LEÇON 105 - GROUPE DES PERMUTATIONS D'UN ENSEMBLE FINI.

I - Le groupe symétrique.

1 - Définitions.

Définition I.1.1 Soit X un ensemble. Une permutation de X est une bijection de X dans X. L'ensemble des permutations de X est noté $\mathfrak{S}(X)$.

Théorème I.1.2. ~~Pour $X \neq \emptyset$~~, $(\mathfrak{S}(X), \circ)$ est un groupe

Définition I.1.3. $\mathfrak{S}(\{1 \dots n\})$ est appelé groupe symétrique à n éléments. On le note $\mathfrak{S}_n$.

Proposition I.1.4. Si $|X| = n$ alors $\mathfrak{S}(X) \simeq \mathfrak{S}_n$ et $|\mathfrak{S}(X)| = n!$

On parle alors du groupe symétrique à n éléments.
On représente $\sigma \in \mathfrak{S}_n$ par $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$

2 - Propriétés de structure de $\mathfrak{S}_n$

Remarque I.2.1. $\mathfrak{S}_3$ n'est pas commutatif. En effet,
$$\begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}\begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} \neq \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix} = \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}\begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}$$

Remarque I.2.2. Pour $n \leq m$, $\mathfrak{S}_n \hookrightarrow \mathfrak{S}_m$

Résultat I.2.3. Pour $n \geq 3$, $\mathfrak{S}_n$ n'est pas commutatif. mieux, on a $Z(\mathfrak{S}_n) = \{id\}$

Définition I.2.4. $\alpha, \beta \in \mathfrak{S}_n$. On dit que α et β sont disjointes si $\forall k \in \{1 \dots n\}$, $\alpha(k) = k$ ou $\beta(k) = k$.

Résultat I.2.5. Si α et β disjointes alors $\alpha\beta = \beta\alpha$

Définition I.2.6. Soit $\sigma \in \mathfrak{S}_n$, $k \in \{1, \dots, n\}$. On appelle $\mathcal{O}_\sigma(k) = \{\sigma^i(k), i \in \mathbb{Z}\}$ l'orbite de k sous σ.

La relation définie par $k \sim l \Leftrightarrow k \in \mathcal{O}_\sigma(l)$ est une relation d'équivalence et on peut donc écrire
$\{1, \dots, n\} = \mathcal{O}_\sigma(k_1) \sqcup \dots \sqcup \mathcal{O}_\sigma(k_p)$.

Définition I.2.7. Soit $p > 1$. On appelle <u>p-cycle</u> toute permutation $\sigma \in \mathfrak{S}_n$ qui possède une unique orbite de taille p. On appelle <u>transposition</u> les <u>2-cycles</u>

Remarques I.2.8.
- Un p-cycle est d'ordre p.
On note alors $\sigma = (k, \sigma(k), \dots, \sigma^{p-1}(k))$ pour k tq $\sigma(k) \neq k$
- Soit $\sigma = (x_1, \dots, x_p)$ un p-cycle. Soit $\gamma \in \mathfrak{S}_n$, alors $\gamma\sigma\gamma^{-1} = (\gamma(x_1), \dots, \gamma(x_p))$.
- Deux cycles ont même longueur ss'ils sont conjugués.
- $2 \leq p \leq n$. Il y a $(p-1)!\binom{n}{p}$ p-cycles dans $\mathfrak{S}_n$.

Théorème I.2.9. Toute permutation de $\mathfrak{S}_n$ se décompose en produit de cycles disjoints

Remarque I.2.10. Cette décomposition est unique à l'ordre près

Corollaire I.2.11. $\boxed{\text{Toute permutation se décompose en produit de transpositions.}}$

Remarques I.2.12. On peut se restreindre aux transpositions $(1,i)$, $i\in\{2,\dots n\}$ ou $(i,i+1)$, $i\in\{1,\dots n-1\}$.

Application I.2.13. Algorithmes de tri : p.ex. le tri à bulles.

Définition I.2.14. On appelle profil de $\sigma\in\mathfrak{S}_n$ la suite ordonnée par ordre croissant des longueurs des cycles intervenant dans sa décomposition.

Proposition I.2.15.
- Deux permutations sont conjuguées ssi elles ont le même profil.
- Il y a bijection entre les classes de conjugaison de $\mathfrak{S}_n$ et l'ensemble des suites $\nearrow$, ≥ 0, finies de somme n.

II - Signature d'une permutation et groupe alterné.

1. Signature.

Définition II.1.1. Soit $\sigma\in\mathfrak{S}_n$. On définit la signature de σ par $\varepsilon(\sigma)=\prod_{1\leq i<j\leq n}\dfrac{\sigma(i)-\sigma(j)}{i-j}$.

Propriétés II.1.2.
- ε est un morphisme de groupe surjectif de $\mathfrak{S}_n$ dans $\{-1,1\}$.
- Soit γ un p-cycle. $\varepsilon(\gamma)=(-1)^{p-1}$
- Si $\sigma=t_1\dots t_q$ une décomposition en transposition de σ, alors $\varepsilon(\sigma)=(-1)^q$
- $\sigma\in\mathfrak{S}_n$, $\varepsilon(\sigma)=(-1)^{n-m(\sigma)}$ où $m(\sigma)=$ nbr de σ-orbites.

Remarque II.1.3: ε est l'unique morphisme surjectif de $\mathfrak{S}_n$ dans $\{-1,1\}$

2. Groupe alterné.

Définition II.2.1. On appelle groupe alterné à n éléments et on note $\mathcal{A}_n=\ker\varepsilon$.

Remarque II.2.2. On a $\mathcal{A}_n\triangleleft\mathfrak{S}_n$ et pour $n\geq 2$ on a $\mathfrak{S}_n/\mathcal{A}_n\simeq\{-1,1\}$ donc $[\mathfrak{S}_n:\mathcal{A}_n]=2$ et $|\mathcal{A}_n|=\frac{n!}{2}$.

Proposition II.2.3. [Générateurs de $\mathcal{A}_n$]

$n\geq 3$
- (i) $\mathcal{A}_n$ est engendré par $(1,i)(1,j)$ $2\leq i,j\leq n$
- (ii) $\mathcal{A}_n$ est engendré par les 3-cycles, et même par $(1,2,i)$, $3\leq i\leq n$.
- (iii) $\mathcal{A}_n$ est engendré par les σ^2, $\sigma\in\mathfrak{S}_n$.

Proposition II.2.4. Pour $n\geq 2$, $\mathcal{A}_n$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Théorème II.2.5 $\boxed{\mathcal{A}_n \text{ est simple ssi } n\neq 4}$ [P]

3. Groupe dérivé, résolubilité et automorphismes de $\mathfrak{S}_n$

Proposition II.3.1: $\boxed{D(\mathfrak{S}_n)=\mathcal{A}_n \text{ et pour } n\geq 5\ D(\mathcal{A}_n)=\mathcal{A}_n}$ [P]

Corollaire II.3.2. $\mathfrak{S}_n$ est résoluble ssi $n \leq 4$

Application II.3.3. Résolubilité par radicaux des équations polynomiales. (Critère de).

[P] **Corollaire II.3.3.** Tout sous groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Théorème II.3.4. [Automorphismes de $\mathfrak{S}_n$] [DEV. 1]

[P] $$\boxed{\mathrm{Aut}(\mathfrak{S}_n) \simeq \mathrm{Int}(\mathfrak{S}_n) \Leftrightarrow n \neq 6}$$

III - Actions de groupe et groupe symétrique, réalisation géométrique.

1 - Actions de groupes, théorème de Cayley

Se donner une action d'un groupe G sur un ensemble E est équivalent à donner un morphisme de G dans $\mathfrak{S}(E)$.

Théorème III.1.1 [de Cayley]

> Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$

Application III.1.2. Théorème de Sylow.

2 - Réalisation géométrique de $\mathfrak{S}_n$ et $\mathfrak{A}_n$.

Définition III.2.1. On définit un simplexe régulier t_n de $\mathbb{R}^n$ par $t_n = (A_0, \dots, A_n)$ avec $A_0, \dots A_n$ affinement indépendants et $d(A_i, A_j) = 1$

On note $\mathrm{Isom}(t_n)$ l'ensemble des isométries laissant t_n invariant [X]

Résultat III.2.2. $\boxed{\mathrm{Isom}(t_n) \simeq \mathfrak{S}_{n+1} \text{ et } \mathrm{Isom}^+(t_n) \simeq \mathfrak{A}_{n+1}}$

IV - Application.

1 - Formes multilinéaires alternées.

Définition IV.1.1. Soit K corps ($\mathrm{car}(K) \neq 2$) et E Kev de dim finie n. Une forme n-linéaire de E dans K est dite alternée si
$$(\exists i, j, i \neq j, x_i = x_j) \Longrightarrow (\varphi(x_1 \dots x_n) = 0) \quad \forall (x_1 \dots x_n) \in E^n.$$

Proposition IV.1.2. φ est alternée si et seulement si
$$\forall \sigma \in \mathfrak{S}_n \ \forall (x_1 \dots x_n) \in E^n \quad \varphi(x_{\sigma(1)} \dots x_{\sigma(n)}) = \varepsilon(\sigma) \varphi(x_1 \dots x_n).$$

Théorème IV.1.3.

> L'ensemble des formes n-linéaires alternées sur E est un K-ev de dim 1. De plus, si B base de E on a $\varphi(x_1 \dots x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)} \cdot \varphi(B)$

Définition IV.1.4. $\det_B$ est l'unique forme n-linéaire alternée telle que $\det_B(B) = 1$.

Propositions IV.1.5. • $\det(A) = \det({}^tA)$ • $\det(\lambda A) = \lambda^n \det(A)$
• développement par rapport à une ligne/colonne.

Théorème IV.1.6. [Frobenius-Zolotarev] [DEV 2]

> Soit p premier ≥ 3. V un $\mathbb{F}_p$ ev de dim finie, alors $\forall u \in GL(V)$ on a $\varepsilon(u) = \left(\frac{\det u}{p}\right)$. [OA]

RÉFÉRENCES :

[P] Daniel Perrin, Cours d'algèbre.

[X] Oraux X-ENS algèbre 3.

[OA] objectif agreg.

DÉVELOPPEMENTS POSSIBLES :

- $\mathcal{A}_n$ est simple pour $n \geq 5$
- Coloriage du cube.

AUTRE APPLICATION IMPORTANTE :

Polynômes symétriques. (voir par exemple J.-J. Risler, P. Boyer - Algèbre pour la licence 3.)

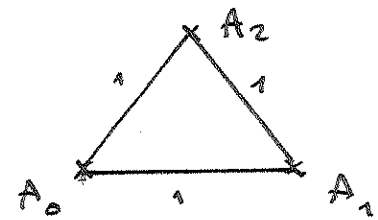
SIMPLEXES RÉGULIERS :

- de $\mathbb{R}$:

segment de longueur 1

- de $\mathbb{R}^2$:

triangle équilatéral



- de $\mathbb{R}^3$:

tétraèdre régulier