Nom de famille (MAJUSCULES) ______________________________

Prénom (MAJUSCULES) ______________________________

Signature ______________________________

Numéro d'étudiant ______________________________

Mat 3541 Solution du test 1

Professeur: D. Daigle Date: 7 octobre 2011 Durée: 75 minutes

Espace réservé au correcteur.

(1) Soit $T : V \to W$ une application linéaire, où V, W sont des espaces vectoriels sur un corps K. Supposons que $\dim V = n$ et $\dim W = m$.

Soient $\mathcal{B}$ une base de V, $\mathcal{D}$ une base de W, et $A = \big[T\big]^{\mathcal{B}}_{\mathcal{D}}$.

Soit $T_A : K^n \to K^m$ l'application linéaire déterminée par la matrice $A = \big[T\big]^{\mathcal{B}}_{\mathcal{D}}$, c'est à dire que T_A est définie par

$$T_A(X) = AX \text{ pour tout } X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n.$$

(a) Montrez que, quel que soit $v \in V$, $\; v \in \ker(T) \Leftrightarrow [v]_{\mathcal{B}} \in \ker(T_A)$.

(b) Montrez que, quel que soit $w \in W$, $\; w \in \operatorname{im}(T) \Leftrightarrow [w]_{\mathcal{D}} \in \operatorname{im}(T_A)$.

On sait que les deux fonctions

$$\begin{array}{ccc} V & \to & K^n \\ v & \mapsto & [v]_{\mathcal{B}} \end{array} \qquad \text{et} \qquad \begin{array}{ccc} W & \to & K^m \\ w & \mapsto & [w]_{\mathcal{D}} \end{array}$$

sont bijectives, car ce sont des isomorphismes d'espaces vectoriels. Notons aussi :

$$(*) \qquad T_A\big([v]_{\mathcal{B}}\big) = \big[T(v)\big]_{\mathcal{D}} \quad \text{pour tout } v \in V.$$

Preuve de $(*)$: si $v \in V$ alors $\big[T(v)\big]_{\mathcal{D}} = [T]^{\mathcal{B}}_{\mathcal{D}}[v]_{\mathcal{B}} = A[v]_{\mathcal{B}} = T_A\big([v]_{\mathcal{B}}\big)$.

(a) Soit $v \in V$.

- Si $v \in \ker T$ alors $T(v) = 0$, donc $T_A\big([v]_{\mathcal{B}}\big) \overset{(*)}{=} \big[T(v)\big]_{\mathcal{D}} = [0]_{\mathcal{D}} = 0$, donc $[v]_{\mathcal{B}} \in \ker T_A$.
- Supposons que $[v]_{\mathcal{B}} \in \ker T_A$. Alors $\big[T(v)\big]_{\mathcal{D}} \overset{(*)}{=} T_A\big([v]_{\mathcal{B}}\big) = 0$. Le fait que $\big[T(v)\big]_{\mathcal{D}} = 0$ implique que $T(v) = 0$, car $w \mapsto [w]_{\mathcal{D}}$ est injective. Donc $T(v) = 0$, donc $v \in \ker T$.

Ainsi, $v \in \ker(T) \Leftrightarrow [v]_{\mathcal{B}} \in \ker(T_A)$.

(b) Soit $w \in W$.

- Si $w \in \operatorname{im} T$ alors il existe $v \in V$ satisfaisant $T(v) = w$,
donc $[w]_{\mathcal{D}} = \big[T(v)\big]_{\mathcal{D}} \overset{(*)}{=} T_A\big([v]_{\mathcal{B}}\big) \in \operatorname{im} T_A$.
- Supposons que $[w]_{\mathcal{D}} \in \operatorname{im} T_A$. Alors il existe $X \in K^n$ satisfaisant $T_A(X) = [w]_{\mathcal{D}}$. Comme $v \mapsto [v]_{\mathcal{B}}$ est en particulier une fonction surjective, il existe $v \in V$ tel que $[v]_{\mathcal{B}} = X$. Alors $\big[T(v)\big]_{\mathcal{D}} \overset{(*)}{=} T_A\big([v]_{\mathcal{B}}\big) = T_A\big(X\big) = [w]_{\mathcal{D}}$.
Le fait que $\big[T(v)\big]_{\mathcal{D}} = [w]_{\mathcal{D}}$ implique que $T(v) = w$, car la fonction $W \to K^m$, $w' \mapsto [w']_{\mathcal{D}}$, est injective. On a donc $T(v) = w$, d'où $w \in \operatorname{im} T$.

Ainsi, $w \in \operatorname{im}(T) \Leftrightarrow [w]_{\mathcal{D}} \in \operatorname{im}(T_A)$.

$$\begin{tikzcd}
v \arrow[d, mapsto] & V \arrow[r, "T"] \arrow[d, "\cong"'] & W \arrow[d, "\cong"] & w \arrow[d, mapsto] \\
{[v]_{\mathcal{B}}} & K^n \arrow[r, "T_A"'] & K^m & {[w]_{\mathcal{D}}}
\end{tikzcd}$$

Quelques erreurs commises dans la question 1

1. L'erreur la plus fréquente est d'affirmer que $[T(v)]_{\mathcal{D}} = 0 \Rightarrow T(v) = 0$ et que $[T(v)]_{\mathcal{D}} = [w]_{\mathcal{D}} \Rightarrow T(v) = w$ sans donner de justification. Ces affirmations sont vraies, mais doivent être justifiées en disant que la fonction $W \to K^m$, $w \mapsto [w]_{\mathcal{D}}$, est injective.

2. Dans la preuve que $[w]_{\mathcal{D}} \in \operatorname{im}(T_A) \implies w \in \operatorname{im} T$ dans 1(b), plusieurs ont écrit :

Supposons que $[w]_{\mathcal{D}} \in \operatorname{im}(T_A)$; alors $\exists_{[v]_{\mathcal{B}} \in K^n}$ tel que $[w]_{\mathcal{D}} = T_A([v]_{\mathcal{B}}) = A[v]_{\mathcal{B}} = \dots$

ou encore une version légèrement différente :

Supposons que $[w]_{\mathcal{D}} \in \operatorname{im}(T_A)$; alors $\exists_{X=[v]_{\mathcal{B}} \in K^n}$ tel que $[w]_{\mathcal{D}} = T_A(X) = AX = A[v]_{\mathcal{B}} = \dots$

Les écritures $\exists_{[v]_{\mathcal{B}} \in K^n}$ et $\exists_{X=[v]_{\mathcal{B}} \in K^n}$ sont dangereuses, parce qu'elles donnent l'impression d'affirmer une seule chose alors qu'elles en affirment deux (et la deuxième affirmation est invisible). Voici les deux affirmations :

- $\exists_{X \in K^n}$ tel que $[w]_{\mathcal{D}} = T_A(X)$,
- $\exists_{v \in V}$ tel que $X = [v]_{\mathcal{B}}$.

Remarquez que la deuxième affirmation est vraie parce que la fonction $V \to K^n$, $v \mapsto [v]_{\mathcal{B}}$, est surjective. Lorsque vous écrivez $\exists_{[v]_{\mathcal{B}} \in K^n}$ ou $\exists_{X=[v]_{\mathcal{B}} \in K^n}$, vous ne vous apercevez même pas que vous utilisez la surjectivité de cette fonction.

3. L'erreur que je vais décrire ici est plus générale : je la vois souvent dans les devoirs et examens de tous les cours que j'enseigne, et je la vois même dans des thèses de maîtrise ou de doctorat.

Une chaîne d'égalités telle que $A = B = C = D$ est une version compacte de :

$$A = B \text{ et } B = C \text{ et } C = D.$$

Donc lorsqu'on écrit $A = B = C = D$, il faut que chacune des égalités $A = B$, $B = C$, $C = D$ soit évidente. Par exemple, voici une faute :

$$\text{Si } [v]_{\mathcal{B}} \in \ker(T_A) \text{ alors } T_A([v]_{\mathcal{B}}) = A[v]_{\mathcal{B}} = [T]_{\mathcal{D}}^{\mathcal{B}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{D}} = 0.$$

C'est une faute parce que la dernière égalité ($[T(v)]_{\mathcal{D}} = 0$) n'est pas évidente. L'écriture correcte est :

$$\text{Si } [v]_{\mathcal{B}} \in \ker(T_A) \text{ alors } 0 = T_A([v]_{\mathcal{B}}) = A[v]_{\mathcal{B}} = [T]_{\mathcal{D}}^{\mathcal{B}}[v]_{\mathcal{B}} = [T(v)]_{\mathcal{D}}, \text{ donc } [T(v)]_{\mathcal{D}} = 0.$$

Voici un deuxième exemple. Dans le but de prouver que $\Phi(a)\Phi(b) = \Phi(b)\Phi(a)$, quelqu'un a écrit :

$$\Phi(ab) = \Phi(a)\Phi(b) = \Phi(b)\Phi(a) = \Phi(ba)$$

Ceci est une faute, car l'égalité centrale n'est pas évidente. L'écriture correcte est :

$$\Phi(a)\Phi(b) = \Phi(ab) = \Phi(ba) = \Phi(b)\Phi(a), \quad \text{donc} \quad \Phi(a)\Phi(b) = \Phi(b)\Phi(a).$$

Le même principe s'applique lorsque l'égalité est remplacée par une autre relation. Par exemple, supposons qu'on sait que $L(M(v)) = M(L(v))$, et qu'on veut prouver que $M(L(v)) \in \operatorname{im} L$. Alors

$$L(M(v)) = M(L(v)) \in \operatorname{im} L$$

est une faute, car $M(L(v)) \in \operatorname{im} L$ n'est pas évident. L'écriture correcte est :

$$M(L(v)) = L(M(v)) \in \operatorname{im} L, \quad \text{donc } M(L(v)) \in \operatorname{im} L.$$

C'est mieux, parce que les deux affirmations $M(L(v)) = L(M(v))$ et $L(M(v)) \in \operatorname{im} L$ sont évidentes.

(2) Soit V un espace vectoriel sur un corps K, et soit $T \in \mathrm{End}_K(V)$. On sait que le noyau $\ker(T)$ et l'image $\mathrm{im}(T)$ de T sont des sous-espaces de V. Supposons que

$$T^2 = T.$$

(a) Montrez que $V = \ker(T) \oplus \mathrm{im}(T)$.

(b) Montrez que les sous-espaces $\ker(T)$ et $\mathrm{im}(T)$ de V sont T-invariants.

(c) Donnez une description complète des opérateurs linéaires

$$T|_{\ker T} : \ker(T) \to \ker(T) \quad \text{et} \quad T|_{\mathrm{im}\, T} : \mathrm{im}(T) \to \mathrm{im}(T).$$

(d) Supposons que $(e_1, \ldots, e_s)$ est une base de $\ker(T)$ et que $(e_{s+1}, \ldots, e_n)$ est une base de $\mathrm{im}(T)$. Alors on sait que $\mathcal{B} = (e_1, \ldots, e_n)$ est une base de V. Donnez la matrice $[T]_{\mathcal{B}}$.

(a) On doit montrer que

(i) $\ker(T) \cap \mathrm{im}(T) = \{0\}$

(ii) $V = \ker(T) + \mathrm{im}(T)$ (autrement dit: pour chaque $v \in V$, il existe $x \in \ker T$ et $y \in \mathrm{im}\, T$ satisfaisant $v = x + y$).

Preuve de (i). Il suffit de montrer que $\ker(T) \cap \mathrm{im}(T) \subseteq \{0\}$, car l'inclusion réciproque est triviale. Soit $v \in \ker(T) \cap \mathrm{im}(T)$. Puisque $v \in \mathrm{im}\, T$, il existe $x \in V$ tel que $T(x) = v$. Puisque $v \in \ker T$, on a $T(v) = 0$. Donc $v = T(x) = T^2(x) = T(T(x)) = T(v) = 0$.

Preuve de (ii). Soit $v \in V$. Alors $T(v - T(v)) = T(v) - T^2(v) = T(v) - T(v) = 0$, donc $v - T(v) \in \ker T$. Si on pose $x = v - T(v)$ et $y = T(v)$, alors on a $x \in \ker T$, $y \in \mathrm{im}\, T$, et $v = x + y$.

(b) On démontre ceci sans utiliser l'hypothèse $T^2 = T$:

- Si $v \in \ker T$ alors $T(v) = 0$ et $0 \in \ker T$, donc $T(v) \in \ker T$. Ainsi, $\ker T$ est T-invariant.
- Si $v \in \mathrm{im}\, T$ alors évidemment $T(v) \in \mathrm{im}\, T$. Donc $\mathrm{im}\, T$ est T-invariant.
  (*Remarque.* TOUS ont cru nécessaire de démontrer l'assertion "$T(v) \in \mathrm{im}\, T$". Pourtant, cette assertion est complètement évidente, par définition de $\mathrm{im}\, T$.)

(c) $T|_{\ker T} : \ker(T) \to \ker(T)$ est l'application nulle, car pour chaque $v \in \ker T$ on a $\big(T|_{\ker T}\big)(v) = T(v) = 0$.

$T|_{\mathrm{im}\, T} : \mathrm{im}(T) \to \mathrm{im}(T)$ est l'application identité, car si $v \in \mathrm{im}\, T$ alors il existe $x \in V$ tel que $T(x) = v$, donc $\big(T|_{\mathrm{im}\, T}\big)(v) = T(v) = T(T(x)) = T^2(x) = T(x) = v$.

(d) Écrivons $\mathcal{C} = (e_1, \ldots, e_s)$ pour la base de $\ker(T)$ et $\mathcal{D} = (e_{s+1}, \ldots, e_n)$ pour la base de $\mathrm{im}(T)$. En vertu de (a) et (b) et d'un théorème vu en classe, on a

$$[T]_{\mathcal{B}} = \left(\begin{array}{c|c} [T|_{\ker T}]_{\mathcal{C}} & 0 \\ \hline 0 & [T|_{\mathrm{im}\, T}]_{\mathcal{D}} \end{array}\right).$$

En vertu de (c), $[T|_{\ker T}]_{\mathcal{C}}$ est la matrice nulle de format $s \times s$ et $[T|_{\mathrm{im}\, T}]_{\mathcal{D}}$ est la matrice identité de format $n - s \times n - s$. Ainsi, $[T]_{\mathcal{B}} = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_{n-s} \end{array}\right)$.

(3) (a) Montrez que si $\Phi : A \to B$ est un homomorphisme d'anneaux et A est commutatif alors $\Phi(A)$ est un anneau commutatif. (On sait déjà que $\Phi(A)$ est un anneau, puisque c'est un sous-anneau de B ; vous devez montrer la commutativité. On ne suppose pas que B est commutatif.)

(b) Soit V un espace vectoriel sur un corps K et soit $T \in \mathrm{End}_K(V)$. Soient $p, q \in K[x]$ et considérez les éléments $p(T)$ et $q(T)$ de $\mathrm{End}_K(V)$. Montrez que $p(T) \circ q(T) = q(T) \circ p(T)$. *Indice :* Servez-vous de (a) et d'une proposition vue en classe.

(a) Considérons des éléments b et b' de $\Phi(A)$. Alors il existe $a, a' \in A$ satisfaisant $\Phi(a) = b$ et $\Phi(a') = b'$. Puisque A est commutatif, on a $aa' = a'a$, donc $\Phi(aa') = \Phi(a'a)$. Alors :

$$bb' = \Phi(a)\Phi(a') = \Phi(aa') = \Phi(a'a) = \Phi(a')\Phi(a) = b'b.$$

Ainsi, la multiplication de l'anneau $\Phi(A)$ est commutative, ce qu'il fallait démontrer.

(b) On a vu en classe que $\Phi : K[x] \to \mathrm{End}_K(V)$, $\Phi(p) = p(T)$, est un homomorphisme d'anneaux. Comme $K[x]$ est un anneau commutatif, on déduit de (a) que le sous-anneau $\Phi(K[x])$ de $\mathrm{End}_K(V)$ est un anneau commutatif. Il est clair que $p(T) = \Phi(p)$ et $q(T) = \Phi(q)$ sont des éléments de $\Phi(K[x])$. Comme la multiplication dans l'anneau $\Phi(K[x])$ est la composition " $\circ$ " des endomorphismes, on conclut que $p(T) \circ q(T) = q(T) \circ p(T)$.

Remarque. (b) est un cas particulier de (a), donc (b) doit être *déduit* de (a). C'est une faute de style de *redémontrer* en (b) le résultat qui a déjà été démontré en (a). Plusieurs ont commis cette faute.

(4) Soit V un espace vectoriel sur un corps K.

(a) Soient $L, M \in \operatorname{End}_K(V)$ tels que $L \circ M = M \circ L$. Montrez que le sous-espace $\operatorname{im}(L)$ de V est M-invariant.

(b) Montrez que pour tout choix de $T \in \operatorname{End}_K(V)$ et de $p, q \in K[x]$, le sous-espace $\operatorname{im}\big(p(T)\big)$ de V est $q(T)$-invariant.

(a) On doit montrer que, pour tout $y \in \operatorname{im}(L)$, on a $M(y) \in \operatorname{im}(L)$.

Soit $y \in \operatorname{im}(L)$. Alors il existe $x \in V$ tel que $L(x) = y$. Donc $M(y) = M(L(x)) = (M \circ L)(x) = (L \circ M)(x) = L(M(x)) \in \operatorname{im}(L)$, d'où $M(y) \in \operatorname{im}(L)$.

(b) Soient $T \in \operatorname{End}_K(V)$ et $p, q \in K[x]$. Écrivons $L = p(T)$ et $M = q(T)$. Alors $L, M \in \operatorname{End}_K(V)$ et, en vertu de la question 3(b), on a $L \circ M = M \circ L$. On déduit de 4(a) que $\operatorname{im}(L)$ est M-invariant, ou autrement dit, que $\operatorname{im}\big(p(T)\big)$ est $q(T)$-invariant.

Même remarque que pour la question précédente: plusieurs ont commis la faute qui consiste à redémontrer en (b) ce qui avait déjà été démontré en (a).

(5) Considérez l'idéal $I = (2, x)$ de l'anneau des polynômes $\mathbb{Z}[x]$.

(a) Soit $q = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}[x]$ (où $a_i \in \mathbb{Z}$ pour tout i, et où il n'y a qu'un nombre fini de a_i non nuls). Montrez que si $q \in I$, alors $a_0 \in 2\mathbb{Z}$.
Déduisez que $I \neq \mathbb{Z}[x]$.

(b) Montrez que si $p \in \mathbb{Z}[x]$ est tel que $I \subseteq (p)$, alors $p \in \{-1, 1\}$.
Déduisez que $(p) = \mathbb{Z}[x]$.

(c) Déduisez de (a) et (b) que I n'est pas un idéal principal de $\mathbb{Z}[x]$.

Plusieurs ont perdu beaucoup de points parce qu'ils ne connaissaient pas la définition de "l'idéal $I = (2, x)$ de l'anneau des polynômes $\mathbb{Z}[x]$". La définition est :

$$(2, x) = \{\, 2f + xg \mid f, g \in \mathbb{Z}[x] \} .$$

Remarquez que f et g (ci-dessus) peuvent être n'importe quels polynômes. Plusieurs ont cru que f, g étaient toujours des entiers.

(a) Soit $q = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{Z}[x]$, et supposons que $q \in I$. Par définition de I, il existe $f, g \in \mathbb{Z}[x]$ tels que $q = 2f + xg$. Écrivons $f = \sum_{i=0}^{\infty} b_i x^i$ et $g = \sum_{i=0}^{\infty} c_i x^i$ (où $b_i, c_i \in \mathbb{Z}$, et où il n'y a qu'un nombre fini de b_i, c_i non nuls). Alors

$$q = 2(b_0 + b_1 x + b_2 x^2 + \cdots) + x(c_0 + c_1 x + c_2 x^2 + \cdots),$$

donc

$$a_0 + a_1 x + a_2 x^2 + \cdots = 2b_0 + (2b_1 + c_0)x + (2b_2 + c_1)x^2 + \cdots$$

La définition d'égalité des polynômes implique que $a_0 = 2b_0$, donc $a_0 \in 2\mathbb{Z}$.

Pour montrer que $I \neq \mathbb{Z}[x]$, on peut par exemple considérer le polynôme $1 \in \mathbb{Z}[x]$. Notons que $1 = \sum_{i=0}^{\infty} a_i x^i$ où $a_0 = 1$ et $a_i = 0$ pour tout $i \geq 1$. Puisque $a_0 = 1 \notin 2\mathbb{Z}$, on a $1 \notin I$. Puisque $1 \in \mathbb{Z}[x]$ et $1 \notin I$, on conclut que $I \neq \mathbb{Z}[x]$.

(b) Soit $p \in \mathbb{Z}[x]$ tel que $I \subseteq (p)$. Comme 2 et x sont des éléments de $I = (2, x)$, on a $2 \in (p)$ et $x \in (p)$.

Puisque $2 \in (p)$, il existe $f \in \mathbb{Z}[x]$ satisfaisant $2 = pf$. Alors $0 = \deg(2) = \deg(pf) = \deg(p) + \deg(f)$, donc $\deg(p) = 0$ et $\deg(f) = 0$, donc :

$$p \in \mathbb{Z}.$$

Puisque $x \in (p)$, il existe $g \in \mathbb{Z}[x]$ satisfaisant $x = pg$. Écrivons $g = \sum_{i=0}^{\infty} a_i x^i$ ($a_i \in \mathbb{Z}$, un nombre fini de $a_i \neq 0$). Alors $x = pg = p \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (pa_i) x^i$, donc

$$0 + 1x + 0x^2 + 0x^3 + \cdots = (pa_0) + (pa_1)x + (pa_2)x^2 + \cdots$$

où $pa_i \in \mathbb{Z}$ pour tout i (car $p \in \mathbb{Z}$). Donc l'égalité des polynômes implique que $1 = pa_1$ (où $p, a_1 \in \mathbb{Z}$). Il s'ensuit que $p \in \{-1, 1\}$. Donc $1 \in (p)$, donc $(p) = \mathbb{Z}[x]$ (car si un idéal J d'un anneau A satisfait $1 \in J$, alors $J = A$).

(c) Supposons que I est principal. Alors il existe $p \in \mathbb{Z}[x]$ tel que $I = (p)$. Puisque $I \subseteq (p)$, la partie (b) implique que $(p) = \mathbb{Z}[x]$, donc $I = \mathbb{Z}[x]$, ce qui contredit (a). Cette contradiction montre que I n'est pas principal.