Algèbre 2, L3
Examen du 16/01/2025 à 9h
Documents/calculatrices interdits
Durée : 3h

Ce sujet est volontairement trop long afin que vous puissiez choisir les exercices qui vont conviennent le mieux. Privilégiez la qualité de la rédaction ainsi que la précision et la concision des arguments par rapport au souhait de traiter une grande partie des exercices.

Exercice 1. (questions de cours)

1. Soit G un groupe. Soit X et H des sous-ensembles de G. Ecrire avec des quantificateurs l'affirmation "H est le sous-groupe engendré par X". Etant donné un groupe B, on notera $A \leq B$ pour dire que A est un sous-groupe de B.
2. Soit $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$ les groupes obtenus en passant au quotient la somme sur $\mathbb{Z}$ (on ne demande pas de donner des détails sur la construction de ces deux groupes). Donner deux morphismes de groupes $\mathbb{Z}/3Z \to \mathbb{Z}/6\mathbb{Z}$.
3. Soit G un groupe fini. On note $|G| = n = \prod_{i=1}^{r} p_i^{\alpha_i}$, où les nombres p_i sont premiers et les α_i sont strictement positifs. Pour les deux affirmations suivantes, dites si elle est vraie en citant un résultat du cours (sans le démontrer) ou en donnant un contre-exemple et en justifiant que c'est bien un contre-exemple.
   (a) Soit $i \in \{1, \dots, r\}$ et $1 \leq j \leq \alpha_i$. Dans G, il existe un sous-groupe d'ordre p_i^j.
   (b) Soit $i \in \{1, \dots, r\}$ et $1 \leq j \leq \alpha_i$. Dans G, il existe un élément d'ordre p_i^j.

Exercice 2. (groupes abéliens finis)

1. Donner la liste de tous les groupes abéliens d'ordre 400 à isomorphisme près.
2. Donner la décomposition cyclique du groupe $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$.

Exercice 3. (groupe symétrique, groupe alterné)

1. Donner la définition du groupe alterné $\mathcal{A}_n$.
2. Dans $\mathfrak{S}_8$, l'élément $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$ est-il dans $\mathcal{A}_8$? Si oui, l'écrire comme produit de 3-cycles.
3. Calculer σ_1^{2025}.
4. Dans $\mathfrak{S}_8$, l'élément $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 5 & 7 & 6 & 8 \end{pmatrix}$ est-il dans $\mathcal{A}_8$? Si oui, l'écrire comme produit de 3-cycles.

Solution :

1. Le groupe alterné $\mathcal{A}_n$ est le sous-groupe de $\mathfrak{S}_n$ comprenant les permutations paires, c'est-à-dire les permutations σ de signature 1 (telles que $\epsilon(\sigma) = 1$).
2. $\sigma_1 = (12345)(67)$ donc $\epsilon(\sigma_1) = (-1)^4(-1) = -1$, donc $\sigma_1 \notin \mathcal{A}_8$.
3. $\sigma_1^{2025} = (12345)^{2025}(67)^{2025} = (67)$.
4. $\sigma_2 = 1234)(67)$ donc $\epsilon(\sigma_2) = (-1)^3(-1) = 1$, donc $\sigma_2 \in \mathcal{A}_8$. De plus,

$$\sigma_2 = (1234)(67) = (12)(23)(34)(67) = (12)(23)(34)(46)(46)(67) = (123)(346)(467).$$

Exercice 4. (produit direct de groupes)

1. Soient G un groupe et H, K deux sous-groupes distingués de G. On suppose que $HK = G$ et $H \cap K = \{e\}$ et on montre que G est isomorphe au produit $H \times K$.
   (a) Soit $x \in H$ et $y \in K$. Montrer que $xyx^{-1}y^{-1} \in H \cap K$.
   (b) En déduire que pour tout $x \in H, y \in K$, on a $xy = yx$.
   (c) Montrer que l'application $\begin{array}{rccc} \mu & : & H \times K & \to & G \\ & & (x, y) & \mapsto & xy \end{array}$ est un morphisme de groupes.

(d) Montrer que μ est injective.

(e) Montrer que $G \simeq H \times K$.

2. Application : on suppose que G est un groupe d'ordre pq avec p et q premiers tels que $3 \leq p \leq 2q$ et $3 \leq q \leq 2p$. On montre que G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

(a) Montrer que $p \not\equiv 1\ [q]$ et que $q \not\equiv 1\ [p]$.

(b) Soit n_p le nombre de p-Sylow et n_q le nombre de q-Sylow. Montrer que $n_p = n_q = 1$. Soit S_p resp. S_q l'unique p-Sylow resp. q-Sylow.

(c) Montrer que $S_p \simeq \mathbb{Z}/p\mathbb{Z}$ et $S_q \simeq \mathbb{Z}/q\mathbb{Z}$.

(d) Montrer que $G \simeq \mathbb{Z}/(pq)\mathbb{Z}$.

3. On donne deux contre-exemples au résultat précédent lorsque les conditions sur p et q ne sont pas satisafaites.

(a) Donner un exemple de groupe d'ordre 6 non isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (contre-exemple au cas $p = 2, q = 3$).

(b) Pour $q \geq 5$ un nombre premier, donner un exemple de groupe d'ordre $2q$ non isomorphe à $\mathbb{Z}/2q\mathbb{Z}$ (contre-exemple au cas $p = 2, q \geq 5$).

Solution :

1. (a) Soit $x \in H$ et $y \in K$. Comme H est un sous-groupe distingué, $yx^{-1}y^{-1} \in H$. Donc $x(yx^{-1}y^{-1}) \in H$. De même, en utilisant que K est un sous-groupe distingué, $(xyx^{-1})y^{-1} \in K$.

(b) On a donc, grâce à l'hypothèse, $xyx^{-1}y^{-1} = e$, d'où on tire $xy = yx$.

(c) Soit $(x_1, y_,), (x_2, y_2) \in H \times K$. D'une part, $\mu((x_1, y_1)(x_2, y_2)) = \mu((x_1x_2, y_1y_2)) = x_1x_2y_1y_2$. D'autre part, $\mu(x_1, y_1)\mu(x_2, y_2) = x_1y_1x_2y_2$. Or on a montré $x_2y_1 = y_1x_2$. D'où $\mu((x_1, y_1)(x_2, y_2)) = \mu(x_1, y_1)\mu(x_2, y_2)$.

(d) Soit (x, y) dans le noyau du morphisme de groupes μ. On a $\mu(xy) = xy = e$, donc $x = y^{-1} \in H \cap K = \{e\}$, donc $x = y^{-1} = e$, donc $(x, y) = (e, e)$ est l'élément neutre de $H \times K$.

(e) φ est un morphisme injectif et surjectif par l'hypothèse $HK = G$, c'est donc un isomorphisme.

2. (a) Si p est congru à 1 modulo q, alors on peut écrire $p = kq + 1$. Comme de plus p et q sont tous les deux impairs, en réduisant cette égalité modulo 2 on voit que k est pair. Ainsi, $p > 2q$, contredisant l'hypothèse. Le raisonnement symétrique vaut pour montrer que $q \not\equiv 1\ [p]$.

(b) On a $n_p | q$ donc $n_p \in \{1, q\}$. De plus, $n_p \simeq 1\ [q]$ (ces deux affirmations résultent du troisième théorème de Sylow), donc $_p = 1$ d'après la questions précédente.

(c) Par définition, un p-Sylow dans G est d'ordre p. Le résultat pour S_p résulte du fait que tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et de même pour S_q.

(d) Comme $n_p = 1$, S_p est distingué (le conjugué d'un p-Sylow est un p-Sylow). De même S_q est distingué. On peut donc appliquer la question 1.

3. (a) On peut prendre le groupe $G = \mathfrak{S}_3$, de cardinal 6 et non commutatif, et les sous-groupes $H = \{e, (12)\}, K = \{e, (123)(132)\}$.

(b) Plus généralement, on peut prendre G un groupe diédral d'ordre $2q$, engendré par x d'ordre 2 et y d'ordre q, et choisir $H = \langle x \rangle, K = \langle y \rangle$.

Exercice 5. (action du groupe linéaire sur un corps fini)
Soit p un nombre premier et k le corps $\mathbb{Z}/p\mathbb{Z}$. On note $G = \mathrm{GL}_n(k)$ le groupe linéaire à coefficients dans k.

1. Rappeler la définition d'une action et montrer que G agit sur l'ensemble des vecteurs de k^n.
2. On détermine le cardinal de G.

(a) Montrer que G agit sur l'ensemble des bases de k^n.

(b) Montrer que cette action est simplement transitive : étant données deux bases $\mathcal{B}_1, \mathcal{B}_2$, il existe un unique $g \in G$ tel que $g \cdot \mathcal{B}_1 = \mathcal{B}_2$.

(c) Déterminer le nombre de bases de k^n.

(d) Montrer que le cardinal de G est

$$p^{n(n-1)/2}(p-1)^n(1+p)(1+p+p^2)\cdots(1+p+\cdots+p^{n-1})$$

3. On étudie l'action de G sur l'ensemble des sous-espaces vectoriels.

(a) Montrer que G agit sur l'ensemble des sous-espaces vectoriels de k^n de dimension r, qu'on note $F(r, n)$.

(b) Montrer que G agit transitivement sur $F(r,n)$.

(c) Soit $(e_1,\dots,e_n)$ la base canonique de k^n et soit F_r le sous-espace vectoriel de k^n engendré par $e_1,\dots,e_r$. Montrer que le stabilisateur de F_r est l'ensemble des matrices de la forme $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ avec $A \in \mathrm{GL}_r, D \in \mathrm{GL}_{n-r}$ et B une matrice quelconque de format $r \times (n-r)$. On note $P_r \leq G$ ce stabilisateur.

4. On calcule le nombre de sous-espaces vectoriels. Pour cela, on considère le cas particulier $r=2$ et $n=4$.

(a) Calculer le cardinal de G en fonction de p.

(b) Calculer le cardinal de P_2 en fonction de p.

(c) Calculer le cardinal de $F(2,4)$. On devra trouver un polynôme en p de degré 4.

Solution :

1. Cf le cours

2. (a) Tout d'abord, G agit sur k^n donc sur $(k^n)^n$. De plus, si $(e_1,\dots,e_n)$ est une base de k^n et si $g \in \mathrm{GL}_n(k)$, alors $(g\cdot e_1,\dots,g\cdot e_n)$ est une base de k^n. Ceci montre que l'action $(k^n)^n$ se restreint à une action sur l'ensemble des bases.

(b) On rappelle le résultat d'algèbre linéaire : étant donné une base $(x_1,\dots,x_n)$ d'un espace vectoriel E, étant donnés n vecteurs $y_1,\dots,y_n$ d'un autre espace vectoriel F, il existe une unique application linéaire $\varphi : E \to F$ telle que $\varphi(x_i) = y_i$ pour tout i. On montre la question en appliquant ce résultat à $E = F = k^n$, x_i et y_i les vecteurs composant les bases $\mathcal{B}_1$ et $\mathcal{B}_2$, ie tels que $\mathcal{B}_1 = (x_1,\dots,x_n)$ et $\mathcal{B}_2 = (y_1,\dots,y_n)$.

(c) Pour construire une base $(e_1,\dots,e_n)$, il faut choisir un premier vecteur e_1 non nul (p^n-1 choix possibles), puis un deuxième vecteur qui ne lui est pas colinéaire (p^n-p choix possibles), et ainsi de suite. Le nombre de bases est donc $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$. Comme $p^n-p^i = p^i(p^{n-i}-1) = p^i(p-1)(1+p+\cdots+p^{i-1})$, on trouve la formule de l'énoncé.

3. (a) On a vu que G agit sur k^n, il agit donc sur les parties de k^n (cf cours), et il est clair qu'il envoie un sous-espace vectoriel sur un sous-espace vectoriel de même dimension.

(b) C'est une conséquence du théorème de la base incomplète. Soit F_1, F_2 de sous-espaces vectoriels de k^n de dimension r. Soit $(e_1,\dots,e_r)$ resp. $(f_1,\dots,f_r)$ une base de F_1 resp. F_2. On complète ces familles libres en des bases $(e_1,\dots,e_n)$, $(f_1,\dots,f_n)$ de k^n. On prend l'élément $g \in G$ qui envoie e_i sur f_i (comme à la question 2b). Alors g envoie $\langle e_1,\dots,e_r\rangle$ sur $\langle f_1,\dots,f_r\rangle$. Il envoie donc F_1 sur F_2.

(c) Avec ce choix de base, un élément g du stabilisateur de F_r doit envoyer chaque e_i pour $i \leq r$ sur une combinaison linéaire des e_j avec $j \leq r$. Lorsqu'on écrit la matrice de g, on voit qu'elle est de la forme indiquée.

4. (a) $|G| = p^6(p-1)^4(1+p)(1+p+p^2)(1+p+p^2+p^3)$

(b) Le nombre d'éléments A est le nombre d'éléments de GL_2, soit $p(p-1)^2(1+p)$. Le nombre d'éléments D est aussi ce nombre. Le nombre d'éléments B est p^4. Le nombre d'éléments de P_2 est donc $p^2(p-1)^4p^4$.

(c) Le nombre d'éléments de $F(2,4)$ est donc

$$\begin{aligned} \frac{|G|}{|P_2|} &= \frac{p^6(p-1)^4(1+p)(1+p+p^2)(1+p+p^2+p^3)}{p^2(p-1)^4(1+p)^2p^4} \\ &= \frac{(1+p+p^2)(1+p+p^2+p^3)}{1+p} \\ &= (1+p+p^2)(1+p^2) = 1+p+2p^2+p^3+p^4 \end{aligned}$$