3.5 Exercices corrigés

3.5.1 Structure de groupe

Exercice 1 :

1. *Montrer que $\mathcal{U}=\{z\in\mathbb{C}$ tels que $|z|=1\}$ est un groupe pour la multiplication.*

   Voilà qui n'est pas si difficile ! !
   - ▷ On montre que si $z\in\mathcal{U}$ et $z'\in\mathcal{U}$, alors $zz'\in\mathcal{U}$
     En effet, nous avons $|zz'|=|z|\times|z'|$, et si $z\in\mathcal{U}$ et $z'\in\mathcal{U}$ alors $|z|=|z'|=1$ et donc $|zz'|=1$, et donc, $zz'\in\mathcal{U}$
   - ▷ D'autre part, 1, le neutre pour la multiplication est élément de $\mathcal{U}$
   - ▷ Si $z\in\mathcal{U}$, alors $|z|^2=z\overline{z}=1$, et donc $z^{-1}=\overline{z}$ et comme $\overline{z}\in\mathcal{U}$, $z^{-1}\in\mathcal{U}$; ainsi, tout $z\in\mathcal{U}$ admet un symétrique $z^{-1}\in\mathcal{U}$
   - ▷ Pour conclure, la multiplication est aussi commutative dans $\mathcal{U}$

   $\mathcal{U}=\{z\in\mathbb{C}$ tels que $|z|=1\}$ est donc un groupe commutatif pour la multiplication

2. *Soit E un ensemble et $\mathcal{B}(E)$ l'ensemble des bijections de E. Montrer que $(\mathcal{B}(E),\circ)$ est un groupe. En étudier la commutativité*

   - ▷ La composition de deux bijections étant une bijection, la loi $\circ$ est bien une loi de composition interne de $\mathcal{B}(E)$
   - ▷ D'autre part, la loi $\circ$ étant, de manière générale, associative ; elle l'est donc, en particulier dans $\mathcal{B}(E)$
   - ▷ L'élément neutre pour $\circ$ est l'application identique de E, notée Id_E
   - ▷ Comme tout $f\in\mathcal{B}(E)$ est bijective, il existe donc $f^{-1}\in\mathcal{B}(E)$ telle que $f\circ f^{-1}=f^{-1}\circ f=\mathrm{Id}_E$. f^{-1} est donc le symétrique de f dans $\mathcal{B}(E)$

   $(\mathcal{B}(E),\circ)$ est donc un groupe.

   Par contre, $(\mathcal{B}(E),\circ)$ n'est pas un groupe commutatif.

   Prenons, par exexemple $E=\{A;B;C\}$ et soient $f\in\mathcal{B}(E)$ et $g\in\mathcal{B}(E)$ telles que :

   $$f:\begin{pmatrix}A&B&C\\\downarrow&\downarrow&\downarrow\\A&C&B\end{pmatrix}\qquad g:\begin{pmatrix}A&B&C\\\downarrow&\downarrow&\downarrow\\C&A&B\end{pmatrix}$$

   Alors :

   $$f\circ g:\begin{pmatrix}A&B&C\\\downarrow&\downarrow&\downarrow\\B&A&C\end{pmatrix}\qquad g\circ f:\begin{pmatrix}A&B&C\\\downarrow&\downarrow&\downarrow\\C&B&A\end{pmatrix}$$

   On voit bient que $f\circ g\neq g\circ f$; il suffit de voir que $f\circ g(A)=f(g(A))=f(C)=B$, alors que $g\circ f(A)=g(f(A))=g(A)=C$; on a donc $f\circ g(A)\neq g\circ f(A)$

   On peut remarquer que $f\circ f=\mathrm{Id}_E$ et donc $f=f^{-1}$.

   D'où $(g\circ f)\circ(f\circ g)=g\circ(f\circ f)\circ g=g\circ\mathrm{Id}_E\circ g=g\circ g$. Nous avons :

   $$g\circ g=g^2:\begin{pmatrix}A&B&C\\\downarrow&\downarrow&\downarrow\\B&C&A\end{pmatrix}$$

   Démontrer que $g^3=\mathrm{Id}_E$ et que donc, $g^2=g^{-1}$

Exercice 2 :

Un ensemble E est muni d'une loi $\star$ interne et associative ; on suppose que, pour tout $a\in G$, γ_a et δ_a sont surjectives (Voir 3.1.2). Montrer que $(E,\star)$ est un groupe

1. Existence d'un élément neutre

   Soit $a\in E$

   γ_a et δ_a étant surjectives :

▷ Il existe $e \in E$ tel que $\delta_a(e) = a \iff a = e \star a$
▷ Il existe $f \in E$ tel que $\gamma_a(f) = a \iff a = a \star f$
Quelque part, ici, e et f jouent un rôle d'élément neutre, mais, c'est un neutre qui, à priori, dépend de a ; ce n'est pas ce que nous cherchons. Ce que nous voudrions démontrer, c'est qu'il existe un élément e tel que, pour tout $x \in E$, $x \star e = e \star x = x$
Soit donc $x \in E$
Il existe $\alpha \in E$ tel que $\delta_a(\alpha) = a \star \alpha = x$; de même, il existe $\beta \in E$ tel que $\gamma_a(\beta) = \beta \star a = x$
Alors :

$$\left\{\begin{array}{rcl} e \star x = & e \star (a \star \alpha) & \\ = & (e \star a) \star \alpha & \text{et} \\ = & a \star \alpha = x & \end{array}\right. \qquad \left\{\begin{array}{rcl} x \star f = & (\beta \star a) \star f & \\ = & \beta \star (a \star f) & \\ = & \beta \star a = x & \end{array}\right.$$

Ainsi, pour tout $x \in E$, nous avons $e \star x = x$ et $x \star f = x$. En particulier :
▷ Si $x = f$, alors $e \star f = f$
▷ Si $x = e$, alors $e \star f = e$
Et donc : $f = e \star f = e$ Et donc, pour tout $x \in E$, $x \star e = e \star x = x$, et e est bien l'élément neutre de $(E, \star)$

2. Existence d'un élément symétrique pour tout $x \in E$
Soit $x \in E$
Il faut montrer qu'il existe $x_1 \in E$ tel que $x \star x_1 = x_1 \star x = e$ où e est l'élément neutre pour $\star$
Comme γ_x et δ_x sont surjectives, il existe $u \in E$ et $v \in E$ tels que :

$$\delta_x(u) = e \iff u \star x = e \text{ et } \gamma_x(v) = e \iff x \star v = e$$

Nous avons alors :

$$\begin{array}{rcl} v = e \star v = & (u \star x) \star v & \\ = & u \star (x \star v) & \\ = & u \star e & \\ = & u & \end{array}$$

Ainsi, pour tout $x \in E$, il existe $u \in E$ tel que $x \star u = u \star x = e$, c'est à dire que pour tout $x \in E$, il existe un symétrique.

Exercice 3 :

Soit E un ensemble quelconque et $a \in E$ un élément de E. Nous savons que $(\mathcal{B}(E), \circ)$ est un groupe. Nous appelons $\mathcal{A}$ l'ensemble des bijections de $\mathcal{B}(E)$ laissant a fixe (c'est à dire $f \in \mathcal{A} \iff f(a) = a$).
Démontrer que $(\mathcal{A}, \circ)$ est un sous-groupe de $(\mathcal{B}(E), \circ)$

Pour le démontrer, nous allons utiliser la caractérisation des sous-groupes vue dans le théorème 3.1.4

1. Tout d'abord, $\mathcal{A} \neq \emptyset$
En effet, l'application identique Id_E est un élément de $\mathcal{A}$
2. D'autre part, si $f \in \mathcal{A}$, alors $f^{-1} \in \mathcal{A}$
En effet, si $f \in \mathcal{A}$, f est une bijection et $f(a) = a$ et sa bijection réciproque f^{-1} vérifie :

$$f(a) = a \iff f^{-1} \circ f(a) = f^{-1}(a) \iff f^{-1}(a) = a$$

Et donc $f^{-1} \in \mathcal{A}$
3. Soient $f \in \mathcal{A}$ et $g \in \mathcal{A}$, alors $f \circ g^{-1} \in \mathcal{A}$
Nous avons $f \circ g^{-1}(a) = f\left[g^{-1}(a)\right] = f(a) = a$
Donc $f \circ g^{-1} \in \mathcal{A}$

Ainsi, $(\mathcal{A}, \circ)$ est un sous-groupe de $(\mathcal{B}(E), \circ)$

Exercice 4 :

Soit $(G,\star)$ un groupe. On appelle centre de G l'ensemble $Z(G)$ des éléments de G qui commutent avec tous les éléments de G, c'est à dire : $Z(G) = \{c \in G \text{ tels que } (\forall x \in G)(x \star c = c \star x)\}$ Démontrer que $(Z(G),\star)$ est un sous-groupe de $(G,\star)$

Une nouvelle fois, nous allons utiliser le théorème 3.1.4

1. Nous avons $Z(G) \neq \emptyset$
   En effet, l'élément neutre e est tel que, pour tout $x \in G$, $e \star x = x \star e$; donc $e \in Z(G)$
2. Si $y \in Z(G)$, alors $y^{-1} \in Z(G)$
   En effet, soit $y \in Z(G)$ et $u \in G$ quelconque ; alors $y \star u = u \star y$. En composant à droite par y^{-1}, nous obtenons :
   $$y\star u = u\star y \iff (y\star u)\star y^{-1} = (u\star y)\star y^{-1} \iff (y\star u)\star y^{-1} = u\star\left(y\star y^{-1}\right) \iff (y\star u)\star y^{-1} = u$$
   En composant maintenant à gauche par y^{-1}, nous obtenons :
   $$(y\star u)\star y^{-1} = u \iff y^{-1}\star(y\star u)\star y^{-1} = y^{-1}\star u \iff \left(y^{-1}\star y\right)\star u\star y^{-1} = y^{-1}\star u \iff u\star y^{-1} = y^{-1}\star u$$
   Et donc $y^{-1} \in Z(G)$
3. Si $x \in Z(G)$ et $y \in Z(G)$, alors $x \star y^{-1} \in Z(G)$
   Soient donc $x \in Z(G)$, $y \in Z(G)$ et $u \in G$, quelconque. Alors :
   $$\left(x\star y^{-1}\right)\star u = x\star\left(y^{-1}\star u\right) = x\star\left(u\star y^{-1}\right) = (x\star u)\star y^{-1} = (u\star x)\star y^{-1} = u\star\left(x\star y^{-1}\right)$$
   Et donc $x \star y^{-1} \in Z(G)$

$(Z(G),\star)$ est donc un sous-groupe de $(G,\star)$

Exercice 5 :

Soit $(G,\star)$ un groupe de neutre e et $a \in G$; on considère les applications f_a définies par :

$$\begin{cases} f_a : G & \longrightarrow & G \\ x & \longmapsto & f_a(x) = a\star x\star a^{-1} \end{cases}$$

Montrer que f_a est un automorphisme

1. Nous allons montrer que f_a est un homomorphisme de groupe *(un endomorphisme donc)*
   Soient $x \in G$ et $y \in G$. Alors :
   $$\begin{aligned} f_a(x\star y) &= a\star(x\star y)\star a^{-1} \\ &= (a\star x)\star\left(y\star a^{-1}\right) \\ &= (a\star x)\star e\star\left(y\star a^{-1}\right) \\ &= (a\star x)\star\left(a^{-1}\star a\right)\star\left(y\star a^{-1}\right) \\ &= \left(a\star x\star a^{-1}\right)\star\left(a\star y\star a^{-1}\right) \\ &= f_a(x)\times f_a(y) \end{aligned}$$
   Nous avons donc, pour tout $x \in G$ et tout $y \in G$ $f_a(x\star y) = f_a(x)\times f_a(y)$
   f_a est bien un endomorphisme de $(G,\star)$
2. IL faut maintenant montrer que f_a est bijectif
   (a) **Montrons que f_a est injective**
   Soient $x \in G$ et $y \in G$ tels que $f_a(x) = f_a(y)$; alors :
   $$f_a(x) = f_a(y) \iff a\star x\star a^{-1} = a\star y\star a^{-1}$$
   En composant à gauche par a^{-1}, nous avons :
   $$a\star x\star a^{-1} = a\star y\star a^{-1} \iff a^{-1}\star a\star x\star a^{-1} = a^{-1}\star a\star y\star a^{-1} \iff x\star a^{-1} = y\star a^{-1}$$
   En composant à droite par a, nous obtenons :
   $$x\star a^{-1} = y\star a^{-1} \iff x\star a^{-1}\star a = y\star a^{-1}\star a \iff x = y$$
   f_a est donc injective

(b) **Montrons que f_a est surjective**
Soit $y \in G$; existe-t-il $x \in G$ tel que $f_a(x) = y$?
Si cet $x \in G$ existe, alors $y = a \star x \star a^{-1}$, en composant à droite par a et à gauche par a^{-1}, on trouve $x = a^{-1} \star y \star a$
Nous avons alors $f_a(x) = a \star \left(a^{-1} \star y \star a\right) \star a^{-1} = y$, et donc f_a est surjective.

f_a est donc bijective

f_a est donc un automorphisme

Correction des exercices complémentaires sur les groupes

Exercice 9 :

Soit $a \in \mathbb{R}$ On définit, sur $\mathbb{R}$ la loi $\star$ définie par : $x \star y = x + y + a$ Démontrer que $(\mathbb{R}, \star)$ est un groupe commutatif

La loi $\star$ est de manière évidente interne et commutative.

▷ Montrons qu'elle est associative
Soient $x \in \mathbb{R}$, $y \in \mathbb{R}$ et $z \in \mathbb{R}$
- $x \star (y \star z) = x \star (y + z + a) = x + (y + z + a) + a = x + y + z + 2a$
- $(x \star y) \star z = (x + y + a) \star z = (x + y + a) + z + a = x + y + z + 2a$

Nous avons donc : $x \star (y \star z) = (x \star y) \star z$; la loi $\star$ est bien associative.

▷ Montrons que la loi $\star$ admet un élément neutre
Si cet élément neutre existe, appelons le e, alors $x \star e = x$, c'est à dire :

$$x \star e = x + e + a = x \Longrightarrow e = -a$$

Donc, si lélément neutre existe, il est égal à $-a$; et réciproquement, nous avons $x \star (-a) = x + (-a) + a = x$

▷ Existe-t-il un symétrique pour la loi $\star$ pour tout $x \in \mathbb{R}$
Si ce symétrique existe, appelons le x_1, alors $x \star x_1 = -a$, et nous avons donc :

$$x \star x_1 = -a \Longleftrightarrow x + x_1 + a = -a \Longleftrightarrow x_1 = -x - 2a$$

Réciproquement, il est clair que $x \star (-x - 2a) = -a$ et donc que tour réel x, admet pour la loi $\star$, un symétrique

$(\mathbb{R}, \star)$ est donc un groupe commutatif

Exercice 10 :

Dans $\mathbb{R}^{*+} \times \mathbb{R}$, on définit la loi $\star$ par : $(a, b) \star (c, d) = (ac, ad + b)$ Vérifier que $(\mathbb{R}^{*+} \times \mathbb{R}, \star)$ est un groupe

1. C'est clairement une loi interne
   Nous avons $(ac, ad + b) \in \mathbb{R}^2$ et comme $a > 0$ et $c > 0$, nous avons $ac > 0$ et donc $(ac, ad + b) \in \mathbb{R}^{*+} \times \mathbb{R}$
2. La loi $\star$ n'est pas commutative
   En effet :
   - $(1, 2) \star (3, 4) = (3, 4 + 2) = (3, 6)$
   - $(3, 4) \star (1, 2) = (3, 6 + 4) = (3, 10)$

   Nous avons $(1, 2) \star (3, 4) \neq (3, 4) \star (1, 2)$ et la loi $\star$ n'est donc pas commutative
3. Montrons que la loi est associative Soient $(a, b) \in \mathbb{R}^{*+} \times \mathbb{R}$, $(c, d) \in \mathbb{R}^{*+} \times \mathbb{R}$ et $(e, f) \in \mathbb{R}^{*+} \times \mathbb{R}$
   - Premièrement :
   $$\begin{aligned}(a, b) \star ((c, d) \star (e, f)) &= (a, b) \star ((ce, cf + d)) \\ &= (ace, a(cf + d) + b) \\ &= (ace, acf + ad + b)\end{aligned}$$
   - En second lieu :
   $$\begin{aligned}((a, b) \star (c, d)) \star (e, f) &= (ac, ad + b) \star (e, f) \\ &= (ace, ac \times f + ad + b) \\ &= (ace, acf + ad + b)\end{aligned}$$

Nous avons donc bien $(a,b)\star((c,d)\star(e,f))=((a,b)\star(c,d))\star(e,f)$ et mla loi $\star$ est associative.

4. Existence d'un élément neutre
   S'il existe un élément neutre noté (e,f), nous devons avoir, pour tout $(a,b)\in\mathbb{R}^{*+}\times\mathbb{R}$:
   $$(a,b)\star(e,f)=(a,b)$$
   Or, $(a,b)\star(e,f)=(ae,af+b)$ et
   $$(a,b)\star(e,f)=(a,b)\Longleftrightarrow(ae,af+b)=(a,b)$$
   D'où nous avons le système déquations, vrai pour tout $a>0$ et tout $b\in\mathbb{R}$:
   $$\left\{\begin{array}{rcl} ae= & a \\ af+b= & b \end{array}\right.\Longleftrightarrow e=1 \text{ et } f=0$$
   D'où, le couple $(1,0)$ est le neutre pour $\star$
5. Existence d'un symétrique
   Soit $(a,b)\in\mathbb{R}^{*+}\times\mathbb{R}$; si (a,b) admet un symétrique pour la loi $\star$, alors, ce symétrique $(c,d)\in\mathbb{R}^{*+}\times\mathbb{R}$ est tel que :
   $$(a,b)\star(c,d)=(1,0)$$
   Nous avons alors :
   $$(ac=1 \text{ et } ad+b=0)\Longleftrightarrow\left(c=\frac{1}{a} \text{ et } d=\frac{-b}{a}\right)$$
   Ainsi, le symétrique de $(a,b)\in\mathbb{R}^{*+}\times\mathbb{R}$ pour la loi $\star$ est donné par : $\left(\frac{1}{a},\frac{-b}{a}\right)$

$(\mathbb{R}^{*+}\times\mathbb{R},\star)$ est donc un groupe non commutatif

Exercice 11 :

Dans $\mathbb{R}^2$, on définit la loi $\star$ par : $(a,b)\star(c,d)=(a+c,be^c+de^{-a})$ Vérifier que $(\mathbb{R}^2,\star)$ est un groupe

C'est clairement une loi de composition interne

1. Ce n'est pas une loi commutative
   En effet :
   - $(1,0)\star(0,1)=\left(1,e^{-1}\right)$
   - $(0,1)\star(1,0)=(1,e)$

   Nous avons $(1,0)\star(0,1)\neq(0,1)\star(1,0)$ et la loi $_star$ n'est pas commutative.
2. Elle est associative
   Soient $(a,b)\in\mathbb{R}^2$, $(c,d)\in\mathbb{R}^2$ et $(g,h)\in\mathbb{R}^2$
   - Premièrement :
   $$\begin{array}{rcl}(a,b)\star((c,d)\star(g,h))= & (a,b)\star((c+g,de^g+he^{-c})) \\ = & (a+c+g,be^{c+g}+(de^g+he^{-c})e^{-a}) \\ = & (a+c+g,be^{c+g}+de^{g-a}+he^{-c-a})\end{array}$$
   - En second lieu :
   $$\begin{array}{rcl}((a,b)\star(c,d))\star(g,h)= & (a+c,be^c+de^{-a})\star(g,h) \\ = & \left(a+c+g,(be^c+de^{-a})e^g+he^{-(a+c)}\right) \\ = & (a+c+g,be^{c+g}+de^{-a+g}+he^{-a-c})\end{array}$$

   Nous avons donc bien $(a,b)\star((c,d)\star(g,h))=((a,b)\star(c,d))\star(g,h)$ et mla loi $\star$ est associative.
3. La loi $\star$ admet un élément neutre
   S'il existe un élément neutre noté (c,d), nous devons avoir, pour tout $(a,b)\in\mathbb{R}^2$:
   $$(a,b)\star(c,d)=(a,b)$$

Ce qui se traduit par :

$$(a,b)\star(c,d)=(a,b)\Longleftrightarrow\left(a+c,be^c+de^{-a}\right)=(a,b)$$

Nous obtenons donc le système :

$$\left\{\begin{array}{rcl}a+c=&a\\be^c+de^{-a}=&b\end{array}\right.\Longrightarrow c=0\text{ et }b+de^{-a}=b\Longrightarrow c=0\text{ et }d=0$$

D'où, le couple $(0,0)$ est le neutre pour $\star$

4. Existence d'un symétrique

Soit $(a,b)\in\mathbb{R}^2$; si (a,b) admet un symétrique pour la loi $\star$, alors, ce symétrique $(c,d)\in\mathbb{R}^2$ est tel que :

$$(a,b)\star(c,d)=(0,0)$$

Nous avons alors :

$$\left(a+c=0\text{ et }be^c+de^{-a}=0\right)\Longleftrightarrow(c=-a\text{ et }d=-b)$$

Ainsi, le symétrique de $(a,b)\in\mathbb{R}^2$ pour la loi $\star$ est donné par : $(-a,-b)$

$\left(\mathbb{R}^2,\star\right)$ est donc un groupe non commutatif

Exercice 12 :

Soit $n\in\mathbb{N}^*$. Dans $\mathbb{R}^*\times\mathbb{R}$, on définit la loi $\star$ par : $(a,b)\star(c,d)=(ac,ad+bc^n)$ Vérifier que $(\mathbb{R}^*\times\mathbb{R},\star)$ est un groupe

1. C'est une loi de composition interne

Si $a\neq0$ et $c\neq0$, alors $ac\neq0$ et donc, nous avons bien $(ac,ac+bc^n)\in\mathbb{R}^*\times\mathbb{R}$

2. Elle n'est pas commutative si $n\geqslant2$

Soient $(a,b)\in\mathbb{R}^*\times\mathbb{R}$, $(c,d)\in\mathbb{R}^*\times\mathbb{R}$; alors :

- $(a,b)\star(c,d)=(ac,ad+bc^n)$
- $(c,d)\star(a,b)=(ac,bc+da^n)$

Bien entendu, à priori, nous avons $(a,b)\star(c,d)\neq(c,d)\star(a,b)$

▷ Si $n=1$, alors $(ac,ad+bc^n)=(ac,ad+bc)$ et $(ac,bc+da^n)=(ac,bc+da)$ et nous avons $(a,b)\star(c,d)=(c,d)\star(a,b)$

La loi $\star$ est commutative pour $n=1$

▷ Si $n\geqslant2$, prenons un cas particulier :

- $(2,0)\star(3,1)=(6,2+0\times3^n)=(6,2)$
- $(3,1)\star(2,0)=(6,0+1\times2^n)=(6,2^n)$

Sauf si $n=1$, nous avons toujours $2^n\neq2$

Ainsi, si $n\geqslant2$, la loi $\star$ n'est pas commutative

3. La loi $\star$ admet un élément neutre

S'il existe un élément neutre noté (c,d), nous devons avoir, pour tout $(a,b)\in\mathbb{R}^*\times\mathbb{R}$:

$$(a,b)\star(c,d)=(a,b)$$

Ce qui se traduit par :

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

Nous obtenons donc le système :

$$\left\{\begin{array}{rcl}ac=&a\\ad+bc^n=&b\end{array}\right.\Longrightarrow c=1\text{ et }ad+b=b\Longrightarrow c=1\text{ et }d=0$$

D'où, le couple $(1,0)$ est le neutre pour $\star$

4. Existence d'un symétrique
   Soit $(a,b) \in \mathbb{R}^* \times \mathbb{R}$; si (a,b) admet un symétrique pour la loi $\star$, alors, ce symétrique $(c,d) \in \mathbb{R}^* \times \mathbb{R}$ est tel que :
   $$(a,b) \star (c,d) = (1,0)$$
   Nous avons alors :
   $$(ac = 1 \text{ et } ad + bc^n = 0) \iff \left(c = \frac{1}{a} \text{ et } d = \frac{-b}{a^{n+1}}\right)$$
   Ainsi, le symétrique de $(a,b) \in \mathbb{R}^* \times \mathbb{R}$ pour la loi $\star$ est donné par : $\left(\frac{1}{a}, \frac{-b}{a^{n+1}}\right)$

Ainsi, $(\mathbb{R}^* \times \mathbb{R}, \star)$ est un groupe *(commutatif si et seulement si $n = 1$)*

Exercice 13 :

Soit $(G,\star)$ un groupe de neutre e tel que, pour tout $x \in G$, $x \star x = e$. Démontrer que $(G,\star)$ est commutatif

Nous devons donc montrer que, pour tout $x \in G$ et tout $y \in G$, $x \star y = y \star x$
De l'égalité $x \star x = e$, on peut déduire que tout $x \in G$ est son propre inverse.
Soient donc $x \in G$ et $y \in G$; alors, $(x \star y) \star (x \star y) = e$.
Composons à droite par y ; alors :

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

Composons à gauche par x ; alors :

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

Nous avons donc $y \star x = x \star y$. $(G,\star)$ est bien commutatif

Exercice 14 :

Soit $a \in \mathbb{N}$ fixé.On considère : $H_a = \left\{q \in \mathbb{Q} \text{ tels que } q = \frac{1+am}{1+an} \text{ où } m \in \mathbb{Z} \text{ et } n \in \mathbb{Z}\right\}$ Il faut montrer que H_a est un sous-groupe de $(\mathbb{Q}^*, \times)$

1. Une première remarque si $a = 0$
   Alors, $H_0 = \{1\}$ et H_0 est un sous groupe trivial de $(\mathbb{Q}^*, \times)$
2. Supposons maintenant $a \in \mathbb{N}^*$
   (a) Dans tous les cas, $H_a \neq \emptyset$ puisque $1 = \frac{1+0\times a}{1+0\times a} \in H_a$ *(Nous avons fait $m = n = 0$, mais nous aurions pu très bien ne faire que $m = n$)*
   (b) Soit $q_1 \in H_a$ et $q_2 \in H_a$.
   Alors $q_1 = \frac{1+am_1}{1+an_1}$ où $m_1 \in \mathbb{Z}$ et $n_1 \in \mathbb{Z}$; de même, $q_2 = \frac{1+am_2}{1+an_2}$ où $m_2 \in \mathbb{Z}$ et $n_2 \in \mathbb{Z}$
   $$q_1 \times (q_2)^{-1} = \frac{1+am_1}{1+an_1} \times \frac{1+an_2}{1+am_2} = \frac{(1+am_1)(1+an_2)}{(1+an_1)(1+am_2)} = \frac{1+a(n_2+m_1+am_1n_2)}{1+a(n_1+m_2+am_2n_1)} = \frac{1+aM}{1+aN}$$
   où $M = n_2 + m_1 + am_1n_2$ et $N = n_1 + m_2 + am_2n_1$; nous avons $M \in \mathbb{Z}$ et $N \in \mathbb{Z}$ et donc $q_1 \times (q_2)^{-1} \in H_a$
   H_a est bien un sous-groupe de $(\mathbb{Q}^*, \times)$

Exercice 15 :

Soit $(G,\star)$ un groupe et $H \subset G$, un sous-groupe de $(G,\star)$. On considère, dans G, la relation $\mathcal{R}$ suivante :

$$(\forall x \in G)\,(\forall y \in G)\,\big((x\mathcal{R}y) \Longleftrightarrow \big(y^{-1}\star x \in H\big)\big)$$

1. *Montrer que $\mathcal{R}$ est une relation d'équivalence*
   - ▷ Elle est réflexive
     Soit $x \in G$. Alors, $x^{-1}\star x = e \in H$ et donc, nous avons $x\mathcal{R}x$
   - ▷ Elle est symétrique
     Soient $x \in G$ et $y \in G$ tels que $x\mathcal{R}y$; alors $y^{-1}\star x \in H$. H étant un sous groupe, l'inverse de $y^{-1}\star x$ est aussi dans H. Or,$\big(y^{-1}\star x\big)^{-1} = x^{-1}\star y$.
     Donc $x^{-1}\star y \in H$ et nous avons $y\mathcal{R}x$
   - ▷ Elle est transitive
     Soient $x \in G$, $y \in G$ et $z \in G$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $y^{-1}\star x \in H$ et $z^{-1}\star y \in H$.
     La loi $\star$ étant interne à H, nous avons donc : $\big(z^{-1}\star y\big)\star\big(y^{-1}\star x\big) \in H$. de l'associativité, nous avons :
     $$\big(z^{-1}\star y\big)\star\big(y^{-1}\star x\big) = z^{-1}\star\big(y\star y^{-1}\big)\star x = z^{-1}\star x$$
     Et donc $z^{-1}\star x \in H$ et donc $x\mathcal{R}z$

   $\mathcal{R}$ est donc bien une relation d'équivalence
2. *Montrer que les classes d'équivalence modulo $\mathcal{R}$ sont du type $x\star H$, où $x \in G$ et où :*

$$x\star H = \{g \in G \text{ tels que } g = x\star h \text{ où } h \in H\}$$

   Nous appelons $\dot{x}$ la classe de x modulo $\mathcal{R}$; il faut donc montrer que $\dot{x} = x\star H$
   - ▷ Soit $y \in \dot{x}$; alors $y\mathcal{R}x$ et donc $x^{-1}y \in H$, c'est à dire qu'il existe $h \in H$ tel que $x^{-1}y = h \Longleftrightarrow y = x\star h$; et donc $y \in x\star H$
     Nous en déduisons que $\dot{x} \subset x\star H$
   - ▷ Soit maintenant $y \in x\star H$; il existe donc $h \in H$ tel que $y = x\star h$ et donc $x^{-1}\star y = h$, c'est à dire $x^{-1}\star y \in H$; nous avons donc $y\mathcal{R}x$, c'est à dire $y \in \dot{x}$
     Nous en déduisons que $x\star H \subset \dot{x}$

   Nous avons donc $x\star H = \dot{x}$; les classes d'équivalence modulo $\mathcal{R}$ sont donc du type $x\star H$, où $x \in G$.
3. *Quelle est la classe d'équivalence de l'élément neutre e ?*

   Clairement, $H = \dot{e}$
4. *On suppose que G est un groupe d'ordre fini n (c'est à dire Card $G = n$).Montrer que l'ordre d'un sous-groupe de G divise l'ordre du groupe G*

   Soit $H \subset G$ un sous-groupe de G de cardinal p. Alors, $p \leqslant n$
   Si nous considérons $\delta_x : H \longrightarrow x\star H$ *(cf 3.1.2)*, δ_x est une bijection de H sur $x\star H$ et donc Card $x\star H$ = Card $H = p$
   D'autre part, les classes d'équivalence modulo $\mathcal{R}$ forment une partition de G et elles sont en nombre fini k. Comme toutes les classes d'équivalence ont le même nombre d'éléments, nous avons $n = k \times p$ et donc p divise n
   D'où le résultat

Exercice 16 :

Soit $(G,\star)$ un groupe non forcément commutatif de neutre e.

1. *On définit, dans G la relation $\mathcal{R}$ définie par : $(\forall x \in G)\,(\forall y \in G)\,\big((x\mathcal{R}y) \Longleftrightarrow \big(\exists a \in G \text{ tel que } y = a\star x\star a^{-1}\big)\big)$ Montrer que $\mathcal{R}$ est une relation d'équivalence.*

▷ Elle est réflexive
Soit $x \in G$. Il existe $a = e$ tel que $x = e \star x \star e$; comme e est son propre inverse, nous avons $x\mathcal{R}x$

▷ Elle est symétrique
Soient $x \in G$ et $y \in G$ tels que $x\mathcal{R}y$
Il existe donc $a \in G$ tel que $y = a \star x \star a^{-1}$
En composant à droite par a, nous avons $y \star a = \left(a \star x \star a^{-1}\right) \star a = (a \star x) \star \left(a^{-1} \star a\right) = a \star x$
En composant, maintenant, à gauche, par a^{-1}, nous avons $a^{-1} \star y \star a = a^{-1} \star (a \star x) = \left(a^{-1} \star a\right) \star x = x$
Il existe donc $u = a^{-1}$ tel que $x = u \star y \star u^{-1}$ et donc $y\mathcal{R}x$

▷ Elle est transitive
Soient $x \in G$, $y \in G$ et $z \in G$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$
Il existe donc $a \in G$ tel que $y = a \star x \star a^{-1}$ et il existe $u \in G$ tel que $z = u \star y \star u^{-1}$
Alors $z = u \star y \star u^{-1} = u \star \left(a \star x \star a^{-1}\right) \star u^{-1} = (u \star a) \star x \star \left(a^{-1} \star u^{-1}\right)$
Or, $(u \star a)^{-1} = a^{-1} \star u^{-1}$.
Ainsi, il existe $W \in G$, $W = u \star a$ tel que $z = W \star x \star W^{-1}$ et donc, nous avons $x\mathcal{R}z$
La relation est bien transitive

$\mathcal{R}$ est donc une relation d'équivalence.

2. *Soit $a \in G$ et $H \subset G$ un sous-groupe de G. Montrer que l'ensemble $a \star H \star a^{-1}$ est un sous-groupe de G*

Rappelons ce qu'est $a \star H \star a^{-1}$:

$$a \star H \star a^{-1} = \left\{g \in G \text{ tel qu'il existe } h \in H \text{ tel que } g = a \star h \star a^{-1}\right\}$$

▷ Tout d'abord $a \star H \star a^{-1}$ n'est pas vide
En effet, $e \in a \star H \star a^{-1}$ car $e = a \star e \star a^{-1}$ et comme $e \in H$, nous avons $e \in a \star H \star a^{-1}$

▷ Montrons que si $x \in a \star H \star a^{-1}$ et $y \in a \star H \star a^{-1}$, alors $x \star y^{-1} \in a \star H \star a^{-1}$
Soient donc $x \in a \star H \star a^{-1}$ et $y \in a \star H \star a^{-1}$
Alors il existe $h_1 \in H$ tel que $x = a \star h_1 \star a^{-1}$ et $h_2 \in H$ tel que $y = a \star h_2 \star a^{-1}$.
Nous avons $y^{-1} = a \star h_2^{-1} \star a^{-1}$ et donc

$$x \star y^{-1} = \left(a \star h_1 \star a^{-1}\right) \star \left(a \star h_2^{-1} \star a^{-1}\right) = (a \star h_1) \star \left(a^{-1} \star a\right) \star \left(h_2^{-1} \star a^{-1}\right) = a \star \left(h_1 \star h_2^{-1}\right) \star a^{-1}$$

Comme H est un sous-groupe, $h_1 \star h_2^{-1} \in H$, et en posant $U = h_1 \star h_2^{-1}$, nous avons $x \star y^{-1} = a \star U \star a^{-1}$ et donc $x \star y^{-1} \in a \star H \star a^{-1}$

$a \star H \star a^{-1}$ est donc un sous-groupe de G

3. *Un sous-groupe $H \subset G$ est dit distingué si, pour tout $a \in G$, $H = a \star H \star a^{-1}$*

(a) *Montrer que le centre de G,$Z(G)$ est un sous-groupe distingué de G*

Il faut donc démontrer que, pour tout $a \in G$, $Z(G) = a \star Z(G) \star a^{-1}$
Soit donc $a \in G$

— Nous avons $Z(G) \subset a \star Z(G) \star a^{-1}$
En effet, soir $z \in Z(G)$; alors $a \star z \star a^{-1} \in a \star Z(G) \star a^{-1}$. Or, comme $z \in Z(G)$, nous avons :

$$(a \star z) \star a^{-1} = (z \star a) \star a^{-1} = z \star \left(a \star a^{-1}\right) = z$$

Donc $z \in a \star Z(G) \star a^{-1}$ et donc $Z(G) \subset a \star Z(G) \star a^{-1}$

— Nous avons $a \star Z(G) \star a^{-1} \subset Z(G)$
Soit $u \in a \star Z(G) \star a^{-1}$ il existe $z \in Z(G)$ tel qie $h = a \star z \star a^{-1}$; comme $z \in Z(G)$, nous avons $h = z$ et $h \in Z(G)$

Et donc, pour tout $a \in G$, nous avons $Z(G) = a \star Z(G) \star a^{-1}$ et $Z(G)$ est un sous-groupe distingué de G

(b) *Montrer que l'intersection de 2 sous-groupes distingués est distinguée*

Soient H_1 et H_2 2 sous-groupes distingués de $(G, \star)$ et posons $X = H_1 \cap H_2$
Tout d'abord, X est un sous-groupe de $(G, \star)$ comme intersection de sous-groupes. Montrons que pour tout $a \in G$, $X = a \star X \star a^{-1}$

▷ Soit $x \in X$
- Alors $x \in H_1$ et, H_1 étant distingué, il existe $h_1 \in H_1$ tel que $x = a \star h_1 \star a^{-1}$
- De même, $x \in H_2$ et, H_2 étant distingué, il existe aussi $h_2 \in H_2$ tel que $x = a \star h_2 \star a^{-1}$

Alors, nous avons $x = a \star h_1 \star a^{-1} = a \star h_2 \star a^{-1}$ et donc, d'après les propriétés de groupe, $h_1 = h_2 = h$, ce qui veut dire que $h \in H_1 \cap H_2$ autrement dit $h \in X$ et $x \in a \star X \star a^{-1}$
En conclusion, $X \subset a \star X \star a^{-1}$

▷ Soit, maintenant, $x \in a \star X \star a^{-1}$
Alors, il existe $y \in X$ tel que $x = a \star y \star a^{-1}$
- Comme $y \in X$, alors $y \in H_1$, et H_1 étant distingué en G, $a \star y \star a^{-1} \in H_1$
- De même, comme $y \in X$, alors $y \in H_2$, et H_2 étant distingué en G, $a \star y \star a^{-1} \in H_2$

Donc $x \in H_1 \cap H_2$, c'est à dire $x \in X$ et $a \star X \star a^{-1} \subset X$

Ainsi, $X = a \star X \star a^{-1}$ et $X = H_1 \cap H_2$ est distingué en G

(c) *Démontrer que $H \subset G$ est un sous groupe distingué si et seulement si, pour tout $x \in G$, $x \star H = H \star x$*

i. Supposons que H est un sous-groupe distingué, alors pour tout $x \in G$, nous avons $x \star H \star x^{-1} = H$
Montrons que $x \star H = H \star x$
Soit $y \in x \star H$; alors, il existe $h \in H$ tel que $y = x \star h$; en composant à gauche par x^{-1}, nous avons $y \star x^{-1} = x \star h \star x^{-1}$.
Nous avons $x \star h \star x^{-1} \in x \star H \star x^{-1}$, et H étant distingué, $x \star h \star x^{-1} \in H \iff y \star x^{-1} \in H$.
Il existe donc $h_1 \in H$ tel que $y \star x^{-1} = h_1$, c'est à dire tel que $y = h_1 \star x$; et donc $y \in H \star x$.
Nous avons donc $x \star H \subset H \star x$; nous démontrerions de la même manière que $H \star x \subset x \star H$
Et donc $x \star H = H \star x$

ii. Supposons que $x \star H = H \star x$
Montrons que H est distingué, c'est à dire que $x \star H \star x^{-1} = H$
▷ Montrons que $H \subset x \star H \star x^{-1}$
Soit $y \in H$ et considérons $y \star x$
$y \star x \in H \star x$, et comme $x \star H = H \star x$, il existe $h_1 \in H$ tel que $y \star x = x \star h_1$. En composant à droite par x^{-1}, nous obtenons $y = x \star h_1 \star x^{-1}$ et donc $y \in x \star H \star x^{-1}$
Nous concluons que $H \subset x \star H \star x^{-1}$
▷ Montrons, maintenant que $x \star H \star x^{-1} \subset H$
Soit donc $y \in x \star H \star x^{-1}$
Il existe donc $h \in H$ tel que $y = x \star h \star x^{-1}$, c'est à dire, en composant à droite par x, que nous avons $y \star x = x \star h$ et donc $y \star x \in x \star H$
Comme $x \star H = H \star x$, il existe $h_1 \in H$ tel que $y \star x = h_1 \star x$; en composant une nouvelle fois à droite par x^{-1}, nous obtenons $y = h_1$ et donc $y \in H$
Et donc $x \star H \star x^{-1} \subset H$

En conclusion, $x \star H \star x^{-1} = H$ et H est distingué.

Exercice 17 :

Soit $(G, \star)$ un groupe de neutre e, H_1 et H_2, 2 sous-groupes de $(G, \star)$. On dit que H_1 et H_2 sont somme directe de G si et seulement si $H_1 \cap H_2 = \{e\}$ et, pour tout $x \in G$, il existe $x_1 \in H_1$ et $x_2 \in H_2$ tels que $x = x_1 \star x_2$ Démontrer que, dans ce cas, la décomposition $x = x_1 \star x_2$ est unique

Soient donc H_1 et H_2 deux sous-groupes de G qui sont somme directe de G
Soit $x \in G$ et supposons qu'il y ait 2 décompositions de x, c'est à dire :

$$x = x_1 \star x_2 = y_1 \star y_2 \text{ où } x_1 \in H_1 \ , \ x_2 \in H_2 \text{ et } y_1 \in H_1 \ , \ y_2 \in H_2$$

Alors, en composant à droite par l'inverse de x_2, nous avons :

$$x_1 \star x_2 = y_1 \star y_2 \iff x_1 \star x_2 \star (x_2)^{-1} = y_1 \star y_2 \star (x_2)^{-1} \iff x_1 = y_1 \star y_2 \star (x_2)^{-1}$$

Composons maintenant à gauche par l'inverse de y_1 ; nous avons :

$$x_1 = y_1 \star y_2 \star (x_2)^{-1} \iff (y_1)^{-1} \star x_1 = (y_1)^{-1} \star y_1 \star y_2 \star (x_2)^{-1} \iff (y_1)^{-1} \star x_1 = y_2 \star (x_2)^{-1}$$

Appelons $z=(y_1)^{-1}\star x_1=y_2\star(x_2)^{-1}$
H_1 étant un sous-groupe, nous avons $(y_1)^{-1}\star x_1\in H_1$; de même, H_2 étant un sous-groupe, nous avons $y_2\star(x_2)^{-1}\in H_2$, c'est à dire $z\in H_1$ et $z\in H_2$; en d'autres termes : $z\in H_1\cap H_2$.
Comme $H_1\cap H_2=\{e\}$, $z=e$ et donc :

$$(y_1)^{-1}\star x_1=e\Longleftrightarrow y_1=x_1 \text{ et } y_2\star(x_2)^{-1}=e\Longleftrightarrow y_2=x_2$$

Il y a donc unicité de la décomposition

Exercice 18 :

Soit $(G,\star)$ un groupe de neutre e et on considère l'application Φ définie par :

$$\left\{\begin{array}{ccc}(G,\star)&\longrightarrow&(G,\star)\\ x&\longmapsto&\Phi(x)=x^{-1}\end{array}\right.$$

Montrer que si Φ est un homomorphisme de groupe, alors $(G,\star)$ est un groupe commutatif

Nous supposons donc que Φ est un homomorphisme de groupe *(c'est même un endomorphisme)*
Il faut donc montrer que, pour tout $x\in G$ et tout $y\in G$, $x\star y=y\star x$
Comme Φ est un homomorphisme, nous avons $\Phi\left(x^{-1}\star y^{-1}\right)=\Phi\left(x^{-1}\right)\star\Phi\left(y^{-1}\right)=x\star y$
Comme $x^{-1}\star y^{-1}=(y\star x)^{-1}$, nous avons :

$$\Phi\left(x^{-1}\star y^{-1}\right)=\Phi\left((y\star x)^{-1}\right)=y\star x$$

Et nous avons donc $x\star y=y\star x$ et $(G,\star)$ est bien un groupe commutatif

Exercice 19 :

1. *Soient $(G,\star)$ et $(G_1,\top)$ 2 groupes et $f:(G,\star)\longrightarrow(G_1,\top)$ un homomorphisme de groupe. Démontrer que $\ker f$ est un sous-groupe distingué de G*

   Il faut donc montrer que, pour tout $x\in G$, $\ker f=x\star\ker f\star x^{-1}$
   ▷ Soit $z\in\ker f$; alors, $f(z)=e$ et $x^{-1}\star z\star x\in\ker f$. En effet :

   $$f\left(x^{-1}\star z\star x\right)=f\left(x^{-1}\right)\star f(z)\star f(x)=(f(x))^{-1}\star e\star f(x)=e$$

   Il existe donc $k\in\ker f$ tel que $x^{-1}\star z\star x=k$, et donc $z=x\star k\star x^{-1}$ et donc $z\in x\star\ker f\star x^{-1}$
   Vous avons donc $\ker f\subset x\star\ker f\star x^{-1}$
   ▷ Réciproquement soit $z\in x\star\ker f\star x^{-1}$
   Il existe donc $k\in\ker f$ tel que $z=x\star k\star x^{-1}$; on démontre facilement que $f(z)=e$ et donc que $z\in\ker f$
   Nous avons donc $x\star\ker f\star x^{-1}\subset\ker f$
   Et donc pour tout $x\in G$, $\ker f=x\star\ker f\star x^{-1}$
2. *On définit, dans $(G,\star)$ une relation $\mathcal{R}$ définie par :*

   $$(\forall x\in G)(\forall y\in G)((x\mathcal{R}y)\Longleftrightarrow(f(x)=f(y)))$$

   Donner une autre définition de la condition $f(x)=f(y)$
   ▷ Il est parfaitement évident que $\mathcal{R}$ est une relation d'équivalence
   ▷ La relation $f(x)=f(y)$ peut effectivement *être définie autrement* :

   $$f(x)=f(y)\Longleftrightarrow f(x)\star(f(y))^{-1}=e_1\Longleftrightarrow f\left(x\star y^{-1}\right)=e_1\Longleftrightarrow x\star y^{-1}\in\ker f$$

   Effectivement, nous avons $\left((x\mathcal{R}y)\Longleftrightarrow\left(x\star y^{-1}\in\ker f\right)\right)$

Exercice 20 :

Soit $(G,\star)$ un groupe non commutatif et $Z(G)$ le centre de G. On appelle $\mathrm{Int}(G)$ l'ensemble des automorphismes intérieurs de G :

$$\mathrm{Int}(G)=\left\{f_a \text{ où } a\in G \text{ et } \left[\begin{array}{ccc} f_a : G & \longrightarrow & G \\ x & \longmapsto & f_a(x)=a\star x\star a^{-1}\end{array}\right.\right\}$$

1. *Pour commencer, un automorphisme intérieur est un automorphisme de groupe*
   - ▷ Pour tout $a\in G$, f_a est un homomorphisme de groupe
     En effet, soient $x\in G$, $y\in G$ et un automorphisme intérieur f_a. Alors :
     $$\begin{array}{rcl} f_a(x\star y) & = & a\star(x\star y)\star a^{-1} \\ & = & (a\star x)\star\left(y\star a^{-1}\right) \\ & = & (a\star x)\star e\star\left(y\star a^{-1}\right) \\ & = & (a\star x)\star\left(a^{-1}\star a\right)\star(y\star) \\ & = & \left(a\star x\star a^{-1}\right)\star(a\star y\star) \\ & = & f_a(x)\star f_a(y)\end{array}$$
   - ▷ Pour tout $a\in G$, f_a est injective
     Soit $z\in\ker f_a$; alors, $f_a(z)=e$, c'est à dire $a\star z\star a^{-1}=e$
     En composant à droite par a, nous obtenons : $a\star z\star a^{-1}=e\Longleftrightarrow a\star z=a$
     Puis, en composant à gauche par a^{-1}, nous obtenons $a\star z=a\Longleftrightarrow z=e$
     Donc, $\ker f_a=\{e\}$ et f_a est injective.
   - ▷ Pour tout $a\in G$, f_a est surjective
     Soit $y\in G$; existe-t-il $x\in G$ tel que $f_a(x)=y$?
     S'il existe, x vérifie l'équation $a\star x\star a^{-1}=y$, et on trouve, facilement, $x=a^{-1}\star y\star a$
     f_a est donc surjective

   f_a est donc bien un automorphisme de groupe ; c'est donc une bijection et $f_a^{-1}=f_{a^{-1}}$
2. *Montrer que $(\mathrm{Int}(G),\circ)$, où $\circ$ est la composition des applications, est un groupe*
   - ▷ Pour commencer, on peut dire que $\mathrm{Int}(G)\neq\emptyset$ puisque $\mathrm{Id}_G\in\mathrm{Int}(G)$ puisque $\mathrm{Id}_G=f_e$ où e est le neutre de G
   - ▷ Ensuite la composition des applications étant associative, elle le sera, en particulier pour les automorphismes intérieurs
   - ▷ Le plus intéressant c'est la question de la composition interne.
     Soit donc $x\in G$, $a\in G$ et $b\in G$:
     $$\begin{array}{rcl} f_a\circ f_b(x) & = & f_a\left[f_b(x)\right] \\ & = & f_a\left[b\star x\star b^{-1}\right] \\ & = & a\star\left(b\star x\star b^{-1}\right)\star a^{-1} \\ & = & (a\star b)\star x\star\left(b^{-1}\star a^{-1}\right) \\ & = & (a\star b)\star x\star(a\star b)^{-1} \\ & = & f_{a\star b}(x)\end{array}$$
     Nous avons donc $f_a\circ f_b=f_{a\star b}$ et la loi $\circ$ est bien de composition interne
   - ▷ Le neutre pour $\circ$ est bien $\mathrm{Id}_G=f_e$ et l'inverse de f_a, pour ${}_circ$ est $f_{a^{-1}}$ qui est bien un élément de $\mathrm{Int}(G)$

   $(\mathrm{Int}(G),\circ)$, est bien un groupe pour la composition des applications.
3. *On considère l'application φ définie par :*
   $$\left\{\begin{array}{ccc} \varphi : G & \longrightarrow & \mathrm{Int}(G) \\ a & \longmapsto & \varphi(a)=f_a\end{array}\right.$$
   Montrer que φ est un homomorphisme de groupe.

   On utilise les questions précédentes :
   $$\varphi(a\star b)=f_{a\star b}=f_a\circ f_b=\varphi(a)\circ\varphi(b)$$
   φ est bien un homomorphisme de groupes

4. *Donner* $\ker\varphi$. *Quand donc* φ *est un isomorphisme ?*
   - ▷ Nous avons $\ker\varphi = \{x \in G \text{ tels que } f_x = \mathrm{Id}_G\}$
     Donc, si $x \in \ker\varphi$, pour tout $z \in G$, $f_x(z) = z \Longleftrightarrow x \star z \star x^{-1} = z$
     Nous avons donc, pour tout $z \in G$, $x \star z = z \star x$, ce qui veut dire que x commute avec tous les éléments de G et donc $x \in Z(G)$ et donc $\ker f \subset Z(G)$
     Réciproquement,
     Si $x \in Z(G)$, alors, pour tout $z \in G$:
     $$f_x(z) = x \star z \star x^{-1} = x \star \left(x^{-1} \star z\right) = \left(x \star x^{-1}\right) \star z = z$$
     Et donc $f_x = \mathrm{Id}_G$ et $x \in \ker\varphi$ d'où $Z(G) \subset \ker\varphi$
     Nous en concluons donc que $\ker f = Z(G)$
   - ▷ φ est un isomorphisme si $\ker\varphi = \{e\}$, c'est à dire que le centre de G, $Z(G)$ est réduit au seul élément neutre

Exercice 21 :

Démontrer qu'un sous groupe $H \subset G$ *d'un groupe* $(G, \star)$ *est distingué si et seulement si il est stable par tous les automorphismes intérieurs de* G

1. Supposons que $H \subset G$ est un sous-groupe distingué
   Ce veut donc dire que, pour tout $a \in G$, $a \star H \star a^{-1} = H$ ou, ce qui est équivalent, $a \star H = H \star a$.
   Démontrons que, pour tout $a \in G$, $f_a(H) \subset H$; nous aurons ainsi montré que H est stable par tous les automorphismes intérieurs de G
   Soit $y \in f_a(H)$; il existe donc $h \in H$ tel que $y = f_a(h) = a \star h \star a^{-1}$
   H étant distingué, $a \star h \star a^{-1} \in H$ et donc $y \in H$. D'où $f_a(H) \subset H$
2. Supposons que H est stable par tous les automorphismes intérieurs de G
   Montrons que H est un sous-groupe distingué.
   - ▷ Soit $y \in H$ et $a \in G$. Alors, $f_{a^{-1}}(y) \in H$, c'est à dire $a^{-1} \star y \star a \in H$
     Il existe donc $h \in H$ tel que $a^{-1} \star y \star a = h \Longleftrightarrow y = a \star h \star a^{-1}$ et $y \in a \star H \star a^{-1}$ et donc, $H \subset a \star H \star a^{-1}$
   - ▷ Soit $y \in a \star H \star a^{-1}$; il faut montrer que $y \in H$
     Il existe $h \in H$ tel que $y = a \star h \star a^{-1} = f_a(h)$. Comme $f_a(h) \in H$, nous avons alors $a \star H \star a^{-1} \subset H$

   Donc $a \star H \star a^{-1} = H$ et H est distingué en G

Exercice 22 :

Soit $n \in \mathbb{N}^*$ *et* $\omega = e^{\frac{2i\pi}{n}}$ *et* φ, *une application définie par :*

$$\begin{cases} \varphi : (\mathbb{Z}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ k & \longmapsto & \varphi(k) = \omega^k \end{cases}$$

1. *Montrer que* φ *est un homomorphisme de groupe*

   C'est très facile ; il suffit d'utiliser les propriétés des puissances dans l'ensemble $\mathbb{C}$ des nombres complexes :
   $$\varphi(k + k_1) = \omega^{k+k_1} = \omega^k \times \omega^{k_1} = \varphi(k) \times \varphi(k_1)$$
   φ est donc bien un homomorphisme de groupe
2. *Rechercher* $\ker\varphi$ *et* $\mathrm{Im}\varphi$
   - ▷ $\ker\varphi = \{k \in \mathbb{Z} \text{ tels que } \varphi(k) = 1\} = \left\{k \in \mathbb{Z} \text{ tels que } e^{\frac{2ik\pi}{n}} = 1\right\}$
     Nous avons alors $e^{\frac{2ik\pi}{n}} = e^{2ip\pi}$ avec $p \in \mathbb{Z}$ et donc $\dfrac{2ik\pi}{n} = 2ip\pi \Longleftrightarrow k = pn$
     Donc k est un multiple de n et $\ker\varphi = n\mathbb{Z}$
   - ▷ Pour trouver $\mathrm{Im}\varphi$, il suffit de voir qui si $z \in \mathrm{Im}\varphi$, alors $|z| = 1$ et donc $\mathrm{Im}\varphi \subset \mathcal{U}$ où $\mathcal{U}$ est le cercle unité : $\mathcal{U} = \{z \in \mathbb{C} \text{ tels que } |z| = 1\}$
     $\mathrm{Im}\varphi$ est, en fait $\mathcal{U}_n$ ensemble des racines n-*ièmes* de 1

3.5.2 Structure d'anneaux et de corps

Exercice 7 :

$\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$ est l'anneau commutatif et unitaire des fonctions numériques d'une variable réelle à valeurs dans $\mathbb{R}$. Pour $x_0\in\mathbb{R}$, on appelle $A\left(x_0\right)=\left\{f\in\mathbb{R}^{\mathbb{R}}\text{ telles que }f\left(x_0\right)=0\right\}$. Il faut montrer que $\left(A\left(x_0\right),+,\times\right)$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$

1. Tout d'abord, $A\left(x_0\right)\neq\emptyset$ puisque la fonction nulle sur $\mathbb{R}$ en entier $\mathcal{O}$ est telle que $\mathcal{O}\left(x_0\right)=0$, et $\mathcal{O}$ est bien un élément de $A\left(x_0\right)$
2. D'autre part, soient $f\in A\left(x_0\right)$ et $g\in A\left(x_0\right)$. Alors :

$$\left(f-g\right)\left(x_0\right)=f\left(x_0\right)-g\left(x_0\right)=0-0=0$$

Donc, $f-g\in A\left(x_0\right)$ et :

$$\left(f\times g\right)\left(x_0\right)=f\left(x_0\right)\times g\left(x_0\right)=0\times 0=0$$

Donc, $f\times g\in A\left(x_0\right)$

D'après le théorème 3.2.5, $\left(A\left(x_0\right),+,\times\right)$ est un sous-anneau de $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$

Exercice 8 :

On appelle $\mathbb{Q}\left(\sqrt{2}\right)=\left\{x+y\sqrt{2}\text{ avec }x\in\mathbb{Q}\text{ et }y\in\mathbb{Q}\right\}$. Montrer que $\left(\mathbb{Q}\left(\sqrt{2}\right),+,\times\right)$ est un corps

Ce type d'ensemble *(ou de corps)* est très intéressant. On peut remarquer que $\mathbb{Q}\subset\mathbb{Q}\left(\sqrt{2}\right)\subset\mathbb{R}$

1. Tout d'abord, $z=x+y\sqrt{2}$ avec $x\in\mathbb{Q}$ et $y\in\mathbb{Q}$ est tel que $z=0$ si et seulement si $x=0$ et $y=0$
   - ▷ Si $x=y=0$, alors $z=x+y\sqrt{2}=0$
   - ▷ Réciproquement, supposons $z=x+y\sqrt{2}=0$ et $x\neq 0$; alors $y\sqrt{2}=-x$ donc $y\neq 0$ et $\sqrt{2}=\dfrac{-x}{y}$. Or, $\dfrac{-x}{y}\in\mathbb{Q}$ et $\sqrt{2}\notin\mathbb{Q}$, ce qui est impossible. Donc $x=y=0$
2. Ce qui permet d'écrire que $x+y\sqrt{2}=x_1+y_1\sqrt{2}$ si et seulement si $x=x_1$ et $y=y_1$.
3. Montrons que $\left(\mathbb{Q}\left(\sqrt{2}\right),+,\times\right)$ est un sous anneau de $(\mathbb{R},+,\times)$
   - ▷ Tout d'abord, $\mathbb{Q}\left(\sqrt{2}\right)\neq\emptyset$ puisque $0=0+0\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right)$
   - ▷ Soient $z_1\in\mathbb{Q}\left(\sqrt{2}\right)$ et $z_2\in\mathbb{Q}\left(\sqrt{2}\right)$. Alors, $z=x+y\sqrt{2}$ et $z_1=x_1+y_1\sqrt{2}$

$$z-z_1=x+y\sqrt{2}-\left(x_1+y_1\sqrt{2}\right)=\left(x-x_1\right)+\left(y-y_1\right)\sqrt{2}$$

   Comme $x\in\mathbb{Q}$ et $x_1\in\mathbb{Q}$, nous avons $x-x_1\in\mathbb{Q}$; de même $y-y_1\in\mathbb{Q}$, et nous en déduisons que $z-z_1\in\mathbb{Q}$
   - ▷ De même, pour $z_1\in\mathbb{Q}\left(\sqrt{2}\right)$ et $z_2\in\mathbb{Q}\left(\sqrt{2}\right)$, nous avons :

$$z_1\times z_2=\left(x+y\sqrt{2}\right)\times\left(x_1+y_1\sqrt{2}\right)=xx_1+xy_1\sqrt{2}+yx_1\sqrt{2}+2yy_1=\left(xx_1+2yy_1\right)+\left(xy_1+yx_1\right)\sqrt{2}$$

   Or, comme $(x,x_1,y,y_1)\in\mathbb{Q}^4$, nous avons $xx_1+2yy_1\in\mathbb{Q}$ et $xy_1+yx_1\in\mathbb{Q}$ et donc $zz_1\in\mathbb{Q}\left(\sqrt{2}\right)$

   $\left(\mathbb{Q}\left(\sqrt{2}\right),+,\times\right)$ est donc un sous anneau de $(\mathbb{R},+,\times)$
4. Montrons que $\left(\mathbb{Q}\left(\sqrt{2}\right)^*,\times\right)$ est un groupe
   - ▷ Tout d'abord, $\mathbb{Q}\left(\sqrt{2}\right)^*\neq\emptyset$ puisque $1=1+0\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right)^*$; le neutre pour la multiplication est donc un élément de $\mathbb{Q}\left(\sqrt{2}\right)^*$
   - ▷ On a montré que la multiplication était interne dans $\mathbb{Q}\left(\sqrt{2}\right)^*$

▷ Montrons que si $z \in \mathbb{Q}\left(\sqrt{2}\right)$, alors $z^{-1} \in \mathbb{Q}\left(\sqrt{2}\right)$

Soit $z = x + y\sqrt{2}$ avec $x \neq 0$ et $y \neq 0$. Alors, $z^{-1} = \dfrac{1}{x+y\sqrt{2}} = \dfrac{x-y\sqrt{2}}{x^2-2y^2} = \dfrac{x}{x^2-2y^2} + \dfrac{-y}{x^2-2y^2}\sqrt{2}$

Comme $x \in \mathbb{Q}$ et $y \in \mathbb{Q}$, nous avons $\dfrac{x}{x^2-2y^2} \in \mathbb{Q}$ et $\dfrac{-y}{x^2-2y^2} \in \mathbb{Q}$ et donc $z^{-1} \in \mathbb{Q}\left(\sqrt{2}\right)$

$\left(\mathbb{Q}\left(\sqrt{2}\right), +, \times\right)$ est donc un sous-corps de $(\mathbb{R}, +, \times)$, donc un corps.

Correction des exercices complémentaires sur les anneaux et les corps

Exercice 23 :

Soit $r = \sqrt[3]{2}$ et $K = \left\{x \in \mathbb{R} \text{ tel que } x = a + br + cr^2 \text{ avec } (a,b,c) \in \mathbb{Z}^3\right\}$. Montrer que $(K, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$

1. Nous allons donc, d'abord, montrer que K est non vide. Il suffit de voir que $0 \in K$ puisque $0 = 0 + 0r + 0r^2$. De même, $1 \in K$ puisque $1 = 1 + 0r + 0r^2$
2. Soient $x = a + br + cr^2$ et $x_1 = a_1 + b_1 r + c_1 r^2$ 2 éléments de K. Alors :
   - $x - x_1 = \left(a + br + cr^2\right) - \left(a_1 + b_1 r + c_1 r^2\right) = (a - a_1) + (b - b_1)\, r + (c - c_1)\, r^2$. Comme $a \in \mathbb{Z}$ et $a_1 \in \mathbb{Z}$, nous avons $a - a_1 \in \mathbb{Z}$; de même $b - b_1 \in \mathbb{Z}$ et $c - c_1 \in \mathbb{Z}$ et donc $x - x_1 \in K$
   - En passant au produit, nous avons :

     $xx_1 = \left(a + br + cr^2\right)\left(a_1 + b_1 r + c_1 r^2\right) = aa_1 + ab_1 r + ac_1 r^2 + ba_1 r + bb_1 r^2 + bc_1 r^3 + a_1 cr^2 + cb_1 r^3 + cc_1 r^4$

     Or, $r^3 = 2$ et $r^4 = 2r$; donc :

     $$\begin{aligned} xx_1 &= aa_1 + (ab_1 + ba_1)\, r + (ac_1 + bb_1 + a_1 c)\, r^2 + 2\,(bc_1 + b_1 c) + 2cc_1 r \\ &= (aa_1 + 2\,(bc_1 + b_1 c)) + (ab_1 + ba_1 + 2cc_1)\, r + (ac_1 + bb_1 + a_1 c)\, r^2 \end{aligned}$$

     Or, $(aa_1 + 2\,(bc_1 + b_1 c)) \in \mathbb{Z}$, $(ab_1 + ba_1 + 2cc_1) \in \mathbb{Z}$ et $(ac_1 + bb_1 + a_1 c) \in \mathbb{Z}$
     Donc, $xx_1 \in K$

Donc, $(K, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$; c'est même un anneau unitaire puisque $1 \in K$

Exercice 24 :

On considère $(\mathbb{Z} \times \mathbb{Z}, \oplus, \otimes)$ où l'addition $\oplus$ est une addition définie par : $(a,b) \oplus (c,d) = (a+c, b+d)$, et la multiplication $\otimes$ par : $(a,b) \otimes (c,d) = (ac, bd)$
Montrer que $(\mathbb{Z} \times \mathbb{Z}, \oplus, \otimes)$ est un anneau commutatif unitaire. Est-il intègre ?

1. Tout d'abord, et très clairement, $(\mathbb{Z} \times \mathbb{Z}, \oplus,)$ est un groupe commutatif.
   - On démontre facilement que la loi $\oplus$ est associative et commutative
   - Le neutre pour $\oplus$ est $(0,0)$
   - Chaque élément $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ admet $(-a,-b)$ comme symétrique pour $\oplus$.
2. Clairement, la loi $\otimes$ est associative et commutative
3. $\otimes$ admet comme neutre le couple $(1,1)$
4. Si $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ admet un inverse $(a',b') \in \mathbb{Z} \times \mathbb{Z}$ pour la loi $\otimes$, alors, nous avons :

   $$aa' = 1 \text{ et } bb' = 1$$

   Les seuls éléments inversibles pour $\otimes$ sont $(1,1)$ et $(-1,-1)$; ils sont même leur propre inverse.
5. Il faut maintenant montrter que $\otimes$ est distributive par rapport à $\oplus$
   Soient $(a,b) \in \mathbb{Z} \times \mathbb{Z}$, $(c,d) \in \mathbb{Z} \times \mathbb{Z}$ et $(e,f) \in \mathbb{Z} \times \mathbb{Z}$. Alors !

   $$\begin{aligned} (a,b) \otimes [(c,d) \oplus (e,f)] &= (a,b) \otimes [(c+e, d+f)] \\ &= (a\,(c+e)\,, b\,(d+f)) \\ &= (ac + ae, bd + bf) \\ &= (ac, bd) \oplus (ae, bf) \\ &= (a,b) \otimes (c,d) \oplus (a,b) \otimes (ae, bf) \end{aligned}$$

Ce que nous voulions

$(\mathbb{Z}\times\mathbb{Z},\oplus,\otimes)$ est donc un anneau commutatif unitaire.
Ce n'est, par contre, pas un anneau intègre : nous avons $(2,0)\neq(0,0)$ et $(0,8)\neq(0,0)$, mais

$$(2,0)\otimes(0,8)=(0,0)$$

Exercice 25 :

Soit $(A,+,\times)$ un anneau, non forcément commutatif, non forcément unitaire. Soit :

$$\mathcal{C}=\{c\in A \text{ tels que } (\forall x\in A)\,(x\times c=c\times x)\}$$

Il faut montrer que $\mathcal{C}$ est un sous-anneau de $(A,+,\times)$

1. Premièrement, $\mathcal{C}\neq\emptyset$ puisque $0\in\mathcal{C}$; en effet : pour tout $x\in A$, $0\times x=x\times 0=0$
2. Soit $c_1\in\mathcal{C}$ et $c_2\in\mathcal{C}$; il faut montrer que $c_1-c_2\in\mathcal{C}$
   Soit donc $x\in A$
   $$x\times(c_1-c_2)=xc_1-xc_2=c_1x-c_2x=(c_1-c_2)\,x$$
   Donc c_1-c_2 commute avec tout $x\in A$ et donc $c_1-c_2\in\mathcal{C}$
3. Montrons maintenant que $c_1\times c_2\in\mathcal{C}$. Soit donc $x\in A$
   $$x\,(c_1c_2)=(xc_1)\,c_2=(c_1x)\,c_2=c_1\,(xc_2)=c_1\,(c_2x)=(c_1c_2)\,x$$
   Et donc $c_1\times c_2\in\mathcal{C}$

Ainsi, $\mathcal{C}$ est un sous-anneau de $(A,+,\times)$

Exercice 26 :

Soit $(A,+,\times)$ un anneau tel que, pour tout $x\in A$, $x^2=x$

1. *Démontrer que, pour tout $x\in A$, $2x=x+x=0$*
   Par hypothèse, nous avons : $(x+x)^2=x+x$, et donc $x^2+x+x+x^2=x+x\iff x+x+x+x=x+x$, et donc $x+x=2x=0$. Ceci sous entend que x est son propre symétrique pour l'addition *(c'est à dire : $x=-x$)* et que l'anneau est de caractéristique 2
2. *Démontrer que $(A,+,\times)$ est un anneau commutatif*
   Il faut montrer que, pour tout $x\in A$ et tout $y\in A$, nous avons $xy=yx$
   Par hypothèse : $(x+y)^2=x+y$. Or :
   $$(x+y)^2=x+y\iff(x+y)\,(x+y)=x^2+xy+yx+y^2=x+y\iff x+xy+yx+y=x+y\iff xy+yx=0$$
   Donc, yx est l'opposé de xy pour l'addition, c'est à dire $yx=-xy=xy$.
   L'anneau est donc commutatif
3. *Démontrer que, pour tout $x\in A$ et tout $y\in A$, $xy\,(x+y)=0$*
   Il suffit de développer, d'utiliser l'hypothèse et la commutativité de la multiplication :
   $$xy\,(x+y)=xyx+xy^2=yxx+xy=yx+xy=0$$

Exercice 27 :

1. *Soit $(A,+,\times)$ un anneau commutatif. Soit $x\in A$ tel qu'il existe $n\in\mathbb{N}$ tel que $x^n=0$. Montrer que si x et y sont nilpotents, alors xy et $x+y$ sont nilpotents*
2. *On suppose que $(A,+,\times)$ est un anneau commutatif et unitaire. Soit $x\in A$ tel qu'il existe $n\in\mathbb{N}$ tel que $x^n=0$. Montrer que $1-x$ est inversible*

3. Soit $(A,+,\times)$ un anneau non forcément commutatif. Soient $u\in A$ et $v\in A$ tels que uv soit nilpotent, c'est à dire qu'il existe $n\in\mathbb{N}$ tel que $(uv)^n=0$. Il faut montrer que vu est nilpotent

1. Soit $(A,+,\times)$ un anneau commutatif.
   (a) On montre que si x et y sont nilpotents, alors xy est nilpotent
   Soient $x\in A$ et $y\in A$ tels que que $x^n=0$ et $y^m=0$
   ▷ **Une première méthode** consiste à calculer $(xy)^{mn}$; en effet, nous avons :
   $$(xy)^{mn}=x^{mn}\times y^{mn}=(x^n)^m\times(y^m)^n=0\times 0=0$$
   ▷ **Une seconde méthode**, puisque l'anneau A est commutatif, consiste à juste calculer $(xy)^n$. En effet :
   $$(xy)^n=x^n\times y^n=0\times(y^n)=0\times y^n=0$$
   En fait, lorsque l'anneau est commutatif, il suffit que l'un des éléments x ou y soit nilpotent pour que le produit xy soit nilpotent
   (b) On montre que si x et y sont nilpotents, alors $x+y$ est nilpotent
   Soient $x\in A$ et $y\in A$ tels que que $x^n=0$ et $y^m=0$ Il suffit de calculer $(x+y)^{m+n}$; du fait de la commutativité de A, nous pouvons utiliser le binôme de Newton :
   $$(x+y)^{m+n}=\sum_{k=0}^{m+n}\binom{m+n}{k}x^k y^{m+n-k}$$
   ▷ Pour $k\geqslant n$, $k=n+r$ où $r\geqslant 0$ et donc $x^k=x^{n+r}=x^n\times x^r=0$ de telle sorte que
   $$(x+y)^{m+n}=\sum_{k=0}^{n-1}\binom{m+n}{k}x^k y^{m+n-k}$$
   ▷ Si $k\leqslant n-1$, alors $n-k\geqslant +1$ et $y^{m+n-k}=y^m\times y^{n-k}=0$ et donc
   $$(x+y)^{m+n}=\sum_{k=0}^{n-1}\binom{m+n}{k}x^k y^{m+n-k}=0$$
   Ainsi, $x+y$ est nilpotent
2. Cette fois $(A,+,\times)$ est un anneau commutatif et unitaire.
   Soit $x\in A$ nilpotent. Montrer que $1-x$ est inversible
   Soit $x\in A$ tel qu'il existe $n\in\mathbb{N}$ tel que $x^n=0$. Nous avons $1-x^n=1$. Or :
   $$1=1-x^n=(1-x)\left(1+x+x^2+x^3+\cdots+x^{n-1}\right)$$
   Ainsi, $1+x+x^2+x^3+\cdots+x^{n-1}$ apparaît bien comme l'inverse de $1-x$
3. Soit $(A,+,\times)$ un anneau non forcément commutatif. Soient $u\in A$ et $v\in A$ tels que uv soit nilpotent.
   Il faut montrer que vu est nilpotent
   Calculons $(vu)^{n+1}$:
   $$(vu)^{n+1}=\underbrace{(vu)(vu)(vu)\cdots(vu)(vu)}_{n+1\text{ fois}}=v\underbrace{(uv)(uv)\cdots(uv)}_{n\text{ fois}}v=v(uv)^n u=0$$

Exercice 28 :

Soit $(A,+,\times)$ un anneau unitaire d'unité 1 et $\mathcal{U}$ l'ensemble des éléments inversibles de A. Il faut montrer que $\mathcal{U},\times$ est un groupe.

1. Tout d'abord, $(A,+,\times)$ étant un anneau, la loi $\times$ est associative dans $\mathcal{U}$
2. Ensuite, $\mathcal{U}\neq\emptyset$ parce que $1\in\mathcal{U}$
3. D'autre part, si $x\in\mathcal{U}$, x admet un symétrique pour $\times$, qui est x^{-1}, et donc $x^{-1}\in\mathcal{U}$
4. Il faut, maintenant, montrer que la loi $\times$ est interne dans $\mathcal{U}$.
   Soient $x\in\mathcal{U}$ et $y\in\mathcal{U}$. Alors :
   $$(x\times y)\times\left(y^{-1}\times x^{-1}\right)=x\times\left(y\times y^{-1}\right)\times x^{-1}=x\times 1\times x^{-1}=x\times x^{-1}=1$$
   L'inverse de $x\times y$ est donc $y^{-1}\times x^{-1}$

Exercice 29 :

On considère $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \text{ avec } a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\right\}$

1. *Montrer que* $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ *est un anneau*

   Nous allons montrer que $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un sous-anneau de $(\mathbb{R}, +, \times)$
   - ▷ Tout d'abord, $\mathbb{Z}\left[\sqrt{2}\right] \neq \emptyset$ puisque $1 = 1 + 0\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$, tout comme $0 \in \mathbb{Z}\left[\sqrt{2}\right]$
   - ▷ Ensuite, soient $x \in \mathbb{Z}\left[\sqrt{2}\right]$ et $y \in \mathbb{Z}\left[\sqrt{2}\right]$. Alors :
     - ◇ $x = a + b\sqrt{2}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$
     - ◇ Et $y = a' + b'\sqrt{2}$ avec $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$

     Donc $x - y = \left(a + b\sqrt{2}\right) - \left(a' + b'\sqrt{2}\right) = (a - a') + (b - b')\sqrt{2}$. Comme $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$, nous avons $x - y \in \mathbb{Z}\left[\sqrt{2}\right]$
   - ▷ D'autre part, $xy = \left(a + b\sqrt{2}\right)\left(a' + b'\sqrt{2}\right) = (aa' + 2bb') + (ba' + ab')\sqrt{2}$. Comme $aa' + 2bb' \in \mathbb{Z}$ et $ba' + ab' \in \mathbb{Z}$, nous avons $xy \in \mathbb{Z}\left[\sqrt{2}\right]$

   Ainsi, $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un anneau

2. *Pour* $x = a + b\sqrt{2}$, *on note* $C(x) = a - b\sqrt{2}$ *; montrer que, pour tout* x *et tout* y *de* $\mathbb{Z}\left[\sqrt{2}\right]$, *on a* $C(xy) = C(x)\,C(y)$

   Cette question se démontre en faisant les calculs

3. *Pour* $x \in \mathbb{Z}\left[\sqrt{2}\right]$, *on note* $N(x) = xC(x) = a^2 - 2b^2$. *Montrer que, pour tout* x *et tout* y *de* $\mathbb{Z}\left[\sqrt{2}\right]$, *on a* $N(xy) = N(x)\,N(y)$

   Il suffit de faire le calcul :

   $$N(xy) = xyC(xy) = xyC(x)\,C(y) = xC(x)\,yC(y) = N(x)\,N(y)$$

4. *En déduire que les éléments inversibles de* $\mathbb{Z}\left[\sqrt{2}\right]$ *sont ceux qui s'écrivent* $a + b\sqrt{2}$ *avec* $a^2 - 2b^2 = \pm 1$.

   - ▷ Soit $x \in \mathbb{Z}\left[\sqrt{2}\right]$, inversible et d'inverse x^{-1} ; alors $xx^{-1} = 1$ et $N\left(xx^{-1}\right) = N(1) = 1$.

     Comme $N\left(xx^{-1}\right) = N(x)\,N\left(x^{-1}\right)$, nous avons $N\left(x^{-1}\right) = \dfrac{1}{N(x)}$, ce qui sous entend que l'entier relatif $N(x)$ doit être inversible dans $\mathbb{Z}$. Or, les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1.
     Donc, pour que $x \in \mathbb{Z}\left[\sqrt{2}\right]$ soit inversible, il faut que $a^2 - 2b^2 = \pm 1$
   - ▷ Réciproquement, si $a^2 - 2b^2 = \pm 1$, alors l'inverse de $a + b\sqrt{2}$ est donné par $\dfrac{1}{a + b\sqrt{2}}$; or :

   $$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm a - b\sqrt{2}$$

   Ainsi, par exemple, l'inverse de $3 + 2\sqrt{2}$ est $3 - 2\sqrt{2}$