Université de Tours et d'Orléans **M2 2019-2020**

Examen du module Compléments d'algèbre

2 Juillet 2020

Exercices à chercher

Exercice 1 :

1) Un groupe G à 33 éléments agit sur un ensemble X à 19 éléments. Démontrer qu'il y a nécessairement un point fixe sous l'action de G.

2)a)Soit G un groupe d'ordre $n > 1$ et p le plus petit diviseur premier de n. Soit H un sous-groupe d'indice p de G, et $G/H = \{gH, g \in G\}$. En faisant agir H sur G/H, démontrer que H est distingué dans G.

b) En déduire qu'un groupe à 147 éléments ne possède qu'un sous-groupe à 49 éléments .

Exercice 2 :

On considèe le corps fini $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ ayant p éléments, p étant un premier impair et le $\mathbb{K}$–espace vectoriel $\mathsf{E} = \mathbb{K}^n$. On consid ?ère l'ensemble des matrices

$$\mathsf{G} = \left\{ M_{a,b,c} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \ / \ a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

1)a) Etablir que G est un sous-groupe, de cardinal p^3, de $\mathrm{SL}_3(\mathbb{K})$, groupe des matrices 3×3 à coefficients dans $\mathbb{K}$ et de déterminant 1.

b) Démontrer que G est non commutatif et que tout élément de G est d'ordre p.

c) Que représente G pour $\mathrm{SL}_3(\mathbb{K})$ (on calculera le cardinal de $\mathrm{SL}_3(\mathbb{K})$) ? Est-il distingué dans $\mathrm{SL}_3(\mathbb{K})$?

2) a) Démontrer directement (sans calcul) que $|Z(G)| = p$ puis déterminer les matrices de $Z(G)$.

b) On pose $H = Z(G) < T_1 >= \{zt, z \in Z(G), t \in < T_1 >\}$, où $T_1 = M_{(1,0,0)}$. Démontrer que H est un sous-groupe de G de cardinal p^2.

c) Etablir que $G \simeq H \rtimes < T_3 >$ si $T_3 = M_{(0,0,1)}$. On pourra utiliser l'exercice 1.

Exercice 3 : Un peu d'ordre et d'automorphismes

Soit p un nombre premier impair. On considè ?re le groupe multiplicatif $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ du corps $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ et on donne une preuve qu'il est cyclique ainsi que $\mathbb{U}(\mathbb{Z}/p^2\mathbb{Z})$.

1) a) Etablir que pour tout facteur premier q de $p-1$, il existe un élément x d'ordre q dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$.

b)Soit $\alpha = v_q(p-1)$, la valuation de q dans $p-1$. Pour chaque $x \in \mathbb{K}^*$, établir que l'ordre de $y_x = x^{\frac{p-1}{q^\alpha}}$ divise q^α ; on note $o(y_x) = q^{r_x}$. On pose $r = \mathrm{Max}_{x \in \mathbb{K}^*}(r_x)$.

c)En considérant le polynôme $X^{\frac{p-1}{q^{\alpha-r}}} - 1$ de $\mathbb{K}[X]$, établir qu'il existe dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ un élément d'ordre q^α (ie que $r = \alpha$).

d)En déduire que $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique. On red ?émontrera que si $x_1, \ldots, x_k$ sont k éléments d'un groupe commutatif $(G, .)$, d'ordres respectifs $q_1, \ldots, q_k$, où l'on suppose que les entiers q_i sont premiers deux à deux, alors l'élément $x_1.x_2 \ldots x_k$ est d'ordre $q_1.q_2 \ldots .q_k$.

2) a) Rappeler pourquoi $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \simeq \mathbb{U}(\mathbb{Z}/p^2\mathbb{Z})$.

b) Démontrer que $v = \tilde{1} + \tilde{p}$ est d'ordre p dans $\mathbb{U}(\mathbb{Z}/p^2\mathbb{Z})$.

c) Etablir que si $u \in \mathbb{Z}$ est tel que $\bar{u}$ engendre $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ et si c désigne l'ordre de la classe de $\tilde{u}$ modulo p^2, alors $p-1$ divise c.

d) En déduire qu'il existe un élément $x = vw$ d'ordre $p(p-1)$ dans $\mathbb{U}(\mathbb{Z}/p^2\mathbb{Z})$ et que $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$, comme $\mathbb{U}(\mathbb{Z}/p^2\mathbb{Z})$, est cyclique, isomorphe ? $\mathbb{Z}/p(p-1)\mathbb{Z}$.
3) En vous inspirant d'un résultat vu lors de la classification des groupes d'ordre pq, montrez grâce à ce qui précède, que tous les produits semi-directs $\mathbb{Z}/p^2\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ sont isomorphes.

Exercice 4 : un grand classique
On pose : $\varphi : (\mathbb{M}_n(\mathbb{R}))^2 \mapsto \mathbb{R}$ avec $\varphi(A, B) = \mathrm{trace}(AB)$.
1) Etablir que φ est une forme bilinéaire symétrique.
2) Déterminer le noyau , le rang et la signature de la forme quadratique q associée à φ.

Exercice 5 :
1) Démontrer le résultat suivant :
Théorème de pseudo Réduction simultanée : si $A \in \mathbb{S}_n^{++}$ et $B \in \mathbb{S}_n$, il existe une matrice de $P \in GL_n(\mathbb{R})$ et D une matrice diagonale réelle de sorte que

$$ {}^tPAP = I_n \quad \text{et} \quad {}^tPBP = D.$$

2) Soient $A_1, \dots A_k$ une famille de matrices symétriques positives de $\mathbb{M}_n(\mathbb{R})$ et $(\lambda_1, \dots \lambda_k)$ un k-uplet de réels. On veut établir que :

$$(*) \qquad |\det(\sum_{i=1}^{k} \lambda_i A_i)| \leq \det(\sum_{i=1}^{k} |\lambda_i| A_i)|.$$

On pose $H = \sum_{i=1}^k \lambda_i A_i$ et $K = \sum_{i=1}^k |\lambda_i| A_i$ et on désigne par q_H et q_K les formes quadratiques associées dans $\mathbb{R}^n$.
a) Comparer $|q_H|$ et q_K.
b) On suppose dans un premier temps que K est inversible. Etablir, grâce à la question 1) et à l'inégalité du a) , que les valeurs propres de $K^{-1}H$ sont réelles et dans l'intervalle $[-1, 1]$.
c) En déduire l'inégalité $(\star)$.
d) On suppose que $\det(K) = 0$. Démontrer que l'inégalité $(*)$ est toujours satisfaite .
Ind : On pourra ajouter une $k+1$ ème matrice $A_{k+1} = I_n$.

Exercice 6 : Déterminants, Formes quadratiques et racines de polynômes
Où l'on rencontre deux déterminants classiques et leur lien avec les polynômes.
A) Etant donnés $K+1$ nombres complexes $(y_0, \dots, y_K)$, on pose

$$V(y_0, \dots, y_K) = \begin{vmatrix} 1 & 1 & \cdots & 1 & \cdots & 1 \\ y_0 & y_1 & \cdots & y_j & \cdots & y_K \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y_0^k & y_1^k & \cdots & y_j^k & \cdots & y_K^k \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y_0^K & y_1^K & \cdots & y_j^K & \cdots & y_K^K \end{vmatrix} = \det(A)$$

On considère le polynôme P unitaire ayant comme racines les $(y_i)_{K \in \{0,\dots,K\}}$.
1)a) Etablir qu 'il existe des complexes $(\lambda_i)_{K \in \{0,\dots,K-1\}}$ de sorte que

$$P(X) = X^{K+1} + \lambda_K X^K + \dots, \lambda_0$$

b) Si L_j désigne la j-ième ligne de la matrice A ci-dessus, calculer :

$$L_{K+2} + \lambda_K L_{K+1} + \dots, \lambda_0 L_1$$

c) En déduire que $V(y_0,\dots,y_K) = P(y_K)V(y_0,\dots,y_{K-1})$.
d) En déduire la valeur de $V(y_0,\dots,y_K)$.

2) Proposer une autre méthode de calcul classique du détermiannt de Vandermonde $V(y_0,\dots,y_K)$.

B) Soit $f \in \mathbb{R}[X]$, de racines $x_1, x_2, \dots, x_n$ dans $\mathbb{C}$, distinctes ou non. On associe à f la matrice suivante (dite matrice de Hankel), formée avec les sommes p_k des puissances k–ième des racines, $p_k = \sum_{i=1}^{n} x_i^k$:

$$H = \begin{pmatrix} n & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \vdots & \vdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{pmatrix}$$

(le déterminant de H est le discriminant de f).
1) Etablir que la matrice $H = (p_{i+j})_{0\le i,j\le n-1}$ est une matrice symétrique réelle associée à la forme quadratique réelle q.

$$q(u) = \sum_{0\le i,j\le n-1} p_{i+j}u_iu_j \quad \text{pour } u = (u_0,u_1,\dots,u_{n-1}) \in \mathbb{R}^n.$$

2) Démontrer que q est somme des carrés des n formes linéaires (sur $\mathbb{C}$) : $l_k(u) = \sum_{i=0}^{n-1} x_k^i u_i$.

3) Désignons par r le nombre de racines distinctes de f, notées $x_1, x_2, \dots, x_r$, chacune de multiplicité m_i. Etablir que le rang de la forme quadratique q est r.

4) En considérant la signature (s,t) de q et le signe des l_k quand x_k est une racine réelle, établir que $s-t$ **est égale au nombre de racines réelles de** f.

On rappelle à ce propos les formules de Newton qui permettent le calcul des p_k :

$$p_k - s_1p_{k-1} + s_2p_{k-2} + \cdots + (-1)^n s_n p_{k-n} = 0 \quad \text{pour } k \ge n$$
$$p_k - s_1p_{k-1} + s_2p_{k-2} + \cdots + (-1)^k k s_k = 0 \quad \text{pour } k \le n$$