3.2 Structure d'anneau

3.2.1 Définition d'anneau

On appelle anneau, un ensemble A muni de 2 lois :

1. **Une première loi $\star$ faisant de $(A,\star)$ un groupe commutatif**
2. **Une seconde loi $\top$, interne, distributive à gauche et à droite par rapport à la loi $\star$, c'est à dire :**

$$(\forall x\in A)\,(\forall y\in A)\,(\forall z\in A)\,(x\top(y\star z)=(x\top y)\star(x\top z))$$

et

$$(\forall x\in A)\,(\forall y\in A)\,(\forall z\in A)\,((x\star y)\top z=(x\top z)\star(y\top z))$$

On dit alors que $(A,\star,\top)$ est un anneau

1. **Si la loi $\top$ est commutative, l'anneau $(A,\star,\top)$ est dit commutatif**
2. **Si la loi $\top$ admet un élément neutre, l'anneau $(A,\star,\top)$ est dit unitaire ; le neutre est noté 1**
3. **Si, pour $a\in A$ où $(A,\star,\top)$ est un anneau unitaire, il existe $a'\in A$ tel que $aa'=1$, l'élément a est dit inversible**

Remarque 8 :

Pour simplifier, nous noterons additivement $+$ la première loi $\star$ et multiplicativement $\times$ la seconde loi $\top$, de telle sorte que l'anneau $(A,\star,\top)$ devient $(A,+,\times)$

Exemple 10 :

1. $(\mathbb{Z},\star,\top)$ est un anneau commutatif et unitaire ; les seuls éléments inversibles de $(\mathbb{Z},\star,\top)$ sont 1 et -1
2. Les ensembles de polynômes $(\mathbb{R}[X],+,\times)$ et $(\mathbb{C}[X],+,\times)$ sont des anneaux unitaires
3. $\mathbb{R}^{\mathbb{R}}$ est l'ensemble des fonctions numériques réelles. On y définit :
   L'addition $(f+g)(x)=f(x)+g(x)$
   La multiplication $(f\times g)(x)=f(x)\times g(x)$
   Muni de ces opérations, $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$ est un anneau commutatif et unitaire
4. Et si nous considérons $\circ$ l'opérateur de composition des applications, alors $\left(\mathbb{R}^{\mathbb{R}},+,\circ\right)$ est un anneau unitaire non commutatif

3.2.2 Règles de calcul

Soit $(A,+,\times)$ un anneau. Alors, pour tout $a\in A$, $b\in A$ et $c\in A$:

1. $a(b-c)=ab-ac$
2. $(c-b)a=ca-ba$
3. $a\times 0=0\times a=0$
4. $a\times(-c)=-ac$
5. $(-b)a=-ba$
6. $(-a)(-b)=ab$

Démonstration

1. Soient $a\in A$, $b\in A$ et $c\in A$, alors :
$$a(b-c)+ac=a[(b-c)+c]=a(b)=ab$$
De $a(b-c)+ac=ab$, on déduit que $a(b-c)=ab-ac$
2. Soient $a\in A$, $b\in A$ et $c\in A$, alors :
$$(c-b)a+ba=[(c-b)+b]a=(c)a=ca$$
De $(c-b)a+ba=ca$, on déduit que $(c-b)a=ca-ba$

3. Pour démontrer que $a \times 0 = 0 \times a = 0$, nous faisons $b = c$ dans les identités $a\,(b-c) = ab - ac$ et $(c-b)\,a = ca - cb$
4. Pour démontrer que $a \times (-c) = -ac$, nous faisons $b = 0$ dans l'identité $a\,(b-c) = ab - ac$
5. Pour démontrer que $(-b)\,a = -ba$, nous faisons $c = 0$ dans l'identité $(c-b)\,a = ca - ba$
6. Soient $a \in A$, $b \in A$, alors nous avons :

$$(-a)\,(-b) + a\,(-b) = (-a)\,(-b) - ab$$

Or, $(-a)\,(-b) + a\,(-b) = (-a+a)\,(-b) = (0)\,(-b) = 0$
Donc : $(-a)\,(-b) + a\,(-b) = (-a)\,(-b) - ab = 0 \Longrightarrow (-a)\,(-b) = ab$

Remarque 9 :

Soit $(A, +, \times)$ un anneau. Pour $n \in \mathbb{Z}$ et $a \in A$, on peut définie a^n et na :

1. Si $n > 0$, $a^n = \underbrace{a \times a \times a \times \cdots \times a}_{n \text{ fois}}$ et $na = \underbrace{a + a + a + \cdots + a}_{n \text{ fois}}$
2. Si $n < 0$, $a^{-n} = \left(a^{-1}\right)^{-n}$ et $na = (-n)\,(-a)$

3.2.3 Définition

Soit $(A, +, \times)$ un anneau.

1. **On dit que $a \in A$ et $b \in A$, sont de véritables diviseurs de 0 si $a \neq 0$ et $b \neq 0$ et $ab = 0$**
2. **Un anneau sans diviseur de 0 est dit intègre**
3. **$a \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$**

Exemple 11 :

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux intègres

Exercice 6 :

Nous considérons $\mathbb{Z} \times \mathbb{Z}$ dans lequel nous avons défini 2 opérations :

L'addition en donnant : $(a, b) + (cd) = (a + c, b + d)$

La multiplication en donnant : $(a, b) \times (cd) = (ac, bd)$

1. Montrer que $(\mathbb{Z} \times \mathbb{Z}, +, \times)$ est un anneau
2. Cet anneau est-il intègre ? Existe-t-il des éléments nilpotents ?

Remarque 10 :

1. Si $a \in A$ est un véritable diviseur de zéro, alors a n'est pas régulier pour la multiplication, puisque si $ab = 0$ avec $a \neq 0$ et $b \neq 0$, nous avons :

$$a \times 0 = a \times b = 0 \text{ mais } b \neq 0$$

2. Si $a \in A$ est inversible, alors a n'est pas un diviseur de zéro. En effet :

$$ab = 0 \Longrightarrow a^{-1} \times ab = 0 \Longrightarrow b = 0$$

3. Dans un anneau intègre, nous avons la règle de simplification :

$$ab = ac \text{ et } a \neq 0 \Longrightarrow b = c$$

En effet, $ab = ac$ et $a \neq 0 \Longleftrightarrow a\,(b-c) = 0 \Longrightarrow b - c = 0 \Longleftrightarrow b = c$

3.2.4 Proposition

Soit $(A, +, \times)$ un anneau. Soient $x \in A$ et $y \in A$, deux éléments qui commutent, c'est à dire que $xy = yx$; alors :

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

Démonstration

Nous ne faisons pas la démonstration ; elle se fait par récurrence sur n, et nous la retrouvons dans le chapitre qui présente le raisonnement par récurrence.
Nous insistons sur l'importance que x **et** y **commutent**. En effet, si x et y ne commutent pas, nous avons, par exemple :

$$(x+y)^2 = (x+y)(x+y) = x^2 + xy + yx + y^2$$

3.2.5 Définition et théorème

Soit $(A, +, \times)$ un anneau.

1. **Un sous-ensemble $B \subset A$, non vide, est un sous-anneau de A si $(B, +, \times)$ un lui même un anneau**
2. **$B \subset A$ est un sous anneau de A si et seulement si :**
   - **B est non vide**
   - **Pour tout $x \in B$ et tout $y \in B$, $x - y \in B$ et $xy \in B$**

Démonstration

1. Supposons que B soit un sous-anneau
   Alors, $(B, +)$ étant un groupe, $0 \in B$ et donc $B \neq \emptyset$; de plus, pour tout $x \in B$ et tout $y \in B$, $x + (-y) = x - y \in B$
   Comme B est un sous anneau, ma multiplication est une loi interne, et donc pour tout $x \in B$ et tout $y \in B$, $xy \in B$
2. Réciproquement, supposons B non vide et que $(\forall x \in B)$ et $(\forall y \in B)$, $x - y \in B$ et $xy \in B$
   - Que B soit non vide et que, $(\forall x \in B)$ et $(\forall y \in B)$, $x - y \in B$, montre que $(B, +)$ est un sous-groupe de $(A, +)$
   - Que, $(\forall x \in B)$ et $(\forall y \in B)$, $xy \in B$ montre que la multiplication est interne à B
   - La multiplication étant distributive dans A, elle l'est forcément dans B

   Donc, $(B, +, \times)$ est un anneau

Remarque 11 :

1. Si $(A, +, \times)$ est un anneau commutatif et intègre, il en est de même de tout sous-anneau.
2. Pour montrer qu'un ensemble A est un anneau, il est possible de démontrer que c'est un sous-anneau d'un anneau « plus gros », contenant A
3. Les sous-anneaux de $(\mathbb{Z}, +, \times)$ sont tous du type $(n\mathbb{Z}, +, \times)$ où $n \in \mathbb{N}^*$

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

$$A(x_0) = \left\{f \in \mathbb{R}^{\mathbb{R}} \text{ telles que } f(x_0) = 0\right\}$$

Il faut montrer que $(A(x_0), +, \times)$ est un sous-anneau de $\mathbb{R}^{\mathbb{R}}$

3.2.6 Définition d'idéal

Soit $(A,+,\times)$ un anneau

1. **On appelle idéal à gauche de A, tout sous groupe $(I,+)$ de $(A,+)$ tel que :**
$$(\forall a \in A)\,(\forall i \in I)\,(a \times i \in I)$$
2. **On appelle idéal à droite de A, tout sous groupe $(I,+)$ de $(A,+)$ tel que :**
$$(\forall a \in A)\,(\forall i \in I)\,(i \times a \in I)$$
3. **Un idéal bilatère est un idéal à droite et à gauche**

Exemple 12 :

1. Si $(A,+,\times)$ est un anneau commutatif, il n'y a alors que des idéaux bilatères
2. Les idéaux de $(\mathbb{Z},+,\times)$ sont de la forme $n\mathbb{Z}$
3. Si $(A,+,\times)$ est un anneau commutatif, alors pour tout $y_0 \in A$, l'ensemble
$$y_0 \times A = \{x \in A \text{ tels qu'il existe } a \in A \text{ tel que } x = a \times y_0\}$$
est un idéal de A
4. L'ensemble $A(x_0) = \left\{f \in \mathbb{R}^{\mathbb{R}} \text{ telles que } f(x_0) = 0\right\}$ est un idéal de $\left(\mathbb{R}^{\mathbb{R}},+,\times\right)$

3.2.7 Proposition

Soit $(A,+,\times)$ un anneau
Si I et J sont 2 idéaux à gauche de A, alors $I \cap J$ est un idéal à gauche de A

Démonstration

Soient $(A,+,\times)$ un anneau et I et J 2 idéaux à gauche de A.

- Tout d'abord, $(I,+)$ et $(J,+)$ sont 2 sous-groupes de $(A,+)$ et donc $(I \cap J,+)$ est aussi un sous-groupe de $(A,+)$
- Soient $a \in A$ et $x \in I \cap J$
  — Comme $x \in I$, et que I est un idéal à gauche, alors $a \times x \in I$
  — De même, comme $x \in J$, et que J est un idéal à gauche, alors $a \times x \in J$
  Et donc, $a \times x \in I \cap J$

En conclusion, $I \cap J$ est un idéal à gauche de A

Remarque 12 :

Nous avons le même résultat pour les idéaux à droite et les idéaux bilatères.

3.2.8 Définition

Soit $(A,+,\times)$ un anneau commutatif

1. **On appelle idéal principal, tout idéal de la forme $a \times A = A \times a$; on note souvent ce type d'idéal $a \times A = A \times a = (a)$**
2. **Un anneau est dit principal si tout idéal de A est principal**

Exemple 13 :

Exemple d'anneau principal : $\mathbb{Z}$

3.2.9 Définition d'homomorphisme d'anneaux

Soient $(A, +, \times)$ et $(A_1, +, \times)$ 2 anneaux. Soit $f : A \longrightarrow A_1$ une aplication.
f est un homomorphisme d'anneaux si et seulement si, pour tout $x \in A$ et tout $y \in A$:

$$\begin{cases} f(x+y) = f(x) + f(y) \\ f(x \times y) = f(x) \times f(y) \end{cases}$$

Remarque 13 :

Le fait que, pour tout $x \in A$ et tout $y \in A$, nous ayions $f(x+y) = f(x) + f(y)$, fait de f un homomorphisme du groupe $(A, +)$ dans le groupe $(A_1, +)$

Exemple 14 :

Exemple d'homomorphisme d'anneaux :

$$\begin{cases} f : \mathbb{C} & \longrightarrow & \mathbb{C} \\ \quad z & \longmapsto & f(z) = \overline{z} \end{cases}$$

3.2.10 Théorème

1. **La composée de 2 homomorphismes d'anneaux est un homomorphisme d'anneaux**
2. **Soit $f : A \longrightarrow A_1$ un homomorphisme d'anneaux ; alors :**
   (a) $f(0) = 0$
   (b) **Pour tout $x \in A$, $f(-x) = -f(x)$**
   (c) **$f(A)$ est un sous-anneau de A_1**
   (d) **$\ker f = \{x \in A$ tel que $f(x) = 0\} = f^{-1}(\{0\})$ est un idéal bilatère de A**

Démonstration

1. On démontre que la composée de 2 homomorphismes d'anneaux est un homomorphisme d'anneaux
   Soient $(A, +, \times)$, $(A_1, +, \times)$ et $(A_2, +, \times)$ 3 anneaux.
   Soient $f : A \longrightarrow A_1$ et $g : A_1 \longrightarrow A_2$ 2 homomorphismes d'anneaux.
   g et f étant des homomorphismes de groupes, $g \circ f$ est aussi un homomorphisme de groupe et donc $g \circ f(x+y) = g \circ f(x) + g \circ f(y)$
   Regardons maintenant la multiplication ; pour tout $x \in A$ et $y \in A$, nous avons :

$$g \circ f(x \times y) = g[f(x \times y)] = g[f(x) \times f(y)] = g[f(x)] \times g[f(y)] = g \circ f(x) \times g \circ f(y)$$

   $g \circ f$ est bien un homomorphisme d'anneaux
2. Soit $f : A \longrightarrow A_1$ un homomorphisme d'anneaux
   (a) Les propriétés $f(0) = 0$ et $f(-x) = -f(x)$ pour tout $x \in A$ sont des propriétés de l'homomorphisme d egroupe
   (b) **Montrons que $f(A)$ est un sous-anneau de A_1**
   - ▷ Par les propriétés d'homomorphisme de groupe, nous savons déjà que $(f(A), +)$ est un sous-groupe de $(A_1, +)$
   - ▷ Soient $y_1 \in f(A)$ et $y_2 \in f(A)$
     Il existe alors $x_1 \in A$ et $x_2 \in A$ tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$
     A étant un anneau, $x_1 \times x_2 \in A$ et donc $f(x_1 \times x_2) \in f(A)$. f étant un homomorphisme d'anneaux, $f(x_1 \times x_2) = f(x_1) \times f(x_2) = y_1 \times y_2$ et donc, $y_1 \times y_2 \in f(A)$

   $f(A)$ est donc un sous-anneau de A_1

(c) **Montrons que** $\ker f$ **est un idéal bilatère de** A
- ▷ Comme f est un homomorphisme de groupe additif, $\ker f$ est un sous-groupoe de A
- ▷ Soit $a \in A$ et $k \in \ker f$; il faut montrer que $a \times k \in \ker f$ et $k \times a \in \ker f$
  Nous avons $f(a \times k) = f(a) \times f(k) = f(a) \times 0 = 0$ et donc $a \times k \in \ker f$
  Nous démontrerions de même que $k \times a \in \ker f$

$\ker f$ est donc un idéal bilatère de A

3.2.11 Théorème

1. **On appelle <u>isomorphisme d'anneaux</u> tout homomorphisme d'anneaux bijectif**
2. **Soient** $(A, +, \times)$ **et** $(A_1, +, \times)$ **2 anneaux et** $f : A \longrightarrow A_1$ **un isomorphisme d'anneaux ; alors** $f^{-1}A_1 :\longrightarrow A$ **est aussi un isomorphisme d'anneaux**

<u>**Démonstration**</u>

1. f est déjà un isomorphisme de groupe et $f^{-1}A_1 :\longrightarrow A$ est aussi un isomorphisme de groupe
2. Soient $y_1 \in A_1$ et $y_2 \in A_1$; il faut montrer que $f^{-1}(y_1 \times y_2) = f^{-1}(y_1) \times f^{-1}(y_2)$
   Il existe donc $x_1 \in A$ et $x_2 \in A$ uniques tels que $y_1 = f(x_1)$ et $y_2 = f(x_2)$; donc :
   $$f^{-1}(y_1 \times y_2) = f^{-1}[f(x_1) \times f(x_2)] = f^{-1}[f(x_1 \times x_2)] = x_1 \times x_2 = f^{-1}(y_1) \times f^{-1}(y_2)$$
   Ce que nous voulions

$f^{-1}A_1 :\longrightarrow A$ est donc un isomorphisme d'anneaux