[UBm]

Cadre : On se placera avec E un ensemble fini

I) Groupe des permutations

1) Définitions et premières propriétés

def 1 Une bijection de E sur lui-même est appelée permutation
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

def 3 On note $\mathfrak{S}_n$ le groupe symétrique de $[\![1,n]\!]$.
On dit que $\mathfrak{S}_n$ est le groupe symétrique de degré n

rem 4 Si $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$
$\forall i \in [\![1,n]\!], \sigma, \rho \in \mathfrak{S}_n, \sigma\rho(i) = \sigma(\rho(i))$

ex 5 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ la permutation de $\mathfrak{S}_3$ laissant pour seul point fixe 3

$\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

prop 6 $\mathcal{Z}(\mathfrak{S}_n)$ est trivial pour $n \geq 3$, donc en particulier $\mathfrak{S}_n$ n'est pas abélien pour $n \geq 3$.

ex 7 $\sigma\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\rho\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \sigma\rho$

Prop 8 $\boxed{|\mathfrak{S}_n| = n!}$

thm 9 On a équivalence bijective entre
- une action de groupe de G sur E
- les morphismes $\delta : G \to \mathfrak{S}_E$

on appelle le morphisme $\varphi : G \to \mathfrak{S}_E$, $g \mapsto \sigma_g : x \mapsto g.x$ le morphisme structurel de l'action de G sur E.

thm 10 [de Cayley] Tout groupe fini G d'ordre $n \in \mathbb{N}$ est isomorphe à un sous-groupe transitif de $\mathfrak{S}_n$

prop 12 $\mathfrak{S}_m \hookrightarrow \mathfrak{S}_n$ pour $m \leq n$ car $\bigcap_{i=m+1}^{n} \mathrm{Stab}_{\mathfrak{S}_n}(i) \cong \mathfrak{S}_m$

ex 13/rem Le morphisme injectif est donné par :
$$\begin{pmatrix} 1 & 2 & \cdots & m \\ \sigma(1) & \sigma(2) & \cdots & \sigma(m) \end{pmatrix} \mapsto \begin{pmatrix} 1 & \cdots & m & m+1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(m) & m+1 & \cdots & n \end{pmatrix}$$

2) Orbites, cycles et supports

def 14 Soient $n \in \mathbb{N}$ et $\sigma \in \mathfrak{S}_n$, on définit :
1) Les points fixes de σ comme les éléments $i \in [\![1,n]\!]$ tq $\sigma(i) = i$
2) Le support de σ l'ensemble $[\![1,n]\!]$ privé des points fixes de σ
Notation : **Supp(σ)**
3) une partie A de $[\![1,n]\!]$ est stable par la permutation σ si son image $\sigma(A)$ est contenue dans A

ex 15 $\sigma = (1\,2) \in \mathfrak{S}_3$, parties stables (1,2), (3)
points fixes (3) Supp(σ) = (1,2)

prop 16 Soient $n \in \mathbb{N}$ et $\sigma, \rho \in \mathfrak{S}_n$
- $\mathrm{Supp}(\sigma\rho) \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$
- Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\rho) = \emptyset$, alors $\mathrm{Supp}(\sigma\rho) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\rho)$

ex 17

prop 18 Si $\mathrm{Supp}(\rho) \cap \mathrm{Supp}(\sigma) = \emptyset$, alors :
1) $\sigma\rho(i) = \begin{cases} \sigma(i) & \text{si } i \in \mathrm{Supp}(\sigma) \\ \rho(i) & \text{si } i \in \mathrm{Supp}(\rho) \end{cases}$ 2) Les permutations à supports disjoints commutent : $\sigma\rho = \rho\sigma$

3) Si $\sigma\rho = e$ alors $\rho = \sigma = \epsilon$

c-ex alg $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ et $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

def 20 - Cycles et transpositions
Soient $p \in \mathbb{N}^*$, $i_1, \dots, i_p \in [\![1,n]\!]$ 2 à 2 distincts, la permutation $\gamma \in \mathfrak{S}_n$ par :

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_p\} \\ i_{k+1} & \text{si } j = i_k,\ k < p \\ i_1 & \text{si } j = i_p \end{cases}$$

$(i_1, \dots, i_p)$ est appelé cycle de longueur p.

cas de cycle de longueur 2 : on les appelle transposition

rem 21 on peut représenter les cycles par des circuits, par ex :

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$:

$1 \xrightarrow{\gamma} 5 \xrightarrow{\gamma} 2 \xrightarrow{\gamma} 3$

thm 22 Toute permutation $\sigma \in \mathfrak{S}_n$ peut s'écrire comme produit de cycles : $\sigma = \gamma_1 \dots \gamma_m$, où γ_i est de longueur ≥ 2 et lorsque $\mathrm{Supp}\,\gamma_i \cap \mathrm{Supp}\,\gamma_j = \emptyset$ $\forall i \neq j$

rem 23
- Les supports de (γ_i) correspondent aux orbites de l'act° $\langle\sigma\rangle \hookrightarrow \mathfrak{S}_n$
- cette décomposition est unique à l'ordre près

ex 24 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1,6)(2,4,7)(3)(5) = (3)(7,2,4)(5)(6,1)$

def 25 Soit $n \in \mathbb{N}$, on appelle type d'une permutation $\sigma \in \mathfrak{S}_n$, noté $[p_1, \dots, p_m]$, la liste p_i où les p_i sont les cardinaux des orbites dans $[\![1,n]\!]$ de l'action $\langle\sigma\rangle \hookrightarrow \mathfrak{S}_n$ rangé dans l'ordre croissant

ex 26 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix} \in \mathfrak{S}_6$, $\sigma = (1,2,4)(3,5)$

type : $[1,2,3]$

def 27 Soit $\sigma \in \mathfrak{S}_n$ de type $[p_1, \dots, p_m]$ a pour ordre $\mathrm{ppcm}(p_1, \dots, p_m)$

ex 27 Plus précédent : ordre 6

prop 28 Soit $n \in \mathbb{N}$, tout cycle $(i_1, \dots, i_p)$ d'ordre p est produit de $(p-1)$ transpositions

[Examen]

3) Signature et groupe alterné

def 29 Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$.
La signature de σ est définie par $\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$

ex 30 $\sigma = (12) \in \mathfrak{S}_3$
$\varepsilon(\sigma) = \frac{2-1}{1-2} = -1$

prop 31
$\varepsilon : \mathfrak{S}_n \to (\mathbb{Q}^*, \cdot)$ est un morphisme de groupes.

prop 32
1) Si σ est une transposition $\varepsilon(\sigma) = -1$
2) $\sigma \in \mathfrak{S}_n$ se décompose en produit de transpositions et si $\ell(\sigma)$ désigne ce nombre.
$$\varepsilon(\sigma) = (-1)^{\ell(\sigma)}$$
3) Si $\sigma \in \mathfrak{S}_n$ est de type $[p_1, \dots, p_m]$,
$$\varepsilon(\sigma) = (-1)^{p_1 - 1} \cdots (-1)^{p_m - 1} = (-1)^{p_1 + \cdots + p_m}$$

ex 33 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 1 & 3 & 6 \end{pmatrix}$ est de signature 1 : calculs plus simples via prop 31.

cor 34 $\varepsilon(\mathfrak{S}_n) = \{-1, 1\}$, ε est donc surjective de $\mathfrak{S}_n$ dans $\{-1,1\}$, sous-groupe de $(\mathbb{Q}^*, \cdot)$

def 35 Soit $n \in \mathbb{N}$, une permutation est dite :
- paire si elle se décompose en un nombre pair de transpositions
- impaire sinon

def 36 Le noyau du morphisme $\varepsilon : \mathfrak{S}_n \to \{-1,1\}$ est un sous-groupe distingué de $\mathfrak{S}_n$. On le note $\mathfrak{A}_n$ et ce groupe s'appelle le groupe alterné.

prop 37 $\forall n \ge 2$, $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$, $|\mathfrak{A}_n| = n!/2$.

ex 38 : Le groupe $\mathfrak{A}_4$ est d'ordre 12. $\mathfrak{A}_4 = \{e, (12)(34), (13)(24), (14)(23), (132), (123), (124), (142), (134), (143), (234), (243)\}$

app° 39 : Frobenius-Zolotarev
Soit $p \in \mathbb{N}$ premier impair, V un $\mathbb{F}_p$-ev de dimension finie
$$\forall u \in GL(V), \quad \varepsilon(u) = \left(\frac{\det(u)}{p}\right).$$

[OA]

[uGm]

II Structure de $\mathfrak{S}_n$ et de $\mathfrak{A}_n$

1) Classes de conjugaison : un outil nécessaire

prop 40. Soient $\sigma, \rho \in \mathfrak{S}_n$.
σ et ρ sont conjuguées dans $\mathfrak{S}_n$ ssi elles sont de même type
- $\forall \omega \in \mathfrak{S}_n$, $\forall (i_1, \dots, i_p) \in \mathfrak{S}_n$
$$\omega(i_1, \dots, i_p)\omega^{-1} = (\omega(i_1), \dots, \omega(i_p))$$

ex 41 Partition de $\mathfrak{S}_4$: types possibles
$|\mathfrak{S}_4| = 1 + 3 + 6 + 6 + 8 = 24$.

$[1,1,1,1]$	(id)
$[1,1,2]$	(transpositions)
$[2,2]$	(double transp°)
$[1,3]$	(3-cycles)
$[4]$	(4 cycles).

ex 42 $\sigma = (163)(24)$ et $\beta(14)(235)$ sont conjugués dans $\mathfrak{S}_6$.

2) Générateurs de $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

prop 43 Si $n \in \mathbb{N}^*$, $\mathfrak{S}_n$ est engendré par :
i) les transpositions
ou ii) de la forme $(1,i)$ $2 \le i \le n$
iii) $(1,2)$ et le n-cycle $(1, \dots, n)$.

rem 44 $(i_1, \dots, i_p) = (i_1, i_2)(i_2, i_3) \cdots (i_{p-1}, i_p)$
$(i, j) = (1, i)(1, j)(1, i)$

ex 45 $\tau = (4,1,5,3) = (4,1)(1,5)(5,3)$

prop 44. Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.
En particulier, $\mathfrak{A}_n$ est engendré par les 3-cycles de la forme $(1, i, j)$ avec $2 < i \ne j \le n$.

Lem 45 [Thm de Sylow] Soit G un groupe, $|G| = p^\alpha m$, $p \nmid m$.
1) Si $H \le G$ est un p-groupe, alors il existe un p-Sylow S avec $H \subset S$.
2) Les p-Sylow sont tous conjugués (et de leur nb diviseur de m)
3) $k \equiv 1 [p]$.

Thm 46 [Dev] $\mathfrak{A}_n$ est simple pour $n \ge 5$.
c-ex 46 $\mathfrak{A}_2$ est trivial $\mathfrak{A}_4$ admet le groupe de Klein comme sous-groupe distingué $\mathfrak{A}_3$ est simple

Thm 47 Pour $n \ne 6$, $\mathrm{Aut}\,\mathfrak{S}_n = \mathrm{Int}\,\mathfrak{S}_n$
[DEV]

[uGm] [Jeanmaret] [Per] [Per] [Per]

III Applications aux autres domaines/outils [Caldero]

1) déterminant

def 48 Soit $A = (a_{ij})_{(i,j)\in[\![1,m]\!]^2}$, on définit le déterminant de A :

$$\det(A) = \sum_{\sigma\in\mathfrak{S}_m} \varepsilon(\sigma)\, a_{\sigma(1),1}\cdots a_{\sigma(m),m}.$$

app 49 (formule de Sarrus)

$$\det(A) = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33}$$

voir annexe

app°50 Soit E un k-ev de dim° m et $f : E^m \to k$ telle que :
1) f est multilinéaire, alternée
2) $f(v_1,\dots,\lambda v_i + \mu w_i,\dots,v_m) = \lambda f(v_1,\dots,v_i,\dots,v_m) + \mu f(v_1,\dots,w_i,\dots,v_m)$
3) $f(v_1,\dots,v_i,\dots,v_i,\dots,v_m) = 0$.

Soit $(e_i)_i$ une base de E, $(v_1,\dots,v_m)$ m vecteurs de E.

$$f(v_1,\dots,v_m) = \det\|v_1,\dots,v_m\|_{(e_i)} f(e_1,\dots,e_m)$$

prop 51 $\forall A\in M_m(k)$, $\det(A) = \det({}^tA)$

rem 52 Le det est l'unique forme m-linéaire alternée valant 1.

ex 53 de det : déterminant de Vandermonde

$$\begin{vmatrix} 1 & a_1 & \cdots & a_1^{m-1} \\ & & & \\ 1 & a_m & \cdots & a_m^{m-1} \end{vmatrix} = \prod_{1\le i<j\le m} (a_j - a_i)$$

2) Polynômes symétriques [RDO] [Gou] Soit A un anneau commutatif unitaire [Gou]

def 54 Un polynome $P\in A[X_1,\dots,X_m]$ est symétrique si $\forall \sigma\in\mathfrak{S}_m$, $P(X_{\sigma(1)},\dots,X_{\sigma(m)}) = P(X_1,\dots,X_m)$

ex 55 $P = XY + YZ + ZX$ dans $\mathbb{R}[X,Y,Z]$

rem 56 Soit $\sigma\in\mathfrak{S}_m$,

$$\varphi_\sigma : A[X_1,\dots,X_m] \to A[X_1,\dots,X_m] \quad \text{où } \sigma(P)(X_1,\dots,X_m) = P(X_{\sigma(1)},\dots,X_{\sigma(m)})$$
$$P \mapsto \sigma(P)$$

est un automorphisme d'algèbre.

def-thm 57 $\forall\, 1\le p\le m$, dans $A[X_1,\dots,X_m]$ les m polynômes Σ_p,

$$\Sigma_p = \sum_{1\le i_1<\cdots<i_p\le m} X_{i_1}\cdots X_{i_p}$$

sont symétriques et on les appelle polynômes symétriques élémentaires

ex 58 $\Sigma_1 = X_1 + \cdots + X_m$, $\Sigma_m = X_1\cdots X_m$

def 59 Soit $P\in\mathbb{N}$, $P = \sum_{(a_i)_i\in\mathbb{N}^m} \in A[X_1,\dots,X_m]$ est P-homogène si $|a| \ne P \Rightarrow a_i = 0$

ex 60 Σ_p est P-homogène et (de degré partiel 1 par rapport à chacune de ses variables)

[RDO]

prop 61 Les polynomes Σ_p vérifient l'égalité (pour $1\le p\le m$) :

$$\prod_{i=1}^{m}(T - X_i) = T^m + \sum_{i=1}^{m} (-1)^i \Sigma_i\, T^{m-i} \quad \text{dans } A[X_1,\dots,X_m,T]$$

app°62 Si $P = \sum_{i=1}^{m} a_i X^{m-i} + a_m \in \mathbb{K}[X]$, scindé sur $\mathbb{K}[X]$, de racines $u_1,\dots,u_m$, alors

$$\forall\, 1\le i\le m \quad (-1)^i a_i = \Sigma_i(u_1,\dots,u_m)$$

thm 63 Soit $P\in A[X_1,\dots,X_m]$ un polynôme symétrique dans $A[X_1,\dots,X_m]$
$\exists!\, \Phi\in A[X_1,\dots,X_m]$ tel que $P = \Phi(\Sigma_1,\dots,\Sigma_m)$

ex 64 $\sum X_i^2 = \Sigma_1^2 - 2\Sigma_2$, $\sum X_i^2 X_2 = \Sigma_1\Sigma_2 - 3\Sigma_3$

3)

def 65 dans $\mathbb{R}^3$ on appelle solide platonicien un polyèdre de dimension 3 (d'intérieur non vide) régulier (face id et régulières) et convexe.

Soit $\mathcal{E}$ un espace affine de dimension 3

prop 66 Soit S un solide de $\mathbb{R}^3$ (barycentriquement centré à l'origine)
$\mathrm{Isom}(S)$ est le sous-groupe d'$\mathrm{Isom}(\mathbb{R}^3)$ des isométries préservant S
Not° : $\mathrm{Isom}^+(S)$, $\mathrm{Isom}^-(S)$ les isométries directes et indirectes
(idem pour $\mathrm{Isom}(\mathbb{R}^3)$)

thm 67 [Admis]
Il est à isométrie et homothétie près de $\mathbb{R}^3$ cinq polyèdres réguliers convexes : le tétraèdre P_4, le cube P_6, l'octaèdre P_8, le dodécaèdre P_{12}, et l'icosaèdre P_{20}.
(voir annexe)

prop 68

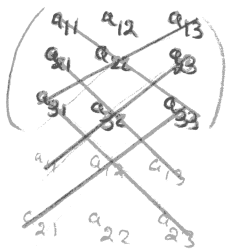
Solide	Isom^+	Isom
P_4	$\mathcal{A}_4$	$\mathfrak{S}_4$
P_6	$\mathfrak{S}_4$	$\mathfrak{S}_4\times\mathbb{Z}/2\mathbb{Z}$
P_8	$\mathfrak{S}_4$	$\mathfrak{S}_4\times\mathbb{Z}/2\mathbb{Z}$
P_{12}	$\mathcal{A}_5$	$\mathcal{A}_5\times\mathbb{Z}/2\mathbb{Z}$
P_{20}	$\mathcal{A}_5$	$\mathcal{A}_5\times\mathbb{Z}/2\mathbb{Z}$

prop 69 / app°69 : dénombrement des colorations possibles du cube à isométries près, pour p couleurs
Pour $p=3$, on en a 57

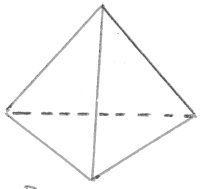
[Gou]

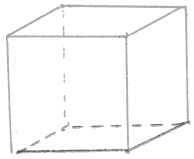
Annexe

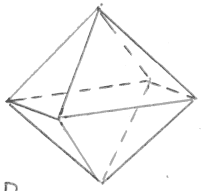
1) Formule de Sarrus

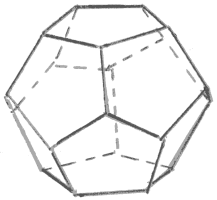


2) Solides de Platon


P_4

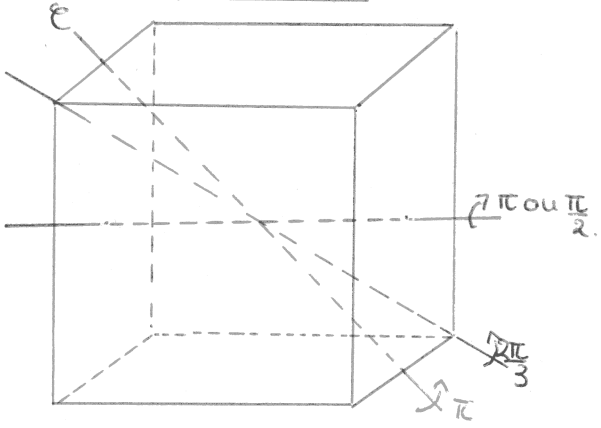

P_6


P_8


P_{12}

P_{20} : faces △

3) Isométries du cube



Références

- [UBm] : Felix Ulmer, Théorie des groupes
- [OA] : Objectif agrégation, Beck.
- [Jeanmeret] : Invitation à l'algèbre, Alain Jeanmeret, Daniel Lime
- [Per] : Cours d'algèbre, Daniel Perrin
- [Gri] : Algèbre linéaire, Joseph Grifone
- [Cocu] : Algèbre 2nd ed, Gourdon
- [RDO] : Alg 1, Ramis - Deschamps - Odoux.

Emily CLEMENT
Julien Gabet

Automorphismes intérieur de $\mathfrak{S}_n$

Emily Clement

7 février 2017

Référence :

— *Cours d'algèbre* de Daniel Perrin

Proposition .1

Pour $n \neq 6$, $Aut\mathfrak{S}_n = Int\mathfrak{S}_n$

Pour rappelle, si on a un groupe G, on définit les automorphismes intérieurs de G par :

$$\mathrm{Int}G = \left\{ i_g : \ x \ \mapsto \ gxg^{-1} \ ; g \in G \right\}$$

L'inclusion $\supseteq$ est donc évidente.
Pour l'inclusion inverse, on va procéder par deux étapes :

Étape 1 : On montre que si un automorphisme de $\mathfrak{S}_n$ transforme les transpositions en transpositions, alors il est intérieur.

Étape 2 : On montre que c'est le cas pour tout automorphisme de $\mathfrak{S}_n$ en caractérisant les transpositions : elles sont d'ordre 2, mais ce ne sont pas les seules...

Démonstration de $\subseteq$: :

Étape 1 **: Un petit lemme** : Soit $\varphi \in \mathrm{Aut}\mathfrak{S}_n$, tel que φ transforme les transpositions en transpositions.
Or, $\mathfrak{S}$ est engendré par les transpositions de la forme $(1i)$ donc on peut se restreindre aux transpositions de cette formes, notons les :

$$\tau_i = (1i) \, , \forall i \geqslant 2$$

Par **hypothèse**, pour tout $i \geqslant 2$, $\varphi(\tau_i)$ est une transposition.
Or, $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne commutent par pour tout $i \neq j$, car comme φ est un morphisme injectif, si elle commuteraient, $\tau_i = (1i)$ et $\tau_j = (1j)$ commuteraient, ce qui est exclut par simple calcul.
Donc $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ne sont pas disjointes (sinon elles commuteraient), elles ont toutes deux à deux un seul éléments de leur support commun :
Posons $\varphi(\tau_2) = (\alpha_1\alpha_2)$ et alors $\varphi(\alpha_1\alpha_3)$, où $(\alpha_1, \cdots, \alpha_n) = \{1, \cdots, n\}$.
Alors $\varphi(\tau_i) = (\alpha_1, \alpha_i)$ pour $i \geqslant 3$ car si on avait $\varphi(\tau_i) = (\alpha_2, \alpha_3)$ par exemple, on aurait alors :

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

Autrement dit :

$$\varphi(\tau_2)\varphi(\tau_3)\varphi(\tau_1) = \varphi(\tau_3)$$

en regroupant à gauche dans φ car c'est un morphisme et en appliquant à gauche φ^{-1} (c'est un automorphisme), on a $\tau_2\tau_3\tau_i = \tau_3$ ce qui donne :

$$(12)\,(13)\,(1i) = (13)$$

Ce qui est exclut.
De plus, les α_i sont distincts $\forall i$, par injectivité de $\varphi : \varphi(\tau_i) = (\alpha_1, \alpha_i)$, $\forall i \geqslant 2$
On pose : $\alpha = \begin{pmatrix} 1 & \cdots & n \\ \alpha_1 & \cdots & \alpha_n \end{pmatrix}$ et comme :

$$\alpha \underbrace{\tau_i}_{(1i)} \alpha^{-1} = (\alpha(1)\,\alpha(i))$$

Alors : φ et i_α coïncident sur les τ_i, qui engendrent $\mathfrak{S}_n$, donc sur $\mathfrak{S}_n$.
Donc :

$$\varphi = i_\alpha \in \mathrm{Int}(\mathfrak{S}_n)$$

Étape 2 :
φ est un automorphisme, donc envoie un élément d'ordre 2 sur un éléments d'ordre 2.
Les transpositions..ne sont cependant pas les seuls éléments d'ordre 2, il y a pas exemple ceux de la formes $(ab)\,(cd)$...
On va s'intéresser au centralisateur :

$$C(s) = \left\{g \in \mathfrak{S}_n, gsg^{-1} = s\right\}$$

Lemme .1

Soit $s \in \mathfrak{S}_n$, on suppose $n = \sum_{i=1}^{n} ik_i$ et que s est le produit de $k_1 + \cdots + k_n$ cycles disjoints : k_1 cycles d'ordre 1, ..., k_n cycles d'ordre n.
Alors :

$$|c(s)| = \prod_{i=1}^{n} k_i! i^{k_i}$$

Si τ est une transposition, $\varphi(\tau)$ est d'ordre 2 donc comme $\varphi(\tau) \in \mathfrak{S}_n$ il est décomposition en produit de k transposition, et comme i lest d'ordre 2, elles sont disjointes.
Ici, $\varphi(c(\tau)) = c(\varphi(\tau))$ car φ est injective et un morphisme, d'où l'égalité :

$$|c(\tau)| = |c(\varphi(\tau_i))|$$

Ici par rapport au lemme, pour τ : $n = 2k_2 + k_1$ et $k = 1$ et $k_2 = n - 2$ donc :

$$\begin{aligned} |c(\tau)| &= \left((n-2)!1^1\right) \cdot \left(1!2^1\right) \\ &= 2\,(n-2)! \end{aligned}$$

Pour $\varphi(\tau)$: $n = k + 1 + 2k$ car on a k transpositions disjointes.

$$\begin{aligned} |c(\varphi(\tau))| &= (n-2k)!1^{(n-2k)} \cdot k!2^k \\ &= 2^k k!\,(n-2k)! \end{aligned}$$

Donc :

$$2\,(n-2)! = 2^k k!\,(n-2k)!$$

Donc $k = 1$ sauf pour $n \neq 6$
Donc $\varphi(\tau)$ est le produit...d'une seule transposition..donc c'est une transposition !
Pour par l'étape 1, comme φ envoie toutes les transpositions sur les transpositions, on a montré que les automorphisme de $\mathfrak{S}_n$ sont tous intérieur, sauf peut-être pour $n = 6$. ■

Simplicité du groupe alterné

Emily Clement

7 février 2017

Référence : Perrin, Cours d'algèbre, page 28-29

simplicité du groupes alterné $\mathfrak{A}_n$

Proposition .1

Le groupe $\mathfrak{A}_n$ est simple pour $n \geqslant 5$

Corollaire .1

Pour $n \geqslant 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}, \mathfrak{A}_n, \mathfrak{S}_n$

Interêt dans la leçon 103 : on a un bon exemple de groupe simple
Question à se poser : et en dessous de 5 ?
Quelques rappels bêtes mais importants :

Définition .1

$\mathfrak{S}_n$ *est le groupe des permutations de l'ensemble* $[\![1, n]\!]$
un k-cycle est une permutation particulière $\sigma = (a_1, \cdots, a_k)$, $a_i \in [\![1, n]\!]$, *où* $\sigma(a_i) = a_{i+1}$
Pour $k = 2$ *on parle de transpositions.*
$\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ *le morphisme signature tel que* $\varepsilon(\sigma) = (-1)^{k+1}$ *pour un* $k-$*cycle.*
On note $\mathfrak{A}_n = \ker(\varepsilon) = \varepsilon^{-1}(1)$ *le groupe des permutations* ***paires****.* $|\mathfrak{A}_n| = \dfrac{n!}{2} = |\mathfrak{S}_n|/2$

Cas $n = 5$: $\mathfrak{A}_5$ est simple.

Démonstration Démonstration du théorème :

$\#\mathfrak{A}_5 = \dfrac{5!}{2} = 60$.

Dénombrons les éléments de $\mathfrak{A}_5$: On peut dénombrer le nombre de $k-$cycle dans $\mathfrak{S}_n$ comme $\binom{n}{k}(k-1)!$:

— Le neutre, Id : 1 élément
— 3 cycles : on en a 20
— 5 cycles : on en a $\binom{5}{5}4! = 24$

— double transpositions à support disjoints, qui sont d'ordre 2 : on a $\binom{5}{2} = 10$ possibilités pour la première transposition, puis $\binom{5}{3} = 3$ possibilités.

Soit un total de 30 choix si on prend l'ordre en compte, mais les transposition commutent $*^0$ donc on a en fait 15 choix.

On a dénombrer ainsi tous les éléments de $\mathfrak{A}_5$. Soit $H \lhd G$ un sous-groupe distingué de G, non trivial.

On invoque le lemme suivant :

Lemme .1

Si $\sigma \in \mathfrak{S}_n$, est un cycle d'ordre p, $\sigma = (a_1, \cdots, a_p)$ et si $\tau \in \mathfrak{S}_n$, on a :

$$\tau\sigma\tau^{-1} = (\tau(a_1), \cdots, \tau(a_n))$$

Démonstration :

Si $x \notin \{\tau(a_1), \cdots, \tau(a_n)\}$, $\tau^{-1}(x) \notin \{a_1, \cdots, a_p\}$ et donc :

$$\tau\sigma\tau^{-1}(x) = \tau\tau^{-1}(x) = x$$

Si $x = \tau(a_i)$, $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$ ■

Il suffit, si on prend (i, j, k) et (i', j', k') :

$$\sigma(i, j, k)\sigma^{-1} = (\sigma(i), \sigma(j), \sigma(k))$$

Donc, :

— Si H contient un élément d'ordre 3, ils le contient tous.

— Si H contient un éléments d'ordre 5, il contient le 5-Sylow engendré par cet élément, donc tous les 5-sous-Sylow (ils sont conjugués), donc tous les éléments d'ordre 5. (1)

H est un sous-groupe de G donc par Lagrange, $|H|\,|60 = |\mathfrak{A}_5|$.

On énumère les possibilités :

1. H contient les doubles transpositions : $16 = 15 + 1$ (on compte le neutre) ne divise pas 60
2. H contient les $3-$cycles : $20 + 1 \nmid 60$
3. H contient les 5-cycles : $24 + 1 = 25 \nmid 60$

Donc H contient au moins deux des trois types de permutations : $|H| \geqslant 1 + 15 + 20 = 36$ donc $|H| = 60$.

Donc $H = \mathfrak{A}_5$

Remarque .1

Pour (1) *on invoque le théorème de Sylow : (5.7 dans Perrin) :*

Théorème .1 (Théorème de Sylow)

Soit G un groupe de cardinal $|G| = p^\alpha m$, $p \nmid m$

1. *Si $H \leqslant G$, qui est un $p-$groupe, il existe un $p-$Sylow, S, avec $H \subset S$*
2. *Les $p-$Sylow sont tous conjugués (et donc leur nombre k divise n)*
3. *$k \equiv 1 \mod p$*

■

Remarque : une version plus poussés pour l'histoire des 3−cycles conjugués :
On utilisera pour cette démonstration les lemmes suivants :

Lemme .2

Si $n \geqslant 5$:
Le groupe $\mathfrak{A}_n$ est $n-2$ fois transitif sur $[\![1,n]\!]$: si on a $a_1, \cdots, a_{n-2}$ distincts et $b_1, \cdots, b_{n-2}$ distincts, $\exists \sigma \in \mathfrak{A}_n$ tel que :

$$\sigma(a_i) b_i$$

Démonstration :
Il suffit d'écrire $\{1, \cdots, n\} = \{a_1, \cdots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, \cdots, b_{n-2}, b_{n-1}, b_n\}$
et on pose σ telle que $\sigma(a_i) = b_i$
Si σ est paire : Ok
Sinon, on prend $\sigma \circ (a_{n-1}, a_n)$ ■

Dont le corollaire nous sera utile :

Corollaire .2

Si $n \geqslant 5$, les cycles d'ordre 3 sont conjugués dans $\mathfrak{A}_n$

Démonstration :
Soit $\sigma \in \mathfrak{S}_n$ ■

Cas général $\mathfrak{A}_n$ est simple pour $n \geqslant 5$

Démonstration :
$E := [\![1,n]\!]$, Soit $H \lhd \mathfrak{A}_n$, non trivial.
Soit $\sigma \in H$, $\sigma \neq 1$.
Ramenons nous au cas précédent : Construire une permutation de $\mathfrak{A}_n$ qui ait $n-5$ point fixes. $\sigma \neq 1$ donc $\exists a \in E$, tel que $b = \sigma(a) \neq a$.
Soit $c \in E$ tel que $c \neq a, b, \sigma(b)$.
On pose $\tau = (acb)$ le 3−cycle.
$b = \sigma(a)$ donc $F = \{a, b, c, \sigma a, \sigma b, \sigma c\}$ est de cardinal $\leqslant 5$

$$\rho := \tau\sigma\tau^{-1}\sigma^{-1} = \tau\left(\sigma\tau^{-1}\sigma^{-1}\right)$$

Donc $rho(F) = F$ et $\rho_{E-F} = \mathrm{Id}_{E-F}$
Quitte à rajouter des éléments, supposons $|F| = 5$, $\rho \neq 1$ car $\rho(b) = \tau\sigma(b) \neq b$, car $\sigma(B) \neq \tau^{-1}(b) = c$
Soit $\mathfrak{A}(F)$ l'ensemble des permutations paires de F.
On pose :

$$\begin{array}{ccccc} \mathfrak{A}(F) & \to & & & \mathfrak{A}_n \\ u & \mapsto & \overline{u} : & x & \mapsto \begin{cases} u(x) & \text{si } x \in F \\ x & \text{sinon} \end{cases} \end{array}$$

On a donc $\mathfrak{A}_5 = \mathfrak{A}(F)$
Posons $H_0 := \{u \in \mathfrak{A}(F) \,|\, \overline{u} \in H\} = H \cap \mathfrak{A}(F)$, $H_0 \lhd \mathfrak{A}(F) \simeq \mathfrak{A}_5$.
$\rho_{|F} \in H_0$, $\rho_{|F} \neq \mathrm{Id}_F$
Or $\mathfrak{A}(F) \simeq \mathfrak{A}_5$ est simple, donc $H_0 = \mathfrak{A}(F)$.
Soit u un 3−cycle de $\mathfrak{A}(F)$, donc $u \in H_0$, donc $\overline{u}$ est un 3−cycle dans H, or les 3-cycle sont conjugués dans $\mathfrak{A}_n$, ils sont donc tous dans H.
Or :

Lemme .3

Les 3-cycles engendrent $\mathfrak{A}_n$

On a donc $H = \mathfrak{A}_n$ ■

Remarque .2

Pourquoi les $3-$cycles engendrent $\mathfrak{A}_n$? Cf Perrin.