NOTES DE COURS DE MAT3223

« FONDEMENTS ALGÈBRIQUES»

EMMANUEL KENGNE

kengem01@uqo.ca

http://www.emmanuel-schl-kengne.com/

UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS

Hiver 2015

Fondements algbriques

(Dated: 23rd December 2014)

Nous étudierons tour à tour:

- Vocabulaire de la logique: Les Opérateurs logiques, Connecteurs logiques, modes de raisonnement (et, ou, négation, implication, équivalence, raisonnement par l'absurde, raisonnement par récurrence). Quantificateurs
- Vocabulaire de théorie des ensembles: Définition, sous-ensemble, intersection, réunion, complé-mentaire, produit cartésien, ensemble des parties.
- Applications: Injection, surjection, bijection, exemples. Dénombrement, combinaisons, arrangements, égalité de Pascal, formule du binôme.
- Relations et lois de composition : Définition, classes d'équivalence, partition d'un ensemble, ensemble quotient, exemples simples, relation d'équivalence, lois de composition.
- Vocabulaire de l'algèbre booléenne: Axiomes et postulats, Principe de dualité, Notation algébrique, Décomposition de Shannon, Table de vérité.

PACS numbers:

Contents

CHAPITRE 1

NOTION DE LOGIQUE

Dans le présent chapitre, nous introduisons la notion de la logique mathématique.

I. LOGIQUE DES PROPOSITIONS

A. Proposition

Définition (Proposition): Une proposition p est un enoncé déclaratif (énoncé mathématique) dont on peut dire s'il est vrai (valeur 1 ou V) ou s'il est faux (valeur 0 ou F), indépendamment de tout context de lieu, de temps, ou de personne qui le prononce. De plus, un enoncé qui est à la fois vrai et faux n'est pas une proposition.

Définition (valeur de vérité): Donner la valeur de vérité $\upsilon(p)$ d'une proposition p c'est dire si la proposition p est vraie ou fausse. Ainsi dire

$$\upsilon(p) = \begin{cases} 1 \text{ ou } V, & \text{si } p \text{ est une proposition vraie,} \\ 0 \text{ ou } F, & \text{si } p \text{ est une proposition fausse.} \end{cases}$$

Exemples: 1) Puisque la proposition p : «$\pi \geq 2$» est vraie, sa valeur de vérité est $\upsilon(p) = 1$;

2) La valeur de vérité de la proposition p : «9 est divisible par 2» est fausse. Par conséquent, sa valeur de vérité est $\upsilon(p) = 0$.

B. Connecteurs logiques

En logique, les propositions sont les atomes. À partir d'une, deux ou plusieurs propositions on peut créer de nouvelles propositions à l'aide de connecteurs logiques. Les nouvelles propositions ainsi formées et les propositions utilisées, sont regroupées dans un tableau appelé **table de vérité**.

Définition (Table de vérité): La table de vérité d'une proposition est un tableau énumérant les valeurs logiques (valeurs de vérié) de ladite proposition pour les différentes combinaisons des valeurs de ses variables indépendantes. Une table de vérité prend, en

entrée les résultats des divers propositions et en sortie, les résultats des opérations logiques faites entre ces propositions. Autrement dit,

Nous allons définir les règles pour les cinq connecteurs «**NON**, de symbole ¬», «**ET**, de symbole ∧», «**OU**, de symbole ∨», «**implication logique** ou **si ... alors**, de symbole →» et «**équivalence logique** ou **si et seulement** si, de symbole ↔».

Définition (Négation, « ¬»): La négation d'une proposition est une proposition qui est vraie si celle-ci est fausse et fausse si celle-ci est vraie.

p	$\neg p$
1	0
0	1

Table de vérité de la négation ¬

Exemples: La négation de la proposition p :«$a > b$» est $\neg p$: «$a \leq b$».

Définition (Conjonction ET, « ∧»): La conjonction de deux propositions p et q est la proposition notée $p \wedge q$ qui est vraie si les deux propositions p et q sont simultanément vraies, et fausse dès que l'une au moins des deux propositions p et q est fausse. Ainsi, on peut dire que

$$\upsilon(p \wedge q) = \upsilon(p) \times \upsilon(q).$$

On en déduit la table de vérité suivante:

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Table de vérité de la conjonction ∧

Exemple: Trouver la valeur de vérité de la proposition p :«$\pi > 3$ et 9 est divisible par 2».

Solution: Puisque $\upsilon(\pi > 3) = 1$ et $\upsilon(9 \text{ est divisible par } 2) = 0$, on a $\upsilon(\pi > 3 \text{ et } 9 \text{ est divisible par } 2) = \upsilon(\pi > 3) \times \upsilon(9 \text{ est divisible par } 2) = 1 \times 0 = 0$. La table de vérité correspondante est:

$\pi > 3$	9 est divisible par 2	$p \wedge q$
1	0	0

Définition (Disjonction = ou inclusif, $\vee$): La disjonction de deux propositions p et q est la proposition notée $p \vee q$ qui est vraie dès que l'une au moins des deux propositions p et q est vraie. Elle est fausse si les deux propositions sont simultanément fausses. Si on adopte l'égalité $1 + 1 = 1$ (vrai et vrai = vrai), alors nous pouvons écrire

$$\upsilon(p \vee q) = \upsilon(p) + \upsilon(q),$$

d'où la table de vérité suivante:

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

Table de vérité de la disjonction $\vee$

Exemple: Soient les propositions $p : 4^2 > 14$ et $q : \sqrt{3} \leq 1.5$. Trouver la valeur de vérité de la proposition $p \vee q$.

Solution: $\upsilon(p \vee q) = \upsilon(p) + \upsilon(p) = \upsilon(4^2 > 14) + \upsilon(\sqrt{3} \leq 1.5)$. Puisque $4^2 = 16 > 14$ et $\sqrt{3} = 1.7321 > 1.5$, on a $\upsilon(4^2 > 14) = 1$ et $\upsilon(\sqrt{3} \leq 1.5) = 0$. Par conséquent, $\upsilon(p \vee q) = \upsilon(p) + \upsilon(p) = \upsilon(4^2 > 14) + \upsilon(\sqrt{3} \leq 1.5) = 1 + 0 = 1$, ce qui revient à dire que la proposition $4^2 > 14$ ou $\sqrt{3} \leq 1.5$ est vraie.

Définition (Implication logique, Conditionnelle, si ... alors, $\rightarrow$): Si p et q sont deux propositions, alors l'implication logique «si p alors q, i.e., $p \rightarrow q$» est une proposition qui est vraie si p est faux, ou bien si p et q sont simultanément vrais. Cette implication est fausse uniquement si l'antécédant p est vrai et le conséquent q faux. Autrement dit, la proposition $p \rightarrow q$ a la même valeur de vérité que $\neg p \vee q$. Par conséquent,

$$\upsilon(p \rightarrow q) = \upsilon(\neg p) + \upsilon(q),$$

d'où la table de vérité

p	$\neg p$	q	$p \rightarrow q = \neg p \vee q$
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	1

Table de vérité de l'implication logique $\rightarrow$

Remarque: Dans la proposition $p \to q$, p est appelée hypothèse, et q la conclusion.

Exemple 1: «si $2 = 0$ alors $x^2 > 0$» est une proposition vraie.

Exemple 2: Soient les propositions $p : \pi \leq 3.12$ et $q : 4^2 > 25$. Trouver la valeur de vérité de la proposition $p \to q$.

Solution: Puisque la proposition $\neg p : \pi > 3.12$ est vraie, on a $\upsilon(p \to q) = 1$.

Exemple 3: Trouver la valeur de vérité de la propostion $p \to q$, si $p : \pi \geq 3.12$ et $q : 4^2 > 25$.

Solution: Puique la proposition $\neg p : \pi < 3.12$ est fausse et la proposition $q : 4^2 = 16 > 25$ est fausse, nous aurons $\upsilon(p \to q) = \upsilon(\neg p) + \upsilon(q) = 0 + 0 = 0$. Ainsi, la proposition $\pi \geq 3.12 \to 4^2 > 25$ est fausse.

Définition (Équivalence logique, si et seulement si, $\leftrightarrow$): Si p et q sont deux propositions, alors l'´equivalence logique «p si et seulement si q» de symbole «$p \leftrightarrow q$» est une proposition qui signifie (p si q) et (p seulement si q). La valeur de vérité de l'équivalence logique «p si et seulement si q» est la valeur de vérité de $(q \to p) \wedge (p \to q)$. Puisque $q \to p = \neg q \vee p$ et $p \to q = \neg p \vee q$, on a

$$\begin{aligned}
\upsilon(p \leftrightarrow q) &= \upsilon((q \to p) \wedge (p \to q)) = \upsilon(q \to p) \times \upsilon(p \to q) \\
&= \upsilon(\neg q \vee p) \times \upsilon(\neg p \vee q) \\
&= [\upsilon(\neg q) + \upsilon(p)] \times [\upsilon(\neg p) + \upsilon(q)] \\
&= \upsilon(\neg p)\upsilon(\neg q) + \upsilon(\neg p)\upsilon(p) + \upsilon(q)\upsilon(\neg q) + \upsilon(q)\upsilon(p) \\
&= \upsilon(\neg p)\upsilon(\neg q) + \upsilon(q)\upsilon(p)
\end{aligned}$$

Ainsi,

$$\upsilon(p \leftrightarrow q) = \begin{cases} 1, \text{ si } \upsilon(q) = \upsilon(p) \\ 0, \text{ si } \upsilon(q) \neq \upsilon(p). \end{cases}$$

Autrement dit, l'équivalence «p si et seulement si q» est donc vraie uniquement si p et q ont la même valeur de vérité. On a alors la table de vérité suivante:

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Table de vérité de l'équivalence logique $\leftrightarrow$

Exemple: La proposition «$x > 0 \leftrightarrow x^3 > 0$» est vraie.

C. Règles logiques

Énonçons quelques règles logiques

Proposition (Loi de non-contradiction): Si p est une proposition, alors $P \wedge \neg P$ est une proposition fausse.

En effet, $\upsilon(P \wedge \neg P) = \upsilon(P) \times \upsilon(\neg P) = 0$, car l'un des termes du produit est 0 (l'autre est 1).

Proposition (Loi du tiers exclu): Si p est une proposition, alors $P \vee \neg P$ est une proposition vraie.

En effet, $\upsilon(P \vee \neg P) = \upsilon(P) + \upsilon(\neg P) = 1 + 0$ (ou bien $0 + 1) = 1$.

Proposition: Si p et q sont deux propositions, alors on aure

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]\,.$$

Exemple: Pour montrer la proposition «$x < 0$ si et seulement si $x^3 < 0$», il faut montrer que «$x < 0 \rightarrow x^3 < 0$» et «$x^3 < 0 \rightarrow x < 0$».

Proposition (Transivité): Soient p et q sont deux propositions. Si la proposition «$(p \rightarrow q) \wedge (q \rightarrow r)$» est vraie alors la proposition «$p \rightarrow r$» sera aussi vraie.

Proposition (Règle d'inférence): Soient p et q deux propositions. Si la proposition «$p \wedge (p \rightarrow q) \rightarrow q$» est vraie alors q est une proposition vraie.

Proposition (Double négation): S p est une proposition, alors on a le résultat $\neg(\neg p) = p$.

Remarque (contre-exemple): On peut démontrer que la proposition $p \rightarrow q$ est fausse par contre-exemple, i.e., en trouvant un exemple pour lequel p est vrai, mais q est faut.

II. PRÉDICATS ET QUANTIFICATEURS

Débutons cette section lar la notion d'ensembles.

A. Notion d'ensembles

Définition (Ensemble): Un ensemble est une collection d'objets. Chaque objet de cette collection s'appelle élément de l'ensemble.

Définition (Appartenance «∈»): Soit E est un ensemble donné. Si x est un élément de E alors on dit que x appatient à E et on écrit $x \in E$. Si x n'est pas un élément de E, on dit que x n'appartient pas à E et on écrit $x \notin E$.

$x \notin E$ est la négation de la proposition $x \in E$.

Exemple 1: L'ensemble des entiers naturels inférieurs à 13 et divisible par deux est $A = \{0,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12\}$. Ainsi, on a $2 \in A$, $3 \notin A$ car, bien que 3 soit inférieur à 13, il n'est pas divisible par deux.

Exemple 2: L'ensemble des nombres rationnels est

$$\mathbf{Q} = \left\{x = \frac{m}{n} : n, m \in N,\ n \neq 0,\ \frac{m}{n} \text{ étant irréductible}\right\}$$

$\sqrt{\frac{9}{4}} \in \mathbf{Q}$. En effet, $\sqrt{\frac{9}{4}} = \frac{3}{2} = \frac{m}{n}$ avec $m = 3$ et $n = 2$.

B. Prédicats

Il se trouve que le langage abstrait des propositions introduit dans la section précedente ne suffit pas pour mettre en formule toutes les propositions du langage usuel et les propositions mathématiques. Considérons par exemple l'énoncé

«x est plus petit que 5».

Cet énoncé n'est pas une proposition car on ne peut pas se prononcer sur sa valeur de vérité. Dans cet énoncé, la variable x est le sujet de l'énoncé alors «est plus petit que 5» est le **prédicat** qui est une propriété. Si nous désignons par $f(x)$ l'énoncé ci-dessus où x est la variable et f est le prédicat «est plus petit que 5», alors $f(x)$ est appelée **fonction propositionnelle** ou **fonction logique**. Une fois qu'une valeur est attribuée à la variable x, l'énoncé $f(x)$ devient une proposition et acquiert une valeur de vérité, vrai (1) ou faux (0).

Par exemple: $f(2)$: «2 est plus petit que 5» est une proposition vraie; $f(8)$: «8 est plus petit que 5» est fausse.

Exemple de fonction propositionnelle: Soit $\mathbf{Z} = \{0, \ \pm 1, \ \pm 2, \ ...\}$ l'ensemble des entiers relatifs. Soit $f(x)$ la fonction propositionnelle (fonction logique) «x est divisible par 3».

(i) La fonction propositionnelle $f(x)$ n'a pas de valeur de vérité tant qu'une valeur n'est pas assignée à la variable x;

(ii) $f(8)$ est une proposition fausse, car $8 \in \mathbf{Z}$, mais n'est pas divisible par 3;

(iii) $f(-21)$ est une proposition vraie, car $-21 \in \mathbf{Z}$ et $-\frac{21}{3} = -7$, i.e., -21 est divisible par 3;

(iv) $f(12) \wedge f(14)$ est une proposition fausse car $v(f(12)) = 1$ et $v(f(14)) = 0$;

(v) $f(15) \vee f(y)$ n'est pas une proposition car la variable y n'a pas de valeur.

Remarque: Spécifier une valeur à une variable permet de transformer une fonction propositionnelle en une proposition.

C. Quantificateur

La quantification est une méthode pour changer une fonction propositionnelle en une proposition. Nous étudierons deux types de quantifications : la quantification universelle et la la quantification existentielle.

De nombreux énoncés mathématiques affirment qu'une propriété est vraie pour toutes les valeurs d'une variable appartenant à un certain domaine, appelé l'**univers du discours** ou **domaine de définition**. Dans une fonction propositionnelle $f(x)$, l'univers du discours ou domaine de définition de f précise les valeurs possibles de la variable x et doit toujours être donné quand un quantificateur est utilisé. Puique la valeur de $f(x)$ dépend de celle de x, $f(x)$ est appelée variable indépendente ou variable liée, alors que x est appelé variable indépendente ou variable libre (cette variable x ne dépend pas de f).

1. Quantificateur universel

Définition (**quantificateur universelle** $\forall$): La **quantification universelle** de la fonction propositionnelle $f(x)$ est la proposition

«$f(x)$ **est vraie pour toutes les valeurs de** x **dans l/univers du discours**».

Ici, la variable x est limitée à l'univers du discours transformant la fonction propositionnelle $f(x)$ en une proposition. Si nous désignons par A l'univers du discours, alors la notation

$$\forall x \in A,\ f(x)$$

se lit «pour tout x dans A, $f(x)$» ou encore «quel que soit x appartenant à A, $f(x)$» et désigne la quantification universelle de $f(x)$. Le symbole $\forall$ est appelé **quantificateur universel**.

Exemple: La proposition «$\forall x \in \mathbf{N},\ x \geq 0$» est vraie. Ici, l'univers du discours est l'ensemble $\mathbf{N}$ et la fonction propositionnelle $f(x)$ est «$x \geq 0$».

Exemple 2: «$\forall x \in \mathbf{R},\ x+5 \leq 0$» est une proposition fausse. Pour cet exemple, l'univers du discours est $\mathbf{R}$ alors que la fonction propositionnelle $f(x)$ est «$x + 5 \leq 0$».

Définition (contre-exemple): On appelle contre-exemple de la quantification universelle «$\forall x \in A,\ f(x)$», tout élément x de l'univers du discours pour lequel la proposition $f(x)$ est fausse.

Remarque: Si l'univers du discours A est vide, alors la quantification iniverselle de $f(x)$ «$\forall x \in A,\ f(x)$» sera vraie.

2. Quantificateur existenciel

Définition (Quantificateur existenciel $\exists$): On appelle **quantification existentielle** de la fonction propositionnelle $f(x)$, la proposition

«**Il existe un élément x dand l'univers du discours tel que f(x) soit vraie**».

La variable x est limitée à l'univers du discours transformant la fonction propositionnelle $f(x)$ en une proposition.

Pour écrire la quantification existentielle de la fonction $f(x)$ sur l'univers du discours A, on utilise les symboles

$$\exists x \in A : f(x).$$

Le symbole $\exists$ s'appelle **quantificateur existentiel** et l'écriture se lit: «il existe x appartenant à A tel que $f(x)$» ou bien «il existe au moins un x dans A tel que $f(x)$» ou encore «pour un certain x dans A, $f(x)$».

Remarque: On accepte qu'il existe x dans l'univers du discours seulement s'il est possible d'en trouver un. Par conséquent, si l'univers du discours est vide, alors «$\exists x \in A : f(x)$» sera une proposition fausse.

Exemple 1: Si nous désignons par $\mathbf{Z}$ l'ensemble des entiers relatifs (0, ± 1, ± 2, ...), alors la proposition

$$\exists x \in \mathbf{Z} : x < 0$$

est vraie. Ici, l'univers du discours est l'ensemble $\mathbf{Z}$ des entiers relatifs et la fonction propositionnelle $f(x)$ est «$x < 0$».

Définition (quantification d'existence unique): On appelle **quantification d'existence unique** de la fonction propositionnelle $f(x)$, la proposition

«Il existe un et un seul élément x de l'univers du discours tel que $f(x)$ soit vraie»

Si A désigne l'univers du discours, on écrit

$$\exists! x \in A : f(x).$$

Cette notation se lit aussi de la façon suivante: «il existe un unique x dans A tel que $f(x)$» ou encore «in existe exactement un x dans A tel que mf(x)» ou encore «on peut trouver un seul x dans A tel que $f(x)$».

Exemple: Si A désigne l'ensemble des nombres premiers et $f(x)$ est la fonction propositionnelle «x est pair», alors

$$\exists! x \in A : f(x)$$

est une proposition vraie. En effet, 2 est le seul nombre premier qui soit pair. Ainsi, $f(2)$ est une proposition vraie et $\forall x \in A \wedge x \neq 2$, $f(x)$ est faux.

D. Négation des quantificateurs

La négation du quantificateur universel est le quantificateur existentiel

$$\neg\left(\forall x \in A,\ p\right) \Leftrightarrow \left(\exists x \in A :\ \neg p\right)$$

alors que la négation du quantificateur existentiel est le quantificateur universel

$$\neg\left(\exists x \in A :\ \neg p\right) \Leftrightarrow \left(\forall x \in A,\ p\right).$$

Exemple: La négation de la proposition

$$p : \ll \forall x \in \mathbf{Q},\ \exists n, m \in \mathbf{N} : x = \frac{m}{n} \gg$$

est

$$\neg p : \ll \exists x \in \mathbf{Q} :\ \forall n, m \in \mathbf{N},\ x = \frac{m}{n} \gg.$$

La première proposition p est vraie alors que la négation $\neg p$ est fausse.

Remarque: Quand on veut trouver la négation d'une proposition, il faut d'abord déterminer ce dont on veut la négation.

Remarque: Quand on combine le quantificateur universel et le quantificateur existentiel, il faut faire attention dans l'ordre:la propositio $\ll \forall x \in A,\ \exists y \in A,\ ... \gg$ n'a pas la même signification que la proposition $\ll \exists y \in A,\ \forall x \in A,\ ... \gg$.

Exemple: la proposition $\ll \forall x \in \mathbf{Q},\ \exists n, m \in \mathbf{N} : x = \frac{m}{n} \gg$ est vraie, alors que la proposition $\ll \exists n, m \in \mathbf{N} : \forall x \in \mathbf{Q},\ x = \frac{m}{n} \gg$ est fausse.

De même, la proposition $\ll \forall x \in \mathbf{Z},\ \exists y \in \mathbf{Z} : x < y \gg$ est vraie, alors que la proposition $\ll\ \exists y \in \mathbf{Z} : \forall x \in \mathbf{Z},\ x < y \gg$ est fausse.

III. MÉTHODES DE DÉMONSTRATION

Em mathématique, il existe plueieures méthodes de démonstration ou plusieurs modes de raisonnement. Dans cette section, nous discuterons les méthodes de démonstration les plus rencontrée en mathématique.

A. Raisonnement par table de vérité

Il est parfois raisonnable de se servir de la table de vérité d'une formule propositionnelle pour montrer sa validité. On utilise la principe suivante: Pour montrer qu'une formule est valide, on vérifie que sa table de vérité ne contient que des 1 (V); pour montrer que deux formules sont équivalentes, on montre qu'elles ont la même table de vérité.

Exemple 1: Vérifions la validité de la formule

$$((p \to q) \wedge (q \to r)) \to (p \to r)\,.$$

Écrivons la table de vérité correspondente:

$$\begin{aligned}
& \upsilon\left(((p \to q) \wedge (q \to r)) \to (p \to r)\right) \\
= \ & \upsilon\left(\neg\left((p \to q) \wedge (q \to r)\right) \vee (p \to r)\right) \\
= \ & \upsilon\left(\neg\left((p \to q) \wedge (q \to r)\right)\right) + \upsilon\left(p \to r\right) \\
= \ & \upsilon\left(\neg\left(p \to q\right) \vee \neg\left(q \to r\right)\right) + \upsilon\left(p \to r\right) \\
= \ & \upsilon\left(\neg\left(p \to q\right)\right) + \upsilon(\neg\left(q \to r\right)) + \upsilon\left(p \to r\right) \\
= \ & \upsilon\left(\neg\left(\neg p \vee q\right)\right) + \upsilon(\neg\left(\neg q \vee r\right)) + \upsilon\left(\neg p \vee r\right) \\
= \ & \upsilon\left(p \wedge \neg q\right) + \upsilon(q \wedge \neg r) + \upsilon\left(\neg p\right) + \upsilon\left(r\right) \\
= \ & \upsilon\left(p\right) \times \upsilon\left(\neg q\right) + \left(\upsilon\left(q\right) \times \upsilon\left(\neg r\right) + \upsilon\left(\neg p\right) + \upsilon\left(r\right)\right),
\end{aligned}$$

i.e.,

$$\begin{aligned}
& \upsilon\left(((p \to q) \wedge (q \to r)) \to (p \to r)\right) \\
= \ & \upsilon\left(p\right) \times \upsilon\left(\neg q\right) + \upsilon\left(q\right) \times \upsilon\left(\neg r\right) + \upsilon\left(\neg p\right) + \upsilon\left(r\right).
\end{aligned}$$

p	q	r	$((p \to q) \wedge (q \to r)) \to (p \to r)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

Ainsi, la formule de la transitivité $((p \to q) \wedge (q \to r)) \to (p \to r)$ est valide.

Exemple 2: Montrer la validité de la formule $((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \to (p \leftrightarrow r)$.

Résolution: Trouvons la valeur de vérié de cette formule:

$$
\begin{aligned}
& \upsilon\left(\left(\left(p \leftrightarrow q\right) \wedge \left(q \leftrightarrow r\right)\right) \rightarrow \left(p \leftrightarrow r\right)\right) \\
= \; & \upsilon\left(\neg\left(\left(p \leftrightarrow q\right) \wedge \left(q \leftrightarrow r\right)\right) \vee \left(p \leftrightarrow r\right)\right) \\
= \; & \upsilon\left(\neg\left(\left(p \leftrightarrow q\right) \wedge \left(q \leftrightarrow r\right)\right)\right) + \upsilon\left(p \leftrightarrow r\right) \\
= \; & \upsilon\left(\left(\neg\left(p \leftrightarrow q\right) \vee \neg\left(q \leftrightarrow r\right)\right)\right) + \upsilon\left(p \leftrightarrow r\right) \\
= \; & \upsilon\left(\neg\left(p \leftrightarrow q\right)\right) + \upsilon\left(\neg\left(q \leftrightarrow r\right)\right) + \upsilon\left(p \leftrightarrow r\right) \\
= \; & \upsilon\left(\neg\left(p \rightarrow q \wedge q \rightarrow p\right)\right) + \upsilon\left(\neg\left(q \rightarrow r \wedge r \rightarrow q\right)\right) + \upsilon\left(p \rightarrow r \wedge r \rightarrow p\right) \\
= \; & \upsilon\left(\neg\left(p \rightarrow q\right) \vee \neg\left(q \rightarrow p\right)\right) + \upsilon\left(\neg\left(q \rightarrow r\right) \vee \neg\left(r \rightarrow q\right)\right) + \upsilon\left(\left(\neg p \vee r\right) \wedge \left(\neg r \vee p\right)\right) \\
= \; & \upsilon\left(\neg\left(\neg p \vee q\right) \vee \neg\left(\neg q \vee p\right)\right) + \upsilon\left(\neg\left(\neg q \vee r\right) \vee \neg\left(\neg r \vee q\right)\right) + \upsilon\left(\neg p \vee r\right) \times \upsilon\left(\neg r \vee p\right) \\
= \; & \upsilon\left(\left(p \wedge \neg q\right) \vee \left(q \wedge \neg p\right)\right) + \upsilon\left(\left(q \wedge \neg r\right) \vee \left(r \wedge \neg q\right)\right) + \upsilon\left(\neg p \vee r\right) \times \upsilon\left(\neg r \vee p\right)
\end{aligned}
$$

$$
\begin{aligned}
= \; & \upsilon\left(p \wedge \neg q\right) + \upsilon\left(q \wedge \neg p\right) + \upsilon\left(q \wedge \neg r\right) + \upsilon\left(r \wedge \neg q\right) + \upsilon\left(\neg p \vee r\right) \times \upsilon\left(\neg r \vee p\right) \\
= \; & \upsilon\left(p\right) \times \upsilon\left(\neg q\right) + \upsilon\left(q\right) \times \upsilon\left(\neg p\right) + \upsilon\left(q\right) \times \upsilon\left(\neg r\right) + \upsilon\left(\left(r\right) \times \upsilon\left(\neg q\right)\right) \\
& + \left[\upsilon\left(\neg p\right) + \upsilon\left(r\right)\right] \times \left[\upsilon\left(\neg r\right) + \upsilon\left(p\right)\right] \\
= \; & \upsilon\left(p\right) \times \upsilon\left(\neg q\right) + \upsilon\left(q\right) \times \upsilon\left(\neg p\right) + \upsilon\left(q\right) \times \upsilon\left(\neg r\right) + \upsilon\left(r\right) \times \upsilon\left(\neg q\right) \\
& + \upsilon\left(\neg p\right) \upsilon\left(\neg r\right) + \upsilon\left(p\right) \upsilon\left(r\right).
\end{aligned}
$$

Ainsi,

$$
\begin{aligned}
& \upsilon\left(\left(\left(p \leftrightarrow q\right) \wedge \left(q \leftrightarrow r\right)\right) \rightarrow \left(p \leftrightarrow r\right)\right) \\
= \; & \upsilon\left(p\right) \times \upsilon\left(\neg q\right) + \upsilon\left(q\right) \times \upsilon\left(\neg p\right) + \upsilon\left(q\right) \times \upsilon\left(\neg r\right) + \upsilon\left(r\right) \times \upsilon\left(\neg q\right) \\
& + \upsilon\left(\neg p\right) \upsilon\left(\neg r\right) + \upsilon\left(p\right) \upsilon\left(r\right).
\end{aligned}
$$

Construisons la table de vérité:

p	q	r	$((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \rightarrow (p \leftrightarrow r)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	1

Exemple 3: Montrer que les formules $\neg(p \wedge q)$ et $\neg p \vee \neg q$ sont équivalentes.

Solution:

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$
1	1	0	0
1	0	1	1
0	1	1	1
0	0	1	1

Puisue les deux formules ont la même table de vérité, on conclut qu'elles sont équivalentes.

B. Raisonnement par contraposition

Définition (contraposition): On appelle **contraposée** de la proposition $p \rightarrow q$, la proposition $\neg q \rightarrow \neg p$.

Proposition: les formules $p \rightarrow q$ et $\neg q \rightarrow \neg p$ sont équivalentes.

Preuve: Démontrons cette proposition par par table de vérité:

$$\begin{aligned} \upsilon(p \rightarrow q) &= \upsilon(\neg p \vee q) = \upsilon(\neg p) + \upsilon(q), \\ \upsilon(\neg q \rightarrow \neg p) &= \upsilon(q \vee \neg p) = \upsilon(q) + \upsilon(\neg p). \end{aligned}$$

p	q	$p \to q$	$\neg q \to \neg p$
1	1	1	1
1	0	0	0
0	1	1	1
0	0	1	1

Puisque les deux formules ont la même table de vérité, on conclut qu'elles sont équivalentes.

Principe du raisonnement par contraposition: Montrer la validité d'une formule par contraposition c'est montrer la validité de la contraposée de ladite formule.

Ainsi, pour montrer la validité d'une formule, il suffit de montrer la validité de sa contraposée.

Exemple: Soit $n \in \mathbf{N}$ et soient p et q deux propositions définies par

$$p \ : \ n^2 \text{ est impair}$$

$$q \ : \ n \text{ est impair.}$$

Montrer que $p \to q$.

Résolution: Montrons cette implication par contraposition. Écrivons d'abord la négation de chacune des deux propositions:

$$\neg p \ : \ n^2 \text{ est pair}$$

$$\neg q \ : \ n \text{ est pair.}$$

Montrons que $\neg q \to \neg p$: Ici, n est pair est l'hypothèse, alors que n^2 est pair est la conclusion. Puisque n est pair, il s'écrit $n = 2m$, m étant un entier. Alors $n^2 = (2m)^2 = 4m^2 = 2\left(2m^2\right)$. Puisque $2m^2 \in \mathbf{N}$ et n^2 est de la forme $n^2 = 2\left(2m^2\right)$, on conclut que n^2 est pair. Nous avons ainsi montré que $\neg q \to \neg p$. On conclut alors que $p \to q$.

C. Démonstration par l'absurde

Le principe de la démonstration par l'absurde est la suivante: Pour démontrer la propriété p, on suppose $\neg p$ (qui ici est appelé hypothèse du raisonnement par l'absurde) et on en déduit une contradiction, i.e., une proposition q qui est à la fois vraie et fausse. On conclut alors que p est vraie.

Exemple: Montrer par l'absurde la validité de la formule $(\neg p \rightarrow (q \wedge \neg q)) \rightarrow p$.

Solution: Supposons le contraire, i.e., supposons que $((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p)$ est faux. Mais alor $\neg ((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p)$ est vraie, ce qui revient à dire que sa valeur de vérité est 1.

$$\begin{aligned}
\neg ((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p) &= \neg (\neg (\neg p \rightarrow (q \wedge \neg q)) \vee p) \\
&= \neg (\neg (\neg\neg p \vee (q \wedge \neg q)) \vee p) \\
&= \neg (\neg (p \vee (q \wedge \neg q)) \vee p) \\
&= (\neg\neg (p \vee (q \wedge \neg q)) \wedge \neg p) \\
&= (p \vee (q \wedge \neg q)) \wedge \neg p
\end{aligned}$$

Mais alors

$$\begin{aligned}
\upsilon (\neg ((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p)) &= \upsilon ((p \vee (q \wedge \neg q)) \wedge \neg p) \\
&= \upsilon (p \vee (q \wedge \neg q)) \times \upsilon (\neg p) \\
&= [(\upsilon (p) + \upsilon (q \wedge \neg q))] \times \upsilon (\neg p) \\
&= [\upsilon (p) + \upsilon (q) \times \upsilon (\neg q)] \times \upsilon (\neg p) \\
&= \upsilon (p) \times \upsilon (\neg p) + \upsilon (q) \times \upsilon (\neg q) \times \upsilon (\neg p) \\
&= 0 + 0 = 0
\end{aligned}$$

Il faut noter que $\upsilon (p) \times \upsilon (\neg p) = 0$ et $\upsilon (q) \times \upsilon (\neg q) = 0$. $\upsilon (\neg ((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p)) = 0$ contredit l'hypothèse selon laquelle $\neg ((\neg p \rightarrow (q \wedge \neg q)) \rightarrow p)$ est vraie.

D. Raisonnement par récurrence

Soit $A = \{n \in \mathbf{N} : n \geq N, \text{ où } N \in \mathbf{N}\}$ un univers du discours et soit $f(n)$ une fonction propositionnelle sur A. Pour démontrer que $f(n)$ est une proposition vraie $\forall n \geq N$, il suffit de montrer que

(i) $f(N)$ est vraie (hypothèse de réccurence)

(ii) Si $f(n)$ est vraie au rang n $(\geq N)$, alors elle sera vraie au rang $n+1$, i.e., que $f(n+1)$ sera vraie.

Une telle démonstration est appelée démonstration par récurrence.

Exemple: Montrer que le produit de deux entiers naturels consécutifs est un entier pair.

Solution: Deux entiers naturels consécutifs sont de la forme n et $n+1$ ou bien $n-1$ et n. L'exemple consiste à montrer que $\forall n \in \mathbf{N}$, $n\,(n+1)$ est pair, i.e., est de la forme $2k$, k étant un entier naturel. Ici, l'univers du discours est l'ensemble $\mathbf{N}$ des entiers naturels et la fonction propositionnelle $f(n)$ est «$n\,(n+1)$ est pair».

1) La proposition $f(1)$:«$1\,(1+1)$ est pair» est vraie, car $1\,(1+1) = 2 = 2 \times 1$ est pair.

2) Supposons la proposition $f(n)$ vraie et montrons que la proposition $f(n+1)$ est vraie. Nous savons alors que $f(n)$: «$n\,(n+1)$ est pair» est vraie et nous voulons montrer que $f(n+1) : ([n+1]\,([n+1]+1)$ est vraie. Éffectuons le calcul

$$\begin{aligned}[n+1]\,([n+1]+1) &= [n+1]\,(n+2)\\ &= n\,(n+1) + 2\,(n+1)\,.\end{aligned}$$

D'après l'hypothèse de récurrence, $n\,(n+1)$ est pair, i.e., $\exists k \in \mathbf{N} : n(n+1) = 2k$. Mais alors

$$\begin{aligned}[n+1]\,([n+1]+1) &= n\,(n+1) + 2\,(n+1)\\ &= 2k + 2\,(n+1) = 2\,[k+n+1] = 2m,\end{aligned}$$

où $m = k + n + 1$. Ainsi, $[n+1]\,([n+1]+1) = 2m$, ce qui revient à dire que $[n+1]\,([n+1]+1)$ est pair, i.e., que $f(n+1)$ est vraie. On conclut alors que le produit de deux entiers naturels consécutifs est pair.

E. Preuve par contre-exemple

Prouver une propriété $f(x)$ par contre-exemple consiste à contredire cette propriété. Contredire une proposition c'est trouver une valeur de la variable x pour laquelle elle est fausse.

Remarque: La preuve par contre-exemple est utilisée seulement pour montrer que une proposition est fausse. Il n'existe pas de preuve par exemple. Autrement, il ne faut jamais utiliser un exemple pour montrer qu'une proposition est vraie.

Exemple: La proposition « **tout nombre premier est impair**» est fausse. Pour montrer que cette proposition est fausse, il suffit de trouver l'exemple d'un nombre premier qui n'est pas impair. 2 est un nombre premier et 2 n'est pas impair.

CHAPITRE 2

THÉORIE DES ENSEMBLES

Dans le premier chapitre, nous avons défini ce que c'est qu'un ensemble. Passons maintenant aux différentes notions liées à la notion d'ensemble.

IV. ENSEMBLE VIDE, CARDINAL D'UN ENSEMBLE, ET INCLUSION DES ENSEMBLES

Définition (Ensemble vide): Un ensemble est dit vide s"il ne contient aucun élément. L'ensemble vide est noté $\varnothing$ ou $\{\}$.

Exemple: L'ensemble $\{n \in \mathbf{N} : n < 0\}$ est un ensemble vide.

Définition (Cardinal d'un ensemble): Un ensemble E est dit fini s'il contient un nombre fini d'éléments. Le nombre d'éléments d'un ensemble E est appelé **cardinal de E** et est noté card(E).

Exemple: Le cardinal de $E = \{n \in \mathbf{N} : n \leq 0\}$ est $card(E) = 1$; $card(\varnothing) = 0$.

Définition (Inclusion $\subset$): Soient A et B deux ensembles. On dit que A est inclu dans B (ou bien, que A est une partie de B, ou bien, que A est un sous-ensemble de B, ou bien, que A est contenu dans B) et on écrit $A \subset B$ si tous les éléments de A sont dans B, i.e., $\forall x \in A$, $x \in B$.

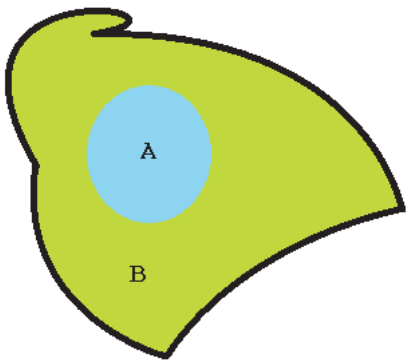


Figure 1: Inclusion de A dans B.

Exemple 1: Pour tout ensemble A, on a $\varnothing \subset A$ et $A \subset A$.

Exemple 2: Soient $A = \{x \in \mathbf{N} : x \leq 5\}$ et $B = \{x \in \mathbf{Z} : |x| \leq 5\}$. Montrer que $A \subset B$.

Solution: En écrivant explicitement $A = \{x \in \mathbf{N} : x \leq 5\} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ et $B = \{x \in \mathbf{Z} : |x| \leq 5\} = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\}$, on voit que tous les éléments de A sont dans B, ce qui signifie que $A \subset B$.

Si on a un certain nombre d'ensembles A_1, A_2, ..., A_n tels que $A_j \subset A_{j+1}$ (i.e., $A_1 \subset A_2$, $A_2 \subset A_3$, ..., $A_{n-1} \subset A_n$) alors écrit la chaîne d'inclusion

$$A_1 \subset A_2 \subset ... \subset A_n.$$

Exemple: Pour les ensembles $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, et $\mathbf{C}$, on a la chaine d'inclusion

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$$

Définition (égalité des deux ensembles): On dira que deux ensembles A et B sont égaux et on écrira $A = B$ si $(A \subset B) \wedge (B \subset A)$:

$$A = B \Leftrightarrow (x \in A \leftrightarrow x \in B)$$

Exemple: Pour les ensembles $A = \{x \in \mathbf{N} : x \leq 5\}$ et $B = \{x \in \mathbf{Z} : x \geq 0 \wedge |x| \leq 5\}$, on a $A = B$.

Remarque: L'écriture $A \subseteq B$ se lit que A est inclu ou égale à B. Quand l'inclusion est stricte, i.e., $A \subset B \wedge \exists x \in B : x \notin A$, on utilise la notation $A \subset B$.

Définition (Ensemble des parties): On appelle **Ensemble des parties** d'un ensemble A,

l'ensemble $\mathcal{P}(A)$ des tous les sous-ensembles de A.

Cette définition signifie que tout élément de $\mathcal{P}(A)$ est un sous-ensemble de A.

Exemple: Trouver les ensemble des parties $\mathcal{P}(A)$ et $\mathcal{P}(B)$ de $A = \{1\}$ et $B = \{2,\ 3,\ 5\}$.

Solution:

$$\mathcal{P}(A) = \{\varnothing,\ \{1\}\}$$

et

$$\mathcal{P}(B) = \{\varnothing,\ \{2\},\ \{3\},\ \{5\},\ \{2,\ 3\},\ \{2,\ 5\},\ \{3,\ 5\},\ \{2,\ 3,\ 5\}\}$$

. On voit que $card(\mathcal{P}(A)) = 2 = 2^1$ et $card(\mathcal{P}(B)) = 8 = 2^3$. En général, si $card(E) = N$, alors $card(\mathcal{P}(E)) = 2^N$.

V. OPÉRATIONS SUR LES ENSEMBLES

Définition (Intersection $\cap$): On appelle intersection des deux ensembles A et B, l'ensemble noté $A \cap B$ formé des éléments qui appartient à la fois à A et à B :

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}.$$

Remarque: L'intersection des ensembles est une opération commutative:

$$A \cap B = B \cap A.$$

Définition (Ensembles disjoints $\cap$): Deux ensembles A et B sont dits disjoints si leur inersection est vide ($A \cap B = \varnothing$).

Définition (Réunion $\cup$): On appelle réunion de deux ensembles A et B, l'ensemble noté $A \cup B$ formé des éléments qui appartient soit à A, soit à B :

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}.$$

Remarque: La réunion des ensembles est une opération commutative:

$$A \cup B = B \cup A.$$

Remarque: Il est évident que l'intersection $A \cap B$ est inclue à la fois dans A et dans B et chacun des ensembles A et B est inclu dans la réunion $A \cup B$, i.e.,

$$(A \cap B \subset A \subset A \cup B) \wedge (A \cap B \subset B \subset A \cup B).$$

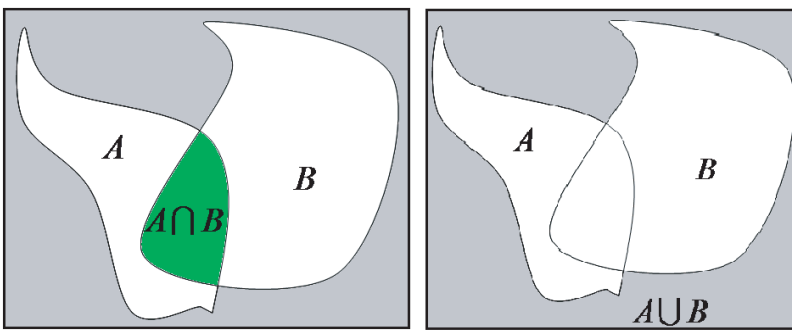


Figure 2: Intersection $A \cap B$ des ensembles A et B (gauche) et réunion $A \cup B$ des ensembles A et B (droite).

Exemple 1: Si $A \subset B$, alors $A \cap B = A$ et $A \cup B = B$.

Exemple 2: Trouver l'intersection et la réunion des ensembles $A = \{x \in \mathbf{Z} : |x| \leq 5\}$ et $B = \{x \in \mathbf{N} : (x \leq 10) \wedge (x + 3 \text{ et pair})\}$.

Solution: Pour trouver l'intersection et la réunion des ensembles A et B, il est utile d'écrire explicitement chacun de ces deux ensembles:

$$\begin{aligned} A &= \{x \in \mathbf{Z} : |x| \leq 5\} = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\} \\ B &= \{x \in \mathbf{N} : (x \leq 10) \wedge (x + 3 \text{ et pair})\} = \{1,\ 3,\ 5,\ 7,\ 9\}\,. \end{aligned}$$

On peut alors facilement écrire $A \cap B$ et $A \cup B$:

$$\begin{aligned} A \cap B &= \{x : (x \in A) \wedge (x \in B)\} = \{1,\ 3,\ 5\} \\ A \cup B &= \{x : (x \in A) \vee (x \in B)\} \\ &= \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 7,\ 9\}\,. \end{aligned}$$

Théorème: Soient A, B, et C trois ensembles. Alors

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

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

Preuve: Pour prouver chacune des deux égalités, nous utilisons l'équivalence mathématique.

(i) Montrons que $x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$:

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee (x \in (B \cap C)) \\ &\Leftrightarrow (x \in A) \vee [(x \in B) \wedge (x \in C)] \\ &\Leftrightarrow [(x \in A) \vee (x \in B)] \wedge [(x \in A) \vee (x \in C)] \\ &\Leftrightarrow [x \in A \cup B] \wedge [x \in A \cup C] \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C)\,. \end{aligned}$$

(ii) Montrons que $x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$:

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee [x \in (B \cap C)] \\ &\Leftrightarrow (x \in A) \vee [(x \in B) \wedge (x \in C)] \\ &\Leftrightarrow [(x \in A) \vee (x \in B)] \wedge [(x \in A) \vee (x \in C)] \\ &\Leftrightarrow [x \in A \cup B] \wedge [x \in A \cup C] \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C)\,. \end{aligned}$$

Définition (Complémentaire): Soient B un ensemble donné et A un sous-ensemble de B. On appelle complémentaire de A dans B, l'ensemble noté $C_A(B)$ formé des des éléments de B qui n'appartient pas à A, i.e.,

$$C_A(B) = \{x : (x \in B) \wedge (x \notin A)\}.$$

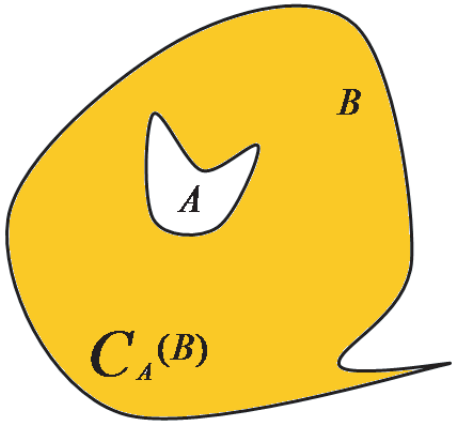


Figure 3: Complémentaire $C_A(B)$ de A dans B.

Exemple: Trouver le complémentaire de A dans B si $A = \{x \in \mathbf{N} : (x \leq 6) \wedge (x + 2 \text{ et impair})\}$ et $B = \{x \in \mathbf{Z} : |x| \leq 5\}$.

Solution: Pour résoudre cet exemple, nous devons d'abord écrire explicitement chacun des ensembles A et B, vérifier que $A \subset B$ avant de trouver le complémentaire de A dans B.

$$\begin{aligned} A &= \{x \in \mathbf{N} : (x \leq 6) \wedge (x + 2 \text{ et impair})\} = \{1,\ 3,\ 5\}, \\ B &= \{x \in \mathbf{Z} : |x| \leq 5\} = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\} \end{aligned}$$

On constate bien que $A \subset B$. Alors

$$C_A(B) = \{x : (x \in B) \wedge (x \notin A)\} = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 2,\ 4\}.$$

Définition (Différence): Soit donné un ensemble E et soient A et B deux sous-ensembles de E. On appelle différence des deux parties B et A, l'ensemble noté $B \backslash A$ formé des éléments de A qui n'appartient pas à B, i.e.,

$$B \backslash A = \{x \in E : (x \in B) \wedge (x \notin A)\}.$$

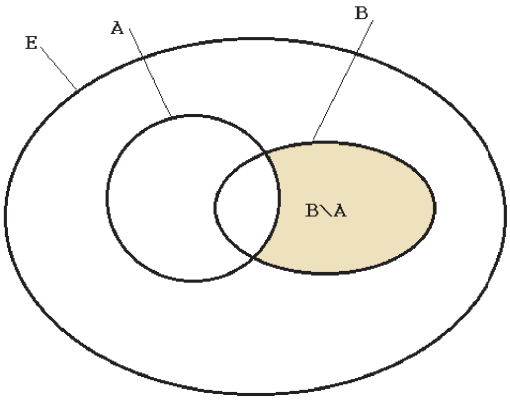


Figure 4: Différence $B\backslash A$ des deux parties B et A de E.

On appelle différence symétrique des ensemble A et B, l'ensemble noté $A\Delta B$ défini par

$$A\Delta B = (A\backslash B) \cup (B\backslash A)\,.$$

Exemple: Trouver les différences $A\backslash B$ et $B\backslash A$ et la différence symétrique $A\Delta B$si $A = \{x \in \mathbf{Z} : |x| \leq 5\}$ et $B = \{x \in \mathbf{Z} : (x+2 \geq -1) \wedge (x-3 \leq 5)\}$.

Solution: Pour cet exemple, $E = \mathbf{Z}$. Écrivons A et B de façon explicite:

$$\begin{aligned} A &= \{x \in \mathbf{Z} : |x| \leq 5\} = \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\} \\ B &= \{x \in \mathbf{Z} : (x+2 \geq -1) \wedge (x-3 \leq 5)\} = \{x \in \mathbf{Z} : -3 \leq x \leq 8\} \\ &= \{-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}\,. \end{aligned}$$

Alors

$$\begin{aligned} A\backslash B &= \{x \in \mathbf{Z} : (x \in A) \wedge (x \notin B)\} = \{-5,\ -4\}\,, \\ B\backslash A &= \{x \in \mathbf{Z} : (x \in B) \wedge (x \notin A)\} = \{6,\ 7,\ 8\}\,. \\ A\Delta B &= (A\backslash B) \cup (B\backslash A) = \{-5,\ -4,\ 6,\ 7,\ 8\}\,. \end{aligned}$$

Cet exemple montre bien que $A\backslash B \neq B\backslash A$. On remarque aussi que

$$\begin{aligned} A \cap B &= \{-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5\}\,, \\ A \cup B &= \{-5,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\} \\ (A \cup B) \setminus (A \cap B) &= \{-5,\ -4,\ 6,\ 7,\ 8\} = A\Delta B. \end{aligned}$$

L'égalité $A\Delta B = (A \cup B) \setminus (A \cap B)$ a toujours lieu.

Nous avons les propriétés suivantes:

Proposition: Soit donné un ensemble E et soient A, B et C trois sous-ensembles de E. Alors

(i) $A \cap C_A(E) = \varnothing$,

(ii) $A \cup C_A(E) = E$,

(iii) $C_{\varnothing}(E) = E$,

(iv) $C_{C_A(E)}(E) = A$,

(v) Si $A \subset B$, alors $C_B(E) \subset C_A(E)$,

(vi) $C_{A\cap B}(E) = C_A(E) \cup C_B(E)$,

(vii) $C_{A\cup B}(E) = C_A(E) \cap C_B(E)$,

(viii) $C_{B\setminus A}(E) = B \cap C_A(E)$,

(ix) $C_E(E) = \varnothing$,

(x) $A\Delta B = (A \cup B) \setminus (A \cap B)$

(xi) Distributivité: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ et $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Ces propriétés se démontrent facilement. Montrons par exemple les popriétés (vi) et (vii).

(vi) Montrons que $C_{A\cap B}(E) = C_A(E) \cup C_B(E)$:

$$\begin{aligned} C_{A\cap B}(E) &= \{x \in E : x \notin A \cap B\} \\ &= \{x \in E : (x \notin A) \vee (x \notin B)\} \\ &= \{x \in E : x \notin A\} \cup \{x \in E : x \notin B\} \\ &= C_A(E) \cup C_B(E). \end{aligned}$$

(vii) Montrons que $C_{A\cup B}(E) = C_A(E) \cap C_B(E)$:

$$\begin{aligned} C_{A\cup B}(E) &= \{x \in E : x \notin (A \cup B)\} \\ &= \{x \in E : (x \notin A) \wedge (x \notin B)\} \\ &= \{x \in E : x \notin A\} \cap \{x \in E : x \notin B\} \\ &= C_A(E) \cap C_B(E). \end{aligned}$$

Définition (Produit cartésien): On appelle produit cartésien de deux ensembles A et B, l'ensemble noté $A \times B$ formé des couples (x, y) tel que $x \in A$ et $y \in B$, i.e.,

$$A \times B = \{(x, y) : (x \in A) \wedge (y \in B)\}.$$

Exemple: $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R} = \{(x, y) : (x \in \mathbf{R}) \wedge (y \in \mathbf{R})\}$.

Définition (Produit cartésien de plusieurs ensembles): On appelle produit cartésien des n ensembles E_1, E_2, ..., E_n, l'ensemble noté $E_1 \times E_2 \times \cdots \times E_n$ des $n-$uplets $(x_1, x_2, ..., x_n)$ tel que $x_j \in E_j$:

$$E_1 \times E_2 \times \cdots \times E_n = \{(x_1, x_2, ..., x_n) : x_1 \in E_1,\ x_2 \in E_2,\ ...,\ x_n \in E_n\}.$$

Exemple: $\mathbf{R}^n = \underbrace{\mathbf{R} \times \mathbf{R} \times \cdots \times \mathbf{R}}_{\text{n fois}}$; $\mathbf{Z}^3 = \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} = \{(x, y, z) : x \in \mathbf{Z},\ y \in \mathbf{Z},\ \text{et}\ z \in \mathbf{Z}\}$.

Remarque: Il faut bien noter que dans l'écriture $(x, y) \in A \times B$, le premier élément x du couple appartient au premier ensemble A du produit alors que le deuxième élément y du couple appartient au deuxième ensemble B du produit.

Définition (égalité dans le produit cartésien): On dira que de éléments $(a_1, a_2, ..., a_n)$ et $(b_1, b_2, ..., b_n)$ du produit cartésien $E_1 \times E_2 \times \cdots \times E_n$ sont égaux et on écrira $(a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n)$ si le éléments occupant la même position sont égaux entre eux:

$$(a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n) \Leftrightarrow a_j = b_j,\ \text{pour tous les}\ j = 1,\ 2,\ ...,\ n.$$

Exemple: $(1, 2) = \left(\frac{3}{3}, \frac{12}{6}\right)$, $(1, 3, 2, 3) \neq (1, 3, 2, 4)$, car les éléments occupant la dernière position ne sont pas égaux $(3 \neq 4)$.

CHAPITRE 3

APPLICATIONS (FONCTIONS)

Dans ce chapitre nous introduisons la notion d'application. Nous débutons par des définitions.

VI. DÉFINITIONS

Définition (Application ou fonction): Soient donnés deux ensembles A et B. On appelle application (fonction) f de A dans B, toute loi qui associe tout élément x de A à un unique élément $y = f(x)$ de B, i.e.,

$$\forall x \in A, \exists! y \in B : y = f(x).$$

Notation: On notera

$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

l'application de A dans B qui à $x \in A$ associe $f(x) \in B$.

Exemple 1: Soient $A = \{1,\ 2,\ 3\}$ et $B = \{1,\ 2,\ 4,\ 5,\ 6,\ 7\ \}$ soit f la loi qui associe tout élément x de A son double dans B, i.e.,

$$\begin{aligned} f : A &\to B \\ x &\mapsto 2x \end{aligned}$$

Alors

$$f(1) = 2,\ \ f(2) = 4,\ \ f(3) = 6.$$

Exemple 2: Soient $A = \mathbf{N}$ et $B = \mathbf{Z}$, on définit l'application (fonction)

$$\begin{aligned} f : \mathbf{N} &\to \mathbf{Z} \\ x &\mapsto 2x - x^2. \end{aligned}$$

Définition(Image et antécédent): Si $f : A \to B$ est une application de A dans B, alors A sera appelé **ensemble de départ** de l'application f et B, l'ensemble d'arrivée de f. Dans l'écriture $y = f(x)$, $f(x) \in B$ est appelée image de x par la fonction (application) f alors que $x \in A$ est appelé antécédent de $y \in B$ si $y = f(x)$.

Exemple: Dans l'exemple

$$f : \mathbf{N} \to \mathbf{Z}$$
$$x \mapsto 2x - x^2,$$

on a $f(0) = 0$, $f(1) = 1$, $f(2) = 0$, $f(4) = -8$, ... Puisque $f(0) = 0$ et $f(2) = 0$, $0 \in Z$ possède deux antécédents, $0 \in \mathbf{N}$ et $2 \in \mathbf{N}$. Ici, l'image de $0 \in \mathbf{N}$ est $0 \in \mathbf{Z}$, de même, l'image de $2 \in \mathbf{N}$ est $0 \in \mathbf{Z}$. Cet exemple montre qu'un élément de l'ensemble d'arrivée d'une application f peut avoir plusieurs antécédents. Notons cependent que l'image d'un élément de l'ensemble de départ, si elle existe, est unique. Autrement dit, un élément de l'ensemble de départ ne peut avoir plus d'une image.

Définition (Graphe de la fonction): On appelle graphe d'une application $f : A \to B$, l'ensemble

$$\mathcal{G}_f = \{(x, f(x)) : x \in A \text{ et } f(x) \in B\}.$$

Il faut remarquer que le graphe $\mathcal{G}_f$ de la fonction $f : A \to B$ est un sous-ensemble du produit cartésien $A \times B$.

Exemple: Soient donnés $A = \{1,\ 2,\ 3\}$ et $B = \{1,\ 2,\ 4,\ 5,\ 6,\ 7\ \}$. Trouver le graphe de l'application

$$f : A \to B$$
$$x \mapsto 2x.$$

Solution: Pour cet exemple, nous avons $f(1) = 2$, $f(2) = 4$, et $f(3) = 6$, de sorte que

$$\mathcal{G}_f = \{(1,2),\ (2,4),\ (3,6)\}.$$

Définition (Égalité de fonctions): Soient données deux fonctions $f : A \to B$ et $g : A' \to B'$. On dira que les deux fonctions f et g sont égales et on écrira $f = g$ si les conditions suivantes sont simultanément satisfaites:

(1) $A = A'$

(2) $B = B'$

(3) $\forall x \in A = A'$, $f(x) = g(x)$.

Définition (Application identité): Si A est un ensemble non vide, alors on appelle application identité, l'application

$$id_A : A \to A$$
$$x \mapsto x.$$

Ainsi, $id_A(x) = x$, $\forall x \in A$.

VII. RESTRICTION ET PROLONGEMENT

Définition (Restriction): Soit $f : E \to F$ une application de E dans F et soit $A \subset E$. On appelle restriction de l'application f à A, l'application notée $f|_A$ définie par

$$\begin{aligned} f|_A : \quad & A \to F \\ x \mapsto & f|_A(x) = f(x), \ \forall x \in A. \end{aligned}$$

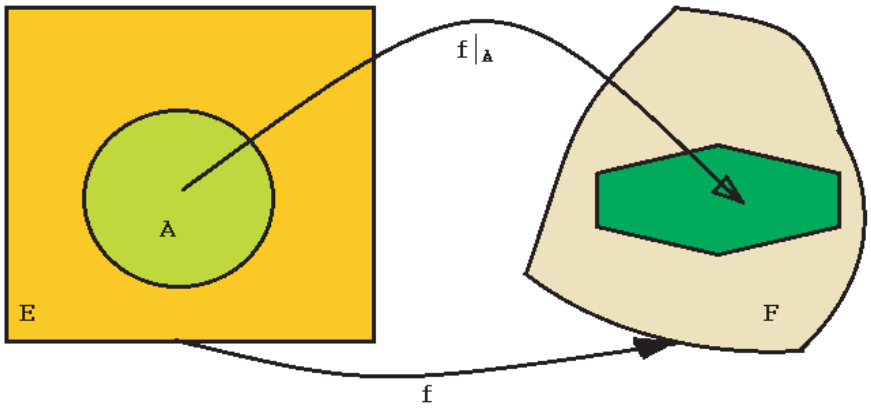


Figure 5: Restriction d'une application f à A.

Définition (Prolongement): Soit $g : A \to E$ une application de A dans F et soit E un ensemble contenant A. On appelle prolongement de g à E, toute application $f : E \to F$ telle que la restriction sur A coincide avec g, i.e., $f|_A = g$.

Cette définition implique que le prolongement d'une fonction sur un ensemble n'est pas unique. Autrement dire, une fonction peut avoir plusieurs prolongement.

Exemple: Soit

$$\begin{aligned} g : \mathbf{R}^* = \mathbf{R}\backslash\{\mathbf{0}\} & \to \mathbf{R} \\ x & \mapsto \sin \tfrac{1}{x}. \end{aligned}$$

Alors, chacune des fonctions suivantes est un prolongement de g sur $\mathbf{R}$:

$$f_1 : \mathbf{R} \to \mathbf{R}$$
$$x \mapsto \begin{cases} \frac{\sin x}{x}, \text{ si } x \neq 0, \\ 0, \text{ si } x = 0 \end{cases}$$

$$f_2 : \mathbf{R} \to \mathbf{R}$$
$$x \mapsto \begin{cases} \frac{\sin x}{x}, \text{ si } x \neq 0, \\ 1, \text{ si } x = 0. \end{cases}$$

En effet, $\mathbf{R}^* \subset \mathbf{R}$, $f_1|_{\mathbf{R}^*} = g$ et $f_2|_{\mathbf{R}^*} = g$.

VIII. COMPOSITION DES APPLICATIONS (FONCTIONS)

Définition (composition des applications): $f : E \to F$ et $g : F \to G$ deux applications. La composée de f et g est l'application de E dans G définie par:

$$\begin{aligned} g \circ f \quad &: \quad E \to G \\ x \quad &\mapsto \quad (g \circ f)(x) = g(f(x)). \end{aligned}$$

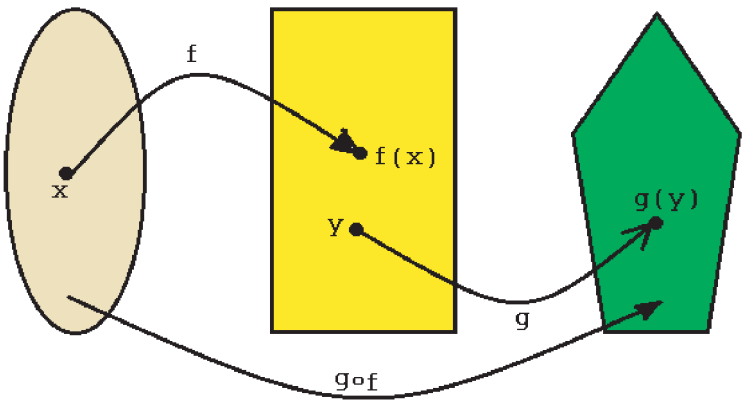


Figure 6: Composition de deux fonctions f et g

Exemple: Soient $f : \underset{x \mapsto f(x)}{\mathbf{R} \to \mathbf{R}}$ telle que $f(x) = \frac{\pi}{1+x^2}$ et $g : \underset{y \mapsto g(y)}{\mathbf{R} \to \mathbf{R}}$ telle que $g(y) = \sin y$. Trouver L'expression analytique de $(g \circ f)(x)$ et évaluer $(g \circ f)(0)$ et $(g \circ f)(1)$

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{\pi}{1+x^2}\right) = \sin\frac{\pi}{1+x^2},$$

de sorte que $g \circ f : \underset{x \mapsto (g \circ f)(x)}{\mathbf{R} \to \mathbf{R}}$ telle que $(g \circ f)(x) = \sin\frac{\pi}{1+x^2}$. Par conséquent, $(g \circ f)(0) = \sin\frac{\pi}{1+0} = 0$ et $(g \circ f)(1) = \sin\frac{\pi}{1+1} = 1$.

IX. IMAGE DIRECTE ET RÉCIPROQUE

Définition (Image directe): Soit $f : E \to F$ une application de E dans F et soit $A \subset E$ (un sous-ensemble de E). On appelle image directe de A par f , l'ensemble noté $f(A)$ défini par

$$f(A) = \{f(x) : x \in A\}.$$

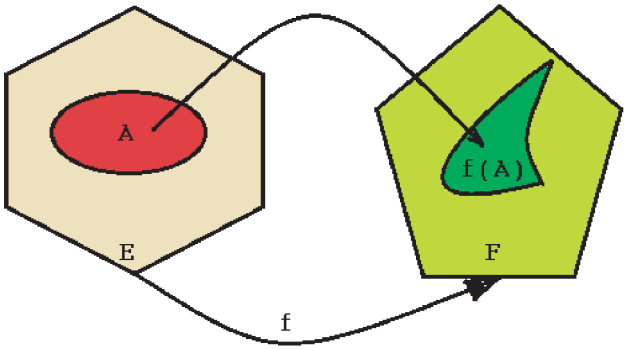


Figure 7: Image directe de A par f

Exemple: Pour l'application (fonction) $f : \mathbf{R} \to \mathbf{R}$ telle que $f(x) = x^3$, trouver l'image directe de chacun des ensembles $A_1 = \mathbf{R}$; $A_2 = [0, \ +\infty]$, $A_3 =]2, 3]$.

Résolution: Nous avons $f(\mathbf{R}) = \mathbf{R}$; $f([0, \ +\infty]) = [0, \ +\infty]$, $f(]2, 3]) =]8, 27]$.

Définition (Image réciproque): Soit $f : E \to F$ une application de E dans F et soit $B \subset F$ (un sous-ensemble de F). On appelle image réciproque de B sur F, l'ensemble noté $f^{-1}(B)$ défini par

$$f^{-1}(B) = \{x \in E : f(x) \in B\}.$$

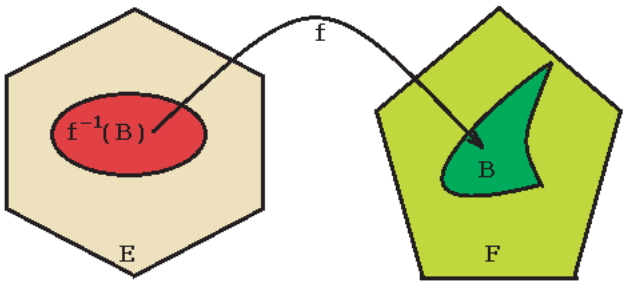


Figure 8: Image réciproque de B sur F.

Il est évident que l'image directe de A par f est un sous-ensemble de F alors que l'image réciproque de B sur F est un sous-ensemble de E.

Exemple: Pour la l'application $f : R \to R$ telle que $f(x) = -x^2$, trouver l'image réciproque de chacun des ensembles $B_1 = \{-4\}$ et $B_2 = \{1\}$.

Résolution:

$$f^{-1}(B_1) = f^{-1}(\{-4\}) = \{x \in \mathbf{R} : f(x) = -4\}.$$

$$\begin{aligned} f(x) &= -4 \Leftrightarrow -x^2 = -4 \\ &\Leftrightarrow x^2 = 4 \Leftrightarrow x = \pm 2, \end{aligned}$$

d'où $f^{-1}(B_1) = \{-2,\ 2\}$.

$$f^{-1}(B_2) = f^{-1}(\{1\}) = \{x \in \mathbf{R} : f(x) = 1\}$$

$$f(x) = 1 \Leftrightarrow -x^2 = 1 \Leftrightarrow x^2 = -1,$$

ce qui est impossible dans $\mathbf{R}$. Par conséquent, $f^{-1}(B_2) = f^{-1}(\{1\}) = \varnothing$.

Remarque: Il ne faut pas confondre l'image réciproque d'un ensemble B sur un ensemble F avec l'application réciproque.

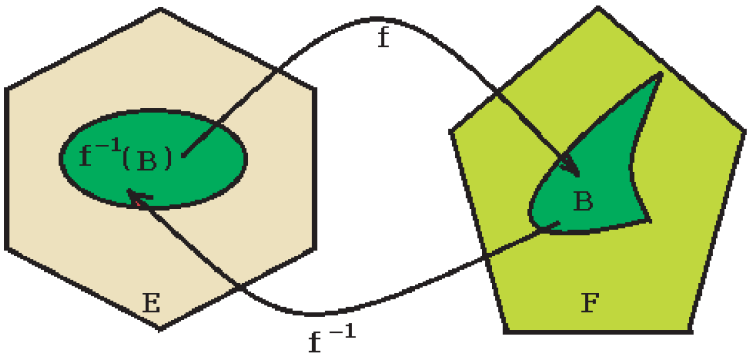


Figure 9: Il faut faire la différence entre l'image réciproque $f^{-1}(B)$ et l'application réciproque (inverse) $f^{-1} : F \to E$ de F dans E, définie seulement sous certaines conditions.

X. INJECTION, SURJECTION ET BIJECTION

Soit $f : E \to F$ une application de E dans F.

Comme nous avons vu plus haut, la définition de l'application (fonction) $f : E \to F$ nous renseigne que $\forall x \in E, \exists! y \in F : y = f(x)$. Elle ne nous renseigne pas sur le nombre d'antécédents qu'un élément y de F peut avoir. Non plus, elle ne nous renseigne pas si chaque élément de F doit avoir ou pas un antécédent dans E.

Définition (Injection): On dira que l'application f est dite injective si tout élément de F admet au plus un antécédent, i.e., si tout élément de F est l'image d'au plus un élément de E.

Remarque: Cette définition nous laisse comprendre que si $f : E \to F$ est une injection, alors il peut arriver que certains éléments de F ne soient images d'aucun élément de E. Elle nous renseigne qu'un élément de F ne peut être image de plus d'un élément de E.

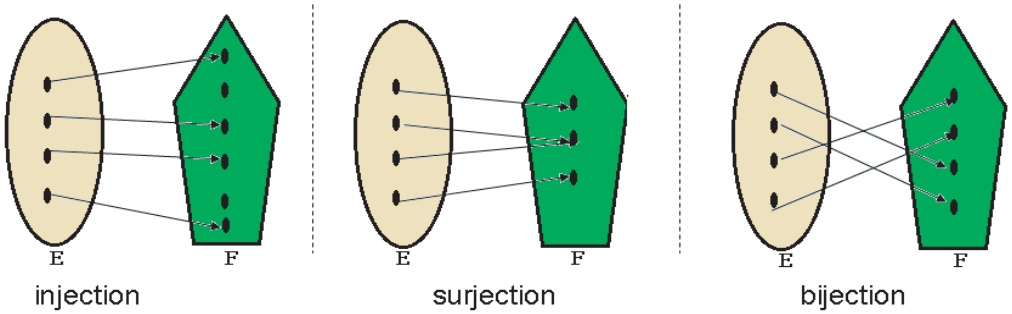


Figure 10: Représentation des fonctions injectives, surjectives et bijectives.

Définition (Surjection): L'application f est dite surjective si tout élément $y \in F$ admet au moins un antécédent. Autrement dit, l'application f est dite surjective si tout élément de F est image d'au moins un élément de E, i.e.,

$$\forall y \in F,\ \exists x \in E : y = f(x).$$

Remarque: Cette définition nous laisse comprendre que si $f : E \to F$ est une surjection, alors un élément de E peut être image de plusieurs éléments de E, i.e., plusieurs éléments de E peuvent avoir une même image dans F.

Définition (Bijection): L'application f est dite bijective si elle est à la fois injective et surjective. Ceci revient à dire que tout élément de F est image d'un unique élément de E, i.e.,

$$\forall y \in F, \exists! x \in E : y = f(x).$$

Autrement dit, $f : E \to F$ est une bijection si tout élément y de F est image d'un unique élément x dans E.

Définition (Réciproque ou application inverse): Soit $f : E \to F$ une bijection de E vers F. On appelle application réciproque ou application inverse de f, l'application f^{-1} définie par

$$F \to E$$
$$y \mapsto f^{-1}(y) = x.$$

Ainsi, si $y = f(x)$, alors $f^{-1}(y) = f^{-1}(f(x)) = (f^{-1} \circ f)(x) = x$. Ceci revient à dire que $f^{-1} \circ f = Id_E$.

Remarque: Soit $f : E \to F$ une bijection. Pour trouver l'application réciproque f^{-1}, on essaye de résoudre l'équation

$$f(x) = y$$

par rapport à x. Autrement dit, on essaye, si possible, d'exprimer x en fonction de y. Si on parvient à le faire, i.e., écrire x sous la forme $x = g(y)$, alors on pose

$$f^{-1}(y) = g(y).$$

Exemple 1: Montrer que l'application $f : \mathbf{R} \to \mathbf{R}$ définie par $f(x) = x + 2$ est bijective et trouver l'application réciproque.

Résolution: Montrons que f est une bijection, i.e., est surjective et injective.

1) *Surjection:* Soient $x_1 \in \mathbf{R}$ et $x_2 \in \mathbf{R}$, $x_1 \neq x_2$. Montrons que $f(x_1) \neq f(x_2)$. Supposons le contraire, i.e., $f(x_1) = f(x_2)$. Alors

$$\begin{aligned} f(x_1) &= f(x_2) \Leftrightarrow x_1 + 2 = x_2 + 2 \\ &\Leftrightarrow x_1 + 2 - (x_2 + 2) = 0 \\ &\Leftrightarrow x_1 - x_2 = 0 \Leftrightarrow x_1 = x_2, \end{aligned}$$

ce qui contredit l'hypothèse suivant laquelle $x_1 \neq x_2$. Cette contradiction montre que $f(x_1) \neq f(x_2)$ et f est injective.

2) *Surjection:* Montrons que f est surjective. Soit $y \in \mathbf{R}$. Trouvons $x \in \mathbf{R}$ tel que $f(x) = y$.

$$\begin{aligned} f(x) &= y \Leftrightarrow x + 2 = y \\ &\Leftrightarrow x = y - 2. \end{aligned}$$

Ainsi, $\forall y \in \mathbf{R}$, $\exists x = y - 2 \in \mathbf{R}$ tel que $f(x = y - 2) = (y - 2) + 2 = y$. Mais alors, f est surjective.

Nous avons ainsi montrer que f est à la fois injective et surjective, ce qui revient à dire que f est bijective.

3) Trouvons f^{-1}. Pour cela, essayons de résoudre l'équation $f(x) = y$ par rapport à x :

$$\begin{aligned} f(x) &= y \Leftrightarrow x + 2 = y \\ &\Leftrightarrow x = y - 2. \end{aligned}$$

Ainsi,

$$\begin{aligned} f^{-1} : \mathbf{R} &\to \mathbf{R} \\ y &\mapsto f^{-1}(y) = y - 2. \end{aligned}$$

Exemple 2: Montrer que $f : R \to [0, +\infty[$ telle que $f(x) = x^2$ n'est pas bijective.

Preuve: L'application de cet exemple est injective, mais n'est pas surjective. Par exemple, $f(-2) = (-2)^2 = 4$ et $f(2) = 2^2 = 4$, de sorte que $4 \in [0, +\infty[$ est l'image de -2 et de 2. Autrement dit, $y = 4$ possède deux antécédents, -2 et 2, ce qui montre que f n'est pas une surjection. Par conséquent, f n'est pas une bijection.

XI. INJECTIVITÉ ET SURJECTIVITÉ DES FONCTIONS COMPOSÉES

Proposition: Soient données deux fonctions $f : E \to F$ et $g : F \to G$. Alors

(1) Si $g \circ f$ est injective, alors f est injective

(2) Si $g \circ f$ est surjective, alors g est surjective.

Preuve: (1) supposons que $g \circ f$ est injective et montrons que f est injective, i.e. que tout élément y de F est image d'au plus un élément x de E. Supposons le contraire (démonstration par l'absurde), i.e., que f n'est pas injective. Alors il existe $x_1 \in E$ et $x_2 \in E$ tels que $x_1 \neq x_2$ et $f(x_1) = f(x_2)$. Désignons par y_0 la valeur commune de $f(x_1)$ et $f(x_2)$, i.e., $y_0 = f(x_1) = f(x_2)$. Évaluons $(g \circ f)(x_1)$:

$$(g \circ f)(x_1) = g(f(x_1)) \overset{\text{car } f(x_2)=f(x_1)}{=} g(f(x_2)) = (g \circ f)(x_2).$$

On trouve alors que $(g \circ f)(x_1) = (g \circ f)(x_2)$ avec $x_1 \neq x_2$, ce qui contredit l'hypothèse selon laquelle $g \circ f$ est injective. Cette contradiction montre que f est injective.

(2) Supposons que $g \circ f$ est surjective et montrons que g est surjective. Montrer que g est surjective revient à montrer que tout élément z de G est image par g d'au moins

un élément y de F. Soit $z \in G$. Puisque $g \circ f$ est surjective, z est image d'au moins un élément de E; autrement dit, il existe au moins un $x_z \in E$ tel que $z = (g \circ f)(x_z)$. Mais alors $z = (g \circ f)(x_z) = g(f(x_z)) = g(y_z)$, où $y_z = f(x_z) \in F$. L'écriture $z = g(y_z)$ où $y_z = f(x_z) \in F$ signifie que z est l'image de $y_z \in F$. Ainsi, $\forall z \in G$, $\exists y_z \in F : z = g(y_z)$, ce qui revient à dire que g est surjective et la proposition est prouvée.

Proposition: Soient données deux fonctions $f : E \to F$ et $g : F \to G$. Alors

(1) Si f et g sont injectives, alors $g \circ f$ sera injective

(2) Si f et g sont surjectives, alors $g \circ f$ sera surjective.

Démonstration: (1) Supposons que chacune des fonctions f et g est injective et montrons que $g \circ f$ est aussi injective. Soient x_1 et x_2 deux éléments de E.

$$(g \circ f)(x_1) = (g \circ f)(x_2) \Leftrightarrow g(f(x_1)) = g(f(x_2)).$$

Puisque g est injective, l'égalité $g(f(x_1)) = g(f(x_2))$ n'est possible que si $f(x_1) = f(x_2)$. Puisque f est injective, cette dernière égalité $f(x_1) = f(x_2)$ n'est possible que si $x_1 = x_2$. Ainsi, l'égalité $(g \circ f)(x_1) = (g \circ f)(x_2)$ n'est possible que si $x_1 = x_2$, ce qui signifie que $g \circ f$ est injective.

(2) Supposons maintenant que chacune des fonctions f et g est surjective et montrons que $g \circ f$ est surjective. Autrement dit, montrons que tout élément de G est image par $g \circ f$ d'au moins un élément de E. Soit $z \in G$. Puisque g est surjective, z est image par g d'au moins un élément de G, i.e., qu'il existe au moins un $y_z \in G : z = g(y_z)$. Puisque $y_z \in G$ et f est surjective, y_z est image par f d'au moins un élément de E. Autrement dit $\exists x_{y_z} \in E : y_z = f(x_{y_z})$. On obtient ainsi que

$$z = g(y_z) \overset{\text{car } y_z = f(x_{y_z})}{=} g(f(x_{y_z})) = (g \circ f)(x_{y_z}),$$

i.e., $z = (g \circ f)(x_{y_z})$ où $x_{y_z} \in E$. Nous avons ainsi montré que $\forall z \in G, \exists x_{y_z} \in E : z = (g \circ f)(x_{y_z})$, ce qui revient à dire que tout élément de G est image par $g \circ f$ d'au moins un élément de E. Ceci signifie que $g \circ f$ est surjective.

XII. INJECTION, SURJECTION ET BIJECTION DES APPLICATIONS DÉFINIES SUR DES ENSEMBLES FINIS

Jetons un coup d'oeil sur la figure 10 où chacun des ensembles E et F contient un nombre fini d'éléments. On remarque que dans le cas de la bijection (figure la plus à droite), les deux ensembles E et F ont le même nombre d'élément, i.e., $card\,(E) = card\,(F)$; dans le cas d'une injection (figure la plus à gauche), l'ensemble d'arrivée F contient plus d'éléments que l'ensemble de départ E, i.e., $card\,(E) \leq card\,(F)$; dans le cas d'une surjection (figure du milieu), l'ensemble de départ E possède plus d'éléments que l'ensemble d'arrivée F, i.e., $card\,(E) \geq card\,(F)$. Ces trois situations ont toujours lieu, d,où la proposition suivante.

Proposition: Soient E et F deux ensembles finis (i.e., que chacun des ensembles E et F possède un nombre fini d'éléments), et soit $f : E \to F$ une application de E vers F. Alors

(i) Si f est bijective, alors $card\,(E) = card\,(F)$;

(ii) Si f est injective, alors $card\,(E) \leq card\,(F)$;

(iii) Si f est surjective, alors $card\,(E) \geq card\,(F)$.

Remarque: Dans chacune des points (i), (ii), et (iii0 de la proposition précedente, il faut bien distinguer l'hypothèse de la conclusion. La réciproque de chacune des trois énoncés est fausse. Par exemple, l'égalité des cardinaux ne veut pas forcement dire que mfm est bijective. Pour l'application $f : E = \{1,\ 2,\ 4\} \to F = \{2,\ 4,\ 6\}$ telle que $f(1) = 2$, $f(2) = 4$, $f(4) = 2$, on $card\,(E) = card\,(F) = 3$, mais l'application f n'est pas bijective (car f n'est par exemple pas surjective, 6 n'étant image d'aucun élément de E).

Comme conséquence de la proposition ci-dessus, nous formulons le corollaire suivant:

Corollaire: Soient E et F deux ensembles finis non vides tel que $card\,(E) = card\,(F)$, et soit $f : E \to F$ une fonction de E vers F. Alors les trois énoncés suivants sont équivalents:

(a) f est injective

(b) f est surjective

(c) f est bijective

XIII. DÉNOMBREMENTS

Définition (Arrangement): Soient E et F deux ensembles de cardinaux finis. On appelle **ensemble des arrangements** de E vers F, l'ensemble

$$\mathcal{F} = \{f : F \to E : f \text{ injective}\}$$

de toutes les injections de E dans F.

Théorème (Arrangement): Soient E et F deux ensembles de cardinaux finis $n = card\,(E)$ et $p = card\,(F)$. Si $p \leq n$, alors l'ensemble des arrangements

$$\mathcal{F} = \{f : F \to E : f \text{ injective}\}$$

de E dans F est un ensemble est fini et son cardinal est $card\,(\mathcal{F}) = n\,(n-1)\,(n-2)\cdots(n-p+1)$.

Preuve: Puisque $card\,(F) = p$ et $card\,(E) = n$, on peut admettre que $F = \{x_1,\ x_2,\ \cdots,\ x_p\}$ et $E = \{y_1,\ y_2,\ ...,\ y_n\}$ Soit $f : F \to E$ une application injective de F dans E. D'après la définition d'une injection, $f(x_i) \neq f(x_j)$ lorsque $i \neq j$. Puisque f est une application, alors $\forall x_i \in F, \exists! y_i \in E : f(x_i) = y_i$. Il y a donc exactement n possibilités pour c hoisir $f(x_1)$ dans E. Comme $f(x_2)$ doit être différent de $f(x_1)$ (car f est une injection), il y aura exactement $n-1$ possibilités pour choisir $f(x_2)$ dans E. Puisque $f(x_3) \in \{f(x_1),\ f(x_2)\}$, i.e., $f(x_3)$ est différente de chacun des $f(x_1)$ et $f(x_2)$, il y aura exactement $n-2$ possibilités pour choisir $f(x_3)$. Ainsi de suite, on trouve qu'il y aura $n-p+1$ possibilités pour choisir $f(x_p)$. D'où $card\,(\mathcal{F}) = n\,(n-1)\,(n-2)\cdots(n-p+1)$.

Remarque: Si nous introduisons la notation

$$n\,(n-1)\,(n-2)\cdots(n-p+1) = \Pi_{j=0}^{p-1}\,(n-j) = (n-p)!,$$

nous pouvons écrire $card\,(\mathcal{F}) = (n-p)!$.

Définition (Permutation): Soit $E = \{x_1,\ x_2,\ ...,\ x_n\}$ un ensemble fini non vide de cardinal $card\,(E) = n$. On appelle permutation, toute application bijective $\sigma : E \to E$.

Exemple: Soit $E = \{x_1,\ x_2,\ x_3\}$ un ensemble fini de cardinal $card\,(E) = 3$. Alors l'application $\sigma : E \to F$, $\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, $\sigma(x_3) = x_1$ est une bijection et par conséquent une permutation.

En appliquant le théorème des arrangements sur E, on obtient le corollaire suivant.

Corollaire (Permutation): Soit E un ensemble fini de cardinal $card\,(E) = n$. Alors l'ensemble des permutations

$$\mathcal{P}_E = \{\sigma : E \to E,\ \sigma \text{ bijective}\}$$

est un ensemble fini de cardinal $card\,(\mathcal{P}_E) = n! = n\,(n-1)\,(n-2)\cdots 2.1 = \Pi_{j=0}^{n-1}\,(n-j)$.

Preuve: Ce corollaire est une conséquence directe du théorème sur les arrangements, toute bijection étant une injection.

Définition (factorielle): On appelle factorielle de n, la quantité

$$n! = \Pi_{j=0}^{n-1}\,(n-j)$$

Par convention, on définit $0! = 1$.

Exemple: Trouver la factorielle de chacun des nombres $n_1 = 1$, $n_2 = 5$, $n_3 = 6$.

Solution: $n_1! = 1! = 1$; $n_2! = 5! = 5\times4\times3\times2\times1 = 120$; $n_3! = 6! = 6\times5\times4\times3\times2\times1 = 720$.

Le corollaire et la définition ci-dessus nous renseignent que le nombre de permutations de E dans E est égale à la factorielle du cardinal de E :

$$card\,(\mathcal{P}_E) = card\,(E)!$$

Définition (Combinaison de p dans n): Soient n et p deux entiers naturels tels que $p \leq n$. On appelle combinaison de p dans n (sous-entendu combiaison de p éléments dans un ensembles ayant n éléments), l'entier naturel noté C_n^p défini par

$$C_n^p = \frac{n!}{p!\,(n-p)!}.$$

Puisque $n! = n\,(n-1)\,(n-2)\cdots(n-p+1)\,(n-p)!$, on peut effectuer la simplification de l'écriture C_n^p pour obtenir

$$C_n^p = \frac{n\,(n-1)\,(n-2)\cdots(n-p+1)}{p!}.$$

Exemple: Calculer C_7^3 et C_{10}^7.

Solution:

$$\begin{aligned} C_7^3 &= \frac{7!}{3!\,(7-3)!} = \frac{7!}{3!4!} = \frac{7\times6\times5\times4!}{3!4!} \\ &= \frac{7\times6\times5}{3!} = \frac{7\times6\times5}{3\times2\times1} = 35 \end{aligned}$$

$$C_{10}^{7} = \frac{10!}{7!\,(10-7)!} = \frac{10!}{7!3!} = \frac{10\times 9\times 8\times 7!}{7!3!}$$
$$= \frac{10\times 9\times 8}{3!} = \frac{10\times 9\times 8}{3\times 2\times 1} = 120.$$

Définition (Combinaison): Soit E un ensemble fini de cardinal $card\,(E) = n$. On appelle combinaison de p éléments ($p \leq n$) de E, l'ensemble de tous les sous-ensembles de E ayant chacun exactement p éléments (i.e., l'ensemble des sous-ensembles de E dont chacun des sous-ensembles contient exactement p éléments).

La combinaison C_n^p est le nombre de possibilités qu'on puisse combiner les éléments d'un ensemble E ayant n éléments pour obtenir des sous-ensembles dont chacun possède p éléments.

Exemple: Pour l'ensemble $E = \{x_1,\ x_2,\ x_3\}$, trouver (i) la combinaison de 1 élément de E et (ii) la combinaison de 2 éléments de E.

Solution: (i) La combinaison de 1 élément de E est $\{\{x_1\},\ \{x_2\},\ \{x_3\}\}$; le cardinal de cet ensemble est $3 = C_3^1$.

(ii) La combinaison de 2 élément de E est $\{\{x_1,\ x_2\},\ \{x_1,\ x_3\},\ \{x_2,\ x_3\}\}$; le cardinal de cet ensemble est $3 = C_3^2$.

Théorème (Combinaison): Soit E un ensemble fini de cardinal fini $card\,(E) = n$ et soit p un entier non nul tel que $1 \leq p \leq n$. Alors l'ensemble des parties (sous-ensembles) de E ayant p éléments est un ensemble fini de cardinal

$$C_n^p = \frac{n!}{p!\,(n-p)!} = \frac{n\,(n-1)\,(n-2)\cdots(n-p+1)}{p!}.$$

Formulons la propriété suivante satisfaite pour les combinaisons de p dans n.

Théorème (Égalité de Pascal): Si n et p sont deux entiers naturels tels que $1 \leq p < n$, alors on a l'égalité

$$C_n^p = C_{n-1}^{p-1} + C_{n-1}^p.$$

Cette dernière égalité est appelée égalité de Pascal.

Formulons la définition suivante qui donne une application de la combinaison de p dans n.

Définition (Formule du binôme de Newton): Soient donnés deux réels a et b et soit $n \geq 1$ un entier naturel. alors la formule du binôme de Newton suivante est valide

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

Exemple:

$$\begin{aligned}(a+b)^3 &= C_3^0 a^0 b^{3-0} + C_3^1 a b^{3-1} + C_3^{3-2} a^2 b^{3-2} + C_3^3 a^3 b^{3-3} \\ &= b^3 + 3ab^2 + 3a^2 b + b^3.\end{aligned}$$

Terminons ce chapitre par la formulation du théorème sur l'ensemble des parties d'un ensemble fini.

Théorème (Cardinal de l'ensemble des partie): Si E est un ensemble fini de cardinal $card\,(E) = n$, alors on a

$$card\,(\mathcal{P}(E)) = 2^n,$$

où $\mathcal{P}(E)$ est l'ensemble des parties de E.

CHAPITRE 4

RELATIONS D'ÉQUIVALENCES, RELATIONS D'ORDRE, LOIS DE COMPOSITION

Dans ce chapitre, nous introduisons les notions des relations d'équivalence, des relations d'ordre, et des lois de composition.

XIV. RELATIONS D'ÉQUIVALENCE

Définition (Relation): Soit E un ensemble non vide. On appelle relation $\mathcal{R}$, tout sous-ensemble du produit cartésien $E \times E$.

Définition (Relation d'équivalence): Soit E un ensemble non vide et soit $\mathcal{R}$ une relation dans E. On dira que $\mathcal{R}$ est une relation d'équivalence si les conditions suivantes sont toutes satisfaites:

(1) **Reflexivité:** La relation $\mathcal{R}$ est reflexive i.e., tout élément x de E est en relation avec lui-même:

$$\forall x \in E,\ x\mathcal{R}x$$

(2) **Symétrie:** La relation $\mathcal{R}$ est symétrie, i.e., si x est en relation avec y alors y doit être en relation avec x :

$$\forall x, \in E,\ \forall y \in E,\ \text{si } x\mathcal{R}y,\ \text{alors } y\mathcal{R}x$$

(3) **Transitivité:** La relation $\mathcal{R}$ est transitive, i.e., si x est en relation avec y et y est en relation avec z, alors x est en relation avec z :

$$\forall x, \in E,\ \forall y \in E,\ \forall z \in E,\ \text{si } x\mathcal{R}y \text{ et } y\mathcal{R}z,\ \text{alors } x\mathcal{R}z.$$

Toute relation $\mathcal{R}$ de E qui satisfait simultanément ces trois conditions (reflexivité, symétrie, et transitivité) est notée $\sim$. Ainsi, si $\mathcal{R}$ est une relation d'équivalence, on écrit $\mathcal{R} = \sim$ et $x \sim y$ au lieu de $x\mathcal{R}y$.

Exemple: Soit $E = \mathbf{Z}$ et $\mathcal{R}$ la relation définie sur $\mathbf{Z}$ comme suit:

$$x\mathcal{R}y \text{ si } y - x \text{ est divisible par } 5.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence.

Solution: Avant tout, notons qu'un entier relatif x est divisible par 5 si et seulement s'il existe un entier relatif m tel que $x = 5m$. Montrons maintenant que $\mathcal{R}$ est une relation d'équivalence.

(a Reflexivité): Pour tout $x \in \mathbf{Z}$, $x - x = 0 = 5 \times 0$, ce qui revient à dire que $x - x$ est divisible par 5. Autrement dit, $x\mathcal{R}x$ et $\mathcal{R}$ est reflexive.

(b Symétrie): Soient x et y deux entiers relatifs tels que $x\mathcal{R}y$, i.e, $y - x$ est divisible par 5. Montrons que $x - y$ est aussi divisible par 5. Puisque $y - x$ est divisible par 5, il existe un entier relatif m tel que $y - x = 5m$. Mais alors $x - y = -5m = 5(-m) = 5m'$, où $m' = -m$ est un entier relatif. Puisque $x - y = 5m'$ et m' est un entier relatif, on conclut que $x - y$ est divisible par 5, ce qui revient à dire que $y\mathcal{R}x$.

(c Transitivité): Soient x, y, $z \in \mathbf{Z}$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors $y - x$ et $z - y$ sont chacun divisible par 5, ce qui revient à dire qu'il existe deux entiers relatifs m_1 et m_2 tels que $y - x = 5m_1$ et $z - y = 5m_2$. Mais alors, $z - x = z - y + y - x = (z - y) + (y - x) = 5m_2 - 5m_1 = 5(m_2 - m_1)$. Puisque m_1 et m_2 sont des entiers relatifs, leur différence $m_2 - m_1 = m_3$ est un entier relatif. Ainsi, il existe un entier relatif m_3 tel que $z - x = 5m_3$, ce qui veut dire que $z - x$ est divisible par 5. Mais alors, $x\mathcal{R}z$ et $\mathcal{R}$ est transitive.

(a), (b), et (c) nous permettent de conclure que $\mathcal{R}$ est une relation d'équivalence.

Définition (Classe d'équivalence): Soit $\sim$ une relation d'équivalence sur E. On appelle classe de x relativement à la relation d'équivalence $\sim$, l'ensemble noté $\overline{x}$ ou $[x]$ défini par

$$\overline{x} = [x] := \{y \in E : x \sim y\}.$$

Autrement dit, la classe d'équivalence de x est l'ensemble des éléments de E qui sont en relation avec x. Il existe d'autres notation pour la classe d'équivalence. Il est évident que $\overline{x} \in \mathcal{P}(E), \forall x \in E$.

Proposition: Si x et y sont deux éléments de E tels que $\overline{x} \neq \overline{y}$, alors $\overline{x} \cap \overline{y} = \varnothing$.

Preuve: Montrons que si $\overline{x} \neq \overline{y}$, alors $\overline{x} \cap \overline{y} = \varnothing$. supposons le contraire, i.e., que $\overline{x} \neq \overline{y}$ et $\overline{x} \cap \overline{y} \neq \varnothing$. Soit $z \in \overline{x} \cap \overline{y}$, i.e., $z \in \overline{x}$ et $z \in \overline{y}$. Mais alors, $z \sim x$ et $z \sim y$. En utilisant la symétrie, on trouve que $x \sim z$ et $z \sim y$. Par la transitivité, on conclut que $x \sim y$. Mais

alors, $\forall x_1 \in \overline{x}$ et tout $y_1 \in \overline{y}$, on aura, par transitivité, $x_1 \sim y \Rightarrow x_1 \in \overline{y} \Rightarrow \overline{x} \subset \overline{y}$ et $y_1 \sim x \Rightarrow y_1 \in \overline{x} \Rightarrow \overline{y} \subset \overline{x}$. On trouve ainsi que $\overline{x} \subset \overline{y}$ et $\overline{y} \subset \overline{x}$, et cette double inclusion signifie que $\overline{x} = \overline{y}$, ce qui contredit l'hypothèse $\overline{x} \neq \overline{y}$. Cette contradiction signifie que $\overline{x} \cap \overline{y} = \varnothing$.

Définition (Ensemble quotient): Soit E un ensemble non vide et soit $\sim$ une relation d'équivalence sur E. On appelle ensemble quotient de E ou ensemble des classes relatif à la relation d'équivalence $\sim$, l'ensemble noté $E/\sim$ défini par

$$E/\sim := \{A \in \mathcal{P}(E) : \exists x \in E,\ A = \overline{x}\},$$

où $\mathcal{P}(E)$ est l'ensemble des parties de E. Autrement dit, $A \in E/\sim$ si $A \in \mathcal{P}(E)$ et il existe $x \in E$ tel que $\overline{x} = A$ (la classe d'équivalence de x coincide avec A).

De façon plus précise, l'ensemble quotient $E/\sim$ est l'ensemble formé de toutes les classes d'équivalence des éléments de E:

$$E/\sim = \{\overline{x} : x \in E\}.$$

Définition (Surjection canonique): Soit E un ensemble non vide et soit $\sim$ une relation d'équivalence sur E. On appelle surjection canonique de E vers $E/\sim$, l'application surjective : $\pi : E \to E/\sim$ définie par $\pi(x) = \overline{x}$.

Ainsi, la surjection canonique est une application de E qui à tout x de E qui à tout x de E fait correspondre sa classe d'équivalence relative à la relation d'équivalence $\sim$.

Exemple: Trouver la classe d'équivalence de tout $x \in \mathbf{Z}$ pour la relation $\sim$ définie par

$$\forall x, y \in \mathbf{Z},\ x \sim y \quad \text{si } y - x \text{ est divisible par } 5,$$

puis en déduire l'ensemble quotient $\mathbf{Z}/\sim$

Solution: Soit $x \in \mathbf{Z}$. Alors

$$\overline{x} = \{y \in \mathbf{Z} : y - x \text{ est divisible par } 5\}.$$

Comme nous avons dit plus haut, $y - x$ est divisible par 5 si et seulement s'il existe $m \in \mathbf{Z}$: $y - x = 5m \Leftrightarrow y = 5m + x$. Ainsi, pour tout entier relatif m, on a $(5m + x) - x = 5m$, ce qui veut dire que $x \sim 5m + x$. Soit $z \in \mathbf{Z}$ tel que $z \neq 5m + x$, pour tous les $m \in \mathbf{Z}$. Alors $z - x \neq 5m$, $\forall m \in \mathbf{Z}$, ce qui signifie que $z - x$ n'est pas divisible par 5 et par conséquent,

x n'est pas en relation avec z. Nous avons ainsi montré que $x \sim y$ si et seulement si $y = 5m + x$ pour un certain $m \in \mathbf{Z}$. Autrement dit,

$$\overline{x} = \{5m + x : m \in \mathbf{Z}\}.$$

Déduisons l'ensemble quotient $\mathbf{Z}/\sim$: Il découle de cette expression que pour x et y dans $\mathbf{Z}$ tels que $x \neq y$, on a $\overline{x} = 5m + x$ et $\overline{y} = 5m_1 + y$, de sorte que $\overline{x} \cap \overline{y}$ sera vide si et seulement si $y - x \neq 5(m - m_1)$ pour tout entiers relatifs m et m_1. Dire que $y - x \neq 5(m - m_1)$ pour tous les m et m_1 signifie que $y - x \in \{0,\ 1,\ 2,\ 3,\ 4\}$. Pour cet ensemble, on a

$$\begin{aligned}
\overline{0} &= \{5m : m \in \mathbf{Z}\}, \\
\overline{1} &= \{5m + 1 : m \in \mathbf{Z}\}, \\
\overline{2} &= \{5m + 2 : m \in \mathbf{Z}\}, \\
\overline{3} &= \{5m + 3 : m \in \mathbf{Z}\}, \\
\overline{4} &= \{5m + 4 : m \in \mathbf{Z}\}.
\end{aligned}$$

On trouve ainsi l'ensemble quotient

$$\mathbf{Z}/\sim = \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\right\}.$$

Définition (Partition d'un ensemble): Soit donné un ensemble E et soient E_1, E_2, ..., E_n des sous-ensembles non vides de E. On dira que E_1, E_2, ..., E_n réalisent une partition de E les deux conditions suivantes sont satisfaites:

(1) $E_i \cap E_j = \varnothing$ quand $i \neq j$;

(2) $\cup_{i=1}^{n} E_i = E$.

Exemple: Si nous désignons par $E = \mathbf{N}$, $E_1 = \{2m : m \in \mathbf{N}\}$ et $E_2 = E_1 = \{2m + 1 : m \in \mathbf{N}\}$ (E_1 est l'ensemble des entiers pairs et E- l'ensemble des entiers impairs), alors on constate que $E_1 \cap E_2 = \varnothing$ et $E_1 \cup E_2 = \mathbf{N} = E$. ceci signifie que E_1 et E_2 réalisent une partition de $\mathbf{N}$.

Définition (Ensemble de représentants): Soit E un ensemble non vide et soit $\sim$ une relation d'équivalence définie sur E. On appelle **ensemble de représentants** pour la relation d'équivalence $\sim$, tout sous-ensemble $\mathcal{T} \subset E$ satisfaisant les deux conditions suivantes:

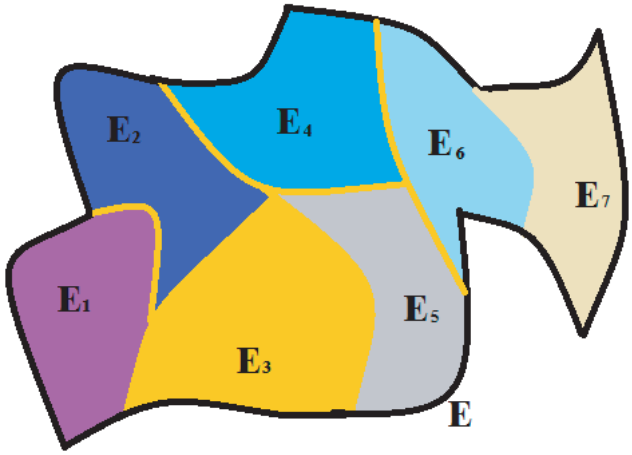


Figure 11: E_1, E_2, ..., E_n réalisent une partition de E.

(i) $\forall x \in E, \exists y \in \mathcal{T} : \overline{x} = \overline{y}$;

(ii) $\forall x, y \in \mathcal{T}$, si $x \neq y$ alors $\overline{x} \neq \overline{y}$.

Remarque: Cette définition nous donne le renseignement suivant: si $\sim$ est une relation d'équivalence sur E et si $\mathcal{T}$ est un ensemble de représentants pour la relation $\sim$, alors l'ensemble quotient sera

$$E/\sim = \{\overline{x} : x \in \mathcal{T}\}.$$

Inversement, si $E/\sim$ est l'ensemble quotient de E relatif à la relation d'équivalence $\sim$, alors on peut facilement former à partir de $E/\sim$ un ensemble de représentants $\mathcal{T}$ pour la relation $\sim$:

$$\mathcal{T} = \{x : \overline{x} \in E/\sim\}.$$

Il est évident que les ensembles $\overline{x} : x \in \mathcal{T}$ sont deux à deux disjoints. On vérifie que la réunion des $\overline{x}$ quand x parcourt $\mathcal{T}$ donne E (i.e., $\cup\{\overline{x} : x \in \mathcal{T}\} = E$), d'où la proposition suivante.

Proposition: Soit E un ensemble non vide et soit $\sim$ une relation d'équivalence sur E. Si $\mathcal{T} \subset E$ est un ensemble de représentants pour la relation $\sim$, alors les ensembles $\overline{x} : x$ parcourt $\mathcal{T}$ réalisent une partition de E.

Exemple: Soit la relation $\sim$ définie sur $\mathbf{Z}$ par

$$\forall x, y \in \mathbf{Z},\ x \sim y \quad \text{si } y - x \text{ est divisible par } 5.$$

Trouver un ensemble de représentants de $\sim$ et en déduire une partition de $\mathbf{Z}$.

Solution: Dans l'exemple ci-dessus, nous avons trouver que $\mathbf{Z}/\sim = \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4}\right\}$. Compte tenue de la remarque ci-dessus, nous avons un ensemble de représentants de $\mathcal{T} = \{0, 1,\ 2,\ 3,\ 4\}$ de $\sim$. D'après la proposition ci-dessus, les ensembles $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ réalisent une partition de $\mathbf{Z}$, d'où

$$\begin{aligned}\mathbf{Z} \ = \ &\{5m : m \in \mathbf{Z}\} \cup \{5m+1 : m \in \mathbf{Z}\} \cup \{5m+2 : m \in \mathbf{Z}\} \\ &\cup \{5m+3 : m \in \mathbf{Z}\} \cup \{5m+4 : m \in \mathbf{Z}\}.\end{aligned}$$

XV. RELATIONS D'ORDRE

Soit E un ensemble non vide et soir $\mathcal{R}$ une relation sur E.

Définition (Relation d'ordre): On dira que $\mathcal{R}$ est une relation d'ordre sur E et on posera $\mathcal{R} = \preceq$ si les trois conditions suivante sont satisfaites:

(1) **Reflixivité:** La relation $\mathcal{R}$ est reflexive i.e., tout élément x de E est en relation avec lui-même:

$$\forall x \in E,\ x\mathcal{R}x,\ \text{i.e.,}\ x \preceq x;$$

(2) **Anti-symétrie:** La relation $\mathcal{R}$ est anti-symétrie, i.e., si x est en relation avec y alors y est en relation avec x, alors $x = y$:

$$\begin{aligned}&\forall x, \in E,\ \forall y \in E,\ \ (x\mathcal{R}y) \wedge (y\mathcal{R}x)\ \text{ si e seulement si } x = y \\ &\text{i.e.,}\ \ (x \preceq y) \wedge (y \preceq x) \Leftrightarrow x = y;\end{aligned}$$

(3) **Transitivité:** La relation $\mathcal{R}$ est transitive, i.e., si x est en relation avec y et y est en relation avec z, alors x est en relation avec z :

$$\begin{aligned}&\forall x, y, z \in E,\ \text{si } x\mathcal{R}y \text{ et } y\mathcal{R}z,\ \text{alors } x\mathcal{R}z \\ &\text{i.e., } \forall x, y, z \in E,\ \ (x \preceq y) \wedge (y \preceq z) \Rightarrow x \preceq z.\end{aligned}$$

Définition (Ensemble ordonné): Tout ensemble E muni d'une relation d'ordre est dit ordonné.

Exemple 1: $\mathbf{R}$ muni de la relation «$\leq$ (inférieur ou égal)» est un ensemble ordonné.

Exemple 2: Soit E un ensemble non vide et soit $\mathcal{P}(E)$ l'ensemble des parties de E. Montrer que l'inclusion $\subset$ est une relation d'ordre sur $\mathcal{P}(E)$.

Résolution: Reflexivité: Soit $E_1 \in \mathcal{P}(E)$. Tout ensemble étant son propre sous-ensemble, on a $E_1 \subset E_1$, ce qui signifie que la relation «$\subset$» est reflexive.

Anti-symétrie: Soient E_1 et E_2 deux éléments de $\mathcal{P}(E)$. Si $E_1 \subset E_2$ et $E_2 \subset E_1$, alors d'après la définition de l'égalité de deux ensembles, la double inclusion $(E_1 \subset E_2) \wedge (E_2 \subset E_1)$ signifie que $E_1 = E_2$. Ainsi, la relation d'incusion «$\subset$» est anti-symétrie.

Transitivité: Soient E_1, E_2, $E_3 \in \mathcal{P}(E)$ tels que $(E_1 \subset E_2) \wedge (E_2 \subset E_3)$. Montrons que $E_1 \subset E_3$. Soit x un élément quelconque de E_1. Puisque $E_1 \subset E_2$, x est forcement un élément de E_2. Par hypothèse, $E_2 \subset E_3$. $(E_2 \subset E_3) \wedge x \in E_2 \Rightarrow x \in E_3$. Nous avons ainsi trouvé que tout élément x de E_1 est aussi élément de E_3, ce qui revient à dire que $E_1 \subset E_3$. Ainsi, la re;ation d'inclusion «$\subset$» est transitive. Ces trois proriétés montrent que la relation d'inclusion «$\subset$» est une relation d'ordre sur l'ensemble $\mathcal{P}(E)$ des parties de E. Muni de cette relation d'ordre, $\mathcal{P}(E)$ est un ensemble ordonné.

Exemple 3: Soit $E = \mathbf{N}^* = \mathbf{N}\backslash\{0\}$. On définit sur E la relation / par

$$\forall n, m \in E,\ n/m \Leftrightarrow n \text{ divise } m.$$

Montrer que / est une relation d'ordre sur $E = \mathbf{N}^* = \mathbf{N}\backslash\{0\}$.

Solution: Rappelons nous que l'expression «n divise m» signifie que m est divisible par n, i.e., que le reste de la division de m par n est zéro. Autrement dit, «n divise m» signifie qu'il existe un entier naturel $q \neq 0$ tel que $m = q \times n$ (ici, q est le quotient de la division de m par n). Ainsi,

$$n \text{ divise } m \Leftrightarrow m = q \times n \text{ pour un certain entier naturel } q \neq 0.$$

Reflexivité: $\forall n \in \mathbf{N}^*$, on a $n = 1 \times n$, ce qui signifie que n/n, i.e., / est reflexive;

Anti-symétrie: Soient $n, m \in \mathbf{N}^*$. Supposons que $n/m \wedge m/n$ et montrons que $n = m$. Si $n/m \wedge m/n$, alors il existe deux entiers naturels non nuls q_1 et q_2 tels que $m = q_1 \times n$ et $n = q_2 \times m$. Alors $m = q_1 \times n = q_1 \times (q_2 \times m)$, i.e., $m = q_1 \times (q_2 \times m) = (q_1 \times q_2) \times m$, i.e., $m = (q_1 \times q_2) \times m$. Puisque $m \neq 0$, on peut simplifier cette dernière égalité par m, ce qui donne $1 = q_1 \times q_2$. Si on résoud cette équation par rapport à q_2, on trouve $q_2 = \frac{1}{q_1}$. Ainis, on trouve que $q_2 = \frac{1}{q_1} \in \mathbf{N}^*$, ce qui n'est possible que si $q_1 = 1$. Mais alors, $m = q_1 \times n = 1 \times n = n$, i.e., $m = n$. Ainsi, on peut avoir simultanément $n/m \wedge m/n$ seulement quand $n = m$, ce qui signifie que la relation «/» est anti-symtétrie.

Transitivité: Soient $x, y, z \in \mathbf{N}^* : (x/y) \wedge (y/z)$. Montrons que x/z.

$$x/y \Leftrightarrow y = q_1 \times x \text{ et } y/z \Leftrightarrow z = q_2 \times y,$$

où q_1 et q_2 sont deux entiers naturels non nuls. Puisque $(y = q_1 \times x) \wedge (z = q_2 \times y)$, on a

$$\begin{aligned} z &= q_2 \times y = q_2 \times (q_1 \times x) \\ &= (q_2 \times q_1) \times x = q_3 \times x, \end{aligned}$$

où $q_3 = q_2 \times q_1$. Puisque q_1 et q_2 sont deux entiers naturels non nuls, $q_3 = q_2 \times q_1$ est aussi un entier naturel non nul. Nous avons ainsi trouver que $z = q_3 \times x$, où q_3 est aussi un entier naturel non nul, ce qui signifie que z est divisible par x, i.e., que x divise z. On obtient ainsi que x/z. Donc si $(x/y) \wedge (y/z)$, alors x/z, ce qui signifie que la relation $\ll/\gg$ est transitive.

Nous avons ainsi montré que $\ll/\gg$ est une relation d'ordre sur $\mathbf{N}^*$. Muni de cette relation d'ordre, $\mathbf{N}^*$ est un ensemble ordonné.

Définition: Soit $\preceq$ une relation d'ordre sur un ensemble non vide E et soit A une partie non vide de E ($A \subset E \wedge A \neq \varnothing$). Alors

(i) On dit que l'ordre $\preceq$ est **total** si

$$\forall x, y \in E, \ \ (x \preceq y) \vee (y \preceq x);$$

(ii) On dira que l'ordre est **partiel** s,il n'est pas total;

(iii) On dira qu'un élément $m \in E$ est un **minorant** de A si

$$\forall x \in A, \ m \preceq x;$$

L'ensemble A sera dit minoré s'il existe un minorant de A dans E.

(iv) On dira qu'un élément $M \in E$ est un **majorant** de A si

$$\forall x \in A, \ x \preceq M;$$

L'ensemble A sera dit majoré s'il existe un majorant de A dans E.

(v) On appelle **plus petit élément** de A, tout minorant de A contenu dans A. Autrement dit, un élément m_A de E est appelé plus petit élément de A si $m_A \in A$ et $\forall x \in A$, $m_A \preceq x$; si m_A est le plus petit élément de A, on écrit note $m_A = \min A$;

(vi) On appelle **plus grand élément** de A, tout majorant de A contenu dans A. Autrement dit, un élément M_A de E est appelé plus grand élément de A si $M_A \in A$ et $\forall x \in A$, $x \preceq M_A$; Si M_A est le plus grand élément de A, on note $M_A = \max A$

(vii) On appelle **borne inférieure** de A, le plus grand des minorants de A. La borne inférieure de A s'il existe est noté $\inf A$;

(viii) On appelle **borne supérieure** de a, le plus petit des majorants de A. La borne supérieure de A s'il existe est notée $\sup A$.

(ix) On dira que l'ensemble A est borné s'il est à la fois majoré et minoré.

Remarque: Le plus petit élément $\min A$ est aussi appelé élément minimal de A alors que le plus grand élément de A est aussi appelé élément maximal de A, d'où les notations $\min A$ et $\max A$.

Proposition:

(a) Le plus petit élément de A, s'il existe, est unique;

(b) Le plus grand élément de A, s'il existe, est unique;

(c) La borne inférieure de A, s'il existe, est unique;

(d) La borne supérieure de A, s'il existe, est unique;

(e) Si l'ensemble A admet un plus petit élément $\min A$, alors $\exists \inf A$ et $\inf A = \min A$ (la réciproque n'est pas vraie);

(f) Si l'ensemble A admet un plus grand élément $\max A$, alors $\exists \sup A$ et $\sup A = \max A$ (la réciproque n'est pas vraie).

(g) Si A admet un minorant, alors il admet une infinité de minorants; si A admet un majorant, alors il admet une infinité de majorants.

Exemple 1: Soit $E = \mathbf{R}$ muni de la relation d'ordre «$\leq$ (inférieur ou égale)» et $A = [a,\ b]$, avec $a < b$. Alors $\inf A = \min A = a$ et $\sup A = \max A = b$.

Exemple 2: Soit $E = \mathbf{R}$ muni de la relation d'ordre «$\leq$ (inférieur ou égale)» et $A =]a,\ b[$, avec $a < b$. Alors $\inf A = a$ et $\sup A = b$. Pour cet exemple, $\min A$ et $\max A$ n'existent pas.

Traduction mathématique de la borne inférieure et de la borne supérieure dans l'ensemble ordonné $(\mathbf{R}, \leq)$: Soit A une partie non vide de $\mathbf{R}$ et soient m et M

deux éléments de $\mathbf{R}$.Alors

$$m = \inf A \Leftrightarrow (\forall x \in A,\ m \leq x) \wedge (\forall \varepsilon > 0,\ \exists x_\varepsilon \in A : x_\varepsilon \leq m + \varepsilon)\,;$$
$$M = \sup A \Leftrightarrow (\forall x \in A,\ x \leq M) \wedge (\forall \varepsilon > 0,\ \exists x_\varepsilon \in A : M - \varepsilon \leq x_\varepsilon)\,.$$

Remarque: On interpréte chacune des expressions à droite de $\Leftrightarrow$ de la façon suivante:

(a) Dans $(\forall x \in A,\ m \leq x) \wedge (\forall \varepsilon > 0,\ \exists x_\varepsilon \in A : x_\varepsilon \leq m + \varepsilon)$, le premier block $(\forall x \in A,\ m \leq x)$ signifie que m est un minorant de A, alors que le second block $(\forall \varepsilon > 0,\ \exists x_\varepsilon \in A : x_\varepsilon < m + \varepsilon)$ signifie que m est le plus grand des minorant de sorte que pour tout $\varepsilon > 0$ aussi petit que possible, $m + \varepsilon$ n'est plus un minorant de A; dire que $m + \varepsilon$ n'est pas un minorant de A revient à dire qu'il existe au moins un élément de A qui soit plus petit ou égale à $m + \varepsilon$.

(a) Interpréter à titre d'exercice l'écriture

$$(\forall x \in A,\ x \leq M) \wedge (\forall \varepsilon > 0,\ \exists x_\varepsilon \in A : M - \varepsilon \leq x_\varepsilon)\,.$$

Exemple: Soit E un ensemble non vide et soit $\mathcal{P}(E)$ l'ensemble des parties de E. Comme nous avons montré plus haut, l'inclusion $\subset$ est une relation d'ordre sur $\mathcal{P}(E)$, de sorte que $\mathcal{P}(E)$ muni de cette relation d'ordre est un ensemble ordonné. Montrer que $(\mathcal{P}(E), \subset)$ est borné et trouver sa borne inférieure et sa borne supérieure.

Solution: Puisque $\mathcal{P}(E)$ est formé des sous ensembles de E y compris E, on aura, $\forall E_1 \in \mathcal{P}(E)$, $E_1 \subset E$, ce qui signifie que E est un majorant de $\mathcal{P}(E)$ et $\mathcal{P}(E)$ est majoré. Puisque $E \in \mathcal{P}(E)$, on conclut que E est le plus grand élément de $\mathcal{P}(E)$ et par conséquent, $\max \mathcal{P}(E) = \sup \mathcal{P}(E) = E$.

Montrons maintenant que $\mathcal{P}(E)$ est minoré et trouvons sa borne inférieure. Puisque $\varnothing \in \mathcal{P}(E)$ et l'ensemble vide est un sous-ensemble de tout ensemble, on conclut que $\forall E_1 \in \mathcal{P}(E)$, $\varnothing \subset E_1$. Mais alors, $\varnothing$ est un minorant de $\mathcal{P}(E)$, ce qui veut dire que $\mathcal{P}(E)$ est minoré. Puisque $\varnothing \in \mathcal{P}(E)$, on conclut que $\varnothing$ est le plus petit élément de $\mathcal{P}(E)$. Mais alors, $\varnothing = \min A = \inf A$.

Puisque $\mathcal{P}(E)$ est à la fois majoré et minoré, on conclut que $\mathcal{P}(E)$ est borné.

XVI. LOIS DE COMPOSITION

Définition (Loi de composition interne): Soit E un ensemble non vide. On appelle **loi de composition interne** sur E, toute application $T : E \times E \to E$. Si T est une loi de

composition interne de $E \times E$ dans E, alors $\forall\,(x,y) \in E \times E$, l'image de (x,y) par T sera notée xTy au lieu de $T(x,y)$:

$$\begin{aligned} T : E \times E &\to E \\ (x,y) &\mapsto xTy. \end{aligned}$$

Définition (Loi de composition externe): Soient E et K deux ensembles non vides. On appelle **loi de composition externe** à domaine d'opérateurs dans K, toute application $T : K \times E \to E$ qui à tout élément $(\lambda, x) \in K \times E$ associe l'élément $\lambda Tx \in E$:

$$\begin{aligned} T : K \times E &\to E \\ (\lambda, x) &\mapsto \lambda Tx. \end{aligned}$$

Exemple 1: L'addition $\ll + \gg$ et la multiplication $\ll \cdot \gg$ sont chacune une loi de composition interne dans $\mathbf{R}$, $\mathbf{N}$, $\mathbf{Z}$, et $\mathbf{Q}$.

Exemple 2: Si E est un ensemble non vide et $\mathcal{F}(E)$ est l'ensemble des applications de E dans E, alors la composition $\ll \circ \gg$ des application est une loi de composition interne dans $\mathcal{F}(E)$.

Exemple 3: Si E est un ensemble non vide et $\mathcal{P}(E)$ est l'ensemble des parties de E. Alors l'intersection $\ll \cap \gg$ et la différence symétrique $\ll \Delta \gg$ sont chacune une loi de composition interne dans $\mathcal{P}(E)$.

Remarque: Il faut noter que

$$\begin{aligned} \cap : \mathcal{P}(E) \times \mathcal{P}(E) &\to \mathcal{P}(E) \\ (E_1, E_2) &\mapsto E_1 \cap E_2 \end{aligned} \quad \text{et} \quad \begin{aligned} \Delta : \mathcal{P}(E) \times \mathcal{P}(E) &\to \mathcal{P}(E) \\ (E_1, E_2) &\mapsto E_1 \Delta E_2 \end{aligned}$$

Définition (commutativité, associativité, distributivité): Soit $T : E \times E \to E$ une loi de composition interne dans E. Alors

1) La loi T est dite commutative si

$$\forall x, y \in E,\ xTy = yTx;$$

2) La loi T est dite associative si

$$\forall x, y, z \in E,\ \ (xTy)\,Tz = xT\,(yTz)\,;$$

3) La loi T est dite distributive par rapport à une deuxième loi interne $S : E \times E \to E$ si

$$\forall x, y, z \in E,\ \text{on a } xT\,(ySz) = (xTy)\,S\,(xSz) \wedge (xSy)\,Tz = (xTz)\,S\,(yTz)\,.$$

Exemple: Dans $\mathbf{R}$, la multiplication «$\cdot$» est commutative, associative, et distributive par rapport à l'addition «$+$».

En effet, $\forall x, y, z \in \mathbf{R}$, on a $x \cdot y = y \cdot x$; $(x \cdot y) \cdot z = x \cdot (y \cdot z)$; $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ et $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Définition (Élément neutre): Soit $T : E \times E \to E$ une loi de composition interne dans E. On dira que la loi T admet un **élément neutre** s'il existe un élément $e \in E$ tel que

$$\forall x \in E,\ xTe = eTx = x;$$

Un tel élément e est appelé **élément neutre** pour la loi T.

Définition (Élément inverse): Soit $T : E \times E \to E$ une loi de composition interne dans E admettant un élément neutre e. On appelle **élément inverse** ou tout simplement **inverse** d'un élément $x \in E$, un élément $x' \in E$ tel que $xTx' = x'Tx = e$.

Exemple 1: L'addition «$+$» et la multiplication «$\cdot$» dans $\mathbf{R}$ sont commutatives et associatives, et la multiplication «$\cdot$» est distributive par rapport à l'addition «$+$». L'élément 0 est l'élément neutre pour l'addition, et 1 est l'élément neutre pour la multiplication.

Exemple 2: Soit E un ensemble non vide et soit $\mathcal{P}(E)$ l'ensemble des parties de E. L'intersection «$\cap$» et la différence des ensembles «Δ» sont commutatives et associatives, et l'intersection est distributive par rapport à la différence symétrique (des ensembles). L'élément neutre pour l'intersection est l'ensemble E et l'élément neutre pour la différence symétrique est l'ensemble vide $\varnothing$. Si $A \in \mathcal{P}(E)$, alors son inverse par rapport à la différence symétrique est A lui-même. En général, il n'existe pas d'élément inverse pour l'intersection.

Définition (Anneau): Le triplet $(A, +, \cdot)$ constitué d,un ensemble non vide A et de deux lois de composition internes $+$ et $\cdot$ est **appelé anneau (unitaire)** si les conditions suivantes sont satisfaites:

(i) L'addition $+$ est commutative, associative, admet un élément neutre (noté 0) et tout élément x de A admet un élément inverse (dans A) pour l'addition,

(ii) La multiplication $\cdot$ est associative, distributive par rapport à l'addition et admet un élément neutre (noté 1).

Définition (Anneau commutatif): Un anneau $(A, +, \cdot)$ est dit commutatif si la loi $\cdot$ est commutative, i.e., si $\forall x, y \in A$, $x \cdot y = y \cdot x$.

Exemple: Chacun des triplet $(\mathbf{R}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{Z}, +, \cdot)$, $(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif (ici, $+$ et $\cdot$ sont respectivement l'addition et la multiplication).

CHAPITRE 5

ALGÈBRE BOOLÉENNE

Le présent chapitre est consacré à l'algèbre, présentant dans un premier temps les postulats, les axiomes et les théorèmes qui en découlent. Une partie du chapitre est consacrée à la manipulation de cette algèbre logique, suivie d'une illustration des applications possibles pour les besoins des circuits logiques. Pour ce faire, une introduction des fondements des portes logiques est présentée.

XVII. NOTIONS THÉORIQUES DE L'ALGÈBRE DE BOOLE

A. Postulats et axiomes de l'algàbre de Boole

Pour avoir une algèbre de Boole, nous avons besoin de:

- Un ensemble E
- deux éléments particuliers de E : 0 et 1 (correspondant respectivement à FAUX et VRAI)
- deux opérations binaires sur E : $+$ et $\cdot$ (correspondant respectivement au OU et ET logiques)
- une opération unaire sur E : $^-$(correspondant à la négation (NON) logique).

Les postulats suivants sont acceptés:

Postulats 1: $0 \cdot 0 = 0$	*Postulats 5:* $1 + 1 = 1$
Postulats 2: $0 \cdot 1 = 1 \cdot 0 = 0$	*Postulats 6:* $1 + 0 = 0 + 1 = 1$
Postulats 3: $1 \cdot 1 = 1$	*Postulats 7:* $0 + 0 = 0$
Postulats 4: $\overline{0} = 1$	*Postulats 8:* $\overline{1} = 0$

Dans ces postulats, il faut bien noter la particularité du postulats 5: $1 + 1 = 1$ (nous avons déjà introduit une telle somme où 1 désignait le VRAI logique).

1. Définition et exemples

Définition (Algèbre de boole): Soit E un ensemble contenant au moins deux éléments que l'on convient de noter 0 et 1 (correspondant respectivement à **FAUX** et **VRAI**), et muni:

- D'une opération binaire appelée « somme » et notée $+$ (correspondant respectivement au **OU** logique):
$$\begin{aligned} + : E \times E &\to E \\ (x, y) &\mapsto x + y \end{aligned}$$
- D'une opération binaire appelée « produit » et notée $\cdot$ (correspondant respectivement au **ET** logique):
$$\begin{aligned} \cdot : E \times E &\to E \\ (x, y) &\mapsto x \cdot y \end{aligned}$$
- D'une opération unaire appelée « complémentation » et notée $^-$ (correspondant à la négation (NON) logique):
$$\begin{aligned} ^- : E \times E &\to E \\ x &\mapsto \overline{x} \end{aligned}$$

On dit que $(E, +, \cdot, ^-)$ a une structure d'algèbre de Boole si les axiomes de structure suivants sont satisfaits:

Axiome 1 (Commutativité): Les deux opérations binaires sont commutatives :

$$\forall x, y \in E,\ x + y = y + x \text{ et } x \cdot y = y \cdot x$$

Axiome 2 (Associativité): Les deux opérations binaires sont associatives :

$$\forall x, y, z \in E,\ (x + y) + z = x + (y + z) \text{ et } (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Axiome 3 (Éléments neutres): 0 est un élément neutre pour $+$ et 1 est un élément neutre pour $\cdot$:

$$\forall x \in E,\ x + 0 = 0 + x = x \text{ et } 1 \cdot x = x \cdot 1 = x$$

Axiome 4 (Distributivité): Chaque opération binaire est distributive par rapport à l'autre :

$$\forall x, y, z \in E,\ x + (y \cdot z) = (x + y) \cdot (x + z) \text{ et } x \cdot (y + z) = x \cdot y + x \cdot z$$

Axiome 5 (Complémentation):

$$\forall x \in E,\ x + \overline{x} = 1 \text{ et } x \cdot \overline{x} = 0$$

Exemple 1: Soient A un ensemble non vide et soit $\mathcal{P}(A)$ l'ensemble des parties de A. Soit $E = \mathcal{P}(A)$ et soient les opérations $+$, $\cdot$, et définies sur $\mathcal{P}(A)$ par

$$\begin{aligned} \forall A, B \ &\in \ \mathcal{P}(A),\ A + B = A \cup B \\ \forall A, B \ &\in \ \mathcal{P}(A),\ A \cdot B = A \cap B \\ \forall A \ &\in \ \mathcal{P}(A),\ \overline{A} = C_E(A). \end{aligned}$$

Montrer que $(\mathcal{P}(A), \cup, \cap,)$ est une algèbre de Boole.

Solution: Pour montrer que $(\mathcal{P}(A), \cup, \cap,)$ est une algèbre de Boole, il nous faut montrer que les cinq axiomes de l'algèbre de Bboole sont tous satisfaits:

Les axiomes 1, 2, et 4 découlent des opérations sur les ensembles. L'ensemble vide $\varnothing$ est l'élément neutre pour la réunion et l'ensemble E est l'élément neutre pour l'intersection (i.e. $0 = \varnothing$ et $1 = E$): $\forall A \in \mathcal{P}(A)$, on a $A \cup \varnothing = A$ et $A \cap E = A$. Ainisi, l'axiome 3 est satisfait. Montrons enfin que l'axiome 5 est aussi satisfait:$\forall A \in \mathcal{P}(A$, on a

$$\begin{aligned} A + \overline{A} &= A \cup \overline{A} \\ &= A \cup C_E(A) = E = 1; \\ A \cdot \overline{A} &= A \cap \overline{A} \\ &= A \cap C_E(A) = \varnothing = 0. \end{aligned}$$

Ainsi, l'axiome 5 est satisfait. Nous avons ainsi montrer que $(\mathcal{P}(A), \cup, \cap,)$ est une algèbre de Boole.

Exemple 2: L'ensmble $E = \{0, 1\}$ muni des opérations booléenne $+$ et $\cdot$ est une algèbre de Boole.

2. Principe de dualité

Chaque axiome et chaque postulat possède un équivalent dual, où les 0 sont remplacés par des 1, les 1 par des 0, les $(\cdot\ )$ par des $(\ +\ )$ et les $(+)$ par des $(\ \cdot\ )$. Aussi, tout théorème de l'algèbre de Boole a son équivalent dual. Le théorème dual est formulé à partir du théorème

de base en remplaçant les 0 par des 1 (respectivement, les 1 par des 0) et les $(\cdot\ )$ par des $(\ +\ )$ (respectivement, les $(+\ )$ par des $(\cdot)$). Par exemple, considérons le théorème suivant :

Théorème: Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors

$$\forall x \in E, \text{ on a } x + x = x.$$

Preuve: La preuve de ce théorème se fait comme suit:

$$\begin{aligned} x + x &= 1 \cdot x + 1 \cdot x && \text{d'après l'axiome de l'élément neutre pour } \cdot \\ &= (1 + 1) \cdot x && \text{d'après l'axiome de distributivité} \\ &= 1 \cdot x && \text{d'après le postulat (5)} \\ &= x && \text{d'après l'axiome de l'élément neutre pour} \cdot \end{aligned}$$

ainsi, nous avons montrer que si $(E, +, \cdot,)$ une algèbre de Boole, alors $x + x = x$ pour tout $x \in E$.

Énonçons le dual de ce théorème:

Théorème dual: Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors

$$\forall x \in E, \text{ on a } x \cdot x = x.$$

Preuve: La preuve de ce théorème se fait comme suit:

$$\begin{aligned} x \cdot x &= (0 + x) \cdot (0 + x) && \text{d'après l'axiome de l'élément neutre pour } + \\ &= (0 \cdot 0) + x && \text{d'après l'axiome de distributivité} \\ &= 0 + x && \text{d'après le postulat (1)} \\ &= x && \text{d'après l'axiome de l'élément neutre pour } +\,. \end{aligned}$$

Remarque: Dans ce théorème dual, nous avons tout simplement remplacer le $(+)$ par le $(\cdot)$.

Remarque: Pour les besoins de clarté, il faut utiliser les parenthèses.

Application du principe de dualité: Nous avons montré ci-dessus que $(\mathcal{P}(A), \cup, \cap,)$ était une algèbre de Boole. En appliquant le principe de dualité, on trouve que $(\mathcal{P}(A), \cap, \cup,)$ sera aussi une algèbre de Boole.

3. Règles sur les égalités

Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors

Règle 1: $\forall a, b, c \in E$, on a

$$a = b \Rightarrow a + c = b + c$$
$$a = b \Rightarrow a \cdot c = b \cdot c$$

Règle 2: $\forall a, b, c \in E$, on a

$$\left.\begin{array}{c} a + c = b + c \\ a \cdot c = b \cdot c \end{array}\right\} \Rightarrow a = b$$

Règle 3: $\forall a, b, c, d \in E$, on a

$$\left.\begin{array}{c} a = b \\ c = d \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a + c = b + d \\ a \cdot c = b \cdot d \end{array}\right.$$

Règle 4: $\forall a, b \in E$, on a

$$a = b \Leftrightarrow \overline{a} = \overline{b}$$

Règle 5: $\forall a, b \in E$, on a

$$a \cdot b = 1 \Leftrightarrow a = 1 \text{ et } b = 1$$
$$a + b = 0 \Leftrightarrow a = 0 \text{ et } b = 0$$

XVIII. THÉORÈMES DE BASE DE L'ALGÈEBRE DE BOOLE

Dans la pratique, on effectue les développements et les simplifications comme en algèbre classique (dans $\mathbf{R}$) et on donne la priorité à l'opérateur « produit » $(\cdot)$; autrement dit, la multiplication aura préséance sur l'addition, et ainsi, ainsi $a + b \cdot c$ signifiera pour nous $(a) + (b \cdot c)$ et non pas $(a + b) \cdot c$. Aussi, des parenthèses seront introduites pour éviter l'ambiguïté le cas échéant, comme nous l'avons fait précédemment sans l'énoncer formellement (par exemple, $(1 + 1) \cdot x$ représente $1 \cdot x + 1 \cdot x$ alors que $1 + 1 \cdot x$ représente $(1) + (1 \cdot x)$). Les développements et Simplifications en algèebre de Boole sont basés sur des théorèmes de base. Ici, nous allons considérer quelques-uns des théorèmes de base que nous aurons à utiliser

abondamment pour nos besoins particuliers. Le cas échéant, les théorèmes sont présentés par paire suivant le principe de dualité.

Théorèmes de base: Soit $(E, +, \cdot,)$ une algèbre de Boole et soient a, b, et c trois éléments de E, alors :

	Forme 1	**Forme 2 (Dual)**	**Nom**
1	$\overline{\overline{a}} = a$		Involution
2	$a + a = a$	$a \cdot a = a$	Idempotence
3	$a + 1 = 1$	$a \cdot 0 = 0$	Absorption
4	$a + a \cdot b = a$	$a \cdot (a + b) = a$	Absorption
5	$\overline{a + b} = \overline{a} \cdot \overline{b}$	$\overline{a \cdot b} = \overline{a} + \overline{b}$	de Morgan
6	$a + \overline{a} \cdot b = a + b$	$a \cdot (\overline{a} + b) = a \cdot b$	
7	$a + \overline{a} = 1$	$a \cdot \overline{a} = 0$	Unicité de $\overline{a}$
8	$a \cdot b + \overline{a} \cdot c = a \cdot b + \overline{a} \cdot c + b \cdot c$	$(a + b) \cdot (\overline{a} + c) = (a + b) \cdot (\overline{a} + c) \cdot (b + c)$	Redondance

Dans ces théorèmes, on note que le dual de $\overline{\overline{a}} = a$ n'existe pas, tout de même comme le 6 n'a pas de nom. Nous avons, dans la section précedente, démontré le théoreme sur l'idempotence (i.e., le théorème 2). La preuve des autres théorèmes est basée sur les postulats et axiomes de l'algèbre de Boole. Démontrons par exemple les théorèmes 3 et 6:

Théorème 3: Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors $\forall a \in E$, on a $a + 1 = 1$ et $a \cdot 0 = 0$.

Preuve: Montrons que $a + 1 = 1$

$$\begin{aligned} a + 1 &= a + (a + \overline{a}) && \text{d'après l'axiome de complémentation } a + \overline{a} = 1 \\ &= (a + a) + \overline{a} && \text{d'après l'axiome de l'associativité} \\ &= a + \overline{a} && \text{d'après le théorème (2) démontré à la section précedente} \\ &= 1 && \text{d'après l'axiome de complémentation.} \end{aligned}$$

Pour démontrer que $a \cdot 0 = 0$, nous utilisons tout simplement le principe de dualité, appliqué sur la preuve de $a + 1 = 1$ en remplaçant les 1 par des 0 et les 0 par des 1, les $+$ par des $\cdot$

et les $\cdot$ par des $+$:

$$\begin{aligned}
a \cdot 0 &= a \cdot (a \cdot \overline{a}) && \text{d'après l'axiome de complémentation } a \cdot \overline{a} = 0 \\
&= (a \cdot a) \cdot \overline{a} && \text{d'après l'axiome de l'associativité} \\
&= a \cdot \overline{a} && \text{d'après le théorème (2) démontré à la section précedente} \\
&= 0 && \text{d'après l'axiome de complémentation.}
\end{aligned}$$

Théorème 6: Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors $\forall a, b \in E$, on a $a + \overline{a} \cdot b = a + b$ et $a \cdot (\overline{a} + b) = a \cdot b$.

Preuve: Soient $a, b \in E$. Montrons que $a \cdot (\overline{a} + b) = a \cdot b$

$$\begin{aligned}
a \cdot (\overline{a} + b) &= (a + 0) \cdot (\overline{a} + b) && \text{d'après l'axiome de l'élément neutre} \\
&= \left(a + b \cdot \overline{b}\right) \cdot (\overline{a} + b) && \text{d'après l'axiome de la complémentation} \\
&= (a + b) \cdot \left(a + \overline{b}\right) \cdot (\overline{a} + b) && \text{d'après l'axiome de la distributivité} \\
&= [(a + b) \cdot (a + b)] \cdot \left(a + \overline{b}\right) \cdot (\overline{a} + b) && \text{d'après le théorème (2)} \\
&= (a + b) \cdot \left[(a + b) \cdot \left(a + \overline{b}\right)\right] \cdot (\overline{a} + b) && \text{d'après l'axiome d'associativité} \\
&= (a + b) \cdot \left(a + \overline{b}\right) \cdot (a + b) \cdot (\overline{a} + b) && \text{d'après l'axiome de la commutativité} \\
&= \left(a + b \cdot \overline{b}\right) \cdot (a \cdot \overline{a} + b) && \text{d'après l'axiome de la distributivité (2 fois)} \\
&= (a + 0) \cdot (0 + b) && \text{d'après l'axiome de la complémentation (2 fois)} \\
&= a \cdot b && \text{d'après l'axiome de l'élément neutre (2 fois);}
\end{aligned}$$

Pour démontrer le dual $a + \overline{a} \cdot b = a + b$, on utilise le principe de dualité en enlevant si necessaire les parenthèses:

$$\begin{aligned}
a + \overline{a} \cdot b &= (a \cdot 1) + (\overline{a} + b) && \text{d'après l'axiome de l'élément neutre} \\
&= \left(a \cdot b + \overline{b}\right) + (\overline{a} \cdot b) && \text{d'après l'axiome de la complémentation} \\
&= a \cdot b + a \cdot \overline{b} + \overline{a} \cdot b && \text{d'après l'axiome de la distributivité} \\
&= [a \cdot b + a \cdot b] + a \cdot \overline{b} + \overline{a} \cdot b && \text{d'après le théorème (2)} \\
&= a \cdot b + \left[a \cdot b + a \cdot \overline{b}\right] + \overline{a} \cdot b && \text{d'après l'axiome d'associativité} \\
&= a \cdot b + a \cdot \overline{b} + a \cdot b + \overline{a} \cdot b && \text{d'après l'axiome de la commutativité} \\
&= \left(a \cdot b + \overline{b}\right) + (a + \overline{a} \cdot b) && \text{d'après l'axiome de la distributivité (2 fois)} \\
&= a \cdot 1 + 1 \cdot b && \text{d'après l'axiome de la complémentation (2 fois)} \\
&= a + b && \text{d'après l'axiome de l'élément neutre (2 fois);}
\end{aligned}$$

XIX. FONCTIONS BOOLÉENNES ET DÉCOMPOSITION DE SHANNON

La décomposition de Shannon est très utile pour la simplification des fonctions logiques, et elle nous servira pour mieux comprendre le fonctionnement de certains circuits usuels. De plus, elle permet de poser des démonstrations élégantes pour des théorèmes récalcitrants. Avant d'énoncer la décomposition de shannon, nous introduisons d'abord la notion de fonctions booléennes.

A. Les fonctions Booléennes et leurs formes canoniques

Définition (Fonctions booléenne): Soit $(E, +, \cdot,)$ une algèbre de Boole. On appelle **fonction booléenne** de n variables x_1, x_2, ..., x_n, toute combinaison de ces variables au moyen des trois opérations booléennes $+$, $\cdot$, et .

Exemple: $f(x, y, z) = x \cdot y + \overline{z}$ est une fonction boolénne de trois variables x, y, z.

Définition (Minterme): Soit $(E, +, \cdot,)$ une algèbre de Boole. On appelle **minterme** de n variables, l'un des produits booléens de ces variables ou de leurs complémentaires. Chaque minterme est affecté d'un indice unique que l'on déterminera plus tard.

Exemple: Si $(E, +, \cdot,)$ une algèbre de Boole, alors en considérant quatre variables x, y, z, et w, on aura,

- $m = x \cdot \overline{y} \cdot \overline{y} \cdot z$ est un minterme;
- $m = \overline{x} \cdot y \cdot z \cdot \overline{w}$ est un minterme;
- $m = x \cdot y \cdot z \cdot \overline{w}$ est un minterme;
- $m = x \cdot y \cdot z \cdot w$ est un minterme;
- $m = \overline{x} \cdot y \cdot \overline{w}$ n'est pas un minterme.

Définition (Maxterme): On appelle **maxterme** de n variables, l'une des sommes booléennes de ces variables ou de leurs complémentaires. Chaque maxterme est affecté d'un indice unique que l'on d´eterminera plus tard.

Exemple: Si $(E, +, \cdot,)$ une algèbre de Boole, alors en considérant quatre variables x, y, z, et w, on aura,

- $m = x + \overline{y} + \overline{y} + z$ est un maxterme;

- $m = \overline{x} + y + z + \overline{w}$ est un maxterme;

- $m = x + y + z + \overline{w}$ est un minterme;

- $m = x + y + w$ n'est pas un maxterme;

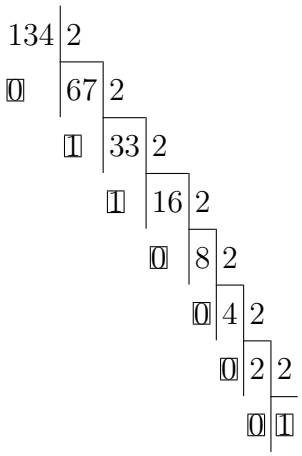
- $m = \overline{x} \cdot (y + z) + \overline{w}$ n'est pas un maxterme.

1. Indexation et Nombre de mintermes et maxtermes

a. Écriture en base 2 *et en base* 10 Avant de formuler la règle d'indexation, rappelons nous de la correspondence entre la base 2 et la base 10: L'écriture d'un nombre en base 2 ne contient que des 0 et des 1; En base 10, l'écriture d'un nombre contient les nombres 0, 1, 2, 3, 4, 5, 6, 7, 8, et 9.

Pour **convertir un nombre donné en base** 10 **en base** 2, on procède par des divisions successives par 2. Mais alors, chaque division ne peut avoir pour reste que 0 ou 1. Les processus de division s'arrête quand le quotient est 1. À la fin du processus des divisions successives, on écrit le nombre en base 2, le premier chiffre du nombre étant le dernier quotient (qui naturellement est 1), et tout les autres chiffres du nombre en base 2 étant les differents restes, partant du dernier au premier reste.

Exemple: Écrire le nombre 134 en base 2.



Divisions de 134 successivement par 2

Aprés la division de 134 successivement par 2, on trouve $(134)_{10} = (10000110)_2$.

Pour convertir le nombre $(a_0a_1a_2...a_n)_2$ écrit en base 2 en base 10 (ici, $a_0 = 1$ et $a_j \in \{0, 1\}$, pour les $j = 1, 2, ..., n$), on porcède de la manière suivante:

$$(aa_1a_2...a_n)_2 = \left(a \times 2^n + a_1 \times 2^{n-1} + a_2 \times 2^{n-2} + \cdots + a_n \times 2^{n-n}\right)_{10}.$$

En appliquant ce principe, on trouve que

$$\begin{aligned}(10000110)_2 &= \left(2^7 + 0 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0\right)_{10} \\ &= 134\end{aligned}$$

b. Règle d'indexation des mintermes et les maxtermes Pour indexer les mintermes et les maxtermes, on utilise la règle suivante:

- Pour chaque minterme (resp. maxterme) on construit un code binaire en posant 1 si une variable est présente, 0 si son complémentaire est présent: $m_i = (110010\cdots10\cdots)_2$ (resp. $M_i = (110010\cdots10\cdots)_2$)
- On convertit ce code binaire en base décimal pour obtenir l'indice du minterme (resp. maxterme): L'index i du minterme (resp. maxterme) sera alors $i = [(110010\cdots10\cdots)_2$ écrit en base 10].

Exemple: Si $(E, +, \cdot,)$ une algèbre de Boole. Soit le minterme de quatre variables

$$m_i = x \cdot \overline{y} \cdot \overline{z} \cdot w.$$

Alors le code binaire associé à ce minterme est $(1001)_2$, i.e., 1001 en base 2. Pour trouver l'index i du minterme $m_i = (1001)_2$ convertit ce minterme en base 10 :

$$i = 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 9.$$

Pour le calculer l'indice du maxterme $M_i = x + y + \overline{z} + w$, on écrit d'abord son code binaire $(1101)_2$. Alors,

$$i = 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 13.$$

Remarque: À deux mintermes différents correspondent deux codes différents, et par conséquent, deux indice différents. Autrement dit, deux minterme (maxterme) différents ont des codes différents et des indices différents.

Formulons le théorème suivant sur le nombre des mintermes de n variables.

Théorème (Nombre de mintermes de n variables): Le nombre N_n de mintermes (resp. maxtermes) de n variables et $N_n = 2^n$.

Énonçons quelques propriétés des mintermes et de maxtermes. Soient $m_i = x \cdot y \cdot z \cdot w$ et $M_i = x + y + z + w$. Alors

$$\begin{aligned} \overline{m_i} &= \overline{x \cdot y \cdot z \cdot w} \overset{\text{car } \overline{a \cdot b} = \overline{a} + \overline{b}}{=} \overline{x} + \overline{y} + \overline{z} + \overline{w} \\ \overline{M_i} &= \overline{x + y + z + w} \overset{\text{car } \overline{a + b} = \overline{a} \cdot \overline{b}}{=} x \cdot y \cdot z \cdot w \end{aligned}$$

de sorte que le complémentaire d'un minterme (resp. d'un maxterme) de 4 variables est un maxterme (resp. un minterme) de 4 variables. Cette remarque est toujours vraie, ce qui donne lieu à la propriété suivante.

Propriété 1 (Complémentaire): Le complémentaire d'un minterme est un maxterme, le complémentaire d'un maxterme est un minterme, et

$$\overline{m_i} = M_{2^n - i - 1} \text{ et } \overline{M_j} = m_{2^n - j - 1}.$$

Formulons d'autres propriété:

Propriété 2 (Somme booléenne des mintermes): La somme booléenne de tous les mintermes vaut 1:

$$\sum_{i=0}^{2^n - 1} m_i = 1$$

Propriété 3 (Produit booléen des maxtermes): Le produit booléen de tous les maxtermes vaut 0:

$$\Pi_{j=0}^{2^n - 1} M_j = 0.$$

Propriété 4 (Produit des mintermes et sommes des maxtermes): Le produit de deux mintermes différents vaut 0 et la somme de deux maxtermes différents vaut 1.

Exemple: Écrire tous les mintermes et tous les maxtermes de trois variables x, y, z puis, écrire le code binaire de chacun et en déduire l'indice correspondent. Présenter les résultats sous forme de tableaux.

Solution:

Mintermes	code binaire	Indice
$x \cdot y \cdot z$	$(111)_2$	7
$x \cdot \overline{y} \cdot z$	$(101)_2$	5
$x \cdot \overline{y} \cdot \overline{z}$	$(100)_2$	4
$x \cdot y \cdot \overline{z}$	$(110)_2$	6
$\overline{x} \cdot \overline{y} \cdot \overline{z}$	$(000)_2$	0
$\overline{x} \cdot y \cdot \overline{z}$	$(010)_2$	2
$\overline{x} \cdot y \cdot z$	$(011)_2$	3
$\overline{x} \cdot \overline{y} \cdot z$	$(001)_2$	1

;

Maxtermes	code binaire	Indice
$x + y + z$	$(111)_2$	7
$x + \overline{y} + z$	$(101)_2$	5
$x + \overline{y} + \overline{z}$	$(100)_2$	4
$x + y + \overline{z}$	$(110)_2$	6
$\overline{x} + \overline{y} + \overline{z}$	$(000)_2$	0
$\overline{x} + y + \overline{z}$	$(010)_2$	2
$\overline{x} + y + z$	$(011)_2$	3
$\overline{x} + \overline{y} + z$	$(001)_2$	1

2. Formes canoniques conjonctives et disjonctives

Soit f une fonction booléenne de n variables.

Définition (Forme canonique disjonctive): Mettre la fonction booléenne f sous forme canonique disjonctive (ou première forme canonique) revient à l'écrire comme la somme de mintermes des n variables.

Définition (Forme canonique conjonctive): Mettre la fonction f sous la forme canonique conjonctive (ou deuxième forme canonique) revient à l'écrire comme le produit de maxtermes des n variables.

Théorème (Sur la forme canonique): Tout fonction booléenne f de n variables peut être mise de manière unique sous forme canonique disjonctive (resp. conjonctive).

Pour mettre une fonction F sous sa forme canonique, on utilise dans un premier temps le calcul booléen afin d,avoir une forme devéloppée, et ensuite dans chaque monôme, il faut faire apparaitre les «variables » manquantes.

Exemple 1: Pour trois variables x, y, z, on aura

$$\begin{aligned} f(x,y,z) &= x \cdot \overline{y} = x \cdot \overline{y} \cdot 1 = x \cdot \overline{y} \cdot (z + \overline{z}) \quad \text{car } z + \overline{z} = 1 \\ &= x \cdot \overline{y} \cdot z + x \cdot \overline{y} \cdot \overline{z} \end{aligned}$$

Ainsi, la forme canonique disjonctive de $f(x,y,z) = x \cdot \overline{y}$ est

$$f(x,y,z) = x \cdot \overline{y} \cdot z + x \cdot \overline{y} \cdot \overline{z}$$

Exemple 2: Pour quatre variables,

$$\begin{aligned} f(x,y,z,w) &= x\cdot\overline{y} \\ &= x\cdot\overline{y}\cdot z + x\cdot\overline{y}\cdot\overline{z} \\ &= x\cdot\overline{y}\cdot z\cdot(w+\overline{w}) + x\cdot\overline{y}\cdot\overline{z}\cdot(w+\overline{w}) \\ &= x\cdot\overline{y}\cdot z\cdot w + x\cdot\overline{y}\cdot z\cdot\overline{w} + x\cdot\overline{y}\cdot\overline{z}\cdot w + x\cdot\overline{y}\cdot\overline{z}\cdot\overline{w}. \end{aligned}$$

B. Décomposition de Shannon

Théorème (Énoncé de la décomposition de Shannon): Soit f une fonction propositionnelle (fonction logique) définie sur un univers de discours de variables x_1, x_2, ..., x_n. Alors

$$f(x_1,x_2,...,x_n) = \overline{x_1}\cdot f(0,x_2,...,x_n) + x_1\cdot f(1,x_2,...,x_n). \tag{1}$$

La décomposition (1) est dénommée **décomposition de Shannon** de la fonction logique f.

Preuve: Si $x_1 = 0$, alors l'expression à gauche de l'égalité (1) vaut $f(0,x_2,...,x_n)$, alors que l'expression à droite vaut

$$\begin{aligned} &\overline{x_1}\cdot f(0,x_2,...,x_n) + x_1\cdot f(1,x_2,...,x_n) \\ =\ &\overline{0}\cdot f(0,x_2,...,x_n) + 0\cdot f(1,x_2,...,x_n) = 1\cdot f(0,x_2,...,x_n) = f(0,x_2,...,x_n). \end{aligned}$$

Ainsi, l'égalité est satisfaite, i.e. que l'expression à gauche de (1) est bien égale à l'expression à droite.

Si $x_1 = 1$, alors l'expression à gauche de l'égalité (1) vaut $f(1,x_2,...,x_n)$, alors que l'expression à droite sera

$$\begin{aligned} &\overline{x_1}\cdot f(0,x_2,...,x_n) + x_1\cdot f(1,x_2,...,x_n) \\ =\ &\overline{1}\cdot f(0,x_2,...,x_n) + 1\cdot f(1,x_2,...,x_n) \\ =\ &0\cdot f(0,x_2,...,x_n) + f(1,x_2,...,x_n) = f(1,x_2,...,x_n), \end{aligned}$$

d'où l'égalité (1) est satisfaite.

Remarque: Il est important de noter que dans la décomposition (1), la variable x_1 peut être remplacée par n'importe quelle autre des variables restantes x_2, x_3, ..., x_n, par exemple,

$$f(x_1,x_2,...,x_n) = \overline{x_n}\cdot f(0,x_2,...,x_n) + x_n\cdot f(1,x_2,...,1).$$

Si on applique le principe de dualité sur la décomposition (1), on obtiendra la factorisation

$$(x_1, x_2, ..., x_n) = [\overline{x_1} + f(1, x_2, ..., x_n)] \cdot [x_1 + f(0, x_2, ..., x_n)] \tag{2}$$

De plus, il faut noter que la décomposition (1) peut également être appliquée récursivement sur l'ensemble des variables. Par exemple, en écrivant

$$\begin{aligned} f(0, x_2, ..., x_n) &= \overline{x_2} \cdot f(0, 0, ..., x_n) + x_2 \cdot f(0, 1, ..., x_n) \text{ et} \\ f(1, x_2, ..., x_n) &= \overline{x_2} \cdot f(1, 0, ..., x_n) + x_2 \cdot f(1, 1, ..., x_n), \end{aligned}$$

on obtiendra

$$\begin{aligned} f(x_1, x_2, ..., x_n) &= \overline{x_1} \cdot f(0, x_2, ..., x_n) + x_1 \cdot f(1, x_2, ..., x_n) \\ &= \overline{x_1} \cdot [\overline{x_2} \cdot f(0, 0, ..., x_n) + x_2 \cdot f(0, 1, ..., x_n)] \\ &\quad + x_1 \cdot [\overline{x_2} \cdot f(1, 0, ..., x_n) + x_2 \cdot f(1, 1, ..., x_n)] \\ &= \overline{x_1} \cdot \overline{x_2} \cdot f(0, 0, ..., x_n) + \overline{x_1} \cdot x_2 \cdot f(0, 1, ..., x_n) \\ &\quad + x_1 \cdot \overline{x_2} \cdot f(1, 0, ..., x_n) + x_1 \cdot x_2 \cdot f(1, 1, ..., x_n). \end{aligned}$$

Application de la décomposition de shannon: Utilisons la décomposition de shannon pour démontrer le théorème 5 formulé dans le tableau ci-dessus, reformulé ici:

Théorème 5: Soit $(E, +, \cdot,)$ une algèbre de Boole. Alors $\forall a, b \in E$, on a $\overline{a + b} = \overline{a} \cdot \overline{b}$.

Preuve: Soit f la fonction logique définie sur E par $f(a, b) = \overline{a + b}$, $\forall a, b \in E$. alors, la décomposition de Shannon nous donne

$$\begin{aligned} f(a, b) &= \overline{a} \cdot f(0, b) + a \cdot f(1, b) \\ &= \overline{a} \cdot \left[\overline{b} \cdot f(0, 0) + b \cdot f(0, 1)\right] + a \cdot \left[\overline{b} \cdot f(1, 0) + b \cdot f(1, 1)\right] \\ &= \overline{a} \cdot \left[\overline{b} \cdot \overline{0 + 0} + b \cdot \overline{0 + 1}\right] + a \cdot \left[\overline{b} \cdot \overline{1 + 0} + b \cdot \overline{1 + 1}\right] \\ &= \overline{a} \cdot \left[\overline{b} \cdot \overline{0} + b \cdot \overline{1}\right] + a \cdot \left[\overline{b} \cdot \overline{1} + b \cdot \overline{1}\right] \\ &= \overline{a} \cdot \left[\overline{b} \cdot 1 + b \cdot 0\right] + a \cdot \left[\overline{b} \cdot 0 + b \cdot 0\right] \\ &= \overline{a} \cdot \overline{b}. \end{aligned}$$

Ainsi, $\overline{a + b} = f(a, b) = \overline{a} \cdot \overline{b}$.

XX. TABLE DE VÉRITÉ ET TABLE DE KARNAUGH

Comme nous avons souligné plus haut, La table de vérité d'une fonction logique est un tableau énumérant les valeurs logiques (valeurs de vérité) d'une fonction pour les différentes

combinaisons des valeurs de ses variables indépendantes. Comme en logique, nous parlerons ici de correspondance entre la sortie et les entrées. On placera les variables de la fonction dans les colonnes de gauche en les faisant varier de façon à couvrir l'ensemble des possibilités (l'univers des discours), la colonne la plus à droite donne les valeurs prises par la fonction logique pour les différentes combinaisons des valeurs d'entrée.

Avant de procéder dans le cas général, considérons quelques exemples:

Sot $E = \{x,\ y\}$ un ensemble des variables logiques. On admet que $(E, +, \cdot,)$ est une algèbre de Boole. Soient f_1, f_2, f_3, et f_4 des fonctions logiques définies sur E par

$$\begin{aligned} f_1(x,y) &= x+y;\ f_2(x,y) = \overline{x \cdot y} \\ f_3(x,y) &= \overline{x}+\overline{y};\quad f_4(x) = \overline{\overline{x}}. \end{aligned}$$

Les tables de vérité associées à ces quatres fonctions logiques sont :

x	y	f_1
1	1	1
1	0	1
0	1	1
0	0	0

x	y	f_2
1	1	0
1	0	1
0	1	1
0	0	1

x	y	f_3
1	1	0
1	0	1
0	1	1
0	0	1

x	f_4
1	1
0	0

Les tables de vérité constituent un élément important dans la manipulation des fonctions logiques. Comme en logique mathématique, on dira que *deux fonctions logiques sont équivalentes si et seulement si elles possèdent la même table de vérité.* En obvesrvant la table de vérité de f_4, on constate que $\overline{\overline{x}} = x$, qui n'est autre chose que le théorème 1 de l'involution.

Remarque: Il est important de noter que la table de vérité d'une fonction logiques peut contenir plus de deux variables. Par exemple, soit $E = \{x,\ y,\ z,\ w\}$ est un ensemble tel que $(E, +, \cdot,)$ soit une algèbre de Boole. Soient les fonctions logiques $f_5(x,y,z,w) = x \cdot y + z + \overline{w}$, $f_6(x,y,z,w) = x \cdot y + z \cdot w$, $f_7(x,y,z,w) = x \cdot (x+y) + z \cdot w$, $f_8(x,y,z,w) = x \cdot y + x + z \cdot w$. Écrivons la table de vérité de chacune de ces quatres fonction

x	y	z	w	f_5
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	1
1	0	1	0	1
1	0	0	1	0
1	0	0	0	1
0	1	1	1	1
0	1	1	0	1
0	1	0	1	0
0	1	0	0	1
0	0	1	1	1
0	0	1	0	1
0	0	0	1	0
0	0	0	0	1

x	y	z	w	f_6
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	1
1	0	1	0	0
1	0	0	1	0
1	0	0	0	0
0	1	1	1	1
0	1	1	0	0
0	1	0	1	0
0	1	0	0	0
0	0	1	1	1
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0

x	y	z	w	f_7
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	1
1	0	1	0	1
1	0	0	1	1
1	0	0	0	1
0	1	1	1	1
0	1	1	0	0
0	1	0	1	0
0	1	0	0	0
0	0	1	1	1
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0

x	y	z	w	f_8
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	1	0	0	1
1	0	1	1	1
1	0	1	0	1
1	0	0	1	1
1	0	0	0	1
0	1	1	1	1
0	1	1	0	0
0	1	0	1	0
0	1	0	0	0
0	0	1	1	1
0	0	1	0	0
0	0	0	1	0
0	0	0	0	0

A. Table de vérité des opérateurs logiques

Rappelons la particularité de l'algèbre de Boole. Comme nous avons vu dès le début de ce chapitre, l'algèbre de Boole

- admet deux opérations binaires : $+$ et $\cdot$ (correspondant respectivement au OU et ET logiques),
- admet une opération unaire : $\overline{\ }$ (correspondant à la négation (NON) logique).

Pour ce trois opérateurs, nous avons les tables de vérité suivants:

x	y	$x+y$
1	1	1
1	0	1
0	1	1
0	0	0

Opérateur $\vee$ logique

x	y	$x \cdot y$
1	1	1
1	0	0
0	1	0
0	0	0

Opérateur $\wedge$ logique

x	$\overline{x}$
1	0
0	1

Opérateur NON logique

Remarque: Les table de vérité des opérateurs binaires $+$ et $\cdot$ de l'opérateur unitaire correspondent aux 8 postulats que nous avons énuméré au début de ce chapitre, i.e., $1+1=1$, $1=0=1$, $0+1=1$, $0+0=0$, $1\cdot 1=1$, $1\cdot 0=0$, $0\cdot 1=0$, $0\cdot 0=0$, $\overline{1}=0$, et $\overline{0}=1$. Ainsi, pour retenir les 8 postulats, il suffit de retenir ces trois tables de vérité des opérateurs $+$, $\cdot$, et . Notons aussi que toute fonction logique peut s'écrire **uniquement** avec ces trois opérateurs $+$, $\cdot$, et .

XXI. DIAGRAMMES DE VENN ET CERCLES D'EULER

La représentation des ensembles utilisée dans le deuxième chapitre est héritée du mathématicien britannique Venn. Cette représentation peut être utilisée pour illustrer les trois opérateurs de l'algèbre de Boole, on l'appelle aussi représentation par les cercles d'Euler.

La complémentarité (ou négation):

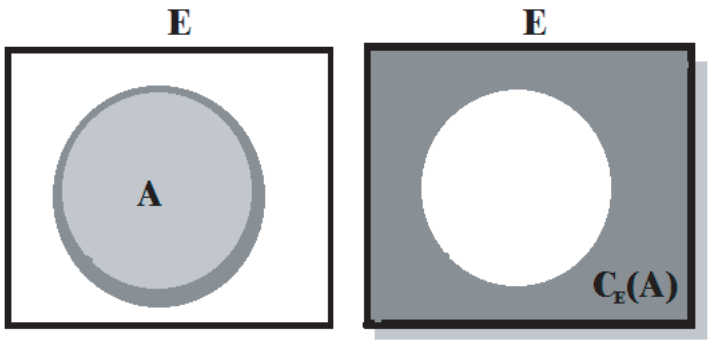


Figure 12: La complémentarité (ou négation) d'un ensemble

L'intersection (ou la conjonction):

L'union (ou la disjonction):

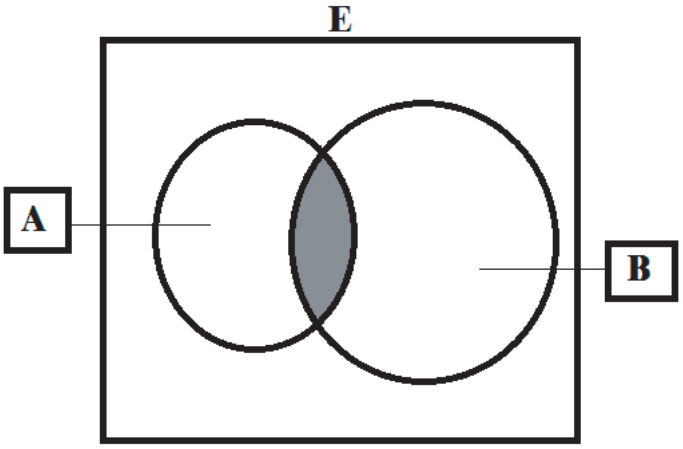


Figure 13: L'intersection (ou la conjonction) de deux ensembles.

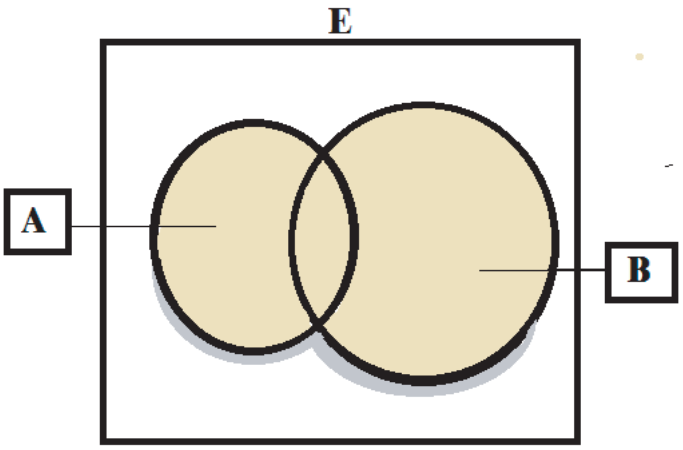


Figure 14: L'union (ou la disjonction) de deux ensembles.

Remarque: Il est possible d'inclure jusqu'à six ensembles (six variables) pour exprimer des énoncés logiques relativement complexes. Par exemple, la fonction $\overline{A \cdot B}$ est exprimée ainsi : Souvenons nous que l'opérateur $\cdot$ est vue comme l'opérateur $\wedge$ logique, alors que l'opérateur est vu comme l'opérateur logique **NON** logique. Ainsi, en terme des ensembles, $A \cdot B$ est vu comme $A \cap B$ et $\overline{A}$ est vu comme **NON** A. ainsi, $\overline{A \cdot B} = \mathbf{NON}(A \cap B) = E \backslash (A \cap B)$.

XXII. NOTIONS DE CIRCUITS LOGIQUES

Dans cette section nous parlerons du lien existant entre les circuits et l'algèbre de Boole, un lien qui date du début du XX^{e} siècle. Initialement, il s'agissait d'une application aux

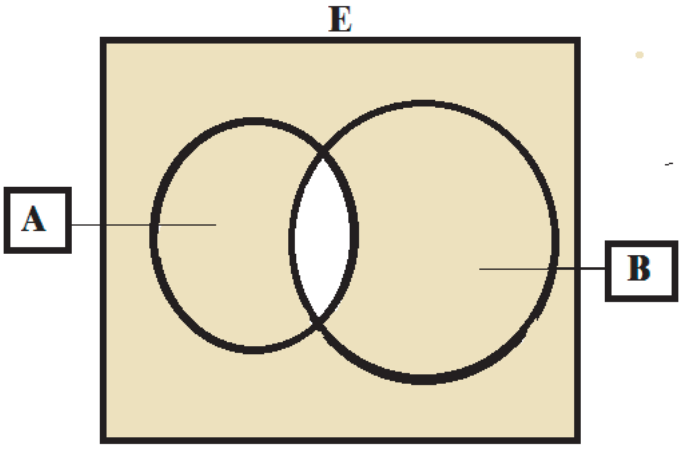


Figure 15: La fonction $\overline{A \cdot B}$ pour deux ensembles.

circuits à relais (sorte d'interrupteurs des figures a et b). Si des relais obéissaient à la même commande (variable) comme c'est la cas sur la figure c, alors une fonction logique pouvait exprimer son fonctionnement général. Comme le montre la figure c, la lampe s'allume si les interrupteurs (A OU B) et l'interrupteur A est fermé. Mais alors, si l'interrupteur A est fermé. Ainsi, on a la fonction logique $(A + B) \cdot A = A$

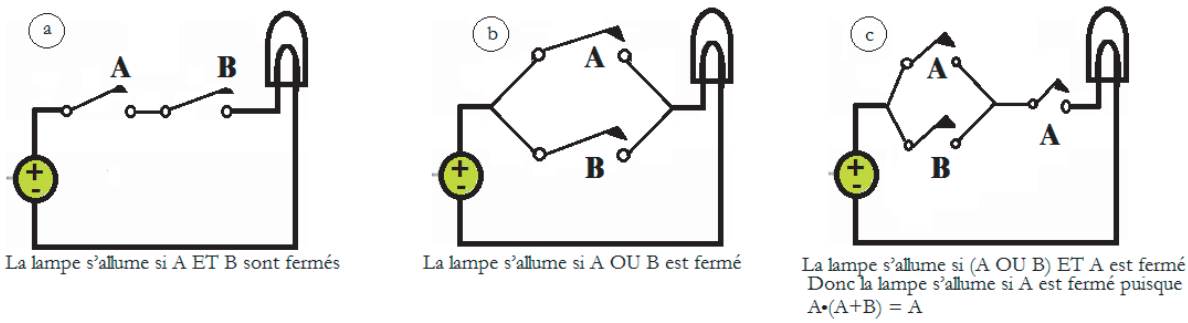


Figure 16: Application de l'algèbre de Boole aux circuits électriques.

A. Portes logiques

Avec l'évolution de la technologie, des composants plus versatiles que les circuits à relais ont ont été inventés, ce qui a donné naissance aux circuits logiques. On définit alors un ensemble de composants appelés **portes logiques**. Chaque porte correspond à une fonction logique précise, à laquelle on associe un symbole. Les portes élémentaires sont son représentées sur la figure 17. Si la porte possède deux entrées, on les note respectivement

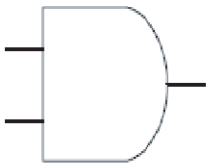
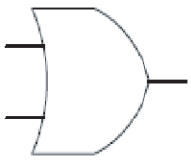
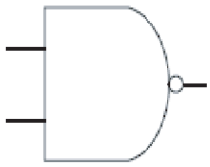
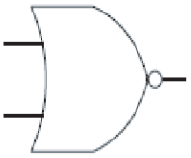
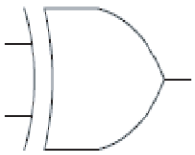
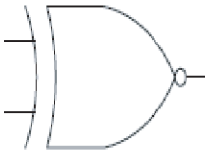
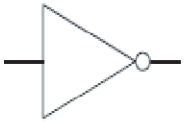
Operateurs logiques	Nom Français	Nom Anglais	Symbole	Table de vérité
A.B	ET	AND		A B F 0 0 0 0 1 0 1 0 0
A+B	OU	OR		A B F 0 0 0 0 1 1 1 1 1
$\overline{A.B}$	NONET	NAND		A B F 0 0 1 0 1 1 1 0 1 1 1 0
$\overline{A+B}$	NONOU	NOR		A B F 0 0 1 0 1 0 1 0 0 1 1 0
$A \oplus B$	OU exclusif	XOR		A B F 0 0 0 0 1 1 1 0 1 1 1 0
$\overline{A \oplus B} = A \otimes B$	NON OU exclusif	XNOR		A B F 0 0 1 0 1 0 1 0 0 1 1 1
$\overline{A}$	NON (inverseur)	NOT (inverter)		A F 0 1 1 0

Figure 17: Exemple des portes les plus élémentaires.

A et B. L'entrée quand elle est unique est notée A. La lettre F sur cette figure désigne la sortie.

Remarque: Il es important de remarque sur la colonne des symboles que certains sym-

boles ont un petit cercle à droite, juste avant la ligne de sortie, alors que d'autre symboles ne possèdent pas ce petit cercle. Le petit cercle représente l'opérateur $\neg$ (négation NON logique) de l'algèbre de Boole. Cet opérateur $\neg$ est appliqué sur tout le block entrant, par exemple, sur la ligne de **NON-OU** (**NOR**), nous avons deux entrées, A et B reliées par l'opérateur booléen $+$ (le **OU** (OR) logique) pour donner $A + B$. À la sortie, nous devons appliquer l'opérateur $\neg$ (négation NON logique), ce qui donne $\overline{A + B}$: c'est le NON-OU (NOR). Il convient alors de bien souligner que sur un symbole des portes logiques, le petit cercle sur une entrée ou une sortie signifie le NON logique, i.e., l'opérateur $\neg$ de l'algèbre de Boole. Notons aussi que sur la figure 17, deux nouveaux opérateurs sont introduits, $\oplus$ pour le XOR (OU exclusif) et $\otimes$ pour le XNOR (NON-OU exclusif). nous reviendrons sur ces deux opérateurs.

Il est à noté que la majorité des portes logiques sont décrits en anglais et c'est pour cela que nous avons indiqué sur la figure ci-dessus les noms Anglais parallèlement avec les noms Français des des différentes portes. Dans la suite de cette section, nous utiliserons soit les noms anglais, soit les noms Français. Nous utiliserons les portes logiques pour exprimer toutes fonction logique. Bien que toute fonction logique se réalise à l'aide de seulement les trois opérateurs logiques **ET, OU**, et **NON**, en termes de circuits logiques, on utilise plusieurs portes logiques, ce qui est due à deux raisons majeurs:

- La première est d'ordre technologique, tenant compte du fait que la réalisation d'une porte **ET** à l'aide de transistors présuppose l'existence d'une porte **NON-ET**, qui à son tour est inversée. La réciproque est tout aussi vraie pour la porte **OU** et la porte **NON-OU**. De la même façon, les portes XOR et XNOR sont très utiles et leur réalisation matérielle est plus simples que l'équivalent utilisant des portes ET, OU et NON.

- La seconde raison tient compte du fait que toute fonction logique peut être exprimée au moyen de NON-ET uniquement (respectivement, à l'aide de NON-OU uniquement).

Le passage d'une fonction logique à un circuit logique induit certaines modifications aux notions vues précédemment. Les variables d'une fonction logique deviennent les entrées du circuit, ce circuit donnant en sortie la valeur de la fonction logique suivant la valeur des entrées. On peut ainsi connecter des portes logiques les unes aux autres pour réaliser une fonction logique. À l'inverse, trouver la fonction logique réalisée par un circuit nous permettra de le manipuler en vue de simplifications éventuelles.

B. Inversion des entrées

En circuits logiques, on rencontre parfois des symboles tels que ceux représentés sur la figure 18 ci-dessous.

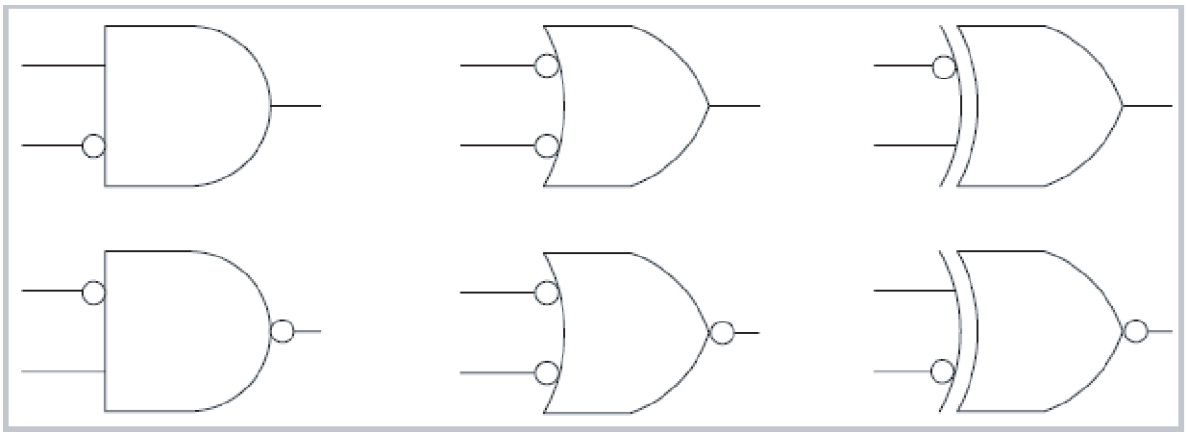


Figure 18: Inversion des entrées.

Il ne s'agit pas ici de nouvelles portes logiques, mais des portes logique de la figure ci-dessus où l'une ou les deux entrées ont été inversées (indiqué par la présence d'un cercle d'inversion). Par exemple, sur la première porte, on note une entrée directe, A et une entrée inversée (l'inversement étant indiqué par un petit cercle à l'entrée), $\overline{B}$. Puisqu'il s'agit ici du même symbole **ET** (**AND**) de la figure 17 (mais avec une entrée inversée), nous aurons à la sortie $A \cdot \overline{B}$. Si nous prenons la dernière porte de la figure 18, nous constatons qu'il s'agit du symbole **NON-OU** (**XNOR**) de la figure 17 (avant dernier symbole) avec une entrée inversée. Si nous désignons par A l'entrée directe, alors l'entrée inversée sera notée $\overline{B}$. En appliquant l'opératuer booléen + (OU (OR) exclusif logique) à l'entrée, nous trouvons $A \oplus \overline{B}$. À la sortie, on applique l'opérateur pour obtenir $\overline{A \oplus \overline{B}} = A \otimes \overline{B}$. De la même façon on traduit les autres symboles de la figure 18. Cette traduction est représentée sur la figure 19 ci-dessous.

C. Portes XOR et XNOR (OU exclusif et NON-OU exclusif)

Comme nous avons noté plus haut, outre les portes NON-ET et NON-OU, nous avons introduit les portes **XOR** et **XNOR** (voir Fig. 17). La formulation logique de la première (i.e., de **XOR (OU exclusif)**) correspond à un **OU** où les deux entrées ne peuvent être

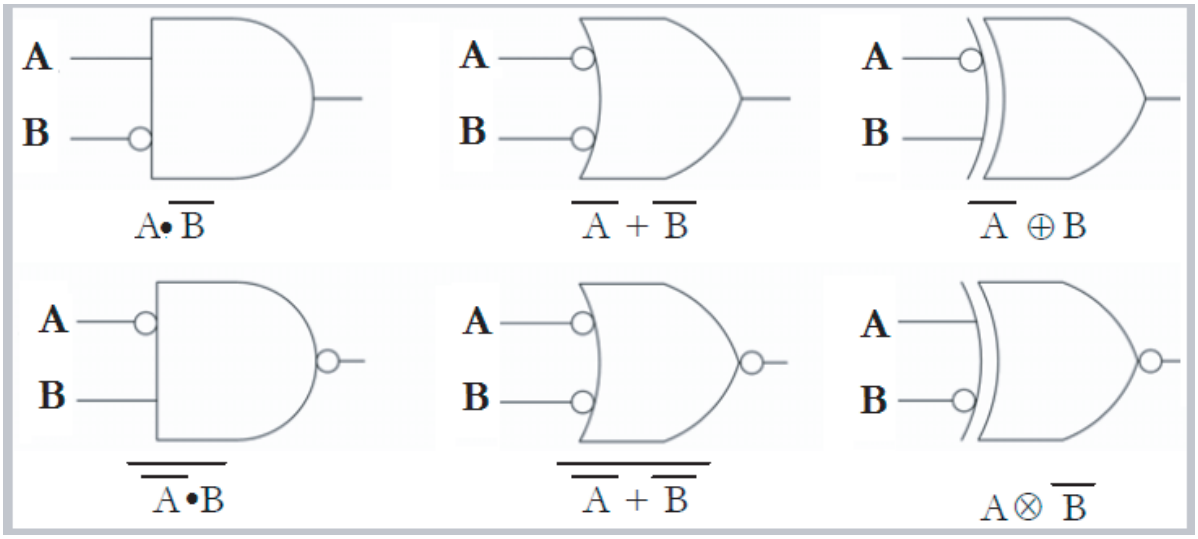


Figure 19: Correspondance des portes de la figure 18.

vraie en même temps (soit l'un, soit l'autre, mais pas les deux à la fois), alors que celle de la seconde (i.e., de XNOR (**NON-OU exclusif**)) est une équivalence logique ($\leftrightarrow$), l'inverse du XOR.

La fonction **XOR** est symbolisée par $\oplus$ et est donnée par l'une des expressions:

$$A \oplus B \overset{\text{déf}}{=} \overline{A} \cdot B + A \cdot \overline{B} \quad \text{ou} \quad A \oplus B \overset{\text{déf}}{=} (A + B) \cdot \left(\overline{A} + \overline{B}\right).$$

La fonction **XNOR**, symbolisée par $\otimes$, est donnée par l'une des expressions:

$$A \otimes B \overset{\text{déf}}{=} \overline{A} \cdot \overline{B} + A \cdot B \quad \text{ou} \quad A \otimes B \overset{\text{déf}}{=} \left(\overline{A} + B\right) \cdot \left(A + \overline{B}\right).$$

Prouvons que les deux expressions dans chacune des définitions de **XOR** et **XNOR** sont égales entre elles. Pour ce faire, nous utilisons la décomposition de shannon:

Pour montrer que $\overline{A} \cdot B + A \cdot \overline{B} = (A + B) \cdot \left(\overline{A} + \overline{B}\right)$, introduisons la fonction logique $f(A, B) = (A + B) \cdot \left(\overline{A} + \overline{B}\right)$. Selon la décomposition de Shannon, nous aurons

$$\begin{aligned} f(A, B) &= \overline{A} \cdot f(0, B) + A \cdot f(1, B) \\ &= \overline{A} \cdot \left[\overline{B} \cdot f(0, 0) + B \cdot f(0, 1)\right] + A \cdot \left[\overline{B} \cdot f(1, 0) + B \cdot f(1, 1)\right] \\ &= \overline{A} \cdot B + A \cdot \overline{B}, \end{aligned}$$

car $f(0, 0) = 0$, $f(0, 1) = 1$, $f(1, 0) = 1$, et $f(1, 1) = 0$. Ainsi, $(A + B) \cdot \left(\overline{A} + \overline{B}\right) = \overline{A} \cdot B + A \cdot \overline{B}$.

Pour démontrer l'égalité des deux expressions de $A \otimes B$, nous utilisons la fonction logique $f(A,B) = \left(\overline{A} + B\right) \cdot \left(A + \overline{B}\right)$. Alors, selon la décomposition de Shannon, on a

$$\begin{aligned} f(A,B) &= \overline{A} \cdot f(0,B) + A \cdot f(1,B) \\ &= \overline{A} \cdot \left[\overline{B} \cdot f(0,0) + B \cdot f(0,1)\right] + A \cdot \left[\overline{B} \cdot f(1,0) + B \cdot f(1,1)\right] \\ &= \overline{A} \cdot \overline{B} + A \cdot B, \end{aligned}$$

car $f(0,0) = 1$, $f(0,1) = 0$, $f(1,0) = 0$, et $f(1,1) = 1$. Ainsi, $\left(\overline{A} + B\right) \cdot \left(A + \overline{B}\right) = \overline{A} \cdot \overline{B} + A \cdot B$.

D. Portes à plusieurs entrées

À l'exception de l'inverseur, les portes logiques peuvent avoir plus de deux entrées. Il est alors important de comprendre comment s'exprime la fonction logique associée à des telles portes logiques, surtout si la sortie est inversée , une situation qui n'est pas toujours intuitif.

Dans le cas simple de portes non inversées (à trois entrées et plus), on peut recourir à l'axiome de l'associativité. Ainsi, nous aurons, disons pour trois portes A, B, et C,

AND $A \cdot B \cdot C = (A \cdot B) \cdot C = A \cdot (B \cdot C)$

OR $A + B + C = (A + B) + C = A + (B + C)$

XOR $A \oplus B \oplus C = (A \oplus B) \oplus C = A \oplus (B \oplus C)$

NON-OU $\overline{A + B + C} = \overline{(A + B) + C} = \overline{(A + (B + C))}$, ainsi de suite.

Dans le cas des portes inversées à plusieurs entrées, on maintient la cohérence de l'équivalence entre les portes logiques et l'algèbre de Boole en considérant que l'inversion est postérieure à l'expression logique qui la précède. Aussi aurons-nous la situation de la figure 20.

E. Notion de synthèse des circuits logiques

Comme nous avons mentionné plus haut, le passage d'une fonction logique à un circuit logique induit certaines modifications aux notions de l'algèbre de Boole. Les variables d'une

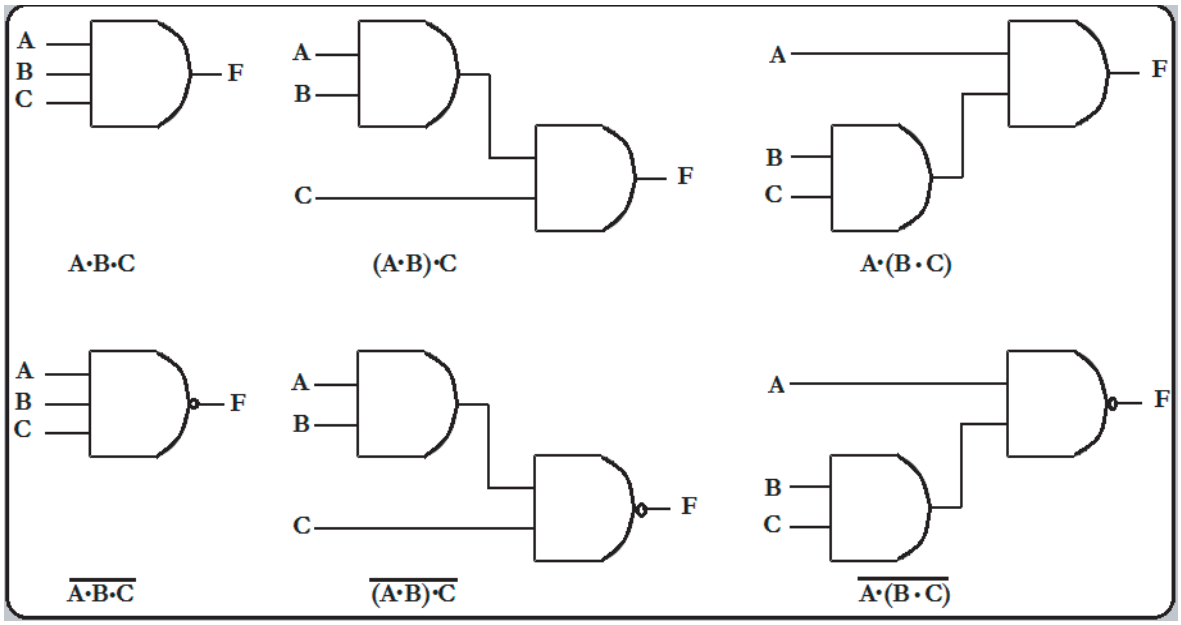


Figure 20: Portes à plusieurs entrées: **AND** (haut) et **NAND** (bas).

fonction logique deviennent les entrées du circuit, ce circuit donnant en sortie la valeur de la fonction logique suivant la valeur des entrées. Nous avons pu constater la chose lorsque nous considérions les portes logiques individuellement. Ainsi, il devient possible de connecter des portes logiques les unes aux autres pour **réaliser une fonction logique**; et de manière symétrique, trouver **la fonction logique réalisée** par un circuit nous permet de le manipuler en vue de simplifications éventuelles.

Pour mieux se fixer les idées, considerons la fonction logique F à trois variables logiques A, B et C, telle que F soit définie par l'équation :

$$F\left(A,B,C\right) = A \cdot B + B \cdot C + \overline{(C + A)}$$

Le circuit correspondant à cette fonction est illustré sur la figure 21.

Pour réaliser le circuit de la figure 21, on a dans un premier temps réalisé les portes associées respectivement à chacune des variables A, B, et C, et par la suite, on les connecte deux à deux suivant les termes $F_1 = A \cdot B$, $F_2 = B \cdot C$, et $F_3 = \overline{C + A}$ de la fonction F, qui enfin sont connectées les unes aux autres. Lorsque les fils se croisent, nous ajoutons un petit cercle plein rouge (•) pour indiquer une connexion. En l'absence de ce point rouge, cette connexion est inexistante. Généralement, nous mettons l'emphase de cette absence de connexion en ajoutant une légère surélévation à l'un des deux fils impliqués (⋔). On peut

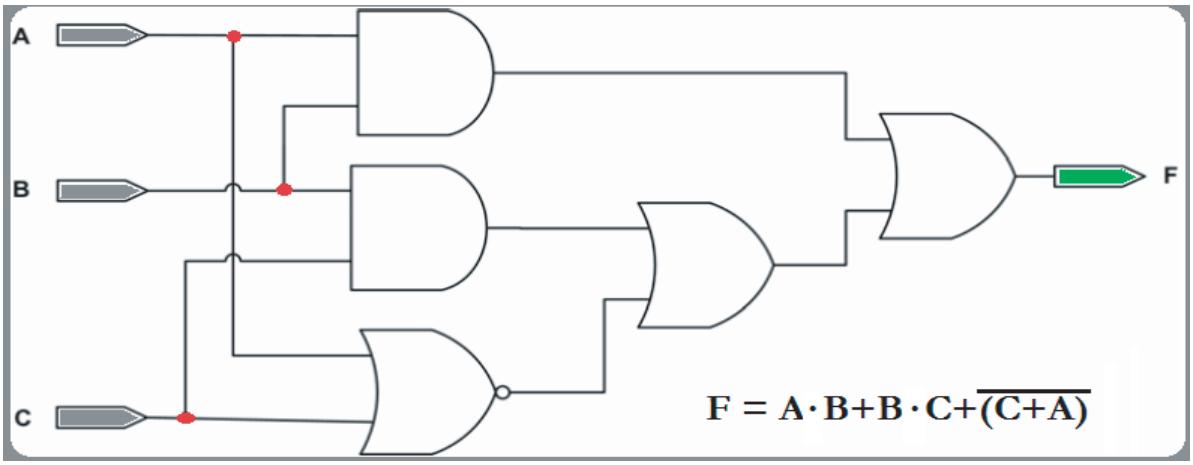


Figure 21: Synthèse des circuits logiques: Réalisation du circuit logique à partir de la fonction logique F.

simplifier ce circuit en faisant intervenir une porte à trois entrées, ce qui donne le circuit de la figure 22.

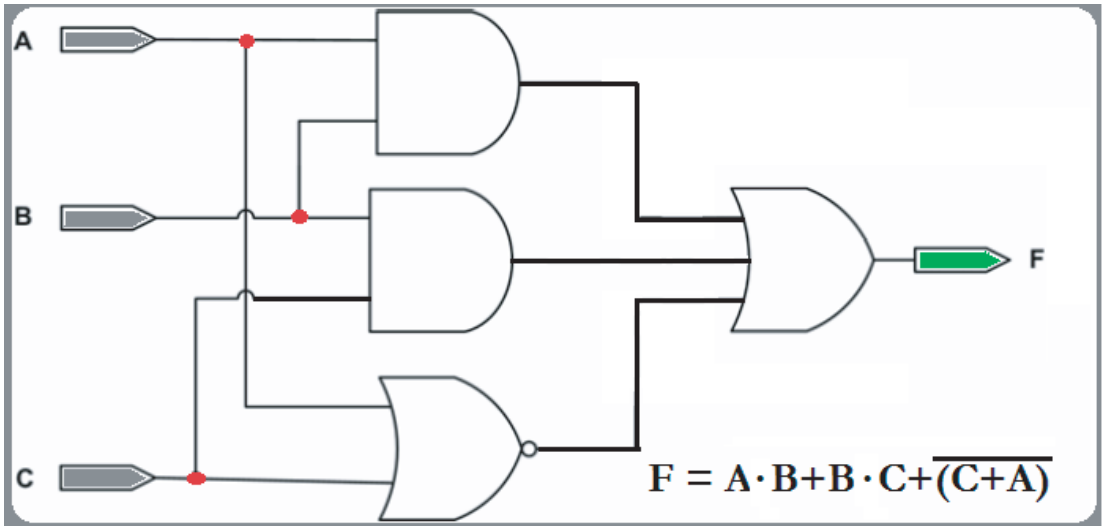


Figure 22: Synthèse des circuits logiques: Réalisation du circuit logique à partir de la fonction logique F. Version simplifée du circuit de la figure 21, un circuit obtenu à l'aide d'une porte avec trois entrées

On peut continuer la simplification de ce circuit pour obtenir celui de la figure 23.

Remarque: Sur les figures 21, 22, et 23, nous avons indiqué la même fonction donnée initiallement, i.e., $F(A,B,C) = A\cdot B + B\cdot C + \overline{C+A}$. En réalité les figures 22 et 23 peuvent correspondre à des fonctions différentes de celle de la figure 21, mais qui sont les formes

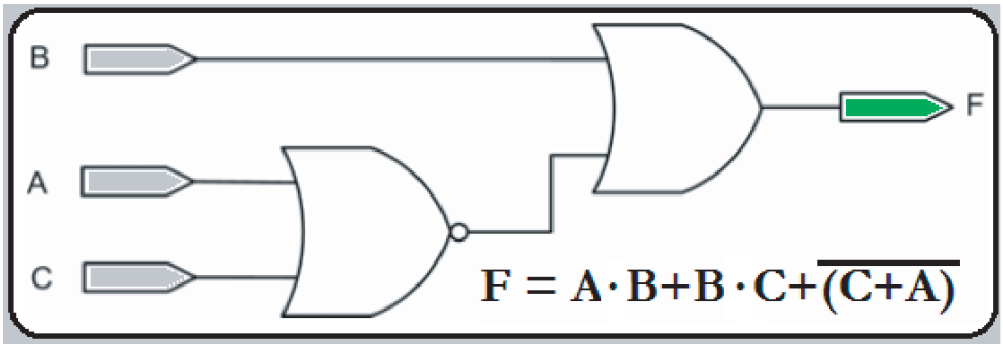


Figure 23: Version simplifiée du circuit de la figure 22.

réduites de la fonction $F(A,B,C) = A \cdot B + B \cdot C + \overline{C + A}$ de la figure 21. Les figures 22 et 23 correspondent respectivement aux fonctions logiques $F_1(A,B,C) = A \cdot B + B \cdot C + \overline{A + C}$ et $F_2(A,B,C) = B + \overline{A + C}$. On peut facilement montrer l'équivalence de ces trois circuits en montrant l'équivalence des trois fonctions y intervenant. Par exemple,

$F(A,B,C) = A \cdot B + B \cdot C + \overline{C + A} = B + \overline{C + A}$ (d'après le théorème sur l'absorption).

Il est plus facile de se servir la table devérité d'une fonction booléenne pour réaliser le circuit logique correspondant à l'expression booléenne. Le passage d'une fonction booléenne au circuit logique cprrespondant se réalise plus facilement quand on utilise la table de Karnaugh qui n'est autre chose que une forme compacte de représenter la table de vérité de la fonction booléenne.

XXIII. TABLE DE KARNAUGH

A. Description de la table de Karnaugh

Une table de Karnaugh est une façon compacte de représenter une table de vérité d'une fonction booléenne. C'est un tableau de 2^n cases, n étant le nombre de variables de la fonction logique (ici, 2^n est le nombres des mintermes de n variables). Les tables de Karnaugh permettent de simplifier facilement et méthodiquement des expressions booléennes comportant un nombre modéré de variables (max 8). Chaque case du tableau correspond à un des mintermes et par conséquent, représente une combinaison des entrées. Une case du tableau ne diffère de l'une de ses voisines que par une variable. Un '1' placé dans une case de la table de Karnaugh correspond à un **minterme** de la fonction. Un '0' placé dans une case de la

table de Karnaugh correspond à un **maxterme** de la fonction. Un développement suivant les "1" (somme des mintermes) donne la fonction correspondante à la table, alors qu'un reproupement suivant les "0" (somme des maxtermes) donne le NON ($\overline{F}$) de la fonction logique associée à la table.

Pour se fixer les idées, construisons la table de Karnaugh pour deux variables, trois variables, et quatre variables. On construit d'abord les tables de vérité donnant les codes de toute combinaison des variables devant intervenir dans le tableau de Karnaugh.

(i) Pour deux variables, a, b, nous construisons d'abord la table de vérité pour a et b (table à gauche) et par la suite, la table de Karnaugh de deux variables

a	b
1	0
0	1

Table de vérité

$a \diagdown b$	0	1
0	$\overline{a} \cdot \overline{b}$	$\overline{a} \cdot b$
1	$a \cdot \overline{b}$	$a \cdot b$

Table de Karnaugh à deux variables

(ii) Table de Karnaugh de trois variables. Dans cette table, nous mettons ab sur la ligne superieure et c sur la la colonne la plus à gauche. Puisque ab interviendra dans la table de Karnaugh, on construit d'abord la table de verité de la fonction $f = ab$

a	b	ab
0	0	00
0	1	01
1	0	10
1	1	11

Table de vérité

$c \diagdown ab$	00	01	11	10
0	$\overline{a} \cdot \overline{b} \cdot \overline{c}$	$\overline{a} \cdot b \cdot \overline{c}$	$a \cdot b \cdot \overline{c}$	$a \cdot \overline{b} \cdot \overline{c}$
1	$\overline{a} \cdot \overline{b} \cdot c$	$\overline{a} \cdot b \cdot c$	$a \cdot b \cdot c$	$a \cdot \overline{b} \cdot c$

Table de Karnaugh à trois variables

(iii) Table de Karnaugh à quatre variables. Pour cette tables, on aura aux entrée ab (ligne supérieure) et cd (colonne la plus à gauche). On peut aussi regrouper les variable en abc et

c

a	b	ab
0	0	00
0	1	01
1	0	10
1	1	11

c	d	cd
0	0	00
0	1	01
1	0	10
1	1	11

a	b	c	abc
1	1	1	111
1	1	0	110
1	0	1	101
1	0	0	100
0	1	1	011
0	1	0	010
0	0	1	001
0	0	0	000

$c \cdot d \diagdown a \cdot b$	00	01	10	11
00	$\overline{a} \cdot \overline{b} \cdot \overline{c} \cdot \overline{d}$	$\overline{a} \cdot b \cdot \overline{c} \cdot \overline{d}$	$a \cdot \overline{b} \cdot \overline{c} \cdot \overline{d}$	$a \cdot b \cdot \overline{c} \cdot \overline{d}$
01	$\overline{a} \cdot \overline{b} \cdot \overline{c} \cdot d$	$\overline{a} \cdot b \cdot \overline{c} \cdot d$	$a \cdot \overline{b} \cdot \overline{c} \cdot d$	$a \cdot b \cdot \overline{c} \cdot d$
10	$\overline{a} \cdot \overline{b} \cdot c \cdot \overline{d}$	$\overline{a} \cdot b \cdot c \cdot \overline{d}$	$a \cdot \overline{b} \cdot \overline{c} \cdot d$	$a \cdot b \cdot c \cdot \overline{d}$
11	$\overline{a} \cdot \overline{b} \cdot c \cdot d$	$\overline{a} \cdot b \cdot c \cdot d$	$a \cdot \overline{b} \cdot c \cdot d$	$a \cdot b \cdot c \cdot d$

Table de Karnaugh à quatre variables

en utilisant abc et c, on aura la table suivante

$c \diagdown abc$	000	001	010	011	100	101	110	111
0	$\overline{a} \cdot \overline{b} \cdot \overline{c} \cdot \overline{d}$	$\overline{a} \cdot \overline{b} \cdot \overline{c} \cdot d$	$\overline{a} \cdot b \cdot \overline{c} \cdot \overline{d}$	$\overline{a} \cdot b \cdot c \cdot \overline{d}$	$a \cdot \overline{b} \cdot \overline{c} \cdot \overline{d}$	$a \cdot \overline{b} \cdot c \cdot \overline{d}$	$a \cdot b \cdot \overline{c} \cdot \overline{d}$	$a \cdot b \cdot c \cdot \overline{d}$
1	$\overline{a} \cdot \overline{b} \cdot \overline{c} \cdot d$	$\overline{a} \cdot \overline{b} \cdot c \cdot d$	$\overline{a} \cdot b \cdot \overline{c} \cdot d$	$\overline{a} \cdot b \cdot c \cdot d$	$a \cdot \overline{b} \cdot \overline{c} \cdot d$	$a \cdot \overline{b} \cdot c \cdot d$	$a \cdot b \cdot \overline{c} \cdot d$	$a \cdot b \cdot c \cdot d$

Table de Karnaugh à quatre variables

B. Passage de la table de vérité au tableau de Karnaugh et réduction de l'équation logique aux formes canoniques

Une équation logique peut être représentée par une table de vérité ou un tableau de Karnaugh. En général, on déduit facilement la table de Karnaugh à partir de la table de vérité. Une fois la table de Karnaugh construite, sa lecture conduit aux formes canonique l'équation logique: Le développement de la table de Karnaugh suivant les 1 (somme des mintermes) conduit à la première forme canonique, alors que le développement suivant les 0 (somme des maxtermes) conduit à la deuxième forme canonique de l'expression logique.

Exemple 1: Écrire les tables de vérité et de Karnaugh de l'équation logique $F = a \cdot b + a \cdot \overline{b} \cdot c + \overline{b} \cdot c$, puis en dédure la première et la deuxième formes canoniques de F.

Solution:

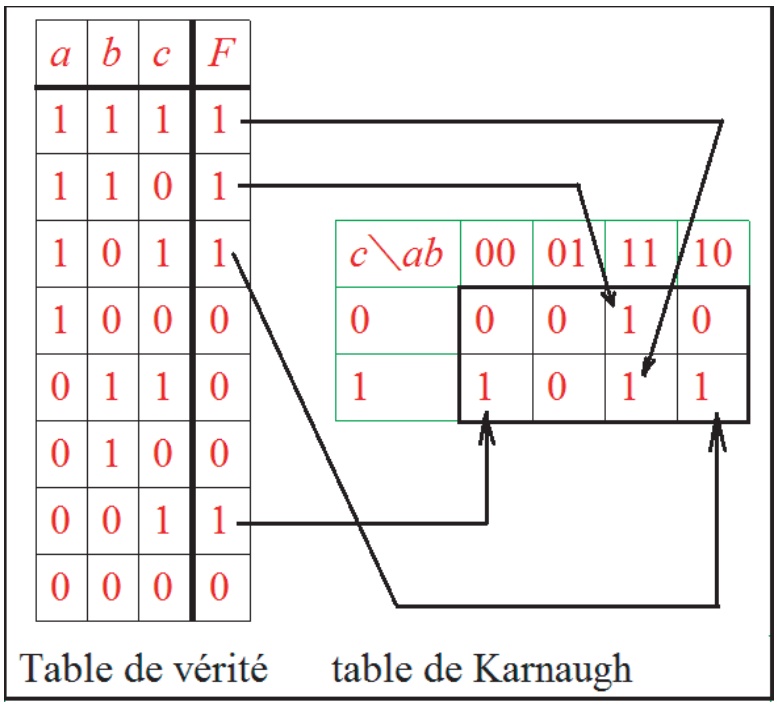


Figure 24: Comment obtenir une table de Karnaugh à partir de la table de vérité pour une équation logique donnée.

a	b	c	F
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

Table de vérité

$c \backslash ab$	00	01	11	10
0	0	0	1	0
1	1	0	1	1

table de Karnaugh

La correspondance entre la table de vérité de la fonction logique $F = a \cdot b + a \cdot \overline{b} \cdot c + \overline{b} \cdot c$

a	b	c	F
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

Table de vérité

$c \backslash ab$	00	01	11	10
0	0 $\bar{a}.\bar{b}.\bar{c}$	0 $\bar{a}.b.\bar{c}$	1 $a.b.\bar{c}$	0 $a.\bar{b}.\bar{c}$
1	1 $\bar{a}.\bar{b}.c$	0 $\bar{a}.b.c$	1 $a.b.c$	1 $a.\bar{b}.c$

table de Karnaugh

Figure 25: Comment obtenir une table de Karnaugh à partir de la table de vérité pour une équation logique donnée.

et la table de Karnaugh est montrée sur la figure 24. Cette figure montre commnt on peut obtenir la table de Karnaugh à partir de la table de vérité d'une fonction logique.

Utilisons la table de Karnaugh ainsi construite pour déterminer les formes canonique de la fonction F. La figure 25 montre la table de Karnaugh avec les mintermes correspondants. En prenant le développement suivant les 1 ou les 0, nous obtenons respectivement

$$\begin{aligned} F(a,b,c) &= \overline{a}\cdot\overline{b}\cdot c + a\cdot b\cdot c + a\cdot b\cdot\overline{c} + a\cdot\overline{b}\cdot c \\ \overline{F}(a,b,c) &= \overline{a}\cdot\overline{b}\cdot\overline{c} + \overline{a}\cdot b\cdot\overline{c} + \overline{a}\cdot b\cdot c + a\cdot\overline{b}\cdot\overline{c} \end{aligned}$$

En utilisant le théorème de de Morgan (i.e., $\overline{a+b} = \overline{a}\cdot\overline{b}$ et $\overline{a\cdot b} = \overline{a}+\overline{b}$), on trouve

$$\begin{aligned} F &= \overline{\overline{F}} = \overline{\overline{a}\cdot\overline{b}\cdot\overline{c} + \overline{a}\cdot b\cdot\overline{c} + \overline{a}\cdot b\cdot c + a\cdot\overline{b}\cdot\overline{c}} \\ &= \overline{\overline{a}\cdot\overline{b}\cdot\overline{c}}\cdot\overline{\overline{a}\cdot b\cdot\overline{c}}\cdot\overline{\overline{a}\cdot b\cdot c}\cdot\overline{a\cdot\overline{b}\cdot\overline{c}} \\ &= (a+b+c)\cdot\left(a+\overline{b}+c\right)\cdot\left(a+\overline{b}+\overline{c}\right)\cdot(\overline{a}+b+c) \end{aligned}$$

Ainsi, la table de Karnaugh nous donne les deux formes canoniques suivantes de la fonction

booléenne $F(a,b,c)$:

$$\begin{aligned} F(a,b,c) &= \overline{a}\cdot\overline{b}\cdot c + a\cdot b\cdot c + a\cdot b\cdot\overline{c} + a\cdot\overline{b}\cdot c \\ F(a,b,c) &= (a+b+c)\cdot\left(a+\overline{b}+c\right)\cdot\left(a+\overline{b}+\overline{c}\right)\cdot(\overline{a}+b+c)\,. \end{aligned}$$

Exemple 2: Écrire les formes canoniques de l'équation logique correspondante à la table de Karnaugh.

$cd \diagdown ab$	00	01	11	10
00	0	1	1	0
01	1	0	0	1
11	1	0	0	1
10	0	1	1	0

Solution: Les regroupements suivant les 1 et 0 donnent respectivement

$$\begin{aligned} F(a,b,c,d) &= \overline{a}\overline{b}\overline{c}d + \overline{a}\overline{b}cd + \overline{a}b\overline{c}\overline{d} + \overline{a}bcd + ab\overline{c}\overline{d} + abcd + a\overline{b}\overline{c}d + \overline{a}b\overline{c}\overline{d} \\ \overline{F}(a,b,c,d) &= \overline{a}\overline{b}\overline{c}\overline{d} + \overline{a}\overline{b}c\overline{d} + \overline{a}b\overline{c}d + \overline{a}bcd + ab\overline{c}d + abcd + a\overline{b}\overline{c}\overline{d} + a\overline{b}c\overline{d} \end{aligned}$$

Pour obtenir la deuxième forme canonique, nous utilisons l'axiome $F = \overline{\overline{F}}$:

$$\begin{aligned} F &= \overline{\overline{F}} = \overline{\overline{a}\overline{b}\overline{c}\overline{d} + \overline{a}\overline{b}c\overline{d} + \overline{a}b\overline{c}d + \overline{a}bcd + ab\overline{c}d + abcd + a\overline{b}\overline{c}\overline{d} + a\overline{b}c\overline{d}} \\ &= \overline{\overline{a}\overline{b}\overline{c}\overline{d}}\cdot\overline{\overline{a}\overline{b}c\overline{d}}\cdot\overline{\overline{a}b\overline{c}d}\cdot\overline{\overline{a}bcd}\cdot\overline{ab\overline{c}d}\cdot\overline{abcd}\cdot\overline{a\overline{b}\overline{c}\overline{d}}\cdot\overline{a\overline{b}c\overline{d}} \\ &= (a+b+c+d)\cdot(a+b+\overline{c}+d)\cdot\left(a+\overline{b}+c+\overline{d}\right) \\ &\quad\cdot\left(a+\overline{b}+\overline{c}+\overline{d}\right)\cdot\left(\overline{a}+\overline{b}+c+\overline{d}\right)\cdot\left(\overline{a}+\overline{b}+\overline{c}+\overline{d}\right) \\ &\quad\cdot(\overline{a}+b+c+d)\cdot(\overline{a}+b+\overline{c}+d) \end{aligned}$$

Ainsi, la deuxième forme canonique est

$$\begin{aligned} F &= (a+b+c+d)\cdot(a+b+\overline{c}+d)\cdot\left(a+\overline{b}+c+\overline{d}\right) \\ &\quad\cdot\left(a+\overline{b}+\overline{c}+\overline{d}\right)\cdot\left(\overline{a}+\overline{b}+c+\overline{d}\right)\cdot\left(\overline{a}+\overline{b}+\overline{c}+\overline{d}\right) \\ &\quad\cdot(\overline{a}+b+c+d)\cdot(\overline{a}+b+\overline{c}+d) \end{aligned}$$

Exemple 3: Soit l'équation logique $f(a,b,c) = a\cdot\overline{b}$.

(i) Ecrire la table de vérité de f, puis en déduire une table de Karnaugh.

(ii) Utiliser la table de Karnaugh pour trouver une première et une deuxième forme canonique de f.

Solution: (i) Écrivons la table de vérité de f et en déduisons une table de Karnaugh:

a	b	c	$f = a \cdot \overline{b}$
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

Table de vérité

$c \diagdown ab$	00	01	11	10
0	0	0	0	1
1	0	0	0	1

Table de Karnaugh

(ii) Déduisons de la table de Karnaugh les formes canonique de f. Un développement suivant les 1 et les 0 donne respectivement

$$\begin{aligned} f(a,b,c) &= a\overline{b}\overline{c} + a\overline{b}c \\ \overline{f}(a,b,c) &= \overline{a}\overline{b}\overline{c} + \overline{a}\overline{b}c + \overline{a}b\overline{c} + \overline{a}bc + ab\overline{c} + abc \end{aligned}$$

Alors

$$\begin{aligned} f(a,b,c) &= \overline{\overline{f}} = \overline{\overline{a}\overline{b}\overline{c} + \overline{a}\overline{b}c + \overline{a}b\overline{c} + \overline{a}bc + ab\overline{c} + abc} \\ &= \overline{\overline{a}\overline{b}\overline{c}}\,\overline{\overline{a}\overline{b}c}\,\overline{\overline{a}b\overline{c}}\,\overline{\overline{a}bc}\,\overline{ab\overline{c}}\,\overline{abc} \\ &= (a+b+c)(a+b+\overline{c})\left(a+\overline{b}+c\right)\left(a+\overline{b}+\overline{c}\right)\left(\overline{a}+\overline{b}+c\right)\left(\overline{a}+\overline{b}+\overline{c}\right), \end{aligned}$$

i.e.,

$$f(a,b,c) = (a+b+c)(a+b+\overline{c})\left(a+\overline{b}+c\right)\left(a+\overline{b}+\overline{c}\right)\left(\overline{a}+\overline{b}+c\right)\left(\overline{a}+\overline{b}+\overline{c}\right),$$

D'où la première et la deuxième formes canoniques suivantes

$$\begin{aligned} f(a,b,c) &= a\overline{b}\overline{c} + a\overline{b}c, \\ f(a,b,c) &= (a+b+c)(a+b+\overline{c})\left(a+\overline{b}+c\right)\left(a+\overline{b}+\overline{c}\right)\left(\overline{a}+\overline{b}+c\right)\left(\overline{a}+\overline{b}+\overline{c}\right). \end{aligned}$$

---

[1] R. CHILL, Logique et théorie des ensembles, Laboratoire de Mathématiques et Applications de Metz, Licence de Mathématiques, 1ère année, 1er semestre.

[2] C. BOULONNE, Notes de cours MAN : Axiomes et nombres, Licence de Mathématiques.

[3] AYRES, Frank Jr. Algèbre moderne, McGraw-Hill, 1987.

[4] MIGNOTTE, Maurice. Algèbre appliquée à l'informatique, Presses Univer. De France, 1987.

[5] VIAU, Denis. Les fondements de l'algèbre, Gaëtan Morin, 1994.

[6] AYRES, Frank Jr. Algèbre moderne, McGraw-Hill, 1987.

[7] TARSKI, Alfred. Introduction to logic and to the methodology and deductive sciences, Dover, 1995.

[8] JACQUES VÉLU, GENEVIÈVRE AVÉROUS, ISABELLE GIL, FRANÇOISE SANTI, Mathématiques pour l'informatique, Licence École d'ingénieurs, Dunod, Paris 2008.

[9] WIKIPEDIA, Implication (logique).

[10] WIKIPEDIA, Équivalence logique.

[11] WIKIPEDIA, Injection (mathématiques).

[12] S. DE BIÈVRE, Une invitation aux mathématiques, Novembre 2005.