Corrigé de l'examen d'algèbre 1 de janvier 2007

Exercice I - Soit $f : \mathbb{N} \mapsto \mathbb{Z}$ définie de la manière suivante : pour tout entier naturel n, $f(n) = -n/2$ si n est pair et $f(n) = (n+1)/2$ si n est impair (on a donc $f(2k) = -k$ et $f(2k+1) = k+1$). Montrons que f est bijective :

• f surjective : soit $p \in \mathbb{Z}$. Si $p \geq 1$, alors en posant $n = p-1$, on obtient : $2n+1 \in \mathbb{N}$ et $f(2n+1) = n+1 = p$. Sinon, $p \leq 0$, et en posant $n = -p$, on obtient : $2n \in \mathbb{N}$ et $f(2n) = -n = p$. Donc dans tous les cas, p a un antécédent par f. Donc f est surjective.

• f injective : soient n et p des entiers naturels tels que $f(n) = f(p)$. Nécessairement, n et p ont même parité (sinon l'un des deux nombres $f(n)$ et $f(p)$ est négatif et l'autre est supérieur ou égal à 1, donc ils ne sont pas égaux). Si n et p sont tous les deux pairs, alors $-n/2 = -p/2$ donc $n = p$; si n et p sont tous les deux impairs, alors $(n+1)/2 = (p+1)/2$ donc $n = p$. Donc dans tous les cas possibles, $n = p$, donc f est injective.

Donc f est bijective. Il existe donc une application bijective de $\mathbb{N}$ dans $\mathbb{Z}$. Donc, par définition, $\mathbb{Z}$ est dénombrable.

Exercice II - Montrons que $\mathcal{R}$ est une relation d'équivalence. On note $\mathcal{M}_n$ pour $\mathcal{M}_n(\mathbb{R})$.

• $\mathcal{R}$ réflexive : soit $A \in \mathcal{M}_n$. I_n est inversible et $A = AI_n$, donc $A\mathcal{R}A$, donc $\mathcal{R}$ est réflexive.

• $\mathcal{R}$ transitive : soient A, B et C dans $\mathcal{M}_n$ telles que $A\mathcal{R}B$ et $B\mathcal{R}C$. Il existe donc des matrices inversibles P_1 et P_2 dans $\mathcal{M}_n$ telles que $A = BP_1$ et $B = CP_2$. On a donc $A = BP_1 = CP_2P_1 = CP$ avec $P = P_2P_1$. Or $P \in \mathcal{M}_n$ et, de plus, le produit de deux matrices inversibles est une matrice inversible, donc P est inversible. Donc $A\mathcal{R}C$. Donc $\mathcal{R}$ est transitive.

• $\mathcal{R}$ symétrique : soient A et B dans $\mathcal{M}_n$ tels que $A\mathcal{R}B$. Il existe donc une matrice inversible $P \in \mathcal{M}_n$ telle que $A = BP$. En multipliant cette égalité à gauche et à droite par P^{-1} on obtient : $AP^{-1} = BPP^{-1} = BI_n = B$. Posons $\tilde{P} = P^{-1}$. $\tilde{P}$ est une matrice inversible de $\mathcal{M}_n$ et on vient de voir que $B = A\tilde{P}$. Donc $B\mathcal{R}A$. Donc $\mathcal{R}$ est symétrique.

Donc $\mathcal{R}$ est réflexive, transitive et symétrique. Donc $\mathcal{R}$ est une relation d'équivalence.

Exercice III

1) On a

$$\begin{aligned}(I-M)(I+M+...+M^k) &= I(I+M+...+M^k) - M(I+M+...+M^k) \\ &= (I+M+M^2+...+M^k) - (M+M^2+...+M^{k+1}) \\ &= I - M^{k+1}\end{aligned}$$

(les autres termes s'éliminent).

2) $M^2 = \begin{pmatrix} 0 & 0 & ab \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et $M^3 = 0$ (matrice nulle). Or d'après le 1) avec $n = k = 3$, $(I_3 - M)A = I_3 - M^3$. Donc $(I_3 - M)A = I_3$. Donc A est inversible d'inverse $I_3 - M$.

3) I_3 commute avec M puisque $I_3 M = M = M I_3$. Donc la formule du binôme de Newton est valable. On a :

$$B^n = (I_3 - M)^n = \sum_{k=0}^{n} C_n^k (I_3)^{n-k}(-M)^k = \sum_{k=0}^{n} C_n^k (I_3)^{n-k}(-1)^k M^k$$

Or $M^3 = 0$ donc $M^k = 0$ pour tout $k \geq 3$. Donc pour tout $n \geq 2$,

$$B^n = I_3 - nM + \frac{n(n-1)}{2} M^2 = \begin{pmatrix} 1 & -na & \frac{n(n-1)ab}{2} \\ 0 & 1 & -nb \\ 0 & 0 & 1 \end{pmatrix}$$

De plus, $B^0 = I_3$ et $B^1 = B = I - M$ donc la formule ci-dessus est encore valable pour $n = 0$ et $n = 1$.

4) D'après le 2), A est inversible et $A^{-1} = B$. Or si A est inversible alors A^k est inversible d'inverse $(A^{-1})^k$. Donc A^{10} est inversible d'inverse B^{10}. Il existe donc un unique vecteur colonne X tel que $A^{10}X = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$. C'est

$$X = B^{10} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & -10a & 45ab \\ 0 & 1 & -10b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 - 10a + 45ab \\ 1 - 10b \\ 1 \end{pmatrix}$$

Exercice IV

1) On a $P(z_m) = P'(z_m) = 0$, donc z_m est racine au moins double de P, donc $(X - z_m)^2$ divise P, donc il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - z_m)^2 Q$. De plus, Q est unique par unicité du quotient dans la division euclidienne de P par $(X - z_m)^2$. Soit $j \in \{1, ..., m-1\}$. On a $P(z_j) = 0 = (z_j - z_m)Q(z_j)$. Comme $z_j - z_m \neq 0$, on a $Q(z_j) = 0$. De plus, en dérivant l'égalité $P = (X - z_m)^2 Q$, on obtient :

$$P' = 2(X - z_m)Q + (X - z_m)^2 Q'$$

Donc $P'(z_j) = 2(z_j - z_m)Q(z_j) + (z_j - z_m)Q'(z_j)$. Comme $P'(z_j) = Q(z_j) = 0$ et $z_j \neq z_m$, on obtient $Q'(z_j) = 0$.

2) On a $P(0) = d$, $P(1) = a + b + c + d$ et $P' = 3aX^2 + 2bX + c$ donc $P'(0) = c$ et $P'(1) = 3a + 2b$. Donc P vérifie $(**)$ si et seulement si (a, b, c, d) est solution du système :

$$\begin{cases} a + b + c + d &= 3a + 2b \\ c &= 0 \\ d &= 0 \end{cases}$$

En réarrangeant la première équation, en soustrayant la somme des deux dernières lignes à la première ligne, puis en divisant la première ligne par 2, on obtient :

$$\begin{cases} a + \frac{b}{2} = 0 \\ c = 0 \\ d = 0 \end{cases}$$

P vérifie donc $(**)$ si et seulement si $(a, b, c, d) \in \{(-b/2, b, 0, 0), b \in \mathbb{R}\} = \{(a, -2a, 0, 0), a \in \mathbb{R}\}$. P est alors de la forme $P = aX^4 - 2aX^3$, avec $a \in \mathbb{R}$.

3) On a $P(1) = 1 - 1 + 2i - 2i = 0$. Donc $X - 1$ divise P. Il existe donc des complexes a, b, c tels que $P = (X - 1)(aX^2 + bX + c)$. En identifiant les coefficients de P avec ceux du polynôme obtenu en développant le membre de droite, on obtient : $P = (X - 1)(X^2 + 2i)$. De plus, les racines de $X^2 + 2i$ sont les complexes z tels que : $z^2 = -2i = 2e^{-i\pi/2}$, c'est à dire : $z_1 = \sqrt{2}e^{-i\pi/4} = 1 - i$ et $z_2 = -z_1 = -1 + i$. On obtient donc : $P = (X - 1)(X - 1 + i)(X + 1 - i)$.

Remarque : z_2 n'est pas le conjugué de z_1 : ça n'a rien de choquant, puisque P n'est pas un polynôme à coefficients réels.

4)

4a) Supposons qu'il existe deux polynômes P et Q de degré inférieur ou égal à $m - 1$ tels que, pour tout $i \in \{1, ..., m\}$, $P(z_i) = Q(z_i) = z'_i$. On a $deg(P - Q) \leq max(deg(P), deg(Q)) \leq m - 1$. Donc si $P - Q \neq 0$, $P - Q$ a au plus $m - 1$ racines distinctes. Mais pour tout $i \in \{1, ..., m\}$, $(P - Q)(z_i) = 0$, donc $P - Q$ a au moins m racines distinctes. Donc $P - Q = 0$, donc $Q = P$. Il existe donc bien au plus un polynôme P de degré inférieur ou égal à $m - 1$ tel que, pour tout $i \in \{1, ..., m\}$, $P(z_i) = Q(z_i) = z'_i$.

4b) Le polynôme $P = X$ convient. De plus, d'après la question 4a), avec $m = 2$ et $z_i = z'_i = i$ pour tout i de $\{1, 2, 3\}$, il existe au plus un polynôme qui satisfait les conditions du 4b). Donc $P = X$ est l'unique solution.

Exercice V

Supposons f injective. Soit $x \in E$. Posons $y = f(x)$ et $z = f \circ f(x)$. On a $f(z) = f \circ f \circ f(x) = f(x)$. Or f est injective. Donc $z = x$. Donc $f \circ f(x) = x$. Donc $f(y) = x$. Donc x a au moins un antécédent : y. Comme ceci est vrai pour tout x de E, f est surjective.

Supposons f surjective. Soient y et y' des éléments de E tels que $f(y) = f(y')$. Puisque f est surjective, il existe x dans E tel que $y = f(x)$. On a $f \circ f(y) = f \circ f \circ f(x) = f(x) = y$. Donc $f \circ f(y) = y$. De même, $f \circ f(y') = y'$. Or puisque $f(y) = f(y')$, on a $f \circ f(y) = f \circ f(y')$. Donc $y = y'$. Donc f est injective.

On a bien montré que f est injective ssi f est surjective.