105

Groupe des permutations d'un ensemble fini. Applications.

[TAU] p 63

I/ Généralités sur le groupe symétrique

1) Définition et premières propriétés [TAU] p 59 [ULN] p 31

Déf 1 : Soit E un ensemble. Une bijection de E sur lui-même est appelée une permutation de E. On note $\mathfrak{S}_E$ l'ensemble des permutations de E.

Prop 2 : $(\mathfrak{S}_E, \circ)$ est un groupe, appelé groupe symétrique de E.

Déf 3 : On note $\mathfrak{S}_n$ le groupe symétrique de $\mathbb{N}_n^* = \{1,\dots,n\}$, $n \in \mathbb{N}^*$, et on dit que $\mathfrak{S}_n$ est le groupe symétrique d'ordre n. On a $\mathrm{Card}(\mathfrak{S}_n) = n!$ Un élément $\sigma \in \mathfrak{S}_n$ s'écrit $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

Ex 4 : Les 6 éléments de $\mathfrak{S}_3$ sont $e = \begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}$, $\sigma_1 = \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}$, $\tau_1 = \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}$.

Prop 5 : Si E est fini de cardinal n, $\mathfrak{S}_E \simeq \mathfrak{S}_n$. (Ainsi $\mathfrak{S}_n$ peut être considéré comme le groupe des permutations de tout ensemble fini de cardinal n).

Prop 6 : Si $n \geq 3$, le centre Z de $\mathfrak{S}_n$ est $\{e\}$ et $\mathfrak{S}_n$ n'est pas abélien.

Rq 7 : La donnée d'une action d'un groupe G sur un ensemble E est équivalente à celle d'un morphisme $\gamma : G \longrightarrow \mathfrak{S}_E$. En considérant l'action de G sur lui-même par translation à gauche, on obtient le résultat suivant :

Th 8 : (de Cayley) Tout groupe fini G d'ordre $n \in \mathbb{N}$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$. (*)

2) Orbites et cycles [ULN] p 42-46

Déf 9 : Soit $\sigma \in \mathfrak{S}_n$. Le support de σ est l'ensemble $\mathrm{supp}(\sigma) = \{i \in \mathbb{N}_n^*, \sigma(i) \neq i\}$.

Prop 10 : Les permutations à supports disjoints commutent.

Déf 11 : Soient $1 \leq l \in \mathbb{N}$ et $i_1, i_2, \dots, i_l$ des éléments distincts de $\{1,\dots,n\}$. La permutation $\sigma \in \mathfrak{S}_n$ définie par :

$$\sigma(j) = \begin{cases} j & \text{si } j \notin \{i_1,\dots,i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $(i_1, i_2, \dots, i_l)$ est appelée cycle de longueur l. Un cycle de longueur 2 est appelé une transposition.

Th 12 : Tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$ de cycles σ_i de longueur ≥ 2 dont les supports sont 2 à 2 disjoints et correspondent aux orbites de l'action $\langle\sigma\rangle \hookrightarrow \mathfrak{S}_n$ du sous-groupe engendré par σ sur $\{1,\dots,n\}$. Cette décomposition est unique à l'ordre près.

Déf 13 : On appelle type d'une permutation $\sigma \in \mathfrak{S}_n$ et on note $[l_1, l_2, \dots, l_m]$, la liste des cardinaux des orbites de l'action $\langle\sigma\rangle \hookrightarrow \mathfrak{S}_n$, rangée par ordre croissant.

Prop 14 : Une permutation de type $[l_1, l_2, \dots, l_m]$ a pour ordre $\mathrm{ppcm}(l_1, l_2, \dots, l_m)$.

Ex 15 : $\sigma = \begin{pmatrix} 1&2&3&4&5&6 \\ 2&4&5&1&3&6 \end{pmatrix} \in \mathfrak{S}_6$ s'écrit $\sigma = (1,2,4)(3,5)$. Son type est $[1,2,3]$ et son ordre est 6.

Rq 16 : Pour $2 \leq l \leq n$, il y a $(l-1)!\binom{n}{l}$ l-cycles dans $\mathfrak{S}_n$.

Prop 17 : Deux permutations sont conjuguées dans $\mathfrak{S}_n$ ssi elles ont le même type. En particulier $\forall \omega \in \mathfrak{S}_n$ et tout cycle $(i_1, i_2, \dots, i_l) \in \mathfrak{S}_n$ on a : $\omega (i_1, \dots, i_l) \omega^{-1} = (\omega(i_1), \omega(i_2), \dots, \omega(i_l))$

App 18 : Construction de la table de caractères de $\mathfrak{S}_4$.

	Id	[1,1,2]	[1,3]	[4]	[2,2]
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_2	3	1	0	-1	-1
χ_3	3	-1	0	1	-1
χ_4	2	0	-1	0	2

3) Générateurs du groupe $\mathfrak{S}_n$ [TAU] p 61

Prop 19 : Les ensembles suivants engendrent $\mathfrak{S}_n$ $(n \geq 2)$:

1) Les transpositions $(i, i+1)$ pour $1 \leq i \leq n-1$
2) Les transpositions $(1, i)$ pour $2 \leq i \leq n$

(*) App : Théorème de Sylow.

3) La transposition $(1,2)$ et le n-cycle $(1,2,\dots,n)$
En particulier, $\mathfrak{S}_n$ est engendré par les transpositions.

<u>Rq 20</u> : (Formules utiles) : $(i_1,i_2,\dots,i_\ell) = (i_1,i_2)(i_2,i_3)\dots(i_{\ell-1},i_\ell)$
$(i,j) = (1,i)(1,j)(1,i)$

<u>Ex 21</u> : Pour $\tau = (3,1,5,2) \in \mathfrak{S}_5$ on a $\tau = (3,2)(3,5)(3,1)$
$= (1,3)(1,2)(1,5)$

II/ Signature d'une permutation et groupe alterné $\mathcal{A}_n$

1) Signature d'une permutation [ULM] p 49

<u>Déf 22</u> : Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le nombre : $\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i)-\sigma(j)}{i-j}$

<u>Prop 23</u> : 1) L'application $\varepsilon : \mathfrak{S}_n \longrightarrow (\mathbb{C}^*,\cdot)$, $\sigma \longmapsto \varepsilon(\sigma)$ est l'unique morphisme de groupes non trivial de $\mathfrak{S}_n$ dans $(\mathbb{C}^*,\cdot)$.
2) Si σ est une transposition, $\varepsilon(\sigma) = -1$.
3) Si σ est un produit de k transpositions, $\varepsilon(\sigma) = (-1)^k$.
Donc si $\sigma = \tau_1 \dots \tau_k$ et $\sigma = \tau_1' \dots \tau_\ell'$ sont 2 décompositions de σ en produit de transpositions, k et ℓ ont même parité.
4) Si $\sigma \in \mathfrak{S}_n$ est de type $[\ell_1,\dots,\ell_m]$ alors
$\varepsilon(\sigma) = (-1)^{\ell_1-1}(-1)^{\ell_2-1}\dots(-1)^{\ell_m-1} = (-1)^{\ell_1+\dots+\ell_m-m}$
En particulier l'image de ε est le sous-groupe $\{1,-1\}$ de $\mathbb{C}^*$.

<u>Déf 24</u> : $\sigma \in \mathfrak{S}_n$ est dite paire si $\varepsilon(\sigma) = 1$, impaire sinon.

2) Le groupe alterné $\mathcal{A}_n$ [ULM] p 50 [TAU] p 63-64

<u>Déf 25</u> : Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1,1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$ appelé groupe alterné et noté $\mathcal{A}_n$.

<u>Prop 26</u> : Pour $n \geq 2$, $\mathcal{A}_n$ est un sous-groupe d'indice 2 de $\mathfrak{S}_n$ et contient $\frac{n!}{2}$ éléments.

<u>Prop 27</u> : 1) Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les permutations $(1,i)(1,j)$ où $2 \le i,j \le n$.
2) Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1,2,i)$ avec $3 \le i \le n$.
3) $\mathcal{A}_n$ est engendré par les éléments s^2, $s \in \mathfrak{S}_n$
En particulier, $\mathcal{A}_n$ est engendré par les 3-cycles.

<u>Ex 28</u> : $\mathcal{A}_3 = \{e, (1,2,3), (1,3,2)\} = \{e, \tau, \tau^2\}$ où $\tau = (1,2,3)$

<u>Prop 29</u> : Si $n \geq 5$, les cycles d'ordre 3 sont conjugués dans $\mathcal{A}_n$.

3) Structure de $\mathcal{A}_n$ et $\mathfrak{S}_n$. [PER] p 28

<u>Th 30</u> : Le groupe $\mathcal{A}_n$ est simple pour $n \geq 5$. } DVP

<u>Cor 31</u> : $\mathcal{D}(\mathcal{A}_n) = \mathcal{A}_n$ pour $n \geq 5$ et $\mathcal{D}(\mathfrak{S}_n) = \mathcal{A}_n$ pour $n \geq 2$

<u>Rq 32</u> : $\mathcal{A}_4$ n'est pas simple car $\mathcal{D}(\mathcal{A}_4)$ est un sous-groupe distingué d'ordre 4 isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:
$\mathcal{D}(\mathcal{A}_4) = \{Id, (12)(34), (13)(24), (14)(23)\}$

<u>Cor 33</u> : Pour $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

<u>Cor 34</u> : Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$. Alors $H \simeq \mathfrak{S}_{n-1}$.

<u>Prop 35</u> : Soit $\varphi \in Aut(\mathfrak{S}_n)$. Si φ transforme transposition en transposition, φ est intérieur.

<u>Th 36</u> : Pour $n \neq 6$, $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$.

DVP

III / Applications

1) Déterminant [GOU] p 134

$\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-ev de dimension $n \in \mathbb{N}^*$.
$\mathcal{L}_p(E,\mathbb{K})$ = ensemble des formes p-linéaires sur E.

Déf 37 : $f \in \mathcal{L}_p(E,\mathbb{K})$ est dite :
- alternée si $f(x_1,\dots,x_p)=0$ dès que 2 vecteurs parmi les x_i sont égaux
- antisymétrique si l'échange de 2 x_i donne à f des valeurs opposées.

Rq 38 : f antisymétrique $\Leftrightarrow$ $\forall \sigma \in \mathfrak{S}_p$ et $\forall (x_1,\dots,x_p) \in E^p$,
$f(x_{\sigma(1)},\dots,x_{\sigma(p)}) = \varepsilon(\sigma)\, f(x_1,\dots,x_p)$

Th 39 : Si $car(\mathbb{K}) \neq 2$, f antisymétrique $\Leftrightarrow$ f alternée.

Déf 40 : (Antisymétrisation d'une forme p-linéaire)
Pour tout $f \in \mathcal{L}_p(E,\mathbb{K})$ on note $f^\#: E^p \longrightarrow \mathbb{K}$,
$(x_1,\dots,x_p) \longmapsto \sum_{\sigma\in\mathfrak{S}_p} \varepsilon(\sigma)\, f(x_{\sigma(1)},\dots,x_{\sigma(p)})$.
$f^\#$ est une forme p-linéaire alternée.

Th 41 : L'ensemble des formes n-linéaires alternées sur un $\mathbb{K}$-ev de dimension n est un $\mathbb{K}$-ev de dimension 1. De plus il existe une et une seule forme n-linéaire alternée prenant la valeur 1 sur une base donnée $\mathcal{B}=(e_1,\dots,e_n)$. On l'appelle déterminant dans la base $\mathcal{B}$ et on la note $\det_{\mathcal{B}}$.
Si $(x_1,\dots,x_n) \in E^n$ $(x_i = \sum_{j=1}^{n} x_{ij} e_j)$, on a :

$$\det_{\mathcal{B}}(x_1,\dots,x_n) = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma)\, x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$$

2) Polynômes symétriques [RDO1] p 200

Soit A un anneau commutatif.

Prop 42 : L'application
$$\begin{array}{ccc}\mathfrak{S}_n \times A[X_1,\dots,X_n] & \longrightarrow & A[X_1,\dots,X_n] \\ (\sigma, P) & \longmapsto & \sigma(P)\end{array}$$
où $\sigma(P)(X_1,\dots,X_n) = P(X_{\sigma(1)},\dots,X_{\sigma(n)})$ est une action du groupe $\mathfrak{S}_n$ sur $A[X_1,\dots,X_n]$.

Déf 43 : $P \in A[X_1,\dots,X_n]$ est dit symétrique si $\forall \tau \in \mathfrak{S}_n$, $\tau(P)=P$.
" " " alterné si $\forall \tau \in \mathfrak{A}_n$, $\tau(P)=P$.

Ex 44 : $\prod_{1\le i<j\le n} (X_j - X_i)$ est un polynôme alterné mais pas symétrique

Déf 45 : Les n polynômes $\Sigma_p = \sum_{1\le i_1<\dots<i_p\le n} X_{i_1}\cdots X_{i_p}$, $1\le p\le n$
sont symétriques et portent le nom de polynômes symétriques élémentaires.

Prop 46 : Soit $P = \prod_{i=1}^{n}(Y - X_i) \in A[X_1,\dots,X_n,Y]$. Alors on a :
$$P = Y^n + \sum_{p=1}^{n} (-1)^p\, \Sigma_p\, Y^{n-p}.$$

Rq : On retrouve ainsi les relations coefficients - racines.

Déf 47 : • On appelle poids du monôme $X_1^{i_1}\dots X_n^{i_n}$ l'entier $\sum_{k=1}^{n} k\, i_k$.
Le poids d'un polynôme P est le maximum des poids de ses monômes. On le note $\pi(P)$. $(\pi(0) = -\infty)$
• Soit P un polynôme symétrique de $A[X_1,\dots,X_n]$. P a même degré partiel par rapport à chaque indéterminée. Ce degré s'appelle l'ordre de P et est noté $\omega(P)$.

Th 48 : (de structure des polynômes symétriques)
Soit P un polynôme symétrique de $A[X_1,\dots,X_n]$ de degré p et d'ordre ω. Il existe un unique polynôme Q de $A[Y_1,\dots,Y_n]$ tel que $P(X_1,\dots,X_n) = Q(\Sigma_1,\dots,\Sigma_n)$. Q est de poids p et de degré ω.

3) Groupes d'isométries de polyèdres [SPZ] p 422-424

$\mathcal{E}$ espace affine euclidien de dimension 3.

Prop 49. Une isométrie de $\mathcal{E}$ conserve le polyèdre $\mathcal{P}$ ssi elle induit une permutation des sommets de ce polyèdre.
L'application $\Phi : Is_{\mathcal{P}}(\mathcal{E}) \longrightarrow \mathfrak{S}_S$ (où S désigne l'ensemble des sommets de $\mathcal{P}$) est un morphisme injectif de groupes.

Ex 50 : 1) Si T est un tétraèdre régulier, $Is(T) \simeq \mathfrak{S}_4$.
2) Si C est un cube, $Is^+(C) \simeq \mathfrak{S}_4$

Références :

- Perrin, Cours d'Algèbre [PER]
- Gourdon, Algèbre [GOU]
- Ramis, Deschamps, Odoux : Algèbre 1 [RDO1]
- Tauvel, Algèbre [TAU]
- Ulmer, Théorie des groupes [ULM]

Simplicité de A_n pour $n \geqslant 5$

[L3 Pearson Alg p 267]
[Perrin p 28]

<u>Théorème</u> : Le groupe A_n est simple pour $n \geqslant 5$

<u>Le théorème sera démontré pour $n = 5$ uniquement.</u>

<u>Résultats utiles</u>

- <u>Rés 1</u> : Pour $n \geqslant 3$, les 3-cycles sont dans A_n et l'engendrent.

□ . On observe d'abord que si $1 \leq i, j, k \leq n$ sont 3 entiers distincts,

$$(i, j) \circ (j, k) = (i, j, k)$$

Ceci démontre déjà que <u>les 3 cycles sont des permutations paires</u>

. Si $\sigma \in A_n$, $\sigma = \tau_1 \circ \dots \circ \tau_{2k}$ (où $\tau_1, \dots, \tau_{2k}$ sont des transpositions à supports disjoints qu'on regroupe 2 à 2)

On se ramène donc à étudier un produit $\tau \circ \tau'$ de 2 transpositions à supports disjoints

Ecrivons $\tau = (i, j)$ et $\tau' = (k, l)$ où les entiers i, j, k, l sont 2 à 2 distincts

Les transpositions étant d'ordre 2, on peut écrire astucieusement :

$$\tau \circ \tau' = \underbrace{(i, j) \circ (j, k)} \circ \underbrace{(j, k) \circ (k, l)}$$

$$\tau \circ \tau' = (i, j, k) \circ (j, k, l)$$

les 3-cycles engendrent bien A_n □

- <u>Rés 2</u> : Soit $n \geqslant 3$. Le groupe A_n est $(n-2)$ transitif sur $\{1, \dots, n\}$

ie si on a $\begin{cases} (a_1, \dots, a_{n-2}) \in \{1, \dots, n-2\} & \text{2 à 2 distincts} \\ (b_1, \dots, b_{n-2}) \in \{1, \dots, n-2) & \text{2 à 2 distincts} \end{cases}$

alors il existe $\sigma \in A_n$ tq $\forall i \in \{1, \dots, n-2\}$, $\sigma(a_i) = b_i$

□ Si $(a_1, \dots, a_{n-2})$ et $(b_1, \dots, b_{n-2})$ sont deux ensembles de $(n-2)$ entiers 2 à 2 distincts $\in \{1, \dots, n\}$, on les complète en 2 n-uplets $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ définissant chacun une permutation de $\{1, \dots, n\}$

et on considère $\sigma \in \mathfrak{S}_n$ tq $\sigma(a_i) = b_i$ $1 \leq i \leq n$

- Si σ est paire ($\sigma \in A_n$), c'est terminé
- Sinon, on compose σ avec la transposition $\tau = (a_{n-1}, a_n)$ et $\sigma \circ \tau \in A_n$ et $\forall i = 1, \dots, n-2$ $\sigma \circ \tau(a_i) = b_i$ $\square$

- Rés 3 : Si $n \geq 5$, les 3-cycles sont conjugués dans A_n

$\square$ Si $n \geq 5$, pour $\sigma = (a_1, a_2, a_3)$ et $\tau = (b_1, b_2, b_3) \in A_n$

$\underset{(\text{rés } 2)}{\Longrightarrow}$ (A_n agit 3-transitivement) $\exists \rho \in A_n$ tq $\rho(a_i) = b_i$

donc $\tau = (\rho(a_1), \rho(a_2), \rho(a_3)) = \rho \sigma \rho^{-1}$

(rappel : Soit $1 \leq k \leq n$. Si $\sigma = (a_1, \dots, a_k) \in \mathfrak{S}_n$ est un cycle d'ordre k et $\rho \in \mathfrak{S}_n$, on a $\rho\sigma\rho^{-1} = (\rho(a_1), \dots, \rho(a_k))$)

Conclusion : 3-cycles sont conjugués dans A_n. $\square$

- Déf° (Groupe simple)

Un groupe $G \neq \{e\}$ est appelé un groupe simple si ses seuls sous-groupes distingués sont G et $\{e\}$

- Preuve du théorème (pour $n = 5$)

$\square$ Commençons par décrire les $\frac{5!}{2} = 60$ éléments de A_5 regroupés par type :

- $[1\ 1\ 1\ 1\ 1]$: l'identité — 1 élément d'ordre 1
- $[2\ 2\ 1]$: produit de 2 transpositions à supports disjoints

$\rightarrow$ Pour déterminer une telle permutation, il faut se donner un point fixe (5 possibilités) et choisir 2 éléments parmi les 4 restants qui correspondent à une des 2 transpositions (l'autre étant alors automatiquement déterminée)

soit $C_4^2 = 6$ possibilités mais comme $(a,b)(c,d) = (c,d)(a,b)$ $(a,b,c,d \neq)$ il faut diviser par 2 pour obtenir le nombre de permutations d'ordre 2

Finalement, on a $\frac{6 \times 5}{2} = 15$ éléments d'ordre 2

• [3 1 1] les 3-cycles

↳ Pour déterminer un 3-cycle, il faut choisir les 2 points fixes ie $C_5^2 = 10$ possibilités, puis on détermine l'image des 3 points qui ne sont pas fixes par la permutation.

Or, une fois fixée l'image d'un élément, les images des 2 autres sont automatiquement déterminées ie 2 possibilités pour les images des points du 3-cycle qui ne sont pas fixes.

Soit au total $10 \times 2 =$ 20 éléments d'ordre 3

• [5] les 5-cycles

↳ Ici, pas de point fixe : il suffit de déterminer les images des points de la permutation ie pour 1, on a 4 possibilités (2, 3, 4, 5) puis pour 2, 3 possibilités (tout sauf 2 lui-même et l'image de 1 qui est déjà prise) et ainsi de suite ... Au total, $4 \times 3 \times 2 =$ 24 éléments d'ordre 5

On a bien : $1 + 15 + 20 + 24 = 60$ éléments de A_5.

De plus, on sait que les 3-cycles sont conjugués dans A_5 (Rés 3).

Il en est de même pour les produits de 2 transpositions à supports disjoints.

En effet, si $\sigma = (i, j)(k, l)(m)$ et $\sigma' = (i', j')(k', l')(m')$

le groupe A_5 étant 3-transitif (Rés 2) $\exists\, \tau \in A_5$ tel que

$$\tau(i) = i' \qquad \tau(j) = j' \qquad \tau(m) = m'$$

$$\begin{aligned}
\tau \sigma \tau^{-1} &= \tau (i, j)(k, l)(m) \tau^{-1} \\
&= \tau (i, j) \tau^{-1} \, \tau (k, l) \tau^{-1} \, \tau (m) \tau^{-1} \\
&= (\tau(i), \tau(j)) \, (\tau(k), \tau(l)) \, (\tau(m)) \\
&= (i', j') \, (\tau(k), \tau(l)) \, (m') \\
&= (i', j') (k', l') (m')
\end{aligned}$$

$$\tau \sigma \tau^{-1} = \sigma'$$

Soit alors $H \lhd A_5$ et $H \neq \{e\}$

- Si H contient un élément d'ordre 3 (resp 2) alors il les contient tous puisqu'ils sont tous conjugués et H est distingué.

- De plus, si H contient un élément d'ordre 5, il contient aussi le sous-groupe engendré par cet élément, il contient alors le 5-Sylow engendré par cet élément et donc tous les 5-Sylow puisqu'ils sont conjugués (Th de Sylow) ie dans ce cas, H contient tous les éléments d'ordre 5.

Mais H ne peut contenir un seul des 3 types d'éléments précédents (en plus du neutre)

car $15+1=16 \nmid 60$ et $20+1 \nmid 60$ et $24+1 \nmid 60$.

(le cardinal de H divise $|A_5| = 60$ d'après le théorème de Lagrange).

donc H contient au moins 2 des 3 types d'éléments

ie il admet au moins $1+15+20 = 36$ éléments or $36 \nmid 60$

d'où $|H| = 60$ et $H = A_5$ $\square$.

Automorphismes de $\mathfrak{S}_n$

[Perrin p31]

[X ENS Alg 1 p 69-74]

Théorème : Pour $n \neq 6$, tout automorphisme de $\mathfrak{S}_n$ est intérieur
$$\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$$

Rque : Si de plus, $n \geqslant 3$, $\mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n/Z(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ (car $Z(\mathfrak{S}_n) = \{1\}$)
On aura montré que $\mathrm{Aut}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$.

Déf° : $\forall \alpha \in \mathfrak{S}_n$ $i_\alpha : \mathfrak{S}_n \longrightarrow \mathfrak{S}_n$, $\tau \longmapsto \alpha \tau \alpha^{-1}$ est un automorphisme de $\mathfrak{S}_n$.

L'ensemble $\mathrm{Int}(\mathfrak{S}_n) = \{ i_\alpha / \alpha \in \mathfrak{S}_n \}$ est appelé groupe des automorphismes intérieurs de $\mathfrak{S}_n$.

[Rque : la clé de la démonstration est une traduction des propriétés géométriques des éléments de $\mathfrak{S}_n$ (ex : le nombre de points fixes, les cycles, ...) en propriétés algébriques (ordre des éléments, propriétés de commutation, ...)
Les propriétés algébriques se conservent par automorphisme mais pas, a priori, les propriétés géométriques qui nous intéressent ici.]

La preuve de ce théorème s'appuie sur 2 lemmes :

Lemme 1 : Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Si φ transforme les transpositions en transpositions, alors $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$

□ $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1, i)$ où $2 \leq i \leq n$.
Par hypothèse, $\varphi(\tau_i)$ est une transposition.
Si $i \neq j$, comme τ_i et τ_j ne commutent pas, (leurs supports sont non disjoints)
$\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent pas non plus et leurs supports sont non disjoints.
Si on pose $\varphi(\tau_2) = \varphi((1\,2)) = (\alpha_1, \alpha_2)$, on peut donc supposer que
$\varphi(\tau_3) = \varphi((1,3)) = \underset{(\alpha_2 \neq \alpha_3)}{(\alpha_1, \alpha_3)}$ et on a $\varphi(\tau_i) = (\alpha_1, \alpha_i)$ pour $2 \leq i \leq n$.

En effet, si par exple $\varphi(\tau_i) = (\alpha_2, \alpha_3)$ dont le support intersecte bien celui de $\varphi(\tau_1)$ et $\varphi(\tau_2)$

Comme $(\alpha_1, \alpha_2) \circ (\alpha_1, \alpha_3) \circ (\alpha_2, \alpha_3) = (\alpha_1, \alpha_3)$

$\varphi^{-1} \Downarrow$

on aurait $(1,2) \circ (1\,3) \circ (1\,i) = (1,3)$ ce qui est faux

De plus, les α_i sont tous distincts car φ est injective

On a donc construit une permutation $\alpha : i \mapsto \alpha_i \quad (1 \leq i \leq n)$

et on a sur le système générateur τ_i : $\alpha \tau_i \alpha^{-1} = (\alpha(1), \alpha(i)) = (\alpha_1, \alpha_i)$

ie $i_\alpha(\tau_i) = \varphi(\tau_i)$

les automorphismes i_α et φ coïncident sur les transpositions τ_i pour $2 \leq i \leq n$

et par suite sur $\mathfrak{S}_n$: $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$ □

Lemme 2 :

Si $s \in \mathfrak{S}_n$ est un produit de k transpositions à supports disjoints 2 à 2 (ie $s = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$ où $\tau_1, \tau_2, \dots, \tau_k$ sont des transpositions à supports disjoints 2 à 2 avec $2k \leq n$)

alors si $c(s)$ est le centralisateur de s (ie $c(s) = \{\sigma \in \mathfrak{S}_n \,/\, \sigma s = s \sigma\}$

$$|c(s)| = 2^k k! (n-2k)!$$

□ $\sigma \in c(s)$ si $\sigma s \sigma^{-1} = s$

On sait que $\sigma s \sigma^{-1} = (\sigma \tau_1 \sigma^{-1}) \circ \dots \circ (\sigma \tau_k \sigma^{-1})$

où les $\sigma \tau_i \sigma^{-1}$ sont des transpositions à supports disjoints

ie $(\sigma \tau_1 \sigma^{-1}) \circ \dots \circ (\sigma \tau_k \sigma^{-1}) = \tau_1 \circ \dots \circ \tau_k$

- Par unicité de la décomposition en produits de cycles à supports disjoints, on en déduit que les $\sigma \tau_i \sigma^{-1}$ doivent s'obtenir par permutation des τ_i.

Il y a donc $k!$ possibilités.

- Soit une telle permutation des transpositions fixée et par exple une transposition (a,b) qui est envoyée sur (a',b') : $(a',b') = \sigma(a,b)\sigma^{-1}$

$= (\sigma(a), \sigma(b))$

ie $\{\sigma(a), \sigma(b)\} = \{a', b'\}$

Soit 2 possibilités pr définir σ sur l'ensble $\{a,b\}$ sachant que cet ensemble est envoyé sur $\{a',b'\}$.

_Enfin, il reste à déterminer σ sur les éléments qui n'appartiennent pas au support d'une des transpositions τ_i : pour ces $(n-2k)$ éléments, il y a $(n-2k)!$ choix possibles.

Au total, il y a $2^k k!(n-k)!$ permutations qui commutent avec s $\square$

Preuve du th :

$\square$ $\varphi \in Aut(\mathfrak{S}_n)$

Si τ est une transposition, $\varphi(\tau)$ est d'ordre 2 (car l'automorphisme conserve l'ordre d'un élément)

donc $\varphi(\tau)$ est le produit de k transpositions disjointes.

Par ailleurs, on a $\varphi(c(\tau)) = c(\varphi(\tau))$

(le centralisateur d'une transposition est transformé en celui de $\varphi(\tau)$ par φ)

et donc $|c(\tau)| = |c(\varphi(\tau))|$

$$\underset{(\text{lemme } 2)}{\Longrightarrow} \quad 2(n-2)! = 2^k k!(n-2k)!$$

Comme $n \neq 6$, on a $k = 1$: φ envoie les transpositions sur les transpositions

$$\underset{(\text{lemme } 1)}{\Longrightarrow} \quad \varphi \in Int(\mathfrak{S}_n) \quad \square$$