L3 Math 2011 : Algèbre et Arithmétique
Corrigé de l'épreuve du 15 avril 2011

I. *Considérons les applications linéaires de $\mathbb{R}$-espaces vectoriels*

$$\begin{array}{rccc} s_n\colon & M_n(\mathbb{R}) & \to & M_n(\mathbb{R}) \\ & A & \mapsto & A - {}^tA \end{array}$$

(a) *Pour $n = 2$ quelle est la dimension du conoyau de s_2 ?*
Par définition le conoyau de s_n est l'espace vectoriel quotient $\dfrac{M_n(\mathbb{R})}{\operatorname{image} s_n}$.

Pour un sous-espace vectoriel d'un espace vectoriel de dimension finie $F \subset E$, la dimension de l'espace quotient est donnée par

$$\dim E/F = \dim E - \dim F.$$

Donc on a $\dim \operatorname{coker} s_2 = \dim M_2(\mathbb{R}) - \dim \operatorname{image} s_2$. Les membres $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ de $M_2(\mathbb{R})$ dépendent linéairement de 4 coefficients indépendants : a, b, c, d.* Donc la dimension de $M_2(\mathbb{R})$ est 4. L'application s_2 envoye $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ en

$$A - {}^tA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 0 & b-c \\ c-b & 0 \end{pmatrix} = (b-c)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.^{\dagger}$$

Donc l'image de s_2 est de dimension 1 avec base $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. On conclut :

$$\boxed{\dim \operatorname{coker} s_2 = \dim M_2(\mathbb{R}) - \dim \operatorname{image} s_2 = 4 - 1 = 3.}$$

(b) *Quelle est la dimension du conoyau de s_n pour $n \geq 1$ général ?*

On a

$$\dim \operatorname{coker} s_n = \dim M_n(\mathbb{R}) - \dim \operatorname{image} s_n.$$

Mais on a un isomorphisme

$$\frac{M_n(\mathbb{R})}{\ker s_n} \cong \operatorname{image} s_n$$

et donc une équation

$$\dim \operatorname{image} s_n = M_n(\mathbb{R}) - \dim \ker s_n.$$

En substituant on trouve

$$\begin{aligned} \dim \operatorname{coker} s_n &= \dim M_n(\mathbb{R}) - \big(\dim M_n(\mathbb{R}) - \dim \ker s_n\big) \\ &= \dim M_n(\mathbb{R}) - \dim M_n(\mathbb{R}) + \dim \ker s_n \\ &= \dim \ker s_n. \end{aligned}$$

∗. Ils sont *indépendants* parce qu'on a $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ seulement quand $a = b = c = d = 0$.

†. Noter que $\left(\begin{smallmatrix} 0 & b-c \\ c-b & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ n'implique pas $b = c = 0$. Donc les 2 paramètres b et c sont *dépendants*. On a 1 seul paramètre indépendant, qui est $b - c$.

Maintenant on a

$$\ker s_n = \{A \in M_n(\mathbb{R}) \mid A = {}^tA\} = \{\text{matrices } n \times n \text{ symétriques}\}.$$

Les matrices symétriques s'écrivent sous la forme

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{12} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{13} & a_{23} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & a_{3n} & \cdots & a_{1n} \end{pmatrix}$$

Les coefficients sur et au dessus de la diagonale sont indépendants ; les coefficients au dessous de la diagonale sont les mêmes que ceux au-dessus de la diagonale. Or une matrice $n \times n$ contient n^2 coefficients, dont n sont sur la diagonale. Pour les $n^2 - n$ coefficients non diagonaux la moitié sont au dessus de la diagonale, et l'autre moitié sont au dessous de la diagonale. Donc une matrice $n \times n$ a $\frac{1}{2}(n^2 - n)$ coefficients au dessus de la diagonale. En ajoutant les coefficients diagonaux, on voit que les matrices symétriques ont $n + \frac{1}{2}(n^2 - n) = \frac{1}{2}(n^2 + n)$ coefficients indépendants. On trouve

$$\boxed{\dim \operatorname{coker} s_n = \dim \ker s_n = \frac{n(n+1)}{2}.}$$

II. (a) *Quel est le pgcd de* $5 + 14i$ *et* $5 + i$ *dans* $\mathbb{Z}[i]$ *?*

On suit l'algorithme d'Euclide. Pour diviser $5 + 4i$ par $5 + i$ avec quotient et reste dans $\mathbb{Z}[i]$, on divise d'abord dans $\mathbb{C}$.

$$\frac{5+14i}{5+i} = \frac{(5+14i)(5-i)}{(5+i)(5-i)} = \frac{39+65i}{26} = \frac{3}{2} + \frac{5}{2}i.$$

On peut choisir $1 + 2i$ comme une approximation dans $\mathbb{Z}[i]$ de $\frac{3}{2} + \frac{5}{2}i$. C'est le premier quotient. On a $(5 + i)(1 + 2i) = 3 + 11i$ et par conséquent

$$5 + 14i = (5 + i)(1 + 2i) + (2 + 3i).$$

Le premier reste est $2 + 3i$.
Maintenant on divise $5 + i$ par $2 + 3i$. On a

$$\frac{5+i}{2+3i} = \frac{(5+i)(2-3i)}{(2+3i)(2-3i)} = \frac{13-13i}{13} = 1 - i.$$

La deuxième division euclidienne est ainsi

$$5 + i = (2 + 3i)(1 - i) + 0$$

avec quotient $1 - i$ et reste 0. L'algorithme s'arrête parce que le reste est 0.
Le pgcd de $5 + 4i$ et $5 + i$ dans $\mathbb{Z}[i]$ est le dernier reste non nul dans l'algorithme d'Euclide : $\boxed{2 + 3i.}$

Contrôle que $2+3i$ est bien le pgcd. On a déjà la factorisation $5+i = (2+3i)(1-i)$. En divisant

$$\frac{5+14i}{2+3i} = \frac{(5+14i)(2-3i)}{(2+3i)(2-3i)} = \frac{52+13i}{13} = 4+i,$$

on trouve la factorisation $5+14i = (2+3i)(4+i)$. Donc $2+3i$ est bien un diviseur commun de $5+i$ et de $5+14i$. Les autres facteurs dans les factorisations, $1+i$ et $4+i$, sont premiers entre eux parce que (par exemple) leurs normes $N(1+i)=2$ et $N(4+i)=17$ sont premiers entre eux (ou parce qu'on a la division euclidienne donne $4+i = (2-i)(1+i)+1$ avec reste 1). Donc $2+3i$ est bien le pgcd de $5+i$ et $5+14i$.

(b) *Factoriser $9+i$ et $11+2i$ en irréductibles de $\mathbb{Z}[i]$.*

La factorisation de $9+i$. La norme de $9+i$ est $N(9+i) = (9+i)(9-i) = 9^2+1^1 = 81+1 = 82 = 2\cdot 41$. Donc 2 et $9+i$ ne peuvent pas être premiers entre eux. Leur pgcd se calcule par l'algorithme d'Euclide :

$$\begin{aligned} 9+i &= 4\cdot 2 + (1+i). \\ 2 &= (1-i)(1+i)+0. \end{aligned}$$

Donc $\mathrm{pgcd}(9+i, 2) = 1+i$. Cet $1+i$ est un facteur de $9+i$ dont la norme $N(1+i)=2$ est premier. Il est donc un facteur irréductible. Pour trouver l'autre facteur, on divise

$$\frac{9+i}{1+i} = \frac{(9+i)(1-i)}{(1+i)(1-i)} = \frac{10-8i}{2} = 5-4i.$$

La norme $N(5-4i) = 5^4+4^2 = 41$ est aussi premier. Donc $5-4i$ est aussi un irréductible de $\mathbb{Z}[i]$. La factorisation de $9+i$ en irréductibles de $\mathbb{Z}[i]$ est ainsi

$$\boxed{9+i = (1+i)(5-4i).}$$

La factorisation de $11+2i$. La norme de $11+2i$ est $N(11+2i) = (11+2i)(11-2i) = 11^2+2^2 = 125 = 5^3$. Donc $11+2i$ et 5 ne sont pas premiers entre eux, et l'algorithme d'Euclide

$$\begin{aligned} 11+2i &= 2\cdot 5 + (1+2i), \\ 5 &= (1-2i)(1+2i)+0, \end{aligned}$$

révèle que $\mathrm{pgcd}(11+2i, 5) = 1+2i$. En divisant on trouve une factorisation (partielle) $11+2i = (1+2i)(3-4i)$.
Répétant le processus, on calcule $N(3-4i) = 3^2+4^2 = 25 = 5^2$, et

$$\begin{aligned} 3-4i &= (1-i)\cdot 5 + (-2+i), \\ 5 &= (-2-i)(-2+i)+0. \end{aligned}$$

Donc $\text{pgcd}(3-4i, 5) = -2+i$. En divisant on trouve $3-4i = (-2+i)(-2+i)$. Donc on a $11+2i = (1+2i)(-2+i)(-2+i)$. Mais comme on a $-2+i = i(1+2i)$, on peut écrire aussi $11+2i = -(1+2i)^3$ ou

$$\boxed{11+2i = (-1-2i)^3.}$$

L'élément $-1-2i$ est irréductible parce que sa norme $N(-1-2i) = 1^2+2^2 = 5$ est un premier.

III. *Décider lesquels des sous-ensembles suivants de l'anneau commutatif* $\mathbb{Z}[x]$ *sont des idéaux de* $\mathbb{Z}[x]$:

Le critère. Un sous-ensemble J d'un anneau commutatif R est un idéal si et seulement si (i) J contient 0, (ii) J est stable sous l'addition (c-à-d pour tout $a, b \in J$ on a $a+b \in J$), et (iii) J est stable sous la multiplication par tout élément de R (c-à-d pour tout $a \in J$ et tout $r \in R$ on a $ra \in J$).

$$A = \{b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x] \mid b_0 \textit{ est un multiple de } 3\}$$

(i) Clairement le polynôme 0 est dans A.
(ii) Pour $f(x) = \sum_{k=0}^n b_kx^k \in A$ et $g(x) = \sum_{k=0}^n c_kx^k \in A$ les coefficients b_0 et c_0 sont des entiers divisibles par 3. Le coefficient b_0+c_0 de degré 0 de $f(x)+g(x) = \sum_{k=0}^n (b_k+c_k)x^k$ est alors aussi divisible par 3, et on a donc $f(x)+g(x) \in A$. Donc A est stable sous l'addition.
(iii) Pour $f(x) = \sum_{k=0}^n b_kx^k \in A$ et $h(x) = \sum_{k=0}^n a_kx^k \in \mathbb{Z}[x]$ le coefficient $b_0 \in \mathbb{Z}$ est divisible par 3. Alors le coefficient a_0b_0 de degré 0 de $h(x)f(x)$ est aussi divisible par 3, et dont on a $h(x)f(x) \in A$. Ainsi A est stable sous la multiplication par un $h(x) \in \mathbb{Z}[x]$ quelconque.
Donc A est un idéal de $\mathbb{Z}[x]$.

$$B = \{b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x] \mid b_2 \textit{ est un multiple de } 3\}$$

Le sous-ensemble $B \subset \mathbb{Z}[x]$ ne satisfait pas à la condition (iii) du critère. Par exemple on a $x^2 = x^2 + 0x^3 \in B$ et $x \in \mathbb{Z}[x]$, mais on a $x \cdot x^2 = 1x^3 \notin B$.
Donc B n'est pas un idéal de $\mathbb{Z}[x]$.

$$C = \{b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x] \mid b_0 = b_1 = b_2 = 0\}$$

C est un idéal de $\mathbb{Z}[x]$. On peut vérifier les 3 propriétés du critère ci-dessus comme on a fait pour A.
Alternativement, on peut constater que les membres de C sont exactement les polynômes qui s'écrivent sous la forme

$$b_3x^3 + b_4x^4 + \cdots b_nx^n = x^3(b_3 + b_4x + \cdots b_nx^{n-3}) = x^3h(x)$$

avec $h(x) \in \mathbb{Z}[x]$. Donc $C = x^3\mathbb{Z}[x]$, l'idéal principal de $\mathbb{Z}[x]$ engendré par x^3.

$D = \mathbb{Z}[x^2] = \{c_0 + c_2x^2 + c_4x^4 + \cdots + c_{2n}x^{2n} \in \mathbb{Z}[x] \mid n \geq 0 \text{ et les } c_{2i} \in \mathbb{Z}\}$

Le sous-ensemble $D \subset \mathbb{Z}[x]$ ne satisfait pas à la condition (iii) du critère. Par exemple on a $1 \in D$ et $x \in \mathbb{Z}[x]$, mais on a $x \cdot 1 = x \notin D$.

Donc D n'est pas un idéal de $\mathbb{Z}[x]$.

$E = \{b_0 + b_1x + \cdots + b_nx^n \in \mathbb{Z}[x] \mid \sum_{i=0}^{n} b_i = 0\}$

E est un idéal de $\mathbb{Z}[x]$. On vérifie les 3 propriétés du critère ci-dessus comme on a fait pour A. Cette vérification est simplifiée si on constate qu'on a

$$E = \{f(x) \in \mathbb{Z}[x] \mid f(1) = 0\}.$$

Alors il est clair qu'on a (i) $0 \in E$, et que (ii) si on a $f, g \in E$ alors on a $(f+g)(1) = f(1) + g(1) = 0 + 0 = 0$ et donc on a $f + g \in E$, et que (iii) si on a $f \in E$ et $h \in \mathbb{Z}[x]$ alors on a $(fh)(1) = f(1)h(1) = 0h(1) = 0$ et donc on a $fh \in E$.

Essentiellement, E est le noyau du morphisme d'anneaux

$$\begin{array}{rccc} \phi\colon & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z} \\ & f(x) & \longmapsto & f(1). \end{array}$$

Donc il est un idéal comme tout noyau de morphisme d'anneaux.

On peut aussi citer les théorèmes du reste et du facteur pour dire que pour un polynôme $f(x) \in \mathbb{Z}[x]$ on a $f(1) = 0$ ssi $x - 1$ divise $f(x)$ exactement avec reste 0. Donc on a $f(x) \in E$ ssi on a $f(x) = (x-1)q(x)$ avec $q(x) \in \mathbb{Z}[x]$. Donc $E = (x-1)\mathbb{Z}[x]$ est l'idéal principal engendré par $x - 1$.

$F = \{p(x) \in \mathbb{Z}[x] \mid p'(0) = 0\}$. *Ici $p'(x)$ est la dérivée de $p(x)$.*

Le sous-ensemble $F \subset \mathbb{Z}[x]$ ne satisfait pas à la condition (iii) du critère. Par exemple on a $1 \in F$ (la dérivée de 1 est 0, qui s'annule partout) et $x \in \mathbb{Z}[x]$, mais on a $x \cdot 1 = x \notin F$ (car sa dérivée est 1, qui ne s'annule nulpart).

Donc F n'est pas un idéal de $\mathbb{Z}[x]$.

Comment trouve-t-on cet exemple ? Si on prend $p(x) \in F$ (donc avec $p'(0) = 0$) et $q(x) \in \mathbb{Z}[x]$, alors on a $(pq)'(0) = p'(0)q(0) + p(0)q'(0) = p(0)q'(0)$. Donc pour avoir $p(x) \in F$ mais $p(x)q(x) \notin F$ il faut un $p(x)$ avec $p(0) \neq 0$ et $p'(0) = 0$ et un $q(x)$ avec $q'(0) \neq 0$. Un exemple est $p(x) = 1$ et $q(x) = x$.

IV. *Soit K un corps et soit $F(K,K) = \{$toutes les applications $f\colon K \to K\}$. Cet $F(K,K)$ est un anneau commutatif pour les opérations d'addition et de multiplication de fonctions : $(f+g)(a) = f(a) + g(a)$ et $(fg)(a) = f(a)g(a)$.*

Soit $\phi_K\colon K[X] \to F(K,K)$ le morphisme d'anneaux envoyant $P(X)$ en l'application $K \to K$ envoyant $a \mapsto P(a)$. Par exemple ϕ envoie le polynôme $2X^2 - 3$ en l'application $K \to K$ envoyant $a \mapsto 2a^2 - 3$.

(a) *Pour $K = \mathbb{Z}/2\mathbb{Z}$ quel est le noyau de $\phi_{\mathbb{Z}/2\mathbb{Z}}$?*

Pour tout corps K on a $\phi_K(P(X)) = 0$ dans $F(K, K)$ ssi on a $P(a) = 0$ pour tout $a \in K$. Donc on a

$$\ker \phi_K = \{P(X) \in K[X] \mid P(a) = 0 \text{ pour tout } a \in K\}.$$

Donc pour $K = \mathbb{Z}/2\mathbb{Z}$ on a

$$\ker \phi_{\mathbb{Z}/2\mathbb{Z}} = \{P(X) \in (\mathbb{Z}/2\mathbb{Z})[X] \mid P(0) = 0 \text{ et } P(1) = 0\}.$$

Les polynômes avec $P(0) = 0$ sont ceux divisibles par X, et ceux avec $P(1) = 0$ sont ceux divisibles par $X - 1$. Les polynômes avec $P(0) = P(1) = 0$ sont ceux divisibles par X et par $X - 1$ ou équivalemment par $\text{ppcm}(X, X - 1) = X(X - 1)$. Donc on a

$$\boxed{\ker \phi_{\mathbb{Z}/2\mathbb{Z}} = X(X-1)(\mathbb{Z}/2\mathbb{Z})[X].}$$

(b) *Pour $K = \mathbb{R}$ quel est le noyau de $\phi_{\mathbb{R}}$?*

On a

$$\ker \phi_{\mathbb{R}} = \{P(X) \in \mathbb{R}[X] \mid P(r) = 0 \text{ pour tout } r \in \mathbb{R}\}.$$

Pour tout polynôme non nul $P(X)$ il n'y a qu'un nombre fini d'éléments $r \in \mathbb{R}$ tel qu'on ait $P(r) = 0$. Ce sont les racines de $P(X)$, dont le nombre est majoré par $\deg P(X)$. Le seul polynôme avec une infinité de racines est le polynôme 0. Donc

$$\boxed{\ker \phi_{\mathbb{R}} = \{0\}.}$$

(c) *Donner une condition nécessaire et suffisante sur K pour que ϕ_K soit injectif.*

$$\boxed{\text{Le morphisme d'anneaux } \phi_K \colon K[X] \to F(K, K) \text{ est injectif ssi } K \text{ est infini.}}$$

En effet, si K est infini, on a $\ker \phi_K = \{0\}$ par le même raisonnement que pour $K = \mathbb{R}$ dans le (b).

Mais si K est fini, alors $Q(X) = \prod_{a \in K}(X - a)$ est un polynôme non nul qui s'annule en tout $a \in K$. Donc $Q(X)$ est un élément non nul de $\ker \phi_K$, et ϕ_K n'est pas injectif.