

Série 6

Tous les exercices seront corrigés.

Vous êtes fortement encouragés à essayer de résoudre (éventuellement à plusieurs) l'exercice (\star) et à rendre votre solution (éventuellement à plusieurs) avant le mercredi de la semaine suivante. Il faudra transmettre votre solution sur moodle, sous forme d'un fichier pdf unique (éventuellement tape en LaTeX) en suivant le lien moodle de la semaine relative à cette série.

Des SEV

Exercice 1. Les sous-ensembles suivants sont-ils des SEVs (on pourra éventuellement discuter suivant la nature du corps K) ?

1. $U(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2, x^2 - 2y^2 = 0\} \subset \mathbb{R}^2$.
2. $U(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2, x^2 - 2y^2 = 0\} \subset \mathbb{Q}^2$. (on se trouve $\sqrt{2}$?)
3. $\{(x_1, \dots, x_d) \in K^d, x_1 + \dots + x_d = 0_K\} \subset K^d$.
4. $\{(x_1, \dots, x_d) \in K^d, x_1 + \dots + x_d = 6_K\} \subset K^d$.
5. Soit V un K -EV, X un ensemble et et

$$\mathcal{F}(X, V) = \{f : X \mapsto V\}$$

l'EV des fonctions de X à valeurs dans V . Soit $I \subset X$ un sous-ensemble,

$$\mathcal{F}(X, V)_I = \{f : X \mapsto V, \forall x \in I, f(x) = 0_V\} \subset \mathcal{F}(X, V)$$

le sous-ensemble des fonctions s'annulant en tout point de I .

Exercice 2. Soit K un corps, $\mathcal{F}(K, K)$ l'espace vectoriel des fonctions de K à valeurs dans K et $\mathcal{F}(K, K)^+$ le sous-ensemble des fonctions paires (resp. $\mathcal{F}(K, K)^-$ des fonctions impaires) :

$$f : K \mapsto K, \forall x \in K, f(x) = f(-x) \text{ (resp. } f(x) = -f(-x)).$$

1. Montrer que $\mathcal{F}(K, K)^\pm$ sont des SEVs de $\mathcal{F}(K, K)$

2. Montrer que $\text{car}(K) \neq 2$ on a

$$\mathcal{F}(K, K) = \mathcal{F}(K, K)^+ \oplus \mathcal{F}(K, K)^-.$$

3. Que ce passe-t-il si $\text{car}(K) = 2$?

Exercice 3. Dans l'EV K^3 on considère la famille

$$\mathcal{F} = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}.$$

1. Montrer que si $\text{car}(K) \neq 2$ \mathcal{F} est libre.
2. Montrer sans faire de calculs que si $\text{car}(K) \neq 2$ \mathcal{F} est génératrice.
3. Montrer que si $\text{car}(K) \neq 2$ la famille \mathcal{F} est génératrice (et donc une base) en montrant que tout $v = (x, y, z) \in K^3$ s'écrit explicitement comme combinaison linéaire des éléments de cette famille.
4. Montrer que si $\text{car}(K) = 2$ la famille \mathcal{F} n'est ni libre, ni génératrice.

Des applications linéaires

Exercice 4. Soit K un corps, V un K -EV et $X, Y \subset V$ des SEVs tels que V est somme directe de X et Y :

$$V = X \oplus Y.$$

On vu que cela implique que pour tout $v \in V$ il existe un unique $x \in X$ et $y \in Y$ tel que

$$v = x + y. \tag{0.1}$$

1. Montrer que les applications

$$\pi_X : v \in V \mapsto x \in X, \quad \pi_Y : v \in V \mapsto y \in Y$$

(ou x et y sont définis par (0.1)) sont linéaires.

2. Montrer que l'application

$$\bullet + \bullet : \begin{array}{l} X \times Y \mapsto V \\ (x, y) \mapsto x + y \end{array}$$

est un isomorphisme d'espaces vectoriels.

Exercice 5. (\star) Soient V, W deux espaces vectoriels de dimension finie et $\varphi : V \mapsto W$ une application linéaire. Montrer que

1. Si φ est injective alors l'image par φ d'une famille libre est libre.
2. Si φ est surjective alors l'image par φ d'une famille generatrice est generatrice; en deduire que

$$\dim(V) \geq \dim(W).$$

3. Si φ est bijective, montrer que $\dim(V) = \dim(W)$.

Exercice 6. Soit $\varphi : \mathbb{Q}^2 \mapsto \mathbb{Q}^2$ l'application definie par

$$\varphi : \begin{array}{ccc} \mathbb{Q}^2 & \mapsto & \mathbb{Q}^2 \\ (x, y) & \mapsto & (2x + y, x + 2y) \end{array}$$

1. Montrer que φ est lineaire.
2. Montrer $\ker(\varphi) = \{0_2\}$, $\text{Im}(\varphi) = \mathbb{Q}^2$.

Exercice 7. Soit K un corps general, on notera 2 pour $2_K = 2 \cdot 1_K$. Soit $\varphi : K^2 \mapsto K^2$ l'application definie par

$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x, y) & \mapsto & (2x + y, x + 2y) \end{array}$$

On admet que φ est lineaire.

1. Montrer que si $\text{car}(K) \neq 3$ alors $\ker(\varphi) = \{0_2\}$, $\text{Im}(\varphi) = K^2$.
2. Si $\text{car}(K) = 3$ montrer que le noyau et l'image sont de dimension 1 en donnant dans chaque cas un vecteur generateur (on observera que dans ce cas $2_K = -1_K$).

Exercice 8. Soit K un corps, on notera 2 pour $2_K = 2 \cdot 1_K$. Soit $\varphi : K^2 \mapsto K^2$ l'application definie par

$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x, y) & \mapsto & (2x + y, x + y) \end{array}$$

On admet que φ est lineaire.

1. Montrer que $\ker(\varphi) = \{0_2\}$.
2. Montrer que $\text{Im}(\varphi) = K^2$ en trouvant pour chaque $(X, Y) \in K^2$ un (x, y) tel que $\varphi(x, y) = (X, Y)$.

Encore des corps

Les exercices suivants introduisent une methode generale pour construire des corps a partir d'autres corps via des matrices. En particulier on donne une recette pour construire un corps fini \mathbb{F}_{p^2} de cardinal p^2 pour $p \geq 3$ premier.

Exercice 9 (Construction de corps a partir de matrices). Soit K un corps d'element nul et d'unité notes respectivement 0 et 1 et

$$M_2(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in K \right\}$$

l'anneau des matrices 2×2 a coefficients dans K (muni de la somme $+$ et du produit des matrices \times).

On rappelle que la matrice nulle (l'element nul de $M_2(K)$) et la matrice identite (l'identite de $M_2(K)$) sont les matrices

$$0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{Id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et que le groupe des elements inversible de cet anneau est donne par les matrices de determinant inversible (cad non-nul puisque K est un corps)

$$M_2(K)^\times = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in K, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in K^\times \right\}.$$

1. Montrer (si vous ne l'avez jamais fait) que l'anneau $M_2(K)$ est egalement un K -espace vectoriel quand on le muni de la multiplication par les scalaires

$$\lambda \in K, M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K) \mapsto \lambda.M := \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}$$

et que l'on a la propriete d'associativite entre la multiplication par les scalaires et la multiplication des matrices : pour $\lambda \in K, M, N \in M_2(K)$

$$\lambda.(M \times N) = (\lambda.M) \times N$$

(on dit alors que l'anneau $M_2(K)$ est une K -algebre).

2. Montrer que l'ensemble des matrices (dites elementaires)

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$E_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, E_{22} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

forme une famille generatrice de $M_2(K)$. Montrer que $\dim_K M_2(K) = 4$ en exhibant un isomorphisme de K -ev entre K^4 et $M_2(K)$.

3. Montrer que l'ensemble des matrices multiples de l'identité

$$K \cdot \text{Id}_2 = \{\lambda \cdot \text{Id}_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \lambda \in K\}$$

forme un sous-anneau de $M_2(K)$ qui est en fait un corps isomorphe à K . C'est le corps des matrices scalaires 2×2 .

4. Soit $d \in K$ et I_d la matrice

$$I_d = \begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} \in M_2(K).$$

On note

$$K[I_d] := \langle \text{Id}_2, I_d \rangle = K \cdot \text{Id}_2 + K \cdot I_d = \{x \cdot \text{Id}_2 + y \cdot I_d, x, y \in K\} \subset M_2(K)$$

le sous- K espace vectoriel de $M_2(K)$ engendré par les matrices Id_2 et I_d .

Montrer qu'en fait $K[I_d]$ est un sous-anneau non-nul de $M_2(K)$ qui est commutatif (on calculera en particulier $I_d^2 = I_d \times I_d$).

5. Donner une valeur de d telle que cet anneau ne soit pas intègre (ne pas chercher très loin).
6. Montrer que $\{\text{Id}_2, I_d\}$ est une famille libre du K -EV $K[I_d]$. Quelle est la dimension de $K[I_d]$?
7. On suppose que d n'est pas un carré dans K (ie. il n'existe pas de $u \in K$ tel que $u^2 = d$; par exemple si $K = \mathbb{R}$, $d = -1$ marche). Montrer que l'équation polynomiale

$$x^2 - dy^2 = 0$$

n'a pas de solution non-nulle $(x, y) \in K^2 - \{(0, 0)\}$ (distinguer les cas $y = 0$ et $y \neq 0$).

8. On suppose toujours que d n'est pas un carré dans K . Montrer que $K[I_d]$ est un corps. Pour cela on calculera le déterminant d'un élément non-nul de $K[I_d]$, et on vérifiera que la matrice inverse de cet élément (si elle existe) est encore dans $K[I_d]$. Ce corps contient un sous-corps isomorphe à K , lequel ?
9. On suppose que d est un carré dans K (ie. il existe $x \in K$ tel que $x^2 = d$). Montrer que $K[I_d]$ n'est pas intègre.

Exercice 10. On reprend l'exercice précédent en supposant que K est le corps fini \mathbb{F}_p pour p premier.

1. Quel est le cardinal de $M_2(\mathbb{F}_p)$? Celui de $K[I_d]$?
2. Montrer que la classe de congruence $-1 \pmod{3} \in \mathbb{F}_3$ n'est pas un carré dans \mathbb{F}_3 (il n'existe pas de $x \in \mathbb{F}_3$ tel que $x^2 = -1 \pmod{3}$).

3. Montrer que la classe de congruence $2 \pmod{5} \in \mathbb{F}_5$ n'est pas un carre dans \mathbb{F}_5 .
4. Donner un exemple de corps de matrices a 9 elements et a 25 elements? On note ces corps \mathbb{F}_9 et \mathbb{F}_{25} . On rappelle qu'il contiennent des sous-corps isomorphes respectivement a \mathbb{F}_3 et \mathbb{F}_5 (les corps de matrices scalaires $\mathbb{F}_3.\text{Id}_2$ et $\mathbb{F}_5.\text{Id}_2$). Dans la suite, par abus de langage on identifiera \mathbb{F}_3 et \mathbb{F}_5 aux corps de matrices scalaires $\mathbb{F}_3.\text{Id}_2$ et $\mathbb{F}_5.\text{Id}_2$.
5. Montrer que la classe de congruence $-1 \pmod{3} \in \mathbb{F}_3$ est un carre dans \mathbb{F}_9 (il existe $z \in \mathbb{F}_9$ tel que $z^2 = -1$).
6. Montrer que la classe de congruence $2 \pmod{5} \in \mathbb{F}_5$ est un carre dans \mathbb{F}_{25} .