Mathématiques Générales : corrigé
Agrégation Externe de Mathématiques 2022

J. Le Borgne

Exercice 1.

1. On dispose de $P \in GL_n(\mathbf{C})$ telle que $B = P^{-1}AP$. La conjugaison par P, $c_P : \mathcal{M}_n(\mathbf{C}) \to \mathcal{M}_n(C)$ définie par $M \mapsto P^{-1}MP$ est un automorphise de $\mathbf{C}$-algèbre. En particulier, pour tout $M \in \mathcal{M}_n(\mathbf{C})$, $c_P(M^2) = c_P(M)^2$. Il en résulte que $N \in R(B)$ si et seulement si $c_P(N) \in R(A)$. Ainsi, c_P induit une bijection de $R(B)$ sur $R(A)$.

2. Soit $M \in R(\alpha I_n)$, et soit $P \in GL_n(\mathbf{C})$. Alors $(P^{-1}MP)^2 = \alpha I_n$, donc $P^{-1}MP \in R(\alpha I_n)$. En particulier, $R(\alpha I_n)$ est stable par conjugaison. C'est donc une réunion de classes de similitude.

3. Soit $M \in \mathcal{M}_n(\mathbf{C})$ telle que $M^2 = I_n$. Alors le polynôme $X^2 - 1$ est un polynôme annulateur de M. Ce polynôme étant scindé à racines simples (égales à 1 et -1), M est diagonalisable, et semblable à une matrice de la forme $\begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$, où $p, q \in \mathbf{N}$ tels que $p + q = n$. Réciproquement, toute matrice de cette forme est dans $R(I_n)$, donc sa classe de similitude aussi. Il y a $n + 1$ classes de similitude de matrice de cette forme (une classe de similitude étant entièrement déterminée par la valeur de p qui est la multiplicité de 1 comme racine du polynôme caractéristique).

4. Soit $M \in \mathcal{M}_n(\mathbf{C})$ telle que $M^2 = 0$. Alors M est nilpotente d'indice 2, et d'après le théorème de Jordan, M est semblable à une matrice diagonale par blocs dont les blocs diagonaux sont de la forme (0) ou $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Si on note p le nombre de blocs de Jordan de taille 1 et q le nombre de blocs de taille 2, on a $p + 2q = n$. Réciproquement, étant donnés deux entiers p, q tels que $p + 2q = n$, la matrice de Jordan nilpotente ayant p blocs de taille 1 et q blocs de taille 2 vérifie $N^2 = 0$. Comme une classe de similitude de matrices nilpotente est entièrement déterminée par la taille de ses blocs de Jordan, les classes de similitude de $R(0)$ sont en bijection avec les couples d'entiers positifs ou nuls solutions de l'équation $p + 2q = n$, il y en a donc $\lfloor n/2 \rfloor$.

5.a) Supposons que M soit une racine carrée de A. Soit λ une valeur propre de A. Alors $\dim \ker(M^2 - \lambda I_n) = 1$. Notons μ une racine carrée de λ dans $\mathbf{C}$ (il en existe car $\mathbf{C}$ est algébriquement clos). D'après le lemme des noyaux, si $\lambda \neq 0$, $\ker(M - \mu I_n) \oplus \ker(M + \mu I_n) = \ker(A - \lambda I_n)$ est de dimension 1. En particulier, quitte à changer μ en $-\mu$, on peut supposer que $\ker(M - \mu I_n) = \ker(A - \lambda I_n)$. Si 0 est valeur propre de A, alors 0 est aussi valeur propre de M, et comme on a $\ker M \subset \ker M^2 = \ker A$ de dimension 1, on a encore l'égalité. On a donc, pour toute valeur propre λ de A, l'existence d'une unique racine carrée μ de λ dans $\mathbf{C}$ telle que $\ker(M - \mu I_n) = \ker(A - \lambda I_n)$. Comme les colonnes de P sont les éléments

d'une base adaptée à la décomposition en somme directe $\mathbf{C}^n = \bigoplus \ker(A - \lambda I_n)$, ce sont aussi les éléments d'une base adaptée à la décomposition en somme directe $\mathbf{C}^n = \bigoplus \ker(M - \mu I_n)$. En particulier, $P^{-1}MP$ est diagonale.

5.b) La question précédente montre qu'il y a 2^m racines carrées de A, où $m \in \{n-1, n\}$ est le nombre de valeurs propres non nulles de A (correspondant aux 2^m choix de m-uplets de racines carrées de valeurs propres de A).

5.c) Soit $A = 0 \in \mathcal{M}_2(\mathbf{C})$, alors A est diagonale et la racine carrée $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ de A n'est pas diagonalisable (elle est nilpotente et non nulle).

6. Montrons que $-I_n$ a une racine carrée dans $\mathcal{M}_n(\mathbf{R})$ si et seulement si n est pair. Supposons que $M^2 = -I_n$, alors $0 \leq \det(M)^2 = (-1)^n$, donc n la condition est nécessaire. Elle est suffisante car $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ vérifie $M^2 = -I_2$, donc si M_{2n} est diagonale par blocs avec pour blocs diagonaux n copies de M, on a $M_{2n}^2 = -I_{2n}$.

7. Soit $(e_1, \ldots, e_{2n})$ la base canonique de C^{2n}. L'application linéaire j_{2n} dont la matrice dans cette base est J_{2n} vérifie $j_{2n}^2(e_i) = e_{i+2}$ pour tout $3 \leq i \leq 2n$, et $j_{2n}^2(e_1) = j_{2n}^2(e_2) = 0$. En particulier, les sous-espaces vectoriels supplémentaires V_i et V_p engendrés respectivement par $\{e_1, e_3, \ldots, e_{2n-1}\}$ et $\{e_2, e_4, \ldots, e_{2n}\}$ sont stables par j_{2n}^2, et la matrice de l'endomorphisme induit par j_{2n}^2 sur chacun de ces sous-espaces dans ces bases est J_n. Ainsi, J_{2n}^2 est semblable à $\mathrm{diag}(J_n, J_n)$.
Le même argument, appliqué à la base canonique $(e_1, \ldots, e_{2n+1})$ de $\mathbf{C}^{2n+1}$ et aux sous-espaces engendrés par $\{e_1, e_3, \ldots, e_{2n+1}\}$ et $\{e_2, \ldots, e_{2n}\}$ montre le résultat analogue pour J_{2n+1}^2.

8.a) D'après la question 7, $\mathrm{diag}(J_7, J_8)^2$ est semblable à A.

8.b) Si A est un carré, alors une racine carrée de A est nilpotente, donc est aussi semblable à une matrice diagonale par blocs avec pour blocs diagonaux des matrices de la forme J_k. En outre, la question 7 montre qu'un tel bloc (s'il est de taille au moins 2) correspond à 2 blocs de Jordan de A dont les tailles diffèrent d'au plus 1 unité. Or A possède un seul bloc de Jordan de taille 6 mais pas de bloc de taille 5 ni 7. Donc A n'a pas de racine carrée.

8.c) D'après la question 7, $\mathrm{diag}(J_1, J_2, J_6)^2$ est semblable à A.

8.d) Le raisonnement détaillé en question 8)b. permet de donner l'algorithme récursif suivant :

- Si tous les n_i sont égaux à 1, renvoyer *VRAI*
- Sinon, et si $r = 1$, renvoyer *FAUX*
- Sinon, soient n_r et n_{r-1} les deux plus grands entiers de la liste. Si $|n_r - n_{r-1}| > 1$, renvoyer *FAUX*
  - Sinon, renvoyer le résultat de l'algorithme appliqué à la liste des autres nombres de la liste.

Exercice 2.

1. Comme J_n est triangulaire supérieure, on a $\chi_{J_n} = \det(XI_n - J_n) = X^n$. Ainsi, π_{J_n} est un diviseur de X^n. Comme $J_n^{n-1}(e_n) = e_1$, on a $J_n^{n-1} \neq 0$, et donc $\pi_{J_n} = X^n$. En particulier, $d(J_n) = n$.

2. Soit $M = \mathrm{diag}(J_{n_1}, \ldots, J_{n_r})$. Le produit matriciel par blocs montre que $M^{n_r} = 0$ et que $M^{n_r-1} \neq 0$. Donc l'indice de nilpotence de M est n_r.

3.a) Comme N est nilpotente d'indice $d(N)$, elle est annulée par $X^{d(N)}$. Ainsi, le polynôme minimal de N divise $X^{d(N)}$, il est donc de la forme X^δ avec $\delta \leq d(N)$. Par définition de $d(N)$, on a pour $0 \leq d < d(N)$, $N^d \neq 0$. Donc le polynôme minimal de N est $X^{d(N)}$.

3.b) Comme $N^{d(N)} = 0$, $\mathbf{F}[N]$ est engendré (en tant que $\mathbf{F}$-espace vectoriel) par $\{I_n, N, \ldots, N^{d(N)-1}\}$. Cette famille est linéairement indépendante, sans quoi N serait annulé par un polynôme à coefficients dans $\mathbf{F}$ et de degré $< d(N)$, contredisant le résultat de 3.a). Ainsi, cette famille est une base de $\mathbf{F}[N]$, qui est donc de dimension $d(N)$.

4. Soit $M = \sum_{j=0}^{d(N)-1}(-1)^j N^j$. Alors $M(I_n + N) = M - \sum_{j=1}^{d(N)-1} N^j = I_n$. Donc $I_n + N$ est inversible, d'inverse M.

5.a) On a $2N+N^2 = 2N(I_n+N/2)$. La matrice $I_n+N/2$ est inversible d'après la question 4 (comme N est nilpotente, $N/2$ l'est aussi). La matrice $2N$ est nilpotente, d'indice de nilpotence n car $\mathrm{car}(\mathbf{F}) \neq 2$. Les matrices $2N$ et $I_n + N/2$ commutent, donc $2N + N^2$ est nilpotente d'indice $d(N)$.

5.b) On a $2N + N^2 \in \mathbf{F}[N]$, donc $\mathbf{F}[2N + N^2] \subset F[N]$. De plus, comme $2N + N^2$ est nilpotente d'indice $d(N)$, la question 3.*b*) montre que $\dim \mathbf{F}[2N + N^2] = d(N) = \dim \mathbf{F}[N]$. Ainsi, $\mathbf{F}[2N+N^2] = \mathbf{F}[N]$ et en particulier $N \in \mathbf{F}[2N+N^2]$, c'est-à-dire que N est un polynôme en $2N + N^2$.

6.a) L'application ϕ est bien à valeurs dans $\mathcal{N}_n(\mathbf{F})$. Supposons que $N_1, N_2 \in \mathcal{N}_n(\mathbf{F})$ sont telles que $\phi(N_1) = \phi(N_2) = M$. D'après la question 5.b), $N_1, N_2 \in \mathbf{F}[N]$ donc N_1 et N_2 commutent. Comme N_1 et N_2 sont nilpotentes et commutent, la matrice N_1+N_2 est nilpotente, donc d'après la question 4., la matrice $N_1 + N_2 + 2I_n$ est inversible. Ainsi, la relation :

$$0 = \phi(N_1) - \phi(N_2) = (N_1 - N_2)(N_1 + N_2 + 2I_n)$$

montre que $N_1 = N_2$.

6.b) D'après la question 5.a), $M = 2N + N^2$ est nilpotente d'indice n. On dispose donc de $x \in \mathbf{F}^n$ tel que $M^{n-1}X \neq 0$. La famille $\{M^{n-1}X, MX, \ldots, X\}$ forme donc une base de $\mathbf{F}^n$ dans laquelle la matrice de l'endomorphisme canoniquement associé à M est J_n. Donc M est semblable à J_n.

6.c) Soit $M \in \mathcal{N}_n(\mathbf{F})$. On sait que M est semblable à une matrice de la forme $\mathrm{diag}(J_{n_1}, \ldots, J_{n_r})$. D'après la question précédente, pour tout $1 \leq i \leq r$, J_{n_i} est semblable à $2J_{n_i} + J_{n_i}^2$. En particulier, M est semblable à une matrice de la forme $\mathrm{diag}(2J_{n_1}+J_{n_1}^2, \ldots, 2J_{n_r}+J_{n_r}^2)$. On dispose ainsi de $P \in GL_n(\mathbf{F})$ telle que $P^{-1}MP = 2A + A^2$ avec $A = \mathrm{diag}(J_{n_1}, \ldots, J_{n_r}) \in \mathcal{N}_n(\mathbf{F})$. Donc ϕ est surjectif : c'est une bijection d'après 6.a).

7. Le diagramme suivant :

$$\begin{array}{ccc} \mathcal{U}_n(\mathbf{F}) & \xrightarrow{U\mapsto U^2} & \mathcal{U}_n(\mathbf{F}) \\ {\scriptstyle id-I_n}\downarrow & & \downarrow{\scriptstyle id-I_n} \\ \mathcal{N}_n(\mathbf{F}) & \xrightarrow{\phi} & \mathcal{N}_n(\mathbf{F}) \end{array}$$

est commutatif car $(I+N)^2 = I + \phi(N)$ pour tout $N \in \mathcal{N}_n(\mathbf{F})$. Les flèches verticales sont bijectives par définition de $\mathcal{U}_n(\mathbf{F})$, et ϕ est bijective d'après la question précédente, donc $U \mapsto U^2$ est bijective sur $\mathcal{U}_n(\mathbf{F})$.

8.a) Supposons M diagonalisable, on dispose de $Q \in GL_n(\mathbf{C})$ et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ telles que $Q^{-1}MQ = D$. Pour $1 \leq i \leq n$, on fixe μ_i une racine du polynôme $X^2 - \lambda_i$ (qui existe car $\mathbf{C}$ est algébriquement clos). Soit $\Delta = \mathrm{diag}(\mu_1, \ldots, \mu_n)$. On a $\Delta^2 = D$, donc $P = Q\Delta Q^{-1}$ est une racine carrée de M. Notons au possage que $P \in \mathbf{C}[M]$ (le polynôme d'interpolation envoyant λ_i sur μ_i pour tout i envoie M sur P).

8.b) Soit $M \in GL_n(\mathbf{C})$, dont on note $M = D + N = D(I_n + D^{-1}N)$ la décomposition de Dunford. On a donc $D \in GL_n(\mathbf{C})$ (car les valeurs propres de D sont celles de M). Comme D et N commutent, $I + D^{-1}N$ est unipotente. Elle possède donc une racine carrée U d'après la question 7. Comme D est diagonalisable, elle possède aussi une racine carrée P d'après la question 8.a). En outre, la construction de la question 7 comme celle de la question 8.a) montrent que ces racines carrées peuvent être choisies comme des polynômes respectivement en D et en $D^{-1}N$, donc en M car $D, N \in \mathbf{C}[M]$ d'après le théorème de Dunford. En particulier, P et U commutent, donc $(PU)^2 = P^2U^2 = D(I_n + D^{-1}N) = M$. Donc l'élévation au carré est surjective sur $GL_n(\mathbf{C})$. Cette application n'est pas injective : $(-I_n)^2 = I_n^2$.

9. Sur $GL_n(\mathbf{R})$, l'application $P \mapsto P^2$ n'est pas surjective : en effet, si $M = P^2 \in GL_n(\mathbf{R})$, alors $\det M = (\det P)^2 > 0$, or il existe des matrices de déterminant < 0 dans $GL_n(\mathbf{R})$ pour tout $n \geq 1$ (par exemple, la matrice $\mathrm{diag}(-1, I_{n-1})$).

Exerice 3.

1. Comme K contient $\mathbf{F}_p$, on a $1_K = 1_{\mathbf{F}_p}$, donc $p1_K = 0$. Ainsi, K est de caractéristique p.

2. On sait que ϕ_p est un morphisme de corps, il est donc injectif (son noyau est un idéal de $\mathbf{K}$ qui ne peut être égal à $\mathbf{K}$, c'est donc $\{0\}$). Comme ϕ_p est une application polynomiale et $\mathbf{K}$ est algébriquement clos, l'équation $\phi_p(x) = a$ possède une solution pour tout $a \in \mathbf{K}$, donc ϕ_p est surjectif.

3. Démontrons cette formule pour tout $k \geq 1$ par récurrence sur k.
Initialisation. Lorsque $k = 1$, par définition de ϕ_p, on a pour tout $x \in \mathbf{K}$, $\phi_p^1(x) = x^p$.
Hérédité. Supposons le résultat vrai pour un $k \geq 1$. Soit $x \in \mathbf{K}$. On a

$$\phi_p^{k+1}(x) = \phi_p^k(\phi_p(x)) = x^{pp^k} = x^{p^{k+1}},$$

par hypothèse de récurrence, ce qui démontre le résultat.

4. Par définition, $\mathbf{L}$ est l'ensemble des racines de $X^q - X$ dans $\mathbf{K}$. Comme $\mathbf{K}$ est un corps, cet ensemble est de cardinal au plus q.

5. Le polynôme $X^q - X$ est scindé dans $\mathbf{K}[X]$ car $\mathbf{K}$ est algébriquement clos, et $X^q - X$ est à racines simples dans $\mathbf{K}$ car il est premier avec son polynôme dérivé $qX^{q-1} - 1 = -1$ car $p|q$ et $\mathbf{K}$ est de caractéristique p. Ainsi, $X^q - X$ a q racines distinctes dans $\mathbf{K}$, donc $\mathbf{L}$ a q éléments.

6. D'une part, $\mathbf{L}$ est bien un sous-corps de $\mathbf{K}$: il contient 0 et 1, et si $x, y \in \mathbf{L}$, alors $\phi_q(x + y) = x + y$ et $\phi_q(xy) = xy$ (et en particulier, si $x \in \mathcal{L}$ est non nul, alors $x^{-1} \in \mathcal{L}$).
D'autre part, si $\mathbf{F}$ est un sous-corps de $\mathbf{K}$ de cardinal q, alors son groupe multiplicatif $\mathbf{F}^\times$ est d'ordre $q - 1$ donc tout élément non nul de $\mathbf{F}$ vérifie $x^{q-1} = 1$ (théorème de Lagrange). Ainsi, pour tout $x \in \mathbf{F}$, on a $x^q = x$, donc $x \in \mathcal{L}$. Tout sous-corps de $\mathbf{K}$ de cardinal q est donc contenu dans $\mathcal{L}$, et est donc égal à $\mathcal{L}$, ce qui montre l'unicité.

7. Soit $x \in \mathbf{F}_{q^2}$, on a $\phi_q^2(x) = x$. Ainsi, $\phi_q^2(\phi_q(x)) = \phi_q(x)$, donc $\phi_q(x) \in \mathbf{F}_{q^2}$. On a donc bien $\phi_q(\mathbf{F}_{q^2}) \subset \mathbf{F}_{q^2}$.
Par ailleurs, on a par définition $\mathbf{F}_q \subset \mathbf{F}_{q^2}$, donc :

$$\mathbf{F}_q = \mathbf{F}_q^2 \cap \mathbf{F}_q = \mathbf{F}_{q^2} \cap \{x \in \mathbf{K} \text{ tels que } \phi_q(x) = x\} = \{x \in \mathbf{F}_{q^2} \text{ tels que } \phi_q(x) = x\}$$

Exercice 4.

1.a) D'après le théorème de Lagrange, pour tout $x \in H$, $x^{p^\alpha} = I_n$.

1.b) Soit $x \in H$, alors comme l'élévation à la puissance p est un endomorphisme de la sous-algèbre commutative $\mathbf{F}_p[x]$ de $\mathcal{M}_n(\mathbf{F}_p)$ (en vertu de l'identité rappelée au début de l'exercice 3), on a $(x - I_n)^{p^\alpha} = x^{p^\alpha} - I_n = 0$. Donc $x \in \mathcal{U}_n(\mathbf{F}_p)$.

2.a) Soit $x \in \mathcal{U}_n(\mathbf{F}_p)$. Alors $(x - I_n)^n = 0$ d'après le théorème de Cayley-Hamilton. En particulier, si $p^\alpha \geq n$, alors $0 = (x - I_n)^{p^\alpha} = x^{p^\alpha} - I_n$. En particulier, le choix $\alpha = \lceil \ln_p(n) \rceil$ convient.

2.b) Soit ℓ un nombre premier divisant l'ordre de H. Alors, d'après le théorème de Cauchy, on dispose de $x \in H$ tel que x soit d'ordre ℓ. Par ailleurs, x^{p^α} donc $\ell | p^\alpha$. Ainsi, $\ell = p$ est le seul diviseur premier de l'ordre de H, et H est donc un p-groupe.

3.a) Soit $x \in G$. L'application $m_x : G \to G$ définie par $y \mapsto xy$ est une bijection car G est un groupe. L'application $G \to \mathfrak{S}_G$ définie par $x \mapsto m_x$ est injective (car $x = m_x(1_G)$), et son image est un isomorphisme de G sur un sous-groupe de $\mathfrak{S}_G$. Une bijection de $\{1, \ldots, r\}$ sur G (*i.e.* une numérotation des éléments de G par les entiers de 1 à r) induit une bijection de $\mathfrak{S}_r$ sur $\mathfrak{S}_G$, ce qui conclut.

3.b) Soit $\sigma \in \mathfrak{S}_r$. Soit $(e_1, \ldots, e_r)$ la base canonique de $\mathbf{F}_p^r$. Il existe un unique endomorphisme $f_\sigma : \mathbf{F}_p^r \to \mathbf{F}_p^r$ tel que pour tout $1 \leq i \leq r$, $f_\sigma(e_i) = e_{\sigma(i)}$. Pour $\sigma, \tau \in \mathfrak{S}_r$, on a $f_\sigma \circ f_\tau(e_i) = e_{\sigma\tau(i)}$, donc $f_{\sigma\tau} = f_\sigma \circ f_\tau$. Cela montre que $\sigma \mapsto f_\sigma$ est un morphisme de groupes $\mathfrak{S}_r \to GL_r(\mathbf{F}_p)$. Ce morphisme est injectif car si $f_\sigma = I_r$ alors $\sigma(i) = i$ pour tout $1 \leq i \leq r$, donc $\sigma = id$.
En composant avec le morphisme précédent, on obtient un morphisme injectif $G \to GL_r(\mathbf{F}_p)$, donc G est isomorphe à un sous-groupe de ce groupe linéaire.

4. Procédons par double implication :
$(i) \Rightarrow (ii)$. Soit G un p-groupe. D'après la question 3.b), il existe un entier $r \geq 1$ et un sous-groupe H de $GL_r(\mathbf{F}_p)$ tel que G soit isomorphe à H (on peut prendre $r = |G|$). D'après la question 1.b), $H \subset \mathcal{U}_r(\mathbf{F}_p)$.
$(ii) \Rightarrow (i)$. Soit G tel que G soit isomorphe à un sous-groupe H de $GL_r(\mathbf{F}_p)$ contenu dans $\mathcal{U}_r(\mathbf{F}_p)$. D'après la question 2.b), H est un p-groupe, donc G est un p-groupe.

Problème

Partie I.

1. On a $h(x,y,z)h(-x,-y,-z+xy) = h(0,0,0) = I_3$, donc $h(x,y,z)$ est inversible d'inverse $h(-x,-y,-z+xy)$.

2.a) On procède par récurrence sur n. Si $n=1$, le résultat est clair. Supposons que la formule soit valable un entier $n \in \mathbf{N}$, alors :

$$\begin{aligned} h(x,y,z)^{n+1} &= h(x,y,z)h\left(nx, ny, nz + \frac{n(n-1)2}{xy}\right) \\ &= h\left(nx+x, ny+y, nz+z+\frac{n(n-1)}{2}xy + nxy\right) \\ &= h\left((n+1)x, (n+1)y, (n+1)z + \frac{n(n+1)}{2}xy\right), \end{aligned}$$

ce qui est le résultat attendu, et démontre le résultat par principe de récurrence.

2.b) D'après 2.a), on a $h(x,y,z)^p = h(0,0,0) = I_3$, donc l'ordre de $h(x,y,z)$ divise p. Cet ordre est donc 1 ou p.

2.c)(i) On a $h(x,y,z)^4 = h(0,0,0) = I_3$, donc les ordres possibles pour les éléments $\mathcal{H}_3(\mathbf{F})$ sont $1, 2$ et 4.

2.c)(ii) Supposons $\mathbf{F}$ fini de cardinal q. Alors $h(x,y,z)$ est d'ordre 2 si et seulement si $h(x,y,z) \neq 1$, et $1 = h(x,y,z)^2 = h(0,0,xy)$. Ainsi, $h(x,y,z)$ est d'ordre 2 si et seulement si $x=0$ ou $y=0$, et $(x,y) \neq (0,0)$. Il y a donc exactement q^2-1 éléments d'ordre 2 dans $\mathcal{H}_3(\mathbf{F})$.

3. On a $h(x,y,z)^{-1} = h(-x,-y,-z+xy)$, donc par définition du commutateur, si on pose $H = h(x,y,z)$ et $H' = h(x',y',z')$:

$$\begin{aligned} [H,H'] &= h(x,y,z)h(x',y',z')h(-x,-y,-z+xy)h(-x',-y',-z'+x'y') \\ &= h(x+x', y+y', z+z'+xy')h(-x-x', -y-y', -z-z'+xy+x'y'+xy') \\ &= h(0,0,xy+x'y'+2xy'-(x+x')(y+y')) \\ &= h(0,0,xy'-x'y). \end{aligned}$$

4. Soit $h_0 = h(x,y,z) \in Z(\mathcal{H}_3(\mathbf{F}))$. Pour tout $(x',y') \in \mathbf{F}^2$, on a $[h_0, h(x,y,0)] = 0$ donc $xy' = yx'$. En particulier, pour $x'=1$ et $y'=0$, on obtient $x=0$. De même, $x'=0$ et $y'=1$ donne $y=0$. Réciproquement, tout élément de la forme $h(0,0,z)$ est dans $Z(\mathcal{H}_3(\mathbf{F}))$.

De manière analogue, comme $(x,y,x',y') \mapsto xy'-x'y$ est surjective, les commutateurs sont exactement les éléments de la forme $h(0,0,z)$, et comme cet ensemble est un sous-groupe, on a $D(\mathcal{H}_3(\mathbf{F})) = \{h(0,0,z), z \in \mathbf{F}\}$.

5. Vu la formule pour le produit dans $\mathcal{H}_3(\mathbf{F})$, cette application est un morphisme de groupes, qui est manifestement surjectif. Son noyau est $\{h(0,0,z), z \in \mathbf{F}\}$. Ainsi, ce morphisme induit un isomorphisme $\mathrm{Ab}(\mathcal{H}_3(\mathbf{F})) \to \mathbf{F}^2$.

6.a) Soient $x,y,x',y' \in \mathbf{F}$. On a

$$(\psi_1 \otimes \psi_2)\begin{pmatrix} x+x' \\ y+y' \end{pmatrix} = \psi_1(x)\psi_1(x')\psi_2(y)\psi_2(y') = (\psi_1 \otimes \psi_2)\begin{pmatrix} x \\ y \end{pmatrix}(\psi_1 \otimes \psi_2)\begin{pmatrix} x' \\ y' \end{pmatrix}.$$

Comme $\psi_1 \otimes \psi_2(0) = 1$, l'application $\psi_1 \otimes \psi_2$ est bien un morphisme de groupes.

6.b) L'application j est bien définie d'après la question précédente. Un calcul analogue montre aussi que j est un morphisme de groupes. Si $\psi_1 \otimes \psi_2 = 1$, alors pour tout $x \in \mathbf{F}$, $\psi_1(x)\psi_2(0) = 1$, donc $\psi_1 = 1$. De même, $\psi_2 = 1$, donc j est injectif. Enfin, soit $\psi \in \widehat{\mathbf{F}^2}$. Posons $\psi_1 = \psi(\cdot, 0)$ et $\psi_2 = \psi(0, \cdot)$. Comme ψ est un morphisme, on a pour tout $(x, y) \in \mathbf{F}^2$, $\psi(x, y) = \psi_1(x)\psi_2(y)$, donc j est surjectif.

7. On note π la surjection canonique $\mathcal{H}_3(\mathbf{F}) \to \mathrm{Ab}(\mathcal{H}_3(\mathbf{F}))$. On considère l'application $\pi^* : \widehat{\mathrm{Ab}(\mathcal{H}_3(\mathbf{F}))} \to \widehat{\mathcal{H}_3(\mathbf{F})}$ définie par $\pi^*(f) = f \circ \pi$. L'application π^* est bien définie, et c'est un morphisme de groupes comme composée de morphisme de groupes. Elle est injective car π est surjectif. Enfin, soit $f \in \widehat{\mathcal{H}_3(\mathbf{F})}$. Comme f est à valeurs dans le groupe abélien $\mathbf{C}^\times$, f s'annule sur $D(\mathcal{H}_3(\mathbf{F}))$. Par propriété universelle du quotient, il existe un morphisme de groupes $\bar{f} \in \widehat{\mathrm{Ab}(\mathcal{H}_3(\mathbf{F}))}$ tel que $f = \bar{f} \circ \pi = \pi^*(\bar{f})$. Donc π^* est surjectif : c'est un isomorphisme $\widehat{\mathrm{Ab}(\mathcal{H}_3(\mathbf{F}))} \to \widehat{\mathcal{H}_3(\mathbf{F})}$.
Par composition des applications précédentes, on dispose donc de l'isomorphisme $\Phi : \widehat{\mathcal{H}_3(\mathbf{F})} \to \widehat{\mathbf{F}}^2$, défini explicitement par :

$$\Phi(f)(x, y) = (f(h(x, 0, 0)), f(h(0, y, 0))).$$

L'isomorphisme réciproque est $\Psi : \widehat{\mathbf{F}}^2 \to \widehat{\mathcal{H}_3(\mathbf{F})}$ défini par :

$$\Psi((\phi_1, \phi_2))(h(x, y, z)) = \phi_1(x)\phi_2(y).$$

8. Soit $\sigma \in \widehat{\mathbf{F}_p}$. Alors $\sigma(1)^p = \sigma(0) = 1$, donc $\sigma(1)$ est une racine p-ème de l'unité, *i.e.* une racine de $X^p - 1 \in \mathbf{C}[X]$. Réciproquement, si ω est l'une des p racines de ce polynôme, l'unique morphisme de groupes $\mathbf{Z} \to \mathbf{C}^\times$ tel que $1 \mapsto \omega$ se factorise en un morphisme de groupes $\sigma : \mathbf{Z}/p\mathbf{Z} \to \mathbf{C}^\times$ tel que $\sigma(1) = \omega$. Cela montre que $\sigma \mapsto \sigma(1)$ est un isomorphisme de groupes $\widehat{\mathbf{F}_p} \to \mu_p$ où μ_p désigne le groupe des racines p-èmes de l'unité dans $\mathbf{C}$. Le choix d'une racine primitive p-ème, par exemple $\omega = e^{\frac{2i\pi}{p}}$, définit un isomorphisme $\mathbf{Z}/p\mathbf{Z} \to \mu_p$ *via* l'application $k \mapsto \omega^k$ (bien défini par passage au quotient). Ainsi, $\mathbf{F}_p \simeq \mu_p \simeq \widehat{\mathbf{F}_p}$.

9. Le corps $\mathbf{F}_{p^k}$ est un espace vectoriel de dimension finie sur $\mathbf{F}_p$. En tant qu'espace vectoriel, et donc en tant que groupe, il est isomorphe à $\mathbf{F}_p^{\dim_{\mathbf{F}_p}(\mathbf{F}_{p^k})}$. En comparant les cardinaux, on a nécessairement $\dim_{\mathbf{F}_p}(\mathbf{F}_{p^k}) = k$. On a donc $\mathbf{F}_{p^k} \simeq \mathbf{F}_p^k$.

10. D'après la question 9., on a $\widehat{\mathbf{F}_{p^k}} \simeq \widehat{\mathbf{F}_p^k}$. L'argument de la question 6., généralisé par récurrence en définissant $\phi_1 \otimes \cdots \otimes \phi_k$, montre que $\widehat{\mathbf{F}_p^k} \simeq \left(\widehat{\mathbf{F}_p}\right)^k$. D'après la question 8., on a $\widehat{\mathbf{F}_p} \simeq \mathbf{F}_p$. Ainsi, on a déjà établi l'existence d'un isomorphisme $\widehat{\mathbf{F}_{p^k}} \simeq \mathbf{F}_p^k$. D'après la question 7., $\widehat{\mathcal{H}_3(\mathbf{F}_q)} \simeq \widehat{\mathbf{F}_q}^2$, et en vertu de l'isomorphisme précédent, on en déduit qu'il existe un isomorphisme $\widehat{\mathcal{H}_3(\mathbf{F}_{p^k})} \simeq \mathbf{F}_p^{2k}$. En particulier, le groupe $\widehat{\mathcal{H}_3(\mathbf{F}_q)}$ est d'ordre q^2.

Partie II.

11. On a $\sigma(1_G) = 1_G$ donc $1_G \in G^+$. Soient $g, h \in G^+$, alors $\sigma(gh^{-1}) = \sigma(g)\sigma(h)^{-1} = gh^{-1}$ donc $gh^{-1} \in G^+$. Donc G^+ est un sous-groupe de G.

12.a) Comme $|G|$ est impair, $m = \frac{|G|+1}{2}$ est un entier. Soit $y = x^m$, alors $y^2 = x^{2m} = x^{|G|+1}$. D'après le théorème de Lagange, $x^{|G|} = 1_G$, donc $y^2 = x$.

12.b) D'après la question précédente, Φ est surjectif. Comme G est fini, Φ est injectif, donc bijectif.

13. Par injectivité de Φ, l'argument de cardinalité précédent montre qu'il suffit de vérifier que G^+ et G^- sont stables par Φ. Notons par ailleurs que pour tout $g \in G$,

$$\sigma(\Phi(g)) = \sigma(g^2) = \sigma(g)^2 = \Phi(\sigma(g)).$$

Ainsi, si $g \in G^+$, on a $\sigma(\Phi(g)) = \Phi(g)$, et si $g \in G^-$, $\sigma(\Phi(g)) = \Phi(g^{-1}) = \Phi(g)^{-1}$. Cela montre que G^+ et G^- sont stables par Φ et donc que Φ induit bien les deux bijections annoncées.

14. Pour démontrer la bijectivité de m, il suffit d'exhiber une application $s : G \to G^- \times G^+$ telle que $m \circ s = id_G$ et $s \circ m = id_{G^- \times G^+}$ (un tel est est alors unique, et c'est la bijection réciproque de m). Pour construire une telle application, raisonnons par analyse-synthèse.

Analyse. Soit $x \in G$, supposons que x s'écrive $x = x^- x^+$ avec $x^- \in G^-$ et $x^+ \in G^+$. Alors, par définition de G^- et G^+, on a $\sigma(x) = (x^-)^{-1}x^+$, donc

$$x\sigma(x)^{-1} = x^- x^+ (x^+)^{-1} x^- = (x^-)^2.$$

Ainsi, si on a une telle écriture, on a nécessairement $x^- = \Phi^{-1}(x\sigma(x)^{-1})$, et $x^+ = (x^-)^{-1}x$.

Synthèse. Soit $x \in G$. On a $\sigma(x\sigma(x)^{-1}) = \sigma(x)\sigma^2(x^{-1}) = \sigma(x)x^{-1}$ car σ est une involution. En particulier, $x\sigma(x)^{-1} \in G^-$. D'après la question 13., $\Phi^{-1}(x\sigma(x)^{-1}) \in G^-$: notons x^- cet élément de G^-. Soit $x^+ = (x^-)^{-1}x$, on a $\sigma(x^+) = \sigma(x^-)^{-1}\sigma(x) = x^-\sigma(x)$. Par définition de x^-, on a $(x^-)^2 = x\sigma(x)^{-1}$, donc $x^-(x^-\sigma(x)) = x$. On en déduit que $\sigma(x^+) = (x^-)^{-1}x = x^+$. On a donc $x^+ \in G^+$.

Ainsi, l'application $s : G \to G^- \times G^+$ définie par $s(x) = (x^-, x^+)$ (où x^-, x^+ sont donnés par les formules précédentes) vérifie clairement $m \circ s = id_G$, et on a aussi $s(m(x^+, x^-)) = (x^+, x^-)$ d'après l'étape d'analyse. On a montré la bijectivité de m.

15. Notons que l'application τ vérifie, pour tout $g, h \in G$, $\tau(gh) = \tau(h)\tau(g)$. Par ailleurs, si $x \in G^+$, alors $\tau(x) = x^{-1} \in G^+$. Ainsi, si $g \in G$ et $x, y \in G^+$, on a $\tau(xgy) = \tau(y)\tau(g)\tau(x) \in G^+\tau(g)G^+$. Cela montre que $\tau(G^+gG^+) \subset G^+\tau(g)G^+$. Comme τ est une involution, le même argument appliqué à $\tau = \tau^{-1}$ donne $\tau(G^+gG^+) \subset G^+\tau(g)G^+$.

Il reste à montrer que $\tau(g) \in G^+gG^+$. Pour cela, écrivons $(g^-, g^+) = m^{-1}(g)$ (où m est la bijection de la question 14.). On a alors $g = g^-g^+$, et $\tau(g) = \tau(g^+)\tau(g^-) = (g^+)^{-1}g^-$. En particulier, $\tau(g) = (g^+)^{-1}gg^+$, donc $\tau(g) \in G^+gG^+ = G^+$, d'où $G^+\tau(g)G^+ = G^+gG^+$.

Partie III.

16. Soit $(a,b) \in G^2$. Soit $g \in G$. On a

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

Dans le membre de droite, le terme $\delta_a(x)\delta_b(x^{-1}g)$ est nul sauf si $x = a$ et $x^{-1}g = b$, auquel cas ce terme vaut 1. Ainsi, $\delta_a * \delta_b$ s'annule en g si $g \neq ab$, et vaut 1 en ab : c'est donc δ_{ab}.

17. D'après la question 16., on a pour tout $a \in G$, $\delta_e * \delta_a = \delta_a$. Par linéarité de $f \mapsto f * \cdot$, et du fait que la famille $(\delta_a)_{a \in G}$ est une base de $\mathbf{C}[G]$, on a $\delta_e * f' = f'$ pour tout $f' \in \mathbf{C}[G]$: δ_e est bien l'élément neutre de $(\mathbf{C}[G], *)$.

18. Il est clair que $\tilde{\pi}$ est bien défini et linéaire en f. Il s'agit donc de justifier que

1. $\tilde{\pi}(\delta_e) = Id_V$,
2. pour tous $f, f' \in \mathbf{C}[G]$,, $\tilde{\pi}(f * f') = \tilde{\pi}(f)\tilde{\pi}(f')$.

Pour le premier point, on a bien :

$$\tilde{\pi}(\delta_e) = \sum_{g \in G} \delta_e(g)\pi(g) = \pi(e) = Id_V.$$

Pour le deuxième point, on a bien :

$$\begin{aligned}
\tilde{\pi}(f * f') &= \sum_{g \in G} \sum_{x \in G} f(x) f'(x^{-1}g)\pi(g) && \text{(par définition)} \\
&= \sum_{g \in G} \sum_{x \in G} f(x) f'(x^{-1}g)\pi(x)\pi(x^{-1}g) && (\pi \text{ est un morphisme}) \\
&= \sum_{x \in G} f(x)g(x) \left(\sum_{g \in G} f'(x^{-1}g)\pi(x^{-1}g) \right) && \text{(interversion de sommes finies)} \\
&= \sum_{x \in G} f(x)g(x)\tilde{\pi}(f') && (g \leftarrow x^{-1}g) \\
&= \tilde{\pi}(f)\tilde{\pi}(f').
\end{aligned}$$

Partie IV.

19. Supposons (π', V') et (π, V) isomorphes. soit $\varphi : V' \to V$ un isomorphisme de représentations. Montrons que φ induit une bijection $(V')^{G^+} \to V^{G^+}$. Soit $x' \in V'$ tel que pour tout $g \in G^+$, $\pi'(g)(x') = x'$. On a alors $\varphi(x') = \varphi(\pi(g)(x')) = \pi(g)(\varphi(x'))$ car φ est un morphisme de représentations. Donc $\varphi\left((V')^{G^+}\right) \subset V^{G^+}$. Le même raisonnement appliqué à φ^{-1} montre que $\varphi\left((V')^{G^+}\right) = V^{G^+}$. En particulier, comme φ est un isomorphisme, on a bien l'égalité des dimensions attendue.

20. Soient $f, f' \in \mathbf{C}[G]$, et soit $g \in G$. Vu la formule définissant $*$, on a :

$$\begin{aligned}\tilde{\tau}(f * f')(g) &= f * f' \circ \tau(g) \\ &= \sum_{x \in G} f(\tau(x)) f'(\tau(x^{-1}g)) \\ &= \sum_{y \in G} f(y^{-1}g) f'(g) \qquad\qquad (y \leftarrow \tau(g)\sigma(x)),\end{aligned}$$

où le dernier changement d'indice est légitime car $x \mapsto \tau(g)\sigma(x) = \tau(x^{-1}g)$ est bijectif, d'inverse $y \mapsto \tau(g)\sigma(y) = x$, d'où $\tau(x) = y^{-1}g$. On a donc bien $\tilde{\tau}(f * f') = \tilde{\tau}(f) * \tilde{\tau}(f')$.

21. Notons que si $f \in \mathbf{C}[G^+\backslash G/G^+]$, alors pour tous $g, z \in G$ et pour tous $x, y \in G^+$, on a $f(z) = f(x^{-1}z)$ et $f(z^{-1}xgy) = f(z^{-1}xg)$. Par suite, la formule définissant l'opération $*$ montre que pour tous $f, f' \in \mathbf{C}[G^+\backslash G/G^+]$, $g \in G$ et $x, y \in G^+$, on a :

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

Le changement d'indice $z \leftarrow zx^{-1}$ donne alors $(f * f')(xgy) = (f * f')(g)$, donc $\mathbf{C}[G^+\backslash G/G^+]$ est stable par $*$.

22. D'après la question 15., pour tout $g \in G$, on dispose de $x, y \in G^+$ tels que $\tau(g) = xgy$. Ainsi, si $f \in \mathbf{C}[G^+ \setminus G/G^+]$, on a pour tout $g \in G$: $f(g) = f(\tau(g))$. En particulier, pour tout $f \in \mathbf{C}[G^+\backslash G/G^+]$, $\tilde{\tau}(f) = f$.

23. Soient $f, f' \in \mathbf{C}[G^+\backslash G/G^+]$. D'après la question 21., $f' * f \in \mathbf{C}[G^+\backslash G/G^+]$, donc d'après les questions 22. et 20., $f' * f = \tilde{\tau}(f' * f) = \tilde{\tau}(f) * \tilde{\tau}(f') = f * f'$. Les éléments de $\mathbf{C}[G^+\backslash G/G^+]$ commutent donc pour la loi $*$.
L'image de la sous-algèbre commutative $\mathbf{C}[G^+\backslash G/G^+]$ par le morphisme d'algèbre $\tilde{\pi}$ est donc une sous-algèbre commutative de $\mathrm{End}_{\mathbf{C}}(V)$.

24. Soit $f \in \mathbf{C}[G^+\backslash G/G^+]$. Soit $v \in V^{G^+}$. On a $\tilde{\pi}(f)(v) = \sum_{g \in G} f(g)\pi(g)(v)$. Ainsi, si $x \in G^+$, on a :

$$\tilde{\pi}(f)(\pi(x)v) = \sum_{g \in G} f(g)\pi(gx)(v) = \sum_{g \in G} f(gx^{-1})\pi(g)(v),$$

et comme $f \in \mathbf{C}[G^+\backslash G/G^+]$ on a pour tout $g \in G$, $f(gx^{-1}) = f(g)$. Ainsi, $\tilde{\pi}(f)(\pi(x)v) = \tilde{\pi}(f)(v)$, donc V^{G^+} est stable par $\tilde{\pi}(f)$.

25. Soit $u' \in F$ et soit $x \in \ker(u - \lambda Id_{V^{G^+}}$. Alors, puisque u et u' commutent, on a $u(u'(x)) = u'(u(x)) = \lambda v(x)$, donc $u'(x) \in \ker(u - \lambda Id_{V^{G^+}})$. Ce sous-espace est donc bien stable par tous les éléments de F.

26. Soit $v \in V\backslash\{0\}$. Soit $W = \text{Vect}\{\pi(g)(v),\ g \in G\}$. Comme la famille $\{\pi(g)(v),\ g \in G\}$ est stable par chaque $\pi(g)$, le sous-espace vectoriel l'est aussi : c'est une sous-représentation de (π, V). Comme $v \in W$, on a $W \neq \{0\}$. Ainsi, V étant irréductible, on a $W = V$. Par conséquent, pour tout $w \in V$, il existe une application $f : G \to \mathbf{C}$ telle que $w = \sum_{g\in G} f(g)\pi(g)(v)$. Autrement dit, il existe $f \in \mathbf{C}[G]$ telle que $\tilde{\pi}(f)(v) = w$.

27. Soit $v \in V^{G^+} \setminus \{0\}$. Soit $w \in V^{G^+}$. D'après la question précédente, on dispose de $f \in \mathbf{C}[G]$ telle que $\tilde{\pi}(f)(v) = w$. On a alors pour tous $x, y \in G$,

$$\sum_{g\in G} f(xgy)\pi(g) = \pi(x)^{-1}\left(\sum_{g\in G} f(g)\pi(g)\right)\pi(y)^{-1}.$$

En particulier, si $x, y \in G^+$, on a $\sum_{g\in G} f(xgy)\pi(g)(v) = w$ car $v, w \in V^{G^+}$. Ainsi, en posant $\bar{f}(g) = \frac{1}{|G^+|^2}\sum_{(x,y)\in(G^+)^2} f(xgy)$, on a d'une part $\bar{f} \in \mathbf{C}[G^+\backslash G/G^+]$ (par changement d'indice) et d'autre part $\tilde{\pi}(\bar{f})(v) = w$.

28. Soit $u \in F$ et soit $\lambda \in \mathbf{C}$ une valeur propre de u. Soit $V_\lambda = \ker(u - \lambda Id_{V^{G^+}})$. Par définition, $V_\lambda \neq \{0\}$. Soit $x \in V_\lambda\backslash\{0\}$, d'après la question 25. on a pour tout $u' \in F$, $u'(x) \in F$. D'après la question 27., pour tout $w \in V^{G^+}$, on dispose de $u' \in F$ tel que $u'(x) = w$. Ainsi, $V^{G^+} = V_\lambda$, et $u = \lambda Id_{V^{G^+}}$. Ceci vaut pour tout $u \in F$, donc tous les éléments de F sont des homothéties.
Mais alors, en utilisant à nouveau le résultat de la question 27., on voit que pour tout $x \in V^{G^+} \setminus \{0\}$ et pour tout $w \in V^{G^+}$, il existe $\lambda \in \mathbf{C}$ tel que $w = \lambda x$. On a donc $\dim V^{G^+} = 1$.

Partie V.

29. Soit (V, π) une représentation de dimension 1 de $\mathcal{H}_3(\mathbf{F}_q)$. Le choix d'une base de V fixe un isomorphisme $GL(V) \simeq GL_1(\mathbf{C}) \simeq \mathbf{C}^\times$, et l'application $\mathcal{H}_3(\mathbf{F}_q) \to \mathbf{C}^\times$ qui en découle détermine (V, π) à isomorphisme près. Ainsi, les classes d'isomorphisme de représentations de dimension 1 de $\mathcal{H}_3(\mathbf{F}_q)$ sont en bijection avec les morphismes de groupes $\mathcal{H}_3(\mathbf{F}_q) \to \mathbf{C}^\times$, c'est-à-dire avec $\widehat{\mathcal{H}_3(\mathbf{F}_q)}$). D'après la question 10., il y en a q^2.

30. L'application ρ_ψ est à valeurs dans $\mathrm{End}_{\mathbf{C}}(\mathbf{C}[\mathbf{F}_q])$. Soit $f \in \mathbf{C}[\mathbf{F}_q]$ et $x \in \mathbf{F}_q$.
On a $\rho_\psi(I_3)f(x) = \rho_\psi(h(0,0,0))f(x) = f(x)$, donc $\rho_\psi(I_3) = Id_{\mathbf{C}[\mathbf{F}_q]}$.
Soient $H_0 = h(x_0, y_0, z_0)$ et $H_1 = h(x_1, y_1, z_1) \in \mathcal{H}_3(\mathbf{F}_q)$. On a d'une part, par composition :

$$\rho_\psi(H_0)\rho_\psi(H_1)f(x) = \psi(z_0 + xy_0)\psi(z_1 + (x + x_0)y_1)f(x + x_0 + x_1),$$

et d'autre part, vu la formule pour H_0H_1 :

$$\rho_\psi(H_0H_1)f(x) = \psi(z_0 + z_1 + x_0y_1 + x(y_0 + y_1))f(x + x_0 + x_1).$$

Comme ψ est un morphisme de groupes, on a bien $\rho_\psi(H_0)\rho_\psi(H_1) = \rho_\psi(H_0H_1)$.
Les deux points précédents montrent que ρ_ψ est à valeurs dans $GL(\mathbf{C}[\mathbf{F}_q])$, et que c'est un morphisme de groupes. Autrement dit, $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$ est une représentation de $\mathcal{H}_3(\mathbf{F}_q)$.

31. Soit $x \in \mathbf{F}_q$. Si $x = 0$, alors $\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(xy) = 1q\sum_{y\in\mathbf{F}_q} \psi(0) = 1$.
Soit $x \neq 0$, alors l'application $y \mapsto xy$ est bijective, donc $\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(xy) = \frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(y)$.
Comme ψ n'est pas constant, on dispose de $z \in \mathbf{F}_q$ tel que $\psi(z) \neq 1$. L'application $y \mapsto z + y$ est aussi bijective, donc

$$\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(y) = \frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(z + y) = \psi(z)\left(\frac{1}{q}\sum y \in \mathbf{F}_q\psi(y)\right).$$

Comme $\psi(z) \neq 1$, on a $\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(y) = 0$.
On a donc bien, pour tout $x \in \mathbf{F}_q$, $\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(xy) = \delta_0(x)$.

32. Soit $V \subset \mathbf{C}[\mathbf{F}_q]$ un sous-espace vectoriel. On suppose que V est stable par $\rho_\psi(\mathcal{H}_q(\mathbf{F}_q))$.
Soit $x_0 \in \mathbf{F}_q$. Soit $y \in \mathbf{F}_q$ et soit $H_y = h(x_0, y, 0)$. Soit $f \in \mathbf{C}[\mathbf{F}_q]$ et $x \in \mathbf{F}_q$, alors par définition de ρ_ψ, on a $\rho_\psi(H_y)f(x) = \psi(xy)f(x + x_0)$.
En particulier, si $f \in V$, alors pour tout $y \in \mathbf{F}_q$, l'application $x \mapsto \psi(xy)f(x + x_0)$ est dans V, et donc par linéarité, $x \mapsto \left(\frac{1}{q}\sum_{y\in\mathbf{F}_q} \psi(xy)\right) f(x + x_0) \in V$. D'après la question 31., V contient donc $x \mapsto \delta_0(x)f(x + x_0)$.
Supposons de plus que $f \in V \setminus \{0\}$ (qui est non vide par hypothèse), on dispose de $x_0 \in \mathbf{F}_q$ tel que $f(x_0) \neq 0$. En outre, l'application $x \mapsto \delta_0(x)f(x + x_0)f(x_0)^{-1} \in V$ prend la valeur 1 et 0, et 0 sur $\mathbf{F}_q \setminus \{0\}$: c'est donc δ_0, de sorte que $\delta_0 \in V$.

33. Soit $V \subset \mathbf{C}[\mathbf{F}_q]$ une sous-représentation de $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$. Supposons $V \neq \{0\}$. Pour montrer que $(\rho_\psi, \mathbf{C}[\mathbf{F}_q])$ est irréductible, il suffit de montrer que $V = \mathbf{C}[\mathbf{F}_q]$.
D'après la question précédente, $\delta_0 \in V$. Soit $x_0 \in \mathbf{F}_q$, et soit $x \in \mathbf{F}_q$, alors

$$\rho_\psi(h(-x_0, 0, 0))\delta_0(x) = \delta_0(x - x_0) = \delta_{x_0}(x),$$

on a donc $\delta_{x_0} \in V$ pour tout $x_0 \in \mathbf{F}_q$. Comme cette famille engendre $\mathbf{C}[\mathbf{F}_q]$, on a bien $V = \mathbf{C}[\mathbf{F}_q]$.

34. Considérons $\psi, \psi' \in \widehat{\mathbf{F}_q}$ distincts et non constants. Soit $z_0 \in \mathbf{F}_q$ tel que $\psi(z_0) \neq \psi'(z_0)$. Soit $f \in \mathbf{C}[\mathbf{F}_q]$. Par définition, on a $\rho_\psi(h(0,0,z_0))f = \psi(z_0)f$ donc $\rho_\psi(h(0,0,z_0)) = \psi(z_0)Id_{\mathbf{C}[G]}$. De même, $\rho_\psi(h(0,0,z_0)) = \psi(z_0)Id_{\mathbf{C}[G]}$. Ainsi, si $T \in \mathrm{End}(\mathbf{C}[G])$ induit un morphisme de représentations $(\rho_\psi, \mathbf{C}[G]) \to (\rho_{\psi'}, \mathbf{C}[G])$, on a pour tout $f \in \mathbf{C}[G]$, $T(\psi(z_0)f) = \psi'(z_0)T(f)$. Cela montre que $T = 0$, et en particulier, il n'existe pas d'isomorphisme de représentations $(\rho_\psi, \mathbf{C}[G]) \to (\rho_{\psi'}, \mathbf{C}[G])$.

35. Comme $\mathbf{F}_q$ indexe une base de $\mathbf{C}[\mathbf{F}_q]$ et est de cardinal q, cette représentation est de dimension q.

36. D'après les résultats de cette partie, on a q^2 représentations irréductibles de dimension 1 de $\mathcal{H}_3(\mathbf{F}_q)$ (deux à deux non isomorphes, indexées par $\widehat{\mathcal{H}_3(\mathbf{F}_q)}$), et $q-1$ représentations irréductibles de dimension q de $\mathcal{H}_3(\mathbf{F}_q)$ (deux à deux non isomorphes, indexées par les éléments non triviaux de $\widehat{\mathbf{F}_q}$). D'après un résultat classique de théorie des représentations, si $\mathcal{W}$ est une famille de représentants des classes d'isomorphisme des $\mathbf{C}$-représentations irréductibles d'un groupe fini G, on a $|G| = \sum_{W \in \mathcal{W}} (\dim W)^2$. En considérant les classes d'isomorphismes de représentations $\mathcal{W}_{\mathcal{H}_3(\mathbf{F}_q)}$ déjà identifiées pour $\mathcal{H}_3(\mathbf{F}_q)$, on obtient :

$$\sum_{W \in \mathcal{W}_{\mathcal{H}_3(\mathbf{F}_q)}} (\dim W)^2 = q^2 + (q-1)q^2 = q^3 = |\mathcal{H}_3(\mathbf{F}_q)|.$$

Nous avons donc déterminé toutes les classes d'isomorphisme de représentations irréductibles de $\mathcal{H}_3(\mathbf{F}_q)$.

Partie VI.

37. L'application σ est un morphisme de groupes car s est un morphisme de corps (et par définition du produit dans $\mathcal{H}_\ni(\mathbf{F}_{q^2})$). C'est une involution car s est une involution ($s^2 = \phi_q^2 = Id_{\mathbf{F}_{q^2}}$).

38. Soit $H = h(x, y, z) \in G$ tel que $\sigma(H) = H$. Alors $s(x) = x$, $s(y) = y$ et $s(z) = z$, c'est-à-dire d'après la question 7. de l'exercice 3. que $x, y, z \in \mathbf{F}_q$. Ainsi, $H \in \mathcal{H}_3(\mathbf{F}_q)$. Réciproquement, tous les éléments de $\mathcal{H}_3(\mathbf{F}_q)$ sont invariants par σ. Donc $G^+ = \mathcal{H}_3(\mathbf{F}_q)$.

39. Soit (π, V) une représentation distinguée de dimension 1 de G. Comme elle est distinguée, $V^{G^+} \neq \{0\}$, et comme V est de dimension 1, $V^{G^+} = V$. En particulier, les classes d'isomorphisme de représentations distinguées de dimension 1 de G sont en bijection avec éléments de $\widehat{G}$ dont la restriction à G^+ est triviale.
Soit $\phi \in \widehat{G}$. D'après la partie I, il existe un unique couple (ϕ_1, ϕ_2) d'éléments de $\widehat{\mathbf{F}_{q^2}}$, tels que $\phi(h(x, y, z)) = \phi_1(x)\phi_2(y)$. Un tel morphisme est trivial sur G^+ si et seulement si pour tout $x \in \mathbf{F}_q$, $\phi_1(x) = \phi_2(x) = 1$. Le groupe quotient $\mathbf{F}_{q^2}/\mathbf{F}_q$ étant isomorphe à $\mathbf{F}_q$, les éléments de $\widehat{G}$ dont la restriction à $\mathcal{H}_3(\mathbf{F}_q)$ est triviale sont en bijection avec $\widehat{\mathbf{F}_q}^2$.
Ainsi, les classes d'isomorphisme de représentation distinguées de G de dimension 1 sont en bijection avec $\mathbf{F}_q^2$, il y en a donc q^2.

40. Supposons $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$ distinguée. Alors, il existe $f \in \mathbf{C}[\mathbf{F}_{q^2}]$ non nulle telle que pour tout $(x_0, y_0, z_0) \in \mathbf{F}_q$, $\rho_\psi(h(x_0, y_0, z_0))f = f$. Le cas particulier $x_0 = y_0 = 0$ montre que pour tout $x \in \mathbf{F}_{q^2}$, $\psi(z_0)f(x) = f(x)$. Comme f est non nulle, on en déduit que $\psi(z_0) = 1$ pour tout $z_0 \in \mathbf{F}_q$.
Réciproquement, supposons que $\psi(x) = 1$ pour tout $x \in \mathbf{F}_q$. Soit $\mathbf{1}_{\mathbf{F}_q}$ la fonction indicatrice de $\mathbf{F}_q$, qui prend la valeur 1 sur les éléments de $\mathbf{F}_q$ et 0 sur les éléments de $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$. Soit $(x_0, y_0, z_0) \in \mathbf{F}_q^3$, et soit $x \in \mathbf{F}_{q^2}$. Alors

$$\rho_\psi(h(x_0, y_0, z_0))\mathbf{1}_{\mathbf{F}_q}(x) = \psi(z_0)\psi(y_0 x)\mathbf{1}_{\mathbf{F}_q}(x + x_0) = \begin{cases} 0 & \text{si } x \notin \mathbf{F}_q \\ \psi(y_0 x) = 1 & \text{si } x \in \mathbf{F}_q \end{cases}.$$

Ainsi, $\mathbf{1}_{\mathbf{F}_q} \in \mathbf{C}[F_{q^2}]^{G^+}$. La représentation $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$ est donc distinguée.

41. Soit $x \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$. La famille $\{1, x\}$ est libre sur $\mathbf{F}_q$ (sinon on aurait $x \in \mathbf{F}_q$). Comme $\mathbf{F}_{q^2}$ est un $\mathbf{F}_q$-espace vectoriel de dimension 2, cette famille est une base de $\mathbf{F}_{q^2}$.
Soit $z \in \mathbf{F}_{q^2}$ tel que $\psi(z) \neq 1$, on dispose de $y_0, z_0 \in \mathbf{F}_q$ tels que $z = z_0 + xy_0$. On a alors $\psi(z_0 + xy_0) \neq 1$ comme attendu.

42. Lorsque p est impair, $|\mathcal{H}_3(\mathbf{F}_{q^2})|$ est impair, donc les résultats de la partie IV montrent que $\dim(\mathbf{C}[F_{q^2}]^{G^+}) = 1$. La preuve qui suit montre le résultat sans hypothèse sur p.
La question 40. montre que G^+ agit trivialement sur $\mathrm{Vect}\{\mathbf{1}_{\mathbf{F}_q}\}$. Il suffit donc de montrer que pour tout $f \in \mathbf{C}[\mathbf{F}_{q^2}]$ en dehors de ce sous-espace, il existe $(x_0, y_0, z_0) \in \mathbf{F}_q^3$ tel que $\rho_\psi(h(x_0, y_0, z_0))f \neq f$.
Soit $f \in \mathbf{C}[\mathbf{F}_{q^2}] \setminus \mathrm{Vect}\{\mathbf{1}_{\mathbf{F}_q}\}$. Supposons d'abord qu'il existe $x_0, x_1 \in \mathbf{F}_q$ tels que $f(x_0) \neq f(x_1)$. Alors $\rho_\psi(h(x_1 - x_0, 0, 0))f(x_0) = f(x_1)$, donc $\rho_\psi(h(x_1 - x_0, 0, 0))f \neq f$.
On peut donc supposer qu'on dispose de $x \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ tel que $f(x) \neq 0$. Comme $\psi \neq 1$, d'après la question 41. on dispose de z_0, y_0 tels que $z_0 + y_0 xneq1$. On a alors :

$$\rho_\psi(h(0, y_0, z_0))f(x) = \psi(z_0 + y_0 x)f(x) \neq f(x).$$

Ainsi $\rho_\psi(h(0,y_0,z_0))f \neq f$, ce qui conclut la preuve du fait que $\dim(\mathbf{C}[\mathbf{F}_{q^2}]^{G^+}) = 1$.

43. On a $\mathbf{F}_q \subset \mathbf{F}_{q^2}$. Soit $x \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$, alors l'application $\pi : \mathbf{F}_{q^2} \to \mathbf{F}_q$ définie par $\pi(z_0 + y_0 x) = y_0$ induit un isomorphisme de groupes $\mathbf{F}_{q^2}/\mathbf{F}_q \simeq \mathbf{F}_q$. Fixons maintenant un tel isomorphisme, la propriété universelle du quotient donne alors un isomorphisme $\eta : \widehat{\mathbf{F}_{q^2}/\mathbf{F}_q} \simeq \widehat{\mathbf{F}_q}$. En particulier, les classes d'isomorphisme de représentations distinguées de dimension 1 de G sont en bijection avec les classes d'isomorphisme de représentations de dimension 1 de $\widehat{\mathbf{F}_q}$, c'est-à-dire les classes d'isomorphisme de représentations irréductibles de G^+ d'après la question 29.
D'autre part, les représentations irréductibles de dimension > 1 de G sont à isomorphisme près les $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}])$, et la question 40. montre qu'une telle représentation est distinguée si et seulement si la restriction de ψ à $\mathbf{F}_q$ est triviale, c'est-à-dire si et seulement si ψ se factorise en un morphisme $\bar{\psi} : \mathbf{F}_{q^2}/\mathbf{F}_q \to \mathbf{C}^\times$. En particulier, l'isomorphisme η fournit une bijection entre l'ensemble des (morphismes indexant les) classes d'isomorphisme de représentations irréductibles distinguées de dimension > 1 de G et l'ensemble des (morphismes indexant les) classes d'isomorphisme de représentations irréductibles de dimension > 1 de G^+. Concrètement, cette bijection est $(\rho_\psi, \mathbf{C}[\mathbf{F}_{q^2}]) \mapsto (\rho_{\psi\circ\eta}, \mathbf{C}[\mathbf{F}_q])$.