Examen final - MAT35b Algèbre L3A - 2018/2019
Première Session

Durée : 4h

Documents et appareils électroniques interdits.

Le barème proposé est purement indicatif et est susceptible d'être modifié.

Problème. [30.5 pts]

A. [11pts] Dans cette partie, on introduit le groupe diédral D_n et on étudie quelques unes de ses propriétés.

Soit $n \geq 3$. On munit $\mathbb{R}^2$ de sa structure canonique d'espace euclidien orienté. Pour tout $k \in \mathbb{Z}$, on pose

$$v_k = (\cos\Big(\frac{2k\pi}{n}\Big), \sin\Big(\frac{2k\pi}{n}\Big)) \in \mathbb{R}^2.$$

Remarquer que l'on a alors $v_{k+nm} = v_k$ pour tout $m \in \mathbb{Z}$.

On note D_n le sous-groupe des isométries vectorielles de $\mathbb{R}^2$ qui préservent globalement l'ensemble $\{v_k \mid k \in \mathbb{Z}\}$.

1. **[2]** Justifier qu'un élément $u \in D_n$ est complètement déterminé par l'image des vecteurs v_0 et v_1. Montrer que u envoie le couple (v_0, v_1) sur un couple de la forme (v_k, v_{k+1}) ou (v_k, v_{k-1}), avec $0 \leq k \leq n-1$. En déduire que $|D_n| \leq 2n$.

0.5 pour le premier point, 1 pour le deuxième, 0.5 pour la majoration.

2. **[3]** Soit r la rotation (de centre O) et d'angle $\dfrac{2\pi}{n}$, et soit s la symétrie orthogonale d'axe (Ox).

Pour tout $k \in \mathbb{Z}$, calculer l'image de v_k par r^i et $r^i s$, pour $i \in \mathbb{Z}$, et en déduire que les éléments

$$r^i s^j, 0 \leq i \leq n-1, 0 \leq j \leq 1$$

sont des éléments de D_n, et qu'ils sont deux à deux distincts.

3. **[2]** En déduire que D_n possède exactement $2n$ éléments, et que ce sont exactement les éléments listés en 2. Montrer alors que $D_n = \langle r, s\rangle$.

1 pour le premier point, 1 pour le groupe engendré

4. **[2]** Montrer que $srs^{-1} = r^{-1}$. Le sous-groupe $\langle r\rangle$ est-il distingué dans D_n ?

1+1

5. **[2]** Montrer que D_n possède exactement $n+2$ éléments d'ordre **au plus** 2 si n est pair, et $n+1$ éléments d'ordre **au plus** 2 si n est impair.

B. [19.5 pts] Le but de cette partie est de déterminer tous les groupes d'ordre 15 et 30 à isomorphisme près. On suppose connus les résultats de la partie A, que l'on pourra utiliser en y faisant référence explicitement.

1. **[3]** Montrer que tout groupe d'ordre 15 est cyclique.

1 point pour $N_3 = N_5 = 1$, 1 pour produit direct interne, 1 pour l'iso avec $\mathbb{Z}/15\mathbb{Z}$

2. [**4**] Calculer le nombre d'éléments d'ordre au plus 2 des groupes

$$\mathbb{Z}/30\mathbb{Z}, D_{15}, \mathbb{Z}/5\mathbb{Z} \times D_3 \text{ et } \mathbb{Z}/3\mathbb{Z} \times D_5,$$

et en déduire que ces groupes sont deux à deux non isomorphes.

Nb d'éléments : 1+0.5+1+1, 0.5 pour la non-isomorphie

Dans toute la suite, on suppose que G est un groupe d'ordre 30.

3. Soit $p = 2, 3$ ou 5. On note N_p le nombre de p-Sylow de G.

(a) [**1**] Calculer les valeurs possibles de N_3 et N_5.

(b) [**0.5**]Justifier qu'un p-Sylow de G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

(c) [**1**] Montrer que deux p-Sylow de G distincts s'intersectent trivialement.

(d) [**1**] En déduire que G possède $N_p(p-1)$ éléments d'ordre p.

4. [**1**] En utilisant la question précédente, montrer par l'absurde que $N_3 = 1$ ou $N_5 = 1$.

5. [**2**] Pour $p = 2, 3, 5$, on note H_p un p-Sylow de G. Justifier qu'au moins un des deux sous-groupes H_3 et H_5 est distingué dans G. En déduire que $H = \langle H_3, H_5 \rangle$ est un sous-groupe cyclique d'ordre 15.

0.5 pour H_3 ou H_5 distingué, 1.5 pour H cyclique d'ordre 15

6. [**2**] Montrer que $G = H \rtimes H_2 \simeq H \times_\rho H_2$, où $\rho : H_2 \longrightarrow \mathrm{Aut}(H)$ est un morphisme de groupes.

1.5 pour le produit semi-direct, 0.5 pour l'iso

7. On rappelle que si C est un groupe cyclique d'ordre n, alors $\mathrm{Aut}(C) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

(a) [**1.5**] Combien de solutions l'équation $\overline{x}^2 = \overline{1}$ possède-t-elle dans $(\mathbb{Z}/15\mathbb{Z})^\times$?

(b) [**1.5**] En déduire qu'il y a au plus quatre groupes d'ordre 30 à isomorphisme près.

Indication. Si $\rho : H_2 \longrightarrow \mathrm{Aut}(H)$ est un morphisme de groupes, et si h est l'unique élément non trivial de H_2, que vaut $\rho(h)^2$?

0.5 pour l'indication et 1 pour (b)

8. [**1**] Donner la liste de tous les groupes d'ordre 30, à isomorphisme près.

Exercice. [19.5 pts] Soit A un sous-anneau de $\mathbb{C}$. On pose

$$K_A = \left\{ \frac{a_1}{a_2} \mid a_1 \in A, a_2 \in A \setminus \{0\} \right\}.$$

On admet que c'est un sous-corps de $\mathbb{C}$.

1. On suppose dans cette question que A est un anneau principal.

(a) [**1**] Justifier que tout élément $z \in K_A$ s'écrit $z = \dfrac{z_1}{z_2}$ avec $z_1 \in A, z_2 \in A \setminus \{0\}$, et z_1 et z_2 sont premiers entre eux.

(b) **[2]** Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$. Soient $z_1 \in A, z_2 \in A \setminus \{0\}$, où z_1 et z_2 sont premiers entre eux. Si $P\left(\frac{z_1}{z_2}\right) = 0$, montrer que alors $z_2 \mid a_n$. En déduire que si $z \in K_A$ est racine d'un polynôme $P \in A[X]$ **unitaire**, alors $z \in A$.

Dans la suite, on pose $A = \{a + 2bi \mid a, b \in \mathbb{Z}\}$. On admet que c'est un sous-anneau de $\mathbb{C}$. On rappelle à toutes fins utiles les équivalences

$$z \in \mathbb{Z}[i]^\times \iff |z|^2 = 1 \iff z \in \{\pm 1, \pm i\}.$$

2.

(a) **[1]** Montrer que $K_A = \mathbb{Q}[i] = \{u + vi \mid u, v \in \mathbb{Q}\}$.

(b) **[2]** En déduire que A n'est pas principal.

(c) **[1]** Soit (B, δ) un anneau euclidien. Un sous-anneau de B est-il euclidien par rapport à la restriction de δ à ce sous-anneau ? par rapport à une autre fonction ?

3.

(a) **[4]** Déterminer $A^\times$. Montrer que l'équation $|z|^2 = 2, z \in A$ n'a pas de solutions. En déduire que les éléments 2 et $2i$ sont irréductibles dans A. Sont-ils irréductibles dans $\mathbb{Z}[i]$? Sont-ils associés dans $\mathbb{Z}[i]$? dans A ?

1 pour $A^\times$, 0.5 pour l'indication, 0.5 pour l'irréductibilité dans A, 1 pour la réductibilité dans $\mathbb{Z}[i]$, 0.5 pour l'association dans $\mathbb{Z}[i]$, 0.5 pour la non-association dans A

(b) **[1]** En déduire un élément admettant deux décompositions en irréductibles, et retrouver le fait que A n'est pas principal.

(c) **[1]** En utilisant la définition, dire si oui ou non l'idéal $2iA$ est premier.

(d) **[2]** Calculer la caractéristique de l'anneau $A/2iA$, et en déduire une nouvelle démonstration du résultat trouvé en (c).

1 pour la caractéristique, 1 pour le second point

(e) **[1.5]** Montrer que l'idéal $I = (2, 2i)$ n'est pas un idéal principal de A.

4. **[3]** En utilisant le morphisme d'évaluation en $2i$, montrer que l'on un isomorphisme d'anneaux $A \simeq \mathbb{Z}[X]/(X^2 + 4)$. L'idéal de $\mathbb{Z}[X]$ engendré par $X^2 + 4$ est-il premier ? maximal ?

1 pour le noyau, 0.5 pour l'image, 0.5 thm d'iso, 0.5 idéal premier, 0.5 non maximal