POIRET Aurélien **MPSI**
TD n° 15 ★

Structures algébriques usuelles

1 Loi de composition interne

Exercice N° 1 : On définit une loi de composition interne $\star$ sur $\mathbb{R}$ par

$$\forall a, b \in \mathbb{R},\ a \star b = \ln(\mathrm{e}^a + \mathrm{e}^b).$$

Quelles en sont les propriétés ?

Exercice N° 2 : Soit $E = [0, 1]$. On définit une loi $\star$ sur E par

$$\forall x, y \in E,\ x \star y = x + y - xy.$$

1. Montrer que $\star$ est une loi de composition interne commutative et associative.
2. Montrer que $\star$ possède un neutre.
3. Quels sont les éléments inversibles ?

Exercice N° 3 : Soit $\star$ une loi de composition interne sur E.
Pour $A, B \in \mathcal{P}(E)$ on pose

$$A \perp B = \{a \star b \ /\ a \in A, b \in B\}.$$

1. Étudier les propriétés de $\star$ sur E (commutativité, associativité, existence d'un neutre) conservées par $\perp$ sur $\mathcal{P}(E)$.
2. Étudier les propriétés de $\perp$ sur $\mathcal{P}(E)$ (commutativité, associativité, existence d'un neutre) conservées par $\star$ sur E.
3. La loi $\perp$ est-elle distributive par rapport l'union ? par rapport à l'intersection ?

Exercice N° 4 : Soit E un ensemble munit d'une loi $\star$ de composition interne associative et possédant un élément neutre et fixons $a \in E$.
Montrer que a est inversible si, et seulement si, l'application $f : E \to E$ définie par $f(x) = a \star x$ est bijective.

Exercice N° 5 : Soit E et F deux ensembles et $\varphi : E \to F$ une application bijective.
On suppose E muni d'une loi de composition interne $\star$ et on définit une loi $\top$ sur F par :

$$\forall x, y \in F,\ x \top y = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(y)).$$

1. Montrer que si $\star$ est commutative (respectivement associative) alors $\top$ l'est aussi.
   Étudier la réciproque.
2. Montrer que si $\star$ possède un neutre e alors $\top$ possède aussi un neutre à préciser.
   Étudier la réciproque.

Exercice N° 6 : Soit $\star$ une loi de composition interne associative sur E.
On suppose qu'il existe $a \in E$ tel que l'application $f : E \to E$ définie par $f(x) = a \star x \star a$ soit surjective et on note b un antécédent de a par f.

1. Montrer que $e = a \star b$ (respectivement $e' = b \star a$) est élément neutre à gauche (respectivement à droite) puis que $e = e'$.

2. Montrer que a est inversible et f bijective.

Exercice N° 7 : Soit $\top$ la loi de composition interne définie sur $[-1, 1]$ par

$$x \top y = x\sqrt{1 - y^2} + y\sqrt{1 - x^2}.$$

Étudier les propriétés de la loi $\top$.
Indication : On pourra montrer que 1 *admet plusieurs inverses.*

2 Groupe

Exercice N° 8 : Soit $(G, \star)$ un groupe tel que

$$\forall x \in G,\ x^2 = e.$$

Montrer que G est commutatif.

Exercice N° 9 : Soient $G = \mathbb{R}^\star \times \mathbb{R}$ et $\star$ la loi de composition interne définie sur G par

$$(x, y) \star (x', y') = (xx', xy' + y).$$

1. Montrer que $(G, \star)$ est un groupe non commutatif.
2. Montrer que $\mathbb{R}^{+\star} \times \mathbb{R}$ est un sous-groupe de $(G, \star)$.

Exercice N° 10 : Addition des vitesses en théorie de la relativité
Soient $c > 0$ et $I =]-c, c[$.

1. Montrer
$$\forall (x, y) \in I^2,\ x \star y = \frac{x + y}{1 + \frac{xy}{c^2}} \in I.$$
2. Montrer que la loi $\star$ munit I d'une structure de groupe abélien.

Cette loi $\star$ correspond à l'addition des vitesses portées par un même axe en théorie de la relativité.

Exercice N° 11 : Soit $\top$ la loi de composition interne définie sur $\mathbb{R}$ par

$$x \top y = x\sqrt{1 + y^2} + y\sqrt{1 + x^2}.$$

Montrer que $(\mathbb{R}, \top)$ est un groupe abélien.

3 Sous-groupe

Exercice N° 12 : Soient $\omega \in \mathbb{C}$ et $H = \{a + \omega b \ /\ a, b \in \mathbb{Z}\}$. Montrer que H est un sous-groupe de $(\mathbb{C}, +)$.

Exercice N° 13 : Soient $a \in \mathbb{C}^\star$ et $H = \{a^n \ /\ n \in \mathbb{Z}\}$. Montrer que H est un sous-groupe de $(\mathbb{C}^\star, \times)$.

Exercice N° 14 : Soit a un élément d'un ensemble E. On forme $H = \{f \in S_E \ /\ f(a) = a\}$. Montrer que H est un sous-groupe de $(S_E, \circ)$.

Exercice N° 15 : Soient $(G, \times)$ un groupe, H un sous-groupe de $(G, \times)$ et $a \in G$.

1. Montrer que $aHa^{-1} = \left\{axa^{-1} \ /\ x \in H\right\}$ est un sous-groupe de $(G, \times)$.

2. A quelle condition simple $aH = \{ax \ / \ x \in H\}$ est un sous-groupe de $(G, \times)$?

Exercice N° 16 : On appelle centre d'un groupe $(G, \star)$, la partie C de G définie par

$$\mathcal{Z}(G) = \{x \in G \ / \ \forall y \in G, x \star y = y \star x\} .$$

Montrer que $\mathcal{Z}(G)$ est un sous-groupe de $(G, \star)$.

Exercice N° 17 : Soient H et K deux sous-groupes d'un groupe $(G, \star)$.

1. Montrer que $H \cap K$ est un sous-groupe de G. Ce résultat subsiste-t-il pour une intersection quelconque de sous-groupes ?
2. Montrer que $H \cup K$ est un sous-groupe de $(G, \star)$ si, et seulement si, $H \subset K$ ou $K \subset H$.

Exercice N° 18 : Soit $(G, \star)$ un groupe et A une partie finie non vide de G stable pour $\star$.

1. Soit $x \in A$ et $\varphi : \mathbb{N} \to G$ l'application définie par $\varphi(n) = x^n$. Montrer que φ n'est pas injective.
2. En déduire que $x^{-1} \in A$ puis que A est un sous-groupe de $(G, \star)$.

Exercice N° 19 :

1. Montrer que l'ensemble des similitudes directes du plan complexe est un groupe pour la composition.
2. Que dire de l'ensemble des translations ? De l'ensemble des homothéties ? Et de l'ensemble des rotations ?
3. Soit A un point quelconque du plan complexe. Reprendre la question précédente avec l'ensemble des homothéties fixant A et l'ensemble des rotations fixant A.

Exercice N° 20 : Montrer que H est un sous-groupe fini de $(\mathbb{C}^\star, \times)$ si, et seulement si, il existe $n \in \mathbb{N}^\star$ tel que $H = \mathbb{U}_n$.

4 Anneau et sous-anneau

Exercice N° 21 : On définit sur $\mathbb{Z}^2$ deux lois de compositions internes notées $+$ et $\star$ par :
$(a, b) + (c, d) = (a + c, b + d)$ et $(a, b) \star (c, d) = (ac, ad + bc)$.

1. Montrer que $(\mathbb{Z}^2, +, \star)$ est un anneau commutatif.
2. Montrer que $A = \{(a, 0) \ / \ a \in \mathbb{Z}\}$ est un sous-anneau de $(\mathbb{Z}^2, +, \star)$.

Exercice N° 22 : Soit x et y deux éléments d'un anneau $(A, +, \times)$.

1. Montrer que si x est nilpotent et que x et y commutent, alors xy est nilpotent.
2. Montrer que si x et y sont nilpotents et commutent, alors $x + y$ est nilpotent.
3. Montrer que si xy est nilpotent, alors yx l'est aussi.
4. Montrer que si x est nilpotent alors $1 - x$ est inversible. Préciser $(1 - x)^{-1}$.

Exercice N° 23 : Soit $d \in \mathbb{N}$, on note

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \ / \ (a, b) \in \mathbb{Z}^2\right\} .$$

Montrer que $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice N° 24 : On note

$$\mathbb{D} = \left\{ \frac{n}{10^k} \ / \ n \in \mathbb{Z}, k \in \mathbb{N} \right\}$$

l'ensemble des nombres décimaux.
Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

Exercice N° 25 : Anneau des entiers de Gauss
On note

$$\mathbb{Z}[i] = \left\{ a + ib \ / \ (a, b) \in \mathbb{Z}^2 \right\}.$$

1. Montrer que $\mathbb{Z}[i]$ est un anneau commutatif pour l'addition et la multiplication des nombres complexes.
2. Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i]$.

Exercice N° 26 : Soit

$$A = \left\{ \frac{m}{n} \ / \ m \in \mathbb{Z} \text{ et } n \in \mathbb{N}^\star, \text{ impair} \right\}.$$

1. Montrer que A est un sous anneau de $(\mathbb{Q}, +, \times)$.
2. Quels en sont les éléments inversibles ?

5 Corps

Exercice N° 27 : Pour $a, b \in \mathbb{R}$, on pose $a \top b = a + b - 1$ et $a \star b = ab - a - b + 2$. Montrer que $(\mathbb{R}, \top, \star)$ est un corps commutatif.

Exercice N° 28 : Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$, on note

$$\mathbb{Q}\left[\sqrt{d}\right] = \left\{ a + b\sqrt{d} \ / \ (a, b) \in \mathbb{Q}^2 \right\}.$$

Montrer que $(\mathbb{Q}\left[\sqrt{d}\right], +, \times)$ est un corps.

Exercice N° 29 : Soit F un sous-corps de $(\mathbb{Q}, +, \times)$. Montrer que $F = \mathbb{Q}$.

Correction des exercices

Solution Exercice N° 1 :

♦ Soient $a, b \in \mathbb{R}$. $a \star b = \ln(e^a + e^b) = \ln(e^b + e^a) = b \star a$.
Ainsi $\star$ est commutative.
♦ Soient $a, b, c \in \mathbb{R}$. $(a \star b) \star c = \ln(e^{\ln(e^a+e^b)} + e^c) = \ln(e^a + e^b + e^c) = \ln(e^a + e^{\ln(e^b+e^c)}) = a \star (b \star c)$.
Ainsi $\star$ est associative.
♦ On suppose que $\star$ possède un élément neutre.
Il existe $\mathcal{E} \in \mathbb{R}$ tel que, pour tout $x \in \mathbb{R}$, $x \star \mathcal{E} = x$.
Pour $x = 0$, on obtient $e^{\mathcal{E}}$. C'est absurde puisque exp ne s'annule jamais. Ainsi $\star$ ne possède pas d'élément neutre.

Solution Exercice N° 2 :

1. ♦ Soient $x, y \in [0, 1]$.
$x \star y = x + y - xy = x(1 - y) + y \geqslant 0$ et $x \star y = x + y - xy = x(1 - y) + y \leqslant 1 - y + 1 = 1$.
Ainsi $\star$ est bien une loi de composition interne sur $[0, 1]$.
♦ Soient $x, y \in E$. $x \star y = x + y - xy = y + x - yx = y \star x$. Ainsi $\star$ est commutative.
♦ Soient $x, y, z, \in E$.
$$(x \star y) \star z = (x + y - xy) \star z = (x + y - xy) + z + (x + y - xy)z = x + y + z - xy - xz - yz + xyz.$$
De même,
$$x \star (y \star z) = x \star (y + z - yz) = x + y + z - yz - x(y + z - yz) = x + y + z - xy - xz - yz + xyz.$$
Ainsi $(x \star y) \star z = x \star (y \star z)$ et donc la loi $\star$ est donc associative.
2. Pour tout $x \in E$, $x \star 0 = x + 0 - x \times 0 = x$.
Comme la loi $\star$ est commutative alors 0 est l'élément neutre de la loi $\star$.
3. Cherchons les éléments inversible de $(E, \star)$ par analyse-synthèse.
Analyse.
Soit $x \in E$ inversible pour la loi $\star$. Alors il existe $y \in E$ tel que $x \star y = 0$, c'est-à-dire $x + y - xy = 0$. Ainsi $y(1 - x) = -x$.
Nécessairement $x =\neq 1$ (car sinon $0 = -1$) et donc $y = -\frac{x}{1-x} \leqslant 0$.
Comme $y \in E$ alors $y = 0$ puis $x = 0$.
Synthèse.
0 est inversible car $0 \star 0 = 0$.
Le seul élément inversible de $(E, \star)$ est 0.

Solution Exercice N° 3 :

1. ♦ On suppose que $\star$ est commutative sur E.
Soient $A, B \in \mathcal{P}(E)$. On a :
$$\begin{aligned} A \perp B &= \{a \star b \ / \ a \in A, b \in B\} \\ &= \{b \star a \ / \ a \in A, b \in B\} = B \perp A. \end{aligned}$$
Ainsi $\perp$ est commutative sur $\mathcal{P}(E)$.
♦ On suppose que $\star$ est associative sur E.
Soient $A, B, C \in \mathcal{P}(E)$. On a :
$$\begin{aligned} (A \perp B) \perp C &= \{(a \star b) \star c \ / \ a \in A, b \in B, c \in C\} \\ &= \{a \star (b \star c) \ / \ a \in A, b \in B, c \in C\} = A \perp (B \perp C). \end{aligned}$$
Ainsi $\perp$ est associative sur $\mathcal{P}(E)$.
♦ On suppose que $\star$ possède un élément neutre sur E, notons-le e.
On pose $E = \{e\}$.
Soit $A \in \mathcal{P}(E)$. On a :
$$A \perp E = \{a \star e \ / \ a \in A\} = \{a / \ a \in A\} = A.$$
De même,
$$E \perp A = \{e \star a \ / \ a \in A\} = \{a / \ a \in A\} = A.$$
Ainsi E est l'élément neutre de $\perp$ sur $\mathcal{P}(E)$.
2. ♦ On suppose que $\perp$ est commutative sur $\mathcal{P}(E)$.
On sait donc que, pour tous $A, B \in \mathcal{P}(E)$, $A \perp B = B \perp A$.
Soient $a, b \in E$. En choisissant $A = \{a\}$ et $B = \{b\}$, on obtient $a \star b = b \star a$.
Ainsi $\star$ est commutative sur E.
♦ On suppose que $\perp$ est associative sur $\mathcal{P}(E)$.
On sait donc que, pour tous $A, B, C \in \mathcal{P}(E)$, $(A \perp B) \perp C = A \perp (B \perp C)$.
Soient $a, b, c \in E$. En choisissant $A = \{a\}$, $B = \{b\}$ et $C = \{c\}$, on obtient $(a \star b) \star c = a \star (b \star c)$.
Ainsi $\star$ est associative sur E.
♦ On suppose que $\perp$ possède un élément neutre sur $\mathcal{P}(E)$. Notons-le $\mathcal{E}$.
On sait donc que, pour tous $A \in \mathcal{P}(E)$, $A \perp \mathcal{E} = \mathcal{E} \perp A = A$.
On observe que E est nécessairement non vide.
Soit $a \in E$. Choisissons $A = \{a\}$. On obtient que, pour tout $e \in \mathcal{E}$, $a \star e = e \star a = a$.
On en déduit que $\mathcal{E}$ est réduit à un élément et que $\star$ possède un élément neutre.

3. Soient $A, B, C \in \mathcal{P}(E)$.
$x \in A \perp (B \cup C)$ si, et seulement si, il existe $a \in A$ et $u \in B \cup C$ tels que $x = a \star u$ si, et seulement si, il existe $a \in A$ et $u \in B$ tels que $x = a \star u$ ou il existe $a \in A$ et $u \in C$ tels que $x = a \star u$ si, et seulement si, $x \in A \perp B$ ou $x \in A \perp C$ si, et seulement si, $x \in (A \perp B) \cup (A \perp C)$.
Ainsi, par double inclusion, $A \perp (B \cup C) = (A \perp B) \cup (A \perp C)$.
De même, on montre que $(A \cup B) \perp C = (A \perp C) \cup (B \perp C)$.
Ainsi $\perp$ est distributive par rapport à $\cup$.
En revanche, $\perp$ n'est pas distributive par rapport à $\cap$.
Considérons $E = \mathbb{R}$, $\star = +$ et $A = \mathbb{R}$, $B = \mathbb{R}^+$ et $C = \mathbb{R}^{-\star}$.
Alors $A \perp (B \cap C) = \emptyset$ et $(A \cap B) \perp (A \cap C) = \mathbb{R} + \mathbb{R} = \mathbb{R}$.

Solution Exercice N° 4 :

" $\Rightarrow$: Si a est inversible alors il existe $b \in E$ tel que $a \star b = b \star a = e$.
On pose $g : E \to E$ définie par $g(x) = b \star x$.
On vérifie alors que $g \circ f = f \circ g = \mathrm{Id}_E$. Ainsi f est bijective.
" $\Leftarrow$: Comme f est bijective alors e admet un antécédent par f. Il existe $b \in E$ tel que $a \star b = e$.
Or $f(e) = a \star e = a$ et $f(b \star a) = a \star (b \star a) = (a \star b) \star a = e \star b = b$.
Par injectivité de f, on en déduit que $e = b \star a$
Ainsi a est inversible.

Solution Exercice N° 5 :

1. ♦ On suppose que $\star$ est commutative sur E.
Soient $x, y \in F$.
$$x \top y = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(y)) = \varphi(\varphi^{-1}(y) \star \varphi^{-1}(x)) = y \top x.$$
Ainsi $\top$ est commutative sur F.
♦ On suppose que $\star$ est associative sur E.
Soient $x, y, z \in F$.
$$(x \top y) \top z = \varphi\left(\varphi^{-1}(\varphi(\varphi^{-1}(x) \star \varphi^{-1}(y))) \star \varphi^{-1}(z)\right) = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(y) \star \varphi^{-1}(z)).$$
Et, de même,
$$x \top (y \top z) = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(\varphi(\varphi^{-1}(y) \star \varphi^{-1}(z)))) = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(y) \star \varphi^{-1}(z)).$$
Ainsi $\top$ est associative sur F.

On observe que, pour tout $x, y \in E$, $x \star y = \varphi^{-1}(\varphi(x) \top \varphi(y))$.
2. ♦ On suppose que $\star$ possède un élément neutre noté e. Notons $f = \varphi(e)$. Montrons que f est élément neutre de $\top$.
Pour tout $x \in F$,
$$x \top f = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(f)) = \varphi(\varphi^{-1}(x) \star \varphi^{-1}(\varphi(e))) = \varphi(\varphi^{-1}(x) \star e) = \varphi(\varphi^{-1}(x) = x.$$
De même, on montre que, pour tout $x \in F$, $f \top x = x$.
Ainsi f est élément neutre de $\top$.

Comme précédemment, quitte à remplacer φ par φ^{-1}, on en déduit que la réciproque est vraie.

Solution Exercice N° 6 :

1. On a $a = a \star b \star a$.
Notons $e = a \star b$.
Soit $x \in E$. Par surjectivité de f, il existe $y \in E$ tel que $x = f(y)$.
$$e \star x = a \star b \star a \star y \star a = a \star y \star a = x.$$
Notons $e' = b \star x$.
Soit $x \in E$. Par surjectivité de f, il existe $y \in E$ tel que $x = f(y)$.
$$x \star e' = a \star y \star a \star b \star a = a \star y \star a = x.$$
En particulier, $e' = e \star e' = e$.
2. On en déduit que e est élément neutre de E et a est inversible d'inverse b.
Soient $x, y \in E$ tel que $f(x) = f(y)$. Alors $a \star x \star a = a \star y \star a$. En multipliant à gauche et à droite par a^{-1}, on en déduit que $x = y$.
Ainsi f est injective et, étant surjective, elle est donc bijective.

Solution Exercice N° 7 :
♦ Soient $x, y \in [-1, 1]$. Il existe $u, v \in \mathbb{R}$ tel que $x = \sin(u)$ et $y = \sin(v)$.
Ainsi $x \top y = \sin(u)\sqrt{1-\sin(v)^2} + \sin(v)\sqrt{1-\sin(u)^2} = \pm\sin(u)\cos(v) \pm \sin(v)\cos(u) = \pm\sin(u \pm v) \in [-1, 1]$.
Ainsi $\top$ est bien une loi interne sur $[-1, 1]$.
♦ Soient $x, y \in [-1, 1]$. $x \top y = x\sqrt{1-y^2} + y\sqrt{1-x^2} = y\sqrt{1-x^2} + x\sqrt{1-y^2} = y \top x$. Ainsi $\top$ est commutative sur $\mathbb{R}$.
♦ Pour tout $x \in \mathbb{R}$, $x \top 0 = 0$. Comme $\top$ est commutative alors $\top$ possède un élément neutre : 0.
♦ $1 \top 1 = 1 \top (-1) = 0$. Comme la loi $\top$ est commutative, on en déduit que 1 possède, au moins, deux inverses : 1 et -1. On en déduit que $\top$ n'est pas associative.

Solution Exercice N° 8 : L'hypothèse donne que, pour tout $x \in G$, $x = x^{-1}$.
Soient $x, y \in G$.

$$x \star y = x^{-1} \star y^{-1} = (y \star x)^{-1} = y \star x.$$

Ainsi G est un groupe abélien.

Solution Exercice N° 9 :

1. ♦ $\star$ est une loi de composition interne sur G.
   ♦ Soient $(x, y), (x', y'), (x'', y'') \in G$. On a

   $$(x, y) \star ((x', y') \star (x'', y'')) = (x, y) \star (x'x'', x'y'' + y') = (xx'x'', x(x'y'' + y') + y = (xx'x'', xx'y'' + xy' + y).$$

   De même

   $$((x, y) \star (x', y')) \star (x'', y'') = (xx', xy' + y) \star (x'', y'') = (xx'x'', xx'y'' + xy' + y).$$

   Ainsi $\star$ est associative.
   ♦ Soit $(x, y) \in G$.

   $$(x, y) \star (1, 0) = (x, y) \text{ et } (1, 0) \star (x, y) = (x, y).$$

   Ainsi $\star$ possède un élément neutre.
   ♦ Soit $(x, y) \in G$.

   $$(x, y) \star \left(\frac{1}{x}, -\frac{y}{x}\right) = (1, 0) \text{ et } \left(\frac{1}{x}, -\frac{y}{x}\right) \star (x, y) = (1, 0).$$

   Ainsi (x, y) est inversible dans $(G, \star)$.

   $(G, \star)$ est donc un groupe.
   Comme $(2, 1) \star (1, -2) = (2, -3) \neq (2, -1) = (1, -2) \star (2, 1)$ alors $(G, \star)$ n'est pas commutatif.
2. $\mathbb{R}^{+\star} \times \mathbb{R} \subset G$ et $(G, \star)$ est un groupe.
   Montrons que $\mathbb{R}^{+\star} \times \mathbb{R}$ est un sous-groupe de $(G, \star)$ par caractérisation.
   $(1, 0) \in \mathbb{R}^{+\star} \times \mathbb{R}$ donc $\mathbb{R}^{+\star} \times \mathbb{R}$ est non vide.
   Soient $(x, y), (x', y') \in \mathbb{R}^{+\star} \times \mathbb{R}$.
   $(x, y) \star \left(\frac{1}{x'}, -\frac{y'}{x'}\right) = \left(\frac{x}{x'}, \frac{yx'-xy'}{x'}\right) \in \mathbb{R}^{+\star} \times \mathbb{R}$.

Solution Exercice N° 10 : ♦ Soient $x, y \in I$.
$1 + \frac{xy}{c^2} \neq -1$ et donc la quantité $\frac{x+y}{1+\frac{xy}{c^2}}$ est bien définie.
$y - c < 0$ donc $x(y - c) < -c(y - c)$. Ainsi $c(x + y) < c^2 + xy$ puis $\frac{x+y}{1+\frac{xy}{c^2}} < c$.
De même, $y - c < 0$ donc $x(y - c) > c(y - c)$. Ainsi $c(x + y) > -c^2 + xy$ puis $\frac{x+y}{1+\frac{xy}{c^2}} > -c$.
Ainsi $x \star y \in I$ et, par conséquent, $\star$ est une loi de composition interne sur G.
♦ Soient $x, y \in I$.

$$x \star y = \frac{x+y}{1+\frac{xy}{c^2}} = \frac{y+x}{1+\frac{yx}{c^2}} = y \star x.$$

Ainsi $\star$ est commutative.
♦ Soient $x, y, z \in I$.

$$(x \star y) \star z = \frac{x+y}{1+\frac{xy}{c^2}} \star z = \frac{\frac{x+y}{1+\frac{xy}{c^2}} + z}{1 + \frac{\left(\frac{x+y}{1+\frac{xy}{c^2}}\right)z}{c^2}} = \frac{x+y+z+\frac{xyz}{c^2}}{1+\frac{xy+yz+xz}{c^2}}.$$

De même

$$x \star (y \star z) = x \star \frac{y+z}{1+\frac{yz}{c^2}} = \frac{x + \frac{y+z}{1+\frac{yz}{c^2}}}{1 + \frac{x\left(\frac{y+z}{1+\frac{yz}{c^2}}\right)}{c^2}} = \frac{x+y+z+\frac{xyz}{c^2}}{1+\frac{xy+yz+xz}{c^2}}.$$

Ainsi $\star$ est associative.
♦ Soit $x \in I$.

$$x \star 0 = x \text{ et } 0 \star x = x.$$

Ainsi 0 est l'élément neutre de $(I, \star)$.
♦ Soit $x \in I$. $-x \in I$ et
$$x \star (-x) = (-x) \star x = 0.$$
Ainsi x est inversible dans $(I, \star)$. Tous les éléments de $(I, \star)$ sont donc inversibles.

Ainsi $(I, \star)$ est un groupe abélien.

Solution Exercice N° 11 : $\top$ est clairement une loi interne sur $\mathbb{R}$.
La fonction sh étant strictement croissante et continue sur $\mathbb{R}$, elle induit une bijection de $\mathbb{R}$ dans $\operatorname{sh}(\mathbb{R}) = \mathbb{R}$.
Soient $x, y \in \mathbb{R}$. Il existe $u, v \in \mathbb{R}$ tel que $x = \operatorname{sh}(u)$ et $y = \operatorname{sh}(v)$.
Ainsi $x \top y = \operatorname{sh}(u)\sqrt{1+\operatorname{sh}(v)^2} + \operatorname{sh}(v)\sqrt{1+\operatorname{sh}(u)^2} = \operatorname{sh}(u)\operatorname{ch}(v) + \operatorname{sh}(v)\operatorname{ch}(u) = \operatorname{sh}(u+v) = \operatorname{sh}(\operatorname{sh}^{-1}(x) + \operatorname{sh}^{-1}(y))$.
L'exercice N° 5 permet de conclure à l'associativité de $\top$, la commutativité de $\top$ et à l'existence d'un élément neutre $0 = \operatorname{sh}(0)$.
Soit $x \in \mathbb{R}$. On observe que $x \top (-x) = 0$. Par commutativité de la loi $\top$, on en déduit que x est inversible.
On peut donc conclure que $(\mathbb{R}, \top)$ est un groupe abélien.

Solution Exercice N° 12 : $H \subset \mathbb{C}$ et $(\mathbb{C}, +)$ est un groupe.
Montrons que H est un sous-groupe de $(\mathbb{C}, +)$ par caractérisation.
$0 \in H$ donc $H \neq \emptyset$.
Soient $x, y \in H$. Il existe $a, b, a', b' \in \mathbb{Z}$ tels que $x = a + \omega b$ et $y = a' + \omega b'$.
Ainsi $x - y = (a - a') + \omega(b - b') \in H$.

Solution Exercice N° 13 : $H \subset \mathbb{C}^\star$ et $(\mathbb{C}^\star, \times)$ est un groupe.
Montrons que H est un sous-groupe de $(\mathbb{C}^\star, \times)$ par caractérisation.
$1 \in H$ donc $H \neq \emptyset$.
Soient $x, y \in H$. Il existe $n, n' \in \mathbb{Z}$ tels que $x = a^n$ et $y = a^{n'}$.
Ainsi $\frac{x}{y} = a^{n-n'} \in H$.

Solution Exercice N° 14 : $H \subset S_E$ et $(S_E, \circ)$ est un groupe.
Montrons que H est un sous-groupe de $(S_E, \circ)$ par caractérisation.
$\mathrm{Id}_E \in H$ donc $H \neq \emptyset$.
Soient $f, g \in H$. $f(a) = a$ et $g(a) = a$ donc $g^{-1}(a) = a$.
$f \circ g^{-1}(a) = f(g^{-1}(a)) = f(a) = a$. Ainsi $f \circ g \in H$.

Solution Exercice N° 15 :

1. $aHa^{-1} \subset G$ et $(G, \times)$ est un groupe.
   Montrons que aHa^{-1} est un sous-groupe de $(G, \times)$ par caractérisation.
   $e = aea^{-1} \in aHa^{-1}$ donc $aHa^{-1} \neq \emptyset$.
   Soient $x, y \in aHa^{-1}$. Il existe $h, h' \in H$ tels que $x = aha^{-1}$ et $y = ah'a^{-1}$. Ainsi $y^{-1} = ah'^{-1}a^{-1}$ et donc $xy^{-1} = ahh'^{-1}a^{-1}$. Comme $hh'^{-1} \in H$ alors $xy^{-1} \in H$.
2. Si aH est un sous-groupe de $(G, \times)$ alors $e \in aH$. Ainsi il existe $h \in H$ tel que $e = ah$. On en déduit que $a = h^{-1} \in H$.
   Réciproquement, si $a \in H$ alors $aH = H$ et donc aH est un sous-groupe de $(G, \times)$.
   La condition nécessaire et suffisante recherchée est $a \in H$.

Solution Exercice N° 16 : $\mathcal{Z}(G) \subset G$ et $(G, \star)$ est un groupe.
Montrons que $\mathcal{Z}(G)$ est un sous-groupe de $(G, \star)$ par caractérisation.
$e \in \mathcal{Z}(G)$ puisque, pour tout $x \in G$, $x \star e = e \star x = e$, et donc $\mathcal{Z}(G) \neq \emptyset$.
Soient $x, y \in \mathcal{Z}(G)$.
Soit $u \in G$. Comme $x \in \mathcal{Z}(G)$ alors $x \star u = u \star x$. Comme $y \in \mathcal{Z}(G)$ alors $y \star u = u \star y$ puis $u \star y^{-1} = y^{-1} \star u$.
$$(x \star y^{-1}) \star u = x \star (y^{-1} \star u) = x \star (u \star y^{-1}) = (x \star u) \star y^{-1} = (u \star x) \star y^{-1} = u \star (x \star y^{-1}).$$
Ainsi $x \star y^{-1} \in \mathcal{Z}(G)$.

Solution Exercice N° 17 :

1. $H \cap K \subset G$ et $(G, \star)$ est un groupe.
   Montrons que $H \cap K$ est un sous-groupe de $(G, \star)$ par caractérisation.
   $e \in H$ et $e \in K$ donc $e \in H \cap K$ et donc $H \cap K \emptyset$.
   Soient $x, y \in H \cap K$. Comme H est un sous-groupe de $(G, \star)$ alors $x \star y^{-1} \in H$. Comme H est un sous-groupe de $(G, \star)$ alors $x \star y^{-1} \in K$. Ainsi $x \star y^{-1} \in H \cap K$.

   Bien évidemment, ce résultat subsiste pour une intersection quelconque de sous-groupes.
2. " $\Leftarrow$: Si $H \subset K$ alors $H \cup K = K$ et si $K \subset H$ alors $H \cup K = H$.
   Dans le deux cas, $H \cup K$ est un sous-groupe de $(G, \star)$.
   " $\Rightarrow$ " Par contraposée. On suppose que $H \not\subset K$ et que $K \not\subset H$.
   Ainsi il existe $h \in H$ tel que $h \notin K$ et il existe $k \in K$ tel que $k \notin H$.
   De ce fait $h \in H \cup K$ et $k \in H \cup \mathbb{K}$.
   Si $h \star k \in H$ alors $k = h^{-1} \star (h \star k) \in H$. C'est absurde.
   On fait de même su $h \star k \in K$.
   Ainsi $h \star k \notin H \cup K$.
   $H \cup K$ n'est pas stable par $\star$, ce n'est donc pas un sous-groupe de $(G, \star)$.

Solution Exercice N° 18 :

1. Comme A est fini puisque inclus dans G alors il existe $n < k \in \mathbb{N}$ tels que $x^k = x^n$.
   Ainsi l'application φ n'est pas injective.
2. Comme $x^k = x^n$ alors $x^{k-n} = 1$. Ainsi x est inversible d'inverse x^{k-n-1}.

   A est une partie de G et $(G, \star)$ est un groupe.
   Montrons que A est un sous-groupe de $(G, \star)$ par caractérisation.
   A est non vide par hypothèse.
   Soient $x, y \in A$. Par ce qui précède $y^{-1} \in A$.
   G est stable pour $\star$ donc $x \star y^{-1} \in A$.

Solution Exercice N° 19 :

1. Notons $s_{\mathbb{C}}$ l'ensemble des similitude directes du plan complexe.
   On a : $s_{\mathbb{C}} = \{f_{a,b} : z \mapsto az + b \ / \ a \in \mathbb{C}^\star, b \in \mathbb{C}\}$.
   Soit $f_{a,b} \in s_{\mathbb{C}}$. On observe que $f_{a,b}$ est bijective et que $f_{a,b}^{-1} = f_{\frac{1}{a}, -\frac{b}{a}}$.
   Ainsi $s_C \subset S_C$ et $(S_C, \circ)$ est un groupe.
   Montrons que s_C est un sous-groupe de $(S_{\mathbb{C}}, \circ)$ par caractérisation.
   $\mathrm{Id}_{\mathbb{C}} = f_{1,0} \in s_{\mathbb{C}}$ donc $s_{\mathbb{C}}$ est non vide.
   Soient $f_{a,b}, f_{a',b'} \in s_C$.
   On a $f_{a,b} \circ f_{a',b'}^{-1} = f_{\frac{a}{a'}, \frac{ba'-ab'}{a'}} \in s_{\mathbb{C}}$.
   On en déduit que $(s_{\mathbb{C}}, \circ)$ est un groupe en tant que sous-groupe d'un groupe.
2. ♦ Notons $t_{\mathbb{C}} = \{f_{1,b} \ / \ b \in \mathbb{C}\}$ l'ensemble des translations de $s_{\mathbb{C}}$.
   On a $t_{\mathbb{C}} \subset s_{\mathbb{C}}$ et $(s_{\mathbb{C}}, \circ)$ est un groupe.
   Montrons que $t_{\mathbb{C}}$ est un sous-groupe de $(s_{\mathbb{C}}, \circ)$ par caractérisation.
   $\mathrm{Id}_{\mathbb{C}} = f_{1,0} \in t_{\mathbb{C}}$ donc $t_{\mathbb{C}}$ est non vide.
   Soient $f_{1,b}, f_{1,b'} \in t_{\mathbb{C}}$.
   On a $f_{1,b} \circ f_{1,b'}^{-1} = f_{1,b-b'} \in t_{\mathbb{C}}$.

   ♦ Notons $h_{\mathbb{C}}$ l'ensemble des homothéties de $s_{\mathbb{C}}$.
   $f_{2,2} \in h_{\mathbb{C}}$ et $f_{1/2,1} \in h_{\mathbb{C}}$ alors que $f_{2,2} \circ f_{1/2,1} = f_{1,2} \notin h_{\mathbb{C}}$.
   Ainsi $h_{\mathbb{C}}$ n'est pas un sous-groupe de $(s_{\mathbb{C}}, \circ)$.

   ♦ Notons $r_{\mathbb{C}}$ l'ensemble des homothéties de $r_{\mathbb{C}}$.
   $f_{-1,2} \in r_{\mathbb{C}}$ et $f_{-1,1} \in r_{\mathbb{C}}$ alors que $f_{-1,2} \circ f_{-1,1} = f_{1,1} \notin r_{\mathbb{C}}$.
   Ainsi $r_{\mathbb{C}}$ n'est pas un sous-groupe de $(s_{\mathbb{C}}, \circ)$.
3. Notons a l'affixe de A.

   ♦ Notons $h_{\mathbb{C}}^A = \{f_{\lambda, a(1-\lambda)} \ / \ a \in \mathbb{R}^\star\}$ l'ensemble des homothéties de $s_{\mathbb{C}}$ de centre A.
   Montrons que $h_{\mathbb{C}}^A$ est un sous-groupe de $(s_{\mathbb{C}}, \circ)$ par caractérisation.
   $\mathrm{Id}_{\mathbb{C}} = f_{1,0} \in h_{\mathbb{C}}^A$ et donc $h_{\mathbb{C}}^A \neq \emptyset$.
   Soient $f_{\lambda, a(1-\lambda)}, f_{\mu, a(1-\mu)} \in h_{\mathbb{C}}^A$. Alors

   $$f_{\lambda, a(1-\lambda)} \circ f_{\mu, a(1-\mu)}^{-1} = f_{\frac{\lambda}{\mu}, a(1-\frac{\lambda}{\mu})} \in h_{\mathbb{C}}^A.$$

   Ainsi $h_{\mathbb{C}}^A$ est un sous-groupe de $(s_{\mathbb{C}}, \circ)$.

   ♦ Notons $r_{\mathbb{C}}^A = \{f_{e^{i\theta}, a(1-e^{i\theta})} \ / \ \theta \in \mathbb{R}\}$ l'ensemble des rotations de $s_{\mathbb{C}}$ de centre A.
   Montrons que $r_{\mathbb{C}}^A$ est un sous-groupe de $(s_{\mathbb{C}}, \circ)$ par caractérisation.
   $\mathrm{Id}_{\mathbb{C}} = f_{1,0} \in r_{\mathbb{C}}^A$ et donc $r_{\mathbb{C}}^A \neq \emptyset$.
   Soient $f_{\lambda, a(1-\lambda)}, f_{\mu, a(1-\mu)} \in h_{\mathbb{C}}^A$. Alors

   $$f_{e^{i\theta}, a(1-e^{i\theta})} \circ f_{e^{i\theta'}, a(1-e^{i\theta'})}^{-1} = f_{e^{i\theta-\theta'}, a(1-e^{i\theta-\theta'})} \in r_{\mathbb{C}}^A.$$

   Ainsi $r_{\mathbb{C}}^A$ est un sous-groupe de $(s_{\mathbb{C}}, \circ)$.

Solution Exercice N° 20 :

" $\Leftarrow$: D'après le cours, $\mathbb{U}_n$ est un sous-groupe de $(\mathbb{C}^\star, \times)$. De plus, $\mathbb{U}_n$ contient n élément donc est un sous-groupe fini de $(\mathbb{C}^\star, \times)$.
" $\Rightarrow$: Soit H un sous-groupe fini de $(\mathbb{C}^\star, \times)$.
♦ Notons n le nombre d'élément de G. Si $n = 1$ alors le résultat est banal. On suppose donc $n \geqslant 2$.
♦ Soit $z \in H$. Pour tout $k \in \mathbb{N}$, $z^k \in H$. Comme H est fini donc il existe $k < \ell \in N$ tels que $z^k = z^\ell = 1$. Ainsi $z^{\ell-k} = 1$. En particulier, tous les éléments de H sont racine de l'unité. En particulier, tous les éléments de H sont de module 1.
♦ On écrit $H = \{1, e^{i\theta_1}, \cdots, e^{i\theta_{n-1}}\}$ avec $0 < \theta_1 < \cdots < \theta_{n-1} < 2\pi$.
♦ Montrons que $H = \{e^{i\theta_1 k} \ / \ k \in \mathbb{N}\}$ par double inclusion.
" $\supset$ " : Cette inclusion est claire car $e^{i\theta_1 k} = \left(e^{i\theta_1}\right)^k$, que $e^{i\theta_1} \in H$ et que H est un sous-groupe de $(\mathbb{C}^\star, \times)$.

" $\subset$ " : Soit $1 \leqslant i \leqslant n-1$. On note $k = \left\lfloor \frac{\theta_i}{\theta_1} \right\rfloor \in \mathbb{N}$ et $r = \theta_i - k\theta_1$ de sorte que $\theta_i = k\theta_1 + r$ avec $0 \leqslant r < \theta_1$.
Alors $e^{ir} = e^{i\theta_i} \times \left(e^{i\theta_1}\right)^{-k} \in H$. Par conséquent $r = 0$ puis $\theta_i = k\theta_1$ avec $k \in \mathbb{N}$.
Cela prouve la seconde inclusion et on a bien

$$H = \{e^{i\theta_1 k} \ / \ k \in \mathbb{N}\}.$$

♦ Comme $e^{i\theta_1}$ est une racine de l'unité alors il existe deux entiers a et b tels que $a \wedge b = 1$, $1 \leqslant a < b$ et $e^{i\theta_1} = e^{\frac{2i\pi a}{b}}$. Ainsi

$$H = \{e^{\frac{2i\pi ak}{b}} \ / \ k \in \mathbb{N}\}.$$

♦ Soit $k \in \mathbb{N}$.
On note $u = \left\lfloor \frac{ka}{b} \right\rfloor \in \mathbb{N}$ et $r = ka - bu$ de sorte que $ka = bu + r$ avec $0 \leqslant r < b$. Alors

$$e^{\frac{2i\pi ak}{b}} = e^{\frac{2i\pi(bu+r)}{b}} = e^{\frac{2i\pi r}{b}}.$$

Ainsi

$$H = \{e^{\frac{2i\pi ar}{b}} \ / \ 0 \leqslant r \leqslant b-1\}.$$

♦ Les éléments $\left(e^{\frac{2i\pi ar}{b}}\right)_{0 \leqslant r \leqslant b-1}$ sont deux à deux distincts et, par conséquent, $b = n$. On en déduit que $H = \mathbb{U}_n$.

Solution Exercice N° 21 :

1. ♦ $+$ et $\star$ sont les lois de composition internes sur $\mathbb{Z}^2$.
♦ Soient $(a,b), (c,d) \in \mathbb{Z}^2$.

$$(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b).$$

Donc $+$ est commutative sur $\mathbb{Z}^2$.
♦ Soient $(a,b), (c,d) \in \mathbb{Z}^2$.

$$(a,b) \star (c,d) = (ac, ad+bc) = (ca, cb+da) = (c,d) \star (a,b).$$

Donc $\star$ est commutative sur $\mathbb{Z}^2$.
♦ Soient $(a,b), (c,d), (e,f) \in \mathbb{Z}^2$.

$$((a,b) + (c,d)) + (e,f) = (a+c, b+d) + (e,f) = (a+b+e, c+d+f) = (a,b) + ((c,d) + (e,f)).$$

Donc $+$ est associative sur $\mathbb{Z}^2$.
♦ Soient $(a,b), (c,d), (e,f) \in \mathbb{Z}^2$.

$$((a,b) \star (c,d)) \star (e,f) = (ac, ad+bc) \star (e,f) = (ace, acf + (ad+bc)e) = (ace, acf + ade + bce).$$

De même,

$$(a,b) \star ((c,d) \star (e,f)) = (a,b) \star (ce, cf+de) = (ace, a(cf+de) + bce) = (ace, acf + ade + bce).$$

Donc $\star$ est associative sur $\mathbb{Z}^2$.
♦ Soit $(a,b) \in \mathbb{Z}^2$.

$$(a,b) + (0,0) = (a+0, b+0) = (a,b).$$

Par commutativité de $+$, on en déduit que $+$ possède un élément neutre.
♦ Soit $(a,b) \in \mathbb{Z}^2$.

$$(a,b) \star (1,0) = (a \times 1, a \times 0 + b \times 1) = (a,b).$$

Par commutativité de $\star$, on en déduit que $\star$ possède un élément neutre.
♦ Soit $(a,b) \in \mathbb{Z}^2$.

$$(a,b) + (-a,-b) = (0,0).$$

Par commutativité de $+$, on en déduit que (a,b) est inversible pour la loi $+$.
♦ Soient $(a,b), (c,d), (e,f) \in \mathbb{Z}^2$.

$$(a,b) \star ((c,d) + (e,f)) = (a,b) \star (c+e, d+f) = (a(c+e), a(d+f) + b(c+e)) = (ac+ae, ad+af+bc+be).$$

De même

$$((a,b) \star (c,d)) + ((a,b) \star (e,f)) = (ac, ad+bc) + (ae, af+be) = (ac+ae, ad+bc+af+be).$$

Ainsi, par commutativité de $+$ et $\star$, on en déduit que $\star$ est distributive par rapport à $+$.

$(\mathbb{Z}^2, +, \star)$ est un anneau commutatif.

2. $A \subset \mathbb{Z}^2$ et $(\mathbb{Z}^2, +, \star)$ est un anneau commutatif.
Montrons que A est un sous-anneau de $(\mathbb{Z}^2, +, \star)$ par caractérisation.
♦ $(1, 0) \in A$.
♦ Soient $(a, 0), (a', 0) \in A$.
$$(a, 0) - (a', 0) = (a - a', 0) \in A.$$
♦ Soient $(a, 0), (a', 0) \in A$.
$$(a, 0) \star (a', 0) = (aa', a \times 0 + a' \times 0) = (aa', 0).$$

Solution Exercice N° 22 :

1. Comme x et y commutent alors, par une récurrence immédiate, pour tout $n \in \mathbb{N}$, $(xy)^n = x^n y^n$.
En choisissant un $n \in \mathbb{N}$ vérifiant $x^n = 0$ alors on obtient que $(xy)^n = 0$.
Ainsi xy est nilpotent.
2. Considérons $p \in \mathbb{N}$ tel que $x^p = 0$ et $n \in \mathbb{N}$ tel que $y^n = 0$.
Par la formule du binôme de Newton (applicable puisque x et y commutent), on obtient
$$(x + y)^{p+n} = \sum_{k=0}^{p+n} \binom{p+n}{k} x^k y^{p+n-k} = \sum_{k=0}^{n-1} \binom{p+n}{k} x^k y^{p+n-k}.$$
En effectuant le changement d'indice $i = p + n - k$, on obtient
$$(x + y)^{p+n} = \sum_{i=p+1}^{p+n} \binom{p+n}{i+p+1} x^{p+n-i} y^i = 0.$$
Ainsi $x + y$ est nilpotent.
3. Par une récurrence immédiate, pour tout $n \in \mathbb{N}^\star$, $(yx)^n = y(xy)^{n-1}x$.
En considérant n tel que $(xy)^n = 0$, on obtient $(yx)^{n+1} = 0$.
Ainsi yx est nilpotent.
4. Soit $n \in \mathbb{N}$ tel que $x^n = 0$. Posons
$$y = \sum_{k=0}^{n} x^k.$$
Par télescopage, on obtient
$$(1 - x)y = y - xy = \sum_{k=0}^{n} x^k - \sum_{k=0}^{n} x^{k+1} = \sum_{k=0}^{n} (x^k - x^{k+1}) = 1 - x^{n+1} = 1.$$
De même, on montre que $y(1 - x) = 1$.
Ainsi $1 - x$ est inversible et
$$(1 - x)^{-1} = \sum_{k=0}^{n} x^k = \sum_{k=0}^{+\infty} x^k.$$

Solution Exercice N° 23 : $\mathbb{Z}\left[\sqrt{d}\right]$ est une partie de $\mathbb{R}$ et $(\mathbb{R}, +, \times)$ est un anneau commutatif.

Montrons que $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$ par caractérisation.

— $1 = 1 + 0 \times \sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$.

— Soient $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$.
$$a + b\sqrt{d} - (a' + b'\sqrt{d}) = a - a' + \sqrt{d}(b - b') \in \mathbb{Z}\left[\sqrt{d}\right].$$

— Soient $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Z}\left[\sqrt{d}\right]$.
$$(a + b\sqrt{d}) \times (a' + b'\sqrt{d}) = aa' + dbb' + \sqrt{d}(ab' + a'b) \in \mathbb{Z}\left[\sqrt{d}\right].$$

Solution Exercice N° 24 : $\mathbb{D} \subset \mathbb{Q}$ et $(\mathbb{Q}, +, \times)$ est un anneau.
Montrons que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ par caractérisation.

— $1 = \frac{1}{10^0} \in \mathbb{D}$.

— Soient $\frac{n}{10^k}, \frac{n'}{10^{k'}} \in \mathbb{D}$.
$$\frac{n}{10^k} - \frac{n'}{10^{k'}} = \frac{10^{k'}n - 10^k n'}{10^{k+k'}} \in \mathbb{D}.$$

— Soient $\frac{n}{10^k}, \frac{n'}{10^{k'}} \in \mathbb{D}$.

$$\frac{n}{10^k} \times \frac{n'}{10^{k'}} = \frac{nn'}{10^{k+k'}} \in \mathbb{D}.$$

Solution Exercice N° 25 :

1. $\mathbb{Z}[i]$ est une partie de $\mathbb{C}$ et $(\mathbb{C}, +, \times)$ est un anneau commutatif.
   Montrons que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$ par caractérisation.
   — $1 = 1 + 0 \times i \in \mathbb{Z}[i]$.
   — Soient $a + ib, a' + ib' \in \mathbb{Z}[i]$.
   $$a + ib - (a' + ib') = a - a' + i(b - b') \in \mathbb{Z}[i].$$
   — Soient $a + ib, a' + ib' \in \mathbb{Z}[i]$.
   $$(a + ib) \times (a' + ib') = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i].$$
2. Soit $z = a + ib \in \mathbb{Z}[i]^\star$.
   Il existe $u = \alpha + i\beta \in \mathbb{Z}[i]^\star$ tel que $uz = 1$.
   En particulier $|u|^2 \times |z|^2 = 1$.
   Comme $|u|^2 \in \mathbb{Z}$ et $|z|^2 \in \mathbb{Z}$ alors $|u|^2 \in \mathbb{Z}^\star = \{\pm 1\}$.
   Comme $|z|^2 \geqslant 0$ alors $|z|^2 = 1$ puis $a^2 + b^2 = 1$.
   Ainsi $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ puis $z \in \{1, -1, i, -i\}$.
   Réciproquement $1 \times 1 = 1$, $(-1) \times (-1) = 1$ et $i \times (-i) = 1$ et donc $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$.
   Ainsi $\mathbb{Z}[i] = \{1, -1, i, -i\}$.

Solution Exercice N° 26 :

1. A est une partie de $\mathbb{Q}$ et $(\mathbb{Q}, +, \times)$ est un anneau commutatif.
   Montrons que A est un sous-anneau de $(\mathbb{Q}, +, \times)$ par caractérisation.
   — $1 = \frac{1}{1} \in A$.
   — Soient $\frac{m}{n}, \frac{m'}{n'} \in A$.
   $$\frac{m}{n} - \frac{m'}{n'} = \frac{mn' - m'n}{nn'} \in A$$
   puisque nn' est impair.
   — Soient $\frac{m}{n}, \frac{m'}{n'} \in A$.
   $$\frac{m}{n} \times \frac{m'}{n'} = \frac{mm'}{nn'} \in A$$
   puisque nn' est impair.
2. Soient $\frac{m}{n} \in A$. Avec $m \wedge n = 1$ et n impair.
   L'inverse de $\frac{m}{n}$ dans $\mathbb{Q}$ est $\frac{n}{m}$. Cet inverse est dans A si, et seulement si, m est impair.
   Ainsi $A^\star = \{\frac{m}{n} \;/\; m \wedge n = 1 \text{ et } m, n \text{ impairs}\}$.

Solution Exercice N° 27 :

♦ $\top$ et $\star$ sont des lois de composition internes sur $\mathbb{R}$.
♦ Soient $a, b \in \mathbb{R}$.

$$a \top b = a + b - 1 = b + a - 1 = b \top a.$$

$\top$ est donc commutative sur $\mathbb{R}$.
♦ Soient $a, b \in \mathbb{R}$.

$$a \star b = ab - a - b + 2 = ba - b - a + 2 = b \star a.$$

$\star$ est donc commutative sur $\mathbb{R}$.
♦ Soient $a, b, c \in \mathbb{R}$.

$$(a \top b) \top c = (a + b - 1) \top c = a + b - 1 + c - 1 = a + (b + c - 1) - 1 = a \top (b + c - 1) = a \top (b \top c).$$

Ainsi $\top$ est associative sur $\mathbb{R}$.
♦ Soient $a, b, c \in \mathbb{R}$.

$$(a \star b) \star c = (ab - a - b + 2) \star c = (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 = abc - ac - bc - ab + a + b + c.$$

De même

$$a \star (b \star c) = a \star (bc - b - c + 2) = a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 = abc - ab - ac - bc + a + b + c.$$

Ainsi $\star$ est associative sur $\mathbb{R}$.
♦ Soit $a \in \mathbb{R}$

$$a \top 1 = a + 1 - 1 = a.$$

Par commutativité de $\top$, on en déduit que $\top$ possède un élément neutre qui est 1.
♦ Soit $a \in \mathbb{R}$

$$a \top (2 - a) = a + (2 - a) - 1 = 1$$

Par commutativité de $\top$, on en déduit que a est inversible dans $(\mathbb{R}, \top)$.

♦ Soit $a \in \mathbb{R}$

$$a \star 2 = 2a - a - 2 + 2 = a.$$

Par commutativité de $\star$, on en déduit que $\star$ possède un élément neutre qui est 2.

♦ Soit $a \in \mathbb{R} \setminus \{1\}$

$$a \top \frac{a}{a-1} = a\frac{a}{a-1} - \frac{a}{a-1} - a + 2 = 2$$

Par commutativité de $\top$, on en déduit que a est inversible dans $(\mathbb{R}, \star)$.

♦ Soient $a, b, c \in \mathbb{R}$.

$$a \star (b \top c) = a \star (b + c - 1) = a(b + c - 1) - a - (b + c - 1) + 2 = ab + ac - 2a - b - c + 3.$$

De même,

$$(a \star b) \top (a \star c) = (ab - a - b + 2) \top (ac - a - c + 2) = ab - a - b + 2 + ac - a - c + 2 - 1 = ab + ac - 2a - b - c + 3.$$

Par commutativité de $\top$ et $\star$, on en déduit que $\star$ est distributive par rapport à $\top$.

$(\mathbb{R}, \top, \star)$ est un corps commutatif.

Solution Exercice N° 28 : $\mathbb{Q}\left[\sqrt{d}\right]$ est une partie de $\mathbb{R}$ et $(\mathbb{R}, +, \times)$ est un anneau commutatif.

Montrons que $\mathbb{Q}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$ par caractérisation.

— $1 = 1 + 0 \times \sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$.

— Soient $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$.

$$a + b\sqrt{d} - (a' + b'\sqrt{d}) = a - a' + \sqrt{d}(b - b') \in \mathbb{Q}\left[\sqrt{d}\right].$$

— Soient $a + b\sqrt{d}, a' + b'\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$.

$$(a + b\sqrt{d}) \times (a' + b'\sqrt{d}) = aa' + dbb' + \sqrt{d}(ab' + a'b) \in \mathbb{Q}\left[\sqrt{d}\right].$$

— Soit $a + b\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right] \setminus \{0\}$.
  $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2} = \frac{a}{a^2-db^2} - \frac{b}{a^2-db^2}\sqrt{d} \in \mathbb{Q}\left[\sqrt{d}\right]$.
  Ainsi $(a + b\sqrt{d})^{-1} \in \mathbb{Q}\left[\sqrt{d}\right]$.

Solution Exercice N° 29 : Soit F un sous-corps de $(\mathbb{Q}, +, \times)$.
Nécessairement $0 \in F$ et $1 \in F$.
Montrons par récurrence que, pour tout $n \in \mathbb{N}$, $n \in F$.

— La propriété est vrai au rang $n = 0$ puisque $0 \in F$.

— Supposons donné $n \in \mathbb{N}$ tel que $n \in F$. Montrons que $n + 1 \in F$.
  $n \in F$, $1 \in F$ et F est stable par addition. Ainsi $n + 1 \in F$.

La récurrence est achevée.
Soit $n \in \mathbb{Z} \setminus \mathbb{N}$. Par ce qui précède $-n \in \mathbb{N}$. Comme F est stable par passage à l'opposée, on en déduit que $n \in F$.
On en déduit que, pour tout $n \in \mathbb{Z}$, $n \in F$.
Enfin comme F est stable par produit et par passage à l'inverse, on en déduit que, pour tout $n \in \mathbb{Z}$, pour tout $m \in \mathbb{N}^\star$, $\frac{m}{n} \in F$.
On en déduit alors que $\mathbb{Q} \subset F$.
Comme F est une partie de $\mathbb{Q}$ alors $\mathbb{Q} = F$.