

Sur les propriétés topologiques des algèbres de Boole

Par : Kebabi Hala & Labachi Houria

Le 25/06/2013

Table des matières

Introduction	4
1 Les ensembles ordonnés et treillis	5
1.1 Rappels et quelques compléments	5
1.1.1 Parties	5
1.1.2 Relations	6
1.1.3 Diagramme de venn	6
1.1.4 Relation induite	7
1.2 Ensembles ordonnés	7
1.2.1 Relation d'ordre sur un ensemble	7
1.2.2 Ordre total et ordre partiel	8
1.2.3 Diagramme de Hasse	9
1.2.4 Exemples d'ordres sur $\mathbb{N} \times \mathbb{N}$	9
1.2.5 Majorant et minorant	11
1.2.6 Élément maximal et élément minimal	12
1.2.7 Représentation des éléments maximaux, maximums et majorants des ensembles	12
1.2.8 Borne supérieure et borne inférieure	13
1.3 Homomorphismes d'ensembles ordonnés	14
1.4 Ensembles bien ordonnés	15
1.5 Les treillis	18
1.5.1 Notions de base	18

1.5.2	Demi-treillis	18
1.5.3	Treillis complets	18
1.5.4	Demi-treillis complet	18
1.5.5	Quelques exemples de treillis :	19
1.5.6	Propriétés algébriques des treillis	19
1.5.7	Treillis distributif	22
1.5.8	Treillis fermé	24
1.5.9	Treillis complémenté	25
1.5.10	Treillis de Boole	26
1.6	Théorie des ensembles (Axiomes de Zermelo-Fraenkel)	28
1.6.1	Axiome d'extensionnalité	29
1.6.2	Axiome de la paire	29
1.6.3	Axiome de la somme (ou de la réunion)	30
1.6.4	Axiome de l'ensemble des parties	31
1.6.5	Les relations	32
1.6.6	Schéma d'axiomes de substitution (ou de remplacement)	33
1.6.7	Schéma de compréhension	33
1.7	Ordinaux et cardinaux	35
1.7.1	Relation de bon ordre	35
1.7.2	La collection des ordinaux	36
1.7.3	L'axiome du choix	38
1.7.4	Cardinaux	38
1.7.5	Axiome de l'infini	39
2	Algèbre de Boole	41
2.1	Rappels d'algèbre et de topologie	41
2.1.1	Algèbre	41
2.1.2	Topologie	44
2.2	Algèbre de Boole	52

2.2.1	Les anneaux	52
2.2.2	Anneau de Boole	52
2.2.3	Propriétés des anneaux de Boole	52
2.2.4	Les algèbres de Boole en tant qu'ensembles ordonnés	56
2.3	Atomes dans une algèbre de Boole	57
2.4	Homomorphisme d'algèbre de Boole	59
2.4.1	Isomorphisme d'algèbre de Boole	61
2.4.2	Définitions	64
2.4.3	Composition des morphismes	64
2.4.4	Sous-algèbre de Boole	65
2.5	Idéaux et filtres	67
2.5.1	Propriétés des idéaux	67
2.5.2	Exemples	68
2.5.3	Idéaux maximaux	69
2.5.4	Filtres	71
2.5.5	Ultrafiltres	72
2.5.6	Exemples	72
2.5.7	Base de filtre	74
3	Théorème de représentation de Stone	76
3.1	L'espace de Stone d'une algèbre de Boole	76
3.2	Théorème de Stone	79
3.3	Les espaces booléens sont des espaces de Stone	81
	Conclusion	84
	Bibliographie	85

Introduction

Vers 1847, le mathématicien anglais **Georges Boole** a définie une nouvelle algèbre dite algèbre de Boole ou algèbre booléenne. Comme en algèbre classique, on traite de fonctions en algèbre booléenne. Mais dans ce dernier cas, les fonctions et les variables ne peuvent prendre que l'une des deux valeurs binaires 0 et 1. Ces fonctions et ces variables sont alors dites booléens ou logiques. L'algèbre de Boole est d'une très grande utilité pour la construction des circuits logiques.

Ainsi, au dix-huitième siècle, la logique a fait son apparition grâce aux travaux de plusieurs chercheurs comme Peirce, Schroder, Dedekind, Skolem, Menger etc..., la théorie des treillis a longtemps été négligée, avant de prendre son essor à partir des années 30, grâce à des auteurs et chercheurs comme Klein, Bir-khoff, Ore, Stone, Kurosh , Tarski , Glivenko, von Neumann, etc..., la transformant en branche fertile de l'algèbre.

C'est à cette époque qu'on découvre que la structure de treillis se retrouve dans de nombreux domaines mathématiques tels que : l'algèbre, la géométrie, la logique, l'analyse fonctionnelle, etc... ; mais ce n'est que vers les années 60 que l'aspect combinatoire des treillis va se développer, en liaison avec la naissance de l'informatique et donc l'accroissement des besoins en informatique, algorithmique, programmes et combinatoire. Ainsi on découvre la notion des ensembles ordonnés et leurs éléments remarquables pour ces ensembles, et on donne aussi un rappel sur la théorie des ensembles, et enfin de compte cite les propriétés topologiques des algèbres de Boole et le théorème de Stone. Dans ce mémoire, nous nous intéressons particulièrement aux propriétés topologiques des algèbres de Boole et le théorème de Stone.

Ce document est organisé de la manière suivante :

Le premier chapitre est constitué des définitions et des concepts de base, on va donner des rappels et quelques compléments sur les ensembles ainsi que sur les ensembles ordonnés et leurs propriétés (borne sup, borne inf, et les autres éléments remarquables), et les homomorphismes d'ensembles ordonnés, ainsi que les ensembles bien ordonnés, et enfin de compte on va introduire la notion de treillis (distributif, complémenté et fermé), et on va conclure par la notion de treillis de Boole, théories axiomatiques des ensembles, des ordinaux et cardinaux.

dans le second chapitre on va étudier les algèbres de Boole en général (atomes dans une algèbre de Boole, homomorphisme d'algèbre de Boole, idéaux et filtres).

Le dernier chapitre sera consacré au théorème de représentation de Stone.

Chapitre 1

Les ensembles ordonnés et treillis

Ce chapitre est constitué des définitions et des concepts de base, on va donner des rappels et quelques compléments sur les ensembles ainsi que sur les ensembles ordonnés et leurs propriétés (borne sup, borne inf, et les autres éléments remarquables), et les homomorphismes d'ensembles ordonnés, ainsi que les ensembles bien ordonnés, et enfin de compte on va introduire la notion de treillis (distributif, complémenté et fermé), et on va conclure par la notion de treillis de Boole, théories axiomatiques des ensembles, des ordinaux et cardinaux.

1.1 Rappels et quelques compléments

Deux ensembles sont égaux si et seulement s'ils possèdent exactement les mêmes éléments (nous verrons plus tard que c'est l'un des principaux axiomes de la théorie des ensembles). Par exemple, les ensembles $\{2, 3, 5, 7\}$ et $\{n \in \mathbb{N} | n \leq 10 \text{ et } n \text{ est premier}\}$ sont égaux. D'autre part (et ce sera aussi un axiome), il existe un ensemble qui ne contient aucun élément, noté \emptyset (ou $\{\}$). On dit que A est inclu dans B ou que B contient A , et on écrit $A \subset B$ lorsque les éléments de A sont tous dans B .

1.1.1 Parties

Pour un ensemble E , on note $\rho(E)$ l'ensemble des parties de E . Si E est fini et possède n éléments alors $\rho(E)$ possède 2^n éléments. Pour A et B deux ensembles, on a les propriétés suivantes :

1. $\rho(A) \cap \rho(B) = \rho(A \cap B)$.
2. $\rho(A) \cup \rho(B) \subset \rho(A \cup B)$.
3. si $A \subset B$ alors $\rho(A) \subset \rho(B)$.

1.1.2 Relations

Définition 1.1. Soient A et B deux ensembles. Une relation entre A et B est une partie de $A \times B$. Si \mathfrak{R} est une relation entre A et B , on dira que a est en relation avec b lorsque $(a, b) \in \mathfrak{R}$. On notera souvent plus simplement $a \mathfrak{R} b$. Lorsque $A = B$, nous parlerons d'une relation binaire sur A .

1.1.3 Diagramme de venn

Définition 1.2. Le diagramme de venn est une représentation graphique pour une telle association entre deux ensembles (pour une relation entre deux ensembles)

Exemple 1. Soit A est un ensemble de personnes :

$$A = \{\text{Audrey, Benoît, Céline, David, Élodie}\}$$

et B un ensemble de loisirs :

$$B = \{\text{cinéma, internet, lecture, sport}\}.$$

Audrey aime le cinéma et la lecture, Benoît aime surfer sur internet, Céline lit beaucoup mais fait aussi du sport, David est cinéphile, passe une partie de son temps sur internet et fait du sport et élodie consacre la plus grande partie de son temps libre à la lecture. On peut représenter tout cela sur un diagramme de Venn.

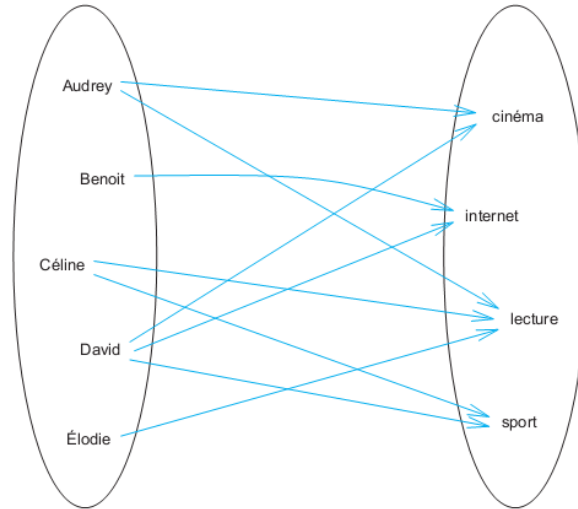


FIGURE 1.1 – Diagramme de venn

1.1.4 Relation induite

Définition 1.3. Soient \mathcal{R} une relation binaire sur un ensemble E et F une partie de E . On obtient une relation binaire sur F , provisoirement notée \mathcal{R}_F , en posant

$$\mathcal{R}_f = \{ (x, y) \in F \times F \mid x \mathcal{R} y \}.$$

Pour $x, y \in F$, on a donc $x \mathcal{R}_f y$ si et seulement si $x \mathcal{R} y$. On appelle \mathcal{R}_f la relation induite par \mathcal{R} sur F .

1.2 Ensembles ordonnés

1.2.1 Relation d'ordre sur un ensemble

Définition 1.4. Une relation \mathcal{R} (noté par \leq) est une relation d'ordre sur un ensemble E , si pour tout $x, y, z \in E$ on a :

1. \mathcal{R} est réflexive si et seulement si $x \mathcal{R} x$.
2. \mathcal{R} est antisymétrique si et seulement si $x \mathcal{R} y$ et $y \mathcal{R} x \implies x = y$.
3. \mathcal{R} est transitive si et seulement si $x \mathcal{R} y$ et $y \mathcal{R} z \implies x \mathcal{R} z$.

Définition 1.5. Un ensemble E est ordonné, s'il est muni d'une relation d'ordre \leq . On le notera (E, \leq) . On dit que deux éléments x et y dans E sont non-comparables, si aucune des relations suivantes $x \leq y$ et $y \leq x$ n'est vérifiée.

Exemple 2. L'ensemble des couples

$$\{(2, 2), (2, 3), (2, 5), (2, 7), (3, 3), (3, 5), (3, 7), (5, 5), (5, 7), (7, 7)\}$$

est une relation d'ordre sur l'ensemble $E = \{2, 3, 5, 7\}$. C'est en fait la relation induite sur E par la relation d'ordre habituelle sur les entiers.

Définition 1.6. (*sous ensemble ordonné*)

Soient (E, \leq) un ensemble ordonné et A une partie de E , la restriction de l'ordre \leq à la partie A est l'ordre noté \leq_A , on dit que alors (A, \leq_A) est un sous-ensemble ordonné de (E, \leq) , souvent noté (A, \leq_A) .

Définition 1.7. Une *chaîne* est un sous-ensemble d'éléments de E deux à deux comparables.

1.2.2 Ordre total et ordre partiel

Ordre partiel

Définition 1.8. Soit un ensemble ordonné (E, \leq) . S'il existe deux éléments x et $y \in E$ tels que x et y sont non-comparables, alors la relation d'ordre \leq est partielle. On dit que aussi (E, \leq) est partiellement ordonné.

Ordre total

Définition 1.9. Soit (E, \leq) , si $x, y \in E$ tels que $x \leq y$ ou $y \leq x$. On dit que l'on a un ordre total et (E, \leq) est appelée un ensemble totalement ordonné.

Exemples

- La relation d'inclusion n'est pas d'ordre total.
- L'ordre \leq naturel sur l'ensemble des nombres réels est une relation d'ordre total.
- $(\mathbb{N}, /)$ La division n'est pas un ordre total mais est un ordre partiel.

1.2.3 Diagramme de Hasse

Définition 1.10. *Le diagramme de Hasse est un critère graphique pour des ensembles totalement ou partiellement ordonnés.*

Exemple 3. *Soit l'ensemble $\{(x, y, z, t)\}$ partiellement ordonné avec son diagramme de Hasse montré dans la (Figure 1.2). Chaque élément est représenté par un point.*

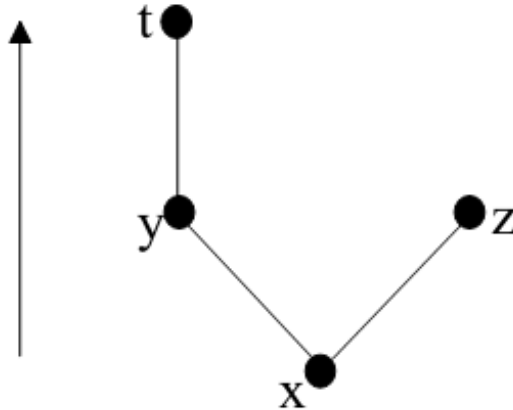


FIGURE 1.2 – Diagramme de Hasse

1.2.4 Exemples d'ordres sur $\mathbb{N} \times \mathbb{N}$

Un même ensemble peut en général être ordonné de plusieurs façons, muni de plusieurs relations d'ordre. C'est en particulier le cas de l'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers naturels qui possède plusieurs relations d'ordre utiles. Nous en donnons deux exemples ici dans un cadre plus général.

L'ordre produit

Définition 1.11. *Soit E un ensemble ordonné par \leq . Pour (x, y) et $(x', y') \in E \times E$, on pose*

$$(x, y) \leq_p (x', y') \text{ si } x \leq x' \text{ et } y \leq y'.$$

L'ordre lexicographique

Définition 1.12. *Soit E un ensemble ordonné par \leq . Pour (x, y) et $(x', y') \in E \times E$, on pose*

$$(x, y) \leq_l (x', y') \text{ si } x < x' \text{ ou } x = x' \text{ et } y \leq y'.$$

Remarque 1.1. *L'ordre lexicographique, généralisé à des n -uplets de lettres de longueur quelconque, est celui utilisé pour classer les mots dans un dictionnaire.*

Propriétés 1.1. *La relation \leq_p est une relation d'ordre sur $E \times E$. Elle n'est pas totale, sauf si E contient moins de deux éléments.*

Démonstration. On voit facilement que \leq_p est une relation réflexive (parce que \leq l'est).

D'autre part, si

$$(x, y) \leq_p (x', y') \text{ et } (x', y') \leq_p (x, y)$$

alors

$$x \leq x' \text{ et } y \leq y' \text{ et } x' \leq x \text{ et } y' \leq y.$$

Parce que \leq est antisymétrique, on en déduit que

$$x = x' \text{ et } y = y'.$$

Donc \leq_p est antisymétrique.

Si

$$(x, y) \leq_p (x', y') \text{ et } (x', y') \leq_p (x'', y'')$$

alors on obtient

$$x \leq x' \leq x'' \text{ et } y \leq y' \leq y''$$

donc

$$(x, y) \leq_p (x'', y'').$$

La relation \leq_p est transitive. On a montré que c'est une relation d'ordre. Supposons que la relation \leq_p est d'ordre total et que E est non vide (s'il est vide, $E \times E$ l'est aussi et la relation \leq_p est alors la relation vide qui est trivialement une relation d'ordre total).

Soient x, y deux éléments de E . Alors on a :

$$(x, y) \leq_p (y, x) \text{ ou } (y, x) \leq_p (x, y).$$

Dans les deux, on obtient

$$x \leq y \text{ et } y \leq x.$$

Donc $x=y$ puisque \leq est antisymétrique. Ainsi, E ne contient au plus qu'un seul élément. \square

Proposition 1.1. *La relation \leq_l est une relation d'ordre sur $E \times E$. Si \leq est un ordre total sur E alors \leq_l est un ordre total sur $E \times E$.*

Démonstration. Il est clair que la relation \leq_l est réflexive. On remarque aussi que l'inégalité $(x, y) \leq_l (x, y)$ implique $x \leq x$.

Supposons que $(x, y) \leq_l (x', y')$ et $(x', y') \leq_l (x, y)$. On a dans ce cas $x \leq x'$ et $x' \leq x$ donc $x = x'$. La définition de l'ordre l indique alors que $y \leq y'$ et $y' \leq y$ donc $y = y'$. Cela montre que la relation \leq_l est antisymétrique. Supposons que $(x, y) \leq_l (x', y')$ et $(x', y') \leq_l (x'', y'')$. Si $x < x'$ ou $x' < x''$ alors on a $x < x''$ et donc $(x, y) \leq_l (x'', y'')$ c'est l'inégalité qu'on cherche à obtenir. Il reste le cas où $x = x'$ et $x' = x''$. Mais alors la définition de l'ordre indique que $y \leq y'$ et $y' \leq y''$, donc $y \leq y''$. On obtient dans ce cas aussi $(x, y) \leq_l (x'', y'')$. La relation \leq_l est donc transitive. Supposons que \leq est un ordre total et considérons deux éléments (x, y) et (x', y') de $E \times E$. Concernant x et x' , nous avons trois cas : $x < x'$, $x = x'$ ou $x > x'$ puisque l'ordre \leq est total. Dans le premier cas, on a $(x, y) \leq_l (x', y')$ et, dans le troisième cas, on a $(x', y') \leq_l (x, y)$. Traitons le cas restant $x = x'$. Nous avons alors deux sous-cas : $y \leq y'$ ou bien $y' \leq y$, encore et parce que \leq est un ordre total. Dans le premier sous-cas $(x, y) \leq_l (x', y')$ et, dans le second $(x', y') \leq_l (x, y)$. L'ordre \leq_l est donc total. \square

1.2.5 Majorant et minorant

Soit E un ensemble ordonné et \leq est une relation d'ordre, considérons un sous-ensemble F de E ordonnée par \leq .

Majorant

Définition 1.13. *On appelle majorant de F tout élément M de E tel que :*

$$\forall x \in F \Rightarrow x \leq M.$$

Proposition 1.2. *Si M appartient à F alors l'élément M est unique et s'appelle le maximum de F .*

Démonstration. Soient M_1 et M_2 deux majorants de F .

M_1 étant majorant de F on a bien évidemment $M_2 \leq M_1$.

or M_2 étant aussi majorant de F on obtient pareillement $M_1 \leq M_2$.

D'où

$$M_2 = M_1$$

contradiction. □

Minorant

Définition 1.14. *On appelle minorant de F tout élément m de E tel que :*

$$\forall x \in F \Rightarrow m \leq x.$$

Proposition 1.3. *Si m appartient à F alors l'élément m est unique et s'appelle le minimum de F .*

Démonstration. Soient m_1 et m_2 deux minorants de F . m_1 étant minorant de F on a bien évidemment $m_1 \leq m_2$ or m_2 étant aussi minorant de F on obtient pareillement $m_2 \leq m_1$

D'où

$$m_2 = m_1$$

contradiction. □

1.2.6 Élément maximal et élément minimal

Définition 1.15. 1. *On dit que M est un **élément maximal** de E si le seul élément x de E vérifiant $M \leq x$ est $x = M$ lui même.*

2. *On dit que m est un **élément minimal** de E si le seul élément x de E vérifiant $x \leq m$ est $x = m$ lui même.*

1.2.7 Représentation des éléments maximaux, maximums et majorants des ensembles

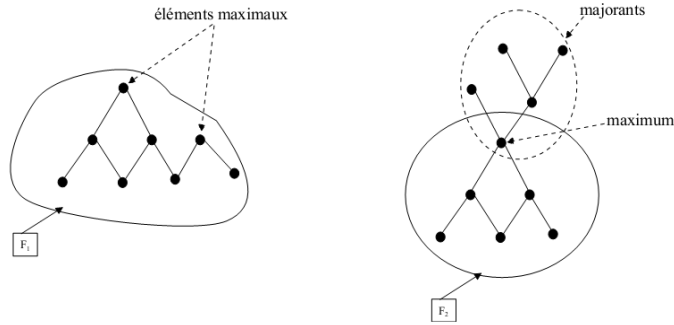


FIGURE 1.3 – Représentation des éléments maximaux, maximums et majorants des ensembles

1.2.8 Borne supérieure et borne inférieure

Définition 1.16. Soit E un ensemble ordonné et F une partie non vide de E .

1. On dit que $M \in E$ est une **borne supérieure** de F dans E si M est le plus petit majorant de F dans E . Si elle existe, cette borne supérieure est unique. On la note \sup_E .
2. On dit que $m \in E$ est une **borne inférieure** de F dans E si m est le plus grand minorant de F dans E . Si elle existe, cette borne inférieure est unique. On la note \inf_E .

Exemple 4. Soit un ensemble $E = \{a, b, c, d, e, f, g, h\}$ ordonné par une relation d'ordre.

- Le sous-ensemble $\{d, e, f\}$ possède 4 majorants (a, b, c, d) et un ppM d .
- Le sous-ensemble $\{d, e, f, g\}$ ne possède ni majorant ni minorant.
- Le sous-ensemble $\{d, f, g, h\}$ ne possède pas de majorants mais possède un minorant (f).
- Le sous-ensemble $\{a, b, c, d\}$ ne possède aucun majorant, 3 minorants (e, d, f) et un pgm (d).

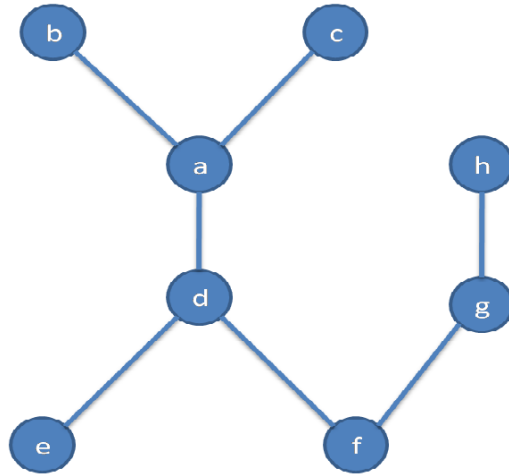


FIGURE 1.4 – Ensemble ordonné

1.3 Homomorphismes d'ensembles ordonnés

Définition 1.17. Une application $f : E \rightarrow F$ telle que $x \leq_1 y$ si et seulement si $f(x) \leq_2 f(y)$ est appelée un **homomorphisme** d'ensembles ordonnés. Si f est en plus une bijection, alors on dit que c'est un **isomorphisme** d'ensembles ordonnés. Si f est un homomorphisme d'un ensemble ordonné dans lui-même (c'est-à-dire lorsque $E = F$), alors on dit que f est un **endomorphisme** d'ensemble ordonné. Un endomorphisme d'ensemble ordonné bijectif est appelé un **automorphisme** d'ensemble ordonné.

Remarque 1.2. Bien noter le « si et seulement si » dans la définition d'un homomorphisme d'ensembles ordonnés.

Proposition 1.4. Un homomorphisme d'ensembles ordonnés est toujours injectif.

Démonstration. Soit $f : E \rightarrow F$ un homomorphisme d'ensembles ordonnés. Soient $x, y \in E$ tels que $f(x) = f(y)$. On a $f(x) \leq f(y)$ donc $x \leq y$. De même, $f(y) \leq f(x)$ donc, $y \leq x$. Par l'antisymétrie de \leq , on obtient $x=y$. Donc, f est injectif. \square

1.4 Ensembles bien ordonnés

Définition 1.18. Soit E un ensemble ordonné par \leq . On dit que \leq est un bon ordre (ou que E est bien ordonné) si toute partie non vide de E admet un minimum. De façon formelle,

$$\forall A \subset E, A \neq \emptyset, \exists x \in A, \forall y \in A, x \leq y.$$

Exemple 5. L'ensemble \mathbb{R}^+ des réels positifs n'est pas bien ordonné par \leq car, par exemple, l'intervalle ouvert $]0, 1[$ ne possède pas un minimum.

Proposition 1.5. Si \leq est un bon ordre sur un ensemble E alors E est totalement ordonné par \leq .

Démonstration. Pour $x, y \in E$, la partie $\{x, y\}$ est non vide, donc possède un plus petit élément. Si x est plus petit élément alors $x \leq y$. Sinon, c'est y et $y \leq x$. \square

Proposition 1.6. Soient E un ensemble bien ordonné par \leq et F une partie de E . Alors F est bien ordonné par l'ordre induit par \leq .

Démonstration. Soit A une partie non vide de F . C'est donc aussi une partie non vide de E . Elle admet donc un minimum. \square

Proposition 1.7. L'ensemble $\mathbb{N} \times \mathbb{N}$ est bien ordonné pour l'ordre lexicographique.

Démonstration. Soit F une partie non vide de $\mathbb{N} \times \mathbb{N}$. Considérons l'ensemble suivant :

$$A = \{a \in \mathbb{N} \mid \text{il existe } b \in \mathbb{N} \text{ tel que } (a, b) \in F\}.$$

C'est une partie de \mathbb{N} . Elle est non vide puisque F ne l'est pas. Donc, A admet un minimum a_0 . Considérons alors

$$B = \{b \in \mathbb{N} \mid (a_0, b) \in F\}.$$

C'est encore une partie non vide de \mathbb{N} . Elle admet un minimum b_0 . Montrons que (a_0, b_0) est un minimum de F . Pour $(a, b) \in F$, on a :

$$a_0 \leq a$$

puisque a_0 est un minimum de A

Si

$$a_0 < a$$

alors on obtient bien l'inégalité

$$(a_0, b_0) \leq_l (a, b)$$

Si

$$a_0 = a$$

alors on voit que

$$b_0 \leq b$$

parce que b_0 est un minimum de B . On obtient encore

$$(a_0, b_0) \leq_l (a, b)$$

□

Proposition 1.8. *Soient E un ensemble bien ordonné et f un endomorphisme de E . Alors, pour tout $a \in E$, on a*

$$a \leq f(a).$$

Démonstration. Posons

$$A = \{a \in E \mid f(a) < a\}.$$

Il s'agit de montrer que la partie A est vide. Supposons au contraire qu'elle est non vide. Alors, elle admet un élément minimum a_0 . Posons

$$a_1 = f(a_0)$$

Puisque $a_0 \in A$, on a

$$f(a_0) < a_0$$

c'est-à-dire

$$a_1 < a_0.$$

Mais $a_1 \notin A$ par minimalité de a_0 . On a donc

$$a_1 \leq f(a_1)$$

c'est-à-dire

$$f(a_0) \leq f(a_1).$$

Cela implique que f n'est pas un endomorphisme, contrairement à l'hypothèse. Donc A est vide.

□

Corollaire 1. *Si f est un automorphisme d'un ensemble bien ordonné E , alors f est l'application identité.*

Démonstration. L'application f^{-1} est aussi un automorphisme de E . Donc, en plus de l'inégalité

$$x \leq f(x)$$

on a aussi

$$f(x) \leq f^{-1}(f(x)) = x$$

pour tout $x \in E$. Donc

$$f(x) = x.$$

□

Corollaire 2. *Soient E, F deux ensembles bien ordonnés et f_1, f_2 deux isomorphismes de E sur F . Alors $f_1 = f_2$.*

Démonstration. La composée $f_2^{-1} \circ f_1$ est un automorphisme de E , et $f_1 \circ f_2^{-1}$ est un automorphisme de F . Le corollaire précédent indique donc que f_2^{-1} est l'inverse de f_1 , donc

$$f_2 = f_1.$$

□

1.5 Les treillis

1.5.1 Notions de base

soit l'ensemble E à trois éléments $\{x, y, z\}$ et l'ensemble S de tous les sous-ensembles de E , que nous allons ordonner par la relation d'inclusion au sens large \subseteq .

$$S = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$$

sur cette structure, il est aisé de voir 2 sous-ensembles possédant toujours un *ppM* qui est leur union et *pgm* qui est leur intersection. Elle a reçu le nom de treillis.

Définition 1.19. *Un treillis T est un ensemble ordonné tel que pour toute paire d'éléments x et y il existe un plus petit majorant et un plus grand minorant. Le **ppM** sera noté $x \vee y$ et le **pgm** sera noté $x \wedge y$.*

1.5.2 Demi-treillis

Définition 1.20. *Un ensemble ordonné (E, \leq) est un **sup-demi-treillis** si toute partie de deux éléments x et y de E admet un plus petit majorant M . On notera $M = x \vee y$. Duale-ment, E est un **inf-demi-treillis** si toute partie de deux éléments x et y de E admet un plus grande minorant m . On notera $m = x \wedge y$.*

1.5.3 Treillis complets

Définition 1.21. *Un treillis est dit complet s'il est à la fois un inf-demi-treillis complet et un sup-demi-treillis complet.*

1.5.4 Demi-treillis complet

Définition 1.22. *Un sup-demi-treillis complet (respectivement inf-demi-treillis complet) est un ensemble E ordonné tel qu'il existe un plus petite majorant (respectivement un plus grande minorant) pour tout sous-ensemble fini ou infini de E .*

1.5.5 Quelques exemples de treillis :

- L'ensemble des parties d'un ensemble muni de l'inclusion forme un treillis ou la borne supérieure est l'union et la borne inférieure est l'intersection.
- L'ensemble des entiers naturels muni de son ordre usuel est un treillis.
- L'ensemble des entiers naturels muni de la relation "divise" forme un treillis, ou la borne supérieure est le *PPCM* et la borne inférieure le *PGCD*.

1.5.6 Propriétés algébriques des treillis

Si x et y sont des éléments d'un treillis, les opérateurs \vee et \wedge possèdent les propriétés suivantes :

1. **Commutativité** $x \vee y = y \vee x$ et $x \wedge y = y \wedge x$.
2. **Associativité** $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ et $(x \vee y) \vee z = x \vee (y \vee z)$.
3. **Idempotence** $x \vee x = x$ et $x \wedge x = x$.
4. **Absorption** $x \vee (x \wedge y) = x$ et $x \wedge (x \vee y) = x$.

Démonstration. 1. Il est évidente.

2. On pose

$$\alpha = x \vee (y \vee z) \text{ et } \beta = (x \vee y) \vee z.$$

On a

$$\alpha \geq x \text{ et } \alpha \geq (y \vee z) \geq y$$

et comme

$$\alpha \geq (y \vee z) \geq z$$

donc

$$\alpha \geq x, \alpha \geq y, \alpha \geq z.$$

alors α est majorat de x et y c'est-à-dire

$$\alpha \geq x \vee y \text{ et } \alpha \geq z$$

$$\alpha \geq (x \vee y) \vee z$$

donc

$$\alpha \geq \beta \tag{1.1}$$

$$\beta = (x \vee y) \vee z$$

on a

$$\beta \geq x \vee y \geq x \text{ et } \beta \geq z$$

et comme

$$\beta \geq (x \vee y) \geq y$$

donc

$$\beta \geq x, \beta \geq y, \beta \geq z$$

alors β est majorat de y et z c'est-à-dire

$$\beta \geq y \vee z, \beta \geq x$$

$$\beta \geq x \vee (y \vee z)$$

donc

$$\beta \geq \alpha. \tag{1.2}$$

la même chose pour l'opérateur \wedge .

3. Cette propriété découle de la définition de la relation d'ordre, le plus petit majorant de $\{x\}$ est x et le plus grand minorant de $\{x\}$ est x .
4. On pose

$$A = x \wedge (x \vee y)$$

A est un majorant de l'ensemble $\{x, x \vee y\}$

donc

$$A \leq x \tag{1.3}$$

et comme $x \leq x$ car \leq est un relation réflexive alors

$$x \vee y = \sup \{x, y\}$$

donc

$$x \vee y \geq x$$

alors

$$A \geq x \tag{1.4}$$

d'après (1.3) et (1.4) alors $A = x$ c'est-à-dire x est un minorant de $\{x, x \vee y\}$.

□

Théorème 1.1. *Si l'ensemble E est muni de deux opérateurs que l'on notera \perp et $*$ et qui ont les propriétés suivantes :*

1. $x \perp y = y \perp x$ et $x * y = y * x$.
2. $(x \perp y) \perp z = x \perp (y \perp z)$ et $(x * y) * z = x * (y * z)$.
3. $x \perp x = x$ et $x * x = x$.
4. $x \perp (x * y) = x$ et $x * (x \perp y) = x$.

alors il existe sur E une seule relation d'ordre qui fait de E un treillis dans lequel les opérateurs \perp et $*$ donnent respectivement le *ppM* et *pgm*.

Pour démontrer ce la, nous devons énoncer les lemmes suivants :

Lemme 1.1. *Légalité $x \perp y = y$ implique légalité $x * y = x$ et réciproquement.*

Démonstration. On suppose que

$$x \perp y = y$$

alors on peut en déduire que

$$x * y = x * (x \perp y) = x$$

réciproquement : on suppose

$$x * y = x$$

alors on peut déduire que

$$x \perp y = (x * y) \perp y = y.$$

□

Lemme 1.2. *Si on définit sur T une relation binaire notée \leq par $x \leq y$ si et seulement si*

$$x \perp y = y$$

alors \leq est une relation d'ordre, de plus cette relation d'ordre fait de E un treillis et les opérateurs \vee et \wedge de ce treillis sont respectivement les opérateurs \perp et $$.*

Démonstration. On va montrer que \leq est une relation d'ordre, réflexive : on a bien

$$x \leq x$$

c'est-à-dire

$$x \perp x = x$$

à cause de l'idempotence

antisymétrique : on a bien

$$x \leq y \implies x \perp y = y \text{ et } y \leq x \implies y \perp x = x$$

et comme

$$x \perp y = y \perp x$$

on a

$$x \leq y \text{ et } y \leq x$$

c'est-à-dire

$$x = y$$

transitive : on a

$$\begin{aligned} x \perp y &= y \text{ et } y \perp z = z \\ x \perp z &= x \perp (y \perp z) = (x \perp y) \perp z = y \perp z = z \end{aligned}$$

La relation \leq est bien une relation d'ordre. Il reste à démontrer que tout couple x et y possède un ppM ($x \perp y$) et un Pgm ($x * y$). \square

Lemme 1.3. *La relation \leq définie ci dessus est la seule relation d'ordre sur E , qui fasse de E un treillis tel que les opérations \perp et $*$ définissent le ppM et le pgm .*

Démonstration. Soit R une relation d'ordre sur E différente de \leq , tel que E soit un treillis dans lequel \perp et $*$ donnent respectivement le ppM et le pgm . Si $x < y$ alors y est le ppM de (x, y) ; comme \perp donne par hypothèse le ppM , alors $x \perp y = y$. Il résulte alors du lemme précédent que $x \leq y$. On montrerait de la même manière que la relation \leq est la seule pour laquelle $x * y$ est le pgm de (x, y) . Si $x < y$ alors x est le pgm de (x, y) ; comme $*$ donne par hypothèse le pgm , alors $x * y = x$. Il résulte alors du lemme précédent que $x \leq y$. \square

1.5.7 Treillis distributif

Théorème 1.2. *Dans un treillis T les propriétés suivantes sont équivalentes :*

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Démonstration. $1 \implies 2$ On prend $(x \vee y) \wedge (x \vee z)$. On pose $\alpha = x \vee y$ par l'application de la loi d'absorption on a :

$$\begin{aligned}
 (x \vee y) \wedge (x \vee z) &= \alpha \wedge (x \vee z) \\
 &= (\alpha \wedge x) \vee (\alpha \wedge z) \\
 &= [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] \\
 &= x \vee [(x \wedge z) \vee (y \wedge z)] \\
 &= x \vee (x \wedge z) \vee (y \wedge z) \\
 &= x \vee (y \wedge z)
 \end{aligned}$$

$2 \implies 1$ On prend $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. On pose $\beta = x \wedge y$ par l'application de la loi d'absorption on a :

$$\begin{aligned}
 (x \wedge y) \vee (x \wedge z) &= \beta \vee (x \wedge z) \\
 &= (\beta \vee x) \wedge (\beta \vee z) \\
 &= [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] \\
 &= x \wedge [(x \vee z) \wedge (y \vee z)] \\
 &= x \wedge (x \vee z) \wedge (y \vee z) \\
 &= x \wedge (y \vee z)
 \end{aligned}$$

□

Définition 1.23. *Un treillis T est dit distributif si $\forall x, y, z \in E$ l'une des deux propriétés suivantes est vérifiées :*

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Proposition 1.9. *Dans un treillis distributif, on peut simplifier les propriétés algébriques suivantes comme suit :*

$$\text{si } \forall x, y, z \in E, x \wedge z = y \wedge z; \text{ et } x \vee z = y \vee z; \text{ alors } x = y.$$

Démonstration. On a

$$\begin{aligned}y &= y \vee (y \wedge z) = y \vee (x \wedge z) \\ &= (y \vee x) \wedge (y \vee z) \\ &= (y \vee x) \wedge (x \vee z) \\ &= x \vee (y \wedge z) \\ &= x \vee (x \wedge z) \\ &= x\end{aligned}$$

Donc, $y = x$. □

Exemples de treillis distributif

- Le treillis S formé par l'ensemble de tous les sous-ensembles d'un ensemble E ordonné par la relation d'inclusion est un treillis distributif.
- L'ensemble des parties de E dans lequel les opérations sont (\cap) et (\cup) au sens ensembliste est un treillis distributif.

Diagramme d'un treillis distributif

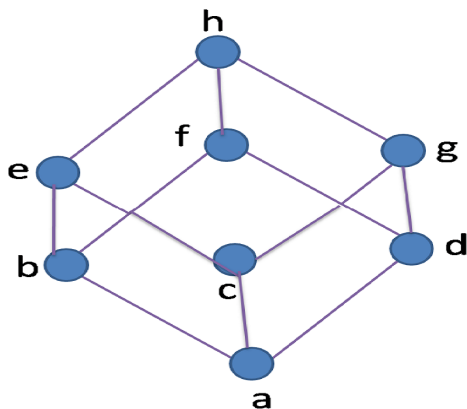


FIGURE 1.5 – treillis distributif

1.5.8 Treillis fermé

Définition 1.24. *Un treillis fermé c'est un treillis qui possède un plus petit élément m et un plus grand élément M .*

Exemples d'un treillis fermé

1. (S, \subseteq) c'est un treillis fermé (S l'ensemble des sous ensembles de E) tel que :

$$\forall A \subseteq S \text{ et } \emptyset \subseteq A.$$

2. (\mathbb{N}, \leq) n'est pas un treillis fermé car il ne possède pas un plus grand élément.

1.5.9 Treillis complémenté

Dans un treillis possédant un plus grand élément (que l'on notera $M=1$) et un plus petit élément (que l'on notera $m=0$), le **complément** d'un élément $x \in E$ est un élément $x' \in E$ tel que :

$$x \vee x' = M \text{ et } x \wedge x' = m$$

Définition 1.25. Un treillis dans lequel tout élément a au moins un complément est un **treillis complémenté**.

Remarque 1.3. Notons au passage qu'en raison de la commutativité, si y est le complément de x alors x est le complément de y .

- Dans un treillis distributif le complément d'un élément s'il existe est unique.

Diagramme d'un treillis complémenté

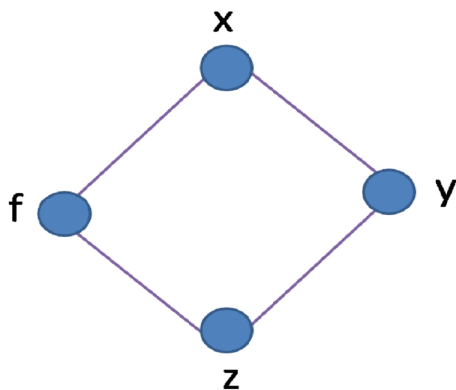


FIGURE 1.6 – treillis complémenté

1.5.10 Treillis de Boole

Définition 1.26. *Un treillis distributif et complémenté est un **treillis de Boole**.*

Théorème 1.3. *Dans un treillis de Boole, le complément est unique.*

Démonstration. Si x avait deux compléments, on aurait :

$$x \wedge y = x \wedge z = m \quad \text{et} \quad x \vee y = x \vee z = M.$$

On peut écrire par application de la loi d'absorption :

$$y = y \vee (y \wedge x)$$

ce qui donne :

$$y = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z)$$

donc,

$$y \leq z \quad \text{et} \quad z \leq y$$

ce qui prouve que y et z sont confondus. □

Exemple 6. • *Un treillis distributif, borné et complémenté s'appelle aussi une algèbre de Boole.*

- *L'ensemble des fonctions booléennes muni des opérations \vee , \wedge et de la complémentation forme une algèbre de boole et, de ce fait, un treillis booléen.*
- *L'ensemble $\rho(E)$ de tous les sous-ensembles d'un ensemble X ordonné par la relation d'inclusion est un treillis de Boole. Il comporte un élément plus grand que tous les autres qui est l'ensemble X , et un élément plus petit que tous les autres qui est l'ensemble vide.*
- *Une algèbre de Boole $\{0, 1\}$ possédant deux opérations \vee et \wedge qui sont commutatives, associatives, idempotentes et vérifiant la loi d'absorption, forme un treillis.*
- *Ces opérations étant distributives et chaque élément possédant un complément, il en résulte que toute algèbre de Boole est un treillis de Boole.*

Diagramme d'un treillis de Boole

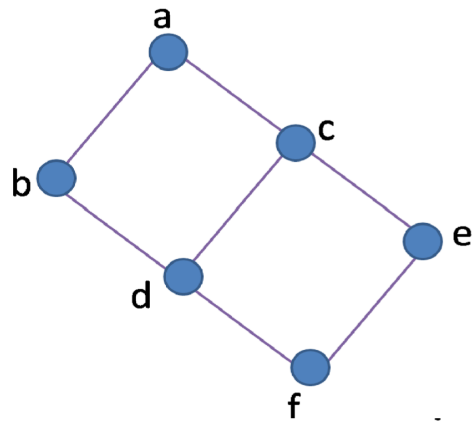


FIGURE 1.7 – treillis de Boole

1.6 Théorie des ensembles (Axiomes de Zermelo-Fraenkel)

Nous avons tous une idée intuitive de ce qu'est un ensemble, et c'est sur cette intuition que nous nous appuyons pour trouver les axiomes de la théorie des ensembles (de même que la notion intuitive de l'espace à trois dimension a conduit aux axiomes d'espace vectoriel). Mais ensuite, ayant écrit ces axiomes, nous étudierons toutes les structures qui les satisfont (de la même façon que, pour les espaces vectoriels, on ne s'intéresse pas seulement à l'espace \mathbb{R}^3 . Ces structures, qui sont appelées habituellement **univers**, sont celles d'ensembles munis d'une relation binaire (la relation d'appartenance), satisfaisant les axiomes en question.

La théorie des ensembles se présente donc comme toutes les théories axiomatiques que le lecteur connaît déjà, la théorie des groupes par exemple, ou celle des anneaux, des corps, espaces vectoriels, treillis, etc.

On considère une collection d'objets, collection que l'on appellera **univers**, et que l'on désignera par U ; on ne dit pas : "considérons un ensemble U ", car ce que nous appellerons ensembles, ce sont précisément les objets de U (il est clair que quand on définit, par exemple, les espaces vectoriels, il faut éviter d'employer le même mot pour désigner l'espace vectoriel et un vecteur de cette espace).

Cette collection, supposée non vide, est munie d'une relation binaire, que l'on note $x \in y$; elle se lit " x appartient y ", ou "l'élément x appartient à l'ensemble y ", ou encore " x est élément de y ". Bien entendu, $x \notin y$ se lit " x n'appartient pas à y ".

On réserve le mot "appartenir" pour désigner cette relation binaire \in , et il faut donc éviter, par la suite, de l'employer dans son sens intuitif (tout au moins sans préciser qu'on l'emploie dans son sens intuitif). On dira, par exemple : l'objet x est dans la collection U , au lieu de : x appartient à U .

Même remarque pour le mot "élément".

un univers se présente donc comme un graphe du genre de ce lui qui est dessiné. Sur la figure, la flèche de a vers b veut dire que $b \in a$. On a, par exemple, $c \in c$.

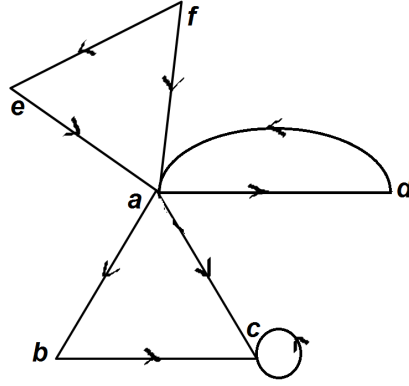


FIGURE 1.8 – Un univers

Les axiomes de la théorie des ensembles, que nous allons énoncer maintenant, expriment les propriétés que l'on impose à la relation binaire \in considérée.

1.6.1 Axiome d'extensionnalité

Définition 1.27. *Il n'existe pas dans U deux ensembles distincts qui ont les mêmes éléments ; ce qu'on peut écrire :*

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y].$$

Cet axiome n'est pas satisfait par la relation binaire représentée sur la figure : b et c sont distincts, et ont tous deux c pour seul élément.

1.6.2 Axiome de la paire

Définition 1.28. *Étant donnés deux ensembles a et b , il existe un ensemble c , qui a comme éléments a et b et eux seulement (il est unique d'après l'axiome d'extensionnalité). Ce qui s'écrit :*

$$\forall x \forall y \exists z \forall t [t \in z \Leftrightarrow (t = x \text{ ou } t = y)].$$

L'ensemble c dont les seuls éléments sont a et b est noté $\{a, b\}$. L'axiome impose en particulier que pour tout ensemble a , il existe un ensemble, noté $\{a\}$, dont le seul élément est a (prendre a et b identiques).

Si $a \neq b$, $\{a, b\}$ est appelé une paire. L'ensemble $\{a\}$ est parfois appelé un singleton.

Étant donnés deux ensembles a, b , l'ensemble $\{\{a\}, \{a, b\}\}$ est noté (a, b) et est appelé paire ordonnées, ou couple. On a :

Théorème 1.4. *si $(a, b) = (a', b')$ alors $a = a'$ et $b = b'$.*

Démonstration. Si $a = b$, alors $(a, b) = \{\{a\}\}$ et (a, b) n'a qu'un seul élément ; donc (a', b') n'a qu'un seul élément et donc $a' = b'$. On alors $\{\{a\}\} = \{\{a'\}\}$, donc $a = a'$ soit $a = a' = b = b'$.

Si $a \neq b$, (a, b) a deux éléments, donc (a', b') a deux éléments et $a' \leq b'$.

Comme $\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$, il y a deux possibilités :

ou bien $\{a\} = \{a', b'\}$ et $\{a, b\} = \{a'\}$,

ou bien $\{a\} = \{a'\}$ et $\{a, b\} = \{a', b'\}$.

La première hypothèse est fautive, puisque $\{a\}$ n'a qu'un élément et $\{a', b'\}$ en a deux. Reste que la deuxième qui donne $a = a'$, et donc $b = b'$. □

Étant donnés trois ensembles a, b, c , on appelle triplet (a, b, c) l'ensemble $(a, b, c) = (a, (b, c))$.

Théorème 1.5. *Si $(a, b, c) = (a', b', c')$ alors $a = a'$, $b = b'$ et $c = c'$.*

Démonstration. Car $(a, b, c) = (a', (b', c'))$, donc $a = a'$ et $(b, c) = (b', c')$ d'où $b = b'$ et $c = c'$. □

On définit de même le quadruplet

$$(a, b, c, d) = (a, (b, c, d))$$

et pour chaque entier $n > 0$, on définit le n-uplet (a_1, a_2, \dots, a_n) par la relation de récurrence $(a_1, a_2, \dots, a_n) = (a_1, (a_2, \dots, a_n))$. On a le :

Théorème 1.6. *Si $(a_1, a_2, \dots, a_n) = (a'_1, a'_2, \dots, a'_n)$ alors $a_1 = a'_1, \dots, a_n = a'_n$.*

Évident par récurrence sur n .

Remarquons que, étant donnés trois objets distincts a, b, c de l'univers, rien ne nous permet encore d'affirmer l'existence d'un ensemble d qui ait a, b, c comme éléments et eux seulement. L'axiome suivant remplit cette lacune.

1.6.3 Axiome de la somme (ou de la réunion)

Définition 1.29. *Pour tout ensemble a , il existe un ensemble b dont les éléments sont les éléments des éléments de a . Ce qu'on écrit :*

$$\forall x \exists y \forall z [z \in y \Leftrightarrow \exists t (t \in x \text{ et } z \in t)].$$

1.6.4 Axiome de l'ensemble des parties

Définition 1.30. Soit a, b deux ensembles ; l'énoncé $\forall x(x \in a \Rightarrow x \in b)$ est noté $a \subset b$ en abrégé et se lit "a est contenu dans b".

L'axiome de l'ensemble des parties exprime que, pour tout ensemble a , il existe un ensemble b dont les éléments sont les objets de U qui sont des parties de a . Ce qui s'écrit :

$$\forall x \exists y \forall z [z \in y \Leftrightarrow z \subset x].$$

Il n'y a qu'un seul ensemble b ayant cette propriété, d'après l'axiome d'extensionnalité. On l'appelle ensemble des parties de a , et on le note $\rho(a)$.

Remarque 1.4. Les relations que l'on peut construire à partir des deux relations binaires $x \in y$ et $x = y$ au moyen des règles ci-dessus, sont donc définies par des énoncés par les symboles $=$, \in , non, ou, \exists , des variables x, y, z, u, v, \dots et des objets de l'univers.

Définition 1.31. Une relation $R(x)$ à un argument sera aussi appelée une **collection**. Une collection est une partie (au sens intuitif) de l'univers U .

Exemple 7. L'énoncé suivant :

$$\forall u[u \in x \Rightarrow \exists v[v \in x \text{ et } \forall t(t \in v \Leftrightarrow t = u \text{ ou } t \in u)]]$$

définit une **collection**.

Exemple 8. L'énoncé $R(u, x)$:

$$u \in x \Rightarrow \exists v[v \in x \text{ et } \forall t(t \in v \Leftrightarrow t = v \text{ ou } t \in a)]$$

définit une relation **binnaire**. Si a est un objet de l'univers, l'énoncé $R(a, x)$ qui est :

$$a \in x \Rightarrow \exists v[v \in x \text{ et } \forall t(t \in v \Leftrightarrow t = a \text{ ou } t \in a)].$$

définit une **collection**

Définition 1.32. Les objets de U qui apparaissent dans un énoncé E sont appelés **les paramètres de l'énoncé E** .

Remarque 1.5. Les théorèmes de la théorie des ensembles (et en particulier les axiomes) sont des énoncés clos sans paramètres (énoncé clos (relation à 0 argument) est soit vrai)

1.6.5 Les relations

Relations d'équivalence

Définition 1.33. Une relation binaire $R(x, y)$ est appelée relation d'équivalence si, quels que soient les objets a, b, c on a :

$$R(a, b) \Rightarrow R(b, a); R(a, b) \text{ et } R(b, c) \Rightarrow R(a, c). \\ R(a, b) \Rightarrow R(a, a) \text{ et } R(b, b).$$

Définition 1.34. La collection $R(x, x)$ est appelée **domaine de la relation d'équivalence** R . $R(a, b)$ est aussi notée " $a \sim b(\text{mod.}R)$ ". Si a est un objet de l'univers, la collection $R(a, y)$ est appelée **la classe d'équivalence de a** .

Relation d'ordre(au sens large)

Définition 1.35. Une relation binaire $R(x, y)$ est une relation d'ordre (au sens large) si, quels que soient les objets a, b, c , on a :

$$R(a, b) \Rightarrow R(a, a) \text{ et } R(b, b); \\ R(a, b) \text{ et } R(b, a) \Rightarrow a = b; \\ R(a, b) \text{ et } R(b, c) \Rightarrow R(a, c).$$

Définition 1.36. La collection $R(x, x)$ est appelée **domaine** de la relation d'ordre R ; $R(a, b)$ est aussi notée " $a \leq b(\text{mod.}R)$ ". " $R(a, b)$ et $b \neq a$ " est également notée " $a < b(\text{mod.}R)$ ".

Remarque 1.6. R est une relation d'ordre total si de plus, quels que soient les objets a, b du domaine de R , on a $R(a, b)$ ou $R(b, a)$.

Relations d'ordre(au sens strict)

Définition 1.37. Considérons une collection $D(x)$ et une relation binaire $R(x, y)$; on dit que $R(x, y)$ définit une relation strict sur D si, quels que soient les objets a, b, c , on a :

$$R(a, b) \Rightarrow D(a) \text{ et } D(b); \text{ non } (R(a, b) \text{ et } R(b, a)); R(a, b) \text{ et } R(b, c) \Rightarrow R(a, c)$$

$R(a, b)$ est également notée " $a < b(\text{mod.}R)$ ".

Relations fonctionnelles

Définition 1.38. *Considérons une relation ternaire (par exemple) $R(x, y, z)$. On dit que c'est une relation fonctionnelle à deux arguments si on a :*

$$\forall x \forall y \forall z \forall z' [R(x, y, z) \text{ et } R(x, y, z') \Rightarrow z = z'].$$

Définition 1.39. *La relation binaire $\exists z R(x, y, z)$ est alors appelée **domaine** de la relation fonctionnelle R . La collection $\exists x \exists y R(x, y, z)$ est appelée **image** de la relation fonctionnelle R .*

Nous pouvons maintenant énoncer d'autres axiomes de la théorie des ensembles.

1.6.6 Schéma d'axiomes de substitution (ou de remplacement)

Définition 1.40. *Soit $E(x, y, a_1, \dots, a_k)$ un énoncé dont les paramètres sont a_1, \dots, a_k , qui définit une relation fonctionnelle à un argument, et soit a un ensemble quelconque ; on impose à l'univers U de satisfaire la collection suivante : il existe un ensemble b dont les éléments sont exactement les images, par la relation fonctionnelle considérée, des éléments de a qui se trouvent dans le domaine de cette relation fonctionnelle.*

Le schéma d'axiomes de substitution consiste donc en la liste infinie des énoncés suivants :

$$\forall x \dots \forall x_k \{ \forall x \forall y \forall y' ((E(x, y, x_1, \dots, x_k) \text{ et } E(x, y', x_1, \dots, x_k) \Rightarrow y = y') \Rightarrow \forall t \exists u \forall y [y \in u \Leftrightarrow \exists x (x \in t \text{ et } E(x, y, x_1, \dots, x_k))]) \}$$

où $E(x, y, x_1, \dots, x_k)$ est un énoncé arbitraire, sans paramètre, qui a au moins deux variables libres x et y .

Remarque 1.7. *Les axiomes (axiome d'extensionnalité, axiome de la paire, axiome de la somme, axiome de l'ensemble des parties) et le schéma d'axiomes, et l'axiome de l'infini sera énoncé après, forment ce qu'on appelle la théorie des ensembles de **Zermelo-Fraenkel** (en abrégé **ZF**).*

1.6.7 Schéma de compréhension

Définition 1.41. *Considérons un ensemble a et un énoncé $E(x, a_1, \dots, a_k)$ à une variable libre dont paramètre sont a_1, \dots, a_k ; alors il existe un ensemble b dont les éléments sont ceux des éléments de a qui satisfont l'énoncé A . Le schéma de compréhension consiste donc en la liste infinie des énoncés suivants :*

$$\forall x_1 \dots \forall x_k \forall x \exists y \forall z [z \in y \Leftrightarrow (z \in x \text{ et } A(z, x_1, \dots, x_k))]$$

dans laquelle $A(x, x_1, \dots, x_k)$ est n'importe quel énoncé sans paramètres qui a moins une variable libre x . Pour le démontrer, il suffit de remarquer que l'énoncé $E(x, y, x_1, \dots, x_k)$ qui s'écrit " $y = x$ et $A(x, a_1, \dots, a_k)$ " définit une relation fonctionnelle à un argument dont le domaine est la collection $A(x, a_1, \dots, a_k)$. D'après le schéma de substitution, il existe donc un ensemble b formé des images des éléments de a qui sont dans ce domaine; b est donc formé des éléments de a qui sont dans la collection $A(x, a_1, \dots, a_k)$. On utilisera la notion $b = \{x \in a; A(x, a_1, \dots, a_k)\}$ pour représenter cet ensemble.

Théorème 1.7. *Il existe un ensemble et un seul qui n'a aucun élément.*

1.7 Ordinaux et cardinaux

1.7.1 Relation de bon ordre

Définition 1.42. *Considérons une relation d'ordre $R(x, y)$ et un ensemble a , dont tous les éléments sont dans le domaine de R . On dit que a est bien ordonnée par R si tout sous-ensemble non vide de a possède un plus petit élément (mod. R). Il est clair que, si a est bien ordonnée par R , tout sous-ensemble de a est bien ordonnée par R .*

Définition 1.43. Ensemble bien ordonnée Un ensemble bien ordonné u est, par définition, un couple (a, r) tel que $r \subset a^2$ et tel que l'ensemble a soit bien ordonnée par la relation " $((x, y) \in r)$ ".

Définition 1.44. *Un ensemble bien ordonné (a, r) est totalement ordonné : en effet, si $x, y \in a$, l'ensemble $\{x, y\}$ a un plus petit élément, donc $(x, y) \in r$ ou $(y, x) \in r$*

Remarque 1.8. *Considérons un ensemble a , bien ordonnée par la relation d'ordre R .*

Définition 1.45. *Un sous-ensemble s de a sera appelé **segment initial** s'il a la propriété suivante : quels que soit $x, y \in a$, si $x \in s$ et $y \leq x$ (mod. R) alors $y \in s$.*

Pour chaque $x_0 \in a$, on désigne par $S_{x_0}(a, R)$, ou par $S_{x_0}(a)$ s'il n'y a pas d'ambiguïté sur R , l'ensemble $\{x \in a; x < x_0(\text{mod.}R)\}$. C'est évidemment un segment initial de a .

Propriétés 1.2. *Pour que $s \subset a$ soit un segment initial, il faut et il suffit que $s = a$, ou que $s = S_{x_0}(a)$ pour un $x_0 \in a$.*

Démonstration. En effet, si s est un segment initial de a , et si $s \neq a$, l'ensemble $\{x \in a; x \notin s\}$ (la différence ensembliste entre a et s , noté $a \setminus s$) est non vide, donc a a un plus petit élément x_0 . Si $x < x_0$, on a donc $x \in s$; si $x \geq x_0$ on ne peut avoir $x \in s$, car alors x_0 serait élément de s . \square

Définition 1.46. *Un segment initial de a , qui est différent de a , est appelé **segment initial strict** de a .*

Définition 1.47. *Une relation d'ordre total R est dite relation de bon ordre si elle a la propriété suivante : pour tout objet x du domaine de R , la collection, (noté $S_x(R)$), des objets y du domaine de R tels que $y < x$ (mod. R) est un ensemble et R est une relation de bon ordre sur cet ensemble.*

Propriétés 1.3. *Soient R une relation de bon ordre, D son domaine, T une sous-collection non vide de D (c'est-à-dire $\forall x(T(x) \Rightarrow D(x))$ et $\exists xT(x)$). Alors T a un plus petit élément (mod. R).*

Démonstration. Soit en effet x_0 un objet de T ; ou bien x_0 est le plus petit élément de T , ou bien la collection " T et $S_{x_0}(R)$ " est non vide; mais cette collection est un ensemble (car $S_{x_0}(R)$ en est un) non vide et contenu dans l'ensemble bien ordonné $S_{x_0}(R)$. Il a donc un plus petit élément, qui est évidemment le plus petit élément de T . \square

1.7.2 La collection des ordinaux

Définition 1.48. On dit qu'un ensemble α est un ordinal, s'il a les deux propriétés suivantes :

1. La relation $x \in y$ est, sur α , une relation d'ordre strict qui est un bon ordre (donc un ordre total).
2. Si $x \in \alpha$, alors $x \subset \alpha$.

Remarque 1.9. La relation à un argument (collection) : " α est un ordinal" est écrit **On**(α).

L'énoncé **On**(α) est donc :

$$\begin{aligned} & \forall x \forall y [x \in \alpha \text{ et } y \in \alpha \Rightarrow x \notin y \text{ ou } y \notin x] \text{ et} \\ & \forall x \forall y \forall z [x \in \alpha \text{ et } y \in \alpha \text{ et } z \in \alpha \text{ et } x \in y \text{ et } y \in z \Rightarrow x \in z] \text{ et} \\ & \forall z [z \subset \alpha \text{ et } z \neq \emptyset \Rightarrow \exists x (x \in z \text{ et } \forall y (y \in z \Rightarrow x \in y \text{ ou } x = y))] \text{ et} \\ & \forall x \forall y [x \in \alpha \text{ et } y \in x \Rightarrow y \in \alpha]. \end{aligned}$$

Exemple 9. On vérifie aisément que $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ sont des ordinaux.

1. Soit α un ordinal; alors les segments initiaux de α sont α et les éléments de α .
2. En effet, les segments initiaux de α , différent de α , sont les $S_\xi(\alpha)$ pour $\xi \in \alpha$.

Or on a :

$$S_\xi(\alpha) = \{\eta \in \alpha; \eta < \xi\} = \{\eta \in \alpha; \eta \in \xi\} = \xi \cap \alpha = \xi.$$

puisque $\xi \subset \alpha$.

Propriétés 1.4. Tous les éléments d'un ordinal α sont des ordinaux.

Démonstration. Soit en effet $\xi \in \alpha$; alors $\xi \subset \alpha$ et donc la relation $x \in y$ est un bon ordre sur ξ . D'autre part, si $x \in \xi$ et $y \in x$, alors $x \in \xi$ (car $\xi \subset \alpha$) donc $y \in \alpha$ (car $x \subset \alpha$). Comme \in est une relation d'ordre sur α , on a donc $y \in \xi$. \square

Propriétés 1.5. Pour tout ordinal α , $\alpha \notin \alpha$.

Démonstration. Soit ξ un élément quelconque de ξ . Alors $\xi \notin \xi$ puisque \in est une relation d'ordre strict sur α . En particulier, si α est élément de α , alors $\alpha \notin \alpha$, ce qui est une contradiction. \square

Propriétés 1.6. *Soit α, β deux ordinaux. Alors $\alpha = \beta$ ou $\beta \in \alpha$ ou $\alpha \in \beta$ et ces trois cas s'excluent l'un l'autre.*

Démonstration. On pose $\xi = \alpha \cap \beta$. Alors ξ est un segment initial de α : si $x \in \xi, y \in x$, alors $x \in \alpha$ et $x \in \beta$, donc $y \in \alpha$ et $y \in \beta$ et donc $y \in \xi$. De même, ξ est un segment initial de β . Donc $(\xi = \alpha$ ou $\xi \in \alpha)$ et $(\xi = \beta$ ou $\xi \in \beta)$. On a donc quatre cas possibles :

- $\xi = \alpha$ et $\xi = \beta$; alors $\alpha = \beta$.
- $\xi = \alpha$ et $\xi \in \beta$; alors $\alpha \in \beta$.
- $\xi = \beta$ et $\xi \in \alpha$; alors $\beta \in \alpha$.
- $\xi \in \alpha$ et $\xi \in \beta$; alors ξ est un ordinal et $\xi \in \alpha \cap \beta$, soit $\xi \in \xi$ ce qui est une contradiction puisque ξ est un ordinal;

On ne peut avoir $\alpha = \beta$ et $\alpha \in \beta$ puisque $\beta \notin \beta$; on ne peut avoir $\alpha \in \beta$ et $\beta \in \alpha$: car $\alpha \in \beta \Rightarrow \alpha \subset \beta$, et si $\beta \in \alpha$ on a alors $\beta \in \beta$.

\square

Propriétés 1.7. *La relation d'appartenance sur la collection \mathbf{On} (c'est-à-dire la relation binaire " $x \in y$ et $\mathbf{On}(x)$ et $\mathbf{On}(y)$ ") est une relation de bon ordre.*

Démonstration. On vient de montrer que c'est une relation d'ordre total strict. De plus, pour tout ordinal $\alpha, S_\alpha(\mathbf{On}) = \alpha$ (car $\xi < \alpha \Leftrightarrow \xi \in \alpha$).

Noter que si α, β sont des ordinaux, $(\alpha \leq \beta \Leftrightarrow \alpha \subset \beta)$.

\square

Remarque 1.10. 1. *La collection \mathbf{On} n'est pas un ensemble.*

2. *Si α est un ordinal, le plus petit ordinal $> \alpha$ est $\alpha \cup \{\alpha\}$. On l'appelle successeur de α et on le note aussi $\alpha + 1$.*
3. *Tout ensemble d'ordinaux a une borne supérieure qui est réunion des éléments de cet ensemble.*

Lemme 1.4. *Soient α et β deux ordinaux, et $f : \alpha \rightarrow \beta$ une application strictement croissante. Alors $\alpha \leq \beta$ et $\xi \leq f(\xi)$ pour tout $\xi \in \alpha$.*

Démonstration. Soit ξ le plus petit élément de α tel que $f(\xi) < \xi$ s'il en existe. Comme f est strictement croissante, on a $f(f(\xi)) < f(\xi)$. Donc, en posant $\eta = f(\xi)$, on a $\eta < \xi$ et $f(\eta) < \eta$, ce qui contredit la définition de ξ . Pour tout $\gamma \in \alpha$, on a donc $\gamma \leq f(\gamma) \in \beta$, donc $\gamma \in \beta$. Il en résulte que $\alpha \subset \beta$, donc $\alpha \leq \beta$. \square

Théorème 1.8. *Soient α et β deux ordinaux, et f un isomorphisme d'ensemble ordonnés de α sur β . Alors $\alpha = \beta$, et f est l'application identique.*

Démonstration. D'après le lemme précédente, on a $\alpha \leq \beta$, et $\gamma \leq f(\gamma)$ pour tout $\gamma \in \alpha$. Comme f^{-1} est un isomorphisme de β sur α , on a $\beta \leq \alpha$ (et donc $\alpha = \beta$), et $\gamma \leq f^{-1}(\gamma)$ pour tout $\gamma \in \beta$. En appliquant f aux deux membres de cette inégalité, on obtient $f(\gamma) \leq \gamma$, et donc $f(\gamma) = \gamma$ pour tout $\gamma \in \alpha$. \square

Théorème 1.9. *Pour chaque ensemble bien ordonné u , il existe un isomorphisme et un seul de u sur un ordinal.*

1.7.3 L'axiome du choix

L'axiome du choix (en abrégé AC) est l'axiome suivant :

Définition 1.49. *Pour chaque ensemble a , dont les éléments sont non vide et disjoints deux à deux, il existe un ensemble dont l'intersection avec chaque élément de a est un ensemble à un seul élément.*

Ce qu'on peut écrire :

$$\forall a \{ [\forall x (x \in a \Rightarrow x \neq \emptyset) \text{ et } \forall x \forall y (x \in a \text{ et } y \in a \Rightarrow x = y \text{ ou } x \cap y = \emptyset)] \Rightarrow \exists b \forall x \exists u (x \in a \Rightarrow b \cap x = \{u\}) \}.$$

Les énoncés suivants sont équivalents à AC (moyennant les autres axiomes) :

- AC' : Pour ensemble a , il existe une application h de l'ensemble des parties non vide de a dans a , telle que $h(x) \in x$ pour tout partie x non vide de a .
- AC'' : Le produit d'une famille d'ensemble non vide est non vide

1.7.4 Cardinaux

Remarque 1.11. *Soient A, B les parties de l'univers U formées respectivement des éléments de a et de b . Alors A et B peuvent être équipotents (au sens intuitif) sans que a et b soient*

équipotents : en effet, dire que a et b sont équipotents revient à dire qu'il existe une bijection (au sens intuitif) de A sur B et, de plus, que cette bijection correspond à un objet de l'univers.

Il est clair que la relation " x est équipotent à y " est une relation d'équivalence dont le domaine est la collection de tous les ensembles.

D'après l'axiome du choix, tout ensemble a est équipotent à un ordinal : car il existe un bon ordre sur a , donc un isomorphisme de a muni de ce bon ordre sur un ordinal.

Définition 1.50. On appelle **cardinal** de a , et on désigne par \bar{a} , ou par $\text{card}(a)$, le plus petit ordinal équipotent à a .

Remarque 1.12. 1. Deux ensembles a et b sont équipotents si et seulement $\bar{a} = \bar{b}$.

2. La collection des cardinaux est désignée par \mathbf{Cn} . Elle est donc définie par l'énoncé suivant, noté $\mathbf{Cn}(\alpha)$: " a est un ordinal qui n'est équipotent à aucun ordinal $\beta < \alpha$ ". notons cette définition n'utilise pas AC.

Théorème 1.10. Soient a, b deux ensembles non vides. Les conditions suivantes sont équivalentes :

1. Il existe une injection de a dans b ;
2. Il existe une surjection de b sur a ;
3. $\bar{a} = \bar{b}$.

Corollaire 3. théorème de Cantor-Bernstein

Pour que deux ensembles a et b soient équipotents, (il faut et) il suffit qu'il existe une injection de chacun des deux dans l'autre.

Démonstration. En effet, s'il existe une injection de a dans b , et une injection de b dans a , on a $\bar{a} \leq \bar{b}$ et $\bar{b} \leq \bar{a}$, d'où $\bar{a} = \bar{b}$. Nous avons démontré ce théorème en utilisant l'axiome du choix, et aussi on peut le démontrer sans cet axiome. □

Théorème 1.11. Cantor • Pour tout ensemble a $\bar{a} < \overline{\rho(a)}$.

Démonstration. Supposons que $\bar{a} \leq \overline{\rho(a)}$; il existe alors une injection h de a sur $\rho(a)$. Soit $b = \{x \in a; x \notin h(x)\}$. Alors b est une partie de a , donc il existe $c \in a$ tel que $h(c) = b$. Mais $c \in b \Leftrightarrow c \notin b$ ce qui est une contradiction. □

1.7.5 Axiome de l'infini

Définition 1.51. On peut énoncer l'axiome de l'infini sous la forme :

- *Il existe un ordinal limite*

La forme de cette axiome :

$$\exists x[0 \in x \text{ et } \forall y(y \in x \implies y \cup \{y\} \in x)].$$

Chapitre 2

Algèbre de Boole

Dans ce chapitre on va étudier les algèbres de Boole en général (atomes dans une algèbre de Boole, homomorphisme d'algèbre de Boole, idéaux et filtres)

2.1 Rappels d'algèbre et de topologie

2.1.1 Algèbre

On considère un anneau commutatif et unitaire $A = \langle E, +, \times, 0, 1 \rangle$.

On supposera toujours que, dans tel anneau, on a $0 \neq 1$. Comme c'est l'usage, nous nous permettons, pour désigner le produit de deux éléments a et b de E , d'utiliser indifféremment la notation $a \times b$ ou la notation ab .

Définition 2.1. Idéal

Un **idéal** de A est un sous-ensemble I de E , tel que :

1. $\langle I, +, 0 \rangle$ est un sous-groupe de $\langle E, +, 0 \rangle$.
2. Pour tout élément x de I et Pour tout élément y de E , $xy \in I$.

L'ensemble E lui-même satisfait clairement ces conditions.

Définition 2.2. Un idéal de A distinct de E est appelé **idéal propre**. Un idéal I de A est un idéal propre si et seulement si $1 \notin I$. (Si $I = E$, alors $1 \in I$, pour tout élément y de E , $1 \times y = y \in I$, donc $E = I$).

Nous ne considérons ici que des idéaux propres. Un idéal de A sera pour nous une partie I de A qui vérifie, en plus des deux conditions ci-dessus, la propriété suivante :

3. $1 \notin I$.

Adopter ce point de vue peut avoir quelques inconvénient : par étant donnés deux idéaux I et J de A , il n'y a pas nécessairement de plus petit idéal de A contenant à la fois I et J , car la **somme** des idéaux I et J (c'est-à-dire l'ensemble $I + J = \{x \in A; (\exists y \in I)(\exists z \in J)(x = y + z)\}$), qui joue habituellement ce rôle, peut fort bien ne pas être un idéal propre. Ainsi, dans l'anneau \mathbb{Z} des entiers relatifs, la somme des idéaux $2\mathbb{Z}$ (ensemble des multiple de 2) et $3\mathbb{Z}$ et l'anneau \mathbb{Z} tout entier.

Définition 2.3. Idéal maximal

Un idéal maximal est un idéal qui n'est strictement inclus dans aucun autre idéal.

Théorème 2.1. Krull. *Tout idéal d'anneau commutatif et unitaire est contenu dans au moins un idéal maximal.*

Démonstration. La démonstration utilise le théorème de **Zorn**. Soit I un idéal de l'anneau A . Désignons par Φ l'ensemble des idéaux de A qui contient I :

$\Phi = \{J \in B(A); J \text{ est un idéal et } I \subseteq J\}$. Le théorème sera démontré si nous prouvons montrer l'existence d'au moins un élément maximal dans l'ensemble ordonné $\langle \Phi, \subseteq \rangle$. Mais il suffit pour cela (théorème de Zorn) de montrer que cet ensemble ordonné est non vide (mais cela est clair car $I \in \Phi$) et que toute partie totalement ordonnée non vide de Φ admet au moins un majorant dans Φ . Soit donc X une partie de Φ totalement ordonnée par la relation d'inclusion (on dit aussi : une **chaîne** de $\langle \Phi, \subseteq \rangle$); on suppose X non vide. Appelons I_0 la réunion des éléments de X : $I_0 = \cup_{J \in X} J$. Comme X est non vide, et comme n'importe quel élément de X contient I , I est inclus dans I_0 , donc $0 \in I_0$. Si x et y sont des éléments de I_0 , il y a deux idéaux J et K dans X tel que $x \in J$ et $y \in K$. Comme X est totalement ordonnée, on a $J \subseteq K$ ou $K \subseteq J$. Si on est, par exemple, dans le premier cas, alors $x \in K$ et $y \in K$, donc $x - y \in K$ et $x - y \in I_0$. On en déduit que $\langle I_0, +, 0 \rangle$ est un sous-groupe de $\langle E, +, 0 \rangle$. Par ailleurs, si $x \in I_0$ et $y \in E$, alors pour au moins un idéal $J \in X$, on a $x \in J$, donc $xy \in J$ et $xy \in I_0$. Enfin, on a $1 \notin I_0$, car dans le cas contraire 1 appartiendrait à l'un des éléments de X , ce qui est exclu. Nous avons ainsi établi que I_0 est un idéal de A qui contient I , c'est-à-dire un élément de Φ . Pour chaque J dans X , $J \subseteq I_0$: il en résulte que I_0 est, dans Φ , un majorant de la chaîne de X . \square

Définition 2.4. *Soit I un idéal de l'anneau A . On définit sur E une relation d'équivalence, appelée **congruence modulo I** et notée \equiv_I , par : quel que soit les éléments x et y de E , $x \equiv_I y$ si et seulement si $x - y \in I$.*

Le fait que c'est bien une relation d'équivalence se prouve très facilement. Notons \bar{a} la classe d'équivalence de l'élément $a \in E$. On a $\bar{0} = I$. La congruence modulo I est compatible avec les

opérations $+$ et \times de l'anneau : cela veut dire que, si a, b, c et d sont des éléments de E , si $a \equiv_I c$ et $b \equiv_I d$, alors $a + b \equiv_I c + d$ et $a \times b \equiv_I c \times d$. Ceci permet de définir sur l'ensemble E/ \equiv des classes d'équivalence deux opérations, qu'on se permettra de noter encore $+$ et \times , définies par : pour tous éléments x et y de E , $\bar{x} + \bar{y} = \overline{x + y}$ et $\bar{x} \times \bar{y} = \overline{x \times y}$. Ces deux opérations confèrent à l'ensemble E/ \equiv une structure d'anneau commutatif et unitaire (le zéro est I , l'élément unité est $\bar{1}$) appelé **anneau quotient** de A par l'idéal I et noté A/I plutôt que A/ \equiv_I . Toutes les vérifications à faire sont élémentaires. L'exemple le plus connu de ce que nous venons de décrire nous est fourni par les anneaux $\mathbb{Z}/n\mathbb{Z}$ (n étant un entier naturel supérieur ou égal à 2).

Théorème 2.2. *L'anneau quotient A/I est un corps si et seulement si l'idéal I est maximal.*

Démonstration. Si on suppose que I n'est pas maximal, on peut alors choisir un idéal J de A tel que $I \subsetneq J$ (inclusion stricte). Soit a un élément de J qui n'appartient pas à I , on a $\bar{a} \neq I$, donc \bar{a} est un élément non nul dans l'anneau quotient. Si cet élément était inversible, il y aurait un élément $b \in E$ tel que $\bar{a} \times \bar{b} = \bar{1}$ c'est-à-dire $ab \equiv_I 1$, ou encore $ab - 1 \in I$, donc aussi $ab - 1 \in J$. Or $a \in J$ et J est un idéal, donc $ab \in J$, alors la différence

$$ab - (ab - 1) = 1$$

appartient à J , ce qui est impossible. On en déduit qu'il existe au moins un élément non nul et non inversible dans l'anneau A/I , celui-ci n'est pas donc un corps. Supposons maintenant que I soit maximal. Soit a un élément de E tel que $\bar{a} \neq \bar{0}$ (autrement dit $a \notin I$). Nous nous proposons de montrer que \bar{a} est un élément inversible dans l'anneau quotient A/I . Considérons l'ensemble K suivant :

$$K = \{x \in E, (\exists y \in E) (\exists z \in I), x = ay + z\}.$$

Il est facile de vérifier que $\langle K, +, 0 \rangle$ est un sous-groupe de $\langle E, +, 0 \rangle$: tout d'abord $0 \in K$ puisque $0 = (a \times 0) + 0$; de plus, si $x_1 \in K$ et $x_2 \in K$, alors on peut trouver des éléments y_1 et y_2 dans E , et z_1 et z_2 dans I , tel que :

$$x_1 = ay_1 + z_1 \quad \text{et} \quad x_2 = ay_2 + z_2$$

on en déduit que

$$\begin{aligned} x_1 - x_2 &= a(y_1 - y_2) + z_1 - z_2 \\ y_1 - y_2 &\in E \quad \text{et} \quad z_1 - z_2 \in I \quad \text{donc} \quad x_1 - x_2 \in K. \end{aligned}$$

D'autre part, si $x \in K$ et $t \in E$, alors $xt \in K$: en effet il y a des éléments $y \in E$ et $z \in I$ tel que

$$x = ay + z$$

donc

$$xt = a(ty) + tz$$

mais $ty \in E$ et $tz \in I$, d'où $xt \in K$. On voit ainsi que les deux premières conditions de la définition d'un idéal sont satisfaites par K . Si la troisième de ces conditions était également satisfaite (donc si $1 \notin K$), K serait un idéal de A .

Mais l'ensemble K contient strictement l'ensemble I : en effet, tout élément x de I peut s'écrire $x = (a \times 0) + x$, donc appartient aussi à K , et l'élément a , qui peut s'écrire $(a \times 1) + 0$, appartient à K mais pas à I . Comme I est un idéal maximal, K ne peut donc pas être un idéal de A . On en déduit que $1 \in K$, on peut donc trouver deux éléments $y \in E$ et $z \in I$ tel que :

$$ay + z = 1.$$

On a donc $1 - ay = z \in I$, ou encore, en passant aux classes d'équivalence pour la relation \equiv_I , $\overline{1 - ay} = \bar{0}$, ce qui se traduit par $\bar{a} \times \bar{y} = \bar{1}$, l'élément \bar{a} admet donc un inverse dans l'anneau quotient A/I . Nous avons donc montré que tout élément non nul de cet anneau est inversible : A/I est donc un corps. \square

Remarque 2.1. *On remarquera qu'il y a dans la démonstration que venons de faire une illustration de ce que nous disions plus haut au sujet de la somme de deux idéaux. En effet, l'ensemble K que nous avons considéré est la somme de l'idéal et ce que l'on appelle l'idéal principal engendré par a (c'est à dire l'idéal constitué des multiples de a). Or nous nous sommes justement trouvés dans un cas où cette somme d'idéaux était l'anneau tout entier.*

2.1.2 Topologie

Soit X un ensemble quelconque et $\rho(X)$ l'ensemble des parties de X .

Définition 2.5. *On appelle topologie sur X toute partie T de $\rho(X)$ vérifiant les trois propriétés suivantes :*

1. *La réunion de toute famille d'éléments de T appartient à T .*
2. *L'intersection de toute famille finie d'éléments de T appartient à T .*
3. *L'ensemble vide \emptyset et X appartient à T .*

Définition 2.6. *On appelle **espace topologique** le couple (X, T) de support X . Les éléments de T sont appelés ouverts de (X, T) ou de T , souvent noté O .*

Remarque 2.2. *1. La réunion de la famille vide de parties de X étant vide et son intersection égale à X , propriété (3) se déduit de (1) et (2).*

2. Pour (2) il suffit de montrer, en général, que l'intersection de deux éléments de T appartient à T .
3. $T \in \rho(\rho(X))$
4. Toute partie de $\rho(X)$ n'est pas une topologie.

Exemple 10. 1. L'ensemble des parties A de \mathbb{R} telle que, pour tout $x \in A$, il existe un intervalle ouvert $]a, b[$ tel que $x \in [a, b] \subset A$ est une topologie sur \mathbb{R} appelée topologie euclidienne.

2. Si $X = \emptyset$, $\rho(X) = \{\emptyset\}$ est la seule topologie sur X .
3. Si X possède au moins deux éléments $X = \{a, b\}$, alors $T = \{\emptyset, \{a\}, X\}$ est une topologie sur X est dite topologie de Sierpink¹.
4. Si $X = \{a\}$, $\rho(X) = \{\emptyset, \{a\}\}$ est la seule topologie sur X .

Base d'une topologie

Définition 2.7. On appelle base d'une topologie T toute partie P de T telle que tout ouvert O de T soit la réunion d'une famille d'ouverts de P .

Remarque 2.3. \emptyset étant la réunion de la famille vide, il n'est pas nécessaire que $\emptyset \in P$.

Exemple 11. 1. T est une base de T .

2. $\{\{x\} | x \in X\}$ est une base de la topologie discrète.

Voisinage

Soit X un espace topologique, qu'on notera pour simplifier X .

Définition 2.8. 1. On appelle voisinage d'un point $x \in X$, toute partie de X qui contient un ouvert contenant $\{x\}$.

2. Plus généralement on appelle voisinage d'une partie A de X , toute partie de X qui contient un ouvert contenant A . On note :

$v(x)$ l'ensemble des voisinages de x .

$v(A)$ l'ensemble des voisinages de A .

Caractérisation des ouverts

Propriétés 2.1. Pour qu'une partie A de X soit ouverte, il faut et il suffit que A soit voisinage de chacun de ses points.

Base de voisinage

Définition 2.9. On appelle base de voisinage de x toute partie $s(x)$ de $v(x)$ telle que, pour tout $V \in v(x)$, V contient un voisinage W de $s(x)$.

Fermé

Soit X un espace topologique. Introduisons la définition suivant :

Définition 2.10. On dit qu'une partie A de X est fermé si son complémentaire par rapport à X , noté $\complement_X A$ est ouvert.

Exemple 12. 1. $\{a\}$, $[a, b]$ et $[a, +\infty[$ sont fermés dans \mathbb{R} .

2. $[a, b[$ et \mathbb{Q} ne sont ni ouverts ni fermés dans \mathbb{R} .

Topologie induite

Définition 2.11. Soient X un espace topologique et Y un sous-ensemble de X . On munit Y d'une topologie, appelée **topologie induite** sur Y par celle de X , en prenant comme ouverts de cette topologie les traces sur Y des ouverts de X , en d'autres termes pour qu'une partie $\Omega \subseteq Y$ soit un ouvert pour la topologie induite, il faut et il suffit qu'il existe un ouvert O de la topologie sur X tel que $\Omega = O \cap Y$.

On voit immédiatement que les fermés pour la topologie induite sont les traces sur Y des fermés de X . Lorsque nous parlerons d'un sous-espace de l'espace topologique X , il s'agira d'une sous-ensemble muni de la topologie induite.

Bases des ouverts

Définition 2.12. Une **base d'ouverts** pour la topologie de l'espace X , c'est une famille $(O_i)_{i \in I}$ d'ouverts de cette topologie, tel que tout ouvert soit réunion d'ouverts de cette famille, autrement dit, pour tout ouvert G , il existe au moins un sous-ensemble $J \subseteq I$ tel que :

$$G = \cup_{j \in J} O_j.$$

Lorsqu'une base d'ouverts a été choisie dans un espace topologique, les éléments de cette base d'ouverts sont appelés **ouverts élémentaires**.

Les complémentaires dans X des ouverts élémentaires sont les **fermés élémentaires** , et il est clair que tout fermé est une intersection de fermés élémentaires.

Pour la topologie usuelle de l'ensemble \mathbb{R} des nombres réels, les intervalles ouverts bornés (c'est-à-dire les ensembles de la forme $]a, b[$ ou $a \in \mathbb{R}, b \in \mathbb{R}$ et $a \leq b$) constituent une base d'ouverts. D'autre part, il est évident que, dans un espace topologique quelconque, la famille de tous les ouverts est une base d'ouverts.

Lemme 2.1. Si $(O_i)_{i \in I}$ est une base d'ouverts pour la topologie de X et si Y est une partie de X , alors la famille $(O_i \cap Y)_{i \in I}$ est une base d'ouverts pour la topologie induite sur Y par celle de X .

Cela signifie que les traces sur Y des ouverts élémentaires de X sont des ouverts élémentaires pour Y .

La continuité dans l'espace topologique

Définition 2.13. Soient X et Y deux espaces topologiques, une application f de X dans Y est dite **continue** si et seulement si l'image réciproque par f de tout ouvert de Y est un ouvert de X . Autrement dit, f est continue si et seulement si, pour tout ouvert Ω de Y , l'ensemble :

$$f^{-1}[\Omega] = \{x \in X, f(x) \in \Omega\}$$

est un ouvert de X .

Lemme 2.2. Soit $(\Omega_i)_{i \in I}$ une base d'ouverts de l'espace topologique Y , et soit f une application de X dans Y . Pour que f soit continue, il est nécessaire et suffisant que, pour tout indice $i \in I$, $f^{-1}[\Omega_i]$ soit un ouvert de X .

Démonstration. C'est nécessaire d'après la définition de la continuité (ce qui est vrai pour tous les ouverts de Y est en particulier vrai pour tous les ouverts élémentaire).

C'est suffisant car si Ω est un ouvert quelconque de Y , alors il existe une partie $J \subseteq I$ tel que :

$$\Omega = \cup_{j \in J} O_j, \text{ d'où } f^{-1}[\Omega] = \cup_{j \in J} f^{-1}[O_j]$$

(c'est là une propriété bien connue de l'image réciproque), si tous les $f^{-1}[O_j]$ sont des ouverts de X , $f^{-1}[\Omega]$ sera une réunion d'ouverts, donc un ouvert de X . \square

Homéomorphisme de l'espace topologique

Définition 2.14. Un **homéomorphisme** de l'espace topologique X sur l'espace topologique Y est une application de X dans Y , bijective, continue, et dont la bijection réciproque est une application continue de Y dans X . (on parle alors d'application bijective et **bicontinue**).

Séparation d'un espace topologique

Définition 2.15. Un espace topologique X est dite **séparé** si et seulement si, quels que soient les éléments distincts x et y de X , on peut trouver deux ouverts disjoints G et H tel que $x \in G$ et $y \in H$.

Lemme 2.3. Soit X un espace topologique séparé et soit Y un sous-ensemble de X . Alors la topologie induite sur Y par celle de X fait de Y un espace séparé.

Démonstration. Si x et y sont des points distincts de Y , les traces sur Y de deux ouverts disjoints de X contenant respectivement x et y sont deux ouverts disjoints de la topologie de Y contenant respectivement x et y . □

Recouvrement de l'espace topologique

Définition 2.16. Un recouvrement de l'espace topologique X est une famille $(E_i)_{i \in I}$ de parties de X tel que $X = \cup_{i \in I} E_i$. Si tout les E_i sont des ensembles ouverts, on parlera de recouvrement ouvert.

Un **sous-recouvrement** du recouvrement $(E_i)_{i \in I}$ est une sous-famille $(E_j)_{j \in J}$, qui est elle même un recouvrement de X . On parlera de recouvrement (ou de sous-recouvrement) **fini** lorsque l'ensemble d'indices correspondant sera un ensemble fini.

Compacité

Définition 2.17. Un espace topologique X est dit **compact** si et seulement si, d'une part, il est séparé, et d'autre part, de tout recouvrement ouvert de X , on peut extraire un sous-recouvrement fini.

Lemme 2.4. Soit X un espace séparé, pour que X soit compact, il faut et il suffit que toute famille de fermés de X dont l'intersection est vide admette une sous-famille finie dont l'intersection soit vide.

Démonstration. Il suffit d'observer que, si $(F_i)_{i \in I}$ est une famille de fermés de X , et si on désigne, pour chaque $i \in I$, par O_i le complémentaire de F_i dans X (qui est un ouvert), alors on a $\cap_{i \in I} F_i = \emptyset$ si et seulement si $\cup_{i \in I} O_i = X$. Ainsi, à une famille de fermés de X dont l'intersection est vide, correspondant par complémentarité un recouvrement ouvert de X , et vice-versa. □

Lemme 2.5. *Soit X un espace séparé muni d'une base d'ouverts $(\Omega_i)_{i \in I}$, pour que X soit compact, il est nécessaire et suffisant que, que de tout recouvrement de X par des ouverts élémentaires, on puisse extraire un sous-recouvrement fini.*

Démonstration. La condition est évidemment nécessaire. Supposons qu'elle soit satisfaite et considérons un recouvrement $(G_k)_{k \in K}$ de X par des ouverts quelconques. On a $X = \cup_{k \in K} G_k$, mais comme chacun des (G_k) est réunion d'ouverts élémentaires, on aura un recouvrement de X par une famille d'ouverts élémentaires $(\Omega_j)_{j \in J}$ ($J \in I$), chaque (Ω_j) étant contenu dans au moins un des ouverts (G_k) . On peut alors, d'après notre hypothèse, extraire de ce recouvrement un sous-recouvrement fini, et on aura par exemple $X = \Omega_{j_1} \cup \Omega_{j_2} \cup \dots \cup \Omega_{j_n}$. Il suffit alors de choisir dans la famille $(G_k)_{k \in K}$ des ouverts $(G_{k_1}, G_{k_2}, \dots, G_{k_n})$ contenant respectivement $X = \Omega_{j_1}, \Omega_{j_2}, \dots, \Omega_{j_n}$, et on aura bien un sous-recouvrement fini de $(G_k)_{k \in K}$ puisqu'alors $X = G_{k_1} \cup G_{k_2} \cup \dots \cup G_{k_n}$. Cela prouve donc que X est compact □

La propriété précédente peut naturellement être traduite en termes de fermés :

Lemme 2.6. *Soit X un espace séparé dans lequel on s'est donné une base d'ouverts. Pour que X soit compact, il faut et il suffit que, de toute famille de fermés élémentaires dont l'intersection est vide, on puisse extraire une sous-famille finie dont l'intersection soit déjà vide.*

Ouvert-fermé

Définition 2.18. *On appellera **ouvert-fermé** dans un espace topologique X tout sous-ensemble de X qui est en même temps un ouvert et un fermé (c'est-à-dire tout ouvert dont le complémentaire dans X est également un ouvert).*

Dimension zéro

Définition 2.19. *Un espace topologique dans lequel il existe une base d'ouverts constituée d'ouverts-fermés est dit de **dimension zéro**. Par exemple, dans l'ensemble \mathbb{Q} des nombres rationnels, les intervalles ouverts bornés à extrémités irrationnelles constituent une base d'ouverts-fermés pour la topologie usuelle (vérification très simple) : \mathbb{Q} donc un espace topologique de dimension zéro.*

Lemme 2.7. *Pour qu'un espace topologique X soit de dimension zéro, il faut et il suffit que la famille de tous ses ouverts-fermés constitue une base d'ouverts.*

Démonstration. Il est évident que toute famille d'ouverts contenant une base d'ouverts de X est elle-même une base d'ouverts de X . Donc, si X est de dimension zéro, alors la famille de tous ses ouverts-fermés en est une base d'ouverts. La réciproque est immédiate. \square

Lemme 2.8. *Tout sous-espace Y d'un espace topologique X de dimension zéro est de dimension zéro.*

Démonstration. Soit $(O_i)_{i \in I}$ une base d'ouverts pour X , constituée d'ouverts-fermés. La famille $(O_i \cap Y)_{i \in I}$ est alors une base d'ouverts pour la topologie de Y (lemme 2.1), mais ces ouverts sont également des fermés de Y , puisque ce sont les traces sur Y de fermés de X . \square

Espace booléen

Définition 2.20. *Un espace topologique compact de dimension zéro est appelé **espace booléen**.*

Topologie produit

Définition 2.21. *Soit $(X_i)_{i \in I}$ une famille d'espaces topologiques. Sur le produit $\prod_{i \in I} X_i$ de cette famille, on définit une topologie en prenant comme ouverts élémentaires les sous-ensembles de la forme $\prod_{i \in I} O_i$, où, pour chaque indice $i \in I$, O_i est un ouvert de X_i , mais où, pour tous les indices i à l'exception d'un nombre fini d'entre eux, on a $O_i = X_i$. On vérifie facilement qu'en prenant toutes les réunions des ensembles ainsi définis, on obtient une famille d'ensembles stables par intersection finie et par union quelconque. C'est cette famille que l'on adopte comme famille d'ouverts pour la topologie sur $\prod_{i \in I} X_i$. La topologie ainsi définie est appelée **topologie produit**.*

Le **théorème de Tychonoff** affirme que :

Théorème 2.3. *Le produit de toute famille d'espaces topologiques compacts est un espace topologique compact.*

La démonstration utilise le théorème de zorn.

Démonstration. On prend la famille d'espace $(X_i)_{i \in I}$ dans laquelle chacun des (X_i) est l'espace $\{0, 1\}$ muni de la topologie discrète (celle où tous les sous-ensembles sont des ouverts).

Le produit $\prod_{i \in I} X_i$ est alors l'ensemble $\{0, 1\}^I$ des applications de I dans $\{0, 1\}$.

Pour avoir un ouvert élémentaire Ω de la topologie produit, on doit se donner un nombre fini d'indices : i_1, i_2, \dots, i_k dans I et des ouverts $O_{i_1}, O_{i_2}, \dots, O_{i_k}$ pris dans $\{0, 1\}$.

Soit, en l'occurrence, des sous ensembles quelconque de $\{0, 1\}$. On pose alors :

$$\Omega = \{0, 1\}^{I - \{i_1, i_2, \dots, i_k\}} \times O_{i_1} \times O_{i_2} \dots \times O_{i_k},$$

ou encore :

$$\Omega = \{f \in \{0, 1\}^I; f(i_1) \in O_{i_1} \text{ et } f(i_2) \in O_{i_2} \text{ et } \dots f(i_k) \in O_{i_k}\}.$$

On peut naturellement supposer qu'on ne s'est intéressé qu'aux indices i_j pour lesquels l'ouvert correspondant est distinct de l'ensemble $\{0, 1\}$ tout entier. Il est également inutile de considérer le cas où l'un des O_{i_j} serait l'ensemble vide, on obtiendrait alors l'ouvert $\Omega = \phi$. Il reste deux possibilités pour le choix de chaque O_{i_j} :

$$O_{i_j} = \{0\} \text{ ou } O_{i_j} = \{1\}$$

On voit donc que, pour obtenir un ouvert élémentaire Ω de la topologie produit sur $\{0, 1\}^I$, on doit se donner un nombre fini d'indices : i_1, i_2, \dots, i_k dans I et un même nombre d'éléments : $\xi_1, \xi_2, \dots, \xi_k$ dans $\{0, 1\}$, et poser alors :

$$\Omega = \{f \in \{0, 1\}^I; f(i_1) = \xi_1 \text{ et } f(i_2) = \xi_2 \text{ et } \dots f(i_k) = \xi_k\}.$$

Un ouvert élémentaire, c'est donc l'ensemble des applications de I dans $\{0, 1\}$ qui prennent des valeurs données en un nombre fini de points donnés.

Remarquons que le complémentaire, c'est donc l'ensemble des applications dans $\{0, 1\}^I$ de l'ensemble Ω que nous venons de considérer est l'ensemble suivant :

$$\cup_{1 \leq j \leq k} \{f \in \{0, 1\}^I; f(i_j) = 1 - \xi_j\}.$$

C'est donc la réunion de k ouverts élémentaires, qui est évidemment un ouvert.

On en déduit que l'ensemble Ω est un fermé.

Les ouverts élémentaires de la topologie de $\{0, 1\}^I$ sont donc des ouverts-fermés. □

Nous avons prouvé le :

Lemme 2.9. *L'espace topologique $\{0, 1\}^I$ est de dimension zéro.*

Comme l'espace topologique $\{0, 1\}$ est à l'évidence compact, on peut, avec le théorème de Tychonoff, conclure :

Théorème 2.4. *L'espace $\{0, 1\}^I$ est un espace topologique booléen.*

2.2 Algèbre de Boole

2.2.1 Les anneaux

Définition 2.22. *Un anneau est un triplet $\langle E, +, \cdot \rangle$ tel que :*

1. $\langle E, + \rangle$ est un groupe commutatif.
2. La multiplication \cdot est associative
3. La multiplication \cdot est distributive par rapport à l'addition $+$.

Remarque 2.4. • *Si la multiplication \cdot est commutative, la structure d'anneau est **commutative**.*

• *Si la multiplication \cdot possède un élément neutre alors l'anneau est **unitaire**.*

2.2.2 Anneau de Boole

Définition 2.23. *Un anneau de Boole (ou une algèbre de Boole) est un anneau dans lequel chaque élément x est idempotent pour la multiplication c'est-à-dire égale à son carré ($x^2 = x$).*

Exemple 13. 1. *L'anneau $\langle \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 \rangle$ est un anneau de Boole.*

2. *L'anneau $\langle B(E), \Delta, \cap, \emptyset, E \rangle$, où E est un ensemble non vide quelconque, Δ et \cap étant respectivement les opérations de différence symétrique et d'intersection sur l'ensemble $B(E)$ des parties de E , est un anneau de Boole.*

2.2.3 Propriétés des anneaux de Boole

Lemme 2.10. 1. *Dans tout anneau de Boole, chaque élément est son propre opposé.*

2. *Tout anneau de Boole est commutatif.*

Démonstration. 1. Soient $A = \langle E, +, \cdot, 0, 1 \rangle$ un anneau de Boole, $\forall x, y \in E$ on a d'après la définition :

$$x^2 = x, y^2 = y \text{ et } (x + y)^2 = (x + y)^2$$

mais par ailleurs, comme dans tout anneau,

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

On en déduit donc :

$$x + y = x + xy + yx + y$$

soit en simplifiant, $xy + yx = 0$, on choisissant $y = 1$, on obtient en particulier $x + x = 0$ ou $x = -x$.

2. Pour x et y quelconques, xy est donc l'opposé de yx , mais puisque $xy + yx = 0$ c'est aussi l'opposé de yx , on en conclut $xy = yx$ est que l'anneau commutatif.

□

Remarque 2.5. *L'anneau de Boole $(\mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1)$ est le seul anneau de Boole qui soit un corps, et même le seul anneau de Boole qui soit intègre : en effet la relation $x^2 = x$, qui équivaut à $x(x - 1) = 0$, exige, dans un anneau intègre, $x = 0$ ou $x = 1$.*

Soit $\langle E, +, \cdot, 0, 1 \rangle$ un anneau de Boole. On définit une relation binaire \leq sur E comme suit :

$\forall x, y \in E; x \leq y$ si et seulement si $xy = x$.

On vérifie qu'il s'agit d'une relation d'ordre, en effet : $\forall x, y, z \in E$ on a :

- $x \leq x$ puisque $x^2 = x$ par la définition.
- Si $x \leq y$ et $y \leq x$ alors $xy = x$ et $yx = y$, donc $x = y$ d'après la commutativité.
- Si $x \leq y$ et $y \leq z$ alors $xy = x$ et $yz = y$, d'où $xz = (xy)z = x(yz) = xy = x$, donc $x \leq z$.

La relation \leq est bien réflexive, transitive et antisymétrique.

Le théorème suivant énumère les principales propriétés de cette relation d'ordre.

Théorème 2.5. 1. *Il y a la relation \leq un plus petit élément 0 et un plus grand élément 1.*

2. *Deux éléments x et y quelconques de E admettent une borne inférieure, notée $x \wedge y$: leur produit xy .*
3. *Deux éléments x et y quelconques de E admettent une borne supérieure, notée $x \vee y$: l'élément $x + y + xy$.*
4. *Les opérations \wedge et \vee ainsi définir sur E sont associatives et commutatives.*
5. *0 est élément neutre pour l'opération \vee et élément absorbant pour l'opération \wedge tandis que 1 est neutre pour l'opération \wedge et absorbant pour l'opération \vee .*
6. *Tout partie finie non vide $\{x_1, x_2, \dots, x_k\}$ de E ($k \in \mathbb{N}^*$) admet une borne inférieure égale à : $x_1 \wedge x_2 \wedge \dots \wedge x_k$, et une borne supérieure égale à : $x_1 \vee x_2 \vee \dots \vee x_k$.*
7. *Les opérations \vee et \wedge sont distributif l'une par rapport à l'autre.*

8. Pour tout élément x et y de E , il existe un élément x' dans E , appelé complément de x , tel que $x \vee x' = 1$ et $x \wedge x' = 0$.
9. L'application $x \mapsto 1 + x$ de E dans E est une bijection qui reverse l'ordre.

Démonstration. 1. En effet, pour tout x , $0 \cdot x = 0$ et $x \cdot 1 = x$, donc $0 \leq x$ et $x \leq 1$.

2. On a $(xy)x = x^2y = xy$ et $(xy)y = xy^2 = xy$, donc xy minore à la fois x et y . De plus, si z est un minorant commun à x et y , on a $zx = z$ et $zy = z$, d'où $z(xy) = (zx)y = zy = z$, ce qui veut dire $z \leq xy$, xy donc le plus grand des minorants communs de x et y .

3. En effet,

$$x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x + 0 = x$$

et de façon analogue :

$$y(x + y + xy) = y.$$

On a donc bien

$$x \leq x + y + xy \text{ et } y \leq x + y + xy$$

D'autre part, si z est un élément de E tel que $x \leq z$ et $y \leq z$, c'est à dire $xz = x$ et $yz = y$, alors :

$$(x + y + xy)z = xz + yz + xyz = x + y + xy$$

donc

$$x + y + xy \leq z$$

alors $x + y + xy$ est le plus petit des majorants communs de x et y .

4. Cela est vrai et on a déjà démontré dans le chapitre 1.
5. Autrement dit : pour tout élément x de E , on a $x \vee 0 = x$, $x \wedge 0 = 0$, et $x \wedge 1 = x$, $x \vee 1 = 1$. Cela est vrai dans tout ensemble ordonné qui satisfait les propriétés 1 et 2 et 3. La vérification est immédiate.
6. Le cas évident ou $k = 0$ mis à part, il s'agit d'une simple généralisation des propriétés 2 et 3, que l'on obtient naturellement par récurrence sur k .

On voudra bien être attentif au fait suivant : l'écriture $x_1 \wedge x_2 \wedge \dots \wedge x_k$ n'est pas une notation nouvelle destinée à un objet nouvellement introduit. Elle désigne un élément de E qui est parfaitement défini (par récurrence) dès lors que l'opération \wedge l'est (c'est l'élément qu'on devrait désigner par : $(\dots((x_1 \wedge x_2) \wedge x_3 \wedge \dots \wedge x_{k-1}) \wedge x_k)$, expression qui contient $k-1$ couples de parenthèses, que nous avons supprimés pour cause d'associativité). A propos de l'opération \wedge , la propriété 6 affirme deux choses distinctes : d'une part, les éléments

x_1, x_2, \dots, x_k admettent un plus grand minorant commun, et d'autre part, ce plus grand minorant commun est $x_1 \wedge x_2 \wedge \dots \wedge x_k$. La démonstration de ces deux faits est certes extrêmement simple (nous nous sommes d'ailleurs abstenus de la faire), mais la difficulté est peut-être justement de déterminer ce qu'il y a lieu de démontrer. (même remarque, bien sur, pour l'opération \vee).

7. D'autre part,

$$x \wedge (y \vee z) = x(y + z + yz) = xy + xz + xyz = xy + xz + xy \cdot xz = (x \wedge y) \vee (x \wedge z)$$

quels que soient les éléments x, y et z de E , ce qui garanti la distributivité de \wedge par rapport à \vee . D'autre part, toujours pour x, y et z quelconques,

$$\begin{aligned} (x \vee y) \wedge (x \vee z) &= (x + y + xy)(x + z + xz) \\ &= x^2 + xz + x^2z + yx + yz + yxz + x^2y + xyz + x^2yz \\ &= x + yz + xyz \end{aligned}$$

après des simplifications évidentes. Mais $x + yz + xyz = x \vee (yz) = x \vee (y \wedge z)$, d'où l'autre distributivité.

8. Si un tel élément x' existe, il vérifie $xx' = 0$ et $x + x' + xx' = 1$, donc aussi $x + x' = 1$, ou encore $x' = 1 + x$. Il est d'autre part facile de vérifier que

$$x \vee (1 + x) = 1 \text{ et } x \wedge (1 + x) = 0.$$

On a ainsi établi l'existence, mais aussi l'unicité du complément de x : c'est $1 + x$.

9. Cette application est même une involution (bijection égale à son inverse) puisque, pour tout $x, 1 + (1 + x) = x$. D'autre part, quels que soient les éléments x et y , on a :

$$(1 + x)(1 + y) = 1 + x + y + xy.$$

Cet élément est égale à $1 + x$ si et seulement si $y + xy = 0$, ou encore $xy = y$. On voit ainsi que $1 + x \leq 1 + y$ si et seulement si $y \leq x$.

□

Remarque 2.6. *La relation d'ordre dans un anneau de Boole est compatible avec la multiplication, cela veut dire que, si des éléments x, y, z et t vérifiant $x \leq y$ et $z \leq t$, alors $xz \leq yt$ (si $xy = x$ et $zt = z$, alors $xyzt = xz$), mais ce qu'il est important de retenir, c'est que cet ordre n'est pas compatible avec l'addition : par exemple, on a $0 \leq 1$ et $1 \leq 1$, mais on n'a pas $0 + 1 \leq 1 + 1$.*

Lemme 2.11. *Quels que soient les éléments x et y de E , on a $x \leq 1 + y$ si et seulement si $xy = 0$.*

Démonstration. En effet, $x \leq 1 + y$ signifie par définition $x(1 + y) = x$, ou encore $x + xy = x$, ce qui équivaut bien à $xy = 0$. \square

2.2.4 Les algèbres de Boole en tant qu'ensembles ordonnés

Les propriétés 1, 2, 3, 7 et 8 du théorème précédent caractérisent en fait les anneaux de Boole, comme le montre théorème suivant, qui nous fournit une deuxième façon de définir ces anneaux.

Théorème 2.6. *Soit (E, \leq) un ensemble ordonné possédant les propriétés suivantes :*

1. *Il y a un plus petit élément 0 et plus grand élément 1.*
2. *Deux éléments quelconques x et y ont une borne inférieure $x \wedge y$ et une borne supérieure $x \vee y$.*
3. *Les opérations \vee et \wedge sont distributif l'une par rapport à l'autre.*
4. *Pour tout élément x de E , il existe au moins un élément x' de E tel que $x \vee x' = 1$ et $x \wedge x' = 0$.*

Alors on peut munir E d'une structure d'anneau de Boole :

$\langle E, +, \cdot, 0, 1 \rangle$ de tel sorte que l'ordre \leq donné sur E coïncide avec l'ordre associé à la structure d'anneau de Boole (c'est à dire qu'on ait $x \leq y$ si et seulement si $xy = x$).

Remarque 2.7. *Un ensemble ordonné qui possède les propriétés 1 et 2 de l'énoncé est appelé un **treillis**.*

*S'il possède aussi la propriété 3, on dit que c'est un treillis **distributif**. Si 1, 2, 3, et 4 sont satisfaites toutes les quatre, on parle de treillis distributif et **complémenté**, le **complément** (ou **complémentaire** d'un élément x étant l'unique élément x' , tel que $x \vee x' = 1$ et $x \wedge x' = 0$. L'unicité est facile à prouver :*

Démonstration. Supposons que x' et x'' soient des compléments de x , et considérons l'élément $y = (x \wedge x') \vee x''$. D'une part, y est égal à $0 \vee x''$, donc à x'' . D'autre part, la distributivité nous conduit à : $y = (x \vee x'') \wedge (x' \vee x'') = 1 \wedge (x' \vee x'') = x' \vee x''$. On a donc $x'' = x' \vee x''$, ce qui veut dire que $x' \leq x''$. Mais en échangeant les rôles de x' et x'' , on obtient naturellement à $x'' \leq x'$, et finalement à $x' = x''$. \square

Définition 2.24. On appelle généralement les *lois de Morgan* le suivant : quel que soit les éléments x et y de E

1. $(x \wedge y)^c = x^c \vee y^c$.

2. $(x \vee y)^c = x^c \wedge y^c$.

Démonstration. La deuxième loi se déduit de la première en y remplaçant x par x^c et y par y^c , puis en passant aux complément dans les deux membres.

Pour établir la première, on montre que $(x^c \vee y^c) \vee (x \wedge y) = 1$ et que $x^c \vee y^c \vee (x \wedge y) = 0$: on utilise pour cela les propriétés de distributivité des opérations \vee et \wedge , ainsi que leur associativité et leur commutativité :

$$(x^c \vee y^c) \vee (x \wedge y) = (x^c \vee y^c \vee x) \wedge (x^c \vee y^c \vee y) = (1 \vee y^c) \wedge (x^c \vee 1) = 1 \wedge 1 = 1.$$

$$(x^c \vee y^c) \wedge (x \wedge y) = (x^c \wedge x \wedge y) \vee (y^c \wedge x \wedge y) = (0 \wedge y) \vee (0 \wedge x) = 0 \vee 0 = 0.$$

□

Une algèbre de Boole, c'est donc, indifféremment, un anneau dans lequel tout élément est égal à son carré, ou un ensemble ordonné qui a une structure de treillis distributif et complémenté.

2.3 Atomes dans une algèbre de Boole

Définition 2.25. Un élément x dans une algèbre de Boole $\langle E, \leq, \vee, \wedge, 0, 1 \rangle$ est appelé **un atome** si et seulement si il non nul et n'a pas de minorant strict non nul. En d'autres termes, x est un atome si et seulement si : $x \neq 0$ et pour tout élément y de E , si $y \leq x$, alors $y = x$ ou $y = 0$.

Exemple 14. • Dans l'algèbre de Boole $B(E)$ des parties de l'ensemble E , les atomes sont les singletons (c'est-à-dire les parties à un élément).

- Il y a des algèbre de Boole sans atomes : c'est le cas de l'algèbre de Boole ζ / \sim des classes de formules du calcul propositionnel, lorsque l'ensemble des variable propositionnelles est infini.

Définition 2.26. Une algèbre de Boole est **atomique** si et seulement si chacun de ses éléments non nuls est minoré par au moins un atome.

C'est le cas, par exemple, de l'algèbre de Boole des parties d'un ensemble (chaque partie non vide contient au moins un singleton).

Théorème 2.7. *Tout algèbre de Boole finie est atomique.*

Démonstration. Soit $\langle E, \leq, \vee, \wedge, 0, 1 \rangle$ une algèbre de Boole finie et x un élément non nul de E .

Désignons par $m(x)$ l'ensemble des minorants stricts non nuls de x dans E . Si $m(x)$ est vide, alors x est un atome. Si $m(x)$ n'est pas vide, alors, comme il est fini, il admet au moins un élément minimal (c'est à dire non strictement minoré) pour l'ordre \leq . Il est facile de voir qu'un tel élément minimal est un atome de E qui minore x . □

Théorème 2.8. *Soit $\langle E, \leq, \vee, \wedge, 0, 1 \rangle$ une algèbre de Boole (finie ou non), alors pour chaque élément a non nul de E et pour tout entier $k \geq 2$, les propriétés suivantes sont équivalentes :*

1. a est un atome.
2. Pour chaque élément x de E , on a $a \leq x$ ou $a \leq 1 + x$
3. Pour tout éléments x_1, x_2, \dots, x_k de E , si $a \leq x_1 \vee x_2 \vee \dots \vee x_k$, alors $a \leq x_1$ ou $a \leq x_2$ ou \dots ou $a \leq x_k$.

Démonstration. observons tout d'abord que, en vertu du lemme (2.11) et de la définition de l'ordre \leq , (2) équivalente à :

(2') : pour tout élément x de E , on a $ax = a$ ou $ax = 0$.

Soient a un élément non nul de E et k un entier naturelle ($k \geq 2$)

- (1) \implies (2') : pour chaque $x \in A$, on a $ax \leq a$, donc, lorsque a est atome, $ax = a$ ou $ax = 0$.
- (2) \implies (3) : supposons (2), et choisissons des éléments x_1, x_2, \dots, x_k de A tel que $a \leq x_1 \vee x_2 \vee \dots \vee x_k$. Si on n'avait ni $a \leq x_1$, ni $a \leq x_2$, ni \dots , ni $a \leq x_k$, on aurait, d'après (2), $a \leq 1 + x_1$, et $a \leq 1 + x_2$, et \dots , et $a \leq 1 + x_k$, a serait alors un minorant commun à $1 + x_1, 1 + x_2, \dots, 1 + x_k$, donc aussi un minorant de leur borne inférieure $1 + (x_1 \vee x_2 \vee \dots \vee x_k)$ (de Morgane). L'élément a minorerait donc à la fois $x_1 \vee x_2 \vee \dots \vee x_k$, et son complément, ce qui est possible puisque a n'est pas nul.
- (3) \implies (1) : supposons (3), et soit b un minorant de a , on a évidemment $a \leq b \vee (1 + b) = 1$. En prenant $x_1 = b$ et $x_2 = x_3 = \dots = x_k = 1 + b$ dans (3), on en déduit que $a \leq b$ ou $a \leq 1 + b$. Dans la première éventualité, on obtient $b = a$, et dans la deuxième, $b = ab = 0$ lemme (2.11). On a ainsi prouvé que a est un atome. □

2.4 Homomorphisme d'algèbre de Boole

Généralité

Un homomorphisme d'algèbre de Boole, c'est ce que l'on appelle en général un homomorphisme d'anneau unitaires, c'est à dire une application qui respecte l'addition et la multiplication, ainsi que leurs éléments neutres. Nous donnerons les définitions, des exemples, des contre exemples, et des caractérisations en termes d'ensemble ordonnés.

Définition 2.27. Soient $A = \langle E, \leq, 0, 1 \rangle$ et $B = \langle F, \leq, 0, 1 \rangle$ deux anneaux de Boole et f est une application de E dans F , on dit que f est un homomorphisme d'algèbre de Boole de A dans B si et seulement si : $\forall x, y, z \in E$ on a :

$$\begin{aligned}f(x + y) &= f(x) + f(y) \\f(x \times y) &= f(x) \times f(y) \\f(1) &= 1\end{aligned}$$

Remarque 2.8. • La condition $f(0) = 0$ ne figure pas dans la définition car elle se déduit immédiatement de la première relation ($x = y = 0$).

- La situation est différente pour l'élément neutre de la multiplication : la troisième relation n'est pas une conséquence de la deuxième.

Remarque 2.9. La notion d'homomorphisme définie ici n'est autre que celle, plus générale, d'homomorphisme d'anneaux unitaire, appliquée au cas particulier des anneaux de Boole. (On observera toute fois qu'il peut exister des homomorphismes d'anneaux unitaires entre un anneau de Boole et un anneaux unitaire qui n'est pas un anneau de Boole). Les propriétés vraies pour les homomorphismes d'anneaux unitaires quelconques demeurent évidemment pour les anneaux de Boole : par exemple l'application composé de deux homomorphismes d'anneaux de Boole est un homomorphisme d'anneaux de Boole.

Lemme 2.12. Soient $A = \langle E, \leq, 0, 1 \rangle$ et $B = \langle F, \leq, 0, 1 \rangle$ deux algèbres de Boole et f est un homomorphisme d'algèbre de Boole de A dans B Alors on a (avec les notations précédemment adoptées, et en perpétuant l'abus mentionné dans la remarque 2.8) : $\forall x, y \in E$:

$$\begin{aligned}f(x \wedge y) &= f(x) \wedge f(y) \\f(x^c) &= (f(x))^c \\f(x \vee y) &= f(x) \vee f(y) \\si \ x \leq y, \text{ alors } f(x) &\leq f(y)\end{aligned}$$

Démonstration. Les opérations \cdot et \wedge étant identiques, la première relation à démontrer est déjà dans la définition d'un homomorphisme. La deuxième s'écrit :

$$f(1 + x) = 1 + f(x),$$

ce qui résulte immédiatement de

$$f(1) = 1$$

et l'additivité de f . La troisième relation découle des deux premières et des lois de Morgan. Enfin, la dernière relation se traduit ainsi : si $xy = x$, alors $f(x)f(y) = f(x)$, cela est vrai puisque $f(xy) = f(x)f(y)$. \square

Théorème 2.9. Soient $A = \langle E, \leq, 0, 1 \rangle$ et $B = \langle F, \leq, 0, 1 \rangle$ deux algèbres de Boole et f est une application de E dans F . Pour que f soit un homomorphisme d'algèbre de Boole, il faut et il suffit que, $\forall x, y \in E$, on ait :

$$\begin{aligned} f(x \wedge y) &= f(x) \wedge f(y), \\ f(x^c) &= (f(x))^c. \end{aligned}$$

Démonstration. La condition est nécessaire d'après le lemme. Supposons qu'elle soit vérifiée, et soient x et y des éléments de E . On a alors :

$$\begin{aligned} f(xy) &= f(x \wedge y) = f(x) \wedge f(y) = f(x)f(y) \\ f(x + y) &= f((x \wedge y^c) \vee (x^c \wedge y)) = f(((x \wedge y^c)^c \wedge (x^c \wedge y)^c)^c) \\ &= (f((x \wedge y^c)^c \wedge (x^c \wedge y)^c))^c = (f((x \wedge y^c)^c) \wedge f((x^c \wedge y)^c))^c \\ &= ((f(x \wedge y^c))^c \wedge (f(x^c \wedge y))^c)^c = f(x \wedge y^c) \vee f(x^c \wedge y) \\ &= (f(x) \wedge f(y^c)) \vee (f(x^c) \wedge f(y)) = (f(x) \wedge (f(y))^c) \vee ((f(x))^c \wedge f(y)) \\ &= f(x) + f(y). \end{aligned}$$

On déduit que $f(0) = 0$ et donc aussi que :

$$f(1) = f(0^c) = (f(0))^c = 0^c = 1.$$

Cela montre bien que f est un homomorphisme. \square

Remarque 2.10. *Il est clair que, dans l'énoncé du théorème précédent, on peut remplacer partout l'opération \wedge par l'opération \vee .*

2.4.1 Isomorphisme d'algèbre de Boole

Définition 2.28. *Un isomorphisme d'algèbre de Boole est un homomorphisme d'algèbre de Boole qui est bijectif.*

Théorème 2.10. *Soient $A = \langle E, \leq, 0, 1 \rangle$ et $B = \langle F, \leq, 0, 1 \rangle$ deux algèbres de Boole et f est une application surjective de E dans F . Pour que f soit un isomorphisme d'algèbre de Boole, il faut et il suffit que, $\forall x, y \in E$, on a :*

$$x \leq y \text{ si et seulement si } f(x) \leq f(y) \quad (2.1)$$

Démonstration. Supposons d'abord que f soit un isomorphisme et soient x et y des éléments de E . Si $x \leq y$, alors d'après le lemme précédente, $f(x) \leq f(y)$. Si $f(x) \leq f(y)$, alors par définition de \leq et parce que f est un homomorphisme,

$$f(x) = f(x) f(y) = f(xy)$$

Mais comme f est injective, cela exige $x = xy$, c'est à dire $x \leq y$.

Réciproquement, supposons (2.1) satisfaite et soient u et v deux éléments de E tel que $f(u) = f(v)$. On a

$$f(u) \leq f(v) \text{ et } f(v) \leq f(u)$$

donc, par (2.1)

$$u \leq v \text{ et } v \leq u$$

soit $u = v$. Ainsi, f est injective, Par ailleurs, soient x et y deux éléments quelconques de E . Posons

$$t = f(x) \wedge f(y)$$

Comme f est bijective, il existe un unique élément z dans E tel que $t = f(z)$. On a

$$f(z) \leq f(x) \text{ et } f(z) \leq f(y)$$

donc d'après (2.1),

$$z \leq x \text{ et } z \leq y$$

et par conséquent, $z \leq x \wedge y$. Mais comme

$$x \wedge y \leq x \text{ et } x \wedge y \leq y$$

on a toujours grâce à (2.1),

$$f(x \wedge y) \leq f(x) \text{ et } f(x \wedge y) \leq f(y)$$

ce qui entraîne

$$f(x \wedge y) \leq f(x) \wedge f(y) = f(z);$$

En utilise encore (2.1) on obtient $x \wedge y \leq z$, et en définitive $z = x \wedge y$, ce qui prouve que :

$$f(x \wedge y) = f(x) \wedge f(y)$$

En remplaçons \wedge par \vee et \leq par \geq dans cette démonstration, on obtient :

$$f(x \vee y) = f(x) \vee f(y)$$

Soit u est un élément quelconques de F et t son unique antécédente dans E par f . Dans E , on a

$$0 \leq t \text{ et } t \leq 1$$

Il en résulte, avec (2.1), que dans F , $f(0) \leq u$ et $u \leq f(1)$. Cela montre que $f(0)$ et $f(1)$ sont respectivement le plus petit et le plus grand élément de F , autrement dit, que $f(0) = 0$ et $f(1) = 1$. Pour tout élément x de E , on a alors f

$$f(x^c) \wedge f(x) = f(x^c \wedge x) = f(0) = 0$$

$$f(x^c) \vee f(x) = f(x^c \vee x) = f(1) = 1$$

$f(x^c)$ est donc le complément de $f(x)$, c'est-à-dire que $(f(x))^c = f(x^c)$. On conclut avec le théorème précédente : f est un homomorphisme d'algèbre de Boole. On remarquera que la relation $f(x \vee y) = f(x) \vee f(y)$ ne nous était pas nécessaire pour appliquer le théorème précédente, mais a servi à prouver que f commute avec l'opération de passage au complément. \square

Corollaire 4. *L'application composée de deux isomorphismes d'algèbres de Boole, ainsi que la bijection réciproque d'un isomorphisme d'algèbre de Boole, sont des isomorphismes d'algèbre de Boole.*

Démonstration. Soient $A = \langle E, +, \cdot, 0, 1 \rangle$, $B = \langle F, +, \cdot, 0, 1 \rangle$ et $C = \langle G, +, \cdot, 0, 1 \rangle$ des algèbres de Boole, φ un isomorphisme d'algèbre de Boole de A sur B , et ψ un isomorphisme d'algèbre de Boole de B sur C . Les applications φ^{-1} et $\psi \circ \varphi$ sont évidemment surjectives,

$$\forall u, v \in F : \varphi^{-1}(u) \leq \varphi^{-1}(v) \iff \varphi(\varphi^{-1}(u)) \leq \varphi(\varphi^{-1}(v))$$

c'est-à-dire $u \leq v$.

D'autre part, $\forall x, y \in E$ on a :

$$x \leq y \text{ si et seulement si } \varphi(x) \leq \varphi(y)$$

et

$$\varphi(x) \leq \varphi(y) \text{ si et seulement si } \psi(\varphi(x)) \leq \psi(\varphi(y)).$$

Avec le théorème précédent, on en déduit que φ^{-1} et $\psi \circ \varphi$ sont des isomorphismes d'algèbres de Boole, respectivement de B sur A et de A sur C . \square

Théorème 2.11. *Tout algèbre de Boole finie est isomorphe à l'algèbre de Boole des parties d'un ensemble.*

Démonstration. Soient $A = \langle E, \leq, 0, 1 \rangle$ une algèbre de Boole finie et soit S l'ensemble de ses atomes. Remarquons que E n'est pas vide puisqu'il y a au moins un atome qui minore l'élément non nul 1 (théorème 2.7). Nous allons montrer que A est isomorphe à l'algèbre des parties de S . Considérons pour cela l'application f de E dans $B(S)$ qui, à tout élément de E associe l'ensemble des atomes qui minorent pour chaque :

$$x \in E, f(x) = \{a \in S; a \leq x\}$$

- f est surjective : en effet, on a tout d'abord $f(0) = \emptyset$ (aucun atome ne minore 0); d'autre part, soit $X = \{a_1, a_2, \dots, a_k\}$ une partie non vide de S , et posons $M_X = a_1 \vee a_2 \vee \dots \vee a_k$; on a $f(M_X) = X$: l'inclusion $X \subseteq f(M_X)$ résulte immédiatement de la définition de f (tout élément de X est un atome qui minore M_X), l'inclusion inverse se montre avec le théorème (2.8) : soit a un élément de $f(M_X)$, c'est à dire un atome qui minore $M_X = a_1 \vee a_2 \vee \dots \vee a_k$, alors on a $a \leq a_i$ pour au moins un indice i (c'est clair si $k = 1$, et c'est la condition 3 du théorème si $k \geq 2$), mais comme a et a_i sont des atomes, cela exige $a = a_i$, donc $a \in X$.
- Pour tous éléments x et y de E , si $x \leq y$, alors $f(x) \subseteq f(y)$: en effet, si $x \leq y$, tout atome qui minore x est un atome qui minore y .

- Pour tous éléments x et y de E , si $f(x) \subseteq f(y)$, alors $x \leq y$: en effet, si x n'est pas inférieur ou égal à y , alors $x(1+y) \neq 0$ (lemme 2.11). Comme A est finie, elle est atomique (2.7), on peut donc trouver un atome $a \in S$ tel que $a \leq x(1+y)$.

L'atome a est donc un minorant de x et de $1+y$, il ne peut pas minorer aussi y , car il n'est pas nul. On a donc $a \in f(x)$ et $a \notin f(y)$, ce qui prouve que $f(x)$ n'est pas inclus dans $f(y)$. Nous pouvons alors conclure, grâce au théorème (2.10), que f est un isomorphisme d'algèbre de Boole de A sur $B(S)$.

□

Corollaire 5. *Tout algèbre de Boole finie a pour cardinal une puissance de 2.*

Démonstration. Si l'ensemble fini E , a pour cardinal n l'ensemble de ses parties, $P(E)$ a pour cardinal 2^n . □

2.4.2 Définitions

Si f est un morphisme Booléen de A dans B , on définira :

Si f est injective alors f est un monomorphisme Booléen.

Si f est surjective alors f est un épimorphisme Booléen.

Si $A = B$ avec la même structure alors f est un endomorphisme Booléen.

Si f est un endomorphisme bijectif alors f est un automorphisme Booléen.

2.4.3 Composition des morphismes

considérons trois anneaux booléens A, B, C et deux morphismes :

$$f : A \longrightarrow B \quad \text{et} \quad g : B \longrightarrow C$$

Proposition 2.1. *L'application $g \circ f$ est un morphisme Booléen de A dans C .*

Si f et g sont deux monomorphismes (resp. épimorphismes, resp. isomorphismes), il en est de même $g \circ f$.

Proposition 2.2. *Si f est un isomorphisme booléen de A dans B , alors l'application réciproque f^{-1} est un isomorphisme booléen de B dans A .*

Démonstration. Soient x_1 et y_1 deux éléments de B :

$$x_1 = f(x) \text{ ou } x \in A \text{ est déterminé de façon unique, } x = f^{-1}(x_1)$$

$$y_1 = f(y) \text{ ou } y \in A \text{ est déterminé de façon unique, } y = f^{-1}(y_1)$$

$$x_1 y_1 = f(x) f(y) = f(xy), \text{ d'où } xy = f^{-1}(x_1 y_1) = f^{-1}(x_1) f^{-1}(y_1).$$

$$\overline{x_1} = \overline{f(x)} = f(\overline{x}), \text{ d'où } \overline{x} = f^{-1}(\overline{x_1}) = f^{-1}(x_1). \quad \square$$

Proposition 2.3. *L'ensemble des automorphismes booléens d'un anneau booléen A est un groupe pour la loi de composition des applications. Ce groupe sera noté $\text{Aut}(A)$.*

2.4.4 Sous-algèbre de Boole

Définition 2.29. *Soit $A = \langle E, +, \times, 0, 1 \rangle$ une algèbre de Boole, une partie B de E constitue une sous-algèbre de Boole de A si et seulement si B contient les éléments 0 et 1 et est stable pour les opérations $+$ et \times (autrement dit $0 \in B$, $1 \in B$ et si $x \in B$ et $y \in B$ alors $x + y \in B$, et $xy \in B$).*

Remarque 2.11. *Une sous-algèbre de Boole de A , c'est donc un sous-anneau de A contenant l'élément 1 . Cette précision est essentielle : dans un anneau unitaire, un sous-anneau peut être lui-même unitaire, sans pour autant contenir l'élément unité de l'anneau tout entier : le rôle d'élément neutre de la multiplication est alors joué par un autre élément. Reprenons l'exemple de l'anneau $\langle B(\mathbb{Z}), \Delta, \cap, \emptyset, \mathbb{Z} \rangle$: $B(\mathbb{N})$ en est un sous-ensemble stable pour les opérations Δ et \cap et il contient \emptyset ; c'est donc un sous-anneau de $B(\mathbb{Z})$.*

Evidemment, $\mathbb{Z} \notin B(\mathbb{N})$. Néanmoins, \mathbb{N} est élément unité pour l'anneau $B(\mathbb{N})$. Ainsi, l'anneau de Boole $B(\mathbb{N})$ est un anneau unitaire, est un sous-anneau de $B(\mathbb{Z})$, mais pas un sous-anneau unitaire : ce n'en est donc pas une sous-algèbre de Boole.

Théorème 2.12. *Soit A une algèbre de Boole, une partie B de E . Pour que B constitue une sous-algèbre de Boole de A , il faut et il suffit qu'il existe une algèbre de Boole A' et un homomorphisme d'algèbre de Boole f de A' dans A tel que l'image de l'application f soit le sous-ensemble B .*

Démonstration. Il faut : prenons $A' = B$, $+ ' = +$, $\times ' = \times$, $0' = 0$, $1' = 1$ et f l'application identique de B dans E . On vérifie immédiatement que f est un homomorphisme d'algèbre de Boole dont l'image est B . il suffit : choisissons A' et f comme indiqué. On a $f(0') = 0$, donc $0 \in B$ et $f(1') = 1$, donc $1 \in B$. De plus, si x et y deux éléments de B , alors on peut

choisir dans A' des éléments x' et y' tel que $x = f(x')$ et $y = f(y')$ on a alors :

$$\begin{aligned}x + y &= f(x') + f(y') = f(x' + y') \quad \text{donc } x + y \in \text{im}(f) = B \\xy &= f(x') f(y') = f(x'y') \quad \text{donc } xy \in \text{im}(f) = B\end{aligned}$$

B est donc bien une sous-algèbre de Boole de A .

□

Théorème 2.13. *Dans une algèbre de Boole A , pour qu'une partie B de l'ensemble E constitue une sous-algèbre de Boole, il faut et il suffit que B contienne 0 et soit stable pour les opérations $x \mapsto x^c$ et $(x, y) \mapsto x \wedge y$.*

Démonstration. • Il faut : comme $x^c = 1 + x$ et $x \wedge y = xy$, et comme B doit contenir 0 et 1 et être stable pour $+$ et \times , le résultat est immédiat.

- Il suffit : on a, pour tout x et y dans E , $x \vee y = (x^c \wedge y^c)^c$. La stabilité de B pour le passage au complément et pour l'opération \wedge garantit donc la stabilité pour l'opération \vee , de plus $1 = \bar{0}$ doit appartenir à B . Comme les opérations $+$ et \cdot peuvent se définir à partir de \wedge , de \vee et du passage au complément exclusivement, on en déduit la stabilité de B pour $+$ et \cdot et le fait que $\langle B, +, \cdot, 0, 1 \rangle$ est une sous-algèbre de Boole de A .

□

Exemple 15. *Soient E un ensemble infini, $A = p(E)$ l'ensemble de ses parties et F le sous-ensemble de A constitué des parties de E qui sont finies ou dont le complémentaire est finie.*

2.5 Idéaux et filtres

2.5.1 Propriétés des idéaux

Comme indiqué dans les rappels, idéal signifiera ici idéal propre.

Théorème 2.14. *Soit $A = \langle E, \leq, 0, 1 \rangle$ une algèbre de Boole et I est un sous-ensemble de E , pour que I soit un idéal, il faut et il suffit que les trois conditions suivantes soient satisfaites :*

1. $0 \in I$ et $1 \notin I$.
2. Pour tous éléments x et y de I : $x \vee y \in I$.
3. Pour tout $x \in I$ et Pour tout $y \in E$, si $y \leq x$, alors $y \in I$

Démonstration. Supposons que d'abord I soit un idéal. C'est donc en particulier un sous-groupe de groupe $\langle E, +, 0 \rangle$, donc $0 \in I$, si 1 était dans I , I serait l'anneau tout entier, ce que nous avons exclu. Si x et y sont dans I , il en est de même du produit xy et, par suite, de la somme $x + y + xy = x \vee y$. Si $x \in I$ et $y \in E$ alors $xy \in I$ et si de plus $y \leq x$, alors $xy = y$ et, par conséquent, $y \in I$. Réciproquement, supposons que (1), (2) et (3) soient vérifiés et montrons que I est un idéal de A , si $x \in I$ et $y \in I$, alors $x \vee y \in I$ d'après (2), mais comme $x + y \leq x \vee y$, et comme $x + y = x - y$ (nous sommes dans un anneau de Boole), on en déduit avec (3) que $x - y \in I$. Puisque $0 \in I$, les conditions sont réunies pour que $\langle I, +, 0 \rangle$ soit un sous-groupe de $\langle E, +, 0 \rangle$. Par ailleurs, si $x \in I$ et $y \in E$, alors puisque $xy \leq x$, (3) permet de conclure que $xy \in I$, l'ensemble I est donc bien un idéal dans A ($I \neq A$ puisque $1 \notin I$). \square

Corollaire 6. *Dans une algèbre de Boole $A = \langle E, +, \times, 0, 1 \rangle$, étant donné un idéal I , il n'existe aucun élément x de E tel que $x \in I$ et $1 + x \in I$.*

Démonstration. Si l'idéal I contient à la fois x et $1+x$, il devrait également contenir $x \vee (1+x) = 1$ (propriété 3). Mais cela est impossible puisque $1 \notin I$. \square

Corollaire 7. *Soient $A = \langle E, \leq, 0, 1 \rangle$ un anneau de Boole et I un idéal de A , $\forall k \geq 1$ et les éléments x_1, x_2, \dots, x_k de I , la borne supérieure $x_1 \vee x_2 \vee \dots \vee x_k$ appartient à I .*

Démonstration. Il s'agit d'une généralisation de la propriété (2) du théorème précédent (le cas $k = 1$ allant de soi) dont la preuve est immédiate par récurrence sur l'entier k . \square

2.5.2 Exemples

1. Si E est un ensemble infini, l'ensemble $P_f(E)$ constitué des parties finies de E est un idéal dans l'algèbre de Boole $P(E)$, les conditions (1), (2) et (3) sont très facile à vérifier : \emptyset est une partie non fini de E mais E n'en est pas une, la réunion de deux parties finies de E est une partie finie de E , et tout partie incluse dans une partie finie de E est une partie finie de E .
2. Dans toute algèbre de Boole, $\{0\}$ est de toute évidence, un idéal.

Lemme 2.13. *Pour tout anneau de Boole A et tout idéal I de A l'anneau quotient A/I est un anneau de Boole.*

Démonstration. pour chaque élément x de E , notons \bar{x} la classe de x modulo I . On sait déjà que A/I est un anneau, il suffit donc de montrer que tout élément est idempotent pour la multiplication. Mais cela résulte immédiatement de la définition de la multiplication dans A/I et du fait que A est un anneau de Boole : si $x \in E$, $\overline{x^2} = \overline{x^2} = \bar{x}$. \square

Théorème 2.15. *Soient $A = \langle E, +, \times, 0, 1 \rangle$ un anneau de Boole et I est un sous-ensemble de E . Les propriétés suivantes sont équivalentes :*

1. I est un idéal de A .
2. Il existe un homomorphisme d'algèbre de Boole f défini sur E dont I est le noyau c'est-à-dire tel que :

$$I = f^{-1}[\{0\}] = \{x \in E : f(x) = 0\}.$$

3. Il existe un homomorphisme d'anneaux unitaires (commutative) défini sur E dont I est le noyau.

Démonstration. le résultat rappelé ci-dessus est l'équivalence (1) et (3), quant à (2) \implies (3), c'est une évidence. Nous allons tout de même démontrer 3 \implies 1 et en suite 1 \implies 2, qui est, comme annoncé, plus précise que 1 \implies 3. (3) \implies (1) : supposons qu'il y ait un homomorphisme f de A dans anneau unitaire $B = \langle F, +, \cdot, 0, 1 \rangle$ tel que :

$$I = f^{-1}[\{0\}] = \{x \in E : f(x) = 0\}.$$

Vérifions que les conditions (1) , (2) et (3) du théorème précédent sont satisfaites : on a $f(0) = 0$ et $f(1) = 1$ donc $0 \in I$ et $1 \notin I$. Si $x \in I$ et $y \in I$, $f(x) = 0$ et $f(y) = 0$ donc

$$f(x \vee y) = f(x + y + xy) = f(x) + f(y) + f(x)f(y) = 0$$

et $x \vee y \in I$. En fin, si $x \in I$ et $y \in E$ et $y \leq x$, alors

$$f(x) = 0 \text{ et } xy = y$$

d'où

$$f(y) = f(x) f(y) = 0$$

c'est à dire $y \in I$. Ainsi, I est un idéal de A .

(1) \implies (2) : supposons que I soit un idéal de A , et considérons l'application f de E dans E/I qui, chaque élément x , associe sa classe modulo \bar{x} (f est donc ce que l'on appelle d'habitude la surjection canonique de E dans E/I). f est un homomorphisme d'algèbre de Boole (l'homomorphisme canonique de E dans E/I). On s'en assure avec le théorème (2.9) si $x \in E$ et $y \in E$, alors :

$$\begin{aligned} f(x \wedge y) &= f(xy) = \overline{xy} = \bar{x} \times \bar{y} = f(x) f(y) = f(x) \wedge f(y) \\ f(x^c) &= f(1+x) = \overline{1+x} = \bar{1} + \bar{x} = \bar{1} + f(x) = (f(x))^c \end{aligned}$$

Il est d'autre part clair que $I = \bar{0} = \{x \in E : f(x) = \bar{0}\}$: I est le noyau de f . □

2.5.3 Idéaux maximaux

Théorème 2.16. *Pour tout anneau de Boole $A = \langle E, +, \times, 0, 1 \rangle$, pour tout idéal I de A et pour tout entier $k \geq 2$, les propriétés suivantes sont équivalentes :*

1. I est un idéal maximal.
2. A/I est isomorphe à l'algèbre de Boole $\{0, 1\}$
3. I est le noyau d'un homomorphisme de A dans $\{0, 1\}$.
4. Pour tout élément x de E , $x \in I$ ou $1+x \in I$.
5. Pour tous éléments x et y de E , si $xy \in I$, alors $x \in I$ ou $y \in I$.
6. Pour tous éléments $x_1, x_2, \dots, x_k \in E$, si $x_1 x_2 \dots x_k \in I$, alors $x_1 \in I$ ou $x_2 \in I$ ou ... ou $x_k \in I$.

Démonstration. (1) \implies (2) : Si l'idéal I est maximal, l'anneau quotient A/I est un corps, mais on a également observé que le seul anneau de Boole qui soit un corps est $\{0, 1\}$, avec le lemme précédent, on obtient donc la conclusion attendue.

(2) \implies (3) : Il suffit de remarquer que I est toujours le noyau d'un homomorphisme canonique f de A dans A/I . Si il y a un isomorphe φ de A/I sur $\{0, 1\}$, il sera évidemment le noyau d'un homomorphisme $\varphi \circ f$ de A dans $\{0, 1\}$.

(3) \implies (4) : Considérons un homomorphisme f de A dans $\{0, 1\}$ dont I soit le noyau, et soit x un élément quelconque de E , on a $f(x) = 0$ ou $f(x) = 1$, dans le premier cas, $x \in I$, dans le second cas, on a $1 + f(x) = 0$, soit $f(1 + x) = 0$ et $1 + x \in I$.

(4) \implies (5) : Soient x et y des éléments de E tel que $x \notin I$ et $y \notin I$. Si (4) vérifié, alors $1 + x \in I$ et $1 + y \in I$ donc $(1 + x) \vee (1 + y) \in I$ (propriété 3 du théorème précédent), mais

$$(1 + x) \vee (1 + y) = 1 + (x \wedge y) = 1 + xy$$

donc d'après le corollaire précédente $xy \notin I$ et (5) démontré.

(5) \implies (1) : Supposons que I ne soit pas maximal. Soient J un idéal de A contenant strictement I et a un élément de J qui n'appartient pas à I . D'après le corollaire précédente $1 + a \notin J$, donc $1 + a \notin I$ puisque $I \subseteq J$. L'idéal I ne contient ni a ni $1 + a$, mais il contient évidemment le produit $a(1 + a) = 0$. On en déduit que (5) n'est pas satisfait.

(5) \implies (1) : on suppose que (5) est satisfait et on raisonne par récurrence sur l'entier k . Pour $k = 2$, (6) coïncide avec (5). Supposons (6) vérifié à l'ordre k et prouvons-le à l'ordre $k + 1$. Considérons des éléments $x_1, x_2, \dots, x_k, x_{k+1}$ dans E tel que $x_1 x_2 \dots x_k x_{k+1} \in I$. D'après (5), on a alors $x_1 x_2 \dots x_k x_{k+1} \in I$ ou $x_{k+1} \in I$, dans la première éventualité, on a par hypothèse de récurrence $x_1 \in I$ ou $x_2 \in I$ ou ... ou $x_k \in I$, on voit donc qu'on doit avoir $x_i \in I$ pour au moins un indice i tel que $1 \leq i \leq k + 1$, ce qui démontre (6) à l'ordre $k + 1$.

(6) \implies (5) : soient x et y deux éléments de E tel que $xy \in I$. Posons $x_1 = x$ et $x_2 = x_3 = \dots = x_k = y$. On a $x_1 x_2 \dots x_k = xy \in I$. Donc, si (6) est vrai, on doit avoir $x_i \in I$ pour au moins un indice i compris entre 1 et k , c'est à dire $x \in I$, et (5) est vérifié.

□

Remarque 2.12. Dans un anneau commutatif quelconque, un idéal qui possède la propriété (5) du théorème précédent est appelé idéal premier. Ce que nous venons de voir, c'est que, dans un anneau de Boole, les idéaux premiers sont exactement les mêmes que les idéaux maximaux. Mais il y a des anneaux où cela cesse d'être vrai. Ce qui est toujours vrai, c'est qu'un idéal est premier si et seulement si l'anneau quotient qui lui est associé est intègre (c'est facile à démontrer), on en déduit aussi qu'un idéal maximal est nécessairement premier (il suffit de considérer l'anneau quotient correspondant). c'est donc la réciproque qui peut être mise en défaut (par exemple, dans l'anneau $\mathbb{R}[X, Y]$ des polynôme à deux indéterminées à coefficients réels, l'idéal engendré par le

polynôme X c'est à dire l'ensemble $\{XP, P \in \mathbb{R}[X, Y]\}$, est premier mais n'est pas maximal car il est strictement inclus dans l'idéal engendré par le polynôme X et Y , c'est à dire l'ensemble $\{XP + YQ, P \in \mathbb{R}[X, Y], Q \in \mathbb{R}[X, Y]\}$.

Remarque 2.13. On retiendra en particulier l'équivalence entre les propriétés (1) et (3), on observera que, si deux homomorphismes g et f d'une algèbre de Boole A dans $\{0, 1\}$ ont même noyau I , ils sont identiques : car pour tout élément x dans E , ou bien $x \in I$ et $g(x) = f(x) = 0$, ou bien $x \notin I$ et $g(x) = f(x) = 1$. On en déduit que l'ensemble des idéaux maximaux d'une algèbre de Boole est en bijection avec l'ensemble des homomorphismes d'une algèbre de Boole de cette algèbre dans $\{0, 1\}$.

2.5.4 Filtres

Nous allons maintenant introduire la notion duale de celle d'idéal dans une algèbre de Boole, nous allons définir les filtres.

Définition 2.30. Un filtre dans une algèbre de Boole A est une partie F de E tel que l'ensemble

$$\{x \in E, x^c \in F\}$$

soit un idéal dans A .

Théorème 2.17. Soient $A = \langle E, \leq, 0, 1 \rangle$ une algèbre de Boole et F un sous-ensemble de E . Pour que F soit un filtre, il faut et il suffit que les trois conditions suivantes soient satisfaites :

1. $0 \notin F$ et $1 \in F$.
2. Pour tous éléments x et y de F : $x \wedge y \in F$.
3. Pour tout $x \in F$ et Pour tout $y \in E$, si $y \geq x$, alors $y \in F$.

Démonstration. Posons $I = \{x \in E, x^c \in F\}$, si F est un filtre, I est l'idéal dual et les conditions (1), (2) et (3) du théorème idéal sont satisfaites. On a donc $0 \in I$, d'où $0^c = 1 \in F$ et $1 \notin I$ d'où $1^c = 0 \notin F$, ce qui prouve (1)

Si $x \in F$ et $y \in F$, alors $x^c \in I$ et $y^c \in I$ donc $x^c \vee y^c \in I$ (2),

comme $x^c \vee y^c = (x \wedge y)^c$, on en conclut que $x \wedge y \in F$ et (2) est établi.

En fin, si $x \in F$, $y \in E$ et $y \geq x$, alors $x^c \in I$ et $y^c \leq x^c$ et (par (3I), $y^c \in I$ et $y \in F$, d'où (3F)). □

Corollaire 8. Soient A une algèbre de Boole et F un filtre de A . Quels que soient l'entier $k \geq 1$ et les éléments x_1, x_2, \dots, x_k de F , la borne inférieure $x_1 \wedge x_2 \wedge \dots \wedge x_k$ appartient à F .

2.5.5 Ultrafiltres

Définition 2.31. Dans une algèbre de Boole, un ultrafiltre est un filtre maximal, c'est-à-dire un filtre qui n'est strictement inclus dans aucun filtre.

Il est clair que, dans la dualité évoquée ci-dessus, les ultrafiltres correspondent aux idéaux maximaux. En d'autres termes, le filtre dual d'un idéal maximal est un ultrafiltre, et l'idéal dual d'un ultrafiltre est un idéal maximal.

Théorème 2.18. Pour tout anneau de Boole $A = \langle E, +, \times, 0, 1 \rangle$, pour tout filtre F de A et pour tout entier $k \geq 2$, les propriétés suivantes sont équivalentes :

- a) F est un ultrafiltre.
- b) Il existe un homomorphisme f de A dans $\{0, 1\}$ tel que :

$$F = \{x \in E, f(x) = 1\}$$

- c) Pour tout élément x de E , $x \in F$ ou $1 + x \in F$.
- d) Pour tous éléments x et y de E , si $x \vee y \in F$, alors $x \in F$ ou $y \in F$.
- e) Pour tous éléments x_1, x_2, \dots, x_k de E , si $x_1 \vee x_2 \vee \dots \vee x_k \in F$, alors $x_1 \in F$ ou $x_2 \in F$ ou \dots ou $x_k \in F$.

Démonstration. L'algèbre A , le filtre F et l'entier k étant donnés, appelons I l'idéal dual de F . Des vérifications tout à fait élémentaires permettent de montrer que les propriétés (a), (b), (c), (d) et (e) pour le filtre F sont respectivement équivalentes aux propriétés du théorème des idéaux maximaux pour l'idéal I (on utilise la correspondance entre I et F les lois de Morgan). \square

Remarque 2.14. Revenons sur la remarque (2.13), nous pouvons la compléter et retenir le fait que, étant donnée une algèbre de Boole A , il y a correspondance bijective canonique entre les idéaux maximaux de A , les ultrafiltres de A , et les homomorphismes d'algèbre de Boole de A dans $\{0, 1\}$.

2.5.6 Exemples

1. Si E est un ensemble infini, l'ensemble des parties cofinies de E est un filtre dans l'algèbre de Boole $\langle P(E), \subseteq, \emptyset, E \rangle$, ce filtre est appelé Filtre de Fréchet sur E , ce n'est pas un ultrafiltre, parce qu'il y a des parties de E qui sont infinies et dont le complémentaire est aussi infini, ce qui fait que la condition (c) du théorème précédent n'est pas satisfaite.

2. l'ensemble $\{1\}$ est le filtre dual de l'idéal $\{0\}$.
3. Si a est un élément non nul dans une algèbre de Boole A , l'ensemble $F_a = \{x \in E, x \geq a\}$ est un filtre appelé **Filtre principale engendré** par a , c'est le filtre dual de l'idéal principale engendré par $1 + a$.

Théorème 2.19. *Soit $A = \langle E, \leq, 0, 1 \rangle$ une algèbre de Boole et a un élément non nul de E , pour que le filtre principale engendré par a soit un ultrafiltre, il faut et il suffit que a soit un atome.*

Démonstration. En vertu du théorème (2.8) et de la définition du filtre F_a , a est un atome si et seulement si, pour tout élément x de E , $x \in F_a$ ou $1 + x \in F_a$, mais pour cela, il faut et il suffit que F_a soit un ultrafiltre. \square

Lemme 2.14. *Soient A une algèbre de Boole et U un ultrafiltre de A , pour que U soit trivial, il faut et il suffit qu'il contienne au moins un atome.*

Démonstration. Si U est trivial, il est engendré par un atome a , et puisque $a \leq a$, $a \in U$. Réciproquement, si U contient un atome b , il contient aussi tous les majorants de b . Il en résulte que le filtre principale F_b engendré par b est inclus dans U . Mais, comme b est un atome, F_b est maximal et ne peut être inclus strictement dans le filtre U . Donc $U = F_b$ et U est un ultrafiltre trivial. \square

Théorème 2.20. *Soit E un ensemble infini et U un ultrafiltre de l'algèbre de Boole $B(E)$, pour que U soit non trivial, il faut et il suffit qu'il contienne le **filtre de Fréchet** sur E .*

Démonstration. Les atomes dans $B(E)$ sont les singleton (partie à un élément); ce sont donc des parties finies. Si μ contient le filtre de Fréchet, toute partie cofinie de E apparaît à μ , donc aucune partie finie de E n'apparaît pas à μ (μ ne peut contenir en même temps une partie de E et son complémentaire). En particulier, aucun atome n'apparaît pas à μ . On en déduit, avec le lemme précédent, que μ est non trivial.

Si μ ne contient pas le filtre de Fréchet, on peut choisir une partie cofinie X de E qui n'apparaît pas à μ , et qui est donc tel que son complémentaire $E - X$ apparaît à μ . Comme E est l'élément unité de l'algèbre de Boole $B(E)$, $E \in \mu$ d'où $X \neq E$. Le complémentaire de X dans E est donc une partie finie non vide de E : par exemple, $E - X = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ ($n \geq 1$). On a donc $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \in \mu$, c'est à dire aussi : $\{\alpha_1\} \cup \{\alpha_2\} \cup \dots \cup \{\alpha_n\} = \{\alpha_1\} \vee \{\alpha_2\} \vee \dots \vee \{\alpha_n\} \in \mu$. Si $n = 1$, $\{\alpha_n\} \in \mu$. Si $n \geq 2$, d'après la propriété (e) du théorème (2.18), on a $\{\alpha_i\} \in \mu$ pour au moins un indice i compris entre 1 et n . On voit que, dans tous les cas, μ contient un singleton, c'est à dire un atome, alors μ est trivial. \square

2.5.7 Base de filtre

Définition 2.32. Dans une algèbre de Boole A , une **base de filtre** est une partie B de E qui possède la propriété suivante, appelée **propriété de l'intersection fini**, toute partie finie non vide de B a une borne inférieure non nulle.

En d'autres termes, $B \subseteq E$ est une base de filtre si et seulement si : $\forall k \geq 1$, et $\forall x_1, x_2, \dots, x_k$ de B , $x_1 \wedge x_2 \wedge \dots \wedge x_k \neq 0$.

Lemme 2.15. Soient A une algèbre de Boole et X une partie de E , pour qu'il existe un filtre de A contenant X , il faut et il suffit que X soit une base de filtre.

Démonstration. Si $X \subseteq F$, et si x_1, x_2, \dots, x_k sont des éléments de X , alors leur borne inférieure $x_1 \wedge x_2 \wedge \dots \wedge x_k$ appartient à F , et comme $0 \notin F$, cette borne inférieure est non nulle, X donc une base de filtre.

Supposons que maintenant X soit une base de filtre :

1. Si $X = \emptyset$, $\{1\}$ est un filtre sur A qui contient X .
2. Si X n'est pas vide, on pose :

$$F_X = \{ \text{il existe un entier } k \geq 1 \text{ et des éléments } x_1, x_2, \dots, x_k \text{ de } X \text{ tel que } x \geq x_1 \wedge x_2 \wedge \dots \wedge x_k \}$$

F_X donc constitué des bornes inférieures des parties finies non vide de X ainsi que de tous les majorants de ces bornes inférieures. En particulier, chaque élément de X appartient à F_X , donc F_X contient X . Il est facile de prouver que F_X est un filtre.

Bornons nous aux indications suivantes :

- $0 \notin F_X$ (sinon la propriété de l'intersection finie ne serait pas vrai pour X) et $1 \in F_X$ (parce que X est non vide : 1 majore alors au moins un élément de X).
- Si $x \geq x_1 \wedge x_2 \wedge \dots \wedge x_h$ et $y \geq y_1 \wedge y_2 \wedge \dots \wedge y_k$ alors on a $x \wedge y \geq x_1 \wedge x_2 \wedge \dots \wedge x_h \wedge y_1 \wedge y_2 \wedge \dots \wedge y_k$.
- Si $x \geq x_1 \wedge x_2 \wedge \dots \wedge x_k$ et $y \geq x$, alors $y \geq x_1 \wedge x_2 \wedge \dots \wedge x_k$.

On a bien trouvé un filtre contenant X .

□

Théorème 2.21. Dans une algèbre de Boole, tout filtre est contenu dans au moins un ultrafiltre.

Démonstration. Étant donné un filtre F , l'idéal dual de F est contenu dans au moins un idéal maximal, dont le filtre dual est un ultrafiltre qui contient F .

□

Bien entendu, la formulation en termes de filtres et la formulation en termes d'idéaux sont, pour les algèbre de Boole, équivalentes.

Le théorème de l'ultrafiltre nous permet de donner une version un peu différente du lemme (après le définition base de filtre)

Lemme 2.16. *Soient A une algèbre de Boole et X une partie de E . Pour qu'il existe un ultrafiltre de A contenant X , il faut et il suffit que X soit une base de filtre.*

Démonstration. Les propriétés (il existe un ultrafiltre de A contenant X) et (il existe un filtre de A contenant X) sont équivalentes : bien évidemment, la première implique la deuxième, l'implication inverse résulte du théorème de l'ultrafiltre. Le lemme (après le définition base de filtre) permet de conclure. □

Chapitre 3

Théorème de représentation de Stone

Dans ce chapitre sera consacré au théorème de représentation de Stone.

3.1 L'espace de Stone d'une algèbre de Boole

On considère une algèbre de Boole $A = \langle E, +, \times, 0, 1 \rangle$

Définition 3.1. On appelle *espace de Stone* de A , et on note $S(A)$, l'ensemble des homomorphismes d'algèbres de Boole de A dans $\{0, 1\}$.

l'ensemble $S(A)$ est une partie de $\{0, 1\}^E$, ensemble des applications de E dans $\{0, 1\}$, que nous avons considéré comme un espace topologie en munissant de la topologie produit de la topologie discrète sur $\{0, 1\}$, on peut donc munir $S(A)$ de la topologie induite de celle de $\{0, 1\}^E$. Les ouverts de la topologie de $S(A)$ sont alors les traces sur $S(A)$ (c'est-à-dire les intersections avec $S(A)$) des ouverts de $\{0, 1\}^E$.

Lemme 3.1. L'espace topologique $S(A)$ est de dimension zéro.

Nous avons mis en évidence, en (définition 2.21) une base d'ouverts $(\Omega_i)_{i \in I}$ de l'espace $\{0, 1\}^E$, constituée d'ouverts-fermés. Chacun des Ω_i est l'ensemble des applications de E dans $\{0, 1\}$ qui prennent des valeurs données en un nombre fini de points donnés. D'après le lemme (2.8), si nous posons, pour chaque $i \in I$, $\Gamma_i = \Omega_i \cap S(A)$, la famille $(\Gamma_i)_{i \in I}$ ainsi obtenue est une base d'ouverts pour $S(A)$ constituée d'ouverts-fermés. Chaque Γ_i est l'ensemble des homomorphismes d'algèbre de Boole de A dans $\{0, 1\}$ qui prennent des valeurs données en un nombre fini de points donnés. Désormais, c'est exclusivement cette base d'ouverts que nous considérons pour l'espace

$S(A)$. Quand nous parlerons d'un ouvert élémentaire de l'espace de Stone de A , il s'agira d'un des ouverts-fermés de la famille $(\Gamma_i)_{i \in I}$.

Lemme 3.2. *pour qu'une partie Δ de $S(A)$ en soit un ouvert élémentaire, il faut et il suffit qu'il existe un élément x dans E tel que : $\Delta = \{f \in S(A); f(x) = 1\}$*

De plus, quand cette condition est réalisée, un tel élément x est unique.

Démonstration. Supposons que $\Delta = \{f \in S(A); f(x) = 1\}$; Δ est l'ensemble des homomorphismes de A dans $\{0, 1\}$ qui prennent la valeur 1 au point x : c'est donc un des ouverts élémentaires de $S(A)$. Supposons que Δ soit un ouvert élémentaire de $S(A)$.

- si $\Delta = \emptyset$, alors $\Delta = \{f \in S(A); f(0) = 1\}$
- si $\Delta \neq \emptyset$, alors il existe un entier $n \geq 1$, des éléments $x_1, x_2, x_3, \dots, x_n$ dans E , et des éléments $\varepsilon_1, \varepsilon_2, \varepsilon_3, \dots, \varepsilon_n$ dans $\{0, 1\}$, tel que :

$$\Delta = \{f \in S(A); f(x_1) = \varepsilon_1 \text{ et } f(x_2) = \varepsilon_2 \text{ et } \dots \text{ et } f(x_n) = \varepsilon_n\}$$

pour chaque $k \in \{1, 2, \dots, n\}$, posons :

$$y_k = \begin{cases} x_k & \text{si } \varepsilon_k = 1 \\ 1 + x_k & \text{si } \varepsilon_k = 0 \end{cases}$$

pour tout homomorphismes $f \in S(A)$, et pour tout $k \in \{1, 2, \dots, n\}$, on a :

$$f(y_k) = \begin{cases} f(x_k) & \text{si } \varepsilon_k = 1 \\ 1 + f(x_k) & \text{si } \varepsilon_k = 0 \end{cases}$$

On en déduit que, pour $f \in S(A)$, $h \in \Delta$ si et seulement si $f(y_k) = 1$ pour tout $k \in \{1, 2, \dots, n\}$. Mais cette dernière condition équivaut à : $f(y_1) \wedge f(y_2) \wedge \dots \wedge f(y_n) = 1$, ou encore puisqu'il s'agit d'homomorphismes, à $f(y_1 \wedge y_2 \wedge \dots \wedge y_n) = 1$. On voit donc que, si on pose $x = y_1 \wedge y_2 \wedge \dots \wedge y_n$, on a :

$$\Delta = \{f \in S(A); f(x) = 1\}$$

2 l'unicité

Supposons que x et y deux éléments distinctes de E , $x + y \neq 0$, on peut considérer le filtre principale engendré par $x + y$ et, d'après le théorème de l'ultrafiltre, un ultrafiltre contenant ce filtre. A un tel ultrafiltre est associé un homomorphisme φ de A dans $\{0, 1\}$ qui est tel que $\varphi(x + y) = 1$, ou encore $\varphi(x) + \varphi(y) = 1$, ce qui signifie que un et un seul des deux éléments $\varphi(x)$ et $\varphi(y)$ est égale à 1.

□

Corollaire 9. *l'ensemble des fermés élémentaires de $S(A)$ coïncide avec l'ensemble des ouverts élémentaires.*

Démonstration. Soit Γ un fermé élémentaire de $S(A)$. Alors $\Delta = S(A) - \Gamma$ est un ouvert élémentaire, donc d'après le lemme précédent, il existe un élément $x \in E$ tel que :

$$\Delta = \{f \in S(A); f(x) = 1\}.$$

D'où

$$\Gamma = \{f \in S(A); f(x) \neq 1\} = \{f \in S(A); f(x) = 0\} = \{f \in S(A); f(1+x) = 1\}$$

On voit, toujours grâce au lemme précédent, Γ est un ouvert élémentaire. □

Lemme 3.3. *L'espace topologique $S(A)$ est compact.*

Démonstration. Tout d'abord, la topologie de $S(A)$ est séparé puisque celle de $\{0, 1\}^E$ l'est.

Il nous faut ensuite montrer que, de toute famille de fermés de $S(A)$ dont l'intersection est vide, on peut extraire une sous-famille finie dont l'intersection est déjà vide. Mais on a vu (lemme 2.6) que l'on peut se contenter de le vérifier pour une famille de fermés élémentaires; or ici, comme on vient de le voir, les fermés élémentaires coïncident avec les ouverts élémentaires. Considérons donc une famille $(\Sigma_j)_{j \in J}$ d'ouverts élémentaires de $S(A)$, infinie, tel que $\bigcap_{j \in J} \Sigma_j = \emptyset$. D'après le lemme précédent, il existe, pour chaque $j \in J$, un unique élément x_j dans E tel que :

$$\Sigma_j = \{f \in S(A); f(x_j) = 1\}.$$

Posons $X = \{x_j; j \in J\}$. Dire que l'intersection de la famille $(\Sigma_j)_{j \in J}$ est vide, c'est-à-dire qu'il n'y a aucun homomorphisme d'algèbre de Boole de A dans $\{0, 1\}$ qui prenne la valeur 1 en chaque élément de X , ou encore qu'il n'y a aucun ultrafiltre de A qui contient X . Cela signifie (lemme 2.16) que X n'est pas une base de filtre. Il existe donc une partie finie non vide $\{x_{j_1}, x_{j_2}, \dots, x_{j_k}\} \subseteq X$ dont la borne inférieure est nulle. Aucun ultrafiltre de A ne peut alors contenir en même temps x_{j_1}, x_{j_2}, \dots et x_{j_k} . en d'autres termes, aucun homomorphisme de A dans $\{0, 1\}$ ne peut prendre la valeur 1 en $x_{j_1}, x_{j_2}, \dots, x_{j_k}$ simultanément. Cela revient à dire que :

$$\Sigma_{j_1} \cap \Sigma_{j_2} \cap \dots \cap \Sigma_{j_k} = \emptyset.$$

On a ainsi une sous-famille finie de la famille $(\Sigma_j)_{j \in J}$ dont l'intersection est vide. □

Corollaire 10. *L'espace de Stone de A est un espace topologique booléen.*

Démonstration. C'est en effet un espace compact (le lemme précédent) et de dimension 0 (lemme 3.1) □

Lemme 3.4. *L'ensemble des ouverts-fermés de $S(A)$ coïncide avec l'ensemble de ses ouverts élémentaires.*

Démonstration. On sait déjà (3.3) que tous les ouverts élémentaires sont des ouverts-fermés. Inversement, soit Γ un ouvert-fermé quelconque de $S(A)$, comme Γ est un ouvert, il est réunion d'ouverts élémentaires : par exemple, $\Gamma = \cup_{j \in J} \Gamma_j$ pour un certain sous-ensemble $J \subseteq I$. Mais comme Γ est un fermé dans l'espace compacte $S(A)$, il est lui même compacte, et du recouvrement ouvert $(\Gamma_j)_{j \in J}$ de Γ , on peut extraire un sous-recouvrement fini, par exemple : $\Gamma = \Gamma_{j_1} \cup \Gamma_{j_2} \cup \dots \cup \Gamma_{j_m}$. On sait (lemme 3.2) qu'on peut trouver des éléments x_1, x_2, \dots, x_m dans E tels que, pour tout $k \in \{1, 2, \dots, m\}$,

$$\Gamma_{j_k} = \{f \in S(A); f(x_k) = 1\}.$$

Posons

$$x = x_1 \cup x_2 \cup \dots \cup x_m, \Delta = \{f \in S(A); f(x) = 1\}$$

et montrons que $\Gamma = \Delta$. Tout élément de Γ est un homomorphisme qui prend la valeur 1 en au moins un des points x_1, x_2, \dots, x_m ; il prend aussi la valeur 1 au point x qui est leur borne supérieure. Donc $\Gamma \subseteq \Delta$. D'autre part, tout homomorphisme qui n'est pas dans Γ , et qui ne prend donc la valeur 1 en aucun des points x_1, x_2, \dots, x_m , doit prendre la valeur 0 en chacun de ces points, donc aussi en leur borne supérieure x , et ne peut appartenir à Δ . Cela prouve que $\Delta \subseteq \Gamma$, donc $\Gamma = \Delta$. □

3.2 Théorème de Stone

Théorème 3.1. *Toute algèbre de Boole est isomorphe à l'algèbre de Boole des ouverts-fermés de son espace de Stone.*

Démonstration. L'algèbre de Boole des ouverts-fermés de $S(A)$ est notée $\mathfrak{N}(S(A))$. Appelons H l'application de E dans $\mathfrak{N}(S(A))$ qui, à tout élément a de E , associe :

$$H(a) = \{f \in S(A); f(a) = 1\}.$$

Montrons que H est un isomorphisme d'algèbres de Boole de A sur $\mathfrak{N}(S(A))$.

D'après le lemme (3.2) et (3.4), l'application H prend ses valeurs dans $\mathfrak{N}(S(A))$ et son image est exactement $\mathfrak{N}(S(A))$, H est donc une surjection de E sur $\mathfrak{N}(S(A))$.

En vertu du théorème (2.10) pour montrer que H est un isomorphisme à d'algèbres de Boole, il suffit alors de s'assurer que, quels que soient les éléments x et y dans E :

$$x \leq y \text{ si et seulement si } H(x) \subseteq H(y).$$

Soient donc les éléments x et y dans E . Si $x \leq y$, alors pour tout homomorphisme $f \in S(A)$, $f(x) \leq f(y)$, donc, pour tout homomorphisme f tel que $f(x) = 1$, on a aussi $f(y) = 1$, ce qui signifie que $H(x)$ est inclus $H(y)$. Si $x \not\leq y$, alors $x(1+y) \neq \emptyset$ (lemme 2.11). On peut donc considérer le filtre principal engendré par $x(1+y)$, puis un ultrafiltre le contenant (théorème de l'ultrafiltre), et l'homomorphisme $f \in S(A)$ associé à cet ultrafiltre. On a :

$$f(x(1+y)) = 1.$$

donc

$$f(x) = 1 \text{ et } f(1+y) = 1,$$

c'est à dire $f(y) = 0$. On en déduit que $f \in H(x)$ et $f \notin H(y)$, et que $H(x)$ n'est pas inclus dans $H(y)$. □

Le théorème de Stone permet de donner une preuve très simple du théorème (2.11).

Corollaire 11. *Toute algèbre de Boole finie est isomorphe à l'algèbre de Boole des parties d'un ensemble.*

Démonstration. Si l'ensemble E est fini, la topologie sur $\{0, 1\}^E$ est la topologie discrète. Il en est donc de même de la topologie induite sur le sous-ensemble $S(A)$. Toutes les parties de $S(A)$ sont donc ouverts et fermés. L'algèbre de Boole $\mathfrak{N}(S(A))$ coïncide donc avec $\mathfrak{N}(S(A))$ et A est isomorphe à $\mathfrak{N}(S(A))$. □

Dans le cas d'une algèbre de Boole quelconque, ce qui montre le théorème de Stone, c'est qu'elle est isomorphe à une sous-algèbre de Boole de l'algèbre des parties d'un ensemble.

3.3 Les espaces booléens sont des espaces de Stone

A chaque algèbre de Boole A , nous avons associé un espace topologique booléen : son espace de Stone $S(A)$, et nous avons vu que A est isomorphe à l'algèbre de Boole des ouverts-fermés de cet espace booléen. Il est donc assez naturel d'étudier le cas où A est donnée comme algèbre de Boole des ouverts-fermés d'un certain espace topologique booléen X . Le problème qui se pose alors est de comparer l'espace X à cet autre espace booléen qu'est l'espace de Stone de A , autrement dit, de comparer X et $S(\mathfrak{N}(X))$. Le résultat de la comparaison est que ces deux objets se ressemblent beaucoup.

Théorème 3.2. *Toute espace topologique booléen X est homéomorphe à l'espace de Stone $S(\mathfrak{N}(X))$ de l'algèbre de Boole des ouverts-fermés de X .*

Démonstration. Soit X un espace booléen. D'après le lemme (2.7) nous pouvons prendre comme base d'ouverts pour la topologie de X l'algèbre de Boole $\mathfrak{N}(X)$ de tous les ouverts-fermés de X . Pour chaque $x \in X$, notons f_x l'application de $\mathfrak{N}(X)$ dans $\{0, 1\}$ définie par : pour tout élément Ω appartenant à $\mathfrak{N}(X)$,

$$f_x(\Omega) = \begin{cases} 1 & \text{si } x \in \Omega \\ 0 & \text{si } x \notin \Omega \end{cases}$$

Nous allons montrer que l'application f qui, à chaque $x \in X$, associe f_x , est un homéomorphisme de l'espace topologique X sur l'espace topologique $S(\mathfrak{N}(X))$.

Comme f est a priori une application de X dans $\{0, 1\}^{\mathfrak{N}(X)}$, nous devons montrer pour commencer qu'elle prend en réalité ses valeurs dans $S(\mathfrak{N}(X))$:

1. Pour chaque $x \in X$, f_x est un homéomorphisme d'algèbres de Boole.

Démonstration. Pour tous ouverts-fermés Ω et Δ de X , on a $f_x(\Omega \cap \Delta) = 1$ si et seulement si $x \in \Omega \cap \Delta$, c'est à dire $x \in \Omega$ et $x \in \Delta$ ce qui équivaut à $f_x(\Omega) = 1$ et $f_x(\Delta) = 1$, et donc $f_x(\Omega)f_x(\Delta) = 1$. On en déduit que $f_x(\Omega \cap \Delta) = f_x(\Omega)f_x(\Delta)$. D'autre part, $f_x(X - \Omega) = 1$ si et seulement si $x \in X - \Omega$, c'est à dire $x \notin \Omega$, ou encore $f_x(\Omega) = 0$, ainsi, $f_x(X - \Omega) = 1 + f_x(\Omega)$. On voit que les conditions du théorème (2.9) sont satisfaites : f_x est bien homomorphisme. \square

2. L'application f est injective.

Démonstration. Soient x et y deux éléments distincts de X . Comme X est un espace séparé, on peut trouver un ouvert O tel que $x \in O$ et $y \notin O$ (on peut par exemple prendre pour O l'ensemble $X - \{y\}$). Mais O est un réunion d'ouverts élémentaires de la base $\aleph(X)$, il y a donc un ouvert-fermé $\Omega \in \aleph(X)$ tel que $x \in \Omega$ et $y \notin \Omega$, on a $f_x(\Omega) = 1$ et $f_y(\Omega) = 0$, ce qui prouve que f_x est différent de f_y . \square

3. L'application f est surjective sur $S(\aleph(X))$.

Démonstration. Soit h un élément de $S(\aleph(X))$, c'est à dire un homomorphisme de $\aleph(X)$ dans $\{0, 1\}$. L'ultrafiltre de $\aleph(X)$ associé à h est :

$$\mu = \{\Omega \in \aleph(X); h(\Omega) = 1\} = h^{-1}[\{1\}].$$

Comme μ a la propriété de l'intersection finie, comme les éléments de μ sont en particulier des fermés, et comme l'espace topologique X est compact, on peut affirmer que l'intersection de tous les éléments de μ est non vide. Soit x un élément de cette intersection.

Pour chaque ouvert-fermé $\Omega \in \aleph(X)$, on a : ou bien $\Omega \in \mu$ et alors $f_x(\Omega) = 1$ et $h(\Omega) = 1$, ou bien $\Omega \notin \mu$, et dans ce cas $X - \Omega \in \mu$; $f_x(\Omega) = 0$ et $h(\Omega) = 0$. Ainsi, pour tout $\Omega \in \aleph(X)$, $f_x(\Omega) = h(\Omega)$. Il en résulte que $h = f_x = f(x)$. \square

Remarque 3.1. On peut remarquer que l'élément x , dont nous venons de montrer que c'est un antécédent de h par l'application f , est l'unique de l'intersection de tous les ouverts-fermés appartenant à μ . En effet, tout élément y de cette intersection vérifierait de la même manière $h = f(y)$, mais comme f est injective, cela exige $y = x$. Cette remarque va nous permettre de décrire la bijection réciproque $f^{-1} : C'est l'application de $S(\aleph(X))$ dans X qui, à tout homomorphisme h de $\aleph(X)$ dans $\{0, 1\}$, associe l'unique élément de l'intersection de tous les ouverts-fermés appartenant à l'ultrafiltre $h^{-1}[\{1\}]$.$

4. L'application f est continue.

Démonstration. Soit G un ouvert appartenant à la base d'ouverts-fermés de $S(\aleph(X))$.

D'après le lemme (3.2), il existe un unique élément Ω de $\aleph(X)$ tel que :

$$G = \{h \in S(\aleph(X)); h(\Omega) = 1\}.$$

L'image réciproque de G par l'application f est :

$$\{x \in X; f_x \in G\} = \{x \in X; f_x(\Omega) = 1\} = \{x \in X; x \in \Omega\} = \Omega.$$

C'est donc un ouvert de X . \square

5. L'application réciproque f^{-1} est continue.

Démonstration. Soit Ω un ouvert élémentaire de l'espace X (c'est à dire un élément de $\aleph(X)$). L'image réciproque de Ω par l'application f^{-1} , c'est son image directe par f , puisque f est bijective. C'est donc l'ensemble $f[\Omega] = \{f_x; x \in \Omega\}$. Nous devons montrer que c'est un ouvert de l'espace $S(\aleph(X))$.

Posons

$$V = \{h \in S(\aleph(X)); h(\Omega) = 1\}.$$

L'ensemble V est un ouvert, montrons que $f[\Omega] = V$, ce qui achèvera la démonstration .

Pour tout $x \in \Omega$, par définition de f_x , on a $f_x(\Omega) = 1$, soit $f_x \in V$, donc $f[\Omega] \subseteq V$.

Pour tout $h \in V$, h admet un antécédent $y \in X$ par la bijection $f : h = f_y$. Comme $h \in V$, on a $h(\Omega) = f_y(\Omega) = 1$, d'où $y \in \Omega$ et $f_y = h \in f[\Omega]$. Ainsi, V inclus dans $f[\Omega]$. \square

Remarque 3.2. *On pourra remarquer que la démonstration du dernière point était superflue : Il y a en effet un célèbre théorème de topologie qui affirme que toute application bijective continue d'un espace topologique compact dans un espace topologique séparé est un homéomorphisme (la continuité de la bijection réciproque étant alors assurée).*

Nous avons en définitive établi entre algèbre de Boole et espaces topologiques booléens une correspondance biunivoque (à isomorphe près d' un coté, à homéomorphisme près de l'autre).

6. Toute algèbre de Boole est (isomorphe à) l'algèbre de Boole des ouverts-fermés d'un espace topologique booléen.

7. Tout espace topologique booléen est (homéomorphisme) à l'espace de Stone d'une algèbre de Boole.

On notera en passant qu'il y avait d'assez bonnes raisons d'appeler, espace booléen, les espaces topologiques compacte de dimension zéro.

8. Pour que deux algèbres de Boole soient isomorphes, il faut et il suffit que leurs espaces de Stone soient homéomorphes.

9. Pour que deux espaces topologiques booléens soient homéomorphes, il faut et il suffit que les algèbres de Boole constituées par leurs ouverts-fermés respectifs soient isomorphes.

\square

Conclusion

L'objectif de ce mémoire est d'introduire l'ensemble des propriétés topologiques des algèbres de Boole. Un algèbre de Boole c'est donc indifféremment un anneau dans lequel tout élément est égal a son carré, ou un ensemble ordonné qui a une structure de treillis distributif et complémenté. En plus on a donné la notion des atomes dans l'algèbre de Boole et les homomorphisme d'algèbre de Boole ainsi que les idéaux et filtre on a fini ce travail par l'application de ces propriétés topologiques sur le théorème de Stone.

Bibliographie

- [1] **Nicolas Bourbaki**. Théorie des ensembles, Hermann, 1954, Masson, 1990.
- [2] **Paul R. Halmos**. Introduction à la théorie des ensembles, Gauthier-Villars.
- [3] **Jean-Louis Krivine**. Théorie axiomatique des ensembles, Presse universitaire de France, 1972.
- [4] **W.Sierpinski**. Cardinal and ordinal numbers, PWN-Polish Scientific Publishers, 1965.
- [5] **Sikorski**. Boolean algebras, Springer-Verlag, 1960.
- [6] **P. Halmos**. Naive set theory, D. Van Nostrand, 1960.
- [7] **P. Suppes**. Axiomatic set theory, D. Van Nostrand, 1960.
- [8] **G.Kreisel et J.L.Krivine**. Eléments de logique mathématique, Dunod, 1966.
- [9] **J.F.Pabion**. logique mathématique, Hermann, 1976.
- [10] **William B. Easton**, Powers of regular cardinals, Annals of math, Logique. 1970.
- [11] **John Myhill, Dana Scott**. Ordinal definability, Summer Institute on axiomatic set theory, Los Angeles, 1967.