Corrigé du TD2 - Algèbre Générale 1
L3 S5 - Avignon

Fernando Costa Jr.

EX. 1 Récurrence en n :

$\boxed{n=1}$ vrai par l'hypothèse $ab - ba = \alpha$.

Supposons que $n \in \mathbb{N}^*$ satisfait

$$a^n b - b a^n = \sum_{k=0}^{n-1} a^{n-1-k} \alpha a^k. \qquad (\star)$$

On trouve

$$\begin{aligned} a^{n+1} b - b a^{n+1} &= a a^n b - a b a^n + a b a^n - b a a^n \\ &= a(a^n b - b a^n) + (ab - ba) a^n \\ &\overset{(\star)}{=} a\left(\sum_{k=0}^{n-1} a^{n-1-k} \alpha a^k\right) + \alpha a^n \\ &= \sum_{k=0}^{n-1} a^{(n+1)-1-k} \alpha a^k + \alpha a^n \\ &= \sum_{k=0}^{(n+1)-1} a^{(n+1)-1-k} \alpha a^k. \end{aligned}$$

Par le principe de récurrence, $(\star)$ est vrai pour tous $n \in \mathbb{N}^*$.

$\nexists$

Ex. 2 $\mathbb{D} = \left\{ \frac{n}{10^k} ; n \in \mathbb{Z}, k \in \mathbb{N} \right\}$.

a) On voit que

i) $1 = \frac{1}{10^0} \in \mathbb{D}$

ii) Si $x, y \in \mathbb{D}$, disons $x = \frac{m}{10^k}$ et $y = \frac{n}{10^l}$, $m, n \in \mathbb{Z}, k, l \in \mathbb{N}$

alors

$$x - y = \frac{10^l m - 10^k y}{10^{k+l}} \in \mathbb{D}.$$

iii) Si $x, y \in \mathbb{D}$ sont comme avant, alors

$$x * y = \frac{mn}{10^{k+l}} \in \mathbb{D}.$$

Par conséquent, $\mathbb{D}$ est sous-anneau de $(\mathbb{Q}, +, \times)$.

b) Affirmation: les unités de $\mathbb{D}$ sont les rationnels de la forme $\pm 2^k \cdot 5^l$, $k, l \in \mathbb{Z}$. En effet, pour tous $k, l \in \mathbb{Z}$, si $k, l \in \mathbb{N}$, il est clair que $\pm 2^k 5^l \in \mathbb{D}$: Si $k \in \mathbb{N}$ et $l \in \mathbb{Z} \setminus \mathbb{N}$, alors $2^k 5^l = \frac{2^k}{5^{-l}} = \frac{2^{k-l}}{5^{-l} 2^{-l}} = \frac{2^{k-l}}{10^{-l}} \in \mathbb{D}$.

Pareil si $k \in \mathbb{Z} \setminus \mathbb{N}$ et $l \in \mathbb{N}$ ou si $k, l \in \mathbb{Z} \setminus \mathbb{N}$.

Réciproquement, supposons que $\frac{p}{q}$ est unité de $\mathbb{D}$, $p, q \in \mathbb{Z}^*$.

Alors $\frac{p}{q} = \frac{m}{10^k}$ et $\frac{q}{p} = \frac{n}{10^l}$ pour certains $m, n \in \mathbb{Z}$, $k, l \in \mathbb{N}$. Donc

$1 = \frac{p}{q} \times \frac{q}{p} = \frac{m}{10^k} \cdot \frac{n}{10^l} \Rightarrow mn = 10^{k+l} \Rightarrow m = \pm 2^r 5^s, \forall r, s \in \mathbb{N}$, c'est-à-dire

$$\frac{p}{q} = \frac{n}{10^l} = \pm 2^{r-l} 5^{s-l}, \quad r-l, s-l \in \mathbb{Z}.$$

#

EX.3 a) $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Z}\}$.

On voit que

i) $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

ii) $\forall a,b,c,d \in \mathbb{Z}$, $(a+b\sqrt{2}) - (c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

iii) $\forall a,b,c,d \in \mathbb{Z}$, $(a+b\sqrt{2}) \times (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

Par conséq., $\mathbb{Z}[\sqrt{2}]$ est sous-anneau de $(\mathbb{R}, +, \times)$.

b) Supposons que $a, a', b, b' \in \mathbb{Z}$ ~~tels que~~ satisfont

$$a + b\sqrt{2} = a' + b'\sqrt{2}.$$

Alors,

$$a - a' = (b' - b)\sqrt{2} \in \mathbb{Z} \Rightarrow b' - b = 0 \Rightarrow b = b' \Rightarrow a = a'$$

Cela montre l'unicité de $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.

c) Soient $x, y \in \mathbb{Z}[\sqrt{2}]$, disons $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$.

Alors,

$$\begin{aligned}
N(x \times y) &= N\left((a+b\sqrt{2}) \times (c+d\sqrt{2})\right) \\
&= N\left((ac+2bd) + (ad+bc)\sqrt{2}\right) \\
&= (ac+2bd)^2 - 2(ad+bc)^2 \\
&= a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2 \\
&= a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2) \\
&= (a^2 - 2b^2)(c^2 - 2d^2) = N(x) \cdot N(y).
\end{aligned}$$

Maintenant, supposons que $x = a + b\sqrt{2}$ est unité de $\mathbb{Z}[\sqrt{2}]$. Alors il existe $x^{-1} \in \mathbb{Z}[\sqrt{2}]$ tel que

$x x^{-1} = 1$, d'où

$$N(x) N(x^{-1}) = N(x x^{-1}) = N(1) = 1$$

$$\Rightarrow N(x) = \pm 1 .$$

Réciproquement, supposons que $N(x) = \pm 1$. Si $N(x) = 1$, alors $x = a + b\sqrt{2}$ est unité de $\mathbb{Z}[\sqrt{2}]$ avec

$$x^{-1} = a - b\sqrt{2} .$$

En effet,

$$x x^{-1} = a^2 - 2b^2 = N(x) = 1 .$$

Si $N(x) = -1$, similairement $x^{-1} = -a + b\sqrt{2}$. ※

EX. 4 ① ⓐ On suppose que $x, y \in A$ commutent, donc y commute aussi avec n'importe quelle puissance de x.

Récurrence en n :

$n=1$: trivial

On suppose que $n \in \mathbb{N}^*$ satisfait

$$y^n - x^n = (y-x)\sum_{k=0}^{n-1} x^k y^{n-1-k}. \qquad (\star)$$

Alors,

$$\begin{aligned}
y^{n+1} - x^{n+1} &= y y^n - y x^n + y x^n - x x^n \\
&= y(y^n - x^n) + (y-x)x^n \\
&\overset{(\star)}{=} y(y-x)\sum_{k=0}^{n-1} x^k y^{n-1-k} + (y-x)x^n \\
&\overset{yx=xy}{=} (y-x)\, y \sum_{k=0}^{n-1} x^k y^{n-1-k} + (y-x)x^n \\
&= (y-x)\sum_{k=0}^{n-1} y x^k y^{n-1-k} + (y-x)x^n \\
&\overset{yx^k = x^k y}{=} (y-x)\left(\sum_{k=0}^{n-1} x^k y y^{n-1-k} + x^n\right) \\
&= (y-x)\left(\sum_{k=0}^{n-1} x^k y^{(n+1)-1-k} + x^n\right) \\
&= (y-x)\sum_{k=0}^{(n+1)-1} x^k y^{(n+1)-1-k}.
\end{aligned}$$

Par le principe de récurrence,

$$y^n - x^n = (y-x)\sum_{k=0}^{n-1} x^k y^{n-1-k}, \quad \forall n \in \mathbb{N}^*.$$

ⓑ De $(\star)$, si $y=1$, on trouve

$$1 - x^n = (1-x)\sum_{k=0}^{n-1} x^k 1^{n-1-k} = (1-x)\sum_{k=0}^{n-1} x^k.$$

#

EX. 4 ② $N(A) = \{x \in A : x \text{ nilpotent}\}$.

a) On suppose que x est nilpotent. Alors il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$

D'après ce qu'on a prouvé en 1.b),

$$(1-x)\sum_{k=0}^{n-1} x^k = 1 - x^n = 1,$$

d'où $(1-x)$ est inversible dans $(A, \times)$, où $(1-x)^{-1} = \sum_{k=0}^{n-1} x^k$.

b) On suppose xy nilpotent, donc $\exists n \in \mathbb{N}^*$ tel que $(xy)^n = 0$. Alors

$$(yx)^{n+1} = yx \cdots yx = y(xy \cdots xy)\cdot x = y \cdot 0 \cdot x = 0.$$

Donc yx est aussi nilpotent.

c) Soit A intègre et $x \in N(A)$. Alors il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$,

càd,

$$x \cdots x = x^n = 0.$$

Par l'intégrité de A, on trouve $x = 0$ ou $x = 0$ ou ... ou $x = 0$, donc

$x = 0$, càd, $N(A) = \{0\}$.

EX. 4 ③ Soit $(A, +, \times)$ anneau commutatif.

a) On a toujours $0 \in N(A)$, donc $N(A) \neq \emptyset$. Si $x, y \in N(A)$, alors il existe $n, m \in \mathbb{N}^*$ tels que $x^n = y^m = 0$. Par conséquent,

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$$

$$= \sum_{k=0}^{n-1} \binom{n+m}{k} x^k \underbrace{y^m}_{=0} y^{n-k} + \sum_{k=n}^{n+m} \binom{n+m}{k} \underbrace{x^n}_{=0} x^{k-n} y^{n+m-k} = 0,$$

càd, $x+y \in N(A)$ et, donc, $N(A)$ est stable par la loi de composition de $(A, +)$.

Soit $x \in N(A)$. Alors il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$. Si 1 est l'unité de $(A, +, \times)$, on sait que son opposé -1 satisfait

$$(-1) \times x = -x.$$

Alors,

$$(-x)^n = \big((-1) \times x\big)^n \overset{(A,\times) \text{ commutatif}}{=} (-1)^n \times x^n = (-1)^n \times 0 = 0,$$

d'où $-x \in N(A)$. Par conséquent, $N(A)$ est stable par passage à l'inverse dans $(A, +)$. Ainsi, $N(A)$ est sous-groupe de $(A, +)$.

Maintenant, soit $a \in A$ quelconque. Pour tout $x \in N(A)$, il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$, donc

$$(ax)^n = a^n x^n \overset{(A,\times) \text{ commutatif}}{=} a^n \times 0 = 0,$$

càd, $aN(A) \subset N(A)$ et, donc, $N(A)$ est idéal de $(A, +, \times)$.

b) Supposons que $\bar{x} \in A/N(A)$ est nilpotent. Alors il existe $n \in \mathbb{N}^*$ tel que

$$\begin{aligned}
\bar{x}^n = \bar{0} &\Rightarrow \overline{x^n} = \bar{0} \\
&\Rightarrow x^n - 0 \in N(A) \\
&\Rightarrow x^n \in N(A) \\
&\Rightarrow \exists m \in \mathbb{N}^* : x^{nm} = (x^n)^m = 0 \\
&\Rightarrow x \in N(A) \\
&\Rightarrow \bar{x} = \bar{0}.
\end{aligned}$$

Par conséquent,

$$N\left(A/N(A)\right) = \{\bar{0}\}.$$

#

EX. 4. (4) Soit $A = \mathbb{Z}/72\mathbb{Z}$. D'abord on note que

$$72 = 2 \cdot 36 = 2 \cdot (2 \cdot 3)^2 = 2^3 \cdot 3^2,$$

$$6 = 2 \cdot 3.$$

Alors,

$$\overline{6}^3 = \overline{2^3 \cdot 3^3} = 3 \cdot \overline{2^3 \cdot 3^2} = 3 \cdot \overline{72} = 3 \cdot \overline{0} = \overline{0},$$

d'où $\overline{6} \in N(A)$. Puisque $N(A)$ est idéal, on trouve

$$\{\lambda \overline{6} : \lambda \in \mathbb{Z}\} \subset N(A).$$

Soit $\overline{x} \in N(A)$. Alors il existe $n \in \mathbb{N}^*$ tel que

$$\overline{x^n} = \overline{x}^n = \overline{0} \Rightarrow x^n \in 72\mathbb{Z}$$

$$\Rightarrow x^n = 72k \text{ pour un certain } k \in \mathbb{Z}$$

$$\Rightarrow 2 \mid x^n \text{ et } 3 \mid x^n$$

$$\Rightarrow 2 \mid x \text{ et } 3 \mid x$$

$$\Rightarrow 6 \mid x$$

$$\Rightarrow x \in \{\lambda \times 6 : \lambda \in \mathbb{Z}\}$$

$$\Rightarrow \overline{x} \in \{\lambda \overline{6} : \lambda \in \mathbb{Z}\}.$$

Par conséquent,

$$N(A) = \{\lambda \overline{6} : \lambda \in \mathbb{Z}\}.$$

#

EX. 5

- $(A, +, \times)$ commutatif
- I, J idéaux de A
- $\sqrt{I} := \{x \in A ; \exists n \in \mathbb{N}^*, x^n \in I\}$.

(1) Soient $x, y \in A$ et $m, n \in \mathbb{N}^*$ tels que $x^m, y^n \in I$.

On veut montrer que $x+y \in \sqrt{I}$. On calcule

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}$$

$$= \sum_{k=0}^{m} \binom{m+n}{k} x^k y^{m-k} y^n + \sum_{k=m+1}^{m+n} \binom{m+n}{k} x^{k-m} y^{m+n-k} x^m$$

(nous avons utilisé la commutativité de A dans la dernière somme)

Comme I est idéal et $x^m, y^n \in I$, on a

$$(x^k y^{m-k}) y^n \in I, \forall k = 0, \dots, m, \quad (x^{k-m} y^{m+n-k}) x^m \in I, \forall k = m+1, \dots, m+n$$

Comme tout idéal est aussi sous-groupe, on conclut

$$(x+y)^{m+n} = \sum_{k=0}^{m} \binom{m+n}{k} x^k y^{m-k} y^n + \sum_{k=m+1}^{m+n} \binom{m+n}{k} x^{k-m} y^{m+n-k} x^m \in I$$

$$\Longrightarrow x+y \in \sqrt{I}.$$

Par conséquent, $\sqrt{I}$ est stable pour l'addition.

Maintenant, soient $a \in A$ et $x \in \sqrt{I}$. On veut montrer que $ax \in \sqrt{I}$. En effet, puisque $x \in \sqrt{I}$, il existe $n \in \mathbb{N}^*$ tel que $x^n \in I$. Comme I est idéal, $(ax)^n = a^n x^n \in I$ (on a utilisé la commutativité de A encore une fois). Donc, $ax \in \sqrt{I}$. Par conséquent $\sqrt{I}$ est idéal de $(A, +, \times)$. Comme chaque $x \in I$ satisfait $x^1 \in I$, on a $I \subset \sqrt{I}$

(2) Soit $A = \mathbb{Z}$.

→ $I = 2\mathbb{Z}$. On a

$$x \in \sqrt{I} \Rightarrow \exists n \in \mathbb{N}^* : x^n \in I = 2\mathbb{Z}$$
$$\Rightarrow \exists n \in \mathbb{N}^* : 2 \mid x^n$$
$$\Rightarrow 2 \mid x$$
$$\Rightarrow x \in 2\mathbb{Z}.$$

Donc $\sqrt{I} \subset 2\mathbb{Z} \subset \sqrt{2\mathbb{Z}} \subset I$, c.à.d, $\sqrt{I} = 2\mathbb{Z}$.

→ $I = 8\mathbb{Z} = 2^3\mathbb{Z}$. On a

$$x \in \sqrt{I} \Rightarrow \exists n \in \mathbb{N}^* : x^n \in 8\mathbb{Z}$$
$$\Rightarrow \exists n \in \mathbb{N}^* : 8 \mid x^n \text{ et } 2 \mid 8$$
$$\Rightarrow 2 \mid x$$
$$\Rightarrow x \in 2\mathbb{Z}.$$

Donc $\sqrt{I} \subset 2\mathbb{Z}$. Inversement,

$$x \in 2\mathbb{Z} \Rightarrow x^3 \in 8\mathbb{Z} = I$$
$$\Rightarrow x \in \sqrt{I},$$

donc $\sqrt{I} = 2\mathbb{Z}$.

→ $I = 18\mathbb{Z} = 2 \cdot 3^2\mathbb{Z}$ Devoir.

→ Cas général, $I = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mathbb{Z}$. On trouve

$$x \in \sqrt{I} \Rightarrow \exists n \in \mathbb{N}^*;\ x^n \in I = p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mathbb{Z}$$

$$\Rightarrow \exists n \in \mathbb{N}^*;\ p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mid x^n$$

$$\Rightarrow p_i \mid x,\ \forall i = 1, \dots, n$$

$$\Rightarrow p_1 \cdots p_n \mid x$$

$$\Rightarrow x \in p_1 \cdots p_n \mathbb{Z},$$

d'où

$$\sqrt{p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mathbb{Z}} \subset p_1 \cdots p_n \mathbb{Z}.$$

Réciproquement,

$$x \in p_1 \cdots p_n \mathbb{Z} \Rightarrow x^{\alpha_1 + \cdots + \alpha_n} \in p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mathbb{Z},$$

donc

$$\sqrt{p_1^{\alpha_1} \cdots p_n^{\alpha_n} \mathbb{Z}} = p_1 \cdots p_n \mathbb{Z}. \quad \#$$

(3) L'inclusion $\sqrt{I} \subset \sqrt{\sqrt{I}}$ a été démontrée en (1).
Soit $x \in \sqrt{\sqrt{I}}$. Alors il existe $m \in \mathbb{N}^*$ tel que $x^m \in \sqrt{I}$.
Donc il existe $n \in \mathbb{N}^*$ tel que $x^{mn} = (x^m)^n \in I$. Par définition on trouve $x \in \sqrt{I}$, ce qui montre l'égalité

$$\sqrt{\sqrt{I}} = \sqrt{I}. \qquad (\star)$$

Maintenant, supposons $x \in A/\sqrt{I}$ nilpotent. Alors il existe $n \in \mathbb{N}^*$ tel que $\overline{x^n} = \overline{x}^n = \overline{0}$, càd, $x^n \in \sqrt{I}$. Par définition de radical, $x \in \sqrt{\sqrt{I}} \overset{(\star)}{=} \sqrt{I}$ et, donc $\overline{x} = \overline{0} \in A/\sqrt{I}$. #

(4) On sait que $IJ \subset I \cap J$ (sinon, devoir).
Alors, $\sqrt{IJ} \subset \sqrt{I \cap J}$. On suppose $x \in \sqrt{I \cap J}$.
Donc il existe $n \in \mathbb{N}^*$ tel que $x^n \in I \cap J$. De $x^n \in I$ on conclut $x \in \sqrt{I}$ et de $x^n \in J$ on conclut $x \in \sqrt{J}$.
Autrement dit, $x \in \sqrt{I} \cap \sqrt{J}$, càd, $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.
Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. De $x \in \sqrt{I}$ on trouve $n \in \mathbb{N}^*$ tel que $x^n \in I$. De $x \in \sqrt{J}$ on trouve $m \in \mathbb{N}^*$ tel que $x^m \in J$. Donc

$$x^{m+n} = x^n \cdot x^m \in I \cdot J \Rightarrow x \in \sqrt{IJ}.$$

Autrement dit, $\sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ}$. Cela montre que

$$\sqrt{IJ} \subset \sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J} \subset \sqrt{IJ}.$$

Par conséquent, $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$. #

Ex. 6 $A = (C^\infty(\mathbb{R}), +, \times)$.

(1)

(2) Si f est inversible dans A, alors il existe $g \in A$ telle que $f \cdot g = 1$, càd,

$$f(x) \cdot g(x) = 1, \ \forall x \in \mathbb{R}.$$

En particulier, $f(x) \neq 0$, $\forall x \in \mathbb{R}$. Dans ce cas, la fonction

$$g = \frac{1}{f} : \mathbb{R} \to \mathbb{R}$$

est continue (vous ne savais pas? exercice!) et satisfait

$$f \cdot g = 1.$$

Par conséquent, f est inversible dans A.

(3) $Z(f) := \{x \in \mathbb{R} : f(x) = 0\}$. Soient $f, g \in C^\infty(\mathbb{R})$ telles que $f | g$. Alors il existe $h \in C^\infty(\mathbb{R})$ telle que

$$g(x) = f(x) \cdot h(x), \ \forall x \in \mathbb{R}.$$

Si $x \in Z(f)$, alors $g(x) = f(x)h(x) = 0 \cdot h(x) = 0$, d'où $x \in Z(g)$.

Cela montre que $Z(f) \subset Z(g)$. Autrement dit,

$$f | g \text{ dans } A \implies Z(f) \subset Z(g).$$

L'implication inverse est fausse. Prenons comme contre-exemple $f(x) = x^2$ et $g(x) = x$, $x \in \mathbb{R}$. Alors $Z(f) = Z(g) = \{0\}$. Par contre, pour $x \neq 0$ on a $\frac{g(x)}{f(x)} = \frac{x}{x^2} = \frac{1}{x}$, donc si $h : \mathbb{R} \to \mathbb{R}$ satisfait $g = f \cdot h$, alors h est forcément discontinue en $x = 0$.

(4) Pour $B \subset \mathbb{R}$, on définit

$$I(B) = \{f \in C^\infty(\mathbb{R}) : f(x) = 0, \forall x \in B\}.$$

On montre que cela est idéal de $C^\infty(\mathbb{R})$. Soient $f, g \in I(B)$. Alors, pour tout $x \in B$, $(f+g)(x) = f(x) + g(x) = 0 + 0 = 0$, donc $f+g \in I(B)$. Soient $f \in C^\infty(\mathbb{R})$ et $g \in I(B)$. Alors, pour tout $x \in B$, comme $g(x) = 0$, on trouve

$$(fg)(x) = f(x) \cdot g(x) = f(x) \cdot 0 = 0.$$

Donc, $fg \in I(B)$. Par conséquent, $I(B)$ est idéal de $C^\infty(\mathbb{R})$

(5) On raisonne par l'absurde et on suppose que, même sous les hypothèse

$$B \neq \emptyset \quad \text{et} \quad \overline{B} \neq \mathbb{R}, \tag{$\star$}$$

l'idéal $I(B)$ est principal. Alors il existe $g \in C^\infty(\mathbb{R})$ telle que $I(B) = gC^\infty(\mathbb{R}) = \{gf : f \in C^\infty(\mathbb{R})\}$. On suit la suggestion de l'énoncé et on définit

$$f := g^{\frac{1}{3}} : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto f(x) = \sqrt[3]{g(x)}.$$

Puisque, pour tout $x \in B$,

$$f(x) = \sqrt[3]{g(x)} = \sqrt[3]{0} = 0,$$

on trouve $f \in I(B)$, donc il existe $h \in C^\infty(\mathbb{R})$ telle que $f = gh$. Cette égalité implique la propriété suivante:

$$f = gh \Rightarrow \sqrt[3]{g(x)} = g(x)h(x), \forall x \in \mathbb{R}$$
$$\Rightarrow h(x) = g(x)^{\frac{1}{3}-1}, \forall x \notin Z(g)$$
$$\Rightarrow h(x) = \frac{1}{\sqrt[3]{g(x)^2}}, \forall x \notin Z(g). \tag{1}$$

← complémentaire

On sait aussi que $Z(g)^c \neq \emptyset$, car sinon $Z(g)^c = \emptyset$ implique $Z(g) = \mathbb{R}$, càd $g \equiv 0$, ou encore $I(B) = gC^\infty(\mathbb{R}) = \{0\}$, ce qui est impossible car B n'est pas dense dans $\mathbb{R}$. Alors, si l'on fixe $x \in \partial(Z(g))$, on sait que $x \in Z(g)$ car

↑ frontière

g continue $\Rightarrow Z(g)$ fermé et on peut trouver $(x_n)_n$ suite d'éléments de $Z(g)^c$ telle que $x_n \longrightarrow x$. (Ici $Z(g)^c \neq \emptyset$ est fondamental). Puisque h est continue, on sait que

$$h(x) = \lim_{n \to +\infty} h(x_n). \tag{2}$$

Par contre, puisque $g(x_n) \neq 0$ pour tout $n \in \mathbb{N}$ et $g(x) = 0$,

$$\lim_{n \to +\infty} h(x_n) = \lim_{n \to +\infty} \frac{1}{\sqrt[3]{g(x_n)^2}} = +\infty. \tag{3}$$

Les lignes (2) et (3) étant contradictoires, on conclut que $I(B)$ n'est pas principal.

EX.7 Solution facile: Soit $a \in A \setminus \{0\}$. Vu que A est fini, la liste

$$a, a^2, a^3, \dots$$

est finie, donc il existe $m > n$ tels que $a^m = a^n$.

Par conséquent,

$$a^m - a^n = 0 \Rightarrow a^n (a^{m-n} - 1) = 0$$

$$\overset{a \neq 0 \text{ A intègre}}{\Longrightarrow} a^{m-n} - 1 = 0$$

$$\Rightarrow a\, a^{m-n-1} = a^{m-n-1}\, a = 1,$$

càd, a est inversible, donc A est corps.

Devoir: Résoudre en appliquant la suggestion.

→ $g_a : x \mapsto ax$, $\ker(g_a) = \{0\} \Rightarrow g_a$ injective

→ A fini, g_a injective $\Rightarrow g_a$ surjective

$\Rightarrow \exists x \in A^* : ax = 1$

→ Similairement, $\exists y \in A^*$ tel que $ya = 1$, dbù

$ya = 1 \Rightarrow y\overset{=1}{\widehat{ax}} = x \Rightarrow y = x$.

EX. 8

Dans $(\mathbb{R}[X], +, \times)$ on pose

$$I = (X^2+1)\mathbb{R}[X].$$

a) Soit $F : P \mapsto P(i)$ de $\mathbb{R}[X]$ dans $\mathbb{C}$.

On vérifie que F est un morphisme :

$\longrightarrow$ L'application est clairement bien définie

$\forall P, Q \in \mathbb{R}[X] \rightarrow F(P+Q) = (P+Q)(i) = P(i) + Q(i) = F(P) + F(Q)$

$\longrightarrow F(P \cdot Q) = (PQ)(i) = P(i)\,Q(i) = F(P)\,F(Q)$

$\longrightarrow 1_{\mathbb{R}[X]} : X \mapsto 1$, $1_{\mathbb{C}} = 1$.

$\Rightarrow F(1_{\mathbb{R}[X]}) = 1_{\mathbb{R}[X]}(i) = 1 = 1_{\mathbb{C}}$.

Par conséquent, F est morphisme d'anneaux.

Étant donné $z \in \mathbb{C}$, disons $z = a+bi, a,b \in \mathbb{R}$, on considère $P(X) = a + bX$. Alors

$$F(P) = P(i) = a + bi = z.$$

Par conséquent, F est surjectif.

b) Puisque $F(X^2+1) = i^2+1 = 0$, on obtient $X^2+1 \in \ker F$ et donc $I \subset \ker F$. Soit $P \in \ker F$. Alors $P(i) = 0$. Puisque les coefficients de P sont réels, on a aussi $P(-i) = P(\bar{i}) = 0$. On peut donc factoriser

$$P(X) = (X-i)(X+i)Q(X) = (X^2+1)Q(X),$$

où $Q(X)$ n'a que des coefficients réels (sinon $(X^2+1)Q(X) = P(X)$ aurait des coefficients complexes).

Par conséquent,

$$P \in (X^2+1)\mathbb{R}[X] = I.$$

Cela montre que

$$\ker F = I.$$

c) D'après le Théorème de Factorization, $\mathbb{R}[X]/I = \mathbb{R}[X]/\ker F$ est isomorphe à $\mathbb{C}$. Étant ce dernier un corps, on conclut que $(\mathbb{R}[X]/I, +, \times)$ est lui aussi un corps.

EX.9.1

a) On affirme que $A = \mathbb{Z}[i]$.

En effet, $\mathbb{Z}[i]$ est clairement sous-anneau de $(\mathbb{C}, +, \times)$ contenant i. Supposons que A' est un autre sous-anneau de $(\mathbb{C}, +, \times)$ contenant i. Alors $0, 1, i \in A'$, d'où $m = 1 + \overset{m}{\cdots} + 1 \in A$ et $ni = i + \overset{n}{\cdots} + i \in A'$ pour tout $m, n \in \mathbb{N}$. Les opposés de ces éléments appartiennent aussi à A', c'à d, $m \in A'$ et $ni \in A'$ pour tous $m, n \in \mathbb{Z}$. Donc, $m + in \in A'$, pour tous $m, n \in \mathbb{Z}$, c'à d, $\mathbb{Z}[i] \subset A'$. Cela montre que $\mathbb{Z}[i]$ est le plus petit sous-anneau de $(\mathbb{C}, +, \times)$ contenant i, ce qu'on voulait montrer.

b) Un calcul pas très compliqué montre que les seules unités de $\mathbb{Z}[i]$ sont ± 1 et $\pm i$. (Devoir)

Si $m + ni$ est inversible, il existe $p, q \in \mathbb{Z}$ tq $(m+ni)(p+qi) = 1 \Rightarrow \begin{cases} ma - nb = 1 \\ na + mb = 0 \end{cases}$. Les seules solutions de ce système dans $\mathbb{Z}$ sont $n = 0$ et $m = \pm 1$ ou $m = 0$ et $n = \pm 1$.

EX. 9.2 Soit B le sous-corps de $(\mathbb{C}, +, \times)$ engendré par i. On affirme que

$$B = \mathbb{Q}[i].$$

En effet, $\mathbb{Q}[i]$ est clairement sous-corps de $(\mathbb{C}, +, \times)$ contenant i. Soit B' un sous-corps de $(\mathbb{C}, +, \times)$ contenant i. On montre que $B' \supset B$. Soit donc $a+bi$ un élément de $\mathbb{Q}[i]$, disons $a = \frac{p}{q}$ et $b = \frac{r}{s}$, avec $p, q, r, s \in \mathbb{Z}$, $q, s \neq 0$. Puisque B' contient 1, il contient aussi q, d'où $\frac{1}{q} = q^{-1} \in B'$. Par l'addition on a $\frac{p}{q} = \frac{1}{q} + \cdots + \frac{1}{q} \in B'$. Similairement, puisque $i \in B'$, on a $-i \in B'$ et donc $-si = (-i) + \cdots + (-i) \in B'$. Cela implique que $(-si)^{-1} = \frac{1}{s} i \in B'$. Par l'addition on obtient $\frac{r}{s} i = \frac{1}{s} i + \cdots + \frac{1}{s} i \in B'$. Par conséquent,

$$a + bi = \frac{p}{q} + \frac{r}{s} i \in B' \Rightarrow B \subset B'.$$

Cela complète la preuve.