Corrigé de l'examen du 9 janvier 2024

1. Soit G un groupe d'ordre p où p est un nombre premier. Montrer que G est cyclique.

   Solution. Soit $x \in G, x \neq 1$. Alors $\langle x \rangle$ est un sous-groupe non trivial de G et son ordre divise p. Comme p est premier, ceci implique que $|\langle x \rangle| = p$ et $\langle x \rangle = G$. □

2. Pour une permutation $\sigma \in S_n$ on note par $\epsilon(\sigma) \in \{\pm 1\}$ sa signature. Soit $\sigma \in S_{10}$ donnée par
$$\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)(8\ 9\ 10).$$
   Calculer $\epsilon(\sigma)$. Est-ce que la réponse change si on considère σ comme un élément de S_{11} ?

   Solution. On sait que la signature d'un cycle est 1 si sa longueur est un nombre impair et -1 si elle est un nombre pair. Comme ϵ est un morphisme, on calcule que $\epsilon(\sigma) = 1(-1)1 = -1$. Le même calcul reste valide dans S_{11} (et dans S_n pour n'importe quel $n \geq 10$). □

3. Combien de classes de conjugaison y a-t-il dans S_4 ? Pour chaque classe de conjugaison, donner un représentant de cette classe.

   Solution. Deux éléments de S_n sont conjugués ssi ils ont les mêmes longueurs des cycles dans leurs décompositions en cycles disjoints. Les possibilités dans S_4 sont : $(1, 1, 1, 1)$ (représentant e), $(1, 1, 2)$ (représentant $(1\ 2)$), $(1, 3)$ (représentant $(1\ 2\ 3)$), $(2, 2)$ (représentant $(1\ 2)(3\ 4)$), (4) (représentant $(1\ 2\ 3\ 4)$). Il y a 5 classes de conjugaison en tout. □

4. Les groupes D_{24} et S_4 sont-ils isomorphes ?

   Solution. Non. D_{24} a un élément d'ordre 12 (la rotation r) et S_4 n'en a pas : les ordres des éléments des classes de l'exercice précédent sont respectivement : $1, 2, 3, 2, 4$. □

5. Soit $\phi \colon G \to H$ un morphisme de groupes et soit $g \in G$ un élément d'ordre fini. Montrer que l'ordre de $\phi(g)$ divise l'ordre de g.

   Solution. Soit n l'ordre de g. On a que $g^n = 1$. Comme ϕ est un morphisme, ceci implique que $\phi(g)^n = 1$, i.e., l'ordre de $\phi(g)$ divise n. □

6. Montrer que tous les éléments du groupe $\mathbf{Q}/\mathbf{Z}$ sont d'ordre fini. (Ici $\mathbf{Q}$ est le groupe additif des nombres rationnels et $\mathbf{Z}$ est le sous-groupe des entiers.)

   Solution. Soit $\pi \colon \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ le morphisme quotient. Pour tout $p/q \in \mathbf{Q}$, on a : $q\pi(p/q) = \pi((qp)/q) = \pi(p) = 0$ (car $p \in \mathbf{Z} = \ker \pi$). On en déduit que l'ordre de $\pi(p/q)$ divise q et qu'il est en particulier fini. □

7. Soit
$$H = \{\frac{a}{2^k} : a, k \in \mathbf{Z}\}.$$

   (a) Montrer que H est un sous-groupe de $(\mathbf{Q}, +)$.

Solution. Si $a/2^k, b/2^\ell \in H$, on a que $a/2^k - b/2^\ell = (2^\ell a - 2^k b)/2^{k+\ell} \in H$ ce qui implique que H est un sous-groupe de $\mathbf{Q}$. □

(b) Montrer que $\phi\colon H \to H$ défini par $\phi(h) = 2h$ est un automorphisme de H.

Solution. Soit ψ défini par $\psi(h) = h/2$. On vérifie directement que $\phi(H) \subseteq H, \psi(H) \subseteq H$ et que ϕ et ψ sont des inverses l'un à l'autre. Ceci implique que $\phi\colon H \to H$ est une bijection. Enfin, ϕ est un morphisme à cause de la loi distributive dans le corps $\mathbf{Q}$. □

(c) Soit $G = H \rtimes \mathbf{Z}$ où le générateur 1 de $\mathbf{Z}$ agit sur H par ϕ. Soit $g \in G$ donné par $g = (1,1)$. Pour tout $n \in \mathbf{N}$ calculer g^n.

Solution. Par la définition de la loi dans le produit semi-direct, on a pour tout $(a,b) \in H \rtimes \mathbf{Z}$, $(1,1)(a,b) = (1+\phi(a), 1+b) = (1+2a, 1+b)$. En utilisant cette formule, on obtient par récurrence que $(1,1)^n = (2^n - 1, n)$. □

8. Soit G un groupe et $H \leq G$ avec $[G:H] = n$ avec n fini. Montrer qu'il existe un sous-groupe $N \trianglelefteq G$ avec $N \leq H$ et $[G:N] \leq n!$.

Solution. Soit $\pi\colon G \to S_n$ le morphisme donné par l'action $G \curvearrowright G/H$ par translation à gauche. Alors $N = \ker \pi$ convient : on a que $[G:N] = |\operatorname{im} \pi| \leq |S_n| = n!$. □

9. Soit G un groupe fini et soient $H \leq G$, $N \trianglelefteq G$.

(a) Montrer que si $|H|$ et $[G:N]$ sont premiers entre eux, alors $H \leq N$.

Solution. Soit $\pi\colon G \to G/N$ le morphisme quotient. Alors $\pi(H)$ est un quotient de H et un sous-groupe de G/N. Il s'ensuit que l'ordre de $\pi(H)$ divise à la fois $|H|$ et $|G/N|$. Par l'hypothèse, $|\pi(H)| = 1$ et donc $H \leq \ker \pi = N$. □

(b) Montrer que si $|N|$ et $[G:H]$ sont premiers entre eux, alors $N \leq H$.

Solution. Considérons l'action $N \curvearrowright G/H$ et observons que toutes les orbites ont le même cardinal (notons le k). En effet, pour tout $gH \in G/H$,

$$|N \cdot gH| = [N : (N \cap gHg^{-1})] = [g^{-1}Ng : (g^{-1}Ng \cap H)] = [N : (N \cap H)],$$

car N est distingué. Donc k est un diviseur commun de $|N|$ et de $|G/H|$ et par l'hypothèse, $k = 1$. Ceci implique que $N \cap H = N$, ou, ce qui est équivalent, $N \leq H$. □

10. Soient p et q deux nombres premiers. Montrer qu'un groupe d'ordre p^2q n'est jamais simple.

Solution. Soit G un groupe d'ordre p^2q. Si $p = q$, on sait du cours que le centre de G est non trivial et donc G n'est pas simple. Supposons maintenant que $p \neq q$ et soient P et Q un p-Sylow et un q-Sylow de G, respectivement. Soit n_p le nombre de conjugués de P et soit n_q le nombre de conjugués de Q. Notre but est de démontrer que $n_p = 1$ ou $n_q = 1$. Supposons que ce n'est pas le cas. Par le théorème de Sylow, $n_p \mid q$, $n_p \equiv 1 (\mathrm{mod}\ p)$, $n_q \mid p^2$ et $n_q \equiv 1 (\mathrm{mod}\ q)$. Les deux premières conditions impliquent que $n_p = q$ et $q > p$. Maintenant les deux autres nous donnent que $n_q = p^2$. Observons que Q est cyclique d'ordre q et que deux conjugués de Q distincts s'intersectent trivialement ; donc G a $n_q(q-1) = p^2q - p^2$ éléments d'ordre q. D'autre part, soit gPg^{-1} un conjugué de P distinct de P. Alors $|P \cup gPg^{-1}| \geq |P| + 1 = p^2 + 1$ et tout élément de cet ensemble est d'ordre une puissance de p. Ceci fait au moins $p^2q - p^2 + p^2 + 1 = p^2q + 1$ éléments distincts de G, contradiction. □