DS 4
Suites - Groupes - Anneaux
Correction

Simon Dauguet
simon.dauguet@gmail.com

Mercredi 6 Décembre 2023

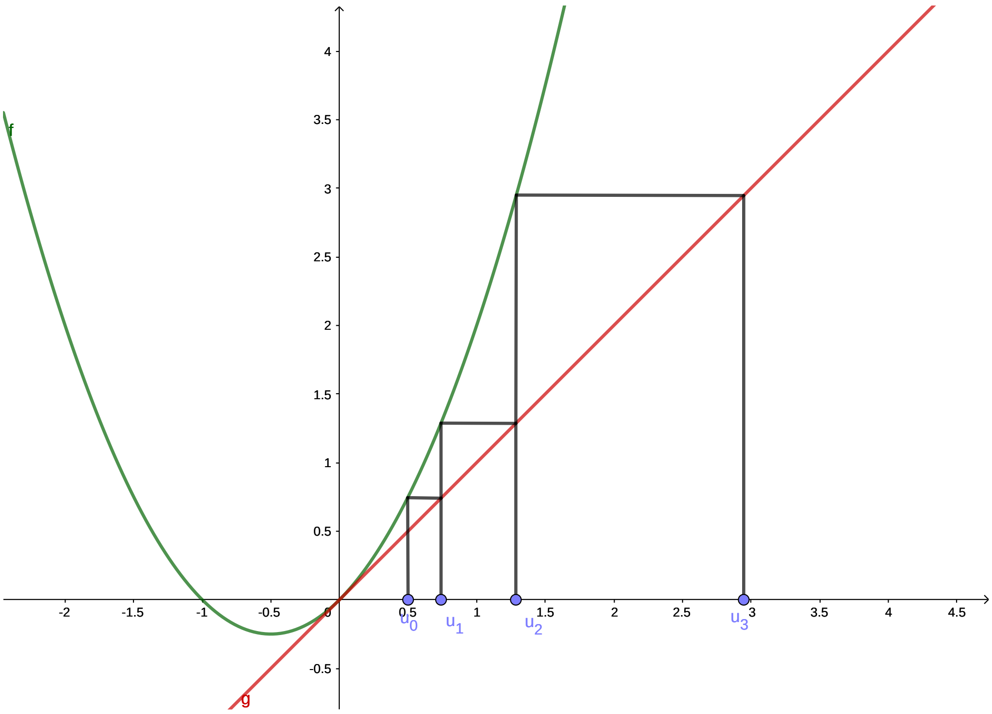
Problème 1 (Étude d'une suite récurrente d'ordre 1) :

Partie 1 : Étude du cas $u_0 \in \mathbb{R}$

1. On introduit la fonction $f : x \mapsto x + x^2$ qui est une fonction polynomiale, donc définie et dérivable sur $\mathbb{R}$. On a $\forall x \in \mathbb{R},\ f'(x) = 1 + 2x$. D'où le tableau de variations :

x	$-\infty$		-1		$-1/2$		0		$+\infty$
$f'(x)$		$-$			0			$+$	
f	$+\infty$	$\searrow$	0	$\searrow$	$-\frac{1}{4}$	$\nearrow$	0	$\nearrow$	$+\infty$

On a donc le graphe de f et les 3 premiers points de la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 = 1/2$ et $\forall n \in \mathbb{N},\ u_{n+1} = f(u_n)$.



2. On notera, d'après le tableau de variations, que $f(\mathbb{R}) = [-1/4, +\infty[$. Donc $f([-1/4, +\infty[) \subset [-1/4, +\infty[$ et donc $[-1/4, +\infty[$ est un intervalle stable par f. De plus, $\forall u_0 \in \mathbb{R}$, $u_1 \in [-1/4, +\infty[$, donc la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 \in \mathbb{R}$ et $\forall n \in \mathbb{N}$, $u_{n+1} = f(u_n)$ est bien définie.

Supposons $u_0 \in [-1/4, 0]$. Notons également que f est croissante sur $[-1/4, 0]$ et que $f(0) = 0$, donc $f([-1/4, 0]) = [f(-1/4), f(0)] = [-3/16, 0] \subset [-1/4, 0]$. Donc l'intervalle $[-1/4, 0]$ est stable par f. Donc si $u_0 \in \mathbb{R}$, alors $\forall n \in \mathbb{N}$, $u_n \in [-1/4, 0]$. Donc la suite (u_n) est bornée. Et f étant croissante sur $[-1/2, +\infty[$, elle l'est en particulier sur $[-1/4, 0]$, donc la suite (u_n) est monotone. Elle est donc monotone et bornée, donc, par théorème de la limite monotone, (u_n) est convergente.

Comme c'est une suite récurrence d'ordre 1, elle converge vers un point fixe de f. Or $f(x) = x \iff x + x^2 = x \iff x^2 = 0 \iff x = 0$. Donc elle converge vers l'unique point fixe de f qui est 0.

Supposons $u_0 > 0$. Comme, d'après le tableau de variations de f, $f(\mathbb{R}_+^*) =]f(0), +\infty[=]0, +\infty[$, l'intervalle $]0, +\infty[$ est donc stable par f et donc $\forall n \in \mathbb{N}$, $u_n > 0$. De plus, f est croissante donc (u_n) est monotone et $u_1 = u_0 + u_0^2 > u_0$. Donc la suite (u_n) est croissante. Si elle convergerait, par théorème de la limite monotone, on aurait $\lim_{n\to+\infty} u_n = \sup_{n\in\mathbb{N}} u_n$. Et comme c'est une suite récurrence d'ordre 1, elle convergerait également un point fixe de f. 0 est l'unique point fixe de f, donc par unicité de la limite, on aurait $0 < u_0 \leq \sup_{n\in\mathbb{N}} u_n = 0$. Donc ☠. Donc (u_n) ne peut pas converger.

Comme (u_n) est croissante et qu'elle est divergente, par théorème de la limite monotone, elle n'est pas bornée. Et donc $u_n \xrightarrow[n\to+\infty]{} +\infty$.

3. Supposons $u_0 < -1/4$. Si $u_0 < -1$, alors, par décroissance stricte de f, $f(u_0) = u_1 > f(-1) = 0$. On se ramène donc au cas précédent et donc (u_n) est divergente vers $+\infty$.

Si $-1 \leq u_0 < -1/4$, alors, $u_1 = f(u_0) \in [-1/4, 0]$ et donc on se ramène au cas précédent aussi et la suite (u_n) est convergente vers 0.

Partie 2 : Vitesse de convergence lorsque $u_0 \in]-1, 0[$

On suppose ici $u_0 \in]-1, 0[$.

4. On notera que $\forall n \in \mathbb{N}$, $f(-\frac{1}{n+1}) = -\frac{n}{(n+1)^2}$. Et aussi

$$\begin{aligned}
&\forall n \in \mathbb{N},\ n^2 + 2n < n^2 + 2n + 1 \\
\iff &\forall n \in \mathbb{N},\ \frac{1}{(n+1)^2} < \frac{1}{n(n+2)} \\
\iff &\forall n \in \mathbb{N},\ \frac{-1}{n+2} < \frac{-n}{(n+1)^2}
\end{aligned}$$

Comme $u_0 \in]-1, 0[$, d'après la tableau de variations de f dans la partie 1, on en déduit $u_1 \in]-1/4, 0[\subset]-1/2, 0[$.

Supposons qu'il existe $n \in \mathbb{N}^*$ tel que $-\frac{1}{n+1} < u_n < 0$. Alors, par croissance de f sur $[-1/2, +\infty[$, on en déduit $f(-\frac{1}{n+1}) < f(u_n) < f(0)$ et donc $-\frac{n}{(n+1)^2} < u_{n+1} < 0$. Enfin, d'après la remarque en début de question, on en déduit finalement que $-\frac{1}{n+2} < u_n < 0$.

Par principe de récurrence, on vient donc de montrer que $\forall n \in \mathbb{N}^*$, $u_n \in]-\frac{1}{n+1}, 0[$. Comme ce résultat est encore vrai pour $n = 0$, on a donc bien montré que $\forall n \in \mathbb{N}$, $-\frac{1}{n+1} < u_n < 0$.

Dans la mesure où $-\frac{1}{n+1} \xrightarrow[n\to+\infty]{} 0$, on en déduit, par le théorème des gendarmes, que $u_n \xrightarrow[n\to+\infty]{} 0$.

5. On définit la suite $(v_n)_{n\in\mathbb{N}}$ par $\forall n \in \mathbb{N}$, $v_n = nu_n$. On a alors

$$\begin{aligned}
\forall n \in \mathbb{N},\ v_{n+1} &= (n+1)u_{n+1} && \text{def de } (v_n) \\
&= (n+1)(u_n + u_n^2) \\
&= nu_n + u_n(1 + (n+1)u_n) \\
&= v_n + u_n(1 + (n+1)u_n) \\
&< v_n && \text{car } u_n < 0 \text{ et } 0 < 1 + (n+1)u_n < 1
\end{aligned}$$

On en déduit donc que $(v_n)_{n\in\mathbb{N}}$ est décroissante.

D'autre part,
$$\forall n \in \mathbb{N},\ v_n > -\frac{n}{n+1} = -1 + \frac{1}{n+1} > -1.$$
Donc la suite $(v_n)_{n\in\mathbb{N}}$ est minorée (par -1). Comme elle est décroissante, par théorème de la limite monotone, $(v_n)_{n\in\mathbb{N}}$ est convergente. On appelle ℓ sa limite.

Comme $\forall n \in \mathbb{N}$, $v_n > -1$, par passage à la limite dans les inégalités, on en déduit $\ell \geq -1$.

D'autre part, par théorème de la limite monotone, on a aussi $\ell = \inf_{n\in\mathbb{N}} v_n$. En particulier, $\ell \leq v_1 = u_1 \in]-1/2, 0[$. Donc $\ell < 0$.

D'où $\ell \in [-1, 0[$.

6. On définit la suite $(w_n)_{n\in\mathbb{N}}$ par $\forall n \in \mathbb{N}$, $w_n = n(v_{n+1} - v_n)$. Alors
$$\begin{aligned}\forall n \in \mathbb{N},\ w_n &= n(v_{n+1} - v_n)\\ &= n((n+1)u_{n+1} - nu_n)\\ &= n((n+1)u_n(1+u_n) - nu_n)\\ &= nu_n((n+1)(1+u_n) - n)\\ &= nu_n(n+1+(n+1)u_n - n)\\ &= nu_n(1 + nu_n + u_n)\\ &= v_n(1 + v_n + u_n).\end{aligned}$$
Mais $u_n \xrightarrow[n\to+\infty]{} 0$ d'après la question 4 et $v_n \xrightarrow[n\to+\infty]{} \ell$ d'après 5. Donc, par opérations sur les suites convergentes,
$$w_n = v_n(1 + v_n + u_n) \xrightarrow[n\to+\infty]{} \ell(1+\ell).$$

7. Soit $(a_n)_{n\in\mathbb{N}}$ une suite décroissante telle que $\exists k > 0$ et $\exists n_0 \in \mathbb{N}$ tels que $\forall n \geq n_0$, $a_{n+1} - a_n \geq \frac{k}{n}$.

Soit $n \geq n_0$. Alors, par télescopage,
$$\sum_{j=n}^{2n-1} (a_{j+1} - a_j) = a_{2n} - a_n$$
D'où
$$\begin{aligned}a_{2n} - a_n &= \sum_{j=n}^{2n-1} (a_{j+1} - a_j)\\ &\geq \sum_{j=n}^{2n-1} \frac{k}{j}\\ &\geq \sum_{j=n}^{2n-1} \frac{k}{2n}\\ &= \frac{k(2n-1-n+1)}{2n}\\ &= \frac{k}{2}.\end{aligned}$$
On vient donc de montrer que $\forall n \geq n_0$, $a_{2n} - a_n \geq k/2$.

On déduit alors que
$$\begin{aligned}\forall n \in \mathbb{N}^*,\ a_{2^n n_0} - a_{n_0} &= \sum_{j=0}^{n-1} (a_{2^{j+1}n_0} - a_{2^j n_0})\\ &\geq \sum_{j=0}^{n-1} (k/2)\end{aligned}$$

$$= nk/2.$$

Et donc, en particulier, $a_{2^n n_0} \xrightarrow[n\to+\infty]{} +\infty$, par corollaire du théorème des gendarmes (branche infinie).

Soit $A > 0$. Alors, par définition d'une limite infinie, $\exists n_1 \in \mathbb{N}$ tel que $\forall n \geq n_1$, $a_{2^n n_0} \geq A$. Et par croissance de $(a_n)_{n\in\mathbb{N}}$, on en déduit alors que $\forall n \geq 2^{n_1}n_0$, $a_n \geq a_{2^{n_1}n_0} \geq A$. Et donc, par définition, $a_n \xrightarrow[n\to+\infty]{} +\infty$.

On aurait pu le montrer aussi par l'absurde : si (a_n) est majorée, alors toutes ses suites le sont et on a une contradiction. Donc (a_n) n'est pas majorée. Par croissance et par théorème de la limite monotone, on en déduit le résultat.

8. Supposons que $\ell \neq -1$. donc, d'après la question 5, $\ell \in]-1, 0[$. Alors $\ell(\ell+1) \in]-1, 0[$. Donc $\ell(\ell+1) > -1$. On pose $\kappa = \frac{\ell(\ell+1)-1}{2} \in]-1, \ell(\ell+1)[$. Comme $w_n \xrightarrow[n\to+\infty]{} \ell(\ell+1)$ d'après la question 6, on en déduit aussi que $\exists n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0$, $w_n < \kappa$. Et donc $\forall n \geq n_0$, $v_{n+1} - v_n < \kappa/n$.

On pose alors, $\forall n \in \mathbb{N}$, $a_n = -v_n$. Comme (v_n) est décroissante, on en déduit que (a_n) est croissante. On pose enfin $k = -\kappa > 1$. Alors $\forall n \geq n_0$, $a_{n+1} - a_n = -(v_{n+1} - v_n) > -\kappa/n = k/n$. En utilisant la question précédente, on en déduit $a_n \xrightarrow[n\to+\infty]{} +\infty$. Autrement dit, $v_n = -a_n \xrightarrow[n\to+\infty]{} -\infty$. Or, à la question 5, on a montré que $v_n \xrightarrow[n\to+\infty]{} \ell \in [-1, 0[$. L'unicité de la limite nous donne alors ☠.

Finalement, on en conclut que notre hypothèse est fausse. Et donc $\ell = -1$.

Remarque :
On vient donc de montrer que $nu_n \xrightarrow[n\to+\infty]{} -1$. Comme $-1 \neq 0$, par "théorème de l'âne", $u_n \underset{n\to+\infty}{\sim} -1/n$.

Partie 3 : Étude du cas où $u_0 \in \mathbb{C}$ avec $|u_0| \geq 2$

9. Soit $a \in \mathbb{C}$ avec $|a| \geq 2$. Alors

$$\begin{aligned} |1+a| &\geq \big||1| - |a|\big| && \text{inéga tri renversée} \\ &= |a| - 1 && \text{car } |a| - 1 > 0 \\ &\geq 1 && \text{car } |a| \geq 2 \end{aligned}$$

Étudions maintenant le cas d'égalité. Pour avoir $|1+a| = 1$, en revenant dans l'étude précédente, il faut

$$\begin{aligned} |1+a| = |a| - 1 &\iff |1+a|^2 = (|a|-1)^2 \\ &\iff (1+a)(1+\overline{a}) = |a|^2 - 2|a| + 1 \\ &\iff 1 + 2\,\mathfrak{Re}(a) + |a|^2 = |a|^2 - 2|a| + 1 \\ &\iff \mathfrak{Re}(a) = -|a| \\ &\iff \begin{cases} \mathfrak{Re}(a) \leq 0 \\ \mathfrak{Im}(a) = 0 \end{cases} && \text{élever au carré} \\ &\iff a \in \mathbb{R}_-. \end{aligned}$$

D'autre part, on a toujours $|a| \geq 2$. Donc $a \leq -2$.

Et enfin, toujours pour avoir l'égalité, il faut $|a| - 1 = 1$ et donc $|a| = 2$. Donc $a = -2$.

10. On suppose ici $u_0 \in \mathbb{C}$ et $|u_0| \geq 2$. Supposons également qu'il existe $n \in \mathbb{N}$ tel que $|u_n| \geq 2$. Alors, d'après la question précédente, $|1 + u_n| \geq 1$. Et donc $|u_{n+1}| = |u_n||1 + u_n| \geq |u_n| \geq 2$. Donc, par principe de récurrence, $\forall n \in \mathbb{N}$, $|u_n| \geq 2$.

11. On pose $k = |u_1| - 2$. Alors

$$\begin{aligned} |u_2| &= |u_1||1 + u_1| \\ &\geq |u_1|\big|1 - |u_1|\big| && \text{inéga tri renversée} \\ &\geq |u_1|(|u_1| - 1) \end{aligned}$$

$$= |u_1|(1+k).$$

Supposons enfin qu'il existe $n \in \mathbb{N}^*$ tel que $|u_{n+1}| \geq (1+k)|u_n|$. Alors

$$\begin{aligned}
|u_{n+2}| &= |u_{n+1}||1+u_{n+1}| \\
&\geq |u_{n+1}|(|u_{n+1}|-1) \\
&\geq |u_{n+1}|((1+k)|u_n|-1) && \text{HR} \\
&\geq |u_{n+1}|(2(1+k)-1) \\
&= (2k+1)|u_{n+1}| \\
&\geq (k+1)|u_{n+1}| && \text{car } k \geq 0
\end{aligned}$$

On vient de montrer, par principe de récurrence, que $\forall n \in \mathbb{N}^*,\ |u_{n+1}| \geq (1+k)|u_n|$.

On en déduit facilement que $\forall n \in \mathbb{N}^*$, $|u_n| \geq (1+k)^{n-1}|u_1|$. Or $1+k > 1$, donc, par suite géométrique et corollaire du théorème des gendarmes, $|u_n| \xrightarrow[n\to+\infty]{} +\infty$.

Partie 4 : Étude de l'ensemble des valeurs $u_0 \in \mathbb{C}$ pour lesquelles (u_n) converge.

On note ici $R = \{a+ib,\ -1 \leq a \leq 0,\ |b| \leq \sqrt{3}/2\}$ et $\mathring{R} = \{a+ib,\ -1 < a < 0,\ |b| < \sqrt{3}/2\}$.

12. On note, $\forall n \in \mathbb{N}$, $a_n = \mathfrak{Re}(a_n)$ et $b_n = \mathfrak{Im}(a_n)$. Alors

$$\begin{aligned}
\forall n \in \mathbb{N},\ u_{n+1} &= u_n + u_n^2 \\
&= u_n + (a_n + ib_n)^2 \\
&= a_n + a_n^2 - b_n^2 + i(b_n + 2a_nb_n)
\end{aligned}$$

On en déduit, par caractérisation d'un complexe par sa forme algébrique que

$$\forall n \in \mathbb{N},\ \begin{cases} a_{n+1} = \mathfrak{Re}(u_{n+1}) = a_n + a_n^2 - b_n^2 \\ b_{n+1} = \mathfrak{Im}(u_{n+1}) = b_n(1+2a_n) \end{cases}$$

13. Soit $z \in R$. Alors $f(z) = (\mathfrak{Re}(z) + \mathfrak{Re}(z)^2 - \mathfrak{Im}(z)^2) + i(\mathfrak{Im}(z) + 2\,\mathfrak{Re}(z)\,\mathfrak{Im}(z))$. Or $\forall x \in \mathbb{R}$, $x + x^2 = (x+1/2)^2 - 1/4$ donc $\forall x[-1,0]$, $x + x^2 \in [-1/4, 0]$. On a donc $\mathfrak{Re}(z) + \mathfrak{Re}(z)^2 \in [-1/4, 0]$. Et $-3/4 \leq \mathfrak{Im}(z)^2 \leq 0$. Donc, par somme, on a $-1 \leq \mathfrak{Re}(f(z)) = \mathfrak{Re}(z) + \mathfrak{Re}(z)^2 - \mathfrak{Im}(z)^2 \leq 0$.

De plus, $-1 \leq 1 + 2\,\mathfrak{Re}(z) \leq 1$ et donc $|\,\mathfrak{Im}(f(z))| = |\,\mathfrak{Im}(z)||1 + 2\,\mathfrak{Re}(z)| \leq |\,\mathfrak{Im}(z)| \leq \sqrt{3}/2$. Donc, par définition, $f(z) \in R$. Donc R est stable par f.

14. On a vu précédemment que $\forall n \in \mathbb{N}$, $|b_{n+1}| = |b_n||1+2a_n| \leq |b_n|$ car $u_n \in R$. Donc $(|b_n|)$ est décroissante. Comme elle est minorée par 0, par théorème de la limite monotone, elle est convergente vers $\lambda \in \mathbb{R}$.

Dans la mesure où on a $\forall n \in \mathbb{N}$, $|b_n| \in [0, \sqrt{3}/2]$, par passage à la limite dans les inégalités, on en déduit $\lambda \in [0, \sqrt{3}/2]$.

15. Supposons $\lambda > 0$. Donc, $\exists n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0$, $|b_n| > 0$. Alors

$$|1 + 2a_n| = \frac{|b_{n+1}|}{|b_n|} \xrightarrow[n\to+\infty]{} 1$$

par opérations sur les suites convergentes. Toujours par opérations sur les suites convergentes, on en déduit $(1+2a_n)^2 = 1 + 4a_n + 4a_n^2 \xrightarrow[n\to+\infty]{} 1$ (on rappelle que (a_n) est une suite réelle). D'où, pour les mêmes raisons, $a_n + a_n^2 \xrightarrow[n\to+\infty]{} 0$. Alors $a_n + a_n^2 - b_n^2 \xrightarrow[n\to+\infty]{} -\lambda^2$. Or, par définition de la suite $(a_n)_{n\in\mathbb{N}}$, on a donc $a_n \xrightarrow[n\to+\infty]{} -\lambda^2$. Et alors $a_n + a_n^2 \xrightarrow[n\to+\infty]{} -\lambda^2 + \lambda^4$. D'où, par unicité de la limite $\lambda^4 - \lambda^2 = 0$. Or, par hypothèse $\lambda > 0$ et donc $\lambda^2 - 1 = 0$, puis $\lambda = 1$.

Mais d'après la question précédente, $\lambda \in [0, \sqrt{3}/2]$. Et bien sûr $\sqrt{3}/2 < 1$. Donc ☠. D'où $\lambda = 0$.

16. On a montré à la question 13 que R est stable par f. Or, par hypothèse, $u_0 \in R$. Donc $\forall n \in \mathbb{N}$, $u_n \in R$. D'autre part, d'après la question 12, on a également,

$$\begin{aligned}
\forall n \in \mathbb{N},\ a_{n+1} + b_{n+1}^2 &= a_n + a_n^2 - b_n^2 + b_n^2(1+2a_n)^2 \\
&= a_n + a_n^2 - b_n^2 + b_n^2 + 4a_n b_n^2 + 4a_n^2 b_n^2 \\
&= a_n + a_n^2 + 4a_n b_n^2 + 4a_n^2 b_n^2 \\
&= a_n(1 + a_n + 4b_n^2 + 4a_n b_n^2) \\
&= a_n(1+a_n)(1+4b_n^2) \\
&\leq 0 && \text{car } u_n \in R.
\end{aligned}$$

D'où $\forall n \in \mathbb{N}^*$, $a_n + b_n^2 \leq 0$.

Alors

$$\begin{aligned}
\forall n \in \mathbb{N}^*,\ |1+u_n|^2 &= (1+a_n)^2 + b_n^2 \\
&= 1 + 2a_n + a_n^2 + b_n^2 \\
&= 1 + a_n(1+a_n) + (a_n + b_n^2)
\end{aligned}$$

On vient de montrer que $\forall n \in \mathbb{N}^*$, $a_n + b_n^2 \leq 0$. D'autre part, d'après la question 12, $\forall n \in \mathbb{N}$, $a_n + 1 \geq 0$ et $a_n \leq 0$. Donc $\forall n \in \mathbb{N}^*$, $a_n(1+a_n) \leq 1$ et donc $\forall n \in \mathbb{N}^*$, $|1+u_n|^2 \leq 1$. Finalement, on en déduit $\forall n \in \mathbb{N}^*$, $|1+u_n| \leq 1$.

Par suite, $\forall n \in \mathbb{N}^*$, $|u_{n+1}| = |u_n||1+u_n| \leq |u_n|$. Donc $(|u_n|)_{n\geq 1}$ est décroissante et évidemment minorée par 0, donc elle est convergente par théorème de la limite monotone.

17. D'après la question précédente et par opérations sur les suites convergentes, $(|u_n|^2)$ est convergente. Donc $(a_n^2 + b_n^2)$ est convergente. Or (b_n) est convergente vers 0 d'après la question 16. Donc (a_n^2) est convergente par opérations sur les suites convergentes. Or $\forall n \in \mathbb{N}$, $a_n^2 \in [0,1]$. Donc la limite de (a_n^2) est dans $[0,1]$, par passage à la limite dans les inégalités. La fonction $x \mapsto \sqrt{x}$ étant continue sur $[0,1]$, on en déduit, par composition dans les limites, que $(|a_n|)$ est convergente.

Donc $(-|a_n|)$ est aussi convergente, toujours par opérations sur les suites convergentes. Et donc (a_n) converge puisque $\forall n \in \mathbb{N}$, $a_n \leq 0$ et donc $\forall n \in \mathbb{N}$, $a_n = -|a_n|$.

On appelle $\ell \in [-1,0]$ la limite de (a_n). En reprenant la relation de récurrence vérifiée par (a_n) et en utilisant la convergence de (b_n) vers 0 et par unicité de la limite, on en déduit $\ell = \ell + \ell^2$ et donc $\ell = 0$.

On vient donc de montrer que $a_n \xrightarrow[n\to+\infty]{} 0$. Et donc $u_n = a_n + ib_n \xrightarrow[n\to+\infty]{} 0$ par linéarité de la limite et opérations sur les suites convergentes.

Problème 2 (Sous-groupes distingués) :
Soit G un groupe multiplicatif. Soit $e \in G$ élément neutre.

Partie I : Définition des sous-groupes distingués

1. Soit H un sous-groupe de G. $\boxed{(i) \Rightarrow (ii)}$ Soit $a \in G$. Soit $h \in H$. Donc $ha \in Ha$ par définition de Ha. Mais, par associativité, $ah = a(ha^{-1})a$. Or $Ha^{-1} \subset a^{-1}H$. Donc $\exists k \in H$ tel que $ha^{-1} = a^{-1}k$. Et donc $ah = a(a^{-1}k)a = ka$ par associativité. Donc $ah \in Ha$. Et donc $aH \subset Ha$.

$\boxed{(ii) \implies (i)}$ Soit $a \in G$. Soit $h \in H$. Alors $ah = a(ha^{-1})a$. Or $Ha^{-1} \subset a^{-1}H$ et donc $\exists k \in H$ tel que $ha^{-1} = a^{-1}k$. Et donc $ah = a(a^{-1}k)a = ka \in Ha$. Donc $aH \subset Ha$.

Donc $(i) \Rightarrow (ii)$ et donc $(i) \Rightarrow (iii)$. De même, $(ii) \Rightarrow (i)$ et donc aussi $(ii) \Rightarrow (iii)$. Or $(iii) \Rightarrow (i)$ et $(iii) \Rightarrow (ii)$. D'où toutes les équivalences.

On dit que H est distingué dans G si $aH = Ha$.

2. Soit H un sous-groupe de G.

Supposons H distingué. Soit $a \in G$. D'après la question précédente, on a $aH = Ha$. Alors $aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H$.

Supposons que $\forall a \in G$, $aHa^{-1} = H$. Alors $\forall a \in G$, $aHa^{-1} \subset H$ par définition de l'égalité entre ensemble.

Supposons $\forall a \in G$, $aHa^{-1} \subset H$. Alors aussi $\forall a \in G$, $aH = (aHa^{-1})a \subset Ha$. Et donc, d'après la question précédente, H est distingué.

D'où les équivalences.

3. Soit $a \in G$ et $\varphi_a : x \mapsto axa^{-1}$.

(a) Soit $x, y \in G$. Alors $\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya{-}1) = \varphi_a(x)\varphi_a(y)$ par associativité. Donc, par définition, φ_a est un morphisme de groupe.

De plus, si $x \in G$ tel que $\varphi_a(x) = e$, alors $axa^{-1} = e$ et donc, $x = a^{-1}(axa^{-1})a = aea^{-1} = e$. Donc $\ker(\varphi_a) \subset \{e\}$. Or $\{e\} \subset \ker(\varphi_a)$. Donc $\ker(\varphi_a) = \{e\}$ par définition de l'égalité entre ensembles. Et donc, par caractérisation de l'injectivité par le noyau, φ_a est injective.

De plus, on a bien sûr $aGa^{-1} \subset G$. Et donc G est un sous-groupe distingué (trivial) de G. Donc $\varphi_a(G) = aGa^{-1} = G$. Donc φ_a est surjectif. Et donc φ_a est bijectif.

Donc φ_a est un automorphisme.

(b) Soit H un sous-groupe de G. H est distingué dans G si et seulement si $\forall a \in G$, $\varphi_a(H) = aHa^{-1} \subset H$ si, et seulement si, $\forall a \in G$, H est stable par φ_a si, et seulement si, $\forall a \in G$, H est stable par tout endomorphisme intérieur.

Partie II : Exemples de sous-groupes distingués

4. G est distingué car $\forall a \in G$, $aGa^{-1} \subset G$ puisque G est stable par la LCI. De plus, $\forall a \in G$, $a\{e\}a^{-1} = \{aea^{-1}\} = \{e\}$. Et donc, par la question 2, $\{e\}$ est distingué dans G.

5. Si G est abélien et si H est un sous-groupe de G, alors $\forall a \in G$, $aHa^{-1} = \{aha^{-1},\ h \in H\} = \{aa^{-1}h,\ h \in H\} = H$ par associativité et commutativité. Donc tout sous-groupe est distingué dans un groupe abélien.

6. Soit G' un groupe. Soit $f : G \to G'$ un morphisme de groupe.

(a) Soit H' un sous-groupe distingué de G'. Alors $f^{-1}(H')$ est un sous-groupe de G. Soit $a \in G$. Soit $x \in f^{-1}(H')$. Alors $f(axa^{-1}) = f(a)f(x)f(a)^{-1}$ car f est un morphisme de groupe.

Or $x \in f^{-1}(H')$, donc, par définition, $f(x) \in H'$. Et H' est distingué de G'. Donc $f(a)f(x)f(a)^{-1} \in H'$ d'après 2.

Donc $f(axa^{-1}) \in H'$. Et donc, par définition, $axa^{-1} \in f^{-1}(H')$ par définition de l'image réciproque d'un ensemble.

On vient donc de montrer que $\forall x \in f^{-1}(H')$, $axa^{-1} \in f^{-1}(H')$. Et donc $af^{-1}(H')a^{-1} \subset f^{-1}(H')$. Et donc $\forall a \in G$, $af^{-1}(H')a^{-1} \subset f^{-1}(H')$. Et donc, par suite, $f^{-1}(H')$ en utilisant 2.

(b) On suppose f surjective. Soit H un sous-groupe distingué de G. Alors $f(H)$ esy un sous-groupe de G'.

Soit $a \in G'$. Alors $\exists x \in G$ tel que $a = f(x)$ par surjectivité de f. Et donc, si $h \in H$, alors $af(h)a^{-1} = f(x)f(h)f(x)^{-1} = f(xhx^{-1})$ par morphisme de groupes. Or H distingué dans G, donc $xhx^{-1} \in H$ d'après 2. Donc $af(h)a^{-1} \in f(H)$. Donc $af(H)a^{-1} \subset f(H)$. Puis, en utilisant 2, $f(H)$ est un sous-groupe distingué de G'.

(c) Comme $\{e_{G'}\}$ est sous-groupe distingué de G', alors $\ker(f) = f^{-1}(\{e_{G'}\})$ est un sous-groupe distingué de G.

Partie IV : Produit de deux sous-groupes

Soit H, K deux sous-groupes de G.

7. Supposons $HK \subset KH$. Soit $h \in H$, $k \in K$. Alors $(kh)^{-1} = h^{-1}k^{-1} \in HK$. Donc $(kh)^{-1} \in KH$. Donc $\exists (h', k') \in H \times K$ tel que $(kh)^{-1} = k'h'$. Et par passage à l'inverse et involution de l'inverse, $kh = (k'h')^{-1} = h'^{-1}k'^{-1} \in HK$ car H et K sont des sous-groupes dont stables par stabilité par passage à l'inverse. Donc $KH \subset HK$.

Par symétrie du problème en H et K, en reprenant le paragraphe précédents et en échangeant les H par des K, on obtient $KH \subset HK \Rightarrow HK \subset KH$.

On a donc $KH \subset HK \iff HK \subset KH$. Et donc l'équivalence avec l'égalité par définition de l'égalité entre ensemble.

8. Si HK est un sous-groupe de G, alors HK est stable par passage à l'inverse. Donc $\forall h \in H$, $\forall k \in K$, $kh = (k^{-1})^{-1}(h^{-1})^{-1} = (h^{-1}k^{-1})^{-1} \in HK$. Donc $KH \subset HK$. Et donc $HK = KH$ par la question précédente.

Réciproquement, supposons $HK = KH$. On $e = ee \in HK$. Soit $h, h' \in H$ et $k, k' \in K$. Alors $(hk)(h'k') = h(kh')k'$. Et $kh' \in KH = HK$. Donc $(hk)(h'k') \in hHKk' \subset HK$. Donc HK est stable par produit. Enfin, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Donc HK est stable par passage à l'inverse. Donc HK est un sous-groupe par caractérisation des sous-groupes.

9. Supposons H distingué dans G. Alors $\forall k \in K$, $kH = Hk$ d'après 1. On en déduit $KH \subset HK$. Et donc, d'après ce qui précède, $HK = KH$.

Alors, HK (et KH) sont des sous-groupes de G.

Par symétrie du problème en H et K, on aboutit à la même conclusion si K est distingué dans G.