TD n°5 : Actions de groupe et groupe symétrique

20 et 24/10/2023

Définition 1. Soit G un groupe. Dans ce TD, un G-ensemble sera un couple $(X, \bullet)$ où X est un ensemble non vide et $\bullet : G \times X \to X$ est une application qui vérifie les deux axiomes d'action de groupe.

Définition 2. Soit X un G-ensemble. L'action de G sera dite fidèle si le morphisme de groupes $m^\bullet : G \to \mathfrak{S}_X$ est injectif.

Exercice 1. Échauffement ?

Petit pot pourri de questions pour commencer.

1. L'action de μ_3 sur $\{z \in \mathbb{C} \mid z^3 = 2\}$ par multiplication est-elle fidèle ?
   Et celle de $\mathbb{Z}$ sur $\mathbb{Z}/3\mathbb{Z}$ telle que $n \bullet (k + 3\mathbb{Z}) = 2^n k + 3\mathbb{Z}$?
   Et l'action canonique de $\mathfrak{S}_3$ sur $\{1, 2, 3\}$?
2. Quel est le groupe engendré par $(1\,2\,3\,4\,5)$ et $(1\,2)$ dans $\mathfrak{S}_5$? Par $(1\,2\,3\,4\,5)$ et $(1\,2\,3)$ dans $\mathfrak{S}_5$?
3. Démontrer que pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
4. Soit G un groupe fini et $(X, \bullet)$ un G-ensemble fini. Démontrer que si l'action est transitive alors $|X|$ divise $|G|$.
5. Soit G un groupe fini et $(X, \bullet)$ un G-ensemble fini. Démontrer que si l'action est fidèle alors $|G|$ divise $|X|!$.

Correction de l'exercice 1 :

1. Pour tout $\zeta \in \mu_3$ et tout racine z de $X^3 + 2$, nous si $\zeta \bullet z = z$, cela signifie $(z \neq 0)$ que $\zeta = 1$. L'action est fidèle ; elle est même libre.
   Puisque $2^2 \equiv 1 \mod 3$, l'action de 2 est triviale :
   $$\forall k,\ 2 \bullet (k + 3\mathbb{Z}) = 2^2 k + 3\mathbb{Z} = k + 3\mathbb{Z}.$$
   L'action n'est pas fidèle puisque 2 est fixe tous les éléments (il est dans le noyau de l'action).
   Si une permutation fixe tous les éléments, c'est l'identité : l'action est fidèle.
2. En conjugant $(1\,2)$ par les puissances $(1\,2\,3\,4\,5)$, on obtient tous les $(i\,i+1)$ et $(1\,5)$. En conjugant à présent ces transpositions entre elles, nous obtenons toutes les permutations. Par exemple,
   $$(1\,3) = (1\,2)(2\,3)(1\,2).$$
   Les permutations engendrant $\mathfrak{S}_5$, il en découle que $\langle (1\,2\,3\,4\,5), (1\,2) \rangle = \mathfrak{S}_5$.

   Les deux permutations étant paires, il est déjà possible d'affirmer que le groupe engendré sera contenu dans $\mathfrak{A}_5$. En conjugant $(1\,2\,3)$ par $(1\,2\,3\,4\,5)^2$, nous obtenons $(3\,4\,5)$. En conjuguant $(1\,2\,3)$ par des puissances de $(3\,4\,5)$, nous obtenons tous les 3-cycles du type $(1\,2\,a)$. Or, un 3-cycle dans $\mathfrak{S}_5$ s'écrit nécessairement $(i\,i+1\,b)$ pour un certain i. En conjugant les $(1\,2\,a)$ par des puissances de $(1\,2\,3\,4\,5)$, nous obtenons tous les 3-cycles, qui engendrent $\mathfrak{A}_5$. Par conséquent,
   $$\langle (1\,2\,3\,4\,5), (1\,2\,3) \rangle = \mathfrak{A}_5.$$
3. Soit $(a\,b\,c)$ un 3-cycle. Soit $\sigma \in \mathfrak{S}_n$ qui envoie $1, 2$ et 3 sur a, b et c. Alors $\sigma(1\,2\,3)\sigma^{-1} = (a\,b\,c)$. C'est également le cas de la conjugaison par $\sigma(4\,5)$. L'une des deux permutations σ ou $\sigma(4\,5)$ est paire ce qui conclut que $(1\,2\,3)$ et $(a\,b\,c)$ sont conjugués sous $\mathfrak{A}_n$.

4. Soit $x \in X$. Il se trouve que $|G| = |G_x||O_x|$ et que dans notre cas $O_x = |X|$. Ceci implique que $|X|$ divise $|G|$.
5. Dire que l'action est fidèle signifie que le morphisme de groupes
$$G \to \mathfrak{S}_X$$
donné par l'action est injectif. Il en découle que G s'identifie à un sous-groupe de $\mathfrak{S}_X$ qui est de cardinal $|X|!$. Le théorème de Lagrange conclut.

Exercice 2. Lemme de Ore

Soit G un groupe fini et p le premier minimal divisant $|G|$. Montrer que tout sous-groupe de G d'indice p est distingué.

Correction de l'exercice 2 :

Soit H un sous-groupe d'indice p. On considère l'action canonique de G sur les classes à gauche G/H. Appelons K le noyau de cette action. C'est un sous-groupe distingué de G contenu dans le stabilisateur de H, qui vaut H. Nous déduisons de $K \subseteq H$ que $p|[G : K]$. Puisque le groupe quotient G/K s'identifie à un sous-groupe de $\mathfrak{S}_p$. L'indice de $[G : K]$ divise $p!$. Enfin, par définition de p, l'indice ne contient que des facteurs premiers supérieurs ou égaux à p. Il en découle que $[G : K] = p$ donc que $K = H$. Le sous-groupe H est par conséquent distingué.

Remarque : vous pouvez essayer de régler le cas $p = 2$ sans action de groupe.

Exercice 3. Morphismes de G-ensembles

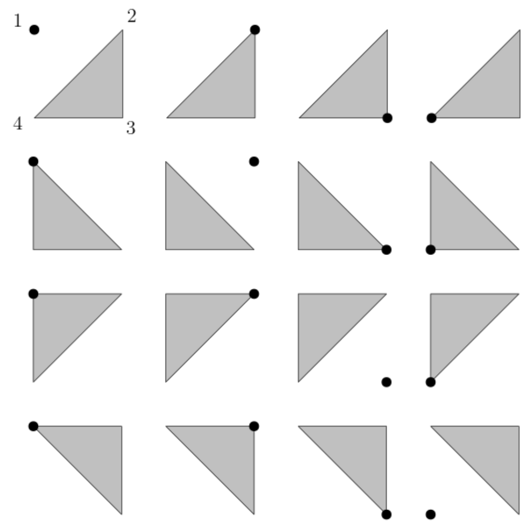
Cet exercice vise à comprendre un peu mieux la notion de morphismes de G-ensembles. Soit G un groupe. Un morphisme entre deux G-ensembles $(X, \bullet)$ et $(Y, \star)$ est une application $f : X \to Y$ telle que
$$\forall (g, x) \in G \times X, \;\; f(g \bullet x) = g \star f(x).$$

1. Démontrer que pour tout élément $x \in X$, nous avons $G_x \subseteq G_{f(x)}$.
2. Démontrer que l'image d'une orbite de X est égale[1] à une orbite de Y.

Ceci nous permet de restreindre la compréhension des morphismes de G-ensembles à celle des morphismes entre G-ensembles transitifs. Nous rappelons que les classes d'isomorphismes de tels G-ensembles sont paramétrées par les classes de conjugaison de sous-groupes de G, un sous-groupe H correspondant à l'ensemble des classes à gauche G/H muni de la multiplication à gauche.

3. Nous fixons H et K deux sous-groupes de G. Démontrer que s'il existe un morphisme $G/H \to G/K$ alors l'un des conjugués de H est contenu dans K.
4. Exhiber une bijection entre les automorphismes de G/H et le quotient $N_G(H)/H$.
5. Pour utiliser ces résultats un peu théoriques, il convient de considérer un exemple concret. Considérons l'ensemble T&P des couples formés d'une partie à trois éléments et d'un élément de $\{1, 2, 3, 4\}$ que nous représentons comme suit.

1. Elle n'est pas seulement contenue dans une orbite de Y.



Les permutations des éléments $1, 2$ et 3 fournissent une action de $\mathfrak{S}_3$ sur T&P. Démontrer qu'elle possède 6 automorphismes.

Correction de l'exercice 3 :

1. Soit $x \in X$ et $g \in G_x$. Alors,
$$g \star f(x) = f(g \bullet x) = f(x)$$
ce qui démontre que $G_x \subseteq G_{f(x)}$.
2. L'orbite de $x \in X$ est l'ensemble des $g \bullet x$, donc son image est $\{f(g \bullet x) \,|\, g \in G\}$. Puisque f est un morphisme de G-ensembles, cette image vaut $\{g \star f(x) \,|\, g \in G\}$. L'orbite de x est envoyée par X exactement sur l'orbite de $f(x)$.
Toute orbite de X est un G-ensemble transitif si on la munit de l'action restreinte. Un morphisme de G-ensemble se décompose orbite par orbite, et il envoie chaque orbite de X sur une unique orbite de Y. Comprendre lesdits morphismes revient donc à les comprendre pour une source et un but transitifs.
3. Soit $f : {}^G/_H \to {}^G/_K$ un morphisme de G-ensembles. Prenons g_f un élément tel que $f(H) = g_f K$. En appliquant la première question et en nous souvenant de l'expression des stabilisateurs pour ces actions canoniques, nous obtenons $H \subseteq g_f K g_f^{-1}$.
Réciproquement, supposons qu'il existe g_0 tel que $H \subseteq g_0 K g_0^{-1}$. Nous voudrions construire une application entre les G-ensembles qui envoie H sur $g_0 K$. Par analyse, elle devrait alors envoyer gH sur gg_0K pour tout $g \in G$. Il faut démontrer que cette définition est correcte, or pour tout $g, h \in H$, alors
$$ghg_0K = g(h(g_0Kg_0^{-1}))g_0 = g(g_0Kg_0^{-1})g_0 = gg_0K$$
puisque $H \subseteq g_0Kg_0^{-1}$. L'application
$$f : {}^G/_H \to {}^G/_K, \;\; gH \mapsto gg_0K$$
est donc bien définie ; c'est par construction un morphisme de G-ensembles.
4. Appliquer le raisonnement de la question précédente avec $K = H$ démontre qu'un automorphisme du G-ensemble ${}^G/_H$ est uniquement déterminé par un élément g_0 tel que $H \subseteq g_0 H g_0^{-1}$. En effet, pour un tel g_0, nous avons même égalité $H = g_0 H g_0^{-1}$ ce qui permet de définir un morphisme pour g_0^{-1} qui est un inverse. Ceci nous définit une surjection
$$\mu : \mathrm{N}_G(H) \twoheadrightarrow \mathrm{Aut}_{G-\mathrm{Ens}}\left({}^G/_H\right), \;\; g_0 \mapsto [gH \mapsto gg_0^{-1}H = gHg_0^{-1}]$$
où nous avons considéré le morphisme associé à g_0^{-1} pour que cette application soit un morphisme de groupes comme le démontre le calcul suivant :

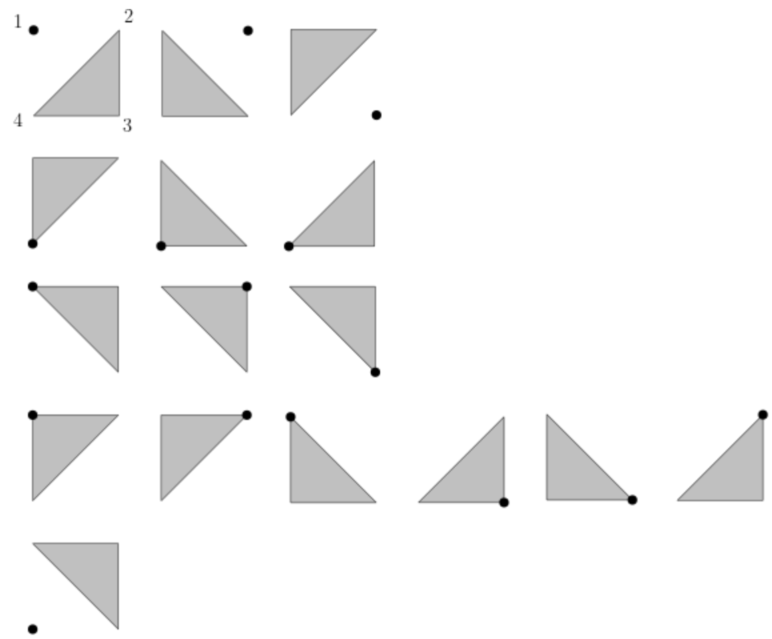
$$\begin{aligned}\mu(g_1g_0)(gH) &= gH(g_1g_0)^{-1} \\ &= (gHg_0^{-1})g_1^{-1} \\ &= (gg_0^{-1}H)g_1^{-1} &&= \mu(g_1)(gg_0^{-1}H) \\ &= [\mu(g_1)\circ\mu(g_2)]\,(gH)\end{aligned}$$

Le noyau de ce morphisme correspond aux g_0 tels que

$$\forall g \in G,\ \ gHg_0 = gH,$$

autrement dit à H. Le premier théorème d'isomorphisme nous fournit un isomorphisme de groupes.

5. Nous commençons par décomposer T&P en orbites, ce que nous illustrons dans la figure suivante où chaque ligne est une orbite :



Les stabilisateurs du premier de la première et troisième ligne, ainsi que du dernier de la deuxième ligne valent $\langle(1\,2)\rangle$ ce qui fournit un isomorphisme desdites orbites avec le $\mathfrak{S}_3$-ensemble ${}^{\mathfrak{S}_3}/_{\langle(1\,2)\rangle}$. Puisque l'avant-dernière orbite est de cardinal 6, elle correspond au sous-groupe trivial. Puisque la dernière orbite est de cardinal 1, elle correspond au sous-groupe $\mathfrak{S}_3$. Un automorphisme s'obtient en permutant les orbites de même type, puis en appliquant un automorphisme. Le normalisateur de $\langle(1\,2)\rangle$ dans $\mathfrak{S}_3$ est lui-même (ce sous-groupe n'est pas distingué et son normalisateur le contient). Ainsi, tous les groupes d'automorphismes des orbites sont triviaux. Un automorphisme de T&P revient à une permutation des trois orbites isomorphes à ${}^{\mathfrak{S}_3}/_{\langle(1\,2)\rangle}$.

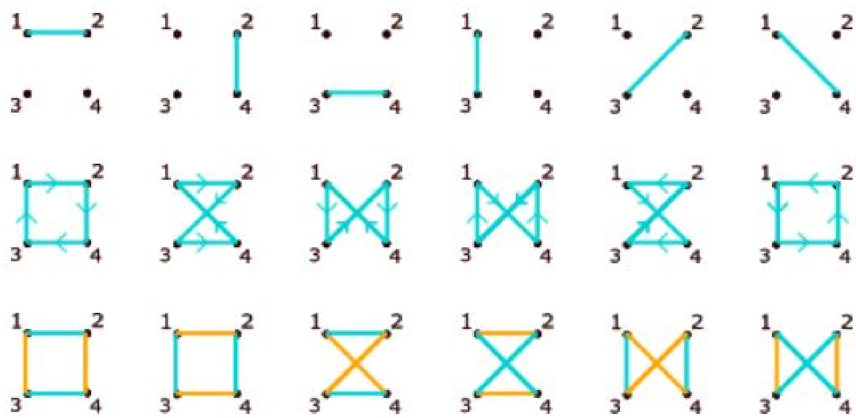
Exercice 9. Action transitive de $\mathfrak{S}_4$ sur 6 éléments

Le but de cet exercice est de classer à isomorphisme près les actions transitives de $\mathfrak{S}_4$ sur 6 éléments.

1. Nous définissons A comme l'ensemble des 4-cycles de $\mathfrak{S}_4$ sur lesquels $\mathfrak{S}_4$ agit par conjugaison. Démontrer que le $\mathfrak{S}_4$-ensemble A est transitif à 6 éléments, que le stabilisateur du cycle c est $\langle c\rangle$ puis que l'action est fidèle.
2. Nous définissons B comme l'ensemble des parties de cardinal 2 de $\{1,2,3,4\}$ et nous faisons agit $\mathfrak{S}_4$ dessus. Démontrer que le $\mathfrak{S}_4$-ensemble B est transitif à 6 éléments, décrire le stabilisateur de $\{i,j\}$ puis démontrer que l'action est fidèle.

3. Trouver une action transitive de $\mathfrak{S}_3$ sur un ensemble à 6 éléments dont tous les stabilisateurs sont triviaux. En déduire une action transitive de $\mathfrak{S}_4$ sur un ensemble à 6 éléments pour laquelle tous les stabilisateurs valent K_4 (en particulier son noyau vaut K_4).
4. Démontrer qu'un sous-groupe d'ordre 4 de $\mathfrak{S}_4$ est égal au stabilisateur d'un élément de A, au stabilisateur d'un élément de B ou à K_4. En déduire un classement des actions transitives de $\mathfrak{S}_4$ sur un ensemble à 6 éléments à isomorphisme près.

Nous donnons une représentation graphique des éléments des trois actions pour se les représenter.



5. Existe-t-il d'autres sous-groupes transitifs d'indice 30 dans $\mathfrak{S}_6$ que ceux obtenus grâce aux actions des deux premiers types ?

Correction de l'exercice 9 :

1. Tout 4-cycle peut s'écrire $(1\,a\,b\,c)$; ils sont effectivement au nombre de 6. De plus, ce sont des permutations de même type et elles sont conjuguées sous l'action de $\mathfrak{S}_4$. L'ensemble A est transitif à 6 éléments. Le stabilisateur de c contient $\langle c\rangle$ puisque c commute avec ses puissances. La formule $|\mathfrak{S}_4| = |\mathrm{Stab}_c||A|$ permet de déduire que le stabilisateur de c est réduit à $\langle c\rangle$. Le noyau de l'action vaut par conséquent
$$\cap_{c\in A}\langle c\rangle = \{\mathrm{Id}\}.$$
2. Il existe effectivement 6 sous-ensembles à deux éléments de $\{1,2,3,4\}$. L'action de $\mathfrak{S}_n$ sur $\{1,2,\ldots,n\}$ est n-transitive ; en particulier l'ensemble B est transitif. Soit $\{i,j\}\in B$. Nous écrivons $\{1,2,3,4\} = \{i,j,k,l\}$. Les éléments Id, $(i\,j)$, $(k\,l)$ et $(i\,j)(k\,l)$ appartiennent au stabilisateur de $\{i,j\}$ et un argument de cardinalité similaire à la question précédente démontre que ce sont les seuls. L'intersection de ces sous-groupe étant triviale, l'action est fidèle.
3. Une action à stabilisateurs triviaux est libre. Pour qu'elle soit transitive, il faut que ce soit l'action de Cayley ; L'action par translation de $\mathfrak{S}_3$ sur lui-même est par conséquent la seule qui convient. Votre cours démontre que le quotient ${}^{\mathfrak{S}_4}/_{K_4}$ est isomorphe à $\mathfrak{S}_3$. Le morphisme de groupe
$$\mathfrak{S}_4 \to {}^{\mathfrak{S}_4}/_{K_4} \cong \mathfrak{S}_3 \to \mathfrak{S}_{\mathfrak{S}_3}$$
où le dernier morphisme correspond à l'action de Cayley fournit une action de $\mathfrak{S}_4$ sur $\mathfrak{S}_3$. L'action d'un élément σ correspond à l'action de son image dans le quotient. Puisque l'action de Cayley est transitive à stabilisateurs triviaux, l'action de $\mathfrak{S}_4$ obtenue est transitive à stabilisateurs égaux à K_4.
4. Soit H un sous-groupe de cardinal 4 de $\mathfrak{S}_4$. Il est isomorphe à ${}^{\mathbb{Z}}/_{4\mathbb{Z}}$ s'il contient un élément d'ordre 4, ou à $({}^{\mathbb{Z}}/_{2\mathbb{Z}})^2$ sinon. S'il contient un élément d'ordre 4, cet élément est un 4-cycle : H est le sous-groupe engendré par ce 4-cycle, a fortiori un stabilisateur dans A. Sinon, supposons que H contienne une transposition $(i\,j)$. Tous les autres éléments de H commutent avec $(i\,j)$. Les seuls éléments possibles

sont dans le stabilisateurs de $\{i, j\}$: H est donc égal à ce stabilisateur. Dans le cas qu'il reste, H est consitué d'éléments d'ordre 2 qui ne sont pas des transpositions. Il est donc inclus dans K_4 qui est le groupe des produits de deux transpositions à supports disjoints, et vaut K_4 par cardinalité.

Les actions transitives de $\mathfrak{S}_4$ sur 6 éléments sont classés par les classes de conjugaisons de sous-groupes de $\mathfrak{S}_4$ d'ordre 4. La discussion qui précède démontre que ces classes sont exactement celle des stabilisateur de A, celle des stabilisateurs dans B et K_4. Les actions des trois premières questions classent par conséquent les actions recherchées à isomorphisme près.

5. Les deux premières actions sont des actions fidèles de $\mathfrak{S}_4$ sur 6 éléments. Elles fournissent donc un morphisme $\mathfrak{S}_4 \hookrightarrow \mathfrak{S}_6$. Attention, considérer le sous-groupe obtenu par conjugaison dans $\mathfrak{S}_6$ revient à considérer d'autres actions isomorphes.

   Je vous laisse le soin de vérifier que le sous-groupe

$$\langle (1\,2), (3\,4), (5\,6), (1\,3\,5)(2\,4\,6) \rangle$$

   est un sous-groupe transitifs d'indice 30 de $\mathfrak{S}_6$ et qu'il contient $(1\,4\,5\,2\,3\,6)$. Les sous-groupes précédemment obtenus étaient isomorphes à $\mathfrak{S}_4$ et ne contenaient par conséquent par d'élément d'ordre 6.