Devoir surveillé n°06 : corrigé

Solution 1.

1. Une récurrence simple montre que $F_n > 0$ pour tout entier $n \in \mathbb{N}^*$. Soit un entier $n \geqslant 3$. Alors $F_n - F_{n-1} = F_{n-2} > 0$ car $n-2 \in \mathbb{N}^*$.

2. On sait que $F_{n+1} = 1 \times F_n + F_{n-1}$. Or $n-1 \geqslant 2$ donc $F_{n-1} < F_n$ d'après la première question. Par ailleurs, $F_{n-1} \geqslant 0$ donc F_{n-1} est le reste de la division euclidienne de F_{n+1} par F_n.

3. On trouve $\varphi = \frac{1+\sqrt{5}}{2}$.

4. Tout d'abord, $F_2 = 1 \geqslant 1 = \varphi^0$. Puis
$$\varphi = \frac{1+\sqrt{5}}{2} \leqslant \frac{1+\sqrt{9}}{2} = 2 = F_3$$
Supposons qu'il existe un certain $n \in \mathbb{N}$ tel que $F_{n+2} \geqslant \varphi^n$ et $F_{n+3} \geqslant \varphi^{n+1}$. Alors
$$F_{n+4} = F_{n+2} + F_{n+3} \geqslant \varphi^n + \varphi^{n+1} = \varphi^n(1+\varphi) = \varphi^n \cdot \varphi^2 = \varphi^{n+2}$$
Par récurrence double, $F_{n+2} \geqslant \varphi^n$ pour $n \in \mathbb{N}$.

5. On a donc $r_0 = 169$ et $r_1 = 104$ puis on trouve successivement $r_2 = 65$, $r_3 = 39$, $r_4 = 26$, $r_5 = 13$ et $r_6 = 0$. Ainsi $N = 6$ et $169 \wedge 104 = 13$.

6. La question **2** permet de montrer par récurrence que $r_k = F_{n+1-k}$ lorsque $n+1-k \geqslant 2$. Notamment $r_{n-2} = F_3$ et $r_{n-1} = F_2$. Ensuite
$$F_3 = 2 = 2 \times F_2 + 0$$
de sorte que $r_n = 0$. Ainsi $N = n$ et $F_{n+1} \wedge F_n = r_{N-1} = r_{n-1} = F_2 = 1$.

7. Pour tout $k \in [\![1, N-1]\!]$, r_{k+1} est le reste de la division euclidienne de r_{k-1} par r_k donc $r_{k+1} < r_k$. Par ailleurs, $a > b$ donc $r_0 > r_1$. La suite $(r_k)_{0 \leqslant k \leqslant N}$ est donc bien strictement décroissante.

8. Comme $(a, b) \neq (0, 0)$, $r_{N-1} = a \wedge b \neq 0$. Ainsi, $r_{N-1} \geqslant 1$. Par ailleurs, en notant q le quotient de la division euclidienne de r_{N-2} par r_{N-1},
$$r_{N-2} = qr_{N-1} + r_N = qr_{N-1}$$
On ne peut avoir $q = 0$ car r_{N-2} n'est pas nul, ni $q = 1$ car $r_{N-1} < r_{N-2}$ puisque r_{N-1} est le reste de la division euclidienne de r_{N-3} par r_{N-2}. Ainsi $q \geqslant 2$. Ainsi $r_{N-2} \geqslant 2r_{N-1}$.

9. On procède par récurrence double. On note $\mathcal{P}_k$ l'assertion «$r_{N+1-k} \geqslant F_k$».
Tout d'abord $r_{N-1} \geqslant 1 = F_2$ et $r_{N-2} \geqslant 2r_{n-1} \geqslant 2 = F_3$ donc $\mathcal{P}_2$ et $\mathcal{P}_3$ sont vraies. Supposons qu'il existe $k \in [\![2, N-2]\!]$ tels que $\mathcal{P}_k$ et $\mathcal{P}_{k+1}$ soient vraies. Alors $r_{N+1-k} \geqslant F_k$ et $r_{N-k} \geqslant F_{k+1}$. En notant q le reste de la division euclidienne de r_{N-1-k} par r_{N-k}, on a
$$r_{N-1-k} = qr_{N-k} + r_{N+1-k}$$
A nouveau, q ne peut être nul puisque $r_{N+1-k} < r_{N-1-k}$. Ainsi $q \geqslant 1$ (q est entier) donc
$$r_{N-1-k} \geqslant r_{N-k} + r_{N-1-k} \geqslant \varphi^k + \varphi^{k+1} = \varphi^k(1+\varphi) = \varphi^k \cdot \varphi^2 = \varphi^{k+2}$$
Ainsi $\mathcal{P}_{k+2}$ est vraie. Finalement, par récurrence double finie, $\mathcal{P}_k$ est vraie pour tout $k \in [\![2, N]\!]$.

10. En particulier, lorsque $k = N$, $b = r_1 \geqslant F_N \geqslant \varphi^{N-2}$ (question **4**). Par croissance de ln, $\ln(b) \geqslant (N-2)\ln(\varphi)$. Or $\varphi > 1$ donc $\frac{\ln(b)}{\ln(\varphi)} \geqslant N-2$. Puisque la partie entière d'un réel est le plus grand entier supérieur à ce réel et que $N-2$ est entier, $N-2 \leqslant \left\lfloor \frac{\ln(b)}{\ln(\varphi)} \right\rfloor$, ce qui donne le résultat voulu.

Remarque. Le résultat démontré est le théorème de Lamé. Le nombre de divisions euclidiennes utilisées dans l'algorithme d'Euclide est $N-1$. Le théorème de Lamé donne donc une majoration de ce nombre de divisions. Cette majoration est optimale comme le montre la question **6**. ■

Solution 2.

1. La fonction f est continue et strictement croissante sur $\mathbb{R}_+^*$. De plus, $\lim_{0^+} f = -\infty$ et $\lim_{+\infty} f = +\infty$ donc f est une bijection de $]0, +\infty[$ sur $]-\infty, +\infty[$, c'est-à-dire de $\mathbb{R}_+^*$ sur $\mathbb{R}$.

2. f^{-1} est de même sens de variation que f, c'est-à-dire strictement croissante. Puisque $\lim_{0^+} f = -\infty$ et $\lim_{+\infty} f = +\infty$, $\lim_{-\infty} f^{-1} = 0^+$ et $\lim_{+\infty} f^{-1} = +\infty$.

   Remarque. Plus rigoureusement, f^{-1} est strictement croissante donc elle admet des limites en $-\infty$ et $+\infty$. De plus,
   $$\lim_{+\infty} f^{-1} = \inf_{\mathbb{R}} f^{-1} = 0$$
   $$\lim_{+\infty} f^{-1} = \sup_{\mathbb{R}} f^{-1} = +\infty$$
   ■

3. Soit $n \in \mathbb{N}^*$. Alors n admet un unique antécédent par f dans $\mathbb{R}_+^*$ car f est une bijection de $\mathbb{R}_+^*$ sur $\mathbb{R}$. Ainsi l'équation $f(x) = n$ admet une unique solution sur $\mathbb{R}_+^*$.

4. La question précédente montre en fait que $x_n = f^{-1}(n)$. Puisque f^{-1} est croissante, pour tout $n \in \mathbb{N}^*$, $f^{-1}(n) \leqslant f^{-1}(n+1)$ i.e. $x_n \leqslant x_{n+1}$. La suite (x_n) est donc croissante.

5. Puisque $\lim_{+\infty} f^{-1} = +\infty$ et que $x_n = f^{-1}(n)$ pour tout $n \in \mathbb{N}^*$, $\lim_{n\to+\infty} x_n = +\infty$.

6. Pour tout $n \in \mathbb{N}^*$, $n = x_n + \ln(x_n)$. Or $\ln(u) \underset{u\to+\infty}{=} o(u)$ et $\lim_{n\to+\infty} x_n = +\infty$ donc $\ln(x_n) \underset{n\to+\infty}{=} o(x_n)$. Ainsi $x_n + \ln(x_n) \underset{n\to+\infty}{=} x_n + o(x_n)$ ou encore $x_n + \ln(x_n) \underset{n\to+\infty}{\sim} x_n$. Finalement, $x_n \underset{n\to+\infty}{\sim} n$.

7. Soit $n \in \mathbb{N}^*$.
   $$x_{n+1} - x_n = (n+1-\ln(x_{n+1})) - (n - \ln(x_n)) = 1 - \ln\left(\frac{x_{n+1}}{x_n}\right)$$
   Or $x_n \underset{n\to+\infty}{\sim} n$ et $x_{n+1} \underset{n\to+\infty}{\sim} n+1 \underset{n\to+\infty}{\sim} n$ donc $\frac{x_{n+1}}{x_n} \underset{n\to+\infty}{\sim} 1$. Ainsi $\lim_{n\to+\infty} \frac{x_{n+1}}{x_n} = 1$ puis $\lim_{n\to+\infty} \ln\left(\frac{x_{n+1}}{x_n}\right) = 0$. Finalement, $\lim_{n\to+\infty} x_{n+1} - x_n = 1$.

8. **a.** Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Remarquons que $n - x_n = \ln(x_n)$ donc
   $$u_n - 1 = \frac{\ln(x_n)}{\ln(n)} - 1 = \frac{\ln(x_n) - \ln(n)}{\ln(n)} = \frac{\ln(x_n/n)}{\ln(n)}$$

   b. On sait que $x_n \underset{n\to+\infty}{\sim} n$ donc $\lim_{n\to+\infty} \frac{x_n}{n} = 1$ puis $\lim_{n\to+\infty} \ln(x_n/n) = 0$. Par ailleurs, $\lim_{n\to+\infty} \ln(n) = +\infty$. Par opérations, $\lim_{n\to+\infty} \frac{\ln(x_n/n)}{\ln(n)} = 0$. Ainsi $\lim_{n\to+\infty} u_n - 1 = 0$ puis $\lim_{n\to+\infty} u_n = 1$.

   c. La question précédente montre que $u_n \underset{n\to+\infty}{=} 1 + o(1)$. On en déduit successivement que
   $$\frac{n - x_n}{\ln(n)} \underset{n\to+\infty}{=} 1 + o(1)$$
   puis que
   $$n - x_n \underset{n\to+\infty}{=} \ln(n) + o(\ln(n))$$
   ensuite que
   $$x_n \underset{n\to+\infty}{=} n - \ln(n) + o(\ln(n))$$
   et enfin que
   $$\frac{x_n}{n} \underset{n\to+\infty}{=} 1 - \frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)$$
   Puisque $\ln(1+u) \underset{u\to0}{=} u + o(u)$ et que $\lim_{n\to+\infty} \frac{\ln(n)}{n} = 0$,
   $$\ln(x_n/n) \underset{n\to+\infty}{=} -\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)$$
   ou encore que
   $$\ln(x_n/n) \underset{n\to+\infty}{\sim} -\frac{\ln(n)}{n}$$
   Ainsi
   $$1 - u_n = -\frac{\ln(x_n/n)}{\ln(n)} \underset{n\to+\infty}{\sim} \frac{1}{n}$$

9. Puisque $u_n = \frac{n-x_n}{\ln(n)}$ pour $n \in \mathbb{N} \setminus \{0, 1\}$, la question précédente montre que

$$1 - \frac{n - x_n}{\ln(n)} \underset{n\to+\infty}{=} \frac{1}{n} + o\left(\frac{1}{n}\right)$$

On déduit successivement que

$$\frac{x_n - n}{\ln(n)} \underset{n\to+\infty}{=} -1 + \frac{1}{n} + o\left(\frac{1}{n}\right)$$

puis que

$$x_n - n \underset{n\to+\infty}{=} -\ln(n) + \frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)$$

et enfin que

$$x_n \underset{n\to+\infty}{=} n - \ln(n) + \frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)$$

Solution 3.

1. Soit $x \in [0, 1]$. Alors $\sqrt{x} \in [0, 1]$ donc $f(x) = 1 - \sqrt{x} \in [0, 1]$.

2. On procède par récurrence. Tout d'abord, $u_0 \in [0, 1]$. Supposons que $u_n \in [0, 1]$ pour un certain $n \in \mathbb{N}$. Alors $u_{n+1} = f(u_n) \in [0, 1]$ d'après la question précédente.

3. f est clairement décroissante sur $[0, 1]$ à valeurs dans $[0, 1]$. On en déduit que $f \circ f$ est croissante sur $[0, 1]$.

4. Pour $x \in [0, 1]$,

$$\begin{aligned}
& f(x) = x \\
\iff\quad & \sqrt{x} = 1 - x \\
\iff\quad & x = (1-x)^2 && \text{car les membres de l'égalité précédente sont positifs} \\
\iff\quad & x^2 - 3x + 1 = 0
\end{aligned}$$

Les racines du trinôme précédent sont $\frac{3-\sqrt{5}}{2}$ et $\frac{3+\sqrt{5}}{2}$. La première racine appartient à l'intervalle $[0, 1]$ puisque $1 \leqslant \sqrt{5} \leqslant 3$ mais la seconde racine n'appartient pas à l'intervalle $[0, 1]$ car $\sqrt{5} > 1$.
Finalement, l'unique point fixe de f sur $[0, 1]$ est $\alpha = \frac{3-\sqrt{5}}{2}$.

5. Puisque $20 \leqslant 25$, $5 \leqslant \frac{25}{4}$ puis $\sqrt{5} \leqslant \frac{5}{2}$ puis $\alpha = \frac{3-\sqrt{5}}{2} \geqslant \frac{1}{4} = u_0$.

6. On procède par récurrence. Tout d'abord, $u_0 \leqslant \alpha$. Supposons $u_{2n} \leqslant \alpha$ pour un certain $n \in \mathbb{N}$. Alors par croissance de $f \circ f$ sur $[0, 1]$,

$$f \circ f(u_{2n}) \leqslant f \circ f(\alpha)$$

c'est-à-dire

$$u_{2n+2} \leqslant \alpha$$

On en déduit que $u_{2n} \leqslant \alpha$ pour tout $n \in \mathbb{N}$.

7. On a $u_0 = \frac{1}{4}$ puis $u_1 = \frac{1}{2}$ et enfin $u_2 = 1 - \frac{1}{\sqrt{2}}$. Puisque $8 \leqslant 9$, $\frac{1}{2} \leqslant \frac{9}{16}$ puis $\frac{1}{\sqrt{2}} \leqslant \frac{3}{4}$ et enfin $u_2 = 1 - \frac{1}{\sqrt{2}} \geqslant \frac{1}{4} = u_0$.
Supposons maintenant que $u_{2n} \leqslant u_{2n+2}$ pour un certain $n \in \mathbb{N}$. Par croissance de $f \circ f$, $u_{2n+2} = f \circ f(u_{2n}) \leqslant f \circ f(u_{2n+2}) = u_{2n+4}$. Par récurrence, on a donc $u_{2n} \leqslant u_{2n+2}$ pour tout $n \in \mathbb{N}$. Ainsi (u_{2n}) est croissante. La suite (u_{2n}) est croissante et majorée par α donc elle converge.

8. Soit $x \in [0,1]$.

$$\begin{aligned}
& f \circ f(x) = x \\
\iff \quad & 1 - \sqrt{1-\sqrt{x}} = x \\
\iff \quad & 1 - x = \sqrt{1-\sqrt{x}} \\
\iff \quad & (1-x)^2 = 1 - \sqrt{x} \qquad \text{car les membres de l'égalité précédente sont positifs} \\
\iff \quad & \sqrt{x} = 1 - (1-x)^2 \\
\iff \quad & \sqrt{x} = x(2-x) \\
\iff \quad & x = x^2(2-x)^2 \qquad \text{car les membres de l'égalité précédente sont positifs} \\
\iff \quad & x^2(2-x)^2 - x = 0 \\
\iff \quad & x\left(x(2-x)^2 - 1\right) = 0 \\
\iff \quad & x(x^3 - 4x^2 + 4x - 1) = 0 \\
\iff \quad & x(x-1)(x^2 - 3x + 1) = 0
\end{aligned}$$

Or on a vu précédemment que α est la seule racine du trinôme $x^2 - 3x + 1$ dans l'intervalle $[0,1]$. On en déduit que les points fixes de $f \circ f$ sur $[0,1]$ sont 0, α et 1.

9. f est continue sur $[0,1]$ à valeurs dans $[0,1]$ donc $f \circ f$ est continue sur $[0,1]$. De plus, $u_{2n+2} = f \circ f(u_{2n})$ et $u_{2n} \in [0,1]$ pour tout $n \in \mathbb{N}$ donc la suite (u_{2n}) converge vers un point fixe de $f \circ f$ sur $[0,1]$, à savoir 0, α ou 1.
Or (u_{2n}) est croissante et majorée par α donc $u_0 \leqslant u_{2n} \leqslant \alpha$ pour tout $n \in \mathbb{N}$. Sa limite ℓ vérifie donc $u_0 \leqslant \ell \leqslant \alpha$.
A fortiori, $0 < \ell \leqslant \alpha$. Puisque ℓ est un point fixe de $f \circ f$, $\ell = \alpha$.
Enfin, $u_{2n+1} = f(u_{2n})$ pour tout $n \in \mathbb{N}$ et f est continue sur $[0,1]$ donc (u_{2n+1}) converge vers $f(\alpha) = \alpha$.
Puisque les suites (u_{2n}) et (u_{2n+1}) convergent toutes les deux vers α, la suite (u_n) converge également vers α.

Solution 4.

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. Soit $(x,y) \in \mathbb{Z}[\sqrt{2}]$. 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

$$\overline{x \cdot y} = \overline{(a + b\sqrt{2})(c + d\sqrt{2})} = \overline{ac + 2bd + (ad + bc)\sqrt{2}} = ac + 2bd - (ad + bc)\sqrt{2}$$
$$\overline{x} \cdot \overline{y} = \overline{a + b\sqrt{2}c + d\sqrt{2}} = (a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bc - (ad + bc)\sqrt{2}$$

On a donc bien $\overline{x \cdot y} = \overline{x} \cdot \overline{y}$.

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

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

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 $-\overline{x}$).

4. **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 $|N(x)| = |x||\overline{x}| = 1$, $|x| \leqslant 1$.

5. **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 $x \geqslant u$. Ainsi u est un minorant de H^+.
   u est donc le minimum de H^+.

6. **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 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 groupe. 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 $x = u^n$.

7. On sait que $u \in H$ donc $u^n \in H$ pour tout $n \in \mathbb{Z}$ car H est un groupe. 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
$$H = \{u^n, n \in \mathbb{Z}\} \cup \{-u^n, n \in \mathbb{Z}\}$$