Préparation à l'agrégation interne 2020-2021

Groupes et actions de groupes
1 : Actions de groupes finis

Objectif : manipuler les principaux résultats sur les actions de groupes et les groupes finis les plus classiques ($\mathbb{Z}/n\mathbb{Z}$, D_{2n}, S_n).

Références
COMBES, *Algèbre et géométrie.*
GOURDON, *Math en tête - Algèbre*
SKANDALIS, *Algèbre générale et algèbre linéaire.*
ULMER, *Théorie des groupes, cours et exercices.*

Voici quelques résultats à connaître. Certaines preuves sont données plus loin en exercice.

1. *Soit n un entier. Tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques et pour tout diviseur d de n, il existe un unique sous-groupe de cardinal d dans $\mathbb{Z}/n\mathbb{Z}$.*

Résultat à connaître sur les sous-groupes d'un groupe cyclique. Deux façons de le prouver : "à la main", chercher un générateur du sous-groupe, ou utiliser la caractérisation des sous-groupes de $\mathbb{Z}$.

2. *Soit G un groupe agissant sur un ensemble X. Soit $g \in G$ et $x \in X$.*
Pour tout $h \in G$, g fixe x si et seulement si hgh^{-1} fixe $h.x$. Autrement dit :

$$\mathrm{Stab}(h.x) = h\,\mathrm{Stab}(x)\,h^{-1}.$$

$\mathrm{Stab}(x)$ désigne le stabilisateur de x, c'est-à-dire l'ensemble des éléments du groupe qui fixent x. Ce résultat est immédiat mais important. Il exprime que dans une orbite, les stabilisateurs des points sont deux à deux conjugués.

3. *Soit G un groupe agissant sur un ensemble X. Soit $x \in X$. On a :*

$$|O_x|.|\mathrm{Stab}(x)| = |G|.$$

Retenir de ce résultat que les orbites sont liées à la structure du groupe G. En particulier pour un groupe fini, le cardinal d'une orbite divise le cardinal du groupe. La preuve est très simple, elle consiste à montrer qu'il y a une bijection naturelle entre l'orbite de x et l'ensemble des classes (à gauche ou à droite) de $\mathrm{Stab}(x)$ dans G (noter qu'en général $\mathrm{Stab}(x)$ n'est pas un sous-groupe distingué de G).

4. *Théorème (Cauchy) : Soit G un groupe fini de cardinal n. Pour tout nombre premier p divisant n, il existe un élément d'ordre p dans G (autrement dit G possède un sous-groupe cyclique de cardinal p).*

La preuve classique de ce résultat est courte et astucieuse, elle utilise une action de groupe sur un ensemble ad hoc. Elle est proposée plus loin en exercice.

5. *Théorème (Frobenius) : Soit G un groupe fini de cardinal n. Si p est le plus petit nombre premier divisant n et si H est un sous-groupe d'indice p de G, alors H est distingué dans G.*

Ce résultat est souvent appelé le théorème de Ore, mais il semble qu'il faut l'attribuer à Frobenius. Attention, il n'existe pas forcément de tel sous-groupe : un groupe fini peut être simple (sans sous-groupe distingué non trivial).

6. *Soient p, q deux nombres premiers, avec $p < q$. Alors :*
   - *si p ne divise pas $q-1$, il y a un seul groupe de cardinal pq à isomorphisme près : c'est $\mathbb{Z}/pq\mathbb{Z}$, isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*
   - *si p divise $q-1$, il y a deux groupes de cardinal pq à isomorphisme près, l'un abélien, $\mathbb{Z}/pq\mathbb{Z}$, l'autre non abélien.*

Ce résultat nécessite des outils un peu élaborés (produit semi-direct). Il peut faire partie de la culture générale. Un cas particulier est $p = 2$: à isomorphisme près, il y a deux groupes de cardinal $2p$, le groupe cyclique $\mathbb{Z}/2p\mathbb{Z}$ et le groupe diédral D_p.

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.

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.

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

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

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 ?
(En fait on demande ici de déterminer ces actions à conjugaison des actions près, c'est-à-dire modulo une bijection de l'ensemble à 5 éléments dans lui-même.)

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 ?

3. Décrire une action géométrique fidèle du groupe $\mathbb{Z}/3\mathbb{Z}$ sur un ensemble à 4 éléments.
Variante : exercice 2.2 p. 50 du [Combes]

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 ?

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.

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).

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

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.*