Chapitre 4

Quelques structures algébriques

4.1 Loi de composition intrene

Définition 4.1.1 *On appelle loi de composition interne (ou opération binaire) sur un ensemble non vide E, toute application $*$ de $E \times E$ dans E.*
 # L'image $*(x, y)$ est souvent notée $x * y$.

C.à. d :
$$\begin{pmatrix} * \text{ est une loi de} \\ \text{composition interne sur } E \end{pmatrix} \Leftrightarrow \begin{cases} \forall x, y \in E, x * y \in E \\ \forall x, y, x', y' \in E, (x = x' \text{ et } y = y') \Rightarrow x * y = x' * y' \end{cases}$$

Exemples
1) On sait que : $\forall x, y \in \mathbb{N} : x + y \in \mathbb{N}$ et $x \cdot y \in \mathbb{N}$
et $\forall x, y, x', y' \in \mathbb{N}, (x = x' \text{ et } y = y') \Rightarrow (x + y = x' + y' \text{ et } x \cdot y = x' \cdot y')$
Alors, l'addition usuelle "$+$" et la multiplication usuelle "$\cdot$" sont des lois de composition internes sur $\mathbb{N}$.

Il est clair que l'addition usuelle "$+$" et la multiplication usuelle "$\cdot$" sont des lois de composition internes sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

2) La soustraction usuelle "$-$" est une loi de composition interne sur $\mathbb{Z}$, $\mathbb{Q}$,$\mathbb{R}$ et $\mathbb{C}$, mais pas sur $\mathbb{N}$.

3) L'addition usuelle "$+$" sur l'ensemble $B = \{0, 1\}$ n'est pas une loi de composition interne. En effet :

(x, y)	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$+(x, y)$	0	1	1	$2 \notin B$

La multiplication usuelle "$\cdot$" sur l'ensemble $B = \{0, 1\}$ est une loi de composition interne. En effet :

(x, y)	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$\cdot(x, y)$	0	0	0	1

4) Le produit scalaire $\diamond : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ défini par $\begin{pmatrix} x \\ y \end{pmatrix} \diamond \begin{pmatrix} x' \\ y' \end{pmatrix} = xx' + yy'$ n'est

pas une loi de composition interne.

5) La composition $\circ$ est une loi de composition interne sur l'ensemble $A(E,E)$ des applications de E dans E. En effet : Si $f : E \to E$ et $g : E \to E$ sont deux applications alors, $f \circ g : E \to E$ est une application.

6) L'intersection $\cap$ est une loi de composition interne sur l'ensemble $\mathcal{P}(E)$ des parties de E.

Définition 4.1.2 *Soit $*$ une loi de composition interne sur un ensemble non vide E. Alors :*

1) La loi $*$ est dite associative, si $\forall x, y, z \in E, (x * y) * z = x * (y * z)$
2) La loi $*$ admet un élément neutre si $\exists e \in E, \forall x \in E, (x * e = x) \wedge (e * x = x)$
L'élément e (s'il existe) est appelé élément neutre de $*$.
3) Dans le cas où $*$ admet un élément neutre e, on dit que tout élément de E est inversible (ou symétrisable) par rapport à $*$, si $\forall x \in E, \exists x' \in E, (x * x' = e) \wedge (x' * x = e)$

L'élément x' (s'il existe) est appelé inverse (ou symétrique) de x et est noté x^{-1}.

4) La loi $*$ est dite commutative, si $\forall x, y \in E, x * y = y * x$

Remarque 4.1.1
1) La disposition des parenthèses est inutile si la loi $*$ est associative et on peut écrire $x * y * z$ au lieu de $(x * y) * z$ et $x * (y * z)$
2) Si x^{-1} existe, alors $(x^{-1})^{-1} = x$.

Exemples
1) On sait que $\forall x, y, z \in \mathbb{R}, x + (y + z) = (x + y) + z$, donc l'addition usuelle "+" est associative dans $\mathbb{R}$.

$\exists e = 0 \in \mathbb{R}, \forall x \in \mathbb{R}, (x + 0 = x) \wedge (0 + x = x)$, donc 0 est l'élément neutre de "+" dans $\mathbb{R}$.

$\forall x \in \mathbb{R}, \exists x' = -x \in \mathbb{R}, (x + (-x) = 0) \wedge ((-x) + x = 0)$, donc tout élément de $\mathbb{R}$ est inversible par rapport à "+".

$\forall x, y \in \mathbb{R}, x + y = y + x$, donc l'addition usuelle "+" est commutative dans $\mathbb{R}$.

2) On sait que $\forall x, y, z \in \mathbb{R}, x \cdot (y \cdot z) = (x \cdot y) \cdot z$, donc la multiplication usuelle "$\cdot$" est associative dans $\mathbb{R}$.

$\exists e = 1 \in \mathbb{R}, \forall x \in \mathbb{R}, (x \cdot 1 = x) \wedge (1 \cdot x = x)$, donc 1 est l'élément neutre de "$\cdot$" dans $\mathbb{R}$.

Pour $x = 0$ on ne peut pas trouver $x' \in \mathbb{R}$ tel que $0 \cdot x' = 1$; donc $x = 0$ n'est pas inversible par rapport à la multiplication usuelle "$\cdot$" :
C.à.d : $\exists x = 0 \in \mathbb{R}, \forall x' \in \mathbb{R}, (x \cdot x' \neq 1) \vee (x' \cdot x \neq 1)$, donc les éléments de $\mathbb{R}$ ne sont pas tous inversibles par rapport à "$\cdot$".

$\forall x, y \in \mathbb{R}, x \cdot y = y \cdot x$, donc la multiplication usuelle "$\cdot$" est commutative dans $\mathbb{R}$.

3) Etudions l'opération $\intercal$ définie sur $\mathbb{Z}$ par $n \intercal m = -n - m$ pour $n, m \in \mathbb{Z}$..

Soient $n, m, s \in \mathbb{Z}$..

$(n \intercal m) \intercal s = (-n - m) \intercal s = n + m - s$
$n \intercal (m \intercal s) = n \intercal (-m - s) = -n + m + s$
On a, par exemple, $(1 \intercal 2) \intercal 3 = (-1 - 2) \intercal 3 = 3 - 3 = 0$
et $1 \intercal (2 \intercal 3) = 1 \intercal (-2 - 3) = -1 + 5 = 4 \neq (1 \intercal 2) \intercal 3$;
donc $\intercal$ n'est pas associative dans $\mathbb{Z}$.

Supposons e est l'élément neutre de l'opération $\intercal$ dans $\mathbb{Z}$.
C.à.d $\forall n \in \mathbb{Z},\ n \intercal e = n \wedge e \intercal n = n$.
$n \intercal e = n \Leftrightarrow -n - e = n \Leftrightarrow e = -2n$
donc $\intercal$ n'admet pas d'élément neutre, car l'élément neutre doit être le même pour tous les $n \in \mathbb{Z}$.

On ne peut pas chercher l'inverse d'un élément, car $\intercal$ n'admet pas d'élément neutre

$n \intercal m = -n - m = -m - n = m \intercal n$, donc $\intercal$ est commutative dans $\mathbb{Z}$.

4.2 Structure de groupe

Définition 4.2.1 *Soit $*$ une loi de composition interne sur un ensemble non vide G. On dit que $(G, *)$ est un groupe si $*$ est associative, admet un élément neutre e et tout élément de G est inversible par rapport à $*$.*

Si en plus, $*$ est commutative, le groupe est dit commutatif ou abélien.

Exemples
1) Les structures $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$,$(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs.

2) Les structures $(\mathbb{Q}, \cdot)$,$(\mathbb{R}, \cdot)$ et $(\mathbb{C}, \cdot)$ ne sont pas des groupes (car 0 n'a pas d'inverse pour la multiplication usuelle "$\cdot$")

3) Les structures $(\mathbb{Q}^*, \cdot)$,$(\mathbb{R}^*, \cdot)$ et $(\mathbb{C}^*, \cdot)$ sont des groupes commutatifs.

4) Les structures $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ ne sont pas des groupes.

5) $(\mathbb{Z}, \intercal)$ telle que $n \intercal m = -n - m$, n'est pas un groupe.

4.2.1 Sous groupe

Définition 4.2.2 *Soit $(G, *)$ un groupe et H une partie de G.*
On dit $(H, *)$ est un sous groupe de $(G, *)$ si $(H, *)$ est lui même un groupe pour la loi $*$ restreinte à H.

Proposition 4.2.1 *Soit H une partie d'un groupe $(G, *)$ d'élément neutre e. Alors,*
$((H, *)$ est un sous groupe de $(G, *))$ $\Leftrightarrow \begin{cases} e \in H \\ \forall x, y \in H : x * y^{-1} \in H \end{cases}$

Preuve : a) Supposons que $(H,*)$ est un sous groupe de $(G,*)$ et montrons que $\begin{cases} e \in H \\ \forall x,y \in H : x * y^{-1} \in H \end{cases}$
Soit x,$y \in H$,
on a x,$y^{-1} \in H$ (car tout élément de H admet un inverse par rapport à $*$ dans H).
et $x * y^{-1} \in H$ (car $*$ est une loi de composition interne dans H).
Donc $\forall x$,$y \in H : x * y^{-1} \in H$.
Mais $H \neq \varnothing$, donc $\exists x_0 \in G : x_0 \in H$, d'où $x_0 * x_0^{-1} \in H$. C.à.d $e \in H$.

b) Supposons que $\begin{cases} e \in H \\ \forall x,y \in H : x * y^{-1} \in H \end{cases}$ et montrons que $(H,*)$ est un sous groupe de $(G,*)$.
On a $H \neq \varnothing$ car $e \in H$,
et comme $\forall x \in G : x * e = x = e * x$. En particulier $\forall x \in H : x * e = x = e * x$
C.à.d : e est l'élément neutre de $*$ dans H.

Soit $y \in H$ et $x = e \in H$, alors $x * y^{-1} = e * y^{-1} = y^{-1} \in H$, donc $\forall y \in H : y^{-1} \in H$.
C.à.d : Tout élément de H admet un inverse par rapport à $*$ dans H.

Soit x,$y \in H$, alors $x, y^{-1} \in H$ d'où $x*(y^{-1})^{-1} = x*y \in H$; donc $\forall x,y \in H : x * y \in H$.
C.à.d : $*$ est une loi de composition interne dans H.

Soit $x,y,z \in H$, alors $x,y,z \in G$, d'où $(x * y) * z = x * (y * z)$, donc
$\forall x,y,z \in H : (x * y) * z = x * (y * z)$. C.à.d : $*$ est une loi associative dans H.
Ainsi $(H,*)$ vérifie toutes les conditions d'un groupe, donc c'est bien un sous groupe de $(G,*)$.

Exemples
1) $\mathbb{Z}$ est une partie de $\mathbb{Q}$ et $(\mathbb{Q},+)$ est un groupe.
On a $\begin{cases} 0 \in \mathbb{Z} \\ \forall x,y \in \mathbb{Z} : x + (-y) \in \mathbb{Z} \end{cases}$, alors $(\mathbb{Z},+)$ est un sous groupe de $(\mathbb{Q},+)$.
De même $(\mathbb{Q},+)$ est un sous groupe de $(\mathbb{R},+)$ et de $(\mathbb{C},+)$.

2) Si $(G,*)$ est un groupe d'élément neutre e.
On a $\begin{cases} e \in G \\ \forall x,y \in G : x * y^{-1} \in G \end{cases}$, alors $(G,*)$ est un sous groupe de $(G,*)$.
On a $\begin{cases} e \in \{e\} \\ \forall x,y \in \{e\} : x * y^{-1} \in \{e\} \end{cases}$, alors $(\{e\},*)$ est un sous groupe de $(G,*)$.
$(\{e\},*)$ et $(G,*)$ sont appelés sous groupes triviaux de $(G,*)$.

3) Le cercle unité $S^1 = \{z \in \mathbb{C} \ / \ |z| = 1\}$ est une partie de $\mathbb{C}^*$ et $(\mathbb{C}^*,\cdot)$ est un groupe.
On a $|1| = 1$ donc $1 \in S^1$.
Soit $z,z' \in S^1$, on a $\left|z \cdot (z')^{-1}\right| = \frac{|z|}{|z'|} = 1$, donc $z \cdot (z')^{-1} \in S^1$
Ainsi, $\begin{cases} 1 \in S^1 \\ \forall z,z' \in S^1 : z \cdot (z')^{-1} \in S^1 \end{cases}$, alors $(S^1,\cdot)$ est un sous groupe de $(\mathbb{C}^*,\cdot)$.

4) $\mathbb{R}^{*+}$ est une partie de $\mathbb{R}^*$ et $(\mathbb{R}^*, \cdot)$ est un groupe.
On a $1 \in \mathbb{R}^{*+}$.
Soit $x, x' \in \mathbb{R}^{*+}$, on a $x \cdot (x')^{-1} = \frac{x}{x'} > 0$, donc $x \cdot (x')^{-1} \in \mathbb{R}^{*+}$
Ainsi, $\begin{cases} 1 \in \mathbb{R}^{*+} \\ \forall x, x' \in \mathbb{R}^{*+} : x \cdot (x')^{-1} \in \mathbb{R}^{*+} \end{cases}$, alors $(\mathbb{R}^{*+}, \cdot)$ est un sous groupe de $(\mathbb{R}^*, \cdot)$.

4.3 Homomorphismes de groupes

Définition 4.3.1 *On appelle homomorphisme du groupe $(G, *)$ dans le groupe $(G', *')$, toute application $f : G \to G'$ telle que :*

$$\forall x, y \in G : f(x * y) = f(x) *' f(y)$$

Exemples
1) Soit l'application $h : \mathbb{R} \to \mathbb{R}^{*+}$ telle que $h(x) = e^x$ et soit $x, y \in \mathbb{R}$.
On a $h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot h(y)$.
Alors h est un homorphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{R}^{*+}, \cdot)$

2) Soit l'application $f : \mathbb{C}^* \to \mathbb{R}^*$ telle que $f(z) = |z|$ et soit $z, z' \in \mathbb{C}^*$.
On a $f(z \cdot z') = |z \cdot z'| = |z| \cdot |z'| = f(z) \cdot f(z')$.
Alors f est un homorphisme du groupe $(\mathbb{C}^*, \cdot)$ dans le groupe $(\mathbb{R}^*, \cdot)$

Théorème 4.3.1 *Soit $f : G \to G'$ un homomorphisme du groupe $(G, *)$ dans le groupe $(G', *')$ d'éléments neutres respectifs e et e' , alors*
1) $f(e) = e'$.
2) $\forall x \in G, (f(x))^{-1} = f(x^{-1})$.

Preuve :
1) On a $f(e) = f(e) *' e' = f(e) *' \left[f(x) *' (f(x))^{-1}\right] = [f(e) *' f(x)] *' (f(x))^{-1}$
$= f(e * x) *' (f(x))^{-1} = f(x) *' (f(x))^{-1} = e'$
2) Soit $x \in G$, on a
$f(x^{-1}) *' f(x) = f(x^{-1} * x) = f(e) = e'$
et $f(x) *' f(x^{-1}) = f(x * x^{-1}) = f(e) = e'$.
Alors $(f(x))^{-1} = f(x^{-1})$.

4.4 Structure d'Anneau

Définition 4.4.1 *Soit A un ensemble non vide muni de deux lois de composition interne $*_1$ et $*_2$. On dit que $(A, *_1, *_2)$ est un anneau si*
1) $(A, *_1)$ est un groupe commutatif.
2) La loi $*_2$ est associative.

3) $\forall x, y, z \in A : \begin{cases} et & x *_2 (y *_1 z) = (x *_2 y) *_1 (x *_2 z) \\ & (y *_1 z) *_2 x = (y *_2 x) *_1 (z *_2 x) \end{cases}$.
(Cette condition est appelée distributivité de la loi $*_2$ *par rapport à la loi* $*_1$*).*

 # Si la loi $*_2$ *admet un élément neutre, on l'appelle unité et on dit que l'anneau est unitaire.*
 # Si la loi $*_2$ *est commutative, on dit que l'anneau est commutatif.*

Exemples
1) On sait que $(\mathbb{Z}, +)$ est un groupe commutatif, et on sait que la multiplication usuelle "$\cdot$" est associative et distributive par rapport à l'addition usuelle "$+$" dans $\mathbb{Z}$. Alors $(\mathbb{Z}, +, \cdot)$ est un anneau.

De plus, la deuxième loi "$\cdot$" est commutative et adment 1 comme élément neutre, donc $(\mathbb{Z}, +, \cdot)$ est un anneau commutatif et unitaire.

De même, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux unitaires, commutatifs.

Remarque 4.4.1
Les lois d'un anneau $(A, *_1, *_2)$ *sont souvent notées* $+_A$ *et* $\cdot_A$ *au lieu de* $*_1$ *et* $*_2$ *et pour cette raison on note l'élément neutre de* $+_A$ *par* 0_A *et l'inverse de* x *par rapport à* $+_A$ *par* $-x$.
Aussi, on note l'élément neutre de $\cdot_A$ *(s'il existe) par* 1_A *et l'inverse de* x *par rapport à* $\cdot_A$ *(s'il existe) par* x^{-1}.

4.4.1 Quelques règles de calcul

Proposition 4.4.1 *Soit* $(A, +_A, \cdot_A)$ *un anneau d'élément neutre* 0_A. *Alors :*
1) $\forall x \in A : x \cdot_A 0_A = 0_A = 0_A \cdot_A x$
2) $\forall x, y \in A : (-x) \cdot_A y = -(x \cdot_A y) = x \cdot_A (-y)$
3) $\forall x, y \in A : (-x) \cdot_A (-y) = x \cdot_A y$
4) Si l'anneau admet un élément unité 1_A, *alors* $\forall x \in A : -x = (-1_A) \cdot_A x$.

Preuve
1) Soit $x \in A$, on a

$$\begin{aligned} x \cdot_A 0_A &= x \cdot_A 0_A +_A 0_A \\ &= x \cdot_A 0_A +_A [x \cdot_A 0_A +_A (-(x \cdot_A 0_A))], && \text{car } -x \cdot_A 0_A \text{ est le symétrique de } x \cdot_A 0_A \\ & && \text{par rapport à } +_A. \\ &= x \cdot_A (0_A +_A 0_A) +_A (-(x \cdot_A 0_A)), && \text{car } \cdot_A \text{ est distributive par rapport à } +_A \\ &= x \cdot_A 0_A +_A (-(x \cdot_A 0_A)) \\ &= 0_A \end{aligned}$$

De la même façon on montre que $-(x \cdot_A y) = x \cdot_A (-y)$

2) Soit $x, y \in A$, on a

$$\begin{aligned} x \cdot_A y +_A ((-x) \cdot_A y) &= (x +_A (-x)) \cdot_A y, && \text{car } \cdot_A \text{ est distributive par rapport à } +_A \\ &= 0_A \cdot_A y \\ &= 0_A, && \text{d'après 1).} \end{aligned}$$

Alors $(-x) \cdot_A y = -(x \cdot_A y)$.

De la même façon on montre que $0_A \cdot_A x = 0_A$.

3) Soient $x, y \in A$, on a

$$\begin{aligned} (-x) \cdot_A (-y) &= -(x \cdot_A (-y)), && \text{d'après 2)} \\ &= -(-(x \cdot_A y)), && \text{d'après 2)} \\ &= x \cdot_A y \end{aligned}$$

4.4.2 Anneau intègre

Définition 4.4.2 *On dit qu'un anneau $(A, +_A, \cdot_A)$ est intègre, si*

$$\forall x, y \in A : (\ x \cdot_A y = 0_A \Rightarrow\ \ (x = 0_A \vee y = 0_A))$$

Exemple
Les structures $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux intègres.

4.5 Structure de corps

Définition 4.5.1 *Soit $(K, +_K, \cdot_K)$ un anneau unitaire.*
On dit que $(K, +_K, \cdot_K)$ est un corps si
1) $1_K \neq 0_K$
2) Tout élément de $K - \{0_K\}$ est inversible par rapport à la loi $\cdot_K$.
 # Le corps est dit commutatif si la loi $\cdot_K$ est commutative.

Remarque 4.5.1 *1) Si $(K, +_K, \cdot_K)$ est un corps, alors $(K^*, \cdot_K)$ est un groupe (où $K^* = K - \{0_K\}$).*
2) Tout corps K est un anneau intègre.
En effet : Soit $a, b \in K$, on a

$$\begin{aligned} a \cdot_K b = 0_K &\Rightarrow (a \cdot_K b = 0_K\ \wedge (a = 0_K \vee a \neq 0_K)) \\ &\Rightarrow ((a \cdot_K b = 0_K\ \wedge a = 0_K) \vee (a \cdot_K b = 0_K\ \wedge a \neq 0_K)) \\ &\Rightarrow ((a = 0_K) \vee (a^{-1} \cdot_K a \cdot_K b = a^{-1} \cdot_K 0_K)), \text{ car } a \neq 0_K \text{ assure que } a^{-1} \text{ existe} \\ &\Rightarrow ((a = 0_K) \vee (b = 0_K)) \end{aligned}$$

Exemples
1) Les structures $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des corps commutatifs.

2) La structure $(\mathbb{Z}, +, \cdot)$ n'est pas un corps, car les seuls éléments inversibles dans $\mathbb{Z}^*$ par rapport à la multiplication usuelle $\cdot$ sont 1 et -1.

4.6 Exercices du chapitre 4

Exercice 4.1 *1) On munit $\mathbb{Z}$ par la loi de composition $*$ définie par :*
$\forall x, y \in \mathbb{Z} \ : x * y = x + y + x^2 y$.
Montrer que $*$ est une loi interne ; puis étudier, pour cette loi, la commutativité, l'associativité, l'existence de l'élément neutre et l'existence du symétrique.
2) Même question pour la loi de composition Δ définie sur $\mathbb{R}_+^*$ par :
$\forall x, y \in \mathbb{R}_+^* : x * y = \sqrt{x^2 + y^2}$.

Exercice 4.2 *On munit l'intervalle $]-1, 1[$ par la loi de composition interne $*$ définie par : $\forall x, y \in \mathbb{Z} : x * y = \frac{x+y}{1+xy}$.*
Montrer que $(]-1, 1[, *)$ est un groupe commutatif.

Exercice 4.3 *Sur $\mathbb{Q}$, on définit l'opération $\triangle$ par*
$\forall \alpha, \beta \in \mathbb{Q} : \alpha \triangle \beta = (\alpha - 1)(\beta - 1) + 1$.
1) Montrer $(\mathbb{Q}, \triangle)$ n'est pas un groupe commutatif.
2) Trouver le plus grand ensemble $E \subset \mathbb{Q}$ pour lequel $(E, \triangle)$ soit un groupe commutatif.
3) Soit $f : E \longrightarrow \mathbb{Q}^*$ l'application définie par : $\forall \alpha \in E : f(\alpha) = \alpha - 1$.
Montrer que f est un homomorphisme du groupe $(E, \triangle)$ dans le groupe $(\mathbb{Q}^*, .)$.

Pour tout $n \in \mathbb{N}^* \setminus \{1\}$ et $\alpha \in E$, posons $\alpha^{(n)} = \underbrace{\alpha \triangle \alpha \triangle ... \triangle \alpha}_{n\text{-}fois}$.
Déterminer une expression simple de $\alpha^{(n)}$, puis calculer $3^{(11)} - 3^{(5)}$.

Exercice 4.4 *Soit $Aff(\mathbb{R})$ l'ensemble des applications affines de $\mathbb{R}$ dans $\mathbb{R}$.*
$Aff(\mathbb{R}) = \left\{\varphi_{(a,b)} : \mathbb{R} \to \mathbb{R} \ / \ (a, b) \in \mathbb{R}^* \times \mathbb{R} \text{ et } \forall x \in \mathbb{R} : \varphi_{(a,b)}(x) = ax + b\right\}$
1) Montrer que $(Aff(\mathbb{R}), \circ)$ est un groupe non commutatif.
2) Montrer que l'ensemble $T(\mathbb{R}) = \left\{\varphi_{(1,b)} \ / b \in \mathbb{R}\right\}$ des translations de $\mathbb{R}$, est un sous groupe de $(Aff(\mathbb{R}), \circ)$.

Exercice 4.5 *Soient $(G, *)$ un groupe et $Z(G)$ l'ensemble des éléments de G qui commutent avec tous les éléments de G. Montrer que $Z(G)$ est un sous groupe de G.*

Exercice 4.6 *Soient $(G, *)$ un groupe d'élément neutre e, tel que pour tout $x \in G$: $x^3 = e$. Montrer que pour tous $x, y \in G$: $(x * y)^2 = y^2 * x^2$ et $x * y^2 * x = y * x^2 * y$.*
Noter que $x^2 = x * x$ et $x^3 = x * x * x$

Exercice 4.7 *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble G muni d'une opération $*$. On dit que $\mathcal{R}$ est compatible avec la loi $*$ si,*
pour tous $x, y, a, b \in G$: $(x\mathcal{R}y$ et $a\mathcal{R}b) \Longrightarrow (x * a)\,\mathcal{R}\,(y * b)$.
On définit l'opération $\overset{\bullet}{*}$ sur $G_{/\mathcal{R}}$ par $\dot{x} \overset{\bullet}{*} \dot{y} = \widehat{x * y}$.
1) Montrer que si $(G, *)$ est un groupe, alors $\left(G_{/\mathcal{R}}, \overset{\bullet}{*}\right)$ est aussi un groupe.
2) Application : $(G, *) = (\mathbb{Z}, +)$ et $\mathcal{R}_n$ la congruence modulo n.

Exercice 4.8 *Soient $*$ l'opération définie sur $\mathbb{R}$ donnée dans l'exercice 1 et la multiplication usuelle de $\mathbb{R}$. Etudier la distributivité de chaque loi par rapport à l'autre.*

Exercice 4.9 *Montrer que $\left(\mathbb{Z}_{/p\mathbb{Z}}, \overset{\bullet}{+}, \overset{\bullet}{\times}\right)$ est un anneau commutatif unitaire et qu'il s'agit d'un corps si p est premier. $(\forall \overset{\bullet}{x}, \overset{\bullet}{y} \in \mathbb{Z}_{/p\mathbb{Z}} : \overset{\bullet}{x} \overset{\bullet}{+} \overset{\bullet}{y} = \widehat{\overset{\bullet}{x+y}}$ et $\overset{\bullet}{x} \overset{\bullet}{\times} \overset{\bullet}{y} = \widehat{\overset{\bullet}{x \times y}})$*

Exercice 4.10 *Soit $(A, +_{_A}, \cdot_{_A})$ un anneau vérifiant $x^2 = x$ pour tout $x \in A$. (On dit que x est idempotent et que A est un anneau de Boole)*
1) Montrer que $2x = 0_A$
2) Montrer que A est commutatif. En déduire la valeur de $(x \cdot_{_A} y) \cdot_{_A} (x +_{_A} y)$ Noter que $x^2 = x \cdot_{_A} x$ et $2x = x +_{_A} x$

Exercice 4.11 *Soit $(G, *)$ un groupe. Trouver une condition pour que l'application $f : G \to G$ telle que $f(x) = x * x$ soit un endomorphisme.*

Exercice 4.12 *Montrer que $(\mu_n, \times)$ est isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}, \overset{\bullet}{+}\right)$*
$\mu_n = \{z \in \mathbb{C} \ / \ z^n = 1\}$ ($n \in \mathbb{N}^*$) est l'ensemble des racines $n-$ème complexes de l'unité 1

Exercice 4.13 *L'application $f : \mathbb{C}^* \to \mathbb{R}^*$ telle que $f(z) = |z|$*
1) Montrer que f est un homomorphisme du groupe $(\mathbb{C}^*, \cdot)$ dans le groupe $(\mathbb{R}^*, \cdot)$

Exercice 4.14 *Montrer que le composé de deux homomorphismes de groupes est un homomorphisme de groupes.*