Université Paris-Sud **M204 2016/2017**

Corrigé du devoir maison n°1

Exercice 1 : On note $\mathbb{A}$ le sous ensemble de $\mathbb{C}$ des éléments de la forme $\sum_{k=0}^{n} a_k(i\sqrt{2})^k$, pour n variant dans $\mathbb{N}$ et les a_k variant dans $\mathbb{Z}$.
1. L'inclusion $\{a + b\,i\sqrt{2}\ ,\ a, b \in \mathbb{Z}\} \subset \mathbb{A}$ est évidente (il suffit de considérer le cas : $(a_0, a_1, a_2, \dots) = (a, b, 0, 0, \dots)$). Pour montrer l'autre inclusion, il suffit de voir que : $\forall k \in \mathbb{N},\ a_k(i\sqrt{2})^k \in \{a + b\,i\sqrt{2}\ ,\ a, b \in \mathbb{Z}\}$. Il suffit de distinguer selon la partié de k :

- si $k = 2n$: $a_k(i\sqrt{2})^k = (-1)^n \cdot a_k \cdot 2^n \in \{a + b\,i\sqrt{2}\ ,\ a, b \in \mathbb{Z}\}$ (avec $b = 0$) ;
- si $k = 2n + 1$: $a_k(i\sqrt{2})^k = (-1)^n \cdot a_k \cdot 2^n \cdot i\sqrt{2} \in \{a + b\,i\sqrt{2}\ ,\ a, b \in \mathbb{Z}\}$ (avec $a = 0$).

D'où l'égalité cherchée.

Pour montrer que $(\mathbb{A}, +, \cdot)$ est un anneau commutatif intègre, il suffit de le voir comme un sous-anneau de $\mathbb{C}$ (comme $\mathbb{C}$ est intègre, puisque c'est un corps).

- $1 = 1 + 0\,i\sqrt{2}$, donc $\mathbb{A} \neq \emptyset$ et $1_{\mathbb{C}} \in \mathbb{A}$;
- si $z = a + b\,i\sqrt{2}, z' = a' + b'\,i\sqrt{2} \in \mathbb{A}$, alors $z - z' = (a - a') + (b - b')i\sqrt{2} \in \mathbb{A}$ (comme $\mathbb{Z}$ est un groupe, donc $a - a', b - b' \in \mathbb{Z}$) ;
- si $z = a + b\,i\sqrt{2}, z' = a' + b'\,i\sqrt{2} \in \mathbb{A}$, alors $z \cdot z' = (aa' - 2bb') + (ab' + a'b)i\sqrt{2} \in \mathbb{A}$ (comme $\mathbb{Z}$ est un anneau, donc $aa' - bb', ab' + a'b \in \mathbb{Z}$).

2. Fixons $M \in \mathcal{R}$, et notons z l'affixe de M. On notera plus simplement $f_{\mathcal{R}}(M)$ la quantité $\min\left(\|\overrightarrow{AM}\|, \|\overrightarrow{BM}\|, \|\overrightarrow{CM}\|, \|\overrightarrow{DM}\|\right)$, qui dépend de $z = a + bi\sqrt{2}$ comme suit :

$$f_{\mathcal{R}}(M) = \begin{cases} |z| = \sqrt{a^2 + 2b^2} & \text{si } a, b \in [0, 1/2] \\ |z - 1| = \sqrt{(1-a)^2 + 2b^2} & \text{si } a \in [1/2, 1], b \in [0, 1/2] \\ |z - 1 - i\sqrt{2}| = \sqrt{(1-a)^2 + 2(1-b)^2} & \text{si } a, b \in [1/2, 1] \\ |z - i\sqrt{2}| = \sqrt{a^2 + 2(1-b)^2} & \text{si } a \in [0, 1/2], b \in [1/2, 1] \end{cases}$$

Il est alors immédiat que :

$$\max_{M \in \mathcal{R}} \min\left(\|\overrightarrow{AM}\|, \|\overrightarrow{BM}\|, \|\overrightarrow{CM}\|, \|\overrightarrow{DM}\|\right) = \sqrt{\frac{1}{4} + \frac{2}{4}} = \frac{\sqrt{3}}{2}.$$

3. La quantité cherchée est égale à la quantité calculée précédemment. En effet, si l'on se donne $M \in \mathbb{C}$ d'affixe z, alors on peut écrire $z = \alpha + \beta\,i\sqrt{2}$ avec $\alpha, \beta \in \mathbb{R}$. Pour $x \in \mathbb{R}$, on note $n(x)$ l'entier le plus proche de x (c'est-à-dire $n(x) = \lfloor x \rfloor$ ou $\lfloor x \rfloor + 1$ selon la valeur de x, de telle sorte que l'on ait toujours $|x - n(x)| \leq 1/2$. Pour que cette fonction soit bien définie, on suppose que $n(x) = \lfloor x \rfloor$ si $x \in 1/2 + \mathbb{Z}$. On a alors l'égalité :

$$\min_{N \in \mathbb{A}} \|\overrightarrow{MN}\| = |(a - n(a)) + (b - n(b))i\sqrt{2}|$$

Et finalement :

$$\max_{M\in\mathbb{C}} \min_{N\in\mathbb{A}} \|\overrightarrow{MN}\| = |(1/2) + (1/2)i\sqrt{2}| \ = \frac{\sqrt{3}}{2}.$$

4. Donnons-nous $z_1, z_2 \in \mathbb{A}$, en supposant que $z_2 \neq 0$. Considérons l'élément $z_1/z_2 \in \mathbb{C}$: d'après la question précédente, il existe $q \in \mathbb{A}$ tel que : $|\frac{z_1}{z_2} - q| \leq \frac{\sqrt{3}}{2}$. Posons $r = z_1 - z_2 \cdot q$, qui est un élément de $\mathbb{A}$ (comme $\mathbb{A}$ est un anneau). On a alors :

$$j(r) = |r|^2 = |z_1 - z_2 \cdot q|^2 = |z_2|^2 \cdot |\frac{z_1}{z_2} - q|^2 \leq \frac{3}{4} j(z_2) < j(z_2)$$

et ainsi :

$$z_1 = q \cdot z_2 + r$$

avec $q, r \in \mathbb{A}$ et $j(r) < j(z_2)$: donc $\mathbb{A}$ est euclidien pour la jauge j.

5. Donnons-nous $z = a + b\,i\sqrt{2}, z' = a' + b'\,i\sqrt{2} \in \mathbb{A}$. On a :

$$\begin{aligned} j(z \cdot z') &= j((aa' - 2bb') + (ab' + a'b)i\sqrt{2}) = (aa' - 2bb')^2 + 2(ab' + a'b)^2 \\ &= a^2a'^2 + 4b^2b'^2 - 4aa'bb' + 2a^2b'^2 + 2a'^2b^2 + 4aa'bb' \\ &= a^2a'^2 + 4b^2b'^2 + 2a^2b'^2 + 2a'^2b^2 \\ j(z) \cdot j(z') &= (a^2 + 2b^2) \cdot (a'^2 + 2b'^2) = a^2a'^2 + 4b^2b'^2 + 2a^2b'^2 + 2a'^2b^2 \end{aligned}$$

d'où l'égalité cherchée.

Si z est inversible (d'inverse z'), alors $j(z) = 1$, donc $a^2 + 2b^2 = 1$, et finalement $z = \pm 1$. Réciproquement, il est immédiat de voir que $z = \pm 1$ est inversible (d'inverse lui-même).

6. Cherchons à écrire les éléments de B. On a :

$$z = a + b\,i\sqrt{2} \in \mathbb{B} \Leftrightarrow a^2 + 2b^2 = 17 \Leftrightarrow a = \pm 3, b = \pm 2$$

(il suffit de constater que, nécessairement, $b \leq 2$ car $2 \cdot 3^2 = 18 > 17$, et de regarder les valeurs possibles pour a selon que $b = 0, \pm 1$ ou ± 2).

Donnons-nous $z \in \mathbb{B}$, et supposons que $z = z_1 \cdot z_2$. Alors : $17 = j(z) = j(z_1) \cdot j(z_2)$: comme 17 est premier, alors nécessairement $17 | j(z_1)$ ou $j(z_2)$, et finalement $j(z_1)$ ou $j(z_2)$ vaut 1, et finalement z_1 ou z_2 vaut ± 1 : donc z est irréductible.

Exercice 2 : La première étape consiste à utiliser l'algorithme d'Euclide pour calculer le pgcd de 872 et 156. On obtient les divisions suivantes :

$$\begin{aligned} 872 &= 5 \cdot 156 + 92 \\ 156 &= 1 \cdot 92 + 64 \\ 92 &= 1 \cdot 64 + 28 \\ 64 &= 2 \cdot 28 + 8 \\ 28 &= 3 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

Et ainsi : $\text{pgcd}(872, 156) = 4$. En remontant les divisions, on trouve que $17 \cdot 872 + (-95) \cdot 156 = 4$.

Cherchons dans un premier temps les solutions de l'équation : $872 \cdot x + 156 \cdot y = 44$. Comme $44 = 4 \cdot 11$, cette équation admet comme solution le couple $(x, y) = 11 \cdot (17, -95) = (187, -1045)$.

L'équation ci-dessus est donc équivalente à : $872 \cdot (x - 187) + 156 \cdot (y + 1045) = 0$, c'est-à-dire (en divisant par 4) : $218 \cdot (x - 187) + 39 \cdot (y + 1045) = 0$, et finalement on est ramenés à l'équation :

$$218 \cdot (x - 187) = -39 \cdot (y + 1045),$$

où on notera que les nombres 218 et 39 sont premiers entre eux.

D'après le théorème de Gauss, on déduit que 218 divise $(y + 1045)$, et que 39 divise $(x - 187)$. On pose alors $y + 1045 = n \cdot 218$ et $x - 187 = m \cdot 39$.

On réinjecte ces valeurs dans l'équation précédente. On a alors :

$$m \cdot 218 \cdot 39 = -n \cdot 39 \cdot 218$$

donc $m = -n$.

Ainsi, les solutions sont nécessairement de la forme :

$$(x, y) = (-n \cdot 39 + 187, n \cdot 218 - 1045), \ n \in \mathbb{Z}.$$

On vérifie facilement que les couples de cette forme sont tous solutions de l'équation précédente.

Pour la seconde équation, comme 74 n'est pas divisible par 4, alors il n'y a pas de solution. En effet, l'équation $872 \cdot x + 156 \cdot y = 74$ est équivalente à :

$$218 \cdot x + 39 \cdot y = 37/2$$

mais $\mathbb{Z}$ est un anneau donc $218 \cdot x + 39 \cdot y \in \mathbb{Z}$ pour $x, y \in \mathbb{Z}$, et il n'y a donc pas de solution comme $37/2 \notin \mathbb{Z}$.

Exercice 3 : Partons du fait que $37 \cdot 27 = 999$. Ainsi, le reste de la division euclidienne de 1000 (et plus généralement de tout entier de la forme 10^{3n}, pour $n \in \mathbb{N}$) par 37 est 1.

On en déduit ainsi les congruences : $n \equiv m_1 \equiv m_2 \bmod 37$. Ainsi, le nombre n est un multiple de 37 si, et seulement si, les nombres m_1 et m_2 le sont aussi, ce qui explique les étapes (i) et (ii).

Considérons donc le nombre $m_2 = \overline{abc}$. On a les égalités :

$$\overline{abc} = m_2 \ , \ \overline{abc0} = 10 \cdot m_2 \ et \ \overline{abc00} = 100 \cdot m_2.$$

Les nombres 10 (ou 100) et 37 sont premiers entre eux. Ainsi, on a les équivalences :

$$m_2 \equiv 0 \bmod 37 \Leftrightarrow 10 \cdot m_2 \equiv 0 \bmod 37 \Leftrightarrow 100 \cdot m_2 \equiv 0 \bmod 37$$

En appliquant l'étape (i) aux nombres $10 \cdot m_2$ et $100 \cdot m_2$, l'équivalence précédente devient :

$$\overline{abc} \equiv 0 \bmod 37 \Leftrightarrow \overline{bca} \equiv 0 \bmod 37 \Leftrightarrow \overline{cab} \equiv 0 \bmod 37$$

Ainsi, peut importe la valeur que l'on prend pour m_3, on aura l'équivalence :

$$m_2 \equiv 0 \bmod 37 \Leftrightarrow m_3 \equiv 0 \bmod 37$$

et donc :

$$n \equiv 0 \bmod 37 \Leftrightarrow m_3 \equiv 0 \bmod 37$$

En divisant l'égalité $37 \cdot 27 = 999$ par 9, on obtient : $37 \cdot 3 = 111$. Ainsi, le nombre $\overline{aaa} = a \cdot 111$ est un multiple de 37, et donc $m_4 = m_4 - \overline{aaa}$ vérifie l'équivalence :

$$m_3 \equiv 0 \bmod 37 \Leftrightarrow m_4 \equiv 0 \bmod 37$$

et donc :

$$n \equiv 0 \bmod 37 \Leftrightarrow m_4 \equiv 0 \bmod 37$$

Enfin, comme 3 et 37 sont premiers entre eux (ce sont deux nombres premiers distincts), on en déduit que :

$$m_4 \equiv 0 \bmod 37 \Leftrightarrow m_5 = 3 \cdot m_4 \equiv 0 \bmod 3 \cdot 37 = 111$$

et donc :

$$n \equiv 0 \bmod 37 \Leftrightarrow m_5 \equiv 0 \bmod 111$$

Ainsi, n est un multiple de 37 si, et seulement si, m_5 est un multiple de 111. Comme m_5 est un nombre à 3 chiffres, l'équivalence précédente se traduit plus facilement par :

$$n \equiv 0 \bmod 37 \Leftrightarrow m_5 \text{ a tous ses chiffres identiques.}$$

On pouvait aussi retirer quelques étapes de l'algorithme. Par exemple, il est facile de savoir que m_4 est ou non un multiple de 37, puisqu'il existe uniquement 3 multiples de 37 à deux chiffres ou moins, à savoir : 0, 37 et 74.

On pouvait aussi oublier les étapes (iii) et (iv). Auquel cas, le nombre m_5 pouvait avoir 4 chiffres, mais il suffit de lui appliquer l'étape (i) pour se ramener au cas d'un nombre m_5 à trois chiffres. Cela demande cependant de vérifier que l'étape (i) préserve la congruence modulo 3, mais on sait bien qu'un nombre est congru modulo 3 à la somme de ses chiffres, donc a fortiori à la somme de ses chiffres "regroupés par paquets de trois chiffres".

Exercice 4 : 1. On a directement les égalités :

$$A^2 = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix} \ , \ A^3 = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}.$$

et l'égalité $\mathrm{I}_3 + A + A^2 + A^3 = 0$ est immédiate.

2. Posons $X^n = Q_n(X) \cdot P(X) + R_n(X)$, où $R_n(X) = a_n X^2 + b_n X + c_n$ est un polynôme à coefficients réels de degré inférieur ou égal à 2. En évaluant l'égalité précédente en $-1, i, -i$ (comme suggéré dans l'énoncé), on en déduit le système :

$$\begin{cases} (-1)^n = a_n - b_n + c_n \\ i^n = -a_n + ib_n + c_n \\ (-i)^n = -a_n - ib_n + c_n \end{cases}$$

où les deuxième et troisième équations sont équivalents (comme les coefficients a_n, b_n, c_n sont réels, et que ces équations sont donc conjuguées complexes l'une de l'autre).

La solution de ce système ne dépend que du reste de la division euclidienne de n par 4 (c'est évident par l'unicité de R_n, et donc par l'unicité du choix de ses coefficients). On a les situations suivantes :

- si $n \equiv 0 \bmod 4$: $(a_n, b_n, c_n) = (0, 0, 1)$, donc $R_n(X) = 1$;
- si $n \equiv 1 \bmod 4$: $(a_n, b_n, c_n) = (0, 1, 0)$, donc $R_n(X) = X$;
- si $n \equiv 2 \bmod 4$: $(a_n, b_n, c_n) = (1, 0, 0)$, donc $R_n(X) = X^2$;
- si $n \equiv 3 \bmod 4$: $(a_n, b_n, c_n) = (-1, -1, -1)$, donc $R_n(X) = -X^2 - X - 1$.

On vérifie assez facilement ces résultats pour $n = 0, 1, 2, 3$. D'ailleurs, comme on sait que R_n ne dépend que de la valeur de n modulo 4, l'étude de ces quatre cas constitue une preuve pour le calcule de l'expression de n.

3. Suivant les notations précédentes, on a donc :

$$A^n = Q_n(A) \cdot P(A) + R_n(A) = R_n(A)$$

comme $P(A) = 0$. En constatant que $A^3 = -A^2 - A - \mathrm{I}_3$, on a donc :

$$A^n = \begin{cases} \mathrm{I}_3 \text{ si } n \equiv 0 \bmod 4 \\ A \text{ si } n \equiv 1 \bmod 4 \\ A^2 \text{ si } n \equiv 2 \bmod 4 \\ A^3 \text{ si } n \equiv 3 \bmod 4 \end{cases}$$

donc A est d'ordre 4 dans le groupe $\mathrm{GL}_3(\mathbb{R})$.

On en déduit que le groupe engendré par A est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, par le morphisme :

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathrm{GL}_3(\mathbb{R}) \\ n & \mapsto & A^n \end{array}$$

dont le noyau est $4 \cdot \mathbb{Z}$. C'est-à-dire que l'application induite :

$$\begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \to & \mathrm{GL}_3(\mathbb{R}) \\ \overline{n} & \mapsto & A^n \end{array}$$

est bien un isomorphisme.