Contrôle continu 2

Exercice 1 (≈ 6 points)

Soit G un groupe. On note $Z(G)$ le centre de G et $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G. On rappelle que $(\mathrm{Aut}(G), \circ)$ est un groupe. Pour tout $g \in G$, on note $\Phi(g) = \phi_g$ l'application de G dans G définie par $\phi_g(x) = gxg^{-1}$.

1. Montrer que pour tout $g \in G$, $\phi_g \in \mathrm{Aut}(G)$.
2. Montrer que Φ est un morphisme de G dans $\mathrm{Aut}(G)$. Quel est le noyau de Φ ? En déduire un groupe isomorphe à $\Phi(G)$.
3. Montrer que $\Phi(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.
4. Dans cette question, on suppose que G est fini.
   (a) Montrer que $\mathrm{Aut}(G)$ est fini.
   (b) Que sait-on sur l'ordre de $\Phi(G)$?
   (c) En déduire que si les ordres de G et de $\mathrm{Aut}(G)$ sont premiers entre eux, alors G est abélien.

Exercice 2 ($\approx 7,5$ points)

Soit G un groupe d'ordre fini n. Pour tout élément g de G, on note $o(g)$ l'ordre de g, $\sigma_g : x \mapsto gx$ la *translation à gauche* par g et $\phi_g : x \mapsto gxg^{-1}$ la *conjugaison* par g. On note $\mathrm{inv} : x \mapsto x^{-1}$ l'application qui à un élément de G associe son inverse. On rappelle que ces applications sont des permutations de G. Pour toute permutation σ de G, on note $\varepsilon(\sigma)$ la signature de σ.

1. (a) Soit $x \in G$. On note $O_{\sigma_g}(x)$ l'orbite de x sous l'action de σ_g. Donner la liste des éléments de $O_{\sigma_g}(x)$ et le cardinal de $O_{\sigma_g}(x)$.
   (b) En déduire le nombre d'orbites de σ_g, et le fait que $\varepsilon(\sigma_g) = (-1)^{n-n/o(g)}$.
   (c) Lorsque n est impair, montrer que $\varepsilon(\sigma_g) = 1$.
   (d) Lorsque n est pair, montrer que $\varepsilon(\sigma_g) = 1$ si $o(g)$ divise $n/2$ et $\varepsilon(\sigma_g) = -1$ sinon.
   (e) En déduire que lorsque n est pair, l'ensemble $H = \{g \in G : g^{n/2} = 1\}$ est un sous-groupe de G, et montrer que H est d'indice 1 ou 2 dans G.
2. (a) Sans calcul, que peut-on dire du nombre et du cardinal des orbites de la permutation $\mathrm{inv} \circ \sigma_g \circ \mathrm{inv}$?
   (b) Pour $x \in G$, expliciter $\big(\mathrm{inv} \circ \sigma_g \circ \mathrm{inv}\big)(x)$ puis $\big(\sigma_g \circ \mathrm{inv} \circ \sigma_g \circ \mathrm{inv}\big)(x)$.
   (c) En déduire que $\varepsilon(\phi_g) = 1$.
   (d) Montrer que le cardinal de chaque orbite de ϕ_g divise $o(g)$.
   (e) Notons $C_g = \{x \in G : gxg^{-1} = x\}$. Montrer que si g est d'ordre 2, alors $|G| - |C_g|$ est multiple de 4.

Exercice 3

Soient p et q deux nombres premiers tels que $q < p$. Soit G un groupe d'ordre pq. On suppose que G n'est pas cyclique. Le but de l'exercice est de montrer que q divise $p-1$. On note E_p (respectivement E_q) l'ensemble des éléments d'ordre p (respectivement q) et $\mathcal{G}_p$ (respectivement $\mathcal{G}_q$) l'ensemble des sous-groupes d'ordre p (respectivement q) dans G. Le théorème de Cauchy assure que E_p et E_q sont non vides. On fixe $a \in E_q$ et $b \in E_p$.

1. Montrer que $|E_p| = (p-1)|\mathcal{G}_p|$. On pourra considérer l'application $f : x \mapsto \langle x \rangle$ de E_p dans $\mathcal{G}_p$.
2. Montrer que $(p-1)|\mathcal{G}_p| + (q-1)|\mathcal{G}_q| = pq - 1$.
3. En déduire que $|\mathcal{G}_p| \leq q$.
4. Dans cette question, on montre que si $H \in \mathcal{G}_p$, alors H est distingué dans G. Pour cela, on pose $g \cdot H = gHg^{-1}$ pour tout $g \in G$.
   (a) Montrer qu'on obtient ainsi une action de groupe de G sur $\mathcal{G}_p$. Dans la suite, on note ρ_g l'application de $\mathcal{G}_p$ dans $\mathcal{G}_p$ définie par $\rho_g(H) = gHg^{-1}$. On rappelle que l'application $\rho : g \mapsto \rho_g$ est un morphisme de groupes de G dans $\mathfrak{S}(\mathcal{G}_p)$.
   (b) Montrer que pour tout $g \in E_p$, $\rho_g^p = \mathrm{id}_{\mathcal{G}_p}$. En déduire que $\rho_g = \mathrm{id}_{\mathcal{G}_p}$ (indication : on rappelle que $|\mathcal{G}_p| \leq q < p$).
   (c) En déduire que le noyau de l'action, $\mathrm{Ker}\ \rho = \{g \in G : \rho_g = \mathrm{id}_{\mathcal{G}_p}\}$ est G tout entier et conclure. Indication : si $\mathcal{G}_p$ n'est pas un singleton, alors $\mathrm{Ker}\ \rho$ contient au moins $2p-1$ éléments.
5. En déduire que $aba^{-1} = b^r$ avec $r \in [\![0, p-1]\!]$
6. Montrer que l'entier r ci-dessus ne vaut ni 0 ni 1.
7. Montrer que pour tout $k \in \mathbb{N}$, $a^k b a^{-k} = b^{r^k}$
8. En déduire que la classe de r dans $\mathbb{Z}/p\mathbb{Z}$ (que l'on notera $\overline{r}$) est d'ordre q dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ et conclure.

Contrôle continu 2

Exercice 1 (1+1,5+1+0,5+1+1 = 6 points)

1. Soit $g \in G$. Pour tous $x, y \in G$, $\phi_g(xy) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \phi_g(x)\phi_g(y)$. Donc ϕ_g est bien un morphisme de groupes de G dans lui-même, et il est bijectif puisque $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \mathrm{id}_G$.
2. D'après la question précédente, Φ est bien à valeurs dans $\mathrm{Aut}(G)$. D'après le cours, $\mathrm{Aut}(G)$ est un groupe. Pour tous $g, g' \in G$ et tout $x \in G$, on a

   $$\Phi(gg')(x) = \phi_{gg'}(x) = gg'xg'^{-1}g^{-1} = g\phi_{g'}(x)g^{-1} = (\phi_g \circ \phi_{g'})(x) = (\Phi(g) \circ \Phi(g'))(x),$$

   donc Φ est un morphisme de G dans $\mathrm{Aut}(G)$. Par ailleurs,

   $$\mathrm{Ker}\Phi = \{g \in G : \forall x \in G, gxg^{-1} = x\} = \{g \in G : \forall x \in G, gx = xg\} = Z(G).$$

   D'après le théorème d'isomorphisme, $\Phi(G)$ est donc isomorphe à $G/Z(G)$.
3. $\Phi(G)$ est un sous-groupe de $\mathrm{Aut}(G)$ comme image de G par un morphisme de groupes de G dans $\mathrm{Aut}(G)$. Soient $g \in G$ et $\psi \in \mathrm{Aut}(G)$. Alors pour tout $x \in G$,

   $$(\psi \circ \phi_g \circ \psi^{-1})(x) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)x\psi(g)^{-1} = \phi_{\psi(g)}(x),$$

   donc $\psi \circ \phi_g \circ \psi^{-1} = \phi_{\psi(g)}$ est bien un élément de $\Phi(G)$. Ainsi, $\Phi(G)$ est bien un sous-groupe distingué de $\mathrm{Aut}(G)$.
4. (a) L'ensemble des automorphismes $\mathrm{Aut}(G)$ est un sous-groupe du groupe des permutations de G, qui est fini de cardinal $|G|!$. C'est donc un ensemble fini.
   (b) Comme $\Phi(G) \simeq G/Z(G)$, $|\Phi(G)| = |G|/|Z(G)|$ divise l'ordre de G, et d'autre part $|\Phi(G)|$ divise $|\mathrm{Aut}(G)|$ puisque $\Phi(G)$ est un sous-groupe de $\mathrm{Aut}(G)$.
   (c) On déduit de la question précédente que si les ordres de G et $\mathrm{Aut}(G)$ sont premiers entre eux, alors $|\Phi(G)| = 1$ d'où $Z(G) = G$, i.e. G est abélien.

Exercice 2 ((1,5+0,5+0,5+1+1,5) + (1+1+1+1+2) = 5+6 = 11 points)

(a) Soit $x \in G$. Pour tout $k \in \mathbb{Z}$,

$$\sigma_g^k(x) = x \iff g^k x = x \iff g^k = 1_G \iff o(k)|x$$

Donc l'orbite de x pour σ_g a exactement $o(g)$ éléments : $x, gx, \ldots, g^{o(g)-1}x$.

(b) Toutes les orbites de σ_g ont pour cardinal $o(g)$, donc d'après l'équation aux classes, il y a $n/o(g)$ orbites. Autrement dit, σ_g se décompose en $n/o(g)$ cycles disjoints de longueur $o(g)$, $\varepsilon(\sigma_g) = ((-1)^{(o(g)-1)})^{n/o(g)} = (-1)^{n-n/o(g)}$.

(c) Si n est impair, l'entier $n/o(g)$ est impair, $n - n/o(g)$ est pair donc $\varepsilon(\sigma_g) = 1$.

(d) Si n est pair, $n - n/o(g)$ a même parité que $n/o(g)$ donc $\varepsilon(\sigma_g) = (-1)^{n/o(g)}$. Ainsi,

$$\begin{aligned} \varepsilon(\sigma_g) = 1 &\iff \exists k \in \mathbb{N} : n/o(g) = 2k \\ &\iff \exists k \in \mathbb{N} : n/2 = ko(g) \\ &\iff o(g) | (n/2) \end{aligned}$$

Autrement dit, $\varepsilon(\sigma_g) = 1$ si $o(g)$ divise $n/2$ et $\varepsilon(\sigma_g) = -1$ sinon.

(e) D'après la question précédente, pour tout $g \in G$

$$\varepsilon(\sigma_g) = 1 \iff o(g)|(n/2) \iff g^{n/2} = 1_G.$$

Remarquons que l'application $\sigma : g \mapsto \sigma_g$ est un morphisme de groupe de G dans $\mathfrak{S}(G)$. Donc $H = \{g \in G : g^{n/2} = 1\} = \{g \in G : \varepsilon(\sigma_g) = 1\}$ est le noyau du morphisme de groupes $\varepsilon \circ \sigma$. En particulier, H est un sous-groupe (distingué) de G. D'après le théorème d'isomorphisme $[G : H] = |\mathrm{Im}(\varepsilon \circ \sigma)|$. Comme $\mathrm{Im}(\varepsilon \circ \sigma)$ est un sous-groupe de $\{-1, 1\}$, le sous-groupe H est d'indice 1 ou 2 dans G.

1. (a) Comme la permutation inv est d'ordre 2, la permutation $\mathrm{inv} \circ \sigma_g \circ \mathrm{inv}$ est conjuguée à σ_g. Donc comme σ_g, elle a exactement $n/o(g)$ orbites, toutes de cardinal $o(g)$.

(b) Soit $x \in G$. Alors $\big(\mathrm{inv} \circ \sigma_g \circ \mathrm{inv}\big)(x) = (gx^{-1})^{-1} = xg^{-1}$ donc

$$\big(\sigma_g \circ \mathrm{inv} \circ \sigma_g \circ \mathrm{inv}\big)(x) = gxg^{-1}.$$

(c) D'après la question précédente, $\phi_g = (\sigma_g \circ \mathrm{inv})^2$. Comme ε est un morphisme de groupes de $\mathfrak{S}(G)$ dans $\{-1, 1\}$, on a donc $\varepsilon(\phi_g) = \varepsilon(\sigma_g \circ \mathrm{inv})^2 = 1$.

(d) Comme $\phi_g^{o(g)} = \phi_{g^{o(g)}} = \phi_{1_G} = \mathrm{id}_G$, l'ordre de la permutation ϕ_g divise $o(g)$. Donc le cardinal de chaque orbite de ϕ_g divise $o(g)$.

(e) Si g est d'ordre 2, les orbites de ϕ_g sont de cardinal 1 ou 2, donc ϕ_g est un produit de transpositions à supports disjoints, en nombre pair puisque $\varepsilon(\phi_g) = 1$. Comme C_g est l'ensemble des points fixes de ϕ_g, $|G| - |C_g|$ vaut deux fois le nombre d'orbites de taille 2, et est multiple de 4.

Exercice 3 (1,5 + 2,5 + 1 + (1,5 + 1,5 + 2) + 1,5 + 2 + 3 = 16,5 points)

1. On a vu en TD que tout groupe d'ordre p premier est cyclique et est engendré par n'importe quel de ses éléments autre que le neutre (mais bien sûr pas par le neutre ni par par un élément hors du groupe). Pour tout $x \in G$ et $H \in \mathcal{G}_p$, on a donc $\langle x \rangle = H$ si et seulement si $x \in H \setminus \{1_G\}$. Tout élément de $\mathcal{G}_p$ a exactement $p - 1$ images réciproques par l'application $f : x \mapsto \langle x \rangle$ de E_p dans $\mathcal{G}_p$. Donc $|E_p| = (p - 1)|\mathcal{G}_p|$.

2. De même, on a $|E_p| = (q-1)|\mathcal{G}_q|$. Or l'ordre de tout élément de G divise pq (Lagrange), donc vaut 1, p, q ou pq. Comme G n'est pas cyclique, il n'y a pas d'élément d'ordre pq. Comme 1_G est le seul élément d'ordre 1, on a ainsi $(p-1)|\mathcal{G}_p| + (q-1)|\mathcal{G}_q| = |E_p| + |E_q| = |G \setminus \{1_G\}| = pq - 1$.
3. Comme $|\mathcal{G}_q| \geq 1$ puisque G a au moins un élément d'ordre q, l'égalité précédente montre que $(p-1)|\mathcal{G}_p| \leq (pq-1) - (p-1) = pq - q$ donc $|\mathcal{G}_p| \leq q$.
4. (a) Pour tous g dans G et $H \in \mathcal{G}_p$, $g \cdot H = gHg^{-1}$ est bien dans $\mathcal{G}_p$ comme image d'un sous-groupe d'ordre p par un automorphisme de G. Pour tous g, g' dans G et $H \in \mathcal{G}_p$, on a $1_G \cdot H = 1_G H 1_G^{-1} = H$ et
$$g \cdot (g' \cdot H) = g(g'H)g'^{-1}g^{-1} = (gg')H(gg')^{-1} = (gg') \cdot H.$$
Donc on a bien une action de groupe de G sur $\mathcal{G}_p$.

   (b) Soit $g \in E_p$. Alors $\rho_g^p = \rho_{g^p} = \rho_{1_G} = \mathrm{id}_{\mathcal{G}_p}$. Comme p est premier, ρ_g est d'ordre 1 ou p. Comme l'ordre de la permutation ρ_g est le PPCM de la longueur des cycles dans sa décomposition en cycles disjoints, les cyles éventuels sont de longueur p, ce qui est impossible car $|\mathcal{G}_p| \leq q < p$. Donc $\rho_g = \mathrm{id}_{\mathcal{G}_p}$.

   (c) Si $\mathcal{G}_p$ est pas un singleton, alors $\mathcal{G}_\mathfrak{p}$ est réduit à $\{\mathrm{id}_{\mathcal{G}_p}\}$ donc le noyau Ker ρ est G tout entier. Remarque : en fait, avec les théorèmes de Sylow, on peut montrer que seul ce cas se produit.

   Si $\mathcal{G}_p$ n'est pas un singleton, alors comme le noyau de l'action contient 1_G et tous les éléments de E_p (d'après la question précédente), il contient donc au moins $2(p-1)+1 = 2p-1$ éléments. Or $|\mathrm{Ker}\ \rho|$ divise $|G| = pq$ (Lagrange) donc vaut 1, p, q ou pq. Comme $2p-1 > p > q > 1$, Ker ρ est G tout entier.

   Dans tous les cas, l'action ρ est triviale.
5. Comme b est d'ordre p, la question précédente montre que le sous-groupe $\langle b \rangle$ est distingué dans G, donc $aba^{-1} \in \langle b \rangle$, i.e. $aba^{-1} = b^r$ avec $r \in [\![0, p-1]\!]$
6. Si l'entier r ci-dessus valait 0, aba^{-1} serait égal à 1_G, donc b serait égal à $a^{-1}1_G a = 1_G$, ce qui contredirait le fait que $o(b) = p$. Si l'entier r ci-dessus valait 1, les éléments a et b commuteraient. Comme il sont d'ordres q et p premiers entre eux, ab serait d'ordre pq, ce qui contredirait le fait que G, n'est pas cyclique. Ainsi $r \in [\![2, p-1]\!]$.
7. Montrons par récurrence que pour tout $k \in \mathbb{N}$, $a^k b a^{-k} = b^{r^k}$.
   Lorsque $k = 0$, l'égalité est vraie car $a^k = a^{-k} = 1_G$ et $r^k = 1$.
   Lorsque $k = 1$, l'égalité est vraie d'après la question 5.
   Fixons $k \geq 1$. Si l'égalité est vraie au rang k, alors comme la conjugaison $\phi_a : x \mapsto axa^{-1}$ est un automorphisme de G, on peut écrire
$$a^{k+1} b a^{-(k+1)} = \phi_a(a^k b a^{-k}) = \phi_a(b^{r^k}) = \phi_a(b)^{r^k} = (b^r)^{r^k} = b^{r^{k+1}},$$
   ce qui montre l'égalité au rang $k+1$ et achève la récurrence.

8. Avec la question précédente et l'égalité $a^q = 1$, on obtient $b^{r^q} = a^q b a^{-q} = b$, donc $b^{r^q-1} = 1_G$. Autrement dit, p divise $r^q - 1$ puisque b est d'ordre p.
   Dans $\mathbb{Z}/p\mathbb{Z}$, on a donc $\overline{r}^q = \overline{1}$. Donc $\overline{r}$ appartient au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ et son ordre dans ce groupe divise q. Or $\overline{r} \neq \overline{1}$ puisque $r \in [\![2, p-1]\!]$ et q est premier donc $\overline{r}$ est d'ordre q. D'après le théorème de Lagrange, q divise donc l'ordre de $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est $p-1$ puisque p est premier.