Préparation à l'agrégation interne 2022-2023

Groupes et actions de groupes

Exercice 1 : le théorème de Lagrange et applications.

Soit G un groupe fini de cardinal n.

1. Montrer que tout sous-groupe de G est de cardinal un diviseur de n.
2. Montrer que tout élément de G est d'ordre un diviseur n.
   On suppose que le groupe G agit sur un ensemble X.
3. Soit $x \in X$. On note $G.x = \{g.x,\ g \in G\}$ l'orbite de x par l'action de G. On appelle *stabilisateur de* x l'ensemble G_x des éléments du groupe G qui fixent x.
   (a) Montrer que G_x est un sous-groupe de G.
   (b) Montrer que pour tout $g \in G$, les éléments de la classe à gauche gG_x envoie x sur $g.x$.
   (c) En déduire une bijection entre l'ensemble G/G_x et l'orbite $G.x$, puis la relation :
   $$\text{card}\,(G) = \text{card}\,(G_x).\text{card}\,(G.x).$$
   En particulier, le cardinal de tout orbite divise le cardinal du groupe.
4. Montrer que tout groupe fini de cardinal un nombre premier est cyclique.

Exercice 2 : groupes d'ordre p^2.

Référence : [Combes, p.65]

Soit p un nombre premier et G un groupe de cardinal p^2. On veut montrer que G est abélien. On note $Z(G) = \{g \in G,\ \forall h \in G,\ hg = gh\}$, le *centre* de G.

1. Montrer que $Z(G)$ est un sous-groupe distingué de G.

On considère l'action de G sur lui-même par conjugaison :

$$\begin{array}{ccc} G & \to & \text{Aut}\,(G) \\ g & \mapsto & (h \mapsto ghg^{-1}) \end{array}$$

2. Montrer que le cardinal des orbites de cette action vaut 1, p ou p^2.
3. Montrer qu'il y a au moins une orbite de cardinal 1. En déduire que $Z(G)$ est de cardinal p ou p^2.
4. On suppose que $Z(G)$ est de cardinal p.
   (a) Montrer que $G/Z(G)$ est cyclique.
   (b) Soit $a \in G$ tel que l'image de a dans $G/Z(G)$ engendre ce groupe. Montrer que tout élément de G s'écrit sous la forme $z.a^r$ avec $z \in Z(G)$ et $r \in \mathbb{Z}$.
   (c) En déduire que G est abélien. Conclure.

Exercice 3 : le théorème de Cauchy

Références : [Combes, th. 2.4], [Gourdon, exercice 11], [X-ENS].

1. Dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ existe-t-il des éléments d'ordre 5 ? 8 ? 12 ? 40 ?

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.

2. 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.

3. Que peut-on dire des orbites à un élément de cette action ?
4. Calculer le cardinal de X. En déduire qu'il existe un élément d'ordre p dans G.

Exercice 4 : Exposant d'un groupe.

Référence : [Gourdon] ex.9 p.26.

Cet exercice contient un développement classique : tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

On appelle *exposant* d'un groupe G le plus petit entier $e \geq 1$, s'il existe, tel que $x^e = 1$ pour tout $x \in G$.

1. Montrer qu'un groupe fini possède un exposant fini.
2. Déterminer l'exposant des groupes $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, S_5.

Soit G un groupe abélien fini d'exposant e. Pour $g \in G$, on note $\langle g \rangle$ le sous-groupe de G engendré par g.

3. Montrer que si deux éléments a, b de G sont d'ordre premier entre eux, alors $\langle a \rangle \cap \langle b \rangle = \{1\}$ (indication : que peut-on dire de l'ordre d'un élément de $\langle a \rangle \cap \langle b \rangle$?) et ordre(ab) = ordre(a).ordre(b).
4. Montrer que si un élément a de G est d'ordre nm, avec n, m entiers, alors G possède un élément d'ordre n.
5. Montrer que si deux éléments a, b de G sont d'ordre n et m respectivement, alors G possède un élément d'ordre ppcm(n, m) (indication : décomposer n et m en produit de facteurs premiers). Donner un exemple où ab n'est pas d'ordre ppcm(n, m).
6. En déduire [1] que e est le maximum des ordres des éléments de G et le ppcm des ordres des éléments de G (indication : trouver un élément de G dont l'ordre est le ppcm des ordres des éléments de G).
7. Application : nous allons montrer que tout sous-groupe fini du groupe multiplicatif d'un corps $\mathbb{K}$ est cyclique. Soit G un tel groupe, n son cardinal et $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ sa décomposition en facteurs premiers.

1. certaines références définissent l'exposant d'un groupe par une de ces deux manières, mais ce n'est pas naturel

(a) Montrer que pour tout $i = 1, ..., k$, G possède un élément d'ordre un multiple de $p_i^{\alpha_i}$ (indication : sinon G serait contenu dans l'ensemble des racines d'un polynôme $X^m - 1$ avec $m < n$).

(b) En déduire que G est cyclique.

(c) Que peut-on en déduire pour le groupe multiplicatif $\mathbb{F}_p^*$? pour $\mathbb{C}^*$?

(d) Combien y a-t-il de générateurs de $\mathbb{F}_7^*$? (indication : il y a l'indicatrice d'Euler quelque part.) Les trouver.

8. Pour tout entier $n > 1$, donner un exemple de groupe (non abélien) possédant deux éléments a et b d'ordre 2 tels que ab est d'ordre n. Même question avec a et b d'ordre 2 et ab est d'ordre infini.

Complément sur l'exposant : Le résultat suivant est un développement classique de l'agrégation :

Théorème de Burnside : Si G est sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ d'exposant fini, alors G est fini.

Il est développé dans [Francinou-Gianella-Nicolas, Oraux x-ens, algèbre 2] ex. 3.6. Le résultat est faux pour un groupe quelconque, il existe des groupes infini d'exposant fini.

Exercice 5 : Un théorème de Frobenius, souvent attribué à Ore.

Référence : [Ulmer] exercice 7.5

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.
4. Montrer que le groupe $\mathcal{A}_4$ n'admet pas de sous-groupe d'indice 2.

Exercice 6 : les groupes d'ordre 35.

On va montrer qu'il n'y a qu'un groupe à 35 éléments à isomorphisme près. Cet exercice utilise les exercices précédents.
Soit G un groupe de cardinal 35.

1. Montrer que G possède un sous-groupe H d'ordre 7 et un sous-groupe K d'ordre 5.
2. Montrer que H est distingué dans G.
3. 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.
4. Montrer [2] que $\mathrm{Aut}\,(\mathbb{Z}/7\mathbb{Z}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$.

2. Attention, on a fait une incursion dans la théorie des anneaux en considérant le groupe des inversibles de l'anneau $\mathbb{Z}/7\mathbb{Z}$.

5. En déduire que $\phi = \mathrm{id}$ (indication : étudier les puissances de ϕ).
6. Montrer que l'application $H \times K \to G$ définie par $(h, k) \mapsto hk$ est bien définie et est un isomorphisme de groupe. En conclure que $G \simeq \mathbb{Z}/35\mathbb{Z}$.

Exercice 7 : la formule de Burnside.

Références : [Combes, Gourdon, Skandalis...]

Soit G un groupe fini agissant sur un ensemble fini X.

1. 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 $E = \{(g, x) \in G \times X \mid g.x = x\}$.
2. Applications :
   (a) Quel est le nombre moyen des points fixes d'une permutation aléatoire de S_n ? (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.)
   (b) 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 (traité ci-dessous).
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.*

Exercice 8 : le groupe d'isométrie du cube.

Références :[Lehman], [Caldero et al], [Neumann et al] cités plus haut.

Cet exercice étudie le groupe des isométries du cube et application. Nous allons commencer par étudier quelques propriétés générales des groupes d'isométrie et quelques exemples de groupes d'isométrie de partie du plan.

Si E est un espace (affine ou vectoriel) euclidien et X est une partie de E, on appelle *groupe d'isométrie de* X l'ensemble $\mathrm{Is}(X)$ des isométries (affines ou linéaires) laissant X invariant, c'est-à-dire les isométries $f \in O(E)$ telles que $f(X) \subset X$. On vérifie facilement que c'est un groupe. On appelle *groupe d'isométrie positive de* X le sous-groupe $\mathrm{Is}^+(X)$ de $\mathrm{Is}(X)$ formé des isométries directes laissant X invariant.

1. Montrer que $\mathrm{Is}^+(X)$ est un sous-groupe distingué d'indice 1 ou 2 de $\mathrm{Is}(X)$ et que si E est de dimension impaire et X est une partie de E symétrique par rapport à 0, alors $\mathrm{Is}(X) \simeq \mathrm{Is}^+(X) \times \{\pm \mathrm{id}\}$.

Dans le plan affine euclidien $\mathbb{R}^2$, on considère les parties suivantes :

$$A = \mathbb{R}(1,0) \cup \mathbb{R}(0,1),\ B = \{(-1,0),(1,0)\},\ C = \{(\pm 1,0), \pm(1,1)\}$$
$$D = \{(\pm 1, \pm 2)\},\ E = \{(\pm 1, \pm 1)\}.$$

2. Déterminer les groupes d'isométrie $\mathrm{Is}(A)$, $\mathrm{Is}(B)$, $\mathrm{Is}(C)$, $\mathrm{Is}(D)$, $\mathrm{Is}(E)$ et leurs sous-groupes des isométries directes. Donner une partie X du plan telle que $\mathrm{Is}(X) = \mathrm{Is}^+(X) \simeq \mathbb{Z}/4\mathbb{Z}$.

On considère maintenant un cube X dans un espace affine euclidien de dimension 3 (indication : on pourra supposer que le cube est formé des sommets $(\pm 1, \pm 1, \pm 1)$ dans $\mathbb{R}^3$ muni de sa structure euclidienne canonique). Le cube pourra désigner au choix l'ensemble des sommets ou l'enveloppe convexe de ces sommets.

3. Montrer que les groupes $\mathrm{Is}^+(X)$ et $\mathrm{Is}(X)$ fixent le centre du cube.
4. En faisant agir le groupe d'isométrie du cube sur des ensembles géométriques associés au cube, construire des morphismes de $\mathrm{Is}(X)$ dans $\mathcal{S}_8$ et $\mathcal{S}_6$, et déterminer leurs noyaux.
5. Montrer qu'il y a exactement 4 paires de sommets réalisant le diamètre du cube, les paires de sommets diamétralement opposés.
6. En déduire des morphismes de $\mathrm{Is}^+(X)$ et $\mathrm{Is}(X)$ dans $\mathcal{S}_4$. Montrer que ces morphismes sont surjectifs (indication : on utilisera un système de générateurs de $\mathcal{S}_4$).
7. En utilisant la matrice des isométries dans différentes bases associées aux sommets du cube, déterminer le noyau de ces morphismes.
8. En déduire que $\mathrm{Is}^+(X) \simeq \mathcal{S}_4$ et $\mathrm{Is}(X) \simeq \mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$. Déterminer tous les éléments de ces groupes.
9. En utilisant la formule de Burnside, en déduire le nombre de cubes différents qu'on peut obtenir en coloriant ses faces à l'aide de (au plus) trois couleurs (les cubes sont considérés identiques si on peut passer de l'un à l'autre par une isométrie directe).