Série 5 (Corrigé)

L'exercice 1 sera discuté pendant le cours du lundi 24 octobre.
L'exercice 4 ($\star$) peut être rendu le jeudi 27 octobre aux assistants jusqu'à 15h.

Exercice 1 - QCM

(a) Déterminer si les énoncés proposés sont vrais ou faux.

- Soit $A \in M_{n\times n}(\mathbb{R}[t])$. S'il existe $B \in M_{n\times n}(\mathbb{R}[t])$ telle que $AB = I_n$, alors il existe $\tilde{B} \in M_{n\times n}(\mathbb{R}[t])$ telle que $\tilde{B}A = I_n$.

  ○ vrai ○ faux

- Soit $A \in M_{n\times n}(\mathbb{F}_2)$. S'il existe $B \in M_{n\times n}(\mathbb{F}_2)$ telle que $AB = I_n$, alors il existe $\tilde{B} \in M_{n\times n}(\mathbb{F}_2)$ telle que $\tilde{B}A = I_n$.

  ○ vrai ○ faux

- Soit $f \in \mathbb{C}[t]$ et soit $a \in \mathbb{C}$. Alors $t - a$ divise $f(t) - f(a)$.

  ○ vrai ○ faux

- Le polynôme $t^4 + 4 \in \mathbb{F}_5[t]$ est scindé dans $\mathbb{F}_5[t]$.

  ○ vrai ○ faux

- Deux polynômes $f, g \in \mathbb{C}[t]$ à coefficients complexes sont premiers entre eux s'ils n'ont aucune racine commune.

  ○ vrai ○ faux

(b) Soit $A \in M_{n\times n}(\mathbb{R})$. Lesquelles des assertions suivantes sont correctes ?

○ Supposons que $Ax = b$ n'a pas de solution dans $\mathbb{R}^n$ pour un vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.

○ Supposons que $Ax = b$ a une seule solution dans $\mathbb{R}^n$ pour chaque vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.

○ Supposons que $Ax = b$ a plusieurs solutions dans $\mathbb{R}^n$ pour un vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.

Indice : Considérer les parties réelles et imaginaires de l'expression $A(\mathrm{Re}(x) + \mathrm{i}\mathrm{Im}(x))$.

Sol.:

(a) Déterminer si les énoncés proposés sont vrais ou faux.

- *Soit $A \in M_{n\times n}(\mathbb{R}[t])$. S'il existe $B \in M_{n\times n}(\mathbb{R}[t])$ telle que $AB = I_n$, alors il existe $\tilde{B} \in M_{n\times n}(\mathbb{R}[t])$ telle que $\tilde{B}A = I_n$.*

  ● *vrai* ○ *faux*

- *Soit $A \in M_{n\times n}(\mathbb{F}_2)$. S'il existe $B \in M_{n\times n}(\mathbb{F}_2)$ telle que $AB = I_n$, alors il existe $\tilde{B} \in M_{n\times n}(\mathbb{F}_2)$ telle que $\tilde{B}A = I_n$.*

  ● *vrai* ○ *faux*

- *Soit $f \in \mathbb{C}[t]$ et soit $a \in \mathbb{C}$. Alors $t - a$ divise $f(t) - f(a)$.*

  ● *vrai* ○ *faux*

- *Le polynôme $t^4 + 4 \in \mathbb{F}_5[t]$ est scindé dans $\mathbb{F}_5[t]$.*

  ● *vrai* ○ *faux*

- *Deux polynômes $f, g \in \mathbb{C}[t]$ à coefficients complexes sont premiers entre eux s'ils n'ont aucune racine commune.*

  ● *vrai* ○ *faux*

(b) Soit $A \in M_{n\times n}(\mathbb{R})$. Lesquelles des assertions suivantes sont correctes ?

● *Supposons que $Ax = b$ n'a pas de solution dans $\mathbb{R}^n$ pour un vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.*

● *Supposons que $Ax = b$ a une seule solution dans $\mathbb{R}^n$ pour chaque vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.*

○ *Supposons que $Ax = b$ a plusieurs solutions dans $\mathbb{R}^n$ pour un vecteur $b \in \mathbb{R}^n$. Alors il n'existe pas de $x \in \mathbb{C}^n \backslash \mathbb{R}^n$ tel que $Ax = b$.*

Exercice 2

Soient $A \in M_{m\times n}(\mathbb{C})$ et $B \in M_{n\times p}(\mathbb{C})$. Montrer que $(AB)^* = B^*A^*$.

Sol.: *Il est facile de voir que, pour $a, b \in \mathbb{C}$ on a $\overline{ab} = \overline{b}\overline{a}$. Maintenant, on a,*

$$(AB)^*_{i,j} = \overline{(AB)_{j,i}} = \sum_{k=1}^{n} \overline{A_{j,k}B_{k,i}} = \sum_{k=1}^{n} \overline{B_{k,i}}\ \overline{A_{j,k}} = (B^*A^*)_{i,j},$$

$i = 1, \ldots, m$, $j = 1, \ldots, p$, ainsi $(AB)^* = B^*A^*$.

Exercice 3

i) Pour quelle(s) valeur(s) de $\alpha, \beta, \gamma \in \mathbb{R}$ la matrice suivante est-elle hermitienne ?

$$A = \begin{pmatrix} 2 & 1+\alpha i & 4-\beta i \\ 1+\alpha i & 0 & \gamma - 3i \\ 4+2i & \beta + 3i & -1 \end{pmatrix}$$

ii) Soit $A \in M_{n\times n}(\mathbb{C})$ une matrice hermitiene et $v \in M_{n\times 1}(\mathbb{C})$. Montrer que v^*Av est réel.

Sol.:

i) Pour que A soit hermitienne, il faut que $4 - \beta i = \overline{4+2i}$, donc $\beta = 2$. De plus on doit avoir, $\gamma - 3i = \overline{\beta + 3i}$ qui donne $\gamma = \beta = 2$. $1 + \alpha i = \overline{1+\alpha i}$ et donc $\alpha = 0$.

ii) En utilisant l'exercice 2 avec v^*Av, on trouve

$$(v^*Av)^* = v^*(v^*A)^* = v^*A^*v = v^*Av.$$

Comme v^*Av est une matrice de taille 1×1 et qu'elle est hermitienne, on peut conclure que v^*Av est réel.

Exercice 4 ($\star$)
Montrer les parties *ii*) et *iv*) du Théorème 2.36 du cours (voir la version du Chapitre 2 actualisée 20.10.2016.).

Sol.:

- *ii*) *On montre que* $(\mathbb{N}_{<p}, \odot)$ *est un monoïde commutatif.*
  - *Soient* $a, b \in \mathbb{N}_{<p} = \{0, 1, 2, \ldots, p-1\}$. *Comme* $a \odot b$ *est la reste dans la division euclidienne de* ab *par* p, *donc* $0 \leq a \odot b \leq p-1$.
  - *L'associativité : soient* $a, b, c \in \mathbb{N}_{<p}$. *Par la definition de la division euclidienne, il existe* $k_1, k_2 \in \mathbb{N}$ *et* $r_1, r_2 \in \mathbb{N}_{<p}$ *tels que* $ab = k_1 p + r_1$, *i.e.* $a \odot b = ab - k_1 p$ *et* $bc = k_2 p + r_2$, *i.e.* $b \odot c = bc - k_2 p$. *Donc,*

    $$\begin{aligned} (a \odot b) \odot c &= (ab - k_1 p) \odot c = \text{reste de la division eucl. de } (ab - k_1 p)c \text{ par } p \\ a \odot (b \odot c) &= a \odot (bc - k_2 p) = \text{reste de la division eucl. de } a(bc - k_2 p) \text{ par } p \end{aligned}$$

    On observe que $(ab - k_1 p)c$ *et* $a(bc - k_2 p)$ *diffère d'un multiple de* p. *Cela implique que* $(a \odot b) \odot c =$ *reste de la division eucl. de* abc *par* p *et* $a \odot (b \odot c)$*reste de la division eucl. de* abc *par* p. *Donc, l'associativité est satisfaite.*
  - *L'élément neutre est* 1.
  - *La commutativité découle de la commutativité dans* $\mathbb{N}$.

- *iv*) *On montre que* $(\mathbb{N}_{<p}, \oplus, \odot)$ *est un anneau commutatif.*
  - *La stabilité de* $\odot$ *est vérifiée comme précédemment.*
  - *D'après Théorème* 2.36, *partie i) (et l'exercices de geometrie),* $(\mathbb{N}_{<p}, \oplus)$ *est un groupe abélien.*
  - *L'associativité de* $\odot$ *est deja montrée.*
  - *L'élément neutre pour* $\odot$ *est* 1.
  - *La distributivité : soient* $a, b, c \in \mathbb{N}_{<p}$. *Donc,*
    - *il existe* $k_1 \in \mathbb{N}$, $r_1 \in \mathbb{N}_{<p}$ *tels que* $a + b = k_1 p + r_1$, *i.e.* $a \oplus b = a + b - k_1 p$ *;*
    - *il existe* $k_2 \in \mathbb{N}$, $r_2 \in \mathbb{N}_{<p}$ *tels que* $ac = k_2 p + r_2$, *i.e.* $a \odot c = ac - k_2 p$ *;*
    - *il existe* $k_3 \in \mathbb{N}$, $r_3 \in \mathbb{N}_{<p}$ *tels que* $bc = k_3 p + r_3$, *i.e.* $b \odot c = bc - k_3 p$.

    On obtient alors, en utilisant la distributivité dans $\mathbb{N}$,

    $$\begin{aligned} (a \oplus b) \odot c &= (a + b - k_1 p) \odot c \\ &= \text{reste de la division eucl. de } (a + b - k_1 p)c \text{ par } p \\ &= \text{reste de la division eucl. de } (ac + bc - k_1 pc) \text{ par } p. \end{aligned} \tag{1}$$

    En utilisant la distributivité et la commutativité dans $\mathbb{N}$, *on obtient*

    $$\begin{aligned} (a \odot c) \oplus (b \odot c) &= (ac - k_2 p) \oplus (bc - k_3 p) \\ &= \text{reste de la division eucl. de } (ac + bc - (k_2 + k_3)p) \text{ par } p. \end{aligned} \tag{2}$$

On observe que (1) *et* (2) *diffère d'un multiple de p. Cela implique que la distributivé est satisfaite.*

Exercice 5

Soient $p \in K[t]$ et $c \in K$. Montrer que p s'écrit sous la forme $p(t) = g(t)(t-c) + p(c)$, où $g \in K[t]$. En particulier, déduire que c est une racine de p si et seulement si $p(c) = 0$.

Sol.: *Soit* $q(t) = t - c$. *Par le Théorème* 2.40, *on obtient que* $p(t) = g(t)(t-c) + r(t)$ *pour unique couple* $g, r \in K[t]$. *On a que* $\deg(r) < \deg(q) = \deg(t-c) = 1$, *ainsi* $\deg(r) \leq 0$. *En évaluant* p *en* c, *l'on a* $p(c) = g(c)(c-c) + r(c)$ *qui implique* $p(c) = r(c)$. c *est une racine de* p *si et seulement si* $(t-c)$ *divise* p, *i.e.* $p(c) = 0$.

Exercice 6

Décomposer les polynômes ci-dessous en produit de facteurs irréductibles dans chacun des cas suivants : $\mathbb{C}[t]$, $\mathbb{R}[t]$, $\mathbb{Q}[t]$, $\mathbb{F}_3[t]$ et $\mathbb{F}_7[t]$

$$t^3 + 2t \quad \text{et} \quad t^2 + t + 1.$$

Sol.: *Quel que soit le corps considéré, on a toujours :*

$$t^3 + 2t = t(t^2 + 2).$$

On peut aussi remarquer que 0 *est racine de* t^3+2t. *Le discriminant de* t^2+2 *est* $-8 < 0$, *donc ce polynôme n'a pas de racine dans* $\mathbb{R}$, *donc pas non plus dans* $\mathbb{Q}$. *Comme il est de degré* 2, *il est irréductible dans* $\mathbb{R}[t]$, *et aussi dans* $\mathbb{Q}[t]$. *Ainsi* $t^3 + 2t = t(t^2 + 2)$ *dans* $\mathbb{R}[t]$ *et dans* $\mathbb{Q}[t]$.

Dans $\mathbb{C}$, *les racines de* $t^2 + 2$ *sont* $\pm \mathrm{i}\sqrt{2}$. *Par conséquent* $t^3 + 2t = t(t + \mathrm{i}\sqrt{2})(t - \mathrm{i}\sqrt{2})$ *dans* $\mathbb{C}[t]$. *Dans* $\mathbb{F}_3[t]$, *le polynôme* $t^3 + 2t$ *devient :*

$$t^3 + 2t = t(t^2 + 2) = t(t+1)(t+2),$$

car les racines de $t^2 + 2$ *dans* $\mathbb{F}_3$ *sont* 1 *et* 2.

Le polynôme $t^2 + 2$ *n'a pas de racines dans* $\mathbb{F}_7$, *car on vérifie directement que* $a^2 + 2 \neq 0$ *pour chaque* $a \in \mathbb{F}_7$. *Comme il est de degré* 2, *il est donc irréductible dans* $\mathbb{F}_7[t]$. *La décomposition cherchée est donc* $t^3 + 2t + 3 = t(t^2 + 2)$ *dans* $\mathbb{F}_7[t]$.

L'autre polynôme $t^2 + t + 1$ *vaut* $(t + \frac{1}{2} + i\frac{\sqrt{3}}{2})(t + \frac{1}{2} - i\frac{\sqrt{3}}{2})$ *dans* $\mathbb{C}[t]$. *Il est irréductible dans* $\mathbb{R}[t]$ *et dans* $\mathbb{Q}[t]$ *car il est de degré* 2 *sans racines. Il vaut* $(t+2)^2$ *dans* $\mathbb{F}_3[t]$, *car* $t^2 + t + 1 = t^2 + 4t + 1 = (t+2)^2$.

Si le corps considéré est $\mathbb{F}_7$, *on obtient la decomposition* $t^2 + t + 1 = (t+5)(t+3)$ *dans* $\mathbb{F}_7[t]$.

Exercice 7

- Soient $p(t) = 3t^4 - 5t^3 + 2t + 1$ et $q(t) = t - 1$. Effectuer la division euclidienne du polynôme p par q dans $\mathbb{R}[t]$.
- Soient $p(t) = t^4 + t^3 + t + 1$ et $q(t) = t + 1$. Effectuer la division euclidienne du polynôme p par q dans $\mathbb{F}_2[t]$.

Sol.:

— *D'abord on calcule* $(3t^4 - 5t^3 + 2t + 1) : (t+1)$ *dans* $\mathbb{R}[t]$.

$$\begin{array}{rrrrrcccl}
(3t^4 & -5t^3 & & +2t & +1) & : & (t-1) & = & 3t^3 \quad -2t^2 \quad -2t \\
-(3t^4 & -3t^3) & & & & & & & \\
\hline
 & -2t^3 & & & & & & & \\
 & -(-2t^3 & +2t^2) & & & & & & \\
\hline
 & & -2t^2 & +2t & & & & & \\
 & & -(-2t^2 & +2t) & & & & & \\
\hline
 & & & & 1 & & & &
\end{array}$$

Donc, $3t^4 - 5t^3 + 2t + 1 = (3t^3 - 2t^2 - 2t)(t-1) + 1$.

— *Maintenant, on calcule* $(t^4 + t^3 + t + 1) : (t+1)$ *dans* $\mathbb{F}_2[t]$.

$$\begin{array}{rrrrcccl}
(t^4 & +t^3 & +t & +1) & : & (t+1) & = & t^3 \quad +1 \\
+(t^4 & +t^3) & & & & & & \\
\hline
 & & t & +1 & & & & \\
 & & t & +1 & & & & \\
\hline
 & & & 0 & & & &
\end{array}$$

Donc, $(t^4 + t^3 + t + 1) = (t^3 + 1)(t+1)$.

Exercice 8

i) Soit $a \in \mathbb{C}$. Définissons $f(t) = (t-a)(t-\bar{a}) \in \mathbb{C}[t]$. Montrer que $f \in \mathbb{R}[t]$.

ii) Soit $g \in \mathbb{R}[t]$. Montrer que si $z \in \mathbb{C}$ est une racine de g, alors il en est de même pour son conjugé $\bar{z}$.

iii) Déterminer tous les polynômes irréductibles unitaires dans $\mathbb{R}[t]$.

Sol.:

i) Comme

$$f(t) = (t-a)(t-\bar{a}) = t^2 - (a+\bar{a})t + a\bar{a},$$

il suffit de montrer que $a + \bar{a}$, $a\bar{a} \in \mathbb{R}$. *Soit* $a = x + iy$ *avec* $x, y \in \mathbb{R}$. *Alors* $\bar{a} = x - iy$ *et donc* $a + \bar{a} = 2x \in \mathbb{R}$. *Par ailleurs* $a\bar{a} = x^2 + y^2 \in \mathbb{R}$. *Donc tous les coefficients de* $f(t)$ *sont réels, c'est-à-dire* $f \in \mathbb{R}[t]$.

ii) Comme z *est une racine de* $g(t)$, *on a* $g(z) = 0$, *et on doit montrer que* $g(\bar{z}) = 0$. *Supposons que* $g(t)$ *soit de la forme* $g(t) = \sum_{i=0}^{n} a_i t^i$ *avec* $a_0, a_1, \ldots, a_n \in \mathbb{R}$. *On a alors* $g(z) = \sum_{i=0}^{n} a_i z^i = 0$. *On obtient que*

$$g(\bar{z}) = \sum_{i=0}^{n} a_i \bar{z}^i = \sum_{i=0}^{n} \overline{a_i} \bar{z}^i = \sum_{i=0}^{n} \overline{a_i} \overline{z^i} = \overline{\sum_{i=0}^{n} a_i z^i} = \overline{g(z)} = \bar{0} = 0,$$

où on a utilisé $\overline{a_i} = a_i$ *(car* $a_i \in \mathbb{R}$*), ainsi que les formules* $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ *et* $\overline{z_1 z_2} = \overline{z_1}\ \overline{z_2}$.

iii) *Soit* $f \in \mathbb{R}[t]$ *un polynôme irréductible unitaire de degré* $n \geq 1$. *Comme tout polynôme de degré* $n \geq 1$ *admet une racine dans* $\mathbb{C}$, *on prend* z *une racine de* f *dans* $\mathbb{C}$. *Ainsi* $t - z$ *divise* f *dans* $\mathbb{C}[t]$.

Si $z \in \mathbb{R}$, *alors* $t - z$ *divise* f *dans* $\mathbb{R}[t]$ *et donc* $f(t) = t - z$, *car* $t - z \in \mathbb{R}[t]$ *et* f *est irréductible et unitaire dans* $\mathbb{R}[t]$.

Si $z \notin \mathbb{R}$, *son conjugé* $\bar{z}$ *est aussi une racine de* $f(t)$ *d'après ii), et donc* $t - \bar{z}$ *divise aussi* $f(t)$ *dans* $\mathbb{C}[t]$. *Il s'en suit que* $(t-z)(t-\bar{z})$ *divise* $f(t)$. *Comme* $(t-z)(t-\bar{z}) \in \mathbb{R}[t]$ *d'après i), et comme* f *est irréductible dans* $\mathbb{R}[t]$, *on doit avoir* $f(t) = (t - z)(t - \bar{z})$. *Notons que le polynôme* $(t - z)(t - \bar{z})$, *de degré* 2, *a un discriminant négatif car les deux racines ne sont pas réelles.*

Les polynômes irréductibles unitaires dans $\mathbb{R}[t]$ *sont donc ou bien de la forme* $t + a$ *avec* $a \in \mathbb{R}$, *ou bien de la forme* $t^2 + bt + c$, *avec* $b, c \in \mathbb{R}$, *et sans racine réelle (c'est-à-dire tels que* $b^2 - 4c < 0$*).*