# 101. Groupes opérant sur un ensemble : Indications de solutions

**1.** a) On vérifie immédiatement que $h.(aH) := (ha)H$ est bien définie (si $aH = bH$, alors $(ha)H = (hb)H$, donc $h.(aH)$ ne dépend pas du représentant $a$ choisi dans une même classe à gauche), et que ceci définit une opération de groupe. Le stabilisateur de $aH$ est $H \cap aHa^{-1}$, car dire que $h \in H$ vérifie $h.(aH) = aH$ signifie que $a^{-1}(ha) \in H$, ou encore $h \in aHa^{-1}$. Il est par ailleurs immédiat que l'orbite de $H$ est réduite à $H$.

b) Si $H$ n'est pas distingué dans $G$, il y a au moins une orbite dont le cardinal n'est pas 1, puisque cela signifie qu'il existe $a \in G$ et $h \in H$ tels que $a^{-1}(ha) \notin H$. Comme le cardinal de cette orbite divise celui de $H$ (donc aussi celui de $G$ par le théorème de Lagrange), ce cardinal est au moins $p$, vu que $p$ est le plus petit diviseur $\geq 2$ de $\#G$.

c) Si $H$ n'est pas distingué dans $G$, on a donc une orbite de cardinal au moins $p$, mais il y a aussi une orbite de cardinal 1 (celle de $H$). L'équation aux classes donne alors que $\#(G/H) \geq p + 1$, ce qui contredit l'hypothèse que $[G : H] = p$.

**2.** a) Clairement, l'orbite d'un sous-espace de dimension $d$ ne contient que des sous-espaces de dimension $d$. Réciproquement, si $F$ et $G$ sont des sous-espaces de dimension $d$, on choisit une base $(f_1, ..., f_d)$ de $F$ qu'on complète en une base $(f_1, ..., f_{d+1}, ..., f_n)$ de $E$. De même on peut prendre une base $(g_1, ..., g_d)$ de $G$ et la compléter en une base $(g_1, ..., g_{d+1}, ..., g_n)$ de $E$. Alors l'endomorphisme $u$ de $E$ qui envoie $f_i$ sur $g_i$ est bijectif et vérifie $u(F) = G$. Finalement, les orbites sont les sous-espaces de dimension $d$ pour $d = 0, ..., n$.

b) Fixons un sous-espace $F$ de dimension 3 (on sait qu'il y en a au moins un). D'après a), le nombre cherché est le cardinal de l'orbite de $F$ pour l'action de $\mathrm{GL}(E)$, ou encore le cardinal de $GL(E)$ divisé par celui du stabilisateur $S$ de $F$. On sait que le cardinal de $GL(E)$ (qu'on obtient par exemple en comptant le nombre de bases de $E$) est :

$$(7^5 - 1)(7^5 - 7)...(7^5 - 7^4).$$

En prenant une base de $F$ que l'on complète en une base de $E$, on voit que $S$ est isomorphe au groupe des matrices-bloc de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

avec $A \in \mathrm{GL}_3(\mathbf{F}_7)$, $C \in \mathrm{GL}_2(\mathbf{F}_7)$ et $B \in M_{3,2}(F_7)$. Ainsi on a

$$\#S = (7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6.$$

On en déduit le cardinal cherché (140050, sauf erreur de calcul...).

**3.** a) On cherche le nombre de morphismes de $\mathbf{Z}/4\mathbf{Z}$ dans le groupe des permutations $\mathcal{S}_5$. Se donner un tel morphisme $f$ revient à se donner un élément d'ordre divisant 4 (à savoir $f(\bar{1})$) dans $\mathcal{S}_5$. Or $\mathcal{S}_5$ contient un élément d'ordre 1 (l'identité), $C_5^2 = 10$ transpositions, $5.3 = 15$ doubles transpositions (cinq façons de choisir le point fixe, puis trois doubles transpositions avec les quatre éléments restants) et $5.6 = 30$ 4-cycles (cinq façons de choisir le point fixe, et six 4-cycles dans le groupe des permutations des quatre éléments restants). Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.

b) Clairement, oui pour l'opération par conjugaison, non pour l'opération par translation.

c) On sait que le groupe des automorphismes de $X$ est isomorphe au groupe multiplicatif des inversibles de l'anneau $\mathbf{Z}/13\mathbf{Z}$ (en effet si on pose $\varphi_a(x) = ax$, on vérifie immédiatement que $a \mapsto \varphi_a$ est un isomorphisme de $(\mathbf{Z}/13\mathbf{Z})^*$ sur $\mathtt{Aut}\, X$), lequel est isomorphe au groupe additif $\mathbf{Z}/12\mathbf{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbf{Z}/3\mathbf{Z}$ dans $\mathbf{Z}/12\mathbf{Z}$, ou encore le nombre déléments de $\mathbf{Z}/12\mathbf{Z}$ d'ordre divisant 3. Il y a ainsi trois solutions.

On voit facilement que les seuls automorphismes de $\mathcal{S}_3$ sont intérieurs. Le groupe des automorphismes de $\mathcal{S}_3$ est donc isomorphe à $\mathcal{S}_3$ quotienté par son centre, i.e. à $\mathcal{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathcal{S}_3$, et il y a trois solutions.

**4.** a) C'est tout à fait analogue à l'exercice 2.a), en notant qu'une famille orthonormée peut se compléter en une base orthonormée, et qu'un endomorphisme envoyant une base orthonormée sur une base orthonormée est dans $O(E)$. Les orbites sont les espaces de dimension $d$ pour chaque $d = 0, 1, ..., n$.

b) Idem en remplaçant le groupe orthogonal de $E$ par son groupe unitaire.

Notons que si maintenant on se pose la question pour le groupe orthogonal d'une forme quadratique $q$ sur un corps quelconque (de caractéristique

différente de 2), c'est beaucoup plus difficile. Il est clair que si $F$ est un sous-espace, une condition nécessaire pour qu'un autre sous-espace $G$ soit dans l'orbite de $F$ est que les restrictions de $q$ à $F$ et $G$ soient des formes quadratiques isomorphes (ce qui implique en particulier $\dim F = \dim G$, mais n'est pas équivalent à cette condition). Cette condition est en fait suffisante, mais c'est un théorème difficile, le théorème de Witt (voir par exemple le cours d'algèbre de D. Perrin).

**5.** a) Il est immédiat que $G_{x_0}$ est un sous-groupe de $G$, mais il n'est pas toujours distingué : par exemple, dans $\mathcal{S}_3$, le centralisateur d'une transposition $\tau$ est le sous-groupe $\{\mathrm{id}, \tau\}$, lequel n'est pas distingué.

b) $G$ opère par conjugaison sur lui-même. Par définition $C$ est l'orbite de $x_0$ et $G_{x_0}$ son stabilisateur, d'où

$$\#G = \#C.\#G_{x_0}.$$

**6.** a) Si le cardinal de $A$ possèdait un diviseur premier $\ell \neq p$, alors d'après le théorème de Sylow $A$ contiendrait un $\ell$-groupe non trivial, et donc un élément d'ordre $\ell^r$ avec $r > 0$. Comme par hypothèse l'ordre de tout élément de $A$ est une puissance de $p$, on obtiendrait une contradiction. On peut aussi utiliser le fait (théorème de structure) que $A$ est isomorphe à un produit $\prod_{i=1}^{m} \mathbf{Z}/d_i$, avec $d_1|d_2|...|d_r$, et l'hypothèse que $A$ est de torsion $p$-primaire impose que tous les $d_i$ sont des puissances de $p$, donc le cardinal de $A$ aussi.

b) L'équation aux classes donne que le cardinal de $A$ est la somme du nombre $f$ de point fixes pour l'action de $G$ et des cardinaux des orbites non réduites à un point. Le cardinal d'une telle orbite divise celui de $G$, donc est une puissance de $p$ autre que 1 vu que $G$ est un $p$-groupe. Ainsi, en utilisant a), $f$ est divisible par $p$ et en particulier $f \geq 2$. Il y a donc au moins un point fixe autre que 0.

c) Par hypothèse, le groupe $B$ est abélien et engendré par une partie finie $S := \{g.a, g \in G\}$. De plus tout élément $x$ de $S$ est annulé par une puissance de $p$, donc comme $S$ est fini il existe un entier $m > 0$ (puissance de $p$) tel que $mx = 0$ pour tout $x \in S$. On voit alors que si $S = \{s_1, ..., s_r\}$, alors $B$ est l'ensemble des combinaisons linéaires de la forme

$$a_1 s_1 + ... + a_r s_r,$$

avec $0 \leq a_i < m$, ce qui montre que $B$ est fini.

d) On observe que $S$ est stable pour l'action de $G$, donc $B$ l'est également puisque $G$ opère par automorphismes. Il suffit d'appliquer alors b) à $B$.