Contrôle continu 2

Documents et calculatrices non-autorisés.
Les exercices sont indépendants.

Barème indicatif : 3 (question de cours) + 6 (exercice) + 11 (problème) = 20 points.

Question de cours

1. On considère une action d'un groupe G sur un ensemble E. Soit $x \in E$.
   (a) Donner la définition du stabilisateur de x, noté $\mathrm{Stab}(x)$, et de l'orbite de x, notée $\mathrm{Orb}(x)$.
   (b) Montrer que pour tout $g \in G$ et $x \in E$, $\mathrm{Stab}(g \cdot x) = g\mathrm{Stab}(x)g^{-1}$.
   (c) Lorsque G est fini, quelle relation y a -t-il entre $|\mathrm{Stab}(x)|$ et $|\mathrm{Orb}(x)|$?
2. Soit E un ensemble fini à n éléments. Indiquer comment contruire un isomorphisme de $\mathfrak{S}_n$ vers $\mathfrak{S}(E)$.

Exercice

Soient $X = \{1, 2, 3, 4, 5\}$ et $\mathcal{E}$ l'ensemble des paires $\{a, b\}$ où a et b sont deux éléments de X distincts.

1. Montrer qu'on définit bien une action de $\mathfrak{S}_5$ sur $\mathcal{E}$ par $\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$.
2. Montrer que cette action est transitive.
3. Établir un isomorphisme entre $\mathrm{Stab}(\{1, 2\})$ et $\mathfrak{S}_2 \times \mathfrak{S}_3$.
4. Plus généralement, montrer que pour tout $\{a, b\} \in \mathcal{E}$, $\mathrm{Stab}(\{a, b\})$ est isomorphe à $\mathfrak{S}_2 \times \mathfrak{S}_3$.
5. L'action de $\mathfrak{S}_5$ sur $\mathcal{E}$ fournit un morphisme de groupes φ de $\mathfrak{S}_5$ dans $\mathfrak{S}(\mathcal{E})$. Ce morphisme est-il surjectif ?
6. Montrer que le morphisme φ est injectif.
7. Exhiber un morphisme de groupes injectif $\psi : \mathfrak{S}_5 \to \mathfrak{S}(\mathcal{E})$ autre que φ.

Suite au dos

Problème

Soit G un groupe fini d'ordre n. Pour tout diviseur premier p de n, on note E_p l'ensemble des éléments d'ordre p dans G, $\mathcal{G}_p$ l'ensemble des sous-groupes d'ordre p et $N_p = |\mathcal{G}_p|$.

1. On considère l'application $f_p : g \mapsto \langle g \rangle$ de E_p dans $\mathcal{G}_p$.
   (a) Montrer que chaque élément de $\mathcal{G}_p$ a exactement $p-1$ antécédents par f_p.
   (b) En déduire que $|E_p| = (p-1)N_p$.
2. Dans cette question on suppose que G contient deux sous-groupes H et K tels que H soit distingué dans G et les ordres $|K|$ et $|\mathrm{Aut}(H)|$ soient deux entiers premiers entre eux.
   (a) Montrer que K agit sur H par conjugaison.
   (b) En déduire un morphisme de groupes $\varphi : K \to \mathrm{Aut}(H)$.
   (c) Montrer que $|\mathrm{Im}(\varphi)|$ divise $|K|$ et $|\mathrm{Aut}(H)|$.
   (d) En déduire que pour tout $k \in K$ et $h \in H$, $kh = hk$.
3. Dans cette question, on prend $n = 35$. On cherche à montrer que G est cyclique. On procède par l'absurde, en supposant que G n'est pas cyclique.
   (a) En raisonnant sur les ordres des éléments de G, montrer que $4N_5 + 6N_7 = 34$. En déduire que $\mathcal{G}_5$ et $\mathcal{G}_7$ ne sont pas vides et que $N_7 \leq 5$.
   (b) On fixe $A \in \mathcal{G}_7$ et $B \in \mathcal{G}_5$. On cherche à montrer que A ou B est distingué. On suppose donc dans cette question que A n'est pas distingué.
      i. Montrer que G agit sur $\mathcal{G}_7$ par conjugaison.
      ii. En étudiant l'orbite de A, en déduire que $N_7 \geq 5$.
      iii. En déduire que B est distingué dans G.
   (c) En déduire que pour tout $a \in A$ et $b \in B$, $ab = ba$.
   (d) Obtenir une contradiction et conclure.

Corrigé de la question de cours

Comme E a n éléments, il existe une bijection de $[\![1, n]\!]$ dans E. On vérifie que l'application $\sigma \mapsto f \circ \sigma \circ f^{-1}$ est un isomorphisme de $\mathfrak{S}_5$ vers $\mathfrak{S}_5(E)$.

Corrigé de l'exercice

1. Pour tout $\{a, b\} \in \mathcal{E}$, pour tout σ et σ' dans $\mathfrak{S}_5$, on a
   — $\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\} \in \mathcal{E}$.
   — $\mathrm{id} \cdot \{a, b\} = \{a, b\}$.
   — $\sigma' \cdot (\sigma \cdot \{a, b\}) = \sigma' \cdot \{\sigma(a), \sigma(b)\} = \{\sigma'(\sigma(a)), \sigma'(\sigma(b))\} = (\sigma' \circ \sigma) \cdot \{a, b\})$.
   Donc on a bien une action de $\mathfrak{S}_5$ sur $\mathcal{E}$.
2. Soient $\{a, b\} \in \mathcal{E}$. Notons $\{c, d, e\} = \{1, 2, 3, 4, 5\} \setminus \{a, b\}$. Soit σ la permutation qui envoie respectivement $1, 2, 3, 4, 5$ sur a, b, c, d, e. Alors $\sigma \cdot \{1, 2\} = \{a, b\}$. L'orbite de $\{1, 2\}$ est $\mathcal{E}$ tout entier, donc l'action est transitive.
3. Soit $\sigma \in \mathrm{Stab}(\{1, 2\})$. Alors σ préserve globablement $A := \{1, 2\}$ et aussi son complémentaire $B := \{3, 4, 5\}$. Donc σ induit donc deux permutations $\sigma_A \in \mathfrak{S}(A)$ et $\sigma_B \in \mathfrak{S}(B)$. L'application $\sigma \mapsto (\sigma_A, \sigma_B)$ est un morphisme de $\mathrm{Stab}(\{1, 2\})$ vers $\mathfrak{S}(A) \times \mathfrak{S}(B)$. Ce morphisme est bijectif : la bijection réciproque envoie tout $(\sigma_1, \sigma_2) \in \mathfrak{S}(A) \times \mathfrak{S}(B)$ sur l'unique permutation sur $\{1, 2, 3, 4, 5\}$ qui prolonge à la fois σ_1 et σ_2. Mais $\mathfrak{S}(A)$ et $\mathfrak{S}(B)$ sont isomorphes à $\mathfrak{S}_2$ et $\mathfrak{S}_3$ (voir question de cours 2). Par produit cartésien et par composition, on en déduit un isomorphisme de $\mathrm{Stab}(\{1, 2\})$ vers $\mathfrak{S}_2 \times \mathfrak{S}_3$.

   Autre rédaction possible : soit H_A le sous-groupe de $\mathfrak{S}_5$ formé des permutations dont le support est inclus dans A. Définissons pareillement H_B. Comme les éléments de H_A sont exactement les permutations obtenues en prolongeant les permutations sur A par l'identité sur B (et comme l'opération consistant à prolonger par l'identité sur B est un morphisme injectif pour la loi $\circ$), H_A est isomorphe à $\mathfrak{S}(A)$, donc à $\mathfrak{S}_2$. De même, H_B est isomorphe à $\mathfrak{S}(B)$, donc à $\mathfrak{S}_3$. Ainsi, $H_A \times H_B$ est isomorphe à $\mathfrak{S}_2 \times \mathfrak{S}_3$. Or pour tout $(\sigma_1, \sigma_2) \in H_A \times H_B$, $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ (car les supports sont disjoints) et cette composée est dans $\mathrm{Stab}(A)$ puisque σ_1 et σ_2 le sont. Donc l'application $(\sigma_1, \sigma_2) \mapsto \sigma_1 \circ \sigma_2$ de $H_A \times H_B$ dans $\mathrm{Stab}(A)$ est un morphisme de groupes. Ce morphisme est bijectif : la bijection réciproque envoie $\sigma \in \mathrm{Stab}(A)$ sur (σ_1, σ_2), où σ_1 est la permutation qui coïncide avec σ sur A et avec l'identité sur B, σ_2 est la permutation qui coïncide avec σ sur B et avec l'identité sur A. Ainsi, $\mathrm{Stab}(A)$ est isomorphe à $H_A \times H_B$, donc à $\mathfrak{S}_2 \times \mathfrak{S}_3$.
4. Soit $\{a, b\} \in \mathcal{E}$. La question 2 fournit une permutation σ la permutation telle que $\sigma \cdot \{1, 2\} = \{a, b\}$. D'après la question de cours 1b, L'automorphisme intérieur associé à σ envoie $\mathrm{Stab}(\{1, 2\})$ sur $\mathrm{Stab}(\{a, b\})$. Ainsi, $\mathrm{Stab}(\{a, b\})$ est isomorphe à $\mathrm{Stab}(\{1, 2\})$ donc à $\mathfrak{S}_2 \times \mathfrak{S}_3$. On peut aussi prouver le résultat directement en adaptant la preuve de la question précédente : poser $A = \{a, b\}$ et B égal au complémentaire de A dans $\{1, 2, 3, 4, 5\}$.

5. Comme $|\mathcal{E}| = \binom{5}{2} = 10$, on a $|\mathfrak{S}(\mathcal{E})| > |\mathfrak{S}_5|$ donc φ ne peut pas être surjectif. Autre argument : la transposition qui échange $\{1,2\}$ et $\{4,5\}$ n'est pas dans l'image de φ. En effet, pour qu'une permutation $s \in \mathfrak{S}(\mathcal{E})$ soit dans l'image de φ, il faut que $s(\{1,2\}) \cap s(\{1,3\})$ soit un singleton, puisque pour tout $\sigma \in \mathfrak{S}_5$,
$$\{\sigma(1), \sigma(2)\} \cap \{\sigma(1), \sigma(3)\} = \{\sigma(1)\}.$$
6. Soit $\sigma \in \mathrm{Ker}\varphi$. Pour tout $a \in \{1,2,3,4,5\}$, on peut choisir b et c distincts dans $\{1,2,3,4,5\} \setminus \{a\}$, et alors
$$\{\sigma(a)\} = \{\sigma(a), \sigma(b)\} \cap \{\sigma(a), \sigma(c)\} = \{a, b\} \cap \{a, c\} = \{a\}.$$
Donc $\sigma = \mathrm{id}$, ce qui montre que le morphisme φ est injectif.
7. Fixons une partie $\mathcal{A} := \{A_1, A_2, A_3, A_4, A_5\}$ de $\mathcal{E}$ à cinq éléments. Soit f la bijection de $\{1,2,3,4,5\}$ dans $\mathcal{A}$ qui envoie chaque i sur A_i. Pour tout $\sigma \in \mathfrak{S}_5$, $f \circ \sigma \circ f^{-1}$ est une permutation sur $\mathcal{A}$; soit $\psi(f)$ la permutation sur $\mathcal{E}$ qui prolonge $f \circ \sigma \circ f^{-1}$ sur $\mathcal{A}$ et qui prolonge id sur $\mathcal{E} \setminus \mathcal{A}$. On vérifie que ψ est un morphisme de groupes de $\mathfrak{S}_5$ dans $\mathfrak{S}(\mathcal{E})$. Ce morphisme est injectif car pour toute permutation $\sigma \in \mathfrak{S}_5$ se retrouve à partir de la permutation induite par $\psi(\sigma)$ sur $\mathcal{A}$ au moyen de la formule $\sigma = f^{-1} \circ \psi(\sigma)_{\mathcal{A}} \circ f$. Comme l'action de groupe associée à ψ n'est pas transitive (il y a cinq points fixes), on a $\psi \neq \varphi$.

Corrigé du problème.

1. On considère l'application $f_p : g \mapsto \langle g \rangle$ de E_p dans $\mathcal{G}_p$.
   (a) Fixons $H \in \mathcal{G}_p$. Alors $f_p^{-1}(H) = E_p \cap H$. En effet, pour tout $g \in E_p$, $|\langle g \rangle| = p = |H|$, donc $\langle g \rangle = H$ si et seulement si $\langle g \rangle \subset H$ c'est-à-dire si $g \in H$. Mais $E_p \cap H = H \setminus \{1_G\}$ car 1_G est le seul élément d'ordre 1 dans H et les autres éléments sont donc d'ordre p puisque leur ordre divise $|H| = p$, qui est premier. Ainsi, $f_p^{-1}(H) = H \setminus \{1_G\}$ a exactement $p - 1$ éléments.
   (b) Comme E_p est l'union disjointe des $f_p^{-1}(H)$ pour $H \in \mathcal{G}_p$, on a
   $$|E_p| = \sum_{H \in \mathcal{G}_p} |f_p^{-1}(H)| = \sum_{H \in \mathcal{G}_p} (p-1) = (p-1)N_p,$$
   d'après la question précédente.
2. Dans cette question on suppose que G contient deux sous-groupes H et K tels que H soit distingué dans G tels que $|K|$ et $|\mathrm{Aut}(H)|$ soient premiers entre eux.
   (a) Soient k et k' dans K, h dans H.
   — $k \cdot h = khk^{-1} \in H$ car $H \triangleleft G$.
   — $1_G \cdot h = 1_G h 1_G^{-1} = h$.
   — $k' \cdot (k \cdot h) = k' \cdot (khk^{-1})) = k'(khk^{-1})k'^{-1} = (k'k)h(k'k)^{-1} = (k'k) \cdot h)$.

Donc K agit sur H par conjugaison.

(b) Pour tout $k \in K$, notons $\varphi(k)$ l'application de H dans lui même définie par $\varphi(k)(h) = k \cdot h = khk^{-1} \in H$. D'après le cours, φ est un morphisme de K dans $\mathfrak{S}(H)$. Mais pour tout $k \in K$, $\varphi(k) \in \mathrm{Aut}(H)$, car $\varphi(k)$ est la restriction de H dans H de l'automorphisme intérieur du groupe G associé à k, ou plus simplement car pour tout h et h' dans H,

$$\varphi(k)(h)\varphi(k)(h') = (khk^{-1})(kh'k^{-1}) = khh'k^{-1} = \varphi(k)(hh').$$

Ainsi, φ est un morphisme de K dans $\mathrm{Aut}(H)$.

(c) D'après la question précédente $|\mathrm{Im}(\varphi)|$ divise $|K|$ car $|K| = |\mathrm{Ker}(\varphi)||\mathrm{Im}(\varphi)|$ et $|\mathrm{Im}(\varphi)|$ divise $|\mathrm{Aut}(H)|$ car $\mathrm{Im}(\varphi)$ est un sous-groupe de $\mathrm{Aut}(H)$.

(d) Comme $|K|$ et $|\mathrm{Aut}(H)|$ sont premiers entre eux, on en déduit que $|\mathrm{Im}(\varphi)| = 1$, d'où $\mathrm{Im}(\varphi) = \{\mathrm{id}_H\}$. Pour tout $k \in K$ et $h \in H$, on a donc $khk^{-1} = \varphi(k)(h) = \mathrm{id}(h) = h$, d'où $kh = hk$.

3. Dans cette question, on prend $n = 35$. On cherche à montrer que G est cyclique. On procède par l'absurde, en supposant que G n'est pas cyclique.

(a) Dans G, l'ordre de tout élément divise $|G| = 35$ donc vaut 1, 5, 7 ou 35. Mais 1_G est le seul élément d'ordre 1 et il n'y a pas d'élément d'ordre 35 puisque G n'est pas cyclique. Ainsi,

$$4N_5 + 6N_7 = |E_5| + |E_7| = |G \setminus \{1_G\}| = 34.$$

Comme ni 6, ni 4 ne divisent 34, N_5 et N_7 ne sont pas nuls donc $\mathcal{G}_5$ et $\mathcal{G}_7$ ne sont pas vides. Donc $N_5 \geq 1$, d'où $6N_7 = 34 - 4N_5 \leq 30$ i.e. $N_7 \leq 5$.

(b) On fixe $A \in \mathcal{G}_7$ et $B \in \mathcal{G}_5$. On cherche à montrer que A ou B est distingué. On suppose donc dans cette question que A n'est pas distingué.

i. Pour $g \in G$ et $H \in \mathcal{G}_7$, notons $g \cdot H := gHg^{-1}$. Alors $g \cdot H \in \mathcal{G}_7$ puisque l'application $\mathrm{int}_g : x \mapsto gxg^{-1}$ est un automorphisme de G. Or l'application $g \mapsto \mathrm{int}_g$ est un morphisme de groupes de D dans $\mathrm{Aut}(G)$ et $\mathrm{Aut}(G) \subset \mathfrak{S}(G)$, donc on a bien une action de G sur $\mathcal{G}_7$ par conjugaison.

ii. Comme A n'est pas distingué, l'orbite de A contient au moins deux éléments de $\mathcal{G}_7$. Mais $|\mathrm{Stab}(A)| \times |\mathrm{Orb}(A)| = |G| = 35$ donc $|\mathrm{Orb}(A)|$ divise 35, donc $|\mathrm{Orb}(A)|$ vaut 5, 7 ou 35. Ainsi $N_7 = |\mathcal{G}_7| \geq |\mathrm{Orb}(A)| \geq 5$.

iii. D'après les questions précédentes, $N_7 = 5$ donc $N_5 = 1$. Comme B est le seul sous-groupe d'ordre 5 dans G, il est égal à ses conjugués (car ce sont aussi des sous-groupes d'ordre 5 dans G), donc distingué dans G.

(c) Les groupes A et B sont d'ordre premier 7 et 5, donc cycliques et isomorphes respectivement à $\mathbb{Z}/7\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$. Donc $\mathrm{Aut}(A)$ et $\mathrm{Aut}(B)$ sont isomorphes respectivement à $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ et $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$. Donc $|\mathrm{Aut}(A)| = 6$ est premier avec $|B| = 5$, et Donc $|\mathrm{Aut}(B)| = 4$ est premier avec $|A| = 7$. Comme A ou B est distingué dans G, on peut appliquer le résultat de la question 2 avec $(H, K) = (A, B)$ ou avec $(H, K) = (B, A)$. Donc pour tout $a \in A$ et $b \in B$, $ab = ba$.

(d) Fixons $a \in A$ et $b \in B$, différents de 1_G. Comme a et b commutent et sont d'ordres premiers entre eux (7 et 5), l'ordre de ab est $o(a)o(b) = 35$. Donc ab engendre G tout entier, si bien que G est cyclique alors qu'on avait supposé qu'il ne l'était pas ! En conclusion, G est donc cyclique.

Barème sur 23, multiplié ensuite par 0,9 et arrondi avec bonus / malus.
Questions de cours : (1+1+0,5)+1 = 3,5 points
Exercice : 1+1+2+0,5+1+1+1 = 7,5 points
Problème : (1+1)+(1+1+1+1)+(2+(1+1+1)+1+1) = 12 points

Remarques sur les copies.
Exercice

Beaucoup ont confondu la paire $\{a, b\}$ avec le couple (a, b) et le stabilisateur de $\{a, b\}$ avec l'ensemble des permutations qui fixent a et b, ce qui oublie la moitié des éléments : $\{\sigma(a), \sigma(b)\} = \{a, b\}$ si et seulement si $(\sigma(a), \sigma(b)) = (a, b)$ ou $(\sigma(a), \sigma(b)) = (b, a)$. La transitivité de l'action sur les paires a été souvent pas ou mal prouvée, avec une disjonction de cas incomplète. Attention, pour trouver une permutation dont les valeurs sur un sous-ensemble sont imposées, on ne peut pas prolonger par l'identité hors de l'ensemble, à moins que cet ensemble soit globalement invariant.

Problème

Quand on veut déterminer le nombre d'antécédents d'un élément quelconque de $\mathcal{G}_p$, on part de $H \in \mathcal{G}_p$ et non de $\langle g \rangle$ avec $g \in G$. Il faut justifier correctement l'égalité $|E_p| = (p-1)N_p$. Écrire « d'après la question 1a »alors que la question 1b commence par « en déduire que »ne constitue pas une preuve.

La question 2 a été faite correctement en général, mais il faut justifier correctement que le morphisme φ fourni par l'action de groupe peut être pris à valeurs dans $\mathrm{Aut}(H)$ au lieu de $\mathfrak{S}(H)$. La conjugaison dans H par un élément $k \in K$, n'est pas en général un automorphisme intérieur, mais c'est la restriction de H dans H de int_k qui est un automorphisme intérieur de G. Cette double restriction au départ et à l'arrivée est bien définie car H est distingué dans G. Le fait que $|\mathrm{Im}\varphi|$ divise $|K|$ a souvent été non vu.

Dans la question 3a, la possibilité d'avoir un élément d'ordre 35 a souvent été omise sans justification. Dans la question 3b où l'on étudie une action sur $\mathcal{G}_7$, il y a beaucoup de confusions (entre sous-groupes et éléments du groupe G) et de notations mal choisies. Il vaut mieux appeler H plutôt que x un élément de $\mathcal{G}_7$. Aller chercher un générateur alourdit pour rien. Dans la question 3c, on ne suppose plus que A n'est pas distingué, donc il y a deux cas à envisager. Peu savent déterminer l'ordre de $\mathrm{Aut}(H)$. Attention aussi à ne pas confondre $\mathrm{Aut}(H)$ et $\mathfrak{S}(H)$.