II.5 Groupes symétriques

II.5.a Généralités

Définition II.5.a.1 *Les bijections d'un ensemble E sur lui-même sont appelés* ***permutations*** *ou* ***substitutions*** *de E, ils forment le* ***groupe symétrique*** *de E, noté $\mathfrak{S}(E)$.*
Pour $E_n = \{1, 2, ..., n\}$, on note $\mathfrak{S}_n = \mathfrak{S}(E_n)$.

Notation II.5.a.2 *Si $E = \{x_1, x_2, \ldots, x_n\}$, on écrit un élément s de $\mathfrak{S}(E)$ sous la forme :*

$$s = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ s(x_1) & s(x_2) & \ldots & s(x_n) \end{pmatrix}$$

Exemple II.5.a.3 *Soit $s \in \mathfrak{S}_6$ définie par :*

$$s(1) = 2\ ,\ s(2) = 4\ ,\ s(3) = 5\ ,\ s(4) = 6\ ,\ s(5) = 3\ ,\ s(6) = 1\ .$$

s se note alors :

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,5\,6\,3\,1 \end{pmatrix}\ .$$

Produit ou composé Le produit $s\,t$ de deux éléments s et t de $\mathfrak{S}_n$ n'est autre que la composée $s \circ t$. Ce produit n'est donc pas commutatif en général, il s'effectue de droite à gauche.

Exemple II.5.a.4 *Dans $\mathfrak{S}_5$,*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

Remarque II.5.a.5 *On peut omettre d'écrire les* ***points fixes****, c-à-d. les k tels que $s(k) = k$. Il faut alors préciser la valeur de n, surtout si n est un point fixe.*

Exemple II.5.a.6 *Dans $\mathfrak{S}_5$,*

$$\begin{pmatrix} 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Dans tout ce qui suit, E désignera un ensemble fini de cardinal n.

Proposition II.5.a.7 *Le groupe symétrique d'un ensemble quelconque de cardinal n est isomorphe à $\mathfrak{S}_n$.*

Démonstration. Si E est un ensemble de cardinal n, il existe une bijection f de E sur E_n. L'application $\varphi : S(E) \to \mathfrak{S}_n \,;\, s \mapsto \varphi(s) = f \circ s \circ f^{-1}$ est alors isomorphisme de groupes : $\varphi^{-1} = s \mapsto f^{-1} \circ s \circ f$ et $\varphi(s \circ t) = \varphi(s) \circ \varphi(t)$. □

Cela justifie de restreindre notre étude dans la suite à $\mathfrak{S}_n$. fin 8e cours 2.10.03

II.5.b Orbite d'un élément

Définition II.5.b.1 *Soient $s \in \mathfrak{S}_n$ et $i \in E_n$. On appelle **orbite** de i suivant s l'ensemble*

$$O_s(i) = \left\{ s^k(i) \;;\; k \in \mathbb{Z} \right\} \;,$$

Remarque : on peut se limiter à des exposants entre 0 et $p = \operatorname{card} O_s(i) \leq n$, car on ne peut obtenir plus de n éléments différents dans E_n.

Exemple II.5.b.2 *Soit $s \in \mathfrak{S}_7$ définie par*

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,4\,5\,7\,3\,6\,1 \end{pmatrix} \qquad \begin{array}{l} O_s(1) = \{\,1,2,4,7\,\} \\ O_s(3) = \{\,3,5\,\} \;,\quad O_s(6) = \{\,6\,\} \;. \end{array}$$

Remarque II.5.b.3 *Les orbites sont les classes d'équivalence pour la relation*

$$\forall i,j \in E_n : i \,\Re\, j \iff \exists k \in \mathbb{Z} : i = s^k(j)$$

qui est en effet une relation d'équivalence sur E_n. (Exercice !)

Proposition II.5.b.4 *Soient $s \in \mathfrak{S}_n$, $i \in E_n$ et $p = \operatorname{card} O_s(i)$ le cardinal de l'orbite de i suivant s. Alors pour tout $j \in O_s(i)$,*

$$\begin{aligned} O_s(j) &= O_s(i) \\ \text{et} \quad s^p(j) &= j. \end{aligned}$$

Démonstration. Soit $j \in O_s(i)$, c-à-d. $\exists k \in \mathbb{Z} : j = s^k(i)$. Donc

$$O_s(j) = \left\{ s^m(s^k(i)) \;;\; m \in \mathbb{Z} \right\} = \left\{ s^{m+k}(i) \;;\; m \in \mathbb{Z} \right\} = O_s(i) \;.$$

Si $s^p(j) \neq j$, alors $s^p(j) \in O_s(j)$ doit être égal à un autre élément « précédent » de l'orbite, c-à-d. il y aurait $k \in \{\,1 \ldots p-1\,\}$ t.q. $s^p(j) = s^k(j)$, d'où aussi $s^{p-k}(j) = j$ et donc $O_s(j) = \left\{ j, s(j), \ldots, s^{p-k-1}(j) \right\}$ de cardinal $\operatorname{card} O_s(j) \leq p-k$ (les éléments se répètent déjà à partir de $s^{p-k}(j)$), contrairement à la définition de p. □

II.5.c Décomposition en cycles disjoints

Définition II.5.c.1 *On appelle* ***cycle*** *toute permutation $s \in \mathfrak{S}(E)$ admettant exactement une orbite qui ne soit pas réduite à un seul élément. Cette orbite est appelée le* ***support*** *du cycle ; son cardinal est dit* ***longueur*** *du cycle. Un cycle de longueur ℓ est aussi appelé ℓ–cycle.*

Remarque II.5.c.2 *On pourrait remplacer « exactement » par « au plus », ainsi l'application identité serait également un cycle, de longueur 1 par définition (voir plus bas) ; mais elle n'a bien sûr aucune orbite non-triviale.*

Exemple II.5.c.3 *Soit $s \in \mathfrak{S}_6$ définie par*

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 2\,4\,3\,6\,5\,1 \end{pmatrix} \qquad \begin{array}{l} O(1) = \{\ 1,2,4,6\ \} \\ O(3) = \{\ 3\ \} \\ O(5) = \{\ 5\ \} \end{array}$$

C'est donc un cycle, de support $O(1)$ et de longueur 4.

Notation II.5.c.4 *Soit s un cycle de $\mathfrak{S}_n$ de longueur ℓ. Soit i un élément du support de s. Alors s se note $(i\ s(i)\ s^2(i)\ \cdots\ s^{\ell-1}(i))$.*

C'est-à-dire, on écrit entre parenthèses les éléments de l'orbite dans l'ordre qu'on les obtient, en commençant avec l'un quelconque d'entre eux, et en appliquant $\ell - 1$ fois la permutation, afin de parcourir l'ensemble de l'orbite.

Exemple II.5.c.5 *Dans l'exemple précédent, s se note*

$$s = (1\ 2\ 4\ 6)\ .$$

Il est évident que la longueur ℓ d'un ℓ-cycle s est égale à l'ordre $|s|$ de cet élément du groupe $\mathfrak{S}_n$: toute puissance inférieure du cycle est différente de l'application identité (sur les éléments de son support), mais lorsque la puissance est égale à la longueur, on obtient bien l'application identité, élément neutre de $\mathfrak{S}_n$. (C'est donc compatible avec la convention que id_E est un 1–cycle.)

Plus généralement, on a l'importante :

Proposition II.5.c.6 *Tout élément s de $\mathfrak{S}_n$ s'écrit de façon unique (à l'ordre des facteurs près) comme produit de cycles disjoints (c-à-d. à supports disjoints). Ces cycles commutent entre eux et le ppcm des longueurs de ces derniers est égal à l'ordre de la permutation.*

Ici il faut bien sûr faire abstraction des 1–cycles, sinon il n'y a pas d'unicité, car on peut toujours composer par id_E un nombre arbitraire de fois. L'identité elle-même s'écrit comme un produit vide, par définition égal à l'élément neutre du groupe.
Cependant, il arrive qu'on rajoute dans cette écriture les points fixes x^* sous forme de 1–cycles $(\,x^*\,)$ à la fin du produit, pour mettre en évidence ces points fixes et en même temps l'ensemble de toutes les orbites.

Démonstration. Soit $s \in \mathfrak{S}_n$. L'ensemble des orbites,

$$O_s = \{\, O_s(i) \;;\; i \in E_n \,\} \;,$$

forme une partition de E_n. En effet, tout $i \in E_n$ appartient à une orbite, $O_s(i)$, et deux orbites sont disjoints ou confondues grâce à la Prop. II.5.b.4. Soit $p = \operatorname{card} O_s$ et $\{\, x_1, ..., x_p \,\}$ un système de représentants de cette partition, c-à-d.

$$O_s = \{\, O_s(x_1), ..., O_s(x_p) \,\} \text{ et } E_n = \bigcup_{k=1,...,p} O_s(x_k)$$

A chaque orbite $O_s(x_i)$ de cardinal ℓ_i, on associe le cycle

$$s_i = (x_i \; s(x_i) \; ... \; s^{\ell_i - 1}(x_i)) \text{ de longueur } \ell_i \;.$$

Par définition, $\forall x \in O_s(x_i) : s_i(x) = s(x)$ et $\forall x \notin O_s(x_i) : s(x) = x$. Cela implique que ces cycles commutent entre eux :

$$s_i \circ s_j(x) = s_j \circ s_i(x) \quad \forall x \in E_n$$

(que l'on peut aussi vérifier en distinguant les cas $x \in O_s(x_i)$ et $x \in O_s(x_j)$).

La composée $s_1 \circ ... \circ s_p$ a donc sur n'importe quel $x \in E_n$ le même effet que s, on a donc l'égalité

$$\begin{aligned} &s = (x_1, s(x_1), \ldots, s^{\ell_1 - 1}(x_1))(x_2, \ldots, s^{\ell_2 - 1}(x_2)) \ldots (x_p, \ldots, s^{\ell_p - 1}(x_p)) \\ &s = s_1 \circ s_2 \circ \cdots \circ s_p \;. \end{aligned}$$

D'autre part si

$$\begin{aligned} &m = ppcm(\ell_1, \ell_2, \ldots, \ell_p) \\ &\forall i \in \{1, \ldots, p\} : m = \ell_i (m/\ell_i) \in \ell_i \, \mathbb{Z} \end{aligned}$$

D'où

$$\begin{aligned} s^m &= s_1^m \circ s_2^m \circ \cdots \circ s_p^m \\ &= s_1^{\ell_1 (m/\ell_1)} \circ s_2^{\ell_2 (m/\ell_2)} \circ \cdots \circ s_p^{\ell_p (m/\ell_p)} \\ &= \mathrm{id}^{(m/\ell_1)} \circ \mathrm{id}^{(m/\ell_2)} \circ \cdots \circ \mathrm{id}^{(m/\ell_p)} = \mathrm{id} \end{aligned}$$

et il est clair que toute puissance inférieure à m n'est pas multiple d'une des longueurs et donne donc lieu à une permutation différente de l'identité sur cette orbite. □

Exemple II.5.c.7 *Dans* $\mathfrak{S}_8$,

$$s = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 4\,8\,7\,3\,5\,6\,1\,2 \end{pmatrix} = (\,1\,4\,3\,7\,)\,(\,2\,8\,) = (2\,8)(1\,4\,3\,7)$$

L'ordre de s *est*

$$o(s) = ppcm(2,4) = 4$$

II.5.d Transpositions

Définition II.5.d.1 *On appelle* ***transposition*** *tout 2–cycle, c-à-d. toute permutation qui échange deux éléments* i *et* $j \neq i$ *en laissant fixe chacun des* $n-2$ *autres ; on la note aussi* τ_{ij},

$$\tau_{ij} = (i\ j) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ 1 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

Exemple II.5.d.2 *Dans* $\mathfrak{S}_4$,

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\,4) \quad \textit{est la transposition } \tau_{24}.$$

Proposition II.5.d.3 *Tout élément de* $\mathfrak{S}_n$ *est produit de transpositions.*

Démonstration. Avec la Prop. II.5.c.6 concernant la décomposition en cycles disjoints, c'est une conséquence immédiate du Lemme suivant. □

Lemme II.5.d.4 *Soit* s *un* k*–cycle de* $\mathfrak{S}_n$,

$$s = (a_1\ a_2\ \dots\ a_k)\ ,$$

alors s *se décompose en produit de* $k-1$ *transpositions :*

$$s = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k).$$

(Rappellons que la « multiplication » de transpositions est la composition, le facteur à droite est donc celui qui agit en premier sur l'élément auquel on applique ce produit.)

Démonstration. Notons τ le produit dans le membre de gauche. On vérifie explicitement que $\forall i < k : \tau(a_i) = a_{i+1} = s(a_i)$ (seule la transposition $(a_i\ a_{i+1})$ a un effet non–trivial sur cet élément), et $\tau(a_q) = a_1 = s(a_q)$. □

Remarque II.5.d.5 *Attention, l'ordre des transpositions est important : si on l'inverse, on obtient la permutation inverse s^{-1}. (Exercice : pourquoi ?) Par contre, il y a d'autres décompositions tout aussi « bonnes », telle que $s = \tau_{a_1,a_q}\tau_{a_1,a_{q-1}} \dots \tau_{a_1,a_2}$ (exercice : vérifier ceci !), où les indices doivent être pris dans l'ordre « décroissant ».*

Remarque II.5.d.6 *En général, la décomposition d'une permutation en un produit de transpositions n'est donc pas unique.*

Exercice II.5.d.7 *Trouver une décomposition en transpositions de la permutation*

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix} \in \mathfrak{S}_{10}$$

Solution : *On écrit d'abord s sous forme de produit de cycles à supports disjoints :*

$$s = (1\ 3\ 6)(2\ 10\ 9\ 8\ 5)(4)(7)$$

On applique ensuite le Lemme pour décomposer chacun des cycles en produit de transpositions :

$$s = (1\ 3)(3\ 6)(2\ 10)(10\ 9)(9\ 8)(8\ 5)$$

II.5.e Signature d'une permutation

Définition II.5.e.1 *On appelle signature d'une permutation $s \in \mathfrak{S}_n$, et on note $\varepsilon(s)$, l'entier $(-1)^{n-m}$, où m est le nombre d'orbites suivant s.*

Exemple II.5.e.2 *a)* $\varepsilon(\mathrm{id}) = (-1)^{n-n} = 1$.
b) Soit τ une transposition de $\mathfrak{S}_n$; alors $\varepsilon(\tau) = (-1)^{n-(n-1)} = -1$.
c) Soit s un cycle de longueur ℓ ; alors $\varepsilon(\tau) = (-1)^{n-(n-\ell+1)} = (-1)^{\ell-1}$.

fin 8e cours
8.10.03 — début
9e cours 9.10.03

Proposition II.5.e.3 *Si $s \in \mathfrak{S}_n$ est le produit de p transpositions, alors $\varepsilon(s) = (-1)^p$.*

Démonstration. Montrons que $\forall s, \tau \in \mathfrak{S}_n : \varepsilon(s\,\tau) = -\varepsilon(s)$ si $\tau = (a\ b)$ est une transposition ; la proposition en résulte par récurrence immédiate (avec $\varepsilon(\mathrm{id}) = 1$). Déterminons la décomposition en cycles disjoints de $s \circ \tau$ pour en déduire la modification des orbites. Les orbites de s ne contenant a, b restent les mêmes, et les cycles correspondants commutent avec τ ; on considère donc :
1er cas : a, b appartiennent à deux orbites distincts de s, supports des cycles disjoints $\sigma_1 = (a\ s(a)\ \cdots\ s^{p-1}(a))$ et $\sigma_2 = (b\ s(b)\ \cdots\ s^{q-1}(b))$. Alors

$$\begin{aligned}\sigma_1 \circ \sigma_2 \circ \tau &= (a\ s(a)\ \cdots\ s^{p-1}(a))\ (s(b)\ \cdots\ s^{q-1}(b)\ b)\ (b\ a)\\ &= (s(a)\ \cdots\ s^{p-1}(a)\ a)\ (a\ s(b)\ \cdots\ s^{q-1}(b)\ b)\\ &= (s(a)\ \cdots\ s^{p-1}(a)\ a\ s(b)\ \cdots\ s^{q-1}(b)\ b)\ ,\end{aligned}$$

en utilisant le Lemme, et en observant que tous les éléments sont distincts. Les deux orbites de s sont donc devenues une seule orbite de $s \circ \tau$.
2e cas : a, b appartiennent à une même orbite de s, support d'un cycle $\sigma = (a\ s(a)\ \cdots\ s^{p-1}(a))$ avec $b = a^q$; $1 \leq q \leq p-1$. Alors

$$\begin{aligned}\sigma \circ \tau &= (s(a)\ \cdots\ s^{p-1}(a)\ a)\ (a\ s^q(a))\\ &= (s(a)\ \cdots\ s^{q+1}(a))\ (s^{q+1}(a)\ \cdots\ s^{p-1}(a)\ a\ s^q(a))\\ &= (s(a)\ \cdots\ s^q(a))\ (s^q(a)s^{q+1}(a))\ (s^q(a)s^{q+1}(a))\ (s^{q+1}(a)\ \cdots\ s^{p-1}(a)\ a)\\ &= (s(a)\ \cdots\ s^q(a))\ (s^{q+1}(a)\ \cdots\ s^{p-1}(a)\ a)\end{aligned}$$

Ainsi l'orbite de s a été scindé en deux orbites différentes de $s \circ \tau$. Donc, dans chacun des cas, le nombre d'orbites change de ± 1, d'où le changement de signe de la signature. □

Exemple II.5.e.4 *(Suite de l'exercice précédent.)*
Trouver la signature de s, permutation de $\mathfrak{S}_{10}$ définie par :

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$$

On avait trouvé les 4 orbites :

$$\begin{aligned} O_s(1) &= \{1\ 3\ 6\} & O_s(4) &= \{4\} \\ O_s(2) &= \{2\ 10\ 9\ 8\ 5\} & O_s(7) &= \{7\} \end{aligned}$$

La signature de s (calculée à l'aide du nombre d'orbites) est donc :

$$\varepsilon(s) = (-1)^{10-4} = 1.$$

On retrouve ce résultat en faisant le calcul en fonction du nombre de permutations :

$$s = (1\ 3)(3\ 6)(2\ 10)(10\ 9)(9\ 8)(8\ 5)$$

s se décompose en produit de 6 permutations , d'où

$$\varepsilon(s) = (-1)^6 = 1.$$

Remarque II.5.e.5 *L'écriture d'une permutation comme produit de transpositions n'est pas unique, mais la proposition montre que la* ***parité*** *du nombre de transpostions du produit est bien défini (c-à-d. toujours le même).*

Théorème II.5.e.6 *La signature*

$$\begin{aligned} \varepsilon : \mathfrak{S}_n &\to \{-1, 1\} \\ s &\mapsto \varepsilon(s) \end{aligned}$$

est un morphisme du groupe $(\mathfrak{S}_n, \circ)$ dans le groupe $(\{-1, 1\}, \cdot)$.

Démonstration. Si s s'écrit comme produit de m transpositions et s' comme produit de m' transpositions, alors $s\,s'$ s'écrit comme produit de $m + m'$ transpositions, d'où $\varepsilon(s\,s') = (-1)^{m+n} = (-1)^m\,(-1)^n = \varepsilon(s)\ \varepsilon(s')$. □

Remarque : on peut *définir* la signature comme l'unique morphisme non–trvial de S_n dans $\{-1, 1\}$.

Définition II.5.e.7 *On appelle $\mathcal{A}_n = \{\, s \in \mathfrak{S}_n \mid \varepsilon(s) = +1 \,\}$ les* ***permutations paires****, et $S_n \setminus \mathcal{A}_n = \{\, s \in \mathfrak{S}_n \mid \varepsilon(s) = -1 \,\}$ les* ***permutations impaires.***

Corollaire II.5.e.8 *On a $\mathcal{A}_n \lhd \mathfrak{S}_n$: l'ensemble des permutations paires est en effet le noyau du morphisme ε, donc un sous-groupe distingué de $\mathfrak{S}_n$, appelé « groupe alterné ».*

Remarque II.5.e.9 *On appelle $I(s) = \operatorname{card}\{\, (i, j) \in E_n^2 \mid i < j \wedge s(i) > s(j) \,\}$ le* **nombre d'inversions** *de s. On a $\varepsilon(s) = (-1)^{I(s)}$.*

Pour trouver le nombre d'inversions, on compte les éléments $s(j)$ inférieurs à $s(1)$ dans les colonnes $j = 2...n$ (de la 2e ligne), puis les $s(j)$ inférieurs à $s(2)$ dans les colonnes $j = 3...n$, etc.

fin du cours
11.oct.2002