105 Groupe des permutations d'un ensemble fini. Application

Dans cette leçon, n désigne un entier naturel non nul, et E un ensemble fini de cardinal n. On supposera connu la théorie des représentations et les théorèmes de Sylow.

I. Généralités et première propriétés [ROM]

p39 Def ①: On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E, appelé groupe symétrique de E (ou groupe des permutations). Pour $E = [\![1,n]\!]$, on note $S(E) = S_n$.

p41 Rq ②: E est en bijection avec $[\![1,n]\!]$: $\exists f : E \to [\![1,n]\!]$ bijective et

$$\varphi : S(E) \to S_n, \quad \sigma \mapsto f \circ \sigma \circ f^{-1}$$ est un iso de groupes

on se ramène donc à l'étude de S_n dans la suite

p42 prop ③: $|S_n| = n!$

p55 Thm ④ (Cayley) soit G groupe fini de cardinal n, alors

$$\varphi : G \to \mathfrak{S}(G), \quad g \mapsto (\sigma_g : h \mapsto gh)$$ est un morphisme injectif de groupes.

donc G est isomorphe à un sous-groupe de $\mathfrak{S}_n$

p39 Def ⑤: • $\forall r \in [\![2,n]\!]$, un r-cycle est une permutation $\sigma \in \mathfrak{S}_n$ telle que $\exists (a_1 \dots a_r) \in [\![1,n]\!]^r$ avec

$$\begin{cases} \sigma(a_k) = a_{k+1} & \forall 1 \leq k \leq r-1 \\ \sigma(a_r) = a_1 \\ \sigma(x) = x & \forall x \notin \{a_1 \dots a_r\} \end{cases}$$ on note $\sigma = (a_1, \dots, a_r)$

• Un 2-cycle est appelé transposition

• si $\sigma \in S_n$, on appelle support de σ l'ensemble :

$$\mathrm{supp}(\sigma) = \{x \in [\![1,n]\!], \sigma(x) \neq x\}$$

prop ⑥: $\forall \sigma, \tau \in \mathfrak{S}_n$, $\mathrm{supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset \Rightarrow \sigma\tau = \tau\sigma$

prop ⑦: un r-cycle est d'ordre r p40

prop ⑧: • si $\sigma = (x_1 \dots x_r)$ est un r-cycle et $\tau \in \mathfrak{S}_n$ alors $\tau\sigma\tau^{-1} = (\tau(x_1) \dots \tau(x_r))$.

• réciproquement deux cycles de même longueur sont conjugués dans σ_n.

prop ⑨: Le centre de S_n est $Z(S_n) = \begin{cases} S_2 & \text{si } n=2 \\ \{id\} & \text{si } n \geq 3 \end{cases}$

(donc S_n n'est pas commutatif si $n \geq 3$).

Def ⑩: Soit $\sigma \in S_n$. $\langle\sigma\rangle$ agit sur $[\![1,n]\!]$ par

$$\langle\sigma\rangle \times [\![1,n]\!] \to [\![1,n]\!], \quad (\tau, i) \mapsto \tau(i)$$. Les orbites pour cette action sont les :

$$\mathrm{Orb}_\sigma(x) = \{\sigma^k(x), k \in \mathbb{Z}\}$$. où $x \in [\![1,n]\!]$.

les orbites non réduites à un point forment une partition de $\mathrm{supp}(\sigma)$.

prop ⑪ $\sigma \in S_n$ est un cycle d'ordre r SSI il n'y a qu'une seule σ-orbite non réduite à un point. p46

Thm ⑫: Toute permutation $\sigma \in S_n$ se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre des facteurs près. p45

si $\sigma = \gamma_1 \dots \gamma_p$ une telle décomposition alors $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(\gamma_1) \dots \mathrm{ord}(\gamma_p))$.

coro ⑬: (i) Les transpositions engendrent S_n p47

(ii) Les transpositions $(1k)$ $2 \leq k \leq n$ engendrent S_n

(iii) Les transpositions $(k, k+1)$ $1 \leq k \leq n-1$ engendrent S_n

(iv) (12) et $(12 \dots n)$ engendrent S_n

DECK p321

Thm 14 : si $\sigma \in S_n$, on lui associe $\delta(\sigma)$ qui est la suite d'entiers décroissante des longueurs des cycles intervenant dans la décomposition en cycles disjoints.
Alors : σ et τ sont conjuguées dans $S_n \iff \delta(\sigma) = \delta(\tau)$

II. Le Groupe Alterné

p49

Def-prop 15 : Il existe un unique morphisme de groupe non trivial $\varepsilon : S_n \to \mathbb{C}^*$. On l'appelle signature et $\forall \tau$ transposition, $\varepsilon(\tau) = -1$.

Def 16 : On appelle groupe alterné noté A_n, le noyau de la signature : $A_n = \{\sigma \in S_n, \varepsilon(\sigma) = 1\}$.
on a donc $A_n \lhd S_n$ et $|A_n| = \frac{n!}{2}$

[SP] p262 p52

prop 17 : . Pour $n \geq 3$, A_n est engendré par les 3-cycles
. Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n

Thm 18 : $\forall n \neq 4$, A_n est simple.

Coro 19 : si $n \neq 4$, les seuls sous-groupes distingués de S_n sont $\{Id\}$, A_n et S_n.

[P]

Rappel 20 : (orthogonalité des caractères) : Soit G un groupe et $\rho_1, \dots, \rho_r$ ses représentations irréductibles (à iso près) et $\chi_1 \dots \chi_r$ les caractères associés, alors si $\forall i$, $n_i = \deg(\rho_i)$, on a :

$$\begin{cases} |G| = \sum_{i=1}^{r} n_i^2 \\ \forall s \in G, s \neq 1, \sum_{i=1}^{r} n_i \chi_i(s) = 0 \end{cases}$$

Thm 21 : les sous-groupes distingués de G sont les $\bigcap_{i \in I} K_{\chi_i}$ où $I \subset \{1, \dots, r\}$ et $K_{\chi_i} = \{x \in G, \chi_i(x) = \chi(1)\}$

[D]

Ex 22 : Table de $\mathfrak{S}_4$:

	id	(12)	(123)	(12)(34)	(1234)
χ_1	1	1	1	1	1
χ_ε	1	-1	1	1	-1
χ_T	3	1	0	-1	-1
$\varepsilon\chi_T$	3	-1	0	-1	1
χ_S	2	0	-1	2	0

groupes distingués :

S_n A_4 V_4 et $\{id\}$

[SP] p277

Thm 23 : Soit G un groupe simple de cardinal 60 alors $G \simeq A_5$.

III. Applications

1) Déterminant

$\mathbb{K}$ corps de carac $\neq 2$

Def 24 : si $A = (a_{ij})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$, le déterminant de A est $\det(A) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i) i}$

p540-1 p56

app 25 : si $A \in \mathcal{M}_n(\mathbb{K})$, alors $\det({}^tA) = \det(A)$

Def 26 : $\forall \sigma \in S_n$, on lui associe la matrice de passage P_σ de $(e_1, \dots, e_n)$ base canonique de $\mathbb{K}^n$ à $(e_{\sigma(1)}, \dots, e_{\sigma(n)})$. P_σ est appelée matrice de permutation associée à σ.

Thm 27 : $p : \begin{array}{l} S_n \longrightarrow GL_n(\mathbb{K}) \\ \sigma \longmapsto P_\sigma : e_k \mapsto e_{\sigma(k)} \end{array}$ est un morphisme de groupes

il est injectif. de plus, si $\chi(\sigma) = tr(P_\sigma)$, on a :
$\chi(\sigma) = |\{x \in [\![1,n]\!],\ \sigma(x) = x\}|$.
on a de plus $\det(P_\sigma) = \varepsilon(\sigma)$.

cor 28 : tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$.

2) Polynômes symétriques

Def 29 : On dit qu'un polynôme $P \in \mathbb{K}[X_1, \ldots, X_n]$ est symétrique si $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1 \ldots X_n)$ $\forall \sigma \in S_n$.

Les polynômes $\sigma_{k,n} = \sum_{\substack{I \subset \{1,\ldots,n\} \\ |I| = k}} \prod_{i \in I} X_i$ sont les polynômes symétriques élémentaires

Thm 30 : Si $P \in \mathbb{K}[X_1, \ldots, X_n]$ est symétrique, il existe un unique polynôme $Q \in \mathbb{K}[X_1, \ldots, X_n]$ tel que $P(X_1, \ldots, X_n) = Q(\Sigma_{1,n}, \ldots, \Sigma_{n,n})$.

[Rom] : Rombaldi (Maths pour l'agreg)
[SP] : Szpirglas
[P] : Peyré (Algèbre discrète ...)