Corrigé de l'entraînement sur les groupes, II

D. Harari

Agrégation

1. a) D'après le théorème de Lagrange, on $x^n = 1$ pour tout x de G. Comme χ est un morphisme, on a $1 = \chi(x^n) = \chi(x)^n$, ce qui montre que $\chi(x) \in \mu_n$.

b) Comme $\mathbf{C}^*$ est abélien, on a pour tout commutateur $xyx^{-1}y^{-1}$ (avec $x, y \in G$) :

$$\chi(xyx^{-1}y^{-1}) = \chi(x)\chi(y)\chi(x)^{-1}\chi(y)^{-1} = 1.$$

Ainsi $\ker \chi$ contient les commutateurs, donc il contient aussi $D(G)$ qui est le sous-groupe engendré par les commutateurs. On obtient ainsi une application u de $\widehat{G}$ dans $\widehat{G^{\mathrm{ab}}}$ en envoyant tout $\chi \in \widehat{G}$ sur le morphisme induit par factorisation $\tilde{\chi}$ de G^{ab} dans $\mathbf{C}^*$ (ce qui a un sens puisqu'on vient de voir que le noyau de χ contient $D(G)$). On a donc

$$u(\chi)(\bar{x}) = \chi(x)$$

pour tout $x \in G$, où $\bar{x}$ est la classe de x dans $G/D(G)$. La formule ci-dessus donne immédiatement que u est un morphisme de groupes injectif de $\widehat{G}$ dans $\widehat{G^{\mathrm{ab}}}$. Si maintenant ψ est dans $\widehat{G^{\mathrm{ab}}}$, l'élément χ de $\widehat{G}$ défini par $\chi(x) = \psi(\bar{x})$ vérifie $u(\chi) = \psi$, donc u est aussi surjectif.

c) Fixons un générateur a de G et une racine primitive n-ième de l'unité $\zeta \in \mathbf{C}^*$. On définit alors un élément χ_1 de $\widehat{G}$ en posant $\chi_1(a^m) = \zeta^m$ pour tout $m \in \mathbf{Z}$ (cette définition est légitime, car $a^m = a^s$ équivaut à $(m - s)$ divisible par n puisque a est d'ordre n, et on a bien alors $\zeta^m = \zeta^s$). On a clairement $\chi_1^n = 1$ et $\chi_1(a)^m \neq 1$ si m n'est pas divisible par n, vu que ζ est d'ordre n dans $\mathbf{C}^*$. Ainsi χ_1 est d'ordre n dans $\widehat{G}$. Enfin, si χ est un élément de $\widehat{G}$, il existe un entier m tel que $\chi(a) = \zeta^m = \chi_1(a)^m$ car on sait que $\chi(a)$ est dans μ_n, groupe qui est engendré par ζ. Comme χ et χ_1 sont des morphismes et G est engendré par a, on obtient $\chi = \chi_1^m$ dans $\widehat{G}$. Finalement $\widehat{G}$ est engendré par χ_1, ce qui montre qu'il est cyclique d'ordre n.

d) On sait que l'abélianisé de $\mathcal{S}_n$ est son quotient par son sous-groupe dérivé $\mathcal{A}_n$, ce qui implique que ce quotient est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. D'après b) et c), on en déduit que $\widehat{\mathcal{S}_n}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

2. Soit g le cardinal de G. Soit h le nombre de classes de conjugaisons de G. On sait qu'il y a h représentations irréductibles de G (à isomorphisme près) et que leurs degrés $n_1, ..., n_h$ sont des entiers > 0 qui vérifient

$$\sum_{i=1}^{h} n_i^2 = g.$$

Si G est abélien, il y a $h = g$ classes de conjugaison, donc la seule possibilité est que tous les n_i soient égaux à 1. Réciproquement, si tous les n_i sont égaux à 1, on obtient $g = h$, donc tout élément de G est seul dans sa classe de conjugaison, ce qui signifie exactement que G est abélien.

3. a) Si le cardinal de A possèdait un diviseur premier $\ell \neq p$, alors d'après le théorème de Sylow A contiendrait un ℓ-groupe non trivial, et donc un élément d'ordre ℓ^r avec $r > 0$. Comme par hypothèse l'ordre de tout élément de A est une puissance de p, on obtiendrait une contradiction.

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.

4. 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 ≥ 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 $[G : H] = p$.

5. a) Il suffit de montrer que les seules matrices qui commutent avec toutes les matrices de $\mathrm{SL}_n(K)$ sont les matrices scalaires. Soit A une telle matrice. Soit x un vecteur non nul de K^n. Alors il existe un endomorphisme u de K^n tel que Kx soit l'espace propre de u associé à la valeur propre 1 : on complète x en une base $(x, e_2, ..., e_n)$ de K^n, et on prend pour u l'endomorphisme dont la matrice dans cette base est $I_n + J$, où J est la matrice de Jordan de taille n. Comme l'endomorphisme associé à A commute avec u, il laisse stable Kx. Ainsi A laisse stable toute droite de K^n, et il est classique qu'alors A est une homothétie.

b) Rappelons que $\mathrm{GL}_n(K)$ a pour cardinal

$$g := (q^n - 1)(q^n - q)...(q^n - q^{n-1}).$$

Par ailleurs $\mathrm{PGL}_n(K)$ a pour cardinal $\frac{g}{q-1}$ puisque le centre de $GL_n(K)$ est isomorphe à K^* d'après a). Comme $\mathrm{SL}_n(K)$ est le noyau du morphisme surjectif det de $GL_n(K)$ dans $K*$, son cardinal est également $\frac{g}{q-1}$.

Il reste à déterminer le cardinal du centre de $\mathrm{SL}_n(K)$, c'est-à-dire d'après a) le cardinal de l'ensemble des $\lambda \in K^*$ vérifiant $\lambda^n = 1$. Comme on sait que K^* est cyclique d'ordre $q-1$, c'est aussi le cardinal de l'ensemble des solutions de l'équation $nx = 0$ dans $\mathbf{Z}/(q-1)\mathbf{Z}$, dont on voit immédiatement qu'il est égal au pgcd $d := (n, q-1)$. Finalement, le cardinal de $\mathrm{PSL}_n(K)$ est $\frac{g}{(q-1)(n,q-1)}$.

6. Non ! Il suffit de considérer n'importe quel groupe G non abélien de cardinal p^3 avec p premier (comme le groupe diédral d'ordre 8 par exemple). On sait que le centre Z de G est non trivial, donc G/Z est de cardinal p ou p^2, et on a vu que ceci implique G/Z abélien (en fait ce quotient est d'ailleurs forcément d'ordre p^2 car si G/Z est cyclique, on sait que G est abélien).

7. On note déjà que G est abélien car tout élement de G est son propre inverse, d'où

$$yx = y^{-1}x^{-1} = (xy)^{-1} = xy$$

pour tous x, y de G. Notons maintenant additivement la loi de G, on a donc $2x = 0$ pour tout x de G, ce qui permet de munir G d'une structure de $\mathbf{Z}/2\mathbf{Z}$-ev via $\bar{m}.x = mx$ pour tout $m \in \mathbf{Z}$, où $\bar{m}$ est la classe de m dans $\mathbf{Z}/2\mathbf{Z}$. Cet espace vectoriel est fini, donc de dimension finie d, ce qui montre que G est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^d$ (comme espace vectoriel, donc aussi comme groupe abélien). Réciproquement, les groupes additifs $(\mathbf{Z}/2\mathbf{Z})^d$ avec $d \in \mathbf{N}$ conviennent.

8. Soit S la dite partie génératrice, l'ensemble T composé des éléments de T et leurs inverses est encore fini. Pour tout $n \in \mathbf{N}$, notons G_n l'ensemble des éléments de G qui s'écrivent $x_1...x_n$ avec $x_i \in T$ pour tout i, alors G_n est fini car l'application $T^n \to G_n$ qui envoie $(x_1, ..., x_n)$ sur $x_1...x_n$ est surjective. Comme G est réunion dénombrable des G_n pour $n \in \mathbf{N}$, il est fini ou dénombrable.

La réciproque est fausse : on a déjà vu que le groupe additif $\mathbf{Q}$ n'est pas engendré par une partie finie.