DS5

Devoir surveillé du 15/03/2025

Exercice 1

1. On écrit cette fonction sous forme exponentielle :

$$\cos(x)^{\tan(x)} = \exp\left(\tan(x)\ln(\cos(x))\right).$$

On rappelle les DL usuels suivants :

$$\tan(x) \underset{x\to 0}{=} x + \frac{1}{3}x^3 + o(x^3),\ \cos(x) \underset{x\to 0}{=} 1 - \frac{x^2}{2} + o(x^3),\ \ln(1+u) \underset{u\to 0}{=} u - \frac{u^2}{2} + \frac{u^3}{3} + o(u^3).$$

En posant $u(x) = -\frac{x^2}{2} + o(x^3)$ et en composant les développements limités :

$$\ln\left(1 - \frac{x^2}{2} + o(x^3)\right) = -\frac{x^2}{2} + o(x^3).$$

Par produit :

$$\tan(x)\ln(\cos(x)) \underset{x\to 0}{=} -\frac{x^3}{2} + o(x^3).$$

En composant les développements limités, et avec $\exp(u) \underset{u\to 0}{=} 1 + u + \frac{u^2}{2} + \frac{u^3}{6} + o(u^3)$, on trouve finalement :

$$\boxed{\cos(x)^{\tan(x)} \underset{x\to 0}{=} 1 - \frac{x^3}{2} + o(x^3).}$$

Remarque. On aurait pu optimiser les calculs en se contentant d'un DL à l'ordre 1 des fonctions tangente, logarithme et exponentielle.

2. Écrivons les développements à l'ordre 3 des fonctions sin et exp (car x se simplifiera dans la fraction) :

$$\sin(x) \underset{x\to 0}{=} x - \frac{x^3}{6} + o(x^3),$$

$$\exp(x) - 1 \underset{x\to 0}{=} x + \frac{x^2}{2} + \frac{x^3}{6} + o(x^3).$$

D'où par quotient :

$$\frac{\sin(x)}{\exp(x)-1} \underset{x\to 0}{=} \frac{x - \frac{x^3}{6} + o(x^3)}{x + \frac{x^2}{2} + \frac{x^3}{6} + o(x^3)} = \frac{1 - \frac{x^2}{6} + o(x^2)}{1 + \frac{x}{2} + \frac{x^2}{6} + o(x^2)}$$

Enfin :

$$\begin{aligned}\frac{1 - \frac{x^2}{6} + o(x^2)}{1 + \frac{x}{2} + \frac{x^2}{6} + o(x^2)} &\underset{x\to 0}{=} \left(1 - \frac{x^2}{6} + o(x^2)\right)\left(1 - \frac{x}{2} - \frac{x^2}{6} + \frac{x^2}{4} + o(x^2)\right) \\ &= 1 - \frac{x}{2} - \frac{x^2}{6} + \frac{x^2}{4} - \frac{x^2}{6} + o(x^2) \boxed{= 1 - \frac{x}{2} - \frac{x^2}{12} + o(x^2).}\end{aligned}$$

3. On se ramène en 0 en posant $h = x - 1$:
$$g(x) = g(1+h) = \frac{\cos(2\pi(h+1)) - 1}{\ln(1+h) - h} = \frac{\cos(2\pi h) - 1}{\ln(1+h) - h}.$$
Or $\cos(2\pi h) - 1 \underset{h\to 0}{\sim} -\frac{(2\pi h)^2}{2}$ et $\ln(1+h) \underset{h\to 0}{=} h - \frac{h^2}{2} + o(h^2)$, donc $\ln(1+h) - h \underset{h\to 0}{\sim} -\frac{h^2}{2}$. Par quotient d'équivalents :
$$g(1+h) \underset{h\to 0}{=} \sim \frac{-\frac{(2\pi h)^2}{2}}{-\frac{h^2}{2}} = 4\pi^2.$$
Ainsi $\boxed{\lim_{x\to 1} g(x) = 4\pi^2.}$

Exercice 2

1. Montrons par récurrence que la suite est bien définie[1] et que pour tout $n \in \mathbb{N}$, $u_n \geq 0$.

   I u_0 est bien définie et $u_0 \geq 0$, donc la propriété est vraie au rang $n = 0$.

   H Soit $n \in \mathbb{N}^*$. Supposons la propriété vraie au rang $n-1$, et montrons la propriété au rang n.

   Puisque $u_{n-1} \geq 0$ par hypothèse de récurrence, $n + u_{n-1} \geq 0$, et $u_n = \sqrt{n + u_{n-1}}$ est bien défini et positif. D'où la propriété au rang n.

   Par principe de récurrence, u_n est bien défini et positif pour tout $n \in \mathbb{N}$.

   Vérifions à présent l'inégalité demandée. Tout d'abord, $u_0 \geq 0 = \sqrt{0}$, et pour tout $n \in \mathbb{N}^*$:
$$n \leq n + u_{n-1}, \text{ d'où } \sqrt{n} \leq \sqrt{n + u_{n-1}} = u_n$$
   par croissance de la fonction racine carrée. Ainsi, $\boxed{u_n \geq \sqrt{n} \text{ pour tout } n \in \mathbb{N}.}$

   Puisque $\sqrt{n} \underset{n\to+\infty}{\longrightarrow} +\infty$, on en déduit par théorème de comparaison que $\boxed{\lim_{n\to+\infty} u_n \text{ existe et vaut } +\infty.}$

2. (a) Pour tout $x \geq 0$:
$$\frac{1+x}{2} - \sqrt{x} = \frac{1 + x - 2\sqrt{x}}{2} = \frac{(1-\sqrt{x})^2}{2} \boxed{\geq 0.}$$
   D'où l'inégalité souhaitée.

   (b) Montrons par récurrence que pour tout $n \in \mathbb{N}$, $u_n \leq n + \frac{u_0}{2^n}$.

   I Comme $u_0 \leq 0 + \frac{u_0}{2^0}$, la propriété est vraie pour $n = 0$.

   H Soit $n \in \mathbb{N}^*$. Supposons la propriété vraie au rang $n-1$. Montrons qu'elle est vraie au rang n.

   On applique l'inégalité de la question précédente à $x = n + u_{n-1}$:
$$u_n = \sqrt{n + u_{n-1}} \leq \frac{1 + n + u_{n-1}}{2} = \frac{1+n}{2} + \frac{u_{n-1}}{2}.$$
   Or par hypothèse de récurrence :
$$u_{n-1} \leq n - 1 + \frac{u_0}{2^{n-1}}.$$
   En remplaçant dans l'expression précédente, on obtient :
$$u_n \leq \frac{1+n}{2} + \frac{n-1}{2} + \frac{u_0}{2^n} = n + \frac{u_0}{2^n}.$$
   D'où la propriété au rang n.

[1] Il se pourrait en effet qu'à un certain rang $n \in \mathbb{N}^*$, on ait $u_{n-1} < n$ et que $u_n = \sqrt{u_{n-1} + n}$ ne soit pas défini.

Par principe de récurrence, $\boxed{u_n \leq n + \frac{u_0}{2^n} \text{ pour tout } n \in \mathbb{N}.}$

Pour tout $n \in \mathbb{N}^*$:

$$0 \leq u_{n-1} \leq n - 1 + \frac{u_0}{2^{n-1}}, \quad \text{d'où} \quad 0 \leq \frac{u_{n-1}}{n^2} \leq \frac{n-1}{n^2} + \frac{u_0}{n^2 2^{n-1}}$$

Puisque $\frac{n-1}{n^2} + \frac{u_0}{n^2 2^{n-1}} = \frac{1}{n} - \frac{1}{n^2} + \frac{u_0}{n^2 2^{n-1}} \underset{n\to+\infty}{\to} 0$, par le théorème des gendarmes, $\lim\limits_{n\to+\infty} \frac{u_{n-1}}{n^2}$ existe et vaut 0. Ainsi, $\boxed{u_{n-1} \underset{n\to+\infty}{=} o(n^2).}$

(c) Pour tout $n \in \mathbb{N}^*$:

$$\frac{u_n}{n} = \frac{\sqrt{n + u_{n-1}}}{n} = \sqrt{\frac{n + u_{n-1}}{n^2}} = \sqrt{\frac{1}{n} + \frac{u_{n-1}}{n^2}}.$$

Puisque $\lim\limits_{n\to+\infty} \frac{1}{n} + \frac{u_{n-1}}{n^2} = 0$ par la question précédente, $\left(\frac{u_n}{n}\right)_{n\geq 1}$ converge vers 0, et $\boxed{u_n \underset{n\to+\infty}{=} o(n).}$

(d) Soit $n \in \mathbb{N}^*$. Alors :

$$\frac{u_n}{\sqrt{n}} = \sqrt{1 + \frac{u_{n-1}}{n}}.$$

Écrivons :

$$\frac{u_{n-1}}{n} = \frac{u_{n-1}}{n-1}\frac{n-1}{n} \underset{n\to+\infty}{\sim} \frac{u_{n-1}}{n-1} \underset{n\to+\infty}{\longrightarrow} 0$$

par la question précédente. Ainsi, $\frac{u_n}{\sqrt{n}} = \sqrt{1 + \frac{u_{n-1}}{n}} \underset{n\to+\infty}{\to} 1$, qui se récrit $\boxed{u_n \underset{n\to+\infty}{\sim} \sqrt{n}.}$

3. (a) Pour tout $n \in \mathbb{N}$:

$$v_n = u_n - \sqrt{n} = \sqrt{n + u_{n-1}} - \sqrt{n} = \sqrt{n}\left(\sqrt{1 + \frac{u_{n-1}}{n}} - 1\right)$$

Or, on a montré que $\lim\limits_{n\to+\infty} \frac{u_{n-1}}{n} = 0$. Avec l'équivalent usuel suivant :

$$\sqrt{1+x} - 1 \underset{x\to 0}{\sim} \frac{1}{2}x$$

il vient :

$$\sqrt{1 + \frac{u_{n-1}}{n}} - 1 \underset{n\to+\infty}{\sim} \frac{1}{2}\frac{u_{n-1}}{n}.$$

Puisque $u_n \underset{n\to+\infty}{\sim} \sqrt{n}$, on obtient :

$$v_n \underset{n\to+\infty}{\sim} \sqrt{n}\frac{u_{n-1}}{2n} \underset{n\to+\infty}{\sim} \sqrt{n}\frac{\sqrt{n-1}}{2n} \underset{n\to+\infty}{\sim} \sqrt{n}\frac{\sqrt{n}}{2n} = \frac{1}{2}.$$

Ainsi, $\boxed{\text{la suite } (v_n)_{n\in\mathbb{N}} \text{ converge vers } \frac{1}{2}.}$

(b) Puisque $\lim\limits_{n\to+\infty} v_n = \frac{1}{2}$, alors $v_n \underset{n\to+\infty}{=} \frac{1}{2} + o(1)$, qui se récrit :

$$\boxed{u_n \underset{n\to+\infty}{=} \sqrt{n} + \frac{1}{2} + o(1).}$$

4. (a) On multiplie par la quantité conjuguée :

$$\sqrt{n}-\sqrt{n-1}=\frac{(\sqrt{n}-\sqrt{n-1})(\sqrt{n}+\sqrt{n-1})}{\sqrt{n}+\sqrt{n-1}}=\frac{n-(n-1)}{\sqrt{n}+\sqrt{n-1}}=\frac{1}{\sqrt{n}+\sqrt{n-1}}.$$

Ainsi, $\boxed{\lim_{n\to+\infty}(\sqrt{n}-\sqrt{n-1})=0.}$

D'autre part, $u_n \underset{n\to+\infty}{=} \sqrt{n}+\frac{1}{2}+o(1)$, d'où en remplaçant :

$$\begin{aligned} u_n-u_{n-1}&=(\sqrt{n}+\frac{1}{2}+o(1))-(\sqrt{n-1}+\frac{1}{2}+o(1))\\ &=(\sqrt{n}-\sqrt{n-1})+o(1)\underset{n\to+\infty}{\longrightarrow}0. \end{aligned}$$

Ainsi, $\boxed{\lim_{n\to+\infty}(u_n-u_{n-1})=0.}$

(b) Calculons :

$$\begin{aligned} u_{n+1}-u_n&=\sqrt{n+u_n}-\sqrt{n-1+u_{n-1}}\\ &=\frac{(\sqrt{n+u_n}-\sqrt{n-1+u_{n-1}})(\sqrt{n+u_n}+\sqrt{n-1+u_{n-1}})}{\sqrt{n+u_n}+\sqrt{n-1+u_{n-1}}}\\ &=\frac{(n+u_n)-(n-1+u_{n-1})}{\sqrt{n+u_n}+\sqrt{n-1+u_{n-1}}}=\frac{1+u_n-u_{n-1}}{\sqrt{n+u_n}+\sqrt{n-1+u_{n-1}}}. \end{aligned}$$

La quantité au dénominateur étant toujours positive, $u_{n+1}-u_n$ est du signe de $1+u_n-u_{n-1}$. Puisque $\lim_{n\to+\infty} 1+u_n-u_{n-1}=1$, il existe un rang $N\in\mathbb{N}$ tel que pour tout $n\geq N$, $1+u_n-u_{n-1}\geq 0$.

Ainsi, pour tout $n\geq N$, $u_{n+1}-u_n\geq 0$, et $\boxed{(u_n) \text{ est croissante à partir d'un certain rang.}}$

5. (a) Par la question précédente :

$$\begin{aligned} u_{n-1}&=\sqrt{n-1}+\frac{1}{2}+o(1)=\sqrt{n}\sqrt{1-\frac{1}{n}}+\frac{1}{2}+o(1)=\sqrt{n}\left(1-\frac{1}{2n}+o\left(\frac{1}{n}\right)\right)+\frac{1}{2}+o(1)\\ &=\sqrt{n}+\frac{1}{2}\underbrace{-\frac{1}{2\sqrt{n}}+o\left(\frac{1}{\sqrt{n}}\right)+o(1)}_{=o(1)}\boxed{=\sqrt{n}+\frac{1}{2}+o(1).} \end{aligned}$$

(b) Calculons :

$$\begin{aligned} w_n&=u_n-\sqrt{n}-\frac{1}{2}=\sqrt{n+u_{n-1}}-\sqrt{n}-\frac{1}{2}=\sqrt{n}\left[\sqrt{1+\frac{u_{n-1}}{n}}-1-\frac{1}{2\sqrt{n}}\right]\\ &=\sqrt{n}\left[\sqrt{1+\frac{1}{\sqrt{n}}+\frac{1}{2n}+o\left(\frac{1}{n}\right)}-1-\frac{1}{2\sqrt{n}}\right]\\ &=\sqrt{n}\left[1+\frac{1}{2}\left(\frac{1}{\sqrt{n}}+\frac{1}{2n}\right)+\frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2!}\left(\frac{1}{\sqrt{n}}+\frac{1}{2n}\right)^2+o\left(\frac{1}{n}\right)-1-\frac{1}{2\sqrt{n}}\right]\\ &=\sqrt{n}\left[\frac{1}{4n}-\frac{1}{8n}+o\left(\frac{1}{n}\right)\right]=\frac{1}{8\sqrt{n}}+o\left(\frac{1}{\sqrt{n}}\right). \end{aligned}$$

Ainsi, $\boxed{w_n \underset{n\to+\infty}{\sim}\frac{1}{8\sqrt{n}}}$, qui se récrit $\boxed{u_n\underset{n\to+\infty}{=}\sqrt{n}+\frac{1}{2}+\frac{1}{8\sqrt{n}}+o\left(\frac{1}{\sqrt{n}}\right).}$

Exercice 3

Partie I. L'anneau $\mathbb{Z}[\sqrt{7}]$.

1. L'existence d'un tel couple relève directement de la définition de $\mathbb{Z}[\sqrt{7}]$, il s'agit donc surtout de prouver l'unicité. Soient a_1, a_2, b_1, b_2 des entiers tels que $a_1 + b_1\sqrt{7} = a_2 + b_2\sqrt{7}$. Alors $(b_1 - b_2)\sqrt{7} = a_2 - a_1$.

   Si $b_1 \neq b_2$, alors $\sqrt{7} = \frac{a_2 - a_1}{b_1 - b_2} \in \mathbb{Q}$, ce qui est absurde. Donc $b_1 = b_2$, et donc $a_1 = a_2$.

   Ainsi, $\boxed{\text{tout élément de } \mathbb{Z}[\sqrt{7}] \text{ s'écrit bien de manière unique sous la forme } a + b\sqrt{7}, (a,b) \in \mathbb{Z}^2.}$

2. Montrons que $\mathbb{Z}[\sqrt{7}]$ est un sous-anneau de $\mathbb{R}$.

   - Le neutre multiplicatif de $\mathbb{R}$ est $1 = 1 + 0\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$.
   - Soient $x, y \in \mathbb{Z}[\sqrt{7}]$, et soient $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x = a_1 + b_1\sqrt{7}$ et $y = a_2 + b_2\sqrt{7}$. Alors :
   $$x - y = \underbrace{(a_1 - a_2)}_{\in\mathbb{Z}} + \underbrace{(b_1 - b_2)}_{\in\mathbb{Z}}\sqrt{7} \in \mathbb{Z}[\sqrt{7}].$$
   Enfin :
   $$xy = \left(a_1 + b_1\sqrt{7}\right)\left(a_2 + b_2\sqrt{7}\right) = \underbrace{a_1a_2 + 7b_1b_2}_{\in\mathbb{Z}} + \underbrace{(a_1b_2 + a_2b_1)}_{\in\mathbb{Z}}\sqrt{7} \in \mathbb{Z}[\sqrt{7}].$$

   Et donc $\boxed{\mathbb{Z}[\sqrt{7}] \text{ est bien un sous-anneau de } \mathbb{R}.}$

   Si $\mathbb{Z}[\sqrt{7}]$ était un corps, alors 2 serait inversible dans $\mathbb{Z}[\sqrt{7}]$, et donc il existerait $a, b \in \mathbb{Z}$ tels que :
   $$\frac{1}{2} = a + b\sqrt{7}, \text{ soit encore } (2a-1) + 2b\sqrt{7} = 0.$$
   Par la question 1, ceci implique que $b = 0$ et $2a - 1 = 0$, ce qui n'est pas possible dans $\mathbb{Z}$. Donc 2 n'est pas inversible dans $\mathbb{Z}[\sqrt{7}]$, et $\boxed{\mathbb{Z}[\sqrt{7}] \text{ n'est pas un corps.}}$

3. Vérifions que l'application $\varphi : x \mapsto \overline{x}$ est un automorphisme d'anneau de $\mathbb{Z}[\sqrt{7}]$.

   - $\varphi(1) = \varphi(1 + 0\sqrt{7}) = 1 - 0\sqrt{7} = 1$.
   - Soient $x, y \in \mathbb{Z}[\sqrt{7}]$, et soient $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ tels que $x = a_1 + b_1\sqrt{7}$ et $y = a_2 + b_2\sqrt{7}$. En utilisant les calculs déjà effectués :
   $$\begin{aligned}\varphi(x+y) &= \varphi((a_1+a_2) + (b_1+b_2)\sqrt{7}) = (a_1+a_2) - (b_1+b_2)\sqrt{7} \\ &= (a_1 - b_1\sqrt{7}) + (a_2 - b_2\sqrt{7}) = \varphi(x) + \varphi(y)\end{aligned}$$
   et :
   $$\begin{aligned}\varphi(x \times y) &= \varphi((a_1a_2 + 7b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{7}) = (a_1a_2 + 7b_1b_2) - (a_1b_2 + a_2b_1)\sqrt{7} \\ &= (a_1a_2 + 7(-b_1)(-b_2)) + (a_1(-b_2) + a_2(-b_1))\sqrt{7} \\ &= (a_1 - b_1\sqrt{7}) \times (a_2 - b_2\sqrt{7}) = \varphi(x) \times \varphi(y).\end{aligned}$$
   Enfin :
   $$\varphi \circ \varphi(x) = \varphi(a_1 - b_1\sqrt{7}) = a_1 + b_1\sqrt{7} = x$$
   donc $\varphi \circ \varphi = \mathrm{id}_{\mathbb{Z}[\sqrt{7}]}$, et φ est bijective.

   Ainsi, $\boxed{x \mapsto \overline{x} \text{ est un automorphisme d'anneau de } \mathbb{Z}[\sqrt{7}].}$

4. (a) Soit $x, x' \in \mathbb{Z}[\sqrt{7}]$. En utilisant le résultat de la question précédente :
   $$N(xx') = (xx') \times \overline{xx'} = (xx') \times \overline{x}\,\overline{x'} = (x\overline{x})(x'\overline{x'}) \boxed{= N(x)N(x').}$$

(b) Soit $x \in \mathbb{Z}[\sqrt{7}]$, inversible. Notons $x' \in \mathbb{Z}[\sqrt{7}]$ son inverse. Alors :

$$1 = N(1) = N(xx') = N(x)N(x').$$

Mais $N(x)$ et $N(x')$ sont deux entiers. Ainsi, $N(x) = \pm 1$.

Inversement, si $x = a + b\sqrt{7}$ est tel que $|N(x)| = 1$. Alors $x \neq 0$ (car $N(0) = 0$), et donc x est inversible dans l'anneau $\mathbb{R}$. Son inverse est

$$\frac{1}{x} = \frac{1}{a+b\sqrt{7}} = \frac{a-b\sqrt{7}}{(a+b\sqrt{7})(a-b\sqrt{7})} = \frac{a-b\sqrt{7}}{a^2-7b^2} = \frac{a}{N(x)} - \frac{b}{N(x)}\sqrt{7}.$$

Et cet inverse appartient bien à $\mathbb{Z}[\sqrt{7}]$ puisque $|N(x)| = 1$. Ainsi, x est bien inversible dans l'anneau $\mathbb{Z}[\sqrt{7}]$.

On a donc montré que $\boxed{x \in \mathbb{Z}[\sqrt{7}] \text{ est inversible si, et seulement si, } N(x) = \pm 1.}$ Et si c'est le cas, $\boxed{\text{son inverse est } \overline{x} \text{ si } N(x) = 1,\ -\overline{x} \text{ si } N(x) = -1.}$

Partie II. Structure du groupe des inversibles de $\mathbb{Z}[\sqrt{7}]$ et équations de Pell-Fermat.

5. Puisque $N(8+3\sqrt{7}) = 8^2 - 7\times 3^2 = 1$, $\boxed{8+3\sqrt{7} \in G}$. Et donc $\boxed{G \text{ contient d'autres éléments que } \pm 1.}$

6. On souhaite montrer que $G \cap \,]1, +\infty[$ possède un plus petit élément u.

(a) Supposons que $x \geq 1$ et $N(x) = 1$. Alors :

$$0 < \frac{1}{x} \leq 1 \leq x.$$

Or, par la question 4.(b), $\dfrac{1}{x} = \overline{x} = a - b\sqrt{7}$. Ainsi, $a - b\sqrt{7} \leq a + b\sqrt{7}$, et donc $\boxed{b \geq 0}$. Et alors $a - b\sqrt{7} > 0$, donc $a > b\sqrt{7} \geq 0$. Puisque $a \in \mathbb{Z}$, $\boxed{a \geq 1.}$

(b) On a toujours l'inégalité :

$$0 < \frac{1}{x} \leq 1 \leq x.$$

avec cette fois $\dfrac{1}{x} = -\overline{x} = -a + b\sqrt{7}$. Ainsi, $-a + b\sqrt{7} \leq a + b\sqrt{7}$ et donc $\boxed{a \geq 0}$. Et donc $b\sqrt{7} > a$, si bien que $\boxed{b \geq 0.}$

(c) Soit $x = a + b\sqrt{7} \in G \cap [1, M]$. Par la question précédente, $a \geq 1$ et $b \geq 0$. On en déduit que :

$$1 \leq a \leq a + b\sqrt{7} \leq M \quad \text{et} \quad 0 \leq b \leq b\sqrt{7} \leq a + b\sqrt{7} \leq M.$$

Autrement dit, $(a, b) \in [\![1, M]\!] \times [\![0, M]\!]$. Donc il y a au plus $M(M+1)$ couples (a, b) tels que $a + b\sqrt{7} \in G \cap [1, M]$. Donc $\boxed{G \cap [1, M] \text{ est fini.}}$

(d) Nous avons déjà dit que G contient $8 + 3\sqrt{7}$. Prenons donc M un entier supérieur ou égal à $8 + 3\sqrt{7}$. Alors $G \cap \,]1, M]$ est non vide et fini, il possède donc un plus petit élément u.

Pour tout $x \in G \cap \,]1, +\infty[$, on a deux cas :

- soit $x \leq M$, et alors $u \leq x$;
- soit $x > M$, et alors $u \leq M \leq x$.

Donc $\boxed{u \text{ est le plus petit élément de } G \cap \,]1, +\infty[.}$

7. (a) Puisque $u > 1$, $u^n \underset{n\to+\infty}{\longrightarrow} +\infty$. Et en particulier, il existe $n_0 \in \mathbb{N}$ tel que pour tout $k \geq n_0$, $u^k > v$.

Soit $A_v = \left\{k \in \mathbb{N} \mid u^k \leq v\right\}$. C'est une partie non vide de $\mathbb{N}$ (car contient 0), majorée par n_0. Elle admet donc un plus grand élément k. Et puisque $k \in A_v$ et $k+1 \notin A_v$, $\boxed{u^k \leq v < u^{k+1}.}$

(b) On a donc $1 \leq \frac{v}{u^k} < u$. Et puisque v et u^k sont deux éléments de G, qui est un groupe, $\frac{v}{u^k} = v\left(u^k\right)^{-1}$ appartient à G.

Puisque u est le plus petit élément de $G \cap]1, +\infty[$, et que $\frac{v}{u^k} < u$, il suit que $\frac{v}{u^k} = 1$, si bien que $\boxed{v = u^k.}$

(c) Puisque $u \in \mathbb{R}_+^*$ (car $u > 1$), $u^k > 0$ pour tout $k \in \mathbb{Z}$, et donc $\langle u \rangle \subset G \cap \mathbb{R}_+^*$.

Inversement, soit $v \in G \cap \mathbb{R}_+^*$.

- Si $v > 1$, alors par la question précédente, $v \in \left\{u^k, k \in \mathbb{N}\right\} \subset \langle u \rangle$.
- Si $v = 1$, alors $v = u^0 \in \langle u \rangle$.
- Si $v < 1$, alors $\frac{1}{v} > 1$, et donc par la question précédente, il existe $k \in \mathbb{N}$ tel que $\frac{1}{v} = u^k$, et donc $v = u^{-k} \in \langle u \rangle$.

Donc $\boxed{G \cap \mathbb{R}_+^* = \langle u \rangle.}$

8. Soient $(\varepsilon_1, k_1), (\varepsilon_2, k_2)$ deux éléments de $\{-1, 1\} \times \mathbb{Z}$. Alors :

$$f\left((\varepsilon_1, k_1) \cdot (\varepsilon_2, k_2)\right) = f\left(\varepsilon_1\varepsilon_2, k_1 + k_2\right) = \varepsilon_1\varepsilon_2 u^{k_1+k_2} = \varepsilon_1 u^{k_1} \varepsilon_2 u^{k_2} = f\left(\varepsilon_1, k_1\right) f\left(\varepsilon_2, k_2\right)$$

Donc $\boxed{f \text{ est bien un morphisme de groupes.}}$

Soit $(\varepsilon, k) \in \operatorname{Ker}(f)$. Alors :

$$f(\varepsilon, k) = \varepsilon u^k = 1.$$

Puisque $u^k > 0$, on a $\varepsilon = 1$. Et alors $u^k = 1$, d'où $k = 0$. Donc $\operatorname{Ker} f = \{(1, 0)\}$, où $(1, 0)$ est le neutre si bien que f est injectif.

Enfin, si $x \in G$, alors :

- soit $x > 0$, et donc par la question 9.c, il existe $k \in \mathbb{Z}$ tel que $x = u^k = f(1, k)$.
- soit $x < 0$, mais alors $-x > 0$, et donc il existe $k \in \mathbb{Z}$ tel que $x = -u^k = f(-1, k)$.

Dans tous les cas, x possède un antécédent par f, qui est donc surjectif.

Ainsi, f est bijectif : c'est un $\boxed{\text{isomorphisme de groupes.}}$

9. (a) Notons que $(x, y) \in \mathbb{Z}^2$ est une solution de $x^2 - 7y^2 = 1$ si et seulement si $\alpha = x + y\sqrt{7}$ est tel que $N(\alpha) = 1$.

Nous savons déjà que $N(8 + 3\sqrt{7}) = 1$, et donc $\boxed{(8, 3) \text{ est solution de l'équation.}}$

Pour tout $k \in \mathbb{N}^*$, $N\left((8 + 3\sqrt{7})^k\right) = N(8 + 3\sqrt{7})^k = 1$, si bien que si on note (a_k, b_k) les entiers tels que $(8 + 3\sqrt{7})^k = a_k + b_k\sqrt{7}$, alors $a_k^2 - 7b_k^2 = 1$. Et donc (a_k, b_k) est solution. Reste à remarquer que puisque $8+3\sqrt{7} > 1$, la suite $\left((8 + 3\sqrt{7})^k\right)_k$ est strictement croissante, et donc injective.

Ainsi, $\boxed{\text{il y a une infinité de solutions à l'équation } x^2 - 7y^2 = 1.}$

Nous avons déjà dit que $(8, 3)$ est l'une d'entre elles. Et puisque $(8 + 3\sqrt{7})^2 = 64 + 7 \times 9 + 48\sqrt{7} = 127 + 48\sqrt{3}$, alors $\boxed{(127, 48) \text{ est une deuxième solution.}}$

(b) Là encore, les couples (x, y) solutions de $x^2 - 7y^2 = -1$ correspondent aux élément $x + y\sqrt{7} \in \mathbb{Z}[\sqrt{7}]$ tels que $N(x + y\sqrt{7}) = -1$.

Notons que de tels éléments sont nécessairement dans G, et il s'agit donc de déterminer le nombre d'éléments de G dont la norme vaut -1.

Soit $g \in G$. On a deux cas :

- si $g \in G \cap \mathbb{R}_+^* = \langle u \rangle$, il existe $k \in \mathbb{Z}$ tel que $g = u^k$. Mais alors :

$$N(g) = N(u^k) = N(u)^k = N(8 + 3\sqrt{7})^k = 1$$

et donc $N(g) \neq -1$.
- si $g \in G \cap \mathbb{R}_-^*$. Alors $-g > 0$ et appartient toujours à G car $N(-g) = N(-1)N(g) = N(g)$. Donc $-g$ appartient à $G \cap \mathbb{R}_+^*$, de sorte que $N(-g) = 1$ par le cas précédemment traité. Ainsi, dans ce cas également, $N(g) = 1$.

AInsi, il n'existe aucun élément de $\mathbb{Z}[\sqrt{7}]$ de norme -1, et donc l'équation $\boxed{x^2 - 7y^2 = -1 \text{ n'a pas de solution.}}$

Exercice 4 (Polynômes de Tchebychev et théorème de Block-Thielmann)

Partie I. Résultats préliminaires

1. Pour tous $n, m \in \mathbb{N}^*$, $\deg(X^n) = n$ et :

$$X^n \circ X^m = (X^m)^n = X^{mn} = (X^n)^m = X^m \circ X^n.$$

Donc $\boxed{\text{la suite } (X^n)_{n \in \mathbb{N}^*} \text{ est commutante.}}$

2. (a) On vérifie les trois points suivants :

- La composition des polynômes est une loi de composition interne sur $\mathscr{G}$ car $\deg(P \circ Q) = \deg(P) \times \deg(Q) = 1$.
- La loi $\circ$ est associative, d'élément neutre $X \in \mathscr{G}$.
- Soit $U = aX + b \in \mathscr{G}$. Pour tout $V = cX + d \in \mathscr{G}$:

$$U \circ V = a(cX + d) + b = acX + (ad + b) \quad \text{et} \quad V \circ U = c(aX + b) + d = acX + (bc + d).$$

Pour $c = \frac{1}{a}$ et $d = -\frac{b}{a}$, $U \circ V = X = V \circ U$. Ainsi, $U = aX + b \in \mathscr{G}$ admet pour symétrique dans $\mathscr{G}$ le polynôme $\boxed{U^{-1} = \dfrac{1}{a}X - \dfrac{b}{a}.}$

Ainsi, $\boxed{(\mathscr{G}, \circ) \text{ est un groupe.}}$

(b) Pour tous $m, n \in \mathbb{N}^*$, $\deg(U \circ P_n \circ U^{-1}) = \deg(U)\deg(P_n)\deg(U^{-1}) = 1 \times \deg(P_n) \times 1 = n$, et :

$$\begin{aligned}(U \circ P_n \circ U^{-1}) \circ (U \circ P_m \circ U^{-1}) &= U \circ P_n \circ P_m \circ U^{-1} = U \circ P_m \circ P_n \circ U^{-1} \\ &= (U \circ P_m \circ U^{-1}) \circ (U \circ P_n \circ U^{-1}).\end{aligned}$$

Donc $\boxed{(U \circ P_n \circ U^{-1})_{n \in \mathbb{N}^*} \text{ est une suite commutante.}}$

Partie II. Polynômes de Tchebychev (de première espèce)

3. Calculons $T_2 = T_{0+2} = 2XT_1 - T_0 \boxed{= 2X^2 - 1}$ puis :

$$T_3 = 2XT_2 - T_1 \boxed{= 4X^3 - 3X} \quad \text{et enfin} \quad \boxed{T_4 = 8X^4 - 8X^2 + 1.}$$

4. Puisque sur les premières valeurs on constate que T_n est de coefficient dominant 2^{n-1}, prouvons par récurrence double sur $n \in \mathbb{N}^*$ la proposition $\mathscr{P}(n)$: « T_n est de degré n et de coefficient dominant 2^{n-1} ».

I Il est clair que T_1 et T_2 sont vraies.

H Soit $n \in \mathbb{N}^*$ tel que $\mathscr{P}(n)$ et $\mathscr{P}(n+1)$ soient vraies.

Soit $Q_n \in \mathbb{R}_{n-1}[X]$ et $Q_{n+1} \in \mathbb{R}_n[X]$ tels que $T_n = 2^{n-1}X^n + Q_n$ et $T_{n+1} = 2^n X^{n+1} + Q_n$. Alors :

$$T_{n+2} = 2XT_{n+1} - T_n = 2^{n+1}X^{n+2} + \underbrace{2XQ_{n+1} - T_n}_{\in \mathbb{R}_{n+1}[X]}$$

si bien que T_{n+2} est de degré $n+2$ et de coefficient dominant 2^{n+1}.

Par le principe de récurrence double, $\boxed{\text{pour tout } n \in \mathbb{N}^*,\ T_n \text{ est de degré } n \text{ et de coefficient dominant } 2^n.}$

5. Soit $\theta \in \mathbb{R}$. Prouvons par récurrence double sur $n \in \mathbb{N}$ que $T_n(\cos(\theta)) = \cos(n\theta)$.

I Pour $n = 0$, $T_0(\cos(\theta)) = 1 = \cos(0\theta)$. Pour $n = 1$, $T_1(\cos(\theta)) = \cos(\theta) = \cos(1\theta)$.

H Soit $n \in \mathbb{N}$ tel que $T_n(\cos(\theta)) = \cos(n\theta)$ et $T_{n+1}(\cos\theta) = \cos((n+1)\theta)$. Alors :

$$\begin{aligned} T_{n+2}(\cos\theta) &= 2\cos(\theta)T_{n+1}(\cos\theta) - T_{n-1}(\cos\theta) = 2\cos(\theta)\cos((n+1)\theta) - \cos(n\theta) \\ &\overset{(*)}{=} \cos((n+2)\theta) + \cos((n+1)\theta - \theta) - \cos(n\theta) = \cos((n+2)\theta), \end{aligned}$$

l'égalité $(*)$ provenant de la formule $\cos(a) + \cos(b) = \dfrac{1}{2}(\cos(a+b) + \cos(a-b))$.

Par le principe de récurrence double, $\boxed{\text{pour tout } n \in \mathbb{N},\ T_n(\cos(\theta)) = \cos(n\theta).}$

6. Soient $m, n \in \mathbb{N}$, et soit $x \in [-1, 1]$. Notons alors $\theta = \operatorname{Arccos}(x)$, de sorte que $x = \cos(\theta)$. Calculons :

- $T_{mn}(x) = T_{mn}(\cos(\theta)) = \cos(mn\theta)$;
- $(T_m \circ T_n)(\cos(\theta)) = T_m(T_n(\cos\theta)) = T_m(\cos(n\theta)) = \cos(mn\theta)$.

Donc pour tout $x \in [-1, 1]$, $T_{mn}(x) = (T_m \circ T_n)(x)$. Le polynôme $T_{mn} - T_m \circ T_n$ s'annule une infinité de fois (sur tous les points de $[-1, 1]$). C'est donc le polynôme nul, si bien que $T_{mn} = T_m \circ T_n$.

Comme de plus, $\deg(T_n) = n$ pour tout $n \in \mathbb{N}^*$, $\boxed{(T_n)_{n \in \mathbb{N}^*} \text{ est une suite commutante.}}$

Partie III. Étude du commutant de $X^2 + p$

7. Soit $P \in \mathscr{C}_p$, et notons n son degré, $a_0, \ldots, a_n$ ses coefficients. Déterminons les coefficients dominants des polynômes $P \circ (X^2 + p)$ et $(X^2 + p) \circ P$.

- $P \circ (X^2 + p) = \displaystyle\sum_{k=0}^{n} a_k \left(X^2 + p\right)^k$ possède un coefficient dominant qui est celui de $a_n \left(X^2 + p\right)^n$ (puisque tous les autres termes de la somme sont de degré inférieur ou égal à $2n - 2$). Or, $\left(X^2 + p\right)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} X^{2k} p^{n-k}$ a pour coefficient dominant 1, et donc $P \circ (X^2 + p)$ a pour coefficient dominant a_n.
- $(X^2 + p) \circ P = P^2 + p$ a le même coefficient dominant que P^2, à savoir a_n^2.

Puisque $P \circ (X^2 + p) = (X^2 + p) \circ P$, il vient $a_n = a_n^2$, et donc $a_n = 1$ puisque $a_n \neq 0$ (par définition, un coefficient dominant est non nul). Ainsi, $\boxed{P \text{ est unitaire.}}$

8. Soient P_1, P_2 deux polynômes de $\mathscr{C}_p$, de même degré n. Alors :

$$P_1 \circ \left(X^2+p\right) - P_2 \circ \left(X^2+p\right) = (P_1 - P_2) \circ \left(X^2+p\right).$$

Mais par ailleurs, par définition de $\mathscr{C}_p$:

$$\begin{aligned} P_1 \circ \left(X^2+p\right) - P_2 \circ \left(X^2+p\right) &= \left(X^2+p\right) \circ P_1 - \left(X^2+p\right) \circ P_2 = \left(P_1^2+p\right) - \left(P_2^2+p\right) \\ &= P_1^2 - P_2^2 = (P_1-P_2)(P_1+P_2) \end{aligned}$$

Alors P_1+P_2 est de degré n, puisque son coefficient de degré n est $1+1=2\neq 0$. Et donc par identification des degrés :

$$\begin{aligned} 2\deg(P_1-P_2) &= \deg\left((P_1-P_2)\circ\left(X^2+p\right)\right) = \deg\left(P_1^2-P_2^2\right) \\ &= \deg(P_1+P_2)+\deg(P_1-P_2) = n+\deg(P_1-P_2) \end{aligned}$$

Si $P_1 \neq P_2$, alors $\deg(P_1-P_2)=n$. Mais ceci est absurde, car les termes de plus haut degré de P_1 et P_2 sont égaux, si bien que P_1-P_2 est de degré au plus $n-1$.

Ainsi, $P_1=P_2$, et $\boxed{\mathscr{C}_p \text{ contient au plus un polynôme de degré } n.}$

9. Supposons donc qu'il existe $P \in \mathscr{C}_p$ de degré 3 . Notons alors $P = aX^3+bX^2+cX+d$, avec $a \in \mathbb{R}^*$ et $(b,c,d) \in \mathbb{R}$. Calculons :

$$\begin{aligned} P \circ \left(X^2+p\right) &= a\left(X^2+p\right)^3 + b\left(X^2+p\right)^2 + c\left(X^2+p\right) + d \\ &= aX^6 + (3ap+b)X^4 + \left(3ap^2+2bp+c\right)X^2 + ap^3+bp^2+cp+d. \end{aligned}$$

Et de même :

$$\begin{aligned} \left(X^2+p\right) \circ P &= \left(aX^3+bX^2+cX+d\right)^2 + p \\ &= a^2X^6 + 2abX^5 + \left(b^2+2ac\right)X^4 + 2(ad+bc)X^3 + \left(c^2+2bd\right)X^2 + 2cdX + d^2 + p \end{aligned}$$

Par identification des coefficients on obtient :

- pour le degré 6, $a^2=a$, et puisque $a\neq 0, a=1$;
- pour le degré 5, $2ab=0$, donc $b=0$;
- pour le degré 4, $2c=3p$, donc $b=0$;
- pour le degré 3, $2d=0$, donc $d=0$;
- pour le degré 2, $3p^2+c=c^2$. Or :

$$3p^2+c=c^2 \Leftrightarrow 3p^3+\frac{3p}{2}=\frac{9p^2}{4} \Leftrightarrow 3p^2+6p=0 \Leftrightarrow p(p+2)=0$$

Et donc $\boxed{p=0 \text{ ou } p=-2.}$

10. Il est évident que pour tout $n\in\mathbb{N}^*$, $X^n\circ X^2 = X^2\circ X^n$, si bien que $\{X^n, n\in\mathbb{N}^*\}\subset\mathscr{C}_0$. Mais alors $\mathscr{C}_0$ contient déjà un polynôme de chaque degré non nul. Et comme elle ne peut pas en contenir plus d'un par la question 8, on obtient $\boxed{\mathscr{C}_0 = \{X^n, n\in\mathbb{N}^*\}.}$

11. (a) Soit $V=aX+b$ de degré 1. Calculons :

$$V\circ\left(X^2-2\right)\circ V^{-1} = a\left(\frac{X-b}{a}\right)^2 - 2a + b = \frac{X^2}{a} - 2bX + \frac{b^2}{a} - 2a + b.$$

Ce polynôme est égal à T_2 si, et seulement si :

$$\begin{cases} \frac{1}{a} = 2 \\ -2b = 0 \\ \frac{b^2}{a} - 2a + b = -1 \end{cases} \Leftrightarrow \begin{cases} a = \frac{1}{2} \\ b = 0 \\ -2a = -1 \end{cases}$$

Ainsi, $\boxed{\text{le polynôme } V = \dfrac{X}{2} \text{ convient.}}$

(b) Soit V comme dans la question précédente, de sorte que $X^2 - 2 = V^{-1} \circ T_2 \circ V$. Alors par la question 2.(b), $\left(V^{-1} \circ T_n \circ V\right)_{n \geq 1}$ est commutante, si bien que pour tout $n \in \mathbb{N}^*$, $V^{-1} \circ T_n \circ V$ commute avec $V^{-1} \circ T_2 \circ V = X^2 - 2$, et donc $V^{-1} \circ T_n \circ V \in \mathscr{C}_{-2}$. Mais $V^{-1} \circ T_n \circ V$ est de degré n, et par la question 8, $\mathscr{C}_{-2}$ contient au plus un polynôme de degré n. Ainsi, $\boxed{\mathscr{C}_{-2} = \left\{V^{-1} \circ T_n \circ V, n \in \mathbb{N}^*\right\}.}$

Partie IV. Théorème de Block-Thielmann

12. Par la question 2.(a) $U^{-1} = \frac{1}{a}\left(X - \frac{b}{2}\right)$, si bien que :

$$P \circ U^{-1} = a\left(\frac{X}{a} - \frac{b}{2a}\right)^2 + b\left(\frac{X}{a} - \frac{b}{2a}\right) + c = \frac{X^2}{a} + \left(-\frac{b}{a} + \frac{b}{a}\right)X + \frac{b^2}{4a} - \frac{b^2}{2a} + c = \frac{X^2}{a} + \frac{4ac - b^2}{4a}.$$

Et donc en composant par U :

$$\boxed{U \circ P \circ U^{-1} = a\left(P \circ U^{-1}\right) + b = X^2 + \frac{4ac - b^2}{4} + \frac{b}{2}}$$

qui est bien de la forme annoncée.

13. Puisque $(X^n)_{n \in \mathbb{N}^*}$ et $(T_n)_{n \in \mathbb{N}^*}$ sont deux suites commutantes, par la question 2.(b), pour tout U de degré 1, $\left(U \circ X^n \circ U^{-1}\right)_{n \in \mathbb{N}^*}$ et $\left(U \circ T_n \circ U^{-1}\right)_{n \in \mathbb{N}^*}$ sont des suites commutantes. Il s'agit donc de prouver que ce sont les seules.

Soit (P_n) une suite commutante. Alors :

- P_2 est de degré 2. Donc par la question 12, il existe $U \in \mathbb{R}[X]$ de degré 1 tel que $U \circ P_2 \circ U^{-1} = X^2 + p$, pour un certain $p \in \mathbb{R}$;
- Par la question 2.(b), $\left(U \circ P_n \circ U^{-1}\right)_{n \in \mathbb{N}^*}$ est encore une suite commutante. Ainsi, pour tout $n \in \mathbb{N}$, $U \circ P_n \circ U^{-1}$ commute avec $U \circ P_2 \circ U^{-1} = X^2 + p$. Autrement dit, $U \circ P_n \circ U^{-1} \in \mathscr{C}_p$.
- Puisque P_3 est de degré 3, $U \circ P_3 \circ U^{-1}$ est un élément de degré 3 de $\mathscr{C}_p$, si bien que $p = 0$ ou $p = -2$.

On a donc deux cas possibles :

- Si $p = 0$, alors pour tout $n \in \mathbb{N}^*$, $U \circ P_n \circ U^{-1} \in \mathscr{C}_0 = \left\{X^k, k \in \mathbb{N}^*\right\}$. Et donc par identification des degrés, $U \circ P_n \circ U^{-1} = X^n$, si bien que $P_n = U^{-1} \circ X^n \circ U$.
- Si $p = -2$, alors pour tout $n \in \mathbb{N}^*$, $U \circ P_n \circ U^{-1} \in \mathscr{C}_{-2} = \left\{V^{-1} \circ T_n \circ V, n \in \mathbb{N}^*\right\}$. Mais encore une fois, $U \circ P_n \circ U^{-1}$ est de degré n, et le seul k pour lequel $V^{-1} \circ T_k \circ V$ est de degré n est $k = n$. Donc $U \circ P_n \circ U^{-1} = V^{-1} \circ T_k \circ V$, si bien que :

$$P_n = U^{-1} \circ V^{-1} \circ T_n \circ V \circ U = (V \circ U)^{-1} \circ T_n \circ (V \circ U)$$

  où $V \circ U$ est bien de degré 1 .

Donc les suites commutantes sont exactement les $\left(U \circ X^n \circ U^{-1}\right)_{n \in \mathbb{N}^*}$ ou les $\left(U \circ T_n \circ U^{-1}\right)_{n \in \mathbb{N}^*}$ pour $U \in \mathbb{R}[X]$ de degré un.