm{Syl}_5(\mathcal{S}_5) \simeq \{1, 2, 3, 4, 5, 6\}$ par conjugaison. La morphisme $\mathcal{S}_5 \to \mathcal{S}_6$ associé est injectif. Notons G son image.*

Lemme 37. *Numérotons arbitrairement de 1 à 6 les éléments de ${}^{\mathcal{S}_6}\!/_{\mathrm{G}}$. Faisons opérer $\mathcal{S}_6$ sur ${}^{\mathcal{S}_6}\!/_{\mathrm{G}} \simeq \{1, 2, 3, 4, 5, 6\}$ par translations.*

Le morphisme $\varphi\colon \mathcal{S}_6 \to \mathcal{S}_6$ associé est un automorphisme.

Lemme 38. *Le groupe G n'a pas de points fixes sur $\{1, 2, 3, 4, 5, 6\}$.*

Le groupe $\varphi(\mathrm{G})$ admet un point fixe.

L'automorphisme φ n'est pas intérieur.

Démonstration du Lemme 35. On a $|\mathcal{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. L'ordre d'un élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est donc 5. Or 5 est premier donc tout élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est isomorphe à ${}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$. Posons $n_5 = \#\mathrm{Syl}_5(\mathcal{S}_5)$. Les théorèmes de Sylow assurent que

$$\begin{cases} n_5 \equiv 1 \bmod 5 \\ n_5 \text{ divise } 2^3 \cdot 3 = 24 \end{cases}$$

Par conséquent n_5 appartient à $\{1, 6\}$.

Supposons que $n_5 = 1$. Alors $\mathcal{S}_5$ a un unique 5-Sylow qui est distingué : contradiction avec le fait que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$. Par suite $n_5 = 6$. □

Démonstration du Lemme 36. Soit K le noyau du morphisme de $\mathcal{S}_5$ vers $\mathcal{S}_{\mathrm{G}}$. Il est contenu dans le stabilisateur de chacun des éléments de $\mathrm{Syl}_5(\mathcal{S}_5)$. L'action de G sur $\mathrm{Syl}_5(\mathcal{S}_5)$ est transitive (théorème de Sylow). Il en résulte que le stabilisateur de chaque élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ a pour cardinal $\frac{120}{6} = 20$. Donc $|\mathrm{K}|$ divise 20. Puisque K est distingué dans $\mathcal{S}_5$, que $|\mathrm{K}|$ divise 20 et que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$, on obtient que $\mathrm{K} = \{\mathrm{id}\}$. □

Démonstration du Lemme 37. Soit K' le noyau du morphisme naturel de $\mathcal{S}_6$ dans $\mathcal{S}_{{}^{\mathcal{S}_6}\!/_{\mathrm{G}}}$. Il est contenu dans le stabilisateur des éléments de ${}^{\mathcal{S}_6}\!/_{\mathrm{G}}$ et en particulier dans celui de la classe triviale G qui n'est autre que G. Ainsi $|\mathrm{K}'|$ divise $|\mathrm{G}| = 120$. On a donc

$$\begin{cases} \mathrm{K}' \lhd \mathcal{S}_6 \\ |\mathrm{K}'| \text{ divise } 120 \\ \text{les sous-groupes distingués de } \mathcal{S}_6 \text{ sont } \{\mathrm{id}, \mathcal{A}_6, \mathcal{S}_6\} \end{cases}$$

d'où $\mathrm{K}' = \{\mathrm{id}\}$. Autrement dit le morphisme φ est injectif. Pour des raisons de cardinalité φ est bijectif. □

Démonstration du Lemme 38. Si G avait un point fixe sur $\{1, 2, 3, 4, 5, 6\} \simeq \mathcal{S}$ cela signifierait qu'il existe un 5-sous-groupe de Sylow invariant par conjugaison, *i.e.* distingué, ce qui est absurde. Par contre $\varphi(\mathrm{G})$ a un point fixe, celui qui correspond à la classe triviale G, invariante sous l'action de G par translation.

Supposons que φ soit intérieur donc de la forme

$$\sigma \mapsto \sigma_0 \circ \sigma \circ \sigma_0^{-1}$$

pour un certain σ_0. Soit p un point fixe de $\varphi(\mathrm{G})$. On aurait alors pour tout $g \in \mathrm{G}$

$$\begin{aligned} g(\sigma_0^{-1}p) &= \sigma_0^{-1}(\sigma_0(g(\sigma_0^{-1}(p)))) \\ &= \sigma_0^{-1}((\sigma_0 \circ g \circ \sigma_0^{-1})(p)) \\ &= \sigma_0^{-1}(\varphi(g)(p)) \\ &= \sigma_0^{-1}(p) \end{aligned}$$

car p est fixe sous $\varphi(\mathrm{G})$. On aboutit alors à une contradiction. □

Automorphismes extérieurs de $\mathcal{S}_6$, version 2

Rappel : soit G un groupe. Si H est un sous-groupe de G d'incide r, nous obtenons un morphisme de G dans $\mathcal{S}_r$ en faisant agir G sur les classes à gauche modulo H. Plus précisément si $g_1\mathrm{H}$, …, $g_r\mathrm{H}$ désignent les r classes à gauche, nous associons une permutation $\sigma \in \mathcal{S}_r$ à un élément $g \in \mathrm{G}$ en posant

$$(gg_i)\mathrm{H} = g_{\sigma(i)}\mathrm{H}$$

Notons que $i \mapsto \sigma(i)$ est une bijection : l'inverse est donné par l'action de g^{-1}.

Lemme 39. *Soit $n \geq 5$. Si* H *est un sous-groupe de $\mathcal{S}_n$ d'indice n qui agit transitivement sur $\{1, 2, \ldots, n\}$, alors le morphisme $\psi\colon \mathcal{S}_n \to \mathcal{S}_n$ associé à l'action de $\mathcal{S}_n$ sur les classes de $\mathcal{S}_n$ modulo* H *est un automorphisme non intérieur.*

Démonstration. Considérons l'action

$$\mathcal{S}_n \times \mathcal{S}_n/\mathrm{H} \to \mathcal{S}_n/\mathrm{H} \qquad\qquad (g, g_i\mathrm{H}) \mapsto g_{\sigma(i)}\mathrm{H} := (gg_i)\mathrm{H}$$

Par définition un élément g appartient à $\ker\psi$ si et seulement si

$$g \in \bigcap_{i=1}^{n} \mathrm{Stab}(g_i\mathrm{H}).$$

En particulier $\ker\psi$ est contenu dans H. Comme H est d'indice $n \geq 3$ et comme les seuls sous-groupes distingués de $\mathcal{S}_n$ sont d'indice 1 ou 2 ou n on a $\ker\psi = \{\mathrm{id}\}$. Par suite ψ est un automorphisme.

Raisonnons par l'absurde : supposons que ψ soit un automorphisme intérieur. Alors il existe $a \in \mathcal{S}_n$ tel que $\psi(\mathrm{H}) = a\mathrm{H}a^{-1}$. Ainsi $\psi(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. En effet soient i, j dans $\{1, 2, \ldots, n\}$; il existe par hypothèse un élément h de H tel que $h(a^{-1}(i)) = a^{-1}(j)$, donc aha^{-1} est un élément de $a\mathrm{H}a^{-1}$ qui envoie i sur j. Remarquons que si $g_i\mathrm{H} = \mathrm{H}$ est la classe de l'élément neutre modulo H, alors $\psi(\mathrm{H})$ fixe i ; en effet si $h \in \mathrm{H}$, alors

$$hg_i\mathrm{H} = h\mathrm{H} = \mathrm{H} = g_i\mathrm{H}$$

et donc n'agit pas transitivement. □

Proposition 40. *Il existe un sous-groupe* H *de* $\mathcal{S}_6$ *d'indice* 6 *qui agit transitivement sur*

$$\{1, 2, 3, 4, 5, 6\}.$$

Démonstration. Considérons l'action de $\mathrm{GL}(2, \mathbb{F}_5)$ sur les six droites du plan $(\mathbb{F}_5)^2$. Cette action est transitive. Elle devient fidèle après avoir quotienté par le sous-groupe des homothéties qui est d'ordre 4. Autrement dit cette action induit un morphisme injectif de $\mathrm{PGL}(2, \mathbb{F}_5)$ dans $\mathcal{S}_6$; l'image H de ce morphisme agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$. L'ordre de $\mathrm{GL}(2, \mathbb{F}_5)$ est $24 \cdot 20 = 5! \cdot 4$. Par conséquent

$$|\mathrm{H}| = |\mathrm{PGL}(2, \mathbb{F}_5)| = 5!$$

Ainsi H est un sous-groupe d'indice 6 dans $\mathcal{S}_6$. □

5.7. **Théorème de Wedderburn.**

Référence : [Per82, p. 82]
Leçons possibles :
101 : Groupe opérant sur un ensemble. Exemples et applications.
123 : Corps finis. Applications.

Théorème 41. *Tout corps fini est commutatif.*

Soit $\mathbb{k}$ un corps et soit $n \in \mathbb{N}^*$. Supposons que n est premier à la caractéristique de $\mathbb{k}$. L'ensemble des racines n-ièmes de l'unité dans $\mathbb{k}$ est noté $\mu_n(\mathbb{k})$

$$\mu_n(\mathbb{k}) = \big\{\zeta \in \mathbb{k} \,|\, \zeta^n = 1\big\}.$$

C'est un sous-groupe de $\mathbb{k}^*$, de cardinal $\leq n$, donc cyclique.

Notons K_n le corps de décomposition de $P_n = X^n - 1$ sur $\mathbb{k}$. Alors $|\mu_n(K_n)| = n$ et $\mu_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$. De plus comme $\mu_n(\mathbb{k})$ est inclus dans $\mu_n(K_n)$, on a $\mu_n(\mathbb{k}) \simeq \mathbb{Z}/d\mathbb{Z}$ pour un certain diviseur d de n.

Une racine n-ième primitive de 1 est un élément ζ de K_n tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. Autrement dit ζ est un générateur du groupe $\mu_n(K_n)$ de sorte qu'il y a $\varphi(n)$ racines primitives de 1 (voir [Perrin, Cours d'algèbre, page 24]). Leur ensemble est noté $\mu_n^*(K_n)$.

Le n-ième polynôme cyclotomique $\phi_{n,\mathbb{k}} \in K_n[X]$ est donné par la formule

$$\phi_{n,\mathbb{k}}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta).$$

Remarques 42.
- ◇ Si ζ est une racine n-ième primitive de l'unité, les autres sont les ζ^m avec $\mathrm{pgcd}(n, m) = 1$.
- ◇ Le polynôme $\phi_{n,\mathbb{k}}$ est unitaire, de degré $\varphi(n)$.

Proposition 43. *On a la formule*

$$X^n - 1 = \prod_{d|n} \phi_{d,\mathbb{k}}(X).$$

Démonstration. Cela résulte de l'égalité

$$\mu_n(K_n) = \bigcup_{d|n} \mu_d^*(K_n)$$

(l'union est ici disjointe) qui dit que si ζ est une racine n-ième de 1, l'ordre de ζ est un diviseur de n. □

Remarque 44. En comparant les degrés des polynômes on retrouve la formule

$$n = \sum_{d|n} \varphi(d).$$

Démonstration du Théorème 41. Considérons un corps fini $\Bbbk$. Notons $Z(\Bbbk)$ le centre de $\Bbbk$:

$$Z(\Bbbk) = \big\{a \in \Bbbk \,|\, \forall\, x \in \Bbbk,\, xa = ax\big\}$$

$Z(\Bbbk)$ est un sous-corps commutatif de $\Bbbk$ de cardinal $q \geq 2$. Puisque $\Bbbk$ est un $Z(\Bbbk)$-espace vectoriel on a $|\Bbbk| = q^n$ (le $Z(\Bbbk)$-espace vectoriel $\Bbbk$ est isomorphe à $Z(\Bbbk)^n$ où n est la dimension du $Z(\Bbbk)$-espace vectoriel $\Bbbk$).

Si $\Bbbk$ est commutatif la démonstration est terminée. Supposons donc $\Bbbk$ non commutatif. En particulier $n > 1$. Alors $\Bbbk^*$ opère sur lui-même par automorphismes intérieurs

$$\iota_g \colon \Bbbk^* \to \Bbbk^*, \qquad\qquad x \mapsto gxg^{-1}.$$

Considérons cette action. Soit $g \in \Bbbk^*$. Nous noterons $\mathcal{O}_g$ l'orbite de g et $\mathrm{Stab}(g)$ son stabilisateur. Notons que $\mathrm{Stab}(g) \cup \{0\}$ est un sur-corps de $Z(\Bbbk)$; nous en déduisons donc comme précédemment qu'il existe $d \in \mathbb{N}^*$ tel que $|\mathrm{Stab}(g)| = q^d - 1$. Comme $\mathrm{Stab}(g) \subset \Bbbk^*$ le théorème de Lagrange assure que $q^d - 1$ divise $q^n - 1$. Alors d divise n [3]. Finalement

$$|\mathcal{O}_g| = \frac{|\Bbbk^*|}{|\Bbbk_g^*|} = \frac{q^n - 1}{q^d - 1}.$$

En utilisant les formules

$$q^n - 1 = \prod_{m|n} \phi_m(q), \qquad\qquad q^d - 1 = \prod_{m|d} \phi_m(q).$$

nous en déduisons que si $d < n$ alors $\phi_n(q)$ divise

$$|\mathcal{O}_g| = \frac{q^n - 1}{q^d - 1} = \prod_{\substack{m|n \\ m\nmid d}} \phi_m(q).$$

3. En effet écrivons la division euclidienne de n par d : il existe $q \in \mathbb{N} \smallsetminus \{0\}$ et $r \in \mathbb{N}$ tels que $n = dq + r$ et $r < d$. Alors

$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + \ldots + q^{n-qd}) + (q^r - 1).$$

Puisque $n - qd = r < d$ cela constitue la division euclidienne de $q^n - 1$ par $q^d - 1$. Comme $q^d - 1$ divise $q^n - 1$ nous en déduisons que $q^r - 1 = 0$ d'où $r = 0$ et d divise n.

Considérons $\{x_1, x_2, \ldots, x_r\} \subset \mathbb{k}^*$ un système de représentants des orbites non triviales. D'après l'équation aux classes

$$|\mathbb{k}^*| = |Z(\mathbb{k})^*| + \sum_{i=1}^{r} |\mathcal{O}_{x_i}|$$

soit d'après ce qui précède

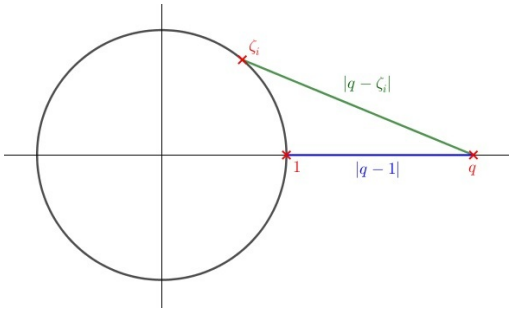
$$q^n - 1 = (q-1) + \sum_{i=1}^{r} |\mathcal{O}_{x_i}|.$$

Par suite $\phi_n(q)$ divise $q-1$. En particulier $|\phi_n(q)| \leq q-1$.

Notons $\zeta_1, \ldots, \zeta_\ell$ les racines primitives $n$ièmes de 1 ; elles vérifient

$$\begin{cases} |\zeta_i| = 1 \\ \zeta_i \neq 1 \text{ (car } n \neq 1) \end{cases}$$

On a $\phi_n(q) = (q-\zeta_1)(q-\zeta_2)\ldots(q-\zeta_\ell)$. Pour tout i on a $|q-\zeta_i| > q-1$:



Ainsi

$$|\phi_n(q)| > (q-1)^\ell \geq q-1$$

contradiction. □

5.8. **Détermination des groupes d'isométries du cube et du tétraèdre.**

Référence : [CG13, Chapitre 12]

Leçons possibles :

101 : Groupe opérant sur un ensemble. Exemples et applications.

105 : Groupe des permutations d'un ensemble fini. Applications.

191 : Exemples d'utilisation des techniques d'algèbre en géométrie.

On illustre l'importance des groupes et des actions de groupes sur des objets concrets de l'espace.

Définitions 2. Un *polyèdre convexe* P est un compact d'intérieur non vide tel que P est l'intersection d'un nombre fini de demi-espaces délimités par des plans affines $H_1, H_2, \ldots, H_n$.

Les *faces* de P sont les intersections de P avec les H_i. Ce sont des polygones convexes. Leurs arêtes sont appelées *arêtes* de P et leurs sommets sont appelés *sommets*.

Proposition 45. *Soit P un polyèdre convexe.*

(1) Le nombre de côtés d'une face est au moins 3.

(2) Le nombre d'arêtes issues d'un sommet est égal au nombre de faces qui contiennent ce sommet et ce nombre est au moins 3.

(3) Une arête appartient à exactement deux faces.

(4) La somme des angles en un sommet est strictement inférieure à 2π.

Pour une démonstration de cet énoncé voir par exemple [Ber77].

Définitions 3. Un polyèdre convexe est *régulier* si toutes ces faces sont des polygones réguliers à p côtés et tous ses sommets appartiennent à exactement q faces.

Dans $\mathbb{R}^3$, un *solide Platonicien* est un polyèdre de dimension 3 régulier (faces identiques et régulières) convexe.

Le couple (p, q) est appelé *symbole de Schläfli* du polyèdre régulier.

Théorème 46. *Il existe exactement cinq types de polyèdres convexes réguliers correspondant aux symboles de Schläfli suivants :*

polyèdre	*symbole de Schläfli*
tétraèdre régulier	$(3, 3)$
cube	$(4, 3)$
octaèdre régulier	$(3, 4)$
icosaèdre régulier	$(3, 5)$
dodécaèdre régulier	$(5, 3)$

Démonstration. Soit (p, q) le symbole de Schläfli d'un polyèdre régulier. Étant donné que chaque face a au moins trois côtés et que chaque sommet est entouré par au moins trois faces, nous avons p, $q \geq 3$.

La somme des angles dans un polygone convexe à p côtés vaut $(p-2)\pi$ (cela se voit en découpant le polygone en $p-2$ triangles à partir d'un sommet choisi). Les angles d'un polygone régulier à p côtés sont donc égaux à $\frac{p-2}{p}\pi$. Puisque $p \geq 3$, nous avons $\frac{p-2}{p}\pi \geq \frac{\pi}{3}$. La somme des angles autour d'un sommet est strictement inférieure à 2π donc $q\frac{\pi}{3} < 2\pi$ et donc $q < 6$. Comme $q \geq 3$, nous avons l'inégalité $3\,\frac{p-2}{p}\pi < 2\pi$ et donc $p < 6$. Il en résulte que $3 \leq p$, $q \leq 5$.

Les couples $(4, 4)$, $(4, 5)$, $(5, 4)$ et $(5, 5)$ ne satisfont pas la condition $q\frac{p-2}{q}\pi < 2\pi$ et donc les seuls couples possibles sont ceux annoncés. □

La liste des polyèdres réguliers étant établie, nous nous intéressons à leurs groupes d'isométries. Le *dual* d'un polyèdre est l'enveloppe convexe des milieux de ses faces. Par exemple le dual du cube est un octaèdre. Plus généralement le dual du polyèdre régulier de symbole (p, q) est le polyèdre régulier de symbole (q, p). Le passage au polyèdre dual échange les faces et les sommets. On peut vérifier qu'un polyèdre et son dual ont le même groupe d'isométries.

Proposition 47. *Soit* $X \subset \mathbb{R}^3$. *Désignons par* $\mathrm{Isom}(X)$ *le groupe des isométries de* $\mathbb{R}^3$ *qui préservent* X.

Si O *est le centre de symétrie de* X *et si* g *est une isométrie de* X, *alors* $g(O) = O$.

De plus $\mathrm{Isom}(X) \simeq \mathrm{Isom}^+(X) \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Démonstration. Tout élément du groupe affine $\mathrm{GA}(3,\mathbb{R})$ conserve le barycentre donc g conserve le centre de symétrie de X, *i.e.* $g(O)=O$.

Notons $s_O \in \mathrm{Isom}^-(X)$ la symétrie centrale en O.

Le morphisme

$$\mathrm{Isom}(X) \to \mathrm{Isom}^+(X) \times \mathbb{Z}/2\mathbb{Z} \qquad\qquad g \mapsto \begin{cases} (g,0) \text{ si } g \in \mathrm{Isom}^+(X) \\ (gs_O,1) \text{ sinon} \end{cases}$$

est un isomorphisme. De plus s_O commute avec tout élément de $\mathrm{Isom}^+(X)$; en effet vectoriellement il s'agit de l'homothétie de rapport -1. Par conséquent le produit est direct. □

Proposition 48. *Le groupe d'isométries du tétraèdre régulier Δ_4 est isomorphe à $\mathcal{S}_4$.*

Le groupe d'isométries directes du tétraèdre régulier Δ_4 est isomorphe à $\mathcal{A}_4$.

Démonstration. Notons Δ_4 le tétraèdre régulier. Désignons par $\mathrm{Isom}(\Delta_4)$ les isométries du tétraèdre régulier et par $\mathrm{Isom}^+(\Delta_4)$ les isométries directes du tétraèdre régulier. Soit $\mathcal{S} = \{A, B, C, D\}$ l'ensemble des sommets du tétraèdre.

Considérons l'action de $\mathrm{Isom}(\Delta_4)$ sur $\mathcal{S}$. Ainsi

$$\varphi\colon \mathrm{Isom}(\Delta_4) \to \mathcal{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{S}}$$

est un morphisme de groupes.

Si $\varphi(g) = \mathrm{id}_{\mathcal{S}}$, alors g stabilise $\mathcal{S}$ qui est un repère de l'espace affine ; il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$. Par suite φ est injectif, *i.e.* $\mathrm{Isom}(\Delta_4)$ s'injecte dans $\mathcal{S}_4$.

Soit M le milieu du segment $[AB]$. La réflexion r_{AB} par rapport au plan MCD réalise la transposition $(A\ B)$, *i.e.* $\varphi(r_{AB}) = (A\ B)$. Ainsi toutes les transpositions appartiennent à $\mathrm{Isom}(\Delta_4)$ d'où l'inclusion $\mathcal{S}_4 \subset \mathrm{Isom}(\Delta_4)$ (rappelons que les transpositions engendrent le groupe symétrique).

Finalement φ est un isomorphisme et $\mathrm{Isom}(\Delta_4) \simeq \mathcal{S}_4$.

Le seul sous-groupe d'indice 2 de $\mathcal{S}_n$ est le groupe alterné $\mathcal{A}_n$. Le groupe $\mathrm{Isom}^+(\Delta_4)$ étant d'indice 2 dans $\mathrm{Isom}(\Delta_4)$ nous avons $\mathrm{Isom}^+(\Delta_4) \simeq \mathcal{A}_4$. □

Proposition 49. *Le groupe d'isométries directes du cube est isomorphe à $\mathcal{S}_4$.*

Le groupe d'isométries du cube est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Par dualité le groupe d'isométries directes de l'octaèdre régulier est isomorphe à $\mathcal{S}_4$ et le groupe d'isométries de l'octaèdre régulier est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Notons C_6 le cube. Désignons par $\mathrm{Isom}(C_6)$ les isométries du cube et par $\mathrm{Isom}^+(C_6)$ les isométries directes du cube. Soit $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube (elles sont préservées par les isométries de C_6 car ce sont les plus grandes longueurs que l'on peut trouver dans le cube).

Ainsi

$$\varphi\colon \mathrm{Isom}^+(C_6) \to \mathcal{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{D}}$$

Notons $D_i = A_iG_i$ les diagonales de C_6. Désignons par s_0 la symétrie centrale en 0. Si $\varphi(g) = \mathrm{id}_{\mathcal{D}}$, alors

- ◇ ou bien $\begin{cases} g(A_1) = A_1 \\ g(G_1) = G_1 \end{cases}$ et dans ce cas en utilisant le fait que g fixe toutes les diagonales et les deux points opposés A_1 et G_1 nous obtenons que g fixe tous les sommets. Il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$.
- ◇ ou bien $\begin{cases} g(A_1) = G_1 \\ g(G_1) = A_1 \end{cases}$ et $s_0 g = \mathrm{id}$ d'après ce qui précède. Il s'en suit que g est la symétrie centrale s_0 en 0 : contradiction avec $g \in \mathrm{Isom}^+(C_6)$.

Ainsi $\ker \varphi = \{\mathrm{id}_{\mathbb{R}^3}\}$ et nous avons l'inclusion $\mathrm{Isom}^+(C_6) \subset \mathcal{S}_4$.

Les transpositions sont toutes réalisées grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales).

Par suite $\mathrm{Isom}^+(C_6) \simeq \mathcal{S}_4$.

La seconde assertion découle du fait que le cube admet un centre de symétrie et de la Proposition 47. □

Proposition 50. *Le groupe d'isométries du dodécaèdre est isomorphe à* $\mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe d'isométries directes du dodécaèdre est isomorphe à $\mathcal{A}_5$.

Par dualité le groupe d'isométries de l'icosaèdre est isomorphe à $\mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ *et son groupe d'isométries directes est isomorphe à* $\mathcal{A}_5$.

Idée de la démonstration. Notons P_{12} le dodécaèdre. Désignons par $\mathrm{Isom}(P_{12})$ les isométries du dodécaèdre et par $\mathrm{Isom}^+(P_{12})$ les isométries du dodécaèdre.

On admet qu'exactement 5 cubes distincts C_1, C_2, …, C_5 sont inscrits dans le dodécaèdre.

Le groupe $\mathrm{Isom}^+(P_{12})$ agit sur l'ensemble $\mathcal{C} = \{C_1, C_2, C_3, C_4, C_5\}$ des cubes inscrits d'où le morphisme

$$\varphi \colon \mathrm{Isom}^+(P_{12}) \to \mathcal{S}_5 \qquad\qquad g \mapsto g_{|\mathcal{C}}$$

Soit g dans $\ker \varphi$, *i.e.* soit g dans $\mathrm{Isom}^+(P_{12})$ tel que $g_{|\mathcal{C}} = \mathrm{id}_{\mathcal{C}}$. Alors $g(C_i) = C_i$ pour $1 \leq i \leq 5$. Alors g fixe les grandes diagonales du dodécaèdre et n'est pas une symétrie centrale ; il s'en suit que $g = \mathrm{id}_{\mathbb{R}^3}$. L'action est donc fidèle et $\mathrm{Isom}^+(P_{12}) \subset \mathcal{S}_5$.

Déterminons le nombre d'éléments de $\mathrm{Isom}^+(P_{12})$. Comme les éléments de $\mathrm{Isom}^+(P_{12})$ sont des rotations cela revient à compter les axes possibles puis les angles possibles :

- ◇ l'identité ;
- ◇ axe de sommet à sommet opposé, $\frac{20}{2} = 10$ axes possibles, les angles (non nuls) $\frac{2\pi}{3}$, $\frac{4\pi}{3}$;
- ◇ axe de milieu d'arête à milieu d'arête opposée, $\frac{30}{2} = 15$ axes possibles, les angles (non nuls) π ;
- ◇ axe passant par le centre de P_{12} et le centre d'une des faces de P_{12}, $\frac{12}{2} = 6$ axes possibles, les angles (non nuls) $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$.

En tout cela fait $10 \times 2 + 15 \times 1 + 6 \times 4 + 1 = 60$ éléments.

Le dodécaèdre ayant un centre de symétrie la Proposition 47 assure que $\mathrm{Isom}(P_{12}) \simeq \mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. □

Sous-groupes de Sylow d'un groupe d'isométries. Les groupes d'isométries des solides platoniciens ont l'avantage d'avoir des p-Sylow « visibles à l'oeil nu ». Voici quelques exemples témoins de l'interaction omniprésente entre groupes et géométrie :

- ◇ On peut se demander combien $\mathcal{A}_4$ possède de 3-Sylow. Bien sûr, nous avons la méthode arithmétique qui consiste à regarder les valeurs possibles (ici 1 et 4) et à éliminer selon certaines considérations. Mais nous pouvons aussi utiliser une méthode algébrique puisque $\mathcal{A}_4$ se réalise comme groupe d'isométries directes du tétraèdre. Comme ses 3-Sylow ont pour ordre 3, ce sont des rotations d'ordre 3 et la seule possibilité est la rotation autour d'un axe passant par le milieu des faces. Il y a donc quatre 3-Sylow correspondant aux quatre faces d'un tétraèdre.
- ◇ On peut se demander combien $\mathcal{S}_4$ possède de 3-Sylow. Même méthode, mais cette fois-ci le groupe $\mathcal{S}_4$ se réalise comme groupe d'isométrie directe de deux manières : celui du cube et celui de l'octaèdre. Visuellement, c'est en tant que groupe de l'octaèdre qu'on voit le mieux les 3-Sylow car ils sont en bijection avec ses paires de faces opposées (triangulaires). Le groupe $\mathcal{S}_4$ contient donc quatre 3-Sylow.
- ◇ On peut se demander combien $\mathcal{A}_5$ possède de 3-Sylow. Réponse : 10 correspondant aux paires de faces opposées de l'icosaèdre.
- ◇ On peut se demander combien $\mathcal{A}_5$ possède de 5-Sylow. Réponse : 6 correspondant aux paires de faces opposées du dodécaèdre.
- ◇ On peut se demander combien $\mathcal{S}_4$ possède de 2-Sylow. Réponse : 3... justification géométrique bien sûr !

5.9. **Dénombrement des colorations du cube.**

Références : [CG13, Exercice C.6, p. 375]
Leçons possibles :
101 : Groupe opérant sur un ensemble. Exemples et applications.
104 : Groupes abéliens et non abéliens finis. Exemples et applications.
190 : Méthodes combinatoires, problèmes de dénombrement.
191 : Exemples d'utilisation des techniques d'algèbre en géométrie.

Petit rappel sur les isométries

Considérons l'espace euclidien $\mathbb{R}^n$ muni du produit scalaire $\langle\,,\,\rangle$ qui donne la norme euclidienne $||v|| = \sqrt{\langle v,\, v\rangle}$. La distance associée est donnée par $d(x,y) = ||x-y||$.

Définition 4. Une *isométrie euclidienne* φ est une application bijective de $\mathbb{R}^n$ qui préserve la norme euclidienne, *i.e.* qui vérifie

$$\forall\, x,\, y \in \mathbb{R}^n \qquad d(\varphi(x), \varphi(y)) = d(x,y).$$

Le *groupe des isométries euclidiennes* est $\mathrm{Isom}(\mathbb{R}^n, d)$.

Les translations et les éléments du groupe orthogonal $\mathrm{O}(n,\mathbb{R})$ sont des isométries euclidiennes. L'énoncé suivant donne toutes ces isométries :

Théorème 51. *Toute isométrie de $(\mathbb{R}^n, d)$ est une application affine.*
Toute isométrie de $(\mathbb{R}^n, d)$ qui fixe l'origine est donnée par un élément de $\mathrm{O}(n,\mathbb{R})$.
Le groupe $\mathrm{Isom}(\mathbb{R}^n)$ se décompose en un produit semi-direct de la façon suivante :

$$\mathrm{Isom}(\mathbb{R}^n) = \mathrm{O}(n,\mathbb{R}) \ltimes (\mathbb{R}^n, +)$$

où $(\mathbb{R}^n, +)$ est identifié au groupe des translations de $\mathbb{R}^n$.

Rappelons qu'une application $f\colon \mathbb{R}^n \to \mathbb{R}^n$ est *affine* s'il existe une application linéaire $A\colon \mathbb{R}^n \to \mathbb{R}^n$ et un élément b de $\mathbb{R}^n$ tels que pour tout $x \in \mathbb{R}^n$ on ait $f(x) = Ax + b$. Remarquons que le couple (A, b) est unique. En effet $b = f(0)$ et A est l'application linéaire $x \mapsto f(x) - f(0)$.

Pour $x \in \mathbb{R}^n$ nous notons τ_x la translation de vecteur x ; autrement dit $\tau_x(y) = y + x$ pour tout $y \in \mathbb{R}^n$.

Attardons-nous un instant sur la dimension trois. Avant d'énoncer la classification des isométries en dimension trois rappelons qu'un *vissage* (ou *rotation glissée*) est un déplacement dans un espace affine euclidien qui est la composée commutative d'une rotation et d'une translation selon un vecteur dirigeant l'axe de rotation (si la rotation n'est pas l'identité). Une *anti-rotation* est un type particulier d'antidéplacement (*i.e.* d'isométrie qui renverse l'orientation) de l'espace euclidien de dimension 3 (espace affine euclidien ou espace vectoriel euclidien, suivant le contexte) : c'est la composée commutative d'une rotation d'angle ϑ autour d'un axe Δ et d'une réflexion par rapport à un plan perpendiculaire à Δ.

Théorème 52. *Les éléments de* $\mathrm{Isom}(\mathbb{R}^3)$ *sont :*
- *les translations,*
- *les rotations,*
- *les rotations glissées,*
- *les symétries orthogonales par rapport à un plan,*
- *les symétries glissées,*
- *les anti-rotations.*

Pour une preuve on renvoie à [Aud06].

Groupe des isométries directes du cube

Si $E \subset \mathbb{R}^n$, nous notons $\mathrm{Isom}(E)$ le sous-groupe de $\mathrm{Isom}(\mathbb{R}^n)$ qui préserve E. Nous notons aussi $\mathrm{Isom}^+(E)$ le sous-groupe de $\mathrm{Isom}(E)$ des isométries qui préservent l'orientation.

Proposition 53. *Le groupe d'isométries directes du cube est isomorphe à* $\mathcal{S}_4$.

Démonstration. Notons C_6 le cube. Désignons par $\mathrm{Isom}(C_6)$ les isométries du cube et par $\mathrm{Isom}^+(C_6)$ les isométries directes du cube. Soit $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube (elles sont préservées par les isométries de C_6 car ce sont les plus grandes longueurs que l'on peut trouver dans le cube).

Ainsi

$$\varphi\colon \mathrm{Isom}^+(C_6) \to \mathcal{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{D}}$$

Notons $D_i = A_iG_i$ les diagonales de C_6. Désignons par s_0 la symétrie centrale en 0. Si $\varphi(g) = \mathrm{id}_{\mathcal{D}}$, alors

- ◇ ou bien $\begin{cases} g(A_1) = A_1 \\ g(G_1) = G_1 \end{cases}$ et dans ce cas en utilisant le fait que g fixe toutes les diagonales et les deux points opposés A_1 et G_1 nous obtenons que g fixe tous les sommets. Il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$.
- ◇ ou bien $\begin{cases} g(A_1) = G_1 \\ g(G_1) = A_1 \end{cases}$ et $s_0 g = \mathrm{id}$ d'après ce qui précède. Il s'en suit que g est la symétrie centrale s_0 en 0 : contradiction avec $g \in \mathrm{Isom}^+(C_6)$.

Ainsi $\ker\varphi = \{\mathrm{id}_{\mathbb{R}^3}\}$ et nous avons l'inclusion $\mathrm{Isom}^+(C_6) \subset \mathcal{S}_4$.

Les transpositions sont toutes réalisées grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales).

Par suite $\mathrm{Isom}^+(C_6) \simeq \mathcal{S}_4$. □

Coloriages du cube

Par coloriage d'un cube on entend le choix d'une couleur pour chaque face et deux cubes coloriés sont considérés comme identiques s'ils diffèrent par une rotation.

Théorème 54. *Le nombre de façons de colorier un cube avec au plus c couleurs est :*

$$\frac{c^6 + 3c^4 + 12c^3 + 8c^2}{24}$$

Démonstration. Avant l'identification par rotation il y a c^6 coloriages possibles. On fait agir le groupe $\mathcal{S}_4$ des rotations du cube sur l'ensemble E de ces c^6 coloriages. Il s'agit de compter le nombre n d'orbites. La formule de Burnside assure que n est la moyenne du nombre de points fixes ;

$$n = \frac{1}{24}\sum_{g\in\mathcal{S}_4} \#\mathrm{Fix}(g)$$

On estime $\#\mathrm{Fix}(g)$ pour chaque type de permutation :

- ◇ si g est l'identité, alors $\mathrm{Fix}(g) = E$ et $\#\mathrm{Fix}(g) = c^6$.
- ◇ si g est une rotation d'ordre 2 d'axe pensant par le milieu d'arêtes, alors $\#\mathrm{Fix}(g) = c^3$; remarquons qu'il y a 6 telles rotations.
- ◇ si g est une rotation d'ordre 3, alors $\#\mathrm{Fix}(g) = c^2$; notons qu'il y a 8 telles rotations.
- ◇ si g est une rotation d'ordre 4, alors $\#\mathrm{Fix}(g) = c^3$; remarquons qu'il y a 6 telles rotations.
- ◇ si g est une rotation d'ordre 2 d'axe passant par les milieux des faces, alors $\#\mathrm{Fix}(g) = c^4$; remarquons qu'il y a 3 telles rotations.
- ◇ si g est une rotation d'ordre 2 d'axe joignant les milieux de deux côtés, alors $\#\,\mathrm{Fix}(g) = c^3$; il y a 6 telles rotations [4].
- ◇ si g est une rotation d'angle (géométrique) $\frac{2\pi}{3}$ autour de l'une des diagonales, alors $\#\,\mathrm{Fix}(g) = c^2$; il y a 8 telles rotations [5].
- ◇ si g est une rotation d'angle $\frac{\pi}{2}$ autour d'un axe orthogonal à 2 faces du cube, alors $\#\,\mathrm{Fix}(g) = c^3$; il y a 6 telles rotations [6].
- ◇ g est le carré de l'une des rotations d'angle $\frac{\pi}{2}$ ci-dessus, alors $\#\,\mathrm{Fix}(g) = c^4$; il y a 3 telles rotations [7].

Ainsi

$$n = \frac{1}{24}\sum_{g\in\mathcal{S}_4} \#\mathrm{Fix}(g) = \frac{1}{24}\Big(c^6 + 6c^3 + 3c^2 + 6c^3 + 3c^4\Big) = \frac{c^6 + 12c^3 + 3c^2 + 3c^4}{24}$$

□

4. Elles correspondent aux transpositions.
5. Elles correspondent aux 3-cycles.
6. Elles correspondent aux 4-cycles.
7. Elles correspondent aux doubles transpositions.

Remarque 55. On peut vérifier que pour $c = 2$ on trouve 10 coloriages possibles que l'on peut facilement énumérer.

Références

[Aud06] M. Audin. *Géométrie*. EDP Sciences. 2006.

[Ber77] M. Berger. *Géométrie. Vol. 2*. CEDIC, Paris ; Nathan Information, Paris, 1977. Espaces euclidiens, triangles, cercles et sphères.

[CG13] P. Caldero and J. Germoni. *Histoires Hédonistes de Groupes et de Géométries. Tome premier*. Calvage et Mounet, 2013.

[CG15] P. Caldero and J. Germoni. *Histoires Hédonistes de Groupes et de Géométries-Tome 2*. Calvage et Mounet, 2015.

[CG17] P. Caldero and J. Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries*. Calvage et Mounet, 2017.

[Com98] F. Combes. *Alèbre et Géométrie*. Bréal, 1998.

[CP19] P. Caldero and M. Péronnier. *Carnet de voyages en Algébrie*. Calvage et Mounet, 2019.

[FGN09] S. Francinou, H. Gianella, and S. Nicolas. *Exercices de mathématiques oraux x-ens, algèbre 2*. Cassini, 2009.

[Per82] D. Perrin. *Cours d'algèbre*, volume 18 of *Collection de l'École Normale Supérieure de Jeunes Filles*. École Normale Supérieure de Jeunes Filles, Paris, 1982. Edited with the collaboration of Marc Cabanes and Martine Duchene.

[Szp08] A. Szpirglas. *Exercices d'Alèbre*. Cassini, 2008.

[Szp09] A. Szpirglas. *Mathématiques L3 : Algèbre*. Pearson, 2009.