104. Groupes finis, exemple et applications : indications de solutions

1. a) Montrons plus généralement (sur un corps K quelconque) que si un endomorphisme u de K^n commute avec tous les endomorphismes de déterminant 1, alors u est une homothétie. Il suffit pour cela (classique) de voir que tout vecteur $x \neq 0$ de K^n est vecteur propre pour u. Complétons x en une base $(x, e_1, ..., e_{n-1})$ de K^n; soit M la matrice de u dans cette base, alors M commute avec la matrice de Jordan J_n, ce qui implique qu'elle laisse stable le noyau de J_n, lequel est $K.x$. Ainsi x est bien vecteur propre pour u comme on voulait.

b) On sait que le cardinal de $\mathrm{GL}_n(K)$ est

$$\#\mathrm{GL}_n(K) = (q^n - 1)(q^n - q)...(q^n - q^{n-1}).$$

Comme par définition $\mathrm{SL}_n(K)$ est le noyau du morphisme de groupes surjectif $\det : \mathrm{GL}_n(K) \to K^*$, son cardinal est celui de $\mathrm{GL}_n(K)$ divisé par $q - 1$, soit

$$\#\mathrm{SL}_n(K) = (q^n - 1)(q^n - q)...(q^n - q^{n-2}).q^{n-1}.$$

D'autre part $\mathrm{PGL}_n(K)$ est le quotient de $\mathrm{GL}_n(K)$ par un groupe isomorphe à K^* (les matrices scalaires non nulles), donc $\#\mathrm{PGL}_n(K) = \#\mathrm{SL}_n(K)$.

Enfin, le cardinal de $\mathrm{PSL_n}(K)$ est celui de $\mathrm{SL}_n(K)$ divisé par celui de son centre, lequel consiste en les matrices λI_n avec $\lambda^n = 1$. Or, il y a $\mathrm{pgcd}(n, q-1)$ racines n-ièmes de l'unité dans un corps K de cardinal q : en effet, on sait que K^* est un groupe cyclique d'ordre $q-1$, et on est donc ramené à compter le nombre de solutions x de $nx = 0$ dans $\mathbf{Z}/(q-1)\mathbf{Z}$, ce qui donne facilement le résultat. Finalement

$$\#\mathrm{PSL_n}(K) = \frac{(q^n - 1)(q^n - q)...(q^n - q^{n-2}).q^{n-1}}{\mathrm{pgcd}(n, q-1)}.$$

2. a) On fait opérer $\mathrm{PGL}_n(K)$ sur l'ensemble $\mathbf{P}(E)$ des droites vectorielles de E par $\bar{g}.D = g(D)$, où $g \in \mathrm{GL}_n(K)$ et $\bar{g}$ est son image dans

$\mathrm{PGL}_n(K)$. Ceci est bien défini car si $\bar{g}_1 = \bar{g}_2$, alors g_1 et g_2 sont proportionnels donc $g_1(D) = g_2(D)$. L'opération est fidèle car les seuls $g \in \mathrm{GL}_n(K)$ qui stabilisent toutes les droites sont les homothéties. On obtient donc un morphisme injectif Φ de $\mathrm{PGL}_n(K)$ dans $\mathcal{S}(\mathbf{P}(E))$.

b) Les droites vectorielles de E sont données par une équation $y = ax$ dans le plan (avec $a \neq 0$) ou par l'équation $x = 0$. On obtient ainsi $q + 1$ droites.

c) D'après a), les groupes $\mathrm{PGL}_2(\mathbf{F}_2)$ et $\mathrm{PSL}_2(\mathbf{F}_2)$ sont égaux et de cardinal 6, qui est aussi le cardinal de $\mathcal{S}_3$. Ainsi, le morphisme injectif Φ est aussi surjectif, d'où le résultat.

d) Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_3)$ est ici $(3^2 - 1).3 = 24$. Comme $\mathcal{S}_4$ est aussi de cardinal 24, Φ est bien un isomorphisme. De plus $\mathrm{PSL}_2(\mathbf{F}_3)$ est un sous-groupe d'indice 2 de $\mathrm{PGL}_2(\mathbf{F}_3)$ d'après a), car $\mathrm{pgcd}(2, 3 - 1) = 2$. Comme le seul sous-groupe d'indice 2 de $\mathcal{S}_4$ est $\mathcal{A}_4$ (pour $m \geq 2$, le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature), on en déduit que Φ induit un isomorphisme de $\mathrm{PSL}_2(\mathbf{F}_3)$ sur $\mathcal{A}_4$.

Bien qu'ils aient même cardinal, les groupes $\mathrm{PGL}_2(\mathbf{F}_3)$ et $\mathrm{SL}_2(\mathbf{F}_3)$ ne sont pas isomorphes, par exemple parce que $\mathrm{SL}_2(\mathbf{F}_3)$ a un centre non trivial (De cardinal 2) alors que le centre de $\mathrm{PGL}_2(\mathbf{F}_3) \simeq \mathcal{S}_4$ est réduit au neutre. Noter du reste que la même preuve que dans l'exercice 1. montre que les centres de $\mathrm{PGL}_n(K)$ et $\mathrm{PSL_n}(K)$ sont triviaux pour tout $n \geq 2$ (sur un corps quelconque).

e) Ici le cardinal de $\mathrm{PGL}_2(\mathbf{F}_4)$ est $(4^2 - 1).4 = 60$, et on a $\mathrm{PGL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_4)$ vu que $\mathrm{pgcd}(2, 4 - 1) = 1$. Ainsi Φ induit un des isomorphismes de $\mathrm{PGL}_2(\mathbf{F}_4)$ et $\mathrm{PSL}_2(\mathbf{F}_4)$ sur un sous-groupe d'indice 2 de $\mathcal{S}_5$, qui ne peut être que $\mathcal{A}_5$ comme on l'a vu plus haut.

f) Le cardinal de $\mathrm{PGL}_2(\mathbf{F}_5)$ est $(5^2 - 1).5 = 120$, ce qui montre que Φ induit un isomorphisme de $\mathrm{PGL}_2(\mathbf{F}_5)$ sur un sous-groupe d'indice 6 de $\mathcal{S}_6$, lequel est isomorphe à $\mathcal{S}_5$ d'après le résultat admis. Comme $\mathrm{pgcd}(2, 5-1) = 2$, on a encore que $\mathrm{PSL}_2(\mathbf{F}_5)$ est d'indice 2 dans $\mathrm{PGL}_2(\mathbf{F}_5) \simeq \mathcal{S}_5$, et il est donc isomorphe via Φ à $\mathcal{A}_5$.

On peut montrer que l'image de $\mathrm{PGL}_2(\mathbf{F}_5)$ par Φ, bien qu'isomorphe à $\mathcal{S}_5$ n'est pas conjugué des sous-groupes de $\mathcal{S}_6$ donnés par le stabilisateur d'un élément de $\{1, ..., 6\}$. Ce phénomène (existence d'un sous-groupe d'indice m non conjugué des stabilisateurs d'un point) ne se produit dans $\mathcal{S}_m$ que pour $m = 6$, et explique la présence dans $\mathcal{S}_6$ d'un automorphisme qui n'est pas intérieur. Voir le cours d'algèbre de D. Perrin pour plus de détails.

3. Il suffit de prendre $G = G_1 \times G_2$, où G_1 et G_2 sont deux groupes simples non abéliens (par exemple $G_1 = G_2 = \mathcal{A}_5$). Alors G n'est pas simple

car il contient les sous-groupes distingués non triviaux $G_1 \times \{1\}$ et $\{1\} \times G_2$. On voit tout de suite que le centre de G est le produit direct des centres de G_1 et G_2, et son sous-groupe dérivé est le produit des sous-groupes dérivés de G_1 et G_2, ce qui donne le résultat vu que pour un groupe simple non abélien H, le centre de H est trivial et son sous-groupe dérivé est H.

4. On voit très facilement que le centre Z de D consiste en $\{\pm 1\}$. Comme G/Z est abélien (il est de cardinal 4), son sous-groupe dérivé est inclus dans Z, c'est donc Z car ce ne peut pas être le groupe trivial vu que D n'est pas abélien. Comme tout élément g de D vérifie $g^2 \in Z$ (vérification immédiate), tous les éléments non triviaux de D/Z sont d'ordre 2, ce qui fait que ce groupe d'ordre 4 n'est pas cyclique, il est isomorphe à $(\mathbf{Z}/2)^2$.

Les règles de calcul dans $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ sont $ij = -ji = k$, $ki = -ik = j$, $jk = -kj = i$, ainsi que $i^2 = j^2 = k^2 = -1$. On voit alors que le centre de H_8 est $Z = \{\pm 1\}$. Comme pour D, on en déduit que le sous-groupe dérivé est Z et que l'abélianisé H_8/Z est isomorphe à $(\mathbf{Z}/2)^2$. Noter que D et H_8 ne sont pas pour autant isomorphes, car D possède cinq éléments d'ordre 2 alors que H n'en a qu'un.

5. Non : il suffit de prendre par exemple un groupe non-abélien G de cardinal 8 comme le groupe diédral. Son centre Z est non trivial (car G est un 2-groupe), donc le quotient G/Z est de cardinal au plus 4, ce qui implique G/Z abélien. C'est l'hypothèse G/Z *cyclique* qui implique G abélien (et donc $G = Z$).

6. a) Un tel groupe G est abélien car si x, y sont dans G, alors $x = x^{-1}$ et $y = y^{-1}$, mais aussi $(xy) = (xy)^{-1} = y^{-1}x^{-1}$, ce qui donne $xy = yx$. Notant alors G additivement, on a $2x = 0$ pour tout $x \in G$, et on a déjà vu qu'alors, G est isomorphe au groupe additif $(\mathbf{Z}/2)^r$ avec $r \in \mathbf{N}$ (car G est un $\mathbf{Z}/2$-ev de dimension finie). Réciproquement, un tel groupe convient bien.

b) Mais oui ! Sinon le cardinal de G aurait un autre diviseur premier, disons q; le théorème de Sylow implique alors que G contient un q-groupe non trivial, donc un élément d'ordre q^n avec $n \in \mathbf{N}^*$, ce qui contredit l'hypothèse que les éléments de G ont tous pour ordre une puissance de p (laquelle résulte de ce que $x^{p^m} = 1$ pour un certain m, pour tout $x \in G$).