UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES
Département des Mathématiques

Licence Sciences et Techniques (LST)

MATHEMATIQUES ET APPLICATIONS

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du Diplôme de Licence Sciences et Techniques

INTRODUCTION AUX ANNEAUX DE BOOLE

Présenté par :

- **BOUHAMAMA OUMAYMA**

Encadré par :

- **Pr. AZIZA RAHMOUNI HASSANI (FSTF)**

Soutenu Le 11 Juin 2016 devant le jury composé de:

- **Pr. NAJIB MAHDOU (FSTF)**
- **Pr. ANISS OUADGHIRI (FSTF)**
- **Pr. AZIZA RAHMOUNI HASSANI (FSTF)**

Année Universitaire 2015 / 2016

FACULTE DES SCIENCES ET TECHNIQUES FES – SAISS
B.P. 2202 – Route d'Imouzzer – FES
212 (0)5 35 61 16 86 – Fax : 212 (0)5 35 60 82 14
Site web: http://www.fst-usmba.ac.ma

Remerciement :

Tout d'abord, je remercie le Dieu, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce travail modeste.

Je tiens à exprimer ma gratitude et présenter mes chaleureux remerciements à :

⋆ mon encadrant Madame Aziza Rahmouni Hassani pour sa gentillesse, sa disponibilité et ses précieux conseils.

⋆ Les membres du jury : Pr. Najib Mahdou et Pr. Aniss Ouadghiri qui ont accepté d'évaluer ce travail.

⋆ Toute personne ayant contribué de près ou de loin à l'élaboration de ce modeste travail.

Introduction :

Dans le premier chapitre, nous rappelons les structures algébriques qui sont un type particulier de structure. Elles sont spécifiées par rapport aux autres types de structure, car elles comportent deux lois de composition internes. Il est d'usage courant de qualifier d'additive la première loi et de multiplicative la seconde. Autrement dit, la première loi est nommée addition et la seconde est nommée multiplication ou produit. La seconde loi est distributive bilatéralement par rapport à la première loi. Dans ce chapitre nous allons citer les structures d'anneau, d'idéaux et de corps, en donnant des propriétés et des exemples.

Dans le second chapitre nous introduisons les anneaux de Boole qui sont une partie d'algèbre de Boole, introduite par A. De Morgan et G. Boole qui est né le 2 novembre 1815 à Lincoln (Royaume-Uni) et mort le 8 décembre 1864 à Ballin temple (Irlande), c'est un logicien, mathématicien et philosophe britannique. Il est le créateur de la logique moderne, fondée sur une structure algébrique et sémantique, que l'on appelle algèbre de Boole en son honneur. Les anneaux de Boole jouent un rôle très utile dans plusieurs branches des mathématiques (algèbre, théorie des ensembles ordonnés, calcul des probabilités) et en logique mathématique (logique algébrique, modèles booléens).

Table des matières

1 Structures algébriques : 5
1.1 Anneau 5
1.1.1 Définition : 5
1.1.2 Anneau produit : 7
1.1.3 Sous-anneau 7
1.1.4 Homomorphismes d'anneaux : 8
1.1.5 Monomorphismes et épimorphismes : 9
1.1.6 Anneau intègre : 9
1.2 Idéaux : 11
1.2.1 Définition : 11
1.2.2 Générateur d'un idéal : 13
1.2.3 Anneau quotient : 14
1.2.4 Caractéristique d'un anneau : 15
1.3 Corps 16
1.3.1 Sous-corps : 17
1.3.2 Idéaux premiers-Idéaux maximaux 18
1.3.3 Opérations sur les idéaux : 20

2 Anneau de Boole 25
2.1 Définition : 25
2.2 Propriétés d'anneau de Boole : 25
2.3 Exemples : 26
2.4 Morphisme booléen : 30

Chapitre 1

Structures algébriques :

1.1 Anneau

1.1.1 Définition :

1) On dit qu'un ensemble A muni de deux lois de compositions internes notées $+$ et $\times$ est un anneau si :
i) (A,+) est un groupe commutatif.
ii) La loi $\times$ est associative : $\forall$ x,y,z $\in$ A, on a : $x \times (y \times z) = (x \times y) \times z$.
iii) La loi $\times$ est distributive par rapport à la loi $+$: $\forall$ x,y,z $\in$ A, on a : $x \times (y + z) = x \times y + x \times z$.
iv) La loi $\times$ admet un élément neutre noté 1 : $\forall$ x $\in$ A : 1$\times$ x=x (Dans ce cas on dit que A est un anneau unitaire).
2) On dit que l'anneau $(A, +, \times)$ est commutatif si de plus la loi $\times$ est commutative : $\forall$ x,y $\in$ A :$x \times y = y \times x$.

Exemple : 1) ($\mathbb{Z}$,+,$\times$), ($\mathbb{Q}$,+,$\times$) et ($\mathbb{R}$,+,$\times$) sont des anneaux commutatifs et unitaires.
2) Soit (A,+,$\times$) un anneau et E un ensemble. Alors l'ensemble F(E,A) des applications de E $\longrightarrow$ A muni des deux lois :

(f,g)$\longrightarrow$f+g	(f,g)$\longrightarrow$ $f \times g$
x $\longmapsto$ f(x)+g(x)	x $\longmapsto$ $f(x) \times g(x)$

est un anneau unitaire.

3) Soit n un entier strictement positif et A est unitaire, alors l'ensemble des matrices carrées de type n à coefficients dans A, noté $M_n(A)$, est un anneau unitaire non commutatif pour n supérieur à 2.
4) Soit A un ensemble réduit à un seul élément, A=$\{a\}$. Muni des lois a+a=a.a=a, A est un anneau commutatif qu'on appelle l'anneau nul. Dans cet anneau, 1=0=a.

Proposition :(Formule de Binôme de Newton) Si A est unitaire et a,b $\in$ A tel que ab=ba ; c-à-d que a et b commute, alors on a $\forall$ n $\geq$ 1 :
$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$. où $C_n^k = \dfrac{n!}{k!(n-k)!}$

Preuve :(Par récurrence) Pour n=1 ; $(a+b)^1 = a+b = C_1^0 a^{1-0} b^0 + C_1^1 a^{1-1} b^1$. Supposons la formule juste jusqu'à l'ordre n et montrons la pour n+1.
Un calcul simple donne la relation de Pascal suivante :$C_{n-1}^k + C_{n-1}^{k-1} = C_n^k$.
Ainsi on a :
$(a+b)^{n+1} = (a+b)^n (a+b)$

$= (\sum_{k=0}^{n} C_n^k a^{n-k} b^k)(a+b)$ (Hypothèse de récurrence)

$= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k=0}^{n} C_n^k a^{n-k} b^{k+1}$

$= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k=0}^{n} C_n^k a^{(n+1)-(k+1)} b^{k+1}$

$= \sum_{k=0}^{n} C_n^k a^{n+1-k} b^k + \sum_{k'=1}^{n} C_n^{k'-1} a^{(n+1-k')} b^{k'}$(avec k'=k+1)

$= a^{n+1} + \sum_{k=1}^{n} C_n^k a^{(n+1-k)} b^{n+1} + \sum_{k=1}^{n} C_n^{k-1} a^{n+1-k} b^k$

$= a^{n+1} + \sum_{k=1}^{n} (C_n^k + C_n^{k-1}) a^{n+1-k} b^k + b^{n+1}$

$= C_{n+1}^0 a^{n+1} + \sum_{k=1}^{n} C_{n+1}^k a^{n+1-k} b^k + C_{n+1}^{n+1} a^0 b^{n+1}$(Pascal)

$= \sum_{k=0}^{n+1} C_{n+1}^k a^{(n+1)-k} b^k$

Si A est en plus commutatif ; alors on a $\forall$ a,b $\in$ A :$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$

1.1.2 Anneau produit :

Définition : Soient (A,+,×) et (A',+,×) deux anneaux. On définit des lois + et × sur A×A' en posant :
∀ a,b∈ A ; ∀ c,d ∈ A' :
⋆ (a,b)+(c,d)=(a+c,b+d).
⋆ (a,b)×(c,d)=(a×c,×d).

1.1.3 Sous-anneau

Définition : Soient (A,+,×) un anneau, B une partie de A. On dit que B est un sous anneau de (A,+,×) si seulement si :
Muni des lois induites (B,+,×) possède lui-même une structure d'anneau.

Exemple : 1) (ℤ,+,×) est un sous anneau de l'anneau (ℚ,+,×).
2) (ℚ,+,×) est un sous anneau de l'anneau (ℝ,+,×).

Proposition (Caractéristique d'un sous anneau) : Soient (A,+,×) un anneau, B une partie de A. Pour que B soit un sous anneau de A, il faut et il suffit que :
⋆ $1_A \in$ B.
⋆ ∀(a,b) ∈ B^2, a-b ∈ B.
⋆ ∀(a,b) ∈ B^2, ab ∈ B.

Exemple : Le seul sous-anneau de (ℤ,+,×) est (ℤ,+,×) lui-même.

Proposition : Soit (A,+,×) un anneau. Soit $(B_i)_{i\in I}$ une famille non vide de sous anneau de A, alors $\bigcap_{i\in I} B_i$ est sous-anneau de A.

Preuve : $\forall$ i $\in$ I, B_i est un sous-groupe de A, donc $\bigcap_{i\in I} B_i$ est un sous-groupe de A. Stable par multiplication
x,y$\in \bigcap_{i\in I} B_i \Longleftrightarrow \forall$ i $\in$ I, x $\in B_i$ et y $\in B_i$
$\Longrightarrow \forall$ i $\in$ I, x$\times$y $\in B_i$
$\Longrightarrow$ x $\times$ y $\in \bigcap_{i\in I} B_i$
$\forall$ i $\in$ I, $1_A \in \bigcap_{i\in I} B_i$.

Sous-anneau engendré par partie : Soient A un anneau et S une partie de A. On définit le sous-anneau de A engendré par S par B(S)=intersection de sous anneaux de A contenant S.

Exemple : Le sous-anneau de ($\mathbb{C}$,+,$\times$) engendré par $\{i\}$ est $\mathbb{Z}$[i]=$\{a + ib/a, b \in$Z$\}$ dite anneau de Gaus.
En effet, soit B un sous-anneau de $\mathbb{C}$ contenant le nombre i, alors 1 $\in$ B et par conséquent $\mathbb{Z} \subseteq$ B comme i $\in$ B, alors $\mathbb{Z}$[i] $\subseteq$ B. Comme $\mathbb{Z}$[i] est un sous-anneau de $\mathbb{C}$, il est le sous anneau engendré par $\{i\}$.

1.1.4 Homomorphismes d'anneaux :

Définition : Soient (A,+,$\times$) et (B,+,$\times$) des anneaux. On note 1_A et 1_B les éléments neutres multiplicatifs. On note 0_A et 0_B les éléments neutres additifs. On dit qu'une application f :A $\longrightarrow$ B est un homomorphisme d'anneaux si :
$\star$ f(1_A)=1_B.
$\star$ $\forall$(x,y) $\in$ A^2, $f(x + y) = f(x) + f(y)$.
$\star$ $\forall$(x,y) $\in$ A^2, $f(xy) = f(x)f(y)$.

$\diamond$ Un endomorphisme d'anneau (A,+,$\times$) est un homomorphisme d'anneaux bijectif.
$\diamond$ Un automorphisme d'anneaux (A,+,$\times$) est un endomorphisme bijectif dans l'anneau (A,+,$\times$).

Proposition : 1) Si f : A $\longrightarrow$ B et g :B $\longrightarrow$ C sont des morphismes d'anneaux, alors g $\circ$ f :A $\longrightarrow$ C est un morphisme d'anneaux.
2) Id_A : A$\longrightarrow$A est un automorphisme de l'anneau (A,+,$\times$).
3) Si f : A $\longrightarrow$ B est un isomorphisme d'anneaux, alors f^{-1} : B $\longrightarrow$ A est un isomorphe d'anneaux.

1.1.5 Monomorphismes et épimorphismes :

Définition (monomorphisme) : Un morphisme d'anneaux f :R $\longrightarrow$ S, S est appelée un monomorphisme si et seulement si pour tous deux morphismes d'anneaux g, h :T $\longrightarrow$ R, on a :

$$f \circ g = f \circ h \Rightarrow g = h.$$

Si R $\longrightarrow$ S est un monomorphisme, on dit que S est une extension d'anneau de R.

Définition (épimorphisme) : Un morphisme d'anneaux f :R $\longrightarrow$ S, S est appelée un épimorphisme si et seulement si pour tous deux morphismes d'anneaux g, h :S $\longrightarrow$ T, on a :

$$g \circ f = h \circ f \Rightarrow g = h.$$

1.1.6 Anneau intègre :

Diviseur de zéro :

Définition : Soit (A,+, .) un anneau, on dit qu'un élément a $\in$ A est un diviseur de zéro si :
a $\neq$ 0 et s'il existe b $\neq$ 0 dans A tel que a.b = 0.

Remarque : Un diviseur de zéro dans un anneau unitaire n'est jamais inversible (pour la multiplication) et, par contraposé, un élément inversible ne peut être un diviseur de zéro.

Remarque : Si a est un diviseur de 0, une égalité de la forme a.b=a.c ne peut être simplifiée a priori.
Un élément simplifiable pour le produit ne peut donc être un diviseur de zéro.

Définition : Soient A un sous anneau, a $\in$ A.
1) On dit que a est un diviseur de zéro à gauche dans A si seulement si :
a $\neq$ 0.
$\exists$b $\in$A. b $\neq$ 0 et ab=0.
2) On dit que a est un diviseur de zéro à droite dans A si et seulement si :
a $\neq$ 0 $\exists$ c $\in$ A, c $\neq$ 0 et ca=0.
3) On dit que a est diviseur de zéro dans A si et seulement si a est un diviseur de zéro à gauche dans A et un diviseur de zéro à droite dans A.

Définition : Un anneau (A,+,$\times$) est dit intègre si :
A n'admet aucun diviseur de zéro.
Autrement dit, c'est un anneau vérifiant :
$\forall$ x,y $\in$ A, x$\times$y=0$\Rightarrow$ x=0 ou y=0.

Exemple : L'anneau $\mathbb{Z}$ des entiers est intègre.

Définition : Soient A un anneau intègre, (x,y) $\in A^2$.
Alors si x|y $\Leftrightarrow$ Ay $\subset$ Ax.

Preuve : Si x|y, alors $\exists$ a $\in$ A tel que y=ax.
Donc $\forall$ $\alpha \in$ A, αy=α(ax)=(αa)x $\in$ Ax.
D'où Ay $\subset$ Ax.

Exemple : Soient A, B deux anneaux. Dans l'anneau produit A $\times$ B, on a (a,0).(0,b)=(0,0), c'est-à-dire que pour a $\neq$ 0 et b $\neq$ 0, (a,0) et (0,b) sont des diviseurs de 0.
Donc, pour A et B non réduits à $\{0\}$, A $\times$ B n'est jamais intègre.

Définition : Dans un anneau unitaire (A,+,.), on note $A^\times$ l'ensemble de ses éléments inversibles pour la multiplication, c'est-à-dire l'ensemble des éléments a $\in$ A pour lesquels il existe un élément a' $\in$ A tel que a.a'=a'.a= 1.
Quand il existe un tel inverse est unique et on le note a^{-1}.
On dit aussi que les éléments de $A^\times$ sont les unités de A.
Comme $1 \neq 0$ dans A ; on a $A^\times \subset A \setminus \{0\}$ et cette inclusion peut être stricte.
Par exemple, $\mathbb{Z}^\times = \{-1, 1\}$ et $R[X]^\times = R^*$ (ensemble des polynômes constants non nuls).

Théorème : Soit (A,+,.) un anneau unitaire. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour le produit, d'élément neutre 1.

Preuve : $A^\times$ est non vide puisqu'il contient 1.
Si a, b sont dans $A^\times$, on a alors :

$$b^{-1}a^{-1}ab = b^{-1}b = 1;$$

$$abb^{-1}a^{-1} = aa^{-1} = 1.$$

C'est-à-dire que ab est inversible d'inverse $b^{-1}a^{-1}$. La multiplication définit donc une loi interne sur $A^\times$.
On sait déjà que cette loi est associative, que 1 en est le neutre et tout a $\in$ $A^\times$ est inversible par construction d'inverse $a^{-1} \in A^\times$ (on a $(a^{-1})^{-1} = a$).
($A^\times$,.) est donc un groupe. On dit que $A^\times$ est le groupe des unités de A.

Définition : (Élément nilpotent)
Soit A un anneau non réduit à {0}. Soit a un élément non nul de A.
On dit que a est nilpotent s'il existe un entier n tel que $a^n = 0$, avec ces notations $\forall$ p>n, a^p=0.
Le plus petit entier n tel que a^n=0 est appelé l'indice de nilpotente de a.

1.2 Idéaux :

1.2.1 Définition :

Soit (A,+,×)un anneau commutatif. Soit I une partie de A.
On dit que I est un idéal de A si :

$\star$ (I,+) est sous groupe de (A,+).
$\star$ $\forall$ x $\in$ I, $\forall$ y $\in$ A, on a : xy $\in$ I.

Tout idéal qui est à la fois idéal à gauche et idéal à droite de A est appelé idéal bilatère de A, c-à-d :
1) $\forall$ a $\in$ A, $\forall$ i $\in$ I,$\Rightarrow$ a$\times$i $\in$ I.
2) $\forall$ a $\in$ A, $\forall$ i $\in$ I,$\Rightarrow$ i$\times$a $\in$ I.

Remarque : On remarque qu'un idéal est en particulier un sous-anneau de A. La réciproque est fausse.

Exemple : $\mathbb{Z}$ est un sous anneau de ($\mathbb{Q}$,+,$\times$) mais il n'est pas idéal de ($\mathbb{Q}$,+,$\times$) car 1.(1/2) $\notin \mathbb{Z}$ et 1 $\in \mathbb{Z}$ et 1/2 $\in \mathbb{Q}$.

Idéaux propres et impropres : {0} et A sont deux idéaux de A dit idéaux impropres.
Tout idéal I de A différent de {0} et A est dit idéal propre de A.

Exemple : Un idéal de $\mathbb{Z}$ est toujours sous la forme n$\mathbb{Z}$, avec n $\in \mathbb{N}$ (puisqu'un idéal est un sous groupe de $\mathbb{Z}$ et n$\mathbb{Z}$ est un idéal de $\mathbb{Z}$).

Proposition : Si un idéal I contient un élément inversible x$\in$ A. Alors on a : I=A.

Preuve : Soit I un idéal d'un anneau A (I $\subset$ A) contenant un élément inversible de x dans A. Comme x $\in$ A. Comme x $\in$ I et $x^{-1} \in$ A, alors on a $1=xx^{-1} \in$ I.
Soit maintenant a $\in$ A. On a alors a=a.1 $\in$ I, donc A $\subset$ I de sorte que A=I et cela termine la preuve.
On conclut alors qu'un idéal propre ne contient aucun élément inversible.

1.2.2 Générateur d'un idéal :

Définition : L'idéal engendré par une partie F d'un anneau A est le plus petit idéal contenant cette partie. Il est noté I(F) ou $< F >$.

Proposition : Soit un anneau commutatif. Pour tout x $\in$ A la partie xA=Ax=$\{ax, a\in$ A $\}$ est un idéal de A appelé idéal engendré par x.

Preuve : 1) x=1.x $\in$ Ax.
2) $\forall$(a,b) $\in A^2, ax + bx = (a + b)x \in$ Ax.
3) $\forall$ a $\in$ A, $\forall$ b $\in$ A, b(ax)=(ba)x $\in$ Ax.

Définition : 1. Un idéal I d'un anneau A est dit de type fini s'il existe une partie finie F=$\{a_1, a_2, ..., a_n\}$ tel que : I=$< F >= Aa_1 + Aa_2 + ... + Aa_n$.
2. Un anneau A est dit Noethérien si tout idéal A est de type fini.

Théorème : 1. Le noyau d'un morphisme d'anneau est un idéal.
2. Un morphisme d'anneaux est injectif si et seulement si son noyau est nul.

Preuve : 1. Soit f un morphisme d'un anneau A dans un anneau B.
Le noyau est un groupe additif puisque le morphisme est aussi un morphisme de groupe additif. En outre, si a $\in$ ker(f) et b $\in$ A alors on a f(ab)=f(a).f(b)=0_B, de sorte que ab $\in$ ker(f). Ainsi ker(f) est un idéal de A.

2. Si le morphisme est injectif, le zéro a un seul antécédent, c-à-d que ker(f)=$\{0\}$.
Inversement, l'égalité f(x)=f(y) entraine f(x-y)=0, c-à-d que x-y $\in$ ker(f)=$\{0\}$ et par suite x=y. Cela veut dire que f est injectif et cela termine la preuve.

proposition : Soit f :A $\longrightarrow$ B un morphisme d'anneaux et J un idéal de B. Alors l'image réciproque de J qui est f^{-1}(J) :=$\{a\in$ A ; f(a) $\in$ J $\}$ est un idéal de A.

Preuve : Comme f(0)=0 ∈ J, alors on a $0 \in f^{-1}(J)$. En plus si a, b ∈ f^{-1}(J), on a f(a+b)=f(a)+f(b) ∈ J puisque f(a).f(b) ∈ J et J est un idéal de B. Enfin, si a ∈ A et b ∈ f^{-1}(J), on a f(ab)=f(a)f(b) ∈ J puisque f(b) ∈ J et cela termine la preuve.

Remarque : L'image d'un idéal par un morphisme n'est pas toujours un idéal.
En effet, soit f l'application :

$$f : \mathbb{Z} \longrightarrow \mathbb{Q}$$
$$x \longmapsto x$$

On a f(2ℤ)=2ℤ n'est pas un idéal de ℚ (car $2 \in \mathbb{Z}$, $1/2 \in \mathbb{Q}$ mais $2.1/2 \notin 2\mathbb{Z}$).

1.2.3 Anneau quotient :

Définition : Soit I un idéal de A. A/I muni de la loi additive $(\bar{x}, \bar{y}) \longmapsto \overline{x+y}$ est un groupe commutatif car (A,+) est un groupe commutatif.
On définit de même sur A/I la loi multiplicative suivante : $(\bar{x}, \bar{y}) \longmapsto \overline{xy}$.
A/I muni des deux lois cités précédemment est anneau commutatif unitaire.
On l'appelle l'anneau quotient de A par I.
L'homomorphisme d'anneau A ⟶ A/I est appelé l'homomorphisme canonique.

Premier théorème d'isomorphisme : Soit f : A ⟶ A' un homomorphisme de groupes. Alors la décomposition de f donne l'isomorphisme d'anneaux A/ker(f) ≅ Im(f).

Preuve : Considérons $\bar{f} : A/Ker(f) \longrightarrow f(A)$, $\bar{x} \longmapsto \bar{f}(\bar{x}) = f(x)$. $\bar{f}$ est une application bien définie. Aussi, $Im(\bar{f})$ = Im(f). D'autre part, $\bar{f}$ est un homomorphisme de groupes. En effet, $\bar{f}(\bar{x}\bar{x'})=\bar{f}(\overline{xx'}) = f(xx^{'}) = f(x)f(x') = \bar{f}(\bar{x})\bar{f}(\bar{x'})$. $\bar{f}$ est injectif car si x ∈ A : $\bar{f}(\bar{x})$=e', alors f(x)=e', d'où x ∈ ker(f), i.e., $\bar{x} = \bar{e}$ et aussi $\bar{f}$ est par définition surjectif. Ainsi A/ ker(f) ≅ Im(f).

1.2.4 Caractéristique d'un anneau :

Définition : Soit A un anneau. L'application f : $\mathbb{Z} \longrightarrow$ A qui à n associe n.1 est un homomorphisme d'anneaux. Son noyau ker(f) est donc un idéal de $\mathbb{Z}$ donc de la forme p$\mathbb{Z}$ avec p $\in \mathbb{N}$.
On obtient d'après le résultat précédent que $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à f($\mathbb{Z}$)(=Im(f)) qui est un sous anneau de A.

Définition : L'entier naturel p ainsi défini s'appelle caractéristique de l'anneau A et se note Car(A).

Remarques : Si p=0, alors ker(f)={0} (c-à-d que f est injectif) et donc $\mathbb{Z}$ est isomorphe à f($\mathbb{Z}$)(=Im(f)).
L'anneau A contient un sous-anneau isomorphe à $\mathbb{Z}$ et en particulier A est infini.
Si p $\neq$ 0, alors ker(f)=p$\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à Im(f)(=f($\mathbb{Z}$)). L'entier p est le plus petit naturel non nul tel que p.1=0 et il est caractérisé par pour tout n $\in \mathbb{N}$, n.1=0 implique que n est un multiple de p.

Proposition : Si l'anneau A est intègre, sa caractéristique est soit 0 soit un nombre premier. En particulier la caractéristique d'un corps est donc soit 0 soit un nombre premier.

Preuve : Si la caractéristique de A n'est pas nulle, Im(f) est inclue dans l'anneau A qui est intègre, donc Im(f) est lui même intègre et de plus il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
Donc $\mathbb{Z}/p\mathbb{Z}$ est intègre et par suite p est premier.

Remarque : La réciproque de la proposition précédente est fausse car par exemple Car($\frac{\mathbb{R}[X]}{<X^2>}$)=0, mais $\frac{\mathbb{R}[X]}{<X^2>}$ n'est pas intègre car $\bar{X}^2 = \bar{X}.\bar{X}$=0 mais $\bar{X} \neq \bar{0}$.

Exemple : on a Car($\mathbb{Z}/n\mathbb{Z}$)=n et Car($\mathbb{Q}$)=Car($\mathbb{R}$)=0.

1.3 Corps

Définition : Un corps est un anneau unitaire dans lequel tout élément non nul est inversible.
C-à-d que A\{0} est un groupe pour la multiplication. Si la multiplication d'un corps est commutative, on dit que le corps est commutatif.

Exemples : $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont tous des corps commutatifs.

Remarque : 1. Tout corps k est intègre. En effet, soit a,b $\in$ k si ab=0 avec a $\neq 0$, alors a^{-1} existe et $0=a^{-1}ab = b$ puisque a est inversible étant non nul.

2. Tout corps contient 1 et 0 avec $1 \neq 0$.

3. Comme un corps est un anneau intègre, alors sa caractéristique est soit zéro soit un nombre premier.

Théorème Soit A un anneau non nul. Les assertions suivantes sont équivalentes :
i) A est un corps.
ii) Les seuls idéaux de A sont {0} et A.
iii) Tout homomorphisme non nul de A dans un anneau est injectif.

Preuve : i) $\Rightarrow$ ii) :
Soit I $\neq \{0\}$ un idéal. Soit x $\in$ I et x $\neq 0$ alors $1=x^{-1}x \in$ I et par suite on a : I=A.
ii) $\Rightarrow$ iii) :
Soit f : A $\longrightarrow$ B un morphisme d'anneaux non nul avec B $\neq \{0\}$. c-à-d :
$\exists$ x $\in$ A/ f(x) $\neq 0$. Par suite x $\notin$ ker(f) et ker(f) est un idéal ; donc d'après ii) on a ker(f)={0} et par suite f est injectif.
iii) $\Rightarrow$ i) :
Soit x $\in$ A et x non inversible. On veut montrer que x=0. Comme x est non inversible, alors B :=A/xA $\neq 0$ (car A $\neq$ xA) ; et par suite on a :
f :A $\longrightarrow$ B=A/xA, où f(z)=$\bar{z} = z + xA$, qui est non nul (car B $\neq 0$) est un morphisme qui est injectif d'après iii).

Or on a f(0)=$\bar{0} = \bar{x} = f(x)$. Donc x=0 car f est injectif.

1.3.1 Sous-corps :

Définition : Soit K un corps et K' une partie de K.
On dit que K' est un sous corps de K si K' est un sous corps additif de K et $(K')^*$=K'\{0} est un sous-groupe multiplicatif. Autrement dit :
K' est un sous corps de K si :

$$K' \neq \emptyset$$
$$x - y \in K'; \forall x, y \in K'$$
$$xy^{-1} \in (K')^*; \forall x, y \in (K')^*$$

Exemple : $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$.

Proposition : Tout anneau unitaire intègre fini est un corps.

Preuve : Soit A un tel anneau et soit a $\in$ A ; avec a $\neq$ 0. Soit

$$f : A \longrightarrow A$$
$$x \longmapsto ax$$

f est une application injective : si f(x)=f(x'), on a ax=ax', donc a(x-x')=0 et par suite x-x'=0 (car a $\neq$ 0 et A est intègre), alors x=x'.
f est bijective car A est fini. Donc $\exists$ b $\in$ A tel que : ab=1.

$$g : A \longrightarrow A$$
$$x \longmapsto xa$$

De la même façon ; on montre qu'il existe b' $\in$ A : b'a=1 $\Rightarrow$ (b'a)b=1.b $\Rightarrow$ b'(ab)=b $\Rightarrow$ b'=b.
Ainsi on a : ab=ba=1, et a est inversible. Dès lors, A est un corps.

1.3.2 Idéaux premiers-Idéaux maximaux

Définition : Soit A un anneau commutatif unitaire et P un idéal de A.
1. P est dit premier si $\forall x, y \in A \Rightarrow x \in p$ ou y $\in$ P.
2. P est dit maximal si P $\neq$ A et si les seuls idéaux compris entre P et A sont P et A.

Théorème : Soient A un anneau commutatif unitaire et P un idéal de A. Alors on a :
1. P est premier si et seulement si A/P est intègre.
2. P est maximal si et seulement si A/P est corps.

Preuve : 1. Supposons que P est premier et montrons que A/P est intègre. Soit a,b $\in$ A tel que : $\bar{a}\bar{b} = \bar{0}$ et $\bar{a} \neq 0$. Ces relations se traduisent dans A par ab $\in$ P et a $\notin$ P. L'hypothèse P premier entraine que b $\in$ P ; $\bar{b}$=0. Ainsi, A/P est intègre.
Réciproquement, supposons que A/P est intègre, et considérons deux éléments a et b de A tel que ab $\in$ P. Par passage au quotient on obtient $\overline{ab} = \bar{a}\bar{b}$=$\bar{0}$ et par suite $\bar{a}$=0 ou $\bar{b}$=0 (car A/P est intègre de sorte que)
a $\in$ P ou b $\in$ P. Ainsi P est un idéal premier.

2. Supposons que M est maximal et montrons que A/M est un corps. Soit a $\in$ A tel que $\bar{0} = \bar{a} \in$ A/M. Montrons que $\bar{a}$ est inversible dans A/M. Pour cela considérons l'idéal aA+M=A qui contient strictement l'idéal M (car a $\notin$ M). A cause de la maximalité de M on a aA+M=A. Ainsi il existe t $\in$ A et u $\in$ M tel que : 1=at+u. Par passage aux classes modulo M, on obtient $\bar{a}\bar{t} = \bar{1}$. Ainsi, la classe de a est inversible dans A/M ; et l'anneau A/M est un corps.
Réciproquement, supposons que A/M est un corps ; et prenons un idéal I contenant strictement M.
Soit a $\in$ I-M. On a $\bar{a} \neq 0$ car a $\notin$ M, et par suite $\bar{a}$ est inversible dans A/M ; c-à-d qu'il existe t $\in$ A tel que : $\bar{1} = \overline{at}$ ou $\overline{1 - at}$=0, ou 1-at $\in M \subseteq I$. Donc 1=(1-at)+at avec 1-at $\in M \subseteq I$ et at $\in$ I et par suite I=A.
Ainsi on a M est un idéal maximal de A.

Proposition : Les assertions suivantes sont équivalentes :
(i) I est un idéal premier de A.

(ii) I $\neq$ A et $\forall$ (a, b) $\in$ A $\times$ A on a : a.b $\in$ I a $\in$ I ou b $\in$ I.

Preuve : (i) $\Rightarrow$ (ii) :
Soit I un idéal premier de A. A/I est différent de $\{\bar{0}\}$ donc I $\neq$ A.
Si a,b $\in$ I alors $\bar{a}.\bar{b} = \bar{0}$ dans A/I soit $\bar{a}$ ou $\bar{b}$ est nul car A/I est intègre donc a ou b appartient à I.
(ii) $\Rightarrow$ (i) :
Comme I $\neq$ A, A/I $\neq \{\bar{0}\}$.
D'autre part : $\bar{a}.\bar{b} = \bar{0} \Leftrightarrow$ a.b $\in$ I $\Rightarrow$ a ou b appartient à I $\Leftrightarrow$ $\bar{a}$ ou $\bar{b}$ est nul et donc A/I est intègre.
D'où I est un idéal premier de A.

Proposition : Les assertions suivantes sont équivalentes :
(i) I est un idéal maximal de A.
(ii) I $\neq$ A et si J est un idéal de A distinct de A tel que I $\subset$ J, alors J = I (autrement dit I est maximal pour l'inclusion parmi les idéaux propres de A).

Preuve : (i) $\Rightarrow$ (ii) :
Soit I un idéal maximal de A ; A/I est différent de $\{\bar{0}\}$, donc I $\neq$ A. Soit J un idéal de A distinct de A tel que I $\subset$ J. Si I est distinct de J considérons x $\in$ J $\setminus$ I. On a $\bar{x} \neq \bar{0}$ donc $\bar{x}$ est inversible (car A/I est un corps) : Il existe y $\in$ A tel que $\bar{a}.\bar{b} = \bar{1}$.
Donc il existe z $\in$ I tel que x.y = 1 + z, soit 1 = x.y – z d'où 1 $\in$ J et on aurait J = A contrairement à l'hypothèse. Donc J = I.
(ii) $\Rightarrow$ (i) :
Si $\bar{x}$ appartenant à A/I $\setminus$ $\{\bar{0}\}$ on a x $\notin$ I. L'idéal I+(x) engendré par I et x contient strictement I donc il est égal à A par hypothèse.
Par conséquent, il existe z $\in$ I et y $\in$ A tels que 1 = z + x.y d'où $\bar{1} = \bar{x}.\bar{y}$ et $\bar{x}$ est inversible dans A/I. Comme A/I est non nul car A $\neq$ I.
C'est donc un corps et I est un idéal maximal de A.

Corollaire : Un idéal maximal est premier car un corps est un anneau intègre.

1.3.3 Opérations sur les idéaux :

Intersection, réunion d'idéaux :

Proposition : L'intersection d'une famille d'idéaux est un idéal.

Preuve : Soit $(I_j)_{j\in J}$ une famille d'idéaux d'un anneau (A,+,×).
$\forall$ j $\in$ J, I_j est un sous groupe de A donc l'intersection $\bigcap_{j\in J} I_j$ est un sous groupe de A. Stable par multiplication par un élément de A :
x $\in \bigcap_{j\in J} I_j \Leftrightarrow \forall$ j $\in$ J, x $\in I_j$
$\Rightarrow \forall$ j $\in$ J, $\forall$ a $\in$ A x×a $\in I_j \Rightarrow$ x×a $\in \bigcap_{j\in J} I_j$

Proposition : Soit I et J des idéaux de A. Alors I $\bigcup$ J est un idéal de A $\Leftrightarrow$ I $\subset$ J ou J $\subset$ I.

Preuve : ($\Leftarrow$) Évident.
($\Rightarrow$) I $\bigcup$ J est un idéal de A $\Rightarrow$ I $\bigcup$ J est un sous groupe de (A,+). Or la réunion des deux sous-groupes n'est un sous-groupe que si l'un des sous-groupes est contenue dans l'autre.

Somme de deux idéaux :

Définition : Soit A un anneau, I et J des idéaux de A. La somme des idéaux I et J qu'on note I+J est I+J=$\{i + j, i\in$ I, j $\in$ J $\}$.

Preuve : On a :
I+J=$\{a_1b_1 + ... + a_kb_k, a_i\in$ A, $b_i\in$ I $\bigcup$ J, k ≥ 1 $\}$
=$\{a_1i_1 + ... + a_ni_n + c_1j_1 + ... + c_mj_m, a_l, c_l\in$ A, $i_l\in$ I, $j_l\in$ J, n, m ≥ 1 $\}$
Comme I et J sont des idéaux, les sommes :
$a_1i_1 + ... + a_ni_n\in$ I
$c_1j_1 + ... + c_mj_m\in$ J
Donc $I + J =\{i + j, i\in$ I, j $\in$ J $\}$

Proposition : Soit A un anneau, I et J des idéaux de A. I+J est l'idéal engendré par l'ensemble $I \bigcup J$ et I+J=(I,J).

Preuve : Montrons que I+J est un idéal de A. Soit alors $x_1 + x_2$ et $y_1 + y_2$ deux éléments de I+J, où x_1, $y_1 \in$ I et x_2, $y_2 \in$ J, et a $\in$ A. On a : $(x_1+x_2)+(y_1+y_2) = (x_1+y_1)+(x_2+y_2) \in$ I+J et $a(x_1+x_2) = ax_1+ax_2$ $\in$ I+J, ce qui veut dire que I+J est un idéal de A.

Montrons que l'idéal I+J est engendré par I $\cup$ J. Comme pour tout x $\in$ I, x=x+0 $\in$ I+J, alors on a I $\subseteq$ I+J. De même on a J $\subseteq$ I+J de sorte que I $\cup$ J $\subseteq$ I+J.
Soit H un idéal de A contenant I $\cup$ J et montrons que I+J $\subseteq$ H. Soit alors x+y $\in$ I+J, telque x $\in$ I ($\subseteq$ I $\cup$ J $\subseteq$ H) et y $\in$ J ($\subseteq$ I $\cup$ J $\subseteq$ H). Dés lors, on a x+y $\in$ H puisque H est un idéal de A, ce qui termine la preuve.

Produit d'idéaux :

Définition : Soit A un anneau, I et J des idéaux de A. Le produit des idéaux I et J qu'on note IJ est l'idéal engendré par l'ensemble $\{ij, i\in$ I, j $\in$ J$\}$

Proposition : IJ=$\{i_1j_1 + i_2j_2 + ... + i_kj_k, j_l\in$ J, k ≥ 1 $\}$

Preuve : On pose k=$\{i_1j_1 + i_2j_2 + ... + i_kj_k, j_l\in$ J, k ≥ 1 $\}$
On peut montrer que k est un idéal de A qui contient l'ensemble $\{ij, i\in$ I, j $\in$ J $\}$ et IJ est le plus petit idéal qui contient $\{ij, i\in$ I, j $\in$ J$\}$ donc IJ $\subset$ k.
On montre que k $\subset$ IJ. Soit x $\in$ K, x s'écrit :
x= $i_1j_1 + i_2j_2 + ... + i_kj_k, j_l \in$ J
Soit $1 \leq$ l $\leq$ k, $i_lj_l \in \{ij, i\in$ I, j $\in$ J$\}$. Comme IJ contient $\{ij, i\in$ I, j $\in$ J$\}$: $i_1j_1 \in$ IJ, $\forall$l, $1 \leq$ l $\leq$ k.
Or IJ est un idéal donc :

$$x = \sum_{l=1}^{k} i_l j_l \in IJ$$

Proposition : Soient (A,+,.) un anneau commutatif unitaire et I, J deux idéaux de A.
IJ=$\{\sum$ xy / x ∈ I , y ∈ J $\}$ est un idéal de A est contenu dans I $\bigcap$ J. (C-à-d $IJ \subset I \bigcap J$)

Preuve : ⋆ On montre que IJ est un idéal de A.
◇ IJ $\neq \emptyset$ car 0=0.0 ∈ IJ.
◇ Soit x=$\sum_{fini} a_i b_i$ et y=$\sum_{fini} c_i d_i$ / x,y ∈ IJ avec a_i, c_i ∈ I et b_i, d_i ∈ J
x-y=$\sum a_i b_i - \sum c_i d_i = \sum a_i b_i + \sum(-c_i d_i) \in IJ$.
◇ Soit a ∈ A et $\sum a_i b_i \in IJ$ avec $a_i \in I$ et $b_i \in J$.
a$\sum a_i b_i = \sum(aa_i)(b_i) \in IJ$ avec $aa_i \in I$ et $b_i \in J$.
Donc IJ est un idéal de A.

⋆ On montre que $IJ \subset I \bigcap J$.
Si a ∈ I et b ∈ J, ab appartient à I $\bigcap$ J. Dès lors, l'idéal IJ qui est engendré par les produits ab est contenu dans I $\bigcap$ J.

Propriétés : ∀ I, I', J idéaux de A.

⋆ AI=I

$\star (I + I') \bigcap J \supset (I \bigcap J) + (I' \bigcap J)$

$\star (I \bigcap I') + J \subset (I + J) \bigcap (I' + J)$

$\star (I + I')J = (IJ) + (I'J)$

$\star I \subset I' \Rightarrow IJ \subset I'J$

$\star IJ = JI, (II')J = I(I'J)$

$\star (I \bigcap I')J \subset (IJ) \bigcap (I'J)$

Preuve : ⋆ Montrons que AI=I

◇ I ⊂ AI
I est un ensemble d'un anneau (A,+,.) donc $I \subset AI$

$\diamond$ AI $\subset$ I
Soit xy $\in$ AI avec x $\in$ A et y $\in$ I.
Or xy $\in$ I car I est un idéal de A donc $AI \subset I$. D'où AI=I

$\star$ Montrons que $(I \bigcap J) + (I' \bigcap J) \subset (I + I') \bigcap J$

Soit a $\in ((I \bigcap J) + (I' \bigcap J)) \Rightarrow a = x + x'$ avec x $\in I \bigcap J$ et x' $\in I' \bigcap J$

$\Rightarrow \left\{ \begin{array}{c} x \in \text{ I et x } \in \text{ J} \\ x' \in \text{ I' et x' } \in \text{ J} \end{array} \right. . \Rightarrow \left\{ \begin{array}{c} x + x' \in I + I' \\ x' + x' \in J \end{array} \right. . \Rightarrow x + x' \in I + I' \bigcap J$

$\Rightarrow a \in I + I' \bigcap J$

D'où $(I \bigcap J) + (I' \bigcap J) \subset (I + I') \bigcap J$

$\star$ Montrons que $(I \bigcap I') + J \subset (I + J) \bigcap (I' + J)$

Soit a $\in (I \bigcap I') + J \Rightarrow a = x + x'$ avec x $\in I \bigcap I'$ et x' $\in$ J

$\Rightarrow \left\{ \begin{array}{c} x \in \text{ I et x } \in \text{ I'} \\ x' \in \text{ J} \end{array} \right. . \Rightarrow x + x' \in (I + J) \bigcap (I' + J)$

$\Rightarrow a \in (I + J) \bigcap (I' + J)$

D'où $(I \bigcap I') + J \subset (I + J) \bigcap (I' + J)$

$\star$ Montrons que (I+I')J=(IJ)+(I'J)

Soit a $\in$ (I+I')J $\Rightarrow$ a=bc tel que b $\in$ I+I' et c $\in$ J $\Rightarrow$ a=(x+x')c tel que x $\in$ I, x' $\in$ I', c $\in$ J $a = xc_{\in IJ} + x'c_{\in I'J}$, $a \in (IJ) + (I'J)$.
Soit b $\in$ ((IJ)+(I'J)) $\Rightarrow$ b=a+c tel que a $\in$ IJ et c $\in$ I'J
$\Rightarrow b = (x.x') + (y.x')$
$\Rightarrow b = (x + y).x'$
$\Rightarrow b \in (I + I')J$

D'où (I+I')J=(IJ)+(I'J)

$\star$ Montrons que IJ=JI

Soit a $\in IJ \Rightarrow$ a=xy tel que x $\in$ I, y $\in$ J $\Rightarrow a = yx \in JI$ donc IJ $\subset$ JI.
De même pour JI $\subset$ IJ

D'où IJ=JI

$\star$ Montrons que (II')J=I(I'J)

Soit a $\in (II')J \Rightarrow a = (x_{\in I}x'_{\in I'})y_{\in J} \Rightarrow a = x(x'y) \Rightarrow a \in I(I'J)$

De même pour I(I'J) $\subset$ (II')J
D'où (II')J=I(I'J)

$\star$ Montrons que $(I \bigcap I')J \subset (IJ) \bigcap (I'J)$

Soit a $\in (I \bigcap I')J \Rightarrow$ a=bc tel que b $\in I \bigcap I', c \in J$

$\Rightarrow \left\{ \begin{array}{r} b\in \text{ I et b} \in \text{ I'} \\ c\in \text{ J} \end{array} \right. . \Rightarrow bc \in (IJ) \bigcap (I'J)$

D'où $(I \bigcap I')J \subset (IJ) \bigcap (I'J)$

Chapitre 2

Anneau de Boole

2.1 Définition :

Un anneau de Boole est un anneau (R,+,×) unitaire dans lequel chaque élément est idempotent pour la multiplication. C-à-d $\forall$ x $\in$ R ; x^2=x

De cette définition découle les propriétés suivantes :

2.2 Propriétés d'anneau de Boole :

Lemme 1 : Si R un anneau booléen, alors R est de caractéristique 2. (Car(R)=2) et chaque élément est sont propre opposé.

Preuve Soit x $\in$ R, alors x^2=x et $(x+x)^2$=x+x, ce qui implique que $x^2+2x+x^2=x+x$, et alors 2x=0.
Donc Car(R)=2. Il en résulte que x=-x pour tout x $\in$ R.
Donc dans un anneau de Boole, tout élément est son propre opposé.

Mais, la réciproque est fausse : Un anneau de caractéristique 2 n'est pas forcément un anneau de Boole.

Exemple : Soit k=$\mathbb{Z}/2\mathbb{Z}$, k est un corps puisque 2 est premier.
Considérons alors l'anneau unitaire $M_2(k)$ des matrices carrées d'ordre 2 à coefficients dans k, sa caractéristique est 2 mais la multiplication n'est pas idempotente. Donc n'est pas un anneau de Boole.

Contre exemple :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Lemme 2 Si R est un anneau Booléen, alors R est commutatif.

Preuve : Soient x,y $\in$ R, on veut montrer que xy=yx.
Puisque R est booléen alors $x^2 = x$ et $y^2 = y$.
x+y=$(x + y)^2$=$x^2 + xy + yx + y^2 = x + xy + yx + y$.
Donc xy+yx=0, alors xy=-yx.
En utilisant le lemme précédent on a : x=-x pour tout x $\in$ R.
Donc xy=yx, d'où R est commutatif.

Proposition : Un anneau de Boole vérifie la propriété :
0 est absorbant : $\forall$ x $\in$ E, x$\times$0=0.

Preuve : on sait que x+x=0
a$\times$0 $= a(a + a) = a^2 + a^2 = a + a = 0$.
Donc 0 est absorbant.

2.3 Exemples :

Exemple 1 : L'anneau <$\mathcal{P}$(E),$\triangle$,$\cap$> où E est un ensemble non vide quelconque $\triangle$ et $\cap$ étant respectivement les opérations de différence symétrique et d'intersection sur l'ensemble P(E) des parties de E, est un anneau de Boole.

Preuve : On rappelle que pour A,B dans $\mathcal{P}$(E), on a :

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A),$$

la réunion étant disjointe.
De la commutativité des opérateurs $\cup$ et $\cap$, on déduit que $\triangle$ est commutative.
Pour A, B, C dans $\mathcal{P}$(E), on a :
$(x \in (A \triangle B) \triangle C) \Leftrightarrow (x \in A \triangle B$ et x $\notin$ C) ou $(x \in Cetx \notin A \triangle B)$
$\Leftrightarrow$(x $\in$ A et x $\notin$ B et x $\notin$ C) ou (x $\in$ B et x $\notin$ A et x $\notin$ C)
ou (x $\in$ C et x $\notin$ A et x $\notin$ B) ou (x $\in$ C et x$\in A \cap B$)
$\Leftrightarrow$ (x $\in$ A et x $\notin$ B et x $\notin$ C)ou (x $\in$ B et x $\notin$ A et x $\notin$ C)
ou (x $\in$ C et x $\notin$ A et x $\notin$ B) ou (x $\in$ A $\cap$ B $\cap$ C)
et :
(x $\in$ A $\triangle$ (B $\triangle$ C))$\Leftrightarrow$(x $\in$ A et x $\notin$ B$\triangle$ C) ou (x $\in$ B$\triangle$ C et x $\notin$ A)
$\Leftrightarrow$(x $\in$ A et x $\notin$ B et x $\notin$ C) ou (x $\in$ A et x$\in A \cap C$)
ou (x $\in$ B et x $\notin$ C et x $\notin$ A) ou (x $\in$ C et x $\notin$ B et x $\notin$ A)
$\Leftrightarrow$ (x $\in$ A et x $\notin$ B et x $\notin$ C) ou (x $\in$ A $\cap$ B $\cap$ C)
ou (x $\in$ B et x $\notin$ C et x $\notin$ A) ou (x $\in$ C et x $\notin$ B et x $\notin$ A)

D'où l'égalité (A $\triangle$ B)$\triangle$ C=A $\triangle$ (B $\triangle$ C).
L'ensemble vide $\emptyset$ est le neutre pour $\triangle$ et pour tout A $\in \mathcal{P}$(E), on a :

$$A \triangle A = (A \cup A) \setminus (A \cap A) = (A \setminus A) = \emptyset,$$

C'est-à-dire que A est l'opposé de A pour la loi $\triangle$.
En définitive, ($\mathcal{P}$(E), $\triangle$) est un groupe commutatif.
On vérifie facilement que $\cap$ est commutative et associative. L'ensemble E est le neutre pour $\cap$.

Pour A, B, C dans $\mathcal{P}$(E), on a :
(x $\in$ A $\cap$ (B $\triangle$ C))$\Leftrightarrow$ (x $\in$ A et x $\in$ B$\triangle$ C)
$\Leftrightarrow$ (x $\in$ A et x $\in$ B et x $\notin$ C) ou (x $\in$ A et x $\in$ C et x $\notin$ B)
$\Leftrightarrow$ (x $\in$ A $\cap$ B et x $\notin$ C) ou (x $\in$ A $\cap$ C et x $\notin$ B)
$\Leftrightarrow$ (x $\in$ A $\cap$ B et x $\notin$ A $\cap$ C) ou (x $\in$ A $\cap$ C et x $\notin$ A $\cap$ B)
$\Leftrightarrow$ (x $\in$ (A $\cap$ B)\(A $\cap$ C)) ou (x $\in$ (A $\cap$ C)\(A $\cap$ B))
$\Leftrightarrow$ x $\in$ (A $\cap$ B)$\triangle$(A $\cap$ C)
C'est-à-dire que $\cap$ est distributive par rapport à $\triangle$.
En définitive, ($\mathcal{P}$(E), $\triangle, \cap$) est un anneau commutatif et unitaire.
C'est aussi un anneau de Boole puisque, pour tout X $\in \mathcal{P}$(E), on a X $\cap$ X=X.

Exemple 2 : L'anneau $<\mathbb{Z}/2\mathbb{Z}, +, \times>$ est un anneau de Boole.

Preuve : $\mathbb{Z}/2\mathbb{Z}$ est l'anneau des entiers modulo 2 : Il se réduit à deux éléments $\{\bar{0}, \bar{1}\}$.
C'est un anneau de Boole car x^2=x pour x=$\bar{0}$ et x=$\bar{1}$.
Il en résulte que l'on a : x+x=$\bar{0}$ pour tout x $\in \mathbb{Z}/2\mathbb{Z}$

Proposition : Si R est un anneau de Boole intègre alors R est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Preuve : Soit x $\in$ R et x $\neq 0$
Alors x^2=x et x^2-x=0 ce qui implique que x(x-1)=0, et par suite l'anneau étant intègre et x $\neq 0$ alors x=1.
Donc R=$\{0, 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

Comme conséquence de ce fait on a que :

Proposition : Soit R un anneau Booléen avec identité, alors tout idéal premier est maximal dans R.

Preuve : Soit P un idéal premier de R. Donc P $\in$ spec(R), et donc R/P est un anneau de Boole intègre alors R/P $\cong \mathbb{Z}/2\mathbb{Z}$.
Ce qui montre que P est maximal.

Propriété : Soit A un anneau de Boole.
Si p $\in$ Spec(A) et a, b $\notin$ p alors a + b $\in$ p.

Preuve : Cela découle de ce que si a,b $\notin$ p, alors leurs classes valent 1 dans le quotient A/p $\cong \mathbb{Z}/2\mathbb{Z}$, et donc leur somme est nulle, ce qui signifie justement que a + b $\in$ p.

Propriétés : 1. On suppose que R est fini et de cardinal supérieure à 2, alors A possède des diviseurs de zéro.

2. Un anneau de Boole intègre ne peut pas avoir 3 éléments.

3. Si anneau de Boole R possède au moins trois élément distincts Alors R n'est pas intègre.

Preuve : 1. On suppose que A est fini et qu'il est au moins de cardinal égal à 4.
Soit x(x+1)=x^2+x=x+x=0, alors que ni x ni x+1 ne sont nuls.
On constate donc que l'anneau A possède des diviseurs de zéro.

2. Si R est intègre, on a :
xy(x+y)=$x^2y + xy^2$=xy+xy=0, et donc x=0 ou y=0 ou x+y=0=x+x.
Ainsi lorsque on choisit deux élément de R, soit ils sont nuls soit ils sont égaux.

3. Soit R un anneau de Boole ayant au moins trois élément distincts 0, 1, a.
a(a+1)=a^2+a=a+a=0
$a + 1 \neq 0$ car sinon a+1=0 entrainerait que a=1, ce qui n'est pas possible car a $\neq$ 1.
On a trouvé dans A deux élément non nuls : a et a+1 dont le produit est nul
Donc R n'est pas intègre.

Exemple : Dans un anneau de Boole ($\mathcal{P}$(E),$\triangle$,$\cap$), on a pour toute partie A de E :
A$\cap$(E $\setminus$ A) = $\emptyset$.
Donc tout A$\neq \emptyset$ est un diviseur de $\emptyset$ (le 0 pour la loi $\triangle$).

Théorème : Si R est un anneau de Boole fini alors R a 2^k éléments (k entier).

Preuve : On suppose que card(R)=m, par l'absurde on va montrer que m=2^k.
On suppose que m $\neq 2^k$, alors m a un facteur premier p différent de 2.
Et puisque R est un groupe additif, alors par le théorème de Cauchy (Soit G un groupe fini d'ordre n. Pour tout diviseur premier p de n, il existe dans G au moins un élément d'ordre p), R a un élément x $\neq$ 0 d'ordre p, qui est p.x=0 car p est impaire. Alors p=2x+1. Ainsi (2x+1).x=0.

Mais Car(R)=2 d'après Lemme 1 et donc x=0. Contradiction, donc m=2^k.

Propriété : Le seul élément inversible dans un anneau de Boole est 1.

Preuve : Soit $R^\times$ l'ensemble des éléments inversibles, et soit x $\in R^\times$ et y $\in$ R avec xy=1. De la on tire que x=x(xy)=x^2y=xy=1.
On obtient x = 1.
D'où le seul élément inversible dans un anneau booléen est 1.

Proposition : Si un anneau de Boole ne contient pas de diviseurs de zéro, il est soit $\{0\}$ ou est isomorphe $\mathbb{Z}/2\mathbb{Z}$ (montrer que xy(x + y) = 0 pour tout x, y $\in$ A).

Preuve : Puisque A est Booléen il est commutative et x + x = 0 pour tout x $\in$ A. Soit x, y $\in$ A soit non nul. Or, xy (x + y)=$x^2y + xy^2 = xy + xy = 0$. Par conséquent, ou bien A a un diviseur égal à zéro ou x+y=0 pour tout x non nul ; y $\in$ A. En ce dernier cas, x=-y=y et A peut avoir qu'un seul élément non nul. Par conséquent, A$\cong \mathbb{Z}/2\mathbb{Z}$.

2.4 Morphisme booléen :

Définition : Soient A et B deux anneaux booléens, une application f de A dans B est dite morphisme booléen si f est un morphisme unitaire d'anneaux, c-à-d vérifie :
⋆ f(x+y)=f(x)+f(y).
⋆ f(xy)=f(x)f(y).
⋆f(1)=1.

Propriétés : 1) Un sous anneau d'un anneau Booléen est Booléen.
2) L'image homomorphique d'un anneau de Boole est également anneau de Boole.

Preuve : 1) Soit S un sous anneau d'un anneau de Boole R.
Alors pour tout x ∈ S, x est un élément de R, et donc x est idempotent
D'où S est booléen.

2) Soit T l'image homomorphique de R où $\Pi : R \longrightarrow T$ est un épimorphisme d'anneau.
Soit t ∈ T, alors t=$\Pi(r)$ pour r ∈ R. Donc,

$$\begin{aligned} t^2 &= \Pi(r)\Pi(r) \\ &= \Pi(r^2) \\ &= \Pi(r) \\ &= t \end{aligned}$$

Donc tout élément de T est idempotent.
D'où T est booléen.

Conclusion :

Dans ce rapport nous avons présenté dans le premier chapitre les anneaux-idéaux-corps qui nous amènent à l'étude des anneaux de Boole en introduisant des définitions générales, des théorèmes et des exemples, et dans le second chapitre nous avons présenté une introduction aux anneaux de Boole en donnant des propriétés et définitions caractérisant les anneaux de Boole.

Références :

[1] Najib Mahdou ; Structure algébrique : Cours et exercices corrigés.

[2] El Turkey H. ; Generalizations of Boolean Rings, Master's thesis, The American University of Beirut, Beirut, Lebanon, June 2008.

[3] Giordano Favi ; Des anneaux de Boole

[4] Réné Cori, Daniel Lascar ; Logique mathématique : Calcul propositionnel, algèbre de Boole, calcul des prédicats.