Corrigé du DS02 du 09/11/2023 (4h)
Sujet A (MPI*), exercices 3 et 4

* * *

Exercice 3

1. Si $x \in Ker(A)$, alors $x \in \mathbb{R}^q$ et $Ax = 0_{\mathbb{R}^p}$, donc en notant $\|.\|$ la norme euclidienne sur $\mathbb{R}^p$:

$$\|Bx\|^2 = (Bx)^T(Bx) = x^T(B^TB)x = x^T(A^TA)x = x^TA^T\underbrace{(Ax)}_{0_{\mathbb{R}^p}} = 0,$$

ce qui montre $Bx = 0$, et donc $Ker(A) \subset Ker(B)$. Par symétrie des rôles de A et B, on a l'inclusion réciproque. Donc $Ker(A) = Ker(B)$.

2. Pour tout vecteur $z \in \mathbb{R}^q$, on a $f(z) = Az$ (puique A est la matrice de f dans les bases canoniques de $\mathbb{R}^q$ et $\mathbb{R}^p$), et de même pour g. Donc, pour $(x, y) \in \mathbb{R}^q \times \mathbb{R}^q$:

$$\langle f(x), f(y)\rangle = (Ax)^T(Ay) = x^T(A^TA)y = x^T(B^TB)y = (Bx)^T(By) = \langle g(x), g(y)\rangle.$$

3. Puisque $\mathcal{B} = (\varepsilon_1, \cdots, \varepsilon_r)$ est une base de F et puisque $\mathcal{B}' = (\varepsilon'_1, \cdots, \varepsilon'_r)$ est une famille de vecteurs de F, il existe une unique application linéaire $s : F \to F$ telle que $s(\varepsilon_i) = \varepsilon'_i$ pour tout $i \in [\![1, r]\!]$. Reste à montrer que s est une isométrie.
Tout $x \in F$ se décompose dans la base $\mathcal{B}$:

$$\forall x \in F,\ \exists!(x_1, \cdots, x_r) \in \mathbb{R}^r, \quad x = \sum_{i=1}^{r} x_i\varepsilon_i,$$

donc par linéarité de s :

$$\forall x \in F,\ \exists!(x_1, \cdots, x_r) \in \mathbb{R}^r, \quad s(x) = \sum_{i=1}^{r} x_i s(\varepsilon_i) = \sum_{i=1}^{r} x_i\varepsilon'_i.$$

Il s'ensuit, en utilisant l'hypothèse faite sur les deux bases :

$$\|s(x)\|^2 = \langle s(x), s(x)\rangle = \sum_{1\leq i,j\leq n} x_ix_j\langle\varepsilon'_i, \varepsilon'_j\rangle = \sum_{1\leq i,j\leq n} x_ix_j\langle\varepsilon_i, \varepsilon_j\rangle = \langle x, x\rangle = \|x\|^2.$$

Donc s conserve la norme, c'est-à-dire $s \in \mathcal{O}(F)$.

4. Si $U \in \mathcal{O}_p(\mathbb{R})$ l'égalité $A = UB$ signifie $f = u \circ g$, où $u \in \mathcal{O}(\mathbb{R}^p)$ est l'isométrie vectorielle canoniquement associée à la matrice U.
On va construire $u \in \mathcal{O}(\mathbb{R}^p)$ adéquate à partir d'une base bien choisie de $\mathbb{R}^q$.
Partons du noyau $G = Ker(f)$ (qui est aussi égal à $Ker(g)$ d'après la question 1.). On sait (d'après le théorème d'isomorphisme), que tout supplémentaire de G dans $\mathbb{R}^q$ est isomorphe à $Im(f)$ et à $Im(g)$.
En particulier les restrictions $f : G^\perp \to Im(f)$ et $g : G^\perp \to Im(g)$ sont des isomorphismes. Etant donnée une base $(x_1, \cdots, x_r)$ de $G^\perp$, la famille $(\varepsilon'_1, \cdots, \varepsilon'_r) = (f(x_1), \cdots, f(x_r))$ est donc une base de $Im(f)$, et de même, $(\varepsilon_1, \cdots, \varepsilon_r) = (g(x_1), \cdots, g(x_r))$ est une base de $Im(g)$.
Complétons ces bases avec des bases orthonormées $(\varepsilon'_{r+1}, \cdots, \varepsilon'_p)$ et $(\varepsilon_{r+1}, \cdots, \varepsilon_p)$ de $Im(f)^\perp$ et $Im(g)^\perp$ respectivement.
On dispose alors de deux bases de $\mathbb{R}^p$:

$$\mathcal{B} = (\varepsilon_1, \cdots, \varepsilon_p), \qquad \mathcal{B}' = (\varepsilon'_1, \cdots, \varepsilon'_p)$$

qui vérifient les hypothèses de la question 3., car pour tout $(i,j) \in [\![1,p]\!]^2$:

$$\langle \varepsilon_i, \varepsilon_j \rangle = \begin{cases} \langle g(x_i), g(x_j) \rangle = \langle f(x_i), f(x_j) \rangle = \langle \varepsilon'_i, \varepsilon'_j \rangle & \text{si } 1 \leq i,j \leq r \\ \delta_{i,j} = \langle \varepsilon'_i, \varepsilon'_j \rangle & \text{sinon} \end{cases}$$

D'où l'existence de $u \in \mathcal{O}(\mathbb{R}^p)$ qui envoie ε_i sur ε'_i pour tout $i \in [\![1,p]\!]$, et donc en particulier :

$$\forall i \in [\![1,r]\!], \qquad f(x_i) = \varepsilon'_i = u(\varepsilon_i) = u(g(x_i)).$$

Par linéarité, on a donc f et $u \circ g$ qui coïncident sur $Vect(x_1, \cdots, x_r) = G^\perp$ et elles coïncident bien entendu sur $G = Ker(f) = Ker(g)$ car elles s'annulent sur G. Donc finalement $f = u \circ g$, ce qui amène $A = UB$ en notant $U \in \mathcal{O}_p(\mathbb{R})$ la matrice de u dans la base canonique de $\mathbb{R}^p$.

* * *

Exercice 4 : Cyclicité de $\mathbb{K}^*$ lorsque $\mathbb{K}$ est un corps fini

Extrait de l'agrégation interne 2023 (épreuve 1)

1. Voir le cours (on utilise l'isomorphisme du théorème chinois).
2. Si p est premier et $i \in \mathbb{N}^*$, alors pour tout $k \in [\![1,p^i]\!]$, on a

$$pgcd(k,p^i) = 1 \iff pgcd(k,p) = 1 \iff k \notin p\mathbb{Z},$$

donc

$$\varphi(p^i) = Card\left([\![1,p^i]\!] \setminus \{kp,\ 1 \leq k \leq p^{i-1}\}\right) = p^i - p^{i-1} = p^{i-1}(p-1).$$

On en déduit que pour tout $k \in \mathbb{N}^*$:

$$f(p^k) = \sum_{d \in \mathcal{D}_{p^k}} \varphi(d) = \sum_{i=0}^{k} \varphi(p^i) = 1 + \sum_{i=1}^{k} (p^i - p^{i-1}) = p^k.$$

3. - L'application P est bien définie car $(d_1|m_1 \text{ et } d_2|m_2) \implies d_1 d_2 | m_1 m_2$.
   - Etant donnés deux couples (d_1,d_2) et (d'_1,d'_2) de $\mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ tels que $d_1 d_2 = d'_1 d'_2$, on a $d'_1 | d_1 d_2$ et $pgcd(d'_1, d_2) = 1$ (puisque $pgcd(d'_1,d_2)$ divise d'_1 et d_2, donc m_1 et m_2 qui sont premiers entre eux), donc d'après le lemme de Gaüss, on a $d'_1 | d_1$. Symétriquement $d_1 | d'_1$, donc $d'_1 = d_1$ (puisque ce sont des entiers naturels). Et de même, on a $d'_2 = d_2$, ce qui montre que l'application P est injective.
   - Enfin, étant donné un diviseur $d \in \mathcal{D}_{m_1 m_2}$, il peut s'écrire $d = d_1 d_2$, avec $d_1 | m_1$ et $d_2 | m_2$: en posant $d_1 = pgcd(m_1, d)$ et $d_2 = \frac{d}{d_1}$ on a bien $d_1 d_2 = d$, puis $d_1 | m_1$ et $d_2 | \frac{m_1}{d_1} \times m_2$ avec $pgcd(d_2, \frac{m_1}{d_1}) = 1$, donc par le lemme de Gaüss, $d_2 | m_2$. Cela montre la surjectivité de l'application P.
   En définitive, l'application P est bien une bijection de $\mathcal{D}_{m_1} \times \mathcal{D}_{m_2}$ vers $\mathcal{D}_{m_1 m_2}$.
   Variante : on peut aussi procéder en utilisant les décompositions primaires de m_1, m_2 et d pour montrer la bijectivité de P, en déterminant directement l'antécédent (d_1,d_2) d'un diviseur quelconque d de $m_1 m_2$.
4. Si m_1 et m_2 sont premiers entre eux, alors par définition de f :

$$f(m_1 m_2) = \sum_{d \in \mathcal{D}_{m_1 m_2}} \varphi(d).$$

En utilisant la bijection P, cela se réécrit :

$$f(m_1 m_2) = \sum_{d \in P(\mathcal{D}_{m_1} \times \mathcal{D}_{m_2})} \varphi(d) = \sum_{(d_1,d_2) \in \mathcal{D}_{m_1} \times \mathcal{D}_{m_2}} \varphi(d_1 d_2).$$

Or, les couples (d_1, d_2) de la somme vérifient $pgcd(d_1, d_2) = 1$ (puisque m_1 et m_2 sont premiers entre eux), donc d'après les propriétés de l'indicatrice d'Euler :

$$f(m_1m_2) = \sum_{(d_1,d_2)\in\mathcal{D}_{m_1}\times\mathcal{D}_{m_2}} \varphi(d_1)\varphi(d_2) = \sum_{d_1\in\mathcal{D}_{m_1}} \varphi(d_1) \times \sum_{d_2\in\mathcal{D}_{m_2}} \varphi(d_2) = f(m_1)f(m_2).$$

5. Soit $n \in \mathbb{N}^*$, on considère sa décomposition primaire :

$$n = \prod_{i\in I} p_i^{\alpha_i},$$

avec I une partie finie de $\mathbb{N}^*$, les $(p_i)_{i\in I}$ des nombres premiers distincts et les α_i dans $\mathbb{N}^*$.
Vu que les $(p_i^{\alpha_i})_{i\in I}$ sont premiers entre eux deux à deux, on a directement d'après la question précédente et la question (a) :

$$f(n) = \prod_{i\in I} f(p_i^{\alpha_i}) = \prod_{i\in I} p_i^{\alpha_i} = n,$$

ce qui permet de conclure que $n = f(n) = \sum_{d\in\mathcal{D}_n} \varphi(d)$.

6. On sait que pour tout $x \in \mathbb{K}^*$, l'ordre de x, noté $ord(x)$, est nécessairement un diviseur strictement positif de $Card(\mathbb{K}^*) = c$.
En notant donc $\Omega_d = \{y \in \mathbb{K}^*,\ ord(y) = d\}$ pour tout entier d, on a la réunion disjointe

$$\mathbb{K}^* = \bigcup_{d\in\mathcal{D}_c} \Omega_d,$$

(avec les Ω_d éventuellement vides *a priori*). En passant aux cardinaux, on obtient

$$\sum_{d\in\mathcal{D}_c} N(d) = c.$$

7. (a) On a $H = \langle x\rangle = \{1, x, \cdots, x^{d-1}\}$ cyclique de cardinal $d = ord(x)$. Puisque $x^d = 1$, tous les éléments de H sont des racines du polynôme $P = X^d - 1 \in \mathbb{K}[X]$ (vu que pour tout k, on a $(x^k)^d = (x^d)^k = 1^k = 1$).
Mais $\mathbb{K}$ étant un corps, P possède au maximum d racines dans $\mathbb{K}$, et donc puisque $Card(H) = d$, on a nécessairement

$$H = \{\text{racines de } P \text{ dans } \mathbb{K}\}.$$

Cela entraîne que tout élément $y \in \mathbb{K}^*$ d'ordre d est dans H
(puisque $ord(y) = d \implies y^d = 1 \iff y$ est racine de P).

(b) Puisque x est d'ordre d, on a pour tout $\ell \in \mathbb{N}^*$:

$$(x^k)^\ell = 1 \iff x^{k\ell} = 1 \iff d|k\ell \iff \frac{d}{pgcd(k,d)}|\frac{k\ell}{pcgd(k,d)} \iff \frac{d}{pgcd(k,d)}|\ell,$$

la dernière équivalence résultant du lemme de Gaüss, puisque $\frac{d}{pgcd(k,d)}$ et $\frac{k}{pgcd(k,d)}$ sont premiers entre eux. Ainsi :

$$(x^k)^\ell = 1 \iff l \text{ multiple de } \frac{d}{pgcd(k,d)},$$

ce qui montre que $ord(x^k) = \frac{d}{pgcd(k,d)}$.

(c) Soit $d \in \mathcal{D}_c$.
Si $N(d) = 0$, alors on a évidemment $N(d) \leq \varphi(d)$ (puisque $\varphi(d) \in \mathbb{N}^*$).
Si $N(d) \geq 1$, alors en utilisant 7.(a) et le sous-groupe H :

$$N(d) = Card\{y \in H,\ ord(y) = d\} = Card\{k \in [\![0, d-1]\!],\ ord(x^k) = d\}.$$

Vu que pour tout entier k, on a $ord(x^k) = \frac{d}{pgcd(k,d)}$, on en déduit que

$$N(d) = Card\{k \in [\![0, d-1]\!],\ pgcd(k,d) = 1\} = \varphi(d).$$

Dans tous les cas, on a donc $N(d) \leq \varphi(d)$.

8. Reste à voir que tous les $N(d)$ sont non nuls (c'est-à-dire que tous les ordres possibles sont représentés dans le groupe fini $\mathbb{K}^*$). Cela résulte de l'égalité

$$\sum_{d\in\mathcal{D}_c}(\varphi(d)-N(d))=c-c=0$$

(qui provient des questions 5. et 6.) et de la positivité des termes $\varphi(d)-N(d)$, qui entraînent :

$$\forall d\in\mathcal{D}_c,\qquad N(d)=\varphi(d)\in\mathbb{N}^*.$$

9. En particulier $N(c)\neq 0$, donc $\mathbb{K}^*$ est cyclique, puisqu'il possède au moins un élément d'ordre c.