# Chapitre 13

# Structures algébriques

**Objectifs**

- Rappeler la structure de groupe, les règles de calculs. Définir les notions de morphisme, de noyau, de sous-groupe.
- Rappeler la structure d'anneau, les règles de calculs, les notions d'inversibles et d'intégrité. Définir les notions de morphisme et de sous-anneau.
- Rappeler la structure de corps commutatif, les règles de calculs. Définir les notions de morphisme, de sous-corps.

**Sommaire**



## I) Structure de groupe

### 1) Rappels

Un groupe est un ensemble non vide $G$ muni d'une opération $*$ (ou loi de composition) qui vérifie les propriétés suivantes :

- elle doit être interne : $\forall\ x, y \in G, x * y \in G$.
- elle doit être associative : $\forall\ x, y, z \in G, x * (y * z) = (x * y) * z$.
- elle doit posséder un élément neutre : $\exists\ e \in G, \forall\ x \in G, e * x = x * e = x$. Si la loi est une addition l'élément neutre sera noté $0_G$ et on parlera de groupe additif. Si la loi est une multiplication, l'élément neutre sera noté $1_G$ et on parlera de groupe multiplicatif. Dans le cas général l'élément neutre est souvent noté $e_G$.
- tout élément de $G$ doit avoir un symétrique dans $G$ : $\forall\ x \in G, \exists\ x' \in G, x * x' = x' * x = e_G$. En notation additive, le symétrique de $x$ est appelé **opposé de** $x$ et noté $-x$, en notation multiplicative on l'appelle **inverse de** $x$ et on le note $x^{-1}$.

Lorsque toutes ces conditions sont remplies, on dit $(G, *)$ est un groupe. Si en plus la loi $*$ est commutative ($\forall\ x, y \in G, x * y = y * x$), alors on dit que $(G, *)$ est un **groupe abélien** (ou groupe commutatif).

**Exemples**:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes abéliens.
- $(\mathbb{N}, +)$ et $(\mathbb{Z}^*, \times)$ ne sont pas des groupes.
- Si $(E, +, \times)$ est un corps, alors $(E, +)$ est un groupe abélien et $(E^*, \times)$ est un groupe (abélien si le corps est commutatif).

- $(\mathscr{F}(I,\mathbb{C}),+)$ est un groupe abélien pour l'addition des fonctions (ou des suites si $I=\mathbb{N}$).
- $(\mathbb{K}^n,+)$ pour l'addition des $n$-uplets de scalaires est un groupe abélien.
- Si $E$ est un ensemble non vide, l'ensemble des permutations de $E$ : $\mathscr{S}_E$ est un groupe pour la loi $\circ$ (non abélien en général).

**Règles de calculs** : Soit $(G,*)$ un groupe

- Soient $x,y\in G$, le symétrique de $x*y$ est : $(x*y)'=y'*x'$.
- Soient $a,b\in G$, l'équation $a*x=b$ admet comme unique solution dans $G$, $x=a'*b$.

## 2) Morphisme de groupes

**DÉFINITION 13.1**

*Soit $(G,.)$ et $(G',*)$ deux groupes, un morphisme de groupes de $G$ vers $G'$ est une application $f:G\to G'$ telle que : $\forall\ x,y\in G, f(x.y)=f(x)*f(y)$.*
*Si de plus $f$ est bijective, alors on dit que $f$ est un isomorphisme de groupes.*

**Exemples**:

- $\ln:(]0;+\infty[,\times)\to(\mathbb{R},+)$ est un morphisme de groupes, c'est même un isomorphisme de groupes.
- $\exp:(\mathbb{R},+)\to(]0;+\infty[,\times)$ est un morphisme de groupes, c'est même un isomorphisme de groupes.
- $f:(\mathbb{Z},+)\to(\mathbb{U}_n,\times)$ définie par $f(k)=\exp(2ik\pi/n)$ est un morphisme de groupes, mais non bijectif.

**THÉORÈME 13.1**

*On a les propriétés suivantes :*

- *Si $f:(G,.)\to(G',*)$ est un morphisme de groupes, alors $f(e)=e'$ et $\forall\ x\in G, f(x^{-1})=f(x)^{-1}$ (où $e$ et $e'$ désignent les éléments neutres respectifs de $G$ et $G'$).*
- *La composée de deux morphismes de groupes est un morphisme de groupes.*
- *Si $f:(G,.)\to(G',*)$ est un isomorphisme de groupes, alors la bijection réciproque $f^{-1}:(G',*)\to(G,.)$ est un morphisme de groupes.*

**Preuve**: Celle-ci est laissée en exercice. □

**Exemple**: $\ln:(]0;+\infty[,\times)\to(\mathbb{R},+)$ est isomorphisme de groupes, donc $\ln(1)=0, \forall\ x>0, \ln(1/x)=-\ln(x)$ et la bijection réciproque, exp, est un morphisme de groupes, *i.e.* :

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

**THÉORÈME 13.2**

*Soit $f:(\mathbb{R},+)\to(\mathbb{R},+)$ un morphisme de groupes continu en 0, alors :*

$$\forall x\in\mathbb{R}, f(x)=ax\ \ (\text{avec } a=f(1)).$$

**Preuve**: On pose $a=f(1)$, on montre que $\forall n\in\mathbb{N}, f(n)=an$ (réurrence), on en déduit que $f(-n)=a(-n)$ car $f(-n)=-f(n)$, d'où : $\forall n\in\mathbb{Z}, f(n)=an$.

Soit $r=\frac{p}{q}$ un rationnel avec $q\in\mathbb{N}^*$, alors $f(qr)=f(p)=ap=qf(r)$ d'où $f(r)=ar$.

Soit $x\in\mathbb{R}$ et $(r_n)$ une suite de rationnels qui converge vers $x$, alors $(x-r_n)$ converge vers 0 et donc $f(x-r_n)$ tend vers $f(0)=0$, or $f(x-r_n)=f(x)-f(r_n)$ donc $(f(r_n))$ converge vers $f(x)$. Or $f(r_n)=ar_n\to ax$, par conséquent $f(x)=ax$. □

## 3) Sous-groupes d'un groupe

**DÉFINITION 13.2**

*Soit $(G,.)$ un groupe et $H$ un ensemble, on dit que $H$ est un sous-groupe de $(G,.)$ lorsque :*

$$H\subset G;\quad H\neq\emptyset\ \ et\ \ \forall\ x,y\in H, x.y\in H, x^{-1}\in H.$$

**Exemples**:
- $\{e\}$ et $G$ sont des sous-groupes de $(G,.)$, ils sont appelés sous-groupes triviaux de $(G,.)$.
- Si $(H,.)$ est un groupe inclus dans un groupe $(G,.)$ pour la même loi, alors $H$ est un sous-groupe de $G$, car on vérifie facilement que l'élément neutre de $G$ est forcément égal à l'élément neutre de $H$, ce qui entraîne pour $x \in H$, que son symétrique dans $G$ et son symétrique dans $H$ sont les mêmes.
- L'ensemble des fonctions définies sur $\mathbb{R}$ et $2\pi$-périodiques est un groupe additif, car c'est un sous-groupe de $(\mathcal{F}(\mathbb{R},\mathbb{R}),+)$.
- L'ensemble des entiers pairs est un groupe additif, car c'est un sous-groupe de $(\mathbb{Z},+)$.

*Si $H$ est un sous-groupe de $(G,.)$ alors $(H,.)$ lui-même est un groupe (de même élément neutre que $G$). Ceci est souvent utilisé dans la pratique pour montrer qu'un ensemble est un groupe pour une loi, on essaie de montrer (quand c'est possible) que c'est un sous-groupe d'un groupe connu pour cette même loi.*

**THÉORÈME 13.3 (sous-groupes de $(\mathbb{Z},+)$)**

*$H$ est un sous-groupe de $(\mathbb{Z},+)$ ssi il existe un entier $n$ tel que $H = n\mathbb{Z}$ (ensemble des multiples entiers de $n$). L'entier $n$ est unique au signe près et si $H \neq \{0\}$, alors $n = \min H^{*+}$.*

**Preuve**: Il est facile de vérifier que pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors on peut prendre $n = 0$ et c'est le seul entier qui convienne. Si $H \neq \{0\}$, posons, $n = \min H^{*+}$ ($n$ existe dans $\mathbb{N}$, c'est la propriété fondamentale de $\mathbb{N}$), on a $n \in H$, comme $H$ est un sous-groupe de $(\mathbb{Z},+)$, tout multiple de $n$ est dans $H$, *i.e.* $n\mathbb{Z} \subset H$. Soit $k \in H$ effectuons la division euclidienne de $k$ par $n$ ($n \neq 0$) : $k = nq + r$ avec $0 \leqslant r < n$. On a donc $r = k - nq \in H^+$, si $r \neq 0$ alors $r \geqslant n$ ce qui est absurde, donc $r = 0$ ce qui donne $k = nq \in n\mathbb{Z}$, finalement $H = n\mathbb{Z}$. Si on a aussi $H = m\mathbb{Z}$ avec $m \in \mathbb{N}$, alors $n\mathbb{Z} = m\mathbb{Z}$, donc $n$ et $m$ se divisent mutuellement dans $\mathbb{N}$, donc $n = m$. □

**THÉORÈME 13.4 (sous-groupes de $(\mathbb{R},+)$)**

*Soit $G$ un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$, alors soit $G$ est dense dans $\mathbb{R}$, soit $G$ est de la forme $G = \alpha\mathbb{Z}$ avec $\alpha > 0$.*

**Preuve**: $G_+^*$ est non vide, soit $\alpha = \inf G_+^*$.
- Si $\alpha > 0$ : supposons $\alpha \notin G$, alors on peut trouver deux éléments de $G$, $g_1$ et $g_2$ tels que $\alpha < g_1 < g_2 < 2\alpha$, mais alors $0 < g_2 - g_1 < \alpha$ avec $g_2 - g_1 \in G_+^*$ : absurde., donc $\alpha \in G$. On en déduit alors que $\alpha\mathbb{Z} \subset G$. Soit $g \in G$ et $n = \mathrm{E}(\frac{g}{\alpha})$, alors $n\alpha \leqslant g < ((n+1)\alpha$ et donc $0 \leqslant g - n\alpha < \alpha$, on en déduit que $g - n\alpha$ est nul car c'est un élément positif de $G$, d'où $G = \alpha\mathbb{Z}$.
- Si $\alpha = 0$ : soit $x \in \mathbb{R}$ et $\varepsilon > 0$, il existe $g \in G$ tel que $0 < g < \varepsilon$, soit $n = \mathrm{E}(\frac{x}{g})$ alors $ng \leqslant x < ng + g < ng + \varepsilon$, donc $|x - ng| < \varepsilon$ avec $ng \in G$, donc $G$ est dense dans $\mathbb{R}$.

□

**Exercice**: Soient $a, b \in \mathbb{R}^*$, montrer que $G = a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $(\mathbb{R},+)$ dense dans $\mathbb{R}$ si et seulement si $\frac{a}{b}$ est irrationnel. En déduire que $\{\cos(n) \mid n \in \mathbb{N}\}$ est dense dans $[-1;1]$.

**THÉORÈME 13.5 (propriétés des sous-groupes)**

*Une intersection de sous-groupes de $(G,.)$, est un sous-groupe de $(G,.)$, mais ceci n'est pas vrai pour la réunion.*
*Si $f : (G,.) \to (G',*)$ est un morphisme de groupes, alors :*
- *L'image d'un sous-groupe de $(G,.)$ est un sous-groupe de $(G',*)$.*
- *L'image réciproque d'un sous-groupe de $(G',*)$ est un sous-groupe de $(G,.)$*

**Preuve**: Celle-ci est laissée en exercice. Donnons cependant un contre-exemple pour la réunion : $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z},+)$, car 2 et 3 sont dans la réunion, mais pas $2+3=5$, cet ensemble n'est donc pas stable pour l'addition (les autres conditions sont néanmoins remplies). □

*Si $f : (G,.) \to (G',*)$ est un morphisme de groupes, alors $\mathrm{Im}(f)$, l'ensemble des images, est un sous-groupe de $(G',*)$ puisque c'est l'image directe de $G$ qui est un sous-groupe de $(G,.)$.*

## 4) Noyau d'un morphisme de groupe

**DÉFINITION 13.3**

*Soit $f : (G,.) \to (G',*)$ un morphisme de groupes, on appelle noyau de $f$ l'ensemble noté* $\ker(f)$ *et défini par :* $\ker(f) = \{x \in G \ / \ f(x) = e'\}$.
*C'est donc l'ensemble des antécédents de $e'$ par $f$, c'est donc une partie de $G$ qui contient toujours $e$ (car $f(e) = e'$).*

**Exemples**:
- $f : (\mathbb{Z},+) \to (\mathbb{U}_n,\times)$ définie par $f(k) = \exp(2ik\pi/n)$, est un morphisme de groupes, son noyau est $\ker(f) = n\mathbb{Z}$.
- $\exp : (\mathbb{C},+) \to (\mathbb{C}^*,\times)$ est un morphisme de groupes, son noyau est $\ker(\exp) = 2i\pi\mathbb{Z}$.
- $f : (\mathbb{C}^*,\times) \to (\mathbb{C}^*,\times)$ définie par $f(z) = z^n$ est un morphisme de groupes, son noyau est $\ker(f) = \mathbb{U}_n$.

**THÉORÈME 13.6 (propriétés du noyau)**

*Soit $f : (G,.) \to (G',*)$ un morphisme de groupes, alors :* $\ker(f)$ *est un sous-groupe de $(G,.)$ et $f$ est injective ssi* $\ker(f) = \{e\}$.

**Preuve**: Il est facile de vérifier que $\ker(f)$ est un sous-groupe de $G$. Si $f$ est injective, soit $x \in \ker(f)$, alors $f(x) = e' = f(e)$, donc $x = e$ d'où $\ker(f) = \{e\}$.

Réciproquement, si $\ker(f) = \{e\}$, supposons $f(x) = f(y)$ avec $x, y \in G$, on a $f(x) * f(y)^{-1} = e'$, *i.e.* $f(x) * f(y^{-1}) = e'$ et donc $f(x.y^{-1}) = e'$, ce qui signifie que $x.y^{-1} \in \ker(f)$, mais alors $x.y^{-1} = e$, d'où $x = y$, $f$ est injective. □

*Si $f : (G,.) \to (G',*)$ est un morphisme de groupes, alors $f$ est un ismorphisme de groupes si et seulement si* $\mathrm{Im}(f) = G'$ *(surjectivité)* ***et*** $\ker(f) = \{e\}$ *(injectivité).*

# II) Anneaux et corps

## 1) Anneaux

**DÉFINITION 13.4**

*Un anneau est un ensemble $A$ muni de deux lois de composition internes : une addition et une multiplication, qui vérifient :*
- *$(A,+)$ est un groupe abélien.*
- *La multiplication :*
  - *est associative,*
  - *admet un élément neutre (noté 1).*
  - *est distributive sur l'addition.*

*Si de plus la multiplication est commutative, on dit que $(A,+,\times)$ est un anneau commutatif.*

**Exemples**:
- Tout corps est un anneau (réciproque fausse).
- $(\mathbb{Z},+,\times)$ est un anneau commutatif mais ce n'est pas un corps.
- $(\mathscr{F}(\mathbb{N},\mathbb{C}),+,\times)$ est un anneau commutatif.
- Si $E$ est un ensemble non vide, l'ensemble des fonctions de $E$ dans $\mathbb{C}$ muni des opérations usuelles sur les fonctions, est un anneau commutatif, *i.e.* $(\mathscr{F}(E,\mathbb{C}),+,\times)$ est un anneau commutatif.
- plus généralement, si $(A,+,\times)$ est un anneau et $E$ est un ensemble non vide, alors $(\mathscr{F}(E,A),+,\times)$ est un anneau.

**Règles de calculs dans un anneau** : soit $(A,+,\times)$ un anneau :
- $\forall\ x \in A, x \times 0 = 0 \times x = 0$.
- $\forall\ x, y \in A, -(x \times y) = (-x) \times y = x \times (-y)$.
- $\forall\ x, y \in A$, si $x$ et $y$ sont inversibles (pour la multiplication), alors $x \times y$ est inversible est $(x \times y)^{-1} = y^{-1} \times x^{-1}$.
- $\forall\ x, y \in A$, si $x$ et $y$ commutent (*i.e.* $x \times y = y \times x$), alors on peut utiliser la formule du binôme, c'est à dire :

$$\forall\ n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} . x^k \times y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} . x^{n-k} \times y^k.$$

**THÉORÈME 13.7 (groupe des inversibles)**

*Soit $(A,+,\times)$ un anneau, l'ensemble des inversibles de A est noté $\mathrm{U}(A)$, cet ensemble est un **groupe multiplicatif**. $(\mathrm{U}(A),\times)$ est appelé **groupe des unités** de A.*

**Preuve**: Celle - ci est simple et laissée en exercice. □

**Exemples**:
- $\mathrm{U}(\mathbb{Z})=\{\pm 1\}$.
- Si $A$ est l'anneau des suites complexes, alors $\mathrm{U}(A)$ est l'ensemble des suites complexes qui ne s'annulent pas.

**DÉFINITION 13.5 (anneau intègre)**

*Soit $(A,+,\times)$ un anneau. On dit que A est un anneau intègre lorsque le produit de deux éléments non nuls est toujours non nul, sinon on dit que A est un anneau non intègre.*

**Remarques** :
- Dans un anneau intègre, un produit de facteurs est nul ssi au moins un des facteurs est nul.
- $(\mathbb{Z},+,\times)$ est un anneau intègre.
- L'ensemble des suites complexes est un anneau non intègre.

**DÉFINITION 13.6 (morphisme d'anneaux)**

*Soit $f:(A,+,\times)\to(B,+,\times)$ une application d'un anneau A dans un anneau B, on dit que $f$ est un morphisme d'anneaux lorsque :*
- *$f$ est un morphisme de groupes additifs, i.e. $\forall\, x,y\in A, f(x+y)=f(x)+f(y)$.*
- *$\forall\, x,y\in A, f(x\times y)=f(x)\times f(y)$.*
- *$f(1_A)=1_B$.*

*Si de plus $f$ est bijective, alors on dit que $f$ est un isomorphisme d'anneaux.*

**Exemples**:
- On note $\mathbb{Z}[i]=\{a+ib \;/\; a,b\in\mathbb{Z}\}$, il est facile de voir que pour les opérations usuelles sur les complexes, $\mathbb{Z}[i]$ est un anneau intègre (anneau des entiers de *Gauss*), et que le groupe des inversibles est $U(\mathbb{Z}[i])=\{\pm 1,\pm i\}$. La conjugaison est isomorphisme d'anneaux de $\mathbb{Z}[i]$ dans lui-même.
- Soit $(A,+,\times)$ un anneau, l'application $f:\mathbb{Z}\to A$ définie par $f(n)=n.1_A$ est un morphisme d'anneaux, et que $\mathrm{Im}(f)=G(1_A)$ le sous-groupe additif engendré par $1_A$.

**THÉORÈME 13.8 (propriétés des morphismes d'anneaux)**
- *La composée de deux morphismes d'anneaux est un morphisme d'anneaux.*
- *Si $f:A\to B$ est un morphisme d'anneaux, alors pour tout $x$ inversible dans A, $f(x)$ est inversible dans B et $f(x^{-1})=\big(f(x)\big)^{-1}$.*
- *La réciproque d'un isomorphisme d'anneaux $f$ est un morphisme d'anneaux, et induit un isomorphisme de groupes entre les groupes des inversibles.*

**Preuve**: Celle-ci est laissée en exercice. □

*Il découle du deuxième point que $\tilde{f}:U(A)\to U(B)$ définie par $\tilde{f}(x)=f(x)$, est un morphisme de groupes multiplicatifs.*

**DÉFINITION 13.7 (sous-anneaux d'un anneau)**

*Soit $(A,+,\times)$ un anneau, et soit $H$ un ensemble, on dit que $H$ est un sous-anneau de A lorsque :*
- *$H\subset A$.*
- *$1_A\in H$.*
- *$\forall\, x,y\in H, x+y\in H$, $x\times y\in H$ et $-x\in H$.*

*Si c'est le cas, alors $(H,+,\times)$ est lui-même un anneau.*

**Exemple**: $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C},+,\times)$.

**Propriété** : une intersection de sous-anneaux de $(A,+,\times)$ est un sous-anneau de $A$.

### 2) Corps

**Définition 13.8**

*Un corps est un ensemble $E$ muni de deux opérations (ou deux lois de composition), une addition et une multiplication. Ces deux opérations doivent vérifier les propriétés suivantes :*

- *$(E,+,\times)$ est un anneau.*
- *$U(E) = E \setminus \{0\}$, i.e. : $\forall\ x \in E \setminus \{0\}, x$ a un inverse dans $E$. Si de plus la multiplication est commutative, on dit que $(E,+,\times)$ est un corps commutatif.*

**Exemples**:

- $(\mathbb{R},+,\times),(\mathbb{Q},+,\times),(\mathbb{C},+,\times)$ sont des corps commutatifs, mais $(\mathbb{Z},+,\times)$ n'est pas un corps.
- Il existe des corps non commutatifs (corps des quaternions).

**Remarques** :

- Un corps est toujours intègre.
- Les règles de calculs sont les mêmes que dans un anneau.

**Définition 13.9 (morphisme de corps)**

*Soient $(E,+,\times)$ et $(F,+,\times)$ deux corps commutatifs, et soit $f : E \to F$ une application. On dit que $f$ est un morphisme de corps lorsque :*

- *$\forall\ x,y \in E, f(x+y) = f(x)+f(y)$ et $f(xy) = f(x)f(y)$.*
- *$f(1_E) = 1_F$.*

*Un morphisme de corps est en fait un morphisme d'anneaux entre deux corps.*

**Exemples**:

- La conjugaison dans $\mathbb{C}$ est un morphisme de corps.
- La fonction $g$ de $\mathbb{R}$ vers $\mathbb{C}$ définie par $g(x) = x$ est un morphisme de corps.
- La fonction $h : \mathbb{R} \to \mathbb{R}$ définie par $h(x) = x^2$ n'est pas un morphisme de corps.

**Propriété** : un morphisme de corps est toujours injectif.

**Définition 13.10 (sous-corps d'un corps)**

*Soit $(K,+,\times)$ un corps et soit $H$ un ensemble, on dit que $H$ est un sous-corps de $K$ lorsque :*

- *$H \subset K$.*
- *$1_K \in H$.*
- *$\forall\ x,y \in H$, $x+y \in H$, $-x \in H$ et $x \times y \in H$.*
- *$\forall\ x \in H \setminus \{0\}, x^{-1} \in H$.*

*Si c'est le cas alors $(H,+,\times)$ est lui-même un corps.*

**Exemples**:

- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui est lui-même un sous-corps de $\mathbb{C}$.
- $\mathbb{Q}[i] = \{a+ib \ / \ a,b \in \mathbb{Q}\}$ est un sous-corps de $(\mathbb{C},+,\times)$.
- $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \ / \ a,b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

## III) Exercices

**★Exercice 13.1**

Dire dans les cas suivants si on définit une loi de groupe :

a) $G = ]-1;1[$ et $x * y = \frac{x+y}{1+xy}$ b) $G = \mathbb{R}$ et $x * y = \max(x,y)$.

c) $G = \mathbb{R} \setminus \{-1\}$ et $x * y = x+y+xy$. d) $G = \mathbb{R}$ et $x * y = \sqrt[3]{x^3+y^3}$.

**★Exercice 13.2**
On définit une opération $*$ dans $G = \mathbb{C}^* \times \mathbb{C}$ en posant : $\forall (a,b),\ (c,d) \in G,\ (a,b)*(c,d) = (ac, ad+b)$.

a) Montrer que $(G,*)$ est un groupe. Est-il abélien ?

b) Pour $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$, on appelle $S_{a,b}$ l'application de $\mathbb{C}$ dans $\mathbb{C}$ définie par $\forall z \in \mathbb{C},\ S_{a,b}(z) = az+b$. Montrer que $S_{a,b} \in (S_{\mathbb{C}}, \circ)$ : le groupe des permutations de $\mathbb{C}$. Montrer que l'application : $f : (G,*) \to (S_{\mathbb{C}}, \circ)$ définie par $\forall (a,b) \in G,\ f(a,b) = S_{a,b}$ est un morphisme de groupes injectif.

c) On note $\mathscr{S} = \{S_{a,b} \ / \ (a,b) \in \mathbb{C}^* \times \mathbb{C}\}$. Montrer sans calculs que $(\mathscr{S}, \circ)$ est un groupe.

**★Exercice 13.3**
Soit $H = \{(x,y,z) \in \mathbb{R}^3 \ / \ x+2y-z = 0\}$.

a) Montrer que $(H,+)$ est un groupe abélien.

b) Soit $f : H \to H$ définie par $\forall (x,y,z) \in H, f(x,y,z) = (x-2z, z-y, x-2y)$, montrer que $f$ est un morphisme de groupes, déterminer son noyau et son image.

**★Exercice 13.4**
Soit $(S_3, \circ)$ le groupe des permutations de $[\![1..3]\!]$.

a) Faire la table de $S_3$.

b) Déterminer les sous-groupes de cardinal : 1, puis 2, puis 3.

c) Soit $\tau \in S_3$ définie par $\tau(1) = 2,\ \tau(2) = 1$ et $\tau(3) = 3$. Soit $f : S_3 \to S_3$ définie par $\forall \sigma \in S_3,\ f(\sigma) = \tau \circ \sigma \circ \tau$. Montrer que $f$ est un isomorphisme de groupes.

**★Exercice 13.5**
On cherche à résoudre l'équation $x^2 - 3y^2 = 1$ d'inconnue $(x,y) \in \mathbb{N}^2$. On pose :

$$H = \{a + b\sqrt{3} \ / \ a,b \in \mathbb{Z} \text{ tels que } a^2 - 3b^2 = 1\}.$$

a) i) Montrer que $H$ est un sous-groupe de $(\mathbb{R}^*, \times)$.

ii) On note $H^+ = \{h \in H \ / \ h \geqslant 0\}$, montrer que $H^+$ est un sous-groupe de $(H, \times)$.

b) Montrer qu'il existe $a_0, b_0 \in \mathbb{N}^*$ avec $b_0$ **minimal** tel que $h_0 = a_0 + b_0\sqrt{3} \in H$. Déterminer $h_0$.

c) i) Soit $h = a + b\sqrt{3} \in H$, montrer que si $1 \leqslant h$ alors $b \geqslant 0$ et $a > 0$.

ii) En déduire que si $1 \leqslant h < h_0$, alors $h = 1$.

d) i) Soit $h \in H^+$, montrer qu'il existe $n \in \mathbb{Z}$ tel que $h_0^n \leqslant h < h_0^{n+1}$, puis montrer que $h = h_0^n$.

ii) Déduire de ce qui précède tous les éléments de $H^+$.

e) Donner alors les solutions de l'équation $x^2 - 3y^2 = 1$ dans $\mathbb{N} \times \mathbb{N}$.

**★Exercice 13.6**
Soit $(G,.)$ un groupe, on suppose que tout élément de $G \setminus \{e\}$ est d'ordre 2. Montrer que $(G,.)$ est abélien. Donner des exemples.

**★Exercice 13.7**
Sous-groupes finis de $(\mathbb{C}^*, \times)$. Soit $H$ un sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal $n \geqslant 1$, pour $x \in H$, montrer que : $\prod_{y \in H} y = \prod_{y \in H} xy$. En déduire que $x^n = 1$, puis que $H = \mathbb{U}_n$. Comment sont faits les sous-groupes finis de $(\mathbb{R}^*, \times)$ ?

**★Exercice 13.8**
Soit $(A, +, \times)$ un anneau intègre fini. Montrer que $A$ est un corps.

**★Exercice 13.9**
Morphismes de corps de $\mathbb{R}$. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps.

a) Montrer que $\forall n \in \mathbb{Z}, f(n) = n$, puis que $\forall r \in \mathbb{Q}, f(r) = r$.

b) Monter que si $x$ est positif alors $f(x)$ est positif. En déduire que $f$ est croissante.

c) Montrer que pour tout réel $x$, il existe deux suites rationnelles $(u_n)$ et $(v_n)$ telles que pour tout entier $n$ : $u_n \leqslant x \leqslant v_n$. En déduire que $f(x) = x$.

**★Exercice 13.10**

Soit $(A,+,\times)$ un anneau, un élément $x \in A$ est dit **nilpotent** lorsqu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 0$.

a) Montrer que si $a \in A$ est nilpotent, alors $1_A - a$ est inversible, donner son inverse. Calculer $(1_A - a)^k$ pour $k \in \mathbb{N}$.

b) Soient $a, b \in A$, montrer que si $a \times b$ est nilpotent, alors $b \times a$ aussi.

c) Montrer que si $a$ et $b$ sont deux éléments nilpotents qui commutent, alors $a + b$ est nilpotent. En déduire que lorsque l'anneau $A$ est commutatif, l'ensemble des éléments nilpotents de $A$ forment un groupe additif.

**★Exercice 13.11**

Théorème de Lagrange. Soit $(G,.)$ un groupe fini et $H$ un sous-groupe de $G$. On définit dans $G$ la relation suivante :

$$\forall\ x, y \in G, x \mathfrak{R} y \iff x.y^{-1} \in H.$$

Montrer que $\mathfrak{R}$ est une relation d'équivalence dans $G$. Pour $x \in G$, montrer que la classe d'équivalence de $x$ est $\text{cl}(x) = Hx = \{h.x \ / \ h \in H\}$. En déduire que $\text{card}(H) | \text{card}(G)$.