1
2
3

MAT35B - ALGÈBRE L3A
Premier Semestre — 2022-2023

Soutien d'Algèbre L3A

Justifier toutes les réponses

---

1. Soit G un groupe fini, soit $p \in \mathbb{N}^*$ le plus petit diviseur premier de $|G|$ et soit $H \subseteq G$ un sous-groupe distingué de G d'ordre p. Montrer que $H \subseteq \mathscr{Z}(G)$, où $\mathscr{Z}(G) = \{g \in G : gh = hg \text{ pour tout } h \in G\}$ designe le centre de G.
Indication : considérer l'action de G sur H par conjugaison.

2. Soit $p \in \mathbb{N}^*$ un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. Pour tout polynôme $P \in \mathbb{F}_p[X]$ non nul et unitaire, on pose

$$\varphi(P) = \#\Big(\big(\mathbb{F}_p[X]/(P)\big)^\times\Big),$$

où $A^\times$ designe le groupe d'éléments inversibles de A.

(*a*) Calculer $\varphi(1)$.

(*b*) Soient $P_1, \dots, P_n \in \mathbb{F}_p[X]$ polynômes unitaires et premiers entre eux deux à deux. Montrer que

$$\varphi\Big(\prod_{i=1}^{n} P_i\Big) = \prod_{i=1}^{n} \varphi(P_i).$$

(*c*) Soit $Q \in \mathbb{F}_p[X]$ un polynômes unitaire de degré $d \in \mathbb{N}^*$. Montrer que l'application $\mathbb{F}_p[X]_{<d} \to \mathbb{F}_p[X]/(Q)$ donnée par la restriction de la projection canonique $\pi_Q : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(Q)$ à $\mathbb{F}_p[X]_{<d}$ est une bijection.

(*d*) Soit $P_0 \in \mathbb{F}_p[X]$ un polynômes irréductible unitaire de degré $d_0 \in \mathbb{N}^*$ et soit $N \in \mathbb{N}^*$.

(i) Soit $Q \in \mathbb{F}_p[X]$. Montrer que $\pi_{P_0^N}(Q) \in (\mathbb{F}_p[X]/(P_0^N))^\times$ si et seulement si Q et P_0 sont premiers entre eux, si et seulement si P_0 ne divise pas Q dans $\mathbb{F}_p[X]$.

(ii) En utilisant l'item précédent, montrer que $\varphi(P_0^N) = p^{Nd_0} - p^{(N-1)d_0}$.

(*e*) Soit $Q \in \mathbb{F}_p[X]$ un polynôme unitaire avec décomposition en facteurs irréductibles unitaires donnée par $Q = \prod_{i=1}^{n} P_i^{N_i}$. Calculer $\varphi(Q)$.

(*f*) Soit $P = X^3 + 1 \in \mathbb{F}_2[X]$.

(i) L'anneau $\mathbb{F}_2[X]/(P)$ est-il un corps ?

(ii) Montrer que $X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible et calculer $\varphi(P)$.

3. Soit $p \in \mathbb{N}^*$ un nombre premier impair. Étant donné un nombre entier $n \geq 3$, on rappelle que D_n designe le **groupe diédral** d'ordre $2n$, *i.e.* le groupe d'isométries du n-gone régulier de centre l'origine et qui contient le point $(1,0)$, et que

$$\mathsf{D}_n = \left\{ r^i s^j : i \in [\![0, n-1]\!], j \in \{0,1\} \right\},$$

où r est la rotation de centre l'origine et d'angle $2\pi/n$, et s est la symétrie orthogonale d'axe donné par les abscises.

On considère le produit semi-direct externe $\mathsf{E}_p = (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\psi (\mathbb{Z}/2\mathbb{Z})$ avec $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}((\mathbb{Z}/p\mathbb{Z})^2)$ donné par $\psi(\bar{n})(x) = (-1)^n x$ pour tout $n \in \mathbb{Z}$ et $x \in (\mathbb{Z}/p\mathbb{Z})^2$, où $\bar{n} \in \mathbb{Z}/2\mathbb{Z}$ designe la classe de $n \in \mathbb{Z}$ modulo 2.

(*a*) Montrer que, dans le groupe E_p, $(x, \bar{0})^p = (\mathbf{0}, \bar{0}) = (x, \bar{1})^2$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^2$, où $\mathbf{0} \in (\mathbb{Z}/p\mathbb{Z})^2$ designe l'élément neutre de $(\mathbb{Z}/p\mathbb{Z})^2$.

(*b*) Montrer que l'ordre de tout élément de $\mathsf{D}_p \times (\mathbb{Z}/p\mathbb{Z})$ divise $2p$ et que ce groupe possède un élément d'ordre $2p$.

(*c*) Montrer que les 5 groupes

$$\mathbb{Z}/p^2\mathbb{Z}, (\mathbb{Z}/p\mathbb{Z})^2, \mathsf{D}_{p^2}, \mathsf{D}_p \times (\mathbb{Z}/p\mathbb{Z}) \text{ et } \mathsf{E}_p$$

sont deux à deux non isomorphes.

(*d*) Soit G un groupe d'ordre $2p^2$. Montrer que G est isomorphe à un produit semi-direct externe de la forme $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ ou $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$.
Indication : Vous pouvez utiliser (sans le démontrer) que tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

(*e*) (i) Montrer que $a^2 \equiv 1 \pmod{p^2}$ si et seulement si $a \equiv \pm 1 \pmod{p^2}$ pour tout $a \in \mathbb{Z}$.

(ii) Utiliser l'item précédent pour montrer qu'il existe précisément deux morphismes de groupes $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p^2\mathbb{Z})$.
Indication : Vous pouvez utiliser (sans le démontrer) l'isomorphisme de groupes

$$\mathscr{a} : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/n\mathbb{Z})$$

pour tout $n \in \mathbb{N}^*$ donné par $\mathscr{a}(x)(y) = xy$ pour tous $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $y \in \mathbb{Z}/n\mathbb{Z}$.

(*f*) Étant donné $n \in \mathbb{N}^*$, on rappelle l'isomorphisme de groupes

$$\iota : \mathsf{GL}_n(\mathbb{Z}/p\mathbb{Z}) \to \mathsf{Aut}_{\mathsf{Gr}}((\mathbb{Z}/p\mathbb{Z})^n)$$

qui associe à une matrice inversible $A = (a_{i,j})_{i,j \in [\![1,n]\!]} \in \mathsf{GL}_k(\mathbb{Z}/p\mathbb{Z})$ l'automorphisme de groupes $\iota(A) : (\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^n$ donné par

$$\iota(A)(x_1, \ldots, x_n) = \left(\sum_{j=1}^n a_{1,j} x_j, \ldots, \sum_{j=1}^n a_{n,j} x_j \right)$$

pour tous $x_1, \ldots, x_n \in \mathbb{Z}/p\mathbb{Z}$.

(i) Étant donné $A \in \mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ tel que $A^2 = \mathsf{I}_2$, soit

$$\varphi_A : \mathbb{Z}/2\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}\left((\mathbb{Z}/p\mathbb{Z})^2\right)$$

le seul morphisme de groupes qui satisfait que $\varphi_A(\bar{1}) = \iota(A)$. Montrer que, étant donné $A, P \in \mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ avec $A^2 = \mathsf{I}_2$, l'application

$$\alpha : (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\varphi_A} (\mathbb{Z}/2\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_{\varphi_{PAP^{-1}}} (\mathbb{Z}/2\mathbb{Z})$$

qui associe $(\iota(P)(x), \bar{k})$ à $(x, \bar{k})$ pour $x \in (\mathbb{Z}/p\mathbb{Z})^2$ et $k \in \mathbb{Z}$ est un isomorphisme de groupes.

(ii) Montrer que tout élément de $\mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ d'ordre au plus 2 est conjugué à

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ ou } \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(iii) En déduire qu'il existe au plus 3 produits semi-directs de la forme $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ à isomorphisme près.

(*g*) Utiliser les items précédents pour montrer qu'il y a exactement 5 groupes d'ordre $2p^2$ à isomorphisme près et les préciser.