Devoir surveillé n° 6 : corrigé

Problème 1 — Résolution d'une équation diophantienne

Partie I –

1. Clairement $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$.
$1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Il existe donc $(a, b, c, d) \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$.
Alors $x - y = (a - c) + (b - d)\sqrt{2}$ et $(a - c, b - d) \in \mathbb{Z}^2$ donc $x - y \in \mathbb{Z}[\sqrt{2}]$.
Également, $xy = (ac + 2bd) + (ad + bc)\sqrt{2}$ et $(ac + 2bd, ad + bc) \in \mathbb{Z}^2$ donc $xy \in \mathbb{Z}[\sqrt{2}]$.
Ainsi $\mathbb{Z}[\sqrt{2}]$ est donc un sous-anneau de $(\mathbb{R}, +, \times)$.

2. **a.** Soit $x \in \mathbb{Z}[\sqrt{2}]$. L'existence d'un couple $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$ découle simplement de la définition de $\mathbb{Z}[\sqrt{2}]$. Soit maintenant $(c, d) \in \mathbb{Z}^2$ tel que

$$x = a + b\sqrt{2} = c + d\sqrt{2}$$

On a donc $(a - c) = (d - b)\sqrt{2}$. Si $d \neq b$, $\sqrt{2}$ serait rationnel. Ainsi $b = d$ et par suite $a = c$. D'où l'unicité du couple (a, b).

b. On vérifie aisément que $\varphi(x + y) = \varphi(x) + \varphi(y)$ et que $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ donc φ est un endomorphisme de l'anneau $\mathbb{Z}[\sqrt{2}]$.
Par ailleurs, $\varphi \circ \varphi = \mathrm{Id}_{\mathbb{Z}[\sqrt{2}]}$ donc φ est involutif donc bijectif. φ est donc un automorphisme de l'anneau $\mathbb{Z}[\sqrt{2}]$.

3. **a.** Soient $x \in \mathbb{Z}[\sqrt{2}]$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. Alors $N(x) = a^2 - 2b^2 \in \mathbb{Z}$.

b. Soit $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$. Alors, en utilisant que φ est un endomorphisme d'anneau

$$N(xy) = xy\overline{xy} = xy\overline{x}\,\overline{y} = x\overline{x}y\overline{y} = N(x)N(y)$$

c. Soit $x \in \mathbb{Z}[\sqrt{2}]$.
Supposons x inversible. Il existe donc $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. Ainsi $N(xy) = N(1) = 1$. D'après la question précédente, $N(xy) = N(x)N(y)$ d'où $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont entiers, on a donc $N(x) = \pm 1$ i.e. $|N(x)| = 1$.
Réciproquement soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $|N(x)| = 1$. Si $N(x) = 1$, alors $x\overline{x} = 1$ donc x est inversible (d'inverse $\overline{x}$). Si $N(x) = -1$, alors $x(-\overline{x}) = 1$ donc x est inversible (d'inverse $-\overline{x}$).

Partie II –

1. 0 n'est pas inversible donc $0 \notin H$. Ainsi $H \subset \mathbb{R}^*$. 1 est inversible en tant qu'élément neutre pour la loi $\times$ donc $1 \in H$.
Un produit d'éléments inversibles est inversible (d'inverse le produit des inverses).
Enfin, l'inverse d'un élément inversible est inversible (d'inverse l'élément initial).
On en déduit que H est un sous-groupe de $(\mathbb{R}^*, \times)$.

> **Remarque.** On peut également utiliser le résultat au programme disant que l'ensemble des éléments inversibles d'un anneau est un groupe pour la loi multiplicative. Ainsi $(H, \times)$ est un groupe. Puisque $H \subset \mathbb{R}^*$, H est un sous-groupe de $(\mathbb{R}^*, \times)$.

2. **a.** Supposons $a \geqslant 0$ et $b \geqslant 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin H$. Un des deux entiers naturels a et b est donc non nul. Ainsi $a \geqslant 1$ ou $b \geqslant 1$ et, dans les deux cas, $x \geqslant 1$.

b. Supposons $a \leqslant 0$ et $b \leqslant 0$. On ne peut avoir $(a, b) = (0, 0)$ car $0 \notin H$. Un des deux entiers a et b est donc non nul. Ainsi $a \leqslant -1$ ou $b \leqslant -1$ et, dans les deux cas, $x \leqslant -1$.

c. Supposons $ab \leqslant 0$. Alors $a(-b) \geqslant 0$. Les deux questions précédentes montrent que $|\overline{x}| \geqslant 1$. Puisque $|N(x)| = |x||\overline{x}| = 1$, $|x| \leqslant 1$.

3. **a.** Puisque $x > 1$, la question précédente montre qu'on ne peut avoir $a \leqslant 0$ et $b \leqslant 0$ ni $ab \leqslant 0$. C'est donc que nécessairement $a > 0$ et $b > 0$.

b. $u \in H^+$ car $u > 1$ et $N(u) = -1$.
Soient $x \in H^+$ et $(a, b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$. D'après la question précédente, $a \geqslant 1$ et $b \geqslant 1$ donc $x \geqslant u$. u est donc le plus petit élément de H^+.

4. **a.** Il suffit de poser $n = \left\lfloor \frac{\ln x}{\ln u} \right\rfloor$. On a alors

$$n \leqslant \frac{\ln x}{\ln u} < n + 1$$

ou encore

$$n \ln(u) \leqslant \ln(x) < (n+1) \ln u$$

car $\ln u > 0$. Puis par stricte croissance de l'exponentielle

$$u^n \leqslant x < u^{n+1}$$

b. Supposons $x \neq u^n$. Alors

$$u^n < x < u^{n+1}$$

puis

$$1 < \frac{x}{u^n} < u$$

car $u > 0$. Or H est un sous-groupe de $\mathbb{R}^*$ et $u \in H$ donc $u^n \in H$. On sait également que $x \in H$ donc $\frac{x}{u^n} \in H$ car H est un sous-groupe de $\mathbb{R}^*$. Or $\frac{x}{u^n} > 1$ donc $\frac{x}{u^n} \in H^+$. Or $\frac{x}{u^n} < u$, ce qui contredit la minimalité de u. On a donc prouvé que $x = u^n$.

5. On sait que $u \in H$ donc $u^n \in H$ pour tout $n \in \mathbb{Z}$ car H est un sous-groupe de $\mathbb{R}^*$. Puisque $-1 \in H$, on a également $-u^n \in H$ pour tout $n \in \mathbb{Z}$. Ainsi

$$\{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\} \subset H$$

Soit maintenant $x \in H$. On sait que $0 \notin H$ donc $x \neq 0$.

- Si $x > 1$, alors $x \in H^+$ et il existe donc $n \in \mathbb{Z}$ tel que $x = u^n$ d'après la question précédente.
- Si $x = 1$, alors $x = u^0$.
- Si $0 < x < 1$, alors $\frac{1}{x} \in H^+$ donc il existe $n \in \mathbb{Z}$ tel que $\frac{1}{x} = u^n$ i.e. $x = u^{-n}$.
- Si $x < 0$, alors $-x \in H$ et $-x > 0$, et les cas précédents montrent l'existence d'un $n \in \mathbb{Z}$ tel que $-x = u^n$ i.e. $x = -u^n$.

On a donc prouvé que

$$H \subset \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Par double inclusion

$$H = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$

Solution 1.

1. Puisque toutes les solutions de $(\mathcal{E})$ sont de classe $\mathcal{C}^\infty$, $E \subset \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$. La fonction nulle est clairement solution de $(\mathcal{E})$ donc appartient à E. Soient $(y_1, y_2) \in E^2$ et $(\lambda_1, \lambda_2) \in \mathbb{R}^2$. Alors

$$(\lambda_1 y_1 + \lambda_2 y_2)''' - (\lambda_1 y_1 + \lambda_2 y_2) = \lambda_1(y_1''' - y_1) + \lambda_2(y_2''' - y_2) = 0$$

donc $\lambda_1 y_1 + \lambda_2 y_2 \in E$.
E est donc bien un sous-espace vectoriel de $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$.

2. Soit $y \in F$. Alors $y'' + y' + y = 0$. Puisque y est de classe $\mathcal{C}^\infty$, on obtient en dérivant la relation précédente, $y''' + y'' + y' = 0$. En soustrayant ces deux relations, on obtient $y''' - y = 0$ de sorte que $y \in E$. Ainsi $F \subset E$.
Soit $y \in G$. Alors $y' = y$. En dérivant, on obtient $y'' = y' = y$. En dérivant à nouveau, on obtient $y''' = y' = y$. Ainsi $y \in E$. Finalement, $G \subset E$.

3. Le polynôme caractéristique associé à $(\mathcal{F})$ est X^2+X+1 dont les racines sont $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$ et $-\frac{1}{2}-i\frac{\sqrt{3}}{2}$. Les solutions de $(\mathcal{F})$ sont donc les fontions

$$t \mapsto \left(\lambda\cos\frac{t\sqrt{3}}{2}+\mu\sin\frac{t\sqrt{3}}{2}\right)e^{-\frac{t}{2}} \text{ avec } (\lambda,\mu)\in\mathbb{R}^2$$

En posant $f_1 : t \mapsto e^{-\frac{t}{2}}\cos\frac{t\sqrt{3}}{2}$ et $f_2 : t \mapsto e^{-\frac{t}{2}}\cos\frac{t\sqrt{3}}{2}$, on a donc $F = \text{vect}(f_1,f_2)$ de sorte que (f_1,f_2) est une famille génératrice de F.
Les solutions de $(\mathcal{G})$ sont les fonctions $t \mapsto \nu e^t$ avec $\nu\in\mathbb{R}$. Ainsi $G = \text{vect}(f_3)$ en posant $f_3 : t \mapsto e^t$. Ainsi (f_3) est une famille génératrice de G.

4. **a.** Puisque $y\in E$, $y'''=y$ et donc $y^{(4)}=y'$. Ainsi

$$\begin{aligned} y_1''+y_1'+y_1 &= (2y-y'-y'')''+(2y-y'-y'')'+(2y-y'-y'')\\ &= (2y''-y'''-y^{(4)})+(2y'-y''-y''')+(2y-y'-y'')\\ &= (2y''-y-y')+(2y'-y''-y)+(2y-y'-y'') = 0 \end{aligned}$$

donc $y_1\in F$. De plus

$$y_2' = (y+y'+y'')' = y'+y''+y''' = y'+y''+y = y_2$$

donc $y_2\in G$.

b. Soit $y\in F\cap G$. Puisque $y\in G$, $y'=y$ donc $y''=y'=y$. Or $y''+y'+y=0$ car $y\in F$ donc $3y=0$ puis $y=0$. Finalement $F\cap G=\{0\}$.
Puisque $F\subset E$ et $G\subset E$, $F+G\subset E$. Soit maintenant $y\in E$. Posons $y_1=2y-y'-y''$ et $y_2=y+y'+y''$. On a vu que $y_1\in F$ et $y_2\in G$. Puisque F et G sont des sous-espaces vectoriels, $\frac{1}{3}y_1\in F$ et $\frac{1}{3}y_2\in G$. Puisque $y=\frac{1}{3}y_1+\frac{1}{3}y_2$, $y\in F+G$. Ainsi $E\subset F+G$. Par double inclusion, $E=F+G$.
Mais puisque $F\cap G=\{0\}$, $E=F\oplus G$. Ainsi F et G sont supplémentaires dans E.

5. On déduit de la question précédente que

$$E = F\oplus G = \text{vect}(f_1,f_2)+\text{vect}(f_3) = \text{vect}(f_1,f_2,f_3)$$

Autrement dit, les solutions de $(\mathcal{E})$ sont les combinaisons linéaires de f_1, f_2 et f_3, c'est-à-dire les fonctions

$$t \mapsto \left(\lambda\cos\frac{t\sqrt{3}}{2}+\mu\sin\frac{t\sqrt{3}}{2}\right)e^{-\frac{t}{2}}+\nu e^t \text{ avec } (\lambda,\mu,\nu)\in\mathbb{R}^3$$

Solution 2.

1. **a.** Puisque $a>1$ et $n>0$, $a^n+1>2$. Puisque a^n+1 est premier et distinct de 2, il est impair. Ainsi a^n est pair et donc a est pair.

b. On a $a^k\equiv -1\left[a^k+1\right]$, puis $(a^k)^m\equiv -1\left[a^k+1\right]$. Puisque m est impair, $a^{km}\equiv -1\left[a^k+1\right]$ i.e. $a^n+1\equiv 0\left[a^k+1\right]$. Ainsi a^k+1 divise a^n+1. Puisque a^n+1 est premier, on en déduit que $a^k+1=1$, ce qui est exclu, ou $a^k+1=a^n+1$. Puisque $a>1$, on obtient $k=n$ et donc $m=1$, ce qui est impossible car $m\geqslant 3$.

c. On déduit de la question précédente que n n'admet pas de diviseur premier impair. Le seul diviseur premier de n est donc 2. Le théorème de décomposition en facteurs premiers assure alors que n est une puissance de 2.

2. **a.** Soit $n\in\mathbb{N}$.

$$F_{n+1}-1 = 2^{2^{n+1}} = \left(2^{2^n}\right)^2 = (F_n-1)^2$$

b. On raisonne par récurrence. On a bien $F_1-2=3=F_0$. Supposons qu'il existe $n\in\mathbb{N}^*$ tel que $F_{n+1}=(F_n-1)^2+1$. Alors, d'après la question précédente

$$F_{n+1}-2 = (F_n-1)^2-1 = F_n(F_n-2) = F_n\prod_{k=0}^{n-1}F_k = \prod_{k=0}^{n}F_k$$

Par récurrence, $F_n-2=\prod_{k=0}^{n-1}F_k$ pour tout $n\in\mathbb{N}^*$.

c. On a $n \in \mathbb{N}^*$ et on peut appliquer la question précédente. Ainsi $F_n - 2 = \prod_{k=0}^{n-1} F_k$ ou encore $F_n - \prod_{k=0}^{n-1} F_k = 2$. D'une part, $F_m \wedge F_n$ divise F_n et, d'autre part, $F_m \wedge F_n$ divise F_m donc $\prod_{k=0}^{n-1} F_k$ puisque $m < n$. Ainsi $F_m \wedge F_n$ divise 2. Par ailleurs, F_n est impair donc $F_m \wedge F_n = 1$.

3. **a.** Puisque p divise F_n, $2^{2^n} \equiv -1[p]$. En élevant au carré, $2^{2^{n+1}} \equiv 1[p]$ donc $2^{n+1} \in A$.

b. A est une partie non vide (d'après la question précédente) de $\mathbb{N}^*$: elle admet donc un minimum.

c. Notons q et r le quotient et le reste de la division euclidienne de 2^{n+1} par m. On a donc $2^{n+1} = qm + r$ avec $0 \leqslant r < m$. De plus, $q \in \mathbb{N}$ puisque 2^{n+1} et m sont positifs. Ainsi $2^{2^{n+1}} = (2^m)^q \cdot 2^r$. Or $m \in A$ donc $2^m \equiv 1[p]$ puis $(2^m)^q \equiv 1[p]$. Finalement $2^{2^{n+1}} \equiv 2^r[p]$. Or $2^{n+1} \in A$ donc $2^r \equiv 1[p]$. Si on avait $r > 0$, on aurait $r \in A$ et $r < m$, ce qui est impossible car $m = \min A$. Ainsi $r = 0$ de sorte que m divise 2^{n+1}.

d. Il s'ensuit que m est une puissance de 2. Il existe donc un entier naturel $q \leqslant n+1$ tel que $m = 2^q$. Supposons $q \leqslant n$. Puisque $2^{2^q} \equiv 1[p]$, on obtient en élevant à la puissance 2^{n-q}, $2^{2^n} \equiv 1[p]$. Or p divise F_n donc $2^{2^n} \equiv -1[p]$. Ainsi $2 \equiv 0[p]$ i.e. p divise 2. Puisque p est premier, on aurait $p = 2$, ce qui est impossible car F_n est impair.

e. Puisque F_n est impair, $p \neq 2$ et donc p est impair. En particulier, 2 est premier avec p. D'après le petit théorème de Fermat, $2^{p-1} \equiv 1[p]$ et $p - 1 \in A$.

f. En écrivant à nouveau la division euclidienne de $p-1$ par $m =$, la minimalité de m montre que m divise $p-1$ i.e. $p \equiv 1[m]$. Puisque $m = 2^{n+1}$, $p \equiv 1 \left[2^{n+1}\right]$.