GROUPES SYMÉTRIQUES

REPÈRES

Historique :

- Rencontré dans bien des situations mathématiques dès qu'il est besoin de permuter les éléments d'un ensemble fini, l'ensemble S_n a vu sa structure étudiée et nommée (le terme "groupe" fut choisi à cette occasion) par Galois, en 1832, dans son étude de la résolution des équations algébriques.
- La grande diversité de structures de ses sous-groupes le place au cœur de l'étude des groupes. Il permet notamment d'apporter un éclairage nouveau sur les isométries conservant les polyèdres réguliers (solides de Platon). Et son sous-groupe A_n participe à la classification des groupes simples non commutatifs à la fin du XX^{ème} siècle.

I. GÉNÉRALITÉS

① STRUCTURE

1.1. Le **groupe symétrique** d'un ensemble X est $(S(X), \circ)$, où $S(X)$ est l'ensemble des bijections de $X \to X$ (dites **permutations** de X).
À isomorphisme près, $S(X)$ ne dépend que de $Card(X)$.
Le **groupe symétrique d'ordre** n est $(S_n, \circ)$, où S_n est l'ensemble des permutations de $\{1, 2, ..., n\}$.

☝ Par exemple, le groupe linéaire $GL(E)$, des automorphismes de l'espace vectoriel E, est un sous-groupe de $S(E)$.

🕮 Dans les anciens manuels, S_n est souvent noté $\mathfrak{S}_n$.

☝ Dans S_n, le neutre est l'identité de $\{1, 2, ..., n\}$, qu'on notera Id pour tout n.

✋ Le composé $\sigma\circ\sigma'$ sera noté en général par le produit $\sigma\sigma'$ (on prendra garde au fait que c'est bien σ' qui agit en premier).

1.2. $|S_n| = n\ !$

② ÉLÉMENTS

2.1. Un élément quelconque σ de S_n sera noté $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.
Le **support** de σ est l'ensemble $\{i \in \{1, ..., n\} ; \sigma(i) \neq i\}$. On le note $supp(\sigma)$.

2.2.1. Pour $p \geq 2$, $(i_1\ i_2\ ...\ i_p)$ désigne la **permutation circulaire** (ou **cycle**) de longueur p (ou p-**cycle**), élément σ de S_n tel que :

$$\begin{cases} \sigma(i_1) = i_2 \\ \sigma(i_2) = i_3 \\ \ldots \\ \sigma(i_p) = i_1 \\ \sigma(j) = j \text{ si } j \notin \{i_1, ..., i_p\} \end{cases}.$$

2. Un 2-cycle est une **transposition**.

☝ On dira souvent qu'un nombre appartient à un cycle, au lieu de dire qu'il appartient à son support.
De même, on parlera de cycles disjoints au lieu de cycles à supports disjoints.

☝ Un p-cycle est d'ordre p.

✋ Souvent utile : si $\gamma = (i_1\ i_2\ ...\ i_p)$, alors γ^{-1} est le p-cycle $(i_p\ i_{p-1}\ ...\ i_2\ i_1)$.

✋ γ^{p-1} est un cycle, mais, pour $2 \leq r \leq p-2$, γ^r n'est pas nécessairement un cycle.

③ COMMUTATIONS

3.1.1. S_n est non commutatif pour $n \geq 3$.

2. σ et σ' à supports disjoints $\Rightarrow$ σ et σ' commutent.

☝ S_3, d'ordre 6, est le groupe non commutatif de plus petit ordre (à isomorphisme prés).

3.2. Pour $n \geq 3$, on a : $Z(S_n) = \{Id\}$.

☝ Pour compléter l'étude de la conjugaison (voir **II** ④) , il est classique de chercher à préciser les automorphismes intérieurs d'un groupe.

3.2. permet de montrer que, pour $n \geq 3$, on a : $Int(S_n) \approx S_n$.

✍ Poser $\varphi : S_n \to Int(S_n)$; $\delta \mapsto$ l'automorphisme intérieur $i_\delta : S_n \to S_n$; $\sigma \mapsto \delta\sigma\delta^{-1}$.

Faux pour $n = 2$: $Int(S_2) = \{Id\}$.

Voir aussi les **VI** ③ et ④.

II. GÉNÉRATIONS DE S_n

① σ-ORBITES

Nous verrons dans le chapitre 4 que $(\sigma, i) \mapsto \sigma(i)$ constitue une opération naturelle de S_n sur $\{1, ..., n\}$, pour laquelle l'orbite de tout i est évidemment $\{1, ..., n\}$.

Mais, on peut également faire opérer sur $\{1, ..., n\}$ n'importe quel sous-groupe de S_n, en particulier les $< \sigma >$:

1.1. Quand on fait opérer $< \sigma >$ sur $\{1, ..., n\}$, l'orbite de i est appelée **σ-orbite** (ou **σ-trajectoire**) de i. On la note $\omega_\sigma(i)$.
$\omega_\sigma(i) = \{\sigma^k(i) \ ; \ k \in \mathbb{Z}\}$.
Si $i \notin supp(\sigma)$, alors : $\omega_\sigma(i) = \{i\}$. On dit que c'est une **orbite ponctuelle**.

☝ Dans la pratique, $\omega_\sigma(i)$ est l'ensemble des j de $\{1, ..., n\}$ qu'on rencontre en partant de i et en faisant agir σ jusqu'à retrouver i.

✍ Par exemple, dans S_6, si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}$, on a :

$\omega_\sigma(1) = \omega_\sigma(3) = \omega_\sigma(6) = \{1, 3, 6\}$
$\omega_\sigma(2) = \omega_\sigma(5) = \{2, 5\}$
$\omega_\sigma(4) = \{4\}$: orbite ponctuelle.

☝ Un p-cycle possède 1 orbite non ponctuelle (son support) et $(n - p)$ orbites ponctuelles.
C'est de plus une propriété caractéristique.

☝ La restriction de σ à une de ses orbites non ponctuelles est un cycle.

☝ Les σ-orbites forment une partition de $\{1, ..., n\}$.

② DÉCOMPOSITION EN CYCLES DISJOINTS

Les deux remarques précédentes entraînent :

2.1. Toute permutation $\neq Id$ se décompose en produit de cycles disjoints (décomposition unique, à l'ordre près).

✍ Par exemple, dans S_6 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix} = (163)(25)$.

2.2. Toute permutation se décomposant en cycles disjoints de longueurs $p_1, ..., p_k$ est dite **de type** $\{p_1, ..., p_k\}$.

③ SYSTÈMES GÉNÉRATEURS MINIMAUX DE S_n

3.1. Tout cycle se décompose en produit de transpositions.

☝ Par exemple : $(i_1 \ i_2 \ ... \ i_p) = (i_1 \ i_2)(i_2 \ i_3)...(i_{p-1} \ i_p)$.

✋ Mais, à part dans S_2 bien sûr, la décomposition n'est pas unique (par exemple : $(i\ j) = (i\ k)(j\ k)(i\ k)$).

3.2. Les systèmes suivants sont générateurs de S_n :
- les cycles.
- les $\frac{n(n-1)}{2}$ transpositions.
- les $n - 1$ transpositions de la forme $(1 \ i)$.
  C'est un système minimal.
- les $n - 1$ transpositions de la forme $(i \ i{+}1)$.
  C'est un système minimal.
- la transposition (12) et le cycle $(12...n)$.
  C'est un système minimal.
  S_n est dit **dicyclique**.

✍ Pour le dernier système, on calculera $(12...n)^k(12)(12...n)^{-k}$.

④ CARACTÉRISATION DES CLASSES DE CONJUGAISON

Rappelons que deux permutations σ et σ' sont dites **conjuguées** si : $\exists\, \delta \in S_n$; $\sigma' = \delta\sigma\delta^{-1}$, et que la **conjugaison** est une relation d'équivalence : les classes de conjugaison forment une partition de S_n. Nous allons préciser cette partition :

4.1. Soit δ une permutation et $\gamma = (i_1 \ i_2 \ ... \ i_p)$ un p-cycle.
Alors : $\delta\gamma\delta^{-1}$ est le p-cycle $(\delta(i_1) \ ... \ \delta(i_p))$.

☝ Par conséquent, la conjugaison conserve la longueur d'un cycle :
le conjugué d'un p-cycle est un p-cycle.

4.2. Deux permutations sont conjuguées ⇔ elles sont de même type.

✍ On pourra utiliser $\delta = \begin{pmatrix} a_1 & ... & a_r & b_1 & ... & b_s & ... \\ a'_1 & ... & a'_r & b'_1 & ... & b'_s & ... \end{pmatrix}$ où $(a_1...a_r)(b_1...b_s)...$ et $(a'_1...a'_r)(b'_1...b'_s)...$ sont deux permutations de même type.

☝ En particulier, la classe de conjugaison d'un p-cycle est exactement l'ensemble des p-cycles.

III. PARITÉ ET GROUPE ALTERNÉ A_n

① CONSTRUCTION

• *a)* POSITION DU PROBLÈME :

Si on replace l'étude de S_n dans le contexte historique de la résolution des équations algébriques, le besoin s'est fait de trouver le plus grand sous-groupe distingué propre de S_n (voir Sujets d'étude).

Il est naturel de commencer par chercher un sous-groupe H d'indice 2 (alors nécessairement distingué) : nous allons montrer qu'il en existe un et qu'il est unique.

• *b)* MISE EN PLACE DE LA CONSTRUCTION :

⋆ *i)* Établir l'existence et l'unicité de H équivaut à le faire pour un morphisme φ surjectif de S_n à valeurs dans un groupe d'ordre 2, dont H sera le noyau.

Choisissons par tradition ($\{1, -1\}$, .), plutôt que ($\mathbb{Z}/2\mathbb{Z}$, +), comme groupe d'ordre 2.

Alors : $H = \{\sigma \in S_n ; \varphi(\sigma) = 1\}$.

⋆ *ii)* Commençons par étudier l'image des transpositions, génératrices de S_n par cet éventuel φ.

Supposons : $\exists\ \tau$ transposition ; $\varphi(\tau) = 1$.

Alors : $\tau \in H$.

Mais : $H \lhd S_n \Rightarrow H$ invariant par conjugaison

$\Rightarrow H$ contient la classe de conjugaison de τ,

qui n'est autre, d'après **II** *4.2.*, que l'ensemble de toutes les transpositions

$\Rightarrow H = S_n$ (puisque les transpositions engendrent S_n) : impossible car H doit être d'indice 2 !

Par conséquent, si φ existe : $\forall\ \tau$ transposition ; $\varphi(\tau) = -1$.

⋆ *iii)* Il reste à définir un prolongement à S_n tout entier.

• *c)* 1ÈRE MÉTHODE :

φ devant être un morphisme, on déduit, s'il existe, que pour tout σ de S_n se décomposant en produit de transpositions $\tau_1 ... \tau_t$: $\varphi(\sigma) = \varphi(\tau_1 ... \tau_t) = \varphi(\tau_1) ... \varphi(\tau_t) = (-1)^t$.

Mais, la décomposition en produit de transpositions n'étant pas unique, il ne faut pas que $(-1)^t$ en dépende si l'on veut que φ soit défini par ce moyen !

Il suffit pour cela de montrer que (voir **VII** Annexe) :

1.1. Dans la décomposition d'une permutation, le nombre de transpositions a toujours même parité.

• *d)* 2ÈME MÉTHODE :

On va contourner le problème en trouvant un autre morphisme ψ (un peu artificiel ?) de S_n tout entier dans $\{1, -1\}$, coïncidant avec φ sur l'ensemble des transpositions.

⋆ *i)* Soit une transposition $\tau = (u\ v)$.

Si on a : $u < v$, alors : $\tau(u) > \tau(v)$, autrement dit, τ « inverse » l'ordre de u et v.

Les autres couples pour lesquels c'est le cas sont les $(u\ i)$ et les $(i\ v)$ avec $u < i < v$.

En comptant $(u\ v)$, cela fait en tout $2(v - u - 1) + 1$ **inversions**, nombre toujours impair.

Pour tout couple (i, j), $\dfrac{\tau(i) - \tau(j)}{i - j}$ vaut -1 ou 1 suivant que i et j sont inversés ou non.

Donc l'imparité du nombre d'inversions se traduit par $\prod_{i<j} \dfrac{\tau(i) - \tau(j)}{i - j} = -1$, qui est justement l'image de τ par φ (!).

⋆ *ii)* Prolongeons à une permutation quelconque σ, en posant : $\psi(\sigma) = \prod_{i<j} \dfrac{\sigma(i) - \sigma(j)}{i - j}$.

$$\psi(\sigma\sigma') = \prod_{i<j} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{i - j} = \prod_{i<j} \frac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} \prod_{i<j} \frac{\sigma'(i) - \sigma'(j)}{i - j}.$$

Le deuxième facteur $\prod_{i<j} \dfrac{\sigma'(i) - \sigma'(j)}{i - j}$ est bien $\psi(\sigma')$.

Et le premier facteur s'écrit : $\prod_{\sigma'(i)<\sigma'(j) \text{ et } i<j} \dfrac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} \prod_{\sigma'(i)>\sigma'(j) \text{ et } i<j} \dfrac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)}$

$= \prod_{\sigma'(i)<\sigma'(j) \text{ et } i<j} \dfrac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} \prod_{\sigma'(i)<\sigma'(j) \text{ et } j<i} \dfrac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)}$, par échange des variables i et j

$= \prod_{\sigma'(i)<\sigma'(j)} \dfrac{\sigma\sigma'(i) - \sigma\sigma'(j)}{\sigma'(i) - \sigma'(j)} = \prod_{i<j} \dfrac{\sigma(i) - \sigma(j)}{i - j}$, car, comme σ' est une bijection, les variables i et j peuvent remplacer $\sigma'(i)$ et $\sigma'(j)$.

Donc ψ est un morphisme.

⋆ *iii)* L'existence d'un morphisme surjectif de S_n dans $\{1, -1\}$ est assurée.

Remarquons qu'il est unique, puisque défini de manière unique sur les transpositions, qui engendrent S_n.

Il sera désormais noté ε et appelé **signature**.

On en déduit l'existence et l'unicité d'un sous-groupe d'indice 2 de S_n, qu'on note A_n, appelé **groupe alterné d'ordre** n.

② GROUPE ALTERNÉ

2.1.1. La **signature** de σ, notée $\varepsilon(\sigma)$, est définie de manières équivalentes au moyen :

- *i)* des inversions : $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{I(\sigma)}$, où $I(\sigma)$ est le nombre d'inversions de σ.
- *ii)* des transpositions : $\varepsilon(\sigma) = (-1)^t$, si σ se décompose en t transpositions.

2. σ est dite **paire** si : $\varepsilon(\sigma) = 1$, **impaire** si : $\varepsilon(\sigma) = -1$.

☝ $\varepsilon(Id) = 1$.

La signature d'un p-cycle est $(-1)^{p-1}$.

🕮 On trouve une application de la signature dans la définition du déterminant : l'ensemble des formes n-linéaires alternées de $\mathcal{M}_n(K)$ dans K est un espace vectoriel de dimension 1, engendré par :

$$\varphi_0 : [a_{ij}] \mapsto \sum_{\sigma \in S_n} \varepsilon(\sigma).a_{\sigma(1)1}...a_{\sigma(n)n}$$, appelé le **déterminant**.

Peu utilisable pour les calculs, cette définition peut servir néanmoins à démontrer que : $\det(A) = \det({}^tA)$.

2.2.1. σ étant décomposée en produit de cycles disjoints :

$\varepsilon(\sigma) = (-1)^c$, où c = nombre de cycles + somme des longueurs des cycles.

2. $\varepsilon(\sigma) = (-1)^{n-\Omega(\sigma)}$, où $\Omega(\sigma)$ est le nombre de σ-orbites.

2.3. L'ensemble des permutations paires de S_n forme un groupe, appelé **groupe alterné d'ordre** n, et noté A_n.
C'est l'unique sous-groupe d'indice 2 de S_n et donc son plus grand sous-groupe distingué propre.

🕮 Dans les anciens manuels, A_n est souvent noté $\mathfrak{A}_n$.

③ SYSTÈMES GÉNÉRATEURS DE A_n POUR $n \geq 3$

3.1. Pour $n \geq 3$, le produit de deux transpositions est un 3-cycle ou le produit de deux 3-cycles.

3.2. Pour $n \geq 3$, A_n est engendré par :

- les $\frac{n(n-1)(n-2)}{3}$ trois-cycles,
- les $(n-1)(n-2)$ trois-cycles de la forme $(1\ i\ j)$,
- les $(n-2)$ trois-cycles de la forme $(1\ 2\ i)$.

☝ $A_2 = \{Id\}$ et A_3 est cyclique.

IV. REPRÉSENTATION DES GROUPES FINIS

① THÉORÈME DE CAYLEY

1.1. Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

☝ **Représenter** (ou **réaliser**) un groupe fini consistera à déterminer le sous-groupe de permutations isomorphe.

☝ Tout groupe cyclique d'ordre n est isomorphe à $<\gamma>$, où γ est un n-cycle quelconque.

On notera dans la suite $Is(\mathcal{P})$ le groupe d'isométries conservant la partie $\mathcal{P}$ d'un espace affine. On l'appellera le **groupe de** $\mathcal{P}$.

On notera $Is^+(\mathcal{P})$ le groupe des déplacements (composition d'une rotation et d'une translation) conservant la partie $\mathcal{P}$.

☝ Si le plan $\mathbb{R}^2$ s'identifie au sous-espace $\{(x, y) \in \mathbb{R}^2\}$ de $\mathbb{R}^3 = \{(x, y, z) \in \mathbb{R}^3\}$, alors :

- les rotations planes de centre A et d'angle α s'identifient aux rotations de l'espace d'axe (Az) et d'angle α
- les symétries planes d'axe (Δ) s'identifient aux retournements (rotations d'angle π) d'axe (Δ).

Par conséquent, tout sous-groupe de $Is(2)$ s'identifie à un sous-groupe de $Is^+(3)$.

② REPRÉSENTATION DES GROUPES DIÉDRAUX

On se place dans le plan affine.

● *a)* DÉFINITION :

2.1.1. Les groupes de deux n-gones réguliers $\mathcal{P}_n$ et $\mathcal{P}'_n$ sont isomorphes : $Is(\mathcal{P}_n) \approx Is(\mathcal{P}'_n)$.

2. Ils seront identifiés, appelés **groupe diédral d'ordre** n et notés D_n.

3. $Is^+(\mathcal{P}_n)$ n'est constitué que de rotations. On le note R_n.

● *b)* GROUPE DIÉDRAL D'ORDRE 3 :

Soit un triangle équilatéral ABC.

D_3 est composé de :
- 3 rotations de centre celui de ABC et d'angles 0, $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$: elles s'identifient respectivement à Id et aux 3-cycles (A, B, C) et (A, C, B).
- 3 symétries d'axes les hauteurs : elles s'identifient aux transpositions (A, B), (A, C), (B, C).

2.2.1. $D_3 \approx S_3$.

2. $R_3 \approx A_3$.

● *c)* GROUPE DIÉDRAL D'ORDRE 4 :

Soit un carré *ABCD*.

D_4 est composé de :
- 4 rotations de centre celui de *ABCD* et d'angles 0, $\frac{\pi}{2}$, π et $\frac{3\pi}{2}$: elles s'identifient respectivement à *Id*, au 4-cycle (*A*, *B*, *C*, *D*), au produit (*A*, *C*)(*B*, *D*) et au 4-cycle (*A*, *D*, *C*, *B*).
- 4 symétries d'axes (*AC*), (*BD*), la médiatrice de [*AB*], la médiatrice de [*BC*] : elles s'identifient aux transpositions (*B*, *D*) et (*A*, *C*), et aux produits (*A*, *B*)(*C*, *D*) et (*B*, *C*)(*A*, *D*).

On constate que l'élégant parallélisme entre les D_n, R_n et les S_n, A_n s'arrête à 3 :
- le groupe D_4 est d'ordre 8 et S_4 est d'ordre 24
- si R_4 représente toujours la moitié de D_4, ce n'est plus la parité qui partage déplacements et antidéplacements : les rotations ne sont pas toutes de même parité (ainsi que les symétries)...

Cela vient du fait que le nombre d'isométries est limité par la non-équidistance des sommets du carré (côté ≠ diagonale) :
- par exemple, le 4-cycle $\gamma = (A, B, D, C)$ ne peut être identifié à une isométrie, car : $AB \neq \gamma(A)\gamma(B) = BD$.
- on ne peut avoir 2 points successifs invariants ⇒ aucune isométrie ne s'identifie aux transpositions $(i \;\; i+1)$.
- on ne peut avoir 1 seul point invariant ⇒ aucune isométrie ne s'identifie aux 3-cycles.

Pour avoir isomorphie avec S_4, il faudra ajouter le 4ème sommet de telle sorte qu'il y ait équidistance deux à deux : on obtiendra alors le tétraèdre régulier (voir ③).

● *d)* GROUPE DIÉDRAL D'ORDRE *n* :

2.3. Pour $n \geq 4$, le groupe D_n est isomorphe à un sous-groupe strict de S_n.

☝ Le théorème de Cayley reste valable puisque S_n et ses sous-groupes peuvent être identifiés à des sous-groupes de S_{2n}.

2.4. Considérons :
- un *n*-gone $\mathcal{P}_n$ de centre *O*,
- *r* la rotation de centre *O* et d'angle $\frac{2\pi}{n}$
- *s* une symétrie d'axe passant par *O* et un sommet quelconque de $\mathcal{P}_n$.

Alors : $D_n = \langle r, s \rangle$ et $R_n = \langle r \rangle$.

☝ On en déduit que D_n est d'ordre $2n$.

🕮 Le groupe diédral D_n est défini « canoniquement » comme étant le groupe engendré par deux éléments *a* et *b* d'ordres respectifs *n* et 2 ($a^n = b^2 = e$) tels que *ab* soit d'ordre 2 ($ab^2 = e$).
Un exemple non géométrique en est donné par $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

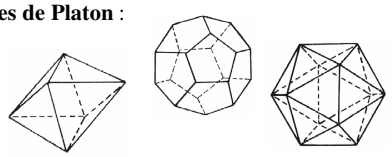
③ REPRÉSENTATION DES GROUPES DES 5 POLYÈDRES DE PLATON

On se place dans l'espace affine de dimension 3.

● *a)* RAPPEL SUR LES POLYÈDRES RÉGULIERS :

3.1.1. Un polyèdre est dit **régulier convexe** s'il est inscriptible dans une sphère et si ses faces sont des polygones réguliers convexes isométriques.

2. À similitude près, il n'y a que 5 polyèdres réguliers convexes, dits **polyèdres de Platon** :
- le tétraèdre régulier ($\triangle_4$), à 4 faces triangles équilatéraux,
- le cube, ou hexaèdre régulier, ($\square_6$), à 6 faces carrées,
- l'octaèdre régulier ($\triangle_8$), à 8 faces triangles équilatéraux,
- le dodécaèdre régulier ($\pentagon_{12}$), à 12 faces pentagones réguliers,
- l'icosaèdre régulier ($\triangle_{20}$), à 20 faces triangles équilatéraux.

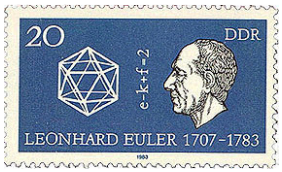


🕮 Connus d'Euclide et Platon au IVème siècle avant JC, on les appelle parfois **corps platoniciens**.

🕮 Il existe quatre polyèdres réguliers concaves : le petit et le grand dodécaèdres étoilés (Képler), et le petit et le grand icosaèdres étoilés (Poinsot).

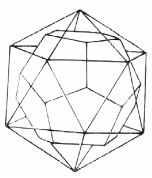
🕮 Citons, pour les polyèdres réguliers convexes, la fameuse relation d'Euler (due en fait à Descartes et démontrée par Cauchy) :

F (nombre de faces) + *S* (nombre de sommets) = *A* (nombre d'arêtes) + 2.



Elle permet de démontrer qu'il n'y a que 5 polyèdres de Platon :
- Si chaque face possède *n* côtés (avec $n \geq 3$) : $A = \frac{nF}{2}$, et donc : $F = \frac{2A}{n}$.
- Si de chaque sommet partent *p* arêtes (avec $p \geq 3$) : $A = \frac{pS}{2}$, et donc : $S = \frac{2A}{p}$.
- La relation d'Euler donne : $\frac{2A}{n} + \frac{2A}{p} = A + 2 \Rightarrow \frac{1}{n} + \frac{1}{p} = \frac{1}{2} + \frac{1}{A} > \frac{1}{2}$.
- $n = 3 \Rightarrow \frac{1}{p} > \frac{1}{2} - \frac{1}{3} = \frac{1}{6} \Rightarrow p$ ne peut valoir que 3 (on a $\triangle_4$), 4 (on a $\triangle_8$) ou 5 (on a $\triangle_{20}$).
- $p = 3 \Rightarrow n$ ne peut valoir que 3 (déjà vu), 4 (on a $\square_6$) ou 5 (on a $\pentagon_{12}$).
- Le cas $n > 3$ et $p > 3$ est impossible car alors $\frac{1}{n} + \frac{1}{p} < \frac{1}{2}$.

☝ En projetant sur la sphère circonscrite les centre de chaque face d'un polyèdre $\mathcal{P}$, on obtient les sommets du polyèdre dit **dual**, noté $\mathcal{P}^*$.

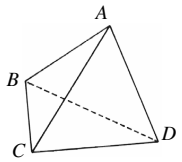


$\mathcal{P}^*$ a donc autant de sommets que $\mathcal{P}$ a de faces. Ils ont par contre même nombre d'arêtes.
En particulier, on a : $Is(\mathcal{P}) = Is(\mathcal{P}^*)$.
($\triangle_4$) est son propre dual.
Comme ($\square_6$) et ($\triangle_8$) sont duaux, ainsi que ($\pentagon_{12}$) et ($\triangle_{20}$), on se restreint à trois cas.

● *b)* REPRÉSENTATION :

Comme dans le cas des polygones, les groupes de deux polyèdres semblables sont isomorphes.

3.2.1. $Is(\Delta_4) \approx S_4$.
2. $Is^+(\Delta_4) \approx A_4$.
3. $Is^+(\square_6) \approx Is^+(\Delta_8) \approx S_4$.
4. $Is^+(\pentagon_{12}) \approx Is^+(\Delta_{20}) \approx A_5$.



☝ $Is(\Delta_4)$ est composé de :
- *Id*
- 6 symétries planes par rapport aux 6 plans médians *(s'identifiant aux transpositions)*
- 8 rotations de centre celui de $\mathcal{P}$et d'axes les 4 hauteurs d'angles $\frac{2\pi}{3}$ ou $\frac{4\pi}{3}$ *(s'identifiant aux 3-cycles)*
- 6 produits d'une rotation par une symétrie plane *(s'identifiant aux 4-cycles)*,
- 3 produits de 2 symétries planes *(s'identifiant aux produits de 2 transpositions)*.

✍ Par exemple :
- la symétrie s par rapport au plan BCI (où I est le milieu de $[AD]$) s'identifie à la transposition (AD).
- la rotation r d'axe la hauteur issue de A et d'angle $\frac{2\pi}{3}$ s'identifie au cycle (BCD).
- la composée ros s'identifie au cycle $(ABCD)$.
- la composée sos', avec s' symétrie par rapport au plan ADJ (où J est le milieu de $[BC]$) s'identifie au produit de transpositions $(AD)(BC)$.

Les rotations engendrent le sous-groupe des déplacements $G^+(\Delta_4)$,
qui s'identifie au sous-groupe engendré par les 3-cycles : A_4.
Il contient *Id*, les 8 rotations et les 3 produits de 2 symétries planes.

🕮 On peut montrer que $Is(\square_6) \approx S_4 \times \mathbb{Z}/2\mathbb{Z}$.

🕮 Les résultats **3.2.1.** et **3.2.2.** se généralisent aux simplexes réguliers T_n de $\mathbb{R}^n$ (ensemble de $n+1$ points de la sphère de $\mathbb{R}^n$ deux à deux équidistants) : $G(T_n) \approx S_{n+1}$, et : $G^+(T_n) \approx A_{n+1}$.

🕮 Les résultats **3.2.2.**, ***3.2.3.*** et ***3.2.4.*** font partie de la recherche plus générale des sous-groupes finis de $O^+(3)$.
On y retrouve, en plus de ces trois types, les groupes cycliques (engendrés par une rotation d'angle $\frac{2\pi}{n}$) et les groupes diédraux laissant invariant un polygone régulier.

V. EXERCICES

① REMISE À NIVEAU

1.1. Donner la liste des éléments de S_k et A_k, pour $k \in \{1, 2, 3, 4\}$.

1.2. On donne les permutations $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$ et $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}$.
a) Pour chacune, donner sa décomposition en cycles disjoints, sa signature et une décomposition en produit de transpositions.
b) Calculer ${\sigma_1}^{50}$ et ${\sigma_2}^{100}$.

1.3. Démontrer, par récurrence, que toute permutation de S_n est produit de transpositions.
(Démonstration qui dispense de* II 2.1. *et* 3.1.*)

1.4. Représenter, au sens du théorème de Cayley de **IV** ①, les groupes d'ordre 2, 3 et 4.
(On prendra comme modèles $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ ***et*** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.***)***

② AUTRES EXERCICES

2.1. Soit une transposition $\tau = (i\ j)$ et une permutation σ.
Démontrer que τ et σ commutent si et seulement si $\{i, j\}$ est stable par σ.

2.2. γ étant un p-cycle de S_n, on veut savoir pour quelles valeurs de k, entre 1 et $p-1$, ${\gamma}^k$ est-il un cycle.
a) Soit i dans $supp(\gamma)$ et h le cardinal de la ${\gamma}^k$-orbite de i. Montrer que : $h = \frac{p}{p \wedge k}$.
b) En déduire en combien de cycles disjoints se décompose ${\gamma}^k$, puis conclure.

2.3. Montrer que, dans un sous-groupe de S_n, soit toutes les permutations sont paires, soit la moitié des permutations sont paires.

2.4. Soit p un nombre premier ≥ 5 et H un sous-groupe de S_p tel que : $[S_p : H] \leq p-1$.
a) Soit γ un p-cycle.
1) Montrer que les classes à gauche H, γH, ${\gamma}^2 H$, ..., ${\gamma}^{p-1} H$ ne sont pas deux à deux disjointes.
2) En déduire que : $\gamma \in H$.
b) H contenant donc tous les p-cycles, montrer qu'il contient tous les 3-cycles.
c) En déduire que $[S_p : H]$ vaut 1 ou 2.
d) Trouver des diviseurs de $|S_5|$ qui ne sont l'ordre d'aucun sous-groupe de S_5 (contre-exemples à la réciproque du théorème de Lagrange).

VI. Sujets d'étude

① RÉSOLUBILITÉ DES S_n

On rappelle (voir Sujet d'étude **XII** ⑤ du chapitre 2 sur les groupes) :
- Le groupe dérivé d'un groupe G est $D(G)$, le groupe engendré par les commutateurs $xyx^{-1}y^{-1}$, avec x et y éléments de G.
- On note $D^2(G)$ le groupe dérivé de $D(G)$, et plus généralement $D^{k+1}(G)$ le groupe dérivé de $D^k(G)$.
- On appelle **suite de composition** de G une suite finie (G_i) de sous-groupes de G telle que :
  $G = G_o \supset G_1 \supset ... \supset G_{s-1} \supset G_s = \{e\}$, avec G_{k+1} distingué propre dans G_k.
- G est dit **résoluble** s'il vérifie l'une des deux propriétés équivalentes suivantes :
  (i) $\exists\, s$; $D^s(G) = \{e\}$.
  (ii) G admet une suite de composition (G_i) telle que tous les quotients G_k/G_{k+1} soient commutatifs.

1.1. Démontrer que S_1 et S_2 sont résolubles.

1.2. *a)* Démontrer que tout 3-cycle est un commutateur de transpositions.
b) En déduire que, pour $n \geq 3$, on a : $D(S_n) = A_n$.

1.3. *a)* Déterminer $D(A_3)$.
b) En déduire que S_3 est résoluble.

1.4. *a)* Dans S_4, on pose H formé de Id et des trois produits de 2 transpositions disjointes :
$H = \{Id, (12)(34), (13)(24), (14)(23)\}$.
Démontrer que H est un sous-groupe distingué de A_4.
b) On pose K formé de Id et d'un autre élément de H.
Démontrer que K est un sous-groupe distingué de H.
c) En déduire que S_4 est résoluble.

☝ On peut aussi démontrer directement que $D^4(S_4) = \{Id\}$, mais c'est très calculatoire.

1.5. On suppose désormais que $n \geq 5$.
a) Soit i, j, k, l et m tous distincts. Calculer : $(i\ l\ k)(k\ j\ m)(i\ l\ k)^{-1}(k\ j\ m)^{-1}$.
b) Soit H et K deux sous-groupes de S_n tels que H/K commutatif
Démontrer que si H contient tous les 3-cycles, alors K contient aussi tous les 3-cycles.
c) Montrer que S_n est non résoluble pour $n \geq 5$.
(Raisonner par l'absurde.)

📖 On dit qu'une équation est résoluble par radicaux si, intuitivement, ses racines peuvent s'exprimer au moyen d'opérations algébriques et de radicaux portant sur les coefficients de l'équation (une définition plus mathématique ferait appel à la théorie des corps).
On connaît, depuis le XVI^{ème} siècle, les formules explicites de résolution par radicaux des équations à coefficients réels du 2ème et 3ème degrés. L'extension de ces résultats, d'une part aux coefficients complexes, d'autre part au 4ème degré, ne pose pas trop de problème. Par contre, il faut attendre le XIX^{ème} siècle pour qu'Abel démontre qu'il n'existe pas de formules équivalentes pour le 5ème degré.
Quelques années plus tard, Galois donne une condition nécessaire et suffisante sur une équation pour qu'elle soit résoluble par radicaux : l'idée générale est de remplacer l'étude de l'équation et du corps de ses racines par l'étude d'un groupe naturellement associé, le **groupe de Galois** de l'équation (trop complexe pour être défini ici). La résolubilité par radicaux de l'équation sera alors traduite par une propriété du groupe, qui se trouve être la résolubilité de groupe.
Or, le groupe de Galois d'une équation de degré n est justement un sous-groupe de S_n (par exemple, le groupe de Galois de l'équation générale $X^n + a_{n-1}X^{n-1} + ... + a_1X + a_o = 0$ n'est autre que S_n lui-même), qui devient brusquement pauvre à partir de $n = 5$, dans le sens où il n'est plus résoluble. Nous voyons ci-dessous que cette pauvreté se traduit également par le fait que son groupe alterné n'admet plus de sous-groupe distingué propre.

② SIMPLICITÉ DES A_n

On rappelle qu'un groupe est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et lui-même.

1.1.1. Démontrer que A_3 est simple.
2. Démontrer que A_4 n'est pas simple.

1.2. On suppose désormais que $n \geq 5$.
Posons H distingué dans A_n, différent de $\{Id\}$.
a) Démontrer que si H contient un 3-cycle, alors : $H = A_n$.
Il suffit maintenant de démontrer que H contient un 3-cycle.
1ère version (courte et peu courante) :
b1) Soit $\sigma \neq Id$ un des éléments de H dont le support est de plus faible cardinal (*i.e.* aucun autre élément que Id n'a plus de points fixes que lui).
α) Démontrer que σ ne peut être ne peut être une transposition.
β) Démontrer que σ ne peut être un produit de transpositions disjointes.
(On suppose σ de la forme $(i\ j)(k\ l)...$ et on pose $\delta = (k\ l\ m)$, puis on étudie les points fixes de $\delta\sigma\delta^{-1}\sigma^{-1}$.)
γ) D'après *β)*, il y a, dans la décomposition de σ, au moins un cycle $\gamma = (i\ j\ k\ ...)$ de longueur ≥ 3.
Démontrer que σ ne peut avoir d'autres éléments que i, j et k dans son support.
(Envisager le cas de quatre éléments dans le support.
Puis, dans le cas où σ aurait deux autres éléments l et m dans son support, on pose $\delta = (k\ l\ m)$ et on étudie les points fixes de $\delta\sigma\delta^{-1}\sigma^{-1}$.)

<u>*2ème version (longue et classique)*</u> :

b2) Démontrer que si H est distingué dans A_n et contient le produit de 2 transpositions distinctes, alors : $H = A_n$.
(Dans le cas où le produit est du type $\sigma = (i\ j)(k\ l)$***, on pose*** $\delta = (i\ j\ m)$ ***et on calcule*** $\sigma^{-1}\delta\sigma\delta^{-1}$***.)***

c2) Posons H distingué dans A_n, différent de $\{Id\}$, et $\sigma \neq Id$ dans H.
Soit $\gamma_1 ... \gamma_r$ la décomposition de σ en cycles disjoints, telle que pour $1 \leq i \leq r$, on a : longueur(γ_i) $\geq$ longueur(γ_{i+1}).

α) Démontrer que si tous les γ_i sont des transpositions, alors $H = A_n$.
(On pose $\gamma_1 = (i\ j)$***,*** $\gamma_2 = (k\ l)$ ***et*** $\delta = (j\ k\ l)$***, puis on calcule*** $\sigma^{-1}\delta\sigma\delta^{-1}$***.)***

β) Démontrer que si γ_1 est un 3-cycle et tous les autres γ_i sont des transpositions, alors $H = A_n$.
(On calcule σ^2***.)***

γ) Démontrer que : longueur(γ_1) $> 3 \Rightarrow H = A_n$.
(On pose $\gamma_1 = (i_1 \dots i_p)$ ***et*** $\delta = (i_1\ i_2\ i_3)$***, puis on calcule*** $\delta\sigma\delta^{-1}\sigma^{-1}$***.)***

δ) Démontrer que γ_1 et γ_2 sont des 3-cycles, alors $H = A_n$.
(On pose $\gamma_1 = (i\ j\ k)$***,*** $\gamma_2 = (i'\ j'\ k')$ ***et*** $\delta = (j\ k\ i')$***, puis on calcule*** $\sigma^{-1}\delta\sigma\delta^{-1}$***.)***

Tous les cas ayant été envisagés, on en déduit que A_n est simple pour $n \geq 5$.

☝ Le schéma de démonstration de la simplicité de $O^+(3)$ est le même :
on montre que H contient un retournement puis, par conjugaison, tous les retournements, générateurs de $O^+(3)$.

🕮 L'étude de la simplicité des A_n s'inscrit dans la classification des groupes simples non commutatifs, débutée en 1960.

🕮 La simplicité de A_n pour $n \geq 5$ permet de démontrer la non résolubilité de S_n, sans utiliser la notion de groupe dérivé :
<u>*Résultats utilisés*</u> :

- G résoluble $\Leftrightarrow$ G admet une suite de composition (G_i) telle que tous les quotients G_{i+1}/G_i soient commutatifs.
- La suite de composition (G_i) est appelée suite de **Jordan-Hölder** de G si chaque G_i est un sous-groupe distingué propre maximal.
- <u>THÉORÈME DE JORDAN-HÖLDER</u> ***(démonstration difficile)*** :
  Si G admet deux suites de Jordan-Hölder,
  alors les quotients de l'une et de l'autre sont, à l'ordre près, isomorphes deux à deux.

Or, $S_n \supset A_n \supset \{Id\}$ constitue une suite de Jordan-Hölder de S_n.
Mais, cette suite ne permet pas d'obtenir la résolubilité de S_n car $A_n/\{Id\} \approx A_n$ n'est pas commutatif.
Etant de Jordan-Hölder, aucun sous-groupe distingué ne peut être ajouté à la suite pour obtenir un quotient commutatif.
Et s'il existe une autre suite de Jordan-Hölder de S_n, l'un de ses quotients est isomorphe à A_n donc non commutatif.
Il est donc impossible de trouver une suite de composition permettant d'assurer la résolubilité de S_n.

③ <u>CARACTÉRISATION DES AUTOMORPHISMES INTÉRIEURS DE S_n</u>

3.1. Montrer que tout automorphisme intérieur de S_n transforme une transposition en une transposition.

On se propose de montrer que cette propriété est caractéristique des automorphismes intérieurs.
Soit φ un automorphisme conservant globalement l'ensemble des transpositions.

3.2. On pose $F_i = \{\varphi(i\ j)\ ;\ i \neq j\}$.
Montrer que les supports de tous les éléments de F_i contiennent un même élément, que l'on notera x_i.

3.3. On pose $\sigma : \{1, ..., n\} \to \{1, ..., n\}$
$i \mapsto x_i$.
Montrer que : $\sigma \in S_n$.

3.4. Montrer que, pour toute transposition τ, on a : $\varphi(\tau) = \sigma\tau\sigma^{-1}$.
Conclure.

④ <u>POUR $n \neq 6$, TOUT AUTOMORPHISME DE S_n EST INTÉRIEUR</u>

Attention, ce sujet d'étude utilise le résultat établi par celui de ③.

4.1. Montrer que tout automorphisme de S_3 est intérieur.

On se propose de montrer que le résultat est vrai pour tout $n \neq 6$.
Soit E l'ensemble des éléments d'ordre 2 de S_n.
Notons C_q l'ensemble des produits de q transpositions disjointes.

4.2. Montrer que les C_q constituent exactement les classes de la conjugaison de S_n sur E.
(Utiliser la caractérisation de la conjugaison dans S_n***.)***

4.3. Montrer que φ transforme un C_q en un $C_{q'}$.

4.4. Montrer que, pour $n \neq 6$ et $q > 1$, C_q n'a pas même cardinal que C_1.
(Raisonner par l'absurde et envisager les cas $q = 2$***,*** $q = 3$ ***et*** $q \geq 4$***.)***

4.5. Conclure.
(Utiliser la caractérisation des automorphismes intérieurs vue en ③.)

VII. Annexe : invariance de la parité du nombre de transpositions

Lors de la construction de A_n, on a besoin de démontrer le résultat suivant :

Dans la décomposition d'une permutation, le nombre de transpositions a toujours même parité.

Attention au fait que nous cherchons à définir la signature au moyen de l'image des transpositions qui ne peut être que –1, mais que nous devons démontrer le résultat en question pour que cela constitue une définition de ε.
Il est entendu que le résultat devient une propriété triviale lorsqu'on définit ε d'autres manières (par les inversions ou le nombre d'orbites). Mais ces définitions sont généralement parachutées, cachant la structure profonde de A_n.

① DÉMONSTRATION DU MUTAFIAN

Considérons une permutation σ décomposée en cycles disjoints $\gamma_1...\gamma_p$.
On prendra en compte dans cette décomposition les éléments invariants en les considérant comme des 1-cycles.

- Montrons que la multiplication à droite par une transposition augmente ou diminue la décomposition de 1 cycle :
  Soit $\tau = (ij)$ une transposition.
  Le fait d'inclure les 1-cycles dans la décomposition de σ entraîne que i et j sont nécessairement dans les cycles de la décomposition.
  - 1er cas : i et j appartiennent à deux cycles distincts γ_r et γ_s.
    Rien n'empêche de faire commencer γ_r par i et γ_s par j :
    $$\gamma_r = (i\ \ \gamma_r(i)\ \ \gamma_r^2(i)\ \ ...\ \ \gamma_r^{r-1}(i))$$
    $$\gamma_s = (j\ \ \gamma_s(j)\ \ \gamma_s^2(j)\ \ ...\ \ \gamma_s^{s-1}(j))$$
    Alors, le calcul de $\sigma\tau$ se réduit au calcul de $\gamma_r\gamma_s\tau$ puisque τ est disjoint de tous les autres cycles.
    On obtient : $\gamma_r\gamma_s\tau = (i\ \ \gamma_s(j)\ \ \gamma_s^2(j)\ \ ...\ \ \gamma_s^{s-1}(j)\ \ j\ \ \gamma_r(i)\ \ \gamma_r^2(i)\ \ ...\ \ \gamma_r^{r-1}(i))$.
    Les autres cycles étant disjoints (ij), leurs supports restent inchangés.
    Donc, on peut en conclure que $\sigma\tau$ comporte un cycle de moins que σ.
  - 2ème cas : i et j appartiennent au même cycle γ_r.
    Rien n'empêche de faire commencer γ_r par i :
    $$\gamma_r = (i\ \ \gamma_r(i)\ \ \gamma_r^2(i)\ \ ...\ \ \gamma_r^{s-1}(i)\ \ j\ \ \gamma_r(j)\ \ \gamma_r^{t-1}(j))\text{, avec } s + t = \text{longueur de } \gamma_r.$$
    Alors, le calcul de $\sigma\tau$ se réduit au calcul de $\gamma_r\tau$ puisque τ est disjoint de tous les autres cycles.
    On obtient : $\gamma_r\tau = (i\ \ \gamma_r(i)\ \ \gamma_r^{s-1}(i))(j\ \ \gamma_r(j)\ \ ...\ \ \gamma_r^{t-1}(j))$.
    Les autres cycles étant disjoints (ij), leurs supports restent inchangés.
  Donc, on peut en conclure que $\sigma\tau$ comporte un cycle de plus que σ.
- Montrons que la parité du nombre de transpositions est invariant :
  Posons $\sigma = \tau_1...\tau_q$.
  Quand on calcule $\sigma\tau_q...\tau_1$, on augmente ou on diminue q fois de 1 cycle.
  Supposons q_1 augmentations et q_2 diminutions : $\sigma\tau_q...\tau_1$ comporte donc $(p + q_1 - q_2)$ cycles.
  Mais : $\sigma\tau_q...\tau_1 = \tau_1...\tau_q\tau_q...\tau_1 = Id$, qui comporte n cycles de longueur 1.
  D'où : $p + q_1 - q_2 = n \Rightarrow n - p = q_1 - q_2$, de même parité que $q_1 + q_2 = q$.
  Finalement, le nombre q de transpositions est de même parité que $n - p$, qui lui ne dépend que de σ.

② DÉMONSTRATION DU MAZET

Posons $\sigma = \tau_1...\tau_p$ et $\tau'_1...\tau'_q$ deux décompositions en produit de transpositions.
Alors : $\tau_1...\tau_p$ et $\tau'_1...\tau'_q\tau'_q...\tau'_1 = Id \Rightarrow \tau_1...\tau_p\tau'_q...\tau'_1 = Id$.
Ce qui constitue une décomposition de Id en $(p + q)$ transpositions.
Si p et q étaient de parité différente, on aurait $(p + q)$ impair.
Or on va montrer que Id ne peut se décomposer en un nombre impair de transpositions.

- Montrons que, si $\tau \neq (i\ j)$, alors $\tau(i\ j)$ peut s'écrire $(i\ k)\tau'$, avec $i \notin supp(\tau')$
  Si $i \in supp(\tau)$, alors τ s'écrit $(i\ k)$ avec $k \neq j$.
  On a : $\tau(i\ j) = (i\ k)(i\ j) = (i\ j)(j\ k)$.
  Si $i \notin supp(\tau)$, alors : $\tau(i\ j) = (i\ \tau(j))(j\ \tau(j))$
- Montrons que Id ne peut se décomposer en un nombre impair de transpositions :
  Récurrence sur n que $Id \neq \tau_1...\tau_{2n+1}$.
  Vrai pour $n = 0$ puisqu'aucune transposition n'est Id.
  Supposons vrai jusqu'à $2n - 1$ et posons : $Id = \tau_1...\tau_{2n+1}$.
  Posons $\tau_{2n+1} = (i\ j)$.
  En utilisant le résultat précédent, on peut faire remonter $(i\ j)$ tant qu'on n'en rencontre pas un autre.
  1er cas : on n'en rencontre pas, alors : $Id = (i\ k)\tau'_2...\tau'_{2n+1}$
  $\Rightarrow (i\ k) = \tau'_2...\tau'_{2n+1}$: impossible car i fixe par les τ'
  2ème cas : on en rencontre, alors : $Id = \tau_1...\tau_k\,(i\ k)(i\ k)\tau'_{k+3}...\tau'_{2n+1}$
  $= \tau_1...\tau_k\tau'_{k+3}...\tau'_{2n+1}$: impossible par hypothèse de récurrence.

Bibliographie

Arnaudiès, Fraysse	*Cours de mathématiques - Algèbre*	Dunod	Théorie complète, exercices nombreux, S_n comme contre-exemple à la réciproque du théorème de Lagrange.
Bouvier, Richard	*Groupes*	Hermann	Théorie complète mais très dispersée, simplicité des A_n, résolubilité des S_n, lien entre les deux.
Calais	*Éléments de la théorie des groupes*	PUF	Théorie complète, simplicité des A_n en exercice.
Francinou, Gianella	*Exercices de mathématiques pour l'agrégation*	Masson	Simplicité des A_n, automorphismes de S_n, résolubilité des S_n.
Gourdon	*Algèbre*	Ellipses	Théorie assez complète, S_n comme contre-exemple à la réciproque du théorème de Lagrange.
Lafon	*Algèbre*	Hermann	Simplicité des A_n.
Mazet	*Algèbre et géométrie pour le CAPES et l'Agrégation*	Ellipses	Théorie complète, construction soignée de A_n, résolubilité des S_n, invariance de la parité du nb de transpositions.
Mutafian	*Le défi algébrique*	Vuibert	Théorie complète, construction très élégante des A_n, simplicité des A_n, automorphismes de S_n.
Perrin	*Cours d'algèbre*	Ellipses	Simplicité des A_n, automorphismes de S_n.