105 : Groupe des permutations d'un ensemble fini. Applications.

Préliminaire Soit E un ensemble $n \in \mathbb{N}^*$.

Déf 1 On note $S(E)$ le groupe des bijections de E dans E. Si $E = [\![1;n]\!]$, $S(E)$ est appelé groupe symétrique, noté S_n.

Notation: pour $\sigma \in S_n$, $\sigma := \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Prop 2 $\#(S_n) = n!$

Théorème 3 si $\#(E) = n$, $S(E) \simeq S_n$. Conséquence : on peut restreindre l'étude à S_n.

I Les éléments de S_n

A) Orbites et cycles

Soit $\sigma \in S_n$, $x \in [\![1;n]\!]$.

S_n induit une action de groupe naturelle sur $[\![1;n]\!]$: $\begin{cases} S_n \times [\![1;n]\!] \to [\![1;n]\!] \\ \sigma \times x \mapsto \sigma(x) \end{cases}$

Déf 4 $\langle\sigma\rangle$ définit une action de groupe sur $[\![1;n]\!]$. On appelle orbite de x par σ l'orbite de x associée à cette action. $O_\sigma(x) = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$

Déf 5 Le support de σ est $supp(\sigma) = \{x \in [\![1;n]\!] \mid \sigma(x) \neq x\}$

Ex 6 $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 6 & 1 & 3 \end{pmatrix}$. $Supp(\sigma) = \{1, 3, 4, 5, 6\}$

$O_\sigma(1) = \{1; 5\}$. $O_\sigma(6) = \{3, 4, 6\}$

Déf 7 Un cycle est une permutation possédant une unique orbite non-ponctuelle. Si le cardinal de cette orbite vaut ℓ, on parle de ℓ-cycle.

Notation Si c est un ℓ-cycle, on note $c := (i_1 \dots i_\ell)$ avec $i_1, \dots, i_\ell$ les éléments de l'orbite non-ponctuelle de c.

Ex 8 $c := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$ est un 3-cycle noté $(1\ 5\ 3)$.

Déf 9 Une transposition est un 2-cycle. On note $\tau_{ij} := (i\ j)$

Prop 10
- l'ordre d'un cycle est égal à sa longueur.
- 2 cycles à supports disjoints commutent
- $\forall \sigma \in S_n$, $\sigma (i_1\ i_2 \dots i_k) \sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \dots \sigma(i_k))$

Exemple 11 $(1\ 4)(2\ 1\ 5\ 3\ 4)(1\ 4) = (2\ 4\ 5\ 3\ 1)$

Application 12 Théorème de Cauchy. Tout groupe d'ordre n admet un sous-groupe d'ordre p avec p un diviseur premier de n.

B) Éléments générateurs

Théorème 13 Toute permutation de S_n se décompose comme un produit de (au plus $n-1$) transpositions (Non-unique)

Ex 14 $(4\ 3\ 1) = (4\ 3)(3\ 1)$

Théorème 15 Soit $\sigma \in S_n$. Soient $O_1, \dots, O_r$ les orbites de $[\![1;n]\!]$ sous l'action $\langle\sigma\rangle$. Alors les permutations c_i définies par $c_i(x) = \begin{cases} x \text{ si } x \notin O_i \\ \sigma(x) \text{ sinon} \end{cases}$ sont des cycles disjoints de longueur $\#(O_i)$, tel que $\sigma = c_1 c_2 \dots c_r$. Cette décomposition est unique, à l'ordre près des facteurs.

Ex 16 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 7 & 5 & 10 & 8 & 1 & 6 & 9 \end{pmatrix} = (1\ 4\ 7\ 8)(2\ 3)(6\ 10\ 9)$

Prop 17 Les familles suivantes engendrent S_n :

(a) $((1\ i))_{i \in [\![1;n]\!]}$ (b) $((i\ i+1))_{i \in [\![1;n-1]\!]}$ (c) $((1\ 2), (1\ 2 \dots n))$

C) Type

Def 18 Soit $\sigma \in S_n$, $\sigma = \prod_{i=1}^{r} c_i$ sa décomposition en cycles à supports disjoints, avec l_i la longueur de c_i. On appelle type de σ le vecteur $(l_1, \dots, l_r)$ (peu importe l'ordre car les c_i commutent).

Théorème 19 σ et σ' sont conjuguées $\Leftrightarrow$ σ et σ' ont mêmes types

Prop 20 L'ordre de σ est le ppcm de son type.

Ex 21 $(1\ 4\ 7\ 8)(2\ 3)(6\ 10\ 9)$ est de type $(4, 2, 3)$. Son ordre est donc 12.

II Signature et Groupe alterné

A) Signature

Remarque : il existe de nombreuses manières de définir la signature

Def 22 La signature ε est l'unique morphisme de groupe non-trivial de $(S_n, \circ)$ dans $(\mathbb{C}^*, \times)$.

Théorème 23 La signature d'une transposition est -1.

Corollaire 24
- $\varepsilon(S_n) = \{-1, 1\}$
- si c est un l-cycle, $\varepsilon(c) = (-1)^{l+1}$
- si $\sigma = c_1 \circ \dots \circ c_k$, $\varepsilon(\sigma) = (-1)^{n-k}$

Prop 25 : $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^{\text{nombre d'inversions de } \sigma}$

B) Groupe Alterné

Def 26 On définit le groupe alterné comme le noyau de la signature. On le note $\mathcal{A}_n$.

Prop 27
- $\mathcal{A}_n$ est un sous-groupe distingué de S_n, d'indice 2
- $\#(\mathcal{A}_n) = \frac{n!}{2}$

Prop 28 Les 3-cycles engendrent $\mathcal{A}_n$.

Ex 29 $\mathcal{A}_4$ possède 12 éléments : $Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$, $(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3)$

III Sous-groupes de S_n

Théorème 30 (de Cayley) Tout groupe G d'ordre n est isomorphe à un sous-groupe de $S(G) \simeq S_n$.

A) Sous-groupes distingués

Théorème 31 : $\mathcal{A}_n$ est simple pour $n \geq 5$ ▶ DEV 1 ◀

Corollaire 32 pour $n \geq 5$, les seuls sous-groupes distingués de S_n sont $\{Id\}$, $\mathcal{A}_n$ et S_n.

Application 33 Les sous-groupes d'indice n de S_n sont isomorphes à S_{n-1}.

B) Centre et groupe dérivé

Prop 34
- pour $n \geq 3$, $Z(S_n) = \{Id\}$
- pour $n \geq 4$, $Z(\mathcal{A}_n) = \{Id\}$

Prop 35 · Le groupe dérivé de S_n est $\mathfrak{A}_n$.
· Le groupe dérivé de $\mathfrak{A}_n$ est $\mathfrak{A}_n$.

IV Applications

A) Déterminant

Soit E un $\mathbb{K}$-ev de dimension n, $\mathbb{K}$ corps commutatif.

Def 36 Soit f une forme n-linéaire sur $E^n \longrightarrow \mathbb{K}$.

· f est dite alternée si $f(x_1, \dots, x_n) = 0$ dès que deux x_i sont égaux

· f est dite antisymétrique si l'échange de deux vecteurs dans $(x_1, \dots, x_n)$ donne à $f(x_1, \dots, x_n)$ des valeurs opposées.

Prop 37 f antisymétrique $\Leftrightarrow$ $\forall \sigma \in S_n$, $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) \times f(x_1, \dots, x_n)$

Théorème 38 L'ens des formes n-linéaires alternées sur E^n est un $\mathbb{K}$-ev de dimension 1. De plus, il existe une unique forme n-linéaire alternée prenant la valeur 1 sur une base $\mathcal{B}$ donnée de E, il s'agit du déterminant dans la base $\mathcal{B}$, noté $\det_{\mathcal{B}}$.

Corollaire 39 Soit $\begin{cases} (e_1, \dots, e_n) = \mathcal{B} \text{ base de } E \\ (x_1, \dots, x_n) \in E^n \text{ avec } x_j = \sum_{i=1}^{n} x_{i,j} e_i \end{cases}$

Alors $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{\sigma(1),1} \cdots x_{\sigma(n),n}$.

Def 40 St $A \in M_n(\mathbb{K})$. On appelle déterminant de A le déterminant de ses colonnes dans $\mathbb{K}^n$

Ex 41 Calcul de déterminant de matrice 3×3 $\rightarrow$ Règle de Sarrus (Voir annexe)

B) Matrice de permutation

Soit $\mathbb{K}$ un corps commutatif.

Def 42 Soit $\sigma \in S_n$. La matrice de permutation associée à σ est $(P_\sigma)_{ij} = \begin{cases} 1 & \text{si } i = \sigma(j) \\ 0 & \text{sinon.} \end{cases}$

Ex 43 $P_{\tau_{12}}$ inverse les 2 premières lignes de $A \in M_n(\mathbb{K})$ par multiplication à gauche.

Prop 44 P_σ est inversible, d'inverse $(P_\sigma)^{-1} = P_{\sigma^{-1}} = {}^{T}P_\sigma$

Théorème 45 $P \begin{cases} S_n \to GL_n(\mathbb{K}) \\ \sigma \mapsto P_\sigma \end{cases}$ est un morphisme de groupe injectif et $\det(P_\sigma) = \varepsilon(\sigma)$

Corollaire : Tout grp fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_q)$. App : 1er théorème de Sylow.

Théorème 46 (De Brauer) · Soient σ et $\sigma' \in S_n$,

σ et σ' sont conjugués $\Longleftrightarrow$ P_σ et $P_{\sigma'}$ sont semblables dans $\mathbb{K}$.

▶ DEV 2 ◀

C) Polynômes Symétriques

Soit $\mathbb{K}$ un corps commutatif de caractéristique différente de 2.

Def 47 $P \in \mathbb{K}[X_1, \dots, X_n]$ est symétrique si :

$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n) \quad \forall \sigma \in S_n$

Ex 48 $\Sigma_{k,n} = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k}$, $1 \leq k \leq n$ sont des polynômes symétriques, appelés polynômes symétriques élémentaires

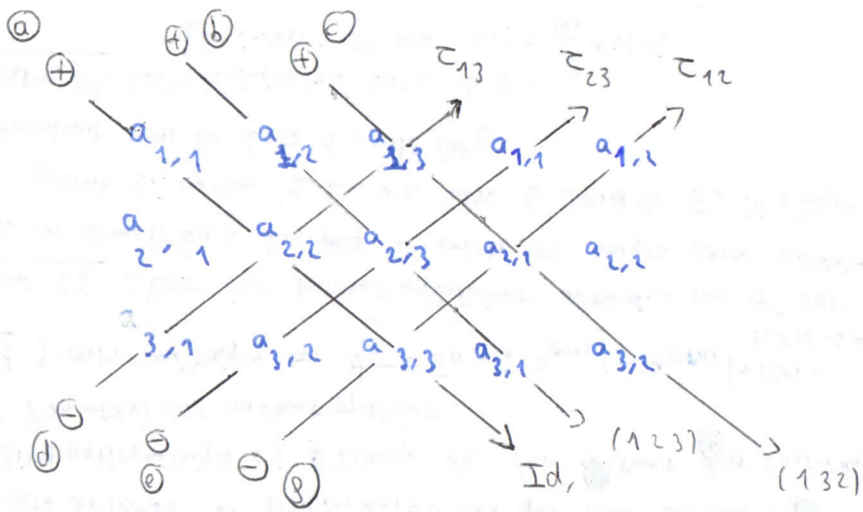
$\Sigma_{1,n} = \sum_{i=1}^{n} X_i$, $\Sigma_{n,n} = \prod_{i=1}^{n} X_i$

Théorème 49 Soit $P \in \mathbb{K}[X_1, \dots, X_n]$ symétrique. Alors il existe un unique polynôme $\varphi \in \mathbb{K}[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = \varphi(\Sigma_{1,n}, \dots, \Sigma_{n,n})$

Annexe

Ex 41 : Règle de Sarrus

S_3	Id	τ_{12}	τ_{23}	τ_{13}	$(1\ 2\ 3)$	$(1\ 3\ 2)$
ε	1	-1	-1	-1	1	1



$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = a + b + c - d - e - f$$