Chapitre 4

STRUCTURES ALGEBRIQUES

4.1 Lois de Compositions Internes

Définition 4.1 *On appelle loi de composition interne (l.c.i) sur un ensemble E, toute application $\star : E \times E \longrightarrow E$.*
Un sous ensemble F de E est dit stable par rapport à la loi $\star$ si :

$$\forall\ a,\ b \in F, \quad a \star b \in F$$

Exemple 4.1 *Soit A un ensemble et $E = \mathcal{P}(A)$, alors l'intersection et la réunion d'ensembles sont deux lois de compositions internes dans E car : $\forall\, X,\ Y \in \mathcal{P}(A)$,*

1. $X \cap Y \subset X \subset A$
et on a

$$\forall\, x, \quad x \in X \cup Y \Longrightarrow \Big(x \in X\Big) \vee \Big(x \in Y\Big) \Longrightarrow \Big(x \in A\Big) \vee \Big(x \in A\Big) \Longrightarrow \Big(x \in A\Big)$$

donc
2. $X \cup Y \subset A$,
ce qui montre que "$\bigcap$" et "$\bigcup$" sont des lois de compositions internes dans $\mathcal{P}(A)$.

□

Exemple 4.2 *Soit $F = \Big\{\{a,b\},\ \{a,c\},\{b,c\}\Big\} \subset \mathcal{P}\Big(\{a,b,c\}\Big)$, alors F n'est pas stable par rapport à l'intersection et la réunion, car :*

$$\begin{array}{ll} \exists X = \{a,b\},\ Y = \{a,c\} \in F; & X \cap Y = \{a\} \notin F \\ \exists X = \{a,b\},\ Y = \{a,c\} \in F; & X \cup Y = \{a,b,c\} \notin F \end{array}$$

□

Définition 4.2 *Soient $\star$ et $\bullet$ deux lois de composition internes sur E, on dit que :*

1. *$\star$ est commutative si : $\forall\ a,\ b \in E,\ a \star b = b \star a$*

2. *$\star$ est associative si : $\forall\ a,\ b,\ c \in E,\ (a \star b) \star c = a \star (b \star c)$,*

3. $\star$ *est distributive par rapport à* $\bullet$ *si :* $\quad \forall\ a,\ b,\ c \in E,$

$$a \star (b \bullet c) = (a \star b) \bullet (a \star c) \text{ et } (b \bullet c) \star a = (b \star a) \bullet (c \star a)$$

4. $e \in E$ *est un élément neutre à gauche (respectivement à droite) de la loi* $\star$ *si*

$$\forall\ a \in E, \quad e \star a = a \quad (\text{respectivement } a \star e = a\ )$$

Si e *est un élément neutre à droite et à gauche de* $\star$ *on dit que* e *est un élément neutre de* $\star$.

Exemple 4.3 *Soit* F *un ensemble et* $E = \mathcal{P}(F)$. *On considère sur* E *les lois de composition internes " $\cap$" et " $\cup$", alors il est très facile de montrer que :*

- *" $\cap$" et " $\cup$" sont associatives*
- *" $\cap$" et " $\cup$" sont commutatives*
- $\emptyset$ *est l'élément neutre de* $\cup$
- F *est l'élément neutre de* $\cap$

□

et on a :

Propriété 4.1 $\cap$ *est distributive par rapport à* $\cup$ *et* $\cup$ *est distributive par rapport à* $\cap$

Preuve. Soient $A,\ B, C$ trois éléments de $E = \mathcal{P}(F)$, alors pour tout x, on a :

$$\begin{array}{rcl} x \in A \cap (B \cup C) & \iff & (x \in A) \wedge (x \in B \cup C) \\ & \iff & (x \in A) \wedge \Big((x \in B) \vee (x \in C)\Big) \\ & \iff & \Big((x \in A) \wedge (x \in B)\Big) \vee \Big((x \in A) \wedge (x \in C)\Big) \\ & \iff & (x \in A \cap B) \vee (x \in A \cap C) \\ & \iff & x \in (A \cap B) \cup (A \cap C) \end{array}$$

ce qui montre que :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

et comme $\cap$ est commutative, on déduit que $\cap$ est distributive par rapport à $\cup$.

De la même manière on montre la distributivité de $\cup$ par rapport à $\cap$.

□

Propriété 4.2 *Si une loi de composition interne* $\star$ *possède un élément neutre à droite* e' *et un élément neutre à gauche* e'', *alors* $e' = e''$ *et c'est un élément neutre de* $\star$.

Preuve. Soit e', respectivement e'', un élément neutre à droite, respectivement à gauche, de $\star$, alors

$$\begin{array}{ll} e' = e'' \star e' & \text{car } e'' \text{ élément neutre à gauche de } \star \\ e'' = e'' \star e' & \text{car } e' \text{ élément neutre à droite de } \star \end{array}$$

ce qui montre que $e' = e''$.

□

Remarque 4.1 *D'après cette dernière propriété, si $\star$ possède un élément neutre, alors il est unique.*

Définition 4.3 *Soit $\star$ une loi de composition interne sur un ensemble E admettant un élément neutre e. On dit qu'un élément $a \in E$ est inversible, ou symetrisable, à droite (respectivement à gauche) de $\star$ si*

$$\exists\ a' \in E, \quad a \star a' = e \quad (respectivement \quad a' \star a = e)$$

et a' est dit un inverse (ou un symétrique) à droite (respectivement à gauche) de a.
S'il existe $a' \in E$ tel que

$$a' \star a = a \star a' = e$$

on dit que a est inversible (ou symetrisable) et a' est dit un inverse (ou un symétrique) de a par rapport à $\star$.

Remarque 4.2
- *a est inversible (ou symetrisable) s'il est inversible à droite et à gauche de $\star$.*
- *Le symétrique d'un élément n'est pas toujours unique*

Exemple 4.4 *Soit $E = \{a, b, \gamma\}$, on définit une l.c.i dans E par :*

$\star$	a	b	γ
a	a	b	γ
b	b	γ	a
γ	γ	a	a

c'est à dire

$$\begin{cases} \textbf{1.} & a \star a = a, & a \star b = b, & a \star \gamma = \gamma \\ \textbf{2.} & b \star a = b, & b \star b = \gamma, & b \star \gamma = a \\ \textbf{3.} & \gamma \star a = \gamma, & \gamma \star b = a, & \gamma \star \gamma = a \end{cases}$$

On remarque que :

I. *a est l'élément neutre de $\star$.*

II. *Tous les éléments de E sont inversibles avec :*
- I) *a est l'inverse de a,*
- II) *γ est l'inverse de b*
- III) *b et γ sont des inverses de γ.*

Propriété 4.3 *Soit $\star$ une loi de composition interne dans un ensemble E admettant un élément neutre* e*, alors :*

1. *e est inversible (ou symétrisable) et son unique inverse (ou symétrique) est e.*

2. *Soit a un élément de E inversible (ou symétrisable) par rapport à la loi $\star$ et a' un inverse (ou un symétrique) de a, alors a' est inversible (ou symétrisable) et a est un inverse (ou un symétrique) de a'.*

Preuve.

1. Soit $x' \in E$, alors

$$\Big(x' \text{ est un inverse (ou un symétrique) de } e\Big) \Longleftrightarrow \Big(e \star x' = x' \star e = e\Big) \Longleftrightarrow \Big(x' = e\Big)$$

ce qui montre que le seul inverse (ou symétrique) de e est e lui même.

2. Soit $a \in E$ un élément inversible (ou symétrisable) par rapport à la loi $\star$ et soit $a' \in E$ un unverse (ou un symétrique) de a, alors

$$a \star a' = a' \star a = e$$

d'où on déduit que a' est inversible (ou sysmétrisable) par rapport à la loi $\star$ et que a est un inverse (ou un symétrique) de a'.

□

4.1.1 Unicité de l'inverse (du symétrique)

Propriété 4.4 *Soit $\star$ une loi de composition interne dans E, associative et admettant un élément neutre e. Si un élément $x \in E$ admet x_1 un inverse (ou symétrique) à droite et x_2 un inverse (ou symétrique) à gauche, alors x_1 et x_2 sont identiques.*

Preuve. Soient x_1 un inverse (ou un symétrique) à droite de x et x_2 un inverse (ou un symétrique) à gauche de x, alors

$$x \star x_1 = e \quad et \quad x_2 \star x = e$$

donc

$$\begin{array}{rcll} x_1 & = & e \star x_1 & \\ & = & (x_2 \star x) \star x_1 & \\ & = & x_2 \star (x \star x_1) & \text{car } \star \text{ est associative} \\ & = & x_2 \star e & \\ & = & x_2 & \end{array}$$

□

Remarque 4.3

- *De cette propriété on déduit que l'associativité de la loi assure l'unicité du symétrique d'un élément s'il existe*
- *D'après cette propriété on déduit que la loi définie dans l'exemple 4.4 n'est pas associative. Pour s'en convaincre, on remarque que :*

$$(b \star b) \star \gamma = \gamma \star \gamma = a \quad et \quad b \star (b \star \gamma) = b \star a = b$$

donc

$$(b \star b) \star \gamma \neq b \star (b \star \gamma)$$

ce qui montre que la loi $\star$ n'est pas associative.

Conventions : Etant donnée une loi de composition interne associative dans un ensemble E,
- Si la loi est notée $+$, son élément neutre est noté 0_E ou 0, et on parle du symétrique de a qu'on note $a' = -a$.
- Si la loi est notée multiplicativement, son élément neutre est noté 1_E ou 1, et on parle de l'inverse de a qu'on note $a' = a^{-1}$.

Avec ces conventions, si e est l'élément neutre d'une loi de composition interne $\star$ dans un ensemble E, alors

$$\boxed{e^{-1} = e \qquad (\text{ou } -e = e)}$$

et on a : $\forall\, a,\ a' \in E$,

$$\boxed{\Big(a' = a^{-1} \Longleftrightarrow a' \star a = a \star a' = e\Big) \quad ou \quad \Big(a' = -a \Longleftrightarrow a' + a = a + a' = e\Big)}$$

Propriété 4.5 *Soit $\star$ une loi de composition interne dans un ensemble E, associative et admettant un élément neutre* e*, alors si a et b sont deux éléments inversibles (symétrisables) il en sera de même de $(a \star b)$ et on a :*

$$\boxed{(a \star b)^{-1} = b^{-1} \star a^{-1}}$$

Preuves : Soient $a,\ b \in E$ deux éléments inversibles, alors

$$\begin{array}{rcll} (a \star b) \star (b^{-1} \star a^{-1}) & = & (a \star (b \star b^{-1})) \star a^{-1} & (\text{car } \star \text{ est associative.}) \\ & = & (a \star e) \star a^{-1} & \\ & = & a \star a^{-1} & \\ & = & e & \end{array}$$

De la même manière on montre que

$$(b^{-1} \star a^{-1}) \star (a \star b) = e$$

d'où on déduit que $(a \star b)$ est inversible et que

$$(a \star b)^{-1} = b^{-1} \star a^{-1}$$

□

Définition 4.4 *Soit $\star$ une loi de composition interne dans un nesemble E. On dit qu'un élément $r \in E$ est régulier à droite (respectivement à gauche) de $\star$ si*

$$\forall b,\ c \in E, \quad b \star r = c \star r \Longrightarrow b = c$$

$$\Big(respectivement\ \ \forall b,\ c \in E, \quad r \star b = r \star c \Longrightarrow b = c\Big)$$

Si r est un élement régulier à droite et à gauche de $\star$, on dit que r est un élément régulier de $\star$ dans E.

Exemple 4.5 *Soient F un ensemble et $E = \mathcal{P}(F)$, alors $\emptyset$ est une élément régulier pour la réunion dans E et F est un élément régulier pour l'intersection dans E.*

Propriété 4.6 *Soit $\star$ une loi de composition interne associative admettant un élément neutre e dans E, alors tout élément symétrisable dans $(E, \star)$ est régulier.*

Preuve. Soit $x \in E$ un élément symétrisable dans E, alors x^{-1} existe et pour tous a et b dans E, on a :

$$\begin{array}{rcl} a \star x = b \star x & \Longrightarrow & (a \star x) \star x^{-1} = (b \star x) \star x^{-1} \\ & \Longrightarrow & a \star (x \star x^{-1}) = b \star (x \star x^{-1}) \quad \text{car } \star \text{ est associative} \\ & \Longrightarrow & a \star e = b \star e \\ & \Longrightarrow & a = b \end{array}$$

Ce qui montre que x est régulier à droite de $\star$.
De la même manière on montre que x est régulier à gauche de $\star$.

□

Remarque 4.4 *Si x est symétrisable à droite, respectivement à gauche, alors x est régulier à droite, respectivement à gauche de $\star$.*

4.2 Structure de Groupe

Définition 4.5 *On appelle groupe, tout ensemble non vide G muni d'un loi de composition interne $\star$ tel que :*

1. *$\star$ est associative ;*
2. *$\star$ possède un élément neutre e ;*
3. *Tout élément de E est symetrisable.*

Si de plus $\star$ est commutative, on dit que $(G, \star)$ est un groupe commutatif, ou groupe Abélien[1]

Exemple 4.6 *Un exemple illustratif de groupe abélien est $(\mathbb{Z}, +)$.*

Exemple 4.7 *On définit l'opération $\star$ par :*

$$\forall\, x,\ y \in]-1, 1[, \quad x \star y = \frac{x + y}{1 + xy}$$

Montrer que $\Big(]-1, 1[, \star\Big)$ est un groupe abélien.

1) *$\star$ est une loi de composition interne dans $]-1, 1[$.*
Soient $x,\ y \in]-1, 1[$, alors

$$\Big(|x| < 1\Big) \wedge \Big(|y| < 1\Big)$$

[1] **ABEL Niels Henrik** : Mathématicien norvégien (île de Finnøy 1802-Arendal 1829). Algébriste, il créa la théorie des fonctions elliptiques. Il est mort de tuberculose.

donc

$$\Big(|xy| = |x|\,|y| < 1\Big)$$

par suite

$$1 + xy > 1 - |xy| > 0$$

Ainsi

$$\begin{array}{rcl}
\forall\, x,\ y \in]-1,1[, \quad \left|\dfrac{x+y}{1+xy}\right| < 1 & \Longleftrightarrow & \dfrac{|x+y|}{|1+xy|} < 1 \\
& \Longleftrightarrow & |x+y| < |1+xy| \\
& \Longleftrightarrow & |x+y| < 1+xy \quad car \ \ 1+xy > 0 \\
& \Longleftrightarrow & -(1+xy) < x+y < 1+xy \\
& \Longleftrightarrow & \begin{cases} x+y-1-xy < 0 \\ x+y+1+xy > 0 \end{cases} \\
& \Longleftrightarrow & \begin{cases} x(1-y)+y-1 < 0 \\ x(1+y)+y+1 > 0 \end{cases} \\
& \Longleftrightarrow & (*) \begin{cases} (1-y)(x-1) < 0 \\ (1+y)(x+1) > 0 \end{cases}
\end{array}$$

comme $-1 < x,\ y < 1$, *alors*

$$\Big(1-y>0\Big) \wedge \Big(x-1<0\Big) \qquad et \qquad \Big(1+y>0\Big) \wedge \Big(x+1>0\Big)$$

donc

$$\Big(\,(1-y)(x-1)<0\,\Big) \wedge \Big(\,(1+y)(x+1)>0\Big),$$

d'où on déduit que $(*)$ *est vraie pour tous* $x,\ y \in]-1,1[$, *par suite :*

$$\forall\, x,\ y \in]-1,1[, \qquad |x \star y| = \left|\frac{x+y}{1+xy}\right| < 1$$

ce qui montre que $\star$ *est une loi de composition interne dans* $]-1,1[$.

2) $\star$ *est commutative.*
D'après la commutativité de l'addition et de la multiplication dans $\mathbb{R}$ *on a :*

$$\forall\, x,\ y \in]-1,1[, \qquad x \star y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y \star x$$

ce qui montre que $\star$ *est commutative.*

3) $\star$ *est associative.*

Soient $x,\ y,\ z \in]-1,1[$, *alors*

$$\begin{aligned}(x\star y)\star z &= \frac{(x\star y)+z}{1+(x\star y)z} = \frac{\dfrac{x+y}{1+xy}+z}{1+x\dfrac{x+y}{1+xy}z}\\ &= \frac{\dfrac{(x+y)+z(1+xy)}{1+xy}}{\dfrac{(1+xy)+(x+y)z}{1+xy}} = \frac{(x+y)+z(1+xy)}{(1+xy)+(x+y)z}\\ &= \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

et on a :

$$\begin{aligned}x\star(y\star z) &= \frac{x+(y\star z)}{1+x(y\star z)} = \frac{x+\dfrac{y+z}{1+yz}}{1+x\dfrac{y+z}{1+yz}}\\ &= \frac{\dfrac{x(1+yz)+(y+z)}{1+yz}}{\dfrac{(1+yz)+x(y+z)}{1+yz}} = \frac{x(1+yz)+(y+z)}{(1+yz)+x(y+z)}\\ &= \frac{(x+xyz)+(y+z)}{(1+yz)+(xy+xz)} = \frac{x+y+z+xyz}{1+xy+xz+yz}\end{aligned}$$

en comparant les deux expressions on obtient :

$$\forall\, x,\ y,\ z \in]-1,1[, \qquad (x\star y)\star z = x\star(y\star z)$$

d'où on déduit que $\star$ *est associative.*

4) $\star$ *admet un élément neutre.*
Soit $e \in \mathbb{R}$, *alors*

$$\Big(e \text{ élément neutre de } \star\Big) \Longleftrightarrow \Big(\forall\, x \in]-1,1[, \quad e\star x = x\star e = x\Big)$$

comme $\star$ *est commutative et*

$$\begin{aligned}x\star e = x &\Longleftrightarrow \frac{x+e}{1+xe} = x\\ &\Longleftrightarrow x+e = x+x^2e\\ &\Longleftrightarrow e = x^2e\\ &\Longleftrightarrow e(1-x^2) = 0\\ &\Longleftrightarrow \Big(e=0\Big)\vee(x=\mp 1)\end{aligned}$$

on déduit que $e = 0 \in]-1,1[$ *est l'élément neutre de* $\star$.

5) *Tout élément de* $]-1,1[$ *est symétrisable.*
Soient $x \in]-1,1[$ *et* $x \in \mathbb{R}$*, alors*

$$\begin{array}{rcl} x \star x' = e & \Longleftrightarrow & \dfrac{x+x'}{1+xx'} = 0 \\ & \Longleftrightarrow & x + x' = 0 \\ & \Longleftrightarrow & x' = -x \end{array}$$

comme $\star$ *est commutative on déduit que tout élément* $x \in]-1,1[$ *est symétrisable et son symétrique est* $x' = -x \in]-1,1[$.

De **1)**, **2)**, **3)**, **4)** *et* **5)** *on déduit que* $\Big(]-1,1[, \star\Big)$ *est un groupe abélien.*

□

4.2.1 Groupes à deux éléments

Soit $G = \{a, b\}$ un ensemble à deux éléments, définir toutes les lois de composition internes dans G qui lui confèrent une structure de groupe.

Soit $\star$ une loi de composition sur G, alors pour que $(G, \star)$ soit un groupe il faut que $\star$ soit interne dans G et admette un élément neutre qui peut être a ou b, donc $\star$ doit être définie de la sorte :

1. Si a est l'élément neutre de $\star$, alors
- $a \star a = a$
- $a \star b = b$
- $b \star a = b$

reste à définir $b \star b$, or pour que $(G, \star)$ soit un groupe il faut que tout élément soit inversible, en particulier il faut trouver b^{-1}. Si on pose $b \star b = b$, alors on remarque que

$$\forall x \in G, \qquad b \star x \neq a$$

donc b ne sera pas inversible, ce qui nous amène à poser
- $b \star b = a$

Ainsi, on a défini une l.c.i. dans G avec un élément neutre a, reste à voir si la loi ainsi définie est associative. On a :
- $(a \star a) \star a = a \star a = a \star (a \star a)$
- $(a \star a) \star b = a \star b = a \star (a \star b)$
- $(a \star b) \star a = b \star a = a \star b = a \star (b \star a)$
- $(a \star b) \star b = b \star b = a = a \star a = a \star (b \star b)$

En remarquant que la loi est commutative on déduit que
- $(b \star a) \star a = b \star (a \star a)$
- $(b \star a) \star b = b \star (a \star b)$

ce qui montre que

$$\forall\, x,\ y,\ z \in G, \quad x \star (y \star z) = (x \star y) \star z$$

donc $\star$ est associative dans G, et par suite $(G, \star)$ est un groupe.

2. Si b est l'élément neutre de $\star$, alors de la même manière on construit la loi $\star$ comme suit :

- $b \star b = b$
- $b \star a = a$
- $a \star b = a$
- $a \star a = b$

D'après ce qui précède : Il existe deux groupes à deux éléments et formellement on les définit ainsi :

$\star$	a	b
a	a	b
b	b	a

et

$\star$	a	b
a	b	a
b	a	b

□

4.2.2 Sous groupes

Définition 4.6 *Soit $(G, \star)$ un groupe, on appelle sous groupe de $(G, \star)$ tout sous ensemble non vide G' de G tel que la restriction de $\star$ à G' en fait un groupe.*

Comme $\star$ est associative dans G alors sa restriction à G' est aussi associative, par suite $G' \neq \emptyset$ est un sous groupe de $(G, \star)$ s'il est stable par rapport à $\star$ et à l'opération inversion, c'est à dire :

$$\begin{cases} (i) & G' \neq \emptyset \\ (ii) & \forall\, a,\ b \in G', \quad a \star b \in G' \\ (iii) & \forall\, a \in G', \quad a^{-1} \in G' \end{cases}$$

Il est claire que si $(G, \star)$ est un groupe, alors G est un sous groupe de G.

Propriété 4.7 *Soient $(G, \star)$ un groupe et $G' \subset G$, alors*

$$G' \text{ est un sous groupe de } G' \Longleftrightarrow \begin{cases} G' \neq \emptyset, \\ \forall\ a,\ b \in G', \quad a \star b^{-1} \in G' \end{cases}$$

Preuve :

1. Soit G' un sous groupe de $(G, \star)$, alors :

i) $\star$ a un élément neutre dans G', donc $G' \neq \emptyset$.

ii) Soient $a,\ b \in G'$, comme G' muni de la restriction de $\star$ est un groupe alors b^{-1} existe dans G' et comme G' est stable par rapport à $\star$ on déduit que $a \star b^{-1} \in G'$.

2. Inversement, soit G' un sous ensemble de G tel que $\begin{cases} G' \neq \emptyset, \\ \forall\ a,\ b \in G', \quad a \star b^{-1} \in G' \end{cases}$

Montrons que G' muni de la restriction de $\star$ est un groupe.

i) Comme $G' \neq \emptyset$ alors il existe $a \in G'$ et d'après la deuxième hypothèse

$$e = a \star a^{-1} \in G',$$

ce qui montre que *la restriction de $\star$ admet un élément neutre e dans G'.*

ii) Soit $x \in G'$, comme $e \in G'$ alors d'après la deuxième hypothèse on aura

$$x^{-1} = e \star x^{-1} \in G'$$

ce qui montre que tout élément x de G' est inversible dans G' par rapport à la restriction de $\star$ à G'.

iii) La restriction de $\star$ à G' est une loi de composition interne, car pour tous x et y dans G', d'après ii) on a

$$y^{-1} \in G'$$

et en utilisant la deuxième hypothèse on déduit que

$$x \star y = x \star (y^{-1})^{-1} \in G'$$

iv) La restriction de $\star$ à G' est associative, car $\star$ est associative dans G.

□

Remarque 4.5 *D'après* i) *de la preuve de la proposition précédente, on voit que : Si e est l'élément neutre d'un groupe $(G, \star)$, alors tout sous groupe de G contient e et on déduit la propriété suivante.*

Propriété 4.8 *Soient $(G, \star)$ un groupe, e l'élément neutre de $\star$ et G' un sous ensemble de G, alors G' est un sous groupe de G si et seulement si :* $\begin{cases} e \in G' \\ \forall\, x,\ y \in G', \quad x \star y^{-1} \in G'. \end{cases}$

Exemple 4.8 *Soit $(G, \star)$ un groupe et $G' = \{x \in G; \quad (\forall y \in G,\ x \star y = y \star x)\}$, alors G' est un sous groupe de G.*

En effet,

i) Si e est l'élément neutre de $\star$, alors $e \in G'$ car :

$$\forall y \in G, \qquad e \star y = y \star e = y$$

ii) Soient $x,\ y \in G'$, alors

$$\begin{array}{lrcll} \forall z \in G, & (x \star y^{-1}) \star z & = & (x \star y^{-1}) \star (z^{-1})^{-1} & \\ & & = & x \star (y^{-1} \star (z^{-1})^{-1}) & car \star \text{ est associative} \\ & & = & x \star (z^{-1} \star y)^{-1} & \\ & & = & x \star (y \star z^{-1})^{-1} & car\ y \in G' \\ & & = & x \star ((z^{-1})^{-1} \star y^{-1}) & \\ & & = & x \star (z \star y^{-1}) & \\ & & = & (x \star z) \star y^{-1} & car \star \text{ est associative} \\ & & = & (z \star x) \star y^{-1} & car\ x \in G' \\ & & = & z \star (x \star y^{-1}) & car \star \text{ est associative} \end{array}$$

ce qui montre que $x \star y^{-1} \in G'$.

De i) et ii) on déduit que G' est un sous groupe de G.

□

Remarque 4.6 *Sachant que si e est l'élément neutre d'un groupe $(G,\star)$, alors il commute avec tous les éléments de G, de l'exemple précédent on déduit que si e est l'élément neutre d'un groupe $(G,\star)$, alors :*

$$\{e\} \text{ est un sous groupe de } G.$$

Définition 4.7 *Soit $(G,\star)$ un groupe, on dit que G' est un sous groupe propre de G si $G' \neq \{e\}$ et $G' \neq G$.*

Exemple 4.9 *Soit $n \in \mathbb{N}$, alors $n\mathbb{Z} = \{n.p\,;\quad p \in \mathbb{Z}\}$ est un sous groupe de $\mathbb{Z}$.*
En effet :

i) $0 \in n\mathbb{Z}$, *car :* $\exists p = 0 \in \mathbb{Z}$; $\quad 0 = n.p$.

ii) Soient $x,\ y \in n\mathbb{Z}$, alors il existe $p_1,\ p_2 \in \mathbb{Z}$ tels que $x = n.p_1$ et $y = n.p_2$, donc

$$x - y = n.p_1 - n.p_2 = n.(p_1 - p_2) = n.p \in n\mathbb{Z}$$

par suite

$$\forall\, x,\ y \in n\mathbb{Z}, \qquad x - y \in n\mathbb{Z}$$

De i) et ii) on déduit que $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.

Pour $n \in \mathbb{N}\backslash\{0,1\}$, $n\mathbb{Z}$ est un sous groupe propre de $\mathbb{Z}$.

□

4.2.3 Goupes Quotients

Soient $(G,\star)$ un groupe et G' un sous groupe de G. On définit une relation binaire $\mathcal{R}$ sur G par :

$$\forall\ a,\ b \in G, \quad a\mathcal{R}b \Longleftrightarrow a \star b^{-1} \in G'$$

Propriété 4.9 *$\mathcal{R}$ est une relation d'équivalence sur G.*

Preuve :
i) $\mathcal{R}$ est Reflexive, car : $\forall x \in G$, comme G' est un sous groupe de G, alors $x\star x^{-1} = e \in G'$, donc

$$\forall\, x \in G, \quad x\mathcal{R}x$$

ii) $\mathcal{R}$ est Symétrique, car : $\forall\, x,\ y \in G$,

$$\begin{array}{rcl} x\mathcal{R}y & \Longleftrightarrow & x \star y^{-1} \in G' \\ & \Longrightarrow & (x \star y^{-1})^{-1} \in G' \\ & \Longrightarrow & y \star x^{-1} \in G' \\ & \Longrightarrow & y\mathcal{R}x \end{array}$$

iii) $\mathcal{R}$ est Transitive, car : $\forall\, x,\ y\ z \in G$,

$$\begin{array}{rcll}(x\mathcal{R}y)\wedge(y\mathcal{R}z) & \Longleftrightarrow & [(x\star y^{-1})\in G']\wedge[(y\star z^{-1})\in G'] & \\ & \Longrightarrow & (x\star y^{-1})\star(y\star z^{-1})\in G', & \text{car } G' \text{ est un sous groupe}\\ & \Longrightarrow & (x\star(y^{-1}\star y)\star z^{-1})\in G', & \text{car } \star \text{ est associative}\\ & \Longrightarrow & (x\star z^{-1})\in G' & \\ & \Longrightarrow & x\mathcal{R}z & \end{array}$$

De i), ii) et iii) on déduit que $\mathcal{R}$ est une relation d'équivalence.

□

On note $G_{/G'}$ l'ensemble quotient $G_{/\mathcal{R}}$. On définit sur $G_{/G'}\times G_{/G'}$ l'opération $\oplus$ par :

$$\forall\ (\dot{a},\ \dot{b})\in G_{/G'}\times G_{/G'},\quad \dot{a}\oplus\dot{b}=\dot{\overline{a\star b}}$$

Propriété 4.10 *Si $\star$ est commutative, alors $\oplus$ est une loi de composition interne dans $G_{/G'}$.*

Preuve : Ceci revient à montrer que $\oplus$ est une application de $G_{/G'}\times G_{/G'}$ dans $G_{/G'}\times G_{/G'}$.
Soient $(\dot{a},\dot{b})$ et $(\dot{c},\dot{d})\in G_{/G'}$, alors

$$\begin{array}{rcl}(\dot{a},\dot{b})=(\dot{c},\dot{d}) & \Longrightarrow & (\dot{a}=\dot{c})\wedge(\dot{b}=\dot{d})\\ & \Longrightarrow & \Big(a\mathcal{R}c\Big)\wedge\Big(b\mathcal{R}d\Big)\\ & \Longrightarrow & \Big(a\star c^{-1}\in G'\Big)\wedge\Big(b\star d^{-1}\in G'\Big)\end{array}$$

Montrons que

$$(\dot{a},\dot{b})=(\dot{c},\dot{d})\Longrightarrow \dot{a}\oplus\dot{b}=\dot{c}\oplus\dot{d}\ .$$

Supposons que $(\dot{a},\dot{b})=(\dot{c},\dot{d})$, alors : $\forall x\in G$,

$$\begin{array}{rcll}x\in\dot{a}\oplus\dot{b} & \Longleftrightarrow & x\in\dot{\overline{a\star b}} & \\ & \Longleftrightarrow & x\mathcal{R}(a\star b) & \\ & \Longleftrightarrow & x\star(a\star b)^{-1}\in G' & \\ & \Longleftrightarrow & x\star(b^{-1}\star a^{-1})\in G' & \\ & \Longrightarrow & (x\star(b^{-1}\star a^{-1}))\star(a\star c^{-1})\in G', & \text{Car } G' \text{ sous-groupe}\\ & \Longrightarrow & ((x\star b^{-1})\star(a^{-1}\star a)\star c^{-1})\in G', & \text{Car } \star \text{ associative}\\ & \Longrightarrow & ((x\star b^{-1})\star c^{-1})\in G' & \\ & \Longrightarrow & ((x\star b^{-1})\star c^{-1})\star(b\star d^{-1})\in G', & \text{Car } G' \text{ sous-groupe}\\ & \Longrightarrow & (x\star(b^{-1}\star b)\star(c^{-1}\star d^{-1}))\in G', & \text{Car } \star \text{ est commutative et associative}\\ & \Longrightarrow & (x\star(c^{-1}\star d^{-1}))\in G' & \\ & \Longrightarrow & (x\star(d\star c)^{-1})\in G' & \\ & \Longrightarrow & x\mathcal{R}(d\star c) & \\ & \Longrightarrow & x\mathcal{R}(c\star d), & \text{car } \star \text{ commutative}\\ & \Longrightarrow & x\in\dot{c}\oplus\dot{d} & \end{array}$$

donc

$$\dot{a} \oplus \dot{b} \subset \dot{c} \oplus \dot{d}$$

et de la même manière on montre que

$$\dot{c} \oplus \dot{d} \subset \dot{a} \oplus \dot{b}$$

par suite :

$$(\dot{a}, \dot{b}) = (\dot{c}, \dot{d}) \Longrightarrow \dot{a} \oplus \dot{b} = \dot{c} \oplus \dot{d}$$

ce qui montre que la loi $\oplus$ est interne dans $G_{/G'}$.

□

Propriété 4.11 *Si $(G, \star)$ est un groupe abélien, alors $(G_{/G'}, \oplus)$ est un groupe abélien, appelé groupe quotient de G par G'.*

Preuve :

i) $\oplus$ est associative car : $\forall\, \dot{x},\ \dot{y}\ \dot{z} \in G_{/G'}$,

$$\begin{aligned} \dot{x} \oplus (\dot{y} \oplus \dot{z}) &= \dot{x} \oplus \dot{\overline{x + y}} \\ &= \dot{\overline{x \star (\dot{y} \star z)}} \\ &= \dot{\overline{(x \star \dot{y}) \star z}} \text{Car } \star \text{ est associative} \\ &= \dot{\overline{(x \star y)}} \oplus \dot{z} \end{aligned}$$

donc :

$$\forall\, x,\ y\ z \in G_{/G'}, \quad \dot{x} \oplus (\dot{y} \oplus \dot{z}) = \dot{\overline{(x \star y)}} \oplus \dot{z}$$

ii) Si e est l'élément neutre de $\star$, alors $\dot{e}$ est l'élément neutre de $\oplus$, car : $\forall\, \dot{x} \in G_{/G'}$,

$$\dot{x} \oplus \dot{e} = \dot{\overline{x \star e}} = \dot{x}$$
$$\dot{e} \oplus \dot{x} = \dot{\overline{e \star x}} = \dot{x}$$

iii) Soit $\dot{x} \in G_{/G'}$ alors $(\dot{x})^{-1} = \dot{\overline{x^{-1}}}$, car

$$\dot{x} \oplus \dot{\overline{x^{-1}}} = \dot{\overline{x \star \dot{x^{-1}}}} = \dot{e}$$
$$\dot{\overline{x^{-1}}} \oplus \dot{x} = \dot{\overline{x^{-1} \star x}} = \dot{e}$$

iv) $\oplus$ est commutative car $\star$ est commutative.

De i), ii), iii) et iv), on déduit que $\left(G_{/G'}, \oplus\right)$ est un groupe abélien

□

Exemple 4.10 *On sait que dans le groupe commutatif $(\mathbb{Z}, +)$; pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous sous groupe de $\mathbb{Z}$, donc on peut parler du groupe quotient $\mathbb{Z}_n = \mathbb{Z}\Big|_{n\mathbb{Z}}$.*

4.2.4 Homomorphismes de Groupes

Dans ce paragraphe, on considère $(G, \bullet)$ et $(H, \star)$ deux groupes, avec e et h leurs éléments neutres respectifs.

Définition 4.8 *Une application $f : G \longrightarrow H$ est appelée homomorphisme de groupes de G dans H si :*

$$\forall\ a,\ b \in G, \quad f(a \bullet b) = f(a) \star f(b).$$

- Si f est bijective, on dit que f est un isomorphisme (de groupes) de G sur H. On dit alors que G est isomorphe à H, ou que G et H sont isomorphes.

- Si $G = H$, on dit que f est un endomorphisme de G, et si de plus f est bijective, on dit que f est un automorphisme (de groupe) de G.

Exemple 4.11 *Etant donnés les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \cdot)$, alors les applications*

$$\begin{array}{rccc} f: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^*,\cdot) \\ & x & \longrightarrow & \exp x \end{array} \qquad et \qquad \begin{array}{rccc} g: & (\mathbb{R}^*,\cdot) & \longrightarrow & (\mathbb{R},+) \\ & x & \longrightarrow & \ln|x| \end{array}$$

Définition 4.9 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes. On appelle noyau de f l'ensemble*

$$\mathrm{Ker}\, f = f^{-1}(\{h\}) = \{a \in G;\ f(a) = h\}$$

et l'image de f l'ensemble

$$\Im m f = f(G) = \{f(a),\ a \in G\ \}.$$

Propriété 4.12 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors*

1. $f(e) = h$
2. $\forall\ a \in G,\ (f(a))^{-1} = f(a^{-1})$

Preuve :

1. h étant l'élément neutre de $\star$ et e celui de $\bullet$, alors

$$f(e + e) = f(e) = h \star f(e)$$

et comme f est un homomorphisme on déduit que

$$h \star f(e) = f(e) \star f(e)$$

et comme tous les éléments du groupe $(H, \star)$ sont réguliers, on déduit que $h = f(e)$.

2. Soit $a \in G$ et montrons que $f(a^{-1})$ est l'inverse de $f(a)$ dans le groupe $(H, \star)$.
f étant un homomorphisme de groupe alors

$$f(a) \star f(a^{-1}) = f(a \bullet a^{-1}) = f(e) \quad et \quad f(a^{-1}) \star f(a) = f(a^{-1} \bullet a) = f(e)$$

sachant que $f(e) = h$, d'après la première propriété, on déduit que $(f(a))^{-1} = f(a^{-1})$.

□

Remarque 4.7 *De la première propriété on déduit que $e \in \ker f$.*

Propriété 4.13 *Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors*

1. *L'image d'un sous groupe de G est un sous groupe de H.*
2. *L'image réciproque d'un sous groupe de H est un sous groupe de G.*

Preuve :

1. Soit G' un sous groupe de G et montrons que $f(G')$ vérifie les deux conditions de la caractérisation des sous groupes.

i) Comme G' est un sous groupe de G, alors $e \in G'$ donc $f(e) \in f(G')$, par suite $f(G') \neq \emptyset$.

ii) Soient $a,\ b \in f(G')$, alors il existe $x,\ y \in G'$ tels que $a = f(x)$ et $b = f(y)$, donc d'après la deuxième propriété on aura

$$a \star b^{-1} = f(x) \star (f(y))^{-1} = f(x) \star f(y^{-1}) = f(x \bullet y^{-1})$$

et comme G' est un sous groupe de G alors $(x \bullet y^{-1}) \in G'$, par suite

$$a \star b^{-1} = f(x \bullet y^{-1}) \in f(G')$$

de i) et ii) on déduit que $f(G')$ est un sous groupe de H.

2. Soit H' un sous groupe de H, alors

i) D'après la première propriété $f(e) = h$ et comme H' est un sous groupe de H alors $h \in H'$ donc $e \in f^{-1}(H')$.

ii) Soient $x,\ y \in f^{-1}(H')$, alors $f(x),\ f(y) \in H'$ et comme H' est un sous groupe de G alors $f(x) \star (f(y))^{-1} \in H'$ et de la deuxième propriété on déduit que

$$f(x \bullet y^{-1}) = f(x) \star f(y^{-1}) = f(x) \star (f(y))^{-1} \in H'$$

ce qui montre que $(x \bullet y^{-1}) \in f^{-1}(H')$.
De i) et ii) on déduit que $f^{-1}(H')$ est un sous groupe de G.

□

Remarque 4.8 *Comme cas particuliers des propriétés,*

$\Im m f$ *est un sous groupe de* $(H, \star)$ *et*

$\mathrm{Ker}\, f$ *est un sous groupe de* $(G, \bullet)$.

Propriété 4.14 *Soit $f : G \longrightarrow H$ un homomorphisme de groupe, alors*

1. *f est injective si et seulement si* $\mathrm{Ker}\, f = \{e\}$.
2. *f est surjective si et seulement si* $\Im m f = H$.
3. *f est un isomorphisme si et seulement si f^{-1} existe et est un homomorphisme de groupe de H dans G.*

Preuve. Soit $f : G \longrightarrow H$ un homomorphisme de groupe, alors

1a. Si f est injectif, sachant que $e \in \ker f$ on va montrer que $\ker f \subset \{e\}$.
Soit $x \in \ker f$, alors $f(x) = h$ et comme $f(e) = h$ on déduit que $f(x) = f(e)$ et comme f est injectif on déduit que $x = e$, donc $x \in \{e\}$ ce qui montre que $\ker f = \{e\}$.

1b. Inversement, supposons que $\ker f = \{e\}$ et montrons que f est injectif.
Soient $x,\ y \in G$, alors

$$\begin{array}{rcll} f(x) = f(y) & \Longrightarrow & f(x) \star (f(y))^{-1} = h & \\ & \Longrightarrow & f(x) \star f(y^{-1}) = h & \\ & \Longrightarrow & f(x \bullet y^{-1}) = h & \\ & \Longrightarrow & (x \bullet y^{-1}) \in \ker f & \\ & \Longrightarrow & x \bullet y^{-1} = e \quad \text{car } \ker f = \{e\} & \\ & \Longrightarrow & x = y & \end{array}$$

ce qui montre que f est injectif.

2. La preuve de cette propriété est immédiate, sachant que $\Im m f = f(G)$.

3. On se limitera à démontrer que si f est un isomorphisme, alors $f^{-1} : H \longrightarrow G$ est aussi un homomorphisme. Soient $x,\ y \in H$, alors il existe $a,\ b \in G$ tels que

$$x = f(a) \qquad et \qquad y = f(b)$$

donc

$$a = f^{-1}(x) \qquad et \qquad b = f^{-1}(y),$$

par suite

$$\begin{array}{rcll} f^{-1}(x \star y) & = & f^{-1}(f(a) \star f(b)) & \\ & = & f^{-1}(f(a \bullet b)) \qquad \text{car } f \text{ homomorphisme} & \\ & = & a \bullet b & \\ & = & f^{-1}(x) \bullet f^{-1}(y) & \end{array}$$

ce qui montre que f^{-1} est un homomorphisme de groupe de H dans G.

□

4.3 Structure d'Anneaux

Définition 4.10 *On appelle anneau, tout ensemble A muni de deux lois de composition internes $+$ et $\bullet$ telles que :*

1. *$(A, +)$ est un groupe abélien (on notera 0 ou 0_A l'élément neutre de $+$),*

2. *$\bullet$ est associative et distributive par rapport à $+$.*

Si de plus $\bullet$ est commutative, on dit que $(A, +, \bullet)$ est un anneau commutatif.

Conventions :

$(A,+)$ étant un groupe, alors tous les éléments de A sont symétrisables et on convient de noter $-x$ le symétrique d'un élément $x \in A$.

Si $\bullet$ possède un élément neutre, on le note 1 ou 1_A et on dit que l'anneau $(A,+,\bullet)$ est unitaire ou unifère.
Dans un tel anneau, on dit qu'un élément est inversible s'il l'est par rapport à la deuxième loi $\bullet$. L'inverse d'un élément $x \in A$ est noté x^{-1}.

Régles de Calcul dans un Anneau

Soit $(A,+,\bullet)$ un anneau, alors on a les règles de calculs suivantes :

Propriété 4.15 *Pour tous x, y et $z \in A$,*

1. $0_A \bullet x = x \bullet 0_A = 0_A$

2. $x \bullet (-y) = (-x) \bullet y = -(x \bullet y)$

3. $x \bullet (y - z) = (x \bullet y) - (x \bullet z)$

4. $(y - z) \bullet x = (y \bullet x) - (z \bullet x)$

Preuve :
1. Soit $x \in A$, alors

$$0_A \bullet x = (0_A + 0_A) \bullet x = (0_A \bullet x) + (0_A \bullet x) \qquad \text{car } \bullet \text{ est distributive par rapport à } +$$

comme tous les éléments de A sont symétrisables, on déduit que $0_A \bullet x = 0_A$.
De la même manière on montre que $x \bullet 0_A = 0_A$.

2. Soient $x,\ y \in A$ et montrons que $x \bullet (-y)$ est le symétrique de $(x \bullet y)$. On a :

$$(x \bullet (-y)) + (x \bullet y) = x \bullet (-y + y) = x \bullet 0_A = 0_A$$

comme $+$ est commutative on déduit que $(x \bullet (-y)) = -(x \bullet y)$.
De la même manière on montre que $(-x) \bullet y = -(x \bullet y)$.

La preuve des propriétés **3.** et **4.** utilise essentiellement la distributivité de la loi $\bullet$ par rapport à $+$.

□

On note $A^* = A \backslash \{0\}$, et pour tout $x \in A^*$ et $n \in \mathbb{N}^*$,

$$n.x = nx = \underbrace{x + x + \ldots + x}_{n \text{ fois}} \qquad et \qquad x^n = \underbrace{x \bullet x \bullet \ldots \bullet x}_{n \text{ fois}}$$

Définition 4.11 *Soit $(A,+,\bullet)$ un anneau commutatif. On dit que $y \in A^*$ divise $x \in A$, ou que y est un diviseur de x ou que x est divisible par y, si*

$$\exists\ z \in A^*, \quad x = y \bullet z.$$

Si 0_A ne possède pas de diviseur dans A, on dit que $(A,+,\bullet)$ est un anneau intègre ou un anneau d'intégrité.

4.3.1 Sous Anneaux

Définition 4.12 *On appelle sous anneau de $(A,+,\bullet)$, tout sous ensemble A' de A tel que muni des restrictions des lois $+$ et $\bullet$ est anneau.*
Si A est un anneau unitaire et $1_A \in A'$, on dit que A' est sous anneau unitaire.

On a la cartérisation suivante des sous anneaux.

Propriété 4.16 *Un sous ensemble A' de A est un sous anneau si et seulement si :*
1. $A' \neq \emptyset$,
2. $\forall\ x,\ y \in A',\ (x-y) \in A'$
3. $\forall\ x,\ y \in A',\ (x \bullet y) \in A'$.

Preuve : On sait que A' est est un sous groupe de $(A,+)$ si et seulement si

$$(A' \neq \emptyset) \wedge (\forall\ x,\ y \in A',\ (x-y) \in A'),$$

donc pour que A' soit un sous anneau de A, il suffit de voir si la restriction de la deuxième loi $\bullet$ est interne dans A', ce qui revient à dire que $(\forall\ x,\ y \in A',\ x \bullet y \in A')$, ce qui termine la preuve de notre proposition.

□

4.3.2 Homomorphismes d'Anneaux

Soient $(A,+,\bullet)$ et $(B,\oplus,\otimes)$ deux anneaux et $f : A \longrightarrow B$.

Définition 4.13 *On dit que f est un homomorphisme d'anneaux si :*

$$\forall\ x,\ y \in A, \quad f(x+y) = f(x) \oplus f(y) \ \ et \ \ f(x \bullet y) = f(x) \otimes f(y)$$

- *Si $A = B$ on dit que f est un endomorphisme d'anneau de A.*
- *Si f est bijective, on dit que f est un isomorphisme d'anneaux*
- *Si f est bijective et $A = B$, on dit que f est un automorphisme d'anneaux.*

On sait que l'image de l'élément neutre du groupe de départ d'un homomorphisme de groupe est l'élément neutre du groupe d'arrivée. Par contre, l'image de l'élément unité de l'anneau de départ par un homomorphisme d'anneau n'est pas toujours l'élément unité de l'anneau d'arrivée. Pour s'en convaincre, il suffit de prendre dans un anneau unitaire $(A,+,\cdot)$,

où $0_A \neq 1_A$[2], l'application $f : A \longrightarrow A$ définie par $f(x) = 0_A$ pour tout $x \in A$.

Ce contre exemple nous amène à poser la définition suivante.

Définition 4.14 *Soient A et B deux anneaux unitaires, on dit qu'un homomorphisme d'anneaux f de A dans B est unitaire si $f(1_A) = 1_B$.*

Proposition 4.1 *Soit $f : A \longrightarrow B$ un homomorphisme d'anneaux, alors*
- *f est injectif si et seulement si $kerf$=$\{0_A\}$*
- *Si A et B sont deux anneaux unitaires et f un homomorphisme d'anneaux surjectif, alors f est unitaire.*

Preuve : La première propriété provient de la caractérisation des homomorphismes injectifs entre les groupes $(A, +)$ et $(B, +)$.

Montrons la deuxième propriété.

Soit $y \in B$, f étant injectif, il existe alors $x \in A$ tel que $y = f(x)$, et comme f est un homomorphisme d'anneau on déduit

$$y = f(x) = f(1_A \cdot x) = f(1_A) \cdot f(x) = f(1_A) \cdot y$$

et de la même manière on montre que $y = y \cdot f(1_A)$, ce qui montre que $f(1_A) = 1_B$.

□

Proposition 4.2 *L'image (respectivement l'image réciproque) d'un sous anneau de A (respectivement de B) par f est un sous anneau de B (respectivement de A).*

4.3.3 Idéaux

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

Définition 4.15 *On appelle idéal à droite (respectivement à gauche) de l'anneau A, tout ensemble $I \subset A$ tel que*

1. *I est un sous groupe de $(A, +)$,*
2. *$\forall\ x \in A$, $(\forall\ y \in I, \quad x \bullet y \in I \quad (respectivement\ y \bullet x \in I))$.*

Si I est idéal à droite et à gauche de A, on dit que I est un idéal bilatère de A.

Si l'anneau A est commutatif, tout idéal de A est bilatère, et dans ce cas on parle seulement d'Idéal sans préciser s'il l'est à droite, à gauche ou bilatère.

Exemple 4.12 *Soit $(A, +, \bullet)$ un anneau, alors $I = \{O_A\}$ est un idéal bilatère de A.*

[2]Ceci revient à dire que A n'est pas un singleton.

Exemple 4.13 *Dans l'anneau commutatif $(\mathbb{Z}, +, \cdot)$, $n\mathbb{Z}$ est un idéal.*

Proposition 4.3 *Soit I un idéal à gauche (ou à droite) d'un anneau unitaire $(A, +, \bullet)$, alors*

$$1_A \in I \Longleftrightarrow I = A \Longleftrightarrow \exists\ x \in I; \quad x \quad \textit{est inversible.}$$

Définition 4.16 *On appelle idéal principal d'un anneau commutatif $(A, +, \bullet)$, tout idéal I de A tel que*

$$\exists x \in A; \quad I = x \bullet A$$

L'anneau A est dit principal si tous ses idéaux sont principaux.

4.3.4 Anneaux Quotients

Soient $(A, +, \bullet)$ un anneau commutatif et I un idéal de A. On considère le groupe quotient $(A_{/I}, \oplus)$, et on définit l'application $\otimes$ de $A_{/I} \times A_{/I}$ dans $A_{/I}$ par

$$\forall\ \dot{a},\ \dot{b} \in A_{/I}, \quad \dot{a} \otimes \dot{b} = \overline{a \bullet b}^{\cdot}$$

Propriété 4.17 *$(A_{/I}, \oplus, \otimes)$ est anneau commutatif. Si de plus A est un anneau unitaire, alors $(A_{/I}, \oplus, \otimes)$ est un anneau unitaire et $\overline{1_A}^{\cdot}$ est son élément unité.*

4.4 Corps

Définition 4.17 *On dit qu'un anneau unitaire $(\mathbb{K}, +, \bullet)$ est un corps si tout élément non nul de $\mathbb{K}$ est inversible. Si de plus $\bullet$ est commutative, on dit que $\mathbb{K}$ est un corps commutatif.*

Il est à remarquer que dans la pratique, tous les corps utilisés sont commutatifs.

Propriété 4.18 *Tout corps est un anneau intègre.*

Définition 4.18 *On appelle sous corps, d'un corps $(\mathbb{K}, +, \bullet)$, tout sous ensemble* **K'** *de $\mathbb{K}$ tel que, muni des restrictions des lois $+$ et $\bullet$ est un corps.*

Proposition 4.4 *$\mathbf{K}' \subset \mathbb{K}$ est un sous corps de $(\mathbb{K}, +, \bullet)$ si et seulement si*
- *$\mathbf{K}' \neq \emptyset$*
- *$\forall\ a, b \in \mathbf{K}', \quad a - b$ et $a \bullet b^{-1} \in \mathbf{K}'$.*

On a aussi la caractérisation suivante des corps.

Proposition 4.5 *Soit $(\mathbb{K}, +, \bullet)$ un anneau commutatif unitaire, alors $\mathbb{K}$ est un corps si et seulement si les seuls idéaux de $\mathbb{K}$ sont $\{\mathbf{0}_K\}$ et lui même.*

4.4.1 Caractéristique d'un corps

Etant donné $n \in \mathbb{N}$, alors $\mathbf{Z}_{/n\mathbf{Z}}$ est un corps si n est premier, et on a

$$n\dot{1} = \dot{1} + \cdots + \dot{1} = \dot{0}.$$

D'une façon générale on a :

Définition 4.19 *Le plus petit entier naturel non nul n tel que $n1_{\mathbb{K}} = 0_{\mathbb{K}}$, s'il existe, est appelé caractéristique du corps commutatif* $\mathbf{K}$. *Si pour tout $n \in \mathbb{N}$, $n1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, on dit que* $\mathbf{K}$ *est de caractéristique nulle.*

Propriété 4.19 *La caractéristique d'un corps est un nombre premier.*

Exemple : Pour $n \in \mathbb{N}$ premier, la caractéristique du corps $\mathbf{Z}_{/n\mathbf{Z}}$ est égale à n.