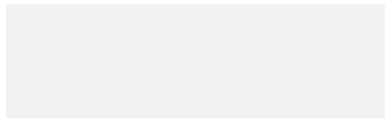




Enseignant: Philippe Michel
Examen: Algèbre Linéaire Avancée, MATH-110
Date: Le 20 Janvier 2021, 12h15-15h15
Durée: 3 heures

Student One

SCIPER: **111111**

Signature: 

Attendez le début de l'examen avant de tourner la page.

Ce document est imprimé recto-verso, il contient 32 pages.

Ne pas dégrafer.

- Aucun document n'est autorisé.
- Une calculatrice simple (sans display graphique) est autorisée.
- Pour les questions à choix multiples:
 - entourez la bonne réponse (sans justification) et utilisez un stylo à encre noire ou bleue foncée; en cas d'erreur effacez proprement avec du correcteur blanc.
 - Une réponse incorrecte compte 0 mais n'entraîne pas de point négatif.
- Pour les questions ouvertes:
 - Répondre dans l'espace dédié.
 - Vous pouvez utiliser un crayon à papier à condition d'écrire lisiblement;
 - Si vous utilisez des résultats du cours, citez-les explicitement.
 - Sauf mention explicite du contraire on a le droit d'admettre un résultat d'un autre exercice ou d'une question précédente du même exercice pour répondre à une question.
- Si une question est erronée, l'enseignant se réserve le droit de l'annuler.
- L'examen est LONG mais il n'est pas nécessaire de le faire correctement intégralement pour obtenir la note maximale.

Exercice 1 (Questions de cours et QCM). .

1. Enoncer le Théorème Noyau-Image.
2. Soit G un groupe et $H, K \subset G$ des sous-groupes distingués alors le sous-groupe engendré par H et K est distingué.

Vrai Faux

3. Un produit d'anneaux intègres est intègre.

Vrai Faux

4. Soit A un anneau fini (comme ensemble), commutatif et intègre et M un A -module de type fini, alors M est libre.

Vrai Faux

(un anneau fini commutatif et intègre est un corps) et un A -module de type fini est un EV de dim fini sur ce corps.

5. Une application linéaire $\varphi : \mathbb{R}^4 \mapsto \mathbb{R}^3$ de rang maximal est injective.

Vrai Faux

(jamais injective: Thm N-I + $4 > 3$)

6. Soit $A, B \in GL_d(K)$ des matrices carrées inversibles alors $({}^t({}^tA.B^{-1}))^{-1}$ vaut

- $A^{-1}.{}^tB$ • ${}^tB.A^{-1}$ • rien car ${}^t({}^tA.B^{-1})$ n'est pas forcément inversible

7. Le polynome caractéristique $P_{car,M}(X)$ de la matrice $M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix} \in M_3(\mathbb{Q})$ vaut

- $-X^3 - 3X^2 - 2X - 1$ • $X^3 - 3X^2 + 2X + 1$ • $X^3 - 3X^2 - 2X - 1$

(le PC doit être unitaire et son coef constant est $(-1)^3 \det(M) = -1 : \det M = 1$ par la règle de Sarrus)

Exercice 2. Soit $\mathcal{F}(\mathbb{R}; \mathbb{C}) := \{f : x \mapsto f(x)\}$ le \mathbb{C} -espace vectoriel des fonctions sur \mathbb{R} à valeurs dans \mathbb{C} (le corps des nombres complexes). Soient

$$f_1(x) = \cos(x), f_2(x) = \sin(x), f_3(x) = \cos(3x), f_4(x) = \sin(3x)$$

et

$$V = \langle f_1, f_2, f_3, f_4 \rangle \subset \mathcal{F}(\mathbb{R}; \mathbb{C})$$

le sous-espace vectoriel engendré par ces 4 fonctions.

Q1: Montrer que $\mathcal{B} = \{f_1, f_2, f_3, f_4\}$ est une base de V . Pour cela on pourra évaluer une combinaison linéaire (nulle) de ces fonctions en des points bien choisis et faire de même pour la dérivée.

Solution:

$$x_1 \cos(x) + x_2 \sin(x) + x_3 \cos(3x) + x_4 \sin(3x) = 0.$$

$$x = 0 \implies x_1 + x_3 = 0, \quad x = \pi/6 \implies \frac{\sqrt{3}}{2}x_1 = 0$$

$$\implies x_1 = x_3 = 0.$$

$$x = \pi/2 \implies x_2 - x_4 = 0, \quad x = \pi/3 \implies x_2/2 = 0$$

$$\implies x_2 = x_4 = 0.$$

La famille est libre donc c'est un base de l'EV qu'elle engendre.

Q2: On considère l'application linéaire (admis) de V à valeurs dans $\mathcal{F}(\mathbb{R}; \mathbb{C})$

$$\varphi : f \in V \mapsto f'' + 2if' + 3f$$

où f', f'' désignent la dérivée première et seconde de f . Montrez que $\varphi(f) \in V$. Ainsi φ définit un endomorphisme de V .

Solution: On a

$$\varphi(f_1) = -f_1 - 2if_2 + 3f_1, \quad \varphi(f_2) = -f_2 + 2if_1 + 3f_2$$

$$\varphi(f_3) = -9f_3 - 6if_4 + 3f_3, \quad \varphi(f_4) = -9f_4 + 6if_3 + 3f_4$$

donc pour $i = 1, 2, 3, 4$ on a $\varphi(f_i) \in V$ et tout $f \in V$ est CL de f_1, f_2, f_3, f_4 (par définition de V) et comme φ est linéaire $\varphi(f) \in V$.

Q3: Donner la matrice de φ dans la base \mathcal{B} et calculer son polynôme caractéristique.

Solution:

$$\begin{pmatrix} 2 & 2i & 0 & 0 \\ -2i & 2 & 0 & 0 \\ 0 & 0 & -6 & 6i \\ 0 & 0 & -6i & -6 \end{pmatrix}$$

C'est un matrice par blocs.

Le polynome caractéristique est le déterminant $P_{car, \varphi}(X) = \det(X \cdot \text{Id}_4 - M)$. Comme la matrice est par blocs

$$\begin{aligned} P_{car, \varphi}(X) &= \det(X \cdot \text{Id}_4 - M) = \det \begin{pmatrix} X-2 & -2i & 0 & 0 \\ 2i & X-2 & 0 & 0 \\ 0 & 0 & X+6 & -6i \\ 0 & 0 & -6i & X+6 \end{pmatrix} \\ &= \det \begin{pmatrix} X-2 & -2i \\ 2i & X-2 \end{pmatrix} \det \begin{pmatrix} X+6 & -6i \\ -6i & X+6 \end{pmatrix} = ((X-2)^2 + (2i)^2)((X+6)^2 + (6i)^2) \\ &= (X^2 - 4X)(X^2 + 12X) = X^4 + 8X^3 - 48X^2. \end{aligned}$$

Q4: Trouver des bases de $\ker \varphi$ et de $\text{Im } \varphi$

Solution: Pour le noyau, on doit résoudre le système:

$$\begin{aligned} 2x_1 + 2ix_2 &= 0 \\ -2ix_1 + 2x_2 &= 0 \\ -6x_3 + 6ix_4 &= 0 \\ -6ix_3 - 6x_4 &= 0 \end{aligned} \iff \begin{aligned} 2x_1 + 2ix_2 &= 0 \\ -6x_3 + 6ix_4 &= 0 \end{aligned} \iff \begin{aligned} x_2 &= ix_1 \\ x_4 &= -ix_3 \end{aligned}$$

et prenant $x_1 = 1$ et $x_3 = 1$) on a

$$\ker \varphi = \text{Vect}(f_1 + if_2, f_3 - if_4)$$

et cette famille $\{f_1 + if_2, f_3 - if_4\}$ est libre car

$$x_1(f_1 + if_2) + x_3(f_3 - if_4) = 0 \iff x_1f_1 + x_1if_2 + x_3f_3 - x_3if_4 = 0 \implies x_1 = x_3 = 0$$

car la famille f_1, f_2, f_3, f_4 est libre par la question 1.

Ainsi $\ker \varphi$ est de dimension 2 et $\varphi(V)$ est de dimension 2 (Thm NI). On a

$$\varphi(V) = \text{Vect}(\varphi(f_1), \varphi(f_2), \varphi(f_3), \varphi(f_4))$$

mais $\varphi(f_2) = i\varphi(f_1)$, $\varphi(f_4) = -i\varphi(f_3)$ et donc une base de $\varphi(V)$ est donnée par

$$\{\varphi(f_1), \varphi(f_3)\} = \{2 \cos(x) - 2i \sin(x), -6 \cos(3x) - 6i \sin(3x)\}$$

Exercice 3. Soit K un corps et U, V des espaces vectoriels sur K de dimensions (finies) d et d' . On notera U^*, V^* les espaces duaux. On notera

$$\mathcal{B} = \{\mathbf{e}_1, \dots, \mathbf{e}_d\} \subset U, \quad \mathcal{B}' = \{\mathbf{f}_1, \dots, \mathbf{f}_{d'}\} \subset V$$

des bases de U et V et

$$\mathcal{B}^* = \{\mathbf{e}_1^*, \dots, \mathbf{e}_d^*\} \subset U^*, \quad \mathcal{B}'^* = \{\mathbf{f}_1^*, \dots, \mathbf{f}_{d'}^*\} \subset V^*$$

les bases duales.

Par ailleurs on fait la définition suivante:

Définition 3.1. Une forme bilinéaire B sur $U \times V$ est une fonction de l'espace produit $U \times V$ à valeurs dans K

$$B : \begin{array}{l} U \times V \mapsto K \\ (u, v) \mapsto B(u, v) \end{array}$$

telle que

- Pour tout $v \in V$, la fonction sur U à valeurs dans K

$$u \in U \mapsto B(u, v) \in K$$

est une forme linéaire.

- Pour tout $u \in U$, la fonction sur V à valeurs dans K

$$v \in V \mapsto B(u, v) \in K$$

est une forme linéaire.

On note $\text{Bil}(U, V)$ l'ensemble de toutes les formes bilinéaires sur $U \times V$.

Dans la suite de cet exercice, on admettra que $\text{Bil}(U, V)$ est un sous-espace vectoriel de l'espace $\mathcal{F}(U \times V; K)$ des fonctions de $U \times V$ à valeurs dans K (pour la structure usuelle de K -espace vectoriel de $\mathcal{F}(U \times V; K)$).

Q1: Soient $\ell \in U^*$ et $\ell' \in V^*$ des formes linéaires; montrer que la fonction

$$\ell \otimes \ell' : (u, v) \in U \times V \mapsto \ell(u).\ell'(v) \in K$$

est une forme bilinéaire sur $U \times V$.

Solution: On a

$$\mathbf{e}_i^* \otimes \mathbf{f}_j^*(u, v) = \mathbf{e}_i^*(u).\mathbf{f}_j^*(v)$$

et pour tout v fixe la fonction

$$u \mapsto \mathbf{e}_i^*(u).\mathbf{f}_j^*(v)$$

est linéaire en u (car proportionnelle à la forme linéaire $u \mapsto \mathbf{e}_i^*(u)$) et de même pour u fixe, la fonction

$$v \mapsto \mathbf{e}_i^*(u).\mathbf{f}_j^*(v)$$

est linéaire en v .

Montrons qu'on a bien une famille génératrice et libre: supposons qu'il existe des coefficients $(x_{ij})_{i \leq d, j \leq d'}$ tels que pour tout $u \in U, v \in V$ on a

$$\sum_{i \leq d} \sum_{j \leq d'} x_{ij} \mathbf{e}_i^* \otimes \mathbf{f}_j^*(u, v) = 0$$

alors prenant $(u, v) = (\mathbf{e}_{i_0}, \mathbf{f}_{j_0})$ on a

$$0 = \sum_{i \leq d} \sum_{j \leq d'} x_{ij} \mathbf{e}_i^* \otimes \mathbf{f}_j^*(\mathbf{e}_{i_0}, \mathbf{f}_{j_0}) = x_{i_0 j_0}$$

et en faisant varier (i_0, j_0) on obtient que tous les coefficients sont nuls. La famille est donc libre. Soit $B(u, v)$ une forme bilinéaire, on a

$$u = \sum_{i \leq d} \mathbf{e}_i^*(u) \mathbf{e}_i, \quad v = \sum_{j \leq d'} \mathbf{f}_j^*(v) \mathbf{f}_j$$

et par linéarité en u puis en v

$$\begin{aligned} B(u, v) &= \sum_{i \leq d} \mathbf{e}_i^*(u) B(\mathbf{e}_i, v) = \sum_{i \leq d} \mathbf{e}_i^*(u) \sum_{j \leq d'} \mathbf{f}_j^*(v) B(\mathbf{e}_i, \mathbf{f}_j) = \sum_{i \leq d} \sum_{j \leq d'} B(\mathbf{e}_i, \mathbf{f}_j) \mathbf{e}_i^*(u) \mathbf{f}_j^*(v) \\ &= \sum_{i \leq d} \sum_{j \leq d'} B(\mathbf{e}_i, \mathbf{f}_j) \mathbf{e}_i^* \otimes \mathbf{f}_j^*(u, v) \end{aligned}$$

et donc

$$\begin{aligned} B &= \sum_{i \leq d} \mathbf{e}_i^*(u) B(\mathbf{e}_i, v) = \sum_{i \leq d} \mathbf{e}_i^*(u) \sum_{j \leq d'} \mathbf{f}_j^*(v) B(\mathbf{e}_i, \mathbf{f}_j) = \sum_{i \leq d} \sum_{j \leq d'} B(\mathbf{e}_i, \mathbf{f}_j) \mathbf{e}_i^*(u) \mathbf{f}_j^*(v) \\ &= \sum_{i \leq d} \sum_{j \leq d'} B(\mathbf{e}_i, \mathbf{f}_j) \mathbf{e}_i^* \otimes \mathbf{f}_j^* \end{aligned}$$

on a bien une famille génératrice et donc une base

Ainsi

$$\dim \text{Bil}(U, V) = dd' = \dim U \dim V.$$

Q2: On considère dorénavant le cas $U = V^*$. Soit $\text{End}(V)$ l'espace des endomorphismes de V (ie. les applications K -linéaires de V sur V) et soit $\varphi \in \text{End}(V)$. Montrer que la fonction sur $V^* \times V$ à valeurs dans K définie par

$$B_\varphi : (\ell, v) \in V^* \times V \mapsto B_\varphi(\ell, v) = \ell(\varphi(v)) \in K$$

est une forme bilinéaire sur $V^* \times V$.

Solution: La fonction

$$B_\varphi : (\ell, v) \mapsto \ell(\varphi(v))$$

est linéaire en v car c'est la composée $\ell \circ \varphi$ de deux applications linéaires.

Soient $\ell_1, \ell' \in V^*$, $\mu \in K$ alors pour v fixe

$$B_\varphi(\mu\ell + \ell', v) = (\mu\ell + \ell')(\varphi(v)) = \mu\ell(\varphi(v)) + \ell'(\varphi(v)) = \mu.B_\varphi(\ell, v) + B_\varphi(\ell', v)$$

et l'application est linéaire en ℓ (on aurait aussi pu dire que $B_\varphi(\bullet, v)$ est l'application $\text{ev}_\varphi(\bullet)$ d'évaluation en le vecteur $\varphi(v)$ qui est linéaire sur V^* . En tout cas B_φ est bilinéaire.

Q3: Montrer que l'application de $\text{End}(V)$ à valeurs dans $\text{Bil}(V^, V)$ définie par*

$$B_\bullet : \varphi \in \text{End}(V) \mapsto B_\varphi \in \text{Bil}(V^*, V)$$

est linéaire et injective (pour ce dernier point on observera que les valeurs $B_\varphi(\mathbf{e}_i^*, \mathbf{e}_j)$ sont liées à la matrice de φ dans une base convenable).

Solution: On a pour $\lambda \in K$, $\varphi, \psi \in \text{End}(V)$ et $\ell \in V^*, v \in V$,

$$B_{\lambda\varphi+\psi}(\ell, v) = \ell(\lambda\varphi + \psi(v)) = \ell(\lambda\varphi(v) + \psi(v)) = \lambda\ell(\varphi(v)) + \ell(\psi(v)) = \lambda B_\varphi(\ell, v) + B_\psi(\ell, v)$$

(l'avant dernière égalité car ℓ est linéaire) et donc

$$B_{\lambda\varphi+\psi} = \lambda B_\varphi + B_\psi.$$

L'application B_\bullet est donc linéaire.

Soit $\{\mathbf{e}_j, j \leq d\}$ une base de V et $\{\mathbf{e}_i^*, i \leq d\}$ la base duale. Supposons que $B_\varphi = 0$. On a pour tout i, j

$$B_\varphi(\mathbf{e}_i^*, \mathbf{e}_j) = \mathbf{e}_i^*(\varphi(\mathbf{e}_j)) = 0$$

qui est le i -ième coefficient de l'image du vecteur \mathbf{e}_j par φ c'est à dire le coefficient (i, j) de la matrice associée à φ dans la base de $\{\mathbf{e}_j, j \leq d\}$. Si tous les coefficients de cette matrice sont nuls c'est que φ est nulle. L'application linéaire B_\bullet est de noyau trivial donc injective.

Q4: Montrer que $\text{End}(V)$ est isomorphe à $\text{Bil}(V^, V)$ (comme K -espace vectoriel).*

Solution: On a une application injective

$$B_\bullet : \text{End}(V) \mapsto \text{Bil}(V^*, V)$$

et les deux espaces sont de même dimension d^2 (par Q1) donc c'est un isomorphisme.

Exercice 4. Soit K un corps et $V = K^2$ le K -espace vectoriel de dimension 2. On rappelle qu'une droite (linéaire) $D \subset V$ est un sous-espace vectoriel de dimension 1:

$$D = K.v = \{\lambda.v, \lambda \in K\}$$

où $v \in V - \{0_V\}$ est un vecteur non-nul. On note

$$P^1(K) = \{D \subset K^2, \dim_K(D) = 1\}$$

l'ensemble des droites de K^2 .

Q1: Montrer que $P^1(K)$ est en bijection avec l'ensemble des vecteurs

$$\{v_\lambda := (1, \lambda), \lambda \in K\} \cup \{v_\infty := (0, 1)\} \subset V$$

Solution: Soit $D = K.v$ un droite engendré par le vecteur non nul $v = (x, y)$. Si $x \neq 0$ alors

$$D = K.x^{-1}(x, y) = K(1, \lambda), \lambda = y/x$$

et si $x = 0$ alors $y \neq 0$ et

$$D = K.y^{-1}(0, y) = K.(0, 1).$$

Ainsi on a défini une application surjective

$$\{v_\lambda, \lambda \in K\} \sqcup \{v_\infty\} \mapsto P^1(K)$$

De plus si

$$K.(1, \lambda) = K.(1, \lambda')$$

alors

$$(1, \lambda') = x.(1, \lambda) = (x, x\lambda) \implies x = 1, \lambda' = \lambda$$

et $K.v_\lambda \neq K.v_\infty$ (car un vecteur de cette dernière droite a sa première coordonnée toujours nulle).

On a donc une application injective et donc bijective.

Q2: Soit $\varphi \in GL(V) \simeq GL_2(K)$ une application K -linéaire inversible. On suppose que pour tout $v \in V$ il existe un scalaire $\lambda_v \in K$ tel que

$$\varphi(v) = \lambda_v.v.$$

Montrer qu'en fait les λ_v sont tous égaux à un même scalaire $\lambda \in K^\times$ de sorte que

$$\varphi = \lambda.Id_V.$$

Solution:

Si $\dim V = 1$ toute application linéaire est de la forme $v \mapsto \lambda v$. Sinon, soit $v, v' \in V$ non colinéaires on a

$$\varphi(v + v') = \lambda_v.v + \lambda_{v'}v' = \lambda_{v+v'}(v + v')$$

et donc

$$(\lambda_v - \lambda_{v+v'})v = (-\lambda_{v'} + \lambda_{v+v'})v'$$

et comme les vecteurs ne sont pas colinéaires on doit avoir

$$\lambda_v - \lambda_{v+v'} = -\lambda_{v'} + \lambda_{v+v'} = 0$$

et

$$\lambda_v = \lambda_{v'} = \lambda_{v+v'}.$$

Q3: Soit $\varphi \in \text{GL}(K^2)$ une application linéaire inversible (on ne fait pas d'autre hypothèse sur φ). Comme φ est linéaire, l'image d'une droite D par φ

$$\varphi(D) = \{\varphi(v'), v' \in D\}$$

est encore une droite (on ne demande PAS de le démontrer). On note

$$\sigma_\varphi : D \in \mathbb{P}^1(K) \mapsto \varphi(D) \in \mathbb{P}^1(K)$$

l'application correspondante sur l'ensemble des droites.

a Montrer que σ_φ est une bijection de l'ensemble $\mathbb{P}^1(K)$ sur lui-même et que l'application

$$\sigma_\bullet : \varphi \in \text{GL}(K^2) \mapsto \sigma_\varphi \in \text{Bij}(\mathbb{P}^1(K))$$

est un morphisme de groupes.

b Montrer que le noyau du morphisme ci-dessus vaut

$$\ker(\sigma_\bullet) = K^\times \cdot \text{Id}_{K^2},$$

ie. le groupe des multiples non-nuls de l'application identité (c.a.d les homothéties linéaires de K^2).

Solution:

a. On a

$$\sigma_\varphi \circ \sigma_\psi : D \mapsto \varphi(\psi(D)) = \sigma_{\varphi \circ \psi}(D)$$

et donc

$$\sigma_\varphi \circ \sigma_\psi = \sigma_{\varphi \circ \psi}.$$

On a également

$$\sigma_{\text{Id}_V} : D \mapsto \text{Id}_V(D) = D = \text{Id}_{\mathbb{P}^1(K)}(D)$$

et

$$\sigma_{\text{Id}_V} = \text{Id}_{\mathbb{P}^1(K)}$$

En particulier en prenant φ^{-1} on a

$$\sigma_\varphi \circ \sigma_{\varphi^{-1}} = \sigma_{\varphi^{-1}} \circ \sigma_\varphi = \sigma_{\text{Id}} = \text{Id}_{\mathbb{P}^1(K)}$$

Cela montre que σ_φ est bijective (de réciproque $\sigma_{\varphi^{-1}}$) et que

$$\varphi \mapsto \sigma_\varphi$$

est un morphisme de groupes.

b. Soit φ dans le noyau. Alors pour tout vecteur non nul v

$$\sigma_\varphi(K.v) = \varphi(K.v) = K.v$$

en particulier $\varphi(v) \in K.v$ et donc $\varphi(v) = \lambda_v.v$ pour $\lambda_v \in K$. Par Q1 on conclut que

$$\varphi = \lambda \cdot \text{Id}_V, \lambda \neq 0$$

(car φ est inversible donc non-nulle). Par ailleurs il est clair que si $\varphi = \lambda \cdot \text{Id}_V$, $\lambda \neq 0$ alors $\varphi(K.v) = K.v$. Le noyau est formé des matrices scalaires.

Q4: On suppose maintenant que $K = \mathbb{F}_p$ est le corps fini à p éléments (ici $p \geq 2$ est un nombre premier). Montrer les égalités suivantes

$$|\mathbb{P}^1(\mathbb{F}_p)| = p + 1, \quad |\text{GL}_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p).$$

Pour la deuxième égalité on pourra (au choix) soit compter le nombre de solutions de l'équation

$$ad - bc = 0_{\mathbb{F}_p}, (a, b, c, d) \in \mathbb{F}_p^4,$$

soit raisonner à partir des vecteurs colonnes qui composent une matrice 2×2 inversible, soit trouver une autre méthode de comptage.

Solution:

On a

$$|\mathbb{P}^1(\mathbb{F}_p)| = |\{v_\lambda := (1, \lambda), \lambda \in \mathbb{F}_p\} \cup \{v_\infty := (0, 1)\}| = p + 1.$$

On a

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in \mathbb{F}_p, \det M = ad - bc \neq 0 \right\}$$

il suffit de compter le nombre de $(a, b, c, d) \in \mathbb{F}_p^4$ tels que

$$ad - bc = 0$$

et de soustraire de $p^4 = |M_2(\mathbb{F}_p)|$.

1. Si on choisit $a \neq 0$ alors on a p^2 choix pour (b, c) et d vaut bc/a : on a $(p-1)p^2$ possibilités.
2. Si on choisit $a = 0$ alors on a p choix pour d et alors $bc = 0$. Si $b = 0$ on a p choix pour c et si $b \neq 0$ alors $c = 0$ (et $p-1$ choix pour b) soit $p(2p-1)$ possibilités.

Au total on a

$$|\mathrm{GL}_2(\mathbb{F}_p)| = p^4 - (p-1)p^2 - p(2p-1) = (p^2-1)(p^2-p)$$

Q5: Montrer que pour $p = 2$, le groupe $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe au groupe $\mathfrak{S}_3 = \mathrm{Bij}(\{1, 2, 3\})$ (ie. le groupe des permutations d'un ensemble de 3 éléments).

Solution:

Si $p = 2$ on a $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$. De plus le noyau

$$\ker \sigma_\bullet = \mathbb{F}_2^\times \cdot \mathrm{Id}_2 = \{\mathrm{Id}_2\}$$

est trivial (car $\mathbb{F}_2^\times = \{1\}$ puisque que $\mathbb{F}_2 = \{0, 1\}$). L'application

$$\sigma_\bullet : \mathrm{GL}_2(\mathbb{F}_2) \mapsto \mathrm{Bij}(\mathbb{P}^1(\mathbb{F}_2)) \simeq \mathfrak{S}_{2+1}$$

est injective et les groupes de départ et d'arrivée sont finis de même cardinal (car $|\mathbb{P}^1(\mathbb{F}_2)| = 2+1 = 3$) on a donc une bijection.

Q6: Donner un exemple de matrice $M_3 \in \mathrm{GL}_2(\mathbb{F}_2)$ qui correspond à un cycle de longueur 3 par un tel isomorphisme.

Solution:

La matrice

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

vérifie

$$M^3 = \mathrm{Id}_2$$

elle est d'ordre 3 et correspond à une permutation d'ordre 3 par l'isomorphisme précédent: c'est nécessairement un cycle de longueur 3.

Exercice 5 (Le lemme de Schur). Soit K un corps et V un K -espace vectoriel de dimension finie (non-nulle). Soit G un groupe fini et

$$\rho : \begin{array}{l} G \mapsto \text{GL}(V) \\ g \mapsto \rho_g \end{array}$$

un morphisme du groupe G vers le groupe linéaire de V ; on notera $\rho_g \in \text{GL}(V)$ l'image d'un élément $g \in G$ par le morphisme ρ .

Définition 5.1. On appelle *endomorphisme d'entrelacement*, une application K -linéaire de V sur V , $\varphi \in \text{End}(V)$ qui commute avec tous les ρ_g :

$$\forall g \in G, \varphi \circ \rho_g = \rho_g \circ \varphi$$

et on note l'ensemble des endomorphismes d'entrelacement

$$\text{End}_\rho(V) := \{\varphi \in \text{End}(V), \forall g \in G, \varphi \circ \rho_g = \rho_g \circ \varphi\}.$$

Le *Lemme de Schur* qui est l'objet de cet exercice établit une propriété fondamentale de l'ensemble des endomorphismes d'entrelacement sous une hypothèse supplémentaire.

Définition 5.2. On dit que V est ρ -irréductible si les seuls sous-espaces vectoriels de V qui sont stables par tous les ρ_g sont les sous-espaces vectoriels triviaux, c'est à dire $\{0_V\}$ et V : si $U \subset V$ est un sous-espace vectoriel de V qui satisfait

$$\forall g \in G, \rho_g(U) \subset U$$

alors $U = \{0_V\}$ ou $U = V$.

On rappelle également que le corps des nombres complexes \mathbb{C} est *algébriquement clos*, c'est à dire que tout polynôme unitaire de degré $d \geq 1$, $P(X) = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0$ admet au moins une racine complexe: il existe $\lambda \in \mathbb{C}$ tel que $P(\lambda) = 0$.

Q1: Montrer que $\text{End}_\rho(V)$ est un sous-espace vectoriel ainsi qu'un sous-anneau de la K -algèbre $\text{End}(V)$ (pour l'addition et la composition des endomorphismes).

Solution:

Soient $\varphi, \psi \in \text{End}_\rho(V)$, on a pour λ un scalaire et $g \in G$

$$(\lambda\varphi + \psi) \circ \rho_g = \lambda.\varphi \circ \rho_g + \psi \circ \rho_g = \lambda.\rho_g \circ \varphi + \rho_g \circ \psi = \rho_g \circ (\lambda\varphi + \psi)$$

donc $\text{End}_\rho(V)$ est un SEV. De plus $\text{Id}_V \in \text{End}_\rho(V)$ (car l'identité commute avec tous les endomorphismes et en particulier les ρ_g) et

$$\varphi \circ \psi \circ \rho_g = \varphi \circ \rho_g \circ \psi = \rho_g \circ \varphi \circ \psi$$

et donc $\text{End}_\rho(V)$ est stable par composition. C'est donc un sous-anneau et une sous- K algèbre.

Q2: On suppose dans la suite que V est ρ -irréductible. Montrer que tout élément non-nul φ de $\text{End}_\rho(V)$ est inversible et que son inverse φ^{-1} appartient à $\text{End}_\rho(V)$. Pour cela on considèrera (au choix) ou bien son noyau $\ker(\varphi) \subset V$ ou bien son image $\text{Im}(\varphi) \subset V$ (ou bien les deux).

Solution:

Soit $\varphi \in \text{End}_\rho(V)$ non-nul. Soit $v \in \ker \varphi$. On a pour tout $g \in G$

$$\varphi(\rho_g(v)) = \rho_g(\varphi(v)) = \rho_g(0) = 0$$

et donc $\rho_g(v) \in \ker \varphi$.

Ainsi $\rho_g(\ker(\varphi)) \subset \ker(\varphi)$ et $\ker \varphi$ est stable. Comme φ est non-nul, $\ker(\varphi) \neq V$ et $\ker \varphi = \{0\}$. Ainsi φ est injective donc bijective (car φ est un endomorphisme).

On a pour tout $g \in G$

$$(\varphi \circ \rho_g)^{-1} = (\rho_g \circ \varphi)^{-1}$$

et c'est égal à

$$\rho_g^{-1} \circ \varphi^{-1} = \varphi^{-1} \circ \rho_g^{-1}$$

c'est à dire

$$\rho_{g^{-1}} \circ \varphi^{-1} = \varphi^{-1} \circ \rho_{g^{-1}}$$

et on remplace g par g^{-1} pour conclure que $\varphi^{-1} \in \text{End}_\rho(V)$.

Q3: On suppose (en plus de la ρ -irréductibilité) que $K = \mathbb{C}$ est le corps des complexes. Soit $\varphi \in \text{End}_\rho(V)$, montrer qu'il existe $\lambda \in \mathbb{C}$ tel que $\varphi_\lambda := \varphi - \lambda \cdot \text{Id}_V$ n'est pas inversible (pensez au polynôme caractéristique) et montrer qu'en fait

$$\varphi = \lambda \cdot \text{Id}_V.$$

Solution:

Soit le polynôme caractéristique

$$P_{\text{car},\varphi}(X) = \det(X\text{Id}_V - \varphi)$$

c'est un polynôme en λ à coefficients dans \mathbb{C} et de degré $\dim V \geq 1$. comme \mathbb{C} est algébriquement clos il admet une racine: il existe $\lambda \in \mathbb{C}$ tel que

$$\det(\lambda\text{Id}_V - \varphi) = 0$$

et donc $\lambda\text{Id}_V - \varphi = -\varphi_\lambda$ n'est pas inversible. Mais $\lambda\text{Id}_V \in \text{End}_\rho(V)$ (car les λId_V commutent avec tous les endomorphismes en particulier les ρ_g) et donc

$$\varphi_\lambda = \varphi - \lambda\text{Id}_V \in \text{End}_\rho(V)$$

Comme φ_λ n'est pas inversible il doit être nul (Q2) :

$$\varphi = \lambda\text{Id}_V.$$

Q4: On suppose en plus du reste que G est un groupe commutatif. Montrer que

a pour tout $g \in G$, ρ_g appartient à $\text{End}_\rho(V)$,

b on a $\dim_{\mathbb{C}}(V) = 1$.

Solution:

a. Pour tout $g' \in G$

$$\rho_g \circ \rho_{g'} = \rho_{g \cdot g'} = \rho_{g' \cdot g} = \rho_{g'} \circ \rho_g$$

donc $\rho_g \in \text{End}_\rho(V)$.

b. Ainsi (Q3) pour tout $g \in G$ on a $\rho_g = \lambda_g \cdot \text{Id}_V$ (ρ_g est une homothétie). Si $W \subset V$ est un sous-espace quelconque de V alors W est stable par toutes les homothéties et en particulier par les ρ_g mais par irréductibilité W doit être soit nul soit V tout entier. Cela force V à être de dimension 1.