Interrogation dispensatoire d'algèbre

Premier bachelier en sciences mathématiques,
janvier 2013

Consignes :

- Répondre à des questions différentes sur des feuilles distinctes et numérotées comportant chacune vos nom et prénom. Rendre au moins une feuille par question (même en cas d'abstention).
- Chacune des deux parties (théorie et exercices) est cotée sur 10 points. La moins bonne cote interviendra pour 55% de la note finale.
- La clarté, la rédaction et la justification des réponses fournies interviennent dans la cotation de l'ensemble de l'examen. Enoncer les résultats utilisés.

Bon travail !

1) Soit $\mathbb{K}$ un champ. Démontrer qu'une matrice $A \in \mathbb{K}_p^n$ est de rang r si et seulement si on peut trouver r colonnes de A linéairement indépendantes telles que toute colonne de A soit combinaison linéaire de celles-ci.

Preuve. La condition est nécessaire. Par définition du rang d'une matrice, si le rang de A vaut r, alors on peut trouver r colonnes linéairement indépendantes $C_{i_1}, \ldots, C_{i_r}$. Si une colonne D de A n'était pas combinaison linéaire de $C_{i_1}, \ldots, C_{i_r}$, alors $C_{i_1}, \ldots, C_{i_r}, D$ seraient linéairement indépendants[1] et on en conclurait que $\mathrm{rg}(A) > r$.

Passons à la réciproque. Si on peut trouver r colonnes de A linéairement indépendantes, alors $\mathrm{rg}(A) \geq r$. Montrons que le rang de A vaut exactement r. Soit $s > r$. Si on considère s colonnes *quelconques* de A, ces s colonnes sont, par hypothèse, combinaisons de r colonnes de A. Elles sont donc, au vu du théorème de Steinitz[2] linéairement dépendantes. Par conséquent, on ne peut pas trouver plus de r colonnes linéairement indépendantes. Donc, A est de rang r.

Enoncer et démontrer la règle des sous-matrices bordées permettant de déterminer le rang d'une matrice $A \in \mathbb{K}_p^n$.

Preuve. *cf.* cours théorique.

2) Enoncer et démontrer le théorème de Bezout relatif au p.g.c.d. de deux entiers. Comment utiliser ce résultat pour la recherche d'inverses dans $\mathbb{Z}_m$?

Preuve. *cf.* cours théorique. Un élément non nul $[x]_m$ de $\mathbb{Z}_m$ est inversible si et seulement si l'entier x est premier avec m. Dans ce cas, au vu du théorème de Bezout, il existe des entiers relatifs α, β tels que $\alpha\, x + \beta\, m = 1$. Dès lors, si on travaille modulo m, on a $\alpha\, x \equiv 1 \pmod{m}$. Autrement dit, $[\alpha]_m$ est l'inverse de $[x]_m$.

3) Définir la somme directe de $p \geq 2$ sous-espaces vectoriels d'un $\mathbb{K}$-vectoriel.

cf. cours théorique (la définition exprimant le fait que le vecteur nul possède une décomposition *unique* comme somme d'éléments des différents sous-espaces suffit).

---

[1] Rappeler la proposition suivante. Soient $x_1 \ldots, x_r$ des vecteurs linéairement indépendants. Les vecteurs $x_1, \ldots, x_r, y$ sont linéairement dépendants si et seulement si y est combinaison linéaire de $x_1, \ldots, x_r$.

[2] $r + 1$ combinaisons linéaires de r colonnes sont toujours linéairement dépendantes.

4) Vrai–Faux. Justifier à chaque fois votre réponse par une preuve (énoncer un résultat théorique du cours peut suffire) ou un contre-exemple explicite.

a. Soit $n \geq 2$ un entier. L'ensemble des racines n-ièmes de l'unité, muni de la multiplication de nombres complexes, forme un groupe.

b. Soient $n \geq 2$ un entier et τ une transposition de $\mathcal{S}_n$. Les applications $f : \mathcal{S}_n \to \mathcal{S}_n,\ \nu \mapsto \tau\nu$ et $g : \mathcal{S}_n \to \mathcal{S}_n,\ \nu \mapsto \nu\tau$ sont des bijections de $\mathcal{S}_n$ dans lui-même.

c. Soient $A, B \in \mathbb{R}^3_3$. Si $\det(A) = \det(B) = 0$, alors $\det(A + B) = 0$.

d. Soient x, y, z trois éléments d'un $\mathbb{C}$-vectoriel E. Les éléments x, y, z sont linéairement indépendants si et seulement si $x, 2y, iz$ le sont.

e. Soient F et G deux sous-espaces vectoriels distincts de dimension 3 de $\mathbb{R}^4$. On a toujours $F + G = \mathbb{R}^4$.

Solution.

a. VRAI. Soit $U_n = \{e^{2ik\pi/n} \mid k = 0, \ldots, n-1\}$ l'ensemble des n racines n-ièmes de l'unité. Autrement dit, $x \in \mathbb{C}$ appartient à U_n si et seulement si $x^n = 1$. La multiplication définie sur U_n est *interne* : soient $x, y \in U_n$. On a $xy \in U_n$, car $(xy)^n = x^n y^n = 1$. La multiplication dans $\mathbb{C}$ est *associative* donc sa restriction à U_n l'est aussi. Le *neutre* 1 appartient bien à U_n. Pour tout élément $e^{2ik\pi/n}$ de U_n, l'élément $e^{2i(n-k)\pi/n}$ de U_n en est l'*inverse*.

b. VRAI. Montrons-le pour f. L'application f est *injective*. Soient $\mu, \nu \in \mathcal{S}_n$ tels que $f(\mu) = f(\nu)$. Il faut vérifier que $\mu = \nu$. On a

$$f(\mu) = \tau\mu = \tau\nu = f(\nu).$$

Puisque τ est permutation, il possède un inverse τ^{-1} dans $\mathcal{S}_n$ (muni du produit de composition). En multipliant à gauche par τ^{-1}, on trouve $\tau^{-1}\tau\mu = \tau^{-1}\tau\nu$ et donc $\mu = \nu$. L'application f est *surjective*. Soit $\sigma \in \mathcal{S}_n$. Existe-t-il $\mu \in \mathcal{S}_n$ tel que $f(\mu) = \sigma$? Puisque $f(\mu) = \tau\mu$, il suffit de prendre $\mu = \tau^{-1}\sigma$ qui est encore un élément de $\mathcal{S}_n$. Même raisonnement pour g (on multipliera à droite par τ^{-1}).

c. FAUX. Un contre-exemple suffit. Soient

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

On a $\det(A) = \det(B) = 0$, mais $A + B = I$ et $\det(A + B) = 1$.

d. VRAI. Si les vecteurs x, y, z sont linéairement dépendants, alors il existe des scalaires α, β, γ non tous nuls tels que $\alpha x + \beta y + \gamma z = 0$. Dans ce cas, on dispose de la combinaison linéaire suivante de $x, 2y, iz$:

$$\alpha x + \frac{\beta}{2} 2y + \frac{\gamma}{i} iz = 0$$

avec des coefficients $\alpha, \frac{\beta}{2}, \frac{\gamma}{i}$ non tous nuls. Donc $x, 2y, iz$ sont linéairement dépendants. Réciproquement, si $x, 2y, iz$ sont linéairement dépendants, alors il existe des scalaires α, β, γ non tous nuls tels que $\alpha x + \beta 2y + \gamma iz = 0$. Ceci montre que x, y, z sont alors linéairement dépendants car les coefficients de x, y, z dans cette dernière combinaison, à savoir $\alpha, 2\beta, i\gamma$ sont non tous nuls.

e. VRAI. Il existe un vecteur f de F n'appartenant pas à G. En effet, sinon F serait inclus dans G et, F et G étant de même dimension, on aurait $F = G$, alors que F et G sont distincts. Soit (g_1, g_2, g_3) une base de G. Dès lors f, g_1, g_2, g_3 sont linéairement indépendants (sinon, f serait combinaison linéaire de g_1, g_2, g_3). Donc le sous-espace $\rangle f, g_1, g_2, g_3 \langle$ est inclus dans $F + G$ et sa dimension vaut 4. Par conséquent, on a $\dim(F + G) = 4$ et donc $F + G = \mathbb{R}^4$.

Répondre à des questions différentes sur des feuilles distinctes et numérotées. Rendre au moins une feuille par question (même en cas d'abstention). Justifier vos réponses. Enoncer les résultats utilisés. Fin de l'interrogation: **12h30**.

1) Soit E un $\mathbb{C}$-vectoriel de dimension $n \geq 3$. On y considère des vecteurs $\{e_1, \ldots, e_n\}$ et on définit les vecteurs

$$t_j = e_j + e_{j+1} + e_{j+2}, \ \forall j \in \{1, \ldots, n-2\}$$

et $t_{n-1} = e_1 + e_{n-1} + e_n$, $t_n = e_1 + e_2 + e_n$.

- Pour $n = 5$, démontrer que $(e_1, \ldots, e_n)$ est une base de E si et seulement si $(t_1, \ldots, t_n)$ en est une.
- Pour $n = 5$, donner la matrice de changement de bases pour passer de la base $(e_1, \ldots, e_n)$ à la base $(t_1, \ldots, t_n)$.

Si $(e_1, \ldots, e_5)$ est une base de E, pour montrer que $t_1, \ldots, t_5$ forment une base de E, il suffit de vérifier qu'ils sont linéairement indépendants. Considérons la matrice

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

où la j-ième colonne contient les composantes de t_j dans la base $U = (e_1, \ldots, e_5)$. Puisque $\det(M) = 3 \neq 0$, les colonnes de M, $\Phi_U(t_1), \ldots, \Phi_U(t_5)$ sont linéairement indépendantes et puisque Φ_U est un isomorphisme entre E et $\mathbb{C}^5$, on en conclut que $t_1, \ldots, t_5$ sont linéairement indépendants. Ces vecteurs étant en nombre égal à la dimension de E, ils en forment une base. On trouve

$$M^{-1} = \frac{1}{3} \begin{pmatrix} 2 & -1 & 2 & -1 & -1 \\ -1 & 2 & -1 & 2 & -1 \\ -1 & -1 & 2 & -1 & 2 \\ 2 & -1 & -1 & 2 & -1 \\ -1 & 2 & -1 & -1 & 2 \end{pmatrix}.$$

Si $V = (t_1, \ldots, t_5)$ est une base de E, alors la j-ième colonne de M^{-1} contient les composantes de e_j dans la base V. Puisque $\det(M^{-1}) = 1/\det(M) = 1/3 \neq 0$, par un raisonnement analogue à celui développé ci-dessus, on a que si V est une base de E, alors $(e_1, \ldots, e_5)$ aussi.

En particulier, M^{-1} est la matrice de changement de bases pour passer de la base $(e_1, \ldots, e_n)$ à la base $(t_1, \ldots, t_n)$.

2) On note $U(\mathbb{Z}_8)$ l'ensemble des éléments inversibles de $\mathbb{Z}_8$. Quels sont éléments de $U(\mathbb{Z}_8)$? Déterminer (et justifier votre réponse) si les fonctions suivantes sont injectives, surjectives, bijectives

- $f : U(\mathbb{Z}_8) \to U(\mathbb{Z}_8), \ x \mapsto x^{-1} \pmod 8$

- $g : \mathbb{Z}_8 \to \mathbb{Z}_8,\ x \mapsto x^2 \pmod 8$
- $h : \mathbb{Z}_8 \to \mathbb{Z}_8,\ x \mapsto 3x \pmod 8$

Si on pose $\mathbb{Z}_8 = \{0, 1, \ldots, 7\}$. On trouve $U = \{1, 3, 5, 7\}$ (il suffit de considérer les éléments premiers avec $8 = 2^3$.

- L'application f est une bijection de $U(\mathbb{Z}_8)$ dans lui-même. On a $f(1) = 1$, $f(3) = 3$ car $3.3 \equiv 1 \pmod 8$, $f(5) = 5$ car $5.5 \equiv 1 \pmod 8$ et $f(7) = 7$ car $7.7 \equiv 1 \pmod 8$. On voit donc que $f : U(\mathbb{Z}_8) \to U(\mathbb{Z}_8)$ est trivialement injective et surjective.
- L'application g n'est pas injective car $g(0) = g(4)$. En effet, $4^2 \equiv 0 \pmod 8$. Elle n'est pas non plus surjective. Une façon de le voir est de remarquer que $\{g(i) \mid i \in \mathbb{Z}_8\} = \{0, 1, 4\}$. On pourrait aussi utiliser le fait que, puisque $\mathbb{Z}_8$ est fini, g est injective si et seulement si elle est surjective.
- L'application h est une bijection. Cela résulte essentiellement du fait que 3 est inversible dans $\mathbb{Z}_8$. Si $x, y \in \mathbb{Z}_8$ sont tels que $h(x) = h(y)$, alors $3x = 3y$ dans $\mathbb{Z}_8$ et en multipliant les deux membres par l'inverse de 3, on trouve $x = y$. Autrement dit, h est injective. Pour la surjectivité, on peut bien sûr utiliser le dernier argument du point précédent, ou encore dresser l'ensemble des valeurs prises par h,

i	0	1	2	3	4	5	6	7
$h(i)$	0	3	6	1	4	7	2	5

  ou enfin, remarquer que pour tout $y \in \mathbb{Z}_8$, $x = 3^{-1}y$ est tel que $f(x) = y$.

3) Soient α, β deux nombres complexes distincts et E le $\mathbb{C}$-vectoriel des polynômes à coefficients complexes de degré au plus 2. On considère le sous-vectoriel F donné par

$$F = \{P \in E \mid P(\alpha) = 0\}.$$

(Pour rappel, si P appartient à F, alors P est divisible par $(x - \alpha)$.)

- Vérifier que $(x - \alpha)^2,\ (x - \alpha)$ est une base de F.
- Si $P = a\,(x-\alpha)^2 + b\,(x-\alpha)$ est un élément de F, avec $a, b \in \mathbb{C}$, quelles sont ses composantes dans la base $x^2, x, 1$ de E ?
- Donner une base d'un supplémentaire de F dans E. Justifier votre réponse.

Soit l'ensemble G donné par

$$G = \{P \in E \mid P(\alpha) + P(\beta) = 0\}.$$

- Montrer que G est un sous-espace vectoriel de E.
- Caractériser les éléments de $F \cap G$. En particulier, quelle est la dimension de $F \cap G$?
- Montrer que G est de dimension 2. La somme de F et de G peut-elle être directe ?

L'espace E est de dimension 3, une base en est donnée par $x^2, x, 1$. Le sous-espace F étant inclus strictement dans E (par exemple, les polynômes $x - \beta$ ou 1 de E n'appartiennent pas à F), sa dimension est au plus 2. Les deux polynômes $x - \alpha$ et $(x - \alpha)^2$ ont des degrés différents. Ils sont donc linéairement indépendants[3] et appartiennent à F. Par conséquent, F est de

[3]Si $a(x - \alpha) + b(x - \alpha)^2 = 0$, alors on en tire que nécessairement $a = b = 0$.

dimension 2. Donc, $x-\alpha$ et $(x-\alpha)^2$ forment une base de F. Pour le deuxième point, il suffit de distribuer,

$$P = a\,(x-\alpha)^2 + b\,(x-\alpha) = a\,x^2 + (b-2a\alpha)x + a\alpha^2 - b\alpha.$$

Ainsi, les composantes de P dans la base $x^2, x, 1$ sont a, $b-2a\alpha$, $a\alpha^2-b\alpha$. Au vu de la discussion menée en préambule, pour construire un supplémentaire H de F dans E, il suffit de trouver un polynôme non nul de E n'appartenant pas à F. Par exemple, $H = \rangle 1 \langle$ convient, car $H \cap F = \{0\}$ et $\dim E = 3 = \dim F + \dim H$.

Le polynôme nul appartient à G. Si P, Q sont des éléments de G, i.e., $P(\alpha) + P(\beta) = 0$ et $Q(\alpha) + Q(\beta) = 0$, alors $P + Q$ appartient encore à G. En effet, $(P+Q)(\alpha) + (P+Q)(\beta) = P(\alpha) + Q(\alpha) + P(\beta) + Q(\beta) = 0$. De façon analogue, si $P \in G$, alors pour tout $\lambda \in \mathbb{C}$, $\lambda P \in G$. En effet, $(\lambda P)(\alpha) + (\lambda P)(\beta) = \lambda(P(\alpha) + P(\beta)) = 0$.

Si un polynôme R appartient simultanément à F et à G, alors on en conclut d'abord que $R(\alpha) = 0$ et donc que $R(\beta) = 0$. Par conséquent, R est de la forme $a(x-\alpha)(x-\beta)$ (un polynôme de degré au plus deux s'annulant en α et β). En particulier, cela signifie que $F \cap G$ est de dimension 1, tout élément du sous-espace étant multiple du polynôme $(x-\alpha)(x-\beta)$.

Pour le dernier point, construisons d'abord un polynôme de degré 1 tel que $S(\alpha) = 1$ et $S(\beta) = -1$. On peut remarquer que les polynômes $T(x) = (x-\alpha)(x-\beta)$ et $S(x) = 1 - 2(x-\alpha)/(\beta-\alpha)$ appartiennent à G. Puisque S et T sont linéairement indépendants (ils ont des degrés différents), $\dim G \geq 2$ mais G est inclus strictement dans E (e.g., $1 \notin G$), donc $\dim G = 2$. Puisque $\dim(F \cap G) = 1$, la somme de F et G ne peut pas être directe.

4) Soient $n \geq 2$ un entier et des réels $s_1, \ldots, s_n$. Calculer par récurrence le déterminant suivant

$$\det \begin{pmatrix} s_1 & \cdots & \cdots & s_1 \\ \vdots & s_2 & \cdots & s_2 \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & \cdots & s_n \end{pmatrix}.$$

En essayant avec de petites valeurs de n, on imagine facilement que la valeur du déterminant recherché est

$$s_1(s_2-s_1)(s_3-s_2)\cdots(s_n-s_{n-1}).$$

Prouvons-le par récurrence sur n. Pour le cas de base, on a

$$\det \begin{pmatrix} s_1 & s_1 \\ s_1 & s_2 \end{pmatrix} = s_1(s_2-s_1).$$

Supposons que le résultat est vérifié pour une matrice $(n-1)\times(n-1)$,

$$\det \begin{pmatrix} t_1 & \cdots & \cdots & t_1 \\ \vdots & t_2 & \cdots & t_2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1 & t_2 & \cdots & t_{n-1} \end{pmatrix} = t_1(t_2-t_1)(t_3-t_2)\cdots(t_{n-1}-t_{n-2}).$$

Pour calculer le déterminant demandé avec une matrice $n \times n$, si on soustrait la première colonne aux autres colonnes[4], on a

$$\det \begin{pmatrix} s_1 & \dots & \dots & s_1 \\ \vdots & s_2 & \dots & s_2 \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 & \dots & s_n \end{pmatrix} = \det \begin{pmatrix} s_1 & 0 & \dots & 0 \\ \vdots & s_2 - s_1 & \dots & s_2 - s_1 \\ \vdots & \vdots & \ddots & \vdots \\ s_1 & s_2 - s_1 & \dots & s_n - s_1 \end{pmatrix}.$$

On est en présence d'une matrice triangulaire et on se ramène donc à calculer le déterminant d'une matrice $(n-1) \times (n-1)$ ayant la même structure ($s_2 - s_1$ joue le rôle de t_1, $s_3 - s_1$ celui de t_2, …, $s_n - s_1$ le rôle de t_{n-1}) et à laquelle on peut donc appliquer l'hypothèse de récurrence. Ainsi, le déterminant demandé vaut bien

$$s_1(s_2 - s_1) \underbrace{\big((s_3 - s_1) - (s_2 - s_1)\big)}_{s_3 - s_2} \cdots \underbrace{\big((s_n - s_1) - (s_{n-1} - s_1)\big)}_{s_n - s_{n-1}}.$$

[4]Ce n'est bien sûr pas la seule façon de mener à bien le calcul.