Licence – Mathématiques
Algèbre 2

DM : GROUPES MONOGÈNES
CORRIGÉ

1. (a) Montrons que $\langle 1 \rangle$ est égal à $\mathbb{Z}$. Par stabilité par prise d'inverse, on a $-1 \in \langle 1 \rangle$; et par stabilité par somme, on a pour tout $n \in \mathbb{N}^*$, $n = \underbrace{1 + \dots + 1}_{n \text{ fois}} \in \langle 1 \rangle$ et $-n = \underbrace{(-1) + \dots + (-1)}_{n \text{ fois}} \in \langle 1 \rangle$.

Enfin, 0 étant l'élément neutre de $\mathbb{Z}$, et $\langle 1 \rangle$ étant un sous-groupe, on a $0 \in \langle 1 \rangle$. On en déduit que $\mathbb{Z} \subset \langle 1 \rangle \subset \mathbb{Z}$ et donc que $\langle 1 \rangle = \mathbb{Z}$. Le groupe $\mathbb{Z}$ est donc monogène, engendré par 1.

- (b) On considère $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ l'épimorphisme canonique. L'ensemble $\pi^{-1}(\langle \bar{1} \rangle)$ est alors un sous-groupe de $\mathbb{Z}$ contenant 1 $\in \pi^{-1}(\bar{1})$. D'après la question précédente, on a donc $\pi^{-1}(\langle \bar{1} \rangle) = \mathbb{Z}$ et donc $\langle \bar{1} \rangle = \pi(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. On en déduit que $\mathbb{Z}/n\mathbb{Z}$ est monogène, et donc cyclique puisqu'il est fini.

- (c) On note $\mathbb{U}_n := \{e^{\frac{ik\pi}{n}} \mid k \in \mathbb{Z}\}$ l'ensemble des racines $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$. Pour montrer que $(\mathbb{U}_n, \cdot)$ forme un groupe, il suffit de montrer qu'il s'agit d'un sous-groupe de $\mathbb{C}$. Or, pour tout $k_1, k_2 \in \mathbb{Z}$, on a bien $e^{\frac{ik_1\pi}{n}} \cdot \left(e^{\frac{ik_2\pi}{n}}\right)^{-1} = e^{\frac{i(k_1-k_2)\pi}{n}} \in \mathbb{U}_n$.

On considère maintenant l'application

$$\zeta_n : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ k & \longmapsto & e^{\frac{ik\pi}{n}} \end{array}$$

qui est clairement un épimorphisme de groupes puisque $e^{\frac{ik_1\pi}{n}} \cdot e^{\frac{ik_2\pi}{n}} = e^{\frac{i(k_1+k_2)\pi}{n}}$ pour tous $k_1, k_2 \in \mathbb{Z}$. En raisonnant comme dans la question précédente, on en déduit que $\mathbb{U}_n$ est monogène engendré par $\zeta_n(1) = e^{\frac{i\pi}{n}}$. Comme il est de plus fini, $\mathbb{U}_n$ est donc cyclique.

- (d) Notons $g_1 \in G_1$ et $g_2 \in G_2$ des éléments tels que $\langle g_1 \rangle = G_1$ et $\langle g_2 \rangle = G_2$, et montrons que (g_1, g_2) engendrent $G_1 \times G_2$. En effet, pour tout $(h_1, h_2) \in G_1 \times G_2$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $h_1 = g_1^{k_1}$ et $h_2 = g_2^{k_2}$. De plus, $|G_1|$ et $|G_2|$ étant premiers entre eux, on sait par le théorème des restes chinois qu'il existe $k \in \mathbb{Z}$ tel que $k \equiv k_1 \pmod{|G_1|}$ et $k \equiv k_2 \pmod{|G_2|}$, c'est-à-dire qu'il existe $r_1, r_2 \in \mathbb{Z}$ tels que $k = k_1 + r_1 \cdot |G_1| = k_2 + r_2 \cdot |G_2|$. Enfin, l'ordre d'un élément d'un groupe fini divisant toujours le cardinal du groupe, on a $g_1^{|G_1|} = e_{G_1}$ et $g_2^{|G_2|} = e_{G_2}$. On en déduit que

$$\begin{aligned} (g_1, g_2)^k &= (g_1^k, g_2^k) = (g_1^{k_1+r_1 \cdot |G_1|}, g_2^{k_2+r_2 \cdot |G_2|}) = \left(g_1^{k_1} \cdot (g_1^{|G_1|})^{r_1}, g_2^{k_2} \cdot (g_2^{|G_2|})^{r_2}\right) \\ &= (g_1^{k_1} \cdot e_{G_1}^{r_1}, g_2^{k_2} \cdot e_{G_2}^{r_2}) = (h_1, h_2). \end{aligned}$$

Le groupe $G_1 \times G_2$ est donc monogène, et comme il est fini d'ordre $|G_1| \cdot |G_2|$, il est cyclique.

2. (a) i. Par stabilité de $\langle g_0 \rangle$ par prise d'inverse et par multiplication, on a $\{g_0^k \mid k \in \mathbb{Z}\} \subset \langle g_0 \rangle$. Mais réciproquement, $\{g_0^k \mid k \in \mathbb{Z}\} \subset \langle g_0 \rangle$ est clairement stable par prise d'inverse et par multiplication, c'est donc un sous-groupe de G contenant g_0 ; par minimalité de celui-ci, on a donc $\langle g_0 \rangle \subset \{g_0^k \mid k \in \mathbb{Z}\}$ et donc $\{g_0^k \mid k \in \mathbb{Z}\} = \langle g_0 \rangle = G$.
ii. C'est immédiat d'après la question précédente.
iii. Pour tout $g_1, g_2 \in G$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $g_1 = g_0^{k_1}$ et $g_2 = g_0^{k_2}$. On a alors

$$g_1 \cdot g_2 = g_0^{k_1} \cdot g_0^{k_2} = g_0^{k_1+k_2} = g_0^{k_2+k_1} = g_0^{k_2} \cdot g_0^{k_1} = g_2 \cdot g_1.$$

Le groupe G est donc abélien.

- iv. A. On considère l'application

$$\psi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & g_0^k \end{array},$$

qui est clairement un épimorphisme de groupes. Supposons par l'absurde que ψ n'est pas injective, alors $\text{Ker}(\psi)$ est un sous-groupe de $\mathbb{Z}$ non trivial, c'est-à-dire de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. Mais alors ψ induit un isomorphisme entre $\text{Im}(\psi) = G$ et $\mathbb{Z}/\text{Ker}(\psi) = \mathbb{Z}/n\mathbb{Z}$ ce qui contredit la finitude, induite par la non cyclicité, de G . L'application ψ est donc injective et définit un isomorphisme entre $\mathbb{Z}$ et G .

- B. Avec les notations de la question précédente, on a $\text{Ker}(\psi) \neq \{0\}$ car sinon G serait isomorphe à $\mathbb{Z}$ et donc non fini. On en déduit que ψ induit un isomorphisme entre G et $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$ le plus petit élément strictement positif de $\text{Ker}(\psi)$, c'est-à-dire le plus petit entier strictement positif tel que $g_0^n = e_G$. Autrement dit, $n = |g_0| = |\{g_0^k \mid k \in \mathbb{Z}\}| = |G|$.
- (b) i. Soit $k = q.d + r$ la division euclidienne de k par d . On a alors $g_0^r = g_0^{k-q.d} = g_0^k \cdot (g_0^d)^{-q} \in H$ avec $0 \leq r < d$. Par minimalité de d , on a donc $r = 0$ et d divise k .
- ii. D'après la question précédente, pour tout $h = g_0^k \in H$, il existe $q \in \mathbb{Z}$ tel que $k = q.d$ et donc $h = (g_0^d)^q$. On en déduit que H est monogène engendré par g_0^d .
- iii. D'après la question précédente, il suffit de montrer que H est fini si et seulement si G l'est. En tant que sous-groupe de G , H est clairement fini si G l'est. Réciproquement, si H est fini, alors il existe $n \in \mathbb{N}^*$ tel que $(g_0^d)^n = e_G$ et donc le noyau de l'application ψ est non trivial puisqu'il contient $d.n$. Il découle alors des questions 2.(a).iv.A et B que G est fini.
- (c) i. Soit $h \in G$ un élément générateur. On a alors $h \in \langle g_0 \rangle$ et il existe donc $k_1 \in \mathbb{Z}$ tel que $h = g_0^{k_1}$, mais aussi $g_0 \in \langle h \rangle$ et il existe donc $k_2 \in \mathbb{Z}$ tel que $g_0 = h^{k_2}$. En combinant ces formules, on en déduit que $g_0 = (g_0^{k_1})^{k_2} = g_0^{k_1.k_2}$. Mais puisque G est non cyclique, l'application ψ est injective et on a donc $k_1.k_2 = 1$. Les seuls solutions dans $\mathbb{Z}$ étant $k_1 = k_2 = 1$ et $k_1 = k_2 = -1$, on en déduit que $h = g_0^{\pm 1}$.
- ii. A. En reprenant les notations de la question précédente, on a $g_0^{k_1.k_2-1} = e_G$ et donc $k_1.k_2 - 1 \in \text{Ker}(\psi) = |G|.\mathbb{Z}$. Autrement dit, il existe $q \in \mathbb{Z}$ tel que $k_1.k_2 - 1 = q.|G|$, ce que l'on peut réécrire sous la forme $k_2.k_1 - q.|G| = 1$ d'une relation de Bézout entre k_1 et $|G|$, montrant que ces derniers sont premiers entre eux.
- B. D'après la question précédente, si g_0^k est générateur, alors k est premier avec $|G|$, et puisque $g_0^{|G|} = e_G$, k peut être remplacé par le reste de sa division euclidienne par $|G|$, lequel est bien dans $\llbracket 1, |G| - 1 \rrbracket$ puisque k ne peut pas être un multiple de $|G|$. Réciproquement, si $k \in \llbracket 1, |G| - 1 \rrbracket$ est premier avec $|G|$, alors il existe $r, s \in \mathbb{Z}$ tels que $r.k + s.|G| = 1$, et donc $g_0 = g_0^{r.k+s.|G|} = (g_0^k)^r \cdot (g_0^{|G|})^s = (g_0^k)^r \cdot e_G^s = (g_0^k)^r \in \langle g_0^k \rangle$. On a alors $G = \langle g_0 \rangle \subset \langle g_0^k \rangle$, montrant que g_0^k engendre G .
- (d) i. Puisque $G = \langle g_0 \rangle$, pour tout $h \in G$ il existe $k \in \mathbb{Z}$ tel que $h = g_0^k$ et on a alors $f(h) = f(g_0^k) = f(g_0)^k$.
- ii. Puisque f est surjective, pour tout $h' \in H$, il existe $h \in G$ tel que $h' = f(h)$, et d'après la question précédente, il existe donc $k \in \mathbb{Z}$ tel que $h' = f(g_0)^k$. On en déduit que H est monogène, engendré par $f(g_0)$.
3. (a) Soit $h \in H$ et $g \in G$. Puisque $h \in H \subset Z(G)$, h commute avec g , et on a donc $g^{-1}.h.g = g^{-1}.g.h = h \in H$. On en déduit que H est stable par conjugaison, et donc qu'il s'agit d'un sous-groupe distingué.
- (b) Par hypothèse, G/H est engendré par un élément $\bar{g}_0$ avec $g_0 \in G$. Pour tout $g_1, g_2 \in G$, il existe donc $k_1, k_2 \in \mathbb{Z}$ tels que $\bar{g}_1 = \bar{g}_0^{k_1}$ et $\bar{g}_2 = \bar{g}_0^{k_2}$, autrement dit il existe $h_1, h_2 \in H$ tels que $g_1 = g_0^{k_1}.h_1$ et $g_2 = g_0^{k_2}.h_2$. Dès lors, puisque h_1 et h_2 commutent avec tout le monde, on a
- $$g_1.g_2 = g_0^{k_1}.h_1.g_0^{k_2}.h_2 = g_0^{k_1+k_2}.h_1.h_2 = g_0^{k_2+k_1}.h_2.h_1 = g_0^{k_2}.h_2.g_0^{k_1}.h_1 = g_2.g_1,$$

montrant que G est abélien.