COURS ET DM AR4 : GROUPE SYMÉTRIQUE

FRANÇOIS MAUCOURANT

1. Groupe symétrique d'un ensemble. $\mathcal{S}_n$.

Soit $E \neq \emptyset$ un ensemble. Rappelons que l'on note $\mathcal{S}_E$ l'ensemble des bijections de E dans E, et que, muni de la loi $\circ$ de composition des applications, c'est un groupe de neutre $e = Id_E$, appelé *groupe symétrique sur l'ensemble* E, et ses éléments sont appelés *permutations* de l'ensemble E. Si E est fini et ses éléments notés $\{a_1, ..., a_k\}$, on notera une permutation $\sigma \in \mathcal{S}_E$ de la manière suivante :

$$\sigma = \begin{pmatrix} a_1 & \dots & a_k \\ \sigma(a_1) & \dots & \sigma(a_k) \end{pmatrix}.$$

Dans le cas particulier où E est l'ensemble des n premiers entiers naturels, $E = \{1, \dots, n\}$, on simplifie la notation en écrivant simplement $\mathcal{S}_n$. Ces tableaux ne sont pas quelconques : ils représentent effectivement une permutation si la ligne du dessous contient une et une seule fois chaque élément de la ligne du dessus. On prendra bien garde au sens dans lequel se calculent les produits, qui est le sens de la compositions des applications, de la droite vers la gauche. Par exemple,

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

calcul qui s'opère simplement en regardant l'image respective de $\{1, 2, 3, 4\}$ par la composée des deux applications : par exemple, l'image de 2 par la permutation de droite du produit est 3, puis on prend l'image de 3 par la permutation à gauche, qui est encore 3, pour en conclure que le produit envoie 2 sur 3.

Exercice 1 : *Calculez le produit*

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

On va rapidement voir que la structure du groupe symétrique ne dépend en réalité que du cardinal de l'ensemble E, ce qui justifie de se limiter à l'étude des groupes $\mathcal{S}_n$.

Proposition 1.1. *Soit E, F deux ensembles, on suppose qu'il existe une bijection $f : E \to F$. Alors il existe un isomorphisme $g : \mathcal{S}_E \to \mathcal{S}_F$.*

Proof. Soit $\sigma \in \mathcal{S}_E$. On pose

$$g(\sigma) = f \circ \sigma \circ f^{-1}.$$

C'est la composée de 3 bijections, donc $g(\sigma)$ est bien une bijection, et elle va bien de F dans F. Donc $g(\sigma)$ est bien un élément de $\mathcal{S}_F$. Vérifions que g est bien un morphisme : soient σ, σ' deux permutations sur E.

$$g(\sigma) \circ g(\sigma') = f \circ \sigma \circ f^{-1} \circ f \circ \sigma' \circ f^{-1} = f \circ \sigma \circ \sigma' \circ f^{-1} = g(\sigma\sigma').$$

Reste à voir que g est bien une bijection, mais on vérifie facilement que si on pose, pour $\mu \in \mathcal{S}_F$,

$$h(\mu) = f^{-1} \circ \mu \circ f,$$

h est bien l'application inverse de g, et donc que g est inversible. □

Exercice 2 : *Enumérer les 6 éléments de $\mathcal{S}_3$, les 6 éléments de $\mathcal{S}_{\{a,b,c\}}$, et décrire explicitement un isomorphisme entre ces deux groupes .*

Proposition 1.2. *Le cardinal du groupe $\mathcal{S}_n$ est $n!$.*

Proof. Une permutation peut se construire en choisissant l'image de 1 parmi les n images possibles, puis l'imgae de 2 parmi les $n-1$ images possibles (les entiers entre 1 et n qui ne sont pas l'image de 1 déjà choisie), etc. Donc on a $n \times (n-1) \times \ldots \times 1$ possibilités. En d'autre termes, choisir une permutation, c'est exactement la même chose que de choisir un arrangement sur un ensemble à n éléments. □

Proposition 1.3. *Le groupe $\mathcal{S}_n$ n'est pas commutatif dès que $n \geq 3$.*

Exercice 3 : *Démontrez la proposition ci-dessus, en calculant $\sigma\tau$ ainsi que $\tau\sigma$ avec*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}.$$

2. Support d'une permutation. Cycles

Définition 2.1. *Soit $\sigma \in \mathcal{S}_n$ une permutation. L'ensemble*

$$supp(\sigma) = \{1 \leq i \leq n \ : \ \sigma(i) \neq i\},$$

est appelé support *de la permutation σ.*

Par exemple, $supp(\sigma) = \emptyset$ si et seulement si $\sigma = e$.

Exercice 4 : *Donnez $supp(\sigma)$, où*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix}.$$

Définition 2.2. *Une partie $X \subset \{1, ..., n\}$ est dite* invariante *(ou* stable*) par $\sigma \in \mathcal{S}_n$ si $\sigma(X) = X$. Un point $i \in \{1, ..., n\}$ est dit* fixe *pour σ si $i \notin supp(\sigma)$, càd $\sigma(i) = i$.*

Remarquons que pour des raisons de cardinalité, comme σ est injective, c'est équivalent à la sous-invariance : $\sigma(X) \subset X$.

Exercice 5 : Soit $\mathcal{P}_\sigma \subset \mathcal{P}(\{1, .., n\})$ l'ensemble des parties de $\{1, .., n\}$ qui sont invariantes par σ. Montrez que c'est une *algèbre unitaire* au sens suivant : stable par union, intersection, complémentaire. Donnez (sans justification) cette algèbre pour chacune des permutations suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Proposition 2.1. (1) *Le support d'une permutation σ est invariant par σ.*
(2) *Deux permutations à supports disjoints commutent.*

Proof. 1. Soit $i \notin supp(\sigma), \sigma(i) = i \notin supp(\sigma)$, ce qui démontre la sous-invariance du complémentaire de $supp(\sigma)$ et donc son invariance.

2. Soit $\sigma, \tau \in \mathcal{S}_n$ deux permutations à supports disjoints. Soit $i \in \{1, .., n\}$, nous voulons montrer que $\sigma\tau(i) = \tau\sigma(i)$. Distinguons trois cas, qui ne sont pas exclusifs :
1er cas : $i \in supp(\sigma)$, donc $i \notin supp(\tau)$ et ainsi $\tau(i) = i$. De plus $\sigma(i) \in supp(\sigma)$ également par invariance par σ, donc de même $\tau(\sigma(i)) = \sigma(i) = \sigma(\tau(i))$, qui était l'égalité recherchée.
2ème cas : $i \in supp(\tau)$, on conclut de même que $\tau(\sigma(i)) = \sigma(\tau(i))$.
3ème cas : $i \notin supp(\tau) \cup supp(\sigma)$. Alors $\sigma(i) = i = \tau(i)$, et donc $\tau(\sigma(i)) = \sigma(\tau(i)) = i$. □

Définition 2.3. *Un* cycle de longueur l *($2 \leq l \leq n$) est une permutation $\sigma \in \mathcal{S}_n$ telle qu'il existe un sous-ensemble ordonné de $\{1, ..., n\}$ de cardinal l, $(j_0, ..., j_{l-1})$, tel que*

(1) *$supp(\sigma) = \{j_0, ..., j_{l-1}\}$, càd $\sigma(k) = k$ si $k \neq j_i$ pour tout i.*
(2) *Pour $i = 0, ..., l-2$, $\sigma(j_i) = j_{i+1}$, et $\sigma(j_{l-1}) = j_0$. Autrement dit, $\sigma(j_i) = j_{i+1 \, mod \, l}$.*

Un tel cycle sera noté $(j_0, ..., j_{l-1})$. On dit parfois l-cycle pour désigner un cycle de longueur l. Un cycle de longueur deux est appelé transposition.

Exemples : le σ_1 de l'exercice 5 est un 6-cycle, que l'on peut noter $(1, 2, 3, 4, 5, 6)$. L'écriture d'un cycle n'est unique qu'à permutation circulaire près : $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$, mais est différent de $(1, 3, 2)$. Notez qu'une transposition est d'ordre 2, et est son propre inverse.

Théorème. *Le groupe $\mathcal{S}_n$ est engendré par les transpositions. Plus précisémment, tout élément de $\mathcal{S}_n$ peut s'écrire comme produit d'au plus $n-1$ transpositions.*

Ce théorème exprime le fait simple suivant : si on a n cartes numérotés de 1 à n, placées en ligne dans un certain ordre, et que l'on ne s'autorise à chaque mouvement que d'échanger la position de deux cartes, on peut remettre les cartes dans l'ordre en moins de $n-1$ mouvements.

Proof. Comme d'habitude, on convient qu'un produit de zéro termes donne le neutre. Nous allons procéder par récurrence sur n. Notre hypothèse de récurrence sur n est la suivante :
($\mathcal{H}_n$) Tout élément de $\mathcal{S}_n$ peut s'écrire comme produit d'au plus $n-1$ transpositions.
Vérifions ($\mathcal{H}_2$) à la main : $\mathcal{S}_2$ n'est constitué que de deux éléments e et la transposition $(1,2)$. D'où ($\mathcal{H}_2$).
Supposons donc ($\mathcal{H}_n$) et montrons ($\mathcal{H}_{n+1}$). Il sera très commode ici de voir $\mathcal{S}_n$ comme un sous-groupe de $\mathcal{S}_{n+1}$, une permutation σ de $\{1,...,n\}$ se prolongeant naturellement en une permutation de $\{1,...,n+1\}$ par la formule $\sigma(n+1)=n+1$. On voit que cette équation caractérise en fait les éléments de $\mathcal{S}_n$ dans $\mathcal{S}_{n+1}$.
Soit $\sigma \in \mathcal{S}_{n+1}$. Il y a deux cas possibles : ou bien $n+1$ est fixe pour σ, auquel cas σ est dans $\mathcal{S}_n$ et par hypothèse de récurrence produit de $n-1$ transpositions, ce qui conclut. Ou bien, $\sigma(n+1) \neq n+1$. Soit τ la transposition $(n+1, \sigma(n+1))$. Alors $\tau\sigma(n+1) = n+1$, ce qui prouve que $\tau\sigma$ est dans $\mathcal{S}_n$ et donc par ($\mathcal{H}_n$) qu'il existe k transpositions $\tau_1, .., \tau_k$, $k \leq n-1$, telles que

$$\tau\sigma = \tau_1....\tau_k,$$

et donc

$$\sigma = \tau^{-1}\tau_1....\tau_k = \tau\tau_1....\tau_k,$$

produit de moins de n transpositions, ce qui démontre ($\mathcal{H}_{n+1}$). □

Attention, cette décomposition en produit de transposition n'est absolument pas unique ! Par exemple $e = (1,2)(1,2)$.

Exercice 6 : Écrire le 4-cycle $(1,3,2,4)$ comme produit d'au plus 3 transpositions. Indication : la preuve du théorème ci-dessus est constructive.

3. σ-orbites; Décomposition canonique en produit de cycles

Définition 3.1. *Soit $x \in \{1,...,n\}$ et $\sigma \in \mathcal{S}_n$. On appelle σ-orbite de x, et on note $\mathcal{O}_\sigma(x)$ le sous-ensemble de $\{1,..,n\}$:*

$$\mathcal{O}_\sigma(x) = \{\sigma^k(x) \ : \ k \in \mathbf{Z}\}.$$

On peut faire le lien avec l'algèbre des ensembles invariants par σ; il n'est en effet pas bien difficile de vérifier que $\mathcal{O}_\sigma(x)$ est le plus petit élément de $\mathcal{P}_\sigma$ contenant x. On n'utilisera pas cette caractérisation.

Proposition 3.1. *Soit $\mathcal{R}_\sigma$ la relation d'équivalence sur $\{1,..,n\}$: $x\mathcal{R}_\sigma y$ ssi il existe $k \in \mathbf{Z}$ tel que $x = \sigma^k(y)$. Alors $\mathcal{O}_\sigma(x)$ est la classe de x modulo $\mathcal{R}_\sigma$, et si $m = |\mathcal{O}_\sigma(x)|$, on a l'égalité*

$$\mathcal{O}_\sigma(x) = \{x, \sigma(x), ..., \sigma^{m-1}(x)\}$$

et de plus $\sigma^m(x) = x$.

Proof. On laisse au lecteur le soin de vérifier que $\mathcal{R}_\sigma$ est bien une relation d'équivalence. Soit d le plus petit entier ≥ 1 tel que $x, \sigma(x), ..., \sigma^d(x)$ ne soient pas deux à deux distincts. Par le principe des tiroirs, $d \leq m$. On va montrer que $\sigma^d(x) = x$. Comme par définition de d, $x, \sigma(x), ..., \sigma^{d-1}(x)$ sont disctincts, il existe $k \in \{0, ..., d-1\}$ tel que $\sigma^d(x) = \sigma^k(x)$. Alors $\sigma^{d-k}(x) = x$, ce qui montre que $x, \sigma(x), ..., \sigma^{k-d}(x)$ ne sont pas 2 à 2 distincts, et par définition de d, que $d - k \geq k$, et donc $k = 0$.

Montrons maintenant que $\mathcal{O}_\sigma(x) = \{x, \sigma(x), ..., \sigma^{d-1}(x)\}$. En effet, soit $k \in \mathbf{Z}$, on voudrait montrer que $\sigma^k(x)$ est dans la liste précédente. Écrivons la division euclidienne de k par d, $k = qd + r$ où $0 \leq r \leq d-1$ et $q \in \mathbf{Z}$. Or comme $\sigma^d(x) = x$, on peut montrer par récurrence sur q que $\sigma^{qd}(x) = x$ en écrivant $\sigma^{qd}(x) = \sigma^{(q-1)d}\sigma^d(x) = \sigma^{(q+1)d}\sigma^{-d}(x)$.
Ainsi, $\sigma^k(x) = \sigma^r(x) \in \{x, \sigma(x), ..., \sigma^{d-1}(x)\}$, ce qui montre une inclusion. L'autre inclusion étant triviale, on a égalité entre $\mathcal{O}_\sigma(x)$ et $\{x, \sigma(x), ..., \sigma^{d-1}(x)\}$. Enfin, comme les éléments de cette liste sont 2 à 2 disctincts, $m = d$. □

Exemple : Les σ-orbites de

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

sont $\{1, 2\}$, $\{3, 4, 6, 8, 5, 7\}$ et $\{9\}$. Elles sont simplements déterminés en regardant l'image d'un élément (par exemple 3), et en itérant la permutation (on obtient ainsi 4, puis 6, puis 8, etc) jusqu'à retomber sur lélément de départ (ici, 3). La proposition précédente assure que l'on a ainsi toute l'orbite.

Exercice 7 : Déterminez la partition en orbite pour la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 6 & 7 & 5 & 4 & 1 \end{pmatrix}.$$

Théorème (Décomposition canonique en produit de cycles à supports disjoints)**.** *Soit $\sigma \in \mathcal{S}_n$, $\sigma \neq e$. Il existe $k \geq 1$ et $c_1, ..., c_k$ des cycles de longueur $l_i \geq 2$, à support 2à 2 disjoints, tels que*

$$\sigma = c_1 ... c_k.$$

Cette décomposition est unique à l'ordre près des facteurs. Le nombre k est le nombre d'orbites non ponctuelles.

L'ordre des facteurs n'est pas important dans le produit ci-dessus, car les permutations à support disjoint commutent.

Proof. Existence : Soit k le nombre d'orbites non ponctuelles, et $A_1, ..., A_k$ ces orbites, et $x_1, ..., x_k$ un point par orbite, $m_i \geq 2$ le cardinal de l'orbite A_i. On considère les cycles

$$c_i = (x_i, \sigma(x_i), ..., \sigma^{m_i-1}(x_i)),$$

le cycle c_i étant de support A_i. Vérifions l'égalité $\sigma = c_1...c_k$. Soit $j \in \{1, ..., n\}$. Si j est fixe pour σ, il est également fixe pour tous les c_i, et on a bien l'égalité $j = \sigma(j) = c_1...c_k(j)$. Sinon il existe un i tel que $j \in A_i$, et d'après la proposition précédente il existe $0 \leq l \leq m_i - 1$ tel que $j = \sigma^l(x_i)$. Comme les c_i sont à support disjoints, ils commutent et on a $c_1...c_k(j) = c_i(c_1...\hat{c_i}...c_k(j))$, où le chapeau désigne un terme manquant; on a $c_s(j) = j$ pour tout $s \neq i$ car le support de c_s est A_s, et donc finalement $c_1...c_k(j) = c_i(j)$. Or, par construction du cycle c_i et la proposition précédente, il est clair que $\sigma(j) = c_i(j)$. D'où égalité.
Unicité : Soit $c_1...c_l$ un produit de cycles à supports disjoints. On vérifie facilement que le nombre d'orbites non ponctuelles de ce produit de cycles est égal à l, que chaque orbite non ponctuelle correspond à un des cycles, et que sur chaque orbites non ponctuelle, l'ordre donné par l'itération du produit de cycle est celui donné par le cycle correspondant. En d'autre termes, chaque cycle c_i est nécessairement un des cycles construit plus haut dans la partie existence, ce qui conclut. □

Exemple : Reprenons l'exemple précédent :

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

se décompose en le produit de deux cycles $\sigma = (1, 2)(3, 4, 6, 8, 5, 7)$.

Exercice 8 : Déterminez la décomposition en produit de cycles à supports disjoints de la permutation de l'exercice 7.

4. Références

Si les notions exposées ici posent problème, on pourra consulter sur le sujet [Calais], chapitre III, paragraphe 2 (page 104 et +), ou bien [Gras], chapitre 2, paragraphe 5 (page 36 et +), ou bien encore [RDC], 2.4 (page 70 et +).

References

[Calais] Josette Calais, *Éléments de théorie des groupes*, puf.
[Gras] G. et M. Gras, *Algèbre fondamentale, Arithmétique*, ellipses.
[RDC] Ramis, Deschamps, Odoux, *Cours de Mathématiques spéciales, tome 1, algèbre.*, Masson.

Université Rennes I, IRMAR, Campus de Beaulieu 35042 Rennes cedex - France
E-mail address: francois.maucourant@univ-rennes1.fr