Chapitre 2 : Groupes symétriques

I Permutations

Définition : Soient X un ensemble et $S(X)$ l'ensemble des bijections de X dans X.
On appelle permutation de X tout élément de $S(X)$.

Intuitivement, c'est l'ensemble des réarrangements des éléments de X.

Propriété : Ensemble des permutations *(admise)*
$(S(X), \circ)$ est un groupe *(en général non commutatif)*.

Vocabulaire : C'est le groupe symétrique sur X.

Démonstration :

- La composée de deux bijections est une bijection, donc $\circ$ est une loi interne sur $S(X)$.
- La loi $\circ$ est associative.
- L'élément neutre est l'identité id_X.
- L'inverse d'une bijection est une bijection (la bijection réciproque). $\square$

Proposition :
Soit Y un ensemble avec une bijection $b : X \to Y$.
L'application $\varphi_b : S(X) \to S(Y)$ définie par $\sigma \mapsto b \circ \sigma \circ b^{-1}$ est un isomorphisme de groupe.

Note de rédaction : À quoi ça sert ? Permet de montrer que le groupe symétrique ne dépend pas de l'ensemble, mais seulement de son cardinal.

Remarque : Donc $S(Y)$ est isomorphe à $S(X)$.

Démonstration :
φ_b est bien définie : comme b et σ sont bijectives, $b \circ \sigma \circ b^{-1}$ est bijective.
φ_b est un morphisme $\forall \sigma, \sigma' \in S(X)$. On a :

$$\varphi_b(\sigma \circ \sigma') = b \circ (\sigma \circ \sigma') \circ b^{-1} = b \circ \sigma \circ b^{-1} \circ b \circ \sigma' \circ b^{-1} = (b \circ \sigma \circ b^{-1}) \circ (b \circ \sigma' \circ b^{-1}) = \varphi_b(\sigma) \circ \varphi_b(\sigma')$$

φ_b est bijective car sa réciproque est donnée par $\tau = b^{-1} \circ \tau \circ b$. $\square$

Définition : Supposons X fini de cardinal n.
Il existe une bijection $\{1, 2, .., n\} \to X$ (numérotation de X).
On prend $S_n = S(1, 2, ...n)$: c'est le **groupe symétrique sur n lettres**. Il est isomorphe à $S(X)$

Notation par tableau : σ

$$\begin{array}{c|ccccc} i & 1 & 2 & 3 & \cdots & n \\ \hline \sigma(i) & \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{array}$$

Définition : Soit $\sigma \in S(X)$.
Le support de σ est $\{x \in X \mid \sigma(x) \neq x\}$.

Intuitivement, c'est l'ensemble des éléments de X que σ "déplace".

Exemple : Prenons $S(X) = S_6$.

i	1	2	3	4	5	6
$\sigma(i)$	3	2	1	6	5	4

σ a pour support $\{1, 3, 4, 6\}$.

Proposition :

Soient $\sigma, \sigma' \in S(X)$ de supports disjoints.
Alors σ et σ' commutent, *i.e.* $\sigma \circ \sigma' = \sigma' \circ \sigma$

Démonstration :
Soient S et S' les supports de σ et σ'. On a $\sigma \circ \sigma'(x) = \sigma'(\sigma(x)) = \sigma'(x)$.
On a $\sigma'(x) \notin S$, sinon $\sigma'(x) \notin S'$ et $\sigma'(\sigma'(x)) = \sigma'(x)$
donc $\sigma'(x) = x$, donc $\sigma'(x) \notin S$.
Donc $\sigma \circ \sigma'(x) = \sigma'(x) = \sigma' \circ \sigma(x)$.

De même, si $x \in X - S'$, on a : $\sigma \circ \sigma'(x) = \sigma' \circ \sigma(x)$.
Comme $S \cap S' = \emptyset$, on a : $\sigma \circ \sigma'(x) = \sigma' \circ \sigma(x)\ \forall x \in X$. $\square$

Propriété : Ordre de S_n

Le groupe S_n est d'ordre $n!$.

Démonstration :
Soient X,Y deux ensembles à n éléments.
Montrons que $\#\{bijections X \to Y\} = n!$.
En effet, si $X = x_1, ..., x_n$ et $f : X \to Y$ est une bijection, il y a :

- n possibilités pour $f(x_1)$
- $n - 1$ possibilités pour $f(x_2)$
  $\vdots$
- 1 possibilité pour $f(x_n)$

II Cycles

Définition : Soit X un ensemble et soit $k \geq 2$ un entier.
Un k-cycle de $S(X)$ est donné par $a_1, a_2, \ldots, a_k \in X \mid a_i \neq a_j sii \neq j$.

et $\sigma(a_i) = a_{i+1}$ pour $1 \leq i < k$ et $\sigma(a_k) = a_1$ et σ de support $a_1, a_2, ...na_k$.
On le note $(a_1 \cdots a_k)$.

Exemple : Soit $X = \{1, 2, 3, 4, 5\}$.
Alors $(1\ 3\ 4)$ est un 3-cycle de $S(X)$ défini par :

i	1	2	3	4	5
$\sigma(i)$	3	2	4	1	5

Remarque : Un k-cycle est juste une notation compacte pour une permutation, par exemple :
$(a_1 a_2 \cdots a_k)$ est la permutation σ définie par :
$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$ et $\sigma(x) = x$ si $x \notin \{a_1, a_2, \ldots, a_k\}$.

✕ Attention ✕ La notation n'est pas unique : $(a_i a_{i+1} \cdots a_k a_1 a_2 \cdots a_{i-1}) = (a_1 \cdots a_k)$

Vocabulaire : On dit qu'une permutation c est un cycle s'il existe $k \geq 2 \mid c$ est un k-cycle. Alors k s'appelle la **longueur** de c.

Proposition :

Comme élément du groupe $S(X)$ un k-cycle c est d'ordre k.

Démonstration :
Posons $c = (a_1 \cdots a_k)$.
On a $\varepsilon(a_1) = a_{1+j} \neq a_1$.
Donc $ordre(c) \geq k$. On a $c^k(a_i) = a_i \forall i$, donc c est d'ordre k. $\square$

Remarque : Rappel
Des cycles à supports disjoints communtent.
Soient $c = (a_1 \cdots a_k)$ et $c' = (a'_1 \cdots a'_{k'})$ deux cycles de $S(X)$ tels que $S(c) \cap S(c') = \emptyset$.
avec $a_1, \ldots, a_k \cap a'_1, \ldots, a'_{k'} = \emptyset$.
On a $c \circ c' = c' \circ c$

Définition : Soit $x \in X$, l'**orbite de** x **sous** σ est $\{\sigma^m(x) \mid m \in Z\}$.

Remarque : On a $x \notin Support(\sigma)$ si $\sigma(x) = x \Leftrightarrow$ orbite de x est un singleton.
Si σ est un k-cycle de support S et $x \in S$, l'orbite de x a k éléments, c'est S.

Théorème :

Si X est fini, tout élément de $S(X)$ s'écrit comme produit de cycles à supports disjoints.
Cette écriture est unique à l'ordre des facteurs près.

Démonstration :

- **Existence :** (par récurrence)
  Si $Support(\sigma) = \emptyset$, on a $\sigma = id_X$: c'est bien un produit (vide) de cycles.
  Supposons maintenant que $Support(\sigma) \neq \emptyset$. Soit $x \in Support(\sigma)$.
  Soit $\sigma' \in S(X)$ donnée par $\sigma'(y) = \sigma(y)$ si $y \notin$ orbite de x, $\sigma'(y) = y$ sinon.
  Considérons le cycle c donné par : $(x\sigma(x)\sigma^2(x) - \sigma^k(x))$ avec $k = min\{m \mid \sigma^m(x) = x\}$.
  C'est un k-cycle de support l'orbite de x.
  Si $y \in$ orbite de x on a $\sigma(y) = c(y)$.
  Alors σ et c sont de supports disjoints et on a : $\sigma = \sigma' c = c\sigma'$.
  En effet, soit $y \in X$,
  $y \notin$ orbite de x on a $\sigma'(y) = c(y)$

✕ Attention ✕ Démonstration non terminée *(le prof n'écrivait pas clair au tableau)*

Exemple : Soit $X = \{1, 2, 3, 4, 5\}$ et $\sigma \in S(X)$ défini par :

$$\sigma(1) = 3, \quad \sigma(2) = 5, \quad \sigma(3) = 1, \quad \sigma(4) = 4, \quad \sigma(5) = 2$$

Alors σ s'écrit comme produit de cycles à supports disjoints :

$$\sigma = (1\ 3)(2\ 5)$$

Cette écriture est unique à l'ordre des facteurs près.

III Signature

Définition : Soit X un ensemble fini et notons $S(X)$ le groupe symétrique sur X.
Posons $Z = \{(i, j) \mid i, j \in X, i \neq j\}$.
Soit R la relation sur Z donnée par : $(i, j)R(i', j') \Leftrightarrow (i, j) = (i', j')$ ou $(i, j) = (j', i')$. *(i.e. $\{i, j\} = \{i', j'\}$).*
C'est une relation d'équivalence. Soit S un système de représentants de R.

Soit $\sigma \in S(X)$.
Alors si $(i, j) \in Z$, on a $(\sigma(i), \sigma(j)) \in Z$.
De plus, $(i, j) \mapsto (\sigma(i), \sigma(j))$ est une bijection de Z notée σ^2.

Soit $(i, j) \in S$.
On dit qu'on a une **inversion** en (i, j) pour σ si $(\sigma(i), \sigma(j)) \notin S$.

Exemple : Si $X = 1, 2, \ldots, n$, on peut prendre $S = \{(i, j) \in X^2 \mid i < j\}$.
Alors $(i, j) \in S$ est une inversion pour $\sigma \Leftrightarrow \sigma(j) < \sigma(i)$.

Propriété : Signature

On pose $\varepsilon_S(\sigma) = (-1)^{\#\{\text{inversions de } \sigma\}} \in \{-1, 1\}$. On a $\varepsilon_S(\sigma)$ ne dépend pas du choix de S.
On le note $\varepsilon(\sigma)$ et on l'appelle la **signature** de σ.

Démonstration :
Soit $(i_0, j_0) \in S$. Posons $S' = S - \{(i_0, j_0)\} \cup \{(j_0, i_0)\}$.
Si $(i, j) \neq (i_0, j_0)$ et $(i, j) \neq (j_0, i_0)$, on a $(i, j) \in S$ est une inversion pour $S \Leftrightarrow (i, j) \in S'$ est une inversion pour S'.
Si $(i, j) = (i_0, j_0)$, on a $(i, j) \in S \backslash S'$ et $(j, i) \in S' \backslash S$.
On a une inversion (i_0, j_0) pour $S \Leftrightarrow$ on a une inversion (j_0, i_0) pour S'.
Donc $\#\{\text{inversions de } \sigma \text{ pour } S\} \equiv \#\{\text{inversions de } \sigma \text{ pour } S'\}$.
Donc $\varepsilon_S(\sigma) = \varepsilon_{S'}(\sigma)$ de proche en proche on a ε_S indépendant de S. $\square$

Proposition :

Soit $f : X \to Y$ injective.
On a :

$$\varepsilon(\sigma) = \prod_{(i,j)\in S} \frac{f(\sigma(j)) - f(\sigma(i))}{f(j) - f(i)}$$

Exemple : Si $X = \{1, 2, \ldots, n\}$ et $f = id_X$, on a :

$$\varepsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Démonstration :
On a $(\sigma(i), \sigma(j)) \in S \Leftrightarrow (i, j)$ est une inversion.
Sinon, on a $(\sigma(j), \sigma(i)) \in S$.
Donc :

$$\prod_{(i,j)\in S} \frac{f(\sigma(j)) - f(\sigma(i))}{f(j) - f(i)} = \prod_{\substack{(i,j)\in S \\ \text{pas une inversion}}} \frac{f(\sigma(j)) - f(\sigma(i))}{f(j) - f(i)} \times \prod_{\substack{(i,j)\in S \\ \text{inversion}}} \frac{f(\sigma(j)) - f(\sigma(i))}{f(j) - f(i)}$$

$$= \prod_{(i,j)\in S} \frac{1}{f(j) - f(i)} \times \prod_{\substack{(i,j)\in S \\ \text{inversion}}} (f(\sigma(j)) - f(\sigma(i))) \times \prod_{\substack{(i,j)\in S \\ \text{pas une inversion}}} (f(\sigma(j)) - f(\sigma(i)))$$

Si $S = \{(\sigma(i), \sigma(j)) \mid \sigma$ pas une inversion sur $S \cup \{(\sigma(j), \sigma(i)) \mid \sigma$ inversion sur $S\}\}$.
Donc : ✗ **Attention** ✗ Démonstration non terminée *(le prof n'écrivait pas clair au tableau et c'était verbeux)*

Théorème : Signature et morphisme

La signature est un morphisme de groupe de $S(X)$ dans $\{-1, 1\}$.
i.e. $\forall \sigma, \varrho \in S(X)$, on a : $\varepsilon(\sigma \circ \varrho) = \varepsilon(\sigma) \times \varepsilon(\varrho)$.

Démonstration :

Lemme : ***pour démontrer le théorème***

On a $\sigma^2(S) = \{(\sigma(i), \sigma(j)) \mid (i, j) \in S\}$ est un système de représentants de R.

Note de rédaction : Demander la démonstration à Laurent

Définition : Soit $\sigma \in S(X)$.
Si $\varepsilon(\sigma) = 1$, on dit que σ est une **paire**.
Si $\varepsilon(\sigma) = -1$, on dit que σ est une **impaire**.

Proposition :

On pose $\mathcal{A}(X) = \{\sigma \in S(X) \mid \varepsilon(\sigma) = 1\}$.
C'est un sous-groupe de $S(X)$ appelé le **groupe alterné** sur X.

En particulier, si $X = \{1, 2, \ldots, n\}$, on le note $\mathcal{A}_n$. (groupe alterné sur n lettres)
Et on a $\#\mathcal{A}_n = ord(\mathcal{A}_n) = \frac{n!}{2}$ pour $n \geq 2$.

Démonstration :
On a $\mathcal{A}(X) = \{\sigma \in S(X) \mid \varepsilon(\sigma) = 1\} = Ker(\varepsilon)$, donc c'est un sous-groupe de $S(X)$.
Supposons que $\mathcal{A}_n$ a un élément τ de signature -1, c'est vrai si $n \geq 2$.
Alors $S(X) = \mathcal{A}(X) \cup \tau\mathcal{A}(X)$ et $\mathcal{A}(X) \cap \tau\mathcal{A}(X) = \emptyset$.
En effet, si $\sigma \in \mathcal{A}(X)$ OK. Sinon si $\sigma \notin \mathcal{A}(X)$, on a $\varepsilon(\sigma) = -1$ et donc $\varepsilon(\sigma\tau^{-1}) = -1 \times -1 = 1$, donc $\sigma\tau^{-1} \in \mathcal{A}(X)$ et $\sigma \in \tau\mathcal{A}(X)$.
On a $\mathcal{A}(X) \cap \tau\mathcal{A}(X) = \emptyset$.
On a une bijection : $\underset{\sigma \mapsto \tau\sigma}{\mathcal{A}(X) \to \tau\mathcal{A}(X)}$.
Donc $\#\mathcal{A}(X) = \#\tau\mathcal{A}(X)$ et $\#S(X) = 2\#\mathcal{A}(X)$.
Donc $\#\mathcal{A}(X) = \frac{\#S(X)}{2}$. Donc $\#\mathcal{A}_n = \frac{n!}{2}$ pour $n \geq 2$. $\square$

IV Transpositions

Définition : Une transposition de X est un 2-cycle. On la note $(a\ b)$.

Propriété : Transpositions et signature

Soit $\sigma \in S(X)$ une transposition.
On a $\varepsilon(\sigma) = (-1)$. (une transposition existe ssi $\#X \geq 2$)

Note de rédaction : Il y a une erreur dans la démonstration du prof, on ne l'a pas notée.

Formulaire :

Soit $c = (a_1 \cdots a_k)$ un l-cycle.

1. On a $c = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k)$ *i.e. c'est un produit de transpositions*.
2. Soit $\sigma \in S(X)$.
   On a $\sigma c \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$ (formule de conjugaison).
3. Soient $c_1, \ldots, c_k$ des cycles.
   On a $\sigma c_1 \cdots c_k \sigma^{-1} = (\sigma c_1 \sigma^{-1}) \cdots (\sigma c_k \sigma^{-1})$.

Note de rédaction : Démonstration laissée à l'appréciation du lecteur.

Corollaire :

Le groupe $S(X)$ est engendré par les transpositions.
i.e. toute permutation σ de $S(X)$ s'écrit comme produit de transpositions $\sigma = \tau_1 \cdots \tau_r$ et $\varepsilon(\sigma) = (-1)^k$. (non unique)

Note de rédaction : Démonstration laissée à l'appréciation du lecteur.

Proposition :

Soit c un cycle de longueur l.
Alors $\varepsilon(c) = -(-1)^l = (-1)^{l-1}$.

Démonstration :
On a $c = (a_1 a_2 \cdots a_l) = (a_1 a_2)(a_2 a_3) \cdots (a_{l-1} a_l)$, donc c est produit de $l-1$ transpositions.
Donc $\varepsilon(c) = \varepsilon((a_1 a_2)) \times \cdots \times \varepsilon((a_{l-1} a_l)) = (-1)^{l-1}$. $\square$

Exemple : Soit $\sigma \in S_{12}$ donné par :

i	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(i)$	10	8	7	4	2	9	1	12	3	11	5	6

Elle vaut $(1\ 10\ 11\ 5\ 2\ 8\ 12\ 6\ 9\ 3\ 7)$.
Donc $\varepsilon(\sigma) = (-1)^{11-1} = 1$.

V Compléments sur les groupes cycliques

Proposition : Ordre d'une permutation

Soit G un groupe et $g \in G$ d'ordre fini n.
L'application $exp_g : \begin{smallmatrix} \mathbb{Z} \to G \\ k \mapsto g^k \end{smallmatrix}$ se factorise *(i.e. passe au quotient)* par $\mathbb{Z}/n\mathbb{Z}$.
L'application quotient est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur $g^{\mathbb{Z}} = \{g^k \mid k \in \mathbb{Z}\}$.

Corollaire :

Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration de la proposition :
Il faut montrer que si $k, k' \in \mathbb{Z}$ et $k \equiv k'[n]$, alors $exp_g(k) = exp_g(k')$.
Comme $k \equiv k'[n]$, $\exists t \in \mathbb{Z}$ tel que $k' - k = tn$ et donc $k' = k + tn$.
On a $exp_g(k') = exp_g(k + tn) = g^{k+tn} = g^k (g^n)^t = g^k e_G = g^k = exp_g(k)$. $\square$

Pour $k \in \mathbb{Z}$, notons $f(\overline{k}) = exp_g(k)$.
On a $f(\overline{k} + \overline{k'}) = f(\overline{k + k'}) = exp_g(k + k') = g^{k+k'} = g^k g^{k'} = f(\overline{k}) + f(\overline{k'})$.
Donc f est un morphisme de groupe.
Pour $k \in \mathbb{Z}$, on a $f(\overline{k}) = g^{\mathbb{Z}}$. Donc $Im(f) = g^{\mathbb{Z}}$.
Montrons f injective.
Soit $k \in \mathbb{Z}$ tel que $f(\overline{k}) = e_G$.
On a $g^k = e_G$. Donc $n \mid k$ et donc $\overline{k} = \overline{0}$. $\square$