Soit $(G,\cdot)$, un groupe commutatif fini de neutre e et de cardinal n. On écrit

$$n = \prod_{i=1}^{r} p_i^{\alpha_i},$$

la décomposition du cardinal n en produit de facteurs premiers (les α_i sont des entiers naturels non nuls). Pour alléger les notations, on posera $\pi_i = p_i^{\alpha_i}$.
Pour tout entier $d \in \mathbb{N}^*$, on pose

$$G_d = \{x \in G \,:\, x^d = e\}.$$

1. *Vérifier que G_d est un sous-groupe de $(G,\cdot)$.*
2. *On suppose que l'entier d est premier à n. Que dire du sous-groupe G_d ?*
3. *On considère le groupe produit*

$$\Gamma = \prod_{i=1}^{r} G_{\pi_i}.$$

Démontrer que l'application f définie par

$$\forall\, (x_1,\dots,x_r) \in \Gamma, \qquad f(x_1,\dots,x_r) = \prod_{i=1}^{r} x_i$$

est un isomorphisme du groupe produit Γ sur le groupe G.
4. *On suppose que $\#(G_d) \leqslant d$ pour tout diviseur d de n.*
4. a. *Démontrer que, pour tout $1 \leqslant i \leqslant r$, il existe un élément g_i d'ordre π_i dans G.*
4. b. *En déduire que le groupe $(G,\cdot)$ est cyclique.*

1. Par définition, $G_d \subset G$.
Puisque $e^d = e$, l'ensemble G_d contient e (et n'est donc pas vide).
Soient x et y, deux éléments de G_d. Par définition, $x^d = y^d = e$ et comme le groupe $(G,\cdot)$ est commutatif,

$$(x\cdot y^{-1})^d = x^d \cdot (y^{-1})^d = e\cdot (y^d)^{-1} = e^{-1} = e,$$

ce qui prouve que $x\cdot y^{-1} \in G_d$.
L'ensemble G_d est donc bien un sous-groupe de $(G,\cdot)$.
2. Comme $(G,\cdot)$ est un groupe fini, d'après le Théorème de Lagrange, l'ordre de tout élément x de G divise l'ordre n de G.
Si $x \in G_d$, alors (par définition) $x^d = e$, donc l'ordre de x est un diviseur de d.
Comme n et d sont ici supposés premiers entre eux, on en déduit que l'ordre de $x \in G_d$ est égal à 1, c'est-à-dire $x = e$.
Ainsi, $G_d = \{e\}$ pour tout entier d premier à n.
3. Soit $x = (x_1,\dots,x_r) \in \Gamma$. Comme les x_k appartiennent tous à G et que $(G,\cdot)$ est un groupe, le produit $x_1\cdots x_r$ appartient aussi à G. Par conséquent, l'application f est bien définie de Γ dans G.
❧ Cette application f est bien un morphisme de groupes : quels que soient $x = (x_1,\dots,x_r)$ et $y = (y_1,\dots,y_r)$ dans Γ,

$$x \otimes y = (x_1\cdot y_1,\dots,x_r\cdot y_r)$$

(par définition de la loi sur le groupe produit) et

$$f(x\otimes y) \overset{\dagger}{=} (x_1\cdot y_1)\cdot\dots\cdot(x_r\cdot y_r) \overset{\ddagger}{=} (x_1\cdot\dots\cdot x_r)\cdot(y_1\cdot\dots\cdot y_r) \overset{\dagger}{=} f(x)\cdot f(y)$$

par définition de f ($\dagger$) et commutativité de la loi $\cdot$ ($\ddagger$).
Donc l'application f est bien un morphisme de groupes du groupe produit $(\Gamma,\otimes)$ dans le groupe $(G,\cdot)$.
❧ Le morphisme de groupes f est injectif si, et seulement si, son noyau est réduit à l'élément neutre du groupe de départ, c'est-à-dire :

$$\operatorname{Ker} f = \{(e,\dots,e)\}.$$

✍ *Comme* $\operatorname{Ker} f$ *est un sous-groupe de* $(\Gamma, \otimes)$*, l'inclusion*

$$\{(e, \dots, e)\} \subset \operatorname{Ker} f$$

est toujours vraie et on n'en parle jamais.

Considérons donc $x = (x_1, \dots, x_r) \in \Gamma$ tel que

$$f(x) = x_1 \cdot \cdots \cdot x_r = e.$$

Par définition des sous-groupes G_{π_i}, on sait que

$$x_1^{\pi_1} = x_2^{\pi_2} = \cdots = x_r^{\pi_r} = e.$$

Comme les entiers $\pi_1 = p_1^{\alpha_1}$, $\pi_2 = p_2^{\alpha_2}$, $\dots$, $\pi_r = p_r^{\alpha_r}$ sont deux à deux premiers entre eux (puisque les entiers $p_1, \dots, p_r$ sont des nombres premiers deux à deux distincts), on déduit du Lemme chinois que, pour tout entier $1 \leqslant i \leqslant r$, il existe un entier n_i tel que

$$n_i \equiv 1 \pmod{\pi_i} \qquad \text{et} \qquad \forall\, j \neq i, \quad n_i \equiv 0 \pmod{\pi_j}.$$

Autrement dit, il existe des entiers $k_{i,1}, \dots, k_{i,r}$ tels que

$$n_i = 1 + k_{i,i}\pi_i \qquad \text{et} \qquad \forall\, j \neq i, \quad n_i = k_{i,j}\pi_j.$$

On déduit alors de $x_1 \cdot \cdots \cdot x_r = e$ que

$$e = (x_1 \cdot \cdots \cdot x_r)^{n_i} = x_1^{n_i} \cdot \cdots \cdot x_r^{n_i} = x_i^{1+k_{i,i}\pi_i} \cdot \prod_{\substack{1 \leqslant j \leqslant r \\ j \neq i}} x_j^{k_{i,j}\pi_j} = x_i$$

pour tout $1 \leqslant i \leqslant r$. On a ainsi démontré l'injectivité de f.

❧ Nous allons maintenant démontrer la surjectivité du morphisme f. Pour cela, nous considérons un élément $y \in G$ et nous cherchons un antécédent $x = (x_1, \dots, x_r) \in \Gamma$ de y par f.

Comme les entiers $\pi_1, \dots, \pi_r$ sont deux à deux premiers entre eux, on en déduit que les entiers

$$q_1 = \prod_{j \neq 1} \pi_j, \quad q_2 = \prod_{j \neq 2} \pi_j, \quad \dots, \quad q_r = \prod_{j \neq r} \pi_j$$

sont premiers dans leur ensemble. Il existe donc des entiers relatifs $a_1, \dots, a_r$ tels que

$$\sum_{i=1}^{r} a_i q_i = 1.$$

Par conséquent,

$$y = y^1 = \prod_{i=1}^{r} y^{a_i q_i} = \prod_{i=1}^{r} (y^{q_i})^{a_i}.$$

Par définition des entiers q_i, on sait que $q_i \pi_i = n$ pour tout $1 \leqslant i \leqslant r$, donc

$$\forall\, 1 \leqslant i \leqslant r, \qquad (y^{q_i})^{\pi_i} = y^{q_i \pi_i} = y^n = e$$

puisque l'ordre de l'élément y divise l'ordre n du groupe $(G, \cdot)$. Cela prouve que

$$\forall\, 1 \leqslant i \leqslant r, \qquad y^{q_i} \in G_{\pi_i}$$

et comme G_{π_i} est un sous-groupe de $(G, \cdot)$, on en déduit que

$$\forall\, 1 \leqslant i \leqslant r, \qquad (y^{q_i})^{a_i} \in G_{\pi_i}$$

(les a_i sont des entiers relatifs). On a ainsi démontré que

$$\forall\, y \in G, \qquad x = \big((y^{q_1})^{a_1}, (y^{q_2})^{a_2}, \dots, (y^{q_r})^{a_r}\big) \in \Gamma$$

et que $y = f(x)$.

❧ En conclusion, l'application f est bien un isomorphisme de groupes du groupe produit $(\Gamma, \otimes)$ sur le groupe $(G, \cdot)$.

4. a. En particulier, le morphisme f réalise une bijection entre deux ensembles finis, donc les cardinaux de ces deux ensembles sont égaux. Ainsi,

$$n = \#(G) = \prod_{i=1}^{r} \#(G_{\pi_i}).$$

On suppose ici que

$$\forall\, 1 \leqslant i \leqslant r, \qquad \#(G_{\pi_i}) \leqslant \pi_i$$

donc

$$\prod_{i=1}^{r} \#(G_{\pi_i}) \leqslant \prod_{i=1}^{r} \pi_i = n.$$

On en déduit que

$$\forall\, 1 \leqslant i \leqslant r, \qquad \#(G_{\pi_i}) = \pi_i.$$

❧ Le Théorème de Lagrange nous assure que l'ordre de tout élément du sous-groupe G_{π_i} divise l'ordre de ce sous-groupe. Comme π_i est un puissance de p_i, on en déduit que l'ordre de tout élément de G_{π_i} est une puissance de p_i.

Par conséquent, s'il n'existe aucun élément de G_{π_i} dont l'ordre soit égal à π_i, alors l'ordre de chaque élément de G_{π_i} est un diviseur strict de π_i :

$$\forall\, x \in G_{\pi_i}, \qquad x^{p_i^{\alpha_i - 1}} = e.$$

Autrement dit,

$$G_{\pi_i} \subset G_{p_i^{\alpha_i - 1}}$$

et donc, en considérant les cardinaux,

$$\pi_i = \#(G_{\pi_i}) \leqslant \#(G_{p_i^{\alpha_i - 1}}) \leqslant p_i^{\alpha_i - 1} < \pi_i,$$

ce qui est absurde.

❧ On a ainsi démontré que chaque sous-groupe G_{π_i} contient un élément g_i dont l'ordre est égal à π_i.

Puisque l'ordre du sous-groupe G_{π_i} est égal à l'ordre de $g_i \in G_{\pi_i}$, le sous-groupe G_{π_i} est en fait cyclique et engendré par g_i :

$$\forall\, 1 \leqslant i \leqslant r, \qquad G_{\pi_i} = \langle g_i \rangle.$$

✍ *Le groupe produit $H = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$ est un groupe commutatif d'ordre 12.*

Le groupe $H_8 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ n'est pas cyclique (l'ordre de chacun de ses éléments est au plus égal à 4, aucun n'est d'ordre 8), alors que le groupe $H_3 = \mathbb{Z}/3\mathbb{Z}$ est cyclique. Par conséquent, le groupe produit $H = H_8 \times H_3$ n'est pas cyclique et, par isomorphisme le groupe $(G, \cdot)$ n'est pas cyclique non plus.

❧ *Non, ce groupe $(G, \cdot)$ n'est pas défini, mais c'est sans importance : quel qu'il soit, il est isomorphe à un groupe (bien défini !) qui n'est pas cyclique, donc il n'est pas cyclique.*

❧ *Oui, on peut expliciter un groupe $(G, \cdot)$ qui vérifie ces propriétés : il suffit de fureter dans le groupe symétrique $(\mathfrak{S}_9, \circ)$.*

4. b. Comme les entiers π_i sont deux à deux premiers entre eux, l'ordre de l'élément

$$g = g_1 \cdot g_2 \cdot \cdots \cdot g_r$$

est égal au produit des entiers π_i, c'est-à-dire à n.

✍ *Voir l'exercice corrigé* `rms135-492` *pour le cas de deux éléments et conclure par récurrence sur r.*

On a donc un élément g de G dont l'ordre est égal à l'ordre du groupe $(G, \cdot)$, ce qui prouve que $G = \langle g \rangle$ et en particulier que le groupe $(G, \cdot)$ est cyclique.