Université Montpellier II **Année universitaire 2012-2013**
L3 Mathématiques, GLMA501

Corrigé Examen d'algèbre générale
vendredi 18 janvier 2013
Durée : 3h

Documents et calculatrices sont interdits. Toutes les réponses doivent être justifiées. Il sera tenu compte du soin apporté à la rédaction.

Exercice 1 *[4 points]* Soit la matrice

$$A = \begin{pmatrix} 4 & 5 & 2 \\ -3 & -4 & -1 \\ -1 & -1 & 3 \end{pmatrix}.$$

1. Déterminer le polynôme minimal et une réduite de Jordan de A.
   Par calcul on trouve $\chi_A(X) = (X-2)^2(X+1)$, et comme on sait que μ_A divise χ_A et a les mêmes racines, on en déduit que μ_A vaut soit $(X-2)^2(X+1)$ soit $(X-2)(X+1)$. Il ne reste plus qu'à tester si $(X-2)(X+1)$ est anulateur de A, ce qui n'est pas le cas (faire rapidement le calcul de quelques coefficients). Du polynôme minimal, on déduit que la réduite de Jordan de A, notée J_A, a au moins un bloc de taille 2 associé à la valeur propre 2 et un bloc de taille 1 associé à la valeur propre -1 (et ce sont les tailles maximales). Mais en fait, il suffit d'avoir ces deux blocs pour reconstituer une matrice de taille $3*3$, d'où (à permutation près des blocs)

$$J_A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

2. En déduire une expression de l'inverse de A en fonction de A.
   On utilise le polynôme minimal : on sait que $(X-2)^2(X+1) = X^3 - 3X^2 + 4$ est annulateur. Donc :

$$A^3 - 3A^2 + 4I_3 = 0 \Leftrightarrow A(A^2 - 3A) = -4I_3 \text{ et donc } A^{-1} = -\frac{1}{4}(A^2 - 3A).$$

Exercice 2 *[5 points]* On considère un sous-groupe fini G de $GL_n(\mathbb{C})$ *d'exposant* 2, c'est-à-dire tel que toute matrice A de G vérifie $A^2 = I_n$.

1. Montrer que G est un groupe abélien.
   On sait déjà que c'est un sous-groupe (par l'énoncé) il ne reste qu'à vérifier le caractère abélien. Soient $A, B \in G$, AB est encore dans G (structure de groupe) et donc

$$(AB)^2 = ABAB = I_n \Leftrightarrow BA = A^{-1}B^{-1} = AB.$$

2. Montrer que toute matrice de G est diagonalisable et a pour valeurs propres -1 ou $+1$.
   Soit $M \in G$. Le polynôme (scindé à racines simples) $X^2-1 = (X+1)(X-1)$ est annulateur de M, donc M est diagonalibsable et les valeurs propres de M sont dans $\{-1, +1\}$.

3. Démontrer qu'il existe une base de $\mathbb{C}^n$ dans laquelle toutes les matrices de G sont diagonalisables (si vous utilisez un résultat du cours, il faut le redémontrer ou au moins donner l'idée de la démonstration).

Les matrices de G sont toutes diagonalisables et elles commutent toutes entres-elles. Pour répondre à la question, il suffit de dire que les matrices de G sont diagonalisables ***dans une même base****. Voici les idées pour redémontrer cette propriété de co-diagonalisabilité pour deux endormorphismes f et g : écrire l'espace total comme somme directe des sous-espaces propres de f. g commutant à f, g stabilise chacun des sous-espaces propres de f. On peut donc considérer l'induit de g sur chacun des espaces propres, qu'on note g_i (l'induit sur le i-ème espace propre de f). On peut alors montrer que g_i est diagonalisable : il s'agit juste d'observer que le polynôme minimal de g annule g_i, donc le polynôme minimal de g_i divise le polynôme minimal de g (qui est scindé à racines simples car g est lui même diagonalisable). On a donc une base de diagonalisation de g_i sur le i-ème espace propre. Si on recolle toutes ces bases, on trouve une base de l'espace total dans laquelle f et g sont diagonales. Maintenant qu'on a le résultat pour deux endomorphismes, par récurrence, c'est également valable pour un nombre fini d'endomorphismes. C'est ce qu'il nous faut.*

4. Déterminer un majorant de l'ordre de G, et montrer que ce majorant est atteint si l'on choisit G convenablement.
   Avec les questions précédentes, on sait qu'il existe une base dans laquelle toutes les matrices de G sont diagonales avec des ± 1 comme coefficients diagonaux. Il y a donc au plus 2^n telles matrices diagonales; et donc $|G| \leq 2^n$. Maintenant, si on choisit $G := \{$matrices diagonales avec des $\pm 1\}$, on vérifie facilement que c'est un groupe d'exposant 2 et qu'il est précisément de cardinal 2^n.

5. On suppose maintenant qu'il existe un isomorphisme entre $GL_n(\mathbb{C})$ et $GL_m(\mathbb{C})$. En utilisant ce qui précède, montrer que $n = m$.
   Si on dispose d'un tel isomorphisme, on doit avoir égalité du cardinal maximal des sous-groupes finis d'exposant 2 dans chacun des deux groupes linéaires (car l'isomorphisme respecte la propriété d'être d'exposant 2). C'est-à-dire qu'on doit avoir $2^n = 2^m$, ce qui force $n = m$.

Exercice 3 *[2 points]* Soit l'application $f : \mathbb{Z}^2 \to \mathbb{Z}$, $(x, y) \mapsto 2x + 6y$.

1. Montrer que f est un morphisme de groupes.

2. Montrer que le groupe quotient $\mathbb{Z}^2/\mathbb{Z}(-3, 1)$ est isomorphe au groupe $2\mathbb{Z}$.
   On veut utiliser un théorème d'isomorphisme, on va donc essayer de montrer que $\mathbb{Z}(-3, 1)$ est le noyau d'un certain morphisme de groupe et $2\mathbb{Z}$ son image. On se sert du morphisme donné à la question précédent et on vérifie que son noyau et son image conviennent. Les vérifications ne sont pas très dures mais il ne faut oublier aucun sens si on le fait par des doubles inclusions.

Exercice 4 *[5 points]* Soit $f : G \to H$ un morphisme de groupes finis, et G' un sous-groupe de G.

1. Montrer que l'ordre de $f(G')$ divise l'ordre de G' et l'ordre de H.
   $f(G')$ étant un sous-groupe de H, son ordre divise celui de H par le théorème de Lagrange. Pour l'autre partie de la question, il faut utiliser un théorème d'isomorphisme : on note $g : G' \to H$ la restriction de f à G', alors on a $G'/\ker g \simeq \text{im } g = f(G')$. En prenant les cardinaux, on trouve le résultat.

2. On suppose que les ordres de G' et de H sont premiers entre eux. Montrer que $G' \subset \text{Ker}(f)$.
   Le cardinal de $f(G')$ divise deux nombres qui sont premiers entre eux, il est donc égal à 1. On en déduit que $G' \subset \ker f$.

3. On suppose que les ordres de G' et de H sont premiers entre eux, que l'ordre de H est un nombre premier, et que le produit des ordres de H et de G' est égal à l'ordre de G. Montrer que si $\mathrm{Im}(f) \neq \{e_H\}$, alors H est isomorphe à G/G' via f.
$|H|$ est un nombre premier et $\mathrm{im}\ f \neq \{e\}$ *donc* $\mathrm{im}\ f = H$ *(car* $\mathrm{im} f \subset H$ *et son cardinal divise celui de H, qui est premier). Cela signifie simplement que f est surjectif. De plus, comme $|H||G'| = |G|$ et $|G| = |imf||kerf| = |H||kerf|$, on a $|G'| = |kerf|$. On déduit de la question précédente que $G' = kerf$, et par passage au quotient que f induit un morphisme injectif $\overline{f} : G/G' \longrightarrow H$. f étant sujectif, il en est de même de $\overline{f}$. C'est donc un isomorphisme.*

Exercice 5 *[5 points]* Soient p et q deux nombres premiers distincts. Le but de l'exercice est de montrer qu'un groupe d'ordre p^2q n'est jamais *simple*, c'est-à dire qu'il admet toujours un sous-groupe distingué différent de lui-même et de l'élément neutre. On suppose que G est un groupe simple d'ordre p^2q.

1. On note n_p et n_q le nombre de p-Sylow et de q-Sylow de G.

   (a) Montrer que $n_p = q$, et que p divise $q - 1$.
   On applique le théorème de Sylow : $n_p = 1[p]$ et $n_p|q$ (en particulier $n_p = 1$ ou q). Or, G étant supposé simple, $n_p \neq 1$, sinon l'unique p-Sylow serait distingué. On en déduit donc $n_p = q$. Traduisons maintenant la première condition du théorème de Sylow : $n_p = 1[p] \Leftrightarrow p|n_p - 1$. Comme $n_p = q$, on a ce qu'il faut.

   (b) En utilisant n_q, montrer que q divise $p + 1$ ou $p - 1$.
   On applique encore le théorème de Sylow : $n_q = 1[q]$ et $n_q|p^2$. De la seconde condition, on en déduit $n_q = p$ ou p^2 (car $n_q \neq 1$ pour les mêmes raisons que ci-dessus) et donc $q|n_q - 1$ se traduit en $q|p-1$ ou $q|p^2-1 = (p-1)(p+1)$. Dans tous les cas on trouve que q divise $p + 1$ ou $p - 1$.

2. En déduire que $p = 2$ et $q = 3$.
On sait que $p|q - 1$ donc en particulier $p \leq q - 1$. Supposons que $q|p - 1$, alors $q \leq p - 1$; et donc $p \leq q - 1 \leq p - 2$ ce qui n'est pas possible. Donc nécessairement, $q|p + 1$ et en particulier $q \leq p + 1$. Mais alors : $q \leq p + 1 \leq (q - 1) + 1 = q \Longleftrightarrow q = p + 1$. Ainsi p, q sont des nombres premiers consécutifs, nécessairement : $p = 2, q = 3$.

3. Montrer qu'un groupe d'ordre 12 ne peut pas être simple. Conclure.
Appliquons les théorèmes de Sylow à un groupe d'ordre $12 = 2^2 \times 3$: $n_2 = 1[2]$ et $n_2|3$; donc $n_2 \in \{1, 3\}$. De la même façon, $n_3 = 1[3]$ et $n_3|4$; donc $n_3 \in \{1, 4\}$. Par l'absurde, supposons que le groupe d'ordre 12 est simple, alors on aurait nécessairement $n_2 = 3$ et $n_3 = 4$. Les éléments non neutres des différents 3-Sylow sont distincts : si on prend deux 3-Sylow (de cardinal 3), leur intersection est un sous-groupe strict des deux 3-Sylow et donc, par le théorème de Lagrange, l'intersection est de cardinal 1. Il y a donc $4 \times (3-1)+1 = 9$ éléments répartis dans les 3-Sylow. Il reste alors juste assez d'éléments pour constituer un seul 2-Sylow (de cardinal 4). Contradiction.

   Le fait que les éléments non neutres des différents 3-Sylow sont distincts est crucial et ça n'est pas vrai si on regarde les 2-Sylow (de cardinal 4) ! C'est-à-dire qu'on peut trouver un élément (qui n'est pas le neutre) commun à deux 2-Sylow différents.

   Conclusion : on a montré que si un groupe d'ordre p^2q était simple, nécessairement $p = 2, q = 3$; et un tel groupe est donc de cardinal 12. Or on a montré (indépendamment) que les groupes d'ordre 12 sont tous non simples. Autrement dit, les groupes d'ordre p^2q ne peuvent pas être simples.