QUELQUES DÉVELOPPEMENTS SUR LES GROUPES

STÉPHANE LAMY

DISCLAIMER. Ce sont mes notes personnelles sur quelques uns des développements que j'ai vu cette année lors des colles groupes (et deux en prime, isomorphismes exceptionnels et sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$, qu'il ne m'aurait pas déplu de voir...). J'indique des références, et ma rédaction est souvent plus concise que la source originale (je vous laisse juger si je simplifie, ou si j'introduis des erreurs). Les propositions de couplages en fin de fichier ne sont ni exhaustives, ni à suivre les yeux fermés. Faites usage d'esprit critique !

TABLE DES MATIÈRES

Simplicité de A_n. [RW10, p. 19], [Szp09, p. 267].

Leçons

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

Plausible, mais pas avec la preuve de [RW10]. Il faut sans doute insister sur le fait qu'il y a deux classes de conjugaison de 5-cycles dans A_5.

- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications

Demande à être bien vendu, car tel quel le développement consiste à montrer que A_n n'admet aucun sous-groupe distingué, et il n'y a pas trace de quotient dans la preuve... Une solution : modifier légèrement pour obtenir un énoncé du type "voici les sous-groupes distingués propres de S_n" (seulement A_n pour $n \geqslant 5$, et V_4, A_4 dans le cas $n = 4$) ?

- 104. Groupes finis. Exemples et applications
- 105. Groupe des permutations d'un ensemble fini. Applications
- 108. Exemples de parties génératrices d'un groupe. Applications

$\sim$

Théorème. *Le groupe alterné A_n est simple pour tout $n \geqslant 5$.*

Proposition. (1) *Pour tout $n \geqslant 3$, les 3-cycles engendrent A_n ;*

(2) *Pour tout $n \geqslant 5$, les 3-cycles sont deux à deux conjugués dans A_n.*

Preuve. (1) Soit $\sigma \in A_n$. Comme S_n est engendré par les transpositions, on peut écrire σ comme la composée d'un nombre pair de transpositions. Reste à remarquer que le produit de deux transpositions τ_1, τ_2 peut également s'écrire à l'aide de 3-cycles : on distingue trois cas suivant que les supports de τ_1 et τ_2 ont 2, 1 ou 0 éléments commun.

- $(ij)(ij) = \mathrm{id}$;
- $(ij)(jk) = (ijk)$;
- $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$.

(2) Soit (ijk) un 3-cycle, il existe une permutation $\sigma \in S_n$ telle que $\sigma(1) = i$, $\sigma(2) = j$, $\sigma(3) = k$. On peut de plus supposer $\sigma \in A_n$, quitte à remplacer σ par $\sigma \circ (45)$. Alors $(ijk) = \sigma(123)\sigma^{-1}$, ainsi tous les 3-cycles sont conjugués à (123) dans A_n, et donc également entre eux. □

Date: Dernière modification : 11 octobre 2018.

Preuve du théorème. Soit H un sous-groupe normal de A_n, que l'on suppose différent de $\{1\}$. Grâce à la proposition, il suffit de montrer que H contient un 3-cycle. Soit $h \in H$ un élément non trivial. Nous allons utiliser de façon répétée l'observation que pour tout $\gamma \in A_n$, on a $\gamma h \gamma^{-1} h^{-1} \in H$. Le support de h est l'ensemble des $i \in \{1, \dots, n\}$ tel que $h(i) \neq i$; on peut supposer que h a son support de cardinal m minimal parmi tous les éléments non triviaux de H. Clairement $m \geqslant 3$, et il s'agit de montrer que $m = 3$. Raisonnons par l'absurde, et supposons $m \geqslant 4$.

Si $m = 4$, alors $h = (ab)(cd)$ est une double transposition. Posons $\gamma = (cde)$, où $e \notin \{a, b, c, d\}$. alors on obtient la contradiction

$$\gamma h \gamma^{-1} h^{-1} = (ab)(de)(ab)(cd) = (edc) \in H.$$

Si $m = 5$, alors $h = (abcde)$ est un 5-cycle. Cette fois on prend $\gamma = (cba)$, et on obtient la contradiction

$$\gamma h \gamma^{-1} h^{-1} = (cba)(bcd) = (acd) \in H.$$

Enfin si $m > 5$, soit a dans le support de h, $b = h(a)$, et c distinct de $a, b, h(b)$. Posons $\gamma = (abc)$, on a

$$f = \gamma h \gamma^{-1} h^{-1} = (abc)(b\, h(c)\, h(b)) \in H.$$

D'une part $f(h(b)) = c$ donc $f \neq \mathrm{id}$, et le support de f est inclus dans l'ensemble à 5 éléments $\{a, b, c, h(b), h(c)\}$ ce qui contredit la minimalité de m. □

Remarques. C'est un classique, de niveau modeste mais convenable.

Si on le propose, il faut absolument faire aussi la preuve des deux points de la proposition (et donc être efficace dans la preuve du théorème). Il y a beaucoup d'autres références, mais elles sont souvent sur le schéma : preuve pour A_5, puis en déduire le cas général. Je trouve la preuve du [RW10] plus rapide à exposer (mais elle ne convient pas pour la leçon 101. Groupe opérant sur un ensemble. Exemples et applications).

Il n'est pas utile (voire un peu ridicule) de dépenser la moindre seconde à expliquer ce qui se passe pour $n = 2$ ou 3 (cela n'empêche pas d'y avoir réfléchi pour pouvoir répondre du tac au tac à une éventuelle question sur ces cas triviaux).

Il est vivement conseillé d'avoir réfléchi au problème qui se pose dans le cas $n = 4$: connaître l'unique sous-groupe distingué propre de A_4, savoir si c'est aussi un sous-groupe distingué de S_4, avoir une interprétation géométrique de ces groupes (en termes d'isométries préservant un tétraèdre régulier, ou un cube, à votre goût...)

Pour étoffer ses plans, on pourra également prendre conscience que la preuve de la plupart des résultats de simplicité (A_n, $\mathrm{PSL}_n(K)$, $\mathrm{SO}_3(\mathbb{R})$...) suivent la même stratégie (identifier des générateurs privilégiés qui forment une classe de conjugaison, puis bricoler avec des commutateurs...) : voir [Per96, bas p. 28].

Une alternative plus (trop ?) ambitieuse consiste à montrer que tout groupe simple d'ordre 60 est isomorphe à A_5 (repose sur les théorèmes de Sylow), ou encore à établir certains isomorphismes exceptionnels comme $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5) \simeq A_5$.

Automorphismes du groupe symétrique. [Per96, p. 30], [Szp09, p. 270] (copie de Perrin)

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 104. Groupes finis. Exemples et applications
- 105. Groupe des permutations d'un ensemble fini. Applications
- 108. Exemples de parties génératrices d'un groupe. Applications

La preuve est une illustration du fait que pour comprendre un morphisme de groupe, il suffit de comprendre l'image des générateurs (ici les transpositions pour S_n).

$\sim$

On s'intéresse aux automorphismes du groupe symétrique S_n pour les cas non triviaux $n \geqslant 3$. Dans ce cas le centre de S_n est réduit à $\{\mathrm{id}\}$, et donc S_n agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(S_n)$ des automorphismes intérieurs de S_n est isomorphe à S_n. On montre que sauf dans le cas exceptionnel $n = 6$ les automorphismes intérieurs sont les seuls automorphismes. En complément on exhibe un automorphisme non intérieur de S_6.

Théorème. *Soit $n \geqslant 3$, $n \neq 6$. Alors*

$$\mathrm{Aut}(S_n) = \mathrm{Int}(S_n) \simeq S_n.$$

Lemme. *Soit $\varphi \in \mathrm{Aut}(S_n)$ qui envoie transpositions sur transpositions. Alors $\varphi \in \mathrm{Int}(S_n)$.*

Preuve. Les transpositions de la forme $(1\, i)$, $i = 2, \dots, n$, engendrent S_n. Notons $\tau_i = \varphi(1\, i)$, et remarquons que pour $i \neq j$, τ_i et τ_j ne commutent pas puisque $(1\, i)$ et $(1\, j)$ ne commutent pas.

On en déduit que les transpositions τ_i et τ_j ont exactement un élément en commun dans leur support. Posons

$$\tau_2 = (\alpha_1\,\alpha_2), \quad \tau_3 = (\alpha_1\,\alpha_3),$$

et montrons que pour tout $k \geqslant 4$, on a $\tau_k = (\alpha_1\,\alpha_k)$ pour un certain $\alpha_k \in \{1,\dots,n\}$. En effet si α_1 n'est pas dans le support de τ_k, on aurait $\tau_k = (\alpha_2\,\alpha_3)$ et donc

$$\tau_2\tau_k = (\alpha_1\,\alpha_2\,\alpha_3), \quad \tau_3\tau_k = (\alpha_1\,\alpha_3\,\alpha_2)$$

sont inverses l'un de l'autre, ce qui n'est pas compatible avec

$$(1\,2)(1\,k) = (2\,1\,k) \text{ qui n'est pas l'inverse de } (1\,3)(1\,k) = (3\,1\,k).$$

Finalement $\alpha\colon k \mapsto \alpha_k$ est un élément de S_n. Comme l'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\,i)$ de S_n, ils coïncident sur S_n tout entier. □

Preuve du théorème. Soit φ un automorphisme non intérieur de S_n. On veut montrer que $n = 6$. Par le lemme, il existe τ une transposition tel que $\varphi(\tau)$ n'est pas une transposition. Comme $\varphi(\tau)$ est d'ordre 2, c'est donc un produit de $k \geqslant 2$ transpositions à supports disjoints. Notons que le centralisateur $C(\tau)$ de la transposition τ est le produit direct de $\mathbb{Z}/2\mathbb{Z}$ (engendré par τ) et de S_{n-2} (correspondant aux permutations de support disjoint de celui de τ). En particulier on a un morphisme surjectif et de noyau $\mathbb{Z}/2\mathbb{Z}$

$$\psi\colon C(\tau) \to S_{n-2}.$$

Maintenant considérons H le centralisateur de $\varphi(\tau)$, qui est isomorphe à $C(\tau)$ via φ. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$, donc H contient un sous-groupe N isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. De plus N est distingué dans H, car c'est le noyau du morphisme $H \to S_k$ qui à un élément de H associe la permutation induite sur les k transpositions de la décomposition de $\varphi(\tau)$.

Donc $C(\tau)$, qui est isomorphe à H, contient un sous-groupe distingué N' isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$. En transportant par ψ on obtient que S_{n-2} contient un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ ou $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ (suivant si τ est dans N' ou non). Mais on connaît les sous-groupes distingués de S_n (pour $n \geqslant 1$) : il n'y a que $\{\mathrm{id}\}$, A_n et S_n, sauf dans le cas S_4 où il faut rajouter $V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ à la liste. On a donc deux possibilités :

- $n = 4$, car $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre au $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ avec $k = 2$;
- $n = 6$, car S_4 contient $V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Montrons que $n = 4$ est impossible : le centralisateur d'une transposition dans S_4 est de cardinal 4 (c'est le groupe V_4), alors que le centralisateur d'une double transposition est de cardinal 8 (divise strictement 24, et multiple strict de 4 car V_4 est dedans mais aussi au moins un 4-cycle). □

En complément, on peut s'employer à exhiber un automorphisme extérieur de S_6. Une jolie façon est d'utiliser (sans avoir à le dire explicitement d'ailleurs) l'isomorphisme $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$. [CG14, p. 244 et D.12 p. 289], voir également D.11 p. 289, et C.22 p. 73...

- $\mathrm{PGL}_2(\mathbb{F}_5)$ agit transitivement sur les 6 droites du plan $(\mathbb{F}_5)^2$ (autrement dit sur la droite projective $\mathbb{P}^1(\mathbb{F}_5)$) ;
- On en déduit l'existence de $H \subset S_6$ d'indice 6 qui agit transitivement sur $\{1,2,3,4,5,6\}$;
- H est d'indice 6, donc l'action à gauche de S_6 sur les classes à gauche fournit un morphisme $\psi\colon S_6 \to S_6$, qui est un isomorphisme (le noyau de ψ est clairement contenu dans H, donc est trivial étant donné la rareté des sous-groupes distingués dans S_n...) ;
- $\psi(H)$ fixe H donc n'agit pas transitivement, en particulier ψ n'est pas intérieur.

On peut si on veut formaliser le raisonnement dans l'énoncé suivant (dont les hypothèses ne sont jamais vérifiées quand $n \neq 6$...)

Lemme. *Soit $n \geqslant 5$ (les cas $n \leqslant 4$ se traitent à la main, de façon différente). Si $H \subset S_n$ est un sous-groupe d'indice n agissant transitivement sur $\{1,\dots,n\}$, alors le morphisme $\psi : S_n \to S_n$ associé à l'action de S_n sur les classes à gauche de S_n modulo H est un automorphisme non intérieur.*

Preuve. Le noyau de ψ est clairement contenu dans H, donc est trivial étant donné la rareté des sous-groupes distingués dans S_n. D'autre part $\psi(H)$ fixe H donc n'agit pas transitivement, en particulier ψ n'est pas intérieur. □

Isomorphisme exceptionnel $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$. [CG13, p. 233 et p. 243], [Szp09, p. 780]

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications

Le développement connecte deux exemples respectivement sur $\mathbb{C}$ et sur $\mathbb{R}$

• 108. Exemples de parties génératrices d'un groupe. Applications

En insistant sur le fait que les retournements engendrent SO_3...

• 154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications

Peut-être un peu limite, mais on utilise le fait qu'une isométrie qui préserve un sous-espace préserve aussi son orthogonal.

• 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie)

• 161. Distances et isométries d'un espace affine euclidien

• 170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Le produit scalaire sur $\mathbb{R}^3$ s'obtient comme restriction de la norme sur les quaternions, qui est bien une forme quadratique. Illustre aussi le fait que sur des matrices 2×2 le déterminant fournit une forme quadratique intéressante...

• 171. Formes quadratiques réelles. Coniques. Exemples et applications

• 182. Applications des nombres complexes à la géométrie.

Peut-être encore mieux avec la preuve via la projection stéréographique [CG13, p. 243], où des homographies apparaissent (mais le mot homographie a disparu en 2015 du titre de la leçon).

• 183. Utilisation des groupes en géométrie

$\sim$

Théorème. *Il existe un isomorphisme explicite* $\mathrm{SU}_2/\{\pm\mathrm{id}\}\simeq\mathrm{SO}_3$.

Preuve via les quaternions [CG13, p. 233]. On va construire un morphisme depuis le groupe spécial unitaire SU_2 vers le groupe orthogonal O_3, puis montrer que son noyau est $\{\pm\mathrm{id}\}$ et son image SO_3, ce qui donnera le résultat par le théorème d'isomorphisme :

$$\begin{array}{ccccc} \mathrm{SU}_2 & \twoheadrightarrow & \mathrm{SO}_3 & \subset & \mathrm{O}_3 \\ \downarrow & \nearrow_{\simeq} & & & \\ \mathrm{SU}_2/\{\pm\mathrm{id}\} & & & & \end{array}$$

Pour construire ce morphisme on utilise les quaternions, et plus précisément leur écriture matricielle :

$$\mathbb{H}=\left\{\begin{pmatrix} a & -\bar b\\ b & \bar a\end{pmatrix}\in\mathcal{M}_2(\mathbb{C});\ a,b\in\mathbb{C}\right\}.$$

En particulier $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel de dimension 4, et la base canonique correspond aux matrices

$$\mathrm{id}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad I=\begin{pmatrix}i&0\\0&-i\end{pmatrix},\qquad J=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\qquad K=\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

Le déterminant correspond à la norme (au carré) $N(h)=h\bar h$, et donc au produit scalaire standard sur $\mathbb{R}^4$. Du point de vue matriciel $\bar h$ correspond à la transposée conjuguée. Le groupe SU_2 correspond à la sphère unité S^3 dans $\mathbb{H}\simeq\mathbb{R}^4$:

$$\mathrm{SU}_2=\left\{\begin{pmatrix} a & -\bar b\\ b & \bar a\end{pmatrix}\in\mathcal{M}_2(\mathbb{C});\ |a|^2+|b|^2=1\right\}.$$

On identifie $\mathbb{R}^3$ à l'espace $\mathbb{I}$ des quaternions "imaginaires purs" (c'est-à-dire a est imaginaire pur). On fait agir SU_2 sur $\mathbb{H}$ par conjugaison. La conjugaison préserve le déterminant, donc la norme euclidienne (on peut aussi utiliser directement que $N(hh')=N(h)N(h')$). Le centre $\mathbb{R}$ est stable, donc également son orthogonal $\mathbb{I}$, et on obtient une action :

$$\begin{aligned}\mathrm{SU}_2\times\mathbb{I}&\to\mathbb{I}\\ h,u&\mapsto huh^{-1}\end{aligned}$$

Cette action correspond à un morphisme $\varphi\colon \mathrm{SU}_2\to\mathrm{SO}_3$ (a priori on arrive dans O_3, mais comme de plus SU_2 est connexe on arrive bien dans la composante connexe de l'identité SO_3). Le noyau de ce morphisme est constitué de matrices commutant avec I,J et K, et correspond donc à l'intersection du centre de $\mathbb{H}$ (les quaternions réels) avec la sphère unité, on obtient donc $\ker\varphi=\{\pm\mathrm{id}\}$. Reste à montrer la surjectivité de φ pour obtenir l'isomorphisme par passage au quotient. Il suffit de montrer que tout retournement est dans l'image (car les retournements, c'est-à-dire les rotations d'angle π, engendrent SO_3). Pour chaque $h\in S^3\cap\mathbb{I}\simeq S^2$, on peut considérer d'une part le retournement r_h de $\mathbb{I}=\mathbb{R}^3$ d'axe $\mathbb{R}h$, et d'autre part la rotation $\varphi(h)$ (dont on sait déjà qu'elle est non-triviale). Montrons que $r_h=\varphi(h)$. Clairement $\varphi(h)(h)=hhh^{-1}=h$, il reste donc à voir que $\varphi(h)(u)=-u$ pour tout $u\in h^\perp$. Or $u\in h^\perp$ équivaut à la condition $u\bar h+h\bar u=0$, car la forme bilinéaire symétrique associée à la norme $N(h)=h\bar h$ est $\langle h,h'\rangle=\frac12(h\bar h'+h'\bar h)$. Comme $u,h\in\mathbb{I}$, cela donne $-uh-hu=0$, ou encore $huh^{-1}=-u$ comme attendu.

NB (fin alternative) : au lieu des 4 dernières lignes on peut montrer que la rotation $\varphi(h)$ est une involution en remarquant que $\varphi(h)^2 = \varphi(h^2)$ et que $h^2 = (-h)(-h) = -h\bar{h} = -\mathrm{id} \in \ker \varphi$. □

Lemme. *Les retournements engendrent* SO_3.

Preuve express (faire un dessin !). Soit D une droite vectorielle de $\mathbb{R}^3$, et θ un angle. Considérons H le plan orthogonal à D, et $D_1, D_2 \subset H$ deux droites formant un angle $\theta/2$. Alors la composée des retournements d'axe D_1 et D_2 est une rotation d'angle θ et d'axe D : en effet D est fixe, et en restriction à H on a la composée de deux symétries axiales, c'est-à-dire une rotation. □

Caractères et sous-groupes normaux de S_4, isométries et coloriages du cube. [CG13, p. 364], [Szp09, p. 422], [Ale99]. Pour la partie "représentation" : [CG14, F. 18 p. 490, p. 523 entre autres], [RW10, p. 55, exo I.1.51 p. 70, p. 534], [Pey04, p. 229-232]. Pour la partie "coloriage" : [CG13, Exercice C.6 p.375].

Il y a pleins de façons de traiter ça (avec ou sans représentations), donc bien expliciter lors de la défense du plan ce qu'on va faire :

Exemple 1: "Je vais montrer que le groupe des rotations préservant un cube est isomorphe à S_4, puis à l'aide de la formule de Burside je vais dénombrer les coloriages d'un cube avec c couleurs."

Exemple 2: "Je vais dresser la liste des classes de conjugaison de S_4 en donnant leur interprétation comme isométries du cube, dresser la table des caractères de S_4 en utilisant des résultats mentionnés dans le plan, et illustrer le fait que la table des caractères permet de retrouver tous les sous-groupes distingués propres (ici V_4 et A_4 dans S_4)."

Leçons :

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

Pas ma préférée sur cette leçon, mais ça semble quand même coller (on fait agir S_4 sur les grandes diagonales du cubes, et les représentations sont bien sûr aussi des actions...).

- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications

Si on montre comment retrouver A_4 ou V_4 géométriquement, et/ou si on illustre comment trouver les sous-groupes distingués d'un groupe à partir de la table des caractères.

- 104. Groupes finis. Exemples et applications
- 105. Groupe des permutations d'un ensemble fini. Applications
- 107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel. Exemples
- 183. Utilisation des groupes en géométrie
- 190. Méthodes combinatoires, problèmes de dénombrements

En ne parlant pas de représentation, mais en incluant le dénombrement des coloriages d'un cube.

$\sim$

Isomorphisme:

Théorème ([CG13, p. 364])**.** *Le groupe* $\mathrm{Isom}^+(\mathit{cube})$ *des rotations de* $\mathbb{R}^3$ *préservant un cube est isomorphe au groupe symétrique* S_4.

Preuve. Les quatres diagonales du cube sont caractérisées comme les couples de sommets réalisant la distance maximale entre deux sommets. On déduit que le groupe $\mathrm{Isom}^+(\mathrm{cube})$ agit sur l'ensemble $\{D_1, D_2, D_3, D_4\}$ des grandes diagonales, ce qui donne un morphisme

$$\begin{aligned} \mathrm{Isom}^+(\mathrm{cube}) &\to S_4 \\ f &\mapsto \sigma \end{aligned}$$

tel que $f(D_i) = D_{\sigma(i)}$ pour tout $1 \leqslant i \leqslant 4$.

Montrons que ce morphisme est injectif. Pour cela, on utilise plusieurs fois la remarque suivante : si une isométrie f fixe trois sommets du cube qui sont deux à deux non opposés, alors $g = \mathrm{id}$ (car ces sommets forment une base de l'espace vectoriel d'origine le centre du cube). Supposons que f préserve chaque diagonale D_i. D'abord f ne peut pas échanger les deux sommets de chaque diagonale, car sinon $f = -\mathrm{id}$ par la remarque précédente appliquée à $-\mathrm{id} \circ f$. Donc il existe deux sommets d'une grande diagonale, disons A_1 et A_1' dans D_1, qui sont fixés par f. Mais pour chaque autre diagonale D_i, les sommets A_i et A_i' ne sont pas équidistants de A, donc fixés également, et finalement f fixe tous les sommets donc $f = \mathrm{id}$.

Finalement on montre que le morphisme est surjectif. Il suffit de montrer que les six transpositions de S_4 sont dans l'image, puisque les transpositions engendrent S_4. Mais on vérifie (dessin !) que les transpositions correspondent aux images des rotations d'angle π et d'axe passant par les milieux d'arêtes opposées. □

Remarque. On pourrait aussi montrer d'abord que $\mathrm{Isom}^+(\text{cube})$ et S_4 sont de même cardinal 24, et on peut alors se contenter de montrer l'injectivité OU la surjectivité dans la preuve précédente. Le dénombrement se fait en termes de "drapeaux" du cube, voir [Szp09, p.414]. C'est aussi l'occasion de méditer sur la définition de polyèdre régulier (celle proposée dans [CG13, p.358] est erronée ! On ne veut pas inclure le "dé à 10 faces" par exemple...).

Coloriage:

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

Théorème ([CG13, Exercice C.6 p.375])**.** *Le nombre de façons de colorier un cube avec au plus c couleurs est*

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

Preuve. Avant l'identification par rotation, il y a c^6 coloriages possibles. On fait agir le groupe S_4 des rotations du cube sur l'ensemble X de ces c^6 coloriages, et il s'agit de compter le nombre n d'orbites. La formule de Burnside dit que n est la moyenne du nombre de points fixes :

$$n = \frac{1}{24} \sum_{g \in S_4} \sharp \,\mathrm{Fix}(g).$$

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

- $g = \mathrm{id}$: $\mathrm{Fix}(g) = X$, de cardinal c^6.
- g une rotation d'ordre 2 d'axe passant par milieux d'arêtes, (il y en a 6), $\sharp\,\mathrm{Fix}(g) = c^3$.
- g une rotation d'ordre 3 (il y en a 8), $\sharp\,\mathrm{Fix}(g) = c^2$.
- g une rotation d'ordre 4 (il y en a 6), $\sharp\,\mathrm{Fix}(g) = c^3$.
- g une rotation d'ordre 2 d'axe passant par milieux de faces (il y en a 3), $\sharp\,\mathrm{Fix}(g) = c^4$.

□

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

Table de caractères: [CG14, F. 18 p. 490, p. 523 entre autres]

Il y a 5 classes de conjugaison dans le groupe S_4, voici leur interprétation (faire des dessins !) en termes d'isométries directes préservant un cube (l'action sur les 4 grandes diagonales permet l'identification avec S_4), ainsi que leur cardinal :

- Classe du neutre, cardinal 1.
- Classe des transpositions, rotations d'angle π d'axe passant par les milieux de deux arêtes opposées, cardinal 6.
- Classe des 3-cycles, rotations d'angle $\pm 2\pi/3$ d'axe passant par deux sommets opposés, cardinal 8.
- Classe des 4-cycles, rotations d'angle $\pm\pi/2$ d'axe passant par les milieux de faces opposées, cardinal 6.
- Classe des double transposition, carré des précédentes (rotation d'angle π d'axe passant par les milieux de faces opposées), cardinal 3.

La théorie générale nous dit donc qu'il y a 5 représentations irréductibles pour S_4, les voici ainsi que leurs caractères.

- La représentation triviale ;
- La représentation signature ε ;
- La représentation de degré 3 provenant de la représentation par permutation de S_4 sur C^4, modulo la droite invariante ;
- La même, tordue par la signature (justifier l'irréductibilité !) ;
- La représentation de degré 2 provenant de la représentation par permutation de S_3, via le morphisme $S_4 \to S_3$ (S_4 agit sur les paires de faces opposées du cube...)

	id	$(**)$	$(***)$	$(****)$	$(**)(**)$
1	1	1	1	1	1
ε	1	−1	1	−1	1
perm	3	1	0	−1	−1
$\varepsilon \otimes$ perm	3	−1	0	1	−1
via S_3	2	0	−1	0	2

La deuxième et cinquième ligne donnent des sous-groupes distingués non triviaux, respectivement A_4 et V_4.

Théorème de Frobenius-Zolotarev. [BMP05, p. 251]

Un développement qui a été mis à toutes les sauces par des générations d'agrégatifs... Ce qui me gêne un peu c'est que ça ressemble un peu à un exercice de style gratuit, je ne vois pas trop à quel problème naturel ça répond. Connaître l'application au calcul de la signature du Frobenius permet d'avoir quelque chose à dire en ce sens. Mais bon, certains l'ont exposé avant vous avec succès, donc pourquoi pas, en restant raisonnable dans les couplages.

Leçons :

- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications

Insister sur le lemme qui est une illustration du théorème de factorisation $G/\ker\varphi \simeq \operatorname{Im}\varphi$ (passage au quotient).

- 104. Groupes finis. Exemples et applications

Bon, mais ça n'illustre quand même pas beaucoup les techniques propres aux groupes finis...

- 105. Groupe des permutations d'un ensemble fini. Applications
- 106. Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications
- 108. Exemples de parties génératrices d'un groupe. Applications

Un peu limite, il faut orienter la présentation du développement en insistant sur le fait qu'on utilise (plusieurs fois) que K^* est cyclique, et qu'on utilise au passage que les transvections engendre SL_n...

- 121. Nombres premiers. Applications

Bon, mais ça n'illustre pas grand chose sur les nombres premiers non plus...

- 123. Corps finis. Applications
- Vouloir caser ça dans 152. Déterminant. Exemples et applications me paraît pousser le bouchon un peu loin... Si on insiste, préparer sa défense avec un soin particulier...

Si p est un nombre premier, on note $\mathbb{F}_{p^n}$ le corps à p^n éléments. Si $u \in \mathrm{GL}(V)$, où V est un $\mathbb{F}_p$-espace vectoriel de dimension finie, on peut voir u comme une permutation de l'ensemble fini des vecteurs de V, et donc parler de la signature de u. Rappelons enfin que pour $a \in \mathbb{Z}$, le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut 0 si $p|a$, $+1$ si a est un carré non nul modulo p, et -1 sinon. En fait on a la caractérisation suivante :

Proposition. *Soit $p \geqslant 3$ un nombre premier. L'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ vers $\{-1,+1\}$ est donné par le symbole de Legendre.*

Preuve. Si $\bar{a}$ est un générateur du groupe cyclique $\mathbb{F}_p^*$ d'ordre pair $p-1$, alors $\left(\frac{b}{p}\right) = 1$ ssi $\bar{b} = \bar{a}^{2k} = (\bar{a}^k)^2$ pour un certain k. □

Théorème (Frobenius-Zolotarev)**.** *Soit $p \geqslant 3$ un nombre premier, V un espace vectoriel de dimension finie sur $\mathbb{F}_p$, et $u \in \mathrm{GL}(V)$. Alors*

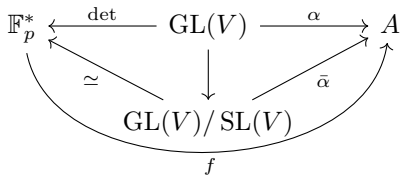
$$sgn(u) = \left(\frac{\det(u)}{p}\right).$$

Lemme. *Le groupe $\mathrm{SL}(V)$ est le groupe dérivé de $\mathrm{GL}(V)$. En particulier, si A est un groupe abélien et $\varphi\colon \mathrm{GL}(V) \to A$ est un morphisme de groupes, alors $\mathrm{SL}(V) \subset \ker\varphi$.*

Preuve. On utilise le fait que $\mathrm{SL}(V)$ est engendré par les transvections. Les transvections sont 2 à 2 conjuguées (dans $\mathrm{GL}(V)$). Si t est une transvection, alors t^2 est encore une transvection (car $p \geqslant 3$), il existe donc $u \in \mathrm{GL}(V)$ tel que $t^2 = utu^{-1}$, et donc $t = utu^{-1}t^{-1}$ est un commutateur. Ainsi le groupe dérivée contient $\mathrm{SL}(V)$, et l'autre inclusion est claire. □

Lemme. *Soit $\alpha\colon \mathrm{GL}(V) \to A$ un morphisme de groupes de $\mathrm{GL}(V)$ vers un groupe abélien A. Alors il existe un unique $f\colon \mathbb{F}_p^* \to A$ tel que $\alpha = f \circ \det$.*

Preuve. Le théorème de factorisation donne un isomorphisme entre $\mathrm{GL}(V)/\mathrm{SL}(V)$ et $\mathbb{F}_p^*$, et un unique morphisme $\bar{\alpha}\colon \mathrm{GL}(V)/\mathrm{SL}(V) \to A$ faisant commuter le diagramme :



□

Preuve du théorème. On applique le lemme au morphisme signature $\mathrm{sgn}\colon \mathrm{GL}(V) \to \{-1,+1\}$. Il existe donc $f\colon \mathbb{F}_p^* \to \{-1,+1\}$ tel que pour tout $u \in \mathrm{GL}(V)$

$$\mathrm{sgn}(u) = f(det(u)).$$

Il reste à voir que f est le symbole de Legendre, ce qui par la proposition revient à voir que f est non trivial. Il suffit de trouver u tel que $\mathrm{sgn}(u) = -1$. Pour cela, considérons V comme le corps $\mathbb{F}_q$, pour $q = p^d$ où d est la dimension de V comme $\mathbb{F}_p$-espace vectoriel. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique, soit x un générateur. Alors la multiplication par x fixe 0 et induit un $(q-1)$-cycle sur les vecteurs non nul de $V = \mathbb{F}_q$, ainsi sa signature est $(-1)^{q-2} = -1$. □

Complément :

Théorème (Base normale sur un corps fini)**.** *Soit p un nombre premier et $q = p^d$ pour un certain $d \geqslant 2$. Alors il existe $\alpha \in \mathbb{F}_q$ tel que $\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$ soit une base de $\mathbb{F}_q$ comme $\mathbb{F}_p$-espace vectoriel. En particulier dans cette base l'automorphisme de Frobenius est cyclique.*

Preuve. On note $F\colon x \mapsto x^p$ l'automorphisme de Frobenius sur $\mathbb{F}_q$. Son polynôme minimal est $X^d - 1$. On sait qu'il existe $\alpha \in \mathbb{F}_q$ dont le polynôme minimal ponctuel est égal au polynôme minimal . Un tel élément α convient. □

Remarque : dans le théorème on ne peut pas prendre n'importe quel α tel que $\mathbb{F}_q = \mathbb{F}_p[\alpha]$, par exemple $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$, mais si α est une racine de $X^4 + X + 1$, on constate que $\alpha^8 - \alpha^4 = \alpha^2 - \alpha$, donc les itérés de α sous l'action du Frobenius ne forment pas une base.

Théorème de Wedderburn. [Per96, p. 82], [RW10, p. 101], [AZ10, Chapter 6].

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications
- 104. Groupes finis. Exemples et applications

A défendre, il me semble que dans un cours sur les groupes finis la preuve s'insèrerait bien après avoir montré qu'un sous-groupe fini de $\mathbf{k}^*$ est cyclique, et que tout p-groupe a un centre non trivial.

- 123. Corps finis. Applications
- 151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications

En insistant sur le fait que tout l'argument tourne autour de calculs de dimension d'espaces vectoriels sur le centre Z...

∼

On commence par un rappel sur les polynômes cyclotomiques. Soit U_n' l'ensemble des racines primitive $n$ièmes de l'unité, et

$$\varphi_n(X) = \prod_{\alpha \in U_n'} X - \alpha$$

le $n$ième polynôme cyclotomique.

Lemme. *Pour tout $n \geqslant 1$, $\varphi_n(X) \in \mathbb{Z}[X]$.*

Preuve. Pour $n = 1$ on a $\varphi_1(X) = X - 1$, and on procède ensuite par récurrence. Puisque

$$X^n - 1 = \left(\prod_{d|n, d \neq n} \varphi_d(X) \right) \varphi_n(X)$$

on obtient le résultat, en constatant que $\varphi_n(X)$ est le quotient de $X^n - 1$ par le polynôme unitaire $\prod_{d|n,d\neq n} \varphi_d(X) \in \mathbb{Z}[X]$. □

Lemme. *Soit $q, n \geqslant d$ des entiers positifs. Alors $q^d - 1 \mid q^n - 1$ implique $d \mid n$.*

Preuve. Le cas $n = d$ étant clair, supposons $n > d$ et procédons par récurrence sur n. Si $q^d - 1 \mid q^n - 1$ alors on a aussi

$$q^d - 1 \mid q^n - 1 - (q^d - 1) = q^n - q^d = q^d(q^{n-d} - 1).$$

Comme q^d et $q^d - 1$ sont premiers entre eux, on obtient $q^d - 1 \mid q^{n-d} - 1$, et on conclut par hypothèse de récurrence. □

Lemme. *Si $d \mid n$, $d \neq n$, alors $\varphi_n(X) \mid \frac{X^n-1}{X^d-1}$. En particulier, pour tout entier q, $\varphi_n(q) \mid \frac{q^n-1}{q^d-1}$.*

Preuve. Par définition

$$X^n - 1 = \prod_{m|n} \varphi_m(X) \text{ et } X^d - 1 = \prod_{m|d} \varphi_m(X),$$

donc

$$\frac{X^n-1}{X^d-1} = \prod_{m|n, m\nmid d} \varphi_m(X)$$

est un multiple de $\varphi_n(X)$. □

Théorème. *Tout corps fini est commutatif*

Preuve. Par l'absurde, supposons qu'il existe un corps fini non commutatif K. On peut supposer K de cardinal minimal pour cette propriété. Le centre Z de K est un sous-corps commutatif d'un certain cardinal $q \geqslant 2$, et K est un Z-espace vectoriel d'une certaine dimension $n \geqslant 2$.

Considérons le groupe multiplicatif K^*. Son centre est Z^*. Pour $x \in K^* \setminus Z^*$, on considère

$$C_x = \{y \in K^*;\ yx = xy\}.$$

C'est un sous-corps de K distinct de K, donc commutatif par minimalité de K. Le cardinal de la classe de conjugaison de x dans K^* est l'indice $[K^* : C_x^*]$, car C_x^* est le stabilisateur de x pour l'action de K^* sur lui-même par conjugaison. En notant S un système de représentants des classes de conjugaisons non ponctuelles de K^*, et n_x la dimension de C_x comme Z-espace vectoriel, on écrit l'équation aux classes :

$$q^n - 1 = |K^*| = |Z^*| + \sum_{x\in S} [K^* : C_x^*] = q - 1 + \sum_{x\in S} \frac{q^n-1}{q^{n_x}-1}.$$

Comme on a une tour d'extensions $Z \subsetneq C_x \subsetneq K$, on en déduit que $q^{n_x} - 1$ divise strictement $q^n - 1$, et donc par le deuxième lemme que n_x divise strictement n.

Enfin par le troisième lemme l'entier $\varphi_n(q)$ divise chaque terme de la somme $\sum_{x\in S} \frac{q^n-1}{q^{n_x}-1}$, et également $q^n - 1$, donc $\varphi_n(q)$ divise $q - 1$. C'est la contradiction attendue, car comme $n \geqslant 2$,

$$\varphi_n(q) = |\varphi_n(q)| = \prod_{\alpha\in U_n'} |q - \alpha|$$

est un produit de termes tous strictement plus grands que $q - 1$. □

Remarque. La terminologie moderne est plutôt de réserver le mot "corps" à une situation commutative, et d'appeler "algèbre à division" un anneau (éventuellement non commutatif) dont tout élément non nul est inversible.

Dans ce cas, le théorème de Wedderburn devient : "Toute algèbre à division finie est un corps".

Groupes d'ordre pq. [RW10, p. 24], [Gou09, problème 9 2) p. 41].

Leçons :

- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications
- 104. Groupes finis. Exemples et applications
- 121. Nombres premiers. Applications
- Il me semble par contre fort douteux de chercher à placer ça dans "Anneau $\mathbb{Z}/n\mathbb{Z}$", vu qu'il n'y pas l'ombre d'un anneau dans ce développement...

∼

Version sans Sylow : [Gou09], mais j'inverse les rôles de p et q pour pouvoir comparer avec [RW10].

Lemme. *Soit G un groupe tel que $G/Z(G)$ soit monogène. Alors G est abélien (et en particulier le groupe monogène $G/Z(G)$ était en fait trivial).*

Preuve. Par hypothèse, il existe $a \in G$ dont la classe $\bar{a} \in G/Z(G)$ engendre $G/Z(G)$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(G)$. Or a commute avec tout élément de la forme $a^k h$, et donc $a \in Z(G)$, et $G/Z(G)$ est trivial. □

Théorème. *Soit $p > q$ deux nombres premiers, et G un groupe non abélien d'ordre pq. Alors G est de centre trivial, admet un unique groupe K d'ordre p, q divise $p - 1$ et G est un produit semi-direct $G = K \rtimes H$ avec H cyclique d'ordre q.*

Preuve. Si le centre de G n'est pas trivial, il est d'ordre p ou q puisque G est non abélien. Mais alors le quotient $G/Z(G)$ serait cyclique d'ordre q ou p, c'est impossible par le lemme.

Supposons maintenant que G n'admette aucun sous-groupe d'ordre p, et considérons l'action de G sur lui-même par conjugaison. La seule orbite singleton est celle du neutre (car le centre est trivial), et chaque orbite non réduite à un singleton est d'ordre p, associée à un stabilisateur d'ordre q. Si on note $k \geqslant 0$ le nombre de telles orbites, on obtient

$$|G| = pq = 1 + kp$$

ce qui donne une contradiction après réduction modulo p. De la même manière, on montre que G admet au moins un sous-groupe H d'ordre q.

S'il existe K_1, K_2 deux sous-groupes distincts d'ordre p, alors par Lagrange $K_1 \cap K_2 = \{1\}$ et donc on obtient une injection (ensembliste, pas un morphisme) $K_1 \times K_2 \to G$, ce qui contredit $p > q$.

Finalement il existe un unique sous-groupe K d'ordre p, donc K est distingué dans G, et il existe (au moins) un sous-groupe H d'ordre q, ce qui donne la structure de produit semi-direct attendu ($H \cap K = \{1\}$ à nouveau par Lagrange).

Pour tout $h \in H \setminus \{1\}$, h ne commute pas avec tous les éléments de K car sinon comme h engendre le groupe cyclique H on aurait $G = H \times K$ abélien. Donc H agit fidèlement par conjugaison sur K, autrement dit H s'injecte dans le groupe $\mathrm{Aut}(K) \simeq \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ qui est d'ordre $p-1$. Par Lagrange, on conclut que q divise $p-1$. □

Complément : on peut réaliser un groupe non-abélien d'ordre pq comme un groupe de matrice 2×2 à coefficients $\mathbb{Z}/p\mathbb{Z}$. On sait que $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$, et comme q divise $p-1$ par hypothèse, il existe un sous-groupe T d'ordre q dans $\mathbb{F}_p^*$: écrire $\mathbb{F}_p^* = \langle \bar{a} \rangle$, et poser $T = \langle \bar{a}^k \rangle$ où $kq = p-1$ Alors le groupe d'ordre pq recherché est

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid 1 \in T, b \in \mathbb{F}_p \right\}$$

et les sous-groupes d'ordre p et q du produit semi-direct sont

$$K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} b \in \mathbb{F}_p \right\} \qquad H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} a \in T \right\}$$

Version avec Sylow :

Théorème. *Soient $p > q$ deux nombres premiers.*

(1) *Si $p \not\equiv 1 \mod q$, alors $\mathbb{Z}/pq\mathbb{Z}$ est l'unique groupe d'ordre pq, à isomorphisme près ;*

(2) *Si $p \equiv 1 \mod q$, il y a un unique (à isomorphisme près) autre groupe d'ordre pq, à isomorphisme près, qui est un produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.*

Pour la preuve on va utiliser les théorèmes de Sylow :

Proposition (Sylow)**.** *Soit G un groupe fini et p un nombre premier.*

(1) *Le nombre de p-Sylow est congru à 1 modulo p, et divise m, où $|G| = p^r m$ avec $p \wedge m = 1$;*

(2) *Les p-Sylow sont deux à deux conjugués dans G.*

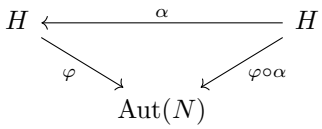
Preuve du théorème. Soit G un groupe d'ordre pq, et soit P un p-Sylow de G, et Q un q-Sylow de G. Le nombre de p-Sylow divise q et est congru à 1 modulo p, donc comme $p > q$ on en déduit que P est l'unique p-Sylow de G, en particulier P est distingué dans G.

Comme $|P| = p$ et $|Q| = q$ on a $P \cap Q = \{1\}$ et en particulier l'application $(x, y) \in P \times Q \mapsto xy \in G$ est injective, donc surjective. Ainsi G est un produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$, où $\varphi \colon \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ correspond à l'action par conjugaison de Q sur P. Observons que le cardinal de l'image de φ doit diviser q et $p-1$. Il y a donc deux cas possibles : ou bien φ est trivial et G est le produit direct de P et Q, ou bien φ est d'image de cardinal q, ce qui n'est possible que si q divise $p-1$, ou autrement dit $p \equiv 1 \mod q$.

Dans ce dernier cas, φ est déterminé par le choix d'un élément d'ordre q dans $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ (image de $1 \in \mathbb{Z}/q\mathbb{Z}$). Or $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est cyclique d'ordre $p-1$, donc contient exactement un sous-groupe d'ordre q. Pour chaque élément u d'ordre q, on a un morphisme $\varphi \colon \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ tel que l'automorphisme $\varphi(1)$ soit $\varphi(1) \colon k \in \mathbb{Z}/p\mathbb{Z} \mapsto uk \in \mathbb{Z}/p\mathbb{Z}$. Si u' est un autre élément d'ordre q, comme $\langle u \rangle = \langle u' \rangle$ il existe $h \in \mathbb{N}$ tel que $u' = u^h$. Donc en posant $\alpha \in \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ l'automorphisme qui envoie 1 sur h, le morphisme φ' associé à u' est égal à $\varphi \circ \alpha$ et on peut appliquer le lemme ci-dessous pour conclure que les produits semi-directs correspondants sont isomorphes. □

On a utilisé le lemme

Lemme. *Considérons un diagramme commutatif, où $\alpha \in \mathrm{Aut}(H)$:*



Alors $\mathrm{id} \times \alpha$ *est un isomorphisme entre les produits semi-directs $N \rtimes_{\varphi\circ\alpha} H$ et $N \rtimes_\varphi H$.*

Isomorphismes exceptionnels. [CG13, p.257], [Per96, 106].

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 103. Exemples de sous-groupes distingués et de groupes quotients. Applications
- 104. Groupes 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 GL(E). Applications

Théorème. *On a les isomorphismes (les deux derniers concernent des groupes simples)*

(*i*) $\mathrm{PSL}_2(\mathbb{F}_2) \simeq S_3$;

(*ii*) $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$;

(*iii*) $\mathrm{PSL}_2(\mathbb{F}_4) \simeq A_5$;

(*iv*) $\mathrm{PSL}_2(\mathbb{F}_5) \simeq A_5$.

Preuve. On fait agir $\mathrm{PGL}_2(\mathbb{F}_q)$ sur les droites vectorielles de $(\mathbb{F}_q)^2$. Il y a $q+1$ telles droites, on obtient dont un morphisme (injectif)

$$\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow S_{q+1}.$$

D'autre part le cardinal de $\mathrm{PGL}_2(\mathbb{F}_q)$ est $(q^2-1)(q^2-q)/(q-1) = q(q^2-1)$, et c'est aussi le cardinal de $\mathrm{SL}_2(\mathbb{F}_q)$. Si $\operatorname{car}\mathbb{F}_q \neq 2$, on a $\mathrm{PSL}_2(\mathbb{F}_q)$ d'indice 2 dans $\mathrm{PGL}_2(\mathbb{F}_q)$. On applique ces remarques à chacun des cas $q = 2, 3, 4, 5$:

(*i*) On a $\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2)$, de cardinal 6.

(*ii*) On trouve $|\mathrm{PGL}_2(\mathbb{F}_3)| = 24$, donc $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$, et comme A_4 est le seul sous-groupe d'indice 2 dans S_4 : $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$.

(*iii*) On trouve $|\mathrm{PGL}_2(\mathbb{F}_4)| = |\mathrm{PSL}_2(\mathbb{F}_4)| = 60$, et comme A_5 est le seul sous-groupe d'indice 2 dans S_5 : $\mathrm{PSL}_2(\mathbb{F}_4) \simeq A_5$.

(*iv*) On trouve $|\mathrm{PGL}_2(\mathbb{F}_5)| = 120$, donc $\mathrm{PGL}_2(\mathbb{F}_5)$ s'identifie à un sous-groupe d'indice 6 de S_6. Par le lemme ci-dessous on en déduit $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$, et comme précédemment, $\mathrm{PSL}_2(\mathbb{F}_5)$ étant d'indice 2 dans $\mathrm{PGL}_2(\mathbb{F}_5)$, il est isomorphe à A_5. □

Lemme ([Per96, p.30])**.** *Tout sous-groupe H d'indice n dans S_n est isomorphe à S_{n-1}.*

Preuve. Pour $n = 2, 3, 4$, ça se vérifie directement. Pour $n \geqslant 5$, on considère l'action par translation de S_n sur les classes à gauche S_n/H :

$$\sigma \cdot \gamma H := (\sigma\gamma)H.$$

On obtient ainsi un morphisme φ de S_n dans S_n. Le noyau est un sous-groupe distingué de S_n d'indice au moins n (car contenu dans H), or les seuls sous-groupes distingué de S_n, pour $n \geqslant 5$, sont S_n, A_n et le groupe trivial. Ainsi φ est injectif, donc un isomorphisme. Comme H est le stabilisateur de la classe $\mathrm{id}H$, on a $\varphi(H) \subset S_n$ stabilisateur d'un point : ainsi $\varphi(H)$ est isomorphe à S_{n-1}. □

Sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$. [CG14, chap. IX], [Szp09, p. 434]

Ne pas chercher à traiter tous les cas de façon exhaustive. Faire des choix, et montrer qu'on sait faire plus en réaction aux questions du jury...

Leçons :

- 101. Groupe opérant sur un ensemble. Exemples et applications
- 104. Groupes finis. Exemples et applications

Dire que pour un groupe quelconque (même infini), une question naturelle est toujours de classifier les sous-groupes finis...

- 160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie) ??
- 161. Distances et isométries d'un espace affine euclidien
- 183. Utilisation des groupes en géométrie

Classifier ces sous-groupes finis revient à classifier les solides platoniciens...

- 190. Méthodes combinatoires, problèmes de dénombrements

Théorème. *Tout sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, A_4, S_4 ou A_5.*

On utilisera les deux lemmes (à mettre dans le plan, et à savoir montrer !) :

Lemme. *Tout sous-groupe fini de $\mathrm{SO}_2(\mathbb{R})$ est cyclique.*

Lemme (Burnside)**.** *Soit G un groupe fini agissant sur un ensemble X fini. Alors le nombre k d'orbites est donné par la formule*

$$k = \frac{1}{|G|} \sum_G |\operatorname{Fix}(g)|$$

Soit $G \subset \mathrm{SO}_3(\mathbb{R})$ un sous-groupe fini d'ordre n. A tout élément de G distinct de l'identité on associe deux pôles, qui par définition sont l'intersection de l'axe de la rotation avec la sphère unité de $\mathbb{R}^3$. Le groupe G agit sur l'ensemble X des pôles des éléments de G, qui est fini, et la définition donne la majoration suivante :

$$|X| \leqslant 2(n-1).$$

Comme toute rotation distincte de l'identité dans G fixe exactement deux pôles, et que l'identité fixe tout les éléments de X, la formule de Burnside donne le nombre k d'orbites de cette action :

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

On a aussi grâce à la majoration précédente

$$k \leqslant \frac{4(n-1)}{n} < 4.$$

On a donc $k \in \{2, 3\}$.

Fait. *Si $k = 2$, alors G est cyclique.*

Preuve. La formule précédente montre que $k = 2$ si et seulement si $|X| = 2$, et dans ce cas les rotations de G ont toutes le même axe. Ainsi G peut être vu comme un sous-groupe fini de rotation du plan orthogonal à cet unique axe, ce qui implique G cyclique. □

Fait. *Si $k = 3$, notons ω_1, ω_2, ω_3 les orbites et $n_1 \leqslant n_2 \leqslant n_3$ les cardinaux des stabilisateurs correspondants.*

(1) *Si $n_1 = n_2 = 2$, alors $|G| = |D_{n_3}| = 2n_3$.*

(2) *Sinon on est dans l'une des situations suivantes :*

- $(n_1, n_2, n_3) = (2, 3, 3)$, *et* $|G| = |A_4| = 12$.
- $(n_1, n_2, n_3) = (2, 3, 4)$, *et* $|G| = |S_4| = 24$.
- $(n_1, n_2, n_3) = (2, 3, 5)$, *et* $|G| = |A_5| = 60$.

Preuve. On commence par déterminer les triplets (n_1, n_2, n_3) possibles. La formule de Burnside se lit $3 = 2 + \frac{|X|-2}{n}$. Par ailleurs on a $|\omega_i| = \frac{n}{n_i}$, et donc

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

Finalement on obtient la condition

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

Par définition, un pôle est fixé par au moins l'identité et une autre rotation, ainsi $n_1 \geqslant 2$. On a donc $n_1 = 2$, sinon la condition précédente ne serait pas remplie. Par le même argument, $3 \geqslant n_2 \geqslant 2$. Si $n_2 = 2$, alors n_3 est arbitraire, et $n = 2n_3$. Si $n_2 = 3$, alors $5 \geqslant n_3 \geqslant 3$, ce qui donne les trois cas listés. De plus on obtient $n = \frac{12n_3}{6-n_3}$, ce qui donne $n = 12, 24, 60$ lorsque $n_3 = 3, 4, 5$. □

On connaît des groupes correspondant aux cas listés : rotations préservant respectivement une double pyramide sur un polygône régulier, un tétraèdre, un cube ou un icosaèdre. Reste à voir que tout groupe avec les invariants (ordre du groupe, des orbites...) d'un tel exemple est en fait égal à un tel exemple. On traite le cas le plus simple, celui où $|G| = 12$:

• Cas $(2, 3, 3)$ (tétraèdre). L'orbite ω_3 est de cardinal $12/3 = 4$, notons x_1, x_2, x_3, x_4 ses éléments. On peut de plus supposer que x_1 et x_2 ne sont pas symétrique par rapport à l'origine. Il existe une rotation $r \in \mathrm{Stab}(x_1)$ d'ordre 3 (par la formule $|\mathrm{Stab}||\mathrm{Orb}| = 12$), et donc quitte à réordonner on a $x_3 = r(x_2)$, $x_4 = r^{-1}(x_2)$. En particulier les points x_2, x_3, x_4 sont équidistants de x_1. Comme on peut faire le même raisonnement pour chaque x_i, on obtient que x_1, x_2, x_3, x_4 sont les sommets d'un tétraèdre régulier préservé par G. Par ailleurs on sait que le groupe des rotations préservant un tétraèdre est d'ordre 12, notre groupe G étant d'ordre 12 il est donc égal au groupe du tétraèdre (isomorphe à A_4, qui est l'unique sous-groupe d'indice 2 dans S_4).

Leçons où l'on peut envisager ces développements

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

- **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$
- **Caractères et sous-groupes normaux de** S_4**, isométries et coloriages du cube**
- **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$
- **Isomorphismes exceptionnels**
- **Théorème de Wedderburn**
- **Automorphismes du groupe symétrique**
- ...

102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications :

- **Théorème de Wedderburn**
- ...

103. Exemples de sous-groupes distingués et de groupes quotients. Applications :

- **Théorème de Frobenius-Zolotarev**
- **Caractères et sous-groupes normaux de** S_4**, isométries et coloriages du cube**
- **Isomorphismes exceptionnels**
- **Simplicité de** A_n
- ...

104. Groupes finis. Exemples et applications :

- **Caractères et sous-groupes normaux de** S_4**, isométries et coloriages du cube**
- **Théorème de Wedderburn**
- **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$
- **Isomorphismes exceptionnels**
- **Automorphismes du groupe symétrique**
- **Simplicité de** A_n
- ...

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

- **Théorème de Frobenius-Zolotarev**
- **Caractères et sous-groupes normaux de** S_4**, isométries et coloriages du cube**
- **Isomorphismes exceptionnels**
- **Automorphismes du groupe symétrique**
- **Simplicité de** A_n
- ...

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

- **Théorème de Frobenius-Zolotarev**
- **Isomorphismes exceptionnels**
- **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$
- ...

107. Représentations et caractères d'un groupe fini sur un C-espace vectoriel. Exemples :

- **Caractères et sous-groupes normaux de** S_4**, isométries et coloriages du cube**
- ...

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

- **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$
- **Théorème de Frobenius-Zolotarev**
- **Automorphismes du groupe symétrique**
- **Simplicité de** A_n
- ...

110. Structure et dualité des groupes abéliens finis. Applications :

- ...

120. Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications :

- ...

121. Nombres premiers. Applications :

- ...

122. Anneaux principaux. Applications :

- ...

123. Corps finis. Applications :

- **Théorème de Frobenius-Zolotarev**
- **Théorème de Wedderburn**
- ...

125. Extensions de corps. Exemples et applications :

- ...

126. Exemples d'équations en arithmétique :

- ...

141. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications. :

- ...

142. PGCD et PPCM, algorithmes de calcul. Applications :

- ...

144. Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications :

- ...

150. Exemples d'actions de groupes sur les espaces de matrices :

- ...

151. Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications :

- **Théorème de Wedderburn**
- ...

152. Déterminant. Exemples et applications :

- ...

153. Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications :

- ...

154. Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications :

- **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$
- ...

155. Endomorphismes diagonalisables en dimension finie :

- ...

156. Exponentielle de matrices. Applications :

- ...

157. Endomorphismes trigonalisables. Endomorphismes nilpotents :

- ...

158. Matrices symétriques réelles, matrices hermitiennes :

- ...

159. Formes linéaires et dualité en dimension finie. Exemples et applications :

- ...

160. Endomorphismes remarquables d'un espace vectoriel euclidien (de dimension finie) :

- **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$
- **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$

??

• ...

161. Distances et isométries d'un espace affine euclidien :

• **Caractères et sous-groupes normaux de S_4, isométries et coloriages du cube**

• **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$

• **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$

• ...

162. Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques :

• ...

170. Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications :

• **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$

• ...

171. Formes quadratiques réelles. Coniques. Exemples et applications :

• **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$

• ...

181. Barycentres dans un espace affine réel de dimension finie, convexité. Applications :

• ...

182. Applications des nombres complexes à la géométrie. :

• **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$

• ...

183. Utilisation des groupes en géométrie :

• **Isomorphisme exceptionnel** $\mathrm{SU}_2/\{\pm 1\} \simeq \mathrm{SO}_3$

• **Caractères et sous-groupes normaux de S_4, isométries et coloriages du cube**

• **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$

• ...

190. Méthodes combinatoires, problèmes de dénombrements :

• **Caractères et sous-groupes normaux de S_4, isométries et coloriages du cube**
Dénombrer les coloriages.

• **Sous-groupes finis de** $\mathrm{SO}_3(\mathbb{R})$
Illustre la technique d'action de groupe via la formule de Burnside.

• ...

Références

[Ale99] M. Alessandri. *Thème de géométrie*. Dunod, 1999. 5

[AZ10] M. Aigner & G. M. Ziegler. *Proofs from The Book*. Springer-Verlag, Berlin, fourth edition, 2010. 8

[BMP05] V. Beck, J. Malick & G. Peyré. *Objectif agrégation*. H&K, 2005. 7

[CG13] P. Caldero & J. Germoni. *Histoires hédonistes de groupes et de géométries, Tome premier*. Calvage & Mounet, 2013. 3, 4, 5, 6, 10

[CG14] P. Caldero & J. Germoni. *Histoires hédonistes de groupes et de géométries, Tome second*. Calvage & Mounet, 2014. 3, 5, 6, 11

[Gou09] X. Gourdon. *Algèbre*. Ellipses, 2009. 9

[Per96] D. Perrin. *Cours d'algèbre*. Ellipses, 1996. 2, 8, 10, 11

[Pey04] G. Peyré. *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004. 5

[RW10] J.-P. Ramis & A. Warusfel. *Cours de mathématique vol.1 algèbre et géométrie*. De Boeck, 2010. 1, 2, 5, 8, 9

[Szp09] A. Szpirglas, editor. *Mathématiques L3 Algèbre*. Pearson Education, 2009. 1, 2, 3, 5, 6, 11