TD 1 – Extrait agrégation interne de 2015

Dans tout ce problème k désigne un corps commutatif. On note $M_2(k)$ l'ensemble des matrices 2×2 à coefficients dans k. La matrice identité et la matrice nulle de $M_2(k)$ sont respectivement notées I et O. 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 $\overline{n}$ la classe modulo p de l'entier n.

1. Soit G un groupe fini, et $f : G \to G$ un morphisme de groupes ; montrer que, pour tout $y \in G$, $\mathrm{Card}\left(\{x \in G;\ f(x) = y\}\right) \leq \mathrm{Card}(\ker f)$. En déduire que, si $g : G \to G$ est aussi un morphisme de groupes, on a
$$\mathrm{Card}(\ker(g \circ f)) \leq \mathrm{Card}(\ker f)\,\mathrm{Card}(\ker g).$$

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

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

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

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

d. On suppose q impair. En déduire que

$$\left\{x^{\frac{q-1}{2}};\ x \in k^*\right\} = \{\pm 1\} \quad \text{et} \quad \left\{x \in k^*; x^{\frac{q-1}{2}} = 1\right\} = \left\{x \in k^*;\ \exists y \in k^*,\ x = y^2\right\}.$$

3. Montrer qua $\mathcal{A}_a$ est un sous-anneau commutatif de $M_2(k)$, et en est un sous k-espace vectoriel dont on donnera une base.

4. Si p est un nombre premier et $k = \mathbb{F}_p$, en déduire que $\mathrm{Card}\left(\mathcal{A}_a\right) = p^2$.

5. Soit $\varphi : \mathcal{A}_a \to \mathcal{A}_a$ la symétrie par rapport à la droite de vecteur directeur I parallèlement à la droite de vecteur de directeur B. Montrer que φ est un morphisme d'anneaux.

6. 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 $\mathcal{A}_a^*$ si et seulement si $\det(M) \neq 0$.

7. Montrer que $\mathcal{A}_a$ est un corps si et seulement si a n'est pas un carré dans k.

8. On suppose que $k = \mathbb{R}$. Montrer que, si $a < 0$, $\mathcal{A}_a$ est isomorphe au corps $\mathbb{C}$ des nombres complexes.

9. 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 $\mathcal{A}_a^*$

10. 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 $\mathcal{A}_a^*$.

11. On suppose que $k = \mathbb{F}_2$. Montrer que les anneaux $\mathcal{A}_{\overline{0}}$ et $\mathcal{A}_{\overline{1}}$ sont isomorphes.