Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE, DE
L'ENSEIGNEMENT
SUPÉRIEUR ET DE
LA RECHERCHE

**EAI MAT 1**

**SESSION 2015**

# AGRÉGATION
# CONCOURS INTERNE
# ET CAER

## Section : MATHÉMATIQUES

## PREMIÈRE ÉPREUVE

Durée : 6 heures

*L'usage de tout ouvrage de référence, de tout dictionnaire et de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.*

*Dans le cas où un(e) candidat(e) repère ce qui lui semble être une erreur d'énoncé, il (elle) le signale très lisiblement sur sa copie, propose la correction et poursuit l'épreuve en conséquence.*

*De même, si cela vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement.*

***NB : La copie que vous rendrez ne devra, conformément au principe d'anonymat, comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé comporte notamment la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de signer ou de l'identifier.***

A

## 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 $\mathrm{tr}(M)$ sa trace. Ainsi, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on a $\det(M) = ad - bc$ et $\mathrm{tr}(M) = a + d$.

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 $\overline{n}$ la classe modulo $p$ de l'entier $n$. Si $E$ est un ensemble fini, on note $\mathrm{Card}E$ 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 $f : G \to G$ un morphisme de groupes ; montrer que, pour tout $y \in G$, $\mathrm{Card}(\{x \in G;\ f(x) = y\}) \leqslant \mathrm{Card}(\ker f)$.
   En déduire que, si $g : G \to G$ est aussi un morphisme de groupes, on a
   $$\mathrm{Card}(\ker(g \circ f)) \leqslant \mathrm{Card}(\ker f)\,\mathrm{Card}(\ker g).$$

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 $\mathrm{Card}\ker f_d \leqslant d$.
   **(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 $\mathrm{Card}\ker f_d = d$, puis que $\ker f_d = \mathrm{Im}\, f_{d'}$.
   **(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 $M^2 = \mathrm{tr}(M)M - \det(M)I$.
   **(b)** Exprimer, pour tout $M \in M_2(k)$, $\mathrm{tr}(M^2)$ en fonction de $(\mathrm{tr}(M))^2$ et $\det(M)$.
   **(c)** Soit $M \in GL_2(k)$, telle que $\det M = 1$.
      i. Montrer que $M + M^{-1} = \mathrm{tr}(M)I$.



Tournez la page S.V.P.

ii. Montrer que $M^2 - M^{-2} = O$ si et seulement si $\mathrm{tr}(M) = 0$ 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 $\mathrm{tr}(M) = 0$. •

## 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 $\mathrm{Card}\ \mathcal{A}_a = p^2$.

**6.** 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 directeur $B$. Montrer que $\varphi$ 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 $k = \mathbb{F}_p$, $p \geqslant 3$, 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 $\mathcal{A}_{\overline{0}}$ et $\mathcal{A}_{\overline{1}}$ sont isomorphes.

**13.** On suppose ici que $a = \overline{3}$ et que $k = \mathbb{F}_p$, où $p$ est un nombre premier $\geqslant 5$.
On considère la suite des entiers $(T_n)_{n\geqslant 0}$ définie par

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

**(a)** Montrer que $A$ est un élément de $U(\mathcal{A}_a)$.

**(b)** Montrer que pour tout $n \in \mathbb{N}$ on a $\mathrm{tr}(A^{2^n}) = \overline{2}\,\overline{T_n}$.

**(c)** Montrer que $p$ divise $T_{n-2}$ $(n \geqslant 2)$ si et seulement si $A^{2^{n-2}}$ est d'ordre 4 dans $U(\mathcal{A}_a)$.

**(d)** Déduire que $p$ divise $T_{n-2}$ $(n \geqslant 2)$ si et seulement si $A$ est d'ordre $2^n$ dans $U(\mathcal{A}_a)$, et qu'alors $2^n \leqslant p^2 - 1$.

## Partie III

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

**14.** Soit $F : \mathcal{A}_a \to \mathcal{A}_a$ l'application définie par $M \mapsto M^p$.

**(a)** Montrer que $F$ 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 $a = 0$. Montrer que $F$ est un projecteur, dont on déterminera le noyau et l'image.

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

**(e)** Dans ce qui suit, on suppose que $a$ n'est pas un carré dans $k$.

i. Montrer que $F = \varphi$.

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

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

**15.** On suppose de plus que $a = \overline{3}$, que $\overline{2}$ est un carré dans $k$ et $\overline{3}$ 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 $\geqslant 5$ et de la forme $p = 2^m - 1$.**

**16.** Montrer que $m$ est un nombre premier impair.

**17.** En déduire que 3 divise $p - 1$.

**18.** Déduire qu'il existe dans $\mathbb{F}_p^*$ un élément $b$ d'ordre 3.

**19.** Vérifier que $(\overline{2}b + \overline{1})^2 = -\overline{3}$.

**20.** Etablir que $-\overline{1}$ n' est pas un carré dans $\mathbb{F}_p^*$.

**21.** Déduire que $\overline{3}$ n'est pas un carré dans $\mathbb{F}_p^*$.

**22.** Démontrer que $\overline{2}$ est un carré dans $\mathbb{F}_p^*$.

**23.** Etablir le critère de primalité suivant :
Soit $q$ un entier $\geqslant 3$. Alors $2^q - 1$ est premier si et seulement si $2^q - 1$ divise $T_{q-2}$.

**24.** Décomposer $T_3$ en facteurs premiers.



**Tournez la page S.V.P.**

## Partie V.

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

**25.** **(a)** Démontrer que l'application $\mathbb{F}_p \to K, x \mapsto xI$ est un morphisme injectif.
On identifie ainsi $\mathbb{F}_p$ à un sous-corps de $K$.

**(b)** Démontrer que pour tout $x \in \mathbb{F}_p$, $xI$ 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.** On considère le groupe $GL_2(\mathbb{F}_p)$ des matrices $2 \times 2$ inversibles, à coefficients dans $\mathbb{F}_p$.

**(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 $\begin{pmatrix} x & uy \\ y & x \end{pmatrix}, x, y \in \mathbb{F}_p$ 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 $K$.

**(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 $GL_2(\mathbb{F}_p)$, le cardinal de celle-ci.

——— FIN DU SUJET ———