Groupe symétrique

Lycée Berthollet, MPSI1 2023-24

X représente ici un ensemble quelconque, fini ou infini, et n un entier naturel non nul.

I Définitions et notations

Définition 1 Les bijections de X vers X sont appelées des *permutations* de X.

Proposition 2 *L'ensemble $\mathcal{S}_X = \mathrm{Bij}(X,X)$, muni de la composition, est un groupe.*

Démonstration: On vérifie immédiatement tous les axiomes de groupe. Le neutre est Id_X. □

Définition 3

Le groupe $\mathcal{S}_X$ est appelé *groupe symétrique* de X ou *groupe des permutations* de X.

On note $\mathcal{S}_n = \mathcal{S}_{[\![1,n]\!]}$.

Dans le cadre de $\mathcal{S}_n$, on note aussi la composition avec un point $(\cdot)$ qu'on omet la plupart du temps et on note aussi l'élément neutre $\mathrm{Id}_{[\![1,n]\!]}$ simplement 1. Une composée de deux permutations est aussi appelée leur *produit*.

Une permutation $\sigma \in \mathcal{S}_n$ peut être notée sous forme de matrice à deux lignes et n colonnes, la première ligne contenant, dans l'ordre, les entiers de 1 à n et la deuxième ligne contenant leurs images.

Exemple 4 La permutation $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 7 & 5 & 2 & 6 & 3 \end{pmatrix}$ est l'élément de $\mathcal{S}_7$ défini par

$$\sigma_1(1) = 1,\ \sigma_1(2) = 4\ldots,\ \sigma_1(7) = 3.$$

Exercice 5 Représenter σ_1 par un diagramme de Venn en traçanr des flèches à l'intérieur d'une "patate" représentant l'ensemble $[\![1,n]\!]$.

Proposition 6 *Dès que* $\mathrm{Card}(X) \geq 3$*, $\mathcal{S}_X$ n'est pas commutatif.*

Démonstration: Soient a,b,c trois éléments de X deux à deux distincts. En notant τ_1 (resp. τ_2) la bijection de X fixant tous les points sauf a et b (resp. b et c) qu'elle échange, on a $\tau_1\tau_2(a) = b \neq c = \tau_2\tau_1(a)$. □

Définition 7 On appelle *support* d'un permutation $f \in \mathcal{S}_X$ l'ensemble des points de X non fixés par f : $\mathrm{supp}(f) = \{x \in X \mid f(x) \neq x\}$.

Proposition 8 *Deux permutations de X à supports disjoints commutent.*

Démonstration: Facile. □

Exercice 9

1. Soient $f,g \in \mathcal{S}_X$ telle que $\text{supp}(f) \cap \text{supp}(g) = \{x\}$ et $h = fgf^{-1}g^{-1}$. Montrer que $\text{Card}(\text{supp}(h)) = 3$ et décrire explicitement les éléments de ce support ainsi que leurs images par h
2. Exhiber deux permutations différentes, non inverses l'une de l'autre et à supports non disjoints, qui commutent cependant.

Enfin, on a la

Proposition 10 *Pour X,Y deux ensembles quelconques, s'il existe une bijection de X vers Y, alors les groupes $\mathcal{S}_X$ et $\mathcal{S}_Y$ sont isomorphes.*

En particulier, si X est fini, $\mathcal{S}_X$ est isomorphe à $\mathcal{S}_{|X|}$, ce qui ramène l'étude des groupes de permutation finis à celle de $\mathcal{S}_n$, $n \in \mathbb{N}^\star$.

Démonstration: Notons f une telle bijection de X vers Y. Alors les deux applications

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{S}_X & \longrightarrow & \mathcal{S}_Y \\ \sigma & \longmapsto & f \circ \sigma \circ f^{-1} \end{array} \right. \quad \text{et} \quad \varphi : \left\{ \begin{array}{ccc} \mathcal{S}_Y & \longrightarrow & \mathcal{S}_X \\ \sigma & \longmapsto & f^{-1} \circ \sigma \circ f \end{array} \right. .$$

sont bien définies, car les composées de bijections sont des bijections, et clairement réciproques l'une de l'autre, donc φ est bijective.

De plus, pour $\sigma, \sigma' \in \mathcal{S}_X$,

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

Ainsi, φ est un isomorphisme de groupes de $\mathcal{S}_X$ vers $\mathcal{S}_Y$. □

II Cycles

Définition 11 Pour $r \geq 2$ et $a_1, a_2, \ldots, a_r \in [\![1,n]\!]$ deux-à-deux distincts, on note $(a_1\ a_2\ \ldots\ a_r)$ et on appelle *r-cycle* la permutation $c \in \mathcal{S}_n$ de support $\{a_1, a_2, \ldots, a_r\}$ définie par $c(a_r) = a_1$ et, pour tout $i \in [\![1, r-1]\!]$, $c(a_i) = a_{i+1}$.

Exemple 12 Dans $\mathcal{S}_5$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix} = (1\ 4\ 5\ 3) = (5\ 3\ 1\ 4) = \ldots$ est un 4-cycle.

Remarque 13 Comme on peut le voir sur l'exemple ci-dessus, l'écriture d'un cycle n'est pas unique.

Définition 14 Un 2-cycle est appelé une *transposition*.

Exemple 15 $(1\ n)$ est une transposition de $\mathcal{S}_n$.

Théorème 16

Tout élément de $\mathcal{S}_n$ s'écrit comme produit de cycles à supports deux-à-deux disjoints.
Par ce qu'on a vu précédemment, cette écriture est commutative.
De plus, cette écriture est unique à l'ordre près, i.e. l'ensemble de ces cycles est unique.

Démonstration: Soit $\sigma \in \mathcal{S}_n$.

On considère la relation binaire sur $[\![1,n]\!]$ définie par $i\mathcal{R}_\sigma j \iff (\exists k \in \mathbb{Z},\ \sigma^k(i) = j)$. C'est clairement une relation d'équivalence. Pour toute classe d'équivalence $\mathcal{C}$ qui n'est pas un singleton (on la dira *non-triviale*), σ induit clairement une bijection sur $\mathcal{C}$, dont on va montrer que c'est un r-cycle, en notant $r = \operatorname{Card}\mathcal{C}$.

Soit $i \in \mathcal{C}$. Comme $\left\{\sigma^k(i); k \in \mathbb{N}^\star\right\} (\subset [\![1,n]\!])$ est fini, il existe deux entiers $1 \leq s < t$ tels que $\sigma^s(i) = \sigma^t(i)$. Alors $\sigma^{t-s}(i) = i$, avec $t-s \in \mathbb{N}^\star$. On pose alors $u = \min\left\{k \in \mathbb{N}^\star \mid \sigma^k(i) = i\right\}$, qui existe bien (minimum d'une partie non vide de $\mathbb{N}$). Pour $k \in \mathbb{Z}$, par division euclidienne, il existe $(q,r') \in \mathbb{Z}\times\mathbb{N}$ tel que $k = uq + r'$ et $r' < u$. On a alors $\sigma^k(i) = \sigma^{r'}(\sigma^{qu}(i)) = \sigma^{r'}(i)$. Ainsi $\mathcal{C} = \left\{\sigma^k(i); k \in \mathbb{Z}\right\} = \left\{\sigma^k(i); k \in [\![0,u-1]\!]\right\}$ et, par minimalité de u, les $\sigma^k(i)$ sont deux-à-deux distincts pour $k \in [\![0,u-1]\!]$ (sinon, quitte à simplifier comme avant par une puissance de σ, on obtiendrait $u' \in [\![1,u-1]\!]$ tel que $\sigma^{u'}(i) = i$). Ainsi le cardinal de $\mathcal{C}$ étant à la fois r et u, $u = r$. La bijection induite par σ sur $\mathcal{C}$ est alors le r-cycle $(i\ \sigma(i)\ \sigma^2(i)\ \ldots\ \sigma^{r-1}(i))$.

On étend ce r-cycle en un r-cycle $c_\mathcal{C}$ de $[\![1,n]\!]$ qui fixe les éléments hors de $\mathcal{C}$. La permutation σ est alors le produit de tous les cycles $c_\mathcal{C}$ obtenus ainsi, *i.e.* $\sigma = \prod_{\mathcal{C}\in Q} c_\mathcal{C}$, où Q est l'ensemble des classes non triviales de la relation d'équivalence $\mathcal{R}_\sigma$ et la notation est justifiée puisque ces cycles commutent deux-à-deux, car leur supports sont des classes différentes, donc disjointes. On vient de montrer l'existence de la décomposition voulue.

Soit une autre décomposition en cycles à supports deux-à-deux disjoints $\sigma = c_1 \cdots c_m$ et $k \in [\![1,m]\!]$. Le support de c_k est évidemment stable par σ, donc réunion de classes d'équivalences. Comme de plus, on peut passer d'un élément quelconque de ce support à un autre élément quelconqe de ce support en lui appliquant un certain nombre de fois le cycle c_k, *i.e.* un certain nombre de fois σ, il y a une seule classe $\mathcal{C}$ dans cette réunion, *i.e.* $\operatorname{supp}(c_k) = \mathcal{C}$. Comme les supports des autres cycles sont disjoints de $\operatorname{supp}(c_k)$, σ et c_k induisent la même permutation sur $\operatorname{supp}(c_k) = \mathcal{C}$, donc $c_\mathcal{C}$ et c_k aussi . Comme $c_\mathcal{C}$ et c_k fixent tous deux les points hors de $\mathcal{C}$, ils sont égaux. En faisant de même pour tout $k \in [\![1,m]\!]$, tout c_k est un $c_\mathcal{C}$, pour une classe d'équivalence non triviale et les classes obtenues sont différentes car disjointes. De plus, toute classe non triviale est atteinte, sinon ses éléments seraient fixés par $\sigma = c_1 \cdots c_m$, ce qui n'est pas le cas. L'ensemble des cycles $\{c_k; k \in [\![1,m]\!]\}$ est donc $\{c_\mathcal{C}; \mathcal{C} \in Q\}$, *i.e.* la décomposition en cycles à supports disjoints est unique à l'ordre près. □

Remarque 17 En pratique, il suffit de prendre un élément non fixe i, son image, l'image de son image... jusqu'à retomber sur i, ce qui donne un premier cycle, puis de recommencer tant qu'il reste des éléments non fixes non encore parcourus.

Exemple 18 En reprenant la permutation de l'exemple 4, on a

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 7 & 5 & 2 & 6 & 3 \end{pmatrix} = (2\ 4\ 5)(3\ 7) = (7\ 3)(4\ 5\ 2) = \ldots$$

Cette décomposition permet de calculer facilement des puissances de permutations, à l'aide du résultat :

Proposition 19

Soit $\sigma \in \mathcal{S}_n$ s'écrivant $\sigma = c_1 \cdots c_m$, produit de cycles à supports deux-à-deux disjoints, c_k étant un r_k-cycle pour tout $k \in [\![1,m]\!]$.

Alors $r_1 \vee r_2 \cdots \vee r_m$ est le plus petit entier r strictement positif tel que $\sigma^r = 1$.

Démonstration: En exercice. □

Exemple 20 Avec les notations précédentes, on obtient $\sigma_1^6 = 1$, donc par exemple, par commutation des cycles à supports disjoints :

$$\sigma_1^{2019} = \sigma_1^{2016}\sigma_1^3 = \sigma_1^3 = (2\ 4\ 5)^3(3\ 7)^3 = (3\ 7).$$

Exercice 21 Si $\sigma \in \mathcal{S}_n$ et $c = (a_1\ a_2\ \ldots\ a_r)$, montrer que $\sigma c \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_p))$.

III Signature

Lemme 22 *Tout cycle s'écrit comme un produit de transpositions. Plus précisément,*

$$(a_1\ a_2\ \ldots\ a_r) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{r-1}\ a_r).$$

Démonstration: Ces deux permutations fixent tous les éléments de $[\![1,n]\!] \setminus \{a_1,\ldots,a_r\}$. Il suffit donc de vérifier qu'ils donnent la même image de tout a_k, $k \in [\![1,r]\!]$, ce qui est immédiat. □

Corollaire 23 *Toute permutation s'écrit comme un produit de transpositions, autrement dit, les transpositions engendrent $\mathcal{S}_n$.*

Démonstration: Immédiat à l'aide de la décomposition en cycles et du lemme. □

Exercice 24

1. Montrer que les transpositions $(i\ i+1)$, $i \in [\![1,n-1]\!]$, engendrent $\mathcal{S}_n$.
2. Montrer que la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ \ldots\ n)$ engendrent $\mathcal{S}_n$.

Le corollaire sert à démontrer le résultat crucial suivant :

Théorème 25 *Il existe une seule application ε, appelée **signature**, de $\mathcal{S}_n$ vers $\mathbb{U}_2 = \{-1,+1\}$ telle que :*

— *Pour toute tranposition τ, $\varepsilon(\tau) = -1$;*
— $\forall \sigma,\sigma' \in \mathcal{S}_n,\ \varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

Démonstration: Comme toute permutation est un produit de transpositions, on a immédiatemet l'unicité.

Pour l'existence, on pose $\varepsilon'(\sigma) = (-1)^{n-c-f}$, où c est le nombre de cycles dans la décomposition de σ en produit de cycles à supports disjoints et f est le nombre de points fixes de σ.

En examinant les différents cas de figure, on peut montrer sans trop de difficultés que si $\sigma \in \mathcal{S}_n$ et τ est une transposition, alors $\varepsilon'(\sigma\tau) = \varepsilon'(\sigma)\varepsilon'(\tau)$.

Si on prend alors $\sigma, \sigma' \in \mathcal{S}_n$, σ' s'écrit comme produit de transpositions : $\sigma' = \tau_1 \cdots \tau_q$, et en appliquant plusieurs fois le résultat précédent, une récurrence évidente donne

$$\varepsilon'(\sigma\sigma') = \varepsilon'(\sigma\tau_1 \cdots \tau_q) = \varepsilon'(\sigma\tau_1 \cdots \tau_{q-1})\varepsilon'(\tau_q) = \ldots = \varepsilon'(\sigma)\varepsilon'(\tau_1)\cdots\varepsilon'(\tau_{q-1})\varepsilon'(\tau_q)$$

et aussi

$$\varepsilon'(\sigma') = \varepsilon'(\tau_1 \cdots \tau_q) = \varepsilon'(\tau_1 \cdots \tau_{q-1})\varepsilon'(\tau_q) = \ldots = \varepsilon'(\tau_1)\cdots\varepsilon'(\tau_{q-1})\varepsilon'(\tau_q),$$

donc

$$\varepsilon'(\sigma\sigma') = \varepsilon'(\sigma)\varepsilon'(\sigma').$$

De plus, pour une tranposition τ, dans la formule de ε', on a $c = 1$ et $f = n-2$, donc $\varepsilon'(\tau) = (-1)^{n-1-(n-2)} = -1$. Ainsi ε' convient, ce qui prouve l'existence. □

Remarque 26 La signature est ce qu'on appelle un *morphisme de groupes* de $\mathcal{S}_n$ vers $\mathbb{U}_2$ (*i.e.* elle préserve le produit).
De plus, on voit facilement que :

- pour $n = 1$, c'est le morphisme trivial (son image est $\{+1\}$) et c'est d'ailleurs le seul morphisme de $\mathcal{S}_1$ vers $\mathbb{U}_2$;
- pour $n \geq 2$, c'est l'**unique morphisme de groupe non trivial** de $\mathcal{S}_n$ vers $\mathbb{U}_2$.

Définition 27 Une permutation de signature $+1$ (resp. -1) est dite *paire* (resp. *impaire*).

On a immédiatement à l'aide du lemme 22 le résultat suivant :

Proposition 28 *Si c est un r-cycle, alors $\varepsilon(c) = (-1)^{r-1}$.*

Exemple 29 Ainsi les transpositions sont impaires, les 3-cycles sont pairs, les 4-cycles sont impairs, *etc*.

Proposition 30 *(Complément)*
L'ensemble des permutations paires est un sous-groupe $\mathcal{A}_n$ de $\mathcal{S}_n$ appelé ***groupe alterné****.*
Il est engendré par les 3-cycles.