# Groupes, anneaux, corps

(*corrigés*)

**Exercice 5** Montrons que $H$ est un sous-groupe de $(\mathbb{R}_+^*, \times)$.

- ⋆ On a $1 \in H$ car $1 = 1 + 0 \times \sqrt{3}$ et $(1,0) \in \mathbb{N} \times \mathbb{Z}$ et $1^2 - 3 \times 0^2 = 1$. Ainsi, $H \neq \varnothing$.
- ⋆ Justifions que $H \subset \mathbb{R}_+^*$. Soit $h \in H$. Il existe $(x,y) \in \mathbb{N} \times \mathbb{Z}$ tel que $h = x + y\sqrt{3}$ et $x^2 - 3y^2 = 1$. Comme $x \geqslant 0$, on a :
$$x = |x| = \sqrt{x^2} = \sqrt{3y^2 + 1} > \sqrt{3y^2} = |y|\sqrt{3}$$
De plus, $|y| \geqslant y$ donc $|y|\sqrt{3} \geqslant y\sqrt{3}$ (car $\sqrt{3} \geqslant 0$). Ainsi :
$$x > y\sqrt{3} \qquad \textit{i.e.} \qquad h = x - y\sqrt{3} > 0$$
Ainsi, $h \in \mathbb{R}_+^*$. Finalement, $H \subset \mathbb{R}_+^*$.
- ⋆ Soient $h, k \in \mathbb{R}_+^*$. Il existe $(x,y),(a,b) \in \mathbb{N} \times \mathbb{Z}$ tels que $h = x + y\sqrt{3}$, $k = a + b\sqrt{3}$ et $x^2 - 3y^2 = 1$, $a^2 - 3b^2 = 1$.
  - On a $x^2 - 3y^2 = 1$ *i.e.* $\big(x - \sqrt{3}y\big)\big(x + \sqrt{3}y\big) = 1$. Ainsi :
  $$h^{-1} = \frac{1}{h} = \frac{1}{x + \sqrt{3}y} = x - \sqrt{3}y$$
  et $x - \sqrt{3}y \in H$ car $x \in \mathbb{N}$, $-y \in \mathbb{Z}$ (car $y \in \mathbb{Z}$) et :
  $$x^2 - 3(-y)^2 = x^2 - 3y^2 = 1$$
  car $x + y\sqrt{3} \in H$. Ainsi, $h^{-1} = x - y\sqrt{3} \in H$.
  - De plus :
  $$h \times k = \big(x + y\sqrt{3}\big)\big(a + b\sqrt{3}\big) = xa + 3yb + (xb + ya)\sqrt{3}$$
  Comme $x, y, a, b \in \mathbb{Z}$, on a $xb + ya \in \mathbb{Z}$. De plus, on sait que $x \geqslant |y|\sqrt{3}$ et $a \geqslant |b|\sqrt{3}$ donc (comme les nombres mis en jeu sont positifs) $xa \geqslant 3|yb|$. Or $|yb| \geqslant -yb$ donc $xa \geqslant -3yb$. Ainsi, l'entier $xa + 3yb$ est positif. Autrement dit, $xa + 3yb \in \mathbb{N}$. Enfin :
  $$\begin{aligned}(xa + 3yb)^2 - 3(xb + ya)^2 &= x^2a^2 + 6xyab + 9y^2b^2 - 3x^2b^2 - 6xyab - 3y^2a^2 \\ &= x^2a^2 + 9y^2b^2 - 3x^2b^2 - 3y^2a^2 \\ &= (x^2 - 3y^2)(a^2 - 3b^2) \\ &= 1 \times 1 \qquad (\text{car } x + y\sqrt{3}, a + b\sqrt{3} \in H) \\ &= 1\end{aligned}$$
  Ainsi, $h \times k \in H$.

Finalement :

$$\boxed{H \text{ est un sous-groupe de } (\mathbb{R}_+^*, \times)}$$

**Exercice 6** Par hypothèse, l'ensemble $A$ est non vide.

- ⋆ Soient $a, b \in A$. On a $\varphi(a), \varphi(b) \in G$ donc $\varphi(a) \star \varphi(b) \in G$ car $\star$ est une loi de composition interne sur $G$ (car $(G, \star)$ est un groupe). Comme $\varphi \in G^A$ est bijective, $\varphi^{-1}(\varphi(a) \star \varphi(b))$ est l'unique antécédent de $\varphi(a) \star \varphi(b)$ par l'application $\varphi$ dans $A$. Ainsi, $a \triangle b \in A$. On en déduit que $\triangle$ est une loi de composition interne sur $A$.
- ⋆ Soient $a, b, c \in A$. On a :
$$\begin{aligned}(a \triangle b) \triangle c &= \underbrace{\big[\varphi^{-1}(\varphi(a) \star \varphi(b))\big]}_{\text{noté } d} \triangle c \\ &= \varphi^{-1}(\varphi(d) \star \varphi(c))\end{aligned}$$
Or $\varphi \circ \varphi^{-1} = \mathrm{Id}_G$ donc :
$$\varphi(d) = \varphi(a) \star \varphi(b)$$
Ainsi :
$$(a \triangle b) \triangle c = \varphi^{-1}\Big((\varphi(a) \star \varphi(b)) \star \varphi(c)\Big)$$
Par un calcul analogue, on obtient :
$$a \triangle (b \triangle c) = \varphi^{-1}\Big(\varphi(a) \star (\varphi(b) \star \varphi(c))\Big)$$
Or la loi $\star$ est associative sur $G$ (car $(G, \star)$ est un groupe) donc :
$$(\varphi(a) \star \varphi(b)) \star \varphi(c) = \varphi(a) \star (\varphi(b) \star \varphi(c))$$
On en déduit que $(a \triangle b) \triangle c = a \triangle (b \triangle c)$. Ainsi, la loi $\triangle$ est associative sur $A$.

★ Notons $e$ l'élément neutre du groupe $(G,\star)$ et posons $\varepsilon = \varphi^{-1}(e) \in A$. Pour tout $a \in A$, on a $\varphi(\varepsilon) = e$ donc :

$$\begin{aligned} a\triangle\varepsilon = \varphi^{-1}(\varphi(a)\star\varphi(\varepsilon)) &= \varphi^{-1}(\varphi(a)\star e) \\ &= \varphi^{-1}(\varphi(a)) \qquad \text{(par définition de } e\text{)} \\ &= a \qquad (\text{car } \varphi^{-1}\circ\varphi = \mathrm{Id}_A) \end{aligned}$$

et, de la même manière, on a $\varepsilon\triangle a = a$. Ainsi, $\varepsilon$ est élément neutre dans $(A,\triangle)$.

★ Soit $a \in A$. Alors $\varphi(a) \in G$ est inversible d'inverse $\varphi(a)^{-1} \in G$ (puisque $(G,\star)$ est un groupe). Montrons que $a$ est inversible (dans $(A,\triangle)$) d'inverse $\varphi^{-1}\Big(\varphi(a)^{-1}\Big)$. Tout d'abord, $\varphi^{-1}\Big(\varphi(a)^{-1}\Big) \in A$ et comme $\varphi\Big(\varphi^{-1}\Big(\varphi(a)^{-1}\Big)\Big) = \varphi(a)^{-1}$, on a :

$$\begin{aligned} a\triangle\varphi^{-1}\Big(\varphi(a)^{-1}\Big) &= \varphi^{-1}\Big(\varphi(a)\star\varphi(a)^{-1}\Big) \\ &= \varphi^{-1}(e) \\ &= \varepsilon \end{aligned}$$

De la même manière, on a $\varphi^{-1}\Big(\varphi(a)^{-1}\Big)\triangle a = \varepsilon$. Finalement, $a$ est inversible dans $(A,\triangle)$ d'inverse $a^{-1} = \varphi^{-1}\Big(\varphi(a)^{-1}\Big)$.

Finalement :

$$\boxed{(A,\triangle) \text{ est un groupe d'élément neutre } \varepsilon = \varphi^{-1}(e)}$$

## Exercice 7

1. (a) Soit $g \in G$. Montrons que $t_g$ est bijective de $G$ sur $G$. Soit $y \in G$. Montrons que $y$ admet un unique antécédent par l'application $t_g$ dans $G$. Comme $g$ est inversible dans $G$ (puisque $G$ est un groupe), on a :

$$\begin{aligned} \forall x \in G, \qquad t_g(x) = y &\iff gx = y \\ &\iff g^{-1}(gx) = g^{-1}y \\ &\iff (g^{-1}g)x = g^{-1}y \quad \text{(associativité de la loi de } G\text{)} \\ &\iff x = g^{-1}y \end{aligned}$$

Donc $y$ admet un unique antécédent par l'application $t_g$ dans $G$. On en déduit donc que :

$$\boxed{\text{l'application } t_g \text{ est bijective}}$$

(b) Posons $P = \prod_{x\in G}(gx)$. Comme $G$ est un groupe commutatif, on a :

$$P = \left(\prod_{x\in G} g\right)\left(\prod_{x\in G} x\right) = g^{|G|}\left(\prod_{x\in G} x\right)$$

Par ailleurs, on sait que $t_g$ est une bijection de $G$ sur $G$. On peut donc effectuer le changement de variable $y = t_g(x) = gx$ dans le produit $P$ de départ et on a :

$$P = \prod_{y\in G} y$$

On a donc l'égalité :

$$P = g^{|G|}\left(\prod_{x\in G} x\right) = \prod_{x\in G} x$$

Or l'élément $\prod_{x\in G} x$ de $G$ est inversible (tout élément d'un groupe étant inversible) donc, en multipliant par $\left(\prod_{x\in G} x\right)^{-1}$ dans l'égalité précédente, on obtient bien :

$$\boxed{g^{|G|} = e}$$

2. On raisonne par analyse-synthèse.

★ **Analyse** : soit $G$ un sous-groupe fini de $\mathbb{C}^*$. Notons $n \in \mathbb{N}^*$ le nombre d'éléments de $G$. Comme $(\mathbb{C}^*,\times)$ est un groupe commutatif, le sous-groupe $G$ est également commutatif. La question 1. s'applique donc et on a :

$$\forall g \in G, \qquad g^n = 1$$

Autrement dit :

$$\forall g \in G, \qquad g \in \mathbb{U}_n,$$

soit encore $G \subset \mathbb{U}_n$. Or on sait que $\mathbb{U}_n$ possède $n$ éléments. Comme $G$ a aussi $n$ éléments, l'inclusion précédente entraîne l'égalité $G = \mathbb{U}_n$.

★ **Synthèse** : pour tout $n \in \mathbb{N}^*$, le sous-groupe $\mathbb{U}_n$ de $\mathbb{C}^*$ est fini (il possède $n$ éléments).

On peut donc conclure que :

$$\boxed{\text{l'ensemble des sous-groupes finis de } \mathbb{C}^* \text{ est } \left\{\mathbb{U}_n \,\middle|\, n \in \mathbb{N}^*\right\}}$$

## Exercice 10

On note $e$ l'élément neutre du groupe $(G,*)$.

1. Soit $x \in G$. Par définition, on a :

$$C_G(x) = \left\{ y \in G \,\middle|\, x * y = y * x \right\}$$

Montrons que $C_G(x)$ est un sous-groupe de $G$.

- ⋆ Il est clair que $C_G(x) \subset G$.
- ⋆ On a $e \in C_G(x)$ car $e * x = x * e = x$ (par définition de l'élément neutre). Ainsi, $C_G(x) \neq \varnothing$.
- ⋆ Soient $y, z \in C_G(x)$. Montrons que $y * z \in C_G(x)$. On a :

$$\begin{aligned} x * (y * z) &= (x * y) * z && \text{(car la loi } * \text{ est associative)} \\ &= (y * x) * z && \text{(car } y \in C_G(x)) \\ &= y * (x * z) && \text{(par associativité de } *) \\ &= y * (z * x) && \text{(car } z \in C_G(x)) \\ &= (y * z) * x && \text{(par associativité de } *) \end{aligned}$$

Ainsi, $y * z \in C_G(x)$.

- ⋆ Soit $y \in C_G(x)$. Montrons que $y^{-1} \in C_G(x)$. Par définition de $y$, on a $x \star y = y \star x$. On en déduit que :

$$\begin{aligned} y^{-1} \star (x \star y) &= y^{-1} \star (y \star x) \\ &= (y^{-1} \star y) \star x && \text{(associativité de la loi } \star) \\ &= e \star x \\ &= x \end{aligned}$$

car $e$ est l'élément neutre du groupe $(G, *)$. On a donc l'égalité :

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

En composant ensuite par $y^{-1}$ à droite, on obtient $y^{-1} \star x = x \star y^{-1}$. Ainsi, $y^{-1} \in C_G(x)$.

Finalement :

$$\boxed{C_G(x) \text{ est un sous-groupe de } G}$$

2. Par définition, le centre $Z(G)$ de $G$ est :

$$Z(G) = \left\{ g \in G \,\middle|\, \forall h \in G,\ g * h = h * g \right\}$$

Montrons que $Z(G)$ est un sous-groupe de $G$.

- ⋆ Tout d'abord, il est clair que $Z(G) \subset G$.
- ⋆ Par définition de l'élément neutre, on a :

$$\forall h \in G, \qquad e * h = h = h * e$$

donc $e \in Z(G)$. Ainsi, $Z(G) \neq \varnothing$.

- ⋆ Soit $g, g' \in Z(G)$. Montrons que $g * g' \in Z(G)$. Soit $h \in G$. Alors :

$$\begin{aligned} (g * g') * h &= g * (g' * h) && \text{(associativité de } *) \\ &= g * (h * g') && \text{(car } g' \in Z(G)) \\ &= (g * h) * g' && \text{(associativité de } *) \\ &= (h * g) * g' && \text{(car } g \in Z(G)) \\ &= h * (g * g') \end{aligned}$$

en utilisant encore l'associativité de $*$. Ainsi, $g * g' \in Z(G)$.

- ⋆ Soit $g \in Z(G)$. Montrons que $g^{-1} \in Z(G)$. Soit $h \in H$. On a $g * h = h * g$ donc :

$$g^{-1} * (g * h) * g^{-1} = g^{-1} * (h * g) * g^{-1}$$

En utilisant encore l'associativité de $*$ dans $G$ et le fait que $g * g^{-1} = g^{-1} * g = e$, on obtient alors l'égalité $g^{-1} * h = h * g^{-1}$. On conclut donc que $g^{-1} \in Z(G)$.

Finalement :

$$\boxed{Z(G) \text{ est un sous-groupe de } G}$$

## Exercice 15

- ⋆ On sait que l'application $\mathrm{sh} \in \mathbb{R}^{\mathbb{R}}$ est bijective de $\mathbb{R}$ sur $\mathbb{R}$.
- ⋆ On sait que :

$$\forall x \in \mathbb{R}, \qquad \mathrm{sh}(x)^2 + 1 = \mathrm{ch}(x)^2$$

En outre, on peut montrer (*cf.* fiche de TD#1) que :

$$\forall x, y \in \mathbb{R}, \qquad \mathrm{sh}(x + y) = \mathrm{sh}(x)\,\mathrm{ch}(y) + \mathrm{ch}(x)\,\mathrm{sh}(y)$$

Pour tous $x, y \in \mathbb{R}$, on a donc :

$$\begin{aligned} \mathrm{sh}(x) \star \mathrm{sh}(y) &= \mathrm{sh}(x)\sqrt{\mathrm{sh}(y)^2 + 1} + \mathrm{sh}(y)\sqrt{\mathrm{sh}(x)^2 + 1} \\ &= \mathrm{sh}(x)\,\sqrt{\mathrm{ch}(y)^2} + \mathrm{sh}(y)\sqrt{\mathrm{ch}(x)^2} \\ &= \mathrm{sh}(x)\,\mathrm{ch}(y) + \mathrm{sh}(y)\mathrm{ch}(x) \end{aligned}$$

car la fonction ch est à valeurs positives et donc :

$$\mathrm{sh}(x) \star \mathrm{sh}(y) = \mathrm{sh}(x + y)$$

On en déduit que $(\mathrm{sh}(\mathbb{R}), \star) = (\mathbb{R}, \star)$ est un groupe.

⋆ Pour tous $x, y \in \mathbb{R}$, on a :

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

par commutativité de l'addition dans $\mathbb{R}$. La loi $\star$ est donc commutative.

Finalement :

$$\boxed{(\mathbb{R}, \star) \text{ est un groupe abélien}}$$

## Exercice 18

1. Soient $x, y \in A$. On veut montrer que $x \times y = y \times x$.
   ⋆ Soit $a \in A$. Comme $A$ est un anneau de Boole, on a $a^2 = a$ et $(-a)^2 = -a$. Or $-a = (-1_A) \times a = a \times (-1_A)$ donc :
   $$(-a)^2 = (-a) \times (-a) = a \times (-1_A) \times (-1_A) \times a = a \times (-1_A)^2 \times a$$
   On a $(-1_A)^2 = 1_A$ donc $(-a)^2 = a^2$ *i.e.* $a = -a$.
   ⋆ On a $(x+y)^2 = x + y$ (car $A$ est un anneau de Boole) *i.e* :
   $$x^2 + x \times y + y \times x + y^2 = x + y$$
   Or $x^2 = x$ et $y^2 = y$ donc $x \times y = -y \times x = y \times x$ d'après le point précédent (avec $a = y \times x$).
2. On suppose que $A$ est un anneau intègre. Soit $x \in A$. On a $x^2 = x$ *i.e.* $x^2 - x = 0_A$ soit encore $x \times (x - 1_A) = 0_A$ par distributivité de $\times$ par rapport à $+$. Comme $A$ est intègre, on a $x = 0_A$ ou $x - 1_A = 0_A$. Autrement dit, $x = 0_A$ ou $x = 1_A$. Ainsi :
   $$\boxed{\text{si } A \text{ est un anneau de Boole intègre, alors } A = \{0_A, 1_A\}}$$
3.

## Exercice 20

Soit $f \in B^A$ un morphisme d'anneaux tel que $f \neq 0_{B^A}$. Montrons que $f$ est injectif. Soit $x \in A \setminus \{0_A\}$. Comme $A$ est un corps, $a$ est inversible. Notons $b = a^{-1} \in A$ son inverse. On a $a \times b = 1$ donc $f(a \times b) = f(1_A)$. Or $f$ est un morphisme d'anneaux donc :

$$f(1_A) = 1_B \qquad f(a \times b) = f(a) \times f(b)$$

On a donc l'égalité $f(a) \times f(b) = 1_B$. On en déduit que $f(a) \neq 0_B$ (car si $f(a) = 0_B$, alors $f(a) \times f(b) = 0_B$, ce qui est absurde car $0_B \neq 1_B$). Par contraposition, si $f(a) = 0_B$, alors $a = 0_A$. Ceci montre l'inclusion $\mathrm{Ker}(f) \subset \{0_A\}$. Comme on sait que $0_A \in \mathrm{Ker}(f)$, on a aussi l'inclusion $\{0_A\} \subset \mathrm{Ker}(f)$. Par double inclusion, on a finalement $\mathrm{Ker}(f) = \{0_A\}$. Finalement :

$$\boxed{f \text{ est injectif}}$$

## Exercice 21

Par hypothèse sur $f$, on a :

$$\forall m, n \in \mathbb{R}, \qquad \begin{cases} f(m+n) = f(m) + f(n) \\ f(mn) = f(m)f(n) \end{cases} \qquad \text{et} \qquad f(1) = 1$$

1. Soit $x \in \mathbb{R}$. Montrons d'abord par récurrence que :
   $$\forall n \in \mathbb{N}, \qquad f(nx) = nf(x)$$
   ⋆ On a :
   $$f(0) = f(0+0) = f(0) + f(0) \qquad \text{donc} \qquad f(0) = 0$$
   Ainsi, $f(0 \times x) = 0 \times f(x)$. La propriété est donc vraie pour $n = 0$.
   ⋆ Soit $n \in \mathbb{N}$. On suppose que $f(nx) = nf(x)$. Montrons que $f((n+1)x) = (n+1)f(x)$. On a :
   $$f((n+1)x) = f(nx + x) = f(nx) + f(x) = nf(x) + f(x) = (n+1)f(x)$$
   en utilisant l'hypothèse de récurrence.
   Par principe de récurrence simple, on a bien $f(nx) = nf(x)$ pour tout $n \in \mathbb{N}$.
   Soit maintenant $n \in \mathbb{Z} \setminus \mathbb{N}$. On a :
   $$0 = f(0) = f(nx + (-nx)) = f(nx) + f(-nx)$$
   Or $-n \in \mathbb{N}$ donc $f(-nx) = -nf(x)$. On déduit de l'égalité ci-dessus que :
   $$f(nx) = -(-nx) = nx$$
   Finalement :
   $$\boxed{\forall x \in \mathbb{R},\ \forall n \in \mathbb{Z}, \qquad f(nx) = nf(x)}$$
2. Soit $r \in \mathbb{Q}$. Il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$. D'après la question précédente (d'abord avec $x = \frac{p}{q}$ puis avec $x = 1$), on a :
   $$qf(r) = qf\left(\frac{p}{q}\right) = f\left(q \times \frac{p}{q}\right) = f(p) = pf(1) = p$$
   Ainsi, $f(r) = \dfrac{p}{q} = r$. Finalement :
   $$\boxed{\forall r \in \mathbb{Q}, \qquad f(r) = r}$$

3. Soit $x \in \mathbb{R}_+$. Alors $x = \left(\sqrt{x}\right)^2$ et comme $f$ est un morphisme d'anneaux, on a :

$$f(x) = f\left(\left(\sqrt{x}\right)^2\right) = f\left(\sqrt{x}\right)^2 \geqslant 0$$

donc :

$$\boxed{\forall x \in \mathbb{R}_+, \qquad f(x) \geqslant 0}$$

Soient $x, y \in \mathbb{R}$ tels que $x \leqslant y$. Alors $y - x \in \mathbb{R}_+$ et donc, d'après ce qui précède, $f(y-x) \geqslant 0$. Mais $f$ est un morphisme d'anneaux donc :

$$f(y) - f(x) \geqslant 0 \qquad \textit{i.e.} \qquad f(x) \leqslant f(y)$$

Ainsi :

$$\boxed{\text{la fonction } f \text{ est croissante sur } \mathbb{R}}$$

4. Soit $x \in \mathbb{R}$. Pour tout $n \in \mathbb{N}$, on pose :

$$\boxed{u_n = \frac{\lfloor 2^n x \rfloor}{2^n} \qquad \text{et} \qquad v_n = \frac{\lfloor 2^n x \rfloor + 1}{2^n}}$$

Montrons que $u_n \xrightarrow[n\to+\infty]{} x$. Soit $x \in \mathbb{N}$. On a $2^n x - 1 \leqslant \lfloor 2^n x \rfloor \leqslant 2^n x$ et donc, en divisant par $2^n > 0$ :

$$\forall n \in \mathbb{N}, \qquad x - \frac{1}{2^n} \leqslant u_n \leqslant x$$

Le résultat est une conséquence du théorème des gendarmes. De même, $v_n \xrightarrow[n\to+\infty]{} x$. Soit $n \in \mathbb{N}$. On a $\lfloor 2^n x \rfloor \leqslant 2^n x \leqslant \lfloor 2^n x \rfloor + 1$ donc, en divisant par $2^n + 1$, on a :

$$u_n = \frac{\lfloor 2^n x \rfloor}{2^n} \leqslant x \leqslant \frac{\lfloor 2^n x \rfloor + 1}{2^n} = v_n$$

La fonction $f$ est croissante sur $\mathbb{R}$ donc $f(u_n) \leqslant f(x) \leqslant f(v_n)$. Or $f|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$ et $u_n, v_n \in \mathbb{Q}$ donc $f(u_n) = u_n$ et $f(v_n) = v_n$. Ainsi :

$$\forall n \in \mathbb{N}, \qquad u_n \leqslant f(x) \leqslant v_n$$

On sait que les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont convergentes de limite $x$ donc, en faisant tendre $n$ vers $+\infty$ dans les inégalités précédentes, on a $x \leqslant f(x) \leqslant x$, *i.e.* $f(x) = x$. Finalement :

$$\boxed{f = \mathrm{Id}_{\mathbb{R}}}$$