Agrégation interne de mathématiques

2024 - Composition 1

Éléments de correction proposés par G. Dupont
http://maths-concours.fr/

Version du 12 février 2024

Notations du corrigé

Outre les notations introduites dans l'énoncé, nous utiliserons librement les notations suivantes :

— Si m et n sont des entiers non nuls, on note $m \wedge n$ leur PGCD et $m \vee n$ leur PPCM.

— Si $(G, \cdot)$ est un groupe multiplicatif, on note e_G sont élément neutre. Dans $(\mathbb{C}^*, \times)$, on le note simplement 1 ou $1_{\mathbb{C}}$.

— Pour tout $N \in \mathbb{N}^*$, on note $\mathbb{U}_N = \left\{z \in \mathbb{C} \,\middle|\, z^N = 1\right\}$ l'ensemble des racines N-ièmes de l'unité.

— Etant donné deux éléments i et j d'un ensemble E, on note $\delta_{i,j}$ le symbole de Kronecker, qui vaut 1 si $i = j$ et 0 sinon.

Exercice 1

1. (a) **Faux**. Un endomorphisme nilpotent non nul n'est pas diagonalisable. Par exemple, l'endomorphisme de $\mathbb{C}^2$ canoniquement associé à la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ n'est pas diagonalisable.

   (b) **Faux**. Par exemple, l'endomorphisme de $\mathbb{C}^2$ associé à la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans une base (e_1, e_2) admet $\mathbb{C}e_1$ pour unique droite propre ; elle n'a donc pas de supplémentaire stable.

   (c) **Vrai**. Si $\mathcal{B} = (e_1, \ldots, e_n)$ est une base de vecteurs propres de E, chaque e_i étant associé à la valeur propre λ_i, alors $\mathrm{Mat}_{\mathcal{B}}(f) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ donc $\mathrm{Mat}_{\mathcal{B}}(f^2) = \mathrm{diag}(\lambda_1^2, \ldots, \lambda_n^2)$, ce qui prouve la diagonalisabilité de f^2.

   (d) **Faux**. Si f l'endomorphisme de $\mathbb{C}^2$ canoniquement associé à la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, alors il n'est pas diagonalisable mais $f^2 = 0$ l'est.

   (e) **Vrai**. Si $\mathcal{B}$ est une base de E et A, B désignent respectivement les matrices représentatives de f et de g dans cette base, alors

$$\mathrm{tr}(f \circ g) = \mathrm{tr}(AB) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} b_{ki} = \sum_{k=1}^{n} \sum_{i=1}^{n} b_{ki} a_{ik} = \mathrm{tr}(BA) = \mathrm{tr}(g \circ f).$$

Exercice 2

2. — <u>(a) ⇒ (b) :</u> Si f est diagonalisable, il existe une base $\mathcal{B}$ de vecteurs propres telle que la matrice dans la base $\mathcal{B}$ de f est $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, les λ_i étant les valeurs propres de f. Quitte à renuméroter, on suppose que

$$\{\lambda_1, \ldots, \lambda_n\} = \{\lambda_1, \ldots, \lambda_r\},$$

   où les λ_i avec $1 \leq i \leq r$ sont deux à deux distinctes.

   Si on pose $P = (X - \lambda_1) \cdots (X - \lambda_r)$, on a $P(D) = 0_n$ de sorte que $P(f) = 0$. Ainsi, f admet un polynôme annulateur scindé à racines simples.

   — <u>(b) ⇒ (c) :</u> Si f admet un polynôme annulateur P scindé à racines simples, le polynôme minimal μ_f de f divisant P, il est aussi scindé à racines simples.

— (c) ⇒ (a) : Si f admet un polynôme minimal scindé à racines simples, on note $\mu_f = (X-\lambda_1)\cdots(X-\lambda_r)$ avec les λ_i deux à deux distinctes. Alors les $X-\lambda_i$ sont deux à deux premiers entre eux et, d'après le lemme des noyaux, on a

$$E = \ker(\mu_f) = \bigoplus_{i=1}^{r} \ker(f-\lambda_i \mathrm{id}_E),$$

ce qui prouve la diagonalisabilité de f.

3. Si f est diagonalisable, alors f admet un polynôme annulateur P scindé à racines simples. On a

$$\forall x \in F, \quad P\left(f_{|F}\right)(x) = P(f)(x) = 0$$

donc $P\left(f_{|F}\right) = 0$ et $f_{|F}$ admet un polynôme annulateur scindé à racines simples ; il est donc diagonalisable.

4. (a) On commence par observer que si deux endomorphismes f et g commutent, alors pour tout $x \in \ker(f)$, on a $f(g(x)) = g(f(x)) = g(0) = 0$ donc $\ker(f)$ est stable par g. D'autre part, si f et g commutent, alors g commute avec tout polynôme en f et donc, pour tout $\lambda \in \mathbb{R}$, $g \circ (f-\lambda \mathrm{id}_E) = (f-\lambda\mathrm{id}_E)\circ f$ de sorte que $\ker(f-\lambda\mathrm{id}_E)$ est stable par g. En particulier, tout espace propre de f est stable par g.

   En appliquant ce résultat aux f_i, on obtient la stabilité des sous-espaces propres de f_k par tous les f_i.

   (b) F étant stable par f_i, la restriction de f_i à F est un endomorphisme de F, qui est diagonalisable d'après la question 3.

   (c) On montre le résultat par récurrence sur k. Si $k=1$, il n'y a rien à montrer. Supposons la propriété vérifiée pour $k \in \mathbb{N}^*$ et montrons qu'elle est vérifiée pour $k+1$. Puisque f_{k+1} est diagonalisable, on peut décomposer

$$E = \bigoplus_{i=1}^{r} F_i,$$

   où les F_i sont les espaces propres de f_{k+1}.

   Soit $j \in [\![1,r]\!]$. D'après 4.a, F_j est stable par $f_1,\ldots,f_k$. Les endomorphismes induits par $f_1,\ldots,f_k$ sur F_j commutent deux à deux et sont diagonalisables d'après 4.b. Il s'ensuit qu'il existe une base $\mathcal{B}_j$ de F_j formée de vecteurs propres communs à $f_1,\ldots,f_k$. Puisque $\mathcal{B}_j$ est une base de l'espace propre F_j de f_{k+1}, $\mathcal{B}_j$ est formée de vecteurs propres communs à $f_1,\ldots,f_k,f_{k+1}$. La concaténation des $\mathcal{B}_j$, pour $j \in [\![1,r]\!]$ fournit alors une base de E, formée de vecteurs propres communs à $f_1,\ldots,f_k,f_{k+1}$.

Exercice 3

On note e le neutre de G.

5. Soit $g \in G$ d'ordre n et d un diviseur de n. On note $q = \frac{n}{d}$. On a

$$\left(g^d\right)^q = g^n = e$$

donc l'ordre de g^d divise q. Par ailleurs, si $q' \in [\![0,q-1]\!]$ vérifie $\left(g^d\right)^{q'} = e$, alors $g^{dq'} = e$ avec $dq' < dq = n$, donc $q' = 0$.
En conclusion :

$$\boxed{\text{Si } d \text{ divise } n, \text{ l'ordre de } g^d \text{ est } q = \frac{n}{d}.}$$

6. Notons $d = (n\wedge d)d'$ et $n = (n\wedge d)n'$. On a donc $n' \wedge d' = 1$. Montrons que l'ordre de g^d est $n' = \dfrac{n}{n\wedge d}$.
On a

$$\left(g^d\right)^{n'} = g^{dn'} = g^{d'(n\wedge d)n'} = g^{nd'} = (g^n)^{d'} = e$$

donc l'ordre de g^d divise n'.
Soit $a \in \mathbb{N}$ tel que $(g^d)^a = e$. On a donc :

$$(g^d)^a = e \;\Rightarrow\; g^{da} = e$$

$$\begin{aligned} &\Rightarrow n|da \\ &\Rightarrow n'(d\wedge n)|d'(d\wedge n)a \\ &\Rightarrow n'|d'a \end{aligned}$$

mais $n' \wedge d' = 1$ donc n' divise a.
En conclusion :

$$\boxed{\text{De manière générale, l'ordre de } g^d \text{ est } \frac{n}{n\wedge d}.}$$

7. (a) Soit $x \in \langle g\rangle \cap \langle h\rangle$. D'après le théorème de Lagrange, l'ordre de x divise l'ordre de $\langle g\rangle$, qui est égal à k, ainsi que l'ordre de $\langle h\rangle$ qui est égal à ℓ. Puisque $k\wedge \ell = 1$, x est d'ordre 1 et donc $x = e$. En conclusion :

$$\boxed{\langle g\rangle \cap \langle h\rangle = \{e\}.}$$

(b) Puisque G est abélien, on a :

$$(gh)^{kl} = g^{kl}h^{kl} = e$$

et, pour tout $a \in \mathbb{N}^*$, si on a $(gh)^a = e$, alors $g^a = h^{-a} \in \langle g\rangle \cap \langle h\rangle = \{e\}$ donc k divise a. De même, $h^a = q^{-a} \in \langle g\rangle \cap \langle h\rangle = \{e\}$ donc ℓ divise a. Puisque $k\wedge\ell = 1$, $k\ell$ divise a et donc :

$$\boxed{\text{L'ordre de } gh \text{ est } k\ell.}$$

8. Par récurrence sur n, on démontre le résultat immédiatement à partir de la question précédente.

9. (a) On note $\mathcal{P}$ l'ensemble des nombres premiers et, pour tout entier naturel n supérieur ou égal à 2 et tout nombre premier p, on note $v_p(n)$ l'exposant de p dans la décomposition en facteurs premiers de n. On rappelle que, pour tout couple (m,n) d'entiers naturels supérieurs ou égaux à 2, on a :

$$m\vee n = \prod_{p\in\mathcal{P}} p^{\max(v_p(n),v_p(m))}$$

donc, par récurrence, on a :

$$\exp(G) = \prod_{p\in\mathcal{P}} p^{v_p(G)}$$

où $v_p(G)$ est le maximum des $v_p(n)$ quand n parcourt l'ensemble des ordres des éléments de G.
Alors, si on a

$$\exp(G) = p_1^{\alpha_1}\cdots p_n^{\alpha_n},$$

alors, pour tout $i \in [\![1,n]\!]$, il existe g d'ordre k dans G tel que $\alpha_i = v_p(k)$, c'est-à-dire tel que $p_i^{\alpha_i}$ divise k.
Si on pose $k = dp_i^{\alpha_i}$, il suit de la question 5 que g^d est d'ordre $p_i^{\alpha_i}$.

(b) Pour tout $i \in [\![1,n]\!]$, G contient un élément g_i d'ordre $p_i^{\alpha_i}$. Il suit alors que la question 8 que $g_1\cdots g_n$ est un élément d'ordre $p_1^{\alpha_1}\cdots p_n^{\alpha_n}$.
En conclusion :

$$\boxed{G \text{ contient un élément d'ordre } \exp(G).}$$

Deuxième partie : définition et exemples

10. (a) i. Si $\theta : G \longrightarrow \mathrm{GL}(E)$ est un morphisme de groupes, alors

$$\boxed{\theta(e_G) = e_{\mathrm{GL}(E)} = \mathrm{id}_E.}$$

ii. Si $\theta : G \longrightarrow \mathrm{GL}(E)$ est un morphisme de groupes, alors, pour tout $g \in G$,

$$\boxed{\theta(g^{-1}) = \theta(g)^{-1}.}$$

(b) Puisque $\mathrm{GL}(E)$ est un groupe et $f \in \mathrm{GL}(E)$, on observe que $f^k \in \mathrm{GL}(E)$ est bien défini pour tout $k \in \mathbb{Z}$. Soit $(k, \ell) \in \mathbb{Z}^2$. On a

$$\theta_1(k+\ell) = f^{k+\ell} = f^k \circ f^\ell = \theta_1(k) \circ \theta_1(\ell)$$

donc

$$\boxed{\theta_1 \text{ est une représentation de } (\mathbb{Z}, +) \text{ d'espace } E.}$$

(c) Puisque $f^n = \mathrm{id}_E$, on a $n\mathbb{Z} \subset \ker(\theta_1)$ donc le morphisme θ_1 passe au quotient en un morphisme de groupes

$$\theta_2 : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathrm{GL}(E).$$

Ainsi,

$$\boxed{\theta_2 \text{ est une représentation de } (\mathbb{Z}/n\mathbb{Z}, +) \text{ d'espace } E.}$$

(d) Soit $\lambda \in \mathbb{C}$. On observe que $f_\lambda \in \mathcal{L}(\mathbb{C}^2)$ et que

$$\det(f_\lambda) = \begin{vmatrix} 1 & \lambda \\ 0 & 1 \end{vmatrix} = 1$$

donc $f_\lambda \in \mathrm{GL}(\mathbb{C}^2)$, de sorte que θ_3 est bien définie.
Soit $(\lambda, \mu) \in \mathbb{C}^2$ et $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2$. On a :

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

donc

$$\theta_3(\lambda+\mu) = \theta_3(\lambda) + \theta_3(\mu)$$

et donc

$$\boxed{\theta_3 \text{ est une représentation de } (\mathbb{C}, +) \text{ d'espace } \mathbb{C}^2.}$$

(e) Notons (e_1, e_2, e_3) la base canonique de $\mathbb{C}^3$ et $\sigma \in \mathfrak{S}_3$. L'application g_σ est clairement linéaire et on a :

$$\forall i \in [\![1, 3]\!], \quad g_\sigma(e_i) = e_{\sigma(i)}.$$

Soit alors $\tau \in \mathfrak{S}_3$ et $i \in [\![1, 3]\!]$. On a :

$$(g_\tau \circ g_\sigma)(e_i) = g_\tau(e_{\sigma(i)}) = e_{(\tau\circ\sigma)(i)} = g_{\tau\circ\sigma}(e_i).$$

Par prolongement par linéarité, on a donc

$$g_\tau \circ g_\sigma = g_{\tau\circ\sigma}$$

et donc

$$\theta_4(\tau \circ \sigma) = \theta_4(\tau) \circ \theta_4(\sigma).$$

Enfin, on observe que $g_\sigma \circ g_{\sigma^{-1}} = g_{\mathrm{id}} = \mathrm{id}_{\mathbb{C}^3}$ donc θ_4 est bien à valeurs dans $\mathrm{GL}(\mathbb{C}^3)$.
En conclusion :

$$\boxed{\theta_4 \text{ est une représentation de } (\mathfrak{S}_3, \circ) \text{ d'espace } \mathbb{C}^3.}$$

11. (a) Soit F un sous-espace invariant par θ et soit $g \in G$. Puisque $\theta(g)(F) \subset F$, la restriction de $\theta(g)$ à F induit un endomorphisme de F. Puisque $\theta(g) \in \mathrm{GL}(E)$, on a $\ker(\theta(g)) = \{0_E\}$ donc

$$\ker(\theta(g)_{|F}) = \ker(\theta(g)) \cap F = \{0_E\}$$

et donc $\theta(g)_{|F}$ est injective. Puisque F est de dimension finie, il s'ensuit que

$$\boxed{\theta(g)_{|F} \in \mathrm{GL}(F).}$$

(b) Soit F un sous-espace invariant par θ. D'après la question précédente, pour tout $g \in G$, $\theta(g)_{|F} \in \mathrm{GL}(F)$ donc $\theta_{|F}$ est bien définie. D'autre part, la restriction de la composition est égale à la composition des restrictions donc

$$\forall (g,h) \in G^2, \quad \theta_{|F}(gh) = \theta_{|F}(g) \circ \theta_{|F}(h)$$

et donc

$$\boxed{\theta_{|F} \text{ est une représentation de } G \text{ d'espace } F.}$$

(c) Les sous-espaces $\{0\}$ et $\mathbb{C}^2$ sont évidemment θ_3-invariants.
Notons (e_1, e_2) la base canonique de $\mathbb{C}^2$. On observe que, pour tout $\lambda \in \mathbb{C}$, on a

$$\theta_3(\lambda)(e_1) = e_1$$

donc $\mathbb{C}e_1$ est un sous-espace θ_3-invariant.
Soit $v = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2$ tel que $y \neq 0$. Pour tout $\lambda \in \mathbb{C}$, on a

$$f_\lambda(v) = f_\lambda \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \lambda y \\ y \end{pmatrix}$$

donc, si $\lambda \neq 0$, v et $f_\lambda(v)$ ne sont pas colinéaires. Il s'ensuit que $\mathbb{C}v$ n'est pas θ_3-invariante.
Par dimension, on obtient :

$$\boxed{\text{Les sous-espaces } \theta_3\text{-invariants sont } \{0\}, \mathbb{C}e_1 \text{ et } \mathbb{C}^2.}$$

(d) Notons (e_1, e_2, e_3) la base canonique de $\mathbb{C}^3$.

i. Pour tout $\sigma \in \mathfrak{S}_3$, $\theta_4(\sigma)$ agit sur $\mathbb{C}^3$ en permutant les coordonnées des vecteurs. Si la somme des coordonnées d'un vecteur $v \in \mathbb{C}^3$ est nulle, il en est donc de même de $\theta_4(\sigma)(v)$. Ainsi,

$$\boxed{F \text{ est } \theta_4\text{-invariant.}}$$

ii. Une base de F est $\mathcal{B}_F = (e_1 - e_2,\ e_1 - e_3)$. Pour tout $\sigma \in \mathfrak{S}_3$, on note M_σ la matrice représentative de

$\theta_{4|F}(\sigma)$ dans la base $\mathcal{B}_F$. On a donc :

σ	M_σ
id	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
(1 2)	$\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$
(1 3)	$\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$
(2 3)	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
(1 2 3)	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$
(1 3 2)	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

iii. Posons $v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ et $F' = \mathrm{Vect}(v)$. Les trois coordonnées des éléments de v étant toutes égales, F' est clairement θ_4-invariant. En outre $F' = F^\perp$ donc F et F' sont supplémentaires dans $\mathbb{C}^3$.
En conclusion :

$$\boxed{\mathrm{Vect}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \text{ est un supplémentaire } \theta_4\text{-invariant de } F \text{ dans } \mathbb{C}^3.}$$

12. Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G' \longrightarrow \mathrm{GL}(E)$ deux représentations de G et f un morphisme de représentations de θ vers θ'.
   (a) Pour tout $x \in \ker(f)$ et pour tout $g \in G$, on a :

$$f(\theta(g)(x)) = (f \circ \theta(g))(x) = (\theta'(g) \circ f)(x) = \theta'(g)(f(x)) = \theta'(g)(0_E) = 0_E$$

   donc $\theta(g)(x) \in \ker(f)$.
   Ainsi,

$$\boxed{\ker(f) \text{ est } \theta\text{-invariant.}}$$

   (b) Soit $y \in \mathrm{im}(f)$ et $x \in E$ tel que $f(x) = y$. Pour tout $g \in G$, on a :

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

   donc

$$\boxed{\mathrm{im}(f) \text{ est } \theta'\text{-invariant.}}$$

   (c) Soit $\lambda \in \mathbb{C}$ et $x \in \ker(f - \lambda \mathrm{id}_E)$. On a, pour tout $g \in G$:

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

   donc $\ker(f - \lambda \mathrm{id}_E)$ est θ-invariant.
   En particulier, si on prend pour λ une valeur propre de f, on obtient :

$$\boxed{\text{Les sous-espaces propres de } f \text{ sont } \theta\text{-invariants.}}$$

13. Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G' \longrightarrow \mathrm{GL}(E)$ deux représentations *irréductibles* de G, avec G *fini*, et f un morphisme de représentations de θ vers θ'.

(a) **Lemme de Schur**

i. Puisque $\ker(f)$ est θ-invariant d'après 12.a et que θ est irréductible, on a :

— ou bien $\ker(f) = \{0_E\}$, et f est injective,

— ou bien $\ker(f) = E$, et f est nulle.

D'autre part, $\mathrm{im}(f)$ est θ'-invariant d'après 12.b et θ' est irréductible donc :

— ou bien $\mathrm{im}(f) = \{0_{E'}\}$, et f est nulle,

— ou bien $\mathrm{im}(f) = E'$, et f est surjective.

En conclusion :

$$\boxed{f \text{ est nulle ou bijective.}}$$

ii. Puisque $\mathbb{C}$ est algébriquement clos, f admet une valeur propre λ. L'espace propre $E_\lambda(f)$ associé à la valeur propre λ est θ-invariant d'après 12.c. Puisque $E_\lambda(f) \neq \{0\}$ et que θ est irréductible, on a nécessairement $E_\lambda(f) = E$, c'est-à-dire $f = \lambda \mathrm{id}_E$.
En conclusion :

$$\boxed{\text{Si } \theta = \theta', \text{ alors } f \text{ est une homothétie.}}$$

(b) Soit $h : E \longrightarrow E'$ linéaire.

i. Pour tout $a \in G$, l'application $g \mapsto ag$ est une bijection de G dans G donc, en effectuant le changement de variable $b = ag$, on a :

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

et donc f est bien un morphisme de représentations de θ vers θ'.

ii. Si θ et θ' ne sont pas isomorphes, f n'est pas un isomorphisme et donc, d'après 13.a.i, f est nulle.

iii. La trace étant linéaire et invariante par conjugaison, on a :

$$\mathrm{tr}(f) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\left(\theta(g) \circ h \circ \theta(g^{-1})\right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\left(\theta(g) \circ h \circ \theta(g)^{-1}\right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\,(h) = \mathrm{tr}(h).$$

mais, d'après le lemme de Schur, il existe $\lambda \in \mathbb{C}$ tel que $f = \lambda \mathrm{id}_E$ donc

$$\mathrm{tr}(f) = \lambda \dim E.$$

Ainsi, on a bien :

$$\boxed{f = \frac{\mathrm{tr}(h)}{\dim E} \mathrm{id}_E.}$$

Troisième partie : théorème de Maschke

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

 (a) Puisque E est de dimension finie, il suit du théorème de la base incomplète que tout sous-espace de E admet un supplémentaire. En particulier,

$$\boxed{F \text{ admet un supplémentaire } F'.}$$

 (b) Pour tout $x \in F$, pour tout $g \in G$, on a $\theta(g^{-1})(x) \in F$ donc $p(\theta(g^{-1})(x)) = \theta(g^{-1})(x)$ et donc

$$\theta(g)\left(p(\theta(g^{-1})(x))\right) = \theta(g)\left(\theta(g^{-1})(x)\right) = \underbrace{\theta(g) \circ \theta(g^{-1})}_{=\theta(gg^{-1})=\mathrm{id}_E}(x) = x$$

 et donc,

$$q(x) = \frac{1}{|G|}\sum_{g\in G} x = \frac{|G|}{|G|}x = x.$$

 En conclusion :

$$\boxed{\forall x \in F, \quad q(x) = x.}$$

 (c) La question précédente montre que $F \subset \mathrm{im}(q)$. Par ailleurs, pour tout $x \in E$ et pour tout $g \in G$, $p(\theta(g^{-1})(x)) \in F$ et $\theta(g)(F) \subset F$ donc chaque terme de la somme définissant $q(x)$ est dans F et donc $q(x) \in F$. Ainsi,

$$\boxed{F = \mathrm{im}(q).}$$

 Montrons que F est un projecteur. Pour tout $x \in E$, on a (en omettant les $\circ$ pour alléger) :

$$\begin{aligned}(q \circ q)(x) &= \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\left[\theta(g)p\theta(g^{-1})\theta(h)p\theta(h^{-1})\right](x)\\ &= \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\theta(g)p\theta(g^{-1})\theta(h)\left[p\left(\theta(h^{-1})(x)\right)\right]\end{aligned}$$

 mais, pour tout $h \in G$, $p\left(\theta(h^{-1})(x)\right) \in F$ et F est θ-invariant donc, pour tout $g \in G$,

$$\theta(g^{-1})\theta(h)\left[p\left(\theta(h^{-1})(x)\right)\right] = \theta(g^{-1}h)\left[p\left(\theta(h^{-1})(x)\right)\right] \in F$$

 et donc

$$p\left(\theta(g^{-1})\theta(h)\left[p\left(\theta(h^{-1})(x)\right)\right]\right) = \theta(g^{-1})\theta(h)\left[p\left(\theta(h^{-1})(x)\right)\right]$$

 de sorte que

$$\begin{aligned}(q \circ q)(x) &= \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\underbrace{\theta(g)\theta(g^{-1})}_{=\mathrm{id}_E}\theta(h)\left[p\left(\theta(h^{-1})(x)\right)\right]\\ &= \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G}\theta(h)p\theta(h^{-1})(x)\\ &= \frac{1}{|G|}\sum_{g\in G} q(x)\\ &= q(x).\end{aligned}$$

 Ainsi,

$$\boxed{q \text{ est un projecteur.}}$$

(d) Soit $a \in G$, il suit de 13.b.i que

$$\boxed{q \text{ est un morphisme de représentation de } \theta \text{ vers elle-même.}}$$

(e) Puisque q est un morphisme de représentation de θ vers elle-même, il suit de 12.a que $\ker(q)$ est θ-invariant. Mais puisque q est un projecteur, on sait que

$$E = \mathrm{im}(q) \oplus \ker(q).$$

Or on a montré en 14.d que $\mathrm{im}(q) = F$ donc

$$\boxed{\ker(q) \text{ est un supplémentaire } \theta\text{-invariant de } F.}$$

15. Si $\dim E = 1$, tout sous-espace de E est ou bien réduit au vecteur nul, ou bien égal à E. En particulier, toute représentation $\theta : G \longrightarrow \mathrm{GL}(E)$ est irréductible.

16. On montre le théorème de Maschke par récurrence forte sur la dimension n de E.

Si $n = 1$, le théorème est vrai d'après la question 15.

Soit $n \geq 2$. On suppose que le théorème de Maschke est vrai pour toutes les dimensions $k \in [\![1, n-1]\!]$. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation.

Si elle est irréductible, le théorème de Maschke est vérifié. Sinon, il existe un sous-espace F qui est θ-invariant tel que $1 \leq \dim F \leq n-1$. D'après la question 14, F admet un supplémentaire F' qui est aussi θ-invariant, et on a $\dim F' = n - \dim F \in [\![1, n-1]\!]$. Par hypothèse de récurrence, on peut décomposer $F = F_1 \oplus \cdots \oplus F_r$ et $F' = F'_1 \oplus \cdots \oplus F'_s$ où les F_i et F'_i sont θ-invariants tels que chaque $\theta_{|F_i}$ et $\theta_{|F'_i}$ est irréductible. Comme F et F' sont supplémentaires dans E, on a :

$$E = F_1 \oplus \cdots \oplus F_r \oplus F'_1 \oplus \cdots \oplus F'_s$$

et le théorème de Maschke est vrai en dimension n.

Par récurrence forte :

$$\boxed{\text{On a établi le théorème de Maschke.}}$$

Quatrième partie : le cas des groupes abéliens finis

Soit G un groupe abélien fini d'ordre N.

17. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation irréductible de G d'espace E.

(a) Pour tout $g \in G$, on a $g^N = e_G$ donc

$$\theta(g)^N = \theta(g^N) = \theta(e_G) = \mathrm{id}_E.$$

Il s'ensuit que $X^N - 1$ est un polynôme annulateur de $\theta(g)$ mais

$$X^N - 1 = \prod_{k=0}^{N-1} \left(X - e^{\frac{2ik\pi}{N}}\right)$$

est scindé à racines simples donc

$$\boxed{\text{Pour tout } g \in G,\ \theta(g) \text{ est diagonalisable.}}$$

(b) Puisque G est fini, on note $G = \{g_1, \dots, g_N\}$. Puisque G est abélien et que θ est un morphisme de groupes, les $\theta(g_i)$, avec $i \in [\![1, N]\!]$ commutent. Puisqu'ils sont tous diagonalisables d'après la question 17.a, il suit de la question 4 que les $\theta(g_i)$ admettent une base commune de diagonalisation. En particulier,

$$\boxed{\text{Les } \theta(g), \text{ pour } g \in G, \text{ admettent un vecteur propre commun.}}$$

(c) Notons v le vecteur propre commun à tous les $\theta(g)$. Alors $\mathbb{C}v$ est une droite θ-invariante. Puisque θ est une représentation irréductible et que $\mathbb{C}v \neq \{0\}$, on a $E = \mathbb{C}v$. En particulier,

$$\boxed{E \text{ est de dimension } 1.}$$

18. Si $\dim E = 1$, alors $\mathrm{GL}(E)$ est isomorphe à $\mathrm{GL}(1, \mathbb{C})$ qui est lui-même isomorphe à $\mathbb{C}^*$. En effet, on a un isomorphisme d'algèbres entre $\mathcal{M}_1(\mathbb{C})$ et $\mathbb{C}$ et les éléments inversibles de $\mathbb{C}$ sont les complexes non nuls puisque $\mathbb{C}$ est un corps.

19. Soit $(a, b) \in \hat{G}^2$. Montrons que $a \cdot b \in \hat{G}$. Soit $(g, h) \in G^2$. Par commutativité du produit dans $\mathbb{C}^*$, on a :

$$(a \cdot b)(gh) = a(gh)b(gh) = a(g)a(h)b(g)b(h) = a(g)b(g)a(h)b(h) = (a \cdot b)(g)(a \cdot b)(h)$$

donc $\cdot$ définit bien une loi de composition interne sur $\hat{G}$.
Montrons que cette loi est associative. Soit $(a, b, c) \in \hat{G}^3$ et $g \in G$. On a, par associativité du produit dans $\mathbb{C}^*$:

$$(a \cdot (b \cdot c))(g) = a(g)(b \cdot c)(g) = a(g)(b(g)c(g)) = (a(g)b(g))c(g) = ((a \cdot b)(g))c(g) = ((a \cdot b) \cdot c)(g)$$

donc

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

De la même manière, la commutativité du produit dans $\mathbb{C}^*$ implique que la loi ainsi définie sur $\hat{G}$ est commutative.
Montrons que cette loi admet un élément neutre. Considérons l'application e constante égale à $1_{\mathbb{C}}$. Alors pour tout $a \in \hat{G}$ et pour tout $g \in G$, on a

$$(a \cdot e)(g) = a(g)1_{\mathbb{C}} = a(g)$$

donc $a \cdot e = a$. La loi étant commutative, e est neutre.
Montrons enfin que tout élément de $\hat{G}$ est symétrisable. Soit $a \in \hat{G}$. Pour tout $g \in G$, $a(g) \in \mathbb{C}^*$ donc $\dfrac{1}{a(g)}$ est bien défini dans $\mathbb{C}^*$ et on pose $b : g \mapsto \dfrac{1}{a(g)}$. Alors

$$(a \cdot b)(g) = \frac{a(g)}{a(g)} = 1 = e(g).$$

Ceci étant vrai pour tout g et la loi étant commutative, a et symétrisable, de symétrique b.
En conclusion

$$\boxed{(\hat{G}, \cdot) \text{ est un groupe abélien.}}$$

20. On suppose que $G = \mathbb{Z}/n\mathbb{Z}$.

(a) Pour tout $(k, \ell) \in \mathbb{Z}^2$, on a

$$\alpha_1(\bar{k} + \bar{\ell}) = \alpha_1(\overline{k + \ell}) = e^{\frac{2i(k+\ell)\pi}{n}} = e^{\frac{2ik\pi}{n}} e^{\frac{2i\ell\pi}{n}} = \alpha_1(\bar{k})\alpha_1(\bar{\ell})$$

donc α_1 est un caractère sur $\mathbb{Z}/n\mathbb{Z}$.

(b) Soit $\alpha \in \hat{G}$. Puisque $\bar{1}$ est d'ordre n dans $\mathbb{Z}/n\mathbb{N}$, on a $1_{\mathbb{C}} = \alpha(\bar{n}) = \alpha(\bar{1})^n$ donc $\alpha(\bar{1})$ est une racine n-ième de l'unité. On peut donc écrire $\alpha(\bar{1}) = e^{\frac{2ik\pi}{n}}$, avec $k \in [\![0, n-1]\!]$. Alors

$$\alpha(\bar{1}) = \alpha_1(\bar{1})^k.$$

En outre, pour tout $m \in \mathbb{Z}$, on a
$$\alpha(\bar{m}) = \alpha(\bar{1})^m = \alpha_1(\bar{1})^{km} = \alpha_1(\bar{m})^k$$
donc
$$\alpha = \alpha_1^k$$
de sorte que $\hat{G} \subset \langle \alpha_1 \rangle$. L'inclusion réciproque étant trivialement vérifiée, on a :
$$\boxed{\hat{G} = \langle \alpha_1 \rangle\,.}$$
Il reste à observer que α_1 est d'ordre n. En effet, $\alpha_1^n = \mathbb{1}_C$ et comme $\alpha_1(\bar{1}) = e^{\frac{2i\pi}{n}}$ est d'ordre n dans $\mathbb{C}^*$, il n'existe pas de $d \in [\![1, n-1]\!]$ tel que $\alpha_1^d = \mathbb{1}_C$. Alors $\hat{G}$ est engendré par un élément d'ordre n donc :
$$\boxed{\hat{G} \text{ est cyclique d'ordre } n.}$$

21. Tous les éléments de $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont d'ordre 2 donc, si α est un caractère sur G, il est à valeurs dans $\{-1_{\mathbb{C}}, 1_C\}$. Puisque G est engendré par $(\bar{0}, \bar{1})$ et $(\bar{1}, \bar{0})$, il suffit de choisir les images de ces deux éléments pour déterminer un morphisme de G vers $\mathbb{C}^*$. On a donc quatre tels morphismes.
Ainsi, $\hat{G}$ est un groupe à quatre éléments, dont tous les éléments sont d'ordre 2. Il est donc isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.
En conclusion :
$$\boxed{\hat{G} \simeq G.}$$

Cinquième partie : prolongement des caractères et théorème de Kronecker

Soit G un groupe abélien fini.

22. Soit H un sous-groupe de G et $\alpha \in \hat{H}$.
    (a) On suppose $H \neq G$, on fixe $x \in G \setminus H$ et on considère le sous-groupe engendré par H et x. Il contient tous les produits finis d'éléments de H et de puissances de x. Puisque G est abélien, on peut regrouper les facteurs issus de H et les puissances de x et il vient :
    $$K = \{x^p h \mid p \in \mathbb{Z},\ h \in H\}\,.$$
    Considérons l'application
    $$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & K/H \\ p & \mapsto & x^p H \end{array} \right. .$$
    C'est un morphisme de groupes surjectif d'après l'observation précédente. Il n'est pas injectif car K/H est fini, comme quotient d'un groupe fini. Ainsi, il existe $r \in \mathbb{N}^*$ tel que $\ker(\varphi) = r\mathbb{Z}$. D'après le premier théorème d'isomorphisme, φ induit un isomorphisme de $\mathbb{Z}/r\mathbb{Z}$ vers K/H. Enfin, on observe que K/H est non nul car $x \notin H$.
    En particulier,
    $$\boxed{K/H \text{ est un groupe cyclique non nul.}}$$
    (b) Soit $g \in K$ et supposons qu'il existe $h, h' \in H$ et p, q entiers tels que $g = hx^p$ et $g = h'x^q$. Alors $x^{p-q} = h'h^{-1} \in H$. Donc, si on note π la projection canonique de K vers K/H, on a $\pi(x^{p-q}) = 0$ mais $\pi(x^{p-q}) = \pi(x)^{p-q}$ et $K/H \simeq \mathbb{Z}/r\mathbb{Z}$ donc r divise $p-q$, c'est-à-dire $q \equiv p\ [r]$. D'après le théorème de division euclidienne,
    $$\boxed{\text{Pour tout } g \in K, \text{ il existe un unique } p \in [\![0, r-1]\!] \text{ tel que } g = hx^p.}$$

(c) Si on note ψ l'isomorphisme entre K/H et $\mathbb{Z}/r\mathbb{Z}$, on a

$$\psi(x^r) = r\psi(x) = \bar{0}$$

donc, toujours en notant $\pi : K \longrightarrow K/H$ la projection canonique, on a $\pi(x^r) = 0_{K/H}$, c'est-à-dire $x^r \in H$. Ainsi,

$$\boxed{x^r \in H.}$$

(d) **NB :** *Il semblerait qu'il y ait une erreur d'énoncé, au lieu de $\omega^r = z$, z n'étant pas défini, on va choisir ω tel que $\omega^r = 1$, ce qui suffit pour achever la démonstration.*
Soit $(g, g') \in K^2$. On écrit $g = hx^p$ et $g' = h'x^q$ avec $(h, h') \in H^2$ et $(p, q) \in [\![0, r-1]\!]^2$. On a alors

$$\tilde{\alpha}(gg') = \tilde{\alpha}(hx^p h' x^q) = \tilde{\alpha}((hh')x^{p+q})$$

mais $\omega^r = 1$ donc ω^{p+q} ne dépend que du reste modulo r de $p+q$. Ainsi, on a

$$\tilde{\alpha}(gg') = \alpha(hh')\omega^{p+q} = \alpha(h)\alpha(h')\omega^p\omega^q = \alpha(h)\omega^p\alpha(h')\omega^q = \tilde{\alpha}(hx^p)\tilde{\alpha}(h'x^q) = \tilde{\alpha}(g)\tilde{\alpha}(g').$$

Il s'ensuit que α est un caractère sur H.
Par ailleurs, pour tout $h \in H$, on a

$$\tilde{\alpha}(h) = \tilde{\alpha}(hx^0) = \alpha(h)\omega^0 = \alpha(h)$$

donc $\tilde{\alpha}$ prolonge bien α.
Ainsi,

$$\boxed{\tilde{\alpha} \in \hat{K} \text{ et } \tilde{\alpha}_{|H} = \alpha.}$$

(e) Fixons un caractère $\alpha \in \hat{H}$. On raisonne par récurrence sur l'indice de H dans G.
Si cet indice est nul, il n'y a rien à montrer car $H = G$.
Sinon, on choisit un élément $x \notin H$ et on pose K le sous-groupe de G engendré par x et par H. D'après les questions précédentes, α se prolonge en $\tilde{\alpha} \in \hat{K}$.
D'autre part, puisque $x \notin H$, l'indice de K dans G est strictement inférieur à celui de H. Par hypothèse de récurrence, on peut donc supposer que tout caractère sur K se prolonge en un caractère sur G. En particulier, il existe $\hat{\alpha} \in \hat{G}$ qui prolonge $\tilde{\alpha}$, et donc qui prolonge α.
En conclusion :

$$\boxed{\text{Tout caractère de } \hat{H} \text{ se prolonge en un caractère de } \hat{G}.}$$

23. (a) Si G est cyclique, G est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$, avec $n \in \mathbb{N}$. On a alors vu à la question 20 que $\hat{G}$ est cyclique d'ordre n. En particulier,

$$\boxed{\text{Si } G \text{ est cyclique, alors } \hat{G} \simeq G.}$$

(b) L'application

$$\theta : \left\{ \begin{array}{ccc} \hat{G} & \longrightarrow & \hat{H} \\ \alpha & \longmapsto & \alpha_{|H} \end{array} \right.$$

est bien définie car la restriction d'un morphisme de groupes à un sous-groupe est un morphisme de groupes. Il s'agit clairement d'un morphisme de groupes, et θ est surjectif d'après le théorème de prolongement établi à la question 22.

(c) Soit $(a, b) \in G$ tels que $\overline{a} = \overline{b}$ dans G/H. On a $ab^{-1} \in H$ donc $\alpha(ab^{-1}) = 1$ et donc $\alpha(a) = \alpha(b)$ de sorte que $\overline{\alpha}$ est bien défini.
Puisque $\alpha \in \ker(\theta)$, on a $H \subset \ker(\alpha)$ et α passe bien au quotient en un morphisme de groupes de G vers $\mathbb{C}^*$.

Ainsi :

$$\boxed{\forall \alpha \in \ker(\theta), \quad \bar{\alpha} \in \widehat{G/H}.}$$

(d) Considérons le morphisme de groupes

$$\Phi : \left\{ \begin{array}{ccc} \ker(\theta) & \longrightarrow & \widehat{G/H} \\ \alpha & \mapsto & \bar{\alpha}. \end{array} \right.$$

Si $\alpha \in \ker(\Phi)$, on a $\bar{\alpha} = 1$ mais $\alpha \in \ker(\theta)$ donc $\alpha_{|H} = 1$ et donc $\alpha = 1$. Ainsi, Φ est injectif.
Soit $\beta \in \widehat{G/H}$. Considérons l'application $\gamma : G \longrightarrow \mathbb{C}^*$ par $\gamma(g) = \beta(\bar{g})$. C'est un caractère sur G qui vérifie $\gamma_{|H} = 1$ donc c'est un élément de $\ker(\theta)$. En outre, on a $\beta = \bar{\gamma} = \Phi(\gamma)$ donc Φ est surjectif.
En conclusion,

$$\boxed{\ker(\theta) \text{ est isomorphe à } \widehat{G/H}.}$$

(e) Montrons par récurrence forte sur l'ordre de G que $\left|\hat{G}\right| = |G|$.
Si G est le groupe trivial, le résultat est vrai.
Si G est cyclique, le résultat suit de 23.a. Sinon, soit $x \in G \setminus \{e\}$ et $H = \langle x \rangle$. On a donc $1 < |H| < |G|$ et $|G/H| < |G|$. Avec les notations précédentes, on sait que $\widehat{G/H} \simeq \ker(\theta)$ donc

$$\left|\widehat{G/H}\right| = |\ker(\theta)|\,.$$

Mais, d'après le premier théorème d'isomorphisme, on a

$$\widehat{G}/\ker(\theta) \simeq \mathrm{im}(\theta) \subset \widehat{H}$$

donc, en passant au cardinal, on a :

$$\frac{\widehat{G}}{|\ker(\theta)|} \leq \left|\widehat{H}\right|.$$

Alors, par hypothèse de récurrence forte, il vient

$$\frac{\widehat{G}}{\left|\widehat{H}\right|} \leq |\ker\theta| = \left|\widehat{G/H}\right| = |G/H| = \frac{|G|}{|H|}$$

mais, toujours par hypothèse de récurrence, on a $|H| = \left|\hat{H}\right|$ donc $|G| = \left|\hat{G}\right|$.
En conclusion :

$$\boxed{\text{Si } G \text{ est abélien fini, } |G| = \left|\hat{G}\right|.}$$

24. Soit G un groupe abélien fini, $N = \exp(G)$, x un élément de G d'ordre N et $H = \langle x \rangle$.

(a) Soit

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

Alors α définit bien un caractère sur H et celui-ci est injectif car x est d'ordre N.
Ainsi,

$$\boxed{\text{Il existe } \alpha \in \hat{H} \text{ injectif.}}$$

(b) D'après le théorème de prolongement établi à la question 22,

$$\boxed{\text{Il existe } \beta \in \hat{G} \text{ tel que } \beta_{|H} = \alpha.}$$

(c) Pour tout $h \in H$, on a $h \in G$ et $\alpha(h) = \beta(h) \in \beta(G)$ donc $\alpha(H) \subset \beta(G)$.
Aussi, par construction de α à la question 23.a, on a $\alpha(H) = \mathbb{U}_N = \left\{z \in \mathbb{C} \,\middle|\, z^N = 1\right\}$.
Par ailleurs, pour tout $g \in G$, l'ordre de g divise l'exposant de G sont $g^N = e_G$ et donc $\beta(g)^N = \beta(g^N) = \beta(e_G) = 1$ de sorte que $\beta(G) \subset \mathbb{U}_N$.
En conclusion, on a bien :

$$\boxed{\beta(G) = \alpha(G) = \mathbb{U}_N.}$$

(d) Soit $x \in \ker(\beta)$. On a $x \in G$ donc $x^N = e_G$. Ainsi l'ordre de x divise N, pour tout $x \in \ker(\beta)$. Le PPCM des ordres des éléments de $\ker(\beta)$ divise donc lui aussi N, c'est-à-dire :

$$\boxed{\exp(\ker(\beta)) \text{ divise } N.}$$

(e) Considérons l'application

$$\varphi : \left\{ \begin{array}{rcl} H \times \ker(\beta) & \longrightarrow & G \\ (h, g) & \longmapsto & hg. \end{array} \right.$$

On vérifie immédiatement que c'est un morphisme de groupes.
φ est injectif car, si $(h, g) \in H \times \ker(\beta)$ vérifie $\varphi(h, g) = e_G$, alors $g = h^{-1} \in H \cap \ker(\beta)$. Or, pour $a \in H \cap \ker(\beta)$, on a $\beta(a) = \alpha(a) = 1$ mais α est injective donc $a = e_G$. Ainsi,

$$H \cap \ker(\beta) = \{e_G\}$$

et donc φ est injectif.
D'autre part, il suit du premier théorème d'isomorphisme que β induit un isomorphisme

$$\bar{\beta} : G/\ker(\beta) \longrightarrow \mathrm{im}(\beta) = \mathbb{U}_N$$

donc

$$\frac{|G|}{|\ker(\beta)|} = |\mathbb{U}_N| = N = |H|$$

de sorte que

$$|H \times \ker(\beta)| = |G|.$$

Par cardinalité, φ est bijectif ; c'est donc un isomorphisme.
Ainsi,

$$\boxed{G \text{ est isomorphe à } H \times \ker(\beta).}$$

(f) On commence par observer que si G est cyclique, alors G est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$ donc le théorème est vérifié.
Raisonnons maintenant par récurrence forte sur l'ordre de G.
Si $|G| = 2$, alors $G \simeq \mathbb{Z}/2\mathbb{Z}$ et le théorème est vérifié.
Soit G un groupe abélien non cyclique d'ordre d supérieur ou égal à 3. Supposons que le théorème de Kronecker est vérifié pour tous les ordres strictement inférieurs à d. Considérons dans x un élément d'ordre $\exp(G)$ et posons $H = \langle x \rangle$.
Puisque G n'est pas cyclique, et que G est un groupe non trivial, on peut affirmer que $1 < |H| < |G|$. Il suit alors de 24.e que G est isomorphe au produit direct $H \times \ker(\beta)$, mais $|\ker(\beta)| = [G : H]$ donc $1 < |\ker(\beta)| < |G|$.
En appliquant le théorème de Kronecker à $\ker(\beta)$, il existe des entiers $N_2, \ldots, N_k$ tels que N_k divise $N_{k-1}, \ldots, N_3$ divise N_2 tel que

$$\ker(\beta) \simeq \mathbb{Z}/N_2\mathbb{Z} \times \cdots \times \mathbb{Z}/N_k\mathbb{Z}$$

mais comme $H = \langle x \rangle$ et que x est d'ordre N, on a

$$H \simeq \mathbb{Z}/N\mathbb{Z}$$

donc

$$G \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N_2\mathbb{Z} \times \cdots \times \mathbb{Z}/N_k\mathbb{Z}.$$

Il reste alors à observer que N_2 divise $\exp(\ker(\beta))$ et, d'après 24.d, $\exp(\ker(\beta))$ divise N. Ainsi, N_2 divise N et on a bien la décomposition de Kronecker de G.
En conclusion,

$$\boxed{\text{Le théorème de Kronecker est démontré.}}$$

25. Commençons par calculer l'exposant de $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. Puisque $|G| = 90$, on sait que $\exp(G)$ est un diviseur de 90. On observe que $(1, 1)$ est d'ordre 30 dans G donc $\exp(G)$ est un multiple de 30. Il ne peut donc s'agir que de 30 ou de 90 lui-même. Mais G ne contient aucun élément d'ordre 90 car $60(a, b) = (0, 0)$ pour tout élément (a, b) de $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. Ainsi, l'exposant de G est égal à 30.
En choisissant un élément x d'ordre 30 et en posant $H = \langle x \rangle$, le raisonnement établi à la question 24 montre que

$$G \simeq \mathbb{Z}/30\mathbb{Z} \times \ker(\beta)$$

et $|\ker(\beta)| = 3$ donc $\ker(\beta) \simeq \mathbb{Z}/3\mathbb{Z}$.
En conclusion, la décomposition de Kronecker recherchée est :

$$\boxed{\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.}$$

Sixième partie : applications centrales

26. (a) L'application nulle, comme toute application constante $G \longrightarrow \mathbb{C}$, est centrale. Soient $f_1, f_2 \in C(G)$ et $\lambda \in \mathbb{C}$. Alors pour tout $(g, h) \in G^2$, on a

$$(\lambda f_1 + f_2)(gh) = \lambda f_1(gh) + f_2(gh) = \lambda f_1(hg) + f_2(hg) = (\lambda f_1 + f_2)(hg)$$

donc $\lambda f_1 + f_2 \in C(G)$.
Ainsi,

$$\boxed{C_G \text{ est un sous-espace vectoriel de l'ensemble des applications de } G \text{ dans } \mathbb{C}.}$$

(b) Soit $\lambda \in C(G)$. Soit $h \in G$. Alors pour tout $g \in G$, on a

$$f(g^{-1}hg) = f(hgg^{-1}) = f(h)$$

donc f est constante sur la classe de conjugaison de h.
Réciproquement, soit $f : G \longrightarrow \mathbb{C}$ une application constante sur les classes de conjugaison et soit $(g, h) \in G^2$. On a $g^{-1}(gh)g = hg$ donc gh et hg sont conjugués, de sorte que $f(gh) = f(hg)$, et f est centrale.
Ainsi,

$$\boxed{f : G \longrightarrow \mathbb{C} \text{ est centrale si, et seulement si, elle est constante sur chaque classe de conjugaison.}}$$

(c) La relation de conjugaison est une relation d'équivalence sur G. Les classes de conjugaison forment donc une partition de G. Puisque G est fini, elles sont en nombre fini et on pose

$$G = \bigsqcup_{i=1}^{r} \Gamma_i,$$

les Γ_i étant les classes de conjugaison.
Alors, pour tout $i \in [\![1, r]\!]$, f est constante égale à un scalaire x_i sur Γ_i de sorte que

$$f = \sum_{i=1}^{r} x_i \iota_{\Gamma_i}.$$

La famille $(\iota_{\Gamma_1}, \dots, \iota_{\Gamma_r})$ est donc génératrice de $C(G)$.
Montrons qu'elle est libre. Soit $(x_1, \dots, x_r) \in \mathbb{C}^r$ tel que

$$0 = \sum_{i=1}^{r} x_i \iota_{\Gamma_i}.$$

Soit $j \in [\![1, r]\!]$ et $g_j \in \Gamma_j$. En évaluant en g_j, on a :

$$0 = \sum_{i=1}^{r} x_i \underbrace{\iota_{\Gamma_i}(g_j)}_{=\delta_{i,j}} = x_j.$$

Ceci étant vrai pour tout $j \in [\![1, r]\!]$, la famille $(\iota_{\Gamma_1}, \dots, \iota_{\Gamma_r})$ est libre, c'est donc une base de $C(G)$.
En particulier,

$$\boxed{\dim C(G) \text{ est égale au nombre de classes de conjugaison dans } G.}$$

27. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation de G.
   (a) Soit $(g, h) \in G^2$, on a d'après 1.e,

$$\chi_\theta(gh) = \mathrm{tr}(\theta(gh)) = \mathrm{tr}(\theta(g)\theta(h)) = \mathrm{tr}(\theta(h)\theta(g)) = \mathrm{tr}(\theta(hg)) = \chi_\theta(hg)$$

   donc

$$\boxed{\chi_\theta \in C(G).}$$

   (b) Comme en 17.a, si $N = |G|$, pour tout $g \in G$, on a :

$$\theta(g)^N = \theta(g^N) = \theta(e_G) = \mathrm{id}_E$$

   donc $X^N - 1$ annule $\theta(g)$ de sorte que $\theta(g)$ est diagonalisable et

$$\mathrm{Sp}(\theta(g)) \subset \mathbb{U}_N = \left\{ e^{\frac{2ik\pi}{N}} \;\middle|\; k \in [\![0, N-1]\!] \right\}.$$

   Pour tout $k \in [\![0, N-1]\!]$, on note n_k la multiplicité géométrique de $e^{\frac{2ik\pi}{N}}$ comme valeur propre de $\theta(g)$, avec la convention que $n_k = 0$ si $e^{\frac{2ik\pi}{N}}$ n'est pas valeur propre.
   En diagonalisant $\theta(g)$, on voit que les valeurs propres de $\theta(g)^{-1}$ sont les inverses des valeurs propres de $\theta(g)$, avec la même multiplicité géométrique. En particulier, on a :

$$\chi_\theta(g^{-1}) = \mathrm{tr}(\theta(g^{-1})) = \sum_{i=0}^{N-1} n_i e^{-\frac{2ik\pi}{N}} = \sum_{i=0}^{N-1} n_i \overline{e^{\frac{2ik\pi}{N}}} = \overline{\sum_{i=0}^{N-1} n_i e^{\frac{2ik\pi}{N}}} = \overline{\mathrm{tr}(\theta(g))} = \overline{\chi_\theta(g)}.$$

   Ainsi,

$$\boxed{\forall g \in G, \quad \chi_\theta(g^{-1}) = \overline{\chi_\theta(g)}.}$$

28. La forme est clairement hermitienne. Vérifions qu'elle est définie positive. Pour tout $\lambda \in C(G)$, on a

$$\langle \lambda, \lambda \rangle = \frac{1}{|G|} \sum_{g \in G} |\lambda(g)|^2 \geq 0$$

avec égalité si, et seulement si, $\lambda(g) = 0$, pour tout $g \in G$, c'est-à-dire si, et seulement si, $\lambda = 0$.
Ainsi,

$$\boxed{\langle -, - \rangle \text{ est une forme hermitienne définie positive sur } C(G).}$$

29. (a) On a

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

(b) D'après les formules de représentation matricielle des compositions, on a

$$Y = \frac{1}{|G|} \sum_{g \in G} M_{\mathcal{B}'}(\theta'(g)) X M_{\mathcal{B}}(\theta(g^{-1}))$$

donc, pour tout $(i, j) \in [\![1, n']\!] \times [\![1, n]\!]$, il suit des formules du produit matriciel que :

$$\begin{aligned}
y_{i,j} &= \frac{1}{|G|} \sum_{g \in G} \sum_{k=1}^{n'} a'_{i,k}(g) [X M_{\mathcal{B}}(\theta(g^{-1}))]_{k,j} \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{k=1}^{n'} \sum_{\ell=1}^{n} a'_{i,k}(g) x_{k,\ell} a_{\ell,j}(g^{-1}).
\end{aligned}$$

(c) Comme θ et θ' sont irréductibles et non isomorphes, le lemme de Schur affirme que tout morphisme de représentations de θ vers θ' est nul. D'autre part, il suit de 13.b.i que f est un morphisme de représentations, on a donc $f = 0$. En particulier, chaque coefficient de Y est nul. En faisant varier h parmi les applications linéaires canoniquement associées aux matrices de la base canonique de $\mathcal{M}_{n',n}(\mathbb{C})$, il vient :

$$\boxed{\forall (i, j) \in [\![1, n']\!]^2, \forall (k, \ell) \in [\![1, n]\!]^2, \quad \frac{1}{|G|} \sum_{g \in G} a'_{i,h}(g) a_{k,\ell}(g^{-1}) = 0.}$$

En injectant dans l'expression trouvée en 28.a et en utilisant 27.c, on obtient :

$$\boxed{\langle \chi_{\theta'}, \chi_\theta \rangle = 0.}$$

(d) i. Si $E = E'$, $\theta = \theta'$ et $\mathcal{B} = \mathcal{B}'$, le lemme de Schur affirme que pour tout morphisme de représentation f de θ vers θ', il existe $\lambda \in \mathbb{C}$ tel que $f = \lambda \mathrm{id}_E$. En particulier $Y = \lambda I_n$. En reprenant le raisonnement de la question précédente, on obtient l'égalité demandée.

ii. De même, en injectant dans l'expression trouvée en 28.a et en utilisant 27.c, on obtient :

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

(e) D'après les questions 27.c et 27.d, la famille $(\chi_{\theta_i})_{1\le i\le k}$ est orthonormée dans $C(G)$ pour le produit hermitien défini à la question 28. Il s'ensuit qu'il s'agit d'une famille libre dans $C(G)$.

En particulier, son cardinal ne peut excéder la dimension de $C(G)$, qui est égal au nombre de classes de conjugaison de G d'après 26.c.

En conclusion, si G possède r classes de conjugaison,

> Le nombre de représentations irréductibles de G (à isomorphisme près) est inférieur ou égal à r.

30. Si G est abélien, pour tout $(g,h) \in G^2$, on a $g^{-1}hg = h$ donc les classes de conjugaison sont des singletons. En conséquence, G possède $|G|$ classes de conjugaison. Il y a donc au plus $|G|$ représentations irréductibles de G.

D'autre part, puisque G est abélien, il suit de la question 23 que $\left|\hat{G}\right| = |G|$. Il y a donc au moins $|G|$ caractères distincts sur G, et donc au moins $|G|$ représentations irréductibles de G à isomorphismes près.

En conclusion,

> Si G est abélien, il y a exactement $|G|$ représentations irréductibles de G à isomorphismes près.

31. **NB :** *La question n'est pas très claire faute d'introduction des notations. Je suppose que θ et θ' sont deux représentations irréductibles de G.*

θ et θ' étant isomorphes, on a $\chi_\theta = \chi_{\theta'}$. En effet, si f est un isomorphisme de représentation de θ vers θ', alors pour tout $g \in G$, la matrice de $\theta(g)$ dans une base $(e_1, \dots, e_n)$ de E est égale à la matrice de $\theta'(g)$ dans une base $(f(e_1), \dots, f(e_n))$ de E, donc $\mathrm{tr}(\theta(g)) = \mathrm{tr}(\theta'(g))$. Il s'ensuit que $\chi_\theta = \chi_{\theta'}$.

Il suit alors de 29.d.ii que :

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

Ainsi, on a établi :

> Si θ et θ' sont isomorphes et irréductibles, alors $\langle \chi_\theta, \chi_{\theta'} \rangle = 1$.

32. (a) Les F_i étant θ-invariants, en se plaçant dans une base adaptée à $E = F_1 \oplus \cdots F_k$, la matrice de chaque $\theta(g)$ est diagonale par blocs correspondant aux $\theta(g)_{|F_i}$ donc

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

Ainsi,

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

(b) On a

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

mais, il suit des questions 29.c et 31 que $\left\langle \chi_{\theta'}, \chi_{\theta_{|F_i}} \right\rangle$ vaut 1 si $\theta_{|F_i}$ est isomorphe à θ' et 0 sinon. Ainsi,

> $\langle \chi_{\theta'}, \chi_\theta \rangle$ est égal au nombre de F_i tels que $\theta_{|F_i}$ est isomorphe à θ'.

33. Si θ et θ' sont isomorphes, on montre que $\chi_\theta = \chi_{\theta'}$ par récurrence sur le nombre de facteurs dans la décompositions de E en sous-espaces irréductibles θ-invariants (resp. θ'-invariants) à partir de la question 32.a.

Réciproquement, supposons $\chi_\theta = \chi_{\theta'}$. Considérons deux décompositions

$$E = F_1 \oplus \cdots F_k \quad \text{et} \quad E = F'_1 \oplus \cdots F'_\ell$$

de sorte que les F_i (resp. les F'_i) soient θ-invariants (resp. θ'-invariants) et irréductibles. Soit θ'' une représentation irréductible. Puisque

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

il suit de 32.a que chacune des deux décompositions contient le même nombre de facteurs F_i (resp. F'_i) tels que $\theta_{|F_i}$ (resp. $\theta_{|F'_i}$) sont isomorphes à θ''. Ceci étant vrai pour toute représentation irréductible θ'', les représentations θ et θ' sont isomorphes.

En conclusion,

$$\boxed{\theta \text{ et } \theta' \text{ sont isomorphes si, et seulement si, } \chi_\theta = \chi_{\theta'}.}$$

*** Fin du sujet ***