Matrices à coefficients dans un corps fini

Ce problème sur des espaces de matrices à coefficients dans un corps fini est l'occasion de revoir les points de cours suivant :

– groupes finis, morphismes de groupes, théorème de Lagrange ;
– carrés dans un corps fini ;
– trace, déterminant et polynôme caractéristique d'une matrice ;
– caractéristique d'un corps ;
– corps finis à p éléments où p est un nombre premier ;
– critère de primalité pour les nombres de Mersenne ;
– actions de groupes et classes de similitudes de matrices.

Sur ces notions, on pourra consulter les ouvrages suivants.

P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).
F. Combes — *Algèbre et géométrie.* Bréal (2003).
J. P. Escoffier. *Toute l'algèbre de la licence.* Dunod (2006).
S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).
F. Liret. *Arithmétique.* Dundod (2011).
D. Perrin. *Cours d'algèbre.* Ellipses (1996).

Notations et rappels

Un corps est un anneau commutatif unitaire dans lequel tout élément non nul est inversible.

Un corps est donc, a priori, commutatif.

Pour tout corps $\mathbb{K}$ on note $\mathcal{M}_2(\mathbb{K})$ l'anneau des matrices d'ordre 2 à coefficients dans $\mathbb{K}$ et $GL_2(\mathbb{K})$ le groupe multiplicatif des matrices inversibles d'ordre 2.

Pour toute matrice $M \in \mathcal{M}_2(\mathbb{K})$, on note $\det(M)$ son déterminant et $\mathrm{Tr}(M)$ sa trace.

Pour tout le problème, on note O la matrice nulle et I la matrice unité dans $\mathcal{M}_2(\mathbb{K})$.

Partie I

1. Soient G un groupe fini et $f : G \to G$ un morphisme de groupes.

   (a) Montrer que, pour tout $y \in G$, on a :
   $$\mathrm{card}\left(f^{-1}(\{y\})\right) \leq \mathrm{card}(\ker(f))$$
   où on a noté :
   $$f^{-1}(\{y\}) = \{x \in G \mid f(x) = y\}$$

   (b) En déduire que si $g : G \to G$ est un autre un morphisme de groupes, on a alors :
   $$\mathrm{card}(\ker(g \circ f)) \leq \mathrm{card}(\ker(f))\,\mathrm{card}(\ker(g))$$

2. Soit $\mathbb{K}$ un corps fini à q éléments.
   Pour tout diviseur d de $q-1$, on désigne par $f_d : \mathbb{K}^* \to \mathbb{K}^*$ le morphisme de groupes défini par :
   $$\forall x \in \mathbb{K}^*,\ f_d(x) = x^d$$

   (a) Montrer que $\mathrm{card}(\ker(f_d)) \leq d$.

   (b) Soit $d' = \dfrac{q-1}{d}$. Montrer que :
   $$\forall x \in \mathbb{K}^*,\ f_d \circ f_{d'}(x) = f_{d'} \circ f_d(x) = 1$$

   (c) En déduire que $\mathrm{card}(\ker(f_d)) = d$, puis que $\ker(f_d) = \mathrm{Im}(f_{d'})$.

   (d) On suppose que q est impair. En déduire que :
   $$\left\{x^{\frac{q-1}{2}} \mid x \in \mathbb{K}^*\right\} = \{-1, 1\}$$
   et que :
   $$\left\{x \in \mathbb{K}^* \mid x^{\frac{q-1}{2}} = 1\right\} = \left\{x \in \mathbb{K}^* \mid \exists y \in \mathbb{K}^*,\ x = y^2\right\}$$

3. Soit $\mathbb{K}$ un corps.

   (a) Montrer que :
   $$\forall M \in \mathcal{M}_2(\mathbb{K}),\ M^2 = \mathrm{Tr}(M)\,M - \det(M)\,I$$

   (b) Exprimer, pour tout $M \in \mathcal{M}_2(\mathbb{K})$, $\mathrm{Tr}(M^2)$ en fonction de $(\mathrm{Tr}(M))^2$ et de $\det(M)$.

(c) Soit $M \in \mathcal{M}_2(\mathbb{K})$ telle que $\det(M) = 1$.

i. Montrer que $M + M^{-1} = \mathrm{Tr}(M)\, I$.

ii. Montrer que $M^2 = M^{-2}$ si, et seulement si, $\mathrm{Tr}(M) = 0$ ou $M^2 = I$.

iii. On suppose ici que $\mathbb{K}$ est de caractéristique différente de 2.
Montrer que M est d'ordre 4 si, et seulement si, $\mathrm{Tr}(M) = 0$.

Partie II

Pour $a \in \mathbb{K}$, on note $B = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$, $A = 2I + B$ et :

$$\mathbb{A}_a = \left\{ M \in \mathcal{M}_2(\mathbb{K}) \mid \exists (x, y) \in \mathbb{K}^2,\ M = xI + yB \right\}$$

Pour tout nombre premier $p \geq 2$, $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ désigne le corps commutatif des classes résiduelles modulo p.

Pour tout entier relatif k, on note $\overline{k}$ la classe de k modulo p.

Pour tout anneau unitaire $\mathbb{A}$, on note $\mathbb{A}^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{A}$.

1. Montrer que $\mathbb{A}_a$ est un sous-anneau commutatif de $\mathcal{M}_2(\mathbb{K})$ et que c'est aussi un sous $\mathbb{K}$-espace vectoriel dont on donnera une base.
2. Pour $\mathbb{K} = \mathbb{F}_p$, où p est un nombre premier, montrer que $\mathrm{card}(\mathbb{A}_a) = p^2$.
3. Soit $\varphi : \mathbb{A}_a \to \mathbb{A}_a$ la symétrie par rapport à la droite de vecteur directeur I parallèlement à la droite de vecteur directeur B.
Montrer que φ est un isomorphisme d'anneaux.
4. Soit $M = xI + yB \in \mathbb{A}_a$.

   (a) Calculer $M\varphi(M)$ en fonction de x et y.

   (b) Montrer que $\det(M) = x^2 - ay^2$.

   (c) Montrer que $M \in \mathbb{A}_a^\times$ si, et seulement si, $\det(M) \neq 0$.
5. Montrer que $\mathbb{A}_a$ est un corps si, et seulement si, a n'est pas un carré dans $\mathbb{K}$.
6. On suppose que $\mathbb{K} = \mathbb{R}$.
Montrer que, pour $a < 0$, $\mathbb{A}_a$ est isomorphe au corps $\mathbb{C}$ des nombres complexes.
7. On suppose que $\mathbb{K}$ est de caractéristique différente de 2 et qu'il existe $b \in \mathbb{K}^*$ tel que $a = b^2$.

   (a) Montrer qu'il existe $P \in GL_2(\mathbb{K})$ telle que :
   $$PBP^{-1} = \begin{pmatrix} b & 0 \\ 0 & -b \end{pmatrix}$$

   (b) En déduire que $\mathbb{A}_a$ est isomorphe à l'anneau produit $\mathbb{K}^2$.

   (c) Pour $\mathbb{K} = \mathbb{F}_p$, où p est un nombre premier impair, calculer $\mathrm{card}(\mathbb{A}_a^\times)$.
8. On suppose que $a = 0$.

(a) Montrer que l'anneau $\mathbb{A}_a$ n'est pas isomorphe à l'anneau produit $\mathbb{K}^2$.

(b) Pour $\mathbb{K} = \mathbb{F}_p$, où p est un nombre premier, calculer $\operatorname{card}\left(\mathbb{A}_a^\times\right)$.

9. Pour $\mathbb{K} = \mathbb{F}_2$, montrer que les anneaux $\mathbb{A}_{\overline{0}}$ et $\mathbb{A}_{\overline{1}}$ sont isomorphes.

10. On suppose ici que $\mathbb{K} = \mathbb{F}_p$, où p est un nombre premier supérieur ou égal à 5 et on prend $a = \overline{3}$.
On considère la suite d'entiers $(T_n)_{n\in\mathbb{N}}$ définie par :

$$\begin{cases} T_0 = 2 \\ \forall n \in \mathbb{N},\ T_{n+1} = 2T_n^2 - 1 \end{cases}$$

(a) Montrer que la matrice $A = 2I + B$ est inversible dans $\mathbb{A}_a$.

(b) Montrer que, pour tout entier $n \in \mathbb{N}$, on a :

$$\operatorname{Tr}\left(A^{2^n}\right) = \overline{2T_n}$$

(c) Pour $n \geq 2$, montrer que p divise T_{n-2} si, et seulement si, $A^{2^{n-2}}$ est d'ordre 4 dans $\mathbb{A}_a^\times$.

(d) Déduire, pour $n \geq 2$, que p divise T_{n-2} si, et seulement si, A est d'ordre 2^n dans $\mathbb{A}_a^\times$ et qu'alors $2^n \leq p^2 - 1$.

Partie III

Dans ce qui suit, $\mathbb{K} = \mathbb{F}_p$ où p est un nombre premier impair.

1. Soit :

$$F : \begin{array}{ccc} \mathbb{A}_a & \to & \mathbb{A}_a \\ M & \mapsto & M^p \end{array}$$

(a) Montrer que l'application F est un morphisme d'anneaux et une application $\mathbb{F}_p$-linéaire.

(b) Montrer que $F(B) = a^{\frac{p-1}{2}} B$.

(c) On suppose que $a = \overline{0}$.
Montrer que F est un projecteur, dont on déterminera le noyau et l'image.

(d) On suppose qu'il existe $u \in \mathbb{F}_p^*$ tel que $a = u^2$. Montrer que F est l'application identique.

(e) Dans ce qui suit, on suppose que a n'est pas un carré dans $\mathbb{F}_p$.

i. Montrer que $F = \varphi$.

ii. Soit $P(X) = X^2 - uX + v$ un polynôme à coefficients dans $\mathbb{F}_p$.
Montrer que, si $M \in \mathbb{A}_a$ est une racine de P, alors $F(M)$ est aussi une racine de P.
En déduire que, si $M \in \mathbb{A}_a$ est une racine de P et si P est irréductible dans $\mathbb{F}_p[X]$, on a alors $uI = M + M^p$ et $vI = M^{p+1}$.

iii. Montrer que, pour tout $M \in \mathbb{A}_a$, on a $M^{p+1} = \det(M) \cdot I$.

2. On suppose de plus que $a = \overline{3}$, que $\overline{2}$ est un carré dans $\mathbb{F}_p$ et que $\overline{3}$ n'en est pas un. On pose $C = B + I$.
   Montrer que $\overline{2}A = C^2$, $C^{p+1} = -\overline{2}I$ et $A^{\frac{p+1}{2}} = -I$.

Partie IV

On suppose désormais, jusqu'à la fin de cette partie, que le nombre premier p est supérieur ou égal à 5 et de la forme $p = 2^m - 1$.

1. Montrer que m est un nombre premier impair.
2. En déduire que 3 divise $p - 1$.
3. Déduire qu'il existe dans $\mathbb{F}_p^*$ un élément b d'ordre 3.
4. Vérifier que $\left(\overline{2}b + \overline{1}\right)^2 = -\overline{3}$.
5. Établir que $-\overline{1}$ n'est pas un carré dans $\mathbb{F}_p^*$.
6. Déduire que $\overline{3}$ n'est pas un carré dans $\mathbb{F}_p^*$.
7. Démontrer que $\overline{2}$ est un carré dans $\mathbb{F}_p^*$.
8. Établir le critère de primalité suivant :
   « Soit q un entier supérieur ou égal à 3. Alors $2^q - 1$ est premier si, et seulement si, $2^q - 1$ divise T_{q-2} ».
9. Décomposer T_3 en facteurs premiers.

Partie V

Dans cette partie, le corps de base est $\mathbb{F}_p$ où p est un nombre premier impair.

Soit $a \in \mathbb{F}_p^*$ qui n'est pas un carré dans $\mathbb{F}_p$. D'après **II-5**, $\mathbb{A}_a$ est un corps, qu'on note $\mathbb{K}$ dans la suite.

1.
   (a) Démontrer que l'application :

   $$\begin{array}{rccc} F: & \mathbb{F}_p & \to & \mathbb{K} \\ & x & \mapsto & x \cdot I \end{array}$$

   est un morphisme de corps injectif.
   On identifie ainsi $\mathbb{F}_p$ à un sous-corps de $\mathbb{K}$.

   (b) Démontrer que pour tout $x \in \mathbb{F}_p$, $x \cdot I$ est un carré dans $\mathbb{K}$.

   (c) Soit $P(X) = X^2 + cX + d$ un polynôme unitaire de degré 2 à coefficients c et d dans $\mathbb{F}_p$.
   Démontrer que ce polynôme est scindé dans $\mathbb{K}[X]$.

2. On considère le groupe $\mathrm{GL}_2(\mathbb{F}_p)$ des matrices 2×2 inversibles, à coefficients dans $\mathbb{F}_p$.

   (a) Déterminer le cardinal de $\mathrm{GL}_2(\mathbb{F}_p)$.

   (b) Soit $M \in \mathcal{M}_2(\mathbb{F}_p)$. Démontrer que M est semblable à une matrice de l'un des quatre types suivants :

i. Une matrice de la forme $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, $x \in \mathbb{F}_p$;

ii. une matrice de la forme $\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$, $x \in \mathbb{F}_p$;

iii. une matrice de la forme $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, $x, y \in \mathbb{F}_p$, $x \neq y$;

iv. une matrice de la forme $\begin{pmatrix} x & u\,y \\ y & x \end{pmatrix}$, $x \in \mathbb{F}_p$, $y \in \mathbb{F}_p^*$ où $u \in \mathbb{F}_p^*$ n'est pas un carré dans $\mathbb{F}_p$.

Indication : on pourra considérer les valeurs propres de M dans $\mathbb{F}_p$ ou dans $\mathbb{K}$.

(c) Déterminer, pour chacun des types ci-dessus, le nombre de classes de similitude de ce type.

(d) Déterminer, pour chaque classe de similitude de $\mathrm{GL}_2(\mathbb{F}_p)$, le cardinal de celle-ci.