Structures algébriques

Loi de composition interne

Exercice 1 [02190] [correction]
On définit une loi de composition interne $\star$ sur $\mathbb{R}$ par

$$\forall (a,b) \in \mathbb{R}^2,\ a \star b = \ln(\mathrm{e}^a + \mathrm{e}^b)$$

Quelles en sont les propriétés ? Possède-t-elle un élément neutre ? Y a-t-il des éléments réguliers ?

Exercice 2 [02191] [correction]
Soit $E = [0,1]$. On définit une loi $\star$ sur E par

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

a) Montrer que $\star$ est une loi de composition interne commutative et associative.
b) Montrer que $\star$ possède un neutre.
c) Quels sont les éléments symétrisables ? réguliers ?

Exercice 3 [02192] [correction]
Soit $\star$ une loi de composition interne sur E.
Pour $A, B \in \mathcal{P}(E)$ on pose

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

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

Exercice 4 [02193] [correction]
Soit E un ensemble et $f : E \to E$.
Montrer que f est un élément régulier de $(E^E, \circ)$ si, et seulement si, f est bijective.

Exercice 5 [02194] [correction]
Soit a un élément d'un ensemble E muni d'une loi $\star$ associative.
Montrer que a est symétrisable si, et seulement si, l'application $f : E \to E$ définie par $f(x) = a \star x$ est bijective.

Exercice 6 [02195] [correction]
Soit $\star$ une loi associative sur un ensemble E. Un élément x de E est dit idempotent si, et seulement si, $x \star x = x$.
a) Montrer que si x et y sont idempotents et commutent, alors $x \star y$ est idempotent.
b) Montrer que si x est idempotent et inversible, alors x^{-1} est idempotent.

Exercice 7 [02196] [correction]
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 :

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

a) Montrer que si $\star$ est commutative (resp. associative) alors $\top$ l'est aussi.
b) Montrer que si $\star$ possède un neutre e alors $\top$ possède aussi un neutre à préciser.

Exercice 8 [02197] [correction]
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.
a) Montrer que $e = a \star b$ et $e' = b \star a$ sont neutres resp. à gauche et à droite puis que $e = e'$.
b) Montrer que a est symétrisable et f bijective.

Exercice 9 [02198] [correction]
Soient $\star$ une loi de composition interne associative sur un ensemble fini E et x un élément régulier de E. Montrer que E possède un neutre.

Exercice 10 [02199] [correction]
Soit $\star$ une loi associative sur un ensemble E fini. On suppose que la loi $\star$ possède un neutre e.
Montrer que tout élément régulier de E est inversible.

Exercice 11 [02200] [correction]
Soit A une partie d'un ensemble E. On appelle fonction caractéristique de la partie A dans E, l'application $1_A : E \to \mathbb{R}$ définie par :

$$1_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{sinon} \end{cases}$$

De quels ensembles les fonctions suivantes sont-elles les fonctions caractéristiques ?

a) $\min(1_A, 1_B)$ b) $\max(1_A, 1_B)$ c) $1_A.1_B$
d) $1 - 1_A$ e) $1_A + 1_B - 1_A.1_B$ f) $1_A + 1_B - 1\chi_A.\chi_B$

Exercice 12 [03043] [correction]
Soit E un ensemble fini non vide muni d'une loi de composition interne associative notée $\top$.
Montrer qu'il existe $e \in E$ tel que $e \top e = e$.

Groupes

Exercice 13 [02201] [correction]
Soit $(G, \star)$ un groupe tel que

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

Montrer que G est commutatif.

Exercice 14 [02202] [correction]
Soit $\star$ une loi de composition interne sur un ensemble E associative et possédant un neutre e. On suppose que

$$\forall x \in E, x^{\star 2} = e$$

Montrer que $(E, \star)$ est un groupe abélien.

Exercice 15 [02203] [correction]
Soit $\star$ une loi de composition interne associative sur un ensemble E fini.
On suppose que tous les éléments de E sont réguliers. Montrer que E est un groupe.

Exercice 16 [02204] [correction]
Soit $(G, \star)$ un groupe à n éléments.
Justifier que sa table de composition est un carré latin c'est à dire que tout élément de G figure une fois et une seule dans chaque ligne et dans chaque colonne.

Exercice 17 [02205] [correction]
Soit $G = \mathbb{R}^\star \times \mathbb{R}$ et $\star$ la loi de composition interne définie sur G par

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

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

Exercice 18 [02206] [correction]
Sur $G = \left]-1, 1\right[$ on définit une loi $\star$ par

$$\forall x, y \in G, x \star y = \frac{x+y}{1+xy}$$

Montrer que $(G, \star)$ est un groupe abélien.

Exercice 19 [02207] [correction]
[Addition des vitesses en théorie de la relativité]
Soit $c > 0$ (c correspond à la vitesse - ou célérité - de la lumière) et $I = \left]-c, c\right[$.
a) Montrer

$$\forall (x, y) \in I^2,\ x \star y = \frac{x+y}{1+\frac{xy}{c^2}} \in I$$

b) 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.

Sous-groupe

Exercice 20 [02208] [correction]
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 21 [02209] [correction]
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 22 [02210] [correction]
Soit a un élément d'un ensemble E. On forme $H = \{f \in \mathcal{S}_E / f(a) = a\}$.
Montrer que H est un sous-groupe du groupe de permutation $(\mathcal{S}_E, \circ)$

Exercice 23 [02211] [correction]
Soit $(G, \times)$ un groupe, H un sous groupe de $(G, \times)$ et $a \in G$.
a) Montrer que $aHa^{-1} = \left\{axa^{-1} / x \in H\right\}$ est un sous groupe de $(G, \times)$.
b) A quelle condition simple $aH = \{ax / x \in H\}$ est un sous groupe de $(G, \times)$?

Exercice 24 [02212] [correction]
On appelle centre d'un groupe $(G, \star)$, la partie C de G définie par

$$C = \{x \in G \mid \forall y \in G, x \star y = y \star x\}$$

Montrer que C est un sous-groupe de $(G, \star)$.

Exercice 25 [02213] [correction]
Soit $f_{a,b} : \mathbb{C} \to \mathbb{C}$ définie par $f_{a,b}(z) = az + b$ avec $a \in \mathbb{C}^\star, b \in \mathbb{C}$.
Montrer que $(\{f_{a,b} / a \in \mathbb{C}^\star, b \in \mathbb{C}\}, \circ)$ est un groupe.

Exercice 26 [02214] [correction]
On considère les applications de $E = \mathbb{R} \setminus \{0, 1\}$ dans lui-même définies par :

$$i(x) = x, f(x) = 1 - x, g(x) = \frac{1}{x}, h(x) = \frac{x}{x-1}, k(x) = \frac{x-1}{x}, \ell(x) = \frac{1}{1-x}$$

a) Démontrer que ce sont des permutations de E.
b) Construire la table donnant la composée de deux éléments quelconques de l'ensemble $G = \{i, f, g, h, k, l\}$.
c) Montrer que G muni de la composition des applications est un groupe non commutatif.

Exercice 27 [02215] [correction]
Soit H et K deux sous-groupes d'un groupe $(G, \star)$ tels que $H \cup K$ en soit aussi un sous-groupe. Montrer que $H \subset K$ ou $K \subset H$.

Exercice 28 [02216] [correction]
Soient $(G, \star)$ un groupe et A une partie finie non vide de G stable pour $\star$.
a) Soient $x \in A$ et $\varphi : \mathbb{N} \to G$ l'application définie par $\varphi(n) = x^n$.
Montrer que φ n'est pas injective.
b) En déduire que $x^{-1} \in A$ puis que A est un sous-groupe de $(G, \star)$.

Exercice 29 [02217] [correction]
Pour $a \in \mathbb{N}$, on note $a\mathbb{Z} = \{ak / k \in \mathbb{Z}\}$.
a) Montrer que $a\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
On se propose de montrer que, réciproquement, tout sous groupe de $\mathbb{Z}$ est de cette forme.
b) Vérifier que le groupe $\{0\}$ est de la forme voulue.
Soit H un sous-groupe de $(\mathbb{Z}, +)$ non réduit à $\{0\}$.
c) Montrer que $H^+ = \{h \in H \mid h > 0\}$ possède un plus petit élément. On note $a = \min H^+$.
d) Etablir que $a\mathbb{Z} \subset H$.
e) En étudiant le reste de la division euclidienne d'un élément de H par a montrer que $H \subset a\mathbb{Z}$.
f) Conclure que pour tout sous-groupe H de $\mathbb{Z}$, il existe un unique $a \in \mathbb{N}$ tel que $H = a\mathbb{Z}$.

Exercice 30 [03354] [correction]
Pour $n \in \mathbb{N}^\star$, on note U_n l'ensemble des racines $n$ème de l'unité :

$$U_n = \{z \in \mathbb{C} / z^n = 1\}$$

Montrer que

$$V = \bigcup_{n \in \mathbb{N}^\star} U_n$$

est un groupe multiplicatif.

Morphisme de groupes

Exercice 31 [02218] [correction]
Soient $n \in \mathbb{N}^\star$ et $f : \mathbb{R}^\star \to \mathbb{R}$ définie par $f(x) = x^n$.

Montrer que f est un morphisme du groupe $(\mathbb{R}^\star, \times)$ dans lui-même.
En déterminer image et noyau.

Exercice 32 [02219] [correction]
Justifier que $\exp : \mathbb{C} \to \mathbb{C}^\star$ est un morphisme du groupe $(\mathbb{C}, +)$ vers $(\mathbb{C}^\star, \times)$.
En déterminer image et noyau.

Exercice 33 [02220] [correction]
Soit G un groupe noté multiplicativement.
Pour $a \in G$, on note τ_a l'application de G vers G définie par $\tau_a(x) = axa^{-1}$.
a) Montrer que τ_a est un morphisme du groupe $(G, \times)$ dans lui-même.
b) Vérifier que

$$\forall a, b \in G,\ \tau_a \circ \tau_b = \tau_{ab}$$

c) Montrer que τ_a est bijective et déterminer son application réciproque.
d) En déduire que $\mathcal{T} = \{\tau_a \mid a \in G\}$ muni du produit de composition est un groupe.

Exercice 34 [02221] [correction]
Soit $(G, \star)$, $(G', \top)$ deux groupes et $f : G \to G'$ un morphisme de groupes.
a) Montrer que pour tout sous-groupe H de G, $f(H)$ est un sous-groupe de $(G', \top)$.
b) Montrer que pour tout sous-groupe H' de G', $f^{-1}(H')$ est un sous-groupe de $(G, \star)$.

Exercice 35 [02222] [correction]
On note $\mathrm{Aut}(G)$ l'ensemble des isomorphismes d'un groupe $(G, \star)$ dans lui-même.
Montrer que $\mathrm{Aut}(G)$ est un sous-groupe du groupe des permutations $(\mathcal{S}_G, \circ)$.

Exercice 36 [02223] [correction]
Soit $(G, \star)$ un groupe et $a \in G$.
On définit une loi de composition interne $\top$ sur G par $x \top y = x \star a \star y$.
a) Montrer que $(G, \top)$ est un groupe.
b) Soit H un sous groupe de $(G, \star)$ et $K = \mathrm{sym}(a) \star H = \{\mathrm{sym}(a) \star x / x \in H\}$.
Montrer que K est un sous groupe de $(G, \top)$.
c) Montrer que $f : x \mapsto x \star \mathrm{sym}(a)$ est un isomorphisme de $(G, \star)$ vers $(G, \top)$.

Etude du groupe symétrique

Exercice 37 [02224] [correction]
Soient n un entier supérieur à 2, $(i, j) \in \{1, 2, \ldots, n\}^2$ tel que $i \neq j$ et $\sigma \in \mathcal{S}_n$.
Montrer que σ et $\tau = \begin{pmatrix} i & j \end{pmatrix}$ commutent si, et seulement si, $\{i, j\}$ est stable par σ.

Exercice 38 [02225] [correction]
Dans $\mathcal{S}_n$ avec $n \geqslant 2$, on considère une permutation σ et un p-cycle :

$$c = \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix}$$

Observer que la permutation $\sigma \circ c \circ \sigma^{-1}$ est un p-cycle qu'on précisera.

Exercice 39 [02226] [correction]
Déterminer la signature de :

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 8 & 7 & 6 & 2 & 1 \end{pmatrix}$ b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 7 & 4 & 8 & 5 & 6 \end{pmatrix}$

Exercice 40 [02227] [correction]
Soit $n \in \mathbb{N}^\star$. Déterminer la signature de la permutation suivante :
a) $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}$.
b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n & n+1 & n+2 & \ldots & 2n-1 & 2n \\ 1 & 3 & 5 & \ldots & 2n-1 & 2 & 4 & \ldots & 2n-2 & 2n \end{pmatrix}$.

Exercice 41 [02228] [correction]
Soit $n \geqslant 2$ et τ une transposition de $\mathfrak{S}_n$.
a) Montrer que l'application $\sigma \mapsto \tau \circ \sigma$ est une bijection de $\mathcal{S}_n$ vers $\mathcal{S}_n$.
b) En déduire le cardinal de l'ensemble $\mathcal{A}_n$ formé des permutations de signature 1 élément de $\mathcal{S}_n$.

Exercice 42 [02229] [correction]
Dans $(\mathcal{S}_n, \circ)$ on considère les permutations

$$\tau = \begin{pmatrix} 1 & 2 \end{pmatrix} \text{ et } \sigma = \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}$$

a) Calculer $\sigma^k \circ \tau \circ \sigma^{-k}$ pour $0 \leqslant k \leqslant n-2$.
b) En déduire que tout élément de $\mathfrak{S}_n$ peut s'écrire comme un produit de σ et de τ.

Exercice 43 [02230] [correction]
Soit $n \geqslant 5$.
Montrer que si $\begin{pmatrix} a & b & c \end{pmatrix}$ et $\begin{pmatrix} a' & b' & c' \end{pmatrix}$ sont deux cycles d'ordre 3 de $\mathcal{S}_n$, alors il existe une permutation σ, paire, telle que

$$\sigma \circ \begin{pmatrix} a & b & c \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} a' & b' & c' \end{pmatrix}$$

Exercice 44 [02231] [correction]
Soit $n \geqslant 2$ et c la permutation circulaire $c = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$.
Déterminer toutes les permutations σ de $\mathcal{S}_n$ qui commutent avec c.

Anneaux

Exercice 45 [02232] [correction]
On définit sur $\mathbb{Z}^2$ deux lois de compositions internes notées $+$ et $\star$ par :

$$(a,b)+(c,d) = (a+c,b+d) \text{ et } (a,b)\star(c,d) = (ac,ad+bc)$$

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

Exercice 46 [02233] [correction]
Montrer qu'un anneau $(A,+,\times)$ n'a pas de diviseurs de zéro si, et seulement si, tous ses éléments non nuls sont réguliers

Exercice 47 [02234] [correction]
On dit qu'un élément x d'un anneau $(A,+,\times)$ est nilpotent s'il existe $n \in \mathbb{N}^\star$ vérifiant

$$x^n = 0_A$$

Soient x et y deux éléments d'un anneau $(A,+,\times)$.
a) Montrer que si x est nilpotent et que x et y commutent, alors xy est nilpotent.
b) Montrer que si x et y sont nilpotents et commutent, alors $x+y$ est nilpotent.
c) Montrer que si xy est nilpotent, alors yx l'est aussi.
d) Montrer que si x est nilpotent alors $1-x$ est inversible. Préciser $(1-x)^{-1}$.

Exercice 48 [02235] [correction]
[Anneau de Boole 1815-1864)
On considère $(A,+,\times)$ un anneau de Boole c'est à dire un anneau non nul tel que tout élément est idempotent pour la deuxième loi ce qui signifie

$$\forall x \in A,\ x^2 = x$$

a) Montrer

$$\forall (x,y) \in A^2,\ xy + yx = 0_A$$

et en déduire que

$$\forall x \in A,\ x + x = 0_A$$

En déduire que l'anneau A est commutatif.
b) Montrer que la relation binaire définie sur A par

$$x \preccurlyeq y \Leftrightarrow yx = x$$

est une relation d'ordre.
c) Montrer que

$$\forall (x,y) \in A^2,\ xy(x+y) = 0_A$$

En déduire qu'un anneau de Boole intègre ne peut avoir que deux éléments.

Exercice 49 [02236] [correction]
Soient a,b deux éléments d'un anneau $(A,+,\times)$ tels que ab soit inversible et b non diviseur de 0.
Montrer que a et b sont inversibles.

Sous-anneau

Exercice 50 [02237] [correction]
Soit $d \in \mathbb{N}$, on note

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

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

Exercice 51 [02238] [correction]
On note

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

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

Exercice 52 [02239] [correction]
[Anneau des entiers de Gauss 1777-1855)
On note

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

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

Exercice 53 [02240] [correction]
Soit

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

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

Exercice 54 [02241] [correction]
Soit

$$A = \left\{\frac{m}{2^n} / m \in \mathbb{Z} \text{ et } n \in \mathbb{N}\right\}$$

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

Corps

Exercice 55 [02243] [correction]
Pour $a, b \in \mathbb{R}$, on pose

$$a \top b = a + b - 1 \text{ et } a \star b = ab - a - b + 2$$

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

Exercice 56 [02244] [correction]
Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$, on note

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

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

Exercice 57 [02245] [correction]
Soit A un anneau commutatif fini non nul.
Montrer que A ne possède pas de diviseurs de zéro si, et seulement si, A est un corps.

Exercice 58 [02246] [correction]
Soit F un sous corps de $(\mathbb{Q}, +, \times)$. Montrer que $F = \mathbb{Q}$.

Corrections

Exercice 1 : [énoncé]
$\forall a, b \in \mathbb{R}$, $b \star a = \ln(e^b + e^a) = \ln(e^a + e^b) = a \star b$. $\star$ est commutative.
$\forall a, b, c \in \mathbb{R}$, $(a \star b) \star c = \ln(e^{a\star b} + e^c) = \ln(e^a + e^b + e^c) = a \star (b \star c)$. $\star$ est associative.
$a \star \varepsilon = a \Leftrightarrow \ln(e^a + e^\varepsilon) = a \Leftrightarrow e^\varepsilon = 0$. Il n'y a donc pas de neutre.
$a \star b = a \star c \Rightarrow \ln(e^a + e^b) = \ln(e^a + e^c) \Rightarrow e^b = e^c \Rightarrow b = c$. Tout élément est régulier

Exercice 2 : [énoncé]
a) $1 - (x + y - xy) = (1 - x)(1 - y)$ donc si $x \leqslant 1$ et $y \leqslant 1$ alors $x \star y \leqslant 1$.
Par suite $\star$ est bien une loi de composition interne sur
$\star$ est clairement commutative et associative.
b) 0 est élément neutre de E.
c) Si $x \in \,]0,1]$ alors pour tout $y \in [0,1]$, $x \star y = x(1 - y) + y > 0$ et donc x n'est pas inversible (dans $[0,1]$).
Ainsi, seul 0 est inversible.
Pour tout $x, y, z \in [0,1]$, $x \star y = x \star z \Leftrightarrow y(1 - x) = z(1 - x)$.
Par suite, tout $x \in [0,1[$ est régulier tandis que 1 ne l'est visiblement pas.

Exercice 3 : [énoncé]
$\star$ est bien une loi de composition interne sur $\mathcal{P}(E)$.
Si $\star$ est commutative sur E, elle l'est aussi sur $\mathcal{P}(E)$.
Si $\star$ est associative sur E, elle l'est aussi sur $\mathcal{P}(E)$.
Si $\star$ possède un neutre e dans E, alors $\star$ possède un neutre dans $\mathcal{P}(E)$ à savoir $\{e\}$ car

$$A \star \{e\} = \{a \star e / a \in A\} = A$$

La loi $\star$ est distributive sur l'union

$$A \star (B \cup C) = \{a \star x / a \in A, x \in B \cup C\} = (A \star B) \cup (A \star C)$$

En revanche la distributivité sur l'intersection est fausse. On obtient un contre exemple dans $\mathbb{R}$ avec $\star = +$, $A = \{1, -1\}$, $B = \{1\}$ et $C = \{-1\}$ où

$$A \star B \cap C = A \star \emptyset = \emptyset$$

et

$$(A \star B) \cap A \star C = \{2, 0\} \cap \{-2, 0\} = \{0\}$$

Exercice 4 : [énoncé]
Supposons f est bijective.
Soient $g, h : E \to E$. Si $f \circ g = f \circ h$ alors $f^{-1} \circ f \circ g = f^{-1} \circ f \circ h$ puis $g = h$.
De même $g \circ f = h \circ f \Rightarrow g = h$ et donc f est un élément régulier.
Supposons que f est un élément régulier.
Soient $x, x' \in E$. Si $f(x) = f(x')$ alors $f \circ g = f \circ h$ avec g et h les fonctions constantes égales à x et x'.
Par la régularité de f, on obtient $g = h$ et donc $x = x'$.
Si E est un singleton alors f est nécessairement surjective.
Sinon, on peut construire deux fonctions g et h telle que

$$\forall x \in E, g(x) = h(x) \Leftrightarrow x \in \mathrm{Im} f$$

On a $g \circ f = h \circ f$ donc, par la régularité de f, $g = h$ d'où $\mathrm{Im} f = E$ puis f surjective.

Exercice 5 : [énoncé]
Si a est symétrisable alors considérons l'application $g : E \to E$ définie par $g(x) = a^{-1} \star x$.
On a $f \circ g = \mathrm{Id}_E$ et $g \circ f = \mathrm{Id}_E$ donc f est bijective.
Si f est bijective alors considérons b l'antécédent du neutre e. On a $a \star b = e$.
De plus $f(b \star a) = a \star b \star a = e \star a = a = f(e)$ donc $b \star a = e$ car f injective.
Par suite, a est symétrisable et b est son symétrique.

Exercice 6 : [énoncé]
a) On a

$$(x \star y) \star (x \star y) = (x \star x) \star (y \star y) = x \star y$$

b) On a

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

Exercice 7 : [énoncé]
a) Supposons $\star$ commutative :

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

donc $\top$ est commutative.
Supposons $\star$ associative :

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

donc $\top$ est associative.
b) Supposons que $\star$ possède un neutre e et montrons que $f = \varphi(e)$ est neutre pour $\top$.

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

et

$$f \top x = \varphi(e \star \varphi^{-1}(x)) = \varphi(\varphi^{-1}(x)) = x$$

donc f est neutre pour $\top$.

Exercice 8 : [énoncé]
Par la surjectivité de f, il existe $b \in E$ tel que $a \star b \star a = a$.
a) $a \star b = a \star a \star c \star a$
Pour tout $x \in E$, il existe $\alpha \in E$ tel qu'on peut écrire $x = a \star \alpha \star a$.
Pour $e = a \star b$, $e \star x = a \star b \star a \star \alpha \star a = a \star \alpha \star a = x$.
Pour $e' = b \star a$, $x \star e' = x \star b \star a = a \star \alpha \star a \star b \star a = a \star \alpha \star a$.
$e \star e' = e = e'$.
b) Puisque $a \star b = b \star a = e$, a est symétrisable et $\mathrm{sym}(a) = b$.
De plus $g : x \to b \star x \star b$ est clairement application réciproque de f.

Exercice 9 : [énoncé]
Considérons l'application $f : \mathbb{N} \to E$ définie par $f(n) = x^{\star n}$.
Puisque N est infini et que l'ensemble E est fini, l'application f n'est pas injective et donc il existe $p > q \in \mathbb{N}$ tels que $f(p) = f(q)$ i.e.

$$x^{\star p} = x^{\star q}$$

Pour tout $y \in E$.

$$x^{\star p} \star y = x^{\star q} \star y$$

Puisque x est régulier, on obtient :

$$x^{\star (p-q)} \star y = y$$

De même $y \star x^{\star (p-q)} = y$ et donc $e = x^{\star (p-q)}$ est neutre.

Exercice 10 : [énoncé]
Soit a un élément régulier.
Considérons l'application $f : E \to E$ définie par $f(x) = a \star x$.
L'application f est injective.
E est fini donc f est bijective et par suite surjective d'où $\exists b \in E$ tel que $a \star b = e$.
$f(e) = a$ et $f(b \star a) = a \star b \star a = e \star a = a$ donc par l'injectivité de f : $b \star a = e$.
Finalement a est inversible.
On peut aussi partir de $f : \mathbb{N} \to E$ définie par $f(n) = a^{\star n}$ qui n'est pas injective.

Exercice 11 : [énoncé]
a) $A \cap B$
b) $A \cup B$
c) $A \cap B$
d) $C_E A$ complémentaire de A dans E.
e) $A \cup B$
f) $A \Delta B = (A \cup B) \backslash (A \cap B)$

Exercice 12 : [énoncé]
Soit $x \in E$. Considérons la suite $(x_n)_{n \in \mathbb{N}^\star}$ déterminée par

$$x_1 = x \text{ et } x_{n+1} = x_n \top x_n$$

i.e.

$$x_{n+1} = x^{2^n}$$

Puisque l'ensemble E est fini, les éléments $x_1, x_2, \ldots$ ne peuvent être deux à deux distincts et donc il existe $p < q$ tels que

$$x^{2^p} = x^{2^q}$$

Posons alors $a = x^{2^p}$ et $n = q - p \in \mathbb{N}^\star$ de sorte que

$$a^{2^n} = a$$

Si $n = 1$, $e = a$ convient.
Si $n > 1$, il faut construire e à partir de a... Après quelques essais pour de premières valeurs de n, on est amené à proposer $e = a^{2^n - 1} \in E$. On constate alors

$$e \top e = e^2 = a^{2^{n+1}-2} = a^{2^n} \top a^{2^n - 2} = a \top a^{2^n - 2} = a^{2^n - 1} = e$$

Exercice 13 : [énoncé]
On observe que

$$\forall x \in G, x^{-1} = x$$

donc

$$\forall x, y \in G,\ y \star x = (y \star x)^{-1} = x^{-1} \star y^{-1} = x \star y$$

Exercice 14 : [énoncé]
Tout élément x de E est symétrisable et $\mathrm{sym}(x) = x$ donc $(E, \star)$ est un groupe.
De plus

$$x \star y = \mathrm{sym}(x \star y) = \mathrm{sym}(y) \star \mathrm{sym}(x) = y \star x$$

donc $(E, \star)$ est abélien.

Exercice 15 : [énoncé]
$\star$ est associative et possède un neutre e, il reste à voir que tout élément $a \in E$ est inversible.
Considérons l'application $f : E \to E$ définie par $f(x) = a \star x$.
a est régulier donc l'application f est injective.
E est fini donc f est bijective et par suite surjective d'où l'existence d'un $b \in E$ tel que $a \star b = e$.
$f(e) = a$ et $f(b \star a) = a \star b \star a = e \star a = a$ donc par l'injectivité de f : $b \star a = e$.
Finalement a est inversible et $(E, \star)$ est un groupe.
On peut aussi partir de $f : \mathbb{N} \to E$ définie par $f(n) = a^{\star n}$ qui n'est pas injective, pour établir que l'élément a est inversible.

Exercice 16 : [énoncé]
Si un élément figure deux fois dans une même ligne correspondant aux valeurs de composition avec x, c'est qu'il existe $a \neq b$ tel que $x \star a = x \star b$.
Or tout élément d'un groupe est régulier, ce cas de figure ci-dessus est donc impossible.
Comme le groupe G à n élément, qu'il y a n cases sur chaque ligne et que chaque ligne ne peut contenir deux fois le même élément, chaque ligne contient chaque élément de G une fois et une seule.
On raisonne de même avec les colonnes.

Exercice 17 : [énoncé]
a) La loi $\star$ est bien définie. Soient $(x,y),(x',y'),(x'',y'') \in G$

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

et

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

donc $\star$ est associative.

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

donc $(1,0)$ est élément neutre.

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

donc tout élément est symétrisable.
Finalement $(G, \star)$ est un groupe.
$(1,2) \star (3,4) = (3,6)$ et $(3,4) \times (1,2) = (3,10)$ donc le groupe n'est pas commutatif.
b) $H = \mathbb{R}^{+\star} \times \mathbb{R}$ est inclus dans G.
$(1,0) \in H$.

$$\forall (x,y),(x',y') \in H,\ (x,y) \star (x',y') \in H$$

car $xx' > 0$

$$\forall (x,y) \in H,\ (x,y)^{-1} = (1/x, -y/x) \in H$$

car $1/x > 0$.
Ainsi H est un sous groupe de $(G, \star)$.

Exercice 18 : [énoncé]
Notons que $\frac{x+y}{1+xy}$ existe pour tout $x,y \in G$ car $1+xy > 0$.
On a

$$x+y-(1+xy) = (1-x)(y-1) < 0$$

donc $\frac{x+y}{1+xy} < 1$ et de même $\frac{x+y}{1+xy} > -1$ d'où

$$\frac{x+y}{1+xy} \in G$$

Par suite la loi $\star$ est bien définie.
La loi $\star$ est clairement commutative.
Soient $x,y,z \in G$,

$$(x \star y) \star z = \frac{(x \star y)+z}{1+(x \star y)z} = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z} = \frac{x+y+z+xyz}{1+xy+xz+yz} = x \star (y \star z)$$

La loi $\star$ est donc associative.
0 est neutre pour $\star$ puisque

$$\forall x \in G, x \star 0 = x$$

Enfin

$$\forall x \in G,\ x \star (-x) = 0$$

donc tout élément x de G est symétrisable et $\mathrm{sym}(x) = -x$.
Finalement $(G, \star)$ est un groupe commutatif.

Exercice 19 : [énoncé]
a) On a

$$x \star y \in I \Leftrightarrow xy + c(x+y) + c^2 > 0 \text{ et } xy - c(x+y) + c^2 > 0$$
$$\Leftrightarrow (x+c)(y+c) > 0 \text{ et } (x-c)(y-c) > 0$$

Par suite
$$\forall (x,y) \in I^2,\ x \star y \in I$$

b) $\star$ est clairement commutative.
$\star$ est associative puisque

$$\forall x,y,z \in I,\ (x \star y) \star z = \frac{x+y+z+\frac{xyz}{c^2}}{1+\frac{xy+yz+zx}{c^2}} = x \star (y \star z)$$

0 est élément neutre car

$$\forall x \in I,\ x \star 0 = 0 \star x = x$$

Enfin
$$\forall x \in I,\ (-x) \star x = x \star (-x) = 0$$

donc tout élément de I est symétrisable dans I.
Finalement $(I, \star)$ est un groupe abélien.

Exercice 20 : [énoncé]
$H \subset \mathbb{C}$, $0 = 0 + \omega.0 \in H$.
Soient $x, y \in H$. On peut écrire $x = a + \omega b$ et $y = a' + \omega b'$ avec $a, b, a', b' \in \mathbb{Z}$ et alors
$$x - y = (a - a') + \omega(b - b')$$

avec $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$ donc $x - y \in H$.
Ainsi H est un sous groupe de $(\mathbb{C}, +)$.

Exercice 21 : [énoncé]
$H \subset \mathbb{C}^\star$, $1 = a^0 \in H$.
Soient $x, y \in H$, on peut écrire $x = a^n$ et $y = a^m$ avec $n, m \in \mathbb{Z}$. On a alors

$$xy^{-1} = a^{n-m}$$

avec $n - m \in \mathbb{Z}$ donc $xy^{-1} \in H$.
Ainsi H est un sous groupe de $(\mathbb{C}^\star, \times)$.

Exercice 22 : [énoncé]
$H \subset \mathcal{S}_E$, $\mathrm{Id}_E \in H$ car $\mathrm{Id}_E(a) = a$.
Soient $f, g \in H$, $(f \circ g)(a) = f(g(a)) = f(a) = a$ donc $f \circ g \in H$.
Soit $f \in H$, $f^{-1}(a) = a$ car $f(a) = a$ donc $f^{-1} \in H$.
Ainsi H est un sous-groupe de $(\mathcal{S}_E, \circ)$.

Exercice 23 : [énoncé]
a) $aHa^{-1} \subset G$, $e = aea^{-1} \in aHa^{-1}$.
Soient $axa^{-1}, aya^{-1} \in aHa^{-1}$ avec $x, y \in H$ on a

$$(axa^{-1})(ay^{-1}a^{-1}) = a(xy^{-1})a^{-1} \in aHa^{-1}$$

b) $e \in aH \Rightarrow a^{-1} \in H \Rightarrow a \in H$. Inversement

$$a \in H \Rightarrow a^{-1} \in H \Rightarrow aH = H$$

La condition simple cherchée est $a \in H$.

Exercice 24 : [énoncé]
$C \subset G$ et $e \in G$ car
$$\forall y \in G,\ e \star y = y = y \star e$$

Soient $x, x' \in C$. Pour tout $y \in G$

$$x \star x' \star y = x \star y \star x' = y \star x \star x'$$

donc $x \star x' \in C$
Soit $x \in C$. Pour tout $y \in G$,

$$x \star y^{-1} = y^{-1} \star x$$

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

i.e.
$$y \star x^{-1} = x^{-1} \star y$$

donc $x^{-1} \in C$.
Ainsi C est un sous-groupe de $(G, \star)$.

Exercice 25 : [énoncé]
Posons $H = \{f_{a,b}/a \in \mathbb{C}^\star, b \in \mathbb{C}\}$ et montrons que H est un sous-groupe du groupe de permutations $(\mathcal{S}_\mathbb{C}, \circ)$.
$\mathrm{Id}_\mathbb{C} = f_{1,0} \in H$.

$$Z = az + b \Leftrightarrow z = \frac{1}{a}Z - \frac{b}{a}$$

donc $f_{a,b} \in \mathcal{S}_\mathbb{C}$ et $f_{a,b}^{-1} = f_{1/a,-b/a}$. Ainsi $H \subset \mathcal{S}_\mathbb{C}$ et

$$\forall f \in H, f^{-1} \in H$$

Enfin $f_{a,b} \circ f_{c,d}(z) = a(cz + d) + b = acz + (ad + b)$ donc $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$.
Ainsi,

$$\forall f, g \in H, f \circ g \in H$$

On peut conclure.

Exercice 26 : [énoncé]
a) Il est clair que i, f et g sont des permutations de E.

$$h(x) = \frac{x}{x-1} = 1 + \frac{1}{x-1} = 1 - \frac{1}{1-x} = f(g(f(x)))$$

donc $h = f \circ g \circ f$ et donc $h \in \mathcal{S}_E$.
De même $k = f \circ g \in \mathcal{S}_E$ et $\ell = g \circ f \in \mathcal{S}_E$
b)

$\circ$	i	f	g	h	k	ℓ
i	i	f	g	h	k	ℓ
f	f	i	k	ℓ	g	h
g	g	ℓ	i	k	h	f
h	h	k	ℓ	i	f	g
k	k	h	f	g	ℓ	i
ℓ	ℓ	g	h	f	i	k

c) G est un sous groupe de $(\mathcal{S}_E, \circ)$ car G contient i, est stable par composition et par passage à l'inverse.
De plus ce groupe n'est pas commutatif car $g \circ f \neq f \circ g$.

Exercice 27 : [énoncé]
Par l'absurde supposons

$$H \not\subset K \text{ et } K \not\subset H$$

Il existe $h \in H$ tel que $h \notin K$ et $k \in K$ tel que $k \notin H$.
On a $h, k \in H \cup K$ donc $h \star k \in H \cup K$ car $H \cup K$ sous-groupe.
Si $h \star k \in H$ alors $k = h^{-1} \star (h \star k) \in H$ car H sous-groupe. Or ceci est exclu.
Si $h \star k \in K$ alors $h = (h \star k) \star k^{-1} \in K$ car K sous-groupe. Or ceci est exclu.
Ainsi $h \star k \notin H \cup K$. Absurde.

Exercice 28 : [énoncé]
a) L'application φ est à valeurs dans A qui est un ensemble fini et au départ de $\mathbb{N}$ qui est infini donc φ n'est pas injective.
b) Par la non injectivité de φ, il existe $n \in \mathbb{N}$ et $p \in \mathbb{N}^\star$ tel que $\varphi(n+p) = \varphi(n)$.
On a alors $x^{(n+p)} = x^n \star x^p = x^n$ donc $x^p = e$ par régularité de $x^n \in G$.
Par suite $x^{-1} = x^{(p-1)} \in A$.
A est non vide, stable pour $\star$ et stable par inversion donc A est un sous-groupe de $(G, \star)$.

Exercice 29 : [énoncé]
a) $a\mathbb{Z} \subset \mathbb{Z}$, $0 = a.0 \in a\mathbb{Z}$.
Soient $x, y \in a\mathbb{Z}$, on peut écrire $x = ak$ et $y = a\ell$ avec $k, \ell \in \mathbb{Z}$.
$x - y = a(k - \ell)$ avec $k - \ell \in \mathbb{Z}$ donc $x - y \in a\mathbb{Z}$.
Ainsi $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
b) Pour $a = 0 \in \mathbb{N}$, $\{0\} = a\mathbb{Z}$.
c) Puisque H est non vide et non réduit à $\{0\}$, il existe $h \in H$ tel que $h \neq 0$.
Si $h > 0$ alors $h \in H^+$, si $h < 0$ alors $-h \in H$ (car H sous-groupe) et $-h > 0$ donc $-h \in H^+$.
Dans les deux cas $H^+ \neq \emptyset$.
H^+ est une partie non vide de $\mathbb{N}$ donc H^+ possède un plus petit élément.
d) $0 \in H$ et $a \in H$.
Par récurrence, la stabilité de H donne

$$\forall n \in \mathbb{N}, a.n = a + \cdots + a \in H$$

Par passage à l'opposé, la stabilité de H par passage au symétrique donne

$$\forall n \in \mathbb{Z}, an \in H$$

Ainsi $a\mathbb{Z} \subset H$.
e) Soit $x \in H$. La division euclidienne de x par $a \neq 0$ donne $x = aq + r$ avec $q \in \mathbb{Z}$ et $0 \leqslant r < a$.
On a $r = x - aq$ avec $x \in H$ et $aq \in a\mathbb{Z} \subset H$ donc $r \in H$.
Si $r > 0$ alors $r \in H^+$ or $r < a = \min H^+$ donc cela est impossible.
Il reste $r = 0$ ce qui donne $x = aq \in a\mathbb{Z}$. Ainsi $H \subset a\mathbb{Z}$ et finalement $H = a\mathbb{Z}$.

f) L'existence est établie ci-dessus. Il reste à montrer l'unicité.
Soit $a, b \in \mathbb{N}$ tel que $a\mathbb{Z} = b\mathbb{Z}$. On a $a \in a\mathbb{Z} = b\mathbb{Z}$ donc $b \mid a$ et de même $a \mid b$, or $a, b \geqslant 0$ donc $a = b$.

Exercice 30 : [énoncé]
Montrons que V est un sous-groupe du groupe $(\mathbb{C}^\star, \times)$.
La partie V est incluse dans $\mathbb{C}^\star$ et évidemment non vide.
Soient $z \in V$. Il existe $n \in \mathbb{N}^\star$ tel que $z^n = 1$ et alors $(z^{-1})^n = 1$ donc $z^{-1} \in V$.
Soient $z, z' \in V$. Il existe $n, m \in \mathbb{N}^\star$ tels que $z^n = z'^m = 1$. On a alors $(zz')^{nm} = (z^n)^m (z'^m)^n = 1$ et donc $zz' \in V$.
Finalement V est bien un sous-groupe de $(\mathbb{C}^\star, \times)$ et donc $(V, \times)$ est un groupe.

Exercice 31 : [énoncé]
Pour $x \in \mathbb{R}^\star$, on a bien $f(x) \in \mathbb{R}^\star$. Pour $x, y \in \mathbb{R}^\star$

$$f(xy) = (xy)^n = x^n y^n = f(x)f(y)$$

donc f est un morphisme de $(\mathbb{R}^\star, \times)$ vers lui-même.
$\ker f = f^{-1}(\{1\})$ et $\mathrm{Im} f = \{x^n / x \in \mathbb{R}^\star\}$.
Si n est pair alors

$$\ker f = \{1, -1\} \text{ et } \mathrm{Im} f = \mathbb{R}^{+\star}$$

Si n est impair alors

$$\ker f = \{1\} \text{ et } \mathrm{Im} f = \mathbb{R}^\star$$

Exercice 32 : [énoncé]
On sait

$$\forall x, y \in \mathbb{C},\ \exp(x + y) = \exp(x)\exp(y)$$

donc $\exp : \mathbb{C} \to \mathbb{C}^\star$ est un morphisme de groupes.

$$\exp(x) = 1 \Leftrightarrow \exists k \in \mathbb{Z}, x = 2ik\pi$$

donc

$$\ker \exp = \{2ik\pi / k \in \mathbb{Z}\}$$

La fonction exponentielle complexe prend toutes les valeurs de $\mathbb{C}^\star$ donc

$$\mathrm{Im} \exp = \mathbb{C}^\star$$

Exercice 33 : [énoncé]
a) Soient $x, y \in G$. On a

$$\tau_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \tau_a(x)\tau_a(y)$$

τ_a est donc un endomorphisme du groupe $(G, \times)$.
b) Pour tout $x \in G$,

$$(\tau_a \circ \tau_b)(x) = \tau_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \tau_{ab}(x)$$

donc

$$\tau_a \circ \tau_b = \tau_{ab}$$

c) $(\tau_a \circ \tau_{a^{-1}}) = \tau_1 = \mathrm{Id}_G$ et $(\tau_{a^{-1}} \circ \tau_a) = \tau_1 = \mathrm{Id}_G$ donc τ_a est bijective et $(\tau_a)^{-1} = \tau_{a^{-1}}$.
d) Montrons que $\mathcal{T}$ est un sous-groupe du groupe des permutations $(\mathcal{S}_G, \circ)$.
$\mathcal{T} \subset \mathcal{S}_G$ et $\mathrm{Id}_G \in \mathcal{T}$ car $\mathrm{Id}_G = \tau_1$.
Soit $f, g \in \mathcal{T}$, on peut écrire $f = \tau_a$ et $g = \tau_b$ avec $a, b \in G$. On a alors

$$f \circ g^{-1} = \tau_a \circ (\tau_b)^{-1} = \tau_a \circ \tau_{b^{-1}} = \tau_{ab^{-1}} \in \mathcal{T}$$

car $ab^{-1} \in G$.
Ainsi $\mathcal{T}$ est un sous-groupe de $(\mathcal{S}_G, \circ)$ et donc $(\mathcal{T}, \circ)$ est un groupe.

Exercice 34 : [énoncé]
a) $f(H) \subset G'$, $e' = f(e) \in f(H)$ car $e \in H$.
Soit $y, y' \in f(H)$, on peut écrire $y = f(x)$ et $y' = f(x')$ avec $x, x' \in H$.

$$y \top y'^{-1} = f(x) \top f(x')^{-1} = f(x) \top f(x'^{-1}) = f(x \star x'^{-1})$$

avec $x \star x'^{-1} \in H$ donc $y \top y'^{-1} \in f(H)$.
Ainsi $f(H)$ est un sous-groupe de $(G', \top)$.
b) $f^{-1}(H') \subset G$ et $e \in f^{-1}(H')$ car $f(e) = e' \in H'$.
Soit $x, x' \in f^{-1}(H')$. On a $f(x), f(x') \in H'$.

$$f(x \star x'^{-1}) = f(x) \top f(x'^{-1}) = f(x) \top f(x')^{-1} \in H'$$

donc $x \star x'^{-1} \in f^{-1}(H')$.
Ainsi $f^{-1}(H')$ est un sous-groupe de $(G, \star)$.

Exercice 35 : [énoncé]
$\mathrm{Aut}(G) \subset \mathcal{S}_G$ et $\mathrm{Id}_G \in \mathrm{Aut}(G)$.
Pour tout $f, g \in \mathrm{Aut}(G)$, on a $f \circ g \in \mathrm{Aut}(G)$ et $f^{-1} \in \mathrm{Aut}(G)$ par les propriétés sur les automorphismes.
Ainsi $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathcal{S}_G, \circ)$.

Exercice 36 : [énoncé]
a) Soit $x, y, z \in G$,

$$(x \top y) \top z = (x \star a \star y) \star a \star z = x \star a \star (y \star a \star z) = x \top (y \top z)$$

L'élément $\mathrm{sym}(a)$ est neutre pour la loi $\top$. En effet, pour $x \in G$, on a

$$x \top \mathrm{sym}(a) = x = \mathrm{sym}(a) \top x$$

Soit $x \in G$. Posons $y = \mathrm{sym}(a) \star \mathrm{sym}(x) \star \mathrm{sym}(a) \in G$. On a

$$x \top y = y \top x = \mathrm{sym}(a)$$

b) $K \subset G$, $\mathrm{sym}(a) = \mathrm{sym}(a) \star e$ donc $\mathrm{sym}(a) \in K$.
Soit $\mathrm{sym}(a) \star x, \mathrm{sym}(a) \star y \in K$. On a

$$(\mathrm{sym}(a) \star x) \top (\mathrm{sym}(a) \star y)^{\top(-1)} = \mathrm{sym}(a) \star x \star a \star \mathrm{sym}(a) \star \mathrm{sym}(y) \star a \star \mathrm{sym}(a) = \mathrm{sym}(a) \star (x \star \mathrm{sym}(y)) \in K$$

c) Pour $x, y \in G$,

$$f(x \star y) = x \star y \star \mathrm{sym}(a) = (x \star \mathrm{sym}(a)) \top (y \star \mathrm{sym}(a)) = f(x) \top f(y)$$

f est un morphisme de groupe et il est bijectif d'application réciproque
$g : x \mapsto x \star a$.

Exercice 37 : [énoncé]
Si $\{i, j\}$ est stable par σ alors $\{\sigma(i), \sigma(j)\} = \{i, j\}$.
On a alors

$$\forall x \notin \{i, j\}, (\sigma \circ \tau)(x) = \sigma(x) = (\tau \circ \sigma)(x)$$

Pour $x = i$ alors $(\sigma \circ \tau)(i) = \sigma(j) = (\tau \circ \sigma)(i)$ et pour $x = j$,
$(\sigma \circ \tau)(j) = \sigma(i) = (\tau \circ \sigma)(j)$.
Par suite

$$\sigma \circ \tau = \tau \circ \sigma$$

Inversement, si $\sigma \circ \tau = \tau \circ \sigma$ alors $\sigma(i) = (\sigma \circ \tau)(j) = (\tau \circ \sigma)(j) = \tau(\sigma(j))$.
Puisque $\tau(\sigma(j)) \neq \sigma(j)$ on a $\sigma(j) \in \{i, j\}$.
De même $\sigma(i) \in \{i, j\}$ et donc $\{i, j\}$ stable par σ.

Exercice 38 : [énoncé]
Pour $x = \sigma(a_i)$, on a

$$(\sigma \circ c \circ \sigma^{-1})(x) = \sigma(a_{i+1})$$

(en posant $a_{p+1} = a_1$).
Pour $x \notin \{\sigma(a_1), \dots, \sigma(a_p)\}$, on a

$$(\sigma \circ c \circ \sigma^{-1})(x) = \sigma \circ \sigma^{-1}(x) = x$$

car $c(\sigma^{-1}(x)) = \sigma^{-1}(x)$ puisque $\sigma^{-1}(x) \notin \{a_1, \dots, a_p\}$.
Ainsi

$$\sigma \circ c \circ \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_p) \end{pmatrix}$$

Exercice 39 : [énoncé]
On note $I(\sigma)$ le nombre d'inversions de la permutation σ :

$$I(\sigma) = \mathrm{Card}(\{1 \leqslant i < j \leqslant n / \sigma(i) > \sigma(j)\}$$

On a $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ et $I(\sigma)$ se calcule en dénombrant, pour chaque de terme de la seconde ligne, le nombre de termes inférieurs qui le suit.
a) $I(\sigma) = 2 + 3 + 2 + 4 + 3 + 2 + 1 + 0 = 17$ donc $\varepsilon(\sigma) = -1$.
b) $I(\sigma) = 0 + 1 + 0 + 3 + 0 + 2 + 0 + 0 = 6$ donc $\varepsilon(\sigma) = 1$.

Exercice 40 : [énoncé]
On note $I(\sigma)$ le nombre d'inversions de la permutation σ :

$$I(\sigma) = \mathrm{Card}(\{1 \leqslant i < j \leqslant n / \sigma(i) > \sigma(j)\}$$

On a $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ et $I(\sigma)$ se calcule en dénombrant, pour chaque de terme de la seconde ligne, le nombre de termes inférieurs qui le suit.
a) $I(\sigma) = (n-1) + (n-2) + \dots + 1 + 0 = \frac{n(n-1)}{2}$ donc

$$\varepsilon(\sigma) = (-1)^{\frac{n(n-1)}{2}}$$

b) $I(\sigma) = 0 + 1 + 2 + \dots + (n-1) + 0 + \dots + 0 = \frac{n(n-1)}{2}$ donc

$$\varepsilon(\sigma) = (-1)^{\frac{n(n-1)}{2}}$$

Exercice 41 : [énoncé]
a) L'application $\sigma \mapsto \tau \circ \sigma$ est involutive, donc bijective.
b) L'application $\sigma \mapsto \tau \circ \sigma$ transforme $\mathcal{A}_n$ en $\mathcal{S}_n \backslash \mathcal{A}_n$ donc $\mathrm{Card}\mathcal{A}_n = \mathrm{Card}\mathcal{S}_n \backslash \mathcal{A}_n$.
Or $\mathcal{S}_n$ est la réunion disjointe de $\mathcal{A}_n$ et de $\mathcal{S}_n \backslash \mathcal{A}_n$ donc

$$\mathrm{Card}\mathcal{A}_n = \frac{1}{2}\mathrm{Card}\mathcal{S}_n = \frac{n!}{2}$$

Exercice 42 : [énoncé]
a) $\sigma \circ \tau \circ \sigma^{-1} = \begin{pmatrix} 2 & 3 \end{pmatrix}$, $\sigma^2 \circ \tau \circ \sigma^{-2} = \begin{pmatrix} 3 & 4 \end{pmatrix}$,...,
$\sigma^k \circ \tau \circ \sigma^{-k} = \begin{pmatrix} k+1 & k+2 \end{pmatrix}$.
b) Il est « connu »que toute permutation de $\mathcal{S}_n$ peut s'écrire comme produit de transpositions de la forme $\begin{pmatrix} k & k+1 \end{pmatrix}$. Ces dernières peuvent s'écrire comme produit de σ, de τ, et de σ^{-1}. Or $\sigma^n = \mathrm{Id}$ et donc $\sigma^{-1} = \sigma^{n-1}$ et par conséquent, σ^{-1} peut s'écrire comme produit de σ.

Exercice 43 : [énoncé]
Notons que

$$\sigma \circ \begin{pmatrix} a & b & c \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} \sigma(a) & \sigma(b) & \sigma(c) \end{pmatrix}$$

Soit $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ une permutation définie par :

$$\sigma(a) = a', \sigma(b) = b' \text{ et } \sigma(c) = c'$$

Si σ est paire alors le problème est résolu.
Si σ est impaire alors soit $c \neq d \in \mathbb{N}_n \setminus \{a, b, c\}$ et $\tau = \begin{pmatrix} c & d \end{pmatrix}$.
$\sigma \circ \tau$ est une permutation paire satisfaisante.

Exercice 44 : [énoncé]
Pour commencer, notons que, pour tout $k \in \{1, \dots, n\}$ $c^{k-1}(1) = k$ et par conséquent $c^{-(k-1)}(k) = 1$.
Soit σ une permutation commutant avec c_n.
Posons $k = \sigma(1) \in \{1, 2, ..., n\}$ et $s = c^{-(k-1)} \circ \sigma$ de sorte que $s(1) = 1$.
Comme σ et c commutent, s et c commutent aussi et on a pour tout $2 \leqslant i \leqslant n$, $s = c^{(i-1)} \circ s \circ c^{-(i-1)}$ d'où
$s(i) = c^{(i-1)} \circ s \circ c^{-(i-1)}(i) = \sigma^{(i-1)} \circ s(1) = \sigma^{(i-1)}(1) = i$ car $c^{-(i-1)}(i) = 1$.
Par conséquent $s = \mathrm{Id}$ puis $\sigma = c^k$.
Inversement les permutations de la forme c^k avec $1 \leqslant k \leqslant n$ commutent avec c.

Exercice 45 : [énoncé]
a) On vérifie aisément que $(\mathbb{Z}^2, +)$ est un groupe commutatif.
Avec des notations entendues

$$(a, b) \star (c, d) = (ac, ad + bc) = (c, d) \star (a, b)$$

La loi $\star$ est donc commutative. De plus

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

La loi $\star$ est donc associative.
Le couple $(1, 0)$ est neutre pour la loi $\star$, car $(a, b) \star (1, 0) = (a, b)$
Enfin

$$((a, b) + (c, d)) \star (e, f) = (a + c, b + d) \star (e, f) = (ae + ce, af + cf + be + de)$$

donc

$$((a, b) + (c, d)) \star (e, f) = (ae, af + be) + (ce, cf + de) = (a, b) \star (e, f) + (c, d) \star (e, f)$$

et la loi $\star$ est distributive sur $+$.
Finalement $(\mathbb{Z}^2, +, \star)$ est un anneau commutatif.
b) $A \subset \mathbb{Z}^2$, $(1, 0) \in A$.
Pour tout $(a, 0), (b, 0) \in A$, on a

$$(a, 0) - (b, 0) = (a - b, 0) \in A$$

et

$$(a, 0) \star (b, 0) = (ab, 0) \in A$$

A est donc un sous-anneau de $(\mathbb{Z}^2, +, \star)$.

Exercice 46 : [énoncé]
Supposons que A n'ait pas de diviseurs de zéro.
Soit $x \in A$ avec $x \neq 0$.

$$\forall a, b \in A,\ xa = xb \Rightarrow x(a - b) = 0 \Rightarrow a - b = 0$$

car $x \neq 0$.
Ainsi x est régulier à gauche. Il en est de même à droite.
Supposons que tout élément non nul de A soit régulier.

$$\forall x, y \in A,\ xy = 0 \Rightarrow xy = x.0 \Rightarrow x = 0 \text{ ou } y = 0$$

(par régularité de x dans le cas où $x \neq 0$).
Par suite l'anneau A ne possède pas de diviseurs de zéro.

Exercice 47 : [énoncé]
a) Soit $n \in \mathbb{N}$ tel que $x^n = 0_A$. Puisque x et y commutent

$$(xy)^n = (xy)(xy)\dots(xy) = x^n y^n = 0_A . y^n = 0_A$$

donc xy nilpotent.

b) Soient $n, m \in \mathbb{N}$ tels que $x^n = y^m = 0_A$. Puisque x et y commutent, on peut exploiter la formule du binôme

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

En séparant la somme en deux

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

Or

$$\forall k \in \{0, \dots, n-1\}, y^{m+n-1-k} = 0_A$$

car $m+n-1-k \geqslant m$ et

$$\forall k \geqslant n, x^k = 0_A$$

donc

$$(x+y)^{m+n-1} = 0_A + 0_A = 0_A$$

Ainsi $x+y$ est nilpotent.
c) Soit $n \in \mathbb{N}$ tel que $(xy)^n = 0_A$.

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

donc yx nilpotent.
d) Soit $n \in \mathbb{N}$ tel que $x^n = 0_A$. Par factorisation, on peut écrire

$$1 = 1 - x^n = (1-x)y = y(1-x)$$

avec $y = 1 + x + \cdots + x^{n-1}$.
Par suite $1-x$ est inversible et y est son inverse.

Exercice 48 : [énoncé]
a) $(x+y)^2 = (x+y)$ donne $x^2 + y^2 + xy + yx = x + y$ puis $xy + yx = 0$ sachant $x^2 = x$ et $y^2 = y$.
Pour $y = 1$ on obtient $x + x = 0_A$.
b) Comme $x^2 = x$, $\preccurlyeq$ est réflexive.
Si $x \preccurlyeq y$ et $y \preccurlyeq x$ alors $yx = x$ et $xy = y$ donc $xy + yx = x + y = 0$.
Or $x + x = 0$, donc $x + y = x + x$, puis $y = x$.
Si $x \preccurlyeq y$ et $y \preccurlyeq z$ alors $yx = x$ et $zy = y$ donc $zx = zyx = yx = x$ i.e. $x \preccurlyeq z$.
Ainsi $\preccurlyeq$ est une relation d'ordre sur A.
c) $xy(x+y) = xyx + xy^2 \underset{yx=-xy}{=} -x^2y + xy^2 = -xy + xy = 0$.
Si A est intègre alors : $xy(x+y) = 0_A \Rightarrow x = 0_A$, $y = 0_A$ ou $x + y = 0_A$.
Or $x + y = 0 = x + x$ donne $y = x$.
Ainsi, lorsqu'on choisit deux éléments de A, soit l'un deux est nul, soit ils sont égaux.
Une telle propriété est impossible si $\operatorname{Card}(A) \geqslant 3$. Par suite $\operatorname{Card}(A) = 2$ car A est non nul.

Exercice 49 : [énoncé]
Soit $x = b(ab)^{-1}$. Montrons que x est l'inverse de a.
On a $ax = ab(ab)^{-1} = 1$ et $xab = b(ab)^{-1}ab = b$ donc $(xa-1)b = 0$ puis $xa = 1$ car b n'est pas diviseur de 0. Ainsi a est inversible et x est son inverse.
De plus $b = a^{-1}(ab)$ l'est aussi par produit d'éléments inversibles.

Exercice 50 : [énoncé]
$\mathbb{Z}\left[\sqrt{d}\right] \subset \mathbb{R}$, $1 \in \mathbb{Z}\left[\sqrt{d}\right]$.
Soient $x, y \in \mathbb{Z}\left[\sqrt{d}\right]$, on peut écrire $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$ avec $a, b, a', b' \in \mathbb{Z}$.
$x - y = (a - a') + (b - b')\sqrt{d}$ avec $a - a', b - b' \in \mathbb{Z}$ donc $x - y \in \mathbb{Z}\left[\sqrt{d}\right]$.
$xy = (aa' + bb'd) + (ab' + a'b)\sqrt{d}$ avec $aa' + bb'd, ab' + a'b \in \mathbb{Z}$ donc $xy \in \mathbb{Z}\left[\sqrt{d}\right]$.
Ainsi $\mathbb{Z}\left[\sqrt{d}\right]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 51 : [énoncé]
$\mathcal{D} \subset \mathbb{Q}$ et $1 \in \mathcal{D}$ car $1 = \frac{1}{10^0}$.
Soient $x, y \in \mathcal{D}$, on peut écrire $x = \frac{n}{10^k}$ et $y = \frac{m}{10^\ell}$ avec $n, m \in \mathbb{Z}$ et $k, \ell \in \mathbb{N}$.
$x - y = \frac{n10^\ell - m10^k}{10^{k+\ell}}$ avec $n10^\ell - m10^k \in \mathbb{Z}$ et $k + \ell \in \mathbb{N}$ donc $x - y \in \mathcal{D}$.
$xy = \frac{nm}{10^{k+\ell}}$ avec $nm \in \mathbb{Z}$ et $k + \ell \in \mathbb{N}$ donc $xy \in \mathcal{D}$.
Ainsi $\mathcal{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

Exercice 52 : [énoncé]
a) Montrer que $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$. $\mathbb{Z}[i] \subset \mathbb{C}$, $1 \in \mathbb{Z}[i]$.
$\forall x, y \in \mathbb{Z}[i]$, on peut écrire $x = a + i.b$ et $y = a' + i.b'$ avec $a, b, a', b' \in \mathbb{Z}$.
$x - y = (a - a') + i.(b - b')$ avec $a - a', b - b' \in \mathbb{Z}$ donc $x - y \in \mathbb{Z}[i]$.
$xy = (aa' - bb') + i(ab' + a'b)$ avec $aa' - bb', ab' + a'b \in \mathbb{Z}$ donc $xy \in \mathbb{Z}[i]$.
Ainsi $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

b) Soit $x = a + i.b \in \mathbb{Z}[i]$ avec $a, b \in \mathbb{Z}$.
Si x est inversible dans $\mathbb{Z}[i]$, il l'est aussi dans $\mathbb{C}$ et de même inverse.
Donc $x \neq 0$ (i.e. $(a, b) \neq (0, 0)$) et

$$x^{-1} = \frac{1}{a + ib} = \frac{a - i.b}{a^2 + b^2} \in \mathbb{Z}[i]$$

d'où

$$\frac{a}{a^2 + b^2} \in \mathbb{Z} \text{ et } \frac{b}{a^2 + b^2} \in \mathbb{Z}$$

Par suite $\frac{ab}{a^2+b^2} \in \mathbb{Z}$ or $\left|\frac{ab}{a^2+b^2}\right| \leqslant \frac{1}{2}$ donc $ab = 0$.
Si $b = 0$ alors $\frac{a}{a^2+b^2} = \frac{1}{a} \in \mathbb{Z}$ donne $a = \pm 1$.
Si $a = 0$ alors $\frac{b}{a^2+b^2} = \frac{1}{b} \in \mathbb{Z}$ donne $b = \pm 1$.
Ainsi, si $x = a + i.b$ est inversible, $x = 1, i, -1$ ou $-i$.
La réciproque est immédiate.

Exercice 53 : [énoncé]
a) $A \subset \mathbb{Q}$, $1 \in A$, $\forall x, y \in A, x - y \in A$ et $xy \in A$: clair.
Par suite A est un sous anneau de $(\mathbb{Q}, +, \times)$.
b) $x \in A$ est inversible si, et seulement si, il existe $y \in A$ tel que $xy = 1$.
$x = \frac{m}{n}, y = \frac{m'}{n'}$ avec n, n' impairs. $xy = 1 \Rightarrow mm' = nn'$ donc m est impair et la réciproque est immédiate.
Ainsi

$$U(A) = \left\{\frac{m}{n} / m \in \mathbb{Z}, n \in \mathbb{N}^\star \text{ impairs}\right\}$$

Exercice 54 : [énoncé]
a) $A \subset \mathbb{Q}$, $1 \in A$, $\forall x, y \in A, x - y \in A$ et $xy \in A$: facile.
Ainsi A est un sous anneau de $(\mathbb{Q}, +, \times)$.
b) $x \in A$ est inversible si, et seulement si, il existe $y \in A$ tel que $xy = 1$.
Puisqu'on peut écrire $x = \frac{m}{2^n}, y = \frac{m'}{2^{n'}}$ avec $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}$,

$$xy = 1 \Rightarrow mm' = 2^{n+n'}$$

Par suite m est, au signe près, une puissance de 2.
La réciproque est immédiate.
Finalement

$$U(A) = \left\{\pm 2^k / k \in \mathbb{Z}\right\}$$

Exercice 55 : [énoncé]
Soit $\varphi : \mathbb{R} \to \mathbb{R}$ définie par $\varphi : x \mapsto x - 1$. φ est une bijection et on vérifie

$$\varphi(a \top b) = \varphi(a) + \varphi(b) \text{ et } \varphi(a \star b) = \varphi(a) \times \varphi(b)$$

Par la bijection φ^{-1} la structure de corps sur $(\mathbb{R}, +, \times)$ est transportée sur $(\mathbb{R}, \top, \star)$.
Notamment, les neutres de $(\mathbb{R}, \top, \star)$ sont 1 et 2.

Exercice 56 : [énoncé]
Montrons que $\mathbb{Q}\left[\sqrt{d}\right]$ est un sous-corps de $(\mathbb{R}, +, \times)$.
$\mathbb{Q}\left[\sqrt{d}\right] \subset \mathbb{R}$, $1 \in \mathbb{Q}\left[\sqrt{d}\right]$.
Soient $x, y \in \mathbb{Q}\left[\sqrt{d}\right]$, on peut écrire $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$ avec $a, b, a', b' \in \mathbb{Q}$.
$x - y = (a - a') + (b - b')\sqrt{d}$ avec $a - a', b - b' \in \mathbb{Q}$ donc $x - y \in \mathbb{Q}\left[\sqrt{d}\right]$.
$xy = (aa' + bb'd) + (ab' + a'b)\sqrt{d}$ avec $aa' + bb'd, ab' + a'b \in \mathbb{Q}$ donc $xy \in \mathbb{Q}\left[\sqrt{d}\right]$.
Si $x \neq 0$ alors

$$\frac{1}{x} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2} = \frac{a}{a^2 - db^2} - \frac{b\sqrt{d}}{a^2 - db^2}$$

avec

$$\frac{a}{a^2 - db^2}, \frac{b}{a^2 - db^2} \in \mathbb{Q}$$

Notons que, ici $a - b\sqrt{d} \neq 0$ car $\sqrt{d} \notin \mathbb{Q}$.
Finalement $\mathbb{Q}\left[\sqrt{d}\right]$ est un sous-corps de $(\mathbb{R}, +, \times)$ et c'est donc un corps.

Exercice 57 : [énoncé]
($\Leftarrow$) tout élément non nul d'un corps est symétrisable donc régulier et n'est donc pas diviseurs de zéro.
($\Rightarrow$) Supposons que A n'ait pas de diviseurs de zéros. Soit $a \in A$ tel que $a \neq 0$.
Montrons que a est inversible Considérons l'application $\varphi : A \to A$ définie par $\varphi(x) = a.x$.
a n'étant pas diviseur de zéro, on démontre aisément que φ est injective, or A est fini donc φ est bijective. Par conséquent il existe $b \in A$ tel que $\varphi(b) = 1$ i.e. $ab = 1$. Ainsi a est inversible. Finalement A est un corps.

Exercice 58 : [énoncé]
$0, 1 \in F$ puis par récurrence $\forall n \in \mathbb{N}, n \in F$. Par passage à l'opposée $\forall p \in \mathbb{Z}, p \in F$.
Par passage à l'inverse : $\forall q \in \mathbb{N}^\star, 1/q \in F$. Par produit $\forall r = p/q \in \mathbb{Q}, r \in F$.