EPFL Automne 2022
Algebre Lineaire Avancee, MATH-110

Série 7

Tous les exercices seront corriges.

Vous etes fortement encourages a essayer de resoudre (eventuellement a plusieurs) l'exercice ($\star$) et a rendre votre solution (eventuellement a plusieurs) avant le mercredi de la semaine suivante. Il faudra transmettre votre solution sur moodle, sous forme d'un fichier pdf unique (eventuellement tape en LaTeX) en suivant le lien moodle de la semaine relative a cette la serie.

Questions de dimension

Exercice 1. soit X et Y des EVs sur un corps K. On note leur produit

$$X \times Y = \{(x, y),\ x \in X,\ y \in Y\}.$$

On rappelle que $X \times Y$ a une structure d'espace vectoriel en posant (avec les additions et multiplications par les scalaires convenable)

$$(x, y) + (x', y') = (x + x', y + y'),\ k.(x, y) = (k.x, k.y).$$

Pour $\mathcal{F}_X \subset X, \mathcal{F}_Y \subset Y$ des sous-ensembles de X et Y, on note

$$\mathcal{F}_X \oplus \mathcal{F}_Y = \{(x, 0_Y),\ x \in \mathcal{F}_X\} \cup \{(0_X, y),\ y \in \mathcal{F}_Y\}.$$

On suppose que X et Y sont de dimension finie.

1. Montrer que si $\mathcal{F}_X$ et $\mathcal{F}_Y$ sont des familles libres alors $\mathcal{F}_X \oplus \mathcal{F}_Y$ est libre.
2. Montrer que si $\mathcal{F}_X$ et $\mathcal{F}_Y$ sont generatrices alors $\mathcal{F}_X \oplus \mathcal{F}_Y$ est generatrice.
3. Montrer que $X \times Y$ est de dimension finie et que

$$\dim(X \times Y) = \dim X + \dim Y.$$

Exercice 2. Soit K un corps.

1. Soit $k \subset K$ un sous-corps. Montrer que K admet une structure naturelle de k-espace vectoriel.

2. Soit K un corps fini de caracteristique $p > 0$ et

$$k = \mathbb{F}_p = \mathrm{Can}_K(\mathbb{Z}) = \mathbb{Z}.1_K \subset K$$

le sous-corps premier. Montrer que K est de dimension finie ($d \geqslant 0$) sur $\mathbb{F}_p$ et que $|K| = p^d$.

3. On suppose que K est encore contenu dans un autre corps fini L. Ainsi

$$\mathbb{F}_p \subset K \subset L$$

et on a donc (par la question precedente) $|L| = p^{d'}$ avec $d' \geqslant 1$. Montrer que d divise d' (on montrera que le quotient d'/d est une certaine dimension).

Autour du Thm Noyau-Image

Exercice 3. Soit K un corps. Soit $\varphi : K^2 \mapsto K^2$ l'application lineaire definie par

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

(ici on notera $2, 3, \cdots$ pour $2_K = 2.1_K,\ 3_k = 3.1_K, \cdots$)

1. Montrer avec un minimum de calculs que $\ker(\varphi) = \{0_2\}$ et $\mathrm{Im}(\varphi) = K^2$.

Exercice 4. Soit $\varphi : K^2 \mapsto K^2$ l'application lineaire definie par

$$\varphi : \begin{array}{ccc} K^2 & \mapsto & K^2 \\ (x,y) & \mapsto & (3x+3y, x+4y) \end{array}$$

(ici on notera $2, 3, \cdots$ pour $2_K = 2.1_K,\ 3_k = 3.1_K, \cdots$)

1. Trouver avec un minimum de calculs les dimensions de $\ker(\varphi)$ et $\mathrm{Im}(\varphi)$ (en fonction de la caracteristique de K).
2. Donner (encore avec le minimum de calculs) une base du noyau et de l'image de φ.

Exercice 5. Soit K un corps de caracteristique 0, $V = K^5$ et

$$W = \{(a,b,c,d,e) \in V,\ a+b = c+d,\ a+2c = 0, 2c+b+4d = 0\}.$$

1. Montrer que W est un SEV de K^5 en montrant que W est le noyau d'une application lineaire convenable.
2. Calculer $\dim W$ (eventuellement en utilisant le Thm Noyau-Image).

3. Donner une base de W.

Exercice 6. ($\star$) Soient $X, Y \subset V$ des SEVs d'un EV de dimension finie et $X+Y \subset V$ leur somme (qui est un SEV de V). On rappelle que X et Y sont en somme directe si $X \cap Y = \{0_V\}$ et on ecrit cela $X \oplus Y$.

1. Montrer que $\dim X + \dim Y = \dim(X+Y) + \dim(X \cap Y)$.
2. On suppose que $\dim X + \dim Y = \dim V$. Montrer que les proprietes suivantes sont equivalentes
   (a) $X \cap Y = \{0_V\}$,
   (b) $X + Y = V$,
   (c) $X \oplus Y = V$.

Pour resoudre cet exercice, on pourra appliquer le Thm Noyau-Image a l'application lineaire

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

Espace vectoriel quotient

Exercice 7. Soit V un K-EV et $\mathrm{K} \subset V$ un SEV. On va definir la notion d'espace vectoriel quotient V/K. La relation sur $(v, v') \in V \times V$ donnee par

$$v \sim_K v' \iff v - v' \in \mathrm{K}$$

est une relation d'equivalence dont l'ensemble des classes d'equivalences est donnee par le sous-ensemble de $\mathscr{P}(V)$

$$V/\mathrm{K} = \{v \,(\mathrm{mod}\,\mathrm{K}) := v + \mathrm{K}, v \in V\}.$$

On muni alors l'espace quotient V/K d'une structure de groupe (commutatif) en posant

$$v \,(\mathrm{mod}\,\mathrm{K}) +_{V/\mathrm{K}} v' \,(\mathrm{mod}\,\mathrm{K}) := v + v' \,(\mathrm{mod}\,\mathrm{K})$$

$$0_{V/\mathrm{K}} := 0 \,(\mathrm{mod}\,\mathrm{K}) = \mathrm{K}, \quad -(v \,(\mathrm{mod}\,\mathrm{K})) := -v + \mathrm{K};$$

on verifie (comme pour le cas du quotient d'un anneau commutatif par un ideal) que ces operations ne dependent pas des choix des vecteurs v et v' dans les classes de congruence $v \,(\mathrm{mod}\,\mathrm{K})$ et $v' \,(\mathrm{mod}\,\mathrm{K})$.

1. Montrer que la multiplication externe

$$\bullet.\bullet : \begin{array}{ccc} K \times V/\mathrm{K} & \mapsto & V/\mathrm{K} \\ (\lambda, v \,(\mathrm{mod}\,\mathrm{K})) & \mapsto & \lambda.v \,(\mathrm{mod}\,\mathrm{K}) := \lambda.v + \mathrm{K} \end{array}$$

est bien definie et donne au groupe quotient V/K une structure de K-EV.

2. Montrer que l'application

$$\bullet \,(\mathrm{mod}\,\mathrm{K}) : \begin{array}{ccc} V & \mapsto & V/\mathrm{K} \\ v & \mapsto & v \,(\mathrm{mod}\,\mathrm{K}) \end{array}$$

est lineaire, surjective et de noyau egal a

$$\ker(\bullet \,(\mathrm{mod}\,\mathrm{K})) = \mathrm{K}.$$

3. Montrer que si V est de dimension finie il en est de meme de V/K et que

$$\dim V/\mathrm{K} = \dim V - \dim \mathrm{K}.$$

4. Soit $\varphi : V \mapsto W$ une application lineaire et $\mathrm{K} := \ker \varphi$. Montrer que si $v' \in v \,(\mathrm{mod}\,\mathrm{K})$ alors
$$\varphi(v') = \varphi(v).$$
En deduire que si on pose pour toute classe $v \,(\mathrm{mod}\,\mathrm{K})$

$$\overline{\varphi}(v \,(\mathrm{mod}\,\mathrm{K})) := \varphi(v),$$

on obtient une application bien definie

$$\overline{\varphi} : V/\mathrm{K} \mapsto W.$$

Montrer que cette application est lineaire pour la structure de K-EV sur V/K definie precedemment.

5. Montrer que $\overline{\varphi} : V/\mathrm{K} \mapsto W$ est injective et que $\overline{\varphi}$ defini un isomorphisme du K-EV V/K sur son image $\varphi(V) \subset W$.

Remarque 0.1. On sait que le noyau d'une application lineaire est un SEV. La question 2 montre reciproquement que tout SEV est le noyau d'une application lineaire convenable.

Remarque 0.2. Etant donne une application lineaire $\varphi : V \mapsto W$ le fait que l'on ai un isomorphisme

$$\overline{\varphi} : V/\mathrm{K} \simeq \varphi(V)$$

(qui est valable que V soit de dimension finie ou pas) est la version plus precise du Thm. Noyau-Image (qui dit que $\dim(V/\mathrm{K}) = \dim \varphi(V)$ mais sans fournir d'isomorphisme explicite entre les deux espaces).

Le petit Theoreme de Fermat

Exercice 8. Soit $p \geqslant 3$ un nombre premier impair et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini a p elements.

1. Montrer par recurrence que pour tout entier $n \geqslant 0$,

$$n^p - n \equiv 0 \,(\mathrm{mod}\, p).$$

(on pourra utiliser la formule du binome de Newton).

2. Montrer que pour tout $x \in \mathbb{F}_p$ on a

$$x^p = x$$

et que pour tout $x \in \mathbb{F}_p^\times$ on a

$$x^{p-1} = 1.$$

(ici on note 1 pour $1_{\mathbb{F}_p} = 1 \,(\mathrm{mod}\, p)$ et on note -1 pour son oppose).

Remarque. On peut montrer que si K est un corps fini de caracteristique p (de sorte que K contient le corps $\mathbb{F}_p$ comme sous-corps premier) alors pour $x \in K$

$$x^p = x \Longrightarrow x \in \mathbb{F}_p.$$

Pour cela on dit (admet) que comme K est un corps, et que le polynome (a coefficients dans $\mathbb{F}_p$)

$$P(X) = X^p - X$$

est de degree $d = p$, la fonction polynomiale sur K ,

$$x \mapsto P(x) = x^p - x$$

ne possede pas plus de d "racines" dans K (de solutions dans K de l'equation

$$P(x) = x^p - x = 0 \ )$$

et comme $\mathbb{F}_p \subset K$ est deja un ensemble de p racines, on les a toutes...

Encore des corps (pour les aficionad.a.o.s)

Exercice 9. On reprend les notations de l'exercice precedent. En particulier p est premier impair. On va etudier l'ensemble des carres de $\mathbb{F}_p$:

$$(\mathbb{F}_p)^2 = \{z^2,\ z \in \mathbb{F}_p\}.$$

L'element nul $0_{\mathbb{F}_p} = 0^2_{\mathbb{F}_p}$ est toujours un carre il reste donc a etudier l'ensemble des carres non-nuls

$$(\mathbb{F}_p^\times)^2 = \{z^2,\ z \in \mathbb{F}_p^\times\}.$$

On va montrer que cet ensemble est non-vide et calculer son cardinal.

1. On note
$$(\mathbb{F}_p^\times)^2 = \{z^2,\ z \in \mathbb{F}_p^\times\}$$
l'ensemble des carres de $\mathbb{F}_p^\times$. Montrer que $(\mathbb{F}_p^\times)^2$ est un sous-groupe du groupe multiplicatif $(\mathbb{F}_p^\times, .)$.
2. Montrer que pour tout $x \in \mathbb{F}_p$ on a
$$x^2 - 1 = (x-1)(x+1)$$
et en deduire que si $x^2 = 1$ alors $x = \pm 1$.
3. Plus generalement, montrer que pour tout $z^2 \in (\mathbb{F}_p^\times)^2$
$$\{x \in \mathbb{F}_p^\times,\ x^2 = z^2\} = \{z, -z\}.$$
Quel est le cardinal de cet ensemble ?.
4. En deduire que
$$|(\mathbb{F}_p^\times)^2| = \frac{p-1}{2}.$$
(on observera que $\mathbb{F}_p^\times$ est la reunion disjointe des sous-ensembles $\{x \in \mathbb{F}_p^\times,\ x^2 = z^2\}$ quand z^2 parcours $(\mathbb{F}_p^\times)^2$).
5. Comme p est impair, $\frac{p-1}{2}$ est un entier. Montrer que pour tout $z \in \mathbb{F}_p^\times$
$$z^{\frac{p-1}{2}} = \pm 1.$$
(calculer $(z^{\frac{p-1}{2}})^2$.)
6. En s'inspirant de la remarque ci-dessus, montrer que
$$|\{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = +1\}| \leqslant \frac{p-1}{2},\ |\{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = -1\}| \leqslant \frac{p-1}{2}$$
et en deduire que
$$|\{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = +1\}| = |\{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = -1\}| = \frac{p-1}{2}.$$
7. Montrer que
$$w \in (\mathbb{F}_p^\times)^2 \Longrightarrow w^{\frac{p-1}{2}} = 1$$
et en deduire qu'en fait
$$(\mathbb{F}_p^\times)^2 = \{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = 1\}.$$
et que
$$\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2 = \{w \in \mathbb{F}_p^\times,\ w^{\frac{p-1}{2}} = -1\}.$$

8. Montrer qu'il existe $w_0 \in \mathbb{F}_p^\times$ tel que $w_0 \notin (\mathbb{F}_p^\times)^2$ (ie. w_0 n'est pas un carre dans $\mathbb{F}_p^\times$) et que
$$\mathbb{F}_p^\times - (\mathbb{F}_p^\times)^2 = w_0.(\mathbb{F}_p^\times)^2 = \{w_0.z^2,\ z \in \mathbb{F}_p^\times\}.$$
9. Montrer que $-1_{\mathbb{F}_p}$ est un carre dans $\mathbb{F}_p$ (il existe $z \in \mathbb{F}_p$ tel que $z^2 = -1_{\mathbb{F}_p}$) si et seulement si $p \equiv 1 \pmod 4$.

Remarque. On peut donc determiner si $w \in \mathbb{F}_p^\times$ est un carre ou pas en calculant sa puissance $w^{\frac{p-1}{2}}$ et en voyant si c'est $+1$ ou -1.

Par exemple prenons $p = 17$ et $w = 3 \pmod{17}$. On a $\frac{p-1}{2} = 8$ et
$$w^8 = ((3^2)^2)^2$$
$$3^2 = 9 \pmod{17},\ 9^2 = 81 \pmod{17} = 13 \pmod{17},$$
$$13^2 = 169 \pmod{17} = 16 \pmod{17} = -1 \pmod{17}$$
et donc $3 \pmod{17}$ n'est pas un carre modulo 17Remarquer que le fait d'ecrire $8 = 2 \times 2 \times 2$ permet de calculer la puissance 8-ieme en trois operations. De la meme maniere pour $p = 23$, $\frac{p-1}{2} = 11$ on calculerait une puissance 11-ieme en decomposant 11 en base 2 :
$$w^{11} = w^8.w^2.w = ((w^2)^2)^2.w^2.w$$
$$3^2 = 9 \pmod{23}, 9^2 \equiv 12 \pmod{23}, 3^8 \equiv 12^2 \equiv 6 \pmod{23}$$
$$6.9.3 = 2.3.9.3 \equiv 2.12 \equiv 1 \pmod{23}$$
de sorte que 3 est un carre modulo 23.

Remarque. Le theoreme Noyau-Image pour les morphismes de groupes finis a ete utiliser sans le dire dans l'argument de la question 4.

Remarque. On a donc montre que pour tout p premier impair, il existe un element de $\mathbb{F}_p$ qui n'est pas un carre dans $\mathbb{F}_p$ (il en existe meme $\frac{p-1}{2}$). Par les exercices 9 et 10 de la serie precedente cela permet de construire un corps fini $\mathbb{F}_{p^2}$ de cardinal p^2 (comme sous-anneau de l'anneau $M_2(\mathbb{F}_p)$).

Exercice 10. Pour $p = 2$, tout element de $\mathbb{F}_2$ est un carre, les exercices de la serie precedente ne permettent donc pas de construire de corps fini a 4 elements. Voici une variante.

1. Pour $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps a deux elements, reprendre l'exercice 9 de la serie 6 avec la matrice
$$I = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2)$$
et montrer que $\mathbb{F}_2[I]$ un anneau commutatif.
2. En utilisant le fait (le montrer) que l'equation $u^2 + u = 1$ n'a pas de solution dans $\mathbb{F}_2$ montrer que $\mathbb{F}_2[I]$ est un corps de cardinal 4. On le note $\mathbb{F}_4$.