Corrigé du devoir surveillé n°3

Exercice 1.

Soit $(A, +, \times)$ un anneau commutatif et B une partie de A.
On appelle **annulateur de** B et on note $\mathrm{Ann}(B)$, l'ensemble :

$$\mathrm{Ann}(B) = \{x \in A \mid \forall\, b \in B,\ xb = 0_A\}.$$

Démontrer que $\mathrm{Ann}(B)$ est un idéal de A.

Correction.

- Montrons que $\mathrm{Ann}(B)$ est un sous-groupe de $(A, +)$.
  - $\mathrm{Ann}(B)$ est inclus dans A car il est défini comme un ensemble d'éléments de A vérifiant une propriété.
  - On a, pour tout $b \in B$, $0_A.b = 0_A$ donc $0_A \in \mathrm{Ann}(B)$.
  - Soit $x, y \in \mathrm{Ann}(B)$. On a, pour tout $b \in B$, par distributivité dans l'anneau A :

    $$(x - y)b = xb - yb = 0_A - 0_A = 0_A$$

    donc $x - y$ appartient à $\mathrm{Ann}(B)$.

  Par suite, $\mathrm{Ann}(B)$ est un sous-groupe de $(A, +)$.
- Soit $a \in A$ et $x \in \mathrm{Ann}(B)$. On a, pour tout $b \in B$, par associativité de $\cdot$:

  $$(ax)b = a(xb) = a0_A = 0_A$$

  donc ax appartient à $\mathrm{Ann}(B)$.

Il en résulte que $\mathrm{Ann}(B)$ est un idéal de A.

Exercice 2. *Centrale MP 2006*

On considère l'espace vectoriel réel $C^2([0,1], \mathbb{R})$ des fonctions de classe C^2 de $[0,1]$ dans $\mathbb{R}$ et on pose $E = \{f \in C^2([0,1], \mathbb{R}) \mid f(0) = f'(0) = 0\}$. De plus, on note, pour $f \in C^2([0,1], \mathbb{R})$:

$$\|f\|_\infty = \sup_{t \in [0,1]} |f(t)|, \quad N(f) = \|f + f''\|_\infty \text{ et } N'(f) = \|f\|_\infty + \|f''\|_\infty$$

1. Montrer que E est un sous-espace vectoriel de $C^2([0,1], \mathbb{R})$.
2. On admet que $\|\cdot\|_\infty$ est bien une norme sur E. Montrer que N et N' sont des fonctions bien définies sur E et que ce sont des normes.
3. Montrer que $\|\cdot\|_\infty$ n'est ni équivalente à N, ni à N'.
4. Montrer que N et N' sont équivalentes.

Indication : on admettra que pour g une fonction, la solution de $y'' + y = g$ avec $y(0) = y'(0) = 0$ est donné par $y : t \mapsto \int_0^t \sin(t-x)g(x)dx$ (les 5/2, prouvez-le !)

Correction.

1. La fonction nulle $\mathbf{0}$ vérifie $\mathbf{0}(0) = 0$ et $\mathbf{0}'(0) = \mathbf{0}(0) = 0$. Donc $\mathbf{0} \in E$.
   Soit $f, g \in E$ et $\lambda, \mu \in \mathbb{R}$. Comme $f(0) = 0$ et $g(0) = 0$, on a :
   $$(\lambda f + \mu g)(0) = \lambda f(0) + \mu g(0) = 0$$
   et comme $f'(0) = 0$ et $g'(0) = 0$, on a, par linéarité de la dérivation :
   $$(\lambda f + \mu g)'(0) = (\lambda f' + \mu g')(0) = \lambda f'(0) + \mu g'(0) = 0$$
   Par suite, E est un sous-espace vectoriel de $C^2([0,1], \mathbb{R})$.

2. En utilisant les propriétés de la norme infinie et la linéarité de la dérivation, la plupart des axiomes de norme pour N et N' se vérifient aisément. Seule l'axiome de spéaration pour la norme N mérite qu'on s'y attarde :
   Soit $f \in E$ tel que $N(f) = 0$. Alors, par séparation de la norme infinie, on a $f + f'' = 0$. Ainsi f est solution du problème de Cauchy :
   $$\begin{cases} y'' + y = 0 \\ y(0) = 0 = y'(0) \end{cases}$$
   qui admet une unique solution : la fonction nulle. En effet, l'équation différentielle homogène $y'' + y = 0$ admet $\{Acos + Bsin \mid A, B \in \mathbb{R}\}$ pour ensemble de solutions. En utilisant les conditions initiales du problème de Cauchy, on obtient $A = B = 0$.
   Par suite $f = 0$.

3. Considérons la suite $(f_n)_{n\geq 2}$ telle que pour tout $n \geq 2$, $f_n : x \mapsto x^n$.
   Pour tout $n \geq 2$, f_n est C^∞ sur $\mathbb{R}$ et donc en particulier C^2 sur $[0,1]$, et on a $f_n'' : x \mapsto n(n-1)x^{n-2}$ d'où $f_n(0) = 0$ et $f_n''(0) = 0$; par suite, f_n appartient à E.
   On a de plus, pour tout $n \geq 2$:
   - $\|f_n\|_\infty = 1$ (atteint pour $x = 1$) ;
   - $N(f_n) = 1 + n(n-1)$ (atteint pour $x = 1$) ;
   - $N'(f_n) = 1 + n(n-1)$ (atteint pour $x = 1$) ;

   ainsi,
   $$\frac{N(f_n)}{\|f_n\|_\infty} = \frac{N(f_n)}{\|f_n\|_\infty} = 1 + n(n-1) \xrightarrow[n\to\infty]{} +\infty$$
   Par suite, N et N' ne sont pas dominées par la norme infinie et a fortiori, elles ne sont pas équivalentes à la normes infinie.

4. Soit $f \in E$. On a, par inégalité triangulaire de la norme infinie :
   $$N(f) = \|f + f''\|_\infty \leq \|f\|_\infty + \|f''\|_\infty = N'(f)$$
   donc N' domine N.
   Montrons désormais que N domine N'. Pour cela, pour $f \in E$, considérons la fonction

$g = f + f''$. Comparons le maximum sur $[0,1]$ de $|f|$ avec celui de $|g|$ (il s'agit de fonctions continues sur le segment $[0,1]$ donc elles admettent un maximum sur $[0,1]$).
Considérons l'équation différentielle $y'' + y = g$ dont f est solution. En utilisant les solutions de l'équation homogène ; en appliquant la méthode de variation de la constante puis en utilisant les conditions initiales, on trouve $f : t \mapsto \int_0^t \sin(t-x)g(x)dx$ (il y a pas mal de boulot calculatoire quand même pour y arriver :)). Par suite, pour tout $t \in [0,1]$:

$$|f(t)| \leq \int_0^t |\sin(t-x)|.|g(x)|dx \leq t|g(x)| \leq |g(x)|$$

D'où $\|f\|_\infty \leq \|g\|_\infty = N(f)$.
De plus, $\|f''\|_\infty = \|f + f'' - f\|_\infty \leq N(f) + \|f\|_\infty \leq 2N(f)$.
Il en résulte que :

$$N'(f) \leq \|f\|_\infty + \|f''\|_\infty \leq 3N(f)$$

Par suite, N et N' sont équivalentes.

Problème 1.

Dans tout le problème, on note I l'intervalle $I =]-1,1[$.
Nous allons munir I d'une structure de groupe un peu particulière.

1. Montrer que : $\forall (s,t) \in I^2,\ 1 + st \neq 0$.
   On pose, pour tous s et t de I : $s * t := \dfrac{s+t}{1+st}$.

2. (a) Soit $s \in I$ *fixé*. Etudier la fonction $f : \left| \begin{array}{ccc} I & \to & \mathbb{R} \\ t & \mapsto & f(t) = s*t = \dfrac{s+t}{1+st} \end{array} \right.$.
   En déduire que $*$ est une loi de composition interne dans I.

   (b) Montrer que $(I, *)$ est un groupe commutatif.

   (c) $([0,1[, *)$ est-il un sous-groupe de $(I, *)$?

   (d) Soit x un réel strictement positif (fixé). On considère l'ensemble $H_x = \left\{ \dfrac{x^n - 1}{x^n + 1},\ \text{avec } n \in \mathbb{Z} \right\}$.
   Ainsi, on a la caractérisation : $(s \in H_x) \Leftrightarrow (\exists n \in \mathbb{Z} \mid s = \dfrac{x^n - 1}{x^n + 1})$
   Montrer que $(H_x, *)$ est un sous-groupe de $(I, *)$.

3. Soit $s \in I$, avec $s \neq 0$.
   Dans cette question, on désire expliciter $\underbrace{s * s * s \cdots * s}_{n \text{ fois}}$, que l'on notera $s^{[n]}$.
   On prendra la convention $s^{[0]} = 0$.

   (a) Montrer que, pour tout $n \in \mathbb{N}$, $s^{[n]}$ peut s'écrire $\dfrac{p_n}{q_n}$ avec les suites $(p_n)_{n\geq 0}$ et $(q_n)_{n \geq 0}$ définies par :

$$\left\{ \begin{array}{l} p_0 = 0 \\ q_0 = 1 \end{array} \right. \text{ et pour tout } n \in \mathbb{N}, \left\{ \begin{array}{l} p_{n+1} = p_n + sq_n \\ q_{n+1} = sp_n + q_n \end{array} \right.$$

(b) Exprimer sq_{n+1} en fonction de p_{n+1} et p_n puis exprimer p_{n+2} en fonction de p_{n+1} et p_n.
(c) En déduire l'expression générale de p_n puis celle de q_n.
(d) Exprimer $s^{[n]}$. On observera que cette formule vaut aussi pour $s = 0$.

4. Montrer que la fonction th (tangente hyperbolique) définie par $\text{th}(x) = \dfrac{\text{sh}(x)}{\text{ch}(x)} = \dfrac{e^{2x}-1}{e^{2x}+1}$ réalise un isomorphisme de $(\mathbb{R}, +)$ vers $(I, *)$.
5. Exploiter ces résultats pour exprimer $\text{th}(nx)$ en fonction de $\text{th}(x)$.
Application : exprimer $\text{th}(2x)$, $\text{th}(3x)$, $\text{th}(3x)$, $\text{th}(4x)$, $\text{th}(5x)$ en fonction de $\text{th}(x)$.

Correction.

1. Soit $s, t \in I =]-1, 1[$. Alors $|st| = |s|.|t| < 1$ car $|s| < 1$ et $|t| < 1$. Par suite, $-1 < st < 1$, donc en particulier, $st \neq -1$. Ainsi, $1 + st \neq 0$.

2. a) Soit $s \in I$. On peut, comme le propose l'énoncé, étudier la fonction f qui est définie et dérivable - quotient de fonctions affines - sur $[-1, 1]$ (elle est bien définie en -1 et 1 car en reprenant la question précédente avec $|t| \leq 1$, on obtient la même conclusion). On trouve alors que f est strictement croissante ; $f(-1) = -1$ et $f(1) = 1$. Ainsi, pour tout $t \in I$, on a $s * t = f(t) \in I$.
On pouvait également remarquer que pour $s, t \in I$, $s < 1$ et $t - 1 < 0$, donc $(t-1)s > (t-1)$. Après développement, on trouve $s + t < 1 + st$. Comme $1 + st > 0$ (d'après le raisonnement de la q1, on a $0 < 1 + st < 2$), $s * t = \frac{s+t}{1+st} < 1$. De plus, de $1 + st < 2$ et $s + t > -2$, on tire $s * t = \frac{s+t}{1+st} > \frac{-2}{2} = -1$. D'où $s * t \in I$.
Il en résulte que pour tout $s, t \in I$, $s * t \in I$ et donc, $*$ est une opération interne sur I.

b) D'après la question précédente, $*$ est une opération interne sur I. Montrons qu'elle est associative, qu'elle possède un élement neutre et que tout élément de I possède un symétrique pour $*$.

— *Associativité :* Soit $s, t, u \in I$. On a :

$$\begin{aligned}(s * t) * u &= \frac{s+t}{1+st} * u \\ &= \frac{\frac{s+t}{1+st} + u}{1 + \frac{s+t}{1+st}u}\end{aligned}$$

On multiplie dénominateur et numérateur par $1 + st$

$$= \frac{s + t + u + stu}{1 + st + su + tu}$$

On repart du bas pour arriver au même endroit :)

$$\begin{aligned}&= \frac{s + \frac{t+u}{1+tu}}{1 + s\frac{t+u}{1+tu}} \\ &= s * \frac{t+u}{1+tu} \\ &= s * (t * u)\end{aligned}$$

— *Élement neutre :* Soit $s \in I$. On a :

$$s * 0 = \frac{s+0}{1+s\times 0} = s (= 0 * s)$$

donc 0 est un élement neutre pour $*$.

— *Symétrique :* Soit $s \in I$. Pour $t = -s$, on a :

$$s * t = \frac{s+t}{1+st} = \frac{s-s}{1-s^2} = 0.$$

Donc s admet un symétrique pour $*$ et ce symétrique est $-s$.

Il en résulte que $(I, *)$ est un groupe.
De plus, pour tout $s, t \in I$, on a, par commutativité de $+$ et $\times$ dans $\mathbb{R}$:

$$s * t = \frac{s+t}{1+st} = \frac{t+s}{1+ts} = t * s$$

Ainsi $(I, *)$ est un groupe commutatif.

Pour l'anecdote, l'opération $*$ représente la loi de composition des vitesses en relativité - en considérant ici la vitesse de lumière c égale à 1 ; on pourrait montrer les mêmes résultats que précédemment pour $I =]-c, c[$ et $u * v = \dfrac{u+v}{1+\frac{uv}{c^2}}$.

c) pour $s = \frac{1}{2} \in [0, 1[$, son symétrique $-s = -\frac{1}{2} \notin [0, 1[$. Donc $[0, 1[$ n'est pas un sous-groupe de I car il n'est pas stable par passage au symétrique.

d) Soit $x \in \mathbb{R}_+^*$. Il faut tout d'abord vérifier que H_x est bien inclus dans I. Soit $s \in H_x$. Alors il existe $n \in \mathbb{Z}$ tel que $s = \frac{x^n-1}{x^n+1}$. Comme $x > 0$, $1 < x^n + 1$ et ainsi $-2 < -\frac{2}{x^n+1} < 0$; or on a

$$s = \frac{x^n-1}{x^n+1} = 1 - \frac{2}{x^n+1}$$

d'où $-1 < s < 1$ i.e. $s \in I$. Ainsi, $H_x \subset I$.

Montrons que H_x est un sous-groupe de $(I, *)$.

— H_x est non vide car pour $n = 0 \in \mathbb{Z}$, $0 = \frac{x^0-1}{x^0+1} \in H_x$.

— Soit $s, t \in H_x$. Montrons que $s * (-t) \in H_x$. Il existe $n, m \in \mathbb{Z}$ tels que $s = \frac{x^n-1}{x^n+1}$ et $t = \frac{x^m-1}{x^m+1}$ et on a :

$$\begin{aligned} s * (-t) &= \frac{\frac{x^n-1}{x^n+1} - \frac{x^m-1}{x^m+1}}{1 - \frac{x^n-1}{x^n+1}\frac{x^m-1}{x^m+1}} \\ &\text{On multiplie dénominateur et numérateur par } (x^n+1)(x^m+1) \\ &= \frac{(x^n-1)(x^m+1) - (x^m-1)(x^n+1)}{(x^n+1)(x^m+1) - (x^n-1)(x^m-1)} \\ &= \frac{2x^n - 2x^m}{2x^n + 2x^m} \\ &\text{On factorise puis simplifie par } 2x^m \neq 0 \\ &= \frac{x^{n-m}-1}{x^{n-m}+1} \in H_x \text{ car } n-m \in \mathbb{Z} \end{aligned}$$

Il en résulte que H_x est un sous-groupe de $(I, *)$. *On peut également montrer grâce au calcul précédent que le sous-groupe H_x est monogène et engendré par $\frac{x-1}{x+1}$.*

3. Soit $s \in I \setminus \{0\}$.

   a) On montre le résultat par récurrence sur $\mathbb{N}$.

   — *Initialisation :* on a $s^{[0]} = 0 = \frac{0}{1} = \frac{p_0}{q_0}$. Donc la propriété est vraie au rang $n = 0$.

   — *Hérédité :* Soit $n \in \mathbb{N}$. On suppose que $s^{[n]} = \frac{p_n}{q_n}$. Alors, on a :

$$\begin{aligned} s^{[n+1]} &= s^{[n]} * s \\ &\text{On applique l'hypothèse de récurrence} \\ &= \frac{\frac{p_n}{q_n} + s}{1 + \frac{p_n}{q_n} s} \\ &\text{On multiplie numérateur et dénominateur par } q_n \\ &= \frac{p_n + sq_n}{q_n + sp_n} = \frac{p_{n+1}}{q_{n+1}} \end{aligned}$$

   Ce qui achève le raisonnement par récurrence.

   b) Soit $n \in \mathbb{N}$. On a $sq_n = p_{n+1} - p_n$ donc :

$$sq_{n+1} = s^2 p_n + sq_n = s^2 p_n + p_{n+1} - p_n = p_{n+1} - (1 - s^2)p_n,$$

   et ainsi,

$$p_{n+2} = p_{n+1} + sq_{n+1} = p_{n+1} + p_{n+1} - (1 - s^2)p_n = 2p_{n+1} - (1 - s^2)p_n.$$

   c) L'expression précédente nous donne la suite $(p_n)_{n\in\mathbb{N}}$ sous forme de suite récurrente double. Son équation caractéristique est $r^2 - 2r + (1 - s^2) = 0$ qui possède deux racines réelles distinctes (car $s \neq 0$) : $r_\pm = 1 \pm s$. Ainsi, l'expression explicite de la suite est, pour $n \in \mathbb{N}$,

$$p_n = A(1 - s)^n + B(1 + s)^n \text{ où } A, B \in \mathbb{R}.$$

   Or on a $p_0 = 0$ et $p_1 = p_0 + sq_0 = s$ donc $A = -\frac{1}{2}$ et $B = \frac{1}{2}$. Par suite, pour tout $n \in \mathbb{N}$,

$$p_n = \frac{(1 + s)^n - (1 - s)^n}{2};$$

   puis,

$$q_n = \frac{p_{n+1} - p_n}{s} = \frac{(1 + s)^n + (1 - s)^n}{2}$$

   d) Soit $n \in \mathbb{N}$. Il en résulte de la question précédente que

$$s^{[n]} = \frac{p_n}{q_n} = \frac{(1 + s)^n - (1 - s)^n}{(1 + s)^n + (1 - s)^n}$$

   ou encore, pour $x = \frac{1+s}{1-s}$,

$$s^{[n]} = \frac{x^n - 1}{x^n + 1}$$

   relation toujours vérifiée si $s = 0$ (car dans ce cas $x = 1$).

   On remarque également que cette relation est aussi vérifiée pour tout $n \in \mathbb{Z}$ en utilisant la question 2.d)

4. Soit $x \in \mathbb{R}$. Alors on a, en posant $a = e^{2x} > 0$, $\text{th}(x) = \frac{a^1-1}{a^1+1} \in H_a \subset I$ d'après la question 2.d). Par suite, th est bien une application de $\mathbb{R}$ dans I.
Pour $x, y \in \mathbb{R}$, on a :

$$\begin{aligned}
\text{th}(x) * \text{th}(y) &= \frac{\frac{e^{2x}-1}{e^{2x}+1} + \frac{e^{2y}-1}{e^{2y}+1}}{1 + \frac{e^{2x}-1}{e^{2x}+1}\frac{e^{2y}-1}{e^{2y}+1}} \\
&\text{On multiplie dénominateur et numérateur par } (e^{2x}+1)(e^{2y}+1) \\
&= \frac{(e^{2x}-1)(e^{2y}+1) + (e^{2y}-1)(e^{2x}+1)}{(e^{2x}+1)(e^{2y}+1) + (e^{2x}-1)(e^{2y}-1)} \\
&= \frac{2}{2} \times \frac{e^{2(x+y)}-1}{e^{2(x+y)}+1} \\
\text{th}(x) * \text{th}(y) &= \text{th}(x+y)
\end{aligned}$$

Donc th est un morphisme de groupe de $(\mathbb{R}, +)$ dans $(I, *)$.
De plus, th est continue, strictement croissante sur $\mathbb{R}$ et d'image I donc elle est bijective de $\mathbb{R}$ dans I *(charge au lecteur de montrer tout cela).*
Il en résulte que th est un isomorphisme de groupes.

5. Comme th est un morphisme, on a, pour tout $n \in \mathbb{N}$ et $x \in \mathbb{R}$:

$$\text{th}(nx) = \underbrace{\text{th}(x) * ... * \text{th}(x)}_{n \text{ termes}} = (\text{th}(x))^{[n]} = \frac{(1+\text{th}(x))^n - (1-\text{th}(x))^n}{(1+\text{th}(x))^n + (1-\text{th}(x))^n}$$

Par suite, en utilisant la formule du binôme de Newton et en simplifiant par 2, on trouve :

$$\text{th}(nx) = \frac{\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1} \text{th}(x)^{2k+1}}{\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} \text{th}(x)^{2k}}$$

- $\text{th}(2x) = \frac{2\text{th}(x)}{\text{th}(x)^2+1}$;
- $\text{th}(3x) = \frac{\text{th}(x)^3+3\text{th}(x)}{3\text{th}(x)^2+1}$;
- $\text{th}(4x) = \frac{4\text{th}(x)^3+4\text{th}(x)}{\text{th}(x)^4+6\text{th}(x)^2+1}$;
- $\text{th}(5x) = \frac{\text{th}(x)^5+10\text{th}(x)^3+5\text{th}(x)}{5\text{th}(x)^4+10\text{th}(x)^2+1}$.

Problème 2.

Soit α un complexe. On note $\mathbb{Z}[\alpha] = \{a + b\alpha \mid (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $\mathbb{Z}[\alpha]$ est un sous-anneau de $\mathbb{C}$ si, et seulement si, α est racine d'un polynôme unitaire de degré égal à 2 et à coefficients dans $\mathbb{Z}$.

   Dans la suite, on considère un entier naturel n qui n'est pas le carré d'un entier.

2. Déduire de la question précédente que $\mathbb{Z}[\sqrt{n}]$ est un anneau. Est-il intègre ?

3. Montrer que l'application $\varphi : \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{n}]$ définie par :

$$\varphi : (a, b) \mapsto a + b\sqrt{n},$$

est bijective.

4. Pour $x = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ on note $\tilde{x} = a - b\sqrt{n}$.
Montrer que l'application $f : \mathbb{Z}[\sqrt{n}] \to \mathbb{Z}[\sqrt{n}]$ telle que $f : x \mapsto \tilde{x}$ est un isomorphisme d'anneaux qui vérifie de plus $f^2 = \mathrm{Id}$.

5. Pour $x \in \mathbb{Z}[\sqrt{n}]$, on pose $N(x) = x\tilde{x}$.
Montrer que :
   a) pour tout $x \in \mathbb{Z}[\sqrt{n}]$, $N(x) = 0 \Leftrightarrow x = 0$;
   b) pour tous $x, y \in \mathbb{Z}[\sqrt{n}]$, $N(xy) = N(x)N(y)$.

6. Montrer que x est inversible dans $\mathbb{Z}[\sqrt{n}]$ si, et seulement si, $|N(x)| = 1$.

7. Dans cette question on pose $n = 7$.
   a) Montrer que $8 + 3\sqrt{7}$ est inversible et donner son inverse.
   b) Montrer qu'il existe une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{7}]$.

8. On revient au cas général sur n.
On note G l'ensemble des éléments inversibles de $\mathbb{Z}[\sqrt{n}]$ et G^+ l'ensemble des éléments inversibles positifs de $\mathbb{Z}[\sqrt{n}]$.
   a) Montrer que $(G^+, \times)$ est un groupe.
   b) Soit $x = a + b\sqrt{n} \in G$. Montrer que

$$x \geq 1 \Leftrightarrow (a \geq 1 \text{ et } b \geq 0).$$

   c) Montrer que $\forall M \geq 1$, $G \cap [1, M]$ est fini.
   d) Montrer que $(G^+, \times)$ est monogène.