Cours d'Algèbre 1 : Chapitre 4, **Structures algébriques**

1ère année Licence LMD **Informatique**

Menouer Mohammed Amine

2 septembre 2024

Chapitre 4

Structures algébriques

4.1 Loi de composition interne

Définition 1. *On appelle* ***loi de composition interne*** *(l.c.i) sur un ensemble E toute application de $E \times E$ dans E. On la note généralement par un symbole : $*, +, \cdot, \circ, \top, \perp, \ldots$:*

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\mapsto x * y \end{aligned}$$

Exemple 1.

1. *L'addition et la multiplication sont des lois de composition interne dans $\mathbb{N}$.*
2. *Pour tout ensemble E, la réunion et l'intersection sont des l.c.i dans $\mathcal{P}(E)$.*
3. *La loi $\circ$ de composition des applications est une l.c.i dans l'ensemble des applications de E dans E.*

Définition 2. *Une l.c.i $*$ dans un ensemble E est dite* ***associative*** *si, et seulement si :*

$$\forall x, y, z \in E,\ (x * y) * z = x * (y * z)$$

Exemple 2.

1. *L'addition et la multiplication dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont associatives.*
2. *La réunion et l'intersection dans $\mathcal{P}(E)$ sont associatives.*
3. *l'application :*

$$\begin{aligned} * : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (x, y) &\mapsto x * y = x - y \end{aligned}$$

n'est pas associtive car pour $2, 6, -1 \in \mathbb{R}$, on a $(2 - 6) - (-1) = -3$ et $2 - (6 - (-1)) = -5$.

Définition 3. *Une l.c.i $*$ dans un ensemble E est dite* ***commutative*** *si, et seulement si :*

$$\forall (x, y) \in E^2,\ x * y = y * x$$

Exemple 3.

1. *L'addition et la multiplication dans $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont commutatives.*
2. *La réunion et l'intersection dans $\mathcal{P}(E)$ sont commutatives.*
3. *l'application :*

$$\begin{aligned} * : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R} \\ (x, y) &\mapsto x * y = x - y \end{aligned}$$

n'est pas commutative car pour $(-5, 2) \in \mathbb{R}^2$, on a $(-5) - 2 = -7$ et $2 - (-5) = 7$.

Définition 4. *Soit E un ensemble sur lequel est définie une l.c.i $*$. On dit que $e \in E$ est un* ***élément neutre*** *pour $*$ si :*

$$\forall x \in E,\ e * x = x * e = x$$

Exemple 4.

1. *1 est l'élément neutre pour $\times$ dans $\mathbb{R}^*$.*
2. *$\varnothing$ est l'élément neutre pour $(\mathcal{P}(E), \cup)$ (l'ensemble $\mathcal{P}(E)$ muni de la loi $\cup$).*
3. *E est l'élément neutre pour $(\mathcal{P}(E), \cap)$ (l'ensemble $\mathcal{P}(E)$ muni de la loi $\cap$).*
4. *L'application identité Id_E est l'élément neutre de l'ensemble des applications de E vers E muni de la loi composition $\circ$.*

Proposition 1. *Soit E un ensemble munis d'une l.c.i $*$. Si E admet un élément neutre pour $*$ alors il est unique.*

Définition 5. *Soit E un ensemble muni d'une l.c.i $*$ et admettant $e \in E$ comme élément neutre pour $*$.*

On dit que $x \in E$ admet un ***symétrique*** *s'il existe un élément $x' \in E$ tel que :*

$$x * x' = x' * x = e$$

On dit alors que x est ***symétrisable*** *(ou inversible). On note ce symétrique x^{-1} qu'on appelle aussi* ***inverse****.*

Exemple 5.

1. *Dans $(\mathbb{R}^*, \times)$ (l'ensemble $\mathbb{R}^*$ muni de la loi $\times$) , tout élément x est symétrisable. L'inverse d'un élément $x \in \mathbb{R}^*$ est donné par $x^{-1} = \dfrac{1}{x}$.*
2. *Dans l'ensemble des applications de E dans E muni de la loi de composition $\circ$, les applications bijectives sont les seuls éléments inversibles.*
3. *Dans $(\mathcal{P}(E), \cup)$ l'élément neutre $\varnothing$ est le seul élément symétrisable.*
4. *Dans $(\mathcal{P}(E), \cap)$ l'élément neutre E est le seul élément symétrisable.*

Proposition 2. *Soit E un ensemble muni d'une loi $*$ associative et admettant un élément neutre pour $*$.*

1. *Si $x \in E$ est symétrisable alors son symétrique x^{-1} est unique.*
2. *Si $x, y \in E$ sont symétrisables, alors $x * y$ est symétrisable et on a :*

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

Définition 6. *Soit E un ensemble muni d'une loi $*$ et A un sous-ensemble de E. On dit que A est stable pour la l.c.i $*$ si :*

$$\forall x, y \in A,\ x * y \in A.$$

Exemple 6.

1. *Soit $\mathbb{N}$ muni de la loi d'addition $+$ et soit $A = \{n \in \mathbb{N}, \exists k \in \mathbb{N}, n = 2k\} \subset \mathbb{N}$. A est stable pour la l.c.i $+$. En effet pour tous entiers $n, m \in A$ on a : $n + m = 2k + 2k' = 2k'' \in A$.*
2. *Soit $\mathbb{Z}$ muni de la loi de soustraction $-$ et soit $\mathbb{N} \subset \mathbb{Z}$. $\mathbb{N}$ n'est pas stable pour la l.c.i $-$. Par contre $\mathbb{Z}$ est stable.*

Définition 7. *Soit E un ensemble muni de deux l.c.i $*$ et $\perp$. On dit que la loi $\perp$ est* ***distributive*** *par rapport à la loi $*$ si :*

$$\forall (x, y, z) \in E^3,\ x \perp (y * z) = (x \perp y) * (x \perp z) \text{ et } (y * z) \perp x = (y \perp x) * (z \perp x)$$

Exemple 7.

1. *Dans $\mathbb{C}$ la multiplication est distributive par rapport à l'addition.*
2. *L'intersection et la réunion dans $\mathcal{P}(E)$ sont distributives l'une par rapport à l'autre.*

4.2 Groupes

4.2.1 Définitions

Définition 8 (Groupe). *On dit qu'un ensemble non vide G muni d'une lci $*$ est un* ***groupe*** *si :*

1. *$*$ est associative*
2. *G admet un élément neutre pour $*$*
3. *Tout élément de G admet un symétrique pour $*$*

Si de plus la loi $*$ est commutative, on dit que $(G,*)$ est un ***groupe abélien*** *(ou* ***groupe commutatif****).*

Exemple 8.

1. *$(\mathbb{C},+)$ est un groupe abélien.*
2. *$(\mathbb{N},+)$ n'est pas un groupe car $\exists 1 \in \mathbb{N}, \forall n \in \mathbb{N},\ 1+n \neq 0$ (l'élément 1 n'a pas de symétrique).*
3. *$(\mathbb{Z}/3\mathbb{Z},+)$ est un groupe commutatif.*

   Preuve. *On définit la loi d'addition dans $\mathbb{Z}/3\mathbb{Z}$ par $\forall x,y \in \mathbb{Z},\ \bar{x}+\bar{y} = \overline{x+y}$.*
   Tout d'abord $+$ est bien une l.c.i dans $\mathbb{Z}/3\mathbb{Z}$.
   1. Soit $x,y,z \in \mathbb{Z}$, $(\bar{x}+\bar{y})+\bar{z} = \overline{x+y}+\bar{z} = \overline{(x+y)+z} = \overline{x+(y+z)} = \bar{x}+\overline{y+z} = \bar{x}+(\bar{y}+\bar{z})$, d'où $+$ est associative.
   2. Soit $x \in \mathbb{Z}$, alors $\bar{x}+\bar{0} = \bar{0}+\bar{x} = \overline{x+0} = \bar{x}$, Donc $\mathbb{Z}/3\mathbb{Z}$ admet un élément neutre qui est $\bar{0}$.
   3. Soit $x \in \mathbb{Z}$ alors $\bar{x}+\overline{-x} = \overline{-x}+\bar{x} = \overline{x-x} = \bar{0}$, donc tout élément de $\mathbb{Z}/3\mathbb{Z}$ possède un symétrique.
   Donc $(\mathbb{Z}/3\mathbb{Z},+)$ est bien un groupe.
   On remarque de plus que pour $x,y \in \mathbb{Z}$, on a : $\bar{x}+\bar{y} = \overline{x+y} = \overline{y+x} = \bar{y}+\bar{x}$, c'est à dire la loi $+$ est commutative.
   Conclusion *$(\mathbb{Z}/3\mathbb{Z},+)$ est un groupe commutatif*

Définition 9. *Si $(G,*)$ est un groupe fini, on appelle* ***ordre*** *de G, le cardinal de G.*

Exemple 9.

1. *Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe fini d'ordre n car $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\bar{1},\dots\overline{n-1}\}$.*
2. *Soit $E = \{1,2,3\}$. Les bijections de E dans lui même s'appellent les* permutations, *car les bijections de E vers E ne sont rien d'autres que des permutations, elles sont au nombre de $3! = 6$. L'ensemble des ces permutations muni de la loi de composition des permutations, forme un groupe qu'on appelle* ***groupe symétrique*** *$\mathcal{S}_3$, ou groupe des permutations $(\mathcal{S}_3,\circ)$.*

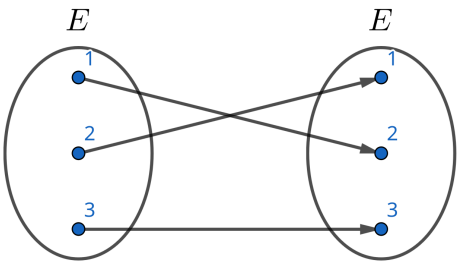

FIGURE 4.1 – Exemple d'une application bijective entre E et lui même. Si on note cette application σ, on a alors :

$$\begin{array}{ccc} \sigma(1) & \sigma(2) & \sigma(3) \\ \| & \| & \| \\ 2 & 1 & 3 \end{array}$$

ce qui signifie que cette bijection a **permuté** entre les éléments 1 et 2 pour obtenir 2, 1, 3.

Explicitons les 6 bijections (permutations) possibles entre E et lui même. Notons les par : $\sigma_i,\ i = 1,\dots 6$ et posons σ_1 l'application vue précédement. On a donc les 6 permutations du groupe $(\mathcal{S}_3,\circ)$:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\ \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\mathcal{S}_3 = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$$

4.2.2 Sous-groupes

Définition 10 (Sous-groupe)**.** *Soit $(G,*)$ un groupe d'élément neutre e et $H \subset G$. On dit que H est un sous-groupe de G si, et seulement si :*

1. $e \in H$
2. $\forall (x,y) \in H^2,\ x * y \in H$
3. $\forall x \in H,\ x^{-1} \in H$

Exemple 10.

1. *L'ensemble $2\mathbb{Z} = \{2a, a \in \mathbb{Z}\} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$, muni de la loi d'addition, est un sous-groupe de $\mathbb{Z}$.*
2. *$(\mathbb{N}, +)$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$.*

Proposition 3 (Caractérisation d'un sous-groupe)**.**
Soit $(G,*)$ un groupe et $H \subset G$, on a donc :

$$H \text{ est un sous-groupe de } G \iff \begin{cases} H \neq \varnothing \\ \forall x, y \in H,\ x * y^{-1} \in H \end{cases}$$

Propriétés 1.

1. *Un sous-groupe est un groupe.*
2. *L'intersection de sous-groupes est un sous-groupe.*
3. *La réunion de sous-groupes n'est pas nécessairement un sous-groupe.*

4.2.3 Morphisme de groupes

Définition 11 (Morphisme de groupes)**.** *Soit $(G,*)$ et $(G', \perp)$ deux groupes*

*On appelle **Morphisme** ou **Homomorphisme** de groupe toute application $f : G \longrightarrow G'$ tel que :*

$$\forall (x,y) \in G^2,\ f(x * y) = f(x) \perp f(y)$$

Exemple 11.

1. *L'application $\ln$ est un morphisme de $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$, car elle vérifie :*

$$\forall (x,y) \in \mathbb{R}_+^* \times \mathbb{R}_+^*,\ \ln(xy) = \ln x + \ln y$$

2. *L'application $|\cdot|$ est un morphisme de $(\mathbb{C}^*, \times)$ vers $(\mathbb{R}_+^*, \times)$, car elle vérifie :*

$$\forall (z, z') \in \mathbb{C}^{*2},\ |zz'| = |z||z'|$$

Définition 12. *Soit $(G,*)$ un groupe*

1. *Un morphisme de $(G,*)$ dans $(G,*)$ est appelé un **endomorphisme**.*
2. *Un morphisme bijectif est appelé un **isomorphisme**.*
3. *Un **endomorphisme** bijectif est appelé un **automorphisme**.*

Exemple 12. *L'application :*

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R}_+^* \\ x &\mapsto f(x) = \mathrm{e}^x \end{aligned}$$

est un isomorphisme du groupe $(\mathbb{R}, +)$ dans le groupe $(\mathbb{R}_+^*, \times)$.

Proposition 4.
Soit $f : (G, *) \longrightarrow (G', \perp)$ un morphisme de groupes, alors :

1. *$f(e) = e'$ (où e et e' sont, respectivement, les éléments neutres de G et G').*
2. *$\forall x \in G,\ f(x^{-1}) = (f(x))^{-1}$*
3. *Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.*
4. *Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.*

Définition 13 (Noyau-Image)**.** *Soit $f : (G, *) \longrightarrow (G', \perp)$ un morphisme de groupes.*

1. *On appelle **noyau** de f, noté $\mathrm{Ker}(f)$, l'ensemble défini par :*
$$\mathrm{Ker}(f) = \{x \in G, f(x) = e'\} = f^{-1}(\{e'\})$$
2. *On appelle **image** de f, noté $\mathrm{Im}(f)$, l'ensemble défini par :*
$$\mathrm{Im}(f) = \{y \in G', \exists x \in G, y = f(x)\} = f(G)$$

Proposition 5. *Soit $f : (G, *) \longrightarrow (G', \perp)$ un morphisme de groupes.*

1. *$\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-groupes de $(G, *)$ et $(G', \perp)$ respectivement.*
2. *f injective $\iff \mathrm{Ker}(f) = \{e\}$*
3. *f surjective $\iff \mathrm{Im}(f) = G'$*

4.3 Anneaux

4.3.1 Définitions

Définition 14 (Anneau)**.** *Soit $(A, +, \times)$ un ensemble muni de deux l.c.i.*
*On dit que $(A, +, \times)$ est un **anneau** si :*

1. *$(A, +)$ est un groupe commutatif d'élément neutre, noté 0_A.*
2. *La loi $\times$ est associative et possède un élément neutre, noté 1_A.*
3. *La loi $\times$ est distributive par rapport à la loi $+$.*

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

Exemple 13.

1. *$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(K[x], +, \times)$ sont des anneaux commutatifs.*
2. *L'ensemble E^E des application de E vers E muni de la loi additive $+$ et de la loi de composition des applications $\circ$, est un anneau non commutatif.*
3. *$(\mathbb{Z}/3\mathbb{Z}, +, \times)$ est un anneau commutatif.*

   Preuve. *On définit dans $\mathbb{Z}/3\mathbb{Z}$ la loi $\times$ par : $\forall a, b \in \mathbb{Z}/3\mathbb{Z}, \bar{a} \times \bar{b} = \overline{a \times b}$.*
   Tout d'abord $\times$ est une l.c.i dans $\mathbb{Z}/3\mathbb{Z}$.
   1. *On a déjà vu que $(\mathbb{Z}/3\mathbb{Z}, +)$ est un groupe commutatif d'élément neutre $\bar{0}$.*
   2. *Soit $a, b, c \in \mathbb{Z}$, $(\bar{a} \times \bar{b}) \times \bar{c} = \overline{(a \times b)} \times \bar{c} = \overline{(a \times b) \times c} = \overline{a \times (b \times c)} = \bar{a} \times \overline{(b \times c)} = \bar{a} \times (\bar{b} \times \bar{c})$ d'où $\times$ est associative. L'élément neutre de $\times$ est $\bar{1}$ puisque pour tout $\bar{a} \in \mathbb{Z}/3\mathbb{Z}\backslash\{\bar{0}\}, \bar{a} \times \bar{1} = \bar{1} \times \bar{a} = \overline{a \times 1} = \bar{a}$.*
   3. *Soit $a, b, c \in \mathbb{Z}$.*
   $\bar{a} \times (\bar{b} + \bar{c}) = \bar{a} \times \overline{(b + c)} = \overline{a \times (b + c)} = \overline{a \times b + a \times c} = \overline{a \times b} + \overline{a \times c} = \bar{a} \times \bar{b} + \bar{a} \times \bar{c}$
   $(\bar{b} + \bar{c}) \times \bar{a} = \overline{(b + c)} \times \bar{a} = \overline{(b + c) \times a} = \overline{b \times a + c \times a} = \overline{b \times a} + \overline{c \times a} = \bar{b} \times \bar{a} + \bar{c} \times \bar{a}$ *d'où $\times$ est distributive par rapport à $+$.*
   Donc $\mathbb{Z}/3\mathbb{Z}$ est un anneau.
   On remarque de plus que pour tout $a, b \in \mathbb{Z}$, on a : $\bar{a} \times \bar{b} = \overline{a \times b} = \overline{b \times a} = \bar{b} \times \bar{a}$, donc $\times$ est commutative.
   Conclusion : *$\mathbb{Z}/3\mathbb{Z}$ est un anneau commutatif.*

4.3.2 Règles de calculs dans un anneau

Dans un anneau $(A, +, \times)$ on a les propriétés suivantes :

1. $\forall x \in A,\ x \times 0 = 0 \times x = 0$ (on dit que 0 est absorbant pour $\times$).
2. $\forall x, y \in A,\ x \times (-y) = -(x \times y) = (-x) \times y$ et $(-x) \times (-y) = xy$, ainsi que $(-x)^n = x^n$ si n est pair et $(-x)^n = -x^n$ si n est impair, où par récurrence on obtient $x^n = x^{n-1} \times x$ sachant que $x^1 = x$.
3. $(x + y)(x + y) = x^2 + x \times y + y \times x + y^2$.
4. $(x - y) \times z = (x \times z + (-y) \times z) = (x \times z - y \times z)$.
5. $(x - y) \times (x + y) = x^2 + x \times y - y \times x - y^2$, le résultat se réduit à $x^2 - y^2$ si l'anneau est commutatif, c'est à dire : $x \times y = y \times x$.
6. Si $(A, +, \times)$ est un anneau commutatif, alors pour tout entier $n \geq 1$ et tout éléments x, y de A, on a la **formule du binôme de Newton** :

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

où $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ et par convention, $x^0 = y^0 = 1_A$. On a alors :

$$(x + y)^1 = x + y$$
$$(x + y)^2 = x^2 + 2xy + y^2$$
$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$
$$\vdots$$
$$(x + y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \binom{n}{3} x^{n-3} y^3 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

Remarquons que la somme des puissances de x et de y, qui sont en produit, est égale à n. Aussi que les puissances de x diminuent et ceux de y augmentent.

Reste à calculer les coefficients $\binom{n}{k}$, ce qui est un peu contraignant. Heureusement, on a le **Triangle de Pascal**, qui nous permet de déterminer facilement ces coefficients.

n	Les coefficients de $(x + y)^n$					
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1
$\vdots$			$\vdots$			

Chaque ligne de ce triangle détermine les coefficients d'une identitée remarquable. On a donc :

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$
$$(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$$

Prenons l'exmple de la ligne $n = 5$ qui détermine les coefficients de $(x + y)^5$.
Le premier coefficient est toujours 1.
Le deuxième coeffcient est obtenu en faisant la somme de 1 et 4 qui se trouvent sur la ligne précédente.
Le troisième coefficient 10 est obtenu en faisant la somme de 4 et 6 qui se trouvent sur la ligne précédente (voir les cellules coloriées sur le triangle), et ainsi de suite jusqu'au dernier.
Le sixième et dernier coefficient qui est toujours 1 est obtenu en faisant la somme de 1 de la ligne précédente avec rien c'est à dire avec 0.

4.3.3 Eléments inversibles

Dans un anneau $(A, +, \times)$, on cherche à déterminer les éléments qui sont inversibles pour la deuxième loi $\times$ car rien ne nous dis que tous les éléments de A sont inversibles pour $\times$ contrairement à la première loi $+$ pour laquelle tous les éléments sont inversible, car c'est une exigence dans la définition d'un groupe.

Théorème 1 (Groupe des inversibles d'un anneau)**.** *Soit $(A, +, \times)$ un anneau. L'ensemble noté $A^\times$ des éléments inversibles de A pour la loi $\times$, muni de la loi $\times$, forme un groupe appelé* ***groupe des éléments inversible*** *ou (****groupe des unités****) de A.*

Exemple 14. *$(\mathbb{Z}/6\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ sont deux anneaux d'élément neutre $\bar{0}$ pour la loi $+$ et d'élémnet neutre $\bar{1}$ pour la loi $\times$. Cherchons les éléments inversibles de $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ et $(\mathbb{Z}/5\mathbb{Z}, +, \times)$, c'est à dire $\mathbb{Z}/6\mathbb{Z}^\times$ et $\mathbb{Z}/5\mathbb{Z}^\times$.*

On va examiner les éléments de $\mathbb{Z}/6\mathbb{Z}$ un à un pour déterminer ceux qui sont inversibles.

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

Pour celà, on va mettre les éléments de $\mathbb{Z}/6\mathbb{Z}$ dans la première colonne (couleur grise) et la première ligne (couleur grise) du tableau suivant, qu'on appelle ***Tableau de multiplication*** *dans $\mathbb{Z}/6\mathbb{Z}$:*

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Avec un exmple on va expliquer le contenu du tableau. On prend le $\bar{2}$ sur la colonne grise et on le multiplie par tous les éléments. On obtient :

$$\bar{2} \times \bar{0} = \overline{2 \cdot 0} = \boxed{\bar{0}}, \quad \bar{2} \times \bar{1} = \overline{2 \cdot 1} = \boxed{\bar{2}}, \quad \bar{2} \times \bar{2} = \overline{2 \cdot 2} = \boxed{\bar{4}},$$
$$\bar{2} \times \bar{3} = \overline{2 \cdot 3} = \bar{6} = \boxed{\bar{0}}, \quad \bar{2} \times \bar{4} = \overline{2 \cdot 4} = \bar{8} = \boxed{\bar{2}}, \quad \bar{2} \times \bar{5} = \overline{2 \cdot 5} = \overline{10} = \boxed{\bar{4}}.$$

Les résultats encadrés sont les valeurs sur la ligne du $\bar{2}$ dans le tableau.

On parcours ensuite le tableau à la recherche du $\bar{1}$ (cellule en rouge). Qaund on en trouve, on regarde les élément correspondant sur la colonne grise (cellule en vert) et la ligne grise (cellule en vert), ces éléments sont les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$, car leurs produits sont égaux à l'élément neutre 1. On déduit donc :

$$\mathbb{Z}/6\mathbb{Z}^\times = \{\bar{1}, \bar{5}\}$$

avec $\bar{1}$ est son propre inverse ainsi que $\bar{5}$ est son propre inverse.

On utilise la même méthode pour $\mathbb{Z}/5\mathbb{Z}$.

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Le ***tableau de multiplication*** *dans $\mathbb{Z}/5\mathbb{Z}$ est :*

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Donc :

$$\mathbb{Z}/5\mathbb{Z}^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

avec l'inverse de $\bar{1}$ est $\bar{1}$, l'inverse de $\bar{2}$ est $\bar{3}$, l'inverse de $\bar{3}$ est $\bar{2}$ et $\bar{4}$ est son propre inverse.

4.3.4 Sous-anneaux

Définition 15 (Sous-anneau)**.** *Soit B une partie d'un anneau $(A, +, \times)$.*
On dit que B est un ***sous-anneau*** *de A si :*

1. *B est un sous-groupe de $(A, +)$.*
2. *B est stable pour la loi $\times$, c'est à dire $\forall (x, y) \in B^2,\ x \times y \in B$.*
3. *$1_A \in B$.*

Exemple 15.

1. *$\mathbb{Z}$ est un sous-anneau de l'anneau $(\mathbb{Q}, +, \times)$.*
2. *$2\mathbb{Z}$ n'est pas un sous-anneau de l'anneau $(\mathbb{Z}, +, \times)$, car $1_{\mathbb{Z}} \notin 2\mathbb{Z}$.*

Proposition 6 (Caractérisation d'un sou-anneau)**.**
Soit B une partie d'un anneau $(A, +, \times)$. B est un ***sous-anneau*** *de A si, et seulement si :*

1. *$\forall (x, y) \in B^2,\ x - y \in B$.*
2. *$\forall (x, y) \in B^2,\ x \times y \in B$.*
3. *$1_A \in B$.*

4.3.5 Anneaux intègres

Définition 16 (Diviseur de zéro)**.** *Soit $(A, +, \times)$ un anneau et $a \in A$ avec $a \neq 0_A$. On dit que :*

$$a \text{ est un } \textbf{\textit{diviseur de}}\ 0$$

s'il existe $b \in A$ avec $b \neq 0_A$ tel que

$$a \times b = 0 \quad \text{ou} \quad b \times a = 0$$

Exemple 16.

1. *$(\mathbb{Z}, +, \times)$ n'a pas de diviseurs de zéro.*
2. *Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}, \bar{3}, \bar{4}$ sont des diviseurs de zéro et $\bar{0}, \bar{1}, \bar{5}$ ne sont pas des diviseurs de zéro. Pour s'en convaincre, il suffit de reprendre le tableau de multiplication dans $\mathbb{Z}/6\mathbb{Z}$ et d'y chercher les $\bar{0}$ correspondants à des éléments non nuls :*

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Le $\bar{0}$ est concidéré comme non-diviseur de zéro, car dans la définition du diviseur de 0, on suppose que $a \neq 0_A$, et puisque $\bar{0}$ ne vérifie pas cette hypothèse, il n'est donc pas concerné par la définition.

Définition 17 (Anneau intègre)**.** *Un anneau $(A, +, \times)$ est dit* ***intègre*** *s'il est :*

1. *Commutatif.*
2. *N'admet aucun diviseur de zéro.*

Autrement dit :

$$\forall (x, y) \in A^2,\ x \times y = 0 \Longrightarrow x = 0 \text{ ou } y = 0.$$

Exemple 17.

1. *$(\mathbb{Z}, +, \times)$ est un anneau intègre.*
2. *$\mathbb{Z}/6\mathbb{Z}$ est un anneau mais qui n'est pas intègre.*

4.3.6 Idéal d'un anneau

Définition 18. *Soit $(A, +, \times)$ un anneaux commutatif. Une partie $\mathcal{I}$ de A est un **idéal** de A si :*

1. *$(\mathcal{I}, +)$ est un groupe*
2. *$\forall a \in A, \forall i \in \mathcal{I}, a \times i \in \mathcal{I}$ (propriété d'absorbtion)*

Exemple 18.

1. *$\{0_A\}$ et A sont des idéaux de A. Ils sont dits des idéaux triviaux. Les autres, s'il en existe, sont dits propres.*
2. *Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.*

Proposition 7 (Caractérisation d'un idéal)**.**

$$\mathcal{I} \text{ est un idéal de } A \iff \begin{cases} \forall i, j \in \mathcal{I},\ i - j \in \mathcal{I} \\ \forall a \in A,\ \forall i \in \mathcal{I},\ a \times i \in \mathcal{I} \end{cases}$$

4.4 Corps

4.4.1 Définitions

Définition 19 (Corps)**.** *Un ensemble K muni de deux lois $+, \times$ est appelé **corps** si :*

1. *$(K, +, \times)$ est un anneau*
2. *Tout élément de $K \backslash \{0\}$ admet un inverse pour $\times$ dans K.*

*Si de plus, $\times$ est commutative dans K, on dit que $(K, +, \times)$ est un **corps commutatif**.*

Exemple 19.

1. *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis des lois usuelles $+, \times$ sont ds corps commutatifs.*
2. *$(\mathbb{Z}, +, \times)$ n'est pas un corps, car pour $x \in \mathbb{Z}^* - \{1, -1\}$ son inverse pour la loi $\times$ est $x^{-1} = \dfrac{1}{x}$, or $\dfrac{1}{x} \notin \mathbb{Z}$.*

Proposition 8. *Tout corps commutatif est un anneau intègre.*

Exemple 20.

1. *$(\mathbb{Z}/6\mathbb{Z}, +, \times)$ n'est pas un corps car il n'est pas intègre.*
2. *$(\mathbb{Z}/3\mathbb{Z}, +, \times)$ est un corps commutatif.*
3. *Si $p \in \mathbb{N}$ est un nombre premier, alors $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps, sinon ce n'est pas un corps.*

4.4.2 Sous-corps

Définition 20 (sous-corp)**.** *Soit $(K, +, \times)$ un corps et $L \subset K$. L est dit **sous-corps** de K si :*

1. *L est un sous-anneau de K.*
2. *$\forall x \in L \backslash \{0\},\ x^{-1} \in L$.*

Proposition 9. *(Caractérisation d'un sous-corps) Un sous ensemble L de K est un sous-corps de $(K, +, \times)$ si, et seulement si :*

1. *$\forall (x, y) \in L^2,\ x - y \in L$.*
2. *$\forall (x, y) \in L^2,\ x \times y \in L$.*
3. *$1_K \in L$.*
4. *$\forall x \in L \backslash \{0\},\ x^{-1} \in L$.*

Exemple 21.

1. *$\mathbb{Q}$ est un sous-corps de $(\mathbb{R}, +, \times)$.*
2. *$\mathbb{R}$ est un sous-corps de $(\mathbb{C}, +, \times)$.*

Proposition 10. *Tout sous-corps est un corps.*

4.4.3 Morphismes d'anneaux ou de corps

Définition 21. *On appelle* ***Morphisme*** *de corps (respectivement d'anneaux) toute application du corps (respectivement de l'anneau)* $(K, +, \times)$ *dans le corps (respectivement l'anneaux)* $(L, +, \cdot)$ *tel que :*

1. $\forall (x, y) \in K^2,\ f(x + y) = f(x) + f(y)$
2. $\forall (x, y) \in K^2,\ f(x \times y) = f(x) \cdot f(y)$
3. $f(1_A) = 1_B$

Exemple 22.

1. *L'application* $z \longrightarrow \bar{z}$ *est un mophisme du corps* $(\mathbb{C}, +, \times)$ *dans lui même.*
2. *L'application* f *de* $\mathbb{Z}$ *vers* $\mathbb{N}$ *définie pour tout* $n \in \mathbb{Z}$, $f(n) = n$ *est un morphisme de l'anneaux* $(\mathbb{Z}, +, \times)$ *vers l'anneaux* $(\mathbb{R}, +, \times)$.

Remarque 1.

1. *un* ***endomorphisme*** *d'un corps* $(K, +, \times)$ *(resp. d'un anneau* $(A, +, \times)$*) est un morphisme du corps* $(K, +, \times)$ *(resp. de l'anneau* $(A, +, \times)$*) dans lui même.*
2. *Un* ***isomorphisme*** *de corps (resp. d'un anneaux) est un morphisme de corps (resp. d'un anneaux) bijectif.*
3. *Un* ***automorphisme*** *de corps (resp. d'anneaux) est un endomorphisme bijectif de corps (resp. d'anneau).*