Contrôle continu 3

Problème

Si E est un ensemble fini, on note $|E|$ son cardinal. Pour tout entier $n \in \mathbf{N}^*$, on note $\varphi(n) = |\mathbf{Z}/n\mathbf{Z}|$. On rappelle que si n a pour décomposition en facteurs premiers $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1, \ldots, p_r$ nombres premiers distincts et $\alpha_1, \ldots, \alpha_r$ dans $\mathbb{N}^*$, alors

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1).$$

Le but du problème est de montrer, pour tout $n \in \mathbf{N}^*$, l'équivalence entre les deux propriétés suivantes :

(P_n)	Tout groupe d'ordre n est cyclique.
(Q_n)	$n \wedge \varphi(n) = 1$.

On rappelle les résultats suivants (vus en TD). Si H et K sont des groupes, alors :

$$H \times K \text{ cyclique} \iff (H, K \text{ cycliques et } |H| \wedge |K| = 1).$$

De plus, pour tout morphisme de groupes $\rho : K \mapsto \mathrm{Aut}(H)$,

$$H \times_\rho K \text{ abélien} \iff (H, K \text{ abéliens et } \rho \text{ trivial}).$$

I. Premiers résultats et implication $P_n \implies Q_n$

1. Montrer que P_1 est vraie.
2. Montrer que pour tout nombre premier p, la proposition P_p est vraie (preuve attendue).
3. Montrer que pour tout nombre premier p, la proposition P_{p^2} est fausse.
4. Montrer que si deux nombres premiers p et q vérifient $q \mid (p-1)$, alors la proposition P_{pq} est fausse.
   Indication : construire un produit semi-direct non direct.
5. Soit $n \geq 2$ un entier. On considère les deux propriétés
   (a) il existe un nombre premier p tel que p^2 divise n ;
   (b) il existe deux nombre premiers p et q divisant n tel que q divise $p-1$.
   Montrer que chacune de ces propriétés implique $n \wedge \varphi(n) \neq 1$.

6. Réciproquement, montrer que si $n \wedge \varphi(n) \neq 1$, alors au moins une des deux propriétés (a),(b) ci-dessus a lieu.
   Indication : prendre un diviseur premier p de $n \wedge \varphi(n)$.
7. Soient $d, n \in \mathbb{N}^*$ tels que d divise n. Montrer que : $P_n \implies P_d$.
   Indication : utiliser un produit direct de groupes.
8. En déduire que si Q_n est fausse, alors P_n est fausse.
9. À l'aide de la question 6, donner un exemple d'entier n qui est le produit de deux nombres premiers et tel que Q_n est vraie. Idem avec trois nombres premiers.
10. Montrer que si Q_n est vraie, alors tout groupe **abélien** d'ordre n est cyclique.
    Indication : montrer qu'on peut écrire n comme produit de nombres premiers distincts et utiliser le théorème de Cauchy.
11. Montrer que si Q_n est vraie, alors pour tout diviseur d de n, Q_d est vraie.
    Indication : on peut raisonner par contraposition à l'aide des questions 6 et 5, ou bien montrer que $\varphi(d)$ divise $\varphi(n)$.

II. Un premier lemme

On se propose de démontrer le lemme suivant.

> Soit $n \geq 2$ un entier tel que la proposition Q_n est vraie.
> Soient G un groupe quelconque d'ordre n et H un sous-groupe cyclique de G.
> Si x, y sont deux éléments de H conjugués dans G, alors $x = y$.

On fixe donc un entier n, un groupe G et un sous-groupe H de G vérifiant les hypothèses du lemme. On fixe un générateur a de H. On prend deux éléments $x = a^k$ et $y = a^\ell$ de H, avec $k, \ell \in \mathbf{Z}$. On suppose qu'il existe $g \in G$ tel que $y = gxg^{-1}$.

1. Montrer que pour tout $d \in \mathbb{N}^*$, $a^{\ell d} = g^d a^{k^d} g^{-d}$.
2. En déduire que $o(a)$ divise $\ell^{o(g)} - k^{o(g)}$, où $o(g)$ et $o(a)$ désignent les ordres de g et a respectivement dans G.
3. Soit p un diviseur premier de $o(a)$. Montrer que p divise $\ell - k$.
   Indication : remarquer qu'on a $\overline{l}^{o(g)} = \overline{k}^{o(g)}$ dans $\mathbf{Z}/p\mathbf{Z}$, et distinguer deux cas, suivant que p divise ou ne divise pas k. Dans le second cas, fixer un entier k' tel que $\overline{k'}$ soit l'inverse de $\overline{k}$ dans $(\mathbf{Z}/p\mathbf{Z})^\times$, montrer que $\overline{k'l}^{o(g)} = \overline{1}$ et montrer que l'ordre de $\overline{k'l}$ dans $(\mathbf{Z}/p\mathbf{Z})^\times$ divise à la fois n et $\phi(n)$.
4. En déduire que $o(a)$ divise $\ell - k$. Conclure.

III. Preuve par récurrence de l'implication $Q_n \implies P_n$

La première partie montre que cette implication est vérifiée lorsque $n \in \{1, 2, 3\}$.
On fixe donc un entier $n \geq 4$ et on suppose que pour tout entier m entre 2 et $n-1$, l'implication $Q_m \implies P_m$ est vraie.
Pour montrer l'implication $Q_n \implies P_n$, on suppose donc dans toute la suite que Q_n est vraie, et on va montrer que P_n est vraie.
Soit G un groupe d'ordre n. Il s'agit donc de montrer que G est cyclique.
On note $Z(G)$ le centre de G. Pour tout $x \in G$, on note $C(x) = \{g \in G : gx = xg\}$.
On rappelle que $Z(G)$ et $C(x)$ sont des sous-groupes de G, ainsi que le fait général suivant : si $G/Z(G)$ est cyclique, alors G est abélien.

1. Montrer qu'il suffit de montrer que G est abélien
   Indication : appliquer le résultat de la question I.10.
2. Montrer qu'il suffit de montrer que $Z(G)$ est non-trivial
   Indication : appliquer le résultat de la question I.11. aux entiers n et $|G/Z(G)|$.
3. Montrer que si H est un sous-groupe strict de G, alors H est cyclique.
   Indication : utiliser la question I.11.
4. En déduire que si $x \in G$ et si H est un sous-groupe contenant x autre que G, alors $H \subset C(x)$.
5. En déduire que si deux éléments x, y de $G \setminus Z(G)$ vérifient $xy = yx$, alors $C(y) = C(x)$.
   Si de plus $y \neq x$, montrer que x et y ne sont pas conjugués dans G. Indication : utiliser le lemme de la partie II.

Pour finir, on démontre par l'absurde que le centre $Z(G)$ est non trivial. **On suppose donc dans les questions 6 à 9 que** $Z(G) = \{1_G\}$.

Pour tout sous-groupe H de G, on note $H^* = H \setminus \{1_G\}$.

6. Montrer que pour tous $x, y \in G^*$, on a $C(x) = C(y)$ ou $C(x) \cap C(y) = \{1_G\}$.
7. Soient x et x' dans G^* tels que $|C(x')| = |C(x)|$. Le but de cette question est de montrer que x' est conjugué à un élément de $C(x)^*$.
   (a) Montrer que $|C(x)|$ possède un diviseur premier p.
   (b) Montrer que $C(x)$ et $C(x')$ possèdent chacun un sous-groupe d'ordre p.
   (c) On note respectivement S et S' de tels sous-groupes. Pourquoi peut-on trouver $g \in G$ tel que $S' = gSg^{-1}$?
   (d) Soient $y \in S^*$ et $y' = gyg^{-1}$. Montrer que $C(y') = gC(y)g^{-1}$.
   (e) Conclure à l'aide de la question 6.
8. Soient $n_1, \ldots, n_k$ les valeurs différentes prises par les $|C(x)|$ pour $x \in G^*$. Pour chaque $i \in [\![1, k]\!]$, on choisit $x_i \in G^*$ tel que $|C(x_i)| = n_i$. Montrer que l'ensemble

$$R := \{1_G\} \cup \bigcup_{i=1}^{k} C(x_i)^*$$

est un système de représentants des classes de conjugaison de G (autrement dit R contient un élément et un seul de chaque classe) et que l'union qui sert à définir l'ensemble R est disjointe.

9. À l'aide de la formule des classes, déduire de la question précédente que

$$1 - \frac{1}{n} = \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) \geq \frac{k}{2}.$$

puis que $k = 1$ et $n_1 = n$, et obtenir une contradiction.

Corrigé du contrôle continu 3

I. Cas particuliers et premiers résultats

1. La propriété P_1 est vraie : tout groupe d'ordre 1 est réduit à l'élément neutre donc engendré par cet élément.
2. Soient G un groupe d'ordre p premier et a un élément autre que le neutre. L'ordre de a est différent de 1 et divise p (Lagrange), donc vaut p. Donc G est engendré par a.
3. Soit p un entier premier. Le groupe $(\mathbb{Z}/p\mathbb{Z})^2$ est d'ordre p^2 et pourtant n'est pas cyclique d'après le rappel (dans ce groupe, l'ordre de tout élément divise p). Donc P_{p^2} est fausse.
4. Soient p et q deux nombres premiers tels que $q \mid (p-1)$. Le groupe $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^\times$ donc d'ordre $p-1$. D'après le théorème de Cauchy, il contient donc un automorphisme α d'ordre q. Le morphisme de groupes $k \mapsto \alpha^k$ de $\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ a pour noyau $q\mathbb{Z}$. Par passage au quotient, il fournit un morphisme de groupes (injectif) non trivial $\rho : \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. Le produit semi-direct $\mathbb{Z}/p\mathbb{Z} \rtimes_\rho \mathbb{Z}/q\mathbb{Z}$ est non abélien (d'après le rappel) donc non cyclique. Donc P_{pq} est fausse.
5. Si la propriété (a) a lieu, l'exposant de p dans la décomposition en facteurs premiers de n est un entier $\alpha \geq 2$. Or la formule donnant $\varphi(n)$ montre que $p^{\alpha-1}$ divise $\varphi(n)$. Donc p est un diviseur commun de n et $\varphi(n)$.

   Si la propriété (b) a lieu, n possède deux facteurs premiers q tels que q divise $p-1$. La formule donnant $\varphi(n)$ montre que $p-1$ divise $\varphi(n)$. Donc q est un diviseur commun de n et $\varphi(n)$.

   Dans les deux cas, $n \wedge \varphi(n) \neq 1$.
6. Réciproquement, supposons que $n \wedge \varphi(n) \neq 1$. Notons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1, \ldots, p_r$ nombres premiers distincts et $\alpha_1, \ldots, \alpha_r$ dans $\mathbb{N}^*$, Soit p un diviseur premier de $n \wedge \varphi(n)$, autrement dit un diviseur commun de n et $\varphi(n)$.

   Alors il existe un et un seul $i \in [\![1, r]\!]$ tel que $p = p_i$.

   Si $\alpha_i \geq 2$, alors la propriété (a) est vérifiée.

   Sinon, $\alpha_i = 1$. Comme p_i est premier et divise

   $$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1),$$

   il divise l'un des facteurs. Or il ne divise aucun des facteurs $p_j^{\alpha_j - 1}$ puisque $p_1, \ldots, p_r$ nombres premiers distincts et puisque $\alpha_i - 1 = 0$. Donc il divise un des facteurs $p_j - 1$, ce qui montre que la propriété (b) est vérifiée.

7. Soit $n \in \mathbb{N}^*$ tel que P_n vraie et d un diviseur de n. Posons $n = dq$ avec $q \in \mathbb{N}^*$. Soit H un groupe d'ordre d. Le groupe $H \times \mathbb{Z}/q\mathbb{Z}$ est d'ordre n donc cyclique, donc H est cyclique d'après le rappel. Par conséquent, P_d est vraie.

8. Si Q_n est fausse, alors on est dans au moins un des cas ci-dessous
   — il existe p premier tel que $p^2 \mid n$; comme la propriété P_{p^2} est fausse, la propriété P_n est fausse d'après la question 7.
   — il existe p, q premiers divisant n tels $q \mid (p-1)$; comme la propriété P_{pq} est fausse, on conclut de même que P_n est fausse.
   Dans les deux P_n est fausse.

9. On peut prendre $n = 3 \times 5$ (auquel cas $\varphi(n) = 2 \times 4 = 2^3$) et $n = 3 \times 5 \times 17$ (auquel cas $\varphi(n) = 2 \times 4 \times 16 = 2^7$).

10. Soit n un entier vérifiant Q_n et G un groupe abélien d'ordre n. Alors pour tout nombre premier p, p^2 ne divise pas n. Donc $n = p_1 \dots p_r$, avec $p_1, \dots, p_r$ nombres premiers deux-à-deux distincts. D'après le théorème de Cauchy, pour tout $i \in \{1, \dots, r\}$, le groupe G contient un élément a_i d'ordre p_i. Comme G est abélien et comme les ordres des éléments $a_1, \dots, a_r$ sont premiers entre eux deux-à-deux, le produit $a_1 \dots a_r$ est d'ordre $p_1 \cdots p_r = |G|$ donc G est cyclique.

11. Soient $n \in \mathbb{N}^*$ et d un diviseur de n. Supposons que la propriété Q_n est vraie. D'après la question 6, on sait que :
   — Pour tout diviseur premier p de n, p^2 ne divise pas n.
   — Pour tous diviseur premier p et q de n, q ne divise pas $p-1$.
   Cela est donc vrai en particulier pour les diviseurs premiers de d (puisque d divise n). D'après la question 6, la propriété Q_d est vraie.

   Autre méthode : posons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec $p_1, \dots, p_r$ nombres premiers distincts et $\alpha_1, \dots, \alpha_r$ dans $\mathbb{N}^*$. Alors $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$, où pour tout $i \in [\![1, r]\!]$, $\beta_i \in [\![0, \alpha_i]\!]$. Soit I l'ensemble des indices $i \in [\![1, r]\!]$ tels que $\beta_i \neq 0$. Alors

$$\varphi(d) = \prod_{i \in I} p_i^{\beta_1 - 1}(p_i - 1) \text{ divise } \prod_{i \in I} p_i^{\alpha_1 - 1}(p_i - 1) \text{ qui divise } \varphi(n).$$

   Comme $d \wedge \varphi(d)$ divise à la fois n et $\varphi(n)$, il vaut 1.

II. Un premier lemme

Soit $n \geq 2$ un entier tel que $n \wedge \varphi(n) = 1$. Soient G un groupe d'ordre n et H un sous-groupe cyclique de G. On considère un générateur a de H et deux éléments $x = a^k$ et $y = a^\ell$ de H, avec $k, \ell \in \mathbb{Z}$. On suppose qu'il existe $g \in G$ tel que $y = gxg^{-1}$.

1. Montrons par récurrence que pour tout $d \in \mathbb{N}^*$, $a^{\ell^d} = g^d a^{k^d} g^{-d}$.
   Pour $d = 1$, on a bien $a^\ell = g a^k g^{-1}$ par hypothèse sur x et y.
   Soit $d \in \mathbb{N}^*$ tel que la propriété est vraie. Par hypothèse de récurrence, on a

$$\begin{aligned} a^{\ell^{d+1}} = (a^{\ell^d})^\ell &= (g^d a^{k^d} g^{-d})^\ell \\ &= g^d (a^{k^d})^\ell g^{-d} \\ &= g^d (a^\ell)^{k^d} g^{-d} \\ &= g^d (g a^k g^{-1})^{k^d} g^{-d} \\ &= g^d (g (a^k)^{k^d} g^{-1}) g^{-d} \\ &= g^{d+1} a^{k^{d+1}} g^{-d-1}. \end{aligned}$$

   ce qui montre que la propriété est vraie au rang $d + 1$.

2. L'égalité précédente appliquée à l'entier $d = o(g)$ montre que $a^{\ell^{o(g)}} = a^{k^{o(g)}}$, i.e. $a^{\ell^{o(g)} - k^{o(g)}} = 1_G$. Donc $o(a)$ divise $\ell^{o(g)} - k^{o(g)}$.

3. Soit p un diviseur premier de $o(a)$. D'après la question précédente, p divise $\ell^{o(g)} - k^{o(g)}$, donc $\overline{\ell}^{o(g)} = \overline{k}^{o(g)}$ dans $\mathbb{Z}/p\mathbb{Z}$.

   Si p divise k, alors $\overline{\ell}^{o(g)} = \overline{k}^{o(g)} = \overline{0}$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $\overline{\ell} = \overline{0}$ Comme p divise à la fois k et ℓ, il divise $\ell - k$.

   Si p ne divise pas k, alors $\overline{k}$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$. Soit $\overline{k'}$ son inverse. En multipliant par $\overline{k'}^{o(g)}$ l'égalité $\overline{\ell}^{o(g)} = \overline{k}^{o(g)}$, on obtient $\overline{k'\ell}^{o(g)} = \overline{1}$. Donc l'ordre de $\overline{k'l}$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $o(g)$, qui divise n (Lagrange) Mais l'ordre de $\overline{k'l}$ divise aussi $|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1$, qui divise $\varphi(n)$. Comme n et $\varphi(n)$ sont supposés premiers entre eux, l'ordre de $\overline{k'l}$ vaut 1, autrement dit $\overline{k'l} = \overline{1}$. En multipliant par $\overline{k}$, on obtient $\overline{l} = \overline{k}$, autrement dit p divise $\ell - k$.

   Dans tous les cas, p divise $\ell - k$.

4. Comme n n'est divisible par aucun carré de nombre premier, il en est de même pour $o(a)$. Donc $o(a)$ est le produit des nombres premiers qui le divisent. Comme ces nombres premiers divisent $\ell - k$, on en déduit que $o(a)$ divise $\ell - k$, d'où $a^{\ell - k} = 1_G$ et $y = a^\ell = a^k = x$.

III. Preuve par récurrence de l'implication $Q_n \implies P_n$

Soit $n \geq 4$. On suppose que pour tout $1 \leq m \leq n-1$, l'implication $Q_m \implies P_m$ est vraie. On suppose aussi que Q_n est vraie, et on va montrer que P_n est vraie. Soit G un groupe d'ordre n.

1. Comme Q_n est vraie, si G est abélien, il est cyclique d'après I.10.
2. Comme Q_n est vraie, le résultat de la question I.11 montre que pour tout diviseur d de n, la propriété Q_d est vraie. L'hypothèse de récurrence montre alors que si d divise strictement de n, alors P_d est vraie.
   Si $Z(G)$ n'est pas trivial, alors l'ordre du groupe $G/Z(G)$ divise strictement n, donc le groupe $G/Z(G)$ est cyclique, donc G est abélien d'après le rappel.
3. Pour tout diviseur strict d de n, P_d est vraie d'après I.7. Pour tout sous-groupe H de G autre que G, l'ordre de H est un diviseur strict de n, ainsi H est cyclique.
4. Soient $x \in G$ et si H est un sous-groupe contenant x autre que G. D'après la question précédente, H est cyclique donc abélien. Comme il contient x, tous ses éléments de H commutent avec x, i.e. $H \subset C(x)$.
5. Soient x, y de $G \setminus Z(G)$ tels que $xy = yx$. Comme y n'est pas un élément du centre, $C(y)$ est un sous-groupe strict de G, et comme ce sous-groupe contient x, la question précédente montre que $C(y) \subset C(x)$. On montre de même que $C(x) \subset C(y)$. Ainsi $C(x) = C(y)$.
   Par hypothèse de récurrence, on sait aussi que le groupe $C(x) = C(y)$ est cyclique. Ce groupe contient x et y. Si x et y sont conjugués dans G on a donc $x = y$, d'après le lemme de la partie II.

Dans la suite, on suppose que $Z(G) = \{1_G\}$ pour obtenir une absurdité.

Pour tout sous-groupe H de G, on note $H^* = H \setminus \{1_G\}$.

6. Soient $x, y \in G^*$. Si $C(x) \cap C(y)$ contient un élément $z \neq 1_G$, alors l'hypothèse ci-dessus assure que x, y, z ne sont pas dans le centre de G. Comme z commute avec x et avec y, la question précédente montre que $C(x) = C(z) = C(y)$.
   Ainsi, $C(x) = C(y)$ ou $C(x) \cap C(y) = \{1_G\}$.
7. Soient x et x' dans G^* tels que $|C(x')| = |C(x)|$.
   (a) Comme $C(x)$ est un sous-groupe fini non trivial (il contient x qui est différent de 1_G), son ordre possède un diviseur premier p.
   (b) D'après le théorème de Cauchy, $C(x)$ possède un élément d'ordre p. Cet élément engendre un sous-groupe S d'ordre p. De même, $C(x')$ possède un sous-groupe S' d'ordre p.
   (c) Comme S et S' sont des sous-groupes de G, leur ordre p divise n. Mais comme la propriété Q_n est vraie, p^2 ne divise pas n. Ainsi, S et S' sont des p-Sylows de G, ils sont donc donc conjugués : il existe $g \in G$ tel que $S' = gSg^{-1}$.

(d) Soient $y \in S^*$ et $y' = gyg^{-1}$. Pour tout $z \in G$, on a les équivalences

$$z \in C(y') \iff zy' = y'z \iff zgyg^{-1} = gyg^{-1}z$$
$$\iff g^{-1}zgy = yg^{-1}zg \iff g^{-1}zg \in C(y) \iff z \in gC(y)g^{-1}.$$

Donc $C(y') = gC(y)g^{-1}$.

(e) Comme $C(x)$ et $C(y)$ contiennent y qui est différent de 1_G, on a $C(y) = C(x)$. De même, $C(y') = C(x')$. D'après la question précédente, on a ainsi

$$x' \in C(y') = gC(y)g^{-1} = gC(x)g^{-1}.$$

Ainsi, x' est conjugué à un élément de $C(x)$, nécessairement autre que 1_G.

8. Montrons que tout élément de G est conjugué à un élément de R et un seul.
L'élément neutre est dans R et n'est conjugué qu'à lui-même.
Soit $g \in G^*$. Alors il existe $i \in [\![1, k]\!]$ tel que $|C(g)| = n_i = |C(x_i)|$. D'après la question précédente, g est conjugué à un élément de $C(x_i)^*$ donc de R.
Si x, x' sont deux éléments de R conjugués à g, donc différents de 1_G, il existe $i, j \in [\![1, k]\!]$ tels que $x \in C(x_i)$ et $x' \in C(x_j)$. D'après III.6, on a alors $C(x) = C(x_i)$ et $C(x') = C(x_j)$. Comme x et x' sont conjugués, $C(x)$ et $C(x')$ aussi (même argument qu'à la question précédente). Ainsi, $n_i = |C(x_i)| = |C(x)| = |C(x')| = |C(x_j)| = n_j$, donc $i = j$ puisque $n_1, \dots, n_k$ sont distincts. Comme x et x' sont conjugués et appartiennent au groupe cyclique $C(x_i)$, on a $x = x'$ d'après III5.
Enfin, les ensembles $C(x_i)^*$ sont distincts car de cardinaux différents ; d'après III.6, ils sont donc disjoints. Et ils sont disjoints de $\{1_G\}$ par construction.

9. La formule des classes donne

$$n = |G| = \sum_{x \in R} |\mathrm{Orb}(x)| = \sum_{x \in R} \frac{|G|}{|C(x)|} = 1 + \sum_{i=1}^{k} \sum_{x \in C(x_i)^*} \frac{|G|}{|C(x)|}$$

Or si $x \in C(x_i)^*$, $C(x) = C(x_i)$. Donc

$$n = 1 + \sum_{i=1}^{k} |C(x_i)^*| \frac{|G|}{|C(x_i)|} = 1 + n \sum_{i=1}^{k} \frac{n_i - 1}{n_i}.$$

En divisant par n et comme pour tout $i \in [\![1, k]\!]$, $n_i \geq 2$, on obtient

$$1 > 1 - \frac{1}{n} = \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right) \geq \frac{k}{2}.$$

Ainsi, $k < 2$ donc $k = 1$ et $1 - 1/n = 1 - 1/n_1$ i.e. $n_1 = n$. Par égalité des ordres, $C(x_1) = G$ i.e. $x_1 \in Z(G)$, ce qui contredit l'hypothèse que le centre est trivial.

Remarques sur les copies.
I3, I4 : beaucoup de hors sujet. On ne demande pas de classifier les groupes d'ordre p^2 ou d'ordre pq, mais d'en construire un qui est non-cyclique. Et il faut donner une bonne raison pour que le groupe exhibé soit non-cyclique : pas d'élément d'ordre p^2 dans le premier cas, groupe non abélien dans le deuxième.
Attention : un produit semi-direct non-direct peut être isomorphe à un produit direct. En effet, soit H un groupe non abélien. Soit K un sous-groupe de H non contenu dans le centre de H. Alors le morphisme $\rho : k \mapsto \mathrm{int}_k$ de K dans Aut(H) n'est pas trivial (puisque pour tout $k \in H \setminus Z(H)$, $\mathrm{int}_k \neq \mathrm{id}_H$). L'application $f : (h,k) \mapsto (hk,k)$ est un morphisme de $H \times_\rho K$ dans $H \times K$. En effet, pour tous (h,k) et (h',k')

$$\begin{aligned} f\big((h,k)\times_\rho (h',k')\big) &= f\big((hkh'k^{-1},kk')\big) \\ &= (hkh'k',kk') \\ &= (hk,k)\times(h'k',k') = f((h,k))\times f((h',k')). \end{aligned}$$

I5a. Si p^2 divie n, alors l'exposant de p dans la décomposition en facteurs premiers de n est **supérieur ou égal** à 2.
I6. Faire apparaître clairement que si le nombre premier p divise un produit d'entiers, il divise l'un des facteurs.
I10. Dire qu'on a des éléments d'ordre premiers entre eux deux à deux et qui commutent pour dire que l'ordre de leur produit est le produit des ordres.
II1. $(a^\ell)^d$ est égal à $a^{\ell d}$ et non à a^{ℓ^d}. Et $(ga^\ell g^{-1})^d$ est égal à $ga^{\ell d}g^{-1}$ et non à $g^d a^{\ell^d} g^{-d}$.
II2. Pour passer de p divise $\ell^{o(g)}$ à p divise ℓ, il faut utiliser le fait que p est premier.
III7bc. Dire que p^2 ne divise pas $|C(x)|$ (car p^2 ne divise pas n) pour affirmer que les p-Sylow de $C(x)$ sont d'ordre p.