101. Groupes opérant sur un ensemble : Indications de solutions

1. Le groupe H opère sur l'ensemble des classes à gauche G/H via : $h.(aH) := (ha)H$ pour tous $h \in H$, $a \in G$. L'équation aux classes donne

$$p = \sum_{\omega \in \Omega} \#\omega,$$

où Ω est l'ensemble des orbites. On observe qu'il existe au moins une orbite réduite à un élément, par exemple celle de $e.H = H$. D'autre part, si une orbite n'est pas réduite à un élément, son cardinal divise celui de G (c'est celui de G divisé par celui d'un stabilisateur), donc est au moins p puisque p est le plus petit diviseur de $\#G$. On aboutit donc à une contradiction puisqu'alors on aurait $\sum_{\omega \in \Omega} \#\omega \geq p + 1$. Finalement, toutes les orbites sont réduites à un point, autrement dit : $(ha)H = aH$ pour tous $h \in H, a \in G$, ou encore $a^{-1}ha \in H$, ce qui montre que H est distingué dans G.

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.

c) (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).