Structures algébriques

Groupes, sous-groupes, morphismes de groupe

Exercice 1. *Groupe symétrique.*

On note S_n l'ensemble des bijections de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, n\}$.

1. Rappeler combien il y a d'éléments dans S_n, puis décrire S_1, S_2, S_3 et S_4.
2. Rappeler pourquoi $(S_n, \circ)$ est un groupe, non commutatif pour $n \geqslant 3$.
3. Donner tous les sous-groupes de S_3.

Exercice 2. *Centre d'un groupe.*

Soit $(G, *)$ un groupe, on considère $C = \{h \in G,\ \forall g \in G,\ h * g = g * h\}$.

Classiquement, C est appelé le ***centre*** *de G.*

1. Que peut-on dire de C si le groupe G est commutatif ?
2. Dans le cas général, montrer que C est un sous-groupe de G.
3. Déterminer C lorsque $(G, *) = (S_3, \circ)$. Généralisation ?
4. Déterminer C lorsque $(G, *) = (GL_2(\mathbb{K}), \times)$. Généralisation ?
   Indication : considérer les matrices de la forme $I_n + E_{i,j}$.

Exercice 3. *Morphismes, noyaux, images.*

Montrer que chacune des applications suivantes est un morphisme de groupes (en précisant les lois considérées). Déterminer leur noyau et leur image. Sont-ils injectifs ? surjectifs ?

$$f : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{C}^\times \\ k & \mapsto & e^{\frac{2ik\pi}{n}} \end{array} \right. \qquad g : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & \mathrm{i}x \end{array} \right. \qquad h : \left\{ \begin{array}{ccc} \mathbb{C}^\times & \to & \mathbb{C}^\times \\ z & \mapsto & z^n \end{array} \right. \qquad \tilde{h} : \left\{ \begin{array}{ccc} \mathbb{R}^\times & \to & \mathbb{R}^\times \\ z & \mapsto & z^n \end{array} \right.$$

Anneaux, sous-anneaux, morphismes d'anneaux

Exercice 4. *Anneaux / pas anneaux.*

Parmi les ensembles munis de deux lois suivants, déterminer lesquels sont des anneaux. Pour ces derniers : déterminer leurs inversibles, lesquels sont des anneaux commutatifs, lesquels sont des anneaux intègres, lesquels sont des corps.

1. $(\mathbb{R}^3, +, \wedge)$, où $\wedge$ est le produit vectoriel.
2. $(\mathbb{C}^{\mathbb{N}}, +, \times)$.
3. $(\mathbb{Z}[i], +, \times)$, où $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$.
4. $(\mathbb{D}, +, \times)$, où $\mathbb{D} = \left\{ \dfrac{n}{10^k}, (n, k) \in \mathbb{Z} \times \mathbb{N} \right\}$ est l'ensemble des nombres décimaux.
5. $(\mathcal{P}(E), \cup, \cap)$ où E est un ensemble.
6. $(\mathcal{P}(E), \Delta, \cap)$ où E est un ensemble.

Exercice 5. *Anneaux de Boole*

On dit que $(A, +, \times)$ est un anneau de Boole si c'est un anneau non nul dans lequel tout élément est idempotent pour la deuxième loi, ce qui signifie : $\forall x \in A,\ x^2 = x$. Dans cet exercice, on étudie quelques résultats vérifié par un anneau de Boole A.

1. Montrer qu'on a $\forall (x, y) \in A^2,\ xy + yx = 0_A$ et en déduire : $\forall x \in A,\ x + x = 0_A$.
   En déduire que l'anneau A est commutatif.
2. Montrer que la relation binaire définie sur A par $x \preccurlyeq y \Leftrightarrow yx = x$ est une relation d'ordre.
3. Montrer qu'on a $\forall (x, y) \in A^2,\ xy(x + y) = 0_A$.
   En déduire tous les anneaux de Boole intègres.
4. Donner d'autres exemples d'anneaux de Boole.

Structures algébriques

Groupes, sous-groupes, morphismes de groupe

Exercice 1. *Groupe symétrique.*

On note S_n l'ensemble des bijections de $\{1, 2, \dots, n\}$ dans $\{1, 2, \dots, n\}$.

1. Rappeler combien il y a d'éléments dans S_n, puis décrire S_1, S_2, S_3 et S_4.

   Tout est dans le cours sauf la description de S_4. Pour cela, un peu de terminologie : on appelle 2-cycle une transposition. On appelle 3-cycle une permutation de la forme $i \mapsto j \mapsto k \mapsto i$, $l \mapsto l$, où i, j, k et l sont tels que $\{1, 2, 3, 4\} = \{i, j, k, l\}$. Enfin, on appelle 4-cycle une permutation de la forme $i \mapsto j \mapsto k \mapsto l \mapsto i$, où i, j, k et l sont tels que $\{1, 2, 3, 4\} = \{i, j, k, l\}$. Ici c'est fini car $n = 4$ mais on pourrait de même définir dans S_n des p-cycles pour $p\{2, \dots, n\}$.

   Qui sont les 24 éléments de S_4 ? On compte :
   - Il y a l'identité qui est toute seule.
   - Les transpositions qui sont au nombre de $\binom{4}{2} = 6$.
   - Les 3-cycles qui sont au nombre de $\binom{4}{3} \times 2! = 8$.
   - Les 4-cycles qui sont au nombre de $\binom{4}{4} \times 3! = 6$.
   - Et on voit qu'il ne manque plus que trois permutations.
     Ce sont les **doubles transpositions** $\tau_{i,j} \circ \tau_{k,l}$ (avec $\{1, 2, 3, 4\} = \{i, j, k, l\}$) qui sont bien au nombre de 3.

2. Rappeler pourquoi $(S_n, \circ)$ est un groupe, non commutatif pour $n \geqslant 3$.

   C'est un groupe car :
   - Il y a bien dans S_n un élément neutre pour $\circ$: c'est id, qui est bien une bijection.
   - Toute permutation $\sigma \in S_n$ a bien un symétrique pour $\circ$: sa réciproque σ^{-1} qui est bien une bijection.
   - $\circ$ est bien associative.

   De plus :
   - Pour $n \geqslant 3$ on peut définir les éléments remarquables $\tau_{1,2}$ et $\tau_{2,3}$ de S_n.
     On a $\tau_{1,2} \circ \tau_{2,3}(1) = 2 \neq 3 = \tau_{2,3} \circ \tau_{1,2}(1)$ donc $\tau_{1,2}$ et $\tau_{2,3}$ ne commutent pas, donc $(S_n, \circ)$ n'est pas commutatif.

   À noter : pour $n \in \{0, 1\}$ on a $S_n = \{\mathrm{id}\}$ (c'est "le" groupe trivial) qui est commutatif et pour $n = 2$ on a $S_2 \simeq \mathbb{Z}/2\mathbb{Z}$ qui est commutatif.

3. Donner tous les sous-groupes de S_3.

   Un tel sous-groupe G comprend id.
   • Premier cas : et personne d'autre. Auquel cas $G = \{\mathrm{id}\}$. C'est bien un sous-groupe.
   • Second cas : et une transposition $\tau_{i,j}$, et personne d'autre. Auquel cas $G = \{\mathrm{id}, \tau_{\mathrm{i,j}}\}$. C'est bien un sous-groupe. Il y a $\binom{3}{2} = 3$ choix possibles pour i et j donc 3 tels sous-groupes.
   • Troisième cas : et une transposition, et une troisième permutation. Quel que soit le choix de la troisième permutation (il y a quatre choix possible), la stabilité par produit (ici le produit c'est la composition) permet de proche en proche de voir que toutes les permutations sont dans G. Dans ce cas on a donc $G = S_3$. C'est bien un sous-groupe.
   • Dernier cas : G n'est pas trivial, mais ne comprend pas de transposition. Dans ce cas par stabilité par produit on a nécessairement $G = \{\mathrm{id}, c, c^{-1}\}$. C'est bien un sous-groupe.

   Total : $1 + 3 + 1 + 1 = 6$ sous-groupes.

EXO STRUCT ALG

2/1 Supposons $(G, *)$ commutatif.

$\forall a, b \in G,\ a * b = b * a$

Donc $C \subset G$

Or $G \subset C$ par définition

Donc $G = C$

2/2 Soit $x, y \in C$

- Montrons $0_G \in C$ ie $\forall g \in G,\ g * 0_G = 0_G * g$
  Soit $g \in G$. On a $g * 0_G = g = 0_G * g$

- Montrons $x * y \in C$
  On a $x * (y * g) = x * y * g$ par assoc
  $= y * g * x$ par commutativité car $y, g, x \in C$
  $= (y * g) * x$ par assoc

- Mq $x^{-1} \in C$

$x * y = y * x \Rightarrow x * y * x^{-1} = y * x * x^{-1}$

$= y$

$\Rightarrow x^{-1} * x * y * x^{-1} = x^{-1} * y$

$\Rightarrow y * x^{-1} = x^{-1} * y$ donc $x^{-1} \in C$

2/3

$$C = \{ f \in S_3,\ \forall \sigma \in S_3,\ f \circ \sigma = \sigma \circ f \} = \{ id \}$$

$\subset$: ok car C est un sous-groupe

$\supset$:

- τ_{12} ne commute pas avec τ_{23} car $\begin{cases} \tau_{12} \circ \tau_{23} = c \\ \tau_{23} \circ \tau_{12} = c^{-1} \end{cases}$
- τ_{23} ——— τ_{12}
- τ_{13} ——— τ_{23}
- c ——— τ_{12} car $\begin{cases} c \circ \tau_{12} = \tau_{13} \\ \tau_{12} \circ c = \tau_{23} \end{cases}$
- c^{-1} ——— τ_{12} car $\begin{cases} c^{-1} \circ \tau_{12} = \tau_{23} \\ \tau_{12} \circ c^{-1} = \tau_{13} \end{cases}$

donc $\{ \tau_{12}, \tau_{23}, \tau_{13}, c, c^{-1} \} \not\subset C$

donc $C \subset \{ id \}$

Généralisation $(G, *) = (S_n, \circ) \Rightarrow C = \{ id \}$ pour $n \geq 3$

$\supset$: ok !

$\subset$: Soit $f \in C$. Montrons $f = id$ par l'absurde.
Supp qu'il existe $i \in [\![1, n]\!]$ tel que $f(i) \neq i$

$n \geq 3$ donc il existe $k \in [\![1, n]\!] \setminus \{ i, f(i) \}$

On sait que $f \circ \tau_{ik} = \tau_{ik} \circ f$ puisque $f \in C$

Donc en particulier $f \circ \tau_{ik}(i) = \tau_{ik} \circ f(i)$

Or $f(i) \notin \{i, k\}$ donc $\tau_{ik} \circ f(i) = f(i)$

et $f \circ \tau_{ik}(i) = f(k)$

donc $f(i) = f(k)$

donc $i = k$ car $f \in$ [illegible]

IMH

2/4 $GL_2(\mathbb{K}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ ad - bc \neq 0 \right\}$

$(G, *) := (GL_2(\mathbb{K}), \times)$

Montrons $C = \mathbb{K} I_2$

Analyse : Considérons une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ convenable.

En particulier, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{I_2 + E_{1,2}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} a & (a+b) \\ c & (c+d) \end{pmatrix} = \begin{pmatrix} (a+c) & (b+d) \\ c & d \end{pmatrix}$$

$$\Leftrightarrow \begin{cases} a = a+c \\ a+b = b+d \\ c = c \\ c+d = d \end{cases} \Leftrightarrow \begin{cases} c = 0 \\ a = d \end{cases}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \times \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Leftrightarrow \begin{matrix} (a+b) & b \\ (c+d) & d \end{matrix} = \begin{matrix} a & b \\ (a+c) & (b+d) \end{matrix}$$

$$\Leftrightarrow \begin{cases} a+b = a \\ b = b \\ c+d = a+c \\ d = b+d \end{cases} \Leftrightarrow \begin{cases} b = 0 \\ a = d \end{cases}$$

Ainsi, $a=d$ et $b=c=0$ donc

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est de la forme $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2$

Candidats $\mathbb{K}I_2$ (car $a \in \mathbb{K}$)

Synthèse: ok!

Généralisation pour $(G, *) := (GL_n(\mathbb{K}), \times)$

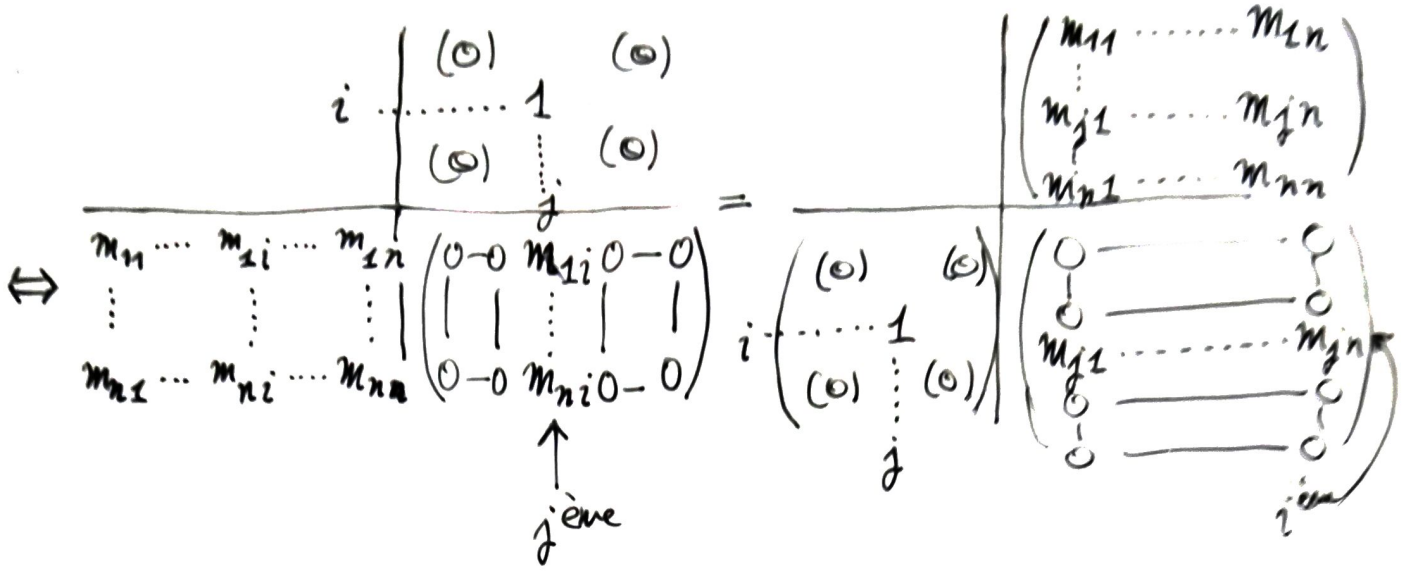
Mq on a encore $C = \mathbb{K}I_n$

Analyse Considérons une matrice $M := (m_{ij})_{ij}$ convenable

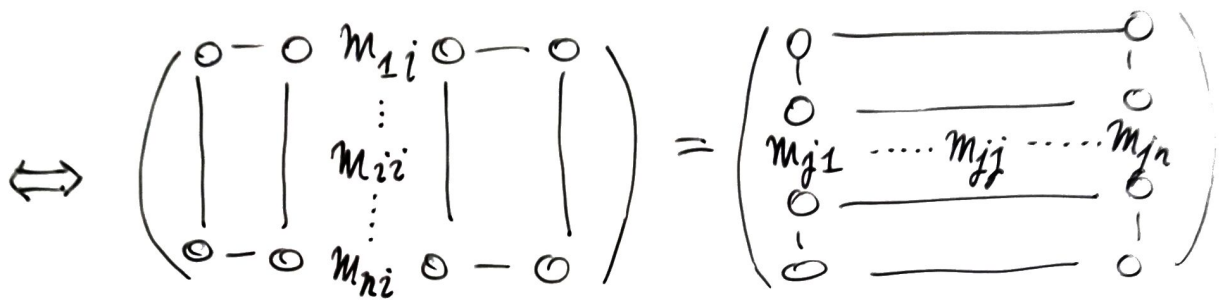
Pour $i \neq j$, on a

$$M(I_n + E_{ij}) = (I_n + E_{ij})M$$

$$\Leftrightarrow \cancel{M} + ME_{ij} = \cancel{M} + E_{ij}M$$



$\Leftrightarrow$



$\Rightarrow$ $\forall i \neq j,\ m_{ii} = m_{jj}$ et tout les coefficients non-diagonaux sont nuls

Donc $M \in \mathbb{K} I_n$

Synthèse : OK !

EXM STRUCTALG

3/f

Soient $k_1, k_2 \in \mathbb{Z}$

$$f(k_1 + k_2) = e^{\frac{2i}{n}(k_1+k_2)\pi}$$
$$= e^{\frac{2i\pi}{n}k_1} e^{\frac{2i\pi}{n}k_2}$$
$$= f(k_1) \cdot f(k_2)$$

$$\mathrm{Ker}(f) = (k \mapsto e^{\frac{i2\pi}{n}k})^{\leftarrow}(\{1\})$$
$$= \{k \in \mathbb{Z},\ e^{\frac{i2\pi}{n}k} = 1\}$$
$$= \{k \in \mathbb{Z},\ \frac{2\pi k}{n} \equiv 0\ [\pi]\}$$
$$= \{k \in \mathbb{Z},\ k \equiv 0\ [n]\}$$
$$= \{k \in \mathbb{Z},\ n \mid k\}$$
$$= n\mathbb{Z}$$
$$\neq \{0\} \quad \text{car } n \neq 0$$

$\Rightarrow f \notin \mathcal{GO}$

$$\mathrm{Im}(f) = \{f(k),\ k \in \mathbb{Z}\}$$
$$= \{e^{\frac{2ik\pi}{n}},\ k \in \mathbb{Z}\}$$
$$= \mathbb{U}_n$$
$$\neq \mathbb{C}^\times$$

$\Rightarrow f \notin \mathcal{GO}$

EXM STRUCTALG

3/g

$$\begin{cases} (\mathbb{R}, +) \longrightarrow (\mathbb{C}, +) \\ x \longmapsto ix \end{cases}$$

Soient $x, y \in \mathbb{R}$

$$g(x+y) = i(x+y)$$
$$= ix + iy \qquad \text{distributivité}$$
$$= g(x) + g(y)$$

donc c'est bien un morphisme

$$\text{Ker}(g) = \{x \in \mathbb{R},\ g(x) = 0\}$$
$$= \{x \in \mathbb{R},\ ix = 0\}$$
$$= \{0\}$$
$$\Rightarrow g \in \text{⊖⊖}$$

$$\text{Im}(g) = (i\,\text{id}_{\mathbb{R}})^{\rightarrow}(\mathbb{R}) = i\mathbb{R} \neq \mathbb{C} \Rightarrow g \notin \text{⊖⊖}$$

3/h

$$h : \begin{cases} (\mathbb{C}^\times, \times) \longrightarrow (\mathbb{C}^\times, \times) \\ z \longmapsto z^n \end{cases}$$

Soient $z_1, z_2 \in \mathbb{C}^\times$. On a:

$$h(z_1 \times z_2) = (z_1 \times z_2)^n = z_1^n \times z_2^n = h(z_1) \times h(z_2)$$

donc c'est un morphise

$$\mathrm{Ker}(h) = \{z \in \mathbb{C}^\times,\ h(z) = 1\}$$

$$= \{z \in \mathbb{C}^\times,\ z^n = 1\}$$

$$= \mu_n \begin{cases} \neq \{1\} \Rightarrow h \notin \mathcal{C}^\infty & \text{si } n \neq 1 \\ = \{1\} \Rightarrow h \in \mathcal{C}^\infty & \text{sinon} \end{cases}$$

$$\mathrm{Im}(h) = \mathrm{id}^n \to (\mathbb{C}^\times)$$

$$\begin{cases} = \mathbb{C}^\times & \text{si } n \neq 0 \\ = \{1\} & \text{sinon} \end{cases}$$

$$\Rightarrow \begin{cases} h \in \mathcal{C}^\infty & \text{si } n \neq 0 \\ h \notin \mathcal{C}^\infty & \text{sinon} \end{cases}$$

4/ $\tilde{h}$ C'est pareil

$$\mathrm{Ker}(\tilde{h}) = \{x \in \mathbb{R}^\times,\ h(x) = 1\}$$

$$= \{x \in \mathbb{R}^\times,\ x^n = 1\}$$

$$= \begin{cases} \{1\} & \text{si } n \in 2\mathbb{N}^\times \\ \pm 1 & \text{si } n \in 2\mathbb{N}+1 \\ \mathbb{R}^\times & \text{sinon} \end{cases}$$

$$\Rightarrow \left(\tilde{h} \in \mathcal{C}^\infty \Leftrightarrow n \in 2\mathbb{N}+1 \right)$$

$$\mathrm{Im}(\tilde{h}) = \mathrm{id}^{n}_{\mathbb{R}^\times}(\mathbb{R}^\times)$$

$$= \begin{cases} \mathbb{R}^\times & \text{si } n \in 2\mathbb{N}+1 \\ \mathbb{R}_+^\times & \text{si } n \in 2\mathbb{N}^\times \\ \{1\} & \text{sinon} \end{cases}$$

$$\Rightarrow \left(\tilde{h} \in \mathcal{GD} \iff n \in 2\mathbb{N}+1\right)$$

8

$$\phi : \begin{cases} (\mathbb{R}[X], +, \times) \longrightarrow (\mathbb{C}, +, \times) \\ P(X) \longmapsto P(i) \end{cases}$$

Mq $\begin{cases} \forall P, Q \in \mathbb{R}[X],\ \phi(P+Q) = \phi(P) + \phi(Q) \\ \forall P, Q \in \mathbb{R}[X],\ \phi(P \times Q) = \phi(P) \times \phi(Q) \\ \phi(1_{\mathbb{R}[X]}) = 1_{\mathbb{C}} \end{cases}$

Soient $P, Q \in \mathbb{R}[X]$. Soit $\square \in \{+, \times\}$

$$\phi(P \square Q) = (P \square Q)(i)$$
$$= P(i) \square Q(i)$$
$$= \phi(P) \square \phi(Q)$$

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

Exercice 4. *Anneaux / pas anneaux.*

Parmi les ensembles munis de deux lois suivants, déterminer lesquels sont des anneaux. Pour ces derniers : déterminer leurs inversibles, lesquels sont des anneaux commutatifs, lesquels sont des anneaux intègres, lesquels sont des corps.

1. $(\mathbb{R}^3, +, \wedge)$, où $\wedge$ est le produit vectoriel.

   Ce n'est pas un anneau, par exemple parce que $\wedge$ n'est pas associatif.

2. $(\mathbb{C}^{\mathbb{N}}, +, \times)$.

   Déjà vu dans le cours sur les suites (pour $\mathbb{K} = \mathbb{R}$, mais pour $\mathbb{K} = \mathbb{C}$ ou plus généralement pour $\mathbb{K}$ un corps, c'est la même chose) : c'est un anneau commutatif mais non intègre dont les inversibles sont les suites qui ne s'annulent pas.

3. $(\mathbb{Z}[i], +, \times)$, où $\mathbb{Z}[i] = \{a + ib,\ (a, b) \in \mathbb{Z}^2\}$.

   $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$, donc $(\mathbb{Z}[i], +, \times)$ est un anneau commutatif et intègre (car $(\mathbb{C}, +, \times)$ est commutatif est intègre). Montrons que $\mathbb{Z}[i]$ est bien un sous anneau de $(\mathbb{C}, +, \times)$:

   - $0 = 0 + 0\mathrm{i} \in \mathbb{Z}[i]$ et $1 = 1 + 0\mathrm{i} \in \mathbb{Z}[i]$ car $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ sont bien dans $\mathbb{Z}^2$.
   - Soient $a + \mathrm{i}b$ et $c + \mathrm{i}d$ dans $\mathbb{Z}[i]$ (*i. e.* $a, b, c, d \in \mathbb{Z}$) on a :
     - $(a + \mathrm{i}b) + (c + \mathrm{i}d) = (a + c) + \mathrm{i}(b + d) \in \mathbb{Z}[i]$ car $\begin{pmatrix} a + c \\ b + d \end{pmatrix} \in \mathbb{Z}^2$ car $(\mathbb{Z}, +)$ est un groupe.
     - $(a + \mathrm{i}b)(c + \mathrm{i}d) = (ac - bd) + \mathrm{i}(ad + bc) \in \mathbb{Z}[i]$ car $\begin{pmatrix} ac - bd \\ ad + bc \end{pmatrix} \in \mathbb{Z}^2$ car $(\mathbb{Z}, +, \times)$ est un anneau.
   - Enfin soit $a + \mathrm{i}b$ dans $\mathbb{Z}[i]$ (*i. e.* $a, b \in \mathbb{Z}$) on a : $-(a + \mathrm{i}b) = (-a) + \mathrm{i}(-b) \in \mathbb{Z}[i]$ car $\begin{pmatrix} -a \\ -b \end{pmatrix} \in \mathbb{Z}^2$ car $(\mathbb{Z}, +)$ est un groupe.

   Reste à déterminer les inversibles.
   • Pour tout $z = a + \mathrm{i}b \in \mathbb{Z}[i]$, notons $N(z) = |z|^2 = a^2 + b^2$.

   • Soit $z \in \mathbb{Z}[\mathrm{i}]$ et supposons z inversible, c'est-à-dire $z^{-1} \in \mathbb{Z}[\mathrm{i}]$. On a alors $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$ par propriétés sur le module. Par conséquent $N(z)$ est un entier naturel qui divise 1, c'est donc 1.

   • Montrons maintenant léquivalence demandée : soit $z \in \mathbb{Z}[\mathrm{i}]$ et notons $z = a + \mathrm{i}b$. Si $z^{-1} \in \mathbb{Z}[\mathrm{i}]$, on a $N(z) = 1$, ce qui s'écrit $a^2 + b^2 = 1$. Si $|a| \geqslant 2$ ou $|b| \geqslant 2$, on a $a^2 + b^2 \geqslant 4$, ces cas sont donc exclus. Si $|a| = |b| = 1$, on a $a^2 + b^2 = 2$, ce cas est donc exclus. C'est donc qu'on a $|a| = 1,\ |b| = 0$ ou $|a| = 0,\ |b| = 1$, ou encore $z \in \mathbb{U}_4$.
   Réciproquement, si on a $z \in \mathbb{U}_4$, on a $z^{-1} \in \mathbb{U}_4 \subset \mathbb{Z}[\mathrm{i}]$ puisqu'on a $1 = 1 \times 1 = (-1) \times (-1) = \mathrm{i} \times (-\mathrm{i}) = (-\mathrm{i}) \times \mathrm{i}$.

4. $(\mathbb{D}, +, \times)$, où $\mathbb{D} = \left\{ \dfrac{n}{10^k}, (n, k) \in \mathbb{Z} \times \mathbb{N} \right\}$ est l'ensemble des nombres décimaux.

   C'est un sous-anneau de $(\mathbb{R}, +, \times)$ (la vérification est immédiate) donc un anneau commutatif et intègre.

   Les inversibles : un décimal $d = \frac{m}{10^k}$ ($m \in \mathbb{Z}$, $k \in \mathbb{N}$) est inversible si et seulement si $\frac{10^k}{m} \in \mathbb{D}$ *i. e.* si et seulement si $\exists m' \in \mathbb{Z},\ k' \in \mathbb{N},\ \frac{10^k}{m} = \frac{m'}{10^{k'}}$ *i. e.* si et seulement si $\exists m' \in \mathbb{Z},\ k' \in \mathbb{N},\ mm' = 10^{k+k'}$. Ceci implique que les seuls diviseurs de m soient 2 et 5, et donc en réinjectant que d soit de la forme $2^p 5^q$ avec $(p, q) \in \mathbb{Z}^2$.
   Réciproquement si $d = 2^p 5^q$ pour un certain couple $(p, q) \in \mathbb{Z}^2$ alors on a bien $d \in \mathbb{D}$ et $d^{-1} \in \mathbb{D}$ (puisque $d^{-1} = 2^{-p} 5^{-q}$ est de la même forme que d).

   L'ensemble des inversibles est donc $\left\{2^p 5^q,\ (p, q) \in \mathbb{Z}^2\right\}$.

5. $(\mathcal{P}(E), \cup, \cap)$ où E est un ensemble.

   Pour $E = \emptyset$, c'est l'anneau nul. Pas très intéressant.

   Sinon :$(\mathcal{P}(E), \cup)$ n'est pas un groupe (le neutre de $\cup$ est $\emptyset$ mais seul $\emptyset$ a un symétrique pour $\cup$) donc ce n'est pas un anneau.

6. $(\mathcal{P}(E), \Delta, \cap)$ où E est un ensemble.

   Vu dans le cours sur l'ordre supérieur : c'est un anneau isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}, +, \times\right)$, donc commutatif, non intègre pour $|E| \geqslant 2$, et ayant pour unique inversible le neutre du produit donc ici E.

5/1

Rem q (la exemple

$(\mathbb{Z}/2\mathbb{Z}, +, \times)$ avec $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

+	$\bar{1}$	$\bar{0}$
$\bar{1}$		
$\bar{0}$		

×	$\bar{1}$	$\bar{0}$
$\bar{1}$		
$\bar{0}$		

Soient $x, y \in A$. Montrons que $xy + yx = 0$

On a $(x+y)^2 = x^2 + xy + yx + y^2$

Or $(A, +, \times)$ est un anneau de Boole:

$$\begin{cases} (x+y)^2 = x+y \\ x^2 = x \\ y^2 = y \end{cases}$$

Donc $x + y = x + xy + yx + y$

d'où $0 = xy + yx$

5/2 On a $\forall x, y \in A,\ xy + yx = 0$

Pour $y = 1$, on obtient $\forall x \in A,\ x + x = 0$

ie $\forall x \in A,\ x = -x$

Montrons que $(A, +, \times)$ est commutatif.

Soient $x, y \in A$.

On a $xy + yx = 0$

donc $xy = -yx$

donc $xy = yx$ d'après ce qui précède.

5/2 $x \preccurlyeq y \iff yx = x$

(R) Soit $x \in A$. par déf $x^2 = x$

ie $xx = x$

$\iff x \preccurlyeq y$

(A) Soient $x, y \in A$. Supp $x \preccurlyeq y$ et $y \preccurlyeq x$

Autrement dit, $yx = x$ et $xy = y$

ie $yx = xy$ par commutativité

ie $x = y$

(T) Soient $x, y, z \in A$. Supp $\begin{cases} x \preccurlyeq y \\ y \preccurlyeq z \end{cases}$

Ainsi $\begin{cases} yx = x \\ zy = y \end{cases}$

d'où $zyx = z(yx) = \boxed{zx}$

$(zy)x = yx = \boxed{x}$.

d'où $x \preccurlyeq z$

yeey. Oooh

5/3 Soient $x, y \in A$

$$\begin{aligned} xy(x+y) &= xyx + xy^2 \\ &= x^2y + xyx && \text{par commutativité} \\ &= xy + yx && \text{par définition de } (A,+,\times) \\ &= 0_A && \text{d'après 5/1} \end{aligned}$$

Si A est intègre, alors

$$\forall x, y \in A,\ xy = 0_A \iff (x = 0_A \text{ ou } y = 0_A)$$

Particularisons :

Soit $x \in A$, $x(x + 1_A) = 0_A$

Si A est intègre, $\forall x \in A,\ x = 0_A$ ou $x = 1_A$

donc $A = \{0_A\}$ (anneau nul, $0_A = 1_A$)

ou $A = \{0_A, 1_A\} = \mathbb{Z}/2\mathbb{Z}$ car $0_A \neq 1_A$

5/4

- $(\mathcal{P}(E), \Delta, \cap)$ un anneau isomorphe à $(\mathcal{F}(E, \mathbb{Z}/2\mathbb{Z}), +, \times)$

Soit $X, Y \in \mathcal{P}(E)$.

$$\begin{aligned} X \leq Y &\iff Y \cap X = X \\ &\iff X \subset Y \end{aligned}$$

cf. cours ordre sup.

Exercice 6. *Sur les éléments nilpotents d'un anneau*

Soit $(A, +, \times)$ un anneau.

1. Soient $(x, y) \in A^2$ **tel que** x **et** y **commutent**, i.e. $xy = yx$. Soit également $n \in \mathbb{N}$.
   a. Montrer qu'on a $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. Contre-exemple si x et y ne commutent pas ?
   b. Montrer qu'on a $x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$. Contre-exemple si x et y ne commutent pas ?
2. On dit d'un élément x de A qu'il est **nilpotent** s'il existe $n \in \mathbb{N}$ tel que $x^n = 0$.
   a. Si A est intègre, montrer que 0 est le seul élément nilpotent de A.
   b. Soient x et y deux éléments de A. On suppose qu'ils sont nilpotents et qu'ils commutent. Montrer alors que $x+y$ et xy sont nilpotents.
   c. Soit $x \in A$ nilpotent. Montrer que $1-x$ est inversible dans A.
3. a. Rappeler un exemple d'anneau non commutatif ayant des éléments non nuls nilpotents.
   b. Trouver un exemple d'anneau commutatif ayant des éléments non nuls nilpotents.

Exercice 7. *Entiers de Gauss.*

On note $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b,\ a \in \mathbb{Z},\ b \in \mathbb{Z}\}$.

1. Montrer que $(\mathbb{Z}[\mathrm{i}], +, \times)$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Quels sont ses éléments inversibles ?

Exercice 8. *Un morphisme d'évaluation*

Montrer que l'application $\left\{ \begin{array}{ccc} \mathbb{R}[X] & \to & \mathbb{C} \\ P(X) & \mapsto & P(\mathrm{i}) \end{array} \right.$ est un morphisme d'anneaux et déterminer son noyau.

Exercice 9. *Automorphismes de* $\mathbb{Z}$

Déterminer tous les automorphismes de l'anneau $\mathbb{Z}$.

Corps, morphismes de corps

Exercice 10. *Anneau intègre fini...*

1. Soit A un anneau commutatif intègre et soit $a \neq 0$. On définit l'application γ_a par : $\forall x \in A,\ \gamma_a(x) = ax$. Montrer que γ_a est injective.
2. En déduire que tout anneau intègre fini commutatif et non nul est un corps.

Exercice 11.

Déterminer tous les automorphismes du corps $(\mathbb{Q}, +, \times)$.

Exercice 12. *Automorphismes de* $\mathbb{R}$.

Dans cet exercice, on montre que le seul automorphisme du corps $(\mathbb{R}, +, \times)$ est l'identité.

Soit f un tel automorphisme.

1. Justifier qu'on a : $f_{|\mathbb{Q}} = id_{\mathbb{Q}}$.
2. Justifier qu'on a : $\forall x \in \mathbb{R}_+,\ f(x) \geqslant 0$.
3. En déduire que f est croissante.
4. Conclure.

Exercice 13.

Exhiber deux automorphismes distincts du corps $(\mathbb{C}, +, \times)$.

Exercice 6. *Sur les éléments nilpotents d'un anneau*

Soit $(A,+,\times)$ un anneau.

1. Soient $(x,y)\in A^2$ **tel que** x **et** y **commutent**, i.e. $xy=yx$. Soit également $n\in\mathbb{N}$.

   a. Montrer qu'on a $(x+y)^n=\sum_{k=0}^{n}\begin{pmatrix} n \\ k \end{pmatrix}x^k y^{n-k}$. Contre-exemple si x et y ne commutent pas ?

   - On a $(x+y)^n=\underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ fois}}$. En utilisant la distributivité, on réécrit cette expression comme la somme des 2^n termes de la forme $c_1c_2\cdots c_n$ où les c_i appartiennent à $\{x,y\}$. **En utilisant le fait que *a* et *b* commutent**, on trouve que ces termes sont tous de la forme x^ky^{n-k} pour un certain entier $k\in\{0,\dots,n\}$. Il suffit de compter alors le nombre de fois qu'apparaît chacun de ces termes. Or, pour obtenir x^ky^{n-k}, il faut et suffit que x apparaisse k fois dans la liste $c_1,\ c_2,\ \dots,\ c_n$, il y a donc autant de façons de le faire que de choisir k éléments parmi n, à savoir $\binom{n}{k}$.

     On peut aussi, bien sûr, recopier la preuve vue dans le cours sur les sommes et identités remarquables, en insistant sur le moment où la commutation intervient.

   - On a déjà vu un contre-exemple lorsque x et y ne commutent pas dans le cours sur les matrices. Peut-être

   $$I_2=\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}\right)^2\neq\begin{pmatrix}0&1\\0&0\end{pmatrix}^2+2\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}^2=\begin{pmatrix}2&0\\0&0\end{pmatrix}.$$

   b. Montrer qu'on a $x^n-y^n=(x-y)\sum_{k=0}^{n-1}x^ky^{n-1-k}$. Contre-exemple si x et y ne commutent pas ?

   - On a $(x-y)\displaystyle\sum_{k=0}^{n-1}x^{n-1-k}y^k=(x-y)\left(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}\right)$ et cette expression se réécrit $\left(x^n+x^{n-1}y+\cdots+x^2y^{n-2}+xy^{n-1}\right)-\left(x^{n-1}y+x^{n-2}y^2+\cdots+xy^{n-1}+y^n\right)$ par distributivité, puis x^n-y^n après télescopage.

   - On a déjà vu un contre-exemple lorsque x et y ne commutent pas dans le cours sur les matrices. Peut-être

   $$(0)=\begin{pmatrix}0&1\\0&0\end{pmatrix}^2-\begin{pmatrix}0&0\\1&0\end{pmatrix}^2\neq\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}-\begin{pmatrix}0&0\\1&0\end{pmatrix}\right)\left(\begin{pmatrix}0&1\\0&0\end{pmatrix}+\begin{pmatrix}0&0\\1&0\end{pmatrix}\right)=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

2. On dit d'un élément x de A qu'il est **nilpotent** s'il existe $n\in\mathbb{N}$ tel que $x^n=0$.

   a. Si A est intègre, montrer que 0 est le seul élément nilpotent de A.

   Supposons A intègre. Soit x un élément nilpotent. Il existe donc $n\in\mathbb{N}$ tel que $x^n=0$. Si $n=0$ alors $1=x^0=x^n=0$ et A est l'anneau nul ; en particulier on a $x=0$. Sinon on peut écrire $x^n=xx^{n-1}$ et par intégrité on a $x=0$ ou $x^{n-1}=0$, puis par récurrence immédiate $x=0$.

   b. Soient x et y deux éléments de A. On suppose qu'ils sont nilpotents et qu'ils commutent. Montrer alors que $x+y$ et xy sont nilpotents.

   Par hypothèse il existe $n\in\mathbb{N}$ tel que $x^n=0$ et il existe $m\in\mathbb{N}$ tel que $y^m=0$. Attention, aucune raison que m et n soient égaux.

   - Posons $N=n+m-1$. Comme x et y commutent, on a $(x+y)^N=\sum_{k=0}^{N}\binom{N}{k}x^ky^{N-k}$. Pour $k<n$ on a $N-k>N-n=m-1$ *i. e.* $N-k\geqslant m$, et donc y^{N-k} est nul ; pour $k\geqslant n$ c'est x^k qui est nul. Ainsi, tous les termes de cette somme sont nuls et donc $(x+y)^N=0$ et $x+y$ est nilpotent.
   - Posons $N=\min(n,m)$. Comme x et y commutent, on a $(xy)^N=x^Ny^N$. Au moins un des deux facteurs est nul donc $(xy)^N=0$, et donc xy est nilpotent.

   c. Soit $x\in A$ nilpotent. Montrer que $1-x$ est inversible dans A.

   Ce résultat est très clairement de l'or en barre, et on l'a déjà démontré et utilisé sans le dire (quand ?).

   Par hypothèse il existe $n\in\mathbb{N}$ tel que $x^n=0$. Comme 1 et x commutent on a

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

et... bah c'est fini, $(1-x)$ est inversible d'inverse $\sum_{k=0}^{n-1} x^k$.

3. a. Rappeler un exemple d'anneau non commutatif ayant des éléments non nuls nilpotents.
   b. Trouver un exemple d'anneau commutatif ayant des éléments non nuls nilpotents.

On a déjà vu plus haut l'exemple de $\mathcal{M}_2(\mathbb{R})$ (ou $\mathcal{M}_n(\mathbb{K})$) qui a plein de nilpotents mais n'est pas commutatif.

On a aussi $\mathbb{Z}/4\mathbb{Z}$ qui est commutatif et dans lequel 2 est nilpotent.

Exercice 7. Inclus dans l'exercice 4 !

$$\mathrm{Im}(\tilde{h}) = \mathrm{id}^{n}_{\mathbb{R}^\times}(\mathbb{R}^\times)$$

$$= \begin{cases} \mathbb{R}^\times & \text{si } n \in 2\mathbb{N}+1 \\ \mathbb{R}_+^\times & \text{si } n \in 2\mathbb{N}^\times \\ \{1\} & \text{sinon} \end{cases}$$

$$\Rightarrow \left(\tilde{h} \in \mathcal{GD} \iff n \in 2\mathbb{N}+1\right)$$

8

$$\phi : \begin{cases} (\mathbb{R}[X], +, \times) \longrightarrow (\mathbb{C}, +, \times) \\ P(X) \longmapsto P(i) \end{cases}$$

Mq $\begin{cases} \forall P, Q \in \mathbb{R}[X],\ \phi(P+Q) = \phi(P) + \phi(Q) \\ \forall P, Q \in \mathbb{R}[X],\ \phi(P \times Q) = \phi(P) \times \phi(Q) \\ \phi(1_{\mathbb{R}[X]}) = 1_{\mathbb{C}} \end{cases}$

Soient $P, Q \in \mathbb{R}[X]$. Soit $\square \in \{+, \times\}$

$$\phi(P \square Q) = (P \square Q)(i)$$
$$= P(i) \square Q(i)$$
$$= \phi(P) \square \phi(Q)$$

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

$$\mathrm{Ker}(\phi) = \{P \in \mathbb{R}[X],\ \phi(P) = 0_{\mathbb{R}[X]}\}$$

$$= \{P \in \mathbb{R}[X],\ P(i) = 0_{\mathbb{R}[X]}$$

ex

$0 \in \mathrm{Ker}\,\phi$

$X^2+1 \in \mathrm{Ker}\,\phi$

$X^4+X^2 \in \mathrm{Ker}\,\phi$

$X^3+X \in \mathrm{Ker}\,\phi$

conj

$$\mathrm{Ker}\,\phi = \{(X^2+1) \times Q(X),\ Q(X) \in \mathbb{R}[X]\}$$

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

dem

$\boxed{\supset}$ Soit $P \in (X^2+1)\,\mathbb{R}[X]$.

Ainsi il existe $Q \in \mathbb{R}[X]$ tq $P = (X^2+1) \times Q$

On a $\phi(P) = P(i)$

$= (i^2+1) \times Q(i)$

$= 0 \times Q(i)$

$= 0$

$\Rightarrow P \in \mathrm{Ker}\,\phi$

⊂ Soit $P \in \ker \phi$ tq $P(i) = 0$.

D'après le théorème de division euclidienne, il existe $P, Q \in \mathbb{R}[X]$ tels que

$$\begin{cases} P = (X^2+1)Q + R \\ \deg R \leq \deg(X^2+1) = 1 \end{cases}$$

Il existe $a, b \in \mathbb{R}$, tel que $R = aX + b$.

Par hypothèse $P(i) = 0$

$$\Leftrightarrow (i^2+1)Q(i) + R(i) = 0$$

$$\Leftrightarrow 0 + ai + b = 0$$

$$\Leftrightarrow \begin{cases} \mathrm{Re}(ai+b) = b = 0 \\ \mathrm{Im}(ai+b) = a = 0 \end{cases}$$

$$\Rightarrow R = 0_{\mathbb{R}[X]}$$

$$\Rightarrow P = (X^2+1)Q$$

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

Exercice 9. Déterminer tous les automorphismes de l'anneau $\mathbb{Z}$.

Soit f un tel automorphisme. En particulier f vérifie $\forall (x,y) \in \mathbb{Z}^2,\ f(x+y) = f(x) + f(y)$ et on a déjà vu dans la feuille d'exercice 17 qu'une telle application est nécessairement de la forme $f = \lambda \,\mathrm{id}$ avec $\lambda \in \mathbb{Z}$ (évidemment, je n'écris pas ça sur une copie, je recopie la preuve !).

Mais on a aussi $f(1) = 1$ donc $\lambda = 1$ et finalement $f = \mathrm{id}_{\mathbb{Z}}$.

Réciproquement, l'identité est bien un automorphisme d'anneau de $\mathbb{Z}$.

D'où $S = \{\mathrm{id}\}$.

Exercice 10. *Anneau intègre fini...*

1. Soit A un anneau commutatif intègre et soit $a \neq 0$. On définit l'application γ_a par : $\forall x \in A,\ \gamma_a(x) = ax$. Montrer que γ_a est injective.
2. En déduire que tout anneau intègre fini commutatif et non nul est un corps.

1. L'application γ_a n'a pas de raison d'être un morphisme d'anneau. Par contre, par distributivité, γ_a est un morphisme du groupe $(A, +)$ dans lui-même.
On utilise la caractérisation de l'injectivité pour les morphismes de groupes : on a $\text{Ker}(\gamma_a) = \{x \in A,\ ax = 0\} = \{0\}$ par intégrité et puisqu'on a $a \neq 0$. Ainsi γ_a est bien injective.
Rappelons le résultat vu dans le chapitre *Applications* : une application injective entre deux ensembles finis de même cardinal est toujours bijective. Donc γ_a est bijective.

2. Soit A un tel anneau. Pour tout $a \in A \setminus \{0\}$, on peut définir γ_a comme précédemment, et on obtient que γ_a est bijective d'après la question précédente. En particulier, 1 a un antécédent par γ_a, c'est-à-dire qu'il existe $x \in A$ tel que $ax = 1$ (et donc $xa = 1$ par commutativité). Ainsi a a un inverse. Ceci étant vrai pour tout élément non nul a, et A étant commutatif, on a bien montré que A est un corps.

Exercice 11. Déterminer tous les automorphismes du corps $(\mathbb{Q}, +, \times)$.

Analyse : Soit $f : \mathbb{Q} \to \mathbb{Q}$ un tel automorphisme. En particulier on a $f(1) = 1$ et $\forall x, y \in \mathbb{Z},\ f(x+y) = f(x) + f(y)$ et donc, comme on l'a vu dans l'exercice 7, on a $\forall p \in \mathbb{Z},\ f(p) = p$. Soit $\frac{p}{q} \in \mathbb{Q}$ (écriture pas nécessairement irréductible). De plus, on a $\forall x, y \in \mathbb{Q},\ f(xy) = f(x)f(y)$ donc en particulier $p = f(p) = f\left(q\frac{p}{q}\right) = qf\left(\frac{p}{q}\right)$ et donc $f\left(\frac{p}{q}\right) = \frac{p}{q}$.

Unique candidat $f = \mathrm{id}_{\mathbb{Q}}$.

Synthèse : Évidemment, $\mathrm{id}_{\mathbb{Q}}$ est un automorphisme du corps $\mathbb{Q}$.

Conclusion : $\boxed{S = \{\mathrm{id}_{\mathbb{Q}}\}}$.

Exercice 12. *Automorphismes de $\mathbb{R}$.*

Dans cet exercice, on montre que le seul automorphisme du corps $(\mathbb{R}, +, \times)$ est l'identité.

Soit f un tel automorphisme.

1. Justifier qu'on a : $f_{|\mathbb{Q}} = id_{\mathbb{Q}}$.
2. Justifier qu'on a : $\forall x \in \mathbb{R}_+,\ f(x) \geqslant 0$.
3. En déduire que f est croissante.
4. Conclure.

1. On a en particulier $f(1) = 1$ ainsi que $\forall x, y \in \mathbb{Q},\ f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ donc d'après l'exercice précédent $f_{|\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.

2. L'astuce ici est que $\mathbb{R}$ est ordonné et qu'un élément est positif si et seulement si c'est un carré (ça ne marchera évidemment plus dans $\mathbb{C}$...). Soit $x \in \mathbb{R}_+$. Alors $x = \left(\sqrt{x}\right)^2$ et donc $f(x) = f\left(\left(\sqrt{x}\right)^2\right) = \left(f\left(\sqrt{x}\right)\right)^2 \geqslant 0$.

3. Soit $x \leqslant y$. Alors $y - x \geqslant 0$ et donc $f(y-x) \geqslant 0$ *i. e.* $f(y) - f(x) \geqslant 0$ *i. e.* $f(x) \leqslant f(y)$. Ainsi f est bien croissante.

4. On a déjà essentiellement résolu cet exercice, mais en supposant f continue. On va essayer ici "d'émuler" la démonstration vue par continuité à l'aide de la croissance.

   C'est typiquement le type de situation où avoir retenu un résultat ne suffit pas, il faut avoir compris comment on le démontre afin de pouvoir en adapter légèrement la démonstration.

   On va comme dans le cas continu utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$, mais il va être nécessaire d'avoir compris comment on la démontre.

   Soit $x \in \mathbb{R}$. Dans la preuve de densité de $\mathbb{Q}$ dans $\mathbb{R}$, on a construit une suite à valeurs dans $\mathbb{Q}$ de limite x.

   Cette suite est $(a_n)_{n\in\mathbb{N}} = \left(\frac{\lfloor 10^n x \rfloor}{10^n}\right)_{n\in\mathbb{N}}$. C'est en fait la suite des **approximations décimales par défaut** de x, et on a $\forall n \in \mathbb{N},\ a_n \leqslant x$. Mais on a aussi vu qu'une autre suite convenable est la suite $(b_n)_{n\in\mathbb{N}} = \left(\frac{\lceil 10^n x \rceil}{10^n}\right)_{n\in\mathbb{N}}$ des **approximations décimales par excès** de x, qui elle vérifie $\forall n \in \mathbb{N},\ x \leqslant b_n$. Ces deux suites convergent toutes les deux vers x par TdG et sont à valeurs dans $\mathbb{Q}$. Mais comme f est croissante et $f_{|\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ on a $\forall n \in \mathbb{N},\ a_n = f(a_n) \leqslant f(x) \leqslant f(b_n) = b_n$ et donc $\lim\limits_{n\to+\infty} f(x) = x$ *i. e.* $f(x) = x$ par unicité de la limite.

   Ceci étant vrai pour tout réel x on a $f = \mathrm{id}_{\mathbb{R}}$. Bien évidemment, réciproquement $\mathrm{id}_{\mathbb{R}}$ est bien un automorphisme du corps $\mathbb{R}$ (même si cette précision n'est pas clairement demandée dans cet exercice).

Exercice 13.
Exhiber deux automorphismes distincts du corps $(\mathbb{C}, +, \times)$.

D'après le cours sur les structures, $\mathrm{id}_{\mathbb{C}} : \mathbb{C} \to \mathbb{C}$ est un automorphisme du corps $\mathbb{C}$. D'après le cours sur les complexes $\mathrm{conj} : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array} \right.$ est aussi un automorphisme du corps $\mathbb{C}$. Ces deux automorphismes sont évidemment distincts puisque par exemple $-\mathrm{i} = \overline{i} = \mathrm{conj}(\mathrm{i}) \neq \mathrm{id}(\mathrm{i}) = \mathrm{i}$.

Y en a-t-il d'autres ? Oui. Mais :

— ils ne sont pas continus ;

— c'est dur ;

— c'est (très) hors-programme.

N'essayez pas d'en exhiber un, la construction est abstraite et s'appuie sur beaucoup de résultats que l'on ne connaît pas.