

COURS ET DM AR4 : GROUPE SYMÉTRIQUE II, ACTION DE GROUPE

FRANÇOIS MAUCOURANT

1. SIGNATURE D'UNE PERMUTATION

Définition 1.1. Soit $\sigma \in \mathcal{S}_n$ une permutations, k le nombre de σ -orbites. On définit la signature de σ et on note $\varepsilon(\sigma)$, le nombre

$$\varepsilon(\sigma) = (-1)^{n-k}.$$

Dans le nombre d'orbites, on compte également les points fixes, c'est-à-dire les orbites ponctuelles. Par exemple, une transposition ayant $n - 2$ points fixes et une orbite de cardinal 2, sa signature est donc $-1 = (-1)^{n-(n-2+1)}$. La signature de l'identité est égale à 1, car ses orbites sont les n points fixes $\{1, \dots, n\}$.

Exercice 1 : Calculez la signature de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 10 & 9 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 8 \end{pmatrix}$$

Nous allons voir que la signature est un morphisme à valeur dans le groupe multiplicatif $\{-1, +1\}$. Commençons par analyser l'effet sur la signature du produit par une permutation.

Proposition 1.1. Soit τ une transposition et σ une permutation. Alors

$$\varepsilon(\sigma\tau) = -\varepsilon(\sigma).$$

Proof. Rappelons que pour déterminer la σ -orbite d'un point $x \in \{1, \dots, n\}$, il suffit de regarder les itérés $x, \sigma(x), \dots, \sigma^k(x)$ jusqu'à retomber sur x . Soient $a, b \in \{1, \dots, n\}$ les deux points permutés par τ . Essayons de comparer les σ -orbites et les $\sigma\tau$ -orbites. Soit $\mathcal{O} = \{x, \sigma(x), \dots, \sigma^k(x)\}$ une σ -orbite.

1er cas : \mathcal{O} ne contient ni a , ni b . Alors pour tout élément $y \in \mathcal{O}$, $\tau(y) = y$ et donc en itérant $\sigma\tau$ qui est égal à σ sur \mathcal{O} , on voit que \mathcal{O} est aussi une orbite de $\sigma\tau$.

2ème cas : \mathcal{O} contient à la fois a et b . On peut toujours écrire l'orbite en respectant l'ordre donné par σ comme

$$\mathcal{O} = \{a, x_1, \dots, x_r, b, x_{r+1}, \dots, x_s\}.$$

L'orbite de a par $\sigma\tau$ est alors $\{a, x_{r+1}, \dots, x_s\}$, et celui de x_1 est $\{x_1, \dots, x_r, b\}$. La σ -orbite \mathcal{O} se scinde donc en deux $\sigma\tau$ -orbites.

3ème cas : \mathcal{O} contient a ou b mais pas les deux. Disons que \mathcal{O} contienne a ,

et qu'une autre orbite \mathcal{O}' contienne b . Ecrivons $\mathcal{O} = \{a, x_1, \dots, x_r\}$ et $\mathcal{O}' = \{b, y_1, \dots, y_r\}$, en respectant l'ordre donné par σ . L'orbite de a par $\sigma\tau$ est donc $\{a, y_1, \dots, y_r, b, x_1, \dots, x_r\}$, qui est exactement la réunion de deux orbites de σ . En conclusion, $\sigma\tau$ a une orbite de plus (si le support de la transposition est inclus dans une orbite), ou une orbite de moins (dans l'autre cas), que la permutation σ . Ainsi, leurs signatures sont de signe opposé. \square

Théorème. (1) Soit $\sigma \in \mathcal{S}_n$, $\sigma = \tau_1 \dots \tau_s$ une décomposition en produit de transpositions. Alors $\varepsilon(\sigma) = (-1)^s$.

(2) La signature ε est un morphisme surjectif de \mathcal{S}_n dans $(\{-1, +1\}, \times)$.

Proof. Pour le premier point, on procède par récurrence sur s , l'utilisation de la proposition précédente étant exactement ce qu'il faut pour se ramener au cas $s - 1$.

Pour le deuxième point, soit σ, σ' deux permutations. On sait que toute permutation peut se décomposer en produit de transpositions : il existe des transposition τ_i telles que

$$\sigma = \tau_1 \dots \tau_s, \quad \sigma' = \tau_{s+1} \dots \tau_{s+r}.$$

Ainsi $\sigma\sigma' = \tau_1 \dots \tau_{r+s}$, et on a

$$\varepsilon(\sigma\sigma') = (-1)^{r+s} = (-1)^s (-1)^r = \varepsilon(\sigma)\varepsilon(\sigma'),$$

ce qui montre que ε est un morphisme. La surjectivité vient du fait qu'il existe des permutations de signature -1 , par exemple les transpositions. \square

On a déjà fait la remarque qu'une décomposition en produit de transpositions n'est pas unique, mais ce théorème nous dit que la parité du nombre de transpositions intervenant dans une telle décomposition est par contre bien définie.

Définition 1.2. Une permutation de signature $+1$ est dite paire, elle est dite impaire sinon. On appelle groupe alterné et on note \mathcal{A}_n le sous-groupe distingué $\text{Ker}(\varepsilon)$ constitué des permutations paires. Il est d'indice 2, et $\mathcal{S}_n/\mathcal{A}_n$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

En effet, le morphisme surjectif ε passe au quotient en un isomorphisme de $\mathcal{S}_n/\mathcal{A}_n$ sur $(\{-1, +1\}, \times)$ qui est isomorphe à $(\mathbf{Z}/2\mathbf{Z}, +)$. Cette terminologie donne lieu à l'énoncé à l'allure paradoxale suivant.

Proposition 1.2. Soit $l \geq 2$. Un cycle de longueur l est de parité opposée à celle de l . Autrement dit un cycle de longueur impaire est une permutation paire, alors qu'un cycle de longueur paire est une permutation impaire.

Proof. Soit $c = (x_1, \dots, x_l)$ un l -cycle. Il a donc une unique orbite de longueur l , et $n - l$ points fixes, donc $n - l + 1$ orbites au total, donc $\varepsilon(c) = (-1)^{l-1}$.

Une autre façon de voir ce résultat est de décomposer c en produit de transposition. On peut ainsi vérifier la formule:

$$c = (x_1, \dots, x_l) = (x_1, x_2)(x_2, x_3) \dots (x_{l-1}, x_l),$$

le produit de droite ayant $l - 1$ termes, chacun de signature -1 . \square

Mentionnons également, sans preuve, une autre formule pour le calcul de la permutation, ainsi qu'une application importante en algèbre linéaire.

Proposition 1.3. *Soit $\sigma \in \mathcal{S}_n$. Alors*

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

Il n'est même pas évident à priori que le produit ci-dessus soit un entier. Les curieux pourront consulter [Gras], page 39-40, pour voir une démonstration de cette formule.

La signature apparaît également dans l'expression du déterminant d'une matrice. Soit M une matrice $n \times n$ de coefficients $m_{i,j}$ à valeurs dans un corps k quelconque (pour ceux qui ne connaissent pas la définition d'un corps, pensez $k = \mathbf{R}$, $k = \mathbf{C}$ ou $k = \mathbf{Q}$). On a alors

$$\det(M) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) m_{1,\sigma(1)} \dots m_{n,\sigma(n)}.$$

En particulier, si M est une matrice de permutation, c'est à dire qu'il existe une permutation σ telle que $M(e_i) = e_{\sigma(i)}$, où (e_1, \dots, e_n) est la base canonique de k^n , alors $\det(M) = \varepsilon(\sigma)$; géométriquement, une telle matrice de permutation M préserve ou renverse l'orientation suivant le signe de $\varepsilon(\sigma)$.

Exercice 2 : Combien \mathcal{A}_3 possède-t-il d'éléments ? A quel groupe connu est-il isomorphe ?

Exercice 3 : Combien \mathcal{A}_4 possède-t-il d'éléments ? Enumérez les éléments du groupe \mathcal{A}_4 ; on exprimera les permutations sous forme de produit de cycles à supports disjoints.

2. ORDRE D'UN ÉLÉMENT DE \mathcal{S}_n . CALCUL DES ITÉRÉS.

Commençons par une remarque concernant l'élevation à la puissance. Si $\sigma = c_1 \dots c_k$ est un produit de cycles à supports disjoints, pour tout $s \in \mathbf{Z}$ on a :

$$\sigma^s = (c_1 \dots c_k) \dots (c_1 \dots c_k) = c_1^s \dots c_k^s,$$

car les cycles c_i commutent entre eux, étant à support disjoints. Il est clair que le support de c_i^s est un sous-ensemble du support de c_i , et que le produit ci-dessus est donc un produit d'éléments à support disjoints. Ce ne sont pourtant pas automatiquement des cycles, comme on le voit dans l'exemple-exercice suivant.

Exercice 4 : Donnez la décomposition en produit de cycles à supports disjoints de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 3 & 4 & 1 & 6 & 5 & 8 & 9 & 10 & 11 & 7 \end{pmatrix},$$

et celle de son carré.

Proposition 2.1. *Soit $\sigma \neq e$ une permutation de \mathcal{S}_n , $\sigma = c_1 \dots c_k$ sa décomposition en produit de cycles à supports disjoints. Soient l_1, \dots, l_k les longueurs des cycles c_1, \dots, c_k . Alors σ est d'ordre le ppcm de l_1, \dots, l_k .*

Proof. Soit $d \geq 1$ l'ordre de σ . Montrons que d divise $m = \text{ppcm}(l_1, \dots, l_k)$. On a :

$$\sigma^m = c_1^m \dots c_k^m,$$

or le cycle c_i étant d'ordre l_i , et comme l_i divise m , on a $c_i^m = e$. Donc $\sigma^m = e$, et ainsi d divise m .

Montrons que d est multiple de m . Il suffit pour cela de prouver que d est multiple de chacun des l_i . Comme

$$e = \sigma^d = c_1^d \dots c_k^d,$$

et que ce produit est un produit de permutations à supports disjoints, ceci implique que chaque permutation est individuellement l'identité, c'est-à-dire pour $i = 1, \dots, k$, $c_i^d = e$. Le cycle c_i étant d'ordre l_i , l_i divise d . \square

Exercice 5 : Montrez le lemme sous-entendu dans la preuve précédente, à savoir que si $\sigma_1, \dots, \sigma_k$ sont des permutations de supports disjoints telles que $\sigma_1 \dots \sigma_k = e$, alors $\sigma_i = e$ pour tout i . Donnez un contre-exemple sans cette hypothèse sur le support.

Exercice 6 : Calculer l'ordre de la permutation σ de l'exercice 4.

3. ACTIONS DE GROUPES

La présentation abstraite des groupes qui a été faite jusqu'à présent a (volontairement) ignoré tout un aspect crucial de la théorie des groupes. Dans la réalité, un groupe n'est pas juste un ensemble muni d'une loi, mais apparaît naturellement comme un ensemble de *transformations*. Par exemple, le groupe \mathcal{S}_n ne se comprend que si on le regarde comme un ensemble de transformations de l'ensemble $\{1, \dots, n\}$; ce qui donne lieu à la notion de cycle, de support, d'orbite. De même, en étudiant le groupe diédral D_n , on est naturellement amené à considérer que c'est un ensemble de transformation de l'ensemble des sommets du polygone régulier à n côtés, qui préserve un ordre de numérotation circulaire sur les sommets ou bien renverse cet ordre.

Donc, à côté du groupe G , on a bien souvent un espace X , qui lui n'a a priori aucune structure, à part que G se comprend comme un ensemble particulier de transformations de X .

Définition 3.1. Soit X un ensemble non vide, G un groupe. Une action de G (à gauche) sur X est une application

$$\cdot : G \times X \rightarrow X,$$

$$(g, x) \mapsto g.x,$$

telle que

- (1) $\forall (g_1, g_2) \in G^2, \forall x \in X, g_1.(g_2.x) = (g_1g_2).x,$
- (2) $\forall x \in X, e.x = x$

On dit alors que G agit sur X , ou que G opère sur X .

Remarques :

- (1) Il existe une notion d'action à droite, telle qu'on peut toujours se ramener au cas d'une action à gauche. On ne détaille donc pas.
- (2) On note un point pour l'opération externe qui à un élément du groupe et un point de X associe un point de X . Il ne faut absolument pas le confondre avec le point de multiplication de la loi interne du groupe : lorsqu'on écrit $g_1.(g_2.x) = (g_1.g_2).x$, le premier point du terme de droite n'a absolument pas le même statut que les trois autres points de la formule. D'ailleurs dans la définition ci-dessus, ce point est omis. On ne mettra en pratique pas souvent les points, le premier axiome nous assurant que l'on peut sans scrupule aucun écrire g_1g_2x sans parenthésage ni même de point, bien que l'opération muette entre g_1 et g_2 puisse s'interpréter de deux façons totalement différentes.
- (3) On parlera souvent par abus de langage de l'action de G sur X . Il peut y avoir en réalité plusieurs actions d'un même groupe G sur un même espace X ; mais on n'en considèrera généralement qu'une à la fois.
- (4) Lorsqu'on travaille avec les actions, on a toujours la règle de simplification à gauche : en partant de $g.x = y$, et en appliquant g^{-1} par la loi externe à cette égalité, on obtient $g^{-1}gx = g^{-1}y$ et donc $x = g^{-1}y$. En particulier en prenant $y = gz$, l'égalité $gx = gz$ entraîne que $x = z$. Par contre, on n'a pas le droit de simplifier à droite : si $gx = g'x$ on n'a pas nécessairement $g = g'$.

Il est d'autant plus crucial de distinguer entre le \cdot de l'opération et la loi interne du groupe, et de comprendre la dissymétrie de leurs statuts, que dans les exemples 5 et 6 suivants, l'espace X et le groupe G sont un seul et même ensemble...

Exemples :

- (1) L'action *triviale* de G sur X , définie par $g.x = x$ pour tout g, x .
- (2) L'application qui à une matrice $M \in GL(n, \mathbf{R})$ et à un vecteur $v \in \mathbf{R}^n$, associe l'image du vecteur par la matrice, Mv , est une action du groupe linéaire sur l'espace vectoriel \mathbf{R}^n .

- (3) Le groupe symétrique \mathcal{S}_n agit naturellement sur l'ensemble $X = \{1, \dots, n\}$ simplement par la formule $\sigma.x = \sigma(x)$.
- (4) L'action du groupe diédral D_n sur l'ensemble des sommets du polygône régulier à n côtés.
- (5) L'action de G sur lui-même par *translation*, où $X = G$, est définie par

$$g.x = gx,$$

où le point à droite est le point de l'action, et gx désigne le produit par la loi interne du groupe.

- (6) Le plus vicieux : l'action de G sur lui-même par *conjugaison*. Ici $X = G$, et on définit l'action par

$$g.x = gxg^{-1}.$$

Exercice 7 : Détaillez l'exemple 6, c'ad montrez que l'action d'un groupe G sur lui-même par conjugaison, est bien une action.

On peut aussi sans peine restreindre une action à un sous-groupe $H \subset G$. Le groupe H agit alors sur X via l'application \cdot restreinte à $H \times X$. Pour restreindre l'ensemble X , c'est un tout petit peu plus délicat et on le verra par la suite. Pour l'instant, montrons que l'on peut interpréter une action comme un certain morphisme vers le groupe symétrique \mathcal{S}_X .

Proposition 3.1. *Soit G un groupe et X un ensemble non vide sur lequel G agit. Alors*

- (1) $\forall g \in G$, l'application $\tau_g : X \rightarrow X$, $\tau_g(x) = g.x$, est une bijection de X dans X .
- (2) L'application $\tau : G \rightarrow \mathcal{S}_X$, $\tau(g) = \tau_g$, est un morphisme.

Proof. 1) Calculons $\tau_g \circ \tau_{g^{-1}}$. Soit $x \in X$,

$$\tau_g \circ \tau_{g^{-1}}(x) = \tau_g(g^{-1}.x) = g.(g^{-1}.x) = gg^{-1}.x = e.x = x,$$

et donc $\tau_g \circ \tau_{g^{-1}} = Id_X$. De même, $\tau_{g^{-1}} \circ \tau_g = Id_X$, et donc τ_g est bijectif, d'inverse $\tau_{g^{-1}}$.

2) Pour tout x dans X , on a $\tau(g_1g_2)(x) = (g_1g_2).x = g_1.(g_2.x) = \tau_{g_1} \circ \tau_{g_2}(x)$, et on peut donc en déduire l'égalité des applications : $\tau(g_1g_2) = \tau(g_1)\tau(g_2)$. \square

Réciproquement, si on dispose d'un morphisme τ d'un groupe G dans le groupe symétrique sur X , \mathcal{S}_X , on peut définir une action de G sur X par composition entre ce morphisme et l'action naturelle de \mathcal{S}_X sur X , par la formule

$$g.x = \tau(g)(x).$$

Définition 3.2. *On dit qu'une action est fidèle si le noyau du morphisme τ ci-dessus est réduit à l'élément neutre. C'est équivalent au fait que pour tout $g \in G - \{e\}$, il existe $x \in X$ avec $g.x \neq x$.*

4. ORBITES ET STABILISATEURS

On considère toujours une action d'un groupe X sur un espace X .

Définition 4.1. Soit $x \in X$, on définit l'orbite de x par G comme

$$\mathcal{O}_G(x) = \{g.x\}_{g \in G} = \{y \in X : \exists g \in G, g.x = y\} = G.x.$$

C'est un sous-ensemble de X . Les orbites forment une partition de X . On définit le stabilisateur de x dans G par

$$\text{Stab}_G(x) = \{g \in G : g.x = x\}.$$

C'est un sous-groupe de G , que l'on note parfois G_x (à ne pas confondre avec l'orbite Gx).

Proof. Soit \mathcal{R} la relation $x\mathcal{R}y$ si il existe $g \in G$ tel que $x = g.y$. Alors

i) \mathcal{R} est réflexive : pour tout $x \in X$, $e.x = x$ et donc $x\mathcal{R}x$.

ii) \mathcal{R} est symétrique : si $x\mathcal{R}y$, alors il existe g tel que $x = g.y$ et donc $g^{-1}.x = g^{-1}g.y$, d'où $y = g^{-1}.x$.

iii) \mathcal{R} est transitive : si $x\mathcal{R}y$ et $y\mathcal{R}z$, il existe $g, g' \in G$ tels que $x = g.y$ et $y = g'.z$, et donc $x = gg'.z$, d'où $x\mathcal{R}z$.

Ainsi \mathcal{R} est une relation d'équivalence, et les orbites sont simplement les classes d'équivalence modulo cette relation. On a donc montré que les orbites forment une partition de X .

Montrons que le stabilisateur d'un point est un sous-groupe. Cet ensemble est non-vidé car il contient e , on a en effet toujours $e.x = x$. Soient $g, g' \in \text{Stab}_G(x)$, alors $g.x = x$ et $g'.x = x$. Donc $x = g.x = g.e.x = g.(g'^{-1}.g').x = g.g'^{-1}.(g'.x) = g.g'^{-1}.x$, et donc gg'^{-1} est encore dans le stabilisateur. D'où le résultat. \square

On dit que $x \in X$ est un *point fixe* si son orbite par G est ponctuelle, c'à-d réduite à $\{x\}$, c'à-d $\forall g \in G, g.x = x$. On note $\text{Fix}(G)$ l'ensemble des points fixes pour l'action de G sur X . Remarquons que dans le cas d'une permutation, on avait déjà défini la notion d'orbite et de point fixe; on peut vérifier sans peine que les définitions coïncident si on considère l'action du groupe engendré par σ sur $X = \{1, \dots, n\}$.

Proposition 4.1. Pour tout $x \in X$,

$$[G : \text{Stab}_G(x)] = |\mathcal{O}_G(x)|.$$

Si G est fini, on a donc

$$|G| = |\mathcal{O}_G(x)| \cdot |\text{Stab}_G(x)|.$$

En particulier, le cardinal d'une orbite et le cardinal d'un stabilisateur divisent toujours le cardinal du groupe.

Proof. On considère l'application $G \rightarrow X$, $g \mapsto g.x$. Par définition de l'orbite, l'image de cette application est l'orbite de x . Appelons ϕ l'application restreinte à l'arrivée : $\phi : G \rightarrow \mathcal{O}_G(x)$, $\phi(g) = g.x$, qui est alors surjective. Soit \mathcal{R}

la relation d'équivalence modulo le sous-groupe $H = \text{Stab}_G(x)$, c'est-à-dire $g\mathcal{R}g'$ ssi $g'^{-1}g \in H$. Montrons que ϕ passe au quotient modulo \mathcal{R} . Soient $g\mathcal{R}g'$, on a donc $\phi(g) = g.x = g'g'^{-1}g.x = g'.x = \phi(g')$. Donc ϕ passe au quotient en une application $\tilde{\phi} : G/H \rightarrow \mathcal{O}_G(x)$, qui est encore surjective. Montrons qu'elle est injective : si $\tilde{\phi}(gH) = \tilde{\phi}(g'H)$, on a alors $\phi(g) = \phi(g')$ et donc $g.x = g'.x$ d'où $g'^{-1}g.x = x$, et ainsi $g'^{-1}g \in \text{Stab}_G(x) = H$ d'où $gH = g'H$. Ainsi, il existe une bijection naturelle entre l'orbite de x et le quotient de G par le stabilisateur, d'où les formules ci-dessus car $[G : \text{Stab}_G(x)] = |G/H|$ et si $|G|$ est fini, on sait que $|G| = |H|.|G/H|$. \square

Exercice 8 : Soit G le sous-groupe de \mathcal{S}_{11} engendré par la permutation σ de l'exercice 4. On fait agir G naturellement sur $X = \{1, \dots, 11\}$. Pour chacun des points de X , décrire l'orbite et le stabilisateur.

Exercice 9 : On considère l'action de \mathcal{S}_3 sur $X = \mathcal{S}_3$ par conjugaison. Pour chaque point $x \in X$, décrire l'orbite et le stabilisateur.

5. EQUATION AUX CLASSES

Derrière ce titre cryptique se cache une équation toute simple : comme les orbites forment une partition de X , si l'on a choisi un élément x_i dans chaque orbite $|X| = \sum_i |\mathcal{O}_G(x_i)|$, et ainsi nous obtenons une première forme de l'équation aux classes :

$$|X| = \sum_i \frac{|G|}{|\text{Stab}_G(x_i)|}.$$

On peut aussi, et c'est souvent assez pratique, mettre de côté les orbites ponctuelles. Si x_1, \dots, x_k sont cette fois un élément dans chaque orbite non ponctuelle, on a alors

$$|X| = |\text{Fix}(G)| + \sum_i |\mathcal{O}_G(x_i)|.$$

Ce qui nous donne une autre forme de l'équation aux classes.

Exercice 10 : Un groupe de cardinal 35 agit sur un ensemble à 4 éléments. Montrez que cette action est triviale.

6. RÉFÉRENCES

Si les notions exposées ici posent problème, on pourra consulter sur le sujet [Calais], page 115 et +, 175 et +, ou bien [Gras], pages 39-40 et page 71 et +.

REFERENCES

- [Calais] Josette Calais, *Éléments de théorie des groupes*, puf.
 [Gras] G. et M. Gras, *Algèbre fondamentale, Arithmétique*, ellipses.

UNIVERSITÉ RENNES I, IRMAR, CAMPUS DE BEAULIEU 35042 RENNES CEDEX - FRANCE
E-mail address: francois.maucourant@univ-rennes1.fr