

NOTATIONS ET RAPPELS

Pour tout corps k , on note $M_2(k)$ l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients $a, b, c, d \in k$ et pour tout $M \in M_2(k)$, on note $\det(M)$ son déterminant et $\text{tr}(M)$ sa trace. Ainsi, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on a $\det(M) = ad - bc$ et $\text{tr}(M) = a + d$.

Dans tout le problème I et O désignent respectivement la matrice Identité et la matrice nulle de $M_2(k)$.

Soit $a \in k$; on pose $B = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$, $A = 2I + B$, et $\mathcal{A}_a = \{M \in M_2(k); \exists x, y \in k, M = xI + yB\}$.

Si p est un nombre premier, on note \mathbb{F}_p le corps fini $\mathbb{Z}/p\mathbb{Z}$. Pour tout $n \in \mathbb{Z}$, on note \bar{n} la classe modulo p de l'entier n . Si E est un ensemble fini, on note $\text{Card}E$ le nombre de ses éléments.

Si R est un anneau unitaire, on note $U(R)$ le groupe multiplicatif des éléments inversibles de R . Soit $x \in R$; on dit que x est un carré dans R s'il existe $y \in R$ tel que $x = y^2$.

Partie I.

1. Soit G un groupe fini, et $f : G \rightarrow G$ un morphisme de groupes; montrer que, pour tout $y \in G$, $\text{Card}(\{x \in G; f(x) = y\}) \leq \text{Card}(\ker f)$.

En déduire que, si $g : G \rightarrow G$ est aussi un morphisme de groupes, on a

$$\text{Card}(\ker(g \circ f)) \leq \text{Card}(\ker f) \text{Card}(\ker g).$$

2. Soit k un corps fini, et $q = \text{Card}k$; pour tout diviseur d de $q - 1$, on note $f_d : k^* \rightarrow k^*$ le morphisme de groupes défini par $f_d(x) = x^d$.

(a) Montrer que $\text{Card} \ker f_d \leq d$.

(b) Soit $d' = (q - 1)/d$. Montrer que, pour tout $x \in k^*$, $f_d \circ f_{d'}(x) = f_{d'} \circ f_d(x) = 1$.

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

(d) On suppose q impair. En déduire que

$$\{x^{\frac{q-1}{2}}; x \in k^*\} = \{\pm 1\}$$

et que

$$\{x \in k^*, x^{\frac{q-1}{2}} = 1\} = \{x \in k^*; \exists y \in k^*, x = y^2\}.$$

3. Soit k un corps.

(a) Montrer que pour tout $M \in M_2(k)$ on a $M^2 = \text{tr}(M)M - \det(M)I$.

(b) Exprimer, pour tout $M \in M_2(k)$, $\text{tr}(M^2)$ en fonction de $(\text{tr}(M))^2$ et $\det(M)$.

(c) Soit $M \in GL_2(k)$, telle que $\det M = 1$.

i. Montrer que $M + M^{-1} = \text{tr}(M)I$.

- ii. Montrer que $M^2 - M^{-2} = O$ si et seulement si $\text{tr}(M) = 0$ ou si $M^2 = I$.
- iii. On suppose ici que k est de caractéristique $\neq 2$. Montrer que M est d'ordre 4 si et seulement si $\text{tr}(M) = 0$. •

Partie II.

4. Montrer que \mathcal{A}_a est un sous-anneau commutatif de $M_2(k)$, et en est un sous- k -espace vectoriel dont on donnera une base.
5. Si p est un nombre premier et $k = \mathbb{F}_p$, en déduire que $\text{Card } \mathcal{A}_a = p^2$.
6. Soit $\varphi : \mathcal{A}_a \rightarrow \mathcal{A}_a$ la symétrie par rapport à la droite de vecteur directeur I parallèlement à la droite de vecteur directeur B . Montrer que φ est un morphisme d'anneaux.
7. Soit $M = xI + yB$ un élément de \mathcal{A}_a .
 - (a) Calculer $M\varphi(M)$ en fonction de x et y .
 - (b) Montrer que $\det M = x^2 - ay^2$.
 - (c) Démontrer qu'une matrice M de \mathcal{A}_a appartient à $U(\mathcal{A}_a)$ si et seulement si $\det(M) \neq 0$.
8. Montrer que \mathcal{A}_a est un corps si et seulement si a n'est pas un carré dans k .
9. On suppose que $k = \mathbb{R}$. Montrer que, si $a < 0$, \mathcal{A}_a est isomorphe au corps \mathbb{C} des nombres complexes.
10. On suppose que k n'est pas de caractéristique 2, et qu'il existe $b \in k^*$ tel que $a = b^2$.
 - (a) Montrer qu'il existe $P \in GL_2(k)$ tel que $PBP^{-1} = \begin{pmatrix} b & 0 \\ 0 & -b \end{pmatrix}$.
 - (b) En déduire que \mathcal{A}_a est isomorphe à l'anneau produit $k \times k$.
 - (c) Lorsque $k = \mathbb{F}_p$, $p \geq 3$, calculer le cardinal de $U(\mathcal{A}_a)$.
11. On suppose que $a = 0$.
 - (a) Montrer que l'anneau \mathcal{A}_a n'est pas isomorphe à $k \times k$.
 - (b) Lorsque $k = \mathbb{F}_p$, calculer le cardinal de $U(\mathcal{A}_a)$.
12. On suppose que $k = \mathbb{F}_2$. Montrer que les anneaux $\mathcal{A}_{\bar{0}}$ et $\mathcal{A}_{\bar{1}}$ sont isomorphes.
13. On suppose ici que $a = \bar{3}$ et que $k = \mathbb{F}_p$, où p est un nombre premier ≥ 5 .
On considère la suite des entiers $(T_n)_{n \geq 0}$ définie par

$$\begin{cases} T_0 & = 2 \\ T_{n+1} & = 2T_n^2 - 1 \quad \text{pour tout } n \geq 0. \end{cases}$$

- (a) Montrer que A est un élément de $U(\mathcal{A}_a)$.
- (b) Montrer que pour tout $n \in \mathbb{N}$ on a $\text{tr}(A^{2^n}) = \bar{2} \bar{T}_n$.
- (c) Montrer que p divise T_{n-2} ($n \geq 2$) si et seulement si $A^{2^{n-2}}$ est d'ordre 4 dans $U(\mathcal{A}_a)$.
- (d) Déduire que p divise T_{n-2} ($n \geq 2$) si et seulement si A est d'ordre 2^n dans $U(\mathcal{A}_a)$, et qu'alors $2^n \leq p^2 - 1$.