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 $x, y, z \in \{1, \dots, n\}$ 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.

Solution :

1. cf cours
2. Puisque $\sigma \neq Id$, soit $x \in \{1 \dots, n\}$ tel que $\sigma(x) \neq x$. On pose $y = \sigma(x)$. Puisque $n \geq 3$, il existe un élément de $\{1 \dots, n\}$ qui n'est ni x ni y : on appelle z un tel élément.
3. On a $\varphi_1(x) = (y, z)(y) = z$ et $\varphi_2(x) = \sigma(x) = y$.
4. On a toujours $Id \in Z(\mathfrak{S}_n)$. De plus, si $\sigma \neq Id$, la question précédente fournit une transposition (y, z) qui ne commute pas à σ : ainsi $\sigma \notin Z(\mathfrak{S}_n)$.
5. Le groupe alterné est l'ensemble des éléments de signature 1.
6. En général, pour un morphisme de groupes finis $f : G \to H$, on a vu que $|G| = |\ker f| \times |f(G)|$. En appliquant cette formule au morphisme surjectif $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ (ε désigne la signature), on obtient $n! = |\mathcal{A}_n| \times 2$, soit $|\mathcal{A}_n| = \frac{n!}{2}$. Ainsi, $\mathfrak{S}_n$ et $\mathcal{A}_n \times \{-1, 1\}$ sont tous les deux d'ordre $n!$.
7. Pour autant, ils ne sont pas isomorphes. En effet, $Z(\mathcal{A}_n \times \{-1, 1\}) \supset \{Id\} \times \{-1, 1\}$, et le centre de $\mathcal{A}_n \times \{-1, 1\}$ est donc au moins d'ordre 2, alors que celui de $\mathfrak{S}_n$ est trivial, comme on l'a vu.

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 $(q_1, \dots, q_k)$ 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).

Solution :

1. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, par définition cela signifie que tout élément non nul est inversible. Ainsi, $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Il est de cardinal $p - 1$.
2. Si $x, y \neq 0$, alors $xy \neq 0$ puisque un corps est intègre. Puisque la loi $\times$ est associative sur $\mathbb{Z}/p\mathbb{Z}$, sa restriction à $(\mathbb{Z}/p\mathbb{Z})^\times$ l'est aussi. 1 est l'élément neutre, et tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ est inversible par définition de $(\mathbb{Z}/p\mathbb{Z})^\times$. Ainsi, $(\mathbb{Z}/p\mathbb{Z})^\times$ est bien un groupe.
3. On a $xy = yx$ pour deux éléments quelconques de $\mathbb{Z}/p\mathbb{Z}$, donc en particulier pour deux éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$. On a déjà vu que $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p - 1$.

4. Le type d'un groupe abélien G est l'unique suite finie d'entiers $(q_1, \dots, q_k)$ telle que d'une part $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$ et d'autre part $2 \leq q_1|q_2|\cdots|q_k$.
5. Notons $\varphi : G \to \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$ un isomorphisme. Soit $x \in G$. On note $\varphi(x) = (x_1, \dots, x_k)$ avec $x_i \in \mathbb{Z}/q_i\mathbb{Z}$. On a $q_i x_i = 0$ dans $\mathbb{Z}/q_i\mathbb{Z}$, et donc puisqu'on peut écrire $q_k = dq_i$ (q_i divise q_k), $q_k x_i = dq_i x_i = d0 = 0$. On a donc $q_k(x_1, \dots, x_k) = (q_k x_1, \dots, q_k x_k) = (0, \dots, 0)$, d'où $q_k\varphi(x) = \varphi(x^{q_k}) = 0$ (nous utilisons une notation additive pour $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$ et multiplicative pour G). En appliquant φ^{-1} à cette égalité, on trouve $x^{q_k} = \varphi^{-1}(0) = 1$.
6. Un polynôme de degré d à coefficients dans un corps ne peut avoir qu'au plus d racines distinctes. Ainsi, le polynômes $X^{q_k} - 1$ ne peut avoir que q_k racines au plus, c'est-à-dire q_k éléments x tels que $x^{q_k} = 1$.
7. Si $k > 1$, alors puisque $q_1 \times \cdots \times q_k = p - 1$, on a $q_k \leq \frac{p-1}{q_1} < p - 1$.
8. Comme tous les éléments x de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifient $x^{q_k} = 1$, il y a $p - 1$ tels éléments. Si $k > 1$, on trouve une contradiction avec la question précédente. Ainsi, $k = 1$, donc $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

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.

Solution :

1. cf cours.
2. On vérifie que $\mathbb{Z}[i\sqrt{5}]$ est un sous-groupe de $(\mathbb{C}, +)$ et que le produit de deux éléments de $\mathbb{Z}[i\sqrt{5}]$ est encore dans $\mathbb{Z}[i\sqrt{5}]$.
3. On a $N(a + bi\sqrt{5}) = a^2 + 5b^2$.
4. Cette relation est vraie dans $\mathbb{C}$, elle est donc vraie en particulier si $x, y \in \mathbb{Z}[i\sqrt{5}]$. Autre argument possible : $N(xy) = (xy)\overline{(xy)} = xy\overline{x}\,\overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$.
5. Soit x inversible. Soit donc $y \in \mathbb{Z}[i\sqrt{5}]$ tel que $xy = 1$. On trouve $1 = N(1) = N(xy) = N(x)N(y)$, et puisque $N(x)$ et $N(y)$ sont des entiers naturels, $N(x) = N(y) = 1$. Si on écrit $x = a + bi\sqrt{5}$, on en déduit $a^2 + 5b^2 = 1$, donc $a = \pm 1$ et $b = 0$. Inversement, 1 et -1 sont bien sûr inversibles.

   Si $x = a + bi\sqrt{5}$ n'est pas inversible, on a $b \neq 0$ (et donc $N(x) \geq 5b^2 \geq 5$) ou $b = 0$ et $|a| > 1$ (et donc $N(x) \geq 2^2 = 4$). Dans tous les cas, $N(x) \geq 4$.
6. Ecrivons $3 = xy$ et montrons que x ou y est inversible. On a $9 = N(3) = N(x)N(y)$. Si x et y sont tous les deux non inversibles, alors $N(x), N(y) \geq 4$, ce qui est contradictoire. Le même argument vaut pour $2 + i\sqrt{5}$ et $2 - i\sqrt{5}$, puisque $N(2 + i\sqrt{5}) = N(2 - i\sqrt{5}) = 9$.
7. $3 \times 3 = 9 = (2 + i\sqrt{5})(2 - i\sqrt{5})$. Ainsi, 9 admet ces deux décompositions en produits d'irréductibles. Si $\mathbb{Z}[i\sqrt{5}]$ était factoriel, ces irréductibles devraient être associés : plus précisément 3 devrait être associé à $2 + i\sqrt{5}$ ou $2 - i\sqrt{5}$. Mais puisque $\mathbb{Z}[i\sqrt{5}]^\times = \{-1, 1\}$, ceci donne $3 = \pm(2 + i\sqrt{5})$ ou $3 = \pm(2 - i\sqrt{5})$, ce qui est clairement faux. L'unicité de l'écriture en produit d'irréductibles est donc mise en défaut, et $\mathbb{Z}[i\sqrt{5}]$ 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.

Solution :

1. cf cours
2. On peut faire cette division euclidienne parce que le coefficient dominant du diviseur D est $\bar{1}$, donc inversible. On trouve $Q = X^2 + \bar{8}$ et $R = 0$.
3. Les racines de D sont $\{\bar{1}, \bar{3}, \bar{6}, \bar{8}\}$ (on les trouve en essayant tous les éléments de $\mathbb{Z}/10\mathbb{Z}$). On observe qu'il y en a plus que 2, le degré de D, ce qui n'est pas contradictoire car D est un polynôme à coefficients dans $\mathbb{Z}/10\mathbb{Z}$ qui n'est pas un corps. Le polynôme Q, lui, n'a pas de racines.
4. On peut factoriser D par tout polynôme $X - \alpha$ si α est une racine. En factorisant par $X - \bar{1}$, par exemple, on trouve $D(X) = (X - \bar{1})(X - \bar{8})$. On pouvait aussi factoriser par $X - \bar{3}$ et trouver $D(X) = (X - \bar{3})(X - \bar{6})$. Cependant, un gag est ici que ces polynômes de degré 1 ne sont pas irréductibles !

   La décomposition de $X - \bar{1}$ en produit d'irréductibles est $X - \bar{1} = (\bar{5}X + \bar{1})(\bar{6}X + \bar{9})$ et celle de $X - \bar{8}$ est $X - \bar{8} = (\bar{5}X + \bar{6})(\bar{6}X + \bar{7})$. En effet, ces décompositions peuvent s'obtenir en utilisant l'isomorphisme $(\mathbb{Z}/10\mathbb{Z})[X] \simeq (\mathbb{Z}/2\mathbb{Z})[X] \times (\mathbb{Z}/5\mathbb{Z})[X]$: via cet isomorphisme elles s'expriment $(X + \bar{1}, X + \bar{4}) = (X + \bar{1}, \bar{1}) \cdot (\bar{1}, X + \bar{4})$ et $(X, X + \bar{2}) = (X, \bar{1}) \cdot (\bar{1}, X + \bar{2})$ respectivement.

   De manière similaire, le polynôme $Q(X) = X^2 + \bar{8}$, bien que n'ayant pas de racines dans $\mathbb{Z}/10\mathbb{Z}$, est réductible. Il s'écrit $Q(X) = (\bar{5}X + \bar{6})^2 \cdot (\bar{6}X^2 + \bar{3})$. Via l'isomorphisme ci-dessus, cette décomposition s'écrit en effet $(X^2, X^2 + \bar{3}) = (X, \bar{1})^2 \cdot (\bar{1}, X^2 + \bar{3})$.

   Une décomposition en produit de facteurs irréductibles de P est alors

$$P(X) = (\bar{5}X + \bar{1})(\bar{6}X + \bar{9})(\bar{6}X + \bar{7})(\bar{5}X + \bar{6})^3(\bar{6}X^2 + \bar{3})$$