[ULM]
[PER]

Groupe opérant sur un ensemble. Exemples et applications

101

I Generalités sur les actions de groupes

Soit G un groupe, X un ensemble

Def 1: Une action à gauche est une application $\begin{cases} G \times X \to X \\ (g,x) \mapsto g.x \end{cases}$ qui vérifie: 1) $e.x = x \quad \forall x \in X$
2) $g.(g'.x) = (gg').x \quad \forall g, g' \in G$

On dit alors que X est un G-ensemble et on note $G \curvearrowright X$ l'action.

exemples:

1) $GL(V) \times V \to V$, $(g,x) \mapsto g(x)$ où V un espace vectoriel

2) $\mathfrak{S}_n \times \{1,\dots n\} \to \{1,\dots n\}$, $(\sigma, i) \mapsto \sigma(i)$

3) P plan affine : $Isom(P) \curvearrowright P$

Thm/def 2:
- Il existe un unique morphisme φ associé à une action $G \curvearrowright X$: $\varphi : \begin{cases} G \to \mathfrak{S}(X) \\ g \mapsto \varphi_g : \begin{cases} X \to X \\ x \mapsto \varphi_g(x) = g.x \end{cases} \end{cases}$
- Réciproquement, un morphisme $\varphi : G \to \mathfrak{S}(X)$ définit une unique action $G \curvearrowright X$.
- φ est le morphisme structurel de l'action.

Def 3: Soit $G \curvearrowright X$ une action,
- le stabilisateur d'un point $x \in X$ est le sous-groupe de G : $Stab_x = \{g \in G / g.x = x\}$
- $Fix(G) := \{x \in X / \forall g \in G, g.x = x\}$
- L'orbite d'un point $x \in X$ est le sous-ensemble de X $Gx = \{g.x / g \in G\}$
- $G \curvearrowright X$ librement si $\forall x \in X$, $Stab_x = \{e\}$
- $G \curvearrowright X$ fidèlement si $\varphi : G \to \mathfrak{S}(X)$ est injectif
- $G \curvearrowright X$ transitivement si il existe exactement une orbite.

prop 4: $\ker \varphi = \bigcap_{x \in X} Stab_x$

exemple: Décomposition des permutations en produit de cycles de supports disjoints: soit $\sigma \in \mathfrak{S}_n$, $\langle \sigma \rangle \curvearrowright \{1,\dots n\}$ alors $\sigma = \gamma_1 \dots \gamma_m$, γ_i cycles dont les supports sont les orbites.

prop 5: 1) $G \curvearrowright X$ et $\psi : \Gamma \to G$ homomorphisme $\Rightarrow$ X est un Γ-ensemble

2) $Y \subset X$ est stable sous l'action de $G \Rightarrow Y$ est un G-ensemble

coro 6: Soit $\varphi : G \to \mathfrak{S}(X)$ une action de groupe, H sous-groupe de G, alors X est un H-ensemble de morphisme structurel $\Phi : H \hookrightarrow G \xrightarrow{\varphi} \mathfrak{S}(X)$.

coro 7: Soit $G \curvearrowright X$ une action, $Y \subset X$ est réunion d'orbites, alors Y est aussi un G-ensemble pour la restriction à Y de l'action $G \curvearrowright X$.

exemple: $D_n = \langle r, s / r^n = s^2 = (rs)^2 = e \rangle$ sous-groupe de $Isom(P)$ donc $D_n \curvearrowright P$; puis D_n laissant fixe $Y = \{n$ sommets d'un polygone$\}$ $D_n \curvearrowright Y$, elle est transitive, non libre et fidèle si $n \geq 3$.

prop 8: $G \curvearrowright X$ une action, alors on définit une relation d'équivalence: $x \sim y$ ssi $x \in Gy$. On a donc $X = \bigcup_{x \in X/\sim} Gx$.

II Faire agir un groupe pour le comprendre

[ULM]
[PER]

1) $G \curvearrowright G$ par translation

def 9: G agit sur lui-même par translation à gauche : $\begin{cases} G \times G \to G \\ (g,h) \mapsto gh \end{cases}$

prop 10: Cette action est transitive, fidèle et libre.

Thm 11: Théorème de Cayley: Tout groupe fini G d'ordre $n \in \mathbb{N}$ est isomorphe à un sous-groupe transitif de $\mathfrak{S}_n$.

Rq: $G \curvearrowright G/H$ est bien définie : $\begin{cases} G \times G/H \to G/H \\ (g, \tilde{g}H) \mapsto (g\tilde{g})H \end{cases}$

Application: Théorème de Lagrange : $|G| = |H| \cdot |G/H|$

prop 12: Soit G un groupe, H un sous-groupe de G. L'action $G \curvearrowright G/H$ est transitive et son morphisme structurel est de la forme $\varphi : G \to \mathfrak{S}_{(G:H)}$.

exemple: On montre que $GL(2,2) \simeq \mathfrak{S}_3$ en considérant le sous-groupe $H = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ et l'action $GL(2,2) \curvearrowright GL(2,2)/H$

2) $G \curvearrowright G$ par conjugaison

Def 13: G agit sur lui-même par conjugaison: $G \times G \to G$, $(g,h) \mapsto ghg^{-1}$

Def 14: * L'orbite de h, $\mathcal{C}_h = \{ghg^{-1} / g \in G\}$ s'appelle la classe de conjugaison de h.
* Le stabilisateur $Stab_h = \{g \in G / ghg^{-1} = h\}$ s'appelle le centralisateur de h dans G, noté $Z_G(h)$.

Rq: Si $G \neq \{e\}$, cette action n'est ni libre ni transitive.

Application: 1) $\sigma\ (a_1 \dots a_p) \in \mathfrak{S}_n$, $\tau \in \mathfrak{S}_n \Rightarrow \tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_p))$.
2) Tous les p-cycles sont conjugués dans $\mathfrak{S}_n$.
3) $n \geq 5 \Rightarrow$ Les 3-cycles sont conjugués dans $\mathcal{A}_n$.

3) Formule des classes et application aux p-groupes

Coro 15: Relation orbite-stabilisateur: $G \curvearrowright X$, $x \in X$, alors $|\mathcal{O}_x| = (G : Stab_x)$ et $|G| = |\mathcal{O}_x| \cdot |Stab_x|$

Coro 16: Formule des classes: G un groupe fini, X un G-ensemble fini, alors:
1. Si $X = \bigcup_{i=1}^{r} X_i$ où X_i orbite de $x_i \in X$, alors:
$$|X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} (G : Stab_{x_i}) = \sum_{i=1}^{r} \frac{|G|}{|Stab_{x_i}|}$$
2. $X^g := Fix(\langle g \rangle)$, $g \in G$, alors le nombre n d'orbites de X par $G \curvearrowright X$ est $n = \frac{1}{|G|} \sum_{g \in G} |X^g|$

Application: Soit G un sous-groupe fini de $SO_3(\mathbb{R})$, alors $G \simeq \mathbb{Z}/m\mathbb{Z}$, D_m, $\mathcal{A}_4$, $\mathcal{A}_5$ ou $\mathfrak{S}_4$ $(m \geq 2)$. DVT

def 17: Soit p premier, un p-groupe est un groupe d'ordre une puissance de p.

Application: Classification des groupes d'ordre 8.

prop 18: Soit p premier, G un p-groupe et X un G-ensemble fini, alors $|X^G| = |X| \mod p$.

Lemme 19: Lemme de Cauchy: G un groupe fini tel que $|G|$ est divisible par un nombre premier p, alors $\exists\, g \in G$ tel que g est d'ordre p.

prop 20: G un p-groupe fini, $G \neq \{e\} \Rightarrow Z(G) \neq \{e\}$.

Application: Un groupe G d'ordre p^2 est toujours abélien et $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$

def 21: p premier, G un groupe fini. Un p-groupe de Sylow de G ou p-sylow de G est un p-sous-groupe de puissance maximale

Thm 22: Théorème de Sylow: p premier, G groupe fini tel que $\#G = p^e m$ où $m \wedge p = 1$. Alors
1 - les p-sylows de G sont les sous-groupes d'ordre p^e
2 - Ils sont tous conjugués. En particulier, notons P un p-sylow, alors le nombre de p-sylows est $n_p = (G : N_G(P))$
3 - $n_p \mid m$ et $n_p \equiv 1 [p]$.

Peut faire un tout développement ↓ Serre, Représentations linéaires

Application: Tout groupe simple (ie $H \trianglelefteq G \Rightarrow H = \{e\}$ ou $H = G$) d'ordre 60 est isomorphe à $\mathcal{A}_5$. DVT

coro 23: Soit S un p-sylow de G, alors: $S \trianglelefteq G \Leftrightarrow n_p = 1$.

III Étudier un ensemble grâce à une action de groupe

Soit $\mathbb{K}$ un corps commutatif.

[GOU] [CAL]

1) L'ensemble des matrices

def 24: $GL_n(\mathbb{K})$ agit par conjugaison sur $\mathcal{M}_n(\mathbb{K})$:

$GL_n(\mathbb{K}) \times \mathcal{M}_n(\mathbb{K}) \longrightarrow \mathcal{M}_n(\mathbb{K})$ par $(P, M) \mapsto PMP^{-1}$

Deux matrices dans une même orbite sont dites semblables

Applications: * Réduction des endomorphismes

* $A, B \in \mathcal{M}_n(\mathbb{R})$ / $A \sim B$ dans $\mathcal{M}_n(\mathbb{C}) \Rightarrow A \sim B$ dans $\mathcal{M}_n(\mathbb{R})$.

DVT

* Nombre d'automorphismes diagonalisables sur $\mathbb{F}_q$.

def 25: $GL_n(\mathbb{K}) \times GL_p(\mathbb{K})$ agit sur $\mathcal{M}_{np}(\mathbb{K})$ par équivalence :

$GL_n(\mathbb{K}) \times GL_p(\mathbb{K}) \times \mathcal{M}_{np}(\mathbb{K}) \longrightarrow \mathcal{M}_{np}(\mathbb{K})$ par $(P, Q, M) \mapsto PMQ^{-1}$

Deux matrices dans la même orbite sont dites équivalentes

prop 26: • Un système de représentants des orbites est donné par les matrices de rang r J_r : $J_r = \begin{pmatrix} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ & 0 & & 0 \end{pmatrix}$ (r lignes, r colonnes)

• Deux matrices sont équivalentes ssi elles ont le même rang.

Applications: * $\forall A \in \mathcal{M}_{np}(\mathbb{K})$, $rg(A) = rg({}^tA)$

* Nombre de matrices de rang r dans $\mathcal{M}_n(\mathbb{F}_q)$.

[GOU] [GRI] [CAL]

2) Les formes quadratiques

def 27: $GL_n(\mathbb{R})$ agit sur $S_n(\mathbb{R})$ par congruence :

$GL_n(\mathbb{R}) \times S_n(\mathbb{R}) \longrightarrow S_n(\mathbb{R})$ par $(P, M) \mapsto {}^tPMP$

def 28: Une forme quadratique q sur un $\mathbb{R}$-ev E de dimension finie est une application $q : \begin{cases} E \to \mathbb{R} \\ x \mapsto \varphi(x,x) \end{cases}$ où φ est une forme bilinéaire symétrique.

Dans une base $\mathcal{B}$, $Mat_{\mathcal{B}}(q) := Mat_{\mathcal{B}}(\varphi) \in S_n(\mathbb{R})$.

Application: Deux matrices congrues représentent la même forme quadratique dans deux bases différentes.

Thm 29: Théorème d'inertie de Sylvester : Soit q une forme quadratique sur E un $\mathbb{R}$-ev de dimension finie. Alors il existe une base $\{e_i\}$ de E telle que si $x = \sum_{i=1}^{n} x_i e_i$, $q(x) = x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_r^2$ et $Mat_{\{e_i\}}(q) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & 0 \\ & & 1 & & \\ & & & -1 & \\ & & & & \ddots \\ & 0 & & & -1 \end{pmatrix}$

On appelle signature de q le couple $(p, r-p)$.

Coro 30: * q définie positive $\iff$ $sign(q) = (n, 0)$ (ie E espace euclidien)

* q définie négative $\iff$ $sign(q) = (0, n)$

* q non dégénérée $\iff$ $sign(q) = (p, n-p)$

exemple: $q(x) = x_1^2 + 2x_2^2 + 15x_3^2 - 4x_1x_2 + 6x_1x_3 - 8x_2x_3$

$= (x_1 - 2x_2 + 3x_3)^2 - 2(x_2 - x_3)^2 + 8x_3^2$

Dans la base $\{y_i\}_{i=1}^3$ de $\mathbb{R}^3$ définie par $y_1 = x_1 - 2x_2 + 3x_3$, $y_3 = \sqrt{2}(x_2 - x_3)$ et $y_2 = 2\sqrt{2}x_3$ on a $Mat_{\{y_i\}}(q) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ et $sign(q) = (2, 1)$

3) Les groupes projectifs

[ULM] [PER]

def 31: k un corps, V un k-ev de dimension $n+1$, on appelle espace projectif de dimension n associé à V, noté $\mathbb{P}(V)$, l'ensemble des droites vectorielles de V. On note $\mathbb{P}_n(k) := \mathbb{P}(V)$.

prop 32: $GL(V) \curvearrowright \mathbb{P}(V)$

$PGL(V) \curvearrowright \mathbb{P}(V)$ fidèlement

Application: On a les isomorphismes suivants :

1) $GL(2, \mathbb{F}_2) = SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$

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

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

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

Nombre d'automorphismes diagonalisables sur un corps fini

Dans le développement proposé ici, on dénombre les matrices inversibles à coefficients dans un corps fini $\mathbb{F}_q$ qui sont diagonalisables. Ce développement peut être utilisé dans les leçons suivantes :

Groupes opérant sur un ensemble. Exemples et applications.
Groupes finis. Exemples et applications.
Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
Nombres premiers. Applications.
Corps finis. Applications.
Endomorphismes diagonalisables.
Méthodes combinatoires, problèmes de dénombrement.

Théorème : *Soit $n \geq 1$ un entier. Alors le nombre de matrices diagonalisables dans le groupe linéaire $\mathrm{GL}_n(\mathbb{F}_q)$ sur le corps fini $\mathbb{F}_q$ est égal à*

$$\sum_{\substack{(n_1,\dots,n_{q-1}) \\ \text{t.q. } n_1+\cdots+n_{q-1}=n}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)|\dots|\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}.$$

La preuve utilise d'abord un exercice de [Gourdon] (page 176), puis adapte un argument que l'on trouve dans [FGN1] (*Nombre d'involutions*, page 17).

Preuve : *On commence par observer qu'une matrice $A \in \mathrm{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q - A = 0$. En effet si A est diagonalisable, on peut écrire $A = PDP^{-1}$ avec D diagonale. Comme les coefficients de D sont dans $\mathbb{F}_q$ on a $D^q = D$ dont on déduit $A^q = A$. Réciproquement, si $A^q = A$, alors A est annulé par le polynôme $X^q - X$, qui est à racines simples. Donc le polynôme minimal de A, diviseur de $X^q - X$, est à racines simples, donc A est diagonalisable.*

Si $A \in \mathrm{GL}_n(\mathbb{F}_q)$, alors A est diagonalisable ssi $A^{q-1} = \mathrm{Id}$. Or on sait que le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique. Choisissons un générateur ζ : c'est donc une racine primitive $(q-1)$-ième de l'unité. Dès lors, on a la factorisation

$$X^{q-1} - 1 = (X-1)(X-\zeta)\dots(X-\zeta^{q-2})$$

On a donc $(A-\mathrm{Id})(A-\zeta\,\mathrm{Id})\dots(A-\zeta^{q-2}\,\mathrm{Id}) = 0$. Comme les polynômes $X-\zeta^i$ sont premiers entre eux, on en déduit que $E = \oplus E_i$ où $E_i = \ker(A-\zeta^i\,\mathrm{Id})$ pour $i = 0,\dots,q-2$. (On peut faire courrir i de 1 à $q-1$, ce qui ne change rien et donne une notation plus agréable.) Soit $n_i = \dim(E_i)$, on a $n_1 + \cdots + n_{q-1} = n$. Réciproquement, étant donné un $(q-1)$-uplet de sous-espaces vectoriels qui décomposent E en somme directe, l'automorphisme A est complètement déterminé puisque sa restriction à E_i est la multiplication par ζ^i. On a donc une bijection entre l'ensemble des matrices diagonalisables et l'ensemble des tels uplets, pour $(n_1,\dots,n_{q-1})$ variable.

Pour chaque $N = (n_1,\dots,n_{q-1})$ fixé, notons Z_N l'ensemble des $(q-1)$-uplets de sous-espaces vectoriels comme ci-dessus ; nous allons dénombrer Z_N. Il y a une action de $G = \mathrm{GL}_n(\mathbb{F}_q)$ sur

Z_N, qui à (E_i) associe $(g(E_i))$. Étant donnés des uplets (E_i) et (E'_i), on peut choisir des bases $(e_{i,j})$, $(e_{i,j})$ de E_i resp. E'_i (avec le même nombre d'éléments). On définit un automorphisme linéaire g qui envoie $e_{i,j}$ sur $e'_{i,j}$, de sorte que $g.(E_i)) = (E'_i)$. Il en résulte que l'action de G sur Z_N n'a qu'une orbite. Par ailleurs, le stabilisateur de (E_i) est constitué des automorphismes qui stabilisent chaque E_i, donc c'est le produit des $\mathrm{GL}_{n_i}(\mathbb{F}_q)$. Il s'ensuit que le cardinal de Z_N est égal à

$$\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)|\dots|\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}$$

Le nombre de matrices diagonalisables dans $\mathrm{GL}_n(\mathbb{F}_q)$ est la somme des cardinaux des Z_N, ce qui donne le résultat. □

Bibliographie

[FGN1] FRANCINOU, GIANELLA, NICOLAS, Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Algèbre, Tome I, *Cassini.*
[Gourdon] GOURDON, Algèbre, *Ellipses.*

DÉVELOPPEMENT 31

SOUS-GROUPES FINIS DE $SO(3)$

Proposition. — *Si G est un sous-groupe fini de $SO(3)$ alors G est isomorphe à l'un des groupes $\mathbb{Z}/n\mathbb{Z}$, D_n, A_4, S_4 ou A_5.*

Démonstration. —

1. Si g est une rotation non triviale alors il existe deux points P et $-P$, appelés *pôles* de g, sur la sphère unité qui sont stables par g. On note $\mathcal{P}$ l'ensemble des pôles des éléments de $G - \{Id\}$. Puisqu'une rotation est une isométrie, G agit sur la sphère. D'autre part, si $h \in G$ et si P est un pôle de $g \in G$ alors $hgh^{-1}h(P) = hg(P) = h(P)$ *i.e.* $h(P)$ est un pôle de hgh^{-1} donc G agit sur l'ensemble $\mathcal{P}$ des pôles. Le nombre k d'orbites de cette action vérifie

$$k = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{n}\left(|\mathcal{P}| + 2(n-1)\right)$$

d'où puisque $2 \leq |\mathcal{P}| \leq 2(n-1)$

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

i.e. $k = 2$ ou 3. Dans le cas où $k = 3$, on note $\mathcal{P}_1, \mathcal{P}_2$ et $\mathcal{P}_3$ les orbites avec $|\mathcal{P}_1| \geq |\mathcal{P}_2| \geq |\mathcal{P}_3|$. Pour $i = 1, 2, 3$, on note m_i l'ordre du stabilisateur d'un point de $\mathcal{P}_i$ (ce qui ne dépend pas du point choisi) alors $m_i\,|\mathcal{P}_i| = n$ d'où $m_1 \leq m_2 \leq m_3$. Si P est un point de $\mathcal{P}_1$ alors P est stabilisé par l'identité et par un élément g dont P est un pôle d'où $m_1 \geq 2$. On a $3n = |\mathcal{P}| + 2(n-1)$ *i.e.* $|\mathcal{P}| = n + 2$ d'où d'après l'équation aux classes

$$n + 2 = |\mathcal{P}_1| + |\mathcal{P}_2| + |\mathcal{P}_3| = \frac{n}{m_1} + \frac{n}{m_2} + \frac{n}{m_3}$$

i.e.

$$\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{n}.$$

On a donc $1 < \frac{3}{m_1}$ *i.e.* $m_1 = 2$, d'où

$$\frac{1}{m_2} + \frac{1}{m_3} = \frac{2}{n} + \frac{1}{2}.$$

On a donc $\frac{1}{2} < \frac{2}{m_2}$ *i.e.* $m_2 = 2$ ou 3. Lorsque $m_2 = 3$, on obtient

$$\frac{1}{m_3} = \frac{2}{n} + \frac{1}{6}$$

i.e. $m_3 = 3, 4$ ou 5. Ainsi, on est dans l'un des cas suivants :
- $k = 2$
- $k = 3$ et $m_2 = 2$
- $k = 3$, $m_2 = 3$ et $m_3 = 3$, alors $n = 12$, $|\mathcal{P}_1| = 6$, $|\mathcal{P}_2| = 4$ et $|\mathcal{P}_3| = 4$
- $k = 3$, $m_2 = 3$ et $m_3 = 4$, alors $n = 24$, $|\mathcal{P}_1| = 12$, $|\mathcal{P}_2| = 8$ et $|\mathcal{P}_3| = 6$
- $k = 3$, $m_2 = 3$ et $m_3 = 5$, alors $n = 60$, $|\mathcal{P}_1| = 30$, $|\mathcal{P}_2| = 20$ et $|\mathcal{P}_3| = 12$

2. On considère le cas où il y a $k = 2$ orbites. Alors $|\mathcal{P}| = 2$ et tous les éléments $g \in G$ distincts de l'identité admettent les deux points P et P' pour pôles *i.e.* ont tous le même axe de rotation donc stabilise tous le plan orthogonal à cet axe. À toute rotation g de G on associe donc canoniquement une

rotation $f(g)$ de ce plan *i.e.* on a un isomorphisme $f : G \to f(G)$. Ainsi $f(G)$ est un sous-groupe d'ordre n du groupe des rotations de $\mathbb{R}^2$ donc est un groupe cyclique d'ordre n. On a donc $G \simeq \mathbb{Z}/n\mathbb{Z}$.

3. On considère le cas où il y a $k = 3$ orbites et où $m_1 = m_2 = 2$. On a alors $|\mathcal{P}| = n + 2$ et

$$|\mathcal{P}_3| = |\mathcal{P}| - |\mathcal{P}_1| - |\mathcal{P}_2| = n + 2 - \frac{n}{2} - \frac{n}{2} = 2.$$

On note P et $-P$ les deux pôles de $\mathcal{P}_3$. Le stabilisateur G_P de P est d'ordre $\frac{n}{2}$ et (en raisonnant comme dans le premier cas) est cyclique i.e. est isomorphe à $\mathbb{Z}/\frac{n}{2}\mathbb{Z}$. Si $g \in G$ ne stabilise pas P alors on a $g.P = -P$ et $g.(-P) = P$ donc g est un demi-tour ; en particulier, tout $g \in G$ qui ne stabilise pas P est d'ordre 2. On en déduit que $G \simeq \langle a, b \mid a^n\ ,\ (ab)^2 \rangle \simeq D_{n/2}$.

4. On considère le cas où il y a $k = 3$ orbites et où $m_2 = 3, m_3 = 3$, alors $n = 12$, $|\mathcal{P}_1| = 6$, $|\mathcal{P}_2| = 4$ et $|\mathcal{P}_3| = 4$. Toute rotation g de G laisse $\mathcal{P}_2$ stable donc induit une permutation s_g de $\mathcal{P}_2$ *i.e.* on a un morphisme

$$s : G \to S_4, g \mapsto s_g.$$

Soit $g \in \ker s$ alors s_g est l'identité *i.e.* g stabilise les quatre points de S ce qui n'est possible que si g est l'identité. Il en résulte que $s(G)$ est un sous-groupe de S_4 isomorphe à G *i.e.* G est isomorphe à un sous-groupe d'ordre 12 de S_4 donc est isomorphe à A_4.

5. On considère le cas où il y a $k = 3$ orbites et où $m_2 = 3$ et $m_3 = 4$, alors $n = 24$, $|\mathcal{P}_1| = 12$, $|\mathcal{P}_2| = 8$ et $|\mathcal{P}_3| = 6$. Les pôles de $|\mathcal{P}_1|$ et $|\mathcal{P}_3|$ ne sont pas d'ordre 3 et si un pôle P est d'ordre 3 alors il en est de même de $-P$; on peut donc écrire $|\mathcal{P}_2| = \{\pm P_1, \ldots, \pm P_4\}$. Toute rotation $g \in G$ non triviale admet soit l'un des couples $\pm P_i$ pour pôles, soit n'admet pas de pôle dans $|\mathcal{P}_2|$ donc G agit par permutation sur les couples $(P_i, -P_i)$ *i.e.* on a un morphisme

$$s : G \to S_4, g \mapsto s_g.$$

Soit $g \in \ker s$ alors g stabilise chaque couple $\{-P_i, P_i\}$. Si on a $g.P_i = -P_i$ alors g n'a que deux pôles donc il existe $k \neq l$ distincts de i tels que $g.P_k = -P_k$ et $g.P_l = -P_l$. Or (O, P_i, P_k, P_l) forme un repère cartésien : en effet, si h stabilise P_1 alors il s'agit d'une rotation d'angle $\pm\frac{2\pi}{3}$ qui permute $P_1, \ldots, P_4$ donc les points P_j pour $j \neq 1$ forment un triangle équilatéral. Ainsi g change l'orientation du repère (O, P_i, P_k, P_l). Par conséquent g n'inverse pas les points de $|\mathcal{P}_2|$ *i.e.* admet chaque point de $|\mathcal{P}_2|$ pour point fixe et c'est donc l'identité. Ainsi s réalise une injection de G dans S_4 *i.e.* $s(G)$ est un groupe (isomorphe à G donc) d'ordre 24 qui est un sous-groupe de S_4 donc G est isomorphe à S_4.

6. Dans le dernier cas, la méthode est analogue (et ce cas est admis). □

Leçons concernées

01 Méthodes combinatoires, problèmes de dénombrements

02 Groupes opérant sur un ensemble. Exemples et applications

05 Groupes finis. Exemples et applications

06 Groupe des permutations d'un ensemble fini. Applications

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

08 Sous-groupes finis de $\mathcal{O}(2, \mathbb{R})$, de $\mathcal{O}(3, \mathbb{R})$. Applications

26 Endomorphismes remarquables d'un espace vectoriel euclidien de dimension finie

28 Isométrie d'un espace affine euclidien de dimension finie. Formes rduites. Applications.

Référence

F. Combes, *Algèbre et géométrie*, Bréal, 1998.

Sébastien Pellerin

Tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$

Damien Le Gléau

3 octobre 2014

Théorème. *Un groupe simple* G *d'ordre 60 est isomorphe à* $\mathcal{A}_5$.

Démonstration.
Soit G un groupe simple d'ordre 60.
Le groupe G agit transitivement sur les classes à gauche d'un sous-groupe H d'indice m par translation à gauche. L'action étant transitive, le morphisme structurel associé :

$$\begin{array}{ccccccc} \varphi & : & G & \longrightarrow & \mathfrak{S}(G/H) & & \\ & & g & \longmapsto & \sigma_g : G/H & \longrightarrow & G/H \\ & & & & \tilde{g}H & \longmapsto & g.\tilde{g}H \end{array}$$

est non trivial si $m \neq 1$.
Donc par simplicité de G on a $\ker(\varphi) = \{e\}$, et donc G s'injecte dans $\mathfrak{S}(G/H)$. Donc $|G/H| = m \geq |G| = 60$. D'où G ne peut pas avoir de sous-groupe d'indice $m \in \{2, 3, 4\}$.

_____ Que se passe t-il s'il existe un sous-groupe d'indice m=5 ? _____

Si m=5, alors $G \simeq \varphi(G) \subset \mathfrak{S}_5$.
G est simple et non abélien. En effet, si ce n'était pas le cas, d'après le théorème de Cauchy, il y aurait des sous-groupes de G d'ordre 3 qui seraient donc distingués ce qui contredit la simplicité de G.
On a donc $\varphi(G) = \varphi(\mathcal{D}(G)) \subset \mathcal{D}(\mathfrak{S}_5) = \mathcal{A}_5 \quad (*)$
Montrons cette dernière égalité en admettant le résultat suivant rappelé dans le plan :

> **Lemme**(Théorème 5.4 du livre de Félix Ulmer) :
> Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit $\sigma = \gamma_1\gamma_2 \cdots \gamma_m$ de cycles γ_i de longueur≥ 2 dont les supports $Supp(\gamma_i)$ sont deux à deux disjoints et correspondent aux orbites de l'action $\langle\sigma\rangle \hookrightarrow \mathfrak{S}_n$ du sous-groupe $\langle\sigma\rangle$ engendré par σ sur l'ensemble $\{1, 2, \cdots n\}$.
> Cette décomposition est unique à l'ordre près.

Montrons que pour $n \geq 3$, $\mathcal{A}_n = \langle (1\ i\ j), i, j \in \{1, \cdots n\}\rangle$
Tout élément $\sigma \in \mathfrak{S}_n$ est produit de cycles à supports disjoints γ_i. On décompose ensuite chaque cycle en produit de permutation : $\gamma_i = (i_1\ i_2 \cdots i_k) = (i_1\ i_m) \cdots (i_1\ i_3)(i_1\ i_2)$.

Puis $(i\ j) = (1\ i)(1\ j)(1\ i)$, donc $\mathfrak{S}_n = \langle (1\ i), i \in \{1, 2, \cdots n\}\rangle$. Soit $H \leq \mathfrak{S}_n$ le groupe engendré par les 3-cycles. Comme $(i\ j\ k) = (i\ k)(i\ j) \in \mathcal{A}_n$, on $H \subset \mathcal{A}_n$. Puis, comme les $(1\ i)$ engendrent $\mathfrak{S}_n$, tout élément de $\mathcal{A}_n$ s'écrit comme un nombre pair de $(1\ i), i \neq 1$. Puis comme $(1\ j)(1\ i) = (1\ i\ j)$ *ou* id, $\mathcal{A}_n \subset H$
Enfin, $\mathcal{A}_n = \mathcal{D}(\mathfrak{S}_n)$. En effet, l'inverse d'un produit de transpositions correspond au produit écrit à l'envers. D'où tout commutateur est produit d'un nombre pair de transpositions.
Pour $n \geq 3$, les 3-cycles $(1\ i\ j)$ engendrent $\mathcal{A}_n$.
Comme $(1\ i)(1\ j)(1\ i)^{-1}(1\ j)^{-1} = (1\ i\ j)$, les commutateurs des éléments de $\mathfrak{S}_n$ engendrent $\mathcal{A}_n$.
Par $(*)$, on a donc par cardinalité, $G \simeq \varphi(G) = \mathcal{A}_5$

Existe t-il bien un sous-groupe d'indice 5 dans G ?

Il ne reste donc plus qu'à montrer qu'il existe un sous-groupe d'indice 5 dans G.
Supposons qu'il n'existe pas de tel groupe, alors $(G : H) \notin \{2, 3, 4, 5\}(**)$ pour tout sous-groupe H de G. Comme $|G| = 2^2 \cdot 3 \cdot 5$, trouvons une contradiction en comptant les éléments de G à partir des 2,3 et 5-sylows.

Appliquons le théorème de Sylow :

Notons n_p, le nombre de p-sylows de G. Puisque les p-sylows S sont tous conjugués, on a $n_p = (G : N_G(S))$, Ici, pour $p \in \{2, 3, 5\}$, on a $n_p > 5$ par $(**)$ et puisque si $n_p = 1$, alors le p-sylow en question est distingué dans G, ce qui contredirait le caractère simple de G.

▶ Les 2-sylows.

On a d'après le théorème de Sylow, $n_2 | 15$ et comme $n_2 > 5$, on a $n_2 = 15$
Pour compter les éléments de G d'ordre 2 ou 4, on montre que l'intersection de deux 2-sylows différents est réduite à $\{e\}$.

Soient $S_2, \tilde{S}_2$ deux 2-sylows différents. Supposons qu'il existe un élément $g \neq e$ dans l'intersection de ces deux 2-sylows. Montrons une contradiction en utilisant le centralisateur $\mathrm{Z}_G(g)$ de g dans G, le stabilisateur de g pour l'action de conjugaison de G sur lui-même.
On a $|\mathrm{Z}_G(g)| > 4$. En effet, puisque les 2-sylows $S_2, \tilde{S}_2$ sont abéliens (d'ordre 4), ils sont contenus dans $\mathrm{Z}_G(g)$. Comme ils sont différents et d'ordre 4, on a $|\mathrm{Z}_G(g)| > 4$.

Comme $S_2 \leq \mathrm{Z}_G(g)$, $|\mathrm{Z}_G(g)|$ est divisible par 4 par le théorème de Lagrange.

Donc $|\mathrm{Z}_G(g)| \geq 12$.
De plus, $\mathrm{Z}(G) = \{e\}$ puisque G est non abélien et simple.
Comme $\mathrm{Z}_G(g) = G \Leftrightarrow g \in G$, on a $\mathrm{Z}_G(g) \neq G$ puisque $g \neq e$.

On a : $\begin{cases} |\mathrm{Z}_G(g)| \geq 12 \Rightarrow |(G : \mathrm{Z}_G(g))| \leq 5 \\ \mathrm{Z}_G(g) \neq G \Rightarrow |(G : \mathrm{Z}_G(g))| \neq 1 \end{cases} \Rightarrow$ contradiction avec $(**)$ Deux 2-sylows distincts ont donc toujours une intersection réduite à $\{e\}$.

▶ Les 3-sylows

$$\begin{cases} n_3 | 20 \\ n_3 > 5 \\ n_3 \equiv 1 (mod\ 3) \end{cases} \implies n_3 = 10$$

Il y a donc 10 3-sylows. Ces 3-sylows étant d'ordre 3, il sont donc cycliques, et donc deux 3-sylows distincts ont toujours une intersection réduite à $\{e\}$.

▶ Les 5-sylows

De manière analogue, on a $n_5 = 6$, et deux 5-sylows distincts ont toujours une intersection réduite à $\{e\}$.

♦ Par ce qui précède, on a peut compter les élément de G :

$$\begin{cases} \bullet\ 45 = 15 \cdot (4-1) \text{ éléments d'ordre 2 ou 4} \\ \bullet\ 20 = 10 \cdot (3-1) \text{ éléments d'ordre 3} \\ \bullet\ 24 = 6 \cdot (5-1) \text{éléments d'ordre 5} \end{cases} \implies 45 + 20 + 24 > 60 \Rightarrow \text{Contradiction}$$

Donc, il existe toujours un sous-groupe d'indice 5, et donc d'après la première partie de la démonstration, $G \simeq \mathcal{A}_5$

□

Références.

▶ *J'ai repris (en la détaillant un peu plus) la démonstration du théorème 9.8 du livre de Félix Ulmer : Théorie des groupes, pages 90,91.*

▶ *Pour montrer $\mathcal{D}(\mathfrak{S}_5) = \mathcal{A}_5$, j'ai repris la démonstration du théorème 5.15, et l'exercice 6.10 (qui est corrigé, à la fin du livre).*