EPFL Automne 2021
Algebre Lineaire Avancee, MATH-110

Série 5

Tous les exercices seront corriges. La correction sera postee sur le moodle apres 2 semaines.

Vous etes fortement encourages a essayer de resoudre (eventuellement a plusieurs) l'exercice ($\star$) et a rendre votre solution (eventuellement a plusieurs) avant le dimanche de la semaine suivante celle ou la serie a ete postee. Il faudra transmettre votre solution sur moodle, sous forme de fichier pdf (eventuellement tape en LaTeX) en suivant le lien a cet effet dans la semaine de la serie.

Exercice 1 (Formule du binome)**.** Soit $(A, +, .)$ un anneau, $x, y \in A$ et $n \geqslant 1$ un entier.

1. Montrer que si x et y COMMUTENT pour la multiplication de A (si $x.y = y.x$) on a la formule du binome de Newton :

$$(x+y)^n = (x+y).\cdots.(x+y)\ n \text{ fois} = \sum_{k=0}^{n} C_n^k.x^k.y^{n-k}$$

   ou pour $0 \leqslant k \leqslant n$, $C_n^k \geqslant 1$ est le nombre de sous-ensembles de cardinal k dans un ensemble de cardinal n.

Remarque 0.1. On rappelle la formule des coefficients du binome obtenue par denombrement

$$C_n^k = \frac{n!}{k!(n-k)!}$$

avec

$$n! = n.(n-1).\cdots.1,\ n \geqslant 1,\ 0! = 1.$$

Exercice 2. Soit A un anneau et $(M, +)$ un A-module dont la multiplication par les scalaire de A est notee $\star$. Pour $n \in \mathbb{Z}$, on rappelle que l'on pose

$$n_A = 1_A + \cdots + 1_A \ (n \text{ fois si } n \geqslant 0), n_A = (-1_A) + \cdots + (-1_A) \ (-n \text{ fois si } n < 0)$$

l'image de $n \in \mathbb{Z}$ par le morphisme canonique $\mathrm{Can}_A : \mathbb{Z} \mapsto A$, et pour $m \in M$, on pose

$$n.m = m + \cdots + m \ (n \text{ fois si } n \geqslant 0), = (-m) + \cdots + (-m) \ (-n \text{ fois si } n < 0)$$

(la multiplication qui fait de M un $\mathbb{Z}$-module car c'est un groupe commutatif note additivement)

1. Montrer que pour tout $n \in \mathbb{Z}$ et $m \in M$ on a

$$n_A \star m = n.m.$$

Autrement dit les structures de $\mathbb{Z}$-module et de A-module sur M sont compatible avec le morphisme canonique.

Exercice 3. Soient $(A, +_A, ._A)$ et $(B, +_B, ._B)$ deux anneaux commutatifs. On considere l'anneau produit

$$A \times B = \{(a, b),\ a \in A,\ b \in B\}$$

muni de l'addition et de la multiplication

$$(a, b) + (a', b') = (a +_B a', b +_B b'),\ (a, b).(a', b') = (a._A a', b._B b')$$

avec comme neutre et unite $0_{A\times B} = (0_A, 0_B),\ 1_{A\times B} = (1_A, 1_B)$.

1. Montrer que si A et B ne sont pas des anneaux nuls alors $A \times B$ n'est pas un anneau integre (meme si A et B sont integres).

Exercice 4. ($\star$) Dans cet exercice on va demontrer le resultat suivant :

Lemme. *Soit A un anneau non-nul commutatif, integre et FINI alors A est un corps (tout element non-nul de A est inversible).*

Soit donc $a \in A - \{0_A\}$ non-nul, on veut montrer que a admet un inverse dans A.

Pour cela on considere la suite d'element de A, donnee pour tout entier $n \geqslant 0$ par

$$a_n := a^n = a.a. \cdots .a \ (n \text{ fois})$$

(avec $a^0 = 1_A$).

1. Montrer qu'il existe deux entiers $0 \leqslant m < n$ tels que $a^n = a^m$.
2. En deduire qu'il existe un entier $k \geqslant 1$ tel que $a^k - 1_A = 0_A$.
3. Conclure.

Exercice 5. Soit K un corps et $I \subset K$ un sous K-espace vectoriel de K (vu que K-EV) ; autrement dit un sous K-module de K, cad un sous-groupe additif de K stable par multiplication par K (aka encore un ideal de l'anneau K).

1. Montrer que $I = \{0_K\}$ ou bien $I = K$.
2. En deduire qu'un morphisme d'anneau $\varphi : K \mapsto A$ est soit nul, soit injectif et que si V est un K-ev un morphisme $\varphi : K \mapsto V$ est soit nul, soit injectif.
3. Montrer qu'un morphisme de K-EVs $\ell : V \mapsto K$ est soit nul soit surjectif.

Exercice 6. Soit K et L des corps et

$$\varphi : K \mapsto L$$

un morphisme d'anneaux non nul ($\varphi \neq \underline{0}_L$). Pour $n \in \mathbb{Z}$ on note

$$n_K = \text{Can}_K(n) = n.1_K \text{ (resp. } n_L = \text{Can}_L(n) = n.1_K)$$

l'image de n par les morphismes canoniques respectifs.

1. Montrer que pour tout $n \in \mathbb{Z}$, $\varphi(n_K) = n_L$.
2. En deduire que necessairement $\text{car}(K) = \text{car}(L)$.

Exercice 7. Soit K un corps de caracteristique $\text{car}(k) = p$ un nombre premier et $\mathbb{F}_p = \mathbb{Z}.1_K = \{n_K = n.1_K,\ n \in \mathbb{Z}\}$ le sous-corps premier de K.

Une consequence de la caracteristique p est que l'application d'elevation a la puissance p dans K

$$\bullet^p : \begin{array}{ccc} K & \mapsto & K \\ x & \mapsto & x^p \end{array},\ x^p = x.\cdots.x\ (p \text{ fois})$$

a des proprietes tres particulieres. On appelle cette application le Frobenius en p et on la note $\text{frob}_p : x \mapsto x^p$.

1. Soit
$$C_p^k = \frac{p!}{k!(p-k)!}$$
les coefficients de la formule du binome. Montrer que pour $1 \leqslant k \leqslant p-1$ on a que p divise C_p^k (utiliser le fait que p est premier).
2. En deduire que pour $x, y \in K$, on a
$$(x+y)^p = x^p + y^p$$
puis que frob_p est un morphisme de corps (cad. d'anneau) de K sur lui-meme.
3. Montrer que si K est un corps fini alors frob_p est un automorphisme de corps (cad. d'anneau).

Exercice 8. Soit p un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini de cardinal p.

1. Montrer que pour tout $x \in \mathbb{F}_p$, on a
$$x^p = x.$$
On pourra ecrire x sous la forme $x = n.1_{\mathbb{F}_p}$ avec $n \geqslant 0$ et raisonnera par recurrence on utilisant les proprietes du Frobenius sur $\mathbb{F}_p$.

2. Montrer que pour tout $x \in \mathbb{F}_p^\times$ on a
$$x^{p-1} = 1.$$
3. Montrer que si $p \equiv 3 \pmod 4$ alors $-1 \pmod p$ n'est pas un carre dans $\mathbb{F}_p$: il n'existe pas de $x \in \mathbb{F}_p$ tel que $x^2 = -1 \pmod p$. Pour cela on calculera de deux manieres la puissance
$$(-1)^{\frac{p-1}{2}} \pmod p.$$

Exercice 9. 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 l'application
$$\bullet + \bullet : \begin{array}{ccc} X \times Y & \mapsto & V \\ (x, y) & \mapsto & x + y \end{array}$$
est un isomorphisme d'espaces vectoriels.
2. Montrer que les applications
$$\pi_X : v \in V \mapsto x \in X, \ \pi_Y : v \in V \mapsto y \in Y$$
(ou x et y sont definis par (0.1)) sont lineaires.

1 Exercices a continuer la semaine prochaine (si necessaire)

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 des corps finis $\mathbb{F}_{p^2}$ de cardinal p^2 pour p premier.

Exercice 10 (Construction de corps a partir de matrices)**.** Soit K un corps d'element nul et d'unite notes respectivement 0 et 1 et
$$M_2(K) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ a, b, c, d \in K \}$$

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

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

et que le groupe des elements inversible de cet anneau est donne par

$$M_2(K)^\times = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix},\ a,b,c,d \in K,\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in K^\times = K - \{0\}\}.$$

1. Montrer 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 scalaire et la multiplication des matrices : pour $\lambda \in K,\ M, N \in M_2(A)$
$$\lambda.(M \times N) = (\lambda.M) \times N$$
(on dit alors que l'anneau $M_2(K)$ est une K-algebre).
2. Montrer que l'ensemble des matrices multiples de l'identite (qu'on appelle matrices scalaires)
$$K.\mathrm{Id}_2 = \{\lambda.\mathrm{Id}_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},\ \lambda \in K\}$$
forme un sous-anneau de $M_2(K)$ qui est en fait un corps isomorphe a K. C'est le corps des matrices scalaires 2×2.
3. 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
$$K[I_d] := \langle \mathrm{Id}_2, I_d \rangle = K.\mathrm{Id}_2 + K.I_d = \{x.\mathrm{Id}_2 + y.I_d,\ x, y \in K\} \subset M_2(K)$$
le sous-K espace vectoriel de $M_2(K)$ engendre 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 $I_d^2 = I_d \times I_d$).

4. Donner une valeur de d pour laquelle $K[I_d]$ n'est pas un anneau integre .
5. On suppose que d n'est pas un carre dans K (ie. il n'existe pas de $u \in K$ tel que $u^2 = d$; par exemple is $K = \mathbb{R}$, $d = -1$ marche). Montrer que l'equation
$$x^2 - dy^2 = 0$$
n'a pas de solution $x, y \in K$.
6. Montrer que $K[I_d]$ est un corps. Pour cela on calculera le determinant d'un element non-nul de $K[I_d]$ et on verifiera que son inverse est encore dans $K[I_d]$.
7. Remarquer que ce corps contient un sous-corps isomorphe a K.
8. On suppose que d est un carre dans K (ie. il existe $x \in K$ tel que $x^2 = d$). Montrer que $K[I_d]$ n'est pas integre.

Exercice 11. On reprend l'exercice precedent en supposant que K est un corps fini $\mathbb{F}_p$ pour p premier.

1. Quel est la cardinal de $M_2(\mathbb{F}_p)$? Celui de $K[I_d]$?
2. Donner un exemple de corps a 9 elements ; de corps a 25 elements ? On note ces corps $\mathbb{F}_9$ et $\mathbb{F}_{25}$ et on rappelle qu'il contiennent des sous-corps isomorphes a $\mathbb{F}_3$ et $\mathbb{F}_5$ (les corps de matrices scalaires $\mathbb{F}_3.\mathrm{Id}_2$ et $\mathbb{F}_5.\mathrm{Id}_2$). Par abus de language et identification on supposera qu'ils contiennent $\mathbb{F}_3$ et $\mathbb{F}_5$.
3. Montrer que la classe de congruence $-1 \pmod 3) \in \mathbb{F}_3$ est un carre dans $\mathbb{F}_9$ bien qu'elle ne soit pas un carre dans $\mathbb{F}_3$.
4. Montrer que la classe de congruence $2 \pmod 5) \in \mathbb{F}_5$ est un carre dans $\mathbb{F}_{25}$ bien qu'elle ne soit pas un carre dans $\mathbb{F}_5$.

Remarque 1.1. Plus generalement on peut montrer que pour tout premier p impair il existe $d \in \mathbb{F}_p$ qui n'est pas un carre (par exemple en montrant que le nombre de non-carres de $\mathbb{F}_p$ vaut $\frac{p-1}{2}$). Cela permet d'exhiber des corps finis a p^2 elements.

Exercice 12. L'exercice 10 ne permet pas de construire un corps fini de cardinal 4 (pourquoi ?).

1. Pour $K = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps a deux elements, reprendre l'exercice 10 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 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.