ISM MP, Mathématiques
Année 2024/2025 20/03/2025

Corrigé du devoir en temps libre n°16

Problème I

1. On a $$\boxed{\forall \sigma \in \mathrm{S}_n \qquad \mathrm{M}_\sigma = \mathrm{mat}_{\mathscr{C}} f_\sigma}$$

Puis $$\forall (j,k) \in [\![1\,;\, n]\!]^2 \qquad \sum_{i=1}^{n} \delta_{i,\sigma(j)}\delta_{i,\sigma(k)} = \delta_{\sigma(j),\sigma(k)} = \delta_{j,k}$$

ce qui prouve que les colonnes de M_σ forment une base orthonormée de $\mathbb{R}^n$. Ainsi

$$\boxed{\text{Pour } \sigma \in \mathrm{S}_n, \text{ la matrice } \mathrm{M}_\sigma \text{ est orthogonale.}}$$

2. Soit $(\sigma, \gamma) \in \mathrm{S}_n^2$. On a

$$\mathrm{mat}_{\mathscr{C}} \sigma \circ \gamma = (\mathrm{mat}_{\mathscr{C}} \sigma)\,(\mathrm{mat}_{\mathscr{C}} \gamma)$$

Ainsi $$\boxed{\forall (\sigma, \gamma) \in \mathrm{S}_n^2 \qquad \mathrm{M}_\sigma \mathrm{M}_\gamma = \mathrm{M}_{\sigma\circ\gamma}}$$

3. On note U la colonne de $\mathscr{M}_{n,1}(\mathbb{R})$ constituée de 1. Pour $\sigma \in \mathrm{S}_n$, on trouve

$$\forall i \in [\![1\,;\, n]\!] \qquad (\mathrm{M}_\sigma \mathrm{U})_i = \sum_{j=1}^{n} \delta_{i,\sigma(j)} = 1$$

Le vecteur u est donc vecteur propre de f_σ pour la valeur propre 1 et comme on a $f_\sigma \in \mathcal{O}(\mathbb{R}^n)$ puisque sa matrice dans la base $\mathscr{C}$ est orthogonale avec $\mathscr{C}$ base orthonormée de $\mathbb{R}^n$, on conclut

$$\boxed{\text{Pour } \sigma \in \mathrm{S}_n, \text{ les sous-espaces } \mathrm{Vect}\,(u) \text{ et } \mathrm{Vect}\,(u)^\perp \text{ sont stables par } f_\sigma.}$$

4. On pose $\varepsilon_1 = \dfrac{1}{\sqrt{n}} u$ que l'on complète en $\mathscr{B} = (\varepsilon_1, \ldots, \varepsilon_n)$ base orthonormée de $\mathbb{R}^n$ et on pose $\mathrm{P} = \mathrm{mat}_{\mathscr{C}} \mathscr{B}$. La matrice P est orthogonale en tant que matrice de passage entre deux bases orthonormées de $\mathbb{R}^n$. Par ailleurs, on a d'après le résultat de la question précédente

$$\forall \sigma \in \mathrm{S}_n \qquad \mathrm{Vect}\,(\varepsilon_1) = \mathrm{E}_1(f_\sigma) \qquad f_\sigma(\mathrm{Vect}\,(\varepsilon_1)^\perp) \subset \mathrm{Vect}\,(\varepsilon_1)^\perp$$

Enfin pour $\sigma \in \mathrm{S}_n$, l'endomorphisme g_σ induit par l'isométrie f_σ sur $\mathrm{Vect}\,(\varepsilon_1)^\perp = \mathrm{Vect}\,(\varepsilon_2, \ldots, \varepsilon_n)$ est une isométrie dont la matrice A_σ dans la base orthonormée $(\varepsilon_2, \ldots, \varepsilon_n)$ de $\mathrm{Vect}\,(\varepsilon_1)$ est orthogonale et on conclut donc

$$\boxed{\exists \mathrm{P} \in \mathcal{O}_n(\mathbb{R}) \quad | \quad \forall \sigma \in \mathrm{S}_n \qquad \mathrm{P}^\top \mathrm{M}_\sigma \mathrm{P} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \mathrm{A}_\sigma \end{array}\right) \quad \text{avec} \quad \mathrm{A}_\sigma \in \mathcal{O}_{n-1}(\mathbb{R})}$$

5. On pose $$\forall \sigma \in \mathrm{S}_n \qquad \varphi(\sigma) = \mathrm{P} \left(\begin{array}{c|c} \det \mathrm{A}_\sigma & 0 \\ \hline 0 & \mathrm{A}_\sigma \end{array}\right) \mathrm{P}^\top$$

Soit $(\sigma, \gamma) \in \mathrm{S}_n^2$. Un produit par bloc donne

$$\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \mathrm{A}_\sigma \mathrm{A}_\gamma \end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \mathrm{A}_\sigma \end{array}\right) \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \mathrm{A}_\gamma \end{array}\right) = \mathrm{P}^\top \mathrm{M}_\sigma \mathrm{P} \mathrm{P}^\top \mathrm{M}_\gamma \mathrm{P} = \mathrm{P}^\top \mathrm{M}_{\sigma\circ\gamma} \mathrm{P} = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & \mathrm{A}_{\sigma\circ\gamma} \end{array}\right)$$

Par conséquent

$$\varphi(\sigma\circ\gamma) = \mathrm{P}\left(\begin{array}{c|c} \det(\mathrm{A}_\sigma\mathrm{A}_\gamma) & 0 \\ \hline 0 & \mathrm{A}_\sigma\mathrm{A}_\gamma \end{array}\right)\mathrm{P}^\top$$
$$= \mathrm{P}\left(\begin{array}{c|c} \det \mathrm{A}_\sigma & 0 \\ \hline 0 & \mathrm{A}_\sigma \end{array}\right)\mathrm{P}^\top\mathrm{P}\left(\begin{array}{c|c} \det \mathrm{A}_\gamma & 0 \\ \hline 0 & \mathrm{A}_\gamma \end{array}\right)\mathrm{P}^\top = \varphi(\sigma)\varphi(\gamma)$$

Enfin, l'application $\mathrm{S}_n \to \mathcal{O}_{n-1}(\mathbb{R}), \sigma \to \mathrm{A}_\sigma$ est injective et on conclut

$$\boxed{\text{On peut plonger } \mathrm{S}_n \text{ dans } \mathcal{SO}_n(\mathbb{R}).}$$

Problème II

1. On a
$$\sum_{k\in[\![1\,;n]\!]}\omega^k = \sum_{d|n}\left(\sum_{k\wedge n=d}\omega^k\right)$$

Or, pour $k \in [\![1\,;n]\!]$ et d diviseur de n, on observe

$$k\wedge n = d \iff \exists!\ell\in[\![1\,;n/d]\!] \mid k = d\ell \quad\text{et}\quad \ell\wedge(n/d)=1$$

Ainsi
$$\sum_{d|n}\left(\sum_{k\wedge n=d}\omega^k\right) = \sum_{d|n}\left(\sum_{\ell\in[\![1\,;n/d]\!],\ \ell\wedge(n/d)=1}\mathrm{e}^{\frac{2\mathrm{i}d\ell\pi}{dn/d}}\right) = \sum_{d|n}\mathrm{M}\left(\frac{n}{d}\right)$$

Enfin, l'application $d \mapsto n/d$ réalise une permutation sur l'ensemble des diviseurs de n (involutive) et on conclut

$$\boxed{\sum_{k=1}^{n}\omega^k = \sum_{d|n}\mathrm{M}\left(\frac{n}{d}\right) = \sum_{d|n}\mathrm{M}(d)}$$

2. Soit $n \geqslant 2$ et d diviseur de n. Si d admet un facteur carré, alors $\mu(d) = 0$. Sinon, d peut s'écrire comme produit de k facteurs pris parmi les r facteurs premiers de n, ce qui signifie donc $\binom{r}{k}$ choix possibles et ce pour $k \in [\![0\,;r]\!]$. Ainsi, on conclut

$$\sum_{d|n}\mu(d) = \sum_{k=0}^{r}\binom{r}{k}(-1)^k = (1-1)^r = 0$$

3. D'après le résultat de la première question, pour n entier non nul, on a

$$\sum_{d|n}\mathrm{M}(d) = \sum_{k=1}^{n}\omega^k = \begin{cases}1 & \text{si } n=1\\ 0 & \text{sinon}\end{cases}$$

On en déduit $\mu(1) = \mathrm{M}(1)$ et pour n entier $\geqslant 2$

$$\mathrm{M}(n) = -\sum_{d|n,\ d<n}\mathrm{M}(d) \quad\text{et}\quad \mu(n) = -\sum_{d|n,\ d<n}\mu(d)$$

Par récurrence forte, on conclut $\boxed{\mathrm{M} = \mu}$

Problème III

1. D'après le petit théorème de Fermat, on a

$$\boxed{2^p \equiv 2\ [p]}$$

2. Soit $k \in [\![1\,;p-1]\!]$. D'après la formule des chefs, on a

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Comme $p \wedge k = 1$, d'après le lemme de Gauss, on obtient

$$\boxed{\forall k \in [\![1\,;\, p-1]\!] \qquad p \text{ divise } \tbinom{p}{k}}$$

Puis $$k!\tbinom{p}{k} = p(p-1)\dots(p-k+1)$$

d'où $$k!\frac{\binom{p}{k}}{p} \equiv (p-1)\dots(p-k+1)\ [p] \equiv (-1)\dots(-(k-1))\ [p]$$

Ainsi $$\boxed{\forall k \in [\![1\,;\, p-1]\!] \qquad k!\frac{\binom{p}{k}}{p} \equiv (-1)^{k-1}(k-1)!\ [p]}$$

3. On a $$2^p - 2 = \sum_{k=0}^{p} \tbinom{p}{k} - 2 = \sum_{k=1}^{p-1} \tbinom{p}{k}$$

d'où $$\frac{2^p-2}{p} = \sum_{k=1}^{p-1} \frac{\binom{p}{k}}{p}$$

D'après l'égalité établie à la question précédente, on obtient pour $k \in [\![1\,;\, n-1]\!]$ en multipliant de part et d'autre par $\overline{k!}^{-1}$

$$(-1)^{k-1}\bar{k}^{-1} = \overline{b_{p,k}} \quad \text{avec} \quad b_{p,k} = \frac{\binom{p}{k}}{p}$$

On conclut $$\boxed{\sum_{k=1}^{p-1} (-1)^{k-1}\bar{k}^{-1} = \overline{a_p}}$$