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.

Solution. On considère le morphisme de groupes

$$\rho : G \to \mathsf{Aut}_{\mathsf{Ens}}(H)$$

qui associe à $g \in G$ la bijection $\rho(g) : H \to H$ donnée par $\rho(g)(h) = ghg^{-1}$, pour $h \in H$. Comme $\rho(g)(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = \rho(g)(h)\rho(g)(h')$ pour tous $g \in G$ et $h, h' \in H$, $\rho(g) \in \mathsf{Aut}_{\mathsf{Gr}}(H)$ pour tout $g \in G$, ce qui implique que ρ se corestreint en un morphisme de groupes

$$\rho : G \to \mathsf{Aut}_{\mathsf{Gr}}(H).$$

Comme H est d'ordre p premier, $H \cong \mathbb{Z}/p\mathbb{Z}$ et

$$\mathsf{Aut}_{\mathsf{Gr}}(H) \cong \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times,$$

ce qui implique que l'image de ρ a cardinalité inférieur ou égal à $p-1$. Soit $K = \mathsf{Ker}(\rho) \subseteq G$. Alors, K est un sous groupe distingué de G et, de façon explicite, $K = \{g \in G : gh = hg \text{ pour tout } h \in H\}$. Il suffit de démontrer que $K = G$. D'après le premier théorème d'isomorphisme, ρ induit un morphisme de groupes injectif $G/K \to (\mathbb{Z}/p\mathbb{Z})^\times$ avec la même image que ρ, ce qui nous dit que $[G : K] \leq p-1$. Comme $[G : K]$ est un diviseur de $|G|$ et p est le plus petit diviseur premier de $|G|$, on conclut que $[G : K] = 1$, *i.e.* $K = G$.

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 $P_1, \ldots, P_n \in \mathbb{F}_p[X]$ 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 $\varphi(P)$.

Solution.

(*a*) On voit bien que $\varphi(1) = 1$, vu que $0 = 1$ est inversible dans l'anneau trivial $\mathbb{F}_p[X]/(1) = \{0\}$.

(*b*) Le théorème des restes chinois nous dit que le morphisme d'anneaux

$$\mathbb{F}_p[X] \to \prod_{i=1}^{n} \mathbb{F}_p[X]/(P_i)$$

qui associe à tout $Q \in \mathbb{F}_p[X]$ l'uplet $(Q+(P_1), \dots, Q+(P_n))$ induit un isomorphisme d'anneaux

$$\mathbb{F}_p[X]/(P) \to \prod_{i=1}^{n} \mathbb{F}_p[X]/(P_i).$$

Cet isomorphisme induit en particulier un isomorphisme de groupes

$$\big(\mathbb{F}_p[X]/(P)\big)^\times \to \Big(\prod_{i=1}^{n} \mathbb{F}_p[X]/(P_i)\Big)^\times \cong \prod_{i=1}^{n} \big(\mathbb{F}_p[X]/(P_i)\big)^\times,$$

qui nous dit que

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

(*c*) On remarque d'abord que l'application $\pi_Q|_{\mathbb{F}_p[X]_{\leq d-1}} : \mathbb{F}_p[X]_{<d} \to \mathbb{F}_p[X]/(Q)$ est surjective. En effet, comme Q est unitaire, par division de polynômes, étant donné $P \in A[X]$, il existe une unique paire $(S,R) \in \mathbb{F}_p[X] \times \mathbb{F}_p[X]_{<d}$ telle que $P = Q.S+R$. Alors, $\pi_Q(P) = \pi_Q(R)$, ce qui implique que

$$\mathbb{F}_p[X]/(Q) = \mathsf{Img}(\pi_Q) \subseteq \mathsf{Img}(\pi_Q|_{\mathbb{F}_p[X]_{<d}}) \subseteq \mathbb{F}_p[X]/(Q)$$

et en particulier les inclusion précédentes sont des égalités.

On considère l'application $r : \mathbb{F}_p[X]/(Q) \to \mathbb{F}_p[X]_{<d}$ définie de la façon suivante. Par division de polynômes, étant donné $P \in A[X]$, il existe une unique paire $(S,R) \in \mathbb{F}_p[X] \times \mathbb{F}_p[X]_{<d}$ telle que $P = Q.S + R$. On pose $r(\pi_Q(P)) = R$. L'expression précédente est bien définie car, si $P_1 - P_2 \in (Q)$, *i.e.* $P_1 - P_2 = Q.T$ avec $T \in \mathbb{F}_p[X]$, et $P_2 = S_2.Q+R$ pour $(S_2,R) \in \mathbb{F}_p[X] \times \mathbb{F}_p[X]_{<d}$, alors $P_1 = (S_2+T).Q+R$. En outre, la définition de r nous dit que $r \circ \pi_Q|_{\mathbb{F}_p[X]_{<d}} = \mathsf{id}_{\mathbb{F}_p[X]_{<d}}$. Cela nous dit que $\pi_Q|_{\mathbb{F}_p[X]_{<d}} \circ r \circ \pi|_{\mathbb{F}_p[X]_{<d}} = \pi|_{\mathbb{F}_p[X]_{<d}} \circ \mathsf{id}_{\mathbb{F}_p[X]_{<d}} = \mathsf{id}_{\mathbb{F}_p[X]/(Q)} \circ \pi_Q|_{\mathbb{F}_p[X]_{<d}}$, ce qui implique que $\pi_Q|_{\mathbb{F}_p[X]_{<d}} \circ r = \mathsf{id}_{\mathbb{F}_p[X]/(Q)}$, car $\pi_Q|_{\mathbb{F}_p[X]_{<d}}$ est surjectif. En conséquence, $\pi_Q|_{\mathbb{F}_p[X]_{<d}}$ est une application bijective avec réciproque r.

(*d*) (i) C'est clair que, si $\pi_{P_0^N}(Q) \in (\mathbb{F}_p[X]/(P_0^N))^\times$, alors Q et P_0 sont premiers entre eux. En effet, la première condition nous dit qu'il existe $S,T \in \mathbb{F}_p[X]$ tels que $S.Q = 1 + T.P_0^N$, ce qui implique que Q et P_0 sont premiers entre eux. De la même façon, c'est clair que si Q et P_0 sont premiers entre eux, alors P_0 ne divise pas Q dans $\mathbb{F}_p[X]$. Pour conclure on va montrer que si P_0 ne divise pas Q dans $\mathbb{F}_p[X]$, alors $\pi_{P_0^N}(Q) \in (\mathbb{F}_p[X]/(P_0^N))^\times$. Or, comme P_0 est irréductible et $\mathbb{F}_p[X]$ est principal, (P_0) est premier. Si P_0 ne divise pas Q dans $\mathbb{F}_p[X]$, alors Q et P_0^N sont premiers entre eux, ce qui implique qu'il existe $S,T \in \mathbb{F}_p[X]$ tels que $S.Q = 1 + T.P_0^N$, i.e. $\pi_{P_0^N}(Q) \in (\mathbb{F}_p[X]/(P_0^N))^\times$.

(ii) À partir du troisième item on voit que

$$\#\big(\mathbb{F}_p[X]/(P_0^N)\big) = \#\big(\mathbb{F}_p[X]_{<Nd_0}\big) = \#\big(\mathbb{F}_p^{Nd_0}\big) = p^{Nd_0}.$$

En outre, l'item précédent nous dit que l'application

$$\mathbb{F}_p[X]_{<(N-1)d_0} \to \mathbb{F}_p[X]/(P_0^N) \setminus \big(\mathbb{F}_p[X]/(P_0^N)\big)^\times$$

qui associe $\pi_{P_0^N}(Q.P_0)$ à $Q \in \mathbb{F}_p[X]_{<(N-1)d_0}$ est surjective. Une vérification immédiate nous dit en plus que l'application est injective, vu que $\deg(Q.P_0) < Nd_0$ si $Q \in \mathbb{F}_p[X]_{<(N-1)d_0}$. En conséquence,

$$\begin{aligned}\#\Big(\mathbb{F}_p[X]/(P_0^N) \setminus \big(\mathbb{F}_p[X]/(P_0^N)\big)^\times\Big) &= \#\big(\mathbb{F}_p[X]_{<(N-1)d_0}\big) \\ &= \#\big(\mathbb{F}_p^{(N-1)d_0}\big) = p^{(N-1)d_0}.\end{aligned}$$

Cela nous dit que

$$\begin{aligned}\varphi(P_0^N) &= \#\Big(\big(\mathbb{F}_p[X]/(P_0^N)\big)^\times\Big) \\ &= \#\Big(\mathbb{F}_p[X]/(P_0^N)\Big) - \#\Big(\mathbb{F}_p[X]/(P_0^N) \setminus \big(\mathbb{F}_p[X]/(P_0^N)\big)^\times\Big) \\ &= p^{Nd_0} - p^{(N-1)d_0}.\end{aligned}$$

(*e*) À partir des items précédents on voit bien que

$$\varphi(Q) = \prod_{i=1}^{n} \varphi(P_i^{N_i}) = \prod_{i=1}^{n} \left(p^{N_i d_i} - p^{(N_i-1)d_i}\right),$$

où $d_i = \deg(P_i)$ pour tout $i \in [\![1, n]\!]$.

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

(i) L'anneau $\mathbb{F}_2[X]/(P)$ n'est pas intègre, vu que $(X+1)(X^2+X+1) = X^3+1 = 0$ dans $\mathbb{F}_2[X]/(P)$, mais les classes de $X+1$ et de X^2+X+1 ne sont pas nulles dans $\mathbb{F}_2[X]/(P)$ par des raisons de degré. Comme $\mathbb{F}_2[X]/(P)$ n'est pas intègre, il n'est pas un corps.

(ii) Le polynôme $Q = X^2+X+1 \in \mathbb{F}_2[X]$ est irréductible car il n'a pas de racines dans $\mathbb{F}_2$, vu que $Q(0) = Q(1) = 1$. Comme $\mathbb{F}_2[X]/(Q)$ est un corps, on voit bien que $\varphi(Q) = 3$. En conséquence, $\varphi(P) = \varphi(Q)\varphi(X+1) = \varphi(Q) = 3$.

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

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

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

(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.

Solution.

(*a*) On voit bien que $(x,\bar{1})^2 = (x,\bar{1})\cdot(x,\bar{1}) = (x+\psi(\bar{1})(x),\bar{1}+\bar{1}) = (x+(-1)x,\bar{1}+\bar{1}) = (\mathbf{0},\bar{0})$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^2$. En outre, c'est clair que $(x,\bar{0})\cdot(y,\bar{0}) = (x+\psi(\bar{0})(y),\bar{0}+\bar{0}) = (x+y,\bar{0})$ pour tous $x,y \in (\mathbb{Z}/p\mathbb{Z})^2$, ce qui nous dit que $(x,\bar{0})^p = (p.x,\bar{0}) = (\mathbf{0},\bar{0})$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^2$.

(*b*) Comme l'ordre d'un élément $(g,x) \in \mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ est le PPCM des ordres de $g \in \mathsf{D}_p$ et de $x \in \mathbb{Z}/p\mathbb{Z}$, el l'ordre de tout élément est un diviseur de l'ordre du groupe qui le contient, on voit que l'ordre de g est un diviseur de $2p = |\mathsf{D}_p|$ et l'ordre de x est un diviseur de $p = |\mathbb{Z}/p\mathbb{Z}|$, ce qui implique que l'ordre de $(g,x) \in \mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ est un diviseur de $2p$ pour tout $(g,x) \in \mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$. On note finalement que l'élément $(s,\bar{1}) \in \mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ est d'ordre $2p$.

(*c*) Les groupes $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$ sont abéliens tandis que les 3 autres groupes ne le sont pas. En effet, comme D_n n'est pas abélien pour $n \geq 3$, D_{p^2} et $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ ne sont pas abéliens, et $(x,\bar{1})\cdot(y,\bar{0}) = (x-y,\bar{1}) \neq (x+y,\bar{1}) = (y,\bar{0})\cdot(x,\bar{1})$ pour $y \neq \mathbf{0}$ implique que E_p n'est pas abélien. En conséquence, $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$ ne sont pas isomorphes aux 3 autres groupes dans l'énoncé. Par ailleurs, $\mathbb{Z}/p^2\mathbb{Z}$ est cyclique, tandis que $(\mathbb{Z}/p\mathbb{Z})^2$ ne l'est pas, vu que l'ordre de tout élément de $(\mathbb{Z}/p\mathbb{Z})^2$ est un diviseur de p. On remarque que les deux items précédents nous disent que l'ordre de tout élément des groupes $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ et E_p est un diviseur de $2p$. Cela implique que le groupe D_{p^2} n'est pas isomorphe au groupe $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ ni au groupe E_p, vu que D_{p^2} possède un élément d'ordre p^2 mais l'ordre de tout élément des groupes $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ et E_p est un diviseur de $2p < p^2$.

Finalement, pour montrer que $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ et E_p ne sont pas isomorphes, on suppose qu'il existe un tel isomorphisme $f|_{\mathscr{Z}(\mathsf{E}_p)} : \mathscr{Z}(\mathsf{E}_p) \to \mathscr{Z}(\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z}))$. On a alors un isomorphisme $f : \mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z}) \to \mathsf{E}_p$. Or, un calcul élémentaire nous dit que $\mathscr{Z}(\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})) = \mathscr{Z}(\mathsf{D}_p) \times (\mathbb{Z}/p\mathbb{Z}) = \{1_{\mathsf{D}_p}\} \times (\mathbb{Z}/p\mathbb{Z})$, tandis que $\mathscr{Z}(\mathsf{E}_p) = \{(\mathbf{0},\bar{0})\}$, ce qui implique que $\mathsf{D}_p \times(\mathbb{Z}/p\mathbb{Z})$ et E_p ne sont pas isomorphes.

(*d*) D'après le théorème de Sylow G possède un p-sous-groupe de Sylow H_p, d'ordre p^2, et un 2-sous-groupe de Sylow H_2, d'ordre 2. Soit N_p la cardinalité de l'ensemble de p-sous-groupe de Sylow de G. Le théorème de Sylow nous dit que $N_p|2$ et que $N_p \equiv 1 \pmod p$, ce qui implique que $N_p = 1$, *i.e.* H_p est un sous-groupe distingué. En conséquence, on a le produit semi-direct interne $G = H_p \rtimes H_2$, vu que $H_2 \cap H_p = \{1_G\}$ (car, par le théorème de Lagrange, $|H_2 \cap H_p|$ divise $2 = |H_2|$ et $p^2 = |H_p|$) et $|G| = |H_2|.|H_p|$. Comme H_p est un groupe d'ordre p^2, on a l'isomorphisme de groupes $H_p \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $H_p \cong (\mathbb{Z}/p\mathbb{Z})^2$, et de façon analogue $H_2 \cong \mathbb{Z}/2\mathbb{Z}$. Par transfert de structures via isomorphismes on conclut qu'il existe un isomorphisme de groupes $G \cong (\mathbb{Z}/p^2\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ ou $G \cong (\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$.

(*e*) (i) C'est clair que $a^2 \equiv 1 \pmod{p^2}$ si et seulement si $p^2|(a^2-1) = (a-1)(a+1)$. Or, on remarque que $p^2|(a^2-1) = (a-1)(a+1)$ si et seulement si $p^2|(a-1)$ ou $p^2|(a+1)$. En effet, $p^2|(a^2-1) = (a-1)(a+1)$ si et seulement si ou bien $p^2|(a-1)$, ou bien $p^2|(a+1)$, ou bien on a que $p|(a+1)$ et $p|(a-1)$. Par contre, le cas $p|(a+1)$ et $p|(a-1)$ est impossible, vu que cela implique $p|((a+1)-(a-1)) = 2$, ce qui est absurde. Finalement, on note que $p^2|(a-1)$ équivaut à $a \equiv 1 \pmod{p^2}$, et $p^2|(a+1)$ équivaut à $a \equiv -1 \pmod{p^2}$.

(ii) On remarque d'abord l'isomorphisme de groupes $\mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p^2\mathbb{Z}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times$. En outre, on rappelle que la donnée d'un moprhisme de groupes

$\psi : \mathbb{Z}/2\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p^2\mathbb{Z}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times$ est équivalente à un élément $\bar{a}_\psi \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ d'ordre 2, via $\bar{a}_\psi = \mathscr{a}^{-1}(\psi(\bar{1}))$. D'après l'item précédent, l'ordre de $\bar{a} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ est un diviseur de 2 si et seulement si $\bar{a} = \bar{1}$ or $\bar{a} = -\bar{1}$ in $(\mathbb{Z}/p^2\mathbb{Z})^\times$. On conclut qu'il existe précisément deux morphismes de groupes $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathsf{Aut}_{\mathsf{Gr}}(\mathbb{Z}/p^2\mathbb{Z})$.

(f) (i) L'application donnée est clairement bijective. La vérification du fait qu'il s'agit d'un morphisme de groupes est immédiate.

(ii) On rappelle que $(\mathbb{Z}/p\mathbb{Z})^2$ est un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/p\mathbb{Z}$, et que tout élément A de $\mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ détermine un endomorphisme linéaire $\iota(A)$ de $(\mathbb{Z}/p\mathbb{Z})^2$. Or, il existe $x \in (\mathbb{Z}/p\mathbb{Z})^2$ non nul tel que $\{x, \iota(A)(x)\}$ est libre, ou pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^2$ non nul l'ensemble $\{x, \iota(A)(x)\}$ est lié. Dans le premier cas, $\{x, \iota(A)(x)\}$ est une base de $(\mathbb{Z}/p\mathbb{Z})^2$ et la représentation matricielle de f dans la nouvelle base $\{x - \iota(A)(x), x + \iota(A)(x)\}$ est

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

vu que $\iota(A)^2(x) = \iota(A^2)(x) = \iota(\mathsf{I}_2)(x) = x$. Dans le deuxième cas, pour n'importe quelle base $\{x, y\}$ de $(\mathbb{Z}/p\mathbb{Z})^2$, $\iota(A)^2(x) = \lambda x$ et $\iota(A)^2(y) = \mu y$, avec $\lambda, \mu \in \mathbb{Z}/p\mathbb{Z}$. Comme $A \in \mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ et $A^2 = \mathsf{I}_2$, $\lambda, \mu \in \{\pm 1\} \subseteq \mathbb{Z}/p\mathbb{Z}$. En plus, si $\lambda \neq \mu$, on peut intervertir x et y si besoin pour que $\lambda = -1$ et $\mu = 1$. On trouve dans ce cas que la représentation matricielle de f dans cette base $\{x, y\}$ est

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

Comme la représentation matricielle de $\iota(A)$ dans une base $\mathscr{B}$ de $(\mathbb{Z}/p\mathbb{Z})^2$ est donnée par PAP^{-1}, où P et P^{-1} sont les matrices de passage entre la base $\mathscr{B}$ et la base canonique de $(\mathbb{Z}/p\mathbb{Z})^2$, on conclut que la matrice A est conjuguée 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) On déduit des items précédents 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) Les trois items précédents nous disent qu'il existe au plus deux groupes non-isomorphes de la forme $(\mathbb{Z}/p^2\mathbb{Z}) \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ et au plus trois groupes non-isomorphes de la forme $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes_\varphi (\mathbb{Z}/2\mathbb{Z})$ à isomorphisme près. Cela nous dit qu'il existe au plus 5 groupes d'ordre $2p^2$ à isomorphisme près. Par ailleurs, le troisième item nous dit qu'il existe au moins 5 groupes d'ordre $2p^2$ à isomorphisme près. En conséquence, il existe précisément 5 groupes d'ordre $2p^2$ à isomorphisme près. La liste est celle donné dans le troisième item.