1
2
3

MAT35B - ALGÈBRE L3A
Premier Semestre — 2022-2023

Premier Devoir Surveillé

Toute réponse non justifiée ne sera pas validée.

Le barème est donné à titre indicatif et non contractuel.

3pt **1.** Soit G un groupe. On rappelle que le centre de G est le sous-groupe de G défini par

$$\mathscr{Z}(G) = \{z \in G : gz = zg \text{ pour tout } g \in G\}.$$

(*a*) Vérifier que $\mathscr{Z}(G)$ est distingué dans G.

(*b*) Sans utiliser la question précédent, montrer que $G/\mathscr{Z}(G)$ admet un structure de groupe pour la loi $\cdot$ donnée par

$$\bar{g} \cdot \bar{g}' = \overline{gg'}$$

pour tous $g, g' \in G$, où $\bar{g} \in G/\mathscr{Z}(G)$ désigne la classe de g.

(*c*) Montrer que si le quotient de G par $\mathscr{Z}(G)$ est monogène alors G est abélien.

Solution.

(*a*) On montrera que

$$g\mathscr{Z}(G)g^{-1} \subseteq \mathscr{Z}(G)$$

pour tout $g \in G$. En effet, étant donné $z \in \mathscr{Z}(G)$ et $g \in G$, alors gzg^{-1}, vu que

$$hgzg^{-1} = hzgg^{-1} = hz = zh = gg^{-1}zh = gzg^{-1}h$$

pour tout $h \in G$, où l'on a utilisé $gz = zg$ dans la première identité et $g^{-1}z = zg^{-1}$ dans la dernière identité, vu que z est dans le centre de G.

(*b*) On voit bien que la loi définie sur $G/\mathscr{Z}(G)$ est bien définie, car si $g_1, g_2, g_1', g_2' \in G$ satisfont que $\bar{g}_1 = \bar{g}_2$ et $\bar{g}_1' = \bar{g}_2'$, alors il existe $z, z' \in \mathscr{Z}(G)$ tels que $g_1 = g_2 z$ et $g_1' = g_2' z'$, ce qui nous dit que $g_1 g_1' = g_2 z g_2' z' = g_2 g_2' zz'$, vu que $z \in \mathscr{Z}(G)$, *i.e.*

$$\overline{g_1 g_1'} = \overline{g_2 g_2'}.$$

L'expression explicite de la loi de $G/\mathscr{Z}(G)$ nous dit qu'elle est associative, que $\bar{1}_G$ est l'élément neutre de $G/\mathscr{Z}(G)$ et

$$\bar{g}^{-1} = \overline{g^{-1}}$$

pour tout $g \in G$.

(*c*) On remarque que, étant donné $H \leq G$ un sous-groupe et $S \subseteq G$ un ensemble de représentants de classes d'équivalences à gauche de G/H (*i.e.* $S \subseteq G$ satisfait que la composition d'applications $S \to G \to G/H$ est bijective), alors

$$G = \bigsqcup_{s \in S} s.H. \tag{1}$$

Soit $g \in G$ tel que la classe d'équivalence $\bar{g} \in G/\mathscr{Z}(G)$ soit un générateur du quotient. On va montrer que, étant donné $x_1, x_2 \in G$, $x_1 x_2 = x_2 x_1$. D'après (1) pour $H = \mathscr{Z}(G)$, il existe $n_1, n_2 \in \mathbb{Z}$ et $h_1, h_2 \in \mathscr{Z}(G)$ tels que $x_i = g^{n_i} h_i$ pour $i \in \{1, 2\}$. En conséquence,

$$\begin{aligned} x_1 x_2 &= g^{n_1} h_1 g^{n_2} h_2 = g^{n_1} g^{n_2} h_1 h_2 = g^{n_1+n_2} h_2 h_1 \\ &= g^{n_2} g^{n_1} h_2 h_1 = g^{n_2} h_2 g^{n_1} h_1 = x_2 x_1, \end{aligned}$$

où l'on a utilisé que h_1, h_2 sont dans le centre de G dans la deuxième, troisième et cinquième eqalités.

12pt

2. Soit p un entier premier et G un groupe dont le cardinal est une puissance de p. On a donc $|G| = p^n$ avec $n \in \mathbb{N}^*$ un entier strictement positif. Le but de l'exercice est de montrer que le centre de G n'est pas réduit à $\{1_G\}$.

(*a*) Pour tout g dans G on définit l'application $\mathsf{Ad}_g : G \to G$ donnée par $\mathsf{Ad}_g(z) = gzg^{-1}$ pour tout $z \in G$. Montrer que Ad_g est un automorphisme de groupes de G.

(*b*) Montrer que l'application $\mathsf{Ad} : G \to \mathsf{Aut}_{\mathsf{Gr}}(G)$ qui à $g \in G$ associe Ad_g est un morphisme de groupes.

(*c*) Vérifier que l'on définit bien une relation d'équivalence $\sim$ sur G en posant

$$g_1 \sim g_2 \text{ si et seulement s'il existe } h \in G \text{ tel que } \mathsf{Ad}_h(g_1) = g_2.$$

On notera $\bar{g}$ la classe d'équivalence de $g \in G$ pour $\sim$.

(*d*) Quelle est la classe $\bar{1}_G$ de 1_G ?

(*e*) Montrer que, étant donné $z \in G$, $z \in \mathscr{Z}(G)$ si et seulement si $\bar{z} = \{z\}$.

(*f*) Pour z dans G on définit $\mathsf{Stab}(z)$ par $\mathsf{Stab}(z) = \{g \in G : \mathsf{Ad}_g(z) = z\}$. Montrer que $\mathsf{Stab}(z)$ est un sous-groupe de G.

(*g*) Étant donné $z \in G$, on considère l'application $f_z : G \to \bar{z}$ donnée par $f_z(g) = \mathsf{Ad}_g(z)$ pour $g \in G$. Montrer que l'on peut déduire de f_z une application $\bar{f}_z : G/\mathsf{Stab}(z) \to \bar{z}$ et que cette application est bijective.

(*h*) En déduire que si z est un élément de G qui n'appartient pas à $\mathscr{Z}(G)$ alors p divise le cardinal de $\bar{z}$.

(*i*) Conclure que p divise le cardinal de $\mathscr{Z}(G)$.

Solution.

(*a*) On voit bien que

$$\mathsf{Ad}_g(z_1z_2) = gz_1z_2g^{-1} = gz_1gg^{-1}z_2g^{-1} = \mathsf{Ad}_g(z_1)\,\mathsf{Ad}_g(z_2)$$

pour tous $z_1, z_2 \in G$, ce qui nous dit que Ad_g est un morphisme de groupes. En outre, on voit bien que $\mathsf{Ad}_{1_G} = \mathsf{id}_G$, car

$$\mathsf{Ad}_{1_G}(z) = 1_G z 1_G^{-1} = z$$

pout tout $z \in G$, et $\mathsf{Ad}_g \circ \mathsf{Ad}_h = \mathsf{Ad}_{gh}$ pour tous $g, h \in G$, car

$$\big(\mathsf{Ad}_g \circ \mathsf{Ad}_h\big)(z) = \mathsf{Ad}_g(hzh^{-1}) = ghzh^{-1}g^{-1} = ghz(gh)^{-1} = \mathsf{Ad}_{gh}(z) \tag{2}$$

pout tout $z \in G$. En particulier,

$$\mathsf{Ad}_g \circ \mathsf{Ad}_{g^{-1}} = \mathsf{Ad}_{gg^{-1}} = \mathsf{Ad}_{1_G} = \mathsf{id}_G = \mathsf{Ad}_{g^{-1}g} = \mathsf{Ad}_{g^{-1}} \circ \mathsf{Ad}_g,$$

ce qui nous dit que $(\mathsf{Ad}_g)^{-1} = \mathsf{Ad}_{g^{-1}}$ est l'application réciproque de Ad_g. En conséquence, Ad_g est une application bijective.

(*b*) L'identité (2) nous dit que Ad est un morphisme de groupes.

(*c*) C'est clair que $\sim$ est réflexive, car $g \sim g$ pour tout $g \in G$, vu que $\mathsf{Ad}_{1_G}(g) = g$. En outre, $\sim$ est symétrique, car, si $g_1 \sim g_2$, il existe $h \in G$ tel que $\mathsf{Ad}_h(g_1) = g_2$, ce qui implique que $\mathsf{Ad}_{h^{-1}}(g_2) = g_1$, vu que $(\mathsf{Ad}_h)^{-1} = \mathsf{Ad}_{h^{-1}}$, et en particulier $g_2 \sim g_1$. Finalement, on affirme que $\sim$ est transitive. En effet, si $g_1 \sim g_2$ et $g_2 \sim g_3$, il existe $h, k \in G$ tels que $\mathsf{Ad}_h(g_1) = g_2$ et $\mathsf{Ad}_k(g_2) = g_3$, ce qui implique que

$$g_3 = \mathsf{Ad}_k(g_2) = \mathsf{Ad}_k(\mathsf{Ad}_h(g_1)) = \mathsf{Ad}_{kh}(g_1),$$

i.e. $g_1 \sim g_3$.

(*d*) C'est clair que $\bar{1}_G = \{\mathsf{Ad}_g(1_G) : g \in G\} = \{1_G\}$, vu que $\mathsf{Ad}_g(1_G) = g1_Gg^{-1} = gg^{-1} = 1_G$.

(*e*) On voit bien que $z \in \mathscr{Z}(G)$ si et seulement si $gz = zg$ pour tout $g \in G$, ce qui équivaut à dire que $gzg^{-1} = z$ pour tout $g \in G$, *i.e.* $\mathsf{Ad}_g(z) = z$ pour tout $g \in G$, ce qui est équivalent à $\bar{z} = \{\mathsf{Ad}_g(z) : g \in G\} = \{z\}$.

(*f*) On voit bien que $1_G \in \mathsf{Stab}(z)$, vu que $\mathsf{Ad}_{1_G} = \mathsf{id}_G$ et, en particulier, $\mathsf{Ad}_{1_G}(z) = z$. Soient $g_1, g_2 \in \mathsf{Stab}(z)$, *i.e.* $\mathsf{Ad}_{g_i}(z) = z$ pour $i \in \{1, 2\}$. On conclut que

$$\mathsf{Ad}_{g_1g_2}(z) = \mathsf{Ad}_{g_1}(\mathsf{Ad}_{g_2}(z)) = \mathsf{Ad}_{g_1}(z) = z,$$

ce qui nous dit que $g_1.g_2 \in \mathsf{Stab}(z)$, où l'on a utilisé (2). Finalement, vu que $(\mathsf{Ad}_g)^{-1} = \mathsf{Ad}_{g^{-1}}$, si $g \in \mathsf{Stab}(z)$, l'identité $\mathsf{Ad}_g(z) = z$ implique que

$$z = (\mathsf{Ad}_g)^{-1}(z) = \mathsf{Ad}_{g^{-1}}(z),$$

ce qui nous dit que $g^{-1} \in \mathsf{Stab}(z)$.

(*g*) Étant donné $g \in G$, on notera $[g] \in G/\mathsf{Stab}(z)$ la classe d'équivalence à gauche associée. On définit l'application $\bar{f}_z : G/\mathsf{Stab}(z) \to \bar{z}$ qui associe à $[g] \in G/\mathsf{Stab}(z)$ l'élément $f_z(g)$. On note d'abord que cette application est bien définie, car, étant donné $g, g' \in G$ tels que $[g] = [g']$, $g^{-1}g' \in \mathsf{Stab}(z)$, ce qui implique que

$$z = \mathsf{Ad}_{g^{-1}g'}(z) = \mathsf{Ad}_{g^{-1}}\big(\mathsf{Ad}_{g'}(z)\big) = (\mathsf{Ad}_g)^{-1}\big(\mathsf{Ad}_{g'}(z)\big), \tag{3}$$

et, en particulier,

$$f_z(g) = \mathsf{Ad}_g(z) = \mathsf{Ad}_{g'}(z) = f_z(g'). \tag{4}$$

En outre, c'est clair que $\bar{f}_z$ est surjectif, car $\mathsf{Ad}_g(z) = f_z(g) = \bar{f}_z([g])$. Finalement, on affirme que $\bar{f}_z$ est injectif. En effet, si $\bar{f}_z([g]) = \bar{f}_z([g'])$ alors $\mathsf{Ad}_g(z) = \mathsf{Ad}_{g'}(z)$, ce qui nous dit que $z = \mathsf{Ad}_{g^{-1}g'}(z)$ d'après (3) et (4), ce qui implique que $g^{-1}g' \in \mathsf{Stab}(z)$, *i.e.* $[g] = [g']$.

(*h*) D'après le théorème de Lagrange on conclut que l'ordre de $\mathsf{Stab}(z)$ est une puissance p^d de p, avec $d \leq n$ entier non négatif. En particulier, $\bar{z}$ a cardinal $|G|/|\mathsf{Stab}(z)| = p^{n-d}$ une puissance de p. Si $\mathsf{Stab}(z) = G$, *i.e.* $z \in \mathscr{Z}(G)$, alors $n = d$ et le cardinal de $\bar{z}$ est 1. Si $\mathsf{Stab}(z) \neq G$, *i.e.* $z \notin \mathscr{Z}(G)$, alors $n > d$ et on conclut que p divise le cardinal de $\bar{z}$.

(*i*) Soit $S \subseteq G$ un ensemble de représentants de classes d'équivalences de $G/\sim$ (*i.e.* $S \subseteq G$ satisfait que la composition d'applications $S \to G \to G/\sim$ est bijective). La description de classes de équivalences de $G/\sim$ implique que $\mathscr{Z}(G) \subseteq S$. Or, la décomposition

$$G = \bigsqcup_{s \in S} \bar{s} \tag{5}$$

nous dit que

$$|G| = \sum_{s\in S} |\bar{s}| = \sum_{s\in \mathscr{Z}(G)} |\bar{s}| + \sum_{s\in S\setminus\mathscr{Z}(G)} |\bar{s}| = \sum_{s\in\mathscr{Z}(G)} 1 + \sum_{s\in S\setminus\mathscr{Z}(G)} |\bar{s}| = |\mathscr{Z}(G)| + \sum_{s\in S\setminus\mathscr{Z}(G)} |\bar{s}|.$$

Comme p divise $\bar{s}$ pour tout $s \in S \setminus \mathscr{Z}(G)$ et p divise $|G|$, on conclut que p divise $|\mathscr{Z}(G)|$.

5pt **3.** Dans cet exercice on pourra utiliser les résultats des exercices précédents. Soit $p \in \mathbb{N}^*$ un entier premier.

(*a*) Montrer que tout groupe G de cardinal p^2 est abélien.

(*b*) En déduire que tout groupe de cardinal p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Solution.

(*a*) D'après l'exercice 2, on conclut que $\mathscr{Z}(G)$ est non trivial, ce qui nous dit que l'ordre de $\mathscr{Z}(G)$ est p ou p^2, d'après le théorème de Lagrange. Si $|\mathscr{Z}(G)| = p^2$, alors

$G = \mathscr{Z}(G)$, ce qui implique que G est abélien. Si $|\mathscr{Z}(G)| = p$, alors le théorème de Lagrange nous dit que $|G/\mathscr{Z}(G)| = |G|/|\mathscr{Z}(G)| = p$. Comme $\mathscr{Z}(G)$ est un sous-groupe distingué de G, d'après le premier item de l'exercice 1, $G/\mathscr{Z}(G)$ est un groupe d'ordre p et, en particulier, il est cyclique. Le deuxième item de l'exercice 1 nous dit alors que G est abélien. En particulier, $|\mathscr{Z}(G)| = p$ est absurde, car G est abélien nous dit que $G = \mathscr{Z}(G)$, ce qui implique que $|\mathscr{Z}(G)| = p^2$.

(*b*) D'après l'item précédent, G est abélien. Si G est cyclique, alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, d'après l'exercice **3** de la fiche 2. On suppose alors que G n'est pas cyclique, ce qui nous dit que G n'a pas d'élément d'ordre p^2. Comme l'ordre de tout élément de G est un diviseur de p^2, et le seul élément d'ordre 1 est le neutre, tout élément de G différent du neutre a ordre p. Soient $g \in G \setminus \{1_G\}$ et $H \subseteq G$ le sous-groupe engendré par g. Comme H est un sous-groupe engendré par un élément d'ordre p, il existe un isomorphisme de groupes $\phi : \mathbb{Z}/p\mathbb{Z} \to H$, d'après l'exercice **3** de la fiche 2. En particulier, $H \neq G$, ce qui nous dit qu'il existe $g' \in G \setminus H$. Comme g' a ordre p, si $K \subseteq G$ désigne le sous-groupe engendré par g', il existe un isomorphisme de groupes $\psi : \mathbb{Z}/p\mathbb{Z} \to K$, d'après l'exercice **3** de la fiche 2. Noter que $H \cap K = \{1_G\}$, vu que $|H \cap K|$ divise $|H| = p = |K|$, mais $H \cap K \neq H$. On considère alors l'application $\rho : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ donnée par $\rho(\bar{m}, \bar{n}) = \psi(\bar{m})\phi(\bar{n})$, pour tous $\bar{m}, \bar{n} \in \mathbb{Z}/p\mathbb{Z}$. Comme G est abélien, et ψ et ϕ sont des morphismes de groupes, cette application est un morphisme de groupes. En outre, on affirme que le noyau de ρ est trivial. En effet, soit $((\bar{m})\phi(\bar{n}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ tel que $\rho(\bar{m}, \bar{n}) = \psi(\bar{m})\phi(\bar{n}) = 1_G$. Cela nous dit que $\psi(\bar{m}) = \phi(\bar{n})^{-1} \in H \cap K = \{1_G\}$, ce qui implique que $\psi(\bar{m}) = \phi(\bar{n}) = 1_G$. Comme ψ et ϕ sont injectifs, on conclut que $\bar{m} = \bar{n}$ est l'élément neutre de $\mathbb{Z}/p\mathbb{Z}$, ce qui nous dit que ρ est injectif. Finalement, comme $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}| = |G| = p^2$ est fini, on conclut que ρ est bijectif, ce qui implique que G est isomorphe au groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.