Contrôle continu 3

L'examen démarre à 8h30 et se termine à 12h30. À la fin du test, vous devez envoyer votre copie par e-mail à

— vanessa.vitse@univ-grenoble-alpes.fr *si vous faites partie du groupe A1 ;*

— christophe.leuridan@univ-grenoble-alpes.fr *si vous faites partie du groupe A2.*

Cet email doit contenir une version numérique de vos réponses : photos lisibles ou scans, **avec une taille totale ne dépassant pas 5Mo**. *Le nom de chaque fichier doit être votre nom de famille, et si vous avez plusieurs fichiers, ils doivent être numérotés consécutivement.*

Vous avez jusqu'à 13h dernier délai pour envoyer votre email.

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 $\mathbf{N}^*$, 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 $d, n \in \mathbf{N}^*$ 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 $d \in \mathbf{N}^*$, $a^{\ell^d} = g^d a^{k^d} g^{-d}$.
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.