DS n°6 : Arithmétique, structures algébriques – Corrigé

Noté sur beaucoup de points, ±5 pts pour le soin et la clarté, puis la note est divisée par 5 pour faire une note sur 20.

Exercice 1 : Une équation diophantienne... avec de l'algèbre

On s'intéresse dans ce problème à l'*équation de Pell-Fermat* $x^2 - 3y^2 = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$. Afin de la résoudre, on pose $\mathbb{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\right\}$.

1) a) Montrer que $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$. **5 pts**

On a $\mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$ par définition.

- $1 = 1 + 0\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$
- Soit $x, y \in \mathbb{Z}[\sqrt{3}]$. Il existe $a, b, c, d \in \mathbb{Z}$ tels que $x = a + b\sqrt{3}$ et $y = c + d\sqrt{3}$. Alors
$$x - y = a - c + (b - d)\sqrt{3}$$
Comme $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$, on a $x - y \in \mathbb{Z}[\sqrt{3}]$.
- De plus,
$$xy = (a + b\sqrt{3})(c + d\sqrt{3}) = ac + 3bd + (ad + bc)\sqrt{3}$$
Comme $ac + 3bd \in \mathbb{Z}$ et $ad + bc \in \mathbb{Z}$, on a $xy \in \mathbb{Z}[\sqrt{3}]$.

Ainsi, $\mathbb{Z}[\sqrt{3}]$ est un sous-anneau de $\mathbb{R}$.

b) Montrer que $\sqrt{3}$ est irrationnel, puis que pour tout $x \in \mathbb{Z}[\sqrt{3}]$, il existe un unique couple $(a, b) \in \mathbb{Z}^2$ pour lequel $x = a + b\sqrt{3}$. **10 pts**

Supposons par l'absurde que $\sqrt{3}$ est rationnel. Il existe donc un couple $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que
$$\sqrt{3} = \frac{a}{b}$$
De plus, on peut supposer $a \wedge b = 1$ pour rendre la fraction irréductible. On

en déduit que $3 = \dfrac{a^2}{b^2}$, puis $a^2 = 3b^2$. En particulier,
$$\begin{aligned} & v_3(a^2) = v_3(3b^2) \\ \Longrightarrow\ & 2v_3(a) = v_3(3) + v_3(b^2) \\ \Longrightarrow\ & 2v_3(a) = 1 + 2v_3(b) \end{aligned}$$
Ainsi, $1 = 2(v_3(a) - v_3(b))$ et donc 1 est pair. Contradiction. Ainsi, $\sqrt{3}$ est irrationnel.

Soit maintenant $x \in \mathbb{Z}[\sqrt{3}]$. Par définition, il existe $a, b \in \mathbb{Z}$ tel que $x = a + b\sqrt{3}$. Il reste à montrer l'unicité du couple (a, b). Soit (a_1, b_1) et (a_2, b_2) deux couples d'entiers tels que
$$x = a_1 + b_1\sqrt{3} = a_2 + b_2\sqrt{3}$$
Alors
$$a_1 - a_2 = (b_2 - b_1)\sqrt{3}$$
Supposons par l'absurde que $b_2 \neq b_1$. Alors $\sqrt{3} = \dfrac{a_1 - a_2}{b_2 - b_1} \in \mathbb{Q}$, ce qui est absurde par ce qui précède. Donc $b_1 = b_2$, et par suite $a_1 - a_2 = 0\sqrt{3} = 0$ donc $a_1 = a_2$. Finalement, on a bien $(a_1, b_1) = (a_2, b_2)$: il y a unicité d'un tel couple.

c) Montrer que l'application $x \mapsto \overline{x}$ est un automorphisme d'anneau de $\mathbb{Z}[\sqrt{3}]$. **9 pts**

Soit $x = a + b\sqrt{3}$ et $y = c + d\sqrt{3}$ deux éléments de $\mathbb{Z}[\sqrt{3}]$, avec $a, b, c, d \in \mathbb{Z}$. On peut remarquer que
$$\overline{x} = a - b\sqrt{3} = a + (-b)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$$
et donc l'application $x \mapsto \overline{x}$ est bien définie de $\mathbb{Z}[\sqrt{3}]$ dans lui-même. Ensuite :

- $$\overline{x + y} = \overline{(a + c) + (b + d)\sqrt{3}} = a + c - (b + d)\sqrt{3}$$
$$\overline{x} + \overline{y} = \overline{a + b\sqrt{3}} + \overline{c + d\sqrt{3}} = a - b\sqrt{3} + c - d\sqrt{3}$$
Ainsi, $\overline{x + y} = \overline{x} + \overline{y}$.

- De plus, par la question 1,

$$\overline{xy} = \overline{ac + 3bd + (ad+bc)\sqrt{3}} = ac + 3bd - (ad+bc)\sqrt{3}$$

$$\overline{x}\,\overline{y} = \left(a - b\sqrt{3}\right)\left(c - d\sqrt{3}\right) = ac + 3bd + (-ad - bc)\sqrt{3}$$

si bien que $\overline{xy} = \overline{x}\,\overline{y}$.

- Enfin, $\overline{1} = \overline{1 + 0\sqrt{3}} = 1 - 0\sqrt{3} = 1$.

Par conséquent, $x \mapsto \overline{x}$ est un morphisme d'anneaux. De plus, c'est clairement un endomorphisme de $\mathbb{Z}[\sqrt{3}]$. Enfin, on a

$$\overline{\overline{x}} = \overline{a - b\sqrt{3}} = a + b\sqrt{3} = x$$

Ainsi, l'application $x \mapsto \overline{x}$ est une involution : elle est en particulier bijective. Ainsi, c'est un automorphisme de l'anneau $\mathbb{Z}[\sqrt{3}]$.

2) Pour tout $x \in \mathbb{Z}[\sqrt{3}]$, on appelle *norme* de x et on note $N(x)$ le réel $x\overline{x}$.

a) Montrer que pour tous $x, x' \in \mathbb{Z}[\sqrt{3}]$, on a $N(xx') = N(x)N(x')$ et $N(x) \in \mathbb{Z}$. **4,5 pts**

Soit $x, x' \in \mathbb{Z}[\sqrt{3}]$. Alors

$$\begin{aligned} N(xx') &= xx'\overline{xx'} \\ &= xx'\overline{x}\,\overline{x'} \qquad \text{par la question 1.c)} \\ &= x\overline{x}\,x'\overline{x'} \\ &= N(x)N(x') \end{aligned}$$

Enfin, si $x = a + b\sqrt{3}$ avec $a, b \in \mathbb{Z}$, on a

$$N(x) = x\overline{x} = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2 \in \mathbb{Z}$$

b) On pose $G = \left\{x \in \mathbb{Z}[\sqrt{3}] \mid x > 0 \quad \text{et} \quad N(x) = 1\right\}$. Montrer que G est un sous-groupe de $\mathbb{R}^*$. **10 pts**

Soit $x \in G$. Alors $x > 0$ et donc $x \in \mathbb{R}^*$. D'où $G \subset \mathbb{R}^*$.

- On a $1 \in \mathbb{Z}[\sqrt{3}]$, $1 > 0$ et $N(1) = N(1 + 0\sqrt{3}) = 1^2 - 3 \times 0^2 = 1$ par la question a). Ainsi, $1 \in G$.

- Soit $x, y \in G$. Montrons que $xy \in G$. Tout d'abord, $xy \in \mathbb{Z}[\sqrt{3}]$ car $\mathbb{Z}[\sqrt{3}]$ est un anneau. De plus, on a $x > 0$ et $y > 0$ donc $xy > 0$. Enfin, $N(xy) = N(x)N(y) = 1 \times 1 = 1$ par la question a). D'où $xy \in G$.

- Soit $x \in G$. Montrons que $x^{-1} = \dfrac{1}{x} \in G$. Comme $N(x) = 1 = x\overline{x}$, on constate que $\dfrac{1}{x} = \overline{x} \in \mathbb{Z}[\sqrt{3}]$. De plus, comme $x > 0$ on a aussi $\dfrac{1}{x} > 0$. Enfin, comme $x\overline{x} = 1$, en passant à la norme, on a

$$N(x\overline{x}) = N(1) \implies N(x)N(\overline{x}) = 1 \implies N(\overline{x}) = 1 \qquad \text{car } N(x) = 1$$

Ainsi, $x^{-1} \in G$

Finalement, G est un sous-groupe de $\mathbb{R}^*$.

3) Soit $x = a + b\sqrt{3} \in G \cap]1, +\infty[$.

a) Montrer que $a > 0$. **8 pts**

Comme $N(x) = x\overline{x} = 1$ et que $x > 0$, on a également $\overline{x} > 0$. Ainsi,

$$x + \overline{x} = 2a > 0$$

on en déduit que $a > 0$. *Note* : on pouvait aussi raisonner par l'absurde. Voici les grandes lignes : si $a \leq 0$, on montre que $b > 0$ puis comme $N(x) > 0$, on a aussi $a - b\sqrt{3} > 0$, ce qui est une contradiction.

b) Montrer que $x^2 = 1 + 2bx\sqrt{3}$, puis que $b > 0$. **7 pts**

On a

$$\begin{aligned} & x^2 = 1 + 2bx\sqrt{3} \\ \iff & (a + b\sqrt{3})^2 = 1 + 2b\sqrt{3}\left(a + b\sqrt{3}\right) \\ \iff & a^2 + 2ab\sqrt{3} + 3b^2 = 1 + 2ab\sqrt{3} + 6b^2 \\ \iff & a^2 - 3b^2 = 1 \\ \iff & N(x) = 1 \end{aligned}$$

Or cette dernière assertion est vraie car $x \in G$. Ainsi, $x^2 = 1 + 2bx\sqrt{3}$.

Montrons que $b > 0$. Comme $x > 1$, on a $x^2 > 1$ et $2x\sqrt{3} > 0$, de sorte que :

$$b = \frac{x^2 - 1}{2x\sqrt{3}} > 0$$

c) En déduire que $2+\sqrt{3}$ est le plus petit élément de $G \cap]1,+\infty[$. **12 pts**

- Tout d'abord, montrons que $2+\sqrt{3} \in G \cap]1,+\infty[$. On a $2+\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, $2+\sqrt{3} > 0$ et

$$N(2+\sqrt{3}) = (2+\sqrt{3})(2-\sqrt{3}) = 4-3 = 1$$

Ainsi, $2+\sqrt{3} \in G$. De plus $2+\sqrt{3} > 1$. Ainsi, $2+\sqrt{3} \in G \cap]1,+\infty[$.

- Pour conclure, il suffit de montrer que pour tout $x \in G \cap]1,+\infty[$, on a $x \geq 2+\sqrt{3}$. Soit $a, b \in \mathbb{Z}$ tels que $x = a+b\sqrt{3}$. Par les questions précédentes, on a $a > 0$ et $b > 0$. Donc $a \geq 1$ et $b \geq 1$. Supposons par l'absurde que $x < 2+\sqrt{3}$. Alors

$$\begin{aligned} & a+b\sqrt{3} < 2+\sqrt{3} \\ \Longrightarrow\ & (b-1)\sqrt{3} < 2-a \end{aligned}$$

Comme $(b-1)\sqrt{3} \geq 0$, on en déduit que $2-a > 0$, donc $a < 2$. Comme on a également $a \geq 1$, on a donc $a = 1$. On en déduit que

$$\begin{aligned} & (b-1)\sqrt{3} < 1 \\ \Longrightarrow\ & b-1 < \frac{1}{\sqrt{3}} \leq 1 \end{aligned}$$

Comme $b-1 < 1$, on a donc $b < 2$. Comme on a également $b \geq 1$, on a donc $b = 1$. Finalement, $x = 1+\sqrt{3}$. Mais alors $N(x) = (1+\sqrt{3})(1-\sqrt{3}) = 1-3 = -2 \neq 1$, donc $x \notin G$. Contradiction. Ainsi $x \geq 2+\sqrt{3}$.

Finalement, $2+\sqrt{3}$ est le minimum de $G \cap]1,+\infty[$.

4) a) Soit $x \in G$. Montrer que $(2+\sqrt{3})^n \leq x < (2+\sqrt{3})^{n+1}$ pour un certain $n \in \mathbb{Z}$, puis que $x = (2+\sqrt{3})^n$. **20 pts**

Soit $x \in G$. On pose

$$A = \left\{ m \in \mathbb{Z} \mid (2+\sqrt{3})^m \leq x \right\}$$

Montrons que A possède un maximum.

- Tout d'abord, on affirme que A est majorée. En effet, si par l'absurde A n'était pas majorée, il existerait une suite $(m_p)_{p\in\mathbb{N}}$ d'entiers dans A telle que $m_p \to +\infty$. Ainsi, pour tout $p \in \mathbb{N}$, on aurait $(2+\sqrt{3})^{m_p} \leq x$. En faisant tendre p vers $+\infty$, on aurait $+\infty \leq x$, ce qui est absurde.

- Par ailleurs, on affirme que $A \neq \varnothing$. En effet, supposons par l'absurde que $A = \varnothing$. Alors pour tout $N \in \mathbb{N}$, on aurait $-N \notin A$ et donc $x < (2+\sqrt{3})^{-N}$. En particulier, en faisant tendre N vers $+\infty$, on obtient $x \leq 0$. Cela est absurde car $x \in G$, donc $x > 0$ par hypothèse. Ainsi $A \neq \varnothing$.

Finalement, A est une partie non vide et majorée de $\mathbb{Z}$, donc admet un maximum. On pose $n = \max A$. Comme $n \in A$, on a $(2+\sqrt{3})^n \leq x$. Comme $n+1 \notin A$, on a $x < (2+\sqrt{3})^{n+1}$. D'où le résultat.

Montrons qu'alors $x = (2+\sqrt{3})^n$. Supposons par l'absurde que $x \neq (2+\sqrt{3})^n$. Alors :

$$(2+\sqrt{3})^n < x < (2+\sqrt{3})^{n+1}$$

On pose $y = (2+\sqrt{3})^{-n}x$. Comme G est un sous-groupe de $\mathbb{R}^*$, $2+\sqrt{3} \in G$ et $x \in G$, on en déduit que $y \in G$. De plus, $y > 1$ car $x > (2+\sqrt{3})^n$. Ainsi, $y \in G \cap]1,+\infty[$. Par la question 3.c), on en déduit que

$$2+\sqrt{3} \leq y$$

et donc en multipliant par $(2+\sqrt{3})^n$ on trouve $(2+\sqrt{3})^{n+1} \leq x$. Contradiction. Ainsi $x = (2+\sqrt{3})^n$.

b) En déduire que $G \cap [1,+\infty[= \left\{ (2+\sqrt{3})^n \mid n \in \mathbb{N} \right\}$. Attention, ici c'est l'intervalle $[1,+\infty[$ fermé en 1. N **pts avec** N **grand**

On procède par double inclusion.

- Soit $x \in \left\{ (2+\sqrt{3})^n \mid n \in \mathbb{N} \right\}$. Montrons que $x \in G \cap [1,+\infty[$. Par définition, il existe donc $n \in \mathbb{N}$ tel que $x = (2+\sqrt{3})^n$. Or, $2+\sqrt{3} \in G$ et comme G est un groupe pour $\times$ par la question 2.b), on en déduit que $x = (2+\sqrt{3})^n \in G$. De plus, $2+\sqrt{3} \geq 1$ donc $x \geq 1$. Finalement, $x \in G \cap [1,+\infty[$.
- Soit $x \in G \cap [1,+\infty[$. Par ce qui précède, il existe $n \in \mathbb{Z}$ tel que $x = (2+\sqrt{3})^n$. Il suffit de montrer que $n \in \mathbb{N}$. Or, si $n \leq -1$, on aurait

$$x = (2+\sqrt{3})^n = \frac{1}{(2+\sqrt{3})^{|n|}} < 1$$

car $2+\sqrt{3} > 1$. D'où $x \in \left\{ (2+\sqrt{3})^n \mid n \in \mathbb{N} \right\}$. Finalement, $G \cap]1,+\infty[\subset \left\{ (2+\sqrt{3})^n \mid n \in \mathbb{N} \right\}$.

Par conséquent, on a bien montré que $G \cap]1, +\infty[\subset \left\{(2+\sqrt{3})^n \mid n \in \mathbb{N}\right\}$.

c) On pose $\mathcal{S}$ l'ensemble des solutions de l'équation de Pell-Fermat $x^2 - 3y^2 = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$. Exhiber une bijection de $\mathcal{S}$ sur $G \cap [1, +\infty[$. **N pts avec $N \to +\infty$**

On pose $\varphi : \mathcal{S} \to G \cap [1, +\infty[$, $(a, b) \mapsto a + b\sqrt{3}$

- Montrons que φ est bien posée. Étant donné $(a, b) \in \mathcal{S}$, montrons que $x := a + b\sqrt{3} \in G \cap [1, +\infty[$. Il est clair que $x \in \mathbb{Z}[\sqrt{3}]$.
  - Tout d'abord, montrons que $x \geq 1$. Il est clair que $(0, 0) \notin \mathcal{S}$. Ainsi, comme $a, b \in \mathbb{N}$, on a $a \geq 1$ ou $b \geq 1$. Dans les deux cas, on a donc $x \geq 1$.
  - Cela montre en particulier que $x > 0$. De plus, on a $N(x) = N(a + b\sqrt{3}) = a^2 - 3b^2 = 1$ car $(a, b) \in \mathcal{S}$. Donc $x \in G$.

  Ainsi, $x \in G \cap [1, +\infty[$. On en déduit que φ est bien définie.
- Montrons que φ est injective. Pour tous (a_1, b_1) et (a_2, b_2) dans $\mathcal{S}$, si $\varphi(a_1, b_1) = \varphi(a_2, b_2)$, alors
$$a_1 + b_1\sqrt{3} = a_2 + b_2\sqrt{3}$$
Or, on a vu à la question 1.b) que cela entraine $(a_1, b_1) = (a_2, b_2)$. Ainsi φ est injective.
- Montrons que φ est surjective. Soit $y \in G \cap [1, +\infty[$. Comme $y \in \mathbb{Z}[\sqrt{3}]$, il existe $a, b \in \mathbb{Z}$ tels que $y = a + b\sqrt{3}$. Pour conclure, il suffit de montrer que $(a, b) \in \mathcal{S}$.
  - Tout d'abord, montrons que $(a, b) \in \mathbb{N}^2$. Par la question précédente, on a
$$\begin{aligned} y = (2+\sqrt{3})^n &= \sum_{k=0}^{n} \binom{n}{k} \sqrt{3}^k 2^{n-k} \\ &= \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} \sqrt{3}^k 2^{n-k} + \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} \sqrt{3}^k 2^{n-k} \\ &= \underbrace{\sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} 3^{\left(\frac{k}{2}\right)} 2^{n-k}}_{a} + \sqrt{3} \underbrace{\sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} 3^{\left(\frac{k-1}{2}\right)} 2^{n-k}}_{b} \end{aligned}$$

  Par la question 2.a), on identifie les valeurs de a et de b ci-dessus. On vérifie que a, b sont bien positifs.
  - Comme $y \in G$, on a $N(y) = 1$, donc $a^2 - 3b^2 = 1$.

  Finalement, (a, b) est une solution de l'équation de Pell-Fermat dans $\mathbb{N}^2$. Donc $(a, b) \in \mathcal{S}$. Ainsi, φ est surjective.

Finalement, φ est bijective de $\mathcal{S}$ sur $G \cap [1, +\infty[$.

Exercice 2 : propriétés arithmétiques de la suite de Fibonacci

Soit u la suite définie par
$$u_0 = 0 \qquad u_1 = 1 \qquad \text{et} \qquad \forall n \in \mathbb{N} \quad u_{n+2} = u_{n+1} + u_n$$

1) Calculer u_2, u_3, u_4, u_5. **1 pt**

$u_2 = 0 + 1 = 1$. On trouve de même $u_3 = 2$, $u_4 = 3$, $u_5 = 5$.

2) Montrer par récurrence que pour tout $n \in \mathbb{N}$,
$$u_{n+1}^2 - u_n u_{n+2} = (-1)^n$$
9 pts

- Pour $n = 0$, on a
$$u_1^2 - u_0 u_2 = 1^2 - 0 = 1 = (-1)^0$$
donc la propriété est vraie pour $n = 0$.
- Supposons la propriété vraie pour un $n \in \mathbb{N}$. Montrons-la au rang $n + 1$. On a
$$\begin{aligned} u_{n+2}^2 - u_{n+1}u_{n+3} &= (u_{n+1} + u_n)^2 - u_{n+1}(u_{n+2} + u_{n+1}) \\ &= \cancel{u_{n+1}^2} + 2u_{n+1}u_n + u_n^2 - u_{n+1}u_{n+2} - \cancel{u_{n+1}^2} \\ &= u_{n+1}u_n + u_n(u_{n+1} + u_n) - u_{n+1}u_{n+2} \\ &= u_{n+1}(u_n - u_{n+2}) + u_n u_{n+2} \\ &= u_{n+1}(-u_{n+1}) + u_n u_{n+2} \\ &= -\left(u_{n+1}^2 - u_n u_{n+2}\right) \\ &= -(-1)^n \qquad \text{par hypothèse de récurrence} \\ &= (-1)^{n+1} \end{aligned}$$

  La propriété est donc vérifiée au rang $n + 1$.

- Finalement, la propriété est vraie pour tout $n \in \mathbb{N}$.

3) En déduire que pour tout $n \in \mathbb{N}$, u_n et u_{n+1} sont premiers entre eux. **6 pts**

Par la question précédente, on a

$$\begin{aligned} & u_{n+1}^2 - u_n u_{n+2} = (-1)^n \\ \Longrightarrow\ & u_{n+1}^2 (-1)^n - (-1)^n u_n u_{n+2} = 1 \\ \Longrightarrow\ & u_{n+1}\left((-1)^n u_{n+1}\right) + u_n\left((-1)^{n+1} u_{n+2}\right) = 1 \end{aligned}$$

Comme $(-1)^n u_{n+1}$ et $(-1)^{n+1} u_{n+2}$ sont des entiers, on conclut par le théorème de Bézout que $u_{n+1} \wedge u_n = 1$. D'où le résultat.

Dans la suite on considère un couple quelconque $(n, p) \in \mathbb{N} \times \mathbb{N}^*$. On admet la propriété suivante :

$$u_{n+p} = u_n u_{p-1} + u_{n+1} u_p$$

4) En déduire que $u_{n+p} \wedge u_n = u_n \wedge u_p$. **14 pts**

On va montrer que $\Delta := u_{n+p} \wedge u_n$ et $\delta := u_n \wedge u_p$ se divisent l'un l'autre.

- Il est clair que δ divise u_n et u_p, donc δ divise $u_n u_{p-1} + u_{n+1} u_p$, càd u_{n+p}. Ainsi, δ divise u_n et u_{n+p}, donc divise $u_n \wedge u_{n+p}$, i.e. Δ.
- Réciproquement, Δ divise u_{n+p} et u_n, donc Δ divise $u_{n+p} - u_n u_{p-1}$, càd $u_{n+1} u_p$.
  - On affirme que Δ et u_{n+1} sont premiers entre eux. En effet, en notant d leur PGCD, on a $d \mid \Delta$ et comme $\Delta \mid u_n$, on a $d \mid u_n$. Comme $d \mid u_{n+1}$, on a donc $d \mid u_n \wedge u_{n+1}$, donc $d \mid 1$ par la question 3. Ainsi, $d = \Delta \wedge u_{n+1} = 1$.
  - Comme $\Delta \mid u_{n+1} u_p$ et $\Delta \wedge u_{n+1} = 1$, on en déduit par le lemme de Gauss que $\Delta \mid u_p$.

  Ainsi, Δ divise u_n et u_p, si bien que $\Delta \mid u_n \wedge u_p$.

Finalement, $\Delta \mid \delta$ et $\delta \mid \Delta$. On en déduit que $|\delta| = |\Delta|$, donc $\delta = \Delta$ car ces deux quantités sont positives. D'où le résultat.

5) En déduire que pour tout $q \in \mathbb{N}$, on a $u_{qn+p} \wedge u_n = u_n \wedge u_p$. **(barème variable)**

On procède par récurrence sur $q \in \mathbb{N}$.

- Pour $q = 0$, l'égalité est évidente.
- Supposons la propriété vraie pour un $q \in \mathbb{N}$. Montrons-là au rang $q+1$. En posant $\mathrm{P} = qn + p \in \mathbb{N}^*$, on a par hypothèse de récurrence,

$$\begin{aligned} u_n \wedge u_p &= u_{qn+p} \wedge u_n \\ &= u_{\mathrm{P}} \wedge u_n \\ &= u_{\mathrm{P}+n} \wedge u_n \qquad \text{par la question 4.} \\ &= u_{qn+p+n} \wedge u_n \\ &= u_{(q+1)n+p} \wedge u_n \end{aligned}$$

- Finalement, la propriété est vraie pour tout $q \in \mathbb{N}$.

6) Démontrer finalement que

$$\forall m, n \in \mathbb{N}^* \qquad u_n \wedge u_m = u_{n \wedge m}$$

On pourra s'inspirer de l'algorithme d'Euclide. **barème variable**

Soit $m, n \in \mathbb{N}^*$. Quitte à échanger m et n, on peut supposer $m \geq n$. Par la division euclidienne de m par n, il existe un unique couple d'entiers (q, r) tel que

$$m = qn + r \qquad 0 \leq r < n$$

On note par ailleurs que $q \in \mathbb{N}^*$ car m est positif et $r < m$. Ainsi,

- Si $r > 0$, alors par la question précédente,

$$u_m \wedge u_n = u_{qn+r} \wedge u_n = u_n \wedge u_r$$

- Si $r = 0$, alors $m = qn = Qn + n$ avec $Q := q - 1 \in \mathbb{N}$. On en déduit par la question 5 que (en posant $p = n \in \mathbb{N}^*$)

$$u_m \wedge u_n = u_{Qn+n} \wedge u_n = u_n \wedge u_n = u_n$$

  Or, comme $u_r = u_0 = 0$, on constate que là encore $u_m \wedge u_n = u_n = u_n \wedge u_r$.

Finalement, dans tous les cas on a $u_m \wedge u_n = u_n \wedge u_r$. En appliquant l'algorithme d'Euclide à m et n, on obtient une suite de restes $(r_1, r_2, \cdots, r_k, 0)$ avec $r_1, \cdots, r_k$ non nuls : on a alors $r_k = m \wedge n$. On a donc par ce qui précède :

$$u_m \wedge u_n = u_n \wedge u_{r_1} = u_{r_1} \wedge u_{r_2} = \cdots = u_{r_k} \wedge u_0 = u_{r_k} = u_{m \wedge n}$$