Compléments de cours d'algèbre

Commentaires sur l'écrit blanc du 8/10/22

Je fais ici quelques commentaires sur des erreurs/confusions fréquentes que j'ai pu constatées en corrigeant les copies. Je vous invite bien entendu à consulter le rapport du jury 2022 lorsque celui-ci sera disponible sur le site `https://agreg.org/index.php?id=archives`.

Deux remarques d'ordre général en guise de préambule :

1. Ce sujet était très long (et mal fichu à mon avis). La rédaction est à optimiser dans ce cas pour ne pas se fatiguer outre-mesure. Je sais bien, c'est plus facile à dire qu'à faire ! Une indication tout de même : lorsque votre réponse commence à dépasser une page, c'est qu'il y a moyen de faire plus court (le découpage des questions était assez fin).
2. Le groupe de Heisenberg $\mathcal{H}_3(\mathbf{F}_p)$ étudié dans le problème est un bon exemple à avoir en tête : c'est un groupe fini non abélien d'ordre p^3 dans lequel tous les éléments sont d'ordre au plus p (si p est impair). Par exemple, cela montre que le résultat classique « si dans un groupe G tous les éléments sont d'ordre 2, alors G est abélien » n'admet pas d'analogue en remplaçant 2 par 3 par exemple ! Le groupe $\mathcal{H}_3(\mathbf{F}_2)$ est quant à lui isomorphe au groupe diédral D_4.

Barème

J'ai noté toutes les questions sur 1 points sauf les questions suivantes :

— les questions 7 et 8.d de l'exercice 1 ;

— les questions 1, 6.a et 8.b de l'exercice 2 ;

— la question 7 de l'exercice 3 ;

— la question 2.b de l'exercice 4 ;

— les questions 4, 13, 14 et 28 du problème.

(ne me demandez pas pourquoi ce choix : on en fait parfois de mauvais !). Il y avait donc 48 points sur les 4 premiers exercices (la moitié des points).

Commentaires

Exercice 1, question 5.a) Il s'agit de montrer ici que PMP^{-1} est **diagonale** et pas seulement diagonalisable. C'est-à-dire que $A = M^2$ et ses racines carrées M sont diagonalisables dans la même base. On peut procéder de plusieurs façons mais il faut de toute façon commencer par remarquer que A et M commutent. On peut alors argumenter des façons suivantes :

1. M laisse stable les espaces propres de A. Comme A possède n valeurs propres distincts, ces espaces propres sont des droites et M envoie donc ces droites dans elles-mêmes. Cela signifie exactement que dans une base de vecteurs propres de A, la matrice de M est diagonale.
2. On montre que M est diagonalisable : si 0 n'est pas valeur propre de A alors M est annulé par un polynôme à racines simples $\prod_{\lambda \in \mathrm{Sp}(A)}(X^2 - \lambda)$ et c'est bon. Sinon, il faut remarquer que $\dim(\mathrm{Ker}(M)) \leq \dim(\mathrm{Ker}(M^2)) = 1$ pour en conclure que M est annulé par $X \prod_{\lambda \in \mathrm{Sp}(A), \lambda \neq 0}(X^2 - \lambda)$ qui est encore à racines simples. Une fois que l'on sait ça, on peut invoquer le fait classique que deux matrices diagonalisables qui commutent sont simultanément diagonalisables.
3. Avec les notations de l'énoncé, on écrit que PMP^{-1} doit commuter avec $PAP^{-1} = D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ avec $\lambda_i \neq \lambda_j$ et on constate que pour $i \neq j$, on doit avoir
$$\lambda_i (PMP^{-1})_{i,j} = \lambda_j (PMP^{-1})_{i,j}$$
et donc que les coefficients non diagonaux de PMP^{-1} sont nuls.

Exercice 1, question 8.d) Pour vérifier si une matrice nilpotente encodée par la taille de ses blocs de Jordan $(n_1, \dots, n_r)$ admet une racine carrée, il vaut mieux lire les blocs de droite à gauche :

— Si $r = 0$, A admet une racine carrée et, si $r = 1$, alors A admet une racine si et seulement si $n = 1$.

— Si $r \geq 2$ et $n_r \geq n_{r-1} + 2$, alors A n'a pas de racines.

— Sinon, on appelle l'algorithme pour $(n_1, \dots, n_{r-2})$.

Exercice 2, question 6.a) Pour montrer l'injectivité, on doit commencer par remarquer que $\mathbf{F}[N] = \mathbf{F}[2N + N^2] = \mathbf{F}[2M + M^2] = \mathbf{F}[M]$. Mais cela ne suffit pas ! Il faut en déduire que N et M commutent et ensuite, on peut par exemple écrire :
$$0 = 2N + N^2 - 2M - M^2 = (N - M)(2I_n + N + M)$$
et, comme N et M commutent, $N + M$ est nilpotente et donc $2I_n + N + M$ est inversible (question 4). Finalement, on obtient $N = M$.

Exercice 2, question 8.b) Si on écrit la décomposition de Jordan–Chevalley (Dunford) sous la forme $M = D + N = D(I_n + D^{-1}N)$ habituelle, alors il n'est pas complètement évident de montrer que M est un carré. En effet, D est diagonalisable inversible donc s'écrit $D = P^2$ (question 8.a) avec P inversible et $I_n + D^{-1}N$ est unipotente donc c'est aussi un carré (question 7). Mais ensuite il faut se fatiguer pour montrer que l'on peut choisir U et P qui commutent car il faut pouvoir écrire $M = P^2U^2 = (PU)^2$! ! C'est possible mais un peu long. Une façon économique est d'écrire la décomposition sous la forme suivante : la décomposition en sous-espaces caractéristiques montre que M est semblable à une matrice de la forme
$$\mathrm{diag}\left(\lambda_1 I_{k_1} + N_1, \dots, \lambda_r I_{k_r} + N_r\right)$$

avec k_i la multiplicité de λ_i dans le polynôme caractéristique de M et N_i la restriction de $M - \lambda_i \,\mathrm{id}$ au sous-espace caractéristique associé à λ_i (qui est donc nilpotente). On applique alors la question 7 à chaque bloc : comme M est inversible, $\lambda_i \neq 0$ et $I_{k_i} + \frac{1}{\lambda_i} N_i$ est unipotente. C'est donc un carré ; en multipliant par une racine carrée de λ_i, on obtient une racine sur le bloc i et donc une racine carrée de M.

Exercice 3 Le corps $\mathbf{K}$ est une clôture algébrique de $\mathbf{F}_p$. Ce corps est de **cardinal infini** ! En effet, un corps fini n'est jamais algébriquement clos : si K est un corps fini, alors le polynôme $P(X) = \prod_{x \in K}(X - x) + 1$ est un polynôme qui n'a aucune racine dans K.

Exercice 3, question 6 Il ne fallait pas oublier de dire que $\mathbf{L}$ est un sous-corps de $\mathbf{K}$!

Exercice 4 Il fallait utiliser plusieurs fois l'identité $(A + B)^p = A^p + B^p$ qui est valable dans $M_n(\mathbf{F}_p)$ **si A et B commutent** (on l'utilisait dans cet exercice avec $B = I_n$).

Problème, question 2.b) Pour dire qu'un élément g est d'ordre 1 ou p (un nombre premier) dans un groupe G, il suffit de vérifier que $g^p = 1$. En effet, dans ce cas l'ordre de g divise p ! La vérification $h(x, y, z)^p = I_3$ pour $p \geq 3$ premier est alors évidente.

Problème, question 2.c) Ici $p = 2$ et la question précédente ne s'applique pas. Il faut vérifier que $h(x, y, z)^4 = 1$: les ordres possibles sont donc 1, 2 ou 4. Ensuite, il faut montrer que ces valeurs sont atteintes ! Par exemple avec $h(1, 0, 0)$ et $h(1, 1, 0)$.

Problème, question 6 On travaille ici dans $\widehat{G}$ (avec G un groupe, le groupe additif d'un corps $(F, +)$ dans notre cas). L'ensemble $\widehat{G}$ est un groupe pour la multiplication des morphismes : $\varphi \cdot \psi(x) := \varphi(x)\psi(x)$ (et là c'est juste la multiplication de deux nombres complexes non nuls). L'élément neutre pour cette multiplication est donc la fonction $\mathbf{1} : G \to \mathbb{C}^\times$ qui vaut 1 tout le temps ! Pour montrer l'injectivité de j, j'ai vu parfois des équations du type $\psi_1 \otimes \psi_2 = \mathrm{id} \ldots$

Problème, partie II La fonction $\Phi(g) = g^2$ n'est pas un morphisme de groupes en général ! C'est seulement le cas si G est abélien. De même, l'application $m(x^-, x^+) = x^- x^+$ n'est pas un morphisme de $G^- \times G^+$ dans G ; de toute façon, G^- n'est même pas un sous-groupe en général.

J'arrête là car seules 2 ou 3 étudiants ont attaqué les dernières parties.