Groupes et actions de groupes
1 : Actions de groupes finis

Quelques corrections d'exercice.

Exercice 1 *(manipulation ***)*

1. Quelle est la liste des ordres des éléments des groupes suivants ? (on ne demande pas l'ordre de chacun des éléments)

a. $\mathbb{Z}/6\mathbb{Z}$, **b.** $\mathbb{Z}/12\mathbb{Z}$, **c.** S_5, **d.** S_6, **e.** S_7.

La première propriété rappelée montre que tout diviseur de n est l'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$. Cela répond à la question pour les groupes $\mathbb{Z}/n\mathbb{Z}$.

L'ordre d'un élément de S_n est le ppcm des ordres des cycles disjoints qui le composent. Donc les ordres dans S_5 sont 1, 2, 3, 4, 5, $\text{ppcm}\,(2,3) = 6$ car $5 = 2+3$. Les ordres dans S_6 sont 1, 2, 3, 4, 5 et 6. Les ordres dans S_7 sont 1, 2, 3, 4, 5, 6, 7, $\text{ppcm}\,(2,5) = 10$ car $7 = 2+5$ et $\text{ppcm}\,(3,4) = 12$ car $7 = 3+4$.

2. Soit G un groupe. Décrire les morphismes de $\mathbb{Z}$ dans G et les morphismes de $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{Z}$, dans G.

Un morphisme de $\mathbb{Z}$ dans G est entièrement déterminé par l'image du générateur 1 de $\mathbb{Z}$, et cette image peut être quelconque dans G. En effet pour tout $g \in G$, l'application $k \mapsto g^k$ est bien définie de $\mathbb{Z}$ dans G et c'est un morphisme.

Soit $\phi : \mathbb{Z}/n\mathbb{Z} \to G$ un morphisme et soit $g = \phi(\overline{1})$ l'image du générateur $\overline{1}$ de $\mathbb{Z}/n\mathbb{Z}$ (on peut choisir ici n'importe quel générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$). Comme ϕ est un morphisme, on a $g^n = \phi(1)^n = \phi(n\overline{1}) = \phi(\overline{0}) = 1_G$. Donc l'ordre de g divise n. Réciproquement pour tout élément g de G d'ordre divisant n, l'application $\overline{k} \mapsto g^k$ est bien définie de $\mathbb{Z}/n\mathbb{Z}$ dans G. Cela montre que le choix d'un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans G revient au choix d'un élément d'ordre divisant n dans G, image du générateur $\overline{1}$ de $\mathbb{Z}/n\mathbb{Z}$.

3. Existe-t-il des morphismes non triviaux :

a. de $\mathbb{Z}/4\mathbb{Z}$ dans S_5 ? (les expliciter tous)

Un tel morphisme est déterminé par l'image du générateur $\overline{1}$. Cette image doit être d'ordre 1,2 ou 4 dans S_5, d'après la question précédente.

Seul le neutre id est d'ordre 1 dans S_5, le morphisme correspondant est le morphisme trivial envoyant tout le groupe $\mathbb{Z}/4\mathbb{Z}$ sur le neutre id.

Les éléments d'ordre 2 dans S_5 sont les $\binom{5}{2} = 10$ transpositions et les $\binom{5}{2}\binom{3}{2} = 30$ produits de deux transpositions de supports disjoints.

Les éléments d'ordre 4 dans S_5 sont les $\frac{5!}{4} = 30$ 4-cycles de S_5.

b. de $\mathbb{Z}/7\mathbb{Z}$ dans S_5 ? **c.** de $\mathbb{Z}/12\mathbb{Z}$ dans S_5 ?

d. de $\mathbb{Z}/221\mathbb{Z}$ dans S_8 ?

4. À quelle condition existe-t-il un morphisme non trivial de $\mathbb{Z}/n\mathbb{Z}$ dans S_m, $m, n \in \mathbb{Z}$?

Exercice 2 *(manipulation ***) Variante : exercice 2.2 p. 50 du [Combes]*

1. Décrire les actions de $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$ sur un ensemble à 5 éléments : combien peut-il y avoir d'orbites pour de telles actions ? Ces actions sont-elles libres ? fidèles ?

Actions de $\mathbb{Z}/3\mathbb{Z}$ sur un ensemble à 5 éléments :

Les orbites sont de cardinal 1 ou 3 (diviseurs du cardinal du groupe). Les décompositions de 5 en 1 ou 3 sont : $5 = 3+1 = 1+1+1+1+1$. Donc une telle action possède 2 ou 5 orbites. Dans tous les cas il y a au moins une orbite à 1 élement, donc l'action n'est pas libre, elle possède même un point fixe global. S'il y a 5 orbites, c'est l'action trivial, non fidèle. S'il y a une orbite à 3 éléments, le générateur $\overline{1}$ de $\mathbb{Z}/3\mathbb{Z}$ ne peut pas fixer de point de cette orbite, sinon tout le groupe fixerait ce point, donc son orbite ne pourrait avoir 3 éléments. Le noyau de l'action (l'ensemble des éléments qui agissent comme l'identité), sous-groupe de $\mathbb{Z}/3\mathbb{Z}$, est donc réduit au neutre. L'action est dans ce cas fidèle.

Actions de $\mathbb{Z}/5\mathbb{Z}$ sur un ensemble X à 5 éléments :

Dans ce cas il y a soit une seule orbite, soit 5 orbites réduites à un élément. Le cas à 5 orbites est trivial, supposons que l'action n'a qu'une seule orbite. Le même raisonnement que précédemment montre que l'action du groupe est fidèle (le noyau de l'action est $\{\overline{1}\}$ ou $\mathbb{Z}/5\mathbb{Z}$). L'action est un morphisme de groupe de $\mathbb{Z}/5\mathbb{Z}$ dans $S(X) \simeq S_5$. D'après l'exercice précédent, l'image de $\overline{1}$ est d'ordre 5, c'est un 5-cycle. Cela montre que l'action est libre (tous les éléments de $\mathbb{Z}/5\mathbb{Z}$ sauf l'identité agissent comme des 5-cycles sur X).

Actions de $\mathbb{Z}/7\mathbb{Z}$ sur un ensemble à 5 éléments :

Dans ce cas il n'y a qu'une décomposition de 5 en diviseurs de 7, c'est $5 = 1+1+1+1+1$. L'action est triviale.

2. À quelle condition sur n existe-t-il des actions fidèles de $\mathbb{Z}/3\mathbb{Z}$ sur un ensemble à n éléments ? des actions libres ?

D'après ce qu'on a vu, il suffit que $n \geq 3$ pour qu'il existe une action fidèle, et $3|n$ pour qu'il existe une action libre (décomposer l'ensemble en orbites de taille 3 sur lesquelles $\mathbb{Z}/3\mathbb{Z}$ agit cycliquement).

3. Décrire une action géométrique fidèle du groupe $\mathbb{Z}/3\mathbb{Z}$ sur un ensemble à 4 éléments.

Le groupe des rotations qui laissent invariant un triangle équilatéral du plan euclidien agit sur le triangle et son centre avec deux orbites, l'orbite réduite au centre et l'orbite à 3 éléments formées des sommets du triangle.

Exercice 3 *(manipulation ***)*

On rappelle la formule de Burnside, qu'on n'utilisera pas mais qu'on vérifiera dans les exemples de cet exercice : si un groupe fini G opère sur un ensemble fini X et si N est le nombre d'orbite de l'action, alors :

$$N = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

Soit G un groupe à 14 éléments agissant sur un ensemble X à 8 éléments.

1. Quel est le nombre possible d'orbites pour l'action de G ?

les orbites sont de cardinal 1, 2, 7 ou 14 et les décompositions de 8 en ces entiers sont

$$8 = 7{+}1 = 2{+}2{+}2{+}2 = 2{+}2{+}2{+}1{+}1 = 2{+}2{+}1{+}1{+}1{+}1 = 2{+}1{+}1{+}1{+}1{+}1{+}1 = 1{+}1{+}1{+}1{+}1{+}1{+}1{+}1,$$

ce qui fait 2, 4, 5, 6, 7 ou 8 orbites.

2. Montrer que l'action de G est sans point fixe global (c'est-à-dire sans point fixé par tous les éléments de G) si et seulement si elle a 4 orbites. Retrouver la formule de Burnside dans ce cas.

La seule action sans orbite à un élément, c'est-à-dire sans point fixe global, possède 4 orbites à 2 éléments. On se place désormais dans ce cas. Le groupe G agit sur les 4 orbites, il suffit de connaître les actions possibles de G sur un ensemble à deux éléments pour connaître toutes les actions de G sur X.

Pour la formule de Burnside, traitons les cas $G = \mathbb{Z}/14\mathbb{Z}$ et $G = D_7$.

Supposons que $G = \mathbb{Z}/14\mathbb{Z}$ agit transitivement (une seule orbite) sur un ensemble à deux éléments. Le générateur $\overline{1}$ de G ne peut pas fixer les deux éléments, sinon tous les éléments de G fixeraient les deux points et il y aurait deux orbites. Donc il les échange. On en déduit l'action de tous les éléments de G : les éléments $\overline{2k}$ fixent les deux points et les éléments $\overline{2k+1}$ les échangent. Sur X union de 4 orbites de cardinal 2, cela signifie que les éléments $\overline{2k}$ de G fixent tous les points de X et les éléments $\overline{2k+1}$ ne fixent aucun point de X. La formule de Burnside s'écrit :

$$4 = \frac{1}{14}(8+0+8+0+8+0+8+0+8+0+8+0+8+0) = \frac{7\times 8}{14}.$$

Supposons maintenant que $G = D_7$ agit transitivement sur un ensemble à deux éléments. Le groupe G contient 6 rotations d'ordre 7 et l'identité, qui forment un groupe cyclique C_7 de cardinal 7 (isomorphe à $\mathbb{Z}/7\mathbb{Z}$), et 7 éléments d'ordre 2, les symétries. Le sous-groupe des rotations agit trivialement sur l'ensemble à deux éléments (les orbites sont de cardinal 1 ou 7, donc 1). Le groupe diédral est engendré par une rotation (qui engendre le sous-groupe des rotations C_7) et une symétrie (la classe à gauche σC_7 de cette symétrie σ modulo C_7 donne toutes les symétries de D_7). Si la symétrie agit trivialement sur l'ensemble à deux éléments, alors D_7 agit trivialement, ce qui contredit que l'action est transitive. Donc la symétrie, et par conséquent toutes les symétries, agissent en permuttant les deux éléments de l'ensemble. Cela montre *qu'à nouveau 7 éléments de G fixent les 8 points de X et 7 éléments ne fixent aucun point. La formule de Burnside est identique à celle pour $\mathbb{Z}/14\mathbb{Z}$.*

Le cas général peut être abordé de deux façons. Si on connait la classification des groupes d'ordre 14, on sait qu'à isomorphisme près, il n'y a que les groupes $\mathbb{Z}/14\mathbb{Z}$ et D_7. Sinon on remarque qu'avec le théorème de Cauchy, un groupe G d'ordre 14 contient un sous-groupe H d'ordre 7. Tout groupe d'ordre premier est cyclique (l'ordre d'un élément divise le cardinal du groupe, donc il y a un élément d'ordre 1 et tous les autres sont d'ordre le cardinal premier, donc engendre le groupe) et on a vu que l'action de $\mathbb{Z}/7\mathbb{Z}$, donc de H, sur X est triviale si elle n'a que des orbites de cardinal 2. Si on prend $a \notin H$, les autres éléments de G sont ceux de la classe aH. Comme H agit trivialement, ces éléments agissent tous comme a (ils sont de la forme ah, donc $ah.x = a.(h.x) = a.x$) pour tout $x \in X$). Si a agit trivialement sur une orbite, tous les éléments de G agissent trivialement et ça contredit que l'orbite est de cardinal 2. Donc a, ainsi que ses translatés de aH, agissent tous en échangeant les points des orbites à 2 éléments. On retrouve ce qui s'est passé pour les deux actions décrites précédemment, et la formule de Burnside est donc la même que précédemment.

Remarque : à partir du moment où on a trouvé 7 éléments dans G qui ont 8 points fixes, la formule de Burnside elle-même oblige les autres éléments du groupe à ne fixer aucun élément. Sinon le terme de droite de la formule serait strictement plus grand que 4.

3. Montrer que si G est abélien, c'est-à-dire $G \simeq \mathbb{Z}/14\mathbb{Z}$ (résultat admis), l'action ne peut pas être fidèle (on vérifiera qu'un élément d'ordre 2 ou un élément d'ordre 7 agit de façon triviale sur X).

Pour simplifier les notations, on supposera $G = \mathbb{Z}/14\mathbb{Z}$. On a vu que si l'action n'est pas triviale, elle a une orbite de cardinal 7 ou une orbite (au moins) de cardinal 2. Si elle a une orbite de cardinal 2, on a vu que les éléments "pairs" de $\mathbb{Z}/14\mathbb{Z}$ (ceux de $2\mathbb{Z}/14\mathbb{Z}$, qu'on peut aussi voir comme formant le noyau du morphisme canonique de $\mathbb{Z}/14\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$) sont d'ordre 1 ou 7 et fixent tous les points de X, donc l'action n'est pas fidèle.

Supposons donc que l'action ait deux orbites, une de cardinal 7 et une de cardinal 1. Il faut montrer que l'action de $\mathbb{Z}/14\mathbb{Z}$ sur l'orbite à 7 éléments n'est pas fidèle. Prenons l'élément $\overline{7}$ d'ordre 2 dans $\mathbb{Z}/14\mathbb{Z}$. Le sous-groupe de cardinal 2 qu'il engendre agit sur l'orbite à 7 éléments et possède donc une orbite à 1 élément (car 7 est impair). Cela signifie que $\overline{7}$ fixe un point x de l'orbite. Les points de cette orbite sont tous de la forme $\overline{k}.x$ avec $\overline{k} \in \mathbb{Z}/14\mathbb{Z}$. Comme $\overline{7}$ fixe x, son conjugué $\overline{k} + \overline{7} - \overline{k}$ (attention à la notation additive ! On constate ici que la notation multiplicative, par exemple $G = \mathbb{U}_{14}$ aurait eu des avantages) fixe $\overline{k}.x$. Par commutativité de $\mathbb{Z}/14\mathbb{Z}$, cela signifie que $\overline{7}$ fixe tous les points de l'orbite. Comme il fixe le 8-ème point de X (seul dans son orbite), cela montre que $\overline{7}$ agit trivialement sur X et donc que l'action n'est pas fidèle.

4. Montrer que si G est non abélien, l'action peut être fidèle. Donner une situation géométrique dans laquelle on retrouve cette action.

C'est le cas de l'action de D_7 sur l'ensemble formé par les sommets d'un 7-gone régulier du plan affine euclidien et son centre.

Exercice 4 *(manipulation et culture ***)*

On va montrer qu'une action fidèle d'un groupe G à 35 éléments sur un ensemble à 14 éléments possède nécessairement 4 orbites. Pour commencer on étudie la structure du groupe et on va montrer que son cardinal le force à être abélien. Ce sera l'occasion d'étudier le groupe des automorphismes d'un groupe, ce qui est une notion importante en théorie des groupes.

1. En utilisant le théorème de Cauchy, montrer que G possède un sous-groupe H d'ordre 7 et un sous-groupe K d'ordre 5. En utilisant le théorème de Frobenius-Ore, montrer que H est distingué dans G.
Remarque : en général on montre l'existence et les propriétés de ces sous-groupes par un théorème plus puissant que les théorèmes de Cauchy et de Frobenius-Ore, le théorème de Sylow. Celui-ci n'est pas au programme de l'agrégation interne.

2. Soit a un générateur du groupe K. Montrer que l'application $\phi : H \to H$ définie par $x \mapsto axa^{-1}$ est bien définie et que c'est un automorphisme de H.

3. Montrer que $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \simeq (\mathbb{Z}/7\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z}$. (Attention, on a fait une incursion dans la théorie des anneaux en considérant le groupe des inversibles de *l'anneau* $\mathbb{Z}/7\mathbb{Z}$. On ne reparlera plus d'anneau dans cet exercice ni dans cette feuille !)

4. En déduire que $\phi = \mathrm{id}$ puis que l'application $H \times K \to G$ définie par $(h, k) \mapsto hk$ est bien définie et est un isomorphisme de groupe (attention à la structure de groupe sur $H \times K$). En conclure que $G \simeq \mathbb{Z}/35\mathbb{Z}$.

5. Montrer qu'une action fidèle de $\mathbb{Z}/35\mathbb{Z}$ sur un ensemble à 14 éléments possède nécessairement 4 orbites.

Exercice 5 *Le théorème de Cauchy [Combes, th. 2.4], [Gourdon, exercice 11] (classique oral ***)*
Soit G un groupe fini de cardinal n et p un nombre premier divisant n. On note $X = \{(g_1, ..., g_p) \in G^p \mid g_1...g_p = 1\}$.
On considère l'action de $\mathbb{Z}/p\mathbb{Z}$ sur G^p par permutation circulaire sur les indices : si $\overline{k} \in \mathbb{Z}/p\mathbb{Z}$ et $(g_1, ..., g_p) \in X$, on définit $\overline{k}.(g_1, ..., g_p) = (g_{1+k}, ..., g_{p+k})$ où les indices sont pris modulo p.

1. Montrer que cela définit bien une action de $\mathbb{Z}/p\mathbb{Z}$ sur G^p et que la partie X est stable sous l'action de $\mathbb{Z}/p\mathbb{Z}$.
On considère donc maintenant l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X.

2. Que peut-on dire des orbites à un élément de cette action ?

3. Calculer le cardinal de X. En déduire qu'il existe un élément d'ordre p dans G.

Exercice 6 *Un théorème de Frobenius, souvent attribué à Ore, [Ulmer] exercice 7.5, (classique *)*
Soit G un groupe fini et p le plus petit nombre premier divisant le cardinal de G. On suppose que G possède un sous-groupe H d'indice p et on va montrer que H est alors distingué dans G.
On fait agir G sur l'ensemble des classes à gauche $G/H = \{gH,\ g \in G\}$ par translation : pour tout $g \in G$ et $g'H \in G/H$, on pose $g.g'H = gg'H$.

1. Vérifier que cela définit bien une action de G sur G/H et que cette action est transitive.
On restreint maintenant cette action à H, qui agit donc par translation sur G/H.

2. Montrer qu'il y a une orbite de cardinal 1 pour cette action et en déduire que toutes les orbites sont de cardinal 1.

3. Vérifier que pour tout $g \in G$, dire que gH est fixe par l'action de H sur G/H signifie exactement que $gHg^{-1} = H$. Conclure.

Exercice 7 *Stabilisateurs conjugués et élément sans point fixe (entrainement et culture *)*
Soit G un groupe fini et H un sous-groupe strict de G, d'indice $k \geq 2$.

1. Montrer que pour tout $g, g' \in G$, si g et g' sont dans la même classe à gauche [ou à droite] modulo H, alors $gHg^{-1} = g'Hg'^{-1}$. En déduire que le nombre de sous-groupes conjugués à H, c'est-à-dire de la forme gHg^{-1}, est inférieur ou égal à k.

2. En utilisant le fait que l'élément neutre appartient à tous les sous-groupes conjugués de H, en déduire que $\cup_{g \in G} gHg^{-1} \neq G$.

3. Application : soit G un groupe fini agissant transitivement sur un ensemble X de cardinal au moins 2. Montrer qu'il existe un élément de G qui ne fixe aucun point de X.

Exercice 8 *La formule de Burnside [Combes, Gourdon, Skandalis...] (classique ***)*
Soit G un groupe fini agissant sur un ensemble fini X.
Montrer que le nombre N d'orbites de l'action est la moyenne des cardinaux des points fixes des éléments de G :

$$N = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Indication : calculer de deux manières différentes le cardinal de l'ensemble $E = \{(g, x) \in G \times X \mid g.x = x\}$.

Applications :

1. On prend une permutation aléatoire de S_n. Quel est le nombre moyen de ses points fixes ? (Remarque : la méthode standard pour calculer cette moyenne est d'utiliser la linéarité de l'espérance et de calculer la loi des variables aléatoires X_k, $k \in \{1, ..., n\}$, valant 1 si k est fixe par la permutation et 0 sinon.)

2. Retrouver à l'aide de la formule de Burnside que si un groupe fini G agit transitivement sur un ensemble X de cardinal au moins 2, alors il existe un élément de G qui ne fixe aucun point de X. En déduire que si H est un sous-groupe strict de G, alors $\cup_{g \in G} gHg^{-1} \neq G$.

Application : la formule de Burnside a deux applications classiques à l'oral de l'agrégation, le nombre de colliers de perles de couleurs prescrites et le nombre de coloriages d'un cube.
Une référence pour le collier de perle :
Combes : Algèbre et Géométrie, exercice 2 p.44 et ex. 2-2 p.50.
Des références pour le cube :
Eric Lehman, *Mathématiques pour l'étudiant de première année. Algèbre et géométrie*, Sec. 4.3
Philippe Caldero, Marie Peronnier, *Carnet de voyage en Algébrie*, 2019, p.141-142.
Peter M. Neumann, Gabrielle A. Story, E. C. Thompson, *Groups and Geometry.*