

## Devoir N° 1

(Agrégation interne 2015 - 1ère épreuve de mathématiques)

### NOTATIONS ET RAPPELS

Si  $E$  est un ensemble fini, on note  $\text{Card}(E)$  le nombre de ses éléments.

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  $R$  est un anneau unitaire, on note  $\mathcal{U}(R)$  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  $x = y^2$ .

Pour tout corps commutatif  $k$ , 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  $\text{tr}(M) = a + d$ .

On note  $GL_2(k)$  le groupe  $\mathcal{U}(M_2(k))$  des matrices inversibles - on a

$$GL_2(k) = \{M \in M_2(k); \det M \neq 0\}.$$

Dans tout le problème  $I_2$  et  $0_2$  désignent respectivement la matrice identité et la matrice nulle de  $M_2(k)$ .

Soit  $a \in k$ ; on pose  $B = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ ,  $A = 2I_2 + B$  et  $\mathcal{A}_a = \{M \in M_2(k); \exists x, y \in k, M = xI_2 + yB\}$ .

### Partie I.

1. Soit  $G$  un groupe fini, et soit  $f : G \rightarrow G$  un homomorphisme de groupes.
  - a) Soit  $y \in G$ . Soit  $h \in G$  tel que  $f(h) = y$ . Démontrer que l'application  $z \mapsto zh$  est une bijection de  $\ker f$  sur l'ensemble  $\{x \in G; f(x) = y\}$  (noté  $f^{-1}(\{y\})$ ).
  - b) En déduire que, pour tout  $y \in G$ , on a  $\text{Card}(f^{-1}(\{y\})) \leq \text{Card}(\ker f)$ .
  - c) Soit  $g : G \rightarrow G$  un homomorphisme de groupes. Démontrer que l'on a

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

2. Soit  $k$  un corps fini commutatif; posons  $q = \text{Card}(k)$ . Pour tout diviseur  $d$  de  $q - 1$ , on note  $f_d : k^* \rightarrow k^*$  l'homomorphisme de groupes défini par  $f_d(x) = x^d$ .
  - a) Démontrer que  $\text{Card}(\ker f_d) \leq d$ .
  - b) Soit  $d' = (q - 1)/d$ . Démontrer 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 que  $q$  est impair. En déduire que

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

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 commutatif.

a) Démontrer que pour tout  $M \in M_2(k)$  on a  $M^2 = \text{tr}(M)M - \det(M)I_2$ .

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  $M \in M_2(k)$ , telle que  $\det M = 1$ .

(i) Démontrer que  $M + M^{-1} = \text{tr}(M)I_2$ .

(ii) Démontrer que  $M^2 - M^{-2} = 0_2$  si et seulement si  $\text{tr}(M) = 0$  ou si  $M^2 = I_2$ .

(iii) On suppose ici que  $k$  est de caractéristique  $\neq 2$ . Démontrer que  $M$  est d'ordre 4 si et seulement si  $\text{tr}(M) = 0$ .

## Partie II.

4. Démontrer 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  $I_2$  parallèlement à la droite de vecteur directeur  $B$ . Démontrer que  $\varphi$  est un homomorphisme d'anneaux.

7. Soit  $M = xI_2 + yB$  un élément de  $\mathcal{A}_a$ .

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

b) Démontrer qu'une matrice  $M$  de  $\mathcal{A}_a$ , appartient à  $\mathcal{U}(\mathcal{A}_a)$  si et seulement si  $\det(M) \neq 0$ .

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

9. On suppose que  $k = \mathbb{R}$ . Démontrer que, si  $a < 0$ , alors le corps  $\mathcal{A}_a$  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) Démontrer 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  $k = \mathbb{F}_p$  où  $p$  est un nombre premier distinct de 2 calculer le cardinal de  $\mathcal{U}(\mathcal{A}_a)$ .

11. On suppose que  $a = 0$ .

a) Démontrer que l'anneau  $\mathcal{A}_a$  n'est pas isomorphe à l'anneau produit  $k \times k$ .

b) Lorsque  $k = \mathbb{F}_p$  (et  $a = \bar{0}$ ), calculer le cardinal de  $\mathcal{U}(\mathcal{A}_a)$ .

12. On suppose que  $k = \mathbb{F}_2$ . Démontrer 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  $\geq 5$ . On considère la suite des nombres entiers  $(T_n)_{n \in \mathbb{N}}$  définie par

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

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

### Partie III.

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

14. Soit  $F : \mathcal{A}_a \rightarrow \mathcal{A}_a$  l'application définie par  $M \mapsto M^p$ .
  - a) Démontrer que  $F$  est un homomorphisme d'anneaux, et une application  $\mathbb{F}_p$ -linéaire.
  - b) Démontrer que  $F(B) = a^{\frac{p-1}{2}}B$ .
  - c) On suppose que  $a = 0$ . Démontrer que  $F$  est un projecteur, dont on déterminera le noyau et l'image.
  - d) On suppose qu'il existe  $u \in k^*$  tel que  $a = u^2$ . Démontrer que  $F$  est l'application identique.
  - e) Dans ce qui suit, on suppose que  $a$  n'est pas un carré dans  $k$ .
    - (i) Démontrer que  $F = \varphi$ .
    - (ii) Soit  $P(X) = X^2 - uX + v$  un polynôme à coefficients dans  $\mathbb{F}_p$ . Démontrer que, si  $M \in \mathcal{A}_a$  est une racine de  $P$  alors  $F(M)$  est aussi une racine de  $P$ . En déduire que, si  $M \in \mathcal{A}_a$  est une racine de  $P$  et si  $P$  est irréductible dans  $\mathbb{F}_p[X]$ , on a  $uI_2 = M + M^p$  et  $vI_2 = M^{p+1}$ .
    - (iii) Démontrer que, pour tout  $M \in \mathcal{A}_a$ , on a  $M^{p+1} = \det(M)I_2$ .
15. On suppose de plus que  $a = \bar{3}$ , que  $\bar{2}$  est un carré dans  $k$  et  $\bar{3}$  n'en est pas un. On pose  $C = B + I_2$ . Démontrer que  $\bar{2}A = C^2$ ,  $C^{p+1} = -\bar{2}I_2$  et  $A^{\frac{p+1}{2}} = -I_2$ .

### Partie IV.

On suppose dans cette partie que le nombre premier  $p$  est  $\geq 5$  et de la forme  $p = 2^m - 1$ .

16. Démontrer que  $m$  est un nombre premier impair.
17. En déduire que 3 divise  $p - 1$ .
18. Dédurre qu'il existe dans  $\mathbb{F}_p^*$  un élément  $b$  d'ordre 3.
19. Vérifier que  $(\bar{2}b + \bar{1})^2 = -\bar{3}$ .

20. Etablir que  $-\bar{1}$  n'est pas un carré dans  $\mathbb{F}_p$ .
21. Dédurre que  $\bar{3}$  n'est pas un carré dans  $\mathbb{F}_p$ .
22. Démontrer que  $\bar{2}$  est un carré dans  $\mathbb{F}_p$ .
23. Etablir le critère de primalité suivant :  
Soit  $q$  un nombre entier  $\geq 3$ . Alors  $2^q - 1$  est premier si et seulement si  $2^q - 1$  divise  $T_{q-2}$ .
24. Décomposer  $T_3$  en facteurs premiers.

### Partie V.

Dans cette partie,  $k = \mathbb{F}_p$ , où  $p$  est un nombre premier impair. On fixe un élément  $a$  de  $k^*$  qui n'est pas un carré dans  $k$ ; d'après II-8,  $\mathcal{A}_a$ , est un corps, que l'on note  $K$  dans la suite.

25. a) Démontrer que l'application  $\mathbb{F}_p \rightarrow K, x \mapsto x I_2$  est un homomorphisme injectif. On identifie ainsi  $\mathbb{F}_p$  à un sous-corps de  $K$ .
- b) Démontrer que pour tout  $x \in \mathbb{F}_p, x I_2$  est un carré dans  $K$ .
- 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  $K[X]$ .
26. a) Déterminer le cardinal de  $GL_2(\mathbb{F}_p)$ .
- b) Soit  $M \in M_2(\mathbb{F}_p)$ . 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  $\begin{pmatrix} x & ay \\ y & x \end{pmatrix}, x, y \in \mathbb{F}_p, y \neq 0$ .

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

- 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  $M_2(\mathbb{F}_p)$ , le cardinal de celle-ci.