Algèbre 2, L3
Examen du 10/01/2023 à 9h
Documents/calculatrices interdits
Durée : 3h

Exercice 1. Cet exercice porte sur le groupe des permutations $\mathfrak{S}_n$ et le groupe alterné $\mathcal{A}_n$.

1. On rappelle que, pour un groupe général G, son centre est défini par
$$Z(G) = \{g \in G \,|\, \forall h \in G, gh = hg\}.$$
Montrer que $Z(G)$ est un sous-groupe distingué de G.
2. Soit $n \geq 3$ et $\sigma \in \mathfrak{S}_n$ telle que $\sigma \neq Id$. Montrer qu'il existe trois éléments distincts $x, y, z \in \{1, \ldots, n\}$ tels que $y = \sigma(x)$. (On pourra commencer par choisir x puis y et z)
3. On considère la transposition (y, z), et les permutations $\varphi_1 = (y, z) \circ \sigma$ et $\varphi_2 = \sigma \circ (y, z)$. Calculer $\varphi_1(x)$ et $\varphi_2(x)$.
4. Montrer que le centre de $\mathfrak{S}_n$ est trivial : $Z(\mathfrak{S}_n) = \{Id\}$.
5. Rappeler comment est défini le sous-groupe alterné $\mathcal{A}_n \subset \mathfrak{S}_n$.
6. On considère le groupe $\{-1, 1\}$ (la structure de groupe est donnée par la multiplication). Quels sont les ordres des groupes $\mathfrak{S}_n$ et $\mathcal{A}_n \times \{-1, 1\}$?
7. Montrer que les groupes $\mathfrak{S}_n$ et $\mathcal{A}_n \times \{-1, 1\}$ ne sont pas isomorphes.

Exercice 2. Soit p un nombre premier. Dans cet exercice, on montre que le groupe des éléments inversibles de l'anneau $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$:
$$(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \tag{1}$$

1. On rappelle que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Déterminer l'ensemble $(\mathbb{Z}/p\mathbb{Z})^\times$ et montrer qu'il est de cardinal $p-1$.
2. Montrer que le produit de deux éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ est encore dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et que ce produit munit $(\mathbb{Z}/p\mathbb{Z})^\times$ d'une structure de groupe dont on précisera l'unité.
3. Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est abélien et fini d'ordre $p-1$.
4. Rappeler la définition du type d'un groupe abélien fini. On note $(q_1, \ldots, q_k)$ le type de $(\mathbb{Z}/p\mathbb{Z})^\times$, et on rappelle que q_k est le plus grand des entiers q_i
5. Montrer que tout élément x de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifie $x^{q_k} = 1$.
6. Montrer qu'il y a au plus q_k éléments x de $(\mathbb{Z}/p\mathbb{Z})^\times$ tels que $x^{q_k} = 1$. (On pourra considérer le polynôme $X^{q_k} - \bar{1}$ de $(\mathbb{Z}/p\mathbb{Z})[X]$)
7. Montrer que si $k > 1$, alors $q_k < p-1$.
8. Montrer que $k = 1$ et en déduire (1).

Exercice 3. On donne un exemple d'anneau non factoriel.

1. Rappeler la définition d'un élément irréductible dans un anneau et d'un anneau factoriel.
2. On considère l'ensemble des nombres complexes z de la forme $z = a + bi\sqrt{5}$ avec $a, b \in \mathbb{Z}$. On le note $\mathbb{Z}[i\sqrt{5}]$. Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de l'anneau $(\mathbb{C}, +, \times)$.
3. Pour $z \in \mathbb{Z}[i\sqrt{5}]$, on note $\overline{z}$ le conjugué complexe de z et on note $N(z) = z\overline{z}$. Déterminer $N(a + bi\sqrt{5})$ en fonction de a et b.
4. Montrer que $\forall x, y \in \mathbb{Z}[i\sqrt{5}]$, on a $N(xy) = N(x)N(y)$.
5. Soit $x \in \mathbb{Z}[i\sqrt{5}]$. Montrer que x est inversible dans $\mathbb{Z}[i\sqrt{5}]$ si et seulement si $N(x) = 1$. En déduire que $\mathbb{Z}[i\sqrt{5}]^\times = \{-1, 1\}$. Montrer que si x n'est pas inversible, et non nul, alors $N(x) \geq 4$.
6. Montrer que $3, 2 + i\sqrt{5}$ et $2 - i\sqrt{5}$ sont irréductibles. (On pourra calculer $N(3), N(2 + i\sqrt{5})$ et $N(2 - i\sqrt{5})$ et utiliser la question précédente)
7. Calculer 3×3 et $(2 + i\sqrt{5}) \times (2 - i\sqrt{5})$ et montrer que $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Exercice 4. On considère l'anneau $A = \mathbb{Z}/10\mathbb{Z}$ et on se place dans l'anneau $B = A[X] = (\mathbb{Z}/10\mathbb{Z})[X]$.

1. Enoncer le théorème concernant la division euclidienne dans des anneaux de polynômes tels que l'anneau B.
2. Soit $P = X^4 + X^3 + \bar{6}X^2 + \bar{8}X + \bar{4} \in B$, et soit $D = X^2 + X + \bar{8} \in B$. Exécuter la division euclidienne de P par D, après avoir justifié qu'on pouvait la faire. On note Q le quotient et R le reste.
3. Déterminer les racines des polynômes D et Q.
4. Ecrire P comme produit d'éléments irréductibles de l'anneau B.