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

Références : Rombaldi, Ulmer (groupes), Perrin (pour $\mathfrak{A}_n$), Gourdon, Gozard

I - Le groupe symétrique

1) Définitions et premières propriétés
2) Support et orbites d'une permutation
3) Parties génératrices de $\mathfrak{S}_n$
4) Classes de conjugaison

II - Morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$

1) Signature
2) Le groupe alterné

III - Applications

1) Déterminant
2) Polynômes symétriques (ou théorèmes de Sylow...)
3) Nombre de dérangements de $\mathfrak{S}_n$

DEV 1 : $\mathfrak{A}_n$ est simple

DEV 2 : Nombre de dérangements

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

I - Le groupe symétrique

1) Définitions et premières propriétés [ROM]

Soit E un ensemble $\#E \geq 2$.

DEF 1 : On note $\mathcal{S}(E)$ le groupe des bijections de E dans E, pour la composition des applications. $\mathcal{S}(E)$ est appelé groupe des permutations de E.

THM 2 : Si E et F sont non vides et en bijection, alors $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont isomorphes.

COR 3 : Ainsi, si E est de cardinal n, $\mathcal{S}(E) \simeq \mathfrak{S}_n$ où $\mathfrak{S}_n$ est le groupe des permutations de $[\![1;n]\!]$.

Dans toute la suite, on étudie donc seulement $\mathfrak{S}_n$, $E = [\![1;n]\!]$.

NOT 4 : Pour tout $\sigma \in \mathfrak{S}_n$, on note $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

PROP 5 : $\forall n \in \mathbb{N}^*$, $\#\mathfrak{S}_n = n!$

DEF 6 : Soit $r \in [\![2;n]\!]$. On appelle cycle d'ordre r (ou r-cycle) toute permutation $\sigma \in \mathfrak{S}_n$ telle que

$$\begin{cases} \forall k \in [\![1;r-1]\!], \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in E \setminus \{x_1, \dots, x_r\}, \sigma(x) = x \end{cases}$$

On notera $\sigma = (x_1 \cdots x_r)$ et on dit que $\{x_1, \dots, x_r\}$ est le support de σ.

PROP 7 : $(x_1 \cdots x_r)^{-1} = (x_r\ x_{r-1} \cdots x_1)$. Si $\sigma = (x_1 \cdots x_r)$ est un r-cycle, alors, pour tout $k \in [\![1;r]\!]$, $\sigma^{k-1}(x_1) = x_k$.

DEF 8 : Un 2-cycle est une transposition

LEMME 9 : Un r-cycle est d'ordre r dans le groupe $(\mathfrak{S}_n, \circ)$.

LEMME 10 : Soit $r \in [\![2;n]\!]$. Le conjugué dans $\mathfrak{S}_n$ d'un r-cycle est encore r-cycle. Plus précisément, pour tout r-cycle $\sigma = (x_1 \cdots x_r)$ et tout $\tau \in \mathfrak{S}_n$, on a :

$$\tau \circ \tau^{-1} = (\tau(x_1) \cdots \tau(x_r))$$

Réciproquement, deux cycles de même longueur sont conjugués dans $\mathfrak{S}_n$.

→ Ajouter le thm de Cayley ! (dans la partie groupes si on la fait)

REM 11 : Le résultat précédent se traduit en disant que pour tout $r \in [\![2;n]\!]$, le groupe $\mathfrak{S}_n$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

LEMME 12 : Le centre de $\mathfrak{S}_n$ est $Z(\mathfrak{S}_n) = \begin{cases} \mathfrak{S}_n & \text{si } n = 2 \\ \{Id_E\} & \text{si } n \geq 3 \end{cases}$.

2) Support et orbites d'une permutation [ROM]

DEF 13 : Le support d'une permutation $\sigma \in \mathfrak{S}_n$ est le complémentaire dans E de l'ensemble de ses points fixes soit l'ensemble $Supp(\sigma) = \{x \in [\![1;n]\!] \mid \sigma(x) \neq x\}$

THM 14 : Soient $\sigma, \sigma' \in \mathfrak{S}_n$.
1) $\sigma(Supp(\sigma)) = Supp(\sigma)$
2) $Supp(\sigma) = Supp(\sigma^{-1})$
3) $\forall r \in \mathbb{Z}$, $Supp(\sigma^r) \subset Supp(\sigma)$
4) Si $Supp(\sigma) \cap Supp(\sigma') = \emptyset$, alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

DEF 15 : Soit $\sigma \in \mathfrak{S}_n$. On a une action naturelle du groupe cyclique $H = \langle \sigma \rangle$ sur E définie par $(\sigma^k, x) \mapsto \sigma^k(x)$. Les σ-orbites pour cette action sont les $\{\sigma^k(x) \mid k \in \mathbb{Z}\}$
On notera $Orb_\sigma(x)$ une telle orbite. On rappelle que ces orbites sont aussi les classes d'équivalence définie sur E par

$$x \mathcal{R}_\sigma y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$$

et les orbites deux à deux distinctes forment une partition de E.
Les σ-orbites non réduites à un point forment une partition du support de σ.

LEMME 16 : Soit $\sigma \in \mathfrak{S}_n$, $\sigma \neq Id_E$. Soit O une σ-orbite de cardinal $r \geq 2$. Pour tout $x \in O$, r est le plus petit entier non nul tel que $\sigma^r(x) = x$ et :

$$O = Orb_\sigma(x) = \{x ; \sigma(x) ; \dots ; \sigma^{r-1}(x)\}.$$

THM 17 : $\sigma \in \mathfrak{S}_n$ est un cycle d'ordre $r \geq 2$ si et seulement si il n'y a qu'une seule σ-orbite non réduite à un point.

DEF 18 : Deux cycles σ et σ' dans $\mathfrak{S}_n$ sont disjoints, si leurs supports sont disjoints dans E.

THM 19 : Tout $\sigma \in \mathfrak{S}_n$, $\sigma \neq I_n$ se décompose en produit de cycles deux à deux à supports disjoints. Cette décomposition est unique à l'ordre près.

PROP 20: Si $\sigma = \gamma_1 \cdots \gamma_p$ est une telle décomposition, on a alors la partition $\mathrm{Supp}(\sigma) = \bigcup_{k=1}^{p} \mathrm{Supp}(\gamma_k)$ et l'ordre de σ est le ppcm des ordres des γ_i.

EX 21: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\,2\,3\,4\,5)(6\,7)$

3) Parties génératrices de $\mathfrak{S}_n$ [ROM]

LEMME 22: Pour $r \in [\![2;n]\!]$, tout r-cycle dans $\mathfrak{S}_n$ s'écrit comme produit de $r-1$ transpositions.

THM 23: Tout $\sigma \in \mathfrak{S}_n$ se décompose en produit de transpositions. $\mathfrak{S}_n$ est donc engendré par les transpositions

LEMME 24: $\mathfrak{S}_n$ est engendré par les transpositions $(1\,i)$, $2 \leq i \leq n$

LEMME 25: $\mathfrak{S}_n$ est engendré par les transpositions $(i\;i{+}1)_{1 \leq i \leq n}$

LEMME 26: $\mathfrak{S}_n$ est engendré par $(1\,2)$ et $(1\,2 \cdots n)$.

4) Classes de conjugaison [ULM]

DEF 27: Soit $n \in \mathbb{N}$. On appelle type de permutation $\sigma \in \mathfrak{S}_n$ et on note $[l_1, l_2, \ldots, l_m]$, la liste des cardinaux l_i des orbites dans $[\![1;n]\!]$ de l'action $\langle\sigma\rangle \curvearrowright \mathfrak{S}_n$ du groupe $\langle\sigma\rangle$ sur $[\![1;n]\!]$ rangée en ordre croissant.

REM 28: En d'autres termes, λ_k est le nombre de k-cycles dans la décomposition de σ, λ_1 est le nombre de points fixes.

PROP 29: Deux permutations σ et ρ de $\mathfrak{S}_n$ sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont même type.

EX 30: Les deux permutations $\sigma = (1\,6\,3)(2\,4)$ et $\rho = (1\,4)(2\,3\,5)$ de $\mathfrak{S}_6$ sont conjuguées: $\rho = \omega\sigma\omega^{-1}$ avec $\omega = (1\,2)(3\,5\,6)$

COR 31: Les classes de conjugaison de $\mathfrak{S}_n$ sont donc en bijection avec les partitions de $[\![1;n]\!]$.

PROP 32: Le nombre de classes de conjugaison de $\mathfrak{S}_n$ est le n-ième nombre de Bell:
$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

II - Morphisme de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^*$

1) Signature [ULM]

DEF 33: Soient $n \geq 1$ et $\sigma \in \mathfrak{S}_n$. On appelle signature de $\sigma \in \mathfrak{S}_n$ et on note $\varepsilon(\sigma)$ le nombre:
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

THM 34: L'application $\varepsilon : \mathfrak{S}_n \to \{-1;1\}$ qui à une permutation σ associe sa signature $\varepsilon(\sigma)$ est un morphisme de groupes

PROP 35: 1) Si σ est une transposition, $\varepsilon(\sigma) = -1$

2) Si $\#(\sigma)$ désigne un nombre de transpositions qui apparaît dans une décomposition de σ en produit de transpositions, alors $\varepsilon(\sigma) = (-1)^{\#(\sigma)}$

En conséquence, la parité de ce nombre de transpositions est indépendante de la décomposition de σ en produit de transpositions: ce nombre est soit toujours pair, soit toujours impair.

3) Si $\sigma \in \mathfrak{S}_n$ est de type $[l_1, \ldots, l_m]$ alors:
$\sigma = (-1)^{l_1 - 1}(-1)^{l_2 - 1} \cdots (-1)^{l_m - 1} = (-1)^{l_1 + l_2 + \cdots + l_m - m}$

THM 36: Les seuls morphismes de groupes de $(\mathfrak{S}_n, \circ)$ dans $(\mathbb{R}^*, \cdot)$ sont l'application constante égale à 1 et la signature ε. La signature étant surjective de $\mathfrak{S}_n$ sur $\{-1;1\}$.

REM 37. ε compte le nombre d'inversions de σ.

2) Le groupe alterné [ROM]

DEF 38: On dit que $\sigma \in \mathfrak{S}_n$ est paire (resp. impaire) lorsque $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

DEF 39: On définit le groupe alterné comme le noyau du morphisme ε. On le note $\mathfrak{A}_n$

DEV 1

THM 40: $\forall n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles

LEMME 41: Les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$, pour $n \geq 5$

THM 42: Pour $n = 3$ et $n \geq 5$, $\mathfrak{A}_n$ est simple.

→ AVANT !

PROP 43 : $\mathfrak{A}_n$ est un sous-groupe distingué d'indice 2 de $\mathfrak{S}_n$. De plus, $\#\mathfrak{A}_n = \frac{n!}{2}$.

THM 44 : Pour $n \geq 5$, les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{Id\}$; $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

COR 45 : Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$, alors H est isomorphe à $\mathfrak{S}_{n-1}$. [PER]

III - Applications

1) Déterminant [GOU] Soit K un corps

DEF 46 : Soient $E_1, \dots, E_p$, F des K-espaces vectoriels. Une application $f : E_1 \times \dots \times E_p \to F$, $(x_1, \dots, x_p) \mapsto f(x_1, \dots, x_p)$ est dite p-linéaire lorsque en tout point, les applications partielles sont linéaires. Si $E_1 = \dots = E_p = E$ on note $\mathcal{L}_p(E, K)$ l'espace vectoriel des formes p-linéaires sur E.

DEF 47 : • f est dite alternée lorsque $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.

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

THM 48 : Si $car(K) \neq 2$, $f \in \mathcal{L}_p(E, K)$, alors f est alternée si et seulement si f est antisymétrique

THM 49 : Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. L'espace des formes n-linéaires alternées sur E est une droite vectorielle. Il existe une unique $f \in \mathcal{L}_n(E, K)$ telle que $f(\mathcal{B}) = 1$. On la note $\det_{\mathcal{B}}$ et 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 [GOZ]

PROP 50 : $\forall \sigma \in \mathfrak{S}_n$, $\forall P \in A[X_1, \dots, X_n]$ (A est un anneau commutatif unitaire)

$(\sigma . P)(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$

• Pour $\sigma \in \mathfrak{S}_n$, $P \mapsto \sigma . P$ est un automorphisme de A-algèbres

• $\sigma \mapsto u_\sigma$ est une action du groupe $\mathfrak{S}_n$ sur $A[X_1, \dots, X_n]$

PROP 51 : Soit $P \in A[X_1, \dots, X_n]$. LASSE :

(1) $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$

(2) $\forall (i,j) \in [\![1;n]\!]^2$, $i < j$, $P(X_1, \dots, X_i, \dots, X_j, \dots, X_n) = P(X_1, \dots, X_j, \dots, X_i, \dots, X_n)$

DEF 52 : Dans ces conditions, on dit que P est un polynôme symétrique.

DEF 53 : Les n polynômes $\sigma_i = \sum_{\substack{I \subset [\![1;n]\!] \\ \#I = i}} \prod_{j \in I} X_j$ sont symétriques et sont appelés polynômes symétriques élémentaires.

THM 54 : Soit $P \in A[X_1, \dots, X_n]$ symétrique de degré k.

$\exists ! Q \in A[X_1, \dots, X_n]$, $P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n)$

3) Nombre de dérangements de $\mathfrak{S}_n$

DEF 55 : On appelle dérangement de $\mathfrak{S}_n$ toute permutation $\sigma \in \mathfrak{S}_n$ sans point fixe i.e $Supp(\sigma) = [\![1;n]\!]$. On note D_n le nombre de dérangement de $\mathfrak{S}_n$.

PROP 56 : On a $n! = \sum_{k=0}^{n} \binom{n}{k} D_k$

On montre que $\sum_{n=0}^{+\infty} \frac{D_n}{n!} x^n = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right) x^n$ d'où $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

PROP 57 : Soit P la probabilité uniforme sur $(\mathfrak{S}_n, \mathcal{P}(\mathfrak{S}_n))$. Soit F_n la variable aléatoire qui compte le nombre de points fixes de $\sigma \in \mathfrak{S}_n$. On a :

$\forall r \in [\![0;n]\!]$, $P(F_n = r) = \frac{\binom{n}{r} D_{n-r}}{\#\mathfrak{S}_n} = \frac{1}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$

COR 58 : En particulier, $F_n \xrightarrow{\mathcal{L}} \mathcal{P}(1)$

De plus, $E[F_n] = Var(F_n) = 1$.