L3B Année 2017/2018

JUSTIFIER TOUTES VOS REPONSES

Exercice 1

1. (a) Montrer que l'anneau $\mathbb{R}[X]$ est intègre

Soient $P, Q \in \mathbb{R}[X]$ non nuls.
Si PQ est nul alors

$$P(\alpha)Q(\alpha) = 0, \forall \alpha \in \mathbb{R}.$$

Or $\mathbb{R}$ est un corps donc intègre
$\Rightarrow P(\alpha) = 0$ ou $Q(\alpha) = 0$. On voit ainsi P ou Q a une infinité de racines.
On peut aussi raisonner avec le degré.

(b) Donner un exemple d'un anneau commutatif A qui n'est pas intègre.

$\mathbb{Z}/12\mathbb{Z}$ n'est pas integre car $\bar{4}\bar{3} = \bar{1}\bar{2} = \bar{0}$.

(c) Montrer que si A est intègre alors $\forall P, Q \in A[X]$

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Soient $P, Q \in A[X]$ avec $\deg(P) = m$, $\deg(Q) = n$.
Il s'ensuit de la definition du produit PQ que :

$$\deg(PQ) \leq \deg(P) + \deg(Q).$$

Par hypothèse $\exists a_m, b_n \in A \setminus \{0_A\}$ et $P_1, Q_1 \in A[X]$
avec $\deg(P_1) < \deg(P)$ et $\deg(Q_1) < \deg(Q)$ tq :

$$\begin{aligned} P &= a_m X^m + P_1 \\ Q &= b_n X^n + Q_1 \end{aligned}$$

On a :

$$PQ = (a_m b_n)X^{m+n} + b_n X^n P_1 + a_n X^m Q_1$$

A integre $\Rightarrow a_m b_n \neq 0_A \Rightarrow \deg(PQ) = m + n$.

(d) Montrer qu'un polynôme $P \in \mathbb{C}[X]$ non nul est inversible si et seulement si $\deg(P) = 0$.

i. On suppose $\deg(P) = 0$ non nul alors $\exists \alpha \in \mathbb{C}^*$ tel que $P = \alpha$ et $P^{-1} = \alpha \in \mathbb{C}^*$.

ii. On suppose P inversible et en part. $P \neq 0 \Rightarrow \deg(P) \geq 0$.

$$0 = \deg(1_A) = \deg(PP^{-1}) = \deg(P) + \deg(P^{-1})$$

$\Rightarrow \deg(P) \leq 0$

(e) En déduire que $\forall \alpha \in \mathbb{C}$ le polynome $X - \alpha$ est irréductible dans $\mathbb{C}[X]$.

On suppose $\exists P, Q \in \mathbb{C}[X]$ tq

$$X - \alpha = PQ.$$

en part P, Q sont non nuls. On a

$$1 = \deg(X - \alpha) = \deg(P) + \deg(Q)$$

$\Rightarrow \deg(P) = 0$ ou $\deg(Q) = 0$.
$\Rightarrow P$ ou Q inversible.

(f) Vrai ou faux : $P \in \mathbb{R}[X]$ est irréductible si et seulement si il est irreductible dans $\mathbb{C}[X]$. Justifier votre réponse.

NON
$X^2 + 1$ est irréductible car il n'a pas de racine dans $\mathbb{R}$.

(g) On rappelle que deux éléments x, y d'un anneau commutatif A sont premiers entre eux ssi les seuls diviseurs communs sont les inversibles de A.

i. Montrer que $X, X - 1, X + 1$ sont 2-à-2 premiers entre eux dans l'anneau $\mathbb{C}[X]$.

Il suffit de montrer que pour chaque paire un diviseur commun divise un inversible:

A. Si d un diviseur commun de $X, X - 1$ alors
d divise $X - (X - 1) = 1$ donc d est inversible.

B. Si d un diviseur commun de $X + 1, X - 1$ alors
d divise $X + 1 - (X - 1) = 2$ donc d est inversible.

ii. Les polynômes $X, X-1, X+1$ sont-ils 2-à-2 premiers entre eux dans l'anneau $\mathbb{Z}[X]$?

OUI
Les arguments pour $X, X-1$ et $X, X+1$ sont tjrs valable.
Pour $X-1, X+1$ on a:

$$2 = (X+1) - (X-1).$$

Donc si d est diviseur commun alors $d|2$ et $d \in \{\pm 1\} \sqcup \{\pm 2\}$.
On suppose $d = \pm 2$ et on a l'equation

$$\pm 2P(X) = (X+1),$$

en evaluant en 0

$$\pm 2P(0) = 1,$$

impossible car $P(0) \in \mathbb{Z}$.
Donc d inversible

(h) Montrer que

$$\mathbb{C}[X]/(X) \simeq \mathbb{C}[X]/(X+1) \simeq \mathbb{C}[X]/(X-1).$$

Si $\alpha \in \mathbb{C}$ alors $(X-\alpha)$ est le noyau du morphisme d'evaluation $\mathrm{ev}_\alpha : \mathbb{C}[X] \to \mathbb{C}$
et on a

$$\mathbb{C}[X]/(X) \simeq \mathrm{Im}(\mathrm{ev}_\alpha) = \mathbb{C}.$$

(i) Montrer que

$$\mathbb{C}[X]/(X) \not\simeq \mathbb{R}[X]/(X+1).$$

D'apres la question precedente

$$\mathbb{C}[X]/(X) \simeq \mathbb{C},\ \mathbb{R}[X]/(X+1) \simeq \mathbb{R}.$$

Suppose qu'il existe $\phi : \mathbb{C} \to \mathbb{R}$ un morphisme d'anneau.
Alors

$$-1 = \phi(-1) = \phi(i^2) = (\phi(i))^2 \geq 0.$$

Contradiction

2. (a) Trouver $a, b, c \in \mathbb{Z}$ tels que

$$aX(X-1) + bX(X+1) + c(X^2-1) = 2.$$

- $X = -1$, $-a(-2) = 2 \Rightarrow a = 1$.
- $X = 1$, $b(2) = 2 \Rightarrow b = 1$.
- $X = 0$, $-c = 2 \Rightarrow c = -2$.

$$X(X-1) + X(X+1) - 2(X^2-1) = 2.$$

(b) Déterminer l'idéal de $\mathbb{R}[X]$ engendré par :

i. $\{X(X-1), X(X+1), X^2-1\}$.

D'apres question (2a) $2 \in (X(X-1), X(X+1), X^2-1)$.
D'apres question (1d). 2 est inversible et donc $(2) = \mathbb{R}[X]$.
On a donc

$$\mathbb{R}[X] = (2) \subset (X(X-1), X(X+1), X^2-1) \subset \mathbb{R}[X].$$

ii. $\{X^2(X+1), (X^2-1)^2\}$

$\mathbb{R}[X]$ est principal et un generateur
de l'ideal $(X^2(X+1), (X^2-1)^2)$ est le PGCD de ces polynomes à savoir $X+1$.

(c) Déterminer l'inverse de $\overline{X(X-1)} \in \mathbb{R}[X]/(X+1)$.

D'apres question (2a):

$$X(X-1) + X(X+1) - 2(X^2-1) = 2.$$

Donc

$$\overline{X(X-1)} + \overline{X(X+1)} - \overline{2(X^2-1)} = \bar{2}.$$

$$\overline{X(X-1)} = \bar{2} \Rightarrow \overline{X(X-1)}^{-1} = \overline{1/2}.$$

(d) Soient $\alpha, \beta, \gamma \in \mathbb{R}$ trouver un polynome $P \in \mathbb{R}[X]$ de degré au plus 2 tel que

$$P(-1) = \alpha,\ P(0) = \beta,\ P(1) = \gamma.$$

$$P(X) = \frac{1}{2}\alpha X(X-1) + \frac{1}{2}\gamma X(X+1) - \beta(X^2-1).$$

(e) Montrer que l'application

$$\begin{array}{rcl} \mathbb{R}[X] & \to & \mathbb{R}\times\mathbb{R}\times\mathbb{R} \\ P & \mapsto & (P(-1),P(0),P(1)) \end{array}$$

est un morphisme surjectif et déterminer son noyau.

- Il suffit de verifier que l'application induit un morphisme sur chaque facteur à l'arrivée.
  Or $P \mapsto P(\alpha)$ est le morphisme d'evaluation $\mathbf{ev}_\alpha$.
- D'apres la question (2d) l'application est surjective.
- Le noyau est l'intersection des noyaux de $\mathbf{ev}_{-1}$, $\mathbf{ev}_0$, $\mathbf{ev}_1$. Or $\ker \mathbf{ev}_\alpha = (X-\alpha)$

  $$(X+1)\cap(X)\cap(X-1) = (X(X^2-1)),$$

  car le PPCM de $X+1, X, X-1$ est $X(X^2-1)$ car ils sont premiers entre eux.

3. (a) Montrer que X^2+X+1 est irréductible dans $\mathbb{R}[X]$.

Un polynome $P \in \mathbb{R}[X]$ tq $2 \leq \deg(P) \leq 3$ est irreductible ssi P n'a pas de racines. Or

$$t^2+t+1 = (t+1/2)^2 + 3/4 \geq 3/4 > 0,\ \forall t \in \mathbb{R}.$$

(b) Déterminer les idéaux de $\mathbb{R}[X]/(X^2+X+1)$.

X^2+X+1 est irreductible
$\Rightarrow (X^2+X+1)$ est maximal
$\Rightarrow \mathbb{R}[X]/(X^2+X+1)$ est un corps ($\simeq \mathbb{C}$).

Un corps a exactement 2 ideaux.

4. Donner tous les inversibles de $(\mathbb{Z}/12\mathbb{Z},+)$.

$\bar{n} \in \mathbb{Z}/12\mathbb{Z}$ est inversible ssi $n \wedge 12 = 1$.
Donc $(\mathbb{Z}/12\mathbb{Z})^* = \bar{1}, \bar{5}, \bar{7}, \bar{11}$.

$$o(\bar{1}) = o(\bar{5}) = o(\bar{7}) = o(\bar{11}) = 12.$$

Exercice 2

1. Soient $n_1, n_2, a_1, a_2 \in \mathbb{Z}$ tels que

$$a_1 n_1 + a_2 n_2 = 1.$$

Montrer que, si

$$y_1 \equiv m_1[n_1] \text{ et } y_2 \equiv m_2[n_2]$$

alors

$$y \equiv m_1[n_1] \text{ et } y \equiv m_2[n_2]$$

où $y := a_1 n_1 y_2 + a_2 n_2 y_1$.

> Par hypothese :
>
> $$a_1 n_1 \equiv= 1[n_2],\ a_2 n_2 = 1[n_1].$$
>
> Donc $y := a_1 n_1 y_2 + a_2 n_2 y_1 \equiv a_1 n_1 y_2[n_2] \equiv 1 y_2[n_2] \equiv m_2[n_2]$.

2. Utiliser le petit théorème de Fermat pour montrer que si $x \in \mathbb{Z}$ n'est pas divisible par 7 alors $x^3 \equiv \pm 1[7]$.

> Fermat : $x^{p-1} \equiv 1\,[p]$ si p premier et $p \not| x$. $\Rightarrow x^6 \equiv 1\,[7]$
> $\Rightarrow (x^3)^2 \equiv 1\,[7]$
> L'equation $y^2 = 1[7]$ a exactement 2 solutions, à savoir $y = \pm 1[7]$.

3. Trouver toutes les solutions de

   (a) $x^3 - x + 1 \equiv 0[5]$

> On notera $f(x) = x^3 - x + 1$
> On a $f(\bar{0}) = \bar{1}, f(\bar{1}) = \bar{1}, f(\bar{2}) = \bar{2}, f(\bar{3}) = \bar{0}, f(\bar{4}) = \bar{1}$

   (b) $x^3 - x + 1 \equiv 0[7]$

> D'apres (2) $x^3 - x + 1 \equiv 0[7] \Rightarrow x = (\pm 1 + 1)[7]$
> - $x = 0$ est visiblement pas une racine
> - $2^3 - 2 + 1 = 8 - 2 + 1 = 7 \Rightarrow$ une solution unique.

   (c) $x^3 - x + 1 \equiv 0[35]$

Toute solution x est une solution du systeme

$$\begin{aligned} x^3 - x + 1 &\equiv 0[5] \\ x^3 - x + 1 &\equiv 0[7] \end{aligned}$$

On a $3 \times 7 - 4 \times 5 = 1$ et d'apres (1)

$$x = 3 \times 7 \times 2 - 4 \times 5 \times 3 = 42 - 50 \equiv 23[35].$$

4. (a) Donner tous les diviseurs de zéro de l'anneau $\mathbb{Z}/13\mathbb{Z}$.

$13 \in \mathbb{Z}$ est premier et $\mathbb{Z}/13\mathbb{Z}$ est un corps
$\Rightarrow$ pas de diviseur de zero.

(b) Déterminer l'ordre de $\bar{4}$ dans le groupe $(\mathbb{Z}/13\mathbb{Z})^*$.

$4^2 = 16 \neq 1[13]$ et $4^3 = 64 = -1[13] \Rightarrow o(\bar{4}) = 6$

(c) Trouver l'inverse de $\bar{4}$ dans le groupe $(\mathbb{Z}/13\mathbb{Z})^*$.

$4 \times 10 = 40 = 1[13] \Rightarrow \bar{4}^{-1} = \overline{10}$

(d) On considère l'application;

$$\begin{aligned} f : (\mathbb{Z}/13\mathbb{Z})^* &\to (\mathbb{Z}/13\mathbb{Z})^* \\ x &\mapsto \bar{4}x \end{aligned}$$

i. Montrer que f est une permutation de l'ensemble $(\mathbb{Z}/13\mathbb{Z})^*$.

Il suffit de montrer que f est une bijection. D'apres la question precedente

$$f^{-1}; x \mapsto \bar{4}^{-1}x = \bar{10}x.$$

ii. Donner la décomposition de f en cycles disjoints.

L'ordre de $\bar{4}$ est 6 et on s'attend à ce que f se decompose en 2 cycles de longueur 6.

$$(\bar{4}, \bar{3}, \bar{12}, \bar{9}, \bar{10}, \bar{1})(\bar{8}, \bar{6}, \bar{11}, \bar{5}, \bar{7}, \bar{2})$$

iii. Déterminer la signature de f.

- La signature est un morphisme de groupes
- La signature d'un cycle ne depend que de la longueur du cycle.
- f est composition de 2 cycles γ_i de longueur 6 :

$$\sigma(f) = \sigma(\gamma_1 \circ \gamma_2) = \sigma(\gamma_1)^2 = 1$$

(e) i. Determiner l'ordre de $\bar{2}$ dans $(\mathbb{Z}/13\mathbb{Z})^*$.

$$\bar{2}^2 = \bar{4} \Rightarrow o(\bar{2}) = 2 \times o(\bar{4}) = 12 = |(\mathbb{Z}/13\mathbb{Z})^*|$$

ii. Vrai ou faux : $((\mathbb{Z}/13\mathbb{Z})^*, \times) \simeq (\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. Justifier votre réponse.

NON
$(\mathbb{Z}/13\mathbb{Z})^*$ est cyclique car élément $\bar{2}$ d'ordre 12.
l'ordre maximal d'un elt dans $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est 6.

iii. Donner tous les éléments d'ordre maximal dans $(\mathbb{Z}/13\mathbb{Z})^*$.

D'apres la question $(\mathbb{Z}/12\mathbb{Z})^* = \bar{1}, \bar{5}, \bar{7}, \bar{11}$
et chacun de ces elts est generateur de $(\mathbb{Z}/12\mathbb{Z}, +)$.
Donc les generateurs de $(\mathbb{Z}/13\mathbb{Z})^*$ sont

$$\bar{2^1}, \overline{2^5} = \bar{6}, \overline{2^7} = \bar{11}, \overline{2^{11}} = \bar{7},$$

Exercice 3

On considère un endomorphisme u de $\mathbb{R}^3$ dont la matrice dans la base usuelle est :

$$A := \begin{pmatrix} 2 & -1 & 1 \\ -2 & 0 & 2 \\ -2 & -3 & 5 \end{pmatrix}$$

1. Calculer le déterminant et la trace de A.

$\operatorname{tr} A = 7$, $\det A = 12$.

2. (a) $f_1 = (0,1,1), f_2 = (-1,1,1) \in \mathbb{R}^3$ et F le sous espace vectoriel engendré par f_1 et f_2. Montrer que F est stable par u.

F stable ssi $u(F) \subset F$.
Puisque $F = \{f_1, f_2\}$ il suffit de verifier que $u(f_i) \in F$

$$A.f_1 = 2f_1 \in F,\ A.f_2 = 2f_1 + 2f_2 \in F.$$

(b) Déterminer la matrice de la restriction de u à F dans la base f_1, f_2.

Il se decoule du calcul ci-dessus que la matrice de $u|_F$ est

$$\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

3. (a) Déterminer le polynôme carateristique $\chi_u(X) \in \mathbb{R}[X]$ de u.

On peut faire sans calculer le determinant usuelle car d'apres question (2b) 2 est racine de multiplicité 2 et la trace de $A = 7$ donc l'autre racine est $7 - 2 \times 2 = 3$.

$$\chi_u(X) = \chi_A(X) = (X-2)^2(X-3).$$

(b) Déterminer les valeurs propres et sous-espaces propres de u.

- vp 2, ep $\langle(0,1,1)\rangle$
- vp 3, ep $\langle(1,0,1)\rangle$ donc $f_3 := (1,0,1)$ est vp.

(c) u est-il diagonalisable sur $\mathbb{R}$? trigonalisable sur $\mathbb{R}$?

- NON - 2 est racine de χ_u de multiplicité 2 mais son espace propre est de dimension 1
- OUI - χ_u est scindé sur $\mathbb{R}$.

4. Donner le polynôme minimal de u.

Le poly minimal a les memes racines que le poly caracteristique (cours).
Afin de voir que χ_u est minimal suffit de verifier que $(u-2)(u-3) \neq 0$.

On a

$(u-2)(u-3) = (u-2)^2-(u-2) \Rightarrow (u-2)(u-3).f_2 = -u(f_2)+2f_2 \neq 0.$

Rq - effectivement on peut remplacer f_2 par n'importe lequel elt de

$$\ker(u-2)^2 \setminus \ker(u-2).$$

5. Ecrire, en utilisant le lemme des noyaux, $\mathbb{R}^3$ comme somme directe de F et d'un sous-espace G stable par u. Donner une base de chacun des ces sous-espaces.

On a

$$\mathbb{R}^3 = \ker(u-2\mathrm{ID})^2 \oplus \ker(u-3\mathrm{ID}).$$

et on pose
$F := \langle (0,1,1), (-1,1,1) \rangle = \ker(u-2\mathrm{ID})^2$
$G := \langle (1,0,1) \rangle = \ker(u-3\mathrm{ID})$

6. Soit p la projection sur F parallèlement à G. Ecrire p comme un polynôme en u. On utilisera Bezout pour les polynômes $(X-2)^2$ et $X-3$.

$$(X-2)^2 - (X-1)(X-3) = 1$$

$F = \ker(u-2\mathrm{ID})^2$
$\Rightarrow p = I_3 - (A-2I_3)^2 = -(A-I_3)(A-3I_3),$
de plus on a $G = \ker(u-3) \subset \ker(u-1) \circ (u-3) = \ker p$
en part $p(f_3) = 0$.

7. Donner la décomposition de Dunford de A. Ecrire chacune des matrices de la décomposition comme un polynôme en A.

$D := 2p + 3(I_3 - p)$ et on a :

$$D.f_i = 2p(f_i) + 3(f_i - p(f_i), i = 1,2,3$$

il s'ensuit que u est diagonalisable car f_i est une base de $\mathbb{R}^3$ de vecteurs propres :

(a) $D.f_i = 2p(f_i) + 3(f_i - p(f_i) = 2f.i - 3(f_i - f_i), i = 1,2$
(b) $D.f_3 = 2p(f_3) + 3(f_3 - p(f_3)) = 3f_3$