(Autour de la) Simplicité de $\mathfrak{A}_n$

Notations : $n \geq 2$ $\quad \mathfrak{S}_n = $ bij de $[\![1,n]\!]$ $\quad X \overset{\text{bij}}{\simeq} X' \Rightarrow \mathfrak{S}_X \underset{\text{gpe}}{\overset{\text{isom}}{\simeq}} \mathfrak{S}_{X'}$

$|\mathfrak{S}_n| = n!$

$\gamma, \tau, \sigma, \sigma_1, \sigma_2 \in \mathfrak{S}_n$

- Soit G fini ; l'action (translation à gauche) $\overset{\text{fidèle}}{}$ $\begin{array}{l} G \times G \to G \\ (g,x) \mapsto g.x \end{array}$ induit (correspond à) un morphisme de gpe inj $G \hookrightarrow \mathfrak{S}_G \underset{\text{gpe}}{\overset{\text{isom}}{\simeq}} \mathfrak{S}_{|G|}$

  « les $\mathfrak{S}_n$ contiennent ts les gpes finis »

- Soit K un corps $\quad \begin{array}{l} \mathfrak{S}_n \overset{\text{repr !}}{\longrightarrow} GL_n(K) \\ \sigma \longmapsto (\delta_{i\sigma(j)})_{1 \leq i,j \leq n} \end{array}$ est un morph de gpe inj

  $j = \sigma(i)$

  $\varphi_\sigma(e_i) = e_{\sigma(i)} \qquad \varphi_\tau \circ \varphi_\sigma(e_i) = \varphi_\tau(e_j) = e_{\tau(j)} = e_{\tau\sigma(i)}$

  j

  $i = \sigma(j)$

  $i \ldots$

- Action $\begin{array}{l} \mathfrak{S}_n \times [\![1,n]\!] \longrightarrow [\![1,n]\!] \\ (\sigma, k) \longmapsto \sigma(k) \end{array}$ Toute action sur un ensemble fini est une restriction de cette action.

I Décomposition en produit de cycles à supports disjoints

1 Support, pts fixes, σ-orbites

Déf: $\mathrm{Supp}\,\sigma = \{k \in [\![1,n]\!],\ \sigma(k) \neq k\}$ $\qquad$ $\mathrm{Supp}\,\sigma = \emptyset \Leftrightarrow \sigma = id$ $\qquad$ $|\mathrm{Supp}\,\sigma| = 0$ ou ≥ 2

$\mathrm{Fix}\,\sigma = \{ \qquad = \}$

σ-orbite = orbite pour l'action de $\langle\sigma\rangle$ sur $[\![1,n]\!]$

Notation: $\omega_\sigma(a) = \sigma$-orbite de $a = \{\sigma^k(a),\ k \in \mathbb{Z}\} \subseteq [\![1,n]\!]$ $\qquad$ $\omega_\sigma(a) = \{a\} \Leftrightarrow a \in \mathrm{Fix}\,\sigma$

$\Omega^*_\sigma = \{\sigma$-orbites de card $\geq 2\}$

Rmq: $[\![1,n]\!] = \bigsqcup_{\omega \in \Omega_\sigma} \omega = \mathrm{Fix}\,\sigma \sqcup \bigsqcup_{\omega \in \Omega^*_\sigma} \omega$ $\quad$ $= \mathrm{Supp}\,\sigma$

Propriétés:
(i) $\sigma(\mathrm{Supp}\,\sigma) = \mathrm{Supp}\,\sigma$; $\forall m \in \mathbb{Z}$ $\mathrm{Supp}\,\sigma^m \underset{\neq \text{ possible } m = o(\sigma)}{\subseteq} \mathrm{Supp}\,\sigma$; $\mathrm{Supp}\,\sigma^{-1} = \mathrm{Supp}\,\sigma$

(ii) $\mathrm{Supp}\,\sigma_1\sigma_2 \overset{*}{\subseteq} \mathrm{Supp}\,\sigma_1 \cup \mathrm{Supp}\,\sigma_2$ $\qquad$ $\mathrm{Fix}\,\sigma_1 \cap \mathrm{Fix}\,\sigma_2 \subseteq \mathrm{Fix}\,\sigma_1\sigma_2$

Si $\mathrm{Supp}\,\sigma_1 \cap \mathrm{Supp}\,\sigma_2 = \emptyset$ ⚠ ~~abs~~ $\sigma_1\sigma_2 = \sigma_2\sigma_1$ et * est =

(iii) $\mathrm{Fix}(\tau\sigma\tau^{-1}) = \tau(\mathrm{Fix}\,\sigma)$ $\qquad$ $\mathrm{Supp}(\tau\sigma\tau^{-1}) = \tau(\mathrm{Supp}\,\sigma)$

Analogie géom
Vrai pr tte action de gpe

2 Cycles

Déf: σ est appelé cycle si $\mathrm{Supp}\,\sigma$ est une σ-orbite, ie $\exists$ une unique σ-orbite de card ≥ 2 $\qquad$ ⇗ $\mathrm{Supp}\,\sigma = \emptyset$

Notation: Pr γ cycle $|\mathrm{Supp}\,\gamma|$ est appelé longueur de γ.
Transposition = cycle de longueur 2

$G \curvearrowright X$ $\qquad$ $G/\mathrm{Stab}_G x \xrightarrow{bij} \omega_G(x)$
$gS \longmapsto g\cdot x$

Ex-prop: Soient $\ell \in [\![2,n]\!]$, $a_1,\dots,a_\ell$ ds $[\![1,n]\!]$ 2 à 2 $\neq$
$\exists!\ \gamma \in \mathfrak{S}_n$ tq : $\forall a \in [\![1,n]\!]$ $\gamma(a) = a$; $\forall i \in [\![1,\ell-1]\!]$ $\gamma(a_i) = a_{i+1}$; $\gamma(a_\ell) = a_1$ ✓
γ est un cycle de supp $\{a_1,\dots,a_\ell\}$ noté $(a_1 \dots a_\ell)$

Réciproque

Prop: Soit γ un cycle de longueur ℓ. Pr tt a ds $\mathrm{Supp}\,\gamma$, $\gamma = (a\ \gamma(a) \dots \gamma^{\ell-1}(a))$ et $\ell = |\mathrm{supp}\,\gamma| = o(\gamma)$

⚠ $\exists$ des élts d'ordre ℓ qui ne sont pas des cycles

D] $\mathrm{Supp}\,\gamma \overset{\gamma\text{-cycle},\ a \in \mathrm{Supp}\,\gamma}{=} \omega_\gamma(a) \underset{\sim}{\overset{bij}{\longleftarrow}} \langle\gamma\rangle / \mathrm{Stab}_{\langle\gamma\rangle} a$ $\qquad$ Soit $\sigma \in \mathrm{Stab}_{\langle\gamma\rangle} a$, $\sigma = \gamma^m$, $m \in \mathbb{Z}$ et $\sigma(a) = a$; $\forall b \in \mathrm{Supp}\,\gamma$, $b = \gamma^k(a)$ $k \in \mathbb{Z}$

D'où $\underset{o(\gamma)}{\langle\gamma\rangle} \xrightarrow{bij} \underset{\ell}{\omega_\gamma(a)}$ $\qquad$ et $\sigma(b) = \gamma^m(b) = \gamma^{m+k}(a) = \gamma^k(\gamma^m(a)) = \gamma^k(a) = b$ dc $\sigma = id$

+ on vérifie action de γ sur $\mathrm{Supp}\,\gamma$

Unicité: $(a_1 \dots a_\ell) = (b_1 \dots b_h) \Leftrightarrow h = \ell$ et $\exists k \in [\![1,\ell]\!]$ tq $\begin{cases} b_1 = a_k \quad b_2 = a_{k+1} \dots \quad b_i = a_{k+i-1} & i \in [\![1,\ell-k+1]\!] \\ b_{\ell-(k-1)+1} = a_1,\quad b_i = a_{i-(\ell-k+1)} & i \in [\![\ell-k+2,\ell]\!] \end{cases}$

Prop: (i) Pr $S \subseteq [\![1,n]\!]$ tq $|S| \geq 2$ Nb de cycles de supp S = $(|S|-1)!$ $\quad$ choix du supp

(ii) Pr $\ell \in [\![2,n]\!]$, nb de cycles de longueur $\ell = \dfrac{n(n-1)\dots(n-\ell+1)}{\ell} = \binom{n}{\ell}(\ell-1)!$ $\qquad$ Ex: $\dfrac{n(n-1)}{2}$ transpo

Prop: Soient $\ell \in [\![2,n]\!]$, $a_1, .., a_\ell$ ds $[\![1,n]\!]$ 2 à 2 $\neq$

(i) $(a_1 \dots a_\ell)^{-1} = (a_1\, a_\ell\, a_{\ell-1} \dots a_2)$ cycle de m̂ supp et longueur

(ii)* $\forall \sigma \in \mathfrak{S}_n \quad \sigma(a_1 \dots a_\ell)\sigma^{-1} = (\sigma(a_1)\, \sigma(a_2) \dots \sigma(a_\ell))$

Corollaire: Pr $\ell \in [\![2,n]\!]$, les ℓ-cycles forment une classe de conjugaison ds $\mathfrak{S}_n$ + un ℓ-cycle et son inverse sont conjugués

3 Décomposition en produit de cycles à support disjoints

Thm: Soit $\sigma \in \mathfrak{S}_n$.

(i) Il existe $r \in [\![1,n]\!]$ et $\gamma_1, .., \gamma_r$ cycles à supp. disjoints tq $\sigma = \gamma_1 \cdots \gamma_r$. $r=0 \Leftrightarrow \sigma = id$ + bien déf

(ii) " Unicité à l'ordre près " Soient $r, \gamma_1, .., \gamma_r$ satisfaisant (i). Alors: $[\![1;r]\!] \to \Omega_\sigma^*$, $i \mapsto \operatorname{Supp}\gamma_i$ est une bij°

et: $\forall i \in [\![1,r]\!]$ $\gamma_{i|\operatorname{supp}\gamma_i} = \sigma_{|\operatorname{Supp}\gamma_i}$ stable car σ-orbite

détermine γ_i car $\gamma_i(a) = a$ pr $a \notin \operatorname{Supp}\gamma_i$

(ii') Si $\gamma_1 \dots \gamma_r = \gamma_1' \dots \gamma_{r'}'$, alors $r = r'$ et $\exists \tau \in \mathfrak{S}_r$ tq $\forall i \in [\![1,r]\!]$ $\gamma_i' = \gamma_{\tau(i)}$

D]

Lemme: Soit $\sigma \in \mathfrak{S}_n \setminus \{id\}$ et $\omega \in \Omega_\sigma^*$. On définit σ_ω de $[\![1,n]\!]$ ds $[\![1,n]\!]$ par $\begin{cases} \forall a \in [\![1,n]\!] \setminus \omega & \sigma_\omega(a) = a \\ \forall a \in \omega & \sigma_\omega(a) = \sigma(a) \end{cases}$

Alors σ_ω est (ds $\mathfrak{S}_n$ et) un cycle de longueur $|\omega|$.

Notation:

Pour $\sigma \in \mathfrak{S}_n$, $\ell \in [\![1,n]\!]$, on note $m_\ell(\sigma)$ = nb de $\langle\sigma\rangle$-orbites de card ℓ $\in [\![0,n]\!]$ (profil/type)

On a $\sum_{\ell=1}^{n} \ell\, m_\ell(\sigma) = n$ (partition) et $m_1(\sigma) = |\operatorname{Fix}\sigma|$, $\forall \ell \in [\![2,n]\!]$ $m_\ell(\sigma)$ = nb de cycle de longueur ℓ ds la décomp. de σ en ...

II Conséquences sur la structure de $\mathfrak{S}_n$

1 Ordre : $o(\sigma) = \text{ppcm}\{\ell \in [\![1,n]\!] \,/\, m_\ell(\sigma) \neq 0\}$ = ppcm de la longueur des cycles apparaissant ds σ

⚠ Faux en général : $\gamma_1\gamma_2 = \gamma_2\gamma_1 \Rightarrow o(\gamma_1\gamma_2) = \text{ppcm}(o(\gamma_1), o(\gamma_2))$ mais | tjs vrai

Ici : à la main ou utiliser récurrence + $\langle\gamma_1\rangle \cap \langle\gamma_2\rangle = \{id\}$

$\sigma^m = \gamma_1^m \dots \gamma_r^m$ les supp restent disjoints dc $\forall i \in [\![1,r]\!]$ $\gamma_i^m = id$ dc $o(\gamma_i) | m$

2 Générateurs de $\mathfrak{S}_n$: les familles suivantes engendrent $\mathfrak{S}_n$

(i) les cycles — ∃ DJ directe par réc sur $|\text{Fix}\,\sigma|$

(ii) les transpositions $(a_1 \dots a_\ell) = (a_1 a_2)(a_2 a_3)\dots(a_{\ell-2}\, a_{\ell-1})(a_{\ell-1}\, a_\ell)$

(iii) les transpo $\{(1\, i), i \in [\![2,n]\!]\}$ $(i\,j) = (1\,i)(1\,j)(1\,i)$ Conjugaison !

(iv) les transpo $\{(i\; i{+}1), i \in [\![1,n-1]\!]\}$ $j > i$ $(i\,j) = (i\; i{+}1 \dots j{-}1)(j{-}1\; j)(i\; i{+}1 \dots j{-}1)^{-1}$ $(i\; i{+}1 \dots j{-}1) = (i\; i{+}1)\dots(j{-}2\; j{-}1)$

(v) $\{(1 2), (1 2 \dots n)\}$ $i \in [\![1;n-1]\!]$ $\gamma^{i-1}(12)\gamma^{i-1} = (i\;\; i{+}1)$

Rmq : Ds (v), 2 est le card min (pr $n \geqslant 3$), sinon cyclique

⚠ N'importe quel couple {transpo, n-cycle} ne fonctionne pas Ex $\langle(13), (1234)\rangle \subsetneq \mathfrak{S}_4$ □

3 Conjugaison ds $\mathfrak{S}_n$

Prop : σ_1 et σ_2 conjuguées $\Leftrightarrow \forall \ell \in [\![1,n]\!]$ $m_\ell(\sigma_1) = m_\ell(\sigma_2)$

DJ On construit la transfo conjugante à la main en définissant τ sur les σ-orbites ■

Csq : σ et σ^{-1} sont conjuguées ds $\mathfrak{S}_n$ — Csq : car. de $\mathfrak{S}_n$ réels ; pas vrai pr ts gpes ex : $\mathfrak{A}_4$

Rmq : $\left\{(m_1, \dots, m_n) \in [\![0,n]\!]^n \,/\, \sum_{\ell=1}^{n} \ell m_\ell = n\right\} \longleftarrow \{\text{cl. de conj de } \mathfrak{S}_n\}$ est une bijection (Partitions de n)

$(m_1(\sigma), \dots, m_n(\sigma)) \longleftarrow \sigma$

Interlude : classes de conjugaison et centralisateur

Action par conjugaison : $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$

Orbite = classe de conj de x ($= \mathcal{C}_G(\sigma)$)

Stabilisateur = centralisateur (ou commutant) $= \{g \in G \,/\, gx = xg\}$ — $\bigcap_{\sigma \in G} Z_G(\sigma) = Z(G)$

$G/Z_G(\sigma) \xrightarrow[\sim]{\text{bij}} \omega_G(\sigma)$ dc $\boxed{|\omega_G(\sigma)| = [G : Z_G(\sigma)] \,|\, |G|}$

Prop : $|Z_G(\sigma)| = \prod_{\ell=1}^{n} \left(m_\ell(\sigma)!\, \ell^{m_\ell(\sigma)}\right)$ — donne aussi $|\omega_{\text{conj}}(\sigma)|$ — sert ds $\text{Aut}\,\mathfrak{S}_n$

III Groupe alterné

1 Signature

en fait ds $\mathbb{C}^\times$

Déf - Prop : Il existe un unique morphisme de gpes non trivial (donc surj) de $\mathfrak{S}_n$ ds $\{-1,+1\}$, noté ε. On l'appelle la signature et $\mathfrak{A}_n = \ker \varepsilon$ le groupe alterné (s/s gpe d'indice 2 de $\mathfrak{S}_n$)

permutation paire

Pratique générale : utile pr morph.

DJ Unicité : image (transpo) $\in\{\pm 1\}$, ttes les transpo ont $\hat{m}$ image (car conjuguées) et engendrent $\mathfrak{S}_n$

Existence : le gros morceau $\rightsquigarrow$ difficile $\rightsquigarrow$ à faire une fois ds sa vie

$$\varepsilon(\sigma) = (-1)^s$$ où σ = produit de s transpo — MQ indép de l'écriture, morph OK

$$= \prod_{\substack{(i,j)\in[[1,n]]\\ i<j}} \frac{\sigma(j)-\sigma(i)}{j-i}$$ déf intrinsèque ; MQ $\in\{\pm1\}$ et morph de gpe

$$= (-1)^{n_\sigma} \quad \text{où} \quad n_\sigma = \left|\{(i,j)\in[[1,n]]^2 \,/\, i<j \text{ et } \sigma(j)<\sigma(i)\}\right|$$ idem, sauf $\in\{\pm1\}$ donné

plutôt ppté $= (-1)^{n-|\mathcal{Z}_\sigma|}$ ← en comptant les pts fixes

Rmq - prop :
- $\varepsilon(\ell\text{-cycle}) = (-1)^{\ell-1}$ — décomp° en $\prod$ cycle donne aussi signature
- $\mathfrak{A}_n$ unique s/s-gpe d'indice 2 de $\mathfrak{S}_n$
- $\sigma\in\mathfrak{A}_n \iff \sum_{\substack{\ell\in[[1,n]]\\ \ell \text{ pair}}} m_\ell(\sigma)$ est pair — nb de cycle de longueur paire est pair

2 Générateurs

les familles suivantes engendrent $\mathfrak{A}_n$:

(i) $\{\tau\tau' \,/\, \tau,\tau' \text{ transpo de } \mathfrak{S}_n\}$ s/s condition sur les supports

★ (ii) 3-cycles $\quad (i\,j)(i\,k) = (i\,k\,j) \quad (i\,j)(k\,\ell) = (i\,j)(i\,k)(i\,k)(k\,\ell)$

(iii) pr $n\geq 3$ $\quad \{(1\,i\,j),\ 2\leq i<j\leq n\}$, $\{(1\,2\,i),\ i\in[[3,n]]\}$, $\{(i\ i{+}1\ i{+}2),\ i\in[[1,n-2]]\}$

(iv) $\{\sigma^2,\ \sigma\in\mathfrak{S}_n\}$

3 Conjugaison

Prop : Si $n\geq 5$, les 3-cycles sont conjugués ds $\mathfrak{A}_n$ — Vrai aussi pr bitranspo

DJ Soient γ,γ' des 3-cycles et σ ds $\mathfrak{S}_n$ tq $\gamma'=\sigma\gamma\sigma^{-1}$; si $\sigma\notin\mathfrak{A}_n$, soit τ transpo de supp disj de Supp γ ; alors $\sigma\tau$ convient. ■

Rmq : • $\mathfrak{A}_3 = \{id, (123), (132)\} \simeq \mathbb{Z}/3\mathbb{Z}$ comm dc ω_{conj} = singleton

• ds $\mathfrak{A}_4$, $8 = 4\times 2$ 3-cycles, $8\nmid|\mathfrak{A}_4| = 12$ dc pas conjugués (en fait 2 classes de conj, ordre 4, $\gamma\chi\gamma^{-1}$)

Prop : Soit $\sigma\in\mathfrak{A}_n$; on est dans l'un (et un seul) des deux cas suivants

Dvpt possible, non trivial

(i) $\exists \ell\in[[1,n]]$ tq ℓ pair et $m_\ell(\sigma)\geq 1$ ou $\exists\ell\in[[1,n]]$ tq ℓ impair et $m_\ell(\sigma)\geq 2$; $Z_{\mathfrak{S}_n}(\sigma)\not\subset\mathfrak{A}_n$; $\omega_{\mathfrak{S}_n}(\sigma) = \omega_{\mathfrak{A}_n}(\sigma)$

(ii) $\forall\ell\in[[1,n]]$, si ℓ pair alors $m_\ell(\sigma)=0$ et si ℓ impair alors $m_\ell(\sigma)\in\{0;1\}$; $Z_{\mathfrak{S}_n}(\sigma)\subseteq\mathfrak{A}_n$;
$\forall\tau\in\mathfrak{S}_n\setminus\mathfrak{A}_n \quad \omega_{\mathfrak{S}_n}(\sigma) = \omega_{\mathfrak{A}_n}(\sigma) \amalg \omega_{\mathfrak{A}_n}(\tau\sigma\tau^{-1})$

$\hat{m}$ cardinal

④ Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$

Thm : Si $n \geq 5$, $\mathfrak{A}_n$ est simple

Rmq : $\mathfrak{A}_2 = \{id\}$; $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ simple ; $\mathfrak{A}_4$ non simple

DJ Soit $\{id\} \neq H \trianglelefteq \mathfrak{A}_n$. On veut MQ $H = \mathfrak{A}_n$.

Idée dé : 3-cycles conjugués ds $\mathfrak{A}_n$ et engendrent $\mathfrak{A}_n$ dc, si H contient un 3-cycle, alors $H = \mathfrak{A}_n$ (alors ts car distingué s/s gpe)

Cas $n=5$ $\quad |\mathfrak{A}_5| = 6 = 2^2 \times 3 \times 5$

Éléments de $\mathfrak{A}_5$:

- id $\quad 1 \quad o = 1$
- 3-cycles $\quad \binom{5}{3} \times 2 = 20 \quad o = 3$ conjugués ds $\mathfrak{A}_5$ (choix supp ; 2 à supp fixé)
- bitranspo $\quad 5 \times 3 = 15$ 3 à supp fixé, choix du pt fixe $\quad o = 2$ (conjugués ds $\mathfrak{A}_5$)
- 5 cycles $\quad 4! = 24$ commence par 1, puis choix des suivantes $\quad$ 2 cl. conj, ordre 12 $\quad 24 \not\mid 60$

$H \neq \{id\}$ donc contient él^t non trivial γ

- si $o(\gamma) = 3$ (γ 3-cycle) $H = \mathfrak{A}_5$

- si $o(\gamma) = 2$ $\quad \gamma = (ab)(cd)$ $\quad a, b, c, d$ ds $[\![1,5]\!]$ 2 à 2 $\neq$

  H contient un 3-cycle : soit e ds $[\![1,5]\!] \setminus \{a,b,c,d\}$

  $\tau = (abe) = (ab)(be) = (ab)(cd)(cd)(be)$
  $= (ab)(cd)\,(abe)\,(ab)(cd)(aeb)$
  $= \gamma \tau \gamma^{-1} \tau^{-1} \in H$

  Abs H contient ttes les bitranspo : $\sigma(ab)\sigma^{-1} = (\sigma(a)\,\sigma(b)) = (b\,e)$

  dc $H = \mathfrak{A}_5$

- si $o(\gamma) = 5$ abs $\langle\gamma\rangle \subseteq H$

  Or $\langle\gamma\rangle$ = un 5-Sylow de $\mathfrak{A}_5$

  5-Sylow ts conjugués ds $\mathfrak{A}_5$ + H distingué dc ts les 5-Sylow sont $\subseteq H$

  Tt 5-cycle est $\subseteq$ un 5-Sylow dc H contient 5-cycles

  $24 + 1 = 25 \not\mid 60$ donc $\exists \gamma \in H$ d'ordre 2 ou 3 * dc $H = \mathfrak{A}_5$

  $\boxed{\text{OU}}$ Si on sait : 2 classes de conj ds $\mathfrak{A}_5$, d'ordre 12 $\quad 1+12 \not\mid 60$, $24+1 \not\mid 60$ dc *

  $\boxed{\text{OU}}$ MQ soit γ, γ' d'ordre 5 ds $\mathfrak{A}_5$; γ' est conj. à γ ou γ^2 [main, via (12345)]

  $\langle\gamma\rangle \subseteq H$ distingué dc $\gamma' \in H$

Cas général $n \geq 5$ $\quad$ Idée : se ramener à $\mathfrak{A}_5$ pr 3-cycle $\subseteq H$

Ⓘ MQ $\exists\, \gamma \in H \setminus \{id\}$ tq $|\operatorname{Supp} \gamma| \leq 5$

Astuce du commutateur :
$\sigma\tau\sigma^{-1}\tau^{-1} = \sigma(\tau\sigma^{-1}\tau^{-1}) \in H$
$= (\sigma\tau\sigma^{-1})\tau^{-1}$ $\quad \operatorname{Supp} \subseteq \operatorname{Supp}(\sigma\tau\sigma^{-1}) \cup \operatorname{Supp}\tau^{-1}$
si τ 3-cycle $\qquad \sigma(\operatorname{Supp}\tau) \cup \operatorname{Supp}\tau$
si un pt commun : gagné $\qquad \{\sigma(a), \sigma(b), \sigma(c)\} \cup \{a, b, c\}$

Soit $\sigma \in H \setminus \{id\}$

Soit $a \in [\![1,n]\!]$ tq $\sigma(a) \neq a$

On pose $b = \sigma(a)$ et on fixe $c \in [\![1,n]\!] \setminus \{a, b, \sigma(b)\}$

Pr $\tau = (a\,b\,c)$, on a

$\gamma = [\sigma, \tau] \in H$, $\quad \operatorname{Supp}\gamma \subseteq \{a, b, c, \sigma(b), \sigma(c)\} = S$

$\gamma \neq id$? $\quad \sigma\tau(a) = \sigma(b) \quad \tau\sigma(a) = \tau(b) = c$. On choisit $c \neq \sigma(b)$

II Se ramener à $\mathfrak{A}_5$ pr MQ H contient un 3 cycle

- Soit $X \subseteq [\![1,n]\!]$ tq $S \subseteq X$ et $|X| = 5$
  On pose $\mathfrak{S}_X = \{\sigma \in \mathfrak{S}_n \,/\, \sigma_{|[\![1,n]\!] \setminus X} = id_{[\![1,n]\!] \setminus X}\}$ ie $\mathrm{Supp}\,\sigma \subseteq X$
  $\mathfrak{S}_X$ est un s/s-gpe de $\mathfrak{S}_n$, isom à $\mathfrak{S}_5$ car image du morphisme de gpe inj
  $$\mathfrak{S}_5 \simeq \mathrm{Bij}\,X \longrightarrow \mathfrak{S}_n \qquad \text{bien déf, morph gpe, inj, surj}$$
  $$s \longmapsto \tilde{s} \text{ tq } \tilde{s}_{|X} = s \text{ et } \tilde{s}_{|^cX} = id_{^cX}$$

- On pose $\mathfrak{A}_X = \mathfrak{S}_X \cap \mathfrak{A}_n$
  $\mathfrak{A}_X$ est un s/s gpe de $\mathfrak{S}_X$ d'indice 2 car $\ker$ de $\varepsilon_{|\mathfrak{S}_X} : \mathfrak{S}_X \longrightarrow \{\pm 1\}$ morph. de gpe, surj $\quad (ab) \mapsto -1$
  dc* $\mathfrak{A}_X \simeq \mathfrak{A}_5$, en particulier simple

- Soit $H_X = H \cap \mathfrak{A}_X = H \cap \mathfrak{S}_X$
  H_X est un s/s-gpe distingué de $\mathfrak{A}_X$ (car $H \trianglelefteq \mathfrak{A}_n \supseteq \mathfrak{A}_X$
  $id \neq \gamma \in H_X$
  dc (cas $n=5$) $H_X = \mathfrak{A}_X$

- $H_X = \mathfrak{A}_X \subseteq H$ dc H contient un (ts les) 3-cycles de $\mathfrak{A}_X$ (p.ex τ)
  dc H contient un 3-cycle de $\mathfrak{S}_n$ dc $H = \mathfrak{S}_n$.

■

Rmq $\mathfrak{A}_3$ simple
$\mathfrak{A}_4$ non simple

IV Sous-groupes distingués (général et particulier)

1 Sous-groupes distingués

- $\mathfrak{S}_3$: $\{id\}$ $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$, $\mathfrak{S}_3$ • $\mathfrak{A}_3$: $\{id\}$ $\mathfrak{A}_3$
- $\mathfrak{S}_4$: $\{id\}$ V $\mathfrak{A}_4$ $\mathfrak{S}_4$

$V = \{id, \overset{\tau}{(12)(34)}, \overset{\tau'}{(13)(24)}, \overset{\tau''}{(14)(23)}\}$ $\gamma^2 = id$ $\tau'' = \tau\tau'$, distingué ds $\mathfrak{S}_n$ car V classe conj

Soit $H \triangleleft \mathfrak{S}_4$: $|H| \mid 24$ et $H = \amalg$ classes de conj $\ni id$

Classes de conj	$\{id\}$	(12)	(123)	$(12)(34)$	(1234)
card	1	6	8	3	6

Div de 24	1	2	4	8	3	6	12	24
	$\{id\}$	×	✓	×	×	×	$\mathfrak{A}_4$	$\mathfrak{S}_4$

Si $|H| = 4$ $H = V$ (seule possé)

- $\mathfrak{A}_4$: $\{id\}$ V $\mathfrak{A}_4$

Cl. conj	$\{id\}$	$(12)(34)$	(123)	(132)
	1	3	4	4

$\underbrace{3 \quad 4 \quad 4}_{\text{à vérifier}}$

Div	1	2	4	3	6	12
	$\{id\}$	×	✓	×	×	$\mathfrak{A}_4$

- Si $n \geq 5$ $\mathfrak{A}_n$: $\{id\}$ $\mathfrak{A}_n$

$\mathfrak{S}_n$: $\{id\}$ $\mathfrak{A}_n$, $\mathfrak{S}_n$ $H \cap \mathfrak{A}_n = \{id\}$ ou $\mathfrak{A}_n$ $= \ker \varepsilon_{|H}$ ↗ $\mathfrak{A}_n \subseteq H$ de $[\mathfrak{S}_n : H] = 1$ ou 2 ↗ $\mathfrak{S}_n$ ↗ $\mathfrak{A}_n$

$\hookrightarrow$ $\varepsilon_{|H} : H \hookrightarrow \{\pm 1\}$ si $|H| = 2$ alors $H = \{id, \sigma\}$ $H \trianglelefteq \mathfrak{S}_n \Rightarrow \sigma \in Z(\mathfrak{S}_n)$ * $\lightning$ $\overset{\shortparallel}{\{id\}}$

* énoncé + tard mais démontrable avant

Exo : $H \leqslant \mathfrak{S}_n$, $[\mathfrak{S}_n : H] = n \Rightarrow H \simeq \mathfrak{S}_{n-1}$ ⚠ Pas tjrs = Stab k (ok si $n \neq 6$) Lien Aut $\mathfrak{S}_6$

2 Centre et automorphismes

$Z(G) = \{g \in G / \forall h \in G \ gh = hg\}$
$=$ noyau de l'action par conjugaison
$\trianglelefteq G$

$G \to \operatorname{Aut} G$ est un morph de gpe qui
$g \mapsto \gamma_g$ induit $G/Z(G) \simeq \operatorname{Int}$
$\operatorname{Int} G \trianglelefteq \operatorname{Aut} G$

Prop : (i) $Z(\mathfrak{S}_2) = \mathfrak{S}_2$ $Z(\mathfrak{A}_2) = \{id\}$ $Z(\mathfrak{A}_3) = \mathfrak{A}_3$
prouvable avant (ii) Si $n \geq 3$ $Z(\mathfrak{S}_n) = \{id\}$ Si $n \geq 4$ $Z(\mathfrak{A}_n) = \{id\}$

D] (i) $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$

(ii) Soit $\sigma \in Z(\mathfrak{S}_n)$, on supp par l'absurde $\sigma \neq id$

Soit $k \in [\![1,n]\!]$ tq $\sigma(k) \neq k$ et ($n \geq 3$) m ds $[\![1,n]\!] \setminus \{k, \sigma(k)\}$ et $\tau = (m\,\sigma(k))$

On a $(\sigma\tau)(k) = (\tau\sigma)(k)$

$\shortparallel$ $k \notin \operatorname{Supp}\tau$ $\shortparallel$

$\sigma(k) = m$ Contradiction

Pr $n \geq 4$ $\sigma \in Z(\mathfrak{A}_n)$ et $k \in [\![1,n]\!]$ tq $\sigma(k) \neq k$. $[\![1,n]\!] \setminus \{k, \sigma(k)\}$ contient au moins 2 élts $\neq$ m, m' $\tau = (\sigma(k)\, m\, m')$

$\sigma(k) = (\sigma\tau)(k) = (\tau\sigma)(k) = m$ $\lightning$

Interlude : Centre et automorphismes

Soit G un gpe qcq. Centre de G : $Z(G)=\{g\in G \,/\, \forall h\in G\ gh=hg\} \trianglelefteq G$

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}_{gpe}\, G \\ g &\longmapsto \gamma_g : G \to G \\ & \qquad\quad x \mapsto gxg^{-1} \end{aligned}$$

est un morph de gpe de noyau $Z(G)$

Image = aut. intérieurs de G $:= \mathrm{Int}\, G$

$\mathrm{Int}\, G \trianglelefteq \mathrm{Aut}\, G$ $\quad \varphi\circ\gamma_g\circ\varphi^{-1}=\gamma_{\varphi(g)}$ et $\mathrm{Aut}\, G/\mathrm{Int}\, G := \mathrm{Out}\, G$ autom extérieurs de G

Thm :
- $\mathrm{Aut}\,\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ $\quad \mathrm{Int}\,\mathfrak{S}_2=\{id\}$
- Pr $n\geqslant 3$ et $n\neq 6$ $\quad \mathrm{Aut}\,\mathfrak{S}_n = \mathrm{Int}\,\mathfrak{S}_n \simeq \mathfrak{S}_n$ $\quad$ utilise $\mathfrak{S}_n = \langle$transpo$\rangle$ / card ou str de $Z(\sigma)$ / s/s gpe d'indice n = Stab k ?
- $\mathfrak{S}_6 \simeq \mathrm{Int}\,\mathfrak{S}_6 \underset{2}{\trianglelefteq} \mathrm{Aut}\,\mathfrak{S}_6$ $\quad$ Constr° : p-Sylow, isom exc (PGL..)

Dvpt possible, Perrin

3 Sous-groupe dérivé

cf autre rappel

Rmq : $D(\mathfrak{S}_n)\subseteq \mathfrak{A}_n$ car $\mathfrak{S}_n/\mathfrak{A}_n$ ab (ou directement sign)

Thm :
- $D(\mathfrak{S}_2)=\{id\}$
- $n\geqslant 3$ $\quad D(\mathfrak{S}_n)=\mathfrak{A}_n$
- $D(\mathfrak{A}_3)=\{id\}$
- $D(\mathfrak{A}_4)=V$
- $n\geqslant 5$ $\quad D(\mathfrak{A}_n)=\mathfrak{A}_n$ parfait, non résoluble

prouvable avant

D/
- $\mathfrak{S}_2, \mathfrak{A}_3$ abéliens ✓
- $|\mathfrak{A}_4/V|=3$ dc ab dc $D(\mathfrak{A}_4)\subseteq V$ $\quad (14)(23)=(12)(34)(13)(24)=(12)(34)\ (234)\ (12)(34)(243)\in D(\mathfrak{A}_4)$
  dc $V\setminus\{id\}=\omega_{\mathfrak{A}_4}((14)(23))\subseteq D(\mathfrak{A}_4)$
- $n\geqslant 3$ $\quad$ Soit γ 3-cycle γ^2 3-cycle dc $\gamma^2=\sigma\gamma\sigma^{-1}$ dc $\gamma=\sigma\gamma\sigma^{-1}\gamma^{-1}\in D(\mathfrak{S}_n)$ $\trianglelefteq \mathfrak{A}_n$ distingué ds $\mathfrak{S}_n$
  dc $D(\mathfrak{S}_n)$ contient ts les 3-cycles dc $D(\mathfrak{S}_n)=\mathfrak{A}_n$
- $n\geqslant 5$ $\quad$ Soit γ 3-cycle, γ^2 3-cycle aussi dc $\exists\sigma\in\mathfrak{A}_n$ tq $\gamma=[\sigma,\gamma]\in D(\mathfrak{A}_n)$
  3-cycle conj ds $\mathfrak{A}_n$ + engendrent $\mathfrak{A}_n$ dc $D(\mathfrak{A}_n)=\mathfrak{A}_n$

■

Modèle d'étude pour tous les groupes !