103 Exemples de parties génératrices d'un groupe. Applications.

[ROM:152] [GOU:20] [PER:24] [PER:40] [GOU:13] [CAL:167-168] [PER:48] [PER:10]

I. Générateurs et relations

Prop 1: Soient G un groupe et $A \subset G$ une partie de G. Il existe un plus petit sous-groupe H de G contenant A.

Déf 2: On dit que H est le sous-groupe engendré par A, ou que les éléments de A sont des générateurs de H. On note $H = \langle A \rangle$.

Ex 3: Le groupe dérivé $D(G)$ est le sous-groupe engendré par les commutateurs de G.

Déf 4: Considérons l'ensemble des "mots" $\mathcal{M}(\mathcal{A})$ de longueur finie sur un alphabet $\mathcal{A}$ en les éléments a_i de $\mathcal{A}$ et leurs "inverses" a_i^{-1}. Deux mots m et m' sont dits équivalents ($m \sim m'$) si l'on peut aller de l'un à l'autre en ajoutant ou en enlevant des termes de la forme $a_i a_i^{-1}$ ou $a_i^{-1} a_i$. On appelle groupe libre sur $\mathcal{A}$, et on note $F(\mathcal{A})$, le groupe dont l'ensemble sous-jacent est $\mathcal{M}(\mathcal{A})/\sim$ et dont la loi est la concaténation de leurs représentants de classes de mots.

Prop 5: Toute application $f : \mathcal{A} \to G$ peut être étendue de manière unique en un morphisme $\varphi_f : F(\mathcal{A}) \to G$.

Déf 6: Soient $\mathcal{A}$ un ensemble, G un groupe et $\varphi_f : F(\mathcal{A}) \to G$ un morphisme surjectif. Un élément de $\ker(\varphi_f)$ est appelé une relation entre les générateurs $\{f(a) \mid a \in \mathcal{A}\}$ de G. Si un sous-ensemble R de $\ker(\varphi_f)$ engendre $\ker(\varphi_f)$ alors on appelle $\mathcal{A}$ et R une présentation par générateurs et relations de G (i.e. $G \simeq F(\mathcal{A})/\langle R \rangle$), on note $G = \langle \mathcal{A} \mid R \rangle$.

II. Groupes abéliens

1) Groupes monogènes et groupes cycliques

Déf 7: Un groupe G est dit monogène s'il existe $a \in G$ tel que $G = \langle a \rangle$. Si de plus G est fini, on dit que G est cyclique.

Rq 8:
- Tout groupe monogène est abélien.
- Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.

Ex 9: $\mathbb{Z}/n\mathbb{Z}$ a un générateur x et relation : $x^n = 1$.

Prop 10: Pour $a \in G$, $\langle a \rangle$ est isomorphe à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}$.

Prop 11: Soit $n \in \mathbb{N}^*$, $n \geq 2$. Si $a \in \mathbb{Z}$, notons $\bar{a}$ son image dans $\mathbb{Z}/n\mathbb{Z}$. Les propriétés suivantes sont équivalentes :
(i) a est premier avec n
(ii) $\bar{a}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$
(iii) $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$.

TR 12: Si l'ordre de G est un nombre premier, le groupe G est cyclique, engendré par tout élément différent du neutre.

Prop 13: Soient G un groupe cyclique d'ordre n et a un générateur de G. Pour tout $k \in \mathbb{Z}$, l'ordre de $a^k \in G$ est $o(a^k) = \frac{n}{n \wedge k}$.

En particulier, a^k est un générateur ssi $n \wedge k = 1$.
Il existe $\varphi(n)$ générateurs distincts dans G.

TR 14: Soient p premier, $n \in \mathbb{N}^*$ et $q = p^n$. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique (isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$). [PER:74]

Rq 15: Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Prop 16: Soient G un groupe cyclique d'ordre n et a un générateur de G. [COM:60]
(i) Soit f un morphisme surjectif de G sur un groupe G'. Alors G' est cyclique, $a' := f(a)$ engendre G' et $|G'|$ divise n.
En particulier, tout quotient de G est cyclique.
(ii) Soit G' un groupe cyclique dont l'ordre n' divise $|G|$. Soit $a' \in G'$. Il existe un unique morphisme f de G dans G' tel que $f(a) = a'$.
Pour que f soit surjectif, il faut et il suffit que a' soit un générateur de G'.

Prop 17: Soient G un groupe cyclique d'ordre n et a un générateur de G. [COM:62]
Tout sous-groupe de G est cyclique et pour tout diviseur d de n, il existe un unique sous-groupe H_d de G d'ordre d. En posant $s = \frac{n}{d}$, H_d est caractérisé par : $H_d = \{x \in G \mid x^d = e\} = \{x \in G \mid \exists y \in G,\ y^s = x\} = \langle a^s \rangle$.

Prop 18: Le produit $G_1 \times G_2$ de deux groupes est cyclique ssi G_1 et G_2 sont cycliques d'ordres m et n premiers entre eux. Dans ce cas, (a,b) est un générateur de $G_1 \times G_2$ ssi a et b sont des générateurs de G_1 et G_2. [COM:63]

Cor 19: Le produit $G_1 \times \dots \times G_k$ de k groupes cycliques est cyclique ssi les ordres de ces groupes $n_1, \dots, n_k$ sont 2 à 2 premiers entre eux.

App 20: Soient G et G' deux groupes cycliques d'ordres n et n'. Alors il existe $d := n \wedge n'$ morphismes de G dans G'. [COM:71 et 74]

2) Groupes abéliens de type fini

TR 21: (de structure des groupes abéliens finis). Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe des entiers $q_1 \geq 2$, $q_1 | q_2 | \dots | q_k$, uniques tels que G soit isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/q_k\mathbb{Z})$. [COM:66]

Déf 22: Cette suite $q_1, \dots, q_k$ est appelée la suite des invariants de G. [COM:67]

App 23: Structures possibles pour un groupe abélien d'ordre $600 = 2^3 5^2 3$. [COM:68]

Prop 24: Un groupe abélien fini A d'ordre $n \in \mathbb{N}$ est cyclique ssi pour tout diviseur d de n, il existe au plus un sous-groupe d'ordre d dans A. [ULM:111]

Déf 25: Un groupe G est dit de type fini s'il existe une partie finie de G qui engendre G. [ULM:103]

[ULM: 104] Rq 26 : Un groupe fini est de type fini.

[ULM: 110] Th 27 : (de structure des groupes abéliens de type fini). Tout groupe abélien A de type fini est isomorphe à un groupe de la forme : $\mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \times \mathbb{Z}^r$, où $(r,k) \in \mathbb{N}^2$ et les m_i sont ≥ 2 tels que $m_i \mid m_{i+1}$ pour $i \in [\![1, k-1]\!]$. Les entiers $r, k, m_1, \dots, m_k$ sont déterminés de manière unique par le groupe A.

Déf 28 : Les entiers $r, k, m_1, \dots, m_k$ sont appelés les invariants de A.

III. Groupes symétriques et groupes diédraux

1) Groupes symétriques et alternés

[PER: 10] Déf 29 : Le groupe des bijections d'un ensemble E s'appelle le groupe symétrique de E et est noté $\mathfrak{S}(E)$. Lorsque $E = \{1, \dots, n\}$, $n \in \mathbb{N}^*$, on pose $\mathfrak{S}(E) = \mathfrak{S}_n$ et on parle du groupe symétrique standard.

[PER: 11] et [COM: 81] Rq 30 : Soit $n \geq 2$.
(i) Les transpositions engendrent $\mathfrak{S}_n$.
(ii) $\mathfrak{S}_n$ est engendré par l'ensemble des $(n-1)$ transpositions de la forme $(1, i)$, où $2 \leq i \leq n$.
(iii) Les transpositions simples $t_i := (i, i+1)$, où $1 \leq i \leq n-1$ engendrent $\mathfrak{S}_n$.
(iv) Les deux permutations $t_1 := (1,2)$ et $c := (1,2,\dots,n)$ engendrent $\mathfrak{S}_n$.

[ULM: 50] Déf 31 : On appelle n-ième groupe alterné, noté $\mathfrak{A}_n$, le noyau du morphisme signature $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$.

[ULM: 52] Rq 32 : Pour $n \geq 3$, $\mathfrak{A}_n$ est engendré par les cycles de la forme $(1, i, j)$ avec i et j distincts dans $[\![2; n]\!]$.
En particulier, $\mathfrak{A}_n$ est engendré par les 3-cycles de $\mathfrak{S}_n$.

[ULM: 73] Lm 33 : Soit $Z_G(h) = \{g \in G \mid ghg^{-1} = h\}$. Soit $\sigma \in \mathfrak{A}_n$.
Notons $\mathfrak{A}_n \cdot \sigma = \{\gamma \sigma \gamma^{-1} \mid \gamma \in \mathfrak{A}_n\}$ la classe de conjugaison de σ dans $\mathfrak{A}_n$ et $\mathfrak{S}_n \cdot \sigma = \{\gamma \sigma \gamma^{-1} \mid \gamma \in \mathfrak{S}_n\}$ la classe de conjugaison de σ dans $\mathfrak{S}_n$.
Alors : - soit $Z_{\mathfrak{S}_n}(\sigma) = Z_{\mathfrak{A}_n}(\sigma) \subseteq \mathfrak{A}_n$ et donc $|\mathfrak{A}_n \cdot \sigma| = \frac{1}{2} |\mathfrak{S}_n \cdot \sigma|$
- soit $\exists \alpha \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ tel que $\alpha\sigma = \sigma\alpha$. Alors $\mathfrak{A}_n \cdot \sigma = \mathfrak{S}_n \cdot \sigma$ et donc $|\mathfrak{A}_n \cdot \sigma| = |\mathfrak{S}_n \cdot \sigma|$.

OVLPT 1

[PER: 28] Th 34 : Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$.

[PER: 28] App 35 : $D(\mathfrak{A}_n) = \mathfrak{A}_n$ pour $n \geq 5$ et $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geq 2$.

[PER: 30] Th 36 : Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur :
$\mathrm{Aut}\, \mathfrak{S}_n = \mathrm{Int}\, \mathfrak{S}_n$.

2) Groupes diédraux

[ULM: 8] Déf 37 : Soit $n \in \mathbb{N}$ avec $n \geq 2$. Dans le plan complexe $\mathbb{C}$ identifié à $\mathbb{R}^2$, considérons le polygone régulier convexe $\mathcal{P}_n$ à n sommets formé par les affixes des racines n-ième de l'unité $\omega_k = e^{\frac{2ik\pi}{n}}$ (où $k \in [\![0, n-1]\!]$). Le groupe diédral D_n pour $n \geq 2$ est le sous-groupe des isométries du plan affine qui laissent $\mathcal{P}_n$ invariant.

[ULM: 9] Prop 38 : Pour un entier $n \geq 2$, D_n est d'ordre $2n$ et il est engendré par la symétrie axiale s et la rotation d'angle $\theta = \frac{2\pi}{n}$ définies par :
$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.
Ces générateurs satisfont aux relations $r^n = e$, $s^2 = e$ et $srs = r^{-1}$.
Et les éléments de D_n sont donnés par la liste $\{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}$.
Le sous-groupe $\langle r \rangle < D_n$ est distingué et d'ordre n.

Ex 39 : Présentation de D_n : $D_n = \langle x, y \mid x^n = 1, y^2 = 1, yxy = x^{-1} \rangle$

[ULM: 10] Prop 40 : $D(D_{2n}) = \langle x^2 \rangle$ et $D(D_{2n+1}) = \langle x \rangle$.

IV. Autour du groupe linéaire

1) $GL(E)$ et $SL(E)$

Soient $\mathbb{K}$ un corps commutatif et E un $\mathbb{K}$-ev de dim finie n.

[PER: 35] Déf 41 : Le groupe linéaire $GL(E)$ est le groupe des $\mathbb{K}$-automorphismes de E. Le noyau de l'application déterminant de $GL(E)$ dans $\mathbb{K}^*$ est appelé groupe spécial linéaire et noté $SL(E)$.

[PER: 36] Rq-déf 42 : Soient H un hyperplan de E et $u \in GL(E)$ tel que $u_H = \mathrm{Id}_H$.
Les conditions suivantes sont équivalentes :
(i) $\det u = d \neq 1$ (i.e. $u \notin SL(E)$)
(ii) u admet une valeur propre $d \neq 1$ (donc une droite propre)

pour d) et u est diagonalisable.
(iii) $\mathrm{Im}(u-\mathrm{Id}) \not\subset H$.
(iv) dans une base convenable, u a pour matrice $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}$, avec $\lambda \in \mathbb{K}^*$, $\lambda \neq 1$.
On dit alors que u est une dilatation d'hyperplan $H = \ker(u-\mathrm{Id})$, de droite $D = \mathrm{Im}(u-\mathrm{Id})$ et de rapport λ.

[PER : 97] **Prop-déf 43** : Soit H un hyperplan de E d'équation $f \in E^*$. Soit $u \in GL(E)$, $u \neq \mathrm{Id}$, tel que $u_{|H} = \mathrm{Id}_H$. Les conditions suivantes sont équivalentes :
(i) $\det u = 1$ (c.-à-d. $u \in SL(E)$)
(ii) u n'est pas diagonalisable
(iii) $D = \mathrm{Im}(u-\mathrm{Id}) \subset H$
(iv) le morphisme induit $\bar{u} : E/H \to E/H$ est l'identité de E/H.
(v) il existe $a \in H$, $a \neq 0$, tel que l'on ait : $\forall x \in E$, $u(x) = x + f(x)a$.
(vi) dans une base convenable, u a pour matrice $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$
On dit alors que u est une transvection d'hyperplan H et de droite D.

[PER : 99] **Th 44** : Les transvections engendrent $SL(E)$.

Cor 45 : Les transvections et les dilatations engendrent $GL(E)$.

[PER : 101] **App 46** : 1) On a $D(GL_n(\mathbb{K})) = SL_n(\mathbb{K})$, sauf dans le cas ($n=2$, $\mathbb{K} = \mathbb{F}_2$).
2) On a $D(SL_n(\mathbb{K})) = SL_n(\mathbb{K})$, sauf dans les cas ($n=2$, $\mathbb{K} = \mathbb{F}_2$) et ($n=2$, $\mathbb{K} = \mathbb{F}_3$).

[ENS2 : 177-178] **App 47** : 1) Le centre de $GL_n(\mathbb{K})$ est l'ensemble des matrices scalaires λI_n avec $\lambda \neq 0$. Il est isomorphe au groupe $(\mathbb{K}^*, \times)$.
2) Le centre de $SL_n(\mathbb{K})$ est l'ensemble des matrices scalaires λI_n avec $\lambda^n = 1$. Il est isomorphe au groupe des racines n-ièmes de l'unité dans le corps $\mathbb{K}$.

2 : 177-178] **App 48** : On suppose $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. $SL_n(\mathbb{K})$ est connexe par arcs.

2 ; 238-239] **App 49** : $GL_n^+(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}), \det(A) > 0\}$ et $GL_n^-(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}), \det(A) < 0\}$ sont connexes par arcs.

2) Le groupe orthogonal $O(E)$

Soit E un ev réel de dim finie n.

) ; 242] **Déf 50** : L'ensemble des isométries d'un espace euclidien E est un groupe, appelé groupe orthogonal de E et noté $O(E)$.

L'ensemble $\{f \in O(E) \mid \det f = 1\}$ est un sous-groupe distingué de $O(E)$ appelé groupe spécial orthogonal de E et noté $SO(E)$ ou $O^+(E)$. [GOU : 243]

Prop-déf 51 : Soit $u \in GL(E)$ tel que $u^2 = \mathrm{Id}$. Alors il existe deux sous-espaces $E^+(u)$ et $E^-(u)$ qui vérifient : [PER : 125]
(i) $E = E^+(u) \oplus E^-(u)$
(ii) $u_{|E^+} = \mathrm{Id}_{E^+}$ et $u_{|E^-} = -\mathrm{Id}_{E^-}$.
Dans une base $(e_1, \dots, e_n)$ telle que $e_1, \dots, e_p \in E^+(u)$ et $e_{p+1}, \dots, e_n \in E^-(u)$, u a donc pour matrice : $U = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -1 \end{pmatrix}$.
Si on a $u^2 = \mathrm{Id}$ et $u \neq \mathrm{Id}$, on dit que u est une involution (ou une symétrie).
Si $\dim E^-(u) = 1$ (resp. 2), on dit que u est une réflexion (resp. un renversement).

Prop 52 : Soit $u \in GL(E)$ avec $u^2 = \mathrm{Id}$, et soient $E^+(u)$ et $E^-(u)$ les sous-espaces associés à u. Alors u est une isométrie ssi $E^+(u)$ et $E^-(u)$ sont orthogonaux. [PER : 125]

Th 53 : Le groupe $O(E)$ est engendré par les réflexions orthogonales. [PER : 143]
Plus précisément, si $u \in O(E)$, u est produit d'au plus n réflexions.

Rq 54 : Si $u \in SO(E)$, u est produit d'un nombre pair de réflexions.

Th 55 : Pour $n \geq 3$, $SO(E)$ est engendré par les renversements.
Plus précisément, si $u \in SO(E)$, u est produit d'au plus n renversements.

Lm 56 : Soient $n \geq 3$ et τ_1, τ_2 des réflexions. Il existe des renversements σ_1, σ_2 tels que $\tau_1 \tau_2 = \sigma_1 \sigma_2$.

App 57 : 1) Pour $n \geq 2$, on a $D(O(E)) = SO(E)$. [PER : 144]
2) Pour $n \geq 3$, on a $D(SO(E)) = SO(E)$.

Rq 58 : Pour $n = 2$, $SO(E)$ est commutatif, et on a alors $D(SO(E)) = \{\mathrm{Id}\}$. [PER : 145]

App 59 : Le groupe $SO_3(\mathbb{R})$ est simple. [PER : 148]

App 60 : $SO_n(\mathbb{R})$ est connexe par arcs. [XENS 3 : 63-65]

Th 61 : Soit G le groupe des quaternions de norme 1. On a un isomorphisme : $\Phi : G/\{-1;1\} \xrightarrow{\sim} SO_3(\mathbb{R})$. DVLPT 2 [PER : 164]

[GOU] : "Les maths en tête : algèbre", Xavier Gourdon
[PER] : "Cours d'algèbre", Daniel Perrin
[COM] : "Algèbre et géométrie", François Combes
[ULM] : "Théorie des groupes", Félix Ulmer
[XENS2] : "Oraux x-ens algèbre 2", Francinou, Gianella, Nicolas
[XENS3] : "Oraux x-ens algèbre 3", Francinou, Gianella, Nicolas.

SIMPLICITÉ DE $\mathcal{A}_n$, $n \geqslant 5$

Référence : PERRIN : Cours d'algèbre p. 28, ULMER : Théorie des groupes p. 73

LEMME 1 (P. 11)

$\mathcal{A}_n$ est engendré par les 3-cycles pour $n \geqslant 3$.

Preuve du Lemme 1

Soit $\sigma \in \mathcal{A}_n$, σ s'écrit comme un produit pair de transposition (car les transpositions engendrent le groupes des permutations et que la signature de σ est 1). Montrons que cette écriture peut se ramener à un produit de 3 cycles.

- $(a\ b)(a\ b) = Id.$
- $(a\ b)(b\ c) = (a\ b\ c)$
- $(a\ b)(a\ c) = (a\ c\ b)$
- $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$

Comme chaque cas consomme deux transpositions, nous avons ce que nous voulions. ■
Au passage, nous avons montré que les cycles d'ordre 3 sont dans $\mathcal{A}_n$.

Les éléments de $\mathcal{A}_5$

$\mathcal{A}_5$ possède 60 éléments. En effet, il y a :

- Le neutre
- 15 élements d'ordre 2 : ce sont les double transpositions disjointes (car une transposition seule a pour signature -1). Il y en a $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ (il faut diviser par 2 car comme elles sont disjointes $\tau_1\tau_2 = \tau_2\tau_1$).) Ou sinon on dit $\frac{5\times4\times3\times2}{2\times2\times2}$ (nombre de choix à inversion près pour chaque transposition (2×2) à inversion près de la transposition totale (2)).
- 20 élements d'ordre 3 : ce sont les 3-cycles. Il y en a $\frac{5\times4\times3}{3}$ (car on peut changer l'ordre des coefficients dedans). Ou sinon on dit $2\binom{5}{3} = 20$ (penser que les coefficients binomiaux ne prennent pas compte de l'ordre)
- 24 élements d'ordre 5 : $4! = 24$ 5-cycles (on fixe les 4 premiers éléments et le dernier est imposé)

Simplicité de $\mathcal{A}_5$ (Ulmer)

Preuve

LEMME 2

Rappel : $Z_G(h) = \{g \in G | ghg^{-1} = h\} = G_h$ (deuxième égalité le stabilisateur pour l'action par conjugaison).
Soit $\sigma \in \mathcal{A}_n$. Notons $\mathcal{A}_n \cdot \sigma = \{\gamma\sigma\gamma^{-1} | \gamma \in \mathcal{A}_n\}$ la classe de conjugaison (=l'orbite) de σ dans $\mathcal{A}_n$. Et $\mathcal{S}_n \cdot \sigma = \{\gamma\sigma\gamma^{-1} | \gamma \in \mathcal{S}_n\}$ la classe de conjugaison de σ dans $\mathcal{S}_n$.
$\rightarrow$ Soit $Z_{\mathcal{S}_n}(\sigma) = Z_{\mathcal{A}_n}(\sigma) \subseteq \mathcal{A}_n$ et donc $|\mathcal{A}_n \cdot \sigma| = \frac{1}{2}|\mathcal{S}_n \cdot \sigma|$.
$\rightarrow$ Soit $\exists \alpha \in \mathcal{S}_n \backslash \mathcal{A}_n$ tel que $\alpha\sigma = \sigma\alpha$. Alors $\mathcal{A}_n \cdot \sigma = \mathcal{S}_n \cdot \sigma$ et donc $|\mathcal{A}_n \cdot \sigma| = |\mathcal{S}_n \cdot \sigma|$.

Preuve du Lemme 2

Indication : utiliser les morphismes signatures $\varepsilon_1 : Z_{\mathcal{S}_n} \to \{\pm 1\}$ et $\varepsilon_2 : Z_{\mathcal{A}_n} \to \{\pm 1\}$ ainsi que la relation orbite-stabilisateur.
$\to$ Si ε_1 est trivial, il envoie tout sur 1. Donc $Z_{\mathcal{S}_n}(\sigma) = Z_{\mathcal{A}_n}(\sigma)$.
Relation orbite-stabilisateur (utilisée 2 fois) :

$$|\mathcal{A}_n \cdot \sigma| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{1}{2}\frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = \frac{1}{2}|\mathcal{S}_n \cdot \sigma|$$

$\to$ Si ε_1 n'est pas trivial, $\exists \alpha \in Z_{\mathcal{S}_n}(\sigma)$ tel que $\text{sign}(\alpha) = -1$. Et $\text{Id} \in Z_{\mathcal{S}_n}$ est telle que $\text{sign}(\text{Id}) = 1$. Donc $\text{Im}(\varepsilon_1) = \{\pm 1\}$. Le théorème d'isomorphisme donne

$$\frac{|Z_{\mathcal{S}_n}(\sigma)|}{|\text{Ker}(\varepsilon_1)|} = 2$$

Mais $\text{Ker}(\varepsilon_1) = Z_{\mathcal{A}_n}(\sigma)$ donne $2\,|Z_{\mathcal{A}_n}(\sigma)| = |Z_{\mathcal{S}_n}(\sigma)|$. Donc (relation orbite-stabilisateur) :

$$|\mathcal{A}_n \cdot \sigma| = \frac{|\mathcal{A}_n|}{|Z_{\mathcal{A}_n}(\sigma)|} = \frac{2\,|\mathcal{A}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = \frac{|\mathcal{S}_n|}{|Z_{\mathcal{S}_n}(\sigma)|} = |\mathcal{S}_n \cdot \sigma| \qquad \blacksquare$$

Pour $\sigma \in \mathcal{A}_5$, la classe de conjugaison de σ dans $\mathcal{A}_5$ est soit identique (de même taille) que la classe de conjugaison de σ dans $\mathcal{S}_5$, soit de taille moitié.
De plus, la classe de conjugaison dans $\mathcal{S}_5$ d'un cycle de n'importe quelle taille est l'ensemble des cycles de cette taille (par $\tau(a\ b\ c...)\tau^{-1} = (\tau(a)\ \tau(b)\ \tau(c)...)$).
On réunit les informations :

Type d'éléments de $\mathcal{A}_5$	Cardinal	# de la classe dans $\mathcal{S}_5$	# de la classe dans $\mathcal{A}_5$
Neutre	1	1	Impair donc 1
Double-transposition	15	15	Impair donc 15
3-cycle	20	20	Si $\gamma = (a\ b\ c)$. Avec $(d\ e) \in \mathcal{S}_5 \backslash \mathcal{A}_5$, on a $(d\ e)(a\ b\ c)(d\ e) = (a\ b\ c)$ donc $(d\ e)$ stabilise γ. D'après le **Lemme 2**, $\lvert\mathcal{A}_5 \cdot \gamma\rvert = \lvert\mathcal{S}_5 \cdot \gamma\rvert = 20$
5-cycle	24	24	D'après la formule des classes $\lvert\mathcal{A}_5 \cdot \tau\rvert\,\lvert Z_{\mathcal{A}_5}(\tau)\rvert = \lvert\mathcal{A}_5\rvert = 60$. Or $24 \nmid 60$ donc nécessairement le cardinal est de moitié : 12

Donc les tailles des classes de conjugaison dans $\mathcal{A}_5$ sont 1,12,15 ou 20. Or, un sous-groupe distingué contient l'identité et une union de classe de conjugaison (car s'il a un élément, il a sa classe de conjugaison par définition de distingué). Le cardinal d'un sous-groupe distingué de $\mathcal{A}_5$ divise 60 donc appartient à 1,2,3,4,5,6,10,12,15,20,60.
Un sous-groupe distingué de $\mathcal{A}_5$ est forcément le neutre ou $\mathcal{A}_5$.

$n \geqslant 5$ quelconque (Perrin)

Preuve

Posons $E = [\![1, n]\!]$. Soit $H \lhd \mathcal{A}_n \setminus \{Id\}$. Soit $\sigma \in H \setminus \{Id\}$.

Etape 1 Construire un ensemble à 5 éléments, pour cela fabriquer à partir de σ un élément non trivial de H qui n'agisse que sur un ensemble à 5 éléments.
Comme $\sigma \neq Id$, il existe $a \in E$ tel que $b = \sigma(a) \neq a$.
Soit également $c \notin \{a, b, \sigma(b)\}$ et τ le 3-cycle $(a\ c\ b) \in \mathcal{A}_n$. Ainsi, $\tau^{-1} = (a\ b\ c)$. On pose $\rho = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$ comme commutateur $\times$ un élément de H.
On a $\rho = \tau(\sigma\tau^{-1}\sigma^{-1}) = (a\ c\ b)(\sigma(a\ b\ c)\sigma^{-1}) = (a\ c\ b)\,(\sigma(a)\ \sigma(b)\ \sigma(c))$
Comme $b = \sigma(a)$, l'ensemble $F := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\} = \text{Supp}(\rho)$ a au plus 5 éléments et $\rho|_{E\setminus F} =$

$Id_{E\setminus F}$.

Quitte a rajouter des éléments dans F, on peut supposer que $|F| = 5$.

Etape 2 Trouver un sous-groupe distingué dans cet ensemble.

Soit maintenant $\mathcal{A}(F)$ l'ensemble des permutations paires d'éléments de F. On a $\mathcal{A}(F) \cong \mathcal{A}_5$.
Considérons le morphisme i d'injection de $\mathcal{A}(F)$ dans $\mathcal{A}_n$

$$i : \begin{array}{ccc} \mathcal{A}(F) & \to & \mathcal{A}_n \\ u & \mapsto & \bar{u} \end{array}$$

avec $\bar{u}|_F = u$ et $\bar{u}|_{E\setminus F} = Id_{E\setminus F}$ (on a prolongé u par l'identité).

Posons $H_0 = \{u \in \mathcal{A}(F) \mid \bar{u} \in H\}$.
$H_0 \lhd \mathcal{A}(F)$ (car $H \lhd \mathcal{A}_n$, s'écrit bien).

Etape 3 Conclure

De plus, H_0 non réduit à $\{Id\}$ car $\rho|_F \in H_0$. En effet $\rho \in H$ et $\rho \neq Id$ car $\rho(b) = (\tau\sigma\tau^{-1})\sigma^{-1}(b) = (\tau\sigma\tau^{-1})(a) = \tau\sigma(b) \neq \tau(c) = b$ car $c \neq \sigma(b)$.
Comme $\mathcal{A}(F) \cong \mathcal{A}_5$ et $\mathcal{A}_5$ simple, on a $H_0 = \mathcal{A}(F)$.
Donc H_0 contient en particulier un 3-cycle, donc $\bar{u}$ est également un 3-cycle et appartient à H. H contient donc tous les 3-cycles puisque ceux-ci sont conjugués dans $\mathcal{A}_n$.
Or $\mathcal{A}_n$ est engendré par les 3-cycles, et finalement $H = \mathcal{A}_n$. ■

Bonus

PROPOSITION

$\mathcal{A}_n$ est $(n-2)$-transitif sur $[\![1, n]\!]$ ie si on a $a_1, \ldots, a_{n-2}$ distincts et $b_1, \ldots, b_{n-2}$ distincts, il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$.

Preuve

On écrit $[\![1, n]\!] = \{a_1, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \ldots, b_{n-2}, b_{n-1}, b_n\}$.
On considère $\tau \in \mathcal{S}_n$ telle que $\tau(a_i) = b_i$. Si τ est paire, c'est terminé. Sinon, on compose τ avec la transposition $(a_{n-1}\ a_n)$, cela nous donne σ. ■

Notes :

✓ **A l'oral**, $n = 5$: 7'40 puis 8'34. Quand on dénombre $\mathcal{A}_5$ on commence déjà le tableau. Tout : 14'16 au feutre en speedant. Développement à retravailler car dur ! En speedant 6'05 pour $\mathcal{A}_5$ et 12'40 au total. Donc on peut aller un peu plus doucement.
✓ La signature c'est $(-1)^{\text{nombre de transpositions}}$ lorsqu'on a décomposé en produit de transpositions (non forcément disjointes).

Théorème: Soit G le groupe des quaternions de norme 1. On a un isomorphisme $\overline{s} : G/\{\pm 1\} \xrightarrow{\sim} SO_3(\mathbb{R})$

Dem: $\mathbb{H}$ est non commutatif, donc l'action de $\mathbb{H}^*$ sur $\mathbb{H}$ par automorphismes intérieurs est non triviale. On peut se restreindre à l'action de G car si $q \in \mathbb{H}^*$, il s'écrit $q = \lambda r$ avec $\lambda = \sqrt{N(q)} \in \mathbb{R}$ et $r \in G$ (où $N(q) = q\bar{q} = \bar{q}q$ et comme λ est central, il ne donne rien dans les automorphismes intérieurs.

On pose donc pour $q \in G$ et $q' \in \mathbb{H}$:

$$s_q(q') = qq'q^{-1} = qq'\bar{q}$$

Nous allons étudier cette action et montrer qu'elle donne une paramétrisation du groupe $SO_3(\mathbb{R})$ par le groupe G.

1) L'application $s_q : \mathbb{H} \to \mathbb{H}$ est $\mathbb{R}$-linéaire et bijective car on a $s_{\bar{q}} = (s_q)^{-1}$. On obtient donc une application

$$s : G \to GL_4(\mathbb{R}) \quad \text{(en identifiant } \mathbb{H} \text{ à } \mathbb{R}^4\text{)}$$

2) L'application s est un homomorphisme car on a $s_{q_1 q_2}(q') = q_1 q_2 q' \bar{q}_2 \bar{q}_1 = s_{q_1} s_{q_2}(q')$. On calcule son noyau:

$s_q = Id \Rightarrow \forall q' \in \mathbb{H} \quad qq'\bar{q} = q'$ donc $qq' = q'q$ et q est central

Donc le noyau de s est $Z(\mathbb{H}) \cap G = \mathbb{R} \cap G = \{\pm 1\}$.

3) Comme 1 est central dans $\mathbb{H}$ on a pour $a \in \mathbb{R}$

$s_q(a) = a$ donc $s_{q|\mathbb{R}} = Id_{\mathbb{R}}$

4) Par ailleurs s_q conserve la norme ie vérifie $N(s_q(q')) = Nq'$.

En effet on a $N(qq'\bar{q}) = N(q)N(q')N(\bar{q}) = N(q')$ puisque $q \in G$ est de norme 1. Donc s_q est un élément du groupe orthogonal euclidien défini par N: $s_q \in O(N) \simeq O_4(\mathbb{R})$

5) La norme $N(q) = q\bar{q} = \bar{q}q$ est une forme quadratique réelle définie positive sur $\mathbb{H}$, la base $(1, i, j, k)$ est orthonormée et la forme bilinéaire symétrique associée est donnée par

$$\langle q, q' \rangle = \frac{1}{2}(q\bar{q}' + q'\bar{q}) \quad \text{pour } q, q' \in \mathbb{H}$$

Par N, l'espace des quaternions purs P est l'orthogonal de $\mathbb{R}$. En effet on a bien $\langle p, r \rangle = 0$ $\forall p \in P$ et $r \in \mathbb{R}$ et réciproquement si $\langle q, r \rangle = 0$ pour $q \in \mathbb{H}$ et $\forall r \in \mathbb{R}$ alors $\bar{q} + q = 0$ car 1 est central donc $N(q) = q\bar{q} = -q^2$ et $q^2 \in \mathbb{R}^-$ entraîne $q \in P$ par caractérisation des quaternions purs.

Comme on a $s_{q|\mathbb{R}} = Id_{\mathbb{R}}$, $\mathbb{R}$ est en particulier stable (et même fixe) par s_q et donc $\mathbb{R}^\perp = P$ est stable par s_q. On pose alors $s_q = s_{q|P}$, on a $s_q \in O(N_{|P}) \simeq O_3(\mathbb{R})$ et $s : G \longrightarrow O_3(\mathbb{R})$ est un homomorphisme de noyau
$q \longmapsto s_q$ $\qquad Z(P) \cap G = \mathbb{R} \cap G = \{\pm 1\}$

5) Munissons $O_3(\mathbb{R})$ de sa topologie naturelle obtenue en le considérant comme sous-espace de $M_3(\mathbb{R})$ lui-même identifié à $\mathbb{R}^9$. L'application s est alors continue comme on le voit en calculant la matrice de s_q dans la base i, j, k. En effet si $q = a + bi + cj + dk$, les coefficients de la matrice sont des polynômes homogènes de degré 2 en a, b, c, d. Par exemple

$$\begin{aligned} s_q(i) = q i \bar{q} &= (a + bi + cj + dk)\, i\, (a - bi - cj - dk) \\ &= (a + bi + cj + dk)(ai + b - ck + dj) \\ &= \underline{a^2 i} + ab - ack + adj \\ &\quad - ba + \underline{b^2 i} + bcj + bdk \\ &\quad - cak + cbj - \underline{c^2 i} - cdk \\ &\quad + daj + dbk + dc - \underline{d^2 i} \end{aligned}$$

d'où $s_{11} = a^2 + b^2 - c^2 - d^2$

$s_{21} = 2(ad + bc)$

$s_{31} = 2(bd - ac)$

Mais det : $O_3(\mathbb{R})$ [illegible] est également continue. Donc det o s : $G \to \{\pm 1\}$ est continue. Or si l'on identifie $\mathbb{H}$ à $\mathbb{R}^4$ muni de sa topologie naturelle on voit que G est homéomorphe à S^3 et en particulier connexe.

Donc l'image de det o s est connexe et comme $s(1) = Id$ c'est nécessairement 1. Autrement dit $s(G) \subset SO_3(\mathbb{R})$

7) Montrons enfin l'égalité $s(G) = SO_3(\mathbb{R})$

Soit $p \in PVG$. On calcule $s_p(p) = ppp^{-1} = p$ donc s_p fixe p et s_p est une rotation d'axe p.

D'autre part comme p est dans PVG on a $\bar{p} = -p$ donc $p^2 = -p\bar{p} = -1$ et $(s_p)^2 = s_{p^2} = s_{-1} = Id$ donc s_p est une involution, et c'est donc le renversement d'axe $\langle p \rangle$. On obtient ainsi tous les renversements de $SO_3(\mathbb{R})$, et comme ils engendrent le groupe, on a bien $s(G) = SO_3(\mathbb{R})$, d'où l'isomorphisme

$$G/\{\pm 1\} \simeq SO_3(\mathbb{R})$$