Les calculatrices, téléphones, tablettes, ordinateurs, montres connectées et tous appareils électroniques de communication ou de stockage, ainsi que les documents sont interdits.

La qualité de la rédaction est un facteur important d'appréciation des copies. Les candidats sont donc invités à produire des raisonnements clairs, complets et concis.

Les candidats peuvent utiliser les résultats énoncés dans les questions ou parties précédentes, en veillant dans ce cas à préciser la référence du résultat utilisé.

Notations, vocabulaire et rappels

Soit $\mathbf{F}$ un corps. On note $\mathrm{car}(\mathbf{F})$ sa caractéristique et $\mathbf{F}^*$ le groupe des éléments inversibles de $\mathbf{F}$. On désigne par $\mathbf{F}[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{F}$. Pour deux entiers naturels non nuls m et n, on note $\mathcal{M}_{m,n}(\mathbf{F})$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans $\mathbf{F}$; lorsque $m = n$, on note aussi $\mathcal{M}_n(\mathbf{F})$ l'algèbre des matrices carrées de taille n à coefficients dans $\mathbf{F}$ et $\mathrm{GL}_n(\mathbf{F})$ le groupe formé par le sous-ensemble des matrices inversibles dans $\mathcal{M}_n(\mathbf{F})$; on note I_n la matrice identité de $\mathcal{M}_n(\mathbf{F})$.

On fixe n un entier $\geqslant 1$. On note $\sim$ la *relation de similitude* sur $\mathcal{M}_n(\mathbf{F})$:

$$A \sim B \text{ s'il existe } P \text{ dans } \mathrm{GL}_n(\mathbf{F}) \text{ telle que } B = PAP^{-1}.$$

On rappelle qu'il s'agit d'une relation d'équivalence dont les classes d'équivalence sont appelées les *classes de similitude*. Deux matrices dans une même classe de similitude sont dites *semblables*.

Pour un entier $r \geqslant 1$, des entiers $n_1, \ldots, n_r$ tous $\geqslant 1$, et des matrices $A_1, ..., A_r$ telles que A_i appartienne à $\mathcal{M}_{n_i}(\mathbf{F})$ pour tout entier i compris entre 1 et r, on note $\mathrm{diag}(A_1, \ldots, A_r)$ la matrice diagonale par blocs, dont les blocs diagonaux sont dans l'ordre $A_1, ..., A_r$. Ainsi, on a :

$$\mathrm{diag}(A_1, \ldots, A_r) = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r \end{pmatrix} \in \mathcal{M}_{n_1+\cdots+n_r}(\mathbf{F}).$$

Pour une matrice M dans $\mathcal{M}_n(\mathbf{F})$, on note μ_M son polynôme minimal et χ_M son polynôme caractéristique. La sous-algèbre de $\mathcal{M}_n(\mathbf{F})$ formée par l'ensemble des polynômes en M est notée $\mathbf{F}[M]$.

On dit qu'une matrice N dans $\mathcal{M}_n(\mathbf{F})$ est *nilpotente* s'il existe un entier $k > 0$ tel que $N^k = 0$; on note alors $d(N)$ *l'indice de nilpotence* de N, c'est à dire le plus petit entier k qui vérifie cette propriété.

On pose

$$J_n = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix} \in \mathcal{N}_n(\mathbf{F}),$$

la *matrice de Jordan nilpotente* de taille n.

On pourra utiliser la *décomposition de Jordan* d'un élément N de $\mathcal{N}_n(\mathbf{F})$:
il existe un unique entier $r \geqslant 1$, et une unique suite d'entiers $n_1, ..., n_r$ vérifiant $1 \leqslant n_1 \leqslant \cdots \leqslant n_r$ et $n_1 + \cdots + n_r = n$ telle que

$$N \sim \mathrm{diag}(J_{n_1}, \dots, J_{n_r}).$$

On dit qu'une matrice M dans $\mathcal{M}_n(\mathbf{F})$ est *unipotente* s'il existe une matrice nilpotente N telle que $M = I_n + N$.
On note $\mathcal{N}_n(\mathbf{F})$ l'ensemble des matrices nilpotentes de $\mathcal{M}_n(\mathbf{F})$. On définit l'ensemble des matrices unipotentes de $\mathcal{M}_n(\mathbf{F})$ comme :

$$\mathcal{U}_n(\mathbf{F}) = I_n + \mathcal{N}_n(\mathbf{F}) = \{I_n + N, N \in \mathcal{N}_n(\mathbf{F})\}.$$

Si V et V' sont des $\mathbf{F}$-espaces vectoriels de dimension finie, on note $\mathrm{Hom}_{\mathbf{F}}(V, V')$ le $\mathbf{F}$-espace vectoriel des applications $\mathbf{F}$-linéaires de V dans V'. On pose $\mathrm{End}_{\mathbf{F}}(V) = \mathrm{Hom}_{\mathbf{F}}(V, V)$, et on note $\mathrm{GL}_{\mathbf{F}}(V)$ l'ensemble des endomorphismes inversibles de $\mathrm{End}_{\mathbf{F}}(V)$; on rappelle que $\mathrm{GL}_{\mathbf{F}}(V)$ est un groupe pour la loi de composition.

On note $\mathbf{C}$ le corps des nombres complexes et $\mathbf{R}$ le corps des nombres réels. Si p est un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

On rappelle le *théorème de Cauchy* :
Soit G un groupe fini. On note n son ordre. Si p est un nombre premier diviseur de n, alors G contient un élément d'ordre p.

Dans tous les exercices, n désigne un entier $\geqslant 1$.

Exercice 1

Soit A une matrice dans $\mathcal{M}_n(\mathbf{C})$. Une matrice M dans $\mathcal{M}_n(\mathbf{C})$ telle que $M^2 = A$ est appelée une *racine carrée* de A. On note $R(A)$ l'ensemble des racines carrées de A.

1. Soient A et B deux matrices semblables dans $\mathcal{M}_n(\mathbf{C})$. Démontrer que $R(A)$ et $R(B)$ sont en bijection.
2. Soit α dans $\mathbf{C}$. Justifier que $R(\alpha I_n)$ est une réunion de classes de similitude.
3. Déterminer le nombre de classes de similitude dont est constitué $R(I_n)$.
4. Déterminer le nombre de classes de similitude dont est constitué l'ensemble $R(0)$ des racines carrées de la matrice nulle de $\mathcal{M}_n(\mathbf{C})$.
   Indication : On pourra utiliser la décomposition de Jordan.
5. On suppose, dans cette question, que A est diagonalisable et que ses valeurs propres sont deux à deux distinctes. On fixe une matrice P dans $\mathrm{GL}_n(\mathbf{C})$ telle que PAP^{-1} est diagonale.
   a) Démontrer que si M est une racine carrée de A, alors PMP^{-1} est également diagonale.
   b) En déduire le nombre de racines carrées de A.
   c) Donner un exemple de matrice de A dans $\mathcal{M}_2(\mathbf{C})$ diagonalisable dont au moins une racine carrée n'est pas diagonalisable.
6. La matrice $-I_n$ admet-elle des racines carrées dans $\mathcal{M}_n(\mathbf{R})$?
   On distinguera selon la parité de n.
7. Démontrer que la matrice J_{2n}^2 est semblable à la matrice $\mathrm{diag}(J_n, J_n)$ et J_{2n+1}^2 à la matrice $\mathrm{diag}(J_n, J_{n+1})$.
8. On suppose dans cette question que A est nilpotente. A est donc semblable à une unique matrice de la forme $\mathrm{diag}(J_{n_1}, \ldots, J_{n_r})$, où r est un entier $\geqslant 1$ et $n_1, \ldots, n_r$ sont des entiers tels que $1 \leqslant n_1 \leqslant \cdots \leqslant n_r$ et $n_1 + \cdots + n_r = n$.
   a) Dans le cas où $r = 4$, et $(n_1, n_2, n_3, n_4) = (3, 4, 4, 4)$, A admet-elle une racine carrée ?
   b) Dans le cas où $r = 4$, et $(n_1, n_2, n_3, n_4) = (3, 4, 4, 6)$, A admet-elle une racine carrée ?
   c) Dans le cas où $r = 5$, et $(n_1, n_2, n_3, n_4, n_5) = (1, 1, 1, 3, 3)$, A admet-elle une racine carrée ?
   d) Décrire brièvement, en langage naturel, un algorithme permettant de déterminer si la matrice A admet une racine carrée à partir de la donnée de la suite ordonnée $n_1, \ldots, n_r$.

Exercice 2

Soit $\mathbf{F}$ un corps.

1. Déterminer le polynôme minimal et le polynôme caractéristique de la matrice J_n. Que vaut l'indice de nilpotence $d(J_n)$?

2. Soit r un entier naturel $\geqslant 1$. Soit $n_1, ..., n_r$ une famille de r entiers vérifiant $1 \leqslant n_1 \leqslant \cdots \leqslant n_r$ et $n_1 + \cdots + n_r = n$. Démontrer que $d(\mathrm{diag}(J_{n_1}, ..., J_{n_r})) = n_r$.
3. Soit N dans $\mathcal{N}_n(\mathbf{F})$.
   a) Démontrer que $\mu_N = X^{d(N)}$.
   b) Déterminer la dimension de $\mathbf{F}[N]$.
4. Soit N dans $\mathcal{N}_n(\mathbf{F})$. Démontrer que $I_n + N$ est une matrice inversible.

On suppose jusqu'à la fin de cette partie que $\mathrm{car}(\mathbf{F}) \neq 2$.

5. Soit N dans $\mathcal{N}_n(\mathbf{F})$.
   a) Démontrer que $2N + N^2$ est une matrice nilpotente telle que $d(2N + N^2) = d(N)$.
   b) Démontrer l'égalité $\mathbf{F}[2N + N^2] = \mathbf{F}[N]$. En déduire que N est un polynôme en $2N + N^2$.
6. On considère l'application

$$\begin{array}{rccc} \phi & : & \mathcal{N}_n(\mathbf{F}) & \to & \mathcal{N}_n(\mathbf{F}) \\ & & N & \mapsto & 2N + N^2 \end{array}$$

   a) Démontrer que l'application ϕ est une injection de $\mathcal{N}_n(\mathbf{F})$ dans lui-même.
   b) Soit N dans $\mathcal{N}_n(\mathbf{F})$ d'indice $d(N) = n$. Démontrer que $2N + N^2 \sim J_n$.
   c) En déduire que ϕ est une bijection de $\mathcal{N}_n(\mathbf{F})$ dans lui-même.
7. En déduire que l'application qui envoie une matrice sur son carré ($U \mapsto U^2$) définit une bijection de $\mathcal{U}_n(\mathbf{F})$ dans lui-même.
8. Dans cette question uniquement, $\mathbf{F}$ est le corps des nombres complexes $\mathbf{C}$.
   a) Soit M une matrice dans $\mathrm{GL}_n(\mathbf{C})$. On suppose M diagonalisable. Démontrer qu'il existe une matrice P dans $\mathrm{GL}_n(\mathbf{C})$ telle que $M = P^2$.
   b) Démontrer que l'application qui envoie une matrice sur son carré ($P \mapsto P^2$) définit une surjection de $\mathrm{GL}_n(\mathbf{C})$ sur lui-même. Est-elle injective ?
   Indication : on pourra utiliser la décomposition de Dunford.
9. L'application qui envoie une matrice sur son carré ($P \mapsto P^2$) définit-elle une surjection de $\mathrm{GL}_n(\mathbf{R})$ sur lui-même ?

Exercice 3

Soit p un nombre premier.
On rappelle que, si $\mathbf{k}$ est un corps de caractéristique p, on a l'identité remarquable :

$$(X + Y)^p = X^p + Y^p$$

dans l'algèbre des polynômes à coefficients dans $\mathbf{k}$ en deux variables X et Y.

Dans cet exercice, $\mathbf{K}$ désigne un corps algébriquement clos qui contient le corps $\mathbf{F}_p$. Pour x dans $\mathbf{K}$, on pose $\phi_p(x) = x^p$.

1. Justifier que $\mathbf{K}$ est un corps de caractéristique p.

On rappelle alors que ϕ_p est un morphisme du corps $\mathbf{K}$, appelé *morphisme de Frobenius*.

Pour tout entier $k \geqslant 1$, on note ϕ_p^k le k-ième itéré de ϕ_p, défini par récurrence sur k :

$$\phi_p^1 = \phi_p \text{ et si } \ k \geqslant 2,\ \phi_p^k = \phi_p^{k-1} \circ \phi_p.$$

2. Démontrer que ϕ_p est un automorphisme du corps $\mathbf{K}$.
3. Démontrer que pour tout entier $k \geqslant 1$, on a :

$$\forall x \in \mathbf{K},\ \phi_p^k(x) = x^{p^k}.$$

Soit k un entier $\geqslant 1$. On pose $q = p^k$ et $\phi_q = \phi_p^k$. Soit $\mathbf{L} = \{x \in \mathbf{K},\ \phi_q(x) = x\}$.

4. Démontrer que $\mathbf{L}$ est de cardinal inférieur ou égal à q.
5. Démontrer que $\mathbf{L}$ est de cardinal exactement q.
6. Démontrer que $\mathbf{L}$ est le seul sous-corps de $\mathbf{K}$ de cardinal q.

On désigne alors par $\mathbf{F}_q$ le corps $\mathbf{L}$, c'est-à-dire l'unique sous-corps de $\mathbf{K}$ de cardinal q.

7. Démontrer que $\phi_q(\mathbf{F}_{q^2}) \subset \mathbf{F}_{q^2}$ puis que $\mathbf{F}_q = \{x \in \mathbf{F}_{q^2},\ \phi_q(x) = x\}$.

Exercice 4

Soit p un nombre premier. Un groupe dont l'ordre est une puissance de p est appelé un *p-groupe*. Si G est un groupe, un sous-groupe de G dont l'ordre est une puissance de p est appelé un *p-sous-groupe* de G.

1. Soit α un entier $\geqslant 1$ et soit H un p-sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$ d'ordre p^α.
   a) Démontrer que tout élément x de H vérifie $x^{p^\alpha} = I_n$.
   b) En déduire que $H \subset \mathcal{U}_n(\mathbf{F}_p)$.
2. Soit H un sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$ contenu dans $\mathcal{U}_n(\mathbf{F}_p)$.
   a) Démontrer qu'il existe un entier $\alpha > 0$ tel que tout élément x de H vérifie $x^{p^\alpha} = I_n$.
   Indication : on pourra considérer α tel que $p^\alpha \geqslant n$.
   b) En déduire que H est un p-groupe.
   Indication : On pourra utiliser le théorème de Cauchy rappelé en préambule du sujet.
3. Soit G un groupe fini. On désigne par r son ordre.
   a) Démontrer que G est isomorphe à un sous-groupe du groupe symétrique $\mathfrak{S}_r$.
   b) En déduire que G est isomorphe à un sous-groupe de $\mathrm{GL}_r(\mathbf{F}_p)$.
4. Soit G un groupe fini. Démontrer que les assertions suivantes sont équivalentes :
   (i) G est un p-groupe.
   (ii) Il existe r dans $\mathbf{N}\backslash\{0\}$ tel que G est isomorphe à un sous-groupe de $\mathrm{GL}_r(\mathbf{F}_p)$ contenu dans $\mathcal{U}_r(\mathbf{F}_p)$.

Problème

Notations, vocabulaire et rappels

Soit G un groupe.

On définit le *centre* de G, noté $Z(G)$ par $Z(G) = \{g \in G,\ \forall x \in G, gx = xg\}$.

Pour tout (g, h) dans G^2, on définit le *commutateur* de g et h, noté $[g, h]$, en posant $[g, h] = ghg^{-1}h^{-1}$.

On définit alors le *sous-groupe dérivé* de G, noté $D(G)$, comme le sous-groupe de G engendré par tous ses commutateurs.

On admet que $Z(G)$ et $D(G)$ sont des sous-groupes distingués de G.

On note $\widehat{G}$ le groupe multiplicatif des morphismes de groupes de G dans $\mathbf{C}^*$.

On note $\mathrm{Aut}(G)$ le groupe des automorphismes de G, c'est-à-dire des morphismes bijectifs de G dans lui-même. Le morphisme identité, noté Id_G, en est l'élément neutre.

Pour g un élément de G et H un sous-groupe de G, on note HgH l'ensemble $\{h_1gh_2, (h_1, h_2) \in H^2\}$.

Soit G un groupe fini et soit V un $\mathbf{C}$-espace vectoriel de dimension finie.

On rappelle que (π, V) est une *représentation* de G si $\pi : G \to \mathrm{GL}_{\mathbf{C}}(V)$ est un morphisme de groupe.

On rappelle qu'une représentation (π, V) de G est *irréductible* si $V \neq \{0\}$ et si les seuls sous-espaces de V stables par $\pi(g)$ pour tout g dans G sont $\{0\}$ et V.

Si H est un sous-groupe de G, on note V^H le sous-espace vectoriel des éléments de V fixés par H pour l'action de G sur V, c'est-à-dire :

$$V^H = \{x \in V,\ \forall h \in H, \pi(h)(x) = x\}.$$

On dit que deux représentations (π, V) et (π', V') de G sont *isomorphes* s'il existe un isomorphisme u de V dans V' tel que pour tout g dans G, $u \circ \pi(g) \circ u^{-1} = \pi'(g)$.

On note $\mathbf{C}[G]$ le $\mathbf{C}$-espace vectoriel des fonctions de G dans $\mathbf{C}$: il a pour dimension l'ordre de G et pour base canonique $(\delta_g)_{g \in G}$, où, pour g dans G, δ_g est la fonction qui à x dans G associe 1 si $x = g$ et 0 sinon.

Soit $\mathbf{F}$ un corps. Pour x, y et z dans $\mathbf{F}$, on pose $h(x, y, z) = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbf{F})$, et :

$$\mathcal{H}_3(\mathbf{F}) = \{h(x, y, z),\ (x, y, z) \in \mathbf{F}^3\}.$$

Partie I

On admet que, pour tout (x, y, z, x', y', z') dans $\mathbf{F}^6$, on a

$$h(x, y, z)h(x', y', z') = h(x + x', y + y', z + z' + xy').$$

1. Pour tout (x, y, z) dans $\mathbf{F}^3$, justifier que $h(x, y, z)$ est inversible et déterminer son inverse.

On admet que $\mathcal{H}_3(\mathbf{F})$ est un sous-groupe de $\mathrm{GL}_3(\mathbf{F})$.

2. Soit (x, y, z) dans $\mathbf{F}^3$.
   a) Pour tout entier naturel n, justifier l'égalité :
   $$h(x, y, z)^n = h\left(nx, ny, nz + \frac{n(n-1)}{2}xy\right).$$
   b) Soit p un nombre premier impair. On suppose dans cette question que $\mathbf{F}$ est un corps de caractéristique p. Justifier que $h(x, y, z)$ est d'ordre 1 ou p.
   c) Dans le cas où $\mathbf{F}$ est un corps de caractéristique 2,
      i. Quels sont les ordres des éléments de $\mathcal{H}_3(\mathbf{F})$?
      ii. Dans le cas où $\mathbf{F}$ est de plus un corps fini de cardinal q, expliciter le nombre d'éléments d'ordre 2.
3. Justifier la relation $[h(x, y, z), h(x', y', z')] = h(0, 0, xy' - yx')$ pour (x, y, z, x', y', z') dans $\mathbf{F}^6$.
4. En déduire que $Z(\mathcal{H}_3(\mathbf{F})) = D(\mathcal{H}_3(\mathbf{F})) = \{h(0, 0, z),\ z \in \mathbf{F}\}$.

On note $Ab(\mathcal{H}_3(\mathbf{F}))$ le quotient $\mathcal{H}_3(\mathbf{F})/D(\mathcal{H}_3(\mathbf{F}))$.

5. En considérant l'application
   $$\begin{array}{ccc} \mathcal{H}_3(\mathbf{F}) & \to & \mathbf{F}^2 \\ h(x, y, z) & \mapsto & \begin{pmatrix} x \\ y \end{pmatrix} \end{array}$$
   démontrer qu'il existe un isomorphisme entre les groupes $Ab(\mathcal{H}_3(\mathbf{F}))$ et $(\mathbf{F}^2, +)$.
6. Soient ψ_1 et ψ_2 dans $\widehat{(\mathbf{F}, +)}$. Soit $\psi_1 \otimes \psi_2$ l'application de $\mathbf{F}^2$ dans $\mathbf{C}^*$ définie par :
   $$\forall (x, y) \in \mathbf{F}^2,\ \psi_1 \otimes \psi_2 \begin{pmatrix} x \\ y \end{pmatrix} = \psi_1(x)\psi_2(y).$$
   a) Justifier que $\psi_1 \otimes \psi_2$ est un morphisme de groupes.
   b) Soit j l'application définie par :
   $$\begin{array}{rccc} j & : & \widehat{(\mathbf{F}, +)}^2 & \to & \widehat{(\mathbf{F}^2, +)} \\ & & (\psi_1, \psi_2) & \mapsto & \psi_1 \otimes \psi_2 \end{array}$$
   Démontrer que j est un isomorphisme entre les groupes $\widehat{(\mathbf{F}, +)}^2$ et $\widehat{(\mathbf{F}^2, +)}$.
7. Exhiber un isomorphisme de groupe entre $\widehat{\mathcal{H}_3(\mathbf{F})}$ et $\widehat{Ab(\mathcal{H}_3(\mathbf{F}))}$, et déterminer enfin un isomorphisme explicite entre $\widehat{\mathcal{H}_3(\mathbf{F})}$ et $\widehat{(\mathbf{F}, +)}^2$.

Soit p un nombre premier et soit k un entier ≥ 1. On pose $q = p^k$. On reprend les notations de l'exercice 3.

8. Démontrer que $(\mathbf{F}_p, +)$ et $\widehat{(\mathbf{F}_p, +)}$ sont isomorphes.
9. Démontrer que $(\mathbf{F}_q, +)$ et $(\mathbf{F}_p^k, +)$ sont isomorphes.
10. En déduire l'ordre de $\widehat{\mathcal{H}_3(\mathbf{F}_q)}$.

Partie II

Soient G un groupe fini et σ dans $\mathrm{Aut}(G)$. On suppose que σ est une involution, c'est à dire que $\sigma^2 = \mathrm{Id}_G$. On note $\tau : G \to G$ l'application définie par $\tau(g) = \sigma(g)^{-1}$. On pose

$$G^+ = \{g \in G, \sigma(g) = g\} \quad \text{et} \quad G^- = \{g \in G, \sigma(g) = g^{-1}\}.$$

11. Démontrer que G^+ est un sous-groupe de G.

On suppose désormais que G est d'ordre impair. On considère l'application

$$\begin{array}{rccc} \Phi & : & G & \to & G \\ & & x & \mapsto & x^2 \end{array}$$

12. a) Soit x dans G. Démontrer qu'il existe y dans G tel que $x = y^2$.
    Indication : on pourra considérer $x^{|G|+1}$ où $|G|$ désigne l'ordre de G.
    b) Démontrer que Φ est une bijection de G dans lui-même.
13. Démontrer que l'application Φ induit deux bijections, de G^+ dans G^+ et de G^- dans G^- respectivement.

On introduit l'application $m : G^- \times G^+ \to G$ définie par

$$m(x^-, x^+) = x^- x^+.$$

14. Démontrer que l'application m est bijective.
15. Démontrer que pour tout g dans G, on a : $\tau(G^+ g G^+) = G^+ \tau(g) G^+ = G^+ g G^+$.

Partie III

Soit G un groupe fini d'élément neutre e. Pour f et f' dans $\mathbf{C}[G]$ et g dans G, on définit :

$$f * f'(g) = \sum_{x \in G} f(x) f'(x^{-1} g).$$

Ainsi $f * f' \in \mathbf{C}[G]$ et la quantité $f * f'$ est clairement linéaire en f et f'.

16. Démontrer que pour tout (a, b) dans G^2, on a : $\delta_a * \delta_b = \delta_{ab}$.
17. On admet que $(\mathbf{C}[G], *)$ est une $\mathbf{C}$-algèbre. Démontrer que δ_e en est l'unité.

Soit (π, V) une représentation de G. On définit une application $\widetilde{\pi}$ de $\mathbf{C}[G]$ dans $\mathrm{End}_{\mathbf{C}}(V)$ en posant pour tout f dans $\mathbf{C}[G]$:

$$\widetilde{\pi}(f) = \sum_{g \in G} f(g) \pi(g) \in \mathrm{End}_{\mathbf{C}}(V).$$

18. Démontrer que $\widetilde{\pi}$ est un morphisme d'algèbres.

Partie IV

Pour G un groupe fini, on considère σ, G^+ et τ comme dans la partie II. Pour f dans $\mathbf{C}[G]$, on note $\widetilde{\tau}(f)$ l'application $f \circ \tau$. On note $\mathbf{C}[G^+\backslash G/G^+]$ le sous-espace vectoriel de $\mathbf{C}[G]$ défini par :

$$\mathbf{C}[G^+\backslash G/G^+] = \{f \in \mathbf{C}[G],\ \forall (x,y) \in (G^+)^2,\ \forall g \in G, f(xgy) = f(g)\}.$$

Une représentation (π, V) de G, est dite *distinguée* si $V^{G^+} \neq \{0\}$.

19. Démontrer que pour deux représentations isomorphes de G, (π', V') et (π, V), on a : $\dim(V'^{G^+}) = \dim(V^{G^+})$.

En particulier la propriété d'être distinguée ne dépend que de la classe d'isomorphisme d'une représentation.

20. Démontrer que pour tous $f,\ f'$ dans $\mathbf{C}[G]$, on a : $\tilde{\tau}(f * f') = \tilde{\tau}(f') * \tilde{\tau}(f)$.
21. Démontrer que $\mathbf{C}[G^+\backslash G/G^+]$ est stable par $*$.

On suppose désormais G d'ordre impair.

22. Démontrer que pour tout f dans $\mathbf{C}[G^+\backslash G/G^+]$, on a : $\tilde{\tau}(f) = f$.
23. En déduire que les éléments de $\mathbf{C}[G^+\backslash G/G^+]$ commutent pour la loi $*$, puis que $\widetilde{\pi}(\mathbf{C}[G^+\backslash G/G^+])$ est une famille commutative dans $\mathrm{End}_{\mathbf{C}}(V)$.
24. Démontrer que, pour tout f dans $\mathbf{C}[G^+\backslash G/G^+]$, V^{G^+} est stable par $\widetilde{\pi}(f)$.

On note, dans toute la suite de cette partie, $F \subset \mathrm{End}_{\mathbf{C}}(V^{G^+})$ l'espace vectoriel des endomorphismes induits par les éléments de $\widetilde{\pi}(\mathbf{C}[G^+\backslash G/G^+])$ sur V^{G^+}.

25. Soit u dans F et soit λ dans $\mathbf{C}$ une valeur propre de u. Démontrer que le sous-espace propre $\mathrm{Ker}(u - \lambda \mathrm{Id}_{V^{G^+}})$ est stable par tous les éléments de F.

On suppose désormais (π, V) irréductible et distinguée.

26. Démontrer que pour tout v dans $V \setminus \{0\}$, pour tout w dans V, il existe f dans $\mathbf{C}[G]$ telle que $\widetilde{\pi}(f)(v) = w$.
27. En déduire que pour tout v dans $V^{G^+} \setminus \{0\}$, pour tout w dans V^{G^+}, il existe f dans $\mathbf{C}[G^+\backslash G/G^+]$ telle que $\widetilde{\pi}(f)(v) = w$.
28. Démontrer que F ne contient que des homothéties puis que $\dim(V^{G^+}) = 1$.

On vient donc de démontrer que si G est d'ordre impair, et que (π, V) est une représentation irréductible distinguée de G, alors $\dim(V^{G^+}) = 1$.

Partie V

Soient p un nombre premier et k un entier ≥ 1. On pose $q = p^k$. On reprend les notations de l'exercice 3.

29. Quelles sont les représentations de dimension 1 de $\mathcal{H}_3(\mathbf{F}_q)$ à isomorphisme près ? Combien y en a-t-il ?

Soit ψ dans $\widehat{(\mathbf{F}_q, +)}$. On suppose ψ n'est pas constant égal à 1. Pour f dans $\mathbf{C}[\mathbf{F}_q]$ et $h(x_0, y_0, z_0)$ dans $\mathcal{H}_3(\mathbf{F}_q)$, on définit $\rho_\psi(h(x_0, y_0, z_0))f$ dans $\mathbf{C}[\mathbf{F}_q]$ par :

$$\rho_\psi(h(x_0, y_0, z_0))f : x \mapsto \psi(z_0 + xy_0)f(x + x_0).$$

On admet que l'application

$$\rho_\psi(h(x_0,y_0,z_0)) : f \mapsto \rho_\psi(h(x_0,y_0,z_0))f$$

est un endomorphisme de $\mathbf{C}[\mathbf{F}_q]$; ainsi, ρ_ψ définit une application de $\mathcal{H}_3(\mathbf{F}_q)$ dans $\mathrm{End}_{\mathbf{C}}(\mathbf{C}[\mathbf{F}_q])$.

30. Démontrer que $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$ est une représentation de $\mathcal{H}_3(\mathbf{F}_q)$.
31. Démontrer que, pour tout x dans $\mathbf{F}_q$, $\frac{1}{q}\sum_{y\in\mathbf{F}_q}\psi(xy) = \delta_0(x)$.
32. Démontrer que tout sous-espace vectoriel non réduit à $\{0\}$ de $\mathbf{C}[\mathbf{F}_q]$ et stable par $\rho_\psi(h(x_0,y_0,z_0))$, pour tout (x_0,y_0,z_0) dans $\mathbf{F}_q^3$, contient δ_0.
33. En déduire que $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$ est une représentation irréductible.
34. Démontrer que, pour tous ψ et ψ', deux éléments distincts et non constants à 1 de $\widehat{(\mathbf{F}_q,+)}$, les représentations $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$ et $(\rho_{\psi'}, \mathbf{C}[\mathbf{F}_q])$ ne sont pas isomorphes (on pourra s'intéresser à l'action de $Z(\mathcal{H}_3(\mathbf{F}_q))$ sur les représentations en question).
35. Quelle est la dimension de $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$?
36. En déduire toutes les classes d'isomorphisme de représentations irréductibles de $\mathcal{H}_3(\mathbf{F}_q)$.

Partie VI

On reprend les notations de l'exercice 3. On note s la restriction de ϕ_q à $\mathbf{F}_{q^2}$. On pose $G = \mathcal{H}_3(\mathbf{F}_{q^2})$ et on définit l'application $\sigma : G \to G$ par :

$$\forall (x,y,z) \in \mathbf{F}_{q^2},\ \sigma(h(x,y,z)) = h(s(x),s(y),s(z)).$$

37. Démontrer que σ est un élément d'ordre 2 de $\mathrm{Aut}(G)$.
38. Justifier que le sous-groupe G^+, défini en partie II, est égal à $\mathcal{H}_3(\mathbf{F}_q)$.
39. Déterminer les représentations de dimension 1 distinguées de G à isomorphisme près. Combien y en a-t-il ?

Soit ψ un élément de $\widehat{(\mathbf{F}_{q^2},+)}$, dont on suppose qu'il n'est pas constant égal à 1. On dispose d'après la partie V d'une représentation $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$ associée à ψ.

40. Démontrer que la représentation $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$ est distinguée si et seulement si, pour tout x dans $\mathbf{F}_q$, $\psi(x) = 1$.

On suppose désormais que la représentation $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$ est distinguée.

41. Démontrer que pour tout x dans $\mathbf{F}_{q^2}\setminus\mathbf{F}_q$, il existe (z_0,y_0) dans $\mathbf{F}_q^2$ tel que $\psi(z_0+xy_0) \neq 1$.
42. En déduire que pour cette représentation, on a : $\dim(\mathbf{C}[\mathbf{F}_{q^2}]^{G^+}) = 1$, même si $p = 2$.
43. Expliciter une bijection naturelle entre les classes d'isomorphisme de représentations irréductibles de G^+ et celles des représentations irréductibles distinguées de G.