Première partie

Exercice 1

1. (a) C'est faux dès lors que la dimension de E est supérieure ou égale à 2. Voici un contre-exemple : soit

$$f : \left\{ \begin{array}{ccc} \mathbb{C}^2 & \longrightarrow & \mathbb{C}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \end{array} \right. .$$

Le polynôme caractéristique de f est X^2 et sa seule valeur propre est 0. Le noyau de f étant de dimension 1, f n'est pas diagonalisable.

(b) C'est faux. Considérons de nouveau l'endomorphisme f précédent. Comme $\mathbb{C}^2$ est de dimension 2, les sous-espaces stables par f sont :
— $\{(0,0)\}$.
— $\mathbb{C}^2$.
— Les sous-espaces stables par f de dimension 1, c'est-à-dire les droites vectorielles engendrées par un vecteur propre non nul. Il en existe donc un seul, noté E, engendré par $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Le sous-espace E ne possède donc aucun supplémentaire stable par f.

(c) C'est vrai. Soit $(e_1, \dots, e_n)$ une base de vecteurs propres de f. Pour tout i, soit $\lambda_i \in \mathbb{C}$ la valeur propre associée à e_i. Pour tout $i \in i \in [\![1, n]\!]$,

$$f^2(e_i) = f \circ f(e_i) = f(\lambda_i e_i) = \lambda_i f(e_i) = \lambda_i^2 e_i.$$

Donc e_i est un vecteur propre de f^2, de valeur propre λ_i^2. Ainsi, f^2 est diagonalisable.

(d) C'est faux. Reprenons une nouvelle fois l'endomorphisme f de la question 1 (a). Alors f^2 est l'endomorphisme nul de $\mathbb{R}^2$, donc est diagonalisable. Mais f n'est pas diagonalisable.

(e) C'est vrai. Choisissons une base $\mathcal{B}$ de E. La matrice de f dans la base $\mathcal{B}$ est notée $A = (a_{i,j})_{1 \leqslant i,j \leqslant n}$ et la matrice de g dans cette base est notée $B = (b_{i,j})_{1 \leqslant i,j \leqslant n}$. La matrice de $f \circ g$ dans la base $\mathcal{B}$ est $AB = (c_{i,j})_{1 \leqslant i,j \leqslant n}$, donc

$$\operatorname{Tr}(f \circ g) = \operatorname{Tr}(AB) = \sum_{i=1}^{n} c_{i,i} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} b_{j,i}.$$

De même, la matrice de $g \circ f$ dans la base $\mathcal{B}$ est $BA = (d_{i,j})_{1 \leqslant i,j \leqslant n}$, donc

$$\operatorname{Tr}(g \circ f) = \operatorname{Tr}(BA) = \sum_{i=1}^{n} d_{i,i} = \sum_{i=1}^{n} \sum_{j=1}^{n} b_{i,j} a_{j,i} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{j,i} b_{i,j} = \operatorname{Tr}(f \circ g).$$

Exercice 2

2. $(a) \Longrightarrow (b)$. Soit $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ les valeurs propres (distinctes) de f. On pose

$$P = (X - \lambda_1) \dots (X - \lambda_k).$$

Les racines de ce polynôme sont simples. Si $x \in \operatorname{Ker}(f - \lambda_i \mathrm{Id}_E)$, alors $f(x) = \lambda_i x$ et par suite,

$$P(f)(x) = (f - \lambda_1 \mathrm{Id}_E) \circ (f - \lambda_{i-1} \mathrm{Id}_E) \circ (f - \lambda_{i+1} \mathrm{Id}_E) \circ (f - \lambda_k \mathrm{Id}_E) \circ \underbrace{(f - \lambda_i \mathrm{Id}_E)(x)}_{=0_E} = 0_E.$$

 Tournez la page S.V.P.

Donc $P(f)$ s'annule sur $\mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$. Comme f est diagonalisable,

$$E = \bigoplus_{i=1}^{k} \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E),$$

donc $P(f)$ s'annule sur E. Autrement dit, P annule f.
$(b) \implies (c)$. Soit P un tel polynôme. Alors le polynôme minimal P_f divise P. Comme P est à racines simples, P_f également.
$(c) \implies (a)$. Soit P_f le polynôme minimal de f. On pose

$$P(f) = (X - \lambda_1) \dots (X - \lambda_k),$$

où les λ_i sont des nombres complexes deux-à-deux distincts. Les polynômes $X - \lambda_i$ étant deux-à-deux premiers entre eux, par le lemme des noyaux,

$$\mathrm{Ker}(P_f(f)) = E = \bigoplus_{i=1}^{k} \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E).$$

Donc f est diagonalisable.

3. Soit P_f le polynôme minimal de f. D'après la question (2), $(a) \implies (c)$, P_f est à racines simples. De plus, $P_f(f)$ est un endomorphisme nul, donc sa restriction à F également :

$$P_f(f)_{|F} = P_f(f_{|F}) = 0_{\mathrm{End}(F)}.$$

D'après la question 2, $(b) \implies (a)$, $f_{|F}$ est diagonalisable.

4. (a) Soit λ la valeur propre associée F. Soit $x \in F$ et soit $i \in [\![1, k-1]\!]$. Alors

$$f_k(f_i(x)) = f_k \circ f_i(x) = f_i \circ f_k(x) = f_i(\lambda x) = \lambda f_i(x),$$

donc $f_i(x)$ est un vecteur propre de f_k de valeur propre λ. Donc $f_i(x) \in F$: F est stable par f_i.

(b) Comme f_i est diagonalisable et que F est stable par f_i (question 4. (a)), d'après la question 3, la restriction de f_i à F est diagonalisable.

(c) On procède par récurrence sur k. Si $k = 1$, il n'y a rien à démontrer car f_1 est diagonalisable. Supposons le résultat vrai à un rang $k-1$, avec $k \geqslant 2$. Soient $F_1, \dots, F_n$ les espaces propres de f_k. On fixe $j \in [\![1, n]\!]$. D'après la question 4. (a), F_i est stable par $f_1, \dots, f_{k-1}$. On note f_i' la restriction de f_i à F_j. Comme $f_1, \dots, f_k$ commutent, $f_1', \dots, f_{k-1}'$ commutent également et sont diagonalisables d'après la question 4. (b). Par l'hypothèse de récurrence, F_j possède une base $\mathcal{B}_j$ de vecteurs propres communs à $f_1', \dots, f_{k-1}'$. Les vecteur de $\mathcal{B}_j$ sont donc des vecteurs propres de $f_1, \dots, f_{k-1}$ mais aussi de f_k, puisque F_j est un espace propre de f_k. Comme f_k est diagonalisable,

$$E = F_1 \oplus \dots \oplus F_n,$$

et la réunion des bases $\mathcal{B}_1, \dots, \mathcal{B}_n$ forme donc une base de E. On obtient ainsi une base de vecteurs propres communs à $f_1, \dots, f_k$.
Par le principe de récurrence, le résultat est donc vrai pour tout $k \geqslant 1$.

Exercice 3

5. Soit $N \in \mathbb{Z}$.

$$\begin{aligned}(g^d)^N = e_G &\iff g^{dN} = e_G \\ &\iff n \mid dN \\ &\iff \frac{n}{d} \mid N.\end{aligned}$$

Par définition de l'ordre de g^d, g^d est d'ordre $\dfrac{n}{d}$.

6. Soit $N \in \mathbb{Z}$. On pose $n' = \dfrac{n}{\mathrm{PGCD}(d,n)}$ et $d' = \dfrac{d}{\mathrm{PGCD}(d,n)}$. Alors d' et n' sont premiers entre eux.

$$\begin{aligned}
(g^d)^N = e_G &\iff g^{dN} = e_G \\
&\iff n \mid dN \\
&\iff n' \mid d'N \qquad \text{après simplification par le PGCD de } n \text{ et } d \\
&\iff n' \mid N \qquad \text{par le lemme de Gauss, } d' \text{ et } n' \text{ étant premiers entre eux.}
\end{aligned}$$

Par définition de l'ordre de g^d, g^d est d'ordre $n' = \dfrac{n}{\mathrm{PGCD}(d,n)}$.

7. (a) $\langle g\rangle \cap \langle h\rangle$ est un sous-groupe de $\langle g\rangle$, donc son ordre divise l'ordre de g, c'est-à-dire k. De même, il divise l et donc divise le PGCD de k et l, qui vaut 1. Par suite, $|\langle g\rangle \cap \langle h\rangle| = 1$ et $\langle g\rangle \cap \langle h\rangle = \{e_g\}$.

   (b) Soit N l'ordre de $g \cdot h$. Alors $(g \cdot h)^N = g^N \cdot h^N$ (le groupe étant abélien), ce qui donne $g^N = h^{-N} \in \langle g\rangle \cap \langle h\rangle = \{e_G\}$, d'après la question 7.(a). Par suite, $g^N = h^{-N} = e_G$, donc k divise N et l divise N, ce qui implique que $\mathrm{PPCM}(k,l)$ divise N. Comme k et l sont premiers entre eux, $\mathrm{PPCM}(k,l) = kl$, donc kl divise N.

   De plus $(g \cdot h)^{kl} = g^{kl} \cdot h^{kl} = e_G \cdot e_G = e_G$, donc N divise kl. On en conclut que $N = kl$.

8. On procède par récurrence sur n. Si $n = 1$, il n'y a rien à démontrer. Supposons le résultat vrai au rang $n-1$, avec $n \geqslant 2$. Par l'hypothèse de récurrence, $g_1 \cdot \ldots \cdot g_{n-1}$ est d'ordre $k_1 \ldots k_{n-1}$. Comme les k_i sont deux-à-deux premiers entre eux, $k_1 \ldots k_{n-1}$ et k_n sont premiers entre eux. D'après la question 7. (b), $g_1 \cdot \ldots \cdot g_n = (g_1 \cdot \ldots \cdot g_{n-1}) \cdot g_n$ est d'ordre $k_1 \ldots k_n$.

   Par le principe de récurrence, le résultat est vrai à tout rang $n \geqslant 1$.

9. (a) La puissance de p_i dans $\exp(G)$ est le maximum des puissances de p_i dans les décompositions en nombres premiers des ordres des éléments de G. Par suite, G possède un élément h_i dont la décomposition en nombres premiers de l'ordre N fait apparaître $p_i^{\alpha_i}$: autrement dit, $p_i^{\alpha_i}$ divise N. D'après la question 5, $g_i = h_i^{\frac{N}{p_i^{\alpha_i}}}$ est d'ordre $p_i^{\alpha_i}$.

   (b) D'après la question 8, les $p_i^{\alpha_i}$ étant deux-à-deux premiers entre eux, $g = g_1 \cdot \ldots \cdot g_n$ est d'ordre $p_1^{\alpha_1} \ldots p_n^{\alpha_n} = \exp(G)$.

Deuxième partie : définition et exemples

10. (a) i. Comme θ est un homomorphisme de groupes, $\theta(e_G) = e_{\mathrm{GL}(E)} = \mathrm{Id}_E$.

    ii. Comme θ est un homomorphisme de groupes, $\theta(g^{-1}) = \theta(g)^{-1}$.

    (b) Soient $k, l \in \mathbb{Z}$.
$$\theta_1(k+l) = f^{k+l} = f^k \circ f^l = \theta_1(k) \circ \theta_1(l).$$
    Donc θ_1 est un homomorphisme de groupes.

    (c) Montrons que θ_2 est bien défini. Soit $k, l \in \mathbb{Z}$ tels que $\overline{k} = \overline{l}$. Alors n divise $k - l$: posons $k - l = pn$, avec $p \in \mathbb{Z}$. Alors
$$f^k = f^{l+pn} = f^l \circ (f^n)^p = f^l \circ \mathrm{Id}_E^p = f^l.$$
    Par suite, θ_2 est bien défini. Soient $\overline{k}$ et $\overline{l}$ dans $\mathbb{Z}/n\mathbb{Z}$.
$$\theta_2(\overline{k} + \overline{l}) = \theta_2(\overline{k+l}) = f^{k+l} = f^k \circ f^l = \theta_2(\overline{k}) \circ \theta_2(\overline{l}).$$
    Donc θ_2 est bien un homomorphisme de groupes.

(d) Tout d'abord, observons que f_λ est bien un automorphisme de $\mathbb{C}^2$, sa matrice dans la base canonique étant $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$, clairement inversible. Soient $\lambda, \mu \in \mathbb{C}$. Pour tout $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2$,

$$f_\lambda \circ f_\mu \begin{pmatrix} x \\ y \end{pmatrix} = f_\lambda \begin{pmatrix} x+\lambda y \\ y \end{pmatrix} = \begin{pmatrix} x+\lambda y+\mu y \\ y \end{pmatrix} = \begin{pmatrix} x+(\lambda+\mu) y \\ y \end{pmatrix} = f_{\lambda+\mu} \begin{pmatrix} x \\ y \end{pmatrix},$$

donc $f_\lambda \circ f_\mu = f_{\lambda+\mu}$. Par suite, $\theta_3(\lambda+\mu) = \theta_3(\lambda) \circ \theta_3(\mu)$: θ_3 est un homomorphisme de groupes.

(e) Tout d'abord, pour tout $\sigma \in \mathfrak{S}_3$, $g_\sigma \in \mathrm{GL}(\mathbb{C}^3)$. Soient $\sigma, \tau \in \mathfrak{S}_3$. Pour tout $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{C}^3$,

$$g_\sigma \circ g_\tau \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = g_\sigma \begin{pmatrix} x_{\tau^{-1}(1)} \\ x_{\tau^{-1}(2)} \\ x_{\tau^{-1}(3)} \end{pmatrix} = \begin{pmatrix} x_{\tau^{-1}\circ\sigma^{-1}(1)} \\ x_{\tau^{-1}\circ\sigma^{-1}(2)} \\ x_{\tau^{-1}\circ\sigma^{-1}(3)} \end{pmatrix} = \begin{pmatrix} x_{(\sigma\circ\tau)^{-1}(1)} \\ x_{(\sigma\circ\tau)^{-1}(2)} \\ x_{(\sigma\circ\tau)^{-1}(3)} \end{pmatrix} = g_{\sigma\circ\tau} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix},$$

donc $g_\sigma \circ g_\tau = g_{\sigma\circ\tau}$. Par suite, θ_4 est un homomorphisme de groupes.

11. (a) On note $\theta(g)_{|F} : F \longrightarrow F$ l'endomorphisme de F induit par $\theta(g)$, pour tout $g \in G$. Comme $\theta(g)$ est un homomorphisme de groupes,

$$\theta(g)_{|F} \circ \theta(g^{-1})_{|F} = \theta(gg^{-1})_{|F} = \mathrm{Id}_{E|F} = \mathrm{Id}_F.$$

De même, $\theta(g^{-1})_{|F} \circ \theta(g)_{|F} = \mathrm{Id}_F$. Donc $\theta(g)_{|F}$ est un automorphisme de F, d'inverse $\theta(g^{-1})_{|F}$.

(b) On vient de montrer que $\theta_{|F}$ prend bien ses valeurs dans $\mathrm{GL}(F)$. Soient $g, h \in G$.

$$\theta_{|F}(g) \circ \theta_{|F}(h) = \theta(g)_{|F} \circ \theta(h)_{|F} = (\theta(g) \circ \theta(h))_{|F} = \theta(gh)_{|F} = \theta_{|F}(gh).$$

Donc $\theta_{|F}$ est bien un homomorphisme de groupes.

(c) L'endomorphisme f_1 a pour matrice dans la base canonique de $\mathbb{C}^2$ la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Le polynôme caractéristique de cette matrice est $(X-1)^2$, sa seule valeur propre est 1 et son seul espace propre est la droite $D = \mathrm{Vect}((1,0))$.

Soit F un sous-espace invariant de θ_3. Sa dimension est 0, 1 ou 2. Si c'est 0, alors $F = \{(0,0)\}$. Si c'est 2, alors $F = \mathbb{C}^2$. Si c'est 1, alors F est une droite stable par f_1, donc une droite de F engendrée par un vecteur propre de f_1 : il s'agit de D. Réciproquement, ces trois sous-espaces sont stables par tous les f_λ, lorsque λ parcourt $\mathbb{C}$. Donc les sous-espaces invariants de θ_3 sont $\{(0,0)\}$, $\mathbb{C}^2$ et D.

(d) i. Soit $(x_1, x_2, x_3) \in F$ et soit $\sigma \in \mathfrak{S}_3$. Alors

$$\theta_4(\sigma) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ x_{\sigma^{-1}(3)} \end{pmatrix} \in F,$$

car $x_{\sigma^{-1}(1)} + x_{\sigma^{-1}(2)} + x_{\sigma^{-1}(3)} = x_1 + x_2 + x_3 = 0$. Par suite, F est un sous-espace invariant de θ_4.

ii. Une base de F est donnée par $\mathcal{B} = \left(\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right)$. La matrice de $\theta_4(\sigma)$ dans cette base $\mathcal{B}$ est donnée dans le tableau suivant :

σ	$M_{\mathcal{B}}(\theta_4(\sigma))$
Id	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
(12)	$\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$
(23)	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
(123)	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$
(213)	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
(13)	$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$

iii. Le sous-espace F' de $\mathbb{C}^3$ engendré par le vecteur $(1,1,1)$ est clairement invariant par θ_4. De plus, comme $1+1+1 \neq 0$, $(1,1,1)$ n'appartient pas à F. Comme F' est de dimension 1, $F \cap F' = \{(0,0,0)\}$. Comme $\dim(F) + \dim(F') = 3 = \dim(C^3)$, $\mathbb{C}^3 = F \oplus F'$.

12. (a) Soit $x \in \mathrm{Ker}(f)$. Pour tout $g \in G$,

$$f(\theta(g)(x)) = f \circ \theta(g)(x) = \theta'(g) \circ f(x) = \theta'(g)(0_{E'}) = 0_{E'},$$

donc $\theta(g)(x) \in \mathrm{Ker}(f)$: $\mathrm{Ker}(f)$ est un sous-espace invariant de θ.

(b) Soit $y \in \mathrm{Im}(f)$. Alors il existe $x \in E$ tel que $y = f(x)$. Pour tout $g \in G$,

$$\theta'(g)(y) = \theta'(g)(f(x)) = \theta'(g) \circ f(x) = f \circ \theta(g)(x) = f(\theta(g)(x)) \in \mathrm{Im}(f),$$

donc $\mathrm{Im}(f)$ est un sous-espace invariant de θ'.

(c) Soit λ une valeur propre de f et soit F le sous-espace propre associé. Soit $x \in F$. Pour tout $g \in G$,

$$f(\theta(g))(x)) = f \circ \theta(g)(x) = \theta(g) \circ f(x) = \theta(g)(\lambda x) = \lambda\theta(g)(x),$$

donc $\theta(g)(x) \in F$: F est un sous-espace invariant de θ.

13. (a) i. Supposons f non nul. Alors $\mathrm{Ker}(f)$ est un sous-espace invariant de θ non égal à E. Comme θ est irréductible, ceci implique que $\mathrm{Ker}(f) = \{0_E\}$, donc f est injective. De plus, $\mathrm{Im}(f)$ est un sous-espace invariant de θ', non nul. Comme θ' est irréductible, ceci implique que $\mathrm{Im}(f) = F$, donc f est surjective. En conclusion, si f est non nul, alors f est un isomorphisme.

ii. Comme $\mathbb{C}$ est algébriquement clos, f possède au moins une valeur propre λ. L'espace propre associé F est alors un sous-espace invariant non nul de θ. Comme θ est irréductible, $F = E$ et donc $f = \lambda \mathrm{Id}_E$.

(b) i. Soit $g' \in G$.

$$\begin{aligned}
f \circ \theta(g') &= \frac{1}{|G|} \sum_{g \in G} \theta'(g) \circ h \circ \theta(g^{-1}) \circ \theta(g') \\
&= \frac{1}{|G|} \sum_{g \in G} \theta'(g) \circ h \circ \theta(g^{-1}g') \\
&= \frac{1}{|G|} \sum_{g'' \in G} \theta'(g'g'') \circ h \circ \theta(g''^{-1}) \\
&= \frac{1}{|G|} \sum_{g'' \in G} \theta'(g') \circ \theta(g'') \circ h \circ \theta(g''^{-1}) \\
&= \theta'(g') \circ \left(\frac{1}{|G|} \sum_{g'' \in G} \theta(g'') \circ h \circ \theta(g''^{-1}) \right) \\
&= \theta'(g') \circ f.
\end{aligned}$$

À la troisième ligne, on a effectué le changement d'indices $g'' = g'^{-1}g$, ce qui donne $g = g'g''$ et $g^{-1}g' = g''^{-1}$ Donc f est un homomorphisme de représentations de θ vers θ'.

ii. Si θ et θ' ne sont pas isomorphes, alors f ne peut pas être un isomorphisme. D'après la question 13 (a) i., $f = 0$.

iii. D'après la question 13. (a) ii, comme θ est irréductible, il existe $\lambda \in \mathbb{C}$ tel que $f = \lambda \mathrm{Id}_E$. Sa trace est donc $\dim(E)\lambda$. De plus,

$$\begin{aligned}
\mathrm{Tr}(f) &= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\theta(g) \circ h \circ \theta(g^{-1})) \\
&= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(\theta(g) \circ h \circ \theta(g)^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \mathrm{Tr}(h) \qquad \text{car } h \text{ et } \theta(g) \circ h \circ \theta(g)^{-1} \text{ sont semblables} \\
&= \mathrm{Tr}(h).
\end{aligned}$$

Donc $\lambda = \dfrac{\mathrm{Tr}(h)}{\dim(E)}$.

Troisième partie : théorème de Maschke

Le but de cette partie est de démontrer le théorème suivant :

14. Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini G et F un sous-espace invariant de θ.

(a) Il s'agit du théorème de la base incomplète.

(b) Si $x \in F$,

$$q(x) = \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1})(x).$$

Comme F est un sous-espace invariant de F, pour tout $g \in G$, $\theta(g^{-1})(x) \in F$, donc $p \circ \theta(g^{-1})(x) = \theta(g^{-1})(x)$. On obtient alors

$$q(x) = \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ \theta(g^{-1})(x) = \frac{1}{|G|} \sum_{g \in G} \theta(gg^{-1})(x) = \frac{1}{|G|} \sum_{g \in G} \theta(e_G)(x) = \frac{1}{|G|} \sum_{g \in G} x = x.$$

(c) La question précédente implique que $F \subseteq \mathrm{Im}(q)$. De plus, pour tout $x \in E$, pour tout $g \in G$, $p \circ \theta(g^{-1})(x)$ est un élément de F. Comme F est un sous-espace invariant de θ, $\theta(g) \circ p \circ \theta(g^{-1})(x) \in F$. En sommant, on obtient donc que $q(x) \in F$ pour tout $x \in E$, donc $\mathrm{Im}(q) \subseteq F$. On a montré que $\mathrm{Im}(q) = F$.

Soit $x \in E$. Alors $q(x) \in F$. D'après la question 14. (b), $q^2(x) = q(q(x)) = q(x)$. Donc $q^2 = q$: q est une projection sur $\mathrm{Im}(q) = F$.

(d) Soit $h \in G$.

$$\begin{aligned} q \circ \theta(h) &= \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1}) \circ \theta(h) \\ &= \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1}h) \\ &= \frac{1}{|G|} \sum_{g' \in G} \theta(hg') \circ p \circ \theta(g'^{-1}) \\ &= \frac{1}{|G|} \sum_{g' \in G} \theta(h) \circ \theta(g') \circ p \circ \theta(g'^{-1}) \\ &= \theta(h) \circ \left(\frac{1}{|G|} \sum_{g' \in G} \theta(g') \circ p \circ \theta(g'^{-1}) \right) \\ &= \theta(h) \circ q. \end{aligned}$$

À la troisième ligne, on a effectué le changement d'indices $g' = h^{-1}g$, ce qui donne $g = hg'$ et $g^{-1}h = g'^{-1}$. Donc q est un homomorphisme de représentations de θ vers elle-même.

(e) Par suite, $\mathrm{Ker}(q)$ est un sous-espace invariant de θ. Comme q est une projection sur F, $E = F \oplus \mathrm{Ker}(q)$.

15. Si E est de dimension 1, les seuls sous-espaces de E sont E et $\{0_E\}$, donc *a fortiori* les seuls sous-espaces invariants de θ sont E et $\{0_E\}$.

16. On procède par récurrence sur $\dim(E)$. Si $\dim(E) = 1$, alors E est irréductible : on prend $k = 1$ et $F_1 = E$. On suppose $\dim(E) \geqslant 2$ et le résultat acquis pour toutes les représentations $\theta' : G \longrightarrow \mathrm{GL}(E')$ de G telles que $\dim(E') < \dim(E)$. Si θ est irréductible, on prend $k = 1$ et $F_1 = E$. Sinon, il existe un sous-espace non trivial F invariant par θ. D'après la question 14. (f), il existe un autre sous-espace invariant non trivial F' tel que $E = F \oplus F'$. Comme F est non trivial, $\dim(F) < \dim(E)$ et $\dim(F') < \dim(E)$. On applique l'hypothèse de récurrence à $\theta_{|F}$ et $\theta_{|F'}$. Il existe $k, l \geqslant 1$, des sous-espaces $F_1, \ldots, F_k$ de F et $F'_1, \ldots, F'_l$ de F', tous invariants par θ, tels que pour tout $i \in [k]$, $(\theta_{|F})_{|F_i} = \theta_{|F_i}$ est irréductible et pour tout $j \in [l]$, $(\theta_{|F'})_{|F'_j} = \theta_{|F'_j}$ est irréductible, avec de plus

$$F = F_1 \oplus \ldots \oplus F_k, \qquad F' = F'_1 \oplus \ldots \oplus F'_l.$$

Alors
$$E = F \oplus F' = F_1 \oplus \ldots \oplus F_k \oplus F'_1 \oplus \ldots \oplus F'_l.$$

Le résultat est donc vrai pour θ. On conclut avec le principe de récurrence.

Quatrième partie : le cas des groupes abéliens finis

17. (a) Par le théorème de Lagrange, pour tout $g \in G$, $g^N = e_G$, donc $\theta(g)^N = \theta(g^N) = \theta(e_G) = \mathrm{Id}_E$. Par suite, $X^N - 1$ est un polynôme annulateur de $\theta(g)$. Ce polynôme étant à racines simples, $\theta(g)$ est diagonalisable (question 2).

(b) Soient $g_1, \dots, g_N$ les éléments de G. Pour tout $i, j \in [\![1, N]\!]$, $g_i g_j = g_j g_i$ dans G, donc

$$\theta(g_i) \circ \theta(g_j) = \theta(g_i g_j) = \theta(g_j g_i) = \theta(g_j) \circ \theta(g_i).$$

De plus, d'après la question 17 (a), les endomorphismes $\theta(g_i)$ sont tous diagonalisables. D'après la question 4, avec $f_i = \theta(g_i)$, il existe une base commune de vecteurs propres au $\theta(g_i)$ et donc en particulier un vecteur propre commun à tous les $\theta(g_i)$.

(c) On note x ce vecteur propre commun et F le sous-espace de E engendré par x. Alors F est stable par tous les $\theta(g_i)$, donc est une sous-représentation de θ de dimension 1. Comme E est irréductible, $E = F$ et E est de dimension 1.

18. Lorsque E est de dimension 1, on a l'isomorphisme de groupes suivant :

$$\left\{ \begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathrm{GL}(E) \\ \alpha & \longmapsto & \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \alpha x. \end{array} \right. \end{array} \right.$$

19. Tout d'abord, montrons que cette application est bien définie. Soient $\alpha, \beta \in \widehat{G}$. Pour tous $g, h \in G$,

$$\begin{aligned} \alpha \cdot \beta(gh) &= \alpha(gh)\beta(gh) \\ &= \alpha(g)\alpha(h)\beta(g)\beta(h) \\ &= \alpha(g)\beta(g)\alpha(h)\beta(h) \\ &= \alpha \cdot \beta(g)\alpha \cdot \beta(h) \end{aligned}$$

donc $\alpha \cdot \beta$ est bien un homomorphisme de groupes de G dans $\mathbb{C}^*$. De plus, comme $\cdot$ est le produit habituel des applications à valeurs dans $\mathbb{C}$, il est associatif et commutatif. Le caractère constant 1 est évidemment un élément de $\widehat{G}$, et c'est un élément neutre pour $\cdot$. Soit enfin $\alpha \in \widehat{G}$. Comme $\iota : z \longrightarrow \dfrac{1}{z}$ est un endomorphisme du groupe $\mathbb{C}^*$, par composition $\iota \circ \alpha \in \widehat{G}$ et pour tout $g \in G$,

$$\alpha \cdot (\iota \circ \alpha)(g) = \alpha(g)\frac{1}{\alpha(g)} = 1,$$

donc $\iota \circ \alpha$ est l'inverse de α dans $(\widehat{G}, \cdot)$. Par suite, $(\widehat{G}, \cdot)$ est un groupe abélien.

20. (a) Tout d'abord, α_1 est bien définie : soit $k, l \in \mathbb{Z}$, tels que $\overline{k} = \overline{l}$. Alors n divise $k - l$: posons $k = l + np$, avec $p \in \mathbb{Z}$.

$$\mathrm{e}^{\frac{2i\pi l}{n}} = \mathrm{e}^{\frac{2i\pi k}{n} + 2pi\pi} = \mathrm{e}^{\frac{2i\pi k}{n}} \mathrm{e}^{2pi\pi} = \mathrm{e}^{\frac{2i\pi k}{n}},$$

donc α_1 est bien définie. Soient $\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z}$.

$$\alpha_1(\overline{k} + \overline{l}) = \mathrm{e}^{\frac{2i\pi(k+l)}{n}} = \mathrm{e}^{\frac{2i\pi k}{n}} \mathrm{e}^{\frac{2i\pi l}{n}} = \alpha_1(\overline{k})\alpha_1(\overline{l}),$$

donc $\alpha_1 \in \widehat{G}$.

(b) Soit $\alpha \in \widehat{G}$. Alors

$$\alpha(n\overline{1}) = \alpha(\overline{0}) = 1 = \alpha(\overline{1})^n,$$

donc $\alpha(\overline{1})$ est une racine n-ième de l'unité : il existe $p \in \mathbb{Z}$ tel que

$$\alpha(\overline{1}) = \mathrm{e}^{\frac{2i\pi p}{n}}.$$

Pour tout $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, on a alors

$$\begin{aligned}\alpha(\overline{k}) &= \alpha(k\overline{1})\\ &= \alpha(\overline{1})^k\\ &= \mathrm{e}^{\frac{2\mathrm{i}\pi kp}{n}}\\ &= \left(\mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}\right)^p\\ &= \alpha_1(\overline{k})^p\\ &= \alpha_1^p(\overline{k}).\end{aligned}$$

Par suite, $\alpha = \alpha_1^p$. Le groupe $\widehat{G}$ est donc engendré par α_1. De plus, $\alpha_1^n = 1$ et si $\alpha_1^m = 1$, avec $m \in \mathbb{Z}$, alors

$$\alpha_1^m(\overline{1}) = \mathrm{e}^{\frac{2\mathrm{i}\pi m}{n}} = 1,$$

donc n divise m : α_1 est d'ordre n dans $\widehat{G}$.

21. Pour alléger, on pose

$$x = (\overline{0}, \overline{1}), \qquad y = (\overline{1}, \overline{0}),$$
$$0 = (\overline{0}, \overline{0}), \qquad z = x + y = (\overline{1}, \overline{1}).$$

Soit $\alpha \in \widehat{G}$, comme $2x = 2y = 0$, nécessairement $\alpha(x)^2 = \alpha(y)^2 = 1$, donc $\alpha(x), \alpha(y) \in \{1, -1\}$. De plus, $\alpha(z) = \alpha(x)\alpha(y)$. Ceci donne quatre possibilités pour α :

$$\alpha_0 : \left\{\begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ 0 & \longmapsto & 1 \\ x & \longmapsto & 1 \\ y & \longmapsto & 1 \\ z & \longmapsto & 1 \end{array}\right. \qquad \alpha_1 : \left\{\begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ 0 & \longmapsto & -1 \\ x & \longmapsto & 1 \\ y & \longmapsto & 1 \\ z & \longmapsto & -1 \end{array}\right.$$

$$\alpha_2 : \left\{\begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ 0 & \longmapsto & 1 \\ x & \longmapsto & 1 \\ y & \longmapsto & -1 \\ z & \longmapsto & -1 \end{array}\right. \qquad \alpha_3 : \left\{\begin{array}{ccc} G & \longrightarrow & \mathbb{C}^* \\ 0 & \longmapsto & 1 \\ x & \longmapsto & -1 \\ y & \longmapsto & -1 \\ z & \longmapsto & 1 \end{array}\right.$$

On vérifie facilement que ces quatre applications sont bien des éléments de $\widehat{G}$. Donc $\widehat{G}$ est un groupe à 4 éléments, constitué de α_0, α_1, α_2 et α_3.

Cinquième partie : prolongement des caractères et théorème de Kronecker

22. (a) De manière évidente, $\{hx^p \mid h \in H,\ p \in \mathbb{Z}\} \subseteq K$, car K est un sous-groupe de G contenant les éléments de H et x. osons $K' = \{hx^p \mid h \in H,\ p \in \mathbb{Z}\}$. Soit hx^p, $h'x^q \in K'$, avec $h, h' \in H$, $p, q \in \mathbb{Z}$. Comme G est abélien,

$$(hx^p)(h'x^q)^{-1} = (\underbrace{hh'^{-1}}_{\in H})x^{p-q} \in K'.$$

Donc K' est un sous-groupe de G. Comme il contient H (pour $p = 0$) et x (pour $h = e_G$ et $p = 1$), il contient K. Donc $K = K'$.
Les éléments de K/H sont les classes des éléments hx^p, avec $h \in H$ et $p \in \mathbb{Z}$:

$$\overline{hx^p} = \overline{h}\overline{x}^p = \overline{x}^p.$$

Donc K/H est un groupe cyclique, engendré par $\overline{x}$. Comme x n'appartient pas à H, K/H est non nul.

(b) *Existence d'une telle écriture*. Soit $g \in K$. Alors comme K/H est un groupe cyclique engendré par $\overline{x}$, d'ordre r, il existe $p \in [\![0, r-1]\!]$ tel que $\overline{g} = \overline{x}^p$. Alors $\overline{gx^{-r}} = \overline{e_G}$, donc $gx^{-r} \in H$: posons $gx^{-r} = h \in H$. On obtient $g = hx^p$.
Unicité d'une telle écriture. Supposons $hx^p = h'x^q$, avec $h, h' \in H$, $p, q \in [\![0, r-1]\!]$. Dans G/H, on obtient
$$\overline{hx^p} = \overline{x}^p = \overline{h'x^q} = \overline{x}^q.$$
Comme $\overline{x}$ est d'ordre r, $p = q$. Par suite, $h = hx^p x^{-p} = h'x^q x^{-q} = h'$.

(c) Comme $\overline{x}$ est d'ordre r dans G/H, $\overline{x^r} = \overline{e_G}$, donc $x^r \in H$.

(d) Par l'unicité de l'écriture (question 22 (b)), $\tilde{\alpha}$ est bien défini. Vérifions qu'il s'agit d'un caractère de K. Soient $g, g' \in K$. Par la question 22 (b), on peut écrire $g = hx^p$ et $g' = h'x^q$, avec $h, h' \in H$ et $0 \leqslant p, q \leqslant r-1$. On considère la division euclidienne de $p+q$ par r : $p + q = ar + b$, avec $a, b \in \mathbb{Z}$ et $0 \leqslant b \leqslant r-1$. Alors
$$\begin{aligned}
\tilde{\alpha}(gg') &= \tilde{\alpha}(hx^p h'x^q) \\
&= \tilde{\alpha}(hh'x^{p+q}) \\
&= \tilde{\alpha}(\underbrace{hh'(x^r)^a}_{\in H} x^b) \\
&= \alpha(hh'(x^r)^a)\omega^b \\
&= \alpha(h)\alpha(h')\alpha(x^r)^a\omega^b && \text{car } \alpha \in \widehat{H} \\
&= \alpha(h)\alpha(h')z^a\omega^b \\
&= \alpha(h)\alpha(h')\omega^{ar+b} \\
&= \alpha(h)\alpha(h')\omega^{p+q} \\
&= \alpha(h)\omega^p\alpha(h')\omega^q \\
&= \tilde{\alpha}(g)\tilde{\alpha}(g').
\end{aligned}$$
Donc $\tilde{\alpha} \in \widehat{K}$. Si $g \in H$, alors
$$\tilde{\alpha}(g) = \alpha(g)\omega^0 = \alpha(g),$$
donc $\tilde{\alpha}$ prolonge α.

(e) On raisonne par récurrence sur $[G : H]$. Si $[G : H] = 1$, alors $G = H$ et il n'y a rien à démontrer. Supposons que pour tout sous-groupe K de G tel que $[G : K] < [G : H]$ et pour tout caractère $\tilde{\alpha} \in \widehat{G/K}$, il existe $\alpha' \in \widehat{G}$ tel que $\alpha'_{|K} = \tilde{\alpha}$, avec $[G : H] > 1$. Choisissons $x \in G \backslash H$ et posons K comme dans la question 22 (a). D'après la question 22 (d), il existe $\tilde{\alpha} \in \widehat{K}$ tel que $\tilde{\alpha}_{|H} = \alpha$. De plus $H \subsetneq K$ puisque $x \in K \backslash H$, donc $[G : K] < [G : H]$. Par l'hypothèse de récurrence, il existe $\alpha' \in \widehat{G}$ tel que $\alpha'_{|K} = \tilde{\alpha}$. Alors
$$\alpha_{|H} = \tilde{\alpha}_{|H} = \alpha.$$
Par le principe de récurrence, le résultat est valable quelque soit $[G : H]$.

23. (a) Dans ce cas, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, où n est l'ordre de G. Par suite, $\widehat{G}$ est isomorphe à $\widehat{\mathbb{Z}/n\mathbb{Z}}$, groupe cyclique d'ordre n d'après la question 20 (b).

(b) La restriction d'un homomorphisme étant encore un homomorphisme, θ prend bien ses valeurs dans $\widehat{H}$. Soient $\alpha, \beta \in \widehat{G}$. Pour tous $h \in H$,
$$\theta(\alpha \cdot \beta)(h) = (\alpha \cdot \beta)(h) = \alpha(h)\beta(h) = \alpha_{|H}(h)\alpha_{|H}(h) = \theta(\alpha) \cdot \theta(\beta)(h),$$
donc $\theta(\alpha \cdot \beta) = \theta(\alpha) \cdot \theta(\beta)$: θ est un homomorphisme de groupes.
Enfin, soit $\alpha \in \widehat{H}$. D'après la question 22, il existe $\alpha' \in \widehat{G}$ tel que $\alpha'_{|H} = \alpha$, donc $\theta(\alpha') = \alpha$: θ est surjectif.

(c) Soient $g, g' \in G$ tels que dans G/H, $\overline{g} = \overline{g'}$. Alors $gg'^{-1} \in H$. Comme $\alpha \in \mathrm{Ker}(\theta)$, $\alpha_{|H}$ est le caractère constant (égal à 1) sur H, donc

$$\alpha(gg'^{-1}) = \alpha(g)\alpha(g')^{-1} = 1,$$

et finalement $\alpha(g) = \alpha(g')$: $\overline{\alpha}$ est bien défini.
Soient $\overline{g}, \overline{g'} \in G/H$.

$$\overline{\alpha}(\overline{g}\overline{g'}) = \alpha(gg') = \alpha(g)\alpha(g') = \overline{\alpha}(\overline{g})\overline{\alpha}(\overline{g'}),$$

donc $\overline{\alpha} \in \widehat{G/H}$.

(d) On a ainsi défini une application Ψ de $\mathrm{Ker}(\theta)$ dans $\widehat{G/H}$, envoyant α sur $\overline{\alpha}$. Montrons que Ψ est un homomorphisme : soient $\alpha, \beta \in \mathrm{Ker}(\theta)$. Pour tout $\overline{g} \in G/H$,

$$\Psi(\alpha \cdot \beta)(\overline{g}) = \alpha \cdot \beta(g) = \alpha(g)\beta(g) = \Psi(\alpha)(\overline{g})\Psi(\beta)(\overline{g}) = \Psi(\alpha) \cdot \Psi(\beta)(\overline{g}),$$

donc $\Psi(\alpha \cdot \beta) = \Psi(\alpha) \cdot \Psi(\beta)$.
Montrons que Ψ est surjectif. Soit $\alpha \in \widehat{G/H}$. Comme la surjection canonique $\pi : G \longrightarrow G/H$ est un homomorphisme de groupes, par composition $\beta = \alpha \circ \pi$ est un homomorphisme de groupes de G dans $\mathbb{C}^*$, donc appartient à $\widehat{G}$ et par construction, $\Psi(\beta) = \alpha$.
Montrons que Ψ est injectif. Soit $\alpha \in \mathrm{Ker}(\psi)$. Alors pour tout $g \in G$,

$$\alpha(g) = \Psi(\alpha)(\overline{g}) = 1_{\widehat{G/H}}(\overline{g}) = 1,$$

donc $\alpha = 1_{\widehat{G}}$. Ainsi, Ψ est injectif.

(e) On procède par récurrence sur $|G|$. Si $|G| = 1$ ou 2, alors G est cyclique et d'après la question 23 (a), $|\widehat{G}| = |G|$. Supposons le résultat vrai pour tous les groupes abéliens H tels que $|H| < |G|$. Si G est cyclique, d'après la question 23 (a), $|\widehat{G}| = |G|$. Sinon, on choisit H comme dans la question 23 (b). Alors H est un sous-groupe non trivial de G et l'hypothèse de récurrence s'applique à H et à G/H. D'après le premier théorème d'isomorphisme appliqué à θ,

$$|\widehat{G}| = |\widehat{H}||\mathrm{Ker}(\theta)|.$$

Par l'hypothèse de récurrence appliquée à H, $|\widehat{H}| = |H|$. De plus, d'après la question 23. (d) et l'hypothèse de récurrence appliquée à G/H,

$$|\mathrm{Ker}(\theta)| = |\widehat{G/H}| = |G/H| = \frac{|G|}{|H|},$$

et pour finir

$$|\widehat{G}| = |H|\frac{[G|}{|H|} = |G|.$$

24. (a) Comme pour la question 20 (a), on montre que l'application suivante est un caractère de H :

$$\alpha : \left\{ \begin{array}{ccc} H & \longrightarrow & \mathbb{C}^* \\ x^k & \longmapsto & \mathrm{e}^{\frac{2ik\pi}{N}}. \end{array} \right.$$

Comme $\mathrm{e}^{\frac{2i\pi}{N}}$ est un élément de $\mathbb{C}^*$ d'ordre N, α est injectif.

(b) La question 22 permet de montrer l'existence d'un tel β.

(c) Comme β est un prolongement de α, $\beta(G)$ contient

$$\alpha(H) = \{e^{\frac{2ik\pi}{N}} \mid k \in \mathbb{Z}\} = \{z \in \mathbb{C} \mid z^N = 1\}.$$

Soit $g \in G$. Par définition de l'exposant de G, l'ordre de g divise N, donc $g^N = e_G$. Par suite,

$$\beta(g^N) = 1 = \beta(g)^N,$$

donc $\beta(g) \in \{z \in \mathbb{C} \mid z^N = 1\}$. Par suite, $\beta(G) = \{z \in \mathbb{C} \mid z^N = 1\}$.

(d) L'exposant de $\mathrm{Ker}(\beta)$ est le PPCM des ordres des éléments de $\mathrm{Ker}(\beta)$, sous-groupe de G. Par suite, il divise le PPCM des ordres des éléments de G, c'est-à-dire l'exposant N de G.

(e) On considère l'application suivante :

$$\phi : \left\{ \begin{array}{rcl} H \times \mathrm{Ker}(\beta) & \longrightarrow & G \\ (h, h') & \longmapsto & hh'. \end{array} \right.$$

C'est un homomorphisme de groupes : soient $(h_1, h'_1), (h_2, h'_2) \in H \times \mathrm{Ker}(\beta)$.

$$\phi((h_1, h'_1)(h_2, h'_2)) = \phi(h_1h_2, h'_1h'_2) = h_1h_2h'_1h'_2 = h_1h'_1h_2h'_2 = \phi(h_1, h'_1)\phi(h_2, h'_2).$$

ϕ est injectif : soit $(h, h') \in \mathrm{Ker}(\phi)$. Alors $hh' = e_G$, donc $h' = h^{-1}$. De plus, comme $h' \in \mathrm{Ker}(\beta)$ et que $h^{-1} \in H$,

$$\beta(h') = 1 = \alpha(h^{-1}).$$

Comme $\alpha = \beta_{|H}$ est injectif, $h^{-1} = e_G$, donc $h = e_G$ et $h' = e_G$.

ϕ est surjectif : soit $g \in G$. Comme $\alpha(H) = \beta(G)$, il existe $h \in H$ tel que $\alpha(h) = \beta(g)$. Alors $\beta(h^{-1}g) = \beta(h)^{-1}\beta(g) = \alpha(h)^{-1}\beta(g) = 1$, donc $h' = h^{-1}g \in \mathrm{Ker}(\beta)$. Par suite, $\phi(h, h') = hh^{-1}g$.

En conclusion, ϕ est un isomorphisme.

(f) On va procéder par récurrence sur $|G|$. Si $|G| = 1$, il n'y a rien à montrer. Supposons le résultat vrai pour tout groupe abélien H tel que $|H| < |G|$. Soit x un élément de G d'ordre l'exposant N de G. D'après la question 24 (e), il existe un sous-groupe K de G tel que G est isomorphe à $\langle x \rangle \times K$. De plus, l'exposant N' de K divise N. En appliquant l'hypothèse de récurrence à K, il existe $N_2, \ldots, N_k \geqslant 2$, avec N_k divisant N_{k-1},..., N_3 divisant N_2, tels que K est isomorphe à

$$\mathbb{Z}/N_2\mathbb{Z} \times \ldots \times \mathbb{Z}/N_k\mathbb{Z}.$$

Les éléments de ce groupe étant tous d'ordre divisant N_2 et ce groupe possédant un élément d'ordre N_2, l'exposant de K est N_2. Donc N_2 divise N_1. Comme $\langle x \rangle$ est isomorphe à $\mathbb{Z}/N\mathbb{Z}$, on obtient que G est isomorphe à

$$Z/N\mathbb{Z} \times Z/N_2\mathbb{Z} \times \ldots \times \mathbb{Z}/N_k\mathbb{Z},$$

qui est une décomposition de Kronecker de G.

25. On applique le théorème des restes chinois de façon répétée :

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} &\approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\approx (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \\ &\approx \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \end{aligned}$$

qui est donc une décomposition de Kronecker de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

Sixième partie : applications centrales

26. (a) La fonction nulle est un élément de $\mathcal{C}(G)$. Soit $\lambda, \mu \in \mathcal{C}(G)$ et soient $x, y \in \mathbb{C}$. Pour tous $g, h \in G$,

$$\begin{aligned}(x\lambda + y\mu)(g \cdot h) &= x\lambda(g \cdot h) + y\mu(g \cdot h)\\ &= x\lambda(h \cdot g) + y\mu(h \cdot g)\\ &= (x\lambda + y\mu)(h \cdot g).\end{aligned}$$

Donc $x\lambda + y\mu \in \mathcal{C}(G)$.

(b) $\Longrightarrow$. Supposons λ centrale. Soient g, g' dans une même classe de conjugaison de G. Alors g et g' sont conjugués : il existe $h \in H$ tel que $g = hg'h^{-1}$. Comme λ est centrale,

$$\lambda(g) = \lambda((hg')h^{-1}) = \lambda(h^{-1}(hg')) = \lambda(g').$$

Donc λ est constante sur chaque classe de conjugaison.

$\Longleftarrow$. Supposons λ constante sur chaque classe de conjugaison de G. Soient $g, h \in G$. Alors

$$hg = hg(hh^{-1}) = h(gh)h^{-1},$$

donc hg et gh sont conjugués. Comme λ est constante sur les classes de conjugaison, $\lambda(hg) = \lambda(gh)$: λ est centrale.

(c) Par définition, ι_C est constante sur chaque classe de conjugaison : par la question 26 (b), $\iota_C \in \mathcal{C}(G)$. On note $\{C_1, \ldots, C_k\}$ l'ensemble des classes de conjugaison de G. Soient $x_1, \ldots, x_k \in \mathbb{C}$ tels que $x_1\iota_{C_1} + \ldots + x_k\iota_{C_k} = 0$. Pour $i \in [\![1, k]\!]$, choisissons $g \in C_i$. Comme les classes de conjugaison de G sont disjointes,

$$(x_1\iota_{C_1} + \ldots + x_k\iota_{C_k})(g) = 0 = 0 + \ldots + 0 + x_i + 0 + \ldots + 0 = x_i.$$

Par suite, la famille $(\iota_{C_1}, \ldots, \iota_{C_k})$ est libre.

Soit $\lambda \in \mathcal{C}(G)$. D'après la question 26 (b), λ est constante sur C_i pour tout $i \in [\![1, k]\!]$: soit x_i la valeur de λ sur chaque élément de C_i. Alors

$$\lambda = x_1\iota_{C_1} + \ldots + x_k\iota_{C_k}.$$

Par suite, la famille $(\iota_{C_1}, \ldots, \iota_{C_k})$ est une famille génératrice de $\mathcal{C}(G)$.

En conclusion, la famille $(\iota_{C_1}, \ldots, \iota_{C_k})$ est une base de $\mathcal{C}(G)$. La dimension de cet espace est donc le nombre de classes de conjugaison de G.

27. (a) Soient $g, h \in G$.

$$\chi_\theta(gh) = \mathrm{Tr}(\theta(gh)) = \mathrm{Tr}(\theta(g) \circ \theta(h)) = \mathrm{Tr}(\theta(h) \circ \theta(g)) = \mathrm{Tr}(\theta(hg) = \chi_\theta(hg)).$$

On a utilisé la propriété de la trace démontrée dans la question 1 (e). Donc χ_θ est centrale.

(b) Soit N l'ordre de G. Alors $g^N = e_G$, donc $\theta(g^N) = \theta(g)^N = \mathrm{Id}_E$. Par suite, $X^N - 1$ est un polynôme annulateur de $\theta(g)$. Comme ce polynôme est à racines simples, d'après la question 2 $\theta(g)$ est diagonalisable. De plus, ses valeurs propres sont racines de $X^N - 1$, donc des racines de l'unité.

(c) Soient $\lambda_1, \ldots, \lambda_n$ les valeurs propres (avec multiplicité) de $\theta(g)$. Alors

$$\chi_\theta(g) = \lambda_1 + \ldots + \lambda_n.$$

De plus,

$$\chi_\theta(g^{-1}) = \frac{1}{\lambda_1} + \ldots + \frac{1}{\lambda_n}.$$

D'après la question 27 (b), $\lambda_1, \dots, \lambda_n$ sont des racines de l'unité et par suite, leurs inverses sont leurs conjugués. Par suite,

$$\chi_\theta(g^{-1}) = \overline{\lambda_1} + \dots + \overline{\lambda_n} = \overline{\chi_\theta(g)}.$$

28. Il est immédiat que cette forme est hermitienne. Soit $\lambda \in \mathcal{C}(G)$.

$$\langle \lambda, \lambda \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\lambda(g)} \lambda(g) = \frac{1}{|G|} \sum_{g \in G} |\lambda(g)|^2$$

est un réel positif ou nul. De plus, si $\langle \lambda, \lambda \rangle = 0$, alors pour tout $g \in G$, $\lambda(g) = 0$ et donc $\lambda = 0$. Donc cette forme est définie positive.

29. (a) On obtient

$$\begin{aligned}
\langle \chi_{\theta'}, \chi_\theta \rangle &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_{\theta'}(g)} \chi_\theta(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^{n'} \overline{a'_{i,i}(g)} \right) \left(\sum_{j=1}^{n} a_{j,j}(g) \right) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n'} \sum_{j=1}^{n} \overline{a'_{i,i}(g)} a_{j,j}(g).
\end{aligned}$$

(b) On obtient

$$y_{i,l} = \frac{1}{|G|} \sum_{g \in G} \sum_{j=1}^{n'} \sum_{k=1}^{n} a'_{i,j}(g) x_{j,k} a_{k,l}(g^{-1}).$$

(c) D'après la question 13 (b) i, f est nulle, quelque soit le choix de de la matrice X. On obtient donc, si $1 \leqslant i \leqslant n'$ et $1 \leqslant j \leqslant n$,

$$y_{i,l} = \frac{1}{|G|} \sum_{g \in G} \sum_{j=1}^{n'} \sum_{k=1}^{n} a'_{i,j}(g) x_{j,k} a_{k,l}(g^{-1}) = 0.$$

Soit $j \in [\![1, n']\!]$ et $k \in [\![1, n]\!]$. On choisit alors X dont le seul coefficient non nul, égal à 1, est $x_{j,k}$. De ce qui précède, si $1 \leqslant i \leqslant n'$ et $1 \leqslant j \leqslant n$,

$$\frac{1}{|G|} \sum_{g \in G} a'_{i,j}(g) a_{k,l}(g^{-1}) = 0.$$

Par suite, avec la question 27 (c) et le changement de variables $g = h^{-1}$,

$$\begin{aligned}
\langle \chi_{\theta'}, \chi_\theta \rangle &= \frac{1}{|G|} \sum_{h \in G} \overline{\chi_{\theta'}(h)} \chi_\theta(h) \\
&= \frac{1}{|G|} \sum_{h \in G} \chi_{\theta'}(h^{-1}) \chi_\theta(h) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{\theta'}(g) \chi_\theta(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n'} \sum_{j=1}^{n} a_{i,i} a_{j,j}(g^{-1}) \\
&= \sum_{i=1}^{n'} \sum_{j=1}^{n} \left(\frac{1}{|G|} \sum_{g \in G} a_{i,i} a_{j,j}(g^{-1}) \right) \\
&= 0.
\end{aligned}$$

(d) i. D'après la question 13 (c), l'application f de la question 29 (b) est égale à $\dfrac{\mathrm{Tr}(h)}{|G|}\mathrm{Id}_E$. On fixe $j,k \in [\![1,]\!]$ et on choisit pour X la matrice dont le seul coefficient non nul vaut 1 et est en position (j,k). Alors si $i,l \in [\![1,]\!]$,

$$y_{i,l} = \frac{1}{|G|}\sum_{g\in G} a_{i,j}(g)a_{k,l}(g^{-1}).$$

De plus, comme $f = \dfrac{\mathrm{Tr}(h)}{|G|}\mathrm{Id}_E$, si $i \neq l$, $y_{i,l} = 0$. Si $i = l$, comme $\mathrm{Tr}(h) = 1$ si $j = k$ et 0 sinon, on obtient

$$y_{i,i} = \begin{cases} \dfrac{1}{|G|} \text{ si } j = k, \\ 0 \text{ sinon.} \end{cases}$$

On obtient ainsi le résultat annoncé.

ii. Comme pour la question 29 (c),

$$\begin{aligned}
\langle \chi_\theta, \chi_\theta \rangle &= \frac{1}{|G|}\sum_{g\in G} \chi_{\theta'}(g)\chi_\theta(g^{-1}) \\
&= \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,i}a_{j,j}(g^{-1}) \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\left(\frac{1}{|G|}\sum_{g\in G} a_{i,i}a_{j,j}(g^{-1})\right) \\
&= \sum_{i=1}^{n}\frac{1}{n} + 0 \\
&= 1.
\end{aligned}$$

(e) D'après les questions 29 (c) et (d), la famille $(\chi_{\theta_i})_{1\leqslant i\leqslant k}$ est orthonormale, donc est libre. Par suite, k est inférieure ou égale à la dimension de $\mathcal{C}(G)$, c'est-à-dire le nombre de classes de conjugaison de G.

30. On a montré dans la quatrième partie que lorsque G est abélien, le nombre de représentations irréductibles à isomorphisme près de G est égal au cardinal de $\widehat{G}$, qui est égal au cardinal de G d'après la question 23. Montrer que si G est abélien, est égal à $|G|$.

31. Si θ et θ' sont isomorphes, soit $f : E \longrightarrow E'$ un isomorphisme. Pour tout $g \in G$, $f\circ\theta(g) = \theta'(g)\circ f$, donc $\theta'(g) = f\circ\theta(g)\circ f^{-1}$: en conséquence, $\theta(g)$ et $\theta'(g)$ ont la même trace, ce qui donne $\chi_\theta = \chi_{\theta'}$. D'après la question 29 (d),

$$\langle \chi_\theta, \chi_{\theta'} \rangle = \langle \chi_\theta, \chi_\theta \rangle = 1.$$

32. Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini G et soit $E = F_1 \oplus \ldots \oplus F_k$ une décomposition de E en sous-espaces invariants irréductibles, obtenue avec le théorème de Maschke.

(a) En utilisant une base adaptée à cette décomposition, pour tout $g \in G$,

$$\chi_\theta(g) = \mathrm{Tr}(\theta(g)) = \sum_{i=1}^{k}\mathrm{Tr}(\theta_{|F_i}(g)) = \sum_{i=1}^{k}\chi_{\theta_{|F_i}}(g).$$

D'où

$$\chi_\theta = \sum_{i=1}^{k}\chi_{\theta_{|F_i}}.$$

(b) Par suite,

$$\langle \chi_{\theta'}, \chi_\theta \rangle = \sum_{i=1}^{k} \langle \chi_{\theta'}, \chi_{\theta_{|F_i}} \rangle.$$

De plus, d'après la question 29, $\langle \chi_{\theta'}, \chi_{\theta_{|F_i}} \rangle$ vaut 1 si θ est $\theta_{|F_i}$ sont isomorphes et 0 sinon. Donc $\langle \chi_{\theta'}, \chi_\theta \rangle$ est égal au nombre de F_i tels que θ' et $\theta_{|F_i}$ sont isomorphes.

33. $\Longrightarrow$. Soit f un isomorphisme de θ vers θ'. Pour tout $g \in G$, $\theta(g) = f \circ \theta'(g) \circ f^{-1}$, donc $\theta(fg)$ et $\theta'(g)$ ont la même trace : $\chi_\theta = \chi_{\theta'}$.

$\Longleftarrow$. Soit $\theta_1, \ldots, \theta_k$ les représentations irréductibles de G à isomorphismes près, avec k inférieur ou égal au nombre de classes de conjugaison de G. On utilise une décomposition de E comme dans la question 32. En posant $n_i = \langle \chi_\theta, \chi_{\theta_i} \rangle$, d'après la question 32 (b), on obtient que θ est isomorphe à

$$\theta'' = \theta_1^{n_1} \times \ldots \times \theta_k^{n_k}.$$

On procède de même pour θ'. On pose $n_i' = \langle \chi_{\theta'}, \chi_{\theta_i} \rangle$ et alors θ' est isomorphe à

$$\theta_1^{n_1'} \times \ldots \times \theta_k^{n_k'}.$$

Mais comme $\chi_\theta = \chi_{\theta'}$, $n_i = n_i'$ pour tout $i \in [\![1, k]\!]$, donc θ et θ' sont tous deux isomorphes à la représentation θ'', donc sont isomorphes.