Feuille d'exercices numéro 4

☞ **Exercice 1.** *On considère la permutation* $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}$.

(a) Décomposer s en produit de cycles et déterminer sa signature.

(b) Calculer s^{100}.

☞ **Exercice 2.** **(a)** Montrer que tout sous-groupe de $\mathbb{Z}$ est réduit à 0 ou isomorphe à $\mathbb{Z}$.

(b) Soit G un groupe commutatif, et H un sous-groupe de G tel que G/H soit isomorphe à $\mathbb{Z}$. Montrer que G est isomorphe à $H \times \mathbb{Z}$.

(c) Soit G un sous-groupe de $\mathbb{Z}^n$ ($n \geq 2$), et soit p la projection canonique de $\mathbb{Z}^n$ sur $\mathbb{Z}$ donnée par $(x_1, \ldots, x_n) \mapsto x_n$. On note K le noyau de p. Montrer que G est isomorphe à $G \cap K$ ou a $(G \cap K) \times \mathbb{Z}$.

(d) En déduire que pour tout sous-groupe G de $\mathbb{Z}^n$ il existe $p \in \mathbb{N}$ tel que $0 \leq p \leq n$ et tel que G soit isomorphe à $\mathbb{Z}^p$.

Soit G un groupe et H un sous-groupe de G. On appelle « normalisateur de H dans G », et on note $N_G(H)$ (ou $N(H)$) le plus grand sous-groupe de G dans lequel H est distingué.

☞ **Exercice 3.** **(a)** Montrer que $N_G(H)$ est bien défini (i.e. que le plus grand sous-groupe en question existe bien).

On note $p : G \to G/H$ la projection canonique, et on fait agir G sur G/H par $(g, aH) \mapsto (ga)H$.

(b) On pose $X = \{C \in G/H \mid H \subset \mathrm{Stab}(C)\}$. Montrer que $X = p(N_G(H))$.

☞ **Exercice 4.** *Soit G un groupe fini de cardinal n.*

(a) Montrer que si $a_1, \ldots, a_m$ sont des éléments de G tels que pour $0 \leq i < m$, a_{i+1} n'appartienne pas au sous-groupe engendré par $a_1, \ldots, a_i$, alors le sous-groupe engendré par $a_1, \ldots, a_m$ a au moins 2^m éléments.

(b) Montrer qu'il existe des éléments $a_1, \ldots, a_m$ de G engendrant G, tels que pour $0 \leq i < m$, a_{i+1} n'appartienne pas au sous-groupe engendré par $a_1, \ldots, a_i$.

(c) En déduire que le nombre de morphismes de G vers un groupe fini G' de cardinal n' est au plus $n'^{\frac{\ln(n)}{\ln(2)}}$.

☞ **Exercice 5.** *Soit G un groupe. On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G et $\mathrm{Int}(G)$ le groupe des automorphismes intérieurs de G.*

(a) Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$.

☞ **Exercice 6.** *Soit K l'unique sous-groupe distingué à 4 éléments du groupe $\mathfrak{S}_4$ des permutations de $\{1, 2, 3, 4\}$.*

(a) Montrer que tout élément x de $\mathfrak{S}_4$ se met de manière unique sous la forme $x = \sigma_x k_x$, avec $k_x \in K$ et $\sigma_x(1) = 1$.

(b) Montrer que $x \mapsto \sigma_x$ est un morphisme de groupes de $\mathfrak{S}_4$ vers lui-même.

(c) En déduire que $\mathfrak{S}_4/K$ est isomorphe à $\mathfrak{S}_3$.

☞ **Exercice 7.** *On considère un morphisme de groupes $\varphi : \mathfrak{S}_4 \to \mathrm{O}(n)$ ($n \neq 0$), qui définit donc une action de $\mathfrak{S}_4$ sur $\mathbb{R}^n$. On suppose que pour tout vecteur x non nul de $\mathbb{R}^n$, le sous-espace vectoriel engendré par l'orbite de x est $\mathbb{R}^n$. Le noyau (groupe alterné) de la signature $\mathfrak{S}_4 \to \{\pm 1\}$ est noté $\mathfrak{A}_4$.*

(a) Montrer que si $\mathfrak{A}_4 \subset \mathrm{Ker}(\varphi)$ on a $n = 1$. (Considérer un élément $\sigma \notin \mathfrak{A}_4$ et un vecteur propre de $\varphi(\sigma)$.)

(b) Montrer réciproquement que si $n = 1$, on a $\mathfrak{A}_4 \subset \mathrm{Ker}(\varphi)$. (Déterminer l'indice du stabilisateur d'un $x \in \mathbb{R}$.)

Soit K l'unique sous-groupe distingué à 4 éléments de $\mathfrak{S}_4$. Dans les questions **(c)**, **(d)** *et* **(e)**, *on suppose que* $\mathrm{Ker}(\varphi) = K$.

(c) Soient ρ et σ deux éléments de $\mathfrak{S}_4$ dont les images dans $\mathfrak{S}_4/K$ sont respectivement d'ordres 3 et 2. Montrer que les sous-espaces spectraux de $r = \varphi(\rho)$ sont stables par $s = \varphi(\sigma)$.

(d) Montrer que le sous-espace propre E de r pour la valeur propre 1 est réduit à 0.

(e) Montrer que $n = 2$.

On suppose désormais que φ est injectif.

(f) On suppose que $n = 2$. Montrer que les trois éléments non nuls de K sont envoyés par φ sur deux symétries orthogonales d'axes orthogonaux et le demi-tour (rotation d'angle π).

(g) On suppose toujours que $n = 2$. En utilisant un élément d'ordre 3 de $\mathfrak{A}_4$, montrer que l'image de φ contient une rotation d'angle $\pi/3$. En déduire une contradiction.

Solutions des exercices de la feuille 4

☞ **Exercice 1.** **(a)** On a immédiatement $s = (1\ 3\ 4)(2\ 5\ 7)(6\ 10\ 8)(9)$. La signature est donc $+1$ (on a un nombre pair (ici zéro) de cycles de longueur paire).

(b) Tous les cycles de la décomposition ayant un ordre qui divise 3, ces cycles étant des permutations qui commutent entre elles, et comme $100 = 33 \times 3 + 1$, on voit que $s^{100} = s$.

☞ **Exercice 2.** **(a)** Si un sous-groupe G de $\mathbb{Z}$ n'est pas réduit à 0, il contient un élément non nul, et donc un élément non nul a de valeur absolue minimale (c'est-à-dire tel que $\forall_{x\in G}\ x \neq 0 \Rightarrow |a| \leq |x|$). Si $x \in G$, on peut écrire $x = aq + r$ avec $0 \leq r < |a|$ (division euclidienne). Comme $q \in \mathbb{Z}$, on a $aq = a + \cdots + a$ ou $aq = -a - \cdots - a$, et donc $aq \in G$. Il en résulte que $r \in G$, donc que $r = 0$ et que les éléments de G sont exactement les multiples entiers (relatifs) de a, autrement-dit que $G = a\mathbb{Z}$, lequel est isomorphe à $\mathbb{Z}$.

(b) Comme G/H est isomorphe à $\mathbb{Z}$, il est monogène, engendré par une classe de la forme $a+H$, avec $a \in G$. On définit $\varphi : H \times \mathbb{Z} \to G$ en posant :

$$\varphi(h, n) = h + na$$

Rappelons que ce qu'on note na est la somme $a + \cdots + a$ (n termes) si $n \geq 0$ et $-a - \cdots - a$ ($|n|$ termes) si $n \leq 0$. Cette application est bien définie, parce que contrairement à ce qu'il pourrait se passer si on avait $\mathbb{Z}/p\mathbb{Z}$ à la place de $\mathbb{Z}$, un élément de $\mathbb{Z}$ est représenté par un unique entier relatif. Alors φ est un morphisme de groupes. En effet, tous les groupes concernés étant commutatifs, on a $\varphi(h + h', n + n') = (h + h') + (n + n')a = (h + na) + (h' + n'a) = \varphi(h, n) + \varphi(h', n')$. Il reste donc à montrer que φ est bijectif.

Si $\varphi(h, n) = 0$, alors $h + na = 0$ et donc $na \in H$. Ceci implique que $n(a+H) = H$, qui est l'élément neutre de G/H. Mais comme $a + H$ n'est pas 0 dans G/H (puisque c'est un générateur) et comme G/H est isomorphe à $\mathbb{Z}$, ceci ne peut arriver que si $n = 0$. On a alors aussi $h = 0$, et φ est injective.

Soit $x \in G$. Il existe un entier relatif tel que $x + H = n(a + H) = (na) + H$ puisque aH est un générateur de G/H. On voit donc que x est de la forme $h + na$ avec $h \in H$, et que φ est surjective.

(c) Si $G \subset K$, alors $G = G \cap K$. Sinon, $p(G) \neq 0$, et $p(G)$ est donc isomorphe à $\mathbb{Z}$ (question **(a)**). Le quotient $G/(G \cap K)$ est alors lui aussi isomorphe à $\mathbb{Z}$. En effet, le morphisme surjectif $p : G \to p(G)$ a exactement $G \cap K$ comme noyau. Il résulte alors de la question **(b)** que G est isomorphe à $(G \cap K) \times \mathbb{Z}$.

(d) On procède par récurrence sur n. Le cas $n = 0$ est trivial, et le cas $n = 1$ a été traité dans la question **(a)**. Comme le noyau K de p est isomorphe à $\mathbb{Z}^{n-1}$, l'hypothèse de récurrence montre que $G \cap K$ est isomorphe à $\mathbb{Z}^q$ pour un certain q tel que $0 \leq q \leq n - 1$. La question **(c)** montre alors que G est isomorphe à $\mathbb{Z}^q$ ou à $\mathbb{Z}^{q+1}$.

☞ **Exercice 3.** **(a)** L'ensemble E des éléments x de G tels que $xHx^{-1} = H$ est un sous-groupe de G. En effet, on a $1 \in E$, et si $x, y \in E$, alors $(xy)H(xy)^{-1} = x(yHy^{-1})x^{-1} = H$. Enfin, en multipliant l'égalité $xHx^{-1} = H$ à gauche par x^{-1} et à droite par x, on obtient $H = x^{-1}Hx$. Il est clair que E contient H et que H est distingué dans E. De plus, tout élément de G laissant H invariant par conjugaison doit être dans E, lequel est donc le plus grand sous-groupe de G dans lequel H est distingué.

(b) Si $x \in N_G(H)$, on a $xHx^{-1} = H$, donc $p(x) = xH = xHH = xx^{-1}HxH = HxH = Hp(x)$, d'où il suit que $H \subset \mathrm{Stab}(p(x))$, donc que $p(x) \in X$. Réciproquement, si $C \in X$, on a $H \subset \mathrm{Stab}(C)$, donc $hC = C$ pour tout $h \in H$. Soit x un élément quelconque de C. On a $hx \in C$, pour tout $h \in H$, et donc pour tout $h \in H$, il existe $h' \in H$ tel que $hx = xh'$. On voit donc que $x^{-1}hx \in H$, et comme ceci est valide pour tout $h \in H$, on a $x^{-1}Hx = H$, donc $x^{-1} \in H_G(H)$, et comme $N_G(H)$ est un sous-groupe de G, on a aussi $x \in N_G(H)$. Comme $C = p(x)$, on a montré que $X \subset p(N_G(H))$.

☞ **Exercice 4.** **(a)** Par récurrence sur m. Le cas $m = 0$ résulte du fait que tout groupe a au moins un élément. Si $m > 0$, l'hypothèse de récurrence montre que le sous-groupe H engendré par $a_1, \ldots, a_{m-1}$ a au moins 2^{m-1} éléments. Comme $a_m \notin H$, a_mH est une classe (à droite) modulo H distincte de H et de même cardinal que H. $H \cup a_mH$ a donc au moins 2^m éléments et est contenu dans le sous-groupe engendré par $a_1, \ldots, a_m$.

(b) Comme les puissances de 2 inférieures ou égales à n sont en nombre fini, il existe un plus grand m tel qu'il existe une suite $a_1, \ldots, a_m$ satisfaisant ls conditions de la question **(a)**. Cette suite engendre G car sinon il existerait une suite de longueur $m + 1$ satisfaisant ces mêmes conditions.

(c) Un automorphisme de G est déterminé par les images d'un ensemble de générateurs, or on vient de voir que G a un ensemble de générateurs à m éléments avec $2^m \leq n$, c'est-à-dire $m \leq n^{\frac{\ln(n)}{\ln(2)}}$. Comme on a au plus n' choix d'image pour chaque générateur, on obtient le résultat annoncé.

☞ **Exercice 5.** **(a)** $\mathrm{Int}(G)$ est clairement un sous-groupe de $\mathrm{Aut}(G)$. Si $f \in \mathrm{Aut}(G)$ et $\varphi \in \mathrm{Int}(G)$, on a $\varphi(x) = axa^{-1}$ pour un certain $a \in G$ et tout x de G. Alors $(f\varphi f^{-1})(x) = f(af^{-1}(x)a^{-1}) = f(a)xf(a)^{-1}$. Ainsi $f\varphi f^{-1}$ est l'automorphisme intérieur $x \mapsto f(a)xf(a)^{-1}$, et $\mathrm{Int}(G)$ est donc distingué dans $\mathrm{Aut}(G)$.

☞ **Exercice 6.** **(a)** Les éléments de K sont $k_1 = 1$, $k_2 = (12)(34)$, $k_3 = (13)(24)$ et $k_4 = (14)(23)$. On remarque que $k_i(i) = 1$ pour $i = 1, 2, 3, 4$, et on a $k_i^{-1} = k_i$. De plus $k_j(i) = 1$ entraîne $i = j$. Posons $k_x = k_{x(1)}$. On a $k_x x(1) = 1$ pour tout x. On peut donc poser $\sigma_x = k_x x$, ce qui donne $x = \sigma_x k_x$, où σ_x satisfait la condition requise. L'unicité résulte du fait que si $\sigma k_i = \sigma' k_j$, avec $\sigma(1) = \sigma'(1) = 1$ et $k_i, k_j \in K$, alors, comme $\sigma k_i(i) = \sigma(1) = 1$, on doit avoir $\sigma' k_j(i) = 1$. Mais ceci implique $k_j(i) = 1$, et donc $i = j$, puis $\sigma = \sigma'$.

(b) Soient $x = \sigma_x k_x$ et $y = \sigma_y k_y$ deux éléments de $\mathfrak{S}_4$. Il s'agit de montrer que $\sigma_{xy} = \sigma_x \sigma_y$. Or, $xy = \sigma_x k_x \sigma_y k_y$, et comme K est distingué dans $\mathfrak{S}_4$, l'automorphisme intérieur $z \mapsto \sigma_y z \sigma_y^{-1}$ induit une bijection $K \to K$. Il existe donc $k' \in K$ tel que $k_x = \sigma_y k' \sigma_y^{-1}$. On a alors $xy = \sigma_x \sigma_y k' \sigma_y^{-1} \sigma_y k_y = \sigma_x \sigma_y k''$, avec $k'' \in K$. Il en résulte que $\sigma_x \sigma_y = \sigma_{xy}$.

(c) Le morphisme de la question précédente a clairement K pour noyau, et son image est isomorphe à $\mathfrak{S}_3$, car il s'agit du groupe des permutations de $\{2, 3, 4\}$. D'où le résultat.

☞ **Exercice 7.** **(a)** Soit $\sigma \in \mathfrak{S}_4$ tel que $\sigma \notin \mathfrak{A}_4$, et posons $f = \varphi(\sigma)$. Alors $f^2 = 1$, donc f est diagonalisable et ses valeurs propres sont parmi $\{+1, -1\}$. Soit $x \neq 0$ un vecteur propre de f. L'orbite de x est alors composée de x tout seul ou de la paire $\{x, -x\}$. Dans tous les cas, elle engendre un sous-espace de dimension 1, et on a donc $n = 1$.

(b) Si $n = 1$, l'image par φ de tout élément de $\mathfrak{S}_4$ est une isométrie de $\mathbb{R}$, donc égale à ± 1. Il s'en suit que l'orbite d'un x quelconque de $\mathbb{R}$ a au plus deux points, et que le stabilisateur de ce x est d'indice 2 ou 1. Le seul sous-groupe d'indice 1 de $\mathfrak{S}_4$ est $\mathfrak{S}_4$ et le seul sous-groupe d'indice 2 (qui doit nécessairement être distingué) de $\mathfrak{S}_4$ est $\mathfrak{A}_4$. Le stabilisateur de tout point de $\mathbb{R}$ contient donc $\mathfrak{A}_4$ et on a $\mathfrak{A}_4 \subset \mathrm{Ker}(\varphi)$.

(c) On sait que $\mathfrak{S}_4/K \simeq \mathfrak{S}_3$, et on a donc $sr^2 = rs$ et $sr = r^2 s$. Comme $r^3 = 1$, les sous-espaces $E = \mathrm{Ker}(r - 1)$ et $F = \mathrm{Ker}(r^2 + r + 1)$ sont en somme directe et leur somme est $\mathbb{R}^n$ (décomposition spectrale). Si on a $r(x) = x$, on a $rs(x) = sr^2(x) = s(x)$. De même, si on a $r^2(x) + r(x) + x = 0$, on a $sr^2(x) + sr(x) + s(x) = 0$, donc $rs(x) + r^2 s(x) + s(x) = 0$. Les sous-espaces spectraux de r sont donc stables par s.

(d) Supposons que $E \neq 0$. Alors s a un vecteur propre x non nul dans E, et on a $s(x) = \pm x$ et $r(x) = x$. Dans ce cas, l'orbite de x ne contient que les deux points (non nécessairement distincts) x et $s(x)$, et engendre une droite, qui doit être $\mathbb{R}^n$ par hypothèse. C'est impossible, car on a vu que cela entraîne que le noyau de φ est $\mathfrak{A}_4$.

(e) D'après ce qui précède, l'autre sous-espace spectral de r (appelons-le F) n'est pas nul, et on a un $x \neq 0$, qui vérifie $r^2(x) + r(x) + x = 0$ et $s(x) = \pm x$. L'orbite de x engendre donc le même sous-espace que les points x, $r(x)$ et $r^2(x)$, qui doit être un plan car ces trois vecteurs sont linéairement dépendants. On a donc $n = 2$.

(f) Le sous-groupe K de $\mathfrak{S}_4$ est formé des permutations $k_1 = 1$, $k_2 = (12)(34)$, $k_3 = (13)(24)$ et $k_4 = (14)(24)$. Les éléments k_2, k_3 et k_4 sont d'ordre 2 et le produit de deux d'entre eux donne le troisième. Or, les éléments d'ordre 2 de $\mathrm{O}(2)$ sont le demi-tour et les symétries orthogonales autour d'une droite. Comme φ est injective, au moins deux éléments parmi les images par φ de k_2, k_3, k_4 doivent être des symétries. Le troisième est nécessairement une rotation, car le composé de deux symétries du plan (déterminant -1) est une rotation (déterminant $+1$). Ainsi, l'un des trois est nécessairement le demi-tour et les deux autres des rotations dont l'angle entre les axes doit être de $\pi/2$, car l'angle de la rotation qui est leur produit est le double de l'angle entre les axes de symétrie des deux symétries.

(g) Prenons un élément ρ d'ordre 3 dans $\mathfrak{A}_4$. $r = \varphi(\rho)$ ne peut être qu'une rotation d'angle $\pm 2\pi/3$. L'image de $\mathfrak{A}_4$ par φ contient donc une rotation d'angle $2\pi/3$ et une rotation d'angle π. Il en résulte qu'elle contient une rotation d'angle $\pi/3$, qui est un élément dordre 6 de $\mathrm{O}(2)$. Or, $\mathfrak{A}_4$ ne contient aucun élément d'ordre 6, et il est donc impossible que n soit égal à 2.