Algèbre 2, L3
Partiel du 10/11/2025 à 9h
Documents/calculatrices interdits
Durée : 2h

Ce sujet est trop long pour être traité en deux heures mais vous permet de choisir les exercices sur lesquels vous êtes le plus à l'aise.

Questions de cours

1. Soit p un nombre premier et G un groupe d'ordre p. Montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
2. Soit G un groupe et $X \subset G$ un sous-ensemble. Soit H une partie de G. Ecrire avec des quantificateurs l'assertion "H est le sous-groupe de G engendré par X".
3. Décrire les sous-groupes d'un groupe cyclique d'ordre n.
4. Soit G un groupe, $a \in G$, et supposons que $|\langle a \rangle| = n$. A quel groupe $\langle a \rangle$ est-il isomorphe et quel est l'ensemble $\{k \,|\, a^k = e\}$?

Exercices standard

1. Soit G un groupe d'ordre 33 agissant sur un ensemble E de cardinal 17. Combien y a-t-il d'orbites pour cette action ?
2. Donner la décomposition cyclique du groupe $\mathbb{Z}/40\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z}$.
3. Donner la liste des groupes abéliens d'ordre 160, à isomorphisme près.

Problème : groupes d'ordre p^3 non abéliens

Soit p un nombre premier. On considère l'ensemble G des matrices triangulaires supérieures unitaires de taille 3×3 à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$:

$$G = UT_3(\mathbb{F}_p) = \left\{ M(a,b,c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{F}_p \right\}$$

On munit G de la multiplication matricielle. Ce groupe est souvent appelé le *groupe de Heisenberg* modulo p.

Partie I : Cas Général (p premier impair)

1. Montrer que G est un groupe et déterminer son ordre $|G|$.
2. Etant donnés a, b, c, a', b', c', déterminer a'', b'', c'' tels que $M(a,b,c)M(a',b',c') = M(a'',b'',c'')$.
3. Calculer le commutateur $[M(a,b,c), M(a',b',c')] = M(a,b,c)M(a',b',c') - M(a',b',c')M(a,b,c)$.
4. Déduire de la question précédente que G est un groupe non abélien.
5. Déterminer le centre $Z(G)$ du groupe G. Montrer que $Z(G)$ est un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
6. Montrer que le groupe quotient $G/Z(G)$ est un groupe abélien isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Partie II : Cas Spécifique $p = 2$ (Isomorphisme avec D_8)

Dans cette partie, on considère le cas $p = 2$. Le groupe G est alors d'ordre 8. On cherche à démontrer l'isomorphisme $G \cong D_8$, où D_8 est le groupe diédral d'ordre 8.

On définit les matrices suivantes :

$$S = M(1,0,0) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad R = M(1,1,1) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

7. Montrer que S est d'ordre 2.
8. Montrer que R est d'ordre 4.
9. Déterminer l'inverse de R, noté R^{-1}.
10. Montrer que la relation fondamentale du groupe diédral est vérifiée, à savoir :

$$SRS = R^{-1}$$

11. Conclure sur la nature du groupe $G = UT_3(\mathbb{F}_2)$.

Solution : Le groupe est défini par :

$$G = UT_3(\mathbb{F}_p) = \left\{ M(a,b,c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{F}_p \right\}$$

---

1 Partie I : Cas Général (p premier)

1. **Ordre et structure de groupe :**
   - **Ordre :** Puisque les trois coefficients a, b, c sont libres et prennent chacun p valeurs distinctes dans $\mathbb{F}_p$, l'ordre du groupe est $|G| = p \times p \times p = \mathbf{p^3}$.
   - **Structure de groupe :** G est un sous-ensemble des matrices $GL_3(\mathbb{F}_p)$.
     - **Loi interne :** Démontrée à la question suivante, le produit de deux matrices de G est dans G.
     - **Élément neutre :** La matrice identité $I = M(0,0,0)$ appartient à G.
     - **Inverse :** L'inverse de $M(a,b,c)$ est $M(-a,-b,ab-c)$, qui appartient bien à G.
     - **Associativité :** Héritée de la multiplication matricielle.

   G est donc un groupe.
2. **Produit de deux matrices :**

$$\begin{aligned} M(a,b,c)M(a',b',c') &= \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+a' & c+c'+ab' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix} \\ &= M(a+a', b+b', c+c'+ab') \end{aligned}$$

   La loi interne est bien définie et est une matrice de G.
3. **Calcul du commutateur :** Nous cherchons $[M, M'] = MM'(M'M)^{-1}$. Le produit dans l'ordre inverse est $M'M = M(a'+a, b'+b, c'+c+a'b)$. Le commutateur est donné par :

$$[M(a,b,c), M(a',b',c')] = M(0,0,ab'-a'b)$$

4. **Non-abélianité :** Le groupe G est non-abélien si et seulement si il existe des matrices M et M' telles que le commutateur $[M, M'] \neq I = M(0,0,0)$. Ceci est équivalent à l'existence de a, b, a', b' tels que $ab' - a'b \neq 0 \pmod{p}$.
   Prenons $M_A = M(1,0,0)$ et $M_B = M(0,1,0)$.
$$[M_A, M_B] = M(0,0,(1)(1) - (0)(0)) = M(0,0,1)$$
   Puisque $\mathbf{1 \neq 0}$ dans $\mathbb{F}_p$ pour tout premier p, nous avons $[M_A, M_B] \neq I$. Le groupe G est donc **non-abélien pour tout** $p \geq 2$.
5. **Centre du groupe** $Z(G)$ **:** $M(a,b,c) \in Z(G) \iff [M(a,b,c), M(a',b',c')] = I$ pour tout a', b', c'. Ceci impose que $ab' - a'b = 0$ pour tout $a', b' \in \mathbb{F}_p$.
   En choisissant $(a', b') = (1,0)$, on obtient $a(0) - (1)b = -b = 0$, donc $b = 0$. En choisissant $(a', b') = (0,1)$, on obtient $a(1) - (0)b = a = 0$.
   Le centre $Z(G)$ est donc l'ensemble des matrices de la forme $M(0,0,c)$, avec $c \in \mathbb{F}_p$.
$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbb{F}_p \right\}$$
   L'application $\phi : c \mapsto M(0,0,c)$ est un isomorphisme de $(\mathbb{F}_p, +)$ vers $Z(G)$. Ainsi, $Z(G) \cong \mathbb{Z}/\mathbf{p}\mathbb{Z}$.
6. **Groupe quotient** $G/Z(G)$ **:** Le quotient $G/Z(G)$ est le groupe des classes d'équivalence de la forme $M(a,b,c)Z(G)$.
   Deux matrices M et M' sont dans la même classe si $M'M^{-1} \in Z(G)$. Ceci se produit si elles ont les mêmes coefficients a et b.
   L'application $\psi : G \to \mathbb{F}_p \times \mathbb{F}_p$ définie par $\psi(M(a,b,c)) = (a,b)$ est un homomorphisme surjectif dont le noyau est $\mathrm{Ker}(\psi) = \{M(0,0,c)\} = Z(G)$.
   Par le Premier Théorème d'Isomorphisme, on a :
$$G/Z(G) \cong \mathrm{Im}(\psi) = \mathbb{F}_p \times \mathbb{F}_p \cong \mathbb{Z}/\mathbf{p}\mathbb{Z} \times \mathbb{Z}/\mathbf{p}\mathbb{Z}$$

---

2 Partie II : Cas Spécifique $p = 2$ (Isomorphisme avec D_8)

Nous avons $|G| = 8$. Le groupe diédral D_8 est défini par $\langle r, s \mid r^4 = I, s^2 = I, srs = r^{-1} \rangle$. Les matrices sont sur $\mathbb{F}_2 = \{0,1\}$.
$$S = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

7. **Ordre de** S **:**
$$S^2 = M(1+1, 0+0, 0) = M(0,0,0) = I \pmod{2}$$
   L'élément S est d'ordre 2 (il joue le rôle de la réflexion s).
8. **Ordre de** R **:**
$$R^2 = M(1+1, 1+1, 1+1+1) = M(0,0,1)$$
$$R^4 = R^2R^2 = M(0+0, 0+0, 1+1+0) = M(0,0,0) = I \pmod{2}$$
   Puisque $R^2 \neq I$, l'élément R est d'ordre 4 (il joue le rôle de la rotation r).
9. **Inverse de** R **:** L'inverse de $M(a,b,c)$ est $M(-a,-b,ab-c)$. Puisque $p = 2$, $-x = x \pmod{2}$.
$$R^{-1} = M(1,1,1-1) = M(1,1,0) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

10. **Vérification de $SRS = R^{-1}$:** Calculons SR :

$$SR = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Calculons SRS :

$$SRS = (SR)S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Le résultat SRS est bien égal à R^{-1} (calculé en Q9).

$$\mathbf{SRS = R^{-1}}$$

11. **Conclusion :** Le groupe $G = UT_3(\mathbb{F}_2)$ est engendré par R (ordre 4) et S (ordre 2) et satisfait les relations :

$$G \cong \langle R, S \mid R^4 = I, S^2 = I, SRS = R^{-1} \rangle$$

Ceci est la présentation standard du groupe diédral D_8. Nous concluons que :

$$\mathbf{UT_3(\mathbb{Z}/2\mathbb{Z}) \cong D_8}$$

Problème : dénombrement des coloriages d'un carré

Cet exercice utilise la théorie des actions de groupes pour déterminer le nombre de façons distinctes de colorier les sommets d'un carré. Les questions sont volontairement moins détaillées que dans les exercices précédents.

On considère un carré $ABCD$. On dispose de k couleurs distinctes ($k \geq 1$). Un *coloriage* (des sommets du carré) est une application $\{A, B, C, D\} \to \{1, \ldots, k\}$. On note $\mathcal{C}$ l'ensemble des coloriages. Deux coloriages sont considérés comme *équivalents* s'ils peuvent être transformés l'un en l'autre par une symétrie (rotation ou réflexion) du carré. On rappelle que le groupe de symétrie est le groupe diédral $G = D_8$.

1. Lister les 8 éléments de G en les classant par type de symétrie (identité, rotations, réflexions).
2. Déterminer le cardinal de $\mathcal{C}$.
3. Rappeler la formule de Burnside.
4. Déterminer le nombre de classes d'équivalences de coloriages, en fonction de k.
5. On suppose dans cette question que $k = 2$. Appliquer la formule précédente pour déterminer le nombre de classes d'équivalence de coloriages, et vérifier directement le résultat, en déterminant le nombre de coloriages en noir et blanc des sommets d'un carré, à isométries près.

Solution :

1. **Groupe d'Action :** L'ordre du groupe $G = D_8$ est $|\mathbf{G}| = \mathbf{8}$. Ses éléments sont :
   - 1 Identité (e).
   - 3 Rotations : ρ (rotation $\pi/2$), ρ^2 (rotation π), ρ^3 (rotation $3\pi/2$).
   - 4 Réflexions : 2 réflexions par rapport aux médiatrices des côtés (σ_m) et 2 réflexions par rapport aux diagonales (σ_d).
2. **Ensemble Coloré :** Chaque sommet peut recevoir k couleurs. L'ensemble total des coloriages sans symétrie est $|X| = \mathbf{k^4}$.
3. **Action et Stabilisateur :**
   - L'**action** de G sur X est le transport des sommets.
   - Le coloriage c est fixé par $g \in G$ (i.e., $c \in X^g$) si et seulement si tous les sommets appartenant à la même **orbite** (cycle) sous l'action du sous-groupe $\langle g \rangle$ ont la même couleur.
4. **Application du Théorème de Burnside :** Soit $c(g)$ le nombre de cycles de la permutation des sommets associée à g. On a $|X^g| = k^{c(g)}$.

(a) **Détermination de $|X^g|$ par type d'élément :**

- **Identité (e)** : 1 élément. Description : 4 sommets fixes. $c(e) = 4$. Contribution : $1 \cdot k^4$.
- **Rotations $\pi/2$ et $3\pi/2$** (ρ, ρ^3) : 2 éléments. Description : 1 cycle de longueur 4. $c(\rho) = 1$. Contribution : $2 \cdot k^1$.
- **Rotation π** (ρ^2) : 1 élément. Description : 2 cycles de longueur 2. $c(\rho^2) = 2$. Contribution : $1 \cdot k^2$.
- **Réflexions axes médians** (2 éléments) : Description : Échange des paires de sommets (2 cycles de longueur 2). $c = 2$. Contribution : $2 \cdot k^2$.
- **Réflexions diagonales** (2 éléments) : Description : Fixe 2 sommets et échange les 2 autres (2 cycles de longueur 1 et 1 cycle de longueur 2). $c = 3$. Contribution : $2 \cdot k^3$.

(b) **Formule générale pour le nombre N :** On somme toutes les contributions et on divise par $|G| = 8$:

$$N = \frac{1}{8}\left[(1 \cdot k^4) + (2 \cdot k) + (1 \cdot k^2) + (2 \cdot k^2) + (2 \cdot k^3)\right]$$

En regroupant les termes :

$$\mathbf{N = \frac{1}{8}\left(k^4 + 2k^3 + 3k^2 + 2k\right)}$$

(c) **Applications Numériques :**

- **Cas $k = 2$ (Noir et Blanc) :**

$$N = \frac{1}{8}\left(2^4 + 2(2^3) + 3(2^2) + 2(2)\right)$$

$$N = \frac{1}{8}\left(16 + 16 + 12 + 4\right) = \frac{48}{8} = \mathbf{6}$$

Il existe **6** coloriages distincts pour le carré avec 2 couleurs. On peut vérifier ce nombre directement : il y a 1 coloriage avec tous les sommets blancs, 1 avec tous les sommets noirs, 1 (à isométries près) avec exactement un sommet blanc, 1 avec exactement un sommet noir, et deux coloriages (à isométries près) avec deux sommets blancs et deux sommets noirs : les deux sommets blancs (et noirs) sont soit sur un côté, soit sur une diagonale.

- **Cas $k = 3$:**

$$N = \frac{1}{8}\left(3^4 + 2(3^3) + 3(3^2) + 2(3)\right)$$

$$N = \frac{1}{8}\left(81 + 54 + 27 + 6\right) = \frac{168}{8} = \mathbf{21}$$

Il existe **21** coloriages distincts pour le carré avec 3 couleurs.