Devoir à la maison n°10 : corrigé

Problème 1 — Parties de $\mathbb{C}$ stable par produit et somme de carrés (d'après Concours Général 2017)

Partie I – Quelques exemples simples

1. **a.** Puisque $|0| = 0 \leqslant 1$, $b(\{0\}) = 1$.
   b. Clairement $b(\mathbb{C}) = \infty$ (puisque $\mathbb{U}$ est infini par exemple).
   c. Les seuls éléments de $\mathbb{N}$ de module inférieur ou égal à 1 sont 0 et 1 donc $b(\mathbb{N}) = 2$.
   d. Le seul élément de $\mathbb{N}^*$ de module inférieur ou égal à 1 est 1 donc $b(\mathbb{N}) = 1$.

2. **a.** On peut par exemple choisir $\mathcal{A} = \mathbb{N}\setminus\{0, 1\}$. En effet, soit $(z_1, z_2) \in \mathcal{A}^2$. Alors z_1z_2 et $z_1^2+z_2^2$ sont clairement des entiers. De plus, $z_1 \geqslant 2$ et $z_2 \geqslant 2$ donc $z_1z_2 \geqslant 4$ et $z_1^2+z_2^2 \geqslant 8$. Par conséquent, $z_1z_2 \in \mathcal{A}$ et $z_1^2+z_2^2 \in \mathcal{A}$.
   b. On peut par exemple prendre $\mathcal{A} = \mathbb{Z}$. Clairement si $(z_1, z_2) \in \mathbb{Z}^2$, alors $z_1z_2 \in \mathbb{Z}$ et $z_1^2 + z_2^2 \in \mathbb{Z}$. Ainsi $\mathcal{A}$ est bien de type S. Par ailleurs, les seuls éléments de $\mathbb{Z}$ de module inférieur ou égal à 1 sont -1, 0 et 1 donc $b(\mathbb{Z}) = 3$.

3. Supposons que $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$. Alors $\mathcal{A}$ est non vide. De plus, si on se donne $(z_1, z_2) \in \mathcal{A}^2$, $z_1z_2 \in \mathcal{A}$ par stabilité de $\mathcal{A}$ par produit. De plus, $z_1^2 \in \mathcal{A}$ et $z_2^2 \in \mathcal{A}$ toujours par stabilité par produit puis $z_1^2 + z_2^2 \in \mathcal{A}$ par stabilité par somme. Ainsi $\mathcal{A}$ est bien de type S.

Partie II – Des exemples plus sophistiqués

1. L'existence provient de la définition de $\mathbb{Z}[j]$.
   Soit $(a, b, c, d) \in \mathbb{Z}^4$ tel que $a + bj = c + dj$. Supposons que $b \neq d$. Alors $j = \frac{a-c}{b-d} \in \mathbb{R}$, ce qui n'est pas le cas. Donc $b = d$ puis $a = c$.

2. **a.** Tout d'abord, $1 = 1 + 0j \in \mathbb{Z}[j]$.
   Soit ensuite $(z_1, z_2) \in \mathbb{Z}[j]^2$. Il existe donc $(a_1, b_1, a_2, b_2) \in \mathbb{Z}^4$ tel que $z_1 = a_1 + b_1j$ et $z_2 = a_2 + b_2j$.
   $$z_1 - z_2 = (a_1 + b_1j) - (a_2 + b_2j) = (a_1 + a_2) + (b_1 + b_2)j$$
   Or $(a_1 - a_2, b_1 - b_2) \in \mathbb{Z}^2$ donc $z_1 - z_2 \in \mathbb{Z}[j]$.
   En utilisant le fait que $j^2 = -j - 1$
   $$\begin{aligned} z_1z_2 &= (a_1 + b_1j)(a_2 + b_2j) = a_1a_2 + (a_1b_2 + a_2b_1)j + b_1b_2j^2 \\ &= (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1 - b_1b_2)j \end{aligned}$$
   Or $(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1 - b_1b_2) \in \mathbb{Z}^2$ donc $z_1z_2 \in \mathbb{Z}[j]$.
   De la même manière, Finalement, $\mathbb{Z}[j]$ est bien un sous-anneau de $\mathbb{C}$ donc une partie de type S.
   b. Soit $z \in \mathbb{Z}[j] \cap \mathcal{U}$. Il existe $(a, b) \in \mathbb{Z}^2$ tel que $z = a + bj$. Alors
   $$|z|^2 = (a + bj)(a + b\bar{j}) = a^2 + b^2 + ab(j + \bar{j}) = a^2 + b^2 - ab$$
   Puisque a et b sont entiers et a fortiori réels, $(a + b)^2 \geqslant 0$ et $(a - b)^2 \geqslant 0$. En développant, on obtient $a^2 + b^2 \geqslant -2ab$ et $a^2 + b^2 \geqslant 2ab$. Or $|z|^2 \leqslant 1$ i.e. $a^2 + b^2 - ab \leqslant 1$ donc $ab \leqslant 1$ et $-3ab \leqslant 1$, autrement dit $-\frac{1}{3} \leqslant ab \leqslant 1$. Or ab est entier donc $ab = 0$ ou $ab = 1$.
   Si $ab = 0$, alors $a = 0$ ou $b = 0$. Si $a = 0$, alors $|z| = |b| \leqslant 1$ donc $b \in \{-1, 0, 1\}$ car b est entier. Si $b = 0$, alors $|z| = |a| \leqslant 1$ donc $a \in \{-1, 0, 1\}$ car a est entier.
   Si $ab = 1$, alors $a = b = -1$ ou $a = b = 1$.
   Finalement si $|z| \leqslant 1$, $(a, b) \in \{(0, 0), (1, 0), (-1, 0), (0, 1), (0, -1), (-1, -1), (1, 1)\}$. Réciproquement, tous les couples (a, b) cités donnent bien $|z| \leqslant 1$. Enfin, la question **II.1** montre que tous ces couples (a, b) donnent bien des complexes $z = a + bj$ distincts.
   Ceci montre que $b(\mathbb{Z}[j]) = 7$.

3. **a.** Il suffit de remarquer que $z_1^2 + z_2^2 = (z_1 + iz_2)(z_1 - iz_2)$.

b. Supposons $x + y\sqrt{3} = 0$. Si $y \neq 0$, alors $\sqrt{3} = -\frac{x}{y} \in \mathbb{Q}$, ce qui contredit l'irrationalité de $\sqrt{3}$. Ainsi $y = 0$ puis $x = -y\sqrt{3} = 0$.

c. Il existe $(a_1, b_1, a_2, b_2) \in \mathbb{Z}^4$ tel que $z_1 = a_1 + b_1 j$ et $z_2 = a_2 + b_2 j$.
Si $z_1 + iz_2 = 0$ alors en considérant les parties réelles et imaginaires, on obtient

$$\begin{cases} a_1 - b_1/2 - b_2\sqrt{3}/2 = 0 \\ b_1\sqrt{3}/2 + a_2 - b_2/2 = 0 \end{cases}$$

ou encore

$$\begin{cases} 2a_1 - b_1 - b_2\sqrt{3} = 0 \\ b_1\sqrt{3} + 2a_2 - b_2 = 0 \end{cases}$$

Puisque $2a_1 - b_1$, $-b_2$, b_1 et $2a_2 - b_2$ sont des entiers, la question précédente montre que

$$2a_1 - b_1 = -b_2 = b_1 = 2a_2 - b_2 = 0$$

On en déduit sans peine que $a_1 = a_2 = b_1 = b_2 = 0$ i.e. $z_1 = z_2 = 0$.
Si $z_1 - iz_2 = 0$, on se ramène au cas précédent en remarquant que $-z_2 \in \mathbb{Z}[j]$. Ainsi $z_1 = -z_2 = 0$ i.e. $z_1 = z_2 = 0$.

4. Soit $(z_1, z_2) \in (\mathbb{Z}[j]^*)^2$. D'après ce qui précède, $z_1 z_2 \in \mathbb{Z}[j]$ mais comme $z_1 \neq 0$ et $z_2 \neq 0$, $z_1 z_2 \neq 0$. Ainsi $z_1 z_2 \in \mathbb{Z}[j]^*$.
Par ailleurs, on a également montré que $z_1^2 + z_2^2 \in \mathbb{Z}[j]$. Mais comme $z_1 \neq 0$ et $z_2 \neq 0$, la question **II.3** montre que $z_1^2 + z_2^2 \neq 0$. Ainsi $z_1^2 + z_2^2 \in \mathbb{Z}[j]^*$.
Ainsi $\mathbb{Z}[j]^*$ est bien de type S. Puisque $b(\mathbb{Z}[j]) = 7$ et $|0| \leqslant 1$, $b(\mathbb{Z}[j]^*) = 6$.

5. Remarquons que pour tout $z \in \mathbb{C}$, $z \in R(\mathbb{Z}[j]) \iff z^2 \in \mathbb{Z}[j]$.

a. Soit $(z_1, z_2) \in R(\mathbb{Z}[j])^2$. Alors $(z_1^2, z_2^2) \in \mathbb{Z}[j]^2$. Puisque $\mathbb{Z}[j]$ est de type S, $z_1^2 z_2^2 \in \mathbb{Z}[j]$ i.e. $(z_1 z_2)^2 \in \mathbb{Z}[j]$. Ceci signifie que $z_1 z_2 \in R(\mathbb{Z}[j])$.
A nouveau, puisque $\mathbb{Z}[j]$ est de type S, $(z_1^2)^2 + (z_2^2)^2 = z_1^4 + z_2^4 \in \mathbb{Z}[j]$. On a vu que $z_1^2 z_2^2 \in \mathbb{Z}[j]$ et, puisque $\mathbb{Z}[j]$ est stable par addition, $z_1^4 + z_2^4 + 2z_1^2 z_2^2 \in \mathbb{Z}[j]$, ce qui peut encore s'écrire $(z_1^2 + z_2^2)^2 \in \mathbb{Z}[j]$. Ainsi $z_1^2 + z_2^2 \in R(\mathbb{Z}[j])$.
Donc $R(\mathbb{Z}[j])$ est bien de type S.

b. Puisque pour tout $z \in \mathbb{C}$, $|z| \leqslant 1 \iff |z^2| \leqslant 1$, les éléments de $R(\mathbb{Z}[j])$ de module inférieur ou égal à 1 sont les racines carrées des éléments de $\mathbb{Z}[j]$ de module inférieur ou égal à 1. Ces éléments ont tous deux racines carrées hormis 0 qui n'en possède qu'une. Puisque $b(\mathbb{Z}[j]) = 7$, $b(R(\mathbb{Z}[j])) = 13$.

6. Il suffit de choisir

$$\mathcal{A} = \mathbb{Z}[i] = \left\{a + bi,\ (a, b) \in \mathbb{Z}^2\right\}$$

On vérifie sans peine que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ donc une partie de type S. Donnons-nous ensuite $z \in \mathbb{Z}[i]$ et $(a, b) \in \mathbb{Z}^2$ tel que $z = a + bi$. Alors $|z| \leqslant 1$ *si et seulement si* $a^2 + b^2 \leqslant 1$. Puisque a et b sont entiers, les seuls couples (a, b) adéquats sont $(0, 0)$, $(1, 0)$, $(-1, 0)$, $(0, 1)$, $(0, -1)$. On a donc bien $b(\mathbb{Z}[i]) = 5$.

7. Il suffit de prendre $\mathcal{A} = R(\mathbb{Z}[i])$. Le même raisonnement qu'à la question **II.5** montre que $\mathcal{A}$ est bien de type S et que $b(\mathcal{A}) = 9$.

Partie III – Sous-groupes de $\mathbb{U}_n$

1. Il existe $m \in \mathbb{N}^*$ tel que $n = md$. Soit alors $z \in H$. Alors $z^n = (z^d)^m = 1$ donc $z \in \mathbb{U}_d$. Ainsi $H \subset \mathbb{U}_n$. Puisque H est déjà un sous-groupe de $\mathbb{C}^*$, c'est un sous-groupe de $\mathbb{U}_n$.

2. **a.** Considérons l'ensemble $A = \{k \in \mathbb{N}^*,\ \omega^k \in H\}$. Cet ensemble est non vide : en effet, $1 \in H$ car H est un sous-groupe de $\mathbb{U}_n$ de sorte que $n \in A$. Or A est une partie de $\mathbb{N}^*$ donc il admet un plus petit élément $m \in \mathbb{N}^*$. Puisque $n \in A$, on a donc $m \leqslant n$.

b. On sait que $\omega^m \in H$ et que H est un sous-groupe de $\mathbb{U}_n$, $(\omega^m)^k \in H$ pour tout $k \in \mathbb{Z}$. Ainsi

$$\left\{\omega^{mk},\ k \in \mathbb{Z}\right\} \subset H$$

Réciproquement, soit $z \in H$. Puisque $H \subset \mathbb{U}_n$, il existe $p \in \mathbb{Z}$ tel que $z = \omega^p$. On note q et r le quotient et le reste de la division euclidienne de p par m. Alors $z = \omega^{qm+r}$ puis $\omega^r = z\omega^{-qm}$. Puisque z et ω^{-qm} appartiennent à H, ω^r également. Par définition de la division euclidienne, $0 \leqslant r \leqslant m-1$. On ne peut avoir $r \geqslant 1$, car cela contredirait la minimalité de m. Ainsi $r = 0$ puis $z = \omega^{mq}$. On en déduit que

$$H \subset \left\{\omega^{mk},\ k \in \mathbb{Z}\right\}$$

Par double inclusion, $H = \left\{\omega^{mk},\ k \in \mathbb{Z}\right\}$.

c. Notons d et r le quotient et le reste de la division euclidienne de n par m. Alors $1 = \omega^n = \omega^{md}\omega^r$ i.e. $\omega^r = \omega^{-md}$. D'après la question précédente, $\omega^r \in H$. Or $0 \leqslant r \leqslant m-1$ et on ne peut avoir $r \geqslant 1$ par minimalité de m. Ainsi $r = 0$ puis $n = md$. Puisque $m \leqslant n$, on a donc $d \geqslant 1$ i.e. $d \in \mathbb{N}^*$.

d. On procède par double inclusion. Soit $z \in H$. D'après la question **III.2.b**, il existe $k \in \mathbb{Z}$ tel que $z = \omega^{mk}$. Alors $z^d = \omega^{kmd} = (\omega^n)^k = 1$ donc $z \in \mathbb{U}_n$.
Réciproquement, soit $z \in \mathbb{U}_d$. Il existe donc $k \in \mathbb{Z}$ tel que $z = e^{\frac{2ik\pi}{d}}$. Alors

$$z = e^{\frac{2ikm\pi}{md}} = e^{\frac{2ikm\pi}{n}} = \omega^{mk} \in H$$

Par double inclusion, $H = \mathbb{U}_d$.

Partie IV – Valeurs possibles de $b(\mathcal{A})$

1. **a.** On raisonne par récurrence. Tout d'abord, $a = a^1 \in \mathcal{A}$. Supposons que $a^n \in \mathcal{A}$ pour un certain $n \in \mathbb{N}^*$. Alors $a^{n+1} = a^n \times a \in \mathcal{A}$ car $\mathcal{A}$ est stable par produit. Finalement, $a^n \in \mathcal{A}$ pour tout $n \in \mathbb{N}$.

b. La suite de terme général $|a|^n = |a^n|$ est strictement décroissante donc injective. Il en est de même de la suite a^n. Puisque pour tout $n \in \mathbb{N}^*$, $a^n \in \mathcal{A}$ et $|a^n| = |a|^n < 1$, $b(\mathcal{A}) = \infty$.

c. Soit $n \in \mathbb{N}^*$. D'après la question **IV.1.a**, a^n et a^{2n} appartiennent à $\mathcal{A}$. Puisque $\mathcal{A}$ est de type S, $(a^n)^2 + (a^{2n})^2 = a^{2n} + a^{4n} \in \mathcal{A}$.

2. **a.** Remarquons déjà que $a = e^{i\theta}$ puisque $a \in \mathbb{U}$. Soit $n \in \mathbb{N}$. On utilise la méthode de l'arc moitié :

$$a^{2n} + a^{4n} = e^{2ni\theta} + e^{4ni\theta} = e^{3ni\theta}(e^{-in\theta} + e^{in\theta}) = 2\cos(n\theta)e^{3ni\theta}$$

Puisque $e^{3ni\theta}$ est de module 1,

$$\left|a^{2n} + a^{4n}\right| = 2|\cos(n\theta)|$$

b. Comme cos est paire, on peut supposer θ positif i.e. $\theta \in [0, \pi]$. De plus,

$$|\cos(n(\pi-\theta))| = |\cos(n\pi - n\theta)| = |\cos(n\theta)|$$

donc on peut même supposer $\theta \in \left[0, \frac{\pi}{2}\right]$.

c. Il suffit de prendre $n = 1$. En effet, $\theta \in \left]\frac{\pi}{3}, \frac{\pi}{2}\right[$ donc $0 < \cos(\theta) < \frac{1}{2}$ et donc $0 < \left|a^2 + a^4\right| < 1$.

d. Il suffit cette fois-ci de prendre $n = 2$. En effet, $2\theta \in \left]\frac{\pi}{3}, \frac{2\pi}{3}\right[\setminus \left\{\frac{\pi}{4}\right\}$ donc $0 < \cos(2\theta) < \frac{1}{2}$ et donc $0 < \left|a^4 + a^8\right| < 1$.

e. Par définition de n, $(n-1)\theta \leqslant \frac{\pi}{3}$ donc

$$\frac{\pi}{3} < n\theta \leqslant \frac{\pi}{3} + \theta < \frac{\pi}{3} + \frac{\pi}{6} = \frac{\pi}{2}$$

Ainsi $0 < \cos(n\theta) < \frac{1}{2}$ et donc $0 < \left|a^{2n} + a^{4n}\right| < 1$.

f. Quelque soit la valeur de θ, il existe $n \in \mathbb{N}^*$ tel que $0 < \left|a^{2n} + a^{4n}\right| < 1$. Or d'après la question **IV.1.c**, $a^{2n} + a^{4n} \in \mathcal{A}$. La question **IV.1.b** montre alors que $b(\mathcal{A}) = \infty$.

3. Supposons $\mathcal{A} \cap \mathbb{U} = \mathbb{U}_3$. Alors 1 et j appartiennent à $\mathcal{A} \cap \mathbb{U}$. Or $\mathcal{A}$ est de type S donc $1^2 + j^2 = e^{\frac{i\pi}{3}} \in \mathcal{A}$. Puisque $e^{\frac{i\pi}{3}} \in \mathbb{U}$, on aurait $e^{\frac{i\pi}{3}} \in \mathbb{U}_3$, ce qui est faux. Ainsi $\mathcal{A} \cap \mathbb{U} \neq \mathbb{U}_3$.

4. **a.** Puisque $b(\mathcal{A}) \geqslant 2$, $\mathcal{A}$ contient au moins deux éléments de module inférieur ou égal à 1. Mais puisque $b(\mathcal{A})$ est fini, ces deux éléments ne peuvent être que de module 0 ou 1 d'après la question **IV.1.b**. Puisqu'il n'existe qu'un seul complexe de module nul (à savoir 0), $\mathcal{A}$ contient forcément un élément de module 1.

b. Soit $a \in \mathcal{A} \cap \mathbb{U}$. Puisque $b(\mathcal{A})$ est fini, la question **IV.2** montre que son argument principal θ est un multiple de $\frac{\pi}{4}$ ou de $\frac{\pi}{6}$. Ainsi

$$a \in \left\{ e^{\frac{ik\pi}{4}},\ k \in \mathbb{Z} \right\} = \mathbb{U}_8$$

ou

$$a \in \left\{ e^{\frac{ik\pi}{6}},\ k \in \mathbb{Z} \right\} = \mathbb{U}_{12}$$

Par conséquent, $\mathcal{A} \cap \mathbb{U} \subset \mathbb{U}_8 \cup \mathbb{U}_{12}$.

c. On a clairement $\mathcal{A} \cap \mathbb{U} \subset \mathbb{U}$. Puisque $\mathcal{A}$ contient un élément de module 1, $\mathcal{A} \cap \mathcal{U}$ est non vide. $\mathcal{A}$ et $\mathbb{U}$ sont tous deux stables par produit donc $\mathcal{A} \cap \mathbb{U}$ également. Soit alors $a \in \mathcal{A} \cap \mathbb{U}$. Alors $a \in \mathbb{U}_8$ ou $a \in \mathbb{U}_{12}$ donc $a^{-1} = a^7$ ou $a^{-1} = a^{11}$. Comme $\mathcal{A} \cap \mathbb{U}$ est stable par produit, a^7 et a^{11} appartiennent tous deux à $\mathcal{A} \cap \mathbb{U}$ donc a^{-1} également. Ceci prouve que $\mathcal{A} \cap \mathbb{U}$ est bien un sous-groupe de $\mathbb{U}$.

d. D'après la question **III.1**, $\mathbb{U}_8 \cup \mathbb{U}_{12} \subset \mathbb{U}_{24}$ car 8 et 12 divisent 24. Ainsi $\mathcal{A} \cap \mathbb{U}$ est un sous-groupe de $\mathbb{U}$ inclus dans $\mathbb{U}_{24}$ donc un sous-groupe de $\mathbb{U}_{24}$. La question **III.2** montre qu'il existe un diviseur m de 24 tel que $\mathcal{A} \cap \mathbb{U} = \mathbb{U}_m$. On ne peut avoir $m = 24$ puisque $\mathbb{U}_{24}$ n'est pas inclus dans $\mathbb{U}_8 \cup \mathbb{U}_{24}$ (par exemple, $e^{\frac{i\pi}{12}}$ n'appartient ni à $\mathbb{U}_8$ ni à $\mathbb{U}_{12}$). On a vu également qu'on ne peut avoir $m = 3$ à la question **IV.3**. On a donc

$$m \in \{1, 2, 4, 6, 8, 12\}$$

e. Si $m \in \{4, 8, 12\}$, alors 1 et i appartiennent à $\mathcal{A}$. Par conséquent $1^2 + i^2 = 0$ appartient aussi à $\mathcal{A}$.

5. Supposons $b(\mathcal{A}) \geqslant 2$ et $b(\mathcal{A})$ fini. Il existe donc $m \in \{1, 2, 4, 6, 8, 12\}$ tel que $\mathcal{A} \cap \mathbb{U} = \mathbb{U}_m$. D'après la question **IV.1.b**, on a $\mathcal{A} \cap \mathcal{U} = \mathcal{A} \cap \mathbb{U}$ ou $\mathcal{A} \cap \mathcal{U} = (\mathcal{A} \cap \mathbb{U}) \cup \{0\}$ donc $b(\mathcal{A}) = m$ ou $b(\mathcal{A}) = m + 1$. De plus, si $m = 4$, $m = 8$ ou $m = 12$, on a vu que 0 appartenait nécessairement à $\mathcal{A}$ donc $b(\mathcal{A}) = m + 1$ dans ces trois cas.
Finalement, l'ensemble des valeurs potentiellement prises par $b(\mathcal{A})$ est

$$\{0, 1, 2, 3, 5, 6, 7, 9, 13, \infty\}$$

Or on a vu dans les exemples des deux premières parties que ces valeurs étaient effectivement prises par $b(\mathcal{A})$.