Séance spécifique sur les structures alégbriques

*Dans ce dernier TD, on revient sur les **structures algébriques** : groupes abéliens, groupes finis, groupes cycliques... il y a là des exercices difficiles. Si le programme de MP ne va pas très loin en théorie des groupes, il peut être intéressant de connaître quelques classiques. J'espère donc que ces exercices vous permettront de mieux appréhender les notions rencontrées.*

Exercice 1 (groupes multiplicatifs de $\mathcal{M}_n(\mathbb{R})$). ★★★ [ ]

Soit $\mathcal{G}$ un groupe multiplicatif de $\mathcal{M}_n(\mathbb{R})$ dont on note N l'élément neutre pour la loi $\times$.

1. Montrer que tous les éléments de $\mathcal{G}$ ont un rang commun r tel que $r = rg(N)$.
2. On note n l'endomorphisme de $\mathbb{R}^n$ canoniquement associé à la matrice N. Etablir qu'il existe $P \in \mathcal{GL}_n(\mathbb{R})$ telle que :

$$\forall M \in \mathcal{G},\ M = P \begin{pmatrix} A & O_{r,n-r} \\ O_{n-r,r} & O_{n-r} \end{pmatrix} P^{-1} \text{ avec } A \in \mathcal{GL}_r(\mathbb{R})$$

Indications 1. Soit $M \in \mathcal{G}$, alors on a d'abord $MN = M$ et donc, $rg(M) = rg(MN) \leq rg(N)$. De la même façon, en notant M' l'inverse de M, $N = MM'$ et donc, $rg(N) = rg(MM') \leq rg(M)$, d'où par antisymétrie $rg(M) = rg(N)$ et ceci pour tout M. 2. On note encore n l'endomorphisme associé à N, et ainsi : $N^2 = N \Rightarrow n$ est un projecteur de sorte que $\mathbb{R}^n = Im(n) \oplus Ker(n)$. On introduit $\mathcal{B}$ une base adaptée à la décompostion précédente et comme $mn = nm$, ces sous-espaces sont stables par m et $Mat_{\mathcal{B}}(m)$ est diagonale par blocs de la forme $diag(A, B)$. De même, celle de m' est de la forme $diag(A', B')$. En rappelant que $MM' = N = diag(I_r, O)$, on retrouve que A est inversible, donc de rang r et par suite, B est nécessairement nul. On en déduit la forme attendue.

Exercice 2 (sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$). ★★★ [ ]

1. On suppose de plus que M est inversible. Montrer qu'il existe un unique couple $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que :

$$M = OS$$

2. Considérons $\mathcal{G}$ un sous-groupe compact de $(\mathcal{GL}_n(\mathbb{R}), \times)$ contenant $O_n(\mathbb{R})$, et $A \in \mathcal{G}$.
   (a) On note S la partie symétrique de A dans sa décomposition polaire. Justifier que pour tout $k \in \mathbb{Z}$, $S^k \in \mathcal{G}$.
   (b) Montrer que 1 est la seule valeur propre de S, puis établir que $\mathcal{G} = O_n(\mathbb{R})$.

*Autrement dit, au sens de l'inclusion, $O_n(\mathbb{R})$ désigne le plus grand sous-groupe compact de $(\mathcal{GL}_n(\mathbb{R}), \times)$: on dit aussi que $O_n(\mathbb{R})$ est un **sous-groupe compact maximal**.*

Indications 1. Par analyse-synthèse... Si (O, S) vérifie l'égalité donnée, S désigne la racine carrée de M^TM et $O = MS^{-1}$. 2.a) On a $S = AO^{-1}$ et par produit, $S \in \mathcal{G}$. Comme $\mathcal{G}$ est un groupe multiplicatif, pour tout $k \in \mathbb{Z}$, $S^k \in \mathcal{G}$. 2.b) $S \in S_n^{++}(\mathbb{R})$, donc $Sp(A) \subset \mathbb{R}_+^*$ et on note $\lambda \in Sp(A)$. Par l'absurde, si $\lambda > 1$, il vient pour un vecteur propre $\|S^kX\|_2 = \lambda^k\|X\|_2 \longrightarrow +\infty$. Mais on a aussi $\|S^kX\| \leq |||S^k|||.\|X\|_2 \leq M\|X\|_2$, car $\mathcal{G}$ est compact et ainsi, il est borné ! CONTRADICTION. De même lorsque $\lambda < 1$, et on en déduit que $Sp(S) = \{1\}$: d'après le théorème spectral, S est semblable à I_n d'où $S = I_n$ et finalement, $A = O \in O_n(\mathbb{R})$.

Exercice 3 (sous-groupe fini de $\mathcal{GL}_n(\mathbb{R})$ satisfaisant une condition sur la trace). ★★★ [ ]

Soit $\mathcal{G}$ un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$ qu'on suppose fini et considérons $M \in \mathcal{G}$ telle que :

$$tr(M) = n$$

Montrer que nécessairement $M = I_n$.

Indications Comme $\mathcal{G}$ est de cardinal fini $p \in \mathbb{N}^*$, on a par le petit théorème de Lagrange, $M^p = I_n$. On en déduit que $P(X) = X^p - 1 \in Ann(M)$. Ce polynôme étant scindé à racines simples sur $\mathbb{C}$, M est diagonalisable sur $\mathbb{C}$ et $Sp(M) \subset \mathbb{U}_p$. De plus, M étant à coefficients réels, on convient alors de noter (λ_i) les valeurs propres réelles distinctes avec $\lambda_1 = 1$, $(\lambda_j, \overline{\lambda_j})$ les valeurs propres complexes distinctes. Ainsi, en posant m_i la multiplicité associée dans χ_M, on a : $\sum_i m_i\lambda_i + \sum_j m_j(\lambda_j + \overline{\lambda_j}) = n = \sum_i m_i + 2\sum_j m_j \Rightarrow \sum_i m_i(1 - \lambda_i) + 2\sum_j m_j(1 - Re(\lambda_j)) = 0$. On reconnait une somme de termes positifs de sorte que $\forall j,\ m_j = 0$ et $\forall i \neq 1,\ m_i = 0$... ainsi $m_1 = n$, la seule valeur propre est 1 et M est semblable à I_n donc, égale à I_n.

Exercice 4 (sous-groupes finis de $\mathcal{GL}_n(\mathbb{C})$ et groupe spécial linéaire). ★★★ [ ]

On se place dans $\mathcal{GL}_n(\mathbb{C})$ et on note :

$$\mathcal{SL}_n(\mathbb{C}) = \{M \in \mathcal{GL}_n(\mathbb{C}),\ det(M) = 1\}$$

1. Montrer que $\mathcal{SL}_n(\mathbb{C})$ est un sous-groupe de $(\mathcal{GL}_n(\mathbb{C}), \times)$.
2. (a) On note H un sous-groupe fini de $(\mathbb{C}^*, \times)$. Justifier rapidement qu'il existe $p \in \mathbb{N}^*$ tel que $H = \mathbb{U}_p =< e^{i2\pi/p} >$.
   (b) Soit $\mathcal{G}$ un sous-groupe de $\mathcal{GL}_n(\mathbb{C})$ qu'on suppose fini et tel que :

$$\mathcal{G} \cap \mathcal{SL}_n(\mathbb{C}) = \{I_n\}$$

   Montrer que G est cyclique.

Indications 1. On revient à la caractérisation des sous-groupes de $(\mathcal{GL}_n(\mathbb{C}), \times)$ et on fera intervenir la multiplicativité du déterminant.

2.a) Si $z \in H$, alors par le petit théorème de Lagrange, on a avec $p = card(H) \in \mathbb{N}^*$, $z^p = 1$ et ainsi, $H \subset \mathbb{U}_p$. De plus, $card(H) = card(\mathbb{U}_p)$, d'où $H = \mathbb{U}_p$. 2.b) Soit $M \in \mathcal{G}$, on a donc $det(M) = 1 \Rightarrow M = I_n$. En fait, le déterminant définit naturellement un morphisme de G sur $\mathbb{C}^*$ et ainsi, la condition précédente nous livre $Ker(det) = \{I_n\}$. On en déduit que $det : G \longrightarrow \mathbb{C}^*$ est injective et on a même $det : G \longrightarrow det(G)$ bijective de sorte que G est isomorphe à $det(G)$: par isomorphisme, l'image de G est par conséquent un sous-groupe fini de $\mathbb{C}^*$, c'est à dire $det(G) =< e^{i2\pi/p} >$ cyclique. Par conséquent, G image réciproque d'un tel groupe est aussi cyclique.

Exercice 5 (exposant d'un groupe abélien fini)**.** **X/ENS** [ ]

Soit G un groupe multiplicatif qu'on suppose abélien et fini. Pour tout $x \in G$, on note $o(x)$ l'ordre de x.

1. Soit $(x, y) \in G^2$ et on pose $m = o(x), n = o(y)$.
   (a) On suppose que m et n sont premiers entre eux. Etablir que $o(xy) = mn$.
   (b) Si m et n ne sont pas premiers entre eux, a t-on $o(xy) = ppcm(m, n)$?
2. Soit $(m, n) \in (\mathbb{N}^*)^2$. Montrer qu'il existe deux entiers m' et n' tels que : $\begin{cases} m'|m \text{ et } n'|n \\ pgcd(m', n') = 1 \\ ppcm(m, n) = m'n' \end{cases}$.
3. On considère $z \in G$ d'ordre maximal m. Montrer que m désigne le ppcm des ordres des éléments de G. On retiendra qu'il existe un élément d'ordre maximal m, appelé aussi **exposant du groupe** G, qui n'est rien d'autres que le ppcm des ordres.
4. (a) Soient K un corps commutatif et G un sous-groupe fini du groupe des éléments inversibles $U(K) = K^*$. Etablir alors que G est nécessairement cyclique.
   (b) En déduire que pour tout nombre premier p, $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ est un groupe cyclique.

Indications 1.a) On justifie d'abord que $(xy)^{mn} = 1$, puis on montre que pour tout $k \in \mathbb{N}$ tel que $(xy)^k = 1$, alors $mn|k$. Autrement dit, c'est bien la plus petite puissance qui permet de toucher le neutre. 1.b) On prend $y = x^{-1}$ et ainsi, $o(xy) = 1$. 2. On écrit la décomposition de m et n en produit de nombres premiers, et on choisit m' et n' à partir de ces facteurs en jouant sur les valuations. 3. Soit x un autre élément de G d'ordre n, on introduit m', n' et on regarde le produit $z^{m/m'}x^{n/n'}$: c'est un élément de G d'ordre $m'n' = ppcm(m, n)$ et donc, inférieur à m choisi maximal. D'où, $ppcm(m, n) = m$ et ainsi, m est bien multiple de chacun des ordres des éléments de G. 4.a) On note m l'exposant du groupe G, et étant le ppcm de tous les ordres, alors pour tout $x \in G$, x est racine du polynôme $X^m - 1$ qui possède un nombre fini de racines, d'où $n = card(G) \leq m$. Or en notant z l'élément d'ordre maximal m, on a par le théorème de Lagrange : $m|n$, et donc $m \leq n$. Finalement, z est d'ordre $m = n$ et ainsi, $G =< z >$. 4.b) Cela découle du point précédent, puisque $p \in \mathcal{P} \Rightarrow \mathbb{Z}/p\mathbb{Z}$ désigne un corps commutatif à p éléments.