105.

GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI. APPLICATIONS

Ref: Tauvel, Perrin, Combes, Ladegaillerie, Gourdon.

Dans cette leçon, E est un ensemble fini de cardinal $n \in \mathbb{N}^*$.
On suppose connue la notion d'action de groupe. On note $[\![1,n]\!] = \{1,\dots,n\}$.

(I) Généralités sur le groupe symétrique

1) Définition et premières propriétés

Déf : L'ensemble des bijections de E dans E est un groupe pour la composition, appelé groupe symétrique de E, et noté $\mathfrak{S}(E)$.
- Si $E = [\![1,n]\!]$, on note $\mathfrak{S}(E) = \mathfrak{S}_n$.
- Un élément de $\mathfrak{S}(E)$ est appelé permutation.

Prop : $|\mathfrak{S}(E)| = n!$ et $\mathfrak{S}(E) \simeq \mathfrak{S}_n$
(On se limitera donc dans la suite à l'étude de $\mathfrak{S}_n$).

Thm : Si $n \geq 3$, $Z(\mathfrak{S}_n) = \{Id\}$. En particulier $\mathfrak{S}_n$ est non abélien. De plus, $\mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$.

2) Orbites et cycles

Déf : Soit $\sigma \in \mathfrak{S}_n$. On appelle support de σ l'ensemble
$\mathrm{Supp}(\sigma) = \{x \in E \,/\, \sigma(x) \neq x\}$

Déf : Soient $\sigma \in \mathfrak{S}_n$ et $x \in [\![1,n]\!]$. On appelle σ-orbite de x l'ensemble
$O_\sigma(x) = \{\sigma^k(x) \,;\, k \in \mathbb{Z}\}$.
La relation R_σ définie sur $E = [\![1,n]\!]$ par $x R_\sigma y$ ssi $y \in O_\sigma(x)$ est une relation d'équivalence, en particulier $y \in O_\sigma(x) \Rightarrow O_\sigma(y) = O_\sigma(x)$.

Déf : On dit que $\sigma \in \mathfrak{S}_n$ est un k-cycle s'il existe une unique σ-orbite O telle que $\mathrm{Card}\, O > 1$, avec $\mathrm{Card}\, O = k$.
Un 2-cycle est appelé transposition.

Rq :
- $\mathrm{Supp}(\sigma) = O$.
- On adopte la notation habituelle $\sigma = (x_1 x_2 \dots x_k)$.

Prop : Deux cycles à supports disjoints commutent.

Prop : Si $\sigma = (x_1 \dots x_k)$ est un k-cycle et $\gamma \in \mathfrak{S}_n$,
$\gamma\sigma\gamma^{-1} = (\gamma(x_1) \dots \gamma(x_k))$. Ainsi, deux cycles de même longueur sont conjugués.

3) Générateurs de $\mathfrak{S}_n$

Thm : Toute permutation se décompose de façon unique à l'ordre des facteurs près en produit de cycles de supports deux à deux disjoints.

Rq : Si σ s'écrit $\sigma = c_1 c_2 \dots c_l$ où les c_i sont des cycles à supports disjoints, et γ une permutation, alors $\gamma\sigma\gamma^{-1}$ se calcule facilement grâce à la proposition ci-dessus.

Déf : On appelle profil d'une permutation $\sigma \in \mathfrak{S}_n$ la suite $(l_1, \dots l_m)$ des longueurs des cycles de la décomposition de σ, ordonnée par ordre croissant.

Cor : (Classes de conjugaison de $\mathfrak{S}_n$)
Deux permutations sont conjuguées si et seulement si elles ont le même profil.

Prop: • Si $n \geq 2$, $2 \leq p \leq n$, alors il y a $(p-1)!\, C_n^p$ p-cycles dans $\mathfrak{S}_n$. En particulier si n est premier, $\mathfrak{S}_n$ contient exactement $(n-1)!$ éléments d'ordre n.

Thm: $\mathfrak{S}_n$ est engendré par l'une (quelconque) des familles suivantes:

i) les transpositions $(1,i)$ pour $2 \leq i \leq n$.

ii) les transpositions $(i,i+1)$ pour $1 \leq i \leq n-1$ (transpositions simples)

iii) La transposition $(1,2)$ et le n-cycle $(1\,2\ldots n)$

Application: Algorithme du tri à bulles.

II Signature et groupe alterné

1) Signature d'une permutation

Déf: Soit $\sigma \in \mathfrak{S}_n$ et $m(\sigma)$ le nombre de σ-orbites. La signature de σ est l'élément $\varepsilon(\sigma) \in \{-1,1\}$ défini par $\varepsilon(\sigma) = (-1)^{n-m(\sigma)}$

Rq: $\varepsilon(id) = 1$; $\varepsilon(\sigma) = (-1)^{p-1}$ pour un p-cycle ; $\varepsilon(\tau) = -1$ pour une transposition.

Thm: Soit $\sigma \in \mathfrak{S}_n$ et τ une transposition. Alors:
$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma)$$

Cor: (i) Si $\sigma \in \mathfrak{S}_n$ est un produit de k transpositions, alors $\varepsilon(\sigma) = (-1)^k$.

(ii) $\varepsilon : \mathfrak{S}_n \longrightarrow \{-1,1\}$ est un morphisme de groupes.

(iii) Si $n \geq 2$ et $\sigma \in \mathfrak{S}_n$, on a
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$$

Rq: Il s'agit du seul morphisme non trivial de $\mathfrak{S}_n$ dans $\{-1,1\}$ (et même dans $\mathbb{C}^*$)

2) Le groupe alterné

Déf: Le noyau de ε est appelé groupe alterné de $[\![1,n]\!]$ et est noté $\mathfrak{A}_n$. On a $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$.

Prop: Si $n \geq 2$, $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{-1,1\}$; $(\mathfrak{S}_n : \mathfrak{A}_n) = 2$; $\mathrm{Card}(\mathfrak{A}_n) = \frac{n!}{2}$

Rq: Les éléments de $\mathfrak{A}_n$ sont les permutations qui se décomposent en produit pair de transpositions : on les appelle les permutations paires.

Prop: (Générateurs de $\mathfrak{A}_n$)

(i) Si $n \geq 3$, $\mathfrak{A}_n$ est engendré par les permutations $(1,i)(1,j)$ où $2 \leq i,j \leq n$

(ii) Si $n \geq 3$, $\mathfrak{A}_n$ est engendré par les 3-cycles de la forme $(1,2,i)$ où $3 \leq i \leq n$

(iii) $\mathfrak{A}_n$ est engendré par les σ^2, où $\sigma \in \mathfrak{S}_n$.

Rq: (ii) $\Rightarrow$ les 3-cycles engendrent $\mathfrak{A}_n$.

Prop: Si $n \geq 2$, $\mathfrak{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Applications: $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$; $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$

Prop: $\mathfrak{A}_n$ opère $(n-2)$-fois transitivement sur $[\![1,n]\!]$ mais pas $(n-1)$ fois transitivement.

Prop: $\mathfrak{A}_n$ est simple ssi $n \neq 1, 2$ ou 4 $\boxed{\text{DEV}}$

Rq: • si $n = 4$, le groupe de Klein $V_4 = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ est un sous-groupe distingué et abélien de $\mathfrak{A}_4$.

• si $n \neq 4$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et $\{Id\}$.

Prop: (i) $D(\mathfrak{S}_n) = \mathfrak{A}_n$

(ii) Si $n \geq 5$, $D(\mathfrak{A}_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$

où $D(G)$ est le groupe dérivé du groupe G.

Cor: $\mathfrak{S}_n$ est résoluble ssi $n \leq 4$.

Application : La théorie de Galois fait le lien entre ce résultat et la résolubilité des équations par radicaux.

Corollaire : Tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Application : $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ et $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$

Thm : $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$ ssi $n \neq 6$

III) Actions de groupe et groupe symétrique

Comme toute action de groupe sur un ensemble E est définie par un morphisme du groupe dans $\mathfrak{S}(E)$, et que tout groupe agit sur lui-même (ex : par translation), on a le :

Thm : (Cayley) Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

1) Groupes d'isométries particuliers

Thm :
- Le groupe des isométries du triangle équilatéral est isomorphe à $\mathfrak{S}_3$, celui des déplacements à $\mathfrak{A}_3$.
- Le groupe des isométries du carré est isomorphe à un sous-groupe de $\mathfrak{S}_4$ (groupe diédral d'ordre 4 - de cardinal 8 -).
- le groupe des isométries du tétraèdre régulier est isomorphe à $\mathfrak{S}_4$, celui des déplacements à $\mathfrak{A}_4$.
- Le groupe des isométries du cube est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$, celui des déplacements à $\mathfrak{S}_4$.

$\boxed{\text{DEV}}$

Application : Nombre de façons différentes de colorier les faces d'un cube.

2) Polynômes symétriques

Déf : Soit A un anneau. L'application $\mathfrak{S}_n \to \mathfrak{S}(A[X_1, \dots, X_n])$, $\sigma \mapsto (P \mapsto P^\sigma)$ où $P^\sigma(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ définit une action de groupe. Si $\mathrm{Stab}(P) = \mathfrak{S}_n$, alors P est dit polynôme symétrique. On appelle polynôme symétrique élémentaire de degré p le polynôme $\Sigma_p = \sum_{1 \le i_1 < \dots < i_p \le n} X_{i_1} \dots X_{i_p}$ $(1 \le p \le n)$.
(Il est bien symétrique).

Lemme : Si P est symétrique et vérifie $P(X_1, \dots, X_{n-1}, 0) = 0$, alors Σ_n divise P.

Thm : Si P est symétrique, il existe un unique polynôme unitaire Q dans $A[X_1, \dots, X_n]$ tel que $P = Q(\Sigma_1, \dots, \Sigma_n)$.

3) Algèbre (multi-)linéaire

a) Matrices de permutations

Déf : Soit k un corps et B la base canonique de k^n. Si $\sigma \in \mathfrak{S}_n$, on appelle matrice de permutation associée à σ la matrice $P_\sigma = (\delta_{i\sigma(j)})_{i,j}$ (qui est associée à l'endomorphisme $u_\sigma : e_i \mapsto e_{\sigma(i)}$)

Prop : $\varphi : \mathfrak{S}_n \to GL_n(k)$, $\sigma \mapsto P_\sigma$ est un morphisme de groupes

Thm : (Brauer) Si σ et $\tau \in \mathfrak{S}_n$, alors σ et τ sont conjuguées ssi P_σ et P_τ le sont. $\boxed{\text{DEV}}$

b) Formes multilinéaires alternées

Déf : k corps de caractéristique $\neq 2$, E k-ev. φ une forme p-linéaire de E dans k est dite alternée si $\varphi(x_1, \dots, x_p) = 0$ dès que 2 vecteurs parmi les x_i sont égaux.

Prop : φ est alternée ssi $\forall \sigma \in \mathfrak{S}_n$, $\forall (x_1, \dots, x_n) \in E^n$,
$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_n)$

Thm : L'ensemble des formes linéaires n-alternées sur un k-ev E de dim n est un k-ev de dim 1. De plus pour une base $\mathcal{B}$ de E donnée, le déterminant dans la base $\mathcal{B}$ est l'unique forme n-linéaire alternée prenant la valeur 1 sur $\mathcal{B}$. On a $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$