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

Algèbre générale
Corrigé de l'examen du 10 juin 2013

Exercice 1 (5 points) On considère dans $M_3(\mathbb{R})$ la matrice

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

dont le polynôme caractéristique est $\chi_A(X) = (X-\alpha)^2(X-2)$.

1. Déterminer α.
2. Mettre A sous forme de Jordan en précisant la matrice de passage.
3. Quel est le polynôme minimal de A ?
4. Donner en fonction de $n \in \mathbb{N}$ l'expression de la suite récurrente donnée par

$$X_{n+1} = AX_n \ , \ X_0 = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}.$$

1. On calcule sans difficulté le polynôme caractéristique de A :

$$\chi_A(X) = \det(XI_3 - A) = (X-1)^2(X-2).$$

Donc $\alpha = 1$.
2. Le sous espace propre E_1 est engendré par le vecteur $(1,-1,0)^t$. Comme E_1 est de dimension 1 et la valeur propre 1 est de multiplicité 2 dans χ_A, A n'est pas diagonalisable. Une forme normale de Jordan A' de A a au moins un bloc de Jordan pour chaque valeur propre, de taille égale à sa multiplicité. À permutation près des blocs on a donc

$$A' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

La matrice $(A-I_3)^2$ est de rang 1, de noyau le sous-espace caractéristique $N_1 = \{x+y+z=0\}$. Soit u un vecteur de $\in N_1 \setminus E_1$, par exemple $u = (0,1,-1)^t$. Les vecteurs $v_0 = (A-I_3)(u)$ et $v_1 = u$ forment une base de N_1 dans laquelle on a $A(v_0) = v_0$ et $A(v_1) = v_0 + v_1$. Soit v_2 un vecteur propre de A pour la valeur propre 2, par exemple $v_2 = (1,-1,1)^t$. Alors la matrice P dont les colonnes sont v_0, v_1 et v_2 vérifie $A' = P^{-1}AP$. Avec les choix de u et v_2 ci-dessus on trouve

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

3. Le polynôme minimal m_A de A divise χ_A et a pour racines les valeurs propres de A. Donc $m_A(X)$ vaut $(1-X)^2(2-X)$ ou $(1-X)(2-X)$. Comme A n'est pas diagonalisable, ses racines ne sont pas toutes les deux simples. Donc $m_A(X) = (X-1)^2(X-2)$.
4. On pose $Y_n = P^{-1}X_n$. Alors $Y_{n+1} = P^{-1}X_{n+1} = P^{-1}AX_n = P^{-1}APP^{-1}X_n = A'Y_n$, d'où l'on déduit $Y_n = (A')^nY_0$. En décomposant A' en ses parties diagonale et nilpotente (qui commutent) et en utilisant la formule du binôme de Newton (qu'on peut appliquer), on obtient

$$Y_n = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right)^n Y_0 \tag{1}$$

$$= \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2^n \end{pmatrix} + n \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \right) Y_0 \tag{2}$$

$$= \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2^n \end{pmatrix} Y_0. \tag{3}$$

$$\tag{4}$$

L'expression de X_n, $n \in \mathbb{N}$, vient en calculant Y_0 et en appliquant P aux deux membres.

Exercice 2 (2 points) Soit G un groupe cyclique d'ordre n et g un générateur de G.

1. Soit $k \in \mathbb{Z}$. Montrer que l'application $\varphi_k : G \to G$ telle que $\varphi_k(g^l) = g^{lk}$ est un morphisme.
2. Donner une condition nécessaire et suffisante sur k pour que φ_k soit inversible. En déduire que les automorphismes de G sont en bijection avec les entiers $k \in \{1, 2, \ldots, n\}$ qui sont premiers à n.

1. Appliquer la définition d'un morphisme (rappeler que g est d'ordre n et $G = \{e_G, g, \ldots, g^{n-1}\}$).
2. Puisque φ_k est un morphisme de G dans G, φ_k est inversible si et seulement si $\mathrm{Ker}(\varphi_k) = \{e_G\}$. On a $g^l \in \mathrm{Ker}(\varphi_k)$ si et seulement si $g^{lk} = e_G$, et $g^{lk} = e_G$ si et seulement si l'ordre de g divise lk (vu de nombreuses fois en TD). Maintenant, si n et k sont premiers entre eux, il n'existe pas d'entier $0 < l < n$ tel que n divise lk, et donc φ_k est inversible. Inversement, si n et k ont des diviseurs communs, alors $l = n/pgcd(n,k)$ est tel que n divise lk et $0 < l < n$, et donc φ_k n'est pas inversible. Finalement, une CNS pour que φ_k soit inversible est que $pgcd(n,k) = 1$. Tout (auto)morphisme de G est de la forme φ_k, pour un certain $k \in \mathbb{Z}$, et $\varphi_k = \varphi_{k'}$ si et seulement si $k' = k \ mod(n)$, donc on peut restreindre k à l'ensemble $\{1, 2, \ldots, n-1\}$. La conclusion s'ensuit.

Exercice 3 (2 points) Montrer que si un groupe fini G a pour seuls sous-groupes $\{e_G\}$ et lui-même, alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Soit $g \in G$. D'après l'hypothèse le sous-groupe de G engendré par g est soit le groupe trivial, et alors $g = e_G$, soit égal à G. Dans ce dernier cas g est un générateur de G, et donc G est cyclique. D'après le cours, tout groupe cyclique d'ordre n admet un (et un seul) sous-groupe d'ordre d, pour chaque diviseur n/d de n. Ici les seuls diviseurs de l'ordre de G sont 1 et lui-même. Donc l'ordre de G est premier.

Exercice 4 (3 points) Soit G un groupe et H un sous-groupe distingué de G d'indice fini p premier.

1. Déterminer l'ordre de G/H. Montrer qu'il existe un morphisme surjectif f de G vers $\mathbb{Z}/p\mathbb{Z}$.

2. Montrer que pour tout élément $g \in G$, l'ordre de $f(g)$ est égal à 1 ou p. En déduire que $g^p \in H$.

3. Montrer que si l'on ne suppose plus que l'indice de H dans G est premier, mais un entier n quelconque, on a encore $g^n \in H$.

1. Par définition $|G/H| = [G : H] = p$. Or tout groupe fini d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Alors $G/H \cong \mathbb{Z}/p\mathbb{Z}$, et la composée de la projection canonique $\pi : G \to G/H$ et d'un isomorphisme $G/H \to \mathbb{Z}/p\mathbb{Z}$ est un morphisme surjectif f.
2. D'après le théorème de Lagrange l'ordre de $f(g)$ est un diviseur de $p = |\mathbb{Z}/p\mathbb{Z}|$. Il est donc égal à 1 ou p. Alors $f(g^p) = f(g)^p = \bar{1} \in \mathbb{Z}/p\mathbb{Z}$, soit $g^p \in \mathrm{Ker}(f) = H$.
3. On considère encore la projection canonique $\pi : G \to G/H$. Pour tout élément $g \in G$, l'ordre de $\pi(g)$ divise $n = |G/H| = [G : H]$, donc $\pi(g^n) = \pi(g)^n = e_{G/H}$, ce qui donne finalement $g^n \in \mathrm{Ker}(\pi) = H$.

Exercice 5 (8 points) Soit G un groupe d'ordre 10.

1. Montrer que G possède un élément τ d'ordre 2 et un élément σ d'ordre 5.

2. Soit H le sous-groupe de G engendré par σ. Montrer que $\tau H \tau = H$.

3. On suppose que $\tau\sigma = \sigma\tau$. Construire un isomorphisme de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ vers G.

4. On suppose que $\tau\sigma \neq \sigma\tau$.

   (a) Montrer que l'application $\varphi : H \to H$ donnée par $\sigma^l \mapsto \tau\sigma^l\tau$ vérifie $\varphi \circ \varphi = id_H$.

   (b) Déterminer les valeurs possibles de $\tau\sigma\tau \in \{e_G, \sigma, \sigma^2, \sigma^3, \sigma^4\}$.

   (c) En utilisant l'ordre de G, déduire que G est engendré par τ et σ vérifiant la relation $\tau\sigma\tau = \sigma^{-1}$.

1. D'après les théorèmes de Sylow, $|G| = 2 \cdot 5$ donne $n_2 \in \{1, 5\}$ sous-groupes 2-Sylow et $n_5 = 1$ sous-groupes 5-Sylow de G.
2. D'après les théorèmes de Sylow, tous les sous-groupes 5-Sylow de G sont conjugués. Comme il n'y en a qu'un, il est distingué.
3. On considère l'application $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to G$ qui à $(\bar{a}, \bar{b})$ associe $\tau^a\sigma^b$. Cette application est bien définie, car τ (resp. σ) étant d'ordre 2 (resp. 5), τ^a (resp. σ^b) ne dépend que de a mod(2) (resp. b mod(5)). Clairement cette application est un morphisme de groupes (appliquer la définition; noter que σ et τ commutent nécessairement puisque la loi de groupe du produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ est commutative). Ce morphisme est injectif, car $\sigma^a\tau^b = e_G$ équivaut à $\sigma^a = \tau^{-b}$, ce qui implique que σ^a appartient simultanément aux sous-groupes de G engendrés par σ et τ; or deux sous-groupes de G d'ordres premiers entre eux ont pour seul élément commun l'élément neutre. Les groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et G ayant même cardinal, c'est un isomorphisme.
4. (a) La vérification est immédiate.
(b) On a bien $\tau\sigma\tau \in H$, puisque $H =< \sigma >$ est distingué dans G, et $H = \{e_G, \sigma, \sigma^2, \sigma^3, \sigma^4\}$ car σ est d'ordre 5. Soit $k \in \{0, 1, 2, 3, 4\}$ tel que $\tau\sigma\tau = \sigma^k$. Alors $\sigma = \tau\sigma^k\tau = \tau\sigma\tau \ldots \tau\sigma\tau$ (k fois), d'où $\sigma = \sigma^{k^2}$. On cherche donc k tel que $k^2 = 1$ mod(5). On vérifie immédiatement que seuls $k = 1$ et $k = 4$ conviennent. Mais $k = 1$ implique $\tau\sigma = \sigma\tau$, qui est exclu par hypothèse. Donc $\tau\sigma\tau = \sigma^4 = \sigma^{-1}$.
(c) En utilisant la relation $\tau\sigma\tau = \sigma^{-1}$ on trouve que le sous-groupe engendré par τ et σ consiste en les dix éléments de G de la forme $\tau^k\sigma^l$, avec $k = 0, 1$ et $l = 0, \ldots, 4$, tous distincts. Comme G est d'ordre 10, ces deux groupes coincident.