Correction du devoir N° 1

(Agrégation interne 2015 - 1ère épreuve de mathématiques)

Partie I.

1. a) L'application $R_h : z \mapsto zh$ est une bijection de G sur G (la bijection réciproque est $z \mapsto zh^{-1}$). On a $f(zh) = f(z)f(h) = f(z)y$. Donc $z \in \ker f \iff R_h(z) \in f^{-1}(y)$. On a prouvé que $R_h(\ker f) = f^{-1}(\{y\})$.

   b) Si $z \in \mathrm{Im}(f)$ on a donc $\mathrm{Card}(f^{-1}(\{y\})) = \mathrm{Card}(\ker f)$. Sinon $\mathrm{Card}(f^{-1}(\{y\})) = 0 < \mathrm{Card}(\ker f)$.

   c) On a $\ker(g \circ f) = f^{-1}(\ker g) = \bigcup_{y \in \ker g} f^{-1}(\{y\})$. Comme cette réunion est disjointe, on a donc $\mathrm{Card}(\ker(g \circ f)) = \sum_{y \in \ker g} \mathrm{Card}(f^{-1}(\{y\})) \leqslant \mathrm{Card}(\ker f)\mathrm{Card}(\ker g)$ (d'après 1.b).

2. a) Le noyau de f_d est l'ensemble des racines du polynôme $X^d - 1$ dans k. Comme k est un corps commutatif, ce polynôme a au plus d racines

   b) On a $f_d \circ f_{d'}(x) = f_{d'} \circ f_d(x) = x^{dd'} = x^{q-1}$. D'après le théorème de Lagrange, comme le groupe k^* a $q-1$ éléments, on a $x^{q-1} = 1$.

   c) On a donc $\mathrm{Card}(\ker(f_d \circ f_{d'})) = q - 1$. D'après 1.c) et 2.a) (appliqué successivement à f_d et à $f_{d'}$), on a donc
   $$q - 1 \leqslant \mathrm{Card}(\ker f_d)\mathrm{Card}(\ker f_{d'}) \leqslant d\,\mathrm{Card}(\ker f_{d'}) \leqslant dd'.$$
   Toutes ces inégalités sont donc des égalités. Il vient $\mathrm{Card}(\ker f_d) = d$ et $\mathrm{Card}(\ker f_{d'}) = d'$. Or $\mathrm{Card}(\mathrm{Im} f_{d'}) = (q-1)/\mathrm{Card}(\ker f_{d'})$ donc $\mathrm{Card}(\mathrm{Im} f_{d'}) = d$.
   Comme $f_d \circ f_{d'}(x) = 1$, on a $\mathrm{Im} f_{d'} \subset \ker f_d$. On en déduit l'égalité - par égalité des cardinaux.

   d) On pose $d = 2$ et $d' = \dfrac{q-1}{2}$. On a $\{x^{\frac{q-1}{2}};\ x \in k^*\} = \mathrm{Im} f_{d'} = \ker f_d = \{1, -1\}$. De même $\{x \in k;\ x^{\frac{q-1}{2}} = 1\} = \ker f_{d'} = \mathrm{Im} f_d = \{x \in k^*;\ \exists y \in k^*,\ x = y^2\}$.

3. a) Le polynôme caractéristique de M est $X^2 - \mathrm{tr}(M)X + \det(M)$. D'après le théorème de Cayley Hamilton, on a $M^2 - \mathrm{tr}(M)M + \det(M)\,\mathrm{I}_2 = 0_2$.
   On peut aussi écrire $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a donc
   $$\begin{aligned} M^2 &= \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix} \\ &= \begin{pmatrix} a(a+d) - (ad - bc) & b(a+d) \\ c(a+d) & d(a+d) - (ad - bc) \end{pmatrix} \\ &= \mathrm{tr}(M)M - \det(M)\,\mathrm{I}_2. \end{aligned}$$

   b) En appliquant la trace dans l'égalité établie en 3.a), il vient $\mathrm{tr}(M^2) = (tr(M))^2 - 2\det(M)$.

   c) (i) Multipliant l'égalité de 3.a) par M^{-1}, on trouve $M = tr(M)\,\mathrm{I}_2 - \det(M)M^{-1} = tr(M)\,\mathrm{I}_2 - M^{-1}$ si $\det(M) = 1$.

   (ii) On a $M^2 - M^{-2} = (M + M^{-1})(M - M^{-1}) = \mathrm{tr}(M)(M - M^{-1})$. Donc $M^2 - M^{-2} = 0_2$ si et seulement si $\mathrm{tr}(M) = 0$ ou $M = M^{-1}$, soit $M^2 = \mathrm{I}_2$.

   (iii) Si M est d'ordre 4, alors $M^4 = \mathrm{I}_2$ et $M^2 \neq \mathrm{I}_2$, donc $M^2 - M^{-2} = 0_2$ et $M \neq M^{-1}$. Alors $\mathrm{tr}(M) = 0$ d'après (ii).
   Si $\mathrm{tr}(M) = 0$, on a $M = -M^{-1}$, donc $M^2 = -\mathrm{I}_2$. Donc $M^4 = \mathrm{I}_2$ et $M^2 \neq \mathrm{I}_2$ (puisque la caractéristique de k n'est pas 2), donc M est d'ordre 4.

Partie II.

4. Par définition, $\mathcal{A}_a$, est le sous-espace vectoriel de $M_2(k)$ engendré par I_2 et B. Comme I_2 et B ne sont pas proportionnels, la famille (I_2, B) est libre : c'est une base de $\mathcal{A}_a$.
On a $B^2 = a\,\mathrm{I}_2$. Donc si $M = x\,\mathrm{I}_2 + yB$ et $M' = x'\,\mathrm{I}_2 + y'B$, alors $MM' = (xx' + ayy')\mathrm{I}_2 + (xy' + yx')B = M'M$. Donc $\mathcal{A}_a$ est un sous-anneau de $M_2(k)$; il est commutatif.

5. L'application $(x, y) \mapsto x\,\mathrm{I}_2 + yB$ est un isomorphisme d'espaces vectoriels de $\mathbb{F}_p^2$ sur $\mathcal{A}_a$. En particulier, c'est une bijection, donc $\mathrm{Card}(\mathcal{A}_a) = \mathrm{Card}(\mathbb{F}_p^2) = p^2$.

6. Par définition φ est linéaire et l'on a $\varphi(x\,\mathrm{I}_2 + yB) = x\,\mathrm{I}_2 - yB$ (pour tous $x, y \in k$). Posons $J = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On a $J^2 = \mathrm{I}_2$ et $\varphi(M) = JMJ$ pour tout $M \in \mathcal{A}_a$. Pour $M, M' \in \mathcal{A}_a$, on a donc $\varphi(M)\varphi(M') = JMJJM'J = JMM'J = \varphi(MM')$.

7. a) Soit $M = x\,\mathrm{I}_2 + yB$. On a $M\varphi(M) = (x\,\mathrm{I}_2 + yB)(x\,\mathrm{I}_2 - yB) = x^2\mathrm{I}_2 - y^2B^2 = (x^2 - ay^2)\mathrm{I}_2$ (remarquons que $\varphi(M)$ est la transposée de la comatrice de M et $\det(M) = x^2 - ay^2$).

   b)
   - Si M est inversible dans $\mathcal{A}_a$, elle l'est dans $M_2(k)$, donc $\det(M) \neq 0$.
   - Si $\det(M) \neq 0$, alors $M^{-1} = \dfrac{1}{\det(M)}\varphi(M)$ est un élément de $\mathcal{A}_a$, donc $M \in \mathcal{U}(\mathcal{A})$.

8. D'après 7.b), $\mathcal{A}_a$ est un corps si et seulement si pour tout $M \in \mathcal{A}_a \setminus \{0_2\}$, on a $\det(M) \neq 0$. Cela a lieu si et seulement si, $\forall (x, y) \in k^2 \setminus \{(0, 0)\}$ on a $x^2 - ay^2 \neq 0$.
   - Si $a = b^2$ est un carré dans k, $b\,\mathrm{I}_2 + B$ n'et pas inversible - donc $\mathcal{A}_a$ n'est pas un corps.
   - S'il existe $(x, y) \neq (0, 0)$ tels que $x^2 = ay^2$, alors $y \neq 0$ (sinon $(x, y) = (0, 0)$) et $a = b^2$ avec $b = xy^{-1}$.

9. Si $k = \mathbb{R}$ et $a < 0$, écrivons $a = -b^2$ avec $b \in \mathbb{R}^*$. Posons $\Psi(x\,\mathrm{I}_2 + yB) = x + iby$. On vérifie immédiatement que Ψ est un isomorphisme de corps de $\mathcal{A}_a$ sur $\mathbb{C}$.

10. a) Le polynôme caractéristique de B est $X^2 - a = (X - b)(X + b)$. Comme $b \neq -b$ (puisque la caractéristique de k n'est pas 2), ce polynôme est scindé à racines simples donc B est diagonalisable et ses valeurs propres étant b et $-b$. Il existe donc $P \in GL_2(k)$ tel que $P^{-1}BP = \begin{pmatrix} b & 0 \\ 0 & -b \end{pmatrix}$.

    b) On a $P^{-1}(x\,\mathrm{I}_2 + yB)P = \begin{pmatrix} x + by & 0 \\ 0 & x - by \end{pmatrix}$. Donc l'application $\Phi : x\,\mathrm{I}_2 + yB \mapsto (x + by, x - by)$ est un isomorphisme d'anneaux de $\mathcal{A}_a$ sur l'anneau produit $k \times k$.

    c) On a $\Phi(\mathcal{U}(\mathcal{A}_a)) = \mathcal{U}(k \times k) = k^* \times k^*$. Donc $\mathrm{Card}(\mathcal{U}(\mathcal{A}_a)) = (p - 1)^2$.

11. a) Pour $(x, y) \in k \times k$, on a $(x, y)^2 = (0, 0) \Rightarrow (x, y) = (0, 0)$. Or, si $a = 0$, on a $B^2 = 0_2$ - alors que $B \neq 0_2$. Donc l'anneau $\mathcal{A}_0$ n'est pas isomorphe l'anneau produit $k \times k$.

    b) On a $\det(x\,\mathrm{I}_2 + yB) = x^2$ donc $\mathcal{U}(\mathcal{A}_0) = \{x\,\mathrm{I}_2 + yB;\ (x, y) \in k^* \times k\}$. Donc $\mathrm{Card}(\mathcal{U}(\mathcal{A}_a)) = (p-1)p$.

12. Si $k = \mathbb{F}_2$, les matrices $B_1 = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$ et $B_0 = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{0} \end{pmatrix}$ sont semblables : on a $B_1 = PB_0P$ où $P = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} = P^{-1}$. L'application $M \mapsto PMP$ est un isomorphisme de $\mathcal{A}_0$ sur $\mathcal{A}_1$.

13. a) $\det(A) = \overline{1}$, donc $A \in \mathcal{U}(\mathcal{A}_a)$.

    b) On effectue une récurrence sur n, en utilisant 3.b) (remarquons que $\det(A^{2^n}) = \overline{1}$).
    - Pour $n = 0$, on a $\mathrm{tr}(A) = \overline{4} = \overline{2}\,\overline{T_0}$.
    - Si on sait que $\mathrm{tr}(A^{2^n}) = \overline{2}\,\overline{T_n}$, alors $\mathrm{tr}(A^{2^{n+1}}) = \mathrm{tr}(A^{2^n})^2 - \overline{2}\det(A^{2^n}) = (\overline{2}\,\overline{T_n})^2 - \overline{2} = \overline{2}\,\overline{T_{n+1}}$.

    c) Posons $M = A^{2^{n-2}}$. On a $\det(M) = \overline{1}$. D'après 3.c).(iii), on a $\mathrm{tr}(M) = \overline{0} \iff M$ est d'ordre 4 dans $\mathcal{U}(\mathcal{A}_a)$. Or $\mathrm{tr}(M) = \overline{2}\,\overline{T}_{n-2}$; donc $\mathrm{tr}(M) = \overline{0} \iff p | T_{n-2}$.

    d)
    - Si A est d'ordre 2^n, alors $M = A^{2^{n-2}}$ vérifié $M^4 = \mathrm{I}_2$ et $M^2 \neq \mathrm{I}_2$ donc M est d'ordre 4.

- Si M est d'ordre 4, alors $A^{2^n} = M^4 = \mathrm{I}_2$, donc l'ordre de A divise 2^n et $A^{2^{n-1}} = M^2 \neq \mathrm{I}_2$ donc cet ordre ne divise pas 2^{n-1}. Cet ordre est 2^n.

L'ordre de A divise l'ordre de $\mathcal{U}_a$, donc $2^n \leqslant \mathrm{Card}(\mathcal{U}(\mathcal{A}_a)) \leqslant \mathrm{Card}(\mathcal{A}_a \setminus \{0_2\}) = p^2 - 1$.

Partie III.

14. a) Soient $M, M' \in \mathcal{A}_a$ et $x \in \mathbb{F}_p$.
   - On a $F(MM') = (MM')^p = M^p(M')^p = F(M) = F(M')$ puisque $\mathcal{A}_a$ est commutatif.
   - On a $(M+M')^p = \sum_{k=0}^{m} \overline{\binom{p}{k}} M^k (M')^k = M^p + M'^p$ puisque pour tout $k \in \mathbb{N}$ avec $1 \leqslant k \leqslant p-1$, on a $p | \binom{p}{k}$.
   - On a $x^p = x$, donc $F(xM) = (xM)^p = x^p M^p$

   Les deux premières propriétés démontrent que F est un homomorphisme d'anneaux ; les deux dernières que F est $\mathbb{F}_p$-linéaire.

   b) On a $B^2 = a\,\mathrm{I}_2$, donc $B^p = (B^2)^{\frac{p-1}{2}} B = a^{\frac{p-1}{2}} B$.

   c) Si $a = 0$, alors $F(B) = 0_2$ et $F(\mathrm{I}_2) = \mathrm{I}_2$. On en déduit que $F \circ F$ coïncide avec F sur la base (I_2, B) donc $F \circ F = F$ et F est un projecteur. Comme F n'est pas l'application nulle, son noyau est de dimension au plus 1 : c'est la droite $\{xB;\ x \in \mathbb{F}_p\}$. Son image est donc de dimension 1 et contient I_2 ; c'est la droite $\{x\,\mathrm{I}_2;\ x \in \mathbb{F}_p\}$.

   d) Si $a = u^2$ avec $u \in k^*$, on a $a^{\frac{p-1}{2}} = u^{p-1} = \overline{1}$, donc $F(B) = B$. Alors F coïncide avec l'application identique sur la base (I_2, B) donc F est l'application identique.

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

   (i) Dans ce cas $a^{\frac{p-1}{2}} = -\overline{1}$ d'après la question 2.d). Donc $F(B) = -B$. Les applications linéaires F et φ qui coïncident sur une base sont égales.

   (ii) Comme F est $\mathbb{F}_p$-linéaire et un morphisme d'anneaux, on a $P(F(M)) = F(P(M))$ pour tout polynôme $P \in \mathbb{F}_p[X]$. Donc si M est racine du polynôme $P = X^2 - uX + v$, alors $F(M)$ est aussi une racine de P.

   Si P est irréductible dans $\mathbb{F}_p$, il n'a pas de racines dans $\mathbb{F}_p$ donc $M \notin \{x\,\mathrm{I}_2;\ x \in \mathbb{F}_p\}$ - donc $F(M) \neq M$. Donc P, vu comme élément de $\mathcal{A}_a[X]$, admet les racines M et $F(M)$ et, comme il est unitaire, il est égal à $(X - M)(X - F(M))$. Il vient $u\,\mathrm{I}_2 = M + F(M)$ et $v\,\mathrm{I}_2 = MF(M)$.

   (iii) On a $M^{p+1} = M\varphi(M) = \det(M)\,\mathrm{I}_2$ d'après la question 7.a).

15. On a $C = \begin{pmatrix} \overline{1} & \overline{3} \\ \overline{1} & \overline{1} \end{pmatrix}$, donc $C^2 = \begin{pmatrix} \overline{4} & \overline{6} \\ \overline{2} & \overline{4} \end{pmatrix} = \overline{2}A$.

On a $C^{p+1} = \det(C)\,\mathrm{I}_2$, or $\det C = -\overline{2}$.

Enfin $A^{\frac{p+1}{2}} = ((\overline{2})^{-1} C^2)^{\frac{p+1}{2}} = ((\overline{2})^{\frac{p+1}{2}})^{-1} C^{p+1}$.

Or, comme $\overline{2}$ est un carré dans $\mathbb{F}_p$, $(\overline{2})^{\frac{p-1}{2}} = 1$, donc $((\overline{2})^{\frac{p+1}{2}})^{-1} = (\overline{2})^{-1}$. Et comme $C^{p+1} = -\overline{2}\,\mathrm{I}_2$, il vient $A^{\frac{p+1}{2}} = -\mathrm{I}_2$.

Partie IV.

16. Si a, b sont des entiers $\geqslant 2$, alors $2^{ab} - 1 = (2^a - 1) \sum_{k=0}^{b-1} 2^{ka}$. Donc $2^{ab} - 1$ n'est pas premier. Donc si $2^m - 1$ est premier, m est premier. Ici $p = 2^m - 1 \geqslant 5$, donc $m \neq 2$: c'est un nombre premier impair.

17. Comme m est impair $m - 1$ est pair de la forme 2ℓ. Or $2^2 \equiv 1 \ \ [3]$, donc $3 | 2(2^{2\ell} - 1) = p - 1$.

18. D'après la question 3.b), il y a 3 éléments dans $\mathbb{F}_p^*$ tels que $x^3 = \overline{1}$. Il y en a donc deux distincts de $\overline{1}$. Ces éléments sont d'ordre 3.
19. On a $\overline{0} = b^3 - \overline{1} = (b - \overline{1})(b^2 + b + \overline{1})$ et, puisque $b \neq \overline{1}$ (et $\mathbb{F}_p$ est un corps), il vient $b^2 + b + \overline{1} = \overline{0}$. Donc $(\overline{2}b + \overline{1})^2 = \overline{4}b^2 + \overline{4}b + \overline{1} = \overline{4}(b^2 + b + \overline{1}) - \overline{3} = -\overline{3}$.
20. Comme $4|2^m$, on a $\dfrac{p-1}{2}$ est impair, donc $(-\overline{1})^{\frac{p-1}{2}} = -\overline{1}$, donc $-\overline{1}$ n'est pas un carré dans $\mathbb{F}_p$ d'après 2.d).
21. Si $\overline{3}$ était un carré, comme $-\overline{3}$ est un carré, leur quotient $-\overline{1}$ serait un carré.
22. On a $\overline{2}^m = \overline{1}$ (puisque $p = 2^m - 1$). Donc $\overline{2} = \overline{2}^{m+1} = (\overline{2}^{\frac{m+1}{2}})^2$. C'est un carré.
23. - Si $p = 2^q - 1$ est premier, alors dans la question 15, $A^{\frac{p+1}{2}} = -\mathrm{I}_2$. Or $\dfrac{p+1}{2} = 2^{q-1}$. On en déduit que $A^{2^q} = \mathrm{I}_2$, donc l'ordre de A divise 2^q mais pas 2^{q-1} donc A est d'ordre 2^q, donc p divise T_{q-2} d'après 13.d).
    - Supposons que $2^q - 1$ divise T_{q-2} et soit p le plus petit diviseur premier de $2^q - 1$. Comme $p|T_{q-2}$, on en déduit que A est d'ordre 2^q dans $\mathcal{U}(\mathcal{A}_a)$ et $2^q \leqslant p^2 - 1$ d'après 13.d). Or p étant le plus petit diviseur $\neq 1$ de $2^q - 1$, on a ou bien $2^q - 1 = p$ ou bien $2^q - 1 \geqslant p^2$. Le deuxième cas est exclu donc $2^q - 1$ est premier.
24. Le nombre $2^5 - 1 = 31$ est premier, donc il divise T_3. On a $T_0 = 2$, $T_1 = 7$, $T_2 = 97$ et $T_3 = 18817 = 31 \times 607$. On vérifie que 607 est premier.

Partie V.

25. a) L'application $\mathbb{F}_p \to K$, $x \mapsto x\,\mathrm{I}_2$ est clairement un homomorphisme injectif.
    b) Si $x = y^2$ est un carré dans $\mathbb{F}_p$, alors $x\,\mathrm{I}_2 = (y\,\mathrm{I}_2)^2$. Si x n'est pas un carré, alors xa^{-1} est un carré. (En effet $(xa^{-1})^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} a^{-\frac{p-1}{2}} = (-\overline{1})(-\overline{1}) = \overline{1}$). Si on écrit $x = ay^2$, on a $x\,\mathrm{I}_2 = (yB)^2$.
    c) D'après 25.b), il existe $M \in K$ tel que $(c^2 - 4d)\mathrm{I}_2 = M^2$. Alors
$$X^2 + cX + d = \Big(X - (\overline{2})^{-1}(-c\,\mathrm{I}_2 + M)\Big)\Big(X - (\overline{2})^{-1}(-c\,\mathrm{I}_2 - M)\Big)$$
    est scindé dans $K[X]$.
26. a) La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible si et seulement si ses vecteurs-colonne sont indépendants, *i.e.* si $(a, b) \in k^2 \setminus \{(\overline{0}, \overline{0})\}$ et $(c, d) \in k^2 \setminus k(a, b)$. On en déduit que $\mathrm{Card}(GL_2(\mathbb{F}_p)) = (p^2 - 1)(p^2 - p)$.
    b)
    - Si M a une valeur propre double x et est diagonalisable, alors $M = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, $x \in \mathbb{F}_p$.
    - Supposons que M a une valeur propre double x et n'est pas diagonalisable. Alors $M - x\,\mathrm{I}_2 \neq 0_2$ et $(M - x\,\mathrm{I}_2)^2 = 0_2$. Soit $V \in \mathbb{F}_p^2 \setminus \ker(M - x\,\mathrm{I}_2)$; posons $U = (M - x\,\mathrm{I}_2)V$. Alors U est un vecteur non nul de $\ker(M - x\,\mathrm{I}_2)$ (puisque $(M - x\,\mathrm{I}_2)^2 = 0_2$, donc (U, V) est une base de $\mathbb{F}_p^2$. Dans cette base, la matrice de $M - x\,\mathrm{I}_2$ est $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$; celle de M est $\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$.
    - Si M a deux valeurs propres distinctes $x, y \in \mathbb{F}_p$, $x \neq y$, alors M est semblable à $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$.
    - Enfin, si le polynôme caractéristique P de M est irréductible dans $\mathbb{F}_p$. Il admet une racine $x\,\mathrm{I}_2 + yB$ dans K avec $y \neq 0$ (puisque x n'est pas racine) - son polynôme caractéristique est donc $X^2 - 2xX + x^2 - ay^2 = (X - x)^2 - ay^2$ et on a donc $(M - x\,\mathrm{I}_2)^2 = ay^2\,\mathrm{I}_2$. Posons $B' = y^{-1}(M - x\,\mathrm{I}_2)$, de sorte que $(B')^2 = a\,\mathrm{I}_2$ et $M = x\,\mathrm{I}_2 + yB'$. Soit U un vecteur non nul ; posons $V = B'U$. Alors, comme B' n'a pas de vecteurs propres, (U, V) est une base de $\mathbb{F}_p^2$. Alors $B'V = aU$ donc la matrice de B' dans la base (U, V) est B. Donc B' est semblable à B et M à $x\,\mathrm{I}_2 + yB$.

c) Dans le cas I) (*resp.* II), il y a une classe de similitude par $x \in \mathbb{F}_p$. Il y en donc p.
Dans la cas III) on a une classe de similitude pour chaque ensemble $\{x, y\}$ à deux éléments (distincts) de $\mathbb{F}_2$: il y a $\dfrac{p(p-1)}{2}$ classes.
Si $x\,\mathrm{I}_2 + yB$ et $x'\,\mathrm{I}_2 + y'B$ sont semblables, elles ont même trace, donc $2x = 2x'$ et $x = x'$, et même déterminant, donc $x^2 - ay^2 = (x')^2 - a(y')^2$, soit $y^2 = (y')^2$, donc $y = \pm y'$. Enfin comme $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -B$, les matrices si $x\,\mathrm{I}_2 + yB$ et $x\,\mathrm{I}_2 - yB$ sont semblables. Il y a donc $\dfrac{p(p-1)}{2}$ classes de type IV) (rappelons que $y \neq 0$).

d) Une matrice scalaire n'est semblable qu'à elle même ($P(x\,\mathrm{I}_2)P^{-1} = x\,\mathrm{I}_2$). Le cardinal des classes de similitude dans le cas I) est 1.
On fait agir $GL_2(\mathbb{F}_p)$ dans $M_2(\mathbb{F}_p)$ par $P \cdot M = PMP^{-1}$. La classe de similitude de M est l'orbite de M sous cette action. Le cardinal de la classe de M est donc $\dfrac{\mathrm{Card}(GL_2(\mathbb{F}_p))}{\mathrm{Card}(\mathrm{Stab}(M))}$.
Or le stabilisateur de M est l'ensemble de matrices inversibles P telles que $PM = MP$.
On a $P\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} P$ si et seulement si $P\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} P$ ce qui a lieu si et seulement si P est de la forme $\begin{pmatrix} z & y \\ 0 & z \end{pmatrix}$ avec $y, z \in \mathbb{F}_p$. Une telle matrice est inversible si et seulement si $z \neq 0$; donc le cardinal d'une orbite de type II) est $\dfrac{(p^2-1)(p^2-p)}{(p-1)p} = p^2 - 1$.
Pour $x \neq y$, on a $P\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} P$ si et seulement si P est diagonale. Le nombre des matrices diagonales inversibles est $(p-1)^2$, donc le cardinal d'une orbite de type III) est $\dfrac{(p^2-1)(p^2-p)}{(p-1)^2} = p(p+1)$.
Pour $y \neq 0$, on a $P(x\,\mathrm{I}_2 + yB) = (x\,\mathrm{I}_2 + yB)P$ si et seulement si $PB = BP$ ce qui a lieu si et seulement si $P \in \mathcal{A}_a$. Comme $\mathcal{A}_a$ est un corpes, il y a $p^2 - 1$ éléments inversibles dans $\mathcal{A}_a$, donc le cardinal d'une orbite de type IV) est $\dfrac{(p^2-1)(p^2-p)}{p^2-1} = p^2 - p$.