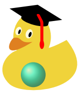
ENS de Lyon — Algèbre 1
L3 — 2024-2025

TD 2 : Théorèmes d'isomorphismes et actions de groupes

Les exercices marqués d'un  seront corrigés en TD, si le temps le permet.

Exercices importants

Exercice 1. (Groupes monogènes)
Soit G un groupe monogène. Montrer que soit $G \cong \mathbb{Z}$, soit $G \cong \mathbb{Z}/n\mathbb{Z}$ pour un entier strictement positif n.



Exercice 2.
Soit $n > 0$ un entier.

1. Montrer que $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(n)$ éléments d'ordre n, $\varphi(n)$ désigne le nombre d'entiers $k \in [\![0, n-1]\!]$ premiers à n.
2. Montrer que pour tout $d > 0$ divisant n, $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe d'ordre d formé des multiples de $\overline{\frac{n}{d}}$.
3. En déduire que pour tout diviseur $d > 0$ de n, $\mathbb{Z}/n\mathbb{Z}$ contient $\varphi(d)$ éléments d'ordre d et que $\sum_{0<d|n} \varphi(d) = n$.

Exercice 3.

1. Montrer que le groupe $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est premier.
2. Soit G un groupe fini abélien. Montrer que G est simple si et seulement si $G = \mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier.

Exercice 4.
Soit G un groupe et H un sous-groupe de G d'indice 2. Montrer que H est distingué dans G. Montrer que le résultat n'est pas vrai si on remplace 2 par 3.

Exercice 5. (p-groupes)
Soit p un nombre premier.

1. Rappeler pourquoi le centre d'un p-groupe est non trivial.
2. Montrer que tout groupe d'ordre p^2 est abélien, et classifier ces groupes.
3. Soit G un groupe d'ordre p^n. Montrer que G admet un sous-groupe distingué d'ordre p^k pour tout $k \in [\![0, n]\!]$.

Exercice 6. (Troisième théorème d'isomorphisme)
Soit G un groupe, et soient H et K des sous-groupes de G tels que $H \lhd G$ et $H \leqslant K$. On notera $\pi_H : G \to G/H$.

1. Montrer que le groupe $\pi_H(K)$ est distingué dans G/H si et seulement si K est distingué dans G.

2. Justifier que H est distingué dans K et que l'on a un isomorphisme $\pi_H(K) \cong K/H$.
3. On suppose que K est distingué dans G et on note $\pi_K : G \to G/K$ la projection canonique.
   (a) Montrer que π_K induit un unique morphisme de groupes $\overline{\pi}_K : G/H \to G/K$ tel que $\pi_K = \overline{\pi}_K \circ \pi_H$.
   (b) Montrer que le noyau de $\overline{\pi}_K$ est le sous-groupe $\pi_H(K) \cong K/H$.
   (c) En déduire le troisième théorème d'isomorphisme : $(G/H)\,/\,(K/H) \cong G/K$.

Exercice 7. (Sous-groupes d'un quotient)
Soient G un groupe, et H un sous-groupe distingué de G. On note $\pi_H : G \to G/H$ la projection canonique.

1. (a) Soit K un sous-groupe de G. Montrer que $\pi_H^{-1}(\pi_H(K)) = KH$.
   (b) En déduire que π_H induit une bijection croissante entre les sous-groupes de G/H et les sous-groupes de G contenant H.
2. Montrer que les sous-groupes distingués de G/H sont en correspondance avec les sous-groupes distingués de G contenant H.
3. Montrer que le correspondance précédente préserve l'indice : si K est un sous-groupe de G d'indice fini contenant H, alors $[G : K] = [G/H : \pi_H(K)]$.

Exercice 8. (Combinatoire algébrique)
Soit K un corps fini à q élements et $n \in \mathbb{N}^*$. On définit $\mathrm{PGL}_n(K)$ comme le quotient $\mathrm{GL}_n(K)/K^\times$ où $K^\times$ correspond au sous-groupe distingué formé de la forme λI_n avec $\lambda \in K^\times$. On considère l'action de $\mathrm{GL}_n(K)$ sur l'ensemble des droites vectorielles de K^n.

1. Déterminer le cardinal des groupes finis $\mathrm{GL}_n(K)$, $\mathrm{SL}_n(K)$, $\mathrm{PGL}_n(K)$. (*Indication : compter les bases de K^n.*)
2. On prend désormais $n = 2$.
   (a) Montrer que le nombre de droites vectorielles de K^2 est égal à $q + 1$.
   (b) En déduire qu'il existe un morphisme de groupes injectif $\mathrm{PGL}_2(K) \to \mathfrak{S}_{q+1}$.
3. Montrer que $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.
4. Montrer que $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$.

Exercice 9. (Formule de Burnside)
Soit G un groupe fini agissant sur un ensemble fini X. On note N le nombre d'orbites de l'action.

1. Soit $Y = \{(g, x) \in G \times X,\ g \cdot x = x\}$. Interpréter le cardinal de Y comme somme sur les éléments de X d'une part, et de G d'autre part.
2. En décomposant X en union d'orbites, montrer la formule de Burnside :
$$N = \frac{1}{\#G} \sum_{g \in G} \#\,\mathrm{Fix}(g).$$
3. Soit n un entier. Quel est le nombre moyen de points fixes des éléments de $\mathfrak{S}_n$, pour l'action naturelle sur $[\![1, n]\!]$?
4. On suppose que G agit transitivement sur X et que X contient au moins 2 éléments. Montrer qu'il existe un $g \in G$ agissant sans point fixe.
5. En déduire qu'un groupe fini n'est jamais l'union des conjugués d'un sous-groupe strict.

Exercices supplémentaires

Exercice 10. (Automorphismes intérieurs)

Soit G un groupe. Pour $g \in G$ on note $\phi_g : G \to G$ la fonction définie par $h \mapsto ghg^{-1}$. On note $\mathrm{Int}(G)$ l'ensemble des ϕ_g pour $g \in G$.

1. Soit $g \in G$, montrer que ϕ_g est un automorphisme de groupes.
2. Montrer que la fonction $\phi : G \to \mathrm{Int}(G)$ qui a g associe ϕ_g est un morphisme de groupes.
3. Montrer l'isomorphisme $G/Z(G) \cong \mathrm{Int}(G)$ où $Z(G)$ est le centre du groupe G.
4. (*Plus difficile*) Montrer que si le groupe des automorphismes $\mathrm{Aut}(G)$ de G est cyclique alors G est abélien.
5. (*Aussi difficile*) Supposons que $\mathrm{Aut}(G)$ est trivial. Démontrer que tous les éléments de G sont d'ordre au plus 2, puis que G est soit trivial, soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exercice 11.

Soient n un entier et $k \in [\![0, n]\!]$. On note $\mathcal{P}_k([\![1, n]\!])$ l'ensemble des parties à k éléments de $[\![1, n]\!]$.

1. Montrer que $\mathfrak{S}_n$ agit naturellement sur $\mathcal{P}_k([\![1, n]\!])$.
2. Justifier que cette action est transitive.
3. Calculer le stabilisateur de $[\![1, k]\!] \in \mathcal{P}_k([\![1, n]\!])$.
4. En appliquant la formule orbite-stabilisateur, retrouver la valeur de $\binom{n}{k}$.

Exercice 12.

Soit G un groupe et soit H un sous-groupe de G. On fait agir H sur l'ensemble G/H par translation.

1. Montrer que H est distingué dans G si et seulement si cette action est triviale.
2. On suppose G fini et on note p le plus petit diviseur premier de l'ordre de G. Déduire que si H est d'*indice* p alors il est distingué.

Exercice 13. (Structure des inversibles de $\mathbb{Z}/n\mathbb{Z}$)

Soit p un nombre premier. On admettra que le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

1. On suppose p différent de 2.
   (a) Montrer que pour tout $k \in \mathbb{N}$, il existe un entier $\lambda_k \equiv 1 \pmod p$ tel que
   $$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$
   (b) En déduire que $1+p$ est d'ordre p^{n-1} dans $(\mathbb{Z}/p^n\mathbb{Z})^\times$.
   (c) En déduire que pour tout $n \geqslant 1$, le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$ est cyclique d'ordre $p^{n-1}(p-1)$.
2. (a) Montrer que pour tout $k \in \mathbb{N}$, il existe un entier μ_k impair tel que
   $$5^{2^k} = 1 + \mu_k 2^{k+2}.$$
   (b) En déduire que pour $n \geqslant 2$, 5 est d'ordre 2^{n-2} dans $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

(c) En déduire un isomorphisme

$$\begin{array}{rcl} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & \longrightarrow & (\mathbb{Z}/2^n\mathbb{Z})^\times \\ (\overline{\varepsilon}, \overline{k}) & \longmapsto & (-1)^\varepsilon 5^k \end{array}.$$

3. Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si n est égal à 1, 2, 4, p^k ou $2p^k$ où $k \in \mathbb{N}^*$ et p est un nombre premier impair.

Exercice 14. (Normalisateur – suite)

Soient G un groupe et H un sous-groupe de G. Soit $N_G(H) = \{g \in G, gHg^{-1} = H\}$ le normalisateur de H dans G. On rappelle que c'est le plus grand sous-groupe de G dans lequel H est distingué.

1. On suppose que $N_G(H)$ est d'indice fini k dans G. Montrer que H admet exactement k conjugué (i.e. il existe exactement k sous-groupes distincts de la forme gHg^{-1} avec $g \in G$).

2. On suppose G fini. Soit S un p-Sylow de G. Montrer que le nombre n_p de p-Sylow de G est égal à l'indice de $N_G(S)$ dans G.