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

Dans tout le cours, les ensembles concernées seront supposés finis et non vide.

## 1 Introduction aux permutations

### 1.1 Groupe symétrique

**Définition 1** (BER 201)**.** L'ensemble des bijections de E sur lui-même est un groupe pour la composition des applications, appelé groupe des permutations de E ou groupe symétrique sur E, et est noté $\mathfrak{S}(E)$. Un élément de $\mathfrak{S}(E)$ est appelé une permutation.

**Exemple 2** (BER 199)**.** Dans l'ensemble des exemples de cette leçon, on se placera dans le cas où $E = \{1, 2, ..., n\}$. On note généralement $\mathfrak{S}_n$ à la place de $\mathfrak{S}(E)$. Pour $\sigma \in \mathfrak{S}_n$, on note :
$(1 \quad 2 \quad ... \quad n \ )$
$(\sigma(1) \ \sigma(2)...\sigma(n))$ (Faire à la main flemme de perdre du temps ici) Par exemple, $(1234)( \ 3 \ 2 \ 1 \ 4)$ est la permutation de $\mathfrak{S}_4$ définie par $\sigma(1) = 3$, $\sigma(2) = 2$, $\sigma(3) = 1$, $\sigma(4) = 4$

Dans le reste du cours, on désignera par $\sigma$ une permutation de $\mathfrak{S}(E)$.

**Proposition 3** (BER 200)**.** Si le cardinal de $E$ est $n$, alors $\mathfrak{S}(E)$ est d'ordre $n!$.

**Théorème 4** (BER 199)**.** Soient $E, E'$ deux ensembles non vides. Si $E$ et $E'$ sont en bijection, alors $\mathfrak{S}(E)$ et $\mathfrak{S}(E')$ sont isomorphes.

**Exemple 5** (BER 200)**.** Soit $E$ un ensemble à $n$ éléments $a_1, ..., a_n$. Alors il existe une bijection entre $E$ et $\{1, ..., n\}$ qui à $i$ associe $a_i$. On a alors que $\mathfrak{S}(E)$ est isomorphe à $\mathfrak{S}_n$. Ceci explique pourquoi on pourrait ramener l'étude à $\mathfrak{S}_n$.

**Théorème 6** (ROM 21, BER 177)**.** [thm de Cayley, Résultat de la théorie des actions de groupes qui motive l'étude de $\mathfrak{S}(E)$] Tout groupe $G$ est isomorphe à un sous groupe de $\mathfrak{S}(G)$.

**Remarque 7** (No ref)**.** Le théorème précédent motive notre étude de $\mathfrak{S}(E)$ (et notamment de ses sous-groupes).

### 1.2 Support et points fixes d'une permutation

**Définition 8** (BER 200)**.** Le support d'une permutation $\sigma$ est l'ensemble $Supp(\sigma) = \{a \in E | \sigma(a) \neq a\}$.

**Proposition 9** (BER 200 1) 4) + BER 201)**.** Soient $\sigma, \rho \in \mathfrak{S}(E)$ .

1. $\sigma(Supp(\sigma)) = Supp(\sigma)$
2. $Supp(\sigma\rho) \subset Supp(\sigma) \cup Supp(\rho)$
3. Si $Supp(\sigma) \cap Supp(\rho) = \emptyset$ alors $\sigma$ et $\rho$ commutent.Pas retrouvé ref :Si de plus $\sigma\rho = id$ on a $\sigma = \rho = id$

**Définition 10** (no ref, un peu BER 200)**.** $i \in E$ est un point fixe de $\sigma$ si $\sigma(i) = i$.

**Exemple 11** (No ref)**.** Reprenons la permutation de $\mathfrak{S}_4$ vu dans le première exemple. 1 et 3 appartiennent au support de $\sigma$ tandis que 2 et 4 sont des points fixes de $\sigma$.

### 1.3 Orbites et cycles

**Définition 12** (BER 202)**.** Pour $x \in E$ et $\sigma$, on définit la $\sigma$-orbite de $x$ (raccourcit orbite lorsque la permutation concerné est évidente) l'ensemble $\mathcal{O}_\sigma(x) = \{\sigma^k(x) | k \in \mathbb{Z}\}$.

**Remarque 13** (BER 202)**.** On peut aussi définir les orbites d'une permutation $\sigma$ comme les orbites de l'action naturelle de $< \sigma >$ sur $E$.

**Proposition 14** (BER 202)**.** Les différentes $\sigma$-orbites forment une partition de $E$ et la réunion des $\sigma$-orbites non réduites à un singleton est égale au support de $\sigma$.

**Définition 15** (BER 202)**.** Une permutation $\sigma$ est un cycle s'il n'existe qu'une seule $\sigma$-orbite non réduite à un singleton. Si $p \geq 2$ est le nombre d'éléments de $Supp(\sigma)$, on dit que $\sigma$ est un $p$-cycle. Un 2-cycle est appelée une transposition.

**Notation 16** (No ref)**.** Soit $\sigma$ est un $p-$cycle et $Supp(\sigma) = \{x_0, .., x_{p-1}\}$ avec $\sigma(x_i) = x_{i+1}$ où les indices sont pris modulo $p$. On note alors ce $p-$cycle $(x_0\ x_1\ ...\ x_{p-1})$

**Exemple 17** (No ref)**.** Les $\sigma$-orbites de notre exemple (réécrire) sont $\mathcal{O}_\sigma(1) = \{1, 3\} = \mathcal{O}_\sigma(3)$, $\mathcal{O}_\sigma(2) = \{2\}$ et $\mathcal{O}_\sigma(4) = \{4\}$. Une seule orbite n'est pas réduite à un élément, notre permutation est donc un 2-cycle, c'est à dire une transposition. Remarquons également que l'on obtient bien une partition de notre ensemble.

**Notation 18** (BER 203)**.** Dans la suite, $\Omega^*$ représentera l'ensemble des $\sigma$-orbites non réduites à un seul élément.

**Proposition 19** ( ROM 38 )**.** Soit $\sigma \in \mathfrak{S}(E)$, $p \geq 2$ et soit $(a_1, ..., a_p)$ un p-cycle. On a : $\sigma(a_1, ..., a_p)\sigma^{-1} = (\sigma(a_1), ..., \sigma(a_p))$.

**Proposition 20** (ROM 38)**.** Soit $p \geq 2$. Un $p$-cycle est d'ordre $p$.

# 2 Résultats sur les groupes symétriques et alternés

## 2.1 Décomposition en produit de cycles et de permutations

**Lemme 21** (BER 202, ROM 41)**.** Soit $\omega$ une $\sigma$-orbite à $p$ éléments et soit $a \in \omega$. Alors, $p$ est le plus petit entier positif tel que $\sigma^p(a) = a$ et on a $w = \{a, \sigma(a), ..., \sigma^{p-1}(a)\}$.

**Lemme 22** (BER 203)**.** Soit $\omega \in \Omega^*$. On définit $\sigma_\omega \in \mathfrak{S}(E)$ par $\sigma_\omega(a) = \sigma(a)$ si $a \in \omega$ et $\sigma_\omega(a) = a$ si $a \notin \omega$. Alors $\sigma_\omega$ est un cycle de support $\omega$, et pour tout $a \in \omega$, on a $\sigma_\omega = (a\ \ \sigma(a)\ ...\ \sigma^{p-1}(a))$, où p est le nombre d'éléments dans $\omega$.
De plus, tout $p$-cycle est de cette forme.

**Théorème 23** ( BER 204, ROM42 DEV 1)**.** Soit $\sigma \in \mathfrak{S}(E)$. Alors $\sigma$ se décompose en produit de cycles à support disjoints, et cette décomposition est unique à l'ordre des facteurs près. Cette décomposition est donnée par : $\sigma = \prod_{\omega \in \Omega^*} \sigma_\omega$ où $\Omega^*$ représente l'ensemble des $\sigma$-orbites non réduite à un singleton.

**Corollaire 24** (BER 206, DEV 1)**.** $\mathfrak{S}(E)$ est engendré par

1. les cycles.
2. les transpositions.

**Corollaire 25** (BER 207, DEV 1)**.** $\mathfrak{S}_n$ est engendré par

1. les transpositions $(k\ k+1)$ pour $1 \leq k \leq n-1$
2. les transpositions $(1\ k+1)$ pour $1 \leq k \leq n-1$
3. $(12)$ et $(1\ 2\ ...\ n\ )$

**Exemple 26** (BER 206 + no ref)**.** Soit $\sigma \in \mathfrak{S}_8$ donné par $\sigma = (1\ 2\ 3\ 5)(3\ 7)(7\ 4\ 8)$. Grâce à l'étude faite en annexe 1, on trouve $\sigma = (1\ 2\ 3\ 7\ 4\ 8\ 5)$. On peut ensuite décomposer cette permutation en produit de transposition : $(1\ 2)(2\ 3)(3\ 7)(7\ 4)(4\ 8)(8\ 5)(5\ 1)$

## 2.2 Signature et groupe alterné

**Définition 27** (No ref, appuyé sur BER 214, ROM 47)**.** On définit la signature de $\sigma$ par l'élément $\epsilon(\sigma) = (-1)^r$, où r est le nombre de transposition dans la décomposistion en transposition de $\sigma$.

**Exemple 28** (BER 214)**.** La signature d'un $p$-cycle $\sigma$ est $(-1)^{p-1}$.

**Proposition 29** (No ref, appuyé sur BER 214, ROM 47)**.** La signature est un morphisme.

**Définition 30** (BER 215)**.** Le groupe alterné, noté $\mathfrak{A}(E)$, est l'ensemble des permutations de $\mathfrak{S}(E)$ de signature 1.

**Proposition 31** (BER 215)**.** $\mathfrak{A}(E)$ est un sous groupe distingué de $\mathfrak{S}(E)$ de cardinal $\frac{n!}{2}$.

**Proposition 32** ( BER 216)**.** Soit $E$ un ensemble à $n$ éléments. Si $n \geq 3$, le groupe alterné $\mathfrak{A}(E)$ est engendré par chacune des familles suivantes :

1. les produits de deux transpositions
2. les 3-cycles.

**Théorème 33** (BER 217)**.** [DVP 2] Soit $E$ un ensemble à $n \geq 3$ éléments. Montrer que le groupe alterné $\mathfrak{A}(E)$ est simple si et seulement si $n \neq 4$.

# 3 Application

## 3.1 Déterminant d'une matrice

Soit $M = (m_{i,j})_{i,j} \in M_n(\mathbb{K})$.

**Définition 34** (BER 69, ROM 550 ). Le déterminant de $M$ est la valeur $\sum_{\sigma \mathfrak{S}(n)} \epsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i),i}$.

**Application 35** (No ref). Grâce au déterminant on peut calculer les sommes

$$\sum_{\sigma \in \mathfrak{S}(n)} \epsilon(\sigma); \sum_{\sigma \in \mathfrak{S}(n)} \epsilon(\sigma)\nu(\sigma) ; \sum_{\sigma \in \mathfrak{S}(n)} \frac{\epsilon(\sigma)}{\nu(\sigma)+1}$$

## 3.2 Dérangement d'un ensemble fini

Dans cette sous partie, considérons $I_n = \{1, 2..., n\}$ pour tout $n \geq 2$.

**Définition 36** (ROM 51). On appelle dérangement de $I_n$ toute permutation $\sigma$ de cet ensemble n'ayant aucun point fixe.

**Notation 37** (ROM 51). On note $\delta_n$ le nombre de dérangements de $I_n$ et on prendra la convention $\delta_0 = 1$ et $\delta_1 = 0$.

**Lemme 38** (ROM 51). Pour tout $n \in \mathbb{N}$, on a : $n! = \sum_{k=0}^{n} \binom{n}{k} \delta_k$

**Théorème 39** (ROM 51). Pour tout $n \in \mathbb{N}$, le nombre de dérangement de $I_n$ est $\delta_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

**Corollaire 40** (ROM 51). Pour tout $n \in \mathbb{N}$, le nombre de permutation de $I_n$ avec r points fixes est $\binom{n}{r}\delta_{n_r} = \frac{n!}{r!} \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}$.

## 3.3 Fonctions symétriques élémentaires

Permet de relier racines et coefficients

**Définition 41** (ROM 367). Soit $n \in \mathbb{N}$. On définit les fonctions symétriques élémentaires $\sigma_{n,k} : \mathbb{K}^n \to \mathbb{K}$, l'entier $k$ étant compris entre 0 et $n$, par : $\forall \alpha = (\alpha_i)_{1 \leq i \leq n} \in K^n$,

$$\sigma_{n,k}(\alpha) = \begin{cases} 1 & \text{si } k = 0 \\ \sum_{1 \leq i_1 \leq ... \leq i_k \leq n} \alpha_{i_1} ... \alpha_{i_k} & \text{si } k \in \{1, ..., n\} \end{cases}$$

**Exemple 42** (ROM 367). $\sigma_{n,1}(\alpha) = \sum_{i=1}^{n} \alpha_i$ et $\sigma_{n,n}(\alpha) = \prod_{i=1}^{n} \alpha_i$.

**Remarque 43** (ROM 367). La qualification "symétrique" vient du fait que pour toute permutation $\tau \in S_n$ , on a $\sigma_{n,k}(\alpha_{\tau(1)}, .., \alpha_{\tau(n)}) = \sigma_{n,n}(\alpha) = \prod_{i=1}^{n} \alpha_i$

**Théorème 44** (ROM 368). Si $P(X) = \prod_{k=1}^{n} (X - \alpha_k)$ est un polynôme unitaire de degré $n \geq 1$ scindé dans $\mathbb{K}[X]$, on a alors $P(X) = \sum_{k=0}^{n} a_k X^{n-k}$ avec $\forall k \in \{0, 1, .., n\}, a_k = (-1)^k \sigma_{n,k}(\alpha_1, .., \alpha_n)$.

**Application 45** (ROM 369 - 370). [Poincaré] Formule de Poincaré : Si $(A_k)_{1 \leq k \leq n}$ est une suite d'évènements d'un espace probabilisé $(\Omega, \mathcal{B}, \mathbb{P})$, on a alors :

$$\mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < ... < i_k \leq n} \mathbb{P}(A_{i_1} \cap ... \cap A_{i_k})$$

## 3.4 Matrice de permutation

On désignera par $\mathbb{K}$ un corps commutatif.

**Définition 46** (ROM 51). La matrice de permutation $P_\sigma$ associée à $\sigma \in \mathfrak{S}_n$ est la matrice de passage de la base canonique $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ de $\mathbb{K}$ à la base $\mathcal{B}_\sigma = (e_{\sigma(j)})_{1 \leq j \leq n}$

**Exemple 47** (No ref). Reprenons la permutation $\sigma = (13) \in \mathfrak{S}_4$. La matrice associé est $P_\sigma = (0010, 0100, 1000, 0001)$.

**Théorème 48** (ROM 54). L'application $P : \sigma \mapsto P_\sigma$ est un morphisme de groupe injectif de $\mathfrak{S}_n$ dans $GL_n(\mathbb{K})$. De plus, pour toute permutation $\sigma \in \mathfrak{S}_n$, on a $det(P) = \epsilon(\sigma)$

**Corollaire 49** (ROM 54). Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p) = \frac{\mathbb{Z}}{p\mathbb{Z}}$ et $p \geq 2$ est un nombre premier.