Corrigé du partiel de mathématiques générales du 21/10/24

Exercice 1 : Vrai ou faux ? (8 points)

a) C'est faux. Par exemple, si G est le groupe additif $(\mathbf{Z}/p\mathbf{Z})^2$, il n'y a pas d'élément d'ordre p^2 vu que tout x de G vérifie $px = 0$ (1 point).

b) C'est vrai. Si G n'était pas un p-groupe, son cardinal serait divisible par un nombre premier $\ell \neq p$. D'après le théorème de Sylow, G aurait alors un sous-groupe d'ordre ℓ^m avec $m > 0$, dont un élément non nul aurait pour ordre ℓ^r avec $r > 0$. Or, l'hypothèse implique que l'ordre de tout élément de G est une puissance de p, d'où une contradiction (1.5 point).

c) C'est vrai. Un morphisme de G dans A avec A abélien est trivial sur les commutateurs, donc aussi sur le sous-groupe $D(G)$ qu'ils engendrent. Du coup, si $G = D(G)$, un tel morphisme est trivial. En sens inverse, si $D(G) \neq G$, alors la surjection canonique $G \to G/D(G)$ est un morphisme non trivial à valeurs dans un groupe abélien (1.5 point).

d) C'est faux. Prendre par exemple $G = \mathcal{A}_n$ et $G' = \mathcal{S}_n$, alors l'inclusion de G dans G' est un morphisme injectif. Or, il n'y a pas de morphisme surjectif de $\mathcal{S}_n$ dans $\mathcal{A}_n$ pour $n \geq 5$, sinon on aurait $\mathcal{S}_n/\ker f$ isomorphe à $\mathcal{A}_n$, or les seuls sous-groupe distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{S}_n$ et $\mathcal{A}_n$, donc les quotients de $\mathcal{S}_n$ sont de cardinal 1, 2, ou $n!$ et non $n!/2$ (1.5 point).

e) C'est vrai, car toute orbite (et donc ici X, qui est la seule orbite) est en bijection avec un ensemble G/Stab_x de classes à gauche, qui est fini de cardinal divisant celui de G (1 point).

f) C'est vrai. En effet, l'opération fidèle donne un morphisme injectif de G dans $\mathtt{Aut}\,(\mathbf{Z}/27\mathbf{Z}) \simeq (\mathbf{Z}/27\mathbf{Z})^*$. Comme $27 = 3^3$, on sait que $(\mathbf{Z}/27\mathbf{Z})^*$ est cyclique, or tout sous-groupe d'un groupe cyclique est cyclique (1.5 point).

Exercice 2 : Automorphismes et groupes symétriques (12 points)

a) Déjà, $\mathrm{Int}\,(G)$ est un sous-groupe de $\mathtt{Aut}\,(G)$, car c'est l'image de G par le morphisme int de G dans $\mathtt{Aut}\,(G)$ qui envoie $a \in G$ sur l'automorphisme intérieur $\mathrm{int}_a : x \mapsto axa^{-1}$. Soit maintenant $u \in \mathtt{Aut}\,(G)$ et $\mathrm{int}_a \in \mathrm{Int}\,(G)$, montrons que $u \circ \mathrm{int}_a \circ u^{-1}$ est encore un élément de $\mathrm{Int}\,(G)$. On calcule, pour $x \in G$,

$$(u \circ \mathrm{int}_a \circ u^{-1})(x) = u(au^{-1}(x)a^{-1}) = u(a)xu(a)^{-1} = \mathrm{int}_{u(a)}(x),$$

ce qui montre que $u \circ \mathrm{int}_a \circ u^{-1} = \mathrm{int}_{u(a)}$ est bien dans $\mathrm{Int}\,(G)$. Ainsi $\mathrm{Int}\,(G)$ est un sous-groupe distingué de $\mathtt{Aut}\,(G)$ (1.5 point).

b) Par définition, le noyau de int est Z et son image est $\mathrm{Int}\,(G)$, d'où le résultat avec le théorème de factorisation (0.5 point).

c) Soit f l'automorphisme $A \mapsto {}^tA^{-1}$ de G dans G (c'est un morphisme qui est son propre inverse), alors il ne peut y avoir d'élément P de G tel que $f(A) = PAP^{-1}$ pour tout A, sinon A serait toujours semblable à ${}^tA^{-1}$, ce qui n'est par exemple pas vrai pour $A = 2I_n$ (1.5 point).

d) On sait que les transpositions engendrent $\mathcal{S}_n$. Il suffit donc de montrer que toute transposition (i, j) est produit de transpositions de la forme $(1, i)$. C'est clair si $i = 1$ ou $j = 1$, sinon on observe que $(i, j) = (1, j)(1, i)(1, j)$, d'où le résultat (1 point).

e) Comme $(1, 2)$ et $(1, 3)$ ne commutent pas, leurs images τ_2 et τ_3 par l'automorphisme φ non plus. Comme τ_2 et τ_3 sont par hypothèse des transpositions, leurs supports ne sont pas disjoints, ce qui permet d'écrire $\tau_2 = (\alpha_1, \alpha_2)$ et $\tau_3 = (\alpha_1, \alpha_3)$, la condition $\alpha_2 \neq \alpha_3$ venant de ce que $\tau_1 \neq \tau_2$ vu que $(1, 2) \neq (1, 3)$ (1.5 point).

f) Supposons donc $\tau_k = (\alpha_2, \alpha_3)$. Alors

$$\tau_2 \circ \tau_k = (\alpha_1, \alpha_2)(\alpha_2, \alpha_3) = (\alpha_1, \alpha_2, \alpha_3)$$

et

$$(\tau_3 \circ \tau_k) = (\alpha_1, \alpha_3)(\alpha_2, \alpha_3) = (\alpha_1, \alpha_3, \alpha_2),$$

ce qui montre que $(\tau_2 \circ \tau_k)$ est l'inverse de $(\tau_3 \circ \tau_k)$. Or, ceci n'est pas possible car leurs antécédents respectifs $(1, 2)(1, k) = (2, 1, k)$ et $(1, 3)(1, k) = (3, 1, k)$ ne sont pas inverses l'un de l'autre, vu que $k \geq 4$ (2 points).

g) Comme $(1, k)$ ne commute pas avec $(1, 2)$ ni avec $(1, 3)$, son image τ_k par φ ne commute ni avec τ_1 ni avec τ_2, donc n'a son support disjoint ni avec τ_1 ni avec τ_2. Du coup, τ_k doit avoir α_1 dans son support, sinon on aurait $\tau_k = (\alpha_2, \alpha_3)$, contradiction avec f). Le fait que les α_k pour $k = 1, ..., n$ soient deux à deux distincts vient alors de ce que $\tau_2, ..., \tau_n$ sont des transpositions deux à deux distinctes (1.5 point).

h) D'après g), φ et int_u coincident sur tous les $(1, i)$ avec $2 \leq i \leq n$, donc d'après d) ils coincident sur $\mathcal{S}_n$ tout entier (1 point).

i) Dans le cas $n = 3$, l'image d'une transposition par φ (qui doit être d'ordre 2) est forcément une transposition. Ainsi d'après h), on a $\texttt{Aut}\,(\mathcal{S}_3) = \operatorname{Int}(\mathcal{S}_3)$, lequel est isomorphe au quotient de $\mathcal{S}_3$ par son centre d'après b). Or, on sait que ce centre est trivial, d'où le résultat (1.5 point).