Université de Bordeaux

Licence 3 - année 2023-2024
Structures algébriques 2 - 4TMFF502U

Corrigé du devoir maison

Soit $n \in \mathbf{N}_{>0}$ tel que $\mathsf{pgcd}(n, \varphi(n)) = 1$ (où φ est l'indicatrice d'Euler). Le but de l'exercice est de prouver que tout groupe d'ordre n est cyclique.
(1) (a) Donner un exemple d'un tel n.
(b) Prouver que la factorisation de n en produit de nombres premiers est de la forme $n = p_1 \cdots p_r$ avec $p_1, \ldots, p_r$ deux à deux distincts.
(c) La condition de (b) est-elle suffisante ?

On procède par récurrence forte sur $r \in \mathbf{N}$, le cas $r \in \{0, 1\}$ étant trivial : on suppose désormais $r > 1$. Soit G un groupe d'ordre n, dont on note e l'élément neutre.

(2) Expliquer pourquoi tout sous-groupe strict de G est cyclique.

(3) Supposons G *simple*. On note $\mathcal{M}$ l'ensemble des sous-groupes stricts maximaux (au sens de l'inclusion) de G (constitué des sous-groupes $H \subsetneq G$ tels que si K est un sous-groupe de G contenant H, on a $K = H$ ou $K = G$).
(a) Montrer que si $H_1, H_2 \in \mathcal{M}$ sont distincts, on a $H_1 \cap H_2 = \{e\}$ [indication : montrer que si $x \in H_1 \cap H_2$, son centralisateur $\mathsf{C}_G(x) = \{g \in G\,;\, g^{-1}xg = x\}$ contient H_1 et H_2].
(b) Montrer que $G \setminus \{e\} = \bigsqcup_{H \in \mathcal{M}} (H \setminus \{e\})$.
(c) On fait agir G sur $\mathcal{M}$ par conjugaison. Montrer que l'orbite de $H \in \mathcal{M}$ est de cardinal $(G : H)$.
(d) En dénombrant les éléments de $G \setminus \{e\}$, montrer que $\mathcal{M}$ ne contient qu'une orbite, puis en déduire une contradiction.

Le groupe G n'est donc pas simple : soit $\{e\} \subsetneq H \subsetneq G$ un sous-groupe distingué non trivial. La restriction à H de l'action de G sur lui-même par conjugaison fournit un morphisme de groupes $\rho\colon G \to \mathsf{Aut}(H)$.

(4) Montrer que $\#\,\mathsf{Aut}(H)$ est premier à n [indication : penser d'abord au cas où $\#H$ est un nombre premier].

(5) En déduire que H est inclus dans le centre $\mathsf{Z}(G)$ de G.

(6) En déduire que G est abélien.

(7) Conclure que G est cyclique.

(8) Réciproquement, montrer que si $n \in \mathbf{N}_{>0}$ est un entier tel que tout groupe d'ordre n est cyclique, alors $\mathsf{pgcd}(n, \varphi(n)) = 1$ [indication : penser aux produits semi-directs].

Solution : (1) Écrivons $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec $p_1 < \cdots < p_r$ premiers et $\alpha_1, \ldots \alpha_r \in \mathbf{N}_{>0}$. On a $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$. Comme $\prod_{i=1}^{r} p_i^{\alpha_i - 1}$ divise $\mathrm{pgcd}(n, \varphi(n)) = 1$, on a $\alpha_1 = \cdots = \alpha_r = 1$.
(2) Soit $H < G$ un sous-groupe strict. Posons $m = \#H$. On a $m \mid n$ (théorème de Lagrange), donc $\varphi(m) \mid \varphi(n)$: comme $\mathsf{pgcd}(n, \varphi(n)) = 1$, on a *a fortiori* $\mathsf{pgcd}(n, \varphi(m)) = 1$, d'où aussi $\mathsf{pgcd}(m, \varphi(m)) = 1$. Par hypothèse de récurrence, le groupe H est cyclique.
(3) (a) Soit $x \in H_1 \cap H_2$. Comme H_1 est cyclique donc abélien, on a $H_1 \subset \mathsf{C}_G(x)$. De même, on a $H_2 \subset \mathsf{C}_G(x)$, et donc $\mathsf{C}_G(x) = G$ vu que le sous-groupe engendré par H_1 et

H_2 est G tout entier (il contient strictement le sous-groupe maximal H_1). Cela implique $x \in \mathsf{Z}(G)$ et donc $x = e$ vu que $\mathsf{Z}(G) = \{e\}$ (car G est simple). On a donc $H_1 \cap H_2 = \{e\}$.
(b) Soit $x \in G \setminus \{e\}$. Comme G est simple d'ordre non premier, il n'est pas cyclique : on a $\langle x \rangle \neq G$. Comme G est fini, on peut donc trouver $H \in \mathcal{M}$ tel que $\langle x \rangle \subset H$, et donc $x \in H \setminus \{e\}$. Cela prouve que $G \setminus \{e\} = \bigcup_{H \in \mathcal{M}} H \setminus \{e\}$. La réunion est disjointe en vertu de la question précédente.
(c) Le stabilisateur de H est le normalisateur $\mathsf{N}_G(H)$. On a $H \subset \mathsf{N}_G(H)$. Comme G est simple et H est strict, on a $\mathsf{N}_G(H) \neq G$ (sinon H serait distingué), donc $\mathsf{N}_G(H) = H$ par maximalité de H. L'orbite de H a donc $(G : \mathsf{N}_G(H)) = (G : H)$ éléments.
(d) Soient $H_1, \ldots, H_s$ un système complet de représentants des orbites dans $\mathcal{M}$ pour cette action. On a alors $\mathcal{M} = \bigsqcup_{i=1}^{s} \{\tau^{-1} H_i \tau\}_{\tau \in G/H_i}$. Pour $i \in \{1, \ldots, s\}$, posons $m_i = \# H_i$. D'après la question (b), on a $G \setminus \{e\} = \bigsqcup_{i=1}^{s} \bigsqcup_{\tau \in G/H_i} \tau^{-1} H_i \tau \setminus \{e\}$ et donc $n - 1 = \sum_{i=1}^{s} \frac{n}{m_i}(m_i - 1)$ d'où $n - 1 = sn - \sum_{i=1}^{s} \frac{n}{m_i}$. On a $\sum_{i=1}^{s} \frac{n}{m_i} \leq \frac{sn}{2}$ (vu que $m_i < n$ et $m_i \mid n$), donc $n - 1 \geq \frac{sn}{2}$, *ie* $2n > sn$ d'où $s = 1$ et $n = m_1$ ce qui est impossible : l'hypothèse G simple est contradictoire.
(4) Posons $m = \# H$. D'après la question (2), le groupe H est cyclique : il est isomorphe à $\mathbf{Z}/m\mathbf{Z}$. On a donc $\mathsf{Aut}(H) \simeq \mathsf{Aut}(\mathbf{Z}/\mathbf{Z}) \simeq (\mathbf{Z}/m\mathbf{Z})^\times$, de sorte que $\# \mathsf{Aut}(H) = \varphi(m)$. Par ailleurs, on a $\mathrm{pgcd}(n, \varphi(m)) = 1$ (*cf* question (2)). Cela montre que $\# \mathsf{Aut}(H)$ est premier à n.
(5) La question précédente implique que le morphisme ρ est trivial. Cela signifie que l'action de G sur H par conjugaison est trivial, ce qui veut précisément dire que $H \subset \mathsf{Z}(G)$.
(6) Posons $d = (G : H)$: c'est un diviseur de n. Comme dans la question (2), cela implique que $\mathsf{pgcd}(d, \varphi(d)) = 1$: comme $d < n$ (parce que $\mathsf{Z}(G)$ n'est pas trivial vu qu'il contient H), l'hypothèse de récurrence s'applique, et $G/\mathsf{Z}(G)$ est cyclique. On sait alors que G est abélien.
(7) Soit $x \in G \setminus \{e\}$. Le groupe quotient $G/\langle x \rangle$ est cyclique : il existe $y \in G$ tel que $G/\langle x \rangle$ soit engendré par l'image de y. Quitte à remplacer y par une puissance convenable, on peut supposer que y est d'ordre $(G : \langle x \rangle)$. Les ordres de x et de y sont alors premiers entre eux, et de produit égal à n : comme G est abélien, l'élément xy est d'ordre n, et G est cyclique.
(8) Supposons que $\mathsf{pgcd}(n, \varphi(n)) \neq 1$. Si n est divisible par un carré, on peut écrire $n = ab$ avec $a, b \in \mathbf{N}_{>0}$ et $\mathsf{pgcd}(a, b) \neq 1$: le groupe $(\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z})$ est d'ordre n et non cyclique. Supposons désormais que n est sans facteur carré : il existe p premier tel que $n = pm$ et $p \mid \varphi(n) = (p-1)\varphi(m)$ (parce que $p \nmid m$), d'où $p \mid \varphi(m)$. Soit $\alpha \in (\mathbf{Z}/m\mathbf{Z})^\times$ un élément d'ordre p : le noyau du morphisme $\mathbf{Z} \to (\mathbf{Z}/m\mathbf{Z})^\times$; $k \mapsto \alpha^k$ est $p\mathbf{Z}$. Il se factorise donc en un morphisme de groupes $f\colon \mathbf{Z}/p\mathbf{Z} \to (\mathbf{Z}/m\mathbf{Z})^\times \simeq \mathsf{Aut}_{\mathsf{gr}}(\mathbf{Z}/m\mathbf{Z})$ tel que $f(\overline{1}) = \alpha$. On dispose alors du produit semi-direct externe $G = (\mathbf{Z}/m\mathbf{Z}) \rtimes_f (\mathbf{Z}/p\mathbf{Z})$. Il est d'ordre n, et la loi de groupe est donnée par $(x_1, y_1) \cdot (x_2, y_2) = (x_1 + f(y_1)(x_2), y_1 + y_2)$. En particulier, on a $(\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0}) = (\alpha, \overline{1})$ et $(\overline{1}, \overline{0}) \cdot (\overline{0}, \overline{1}) = (\overline{1}, \overline{1})$: comme $\alpha \neq \overline{1}$, cela montre que G n'est pas abélien, *a fortiori* non cyclique.