Cours de maths pour l'info de S. Paños

FMdKdD
fmdkdd [à] free.fr

Université du Havre
Année 2008–2009

Table des matières

Chapitre 1

Structures

1.1 Relations d'équivalence et relations d'ordre

Définition 1.1. Soient A et B deux ensembles. On appelle produit cartésien de A par B, et on note $A \times B$, l'ensemble de toutes les paires ordonnées (a, b) où $a \in A$ et $b \in B$. Deux paires ordonnées de $A \times B$, (a, b) et (a', b') seront dites égales si et seulement si $a = a'$ et $b = b'$.

Soient $A_1, \ldots, A_n$ n ensembles. On appelle produit cartésien de $A_1, \ldots, A_n$ l'ensemble de tous les n-uplets ordonnés $(a_1, \ldots, a_n)$ où $\forall i \in \mathbb{N}_n^*, a_i \in A_i$.

Théorème 1.1. *Si* A *et* B *sont des ensembles finis ayant respectivement m et n éléments, alors* $A \times B$ *a mn éléments.*

Démonstration. Désignons par $a_1, \ldots, a_m$ les éléments de A et par $b_1, \ldots, b_n$ ceux de B. Alors :

$$A \times B = \left\{(a_i, b_j)/i \in \mathbb{N}_m^*, j \in \mathbb{N}_n^*\right\}$$

Nous pouvons ranger tous ces éléments dans un tableau de m lignes et n colonnes :

$$\begin{array}{c} (a_1, b_1)(a_1, b_2)\ldots(a_1, b_n) \\ (a_2, b_1)(a_2, b_2)\ldots(a_2, b_n) \\ \vdots \\ (a_m, b_1)(a_m, b_2)\ldots(a_m, b_n) \end{array}$$

Chaque ligne possède n éléments, donc le tableau est constitué de m lignes ayant chacune n éléments. Au total il y a donc mn éléments dans le tableau, c'est à dire dans $A \times B$. □

Remarque. Si pour tout $i \in \mathbb{N}_k^*$, A_i possède n_i éléments alors $A_1 \times \cdots \times A_k$ en possède $n_1 \times \cdots \times n_k$.

Définition 1.2. Soient $A_1, \ldots, A_n$ des ensembles non vides, $n \in \mathbb{N}^*$. On appelle relation n-aire sur la suite de domaines $A_1, \ldots, A_n$, toute partie R du produit cartésien $A_1 \times \cdots \times A_n$.

Lorsque $A_1 = A_2 = \cdots = A_n = A$ on dit que R est une relation n-aire sur A.

Remarques.

1. Une relation unaire ($n = 1$) sur A s'identifie à une partie de A. Par exemple : $\mathbb{N}^*$ est une relation unaire sur $\mathbb{Z}$.
2. Lorsque $n = 2$ on parle de relation binaire et au lieu de noter $(a_1, a_2) \in R$, on note $a_1 R a_2$.

Exemple. Considérons les trois ensembles suivants :
- Jour $= \{\text{lundi}, \text{mardi}, \ldots, \text{dimanche}\}$
- Heure $= \{0, 1, \ldots, 23\}$
- Mois $= \{\text{janvier}, \text{février}, \ldots, \text{décembre}\}$

La relation OUVERTURE_MAGASIN définie sur Jour $\times$ Heure $\times$ Mois par $(j, h, m) \in$ OUVERTURE_MAGASIN si et seulement si :

$$\begin{cases} j \in \{\text{lundi}, \text{mardi}, \ldots, \text{samedi}\} \\ 9 \leqslant h \leqslant 17 \\ m \in \text{Mois} \bigcap \complement_{\text{Mois}} \{\text{août}\} \end{cases}$$

est une relation ternaire.

Définition 1.3. Soient A un ensemble non vide et $\mathscr{A}$ l'ensemble des relations binaires sur l'ensemble A :

1. Si $\mathscr{R} \in \mathscr{A}$, on appelle complément de $\mathscr{R}$ et on note $\overline{\mathscr{R}}$ la relation binaire définie sur A par :

$$\forall x \in A, \forall y \in A, \quad (x, y) \in \overline{\mathscr{R}} \iff (x, y) \notin \mathscr{R}$$

2. Si $S \in \mathscr{A}$ et $T \in \mathscr{A}$, on appelle somme (ou union) de S et de T la relation binaire sur A notée $S + T$ définie par :

$$(x, y) \in S + T \iff (x, y) \in S \cup T$$

3. Si $S \in \mathscr{A}$ et $T \in \mathscr{A}$, on appelle produit (ou intersection) de S et de T la relation binaire sur A notée S.T et définie par :

$$(x, y) \in S.T \iff (x, y) \in S \cap T$$

Théorème 1.2. *Soient* A *un ensemble non vide,* R, S *et* T *des relations binaires sur* A*. Alors :*

1. $R + S = S + R$
2. $R.S = S.R$
3. $(R + S) + T = R + (S + T)$
4. $(R.S).T = R.(S.T)$
5. $R + (S.T) = (R + S)(R + T)$
6. $R(S + T) = R.S + R.T$
7. $R + \emptyset = R$
8. $R.A^2 = R$
9. $R + \bar{R} = A^2$
10. $R.\bar{R} = \emptyset$

Démonstration. Aux étudiants. □

Définition 1.4. Soit A un ensemble non vide et R une relation binaire sur A.

1. On dit que R est réflexive si et seulement si
$$\forall x \in A \quad xRx$$
2. On dit que R est symétrique si et seulement si
$$\forall x \in A, \forall y \in A \quad xRy \Longrightarrow yRx$$
3. On dit que R est antisymétrique si et seulement si
$$\forall x \in A, \forall y \in A \quad (xRy \text{ et } yRx) \Longrightarrow x = y$$
4. On dit que R est transitive si et seulement si
$$\forall x \in A, \forall y \in A, \forall z \in A \quad (xRy \text{ et } yRz) \Longrightarrow xRz$$

Remarque. Les propriétés de symétrie et d'antisymétrie ne sont pas opposées. L'égalité sur un ensemble A est à la fois symétrique et antisymétrique. C'est la seule relation binaire (avec ses restrictions) qui vérifie cette propriété.

Définition 1.5. Une relation binaire R sur un ensemble non vide A est une relation d'équivalence si et seulement si R est à la fois réflexive, symétrique et transitive.

Définition 1.6. Soient R une relation d'équivalence définie sur un ensemble non vide A et x un élément quelconque de A.

On appelle classe d'équivalence de x, et on note $\mathrm{cl}(x)$ (ou $\bar{x}$, $\dot{x}$ ou $[x]_{\mathrm{R}}$) l'ensemble des éléments y de A tels que $x\mathrm{R}y$ (ou $y\mathrm{R}x$ puisque R est symétrique). On dit, lorsqu'il est nécessaire de préciser la relation R, classe d'équivalence par rapport à R, ou encore classe d'équivalence modulo R (dans ce cas on note $x \equiv y \mod \mathrm{R}$).

On appelle ensemble quotient de A par R l'ensemble des classes d'équivalences distinctes modulo R.

Exemples.

1. $\mathrm{A} = \mathbb{N} \quad x\mathrm{R}y \iff x+y$ est pair :
   - $\forall x \in \mathbb{N} \quad x+x = 2x$ est pair donc $x\mathrm{R}x$,
   - $\forall x, y \in \mathbb{N} \quad x\mathrm{R}y \Rightarrow x+y$ est pair donc $y+x$ est pair également d'où $y\mathrm{R}x$,
   - $\forall x, y, z \in \mathbb{N}$ si $x\mathrm{R}y$ et $y\mathrm{R}z$ alors $x+y$ est pair et $y+z$ est pair, $x+y+y+z$ est pair d'où $x+z+2y-2y$ est encore pair donc $x+z$ est pair d'où $x\mathrm{R}z$.

   Quelle est la classe d'équivalence de 2008 ?

   $$[2008]_{\mathrm{R}} = \mathrm{cl}_{\mathrm{R}}(2008) = 2\mathbb{N}$$

   Quelle est la classe d'équivalence de 2009 ?

   $$[2009]_{\mathrm{R}} = 1 + 2\mathbb{N}$$

   Quel est l'ensemble quotient $\mathbb{N}/\mathrm{R}$?

   $$\mathbb{N}/\mathrm{R} = \{2\mathbb{N}, 1+2\mathbb{N}\} = \{\mathrm{cl}(2008), \mathrm{cl}(2009)\}$$

2. $\mathrm{A} = \mathbb{N}$ et $x\mathrm{R}y \iff x = y^2$
   - $2 \in \mathbb{N}$ mais $2 \neq 2^2$ donc $2 \not\mathrm{R} 2$ et R n'est pas réflexive
   - $2 \in \mathbb{N}, 4 \in \mathbb{N}$ on a $4\mathrm{R}2$ mais $2 \not\mathrm{R} 4$
   - $4, 16, 256 \in \mathbb{N}$ on a $4\mathrm{R}16$ et $16\mathrm{R}256$ mais $4 \not\mathrm{R} 256$

3. $\mathrm{A} = \{0,1\}$ et $x\mathrm{R}y \iff x = y^2$
   - $0 = 0^2$ et $1 = 1^2$ donc R est réflexive
   - D'après ce qui précède R est symétrique
   - De même R est transitive

   D'où R est une relation d'équivalence sur A.

   $$\mathrm{A}/\mathrm{R} = \{\{0\}, \{1\}\}$$

Théorème 1.3. *Soient* A *un ensemble non vide et* R *une relation d'équivalence sur* A *:*

1. *Si* $\mathrm{cl}(x)$ *est la classe d'équivalence d'un élément* x *quelconque de* A*,* $\mathrm{cl}(x) \neq \emptyset$.
2. *Si* $\mathrm{cl}(x)$ *et* $\mathrm{cl}(y)$ *sont deux classes d'équivalences distinctes de* A/R*, alors elles sont disjointes :*

$$\mathrm{cl}(x) \neq \mathrm{cl}(y) \Rightarrow \mathrm{cl}(x) \cap \mathrm{cl}(y) = \emptyset$$

3. $\mathrm{A} = \bigcup_{x \in \mathrm{A}} \mathrm{cl}(x)$.

Démonstration.

1. R étant réflexive, $x\mathrm{R}x$ donc $x \in \mathrm{cl}(x)$ et $\mathrm{cl}(x) \neq \emptyset$
2. Supposons $\mathrm{cl}(x) \neq \mathrm{cl}(y)$ c'est à dire : soit il y a un z de $\mathrm{cl}(x)$ qui n'est pas dans $\mathrm{cl}(y)$, soit il y a un $t \in \mathrm{cl}(y)$ qui n'est pas dans $\mathrm{cl}(x)$. Supposons qu'il existe $u \in \mathrm{cl}(x) \cap \mathrm{cl}(y)$ et que nous soyons dans la première situation : alors z et u sont dans $\mathrm{cl}(x)$ donc $z\mathrm{R}u$. Or $u \in \mathrm{cl}(y)$ donc $u\mathrm{R}y$. Par transitivité $z\mathrm{R}y$ et $z \in \mathrm{cl}(y)$ ce qui est contraire à l'hypothèse. Un raisonnement analogue appliqué à la seconde situation mène également à une contradiction.

   Notre hypothèse est donc fausse et son contraire est vrai. D'où $\mathrm{cl}(x) \cap \mathrm{cl}(y) = \emptyset$.
3. Soit x un élément quelconque de A. Alors $x \in \mathrm{cl}(x)$ et $x \in \bigcup_{x \in \mathrm{A}} \mathrm{cl}(x)$ donc $\mathrm{A} \subseteq \bigcup_{x \in \mathrm{A}} \mathrm{cl}(x)$. Réciproquement, si $x \in \bigcup_{x \in \mathrm{A}} \mathrm{cl}(x)$, alors $x \in \mathrm{A}$ car $\forall x \in \mathrm{A} \quad \mathrm{cl}(x) \subseteq \mathrm{A}$. Donc $\bigcup_{x \in \mathrm{A}} \mathrm{cl}(x) \subseteq \mathrm{A}$. D'où l'égalité.

□

Définition 1.7. On considère un ensemble non vide A et $(\mathrm{B}_i)_{i \in \mathrm{I}}$ une famille de parties de A telles que :

1. $\forall i \in \mathrm{I} \quad \mathrm{B}_i \neq \emptyset$
2. $\forall i \in \mathrm{I}, \forall j \in \mathrm{I} \quad i \neq j \Rightarrow \mathrm{B}_i \cap \mathrm{B}_j = \emptyset$
3. $\bigcup_{i \in \mathrm{I}} \mathrm{B}_i = \mathrm{A}$

Une telle famille de parties d'un ensemble s'appelle une partition de cet ensemble.

Théorème 1.4.

1. *Soit* A *un ensemble non vide et* R *une relation d'équivalence sur* A*. Les classes d'équivalence distinctes modulo* R *forment une partition de* A*.*

2. *Soit* A *un ensemble non vide et* $(B_i)_{i\in I}$ *une partition de* A. *Alors la relation* R *définie sur* A *par :*

$$\forall x \in A, \forall y \in A \quad xRy \iff \exists i \in I, x \in B_i \text{ et } y \in B_i$$

est une relation d'équivalence sur A.

Démonstration.

1. C'est une reformulation du théorème 1.3.
2. Soit x un élément quelconque de A. $(B_i)_{i\in I}$ forme une partition de A donc $\exists i \in I, x \in B_i$. Alors xRx et R est réflexive.
   Soient x et y deux éléments de A tels que xRy. Alors $\exists i \in I, x \in B_i$ et $y \in B_i$. D'où $y \in B_i$ et $x \in B_i$ et yRx. R est symétrique.
   Soient x, y et z dans A tels que xRy et yRz. Alors $\exists i \in I, x \in B_i$ et $y \in B_i$, et $\exists j \in I, y \in B_j$ et $z \in B_j$. Donc $y \in B_i \cap B_j$. On a $B_i \cap B_j \neq \emptyset$. Or les $(B_i)_{i\in I}$ forment une partition de A, donc $i \neq j \Rightarrow B_i \cap B_j = \emptyset$. Par conséquent $B_i \cap B_j \neq \emptyset \Rightarrow i = j$. D'où $B_i = B_j$ et R est transitive.
   Donc R est une relation d'équivalence sur A.

□

Exemples.

1. Soit $\mathbb{Q}$ l'ensemble des nombres rationnels et $\mathbb{Z}$ l'ensemble des nombres entiers relatifs. La relation R définie sur $\mathbb{Q}$ par :

$$\forall x, y \in \mathbb{Q} \quad xRy \iff x - y \in \mathbb{Z}$$

   est une relation d'équivalence sur $\mathbb{Q}$. En effet, $(\mathbb{Q}, +)$ est un groupe, $(\mathbb{Z}, +)$ est un sous groupe distingué de $(\mathbb{Q}, +)$ car $(\mathbb{Q}, +)$ est abélien, et nous avons vu en algèbre générale que les relations sur un groupe $(G, \cdot)$ de la forme :

$$xRy \iff xy^{-1} \in H$$

   où H est un sous groupe de G sont des relations d'équivalence compatibles avec la loi de G.
2. Soit $B_i = [i, i+1[\subset \mathbb{Q}$. Alors $(B_i)_{i\in\mathbb{Z}}$ forme une partition de $\mathbb{Q}$. Cette partition correspond à une relation d'équivalence définie par :

$$xRy \iff \text{INT}(x) = \text{INT}(y)$$

   où $\text{INT}(x)$ est le plus grand entier inférieur ou égal à x. Les classes sont les $(B_i)_{i\in\mathbb{Z}}$.

3. Soit S une relation binaire réflexive et transitive sur un ensemble non vide A. Alors la relation R définie sur A par :

$$x\mathrm{R}y \iff x\mathrm{S}y \text{ et } y\mathrm{S}x$$

est une relation d'équivalence sur A. Éxaminons un exemple précis.

On considère 7 étudiants de diverses universités françaises pouvant communiquer par l'intermédiaire d'un réseau informatique. Certains peuvent se contacter directement, et d'autres pas. Ces contacts s'opérant par la connaissance de l'adresse électronique de celui à qui on destine le message. Représentons par une matrice la relation T définie par :

$$x\mathrm{T}y \iff x \neq y \text{ et } x \text{ peut envoyer un message directement à } y$$

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
x_1	0	1	0	0	1	0	0
x_2	0	0	1	1	0	0	1
x_3	0	0	0	0	0	0	0
x_4	0	1	1	0	0	0	1
x_5	1	0	0	1	0	0	0
x_6	0	0	0	0	1	0	0
x_7	0	1	0	1	0	0	0

sur la ligne de x_i les 1 correspondent aux étudiants à qui x_i peut envoyer un message.

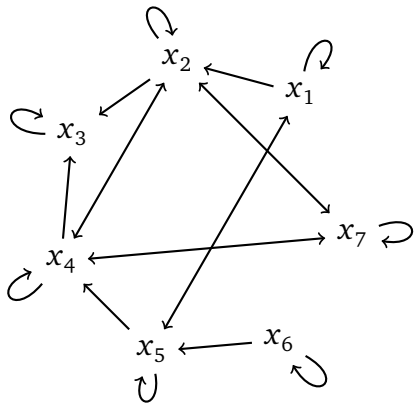
On définit à présent S par :

$$x\mathrm{S}y \iff (x = y) \text{ ou } (x \neq y \text{ et } x \text{ peut envoyer un message à } y \text{ directement, ou par plusieurs intermédiaires})$$

Alors S est réflexive et transitive. Si on définit R à présent comme suit, on obtient une relation d'équivalence :

$$(x\mathrm{R}y) \iff (x = y) \text{ ou } (x \neq y \text{ et aussi bien } x \text{ que } y \text{ peut entrer en contact avec l'autre, soit directement soit par un nombre fini d'intermédiaire})$$

Pour déterminer les classes d'équivalences, nous allons utiliser un graphe orienté. $x_i \to x_j$ signifiant que x_i peut contacter directement x_j.



Les classes d'équivalence sont caractérisées par les circuits fermés :

$$\{x_2, x_4, x_7\}, \{x_6\}, \{x_1, x_5\}, \{x_3\}$$

Définition 1.8. Soit R une relation binaire sur un ensemble non vide A. On dit que R est une relation d'ordre sur A, ou encore un ordre partiel sur A si et seulement si :

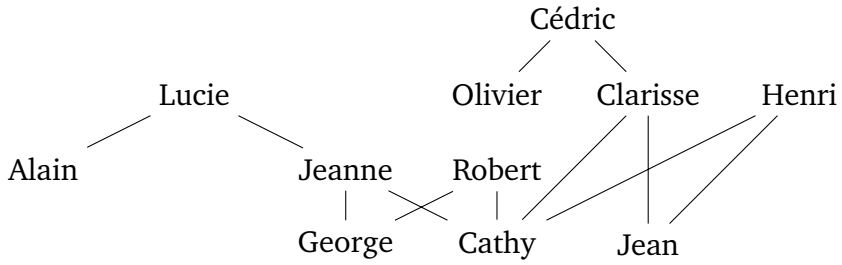
1. R est réflexive,
2. R est antisymétrique,
3. R est transitive.

Si de plus, deux éléments quelconques x et y de A sont tels que $x\mathrm{R}y$ ou $y\mathrm{R}x$, on dit que R est un ordre total. Tous les éléments de A sont ainsi comparables deux à deux. On dit aussi dans ce cas que R est une chaîne, et que A est totalement ordonné.

Exemples.

1. $(\mathbb{Z}, \leqslant)$
2. $(\mathscr{P}(\mathrm{E}), \subseteq)$
3. $(\mathbb{N}^*, |)$
4. George et Cathy se marient et ont deux enfants : Jeanne et Robert. Quelques années plus tard, George disparaît mystérieusement, et Cathy se remarie avec Jean peu de temps après. Très vite ils ont des jumeaux : Clarisse et Henri. Peu après, Jeanne épouse Alain et un bébé Lucie leur arrive un an après. Robert devient moine et ne créera donc pas de famille. Clarisse, elle, épouse Olivier et cette union est récompensée par l'arrivée du petit Cédric.

   La relation « être la même personne ou être l'ancêtre de » est une relation d'ordre sur $\{$George, Cathy, Jean, Clarisse, Henri, Jeanne, Robert, Olivier, Cédric$\}$. Son diagramme de Hasse est le suivant :



Théorème 1.5. *Soit* R *une relation d'ordre sur un ensemble non vide* A*. Alors la relation* R^{-1} *définie sur* A *par :*

$$\forall x, y \in \mathrm{A} \quad x\mathrm{R}^{-1}y \iff y\mathrm{R}x$$

est aussi un ordre sur A*.*

Démonstration. Soit $x \in \mathrm{A}$, $x\mathrm{R}x \Rightarrow x\mathrm{R}^{-1}x$ et R^{-1} est réflexive.

$\forall x, y \in \mathrm{A}$, $x\mathrm{R}^{-1}y$ et $y\mathrm{R}^{-1}x \Rightarrow y\mathrm{R}x$ et $x\mathrm{R}y$. Comme R est antisymétrique, $x = y$ et R^{-1} est antisymétrique.

$\forall x, y, z \in \mathrm{A}$, $x\mathrm{R}^{-1}y$ et $y\mathrm{R}^{-1}z \Rightarrow y\mathrm{R}x$ et $z\mathrm{R}y$ d'où, comme R est transitive, $z\mathrm{R}x$ et donc $x\mathrm{R}^{-1}z$. Donc R^{-1} est transitive.

R^{-1} est une relation d'ordre sur A. □

Définition 1.9. Soient $(\mathrm{A}, \leqslant)$ un ensemble ordonné et B une partie de A.

- On dit que $x \in \mathrm{A}$ est un minorant de B si $\forall y \in \mathrm{B} \quad x \leqslant y$
- On dit que $x \in \mathrm{A}$ est un majorant de B si $\forall y \in \mathrm{B} \quad y \leqslant x$
- On appelle borne inférieure de B (ou infimum de B), le plus grand des minorants de B s'il existe. On le note inf(B).
- On appelle borne supérieure de B (ou supremum de B), le plus petit des majorants de B s'il existe. On le note sup(B).
- On dit que l'élément m de B est un élément minimal de B, si :

$$\forall x \in \mathrm{B} \quad x \leqslant m \Rightarrow x = m$$

- On dit que l'élément M de B est un élément maximal de B, si :

$$\forall x \in \mathrm{B} \quad \mathrm{M} \leqslant x \Rightarrow \mathrm{M} = x$$

- On dit que l'élément μ de B est l'élément minimum de B (ou le plus petit élément de B) si :

$$\forall x \in \mathrm{B} \quad \mu \leqslant x$$

  On le note min(B).

– On dit que l'élément ν de B est l'élément maximum de B (ou le plus grand élément de B) si :

$$\forall x \in \mathrm{B} \quad x \leqslant \nu$$

On le note max(B).

– On dit que l'élément x de A est un élément prédécesseur de l'élément y de A si :

$$x \neq y, x \leqslant y \text{ et } \forall z \in \mathrm{A} \quad x \overline{\leqslant} z \text{ ou } z \overline{\leqslant} y$$

– On dit que l'élément x de A est un élément successeur de l'élément y de A si :

$$x \neq y, y \leqslant x \text{ et } \forall z \in \mathrm{A} \quad y \overline{\leqslant} z \text{ ou } z \overline{\leqslant} x$$

Théorème 1.6. *Soient* (A, R) *et* (B, S) *deux ensembles ordonnés.*

1. *La relation* T *définie sur le produit cartésien* $\mathrm{A} \times \mathrm{B}$ *par :*

$$(a, b)\mathrm{T}(c, d) \iff (a\mathrm{R}c \text{ et } b\mathrm{S}d)$$

est une relation d'ordre sur $\mathrm{A} \times \mathrm{B}$ *appellée ordre produit.*

2. *La relation* L *définie sur le produit cartésien* $\mathrm{A} \times \mathrm{B}$ *par :*

$$(a, b)\mathrm{L}(c, d) \iff [(a \neq c \text{ et } a\mathrm{R}c) \text{ ou } (a = c \text{ et } b\mathrm{S}d)]$$

est une relation d'ordre sur $\mathrm{A} \times \mathrm{B}$ *appelée ordre lexicographique.*

Démonstration.

1. Soit (a, b) un élément quelconque de $\mathrm{A} \times \mathrm{B}$.

$$\left.\begin{array}{c} \mathrm{R} \text{ est réflexive donc } a\mathrm{R}a \\ \mathrm{S} \text{ est réflexive donc } b\mathrm{S}b \end{array}\right\} \Rightarrow a\mathrm{R}a \text{ et } b\mathrm{S}b$$

c'est à dire $(a, b)\mathrm{T}(a, b)$.

Supposons que $(a, b)\mathrm{T}(c, d)$ et $(c, d)\mathrm{T}(a, b)$. Alors :

$$(a\mathrm{R}c \text{ et } b\mathrm{S}d) \text{ et } (c\mathrm{R}a \text{ et } d\mathrm{S}b)$$

d'où $(a\mathrm{R}c$ et $c\mathrm{R}a)$ et $(b\mathrm{S}d$ et $d\mathrm{S}b)$. R et S étant antisymétriques, on a $a = c$ et $b = d$.

Supposons que l'on ait $(a, b)\mathrm{T}(c, d)$ et $(c, d)\mathrm{T}(e, f)$. Alors :

$$(a\mathrm{R}c \text{ et } b\mathrm{S}d) \text{ et } (c\mathrm{R}e \text{ et } d\mathrm{S}f)$$

d'où :

$$(a\mathrm{R}c \text{ et } c\mathrm{R}e) \text{ et } (b\mathrm{S}d \text{ et } d\mathrm{S}f)$$

R et S étant transitives, on en déduit que $a\mathrm{R}e$ et $b\mathrm{S}f$, c'est à dire : $(a, b)\mathrm{T}(e, f)$.

T est bien une relation d'ordre.

2. Soit (a,b) un élément quelconque de A × B. S étant réflexive, on a $a = a$ et bSb d'où $(a,b)\mathrm{L}(a,b)$ et L est réflexive.
   Soient (a,b) et (c,d) deux éléments de A × B tels que $(a,b)\mathrm{L}(c,d)$ et $(c,d)\mathrm{L}(a,b)$. Alors :

$$\begin{aligned}&[(a \neq c \text{ et } a\mathrm{R}c) \text{ ou } (a = c \text{ et } bSd)]\\ \text{et } &[(c \neq a \text{ et } c\mathrm{R}a) \text{ ou } (c = a \text{ et } dSb)]\end{aligned}$$

   – si $a \neq c$ alors $a\mathrm{R}c$ et $c\mathrm{R}a$. Comme R est antisymétrique $a = c$. Absurde.
   – $a = c$ alors bSd et dSb. Comme S est antisymétrique $b = d$.
   D'où $(a,b) = (c,d)$ et L est antisymétrique.
   Soient $(a,b),(c,d)$ et (f,g) tels que :

$$(a,b)\mathrm{L}(c,d) \text{ et } (c,d)\mathrm{L}(f,g)$$

   Alors :

$$\begin{aligned}&[(a \neq c \text{ et } a\mathrm{R}c) \text{ ou } (a = c \text{ et } bSd)]\\ \text{et } &\big[(c \neq f \text{ et } c\mathrm{R}f) \text{ ou } (c = f \text{ et } dSg)\big]\end{aligned}$$

   – si $a = c$ alors bSd, et si $a = f$ alors dSg d'où bSg et $(a,b)\mathrm{L}(f,g)$. Si $a \neq f$ on a $a\mathrm{R}f$ et $(a,b)\mathrm{L}(f,g)$.
   – $a \neq c$ alors $a\mathrm{R}c$: si $c = f$ alors $a\mathrm{R}f$ et $(a,b)\mathrm{L}(f,g)$. Si $c \neq f$, $c\mathrm{R}f$ donc $a\mathrm{R}f$ et $(a,b)\mathrm{L}(f,g)$.
   Donc L est transitive et est une relation d'ordre sur A × B.

□

Remarque. L'ordre lexicographique s'étend sans problèmes à un produit cartésien de n ensembles ordonnés $\mathrm{A}_1,\ldots,\mathrm{A}_n$. On a :

$$(a_1,a_2,\ldots,a_n) \leqslant (b_1,b_2,\ldots,b_n)$$

si et seulement si l'une des conditions suivantes est satisfaite :

1. $a_1 \leqslant b_1$
2. $(a_1 = b_1)$ et $(a_2 \leqslant b_2)$
3. $(a_1 = b_1)$ et $(a_2 = b_2)$ et $(a_3 \leqslant b_3)$

⋮ ⋮

n. $(a_1 = b_1)$ et $(a_2 = b_2)$ et … et $(a_{n-1} = b_{n-1})$ et $(a_n \leqslant b_n)$.

Exemple. L'ordre du dictionnaire. Soit $A = \{a, b, \ldots, z\}$ l'alphabet habituel et A^n l'ensemble des n-uplets de lettres de l'alphabet. Si le n-uplet $(a, x, y, \ldots, k)$ est réecrit $axy\ldots k$ on obtient bien un mot de n lettres.

L'ordre lexicographique sur A^n est simplement l'ordre alphabétique : pour $n = 5$ on a bien :

$$\begin{aligned} \text{mille} &\leqslant \text{pelle} \\ \text{malle} &\leqslant \text{mille} \\ \text{trace} &\leqslant \text{tract} \end{aligned}$$

Considérons $A^* = \bigcup_{n\in\mathbb{N}} A^n$: c'est l'ensemble de tous les mots (suite finie de symboles) que l'on peut former avec l'alphabet A. À l'aide d'une loi de composition interne nommée « concaténation » on peut définir un ordre sur A^* :

$$\text{si } u, v \in A^* \quad u \leqslant v \iff \exists w \in A^*, u.w = v$$

À l'aide de cet ordre partiel, on peut définir sur A^* un ordre total $\preccurlyeq$ par :

$$u \preccurlyeq v \iff \begin{cases} u \leqslant v \\ \exists w, u', v' \in A^*, \exists x, y \in A \text{ tels que} \\ u = wxu', v = wyv', x \neq y \text{ et } x \leqslant y \end{cases}$$

On reconnaît là l'ordre du dictionnaire.

Définition 1.10. Soient $(A_1, \leqslant_1)$ et $(A_2, \leqslant_2)$ deux ensembles ordonnés. On appelle morphisme d'ordre entre A_1 et A_2 toute application f de A_1 dans A_2 telle que :

$$\forall x \in A_1 \forall y \in A_1 \quad x \leqslant_1 y \iff f(x) \leqslant_2 f(y)$$

On appelle aussi ces morphismes des « fonctions croissantes ». On appelle isomorphisme d'ordre entre $(A_1, \leqslant_1)$ et $(A_2, \leqslant_2)$ tout morphisme d'ordre bijectif. On appelle type d'ordre la classe de tous les ensembles ordonnés isomorphes à un même ensemble ordonné.

Définition 1.11. Soit $(A, \leqslant)$ un ensemble ordonné. On dit que $(A, \leqslant)$ est un treillis si pour toute paire $\{a, b\}$ d'éléments de A il existe $\inf\{a, b\}$ et $\sup\{a, b\}$.

Notation. Dans un treillis $(A, \leqslant)$, $\inf\{a, b\}$ se note $a \wedge b$ et $\sup\{a, b\}$ se note $a \vee b$.

Exemples.

1. Si E est un ensemble non vide, $(\mathscr{P}(E), \subseteq)$ est un treillis :

$$\forall A, B \in \mathscr{P}(E) \quad A \vee B = A \cup B \quad A \wedge B = A \cap B$$

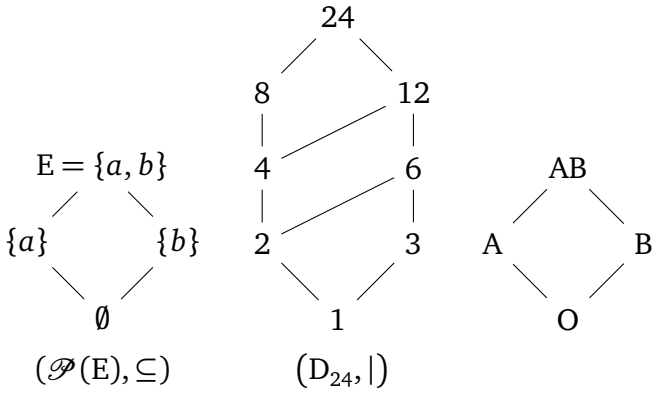
2. Soit D_{24} l'ensemble des diviseurs de 24 dans $\mathbb{N}$ ordonnés par la relation « a divise b » :

$$\forall a, b \in D_{24} \quad a \vee b = \text{ppcm}(a, b) \quad \text{et} \quad a \wedge b = \text{pgcd}(a, b)$$

3. Soit $E = \{O, A, B, AB\}$ l'ensemble des groupes sanguins ordonné par la relation « x peut donner du sang à y ». C'est un treillis :

$$x \wedge y : \text{ le groupe donneur à } x \text{ et à } y$$
$$x \vee y : \text{ le groupe receveur de } x \text{ et de } y$$

On peut associer un diagramme de Hasse à chaque treillis :



$(\mathscr{P}(E), \subseteq)$ $\quad$ $(D_{24}, |)$

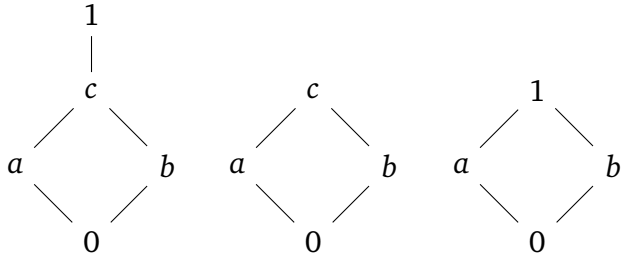
4. Tout ensemble totalement ordonné est un treillis :

$$a \vee b = \max(a, b) \quad \text{et} \quad a \wedge b = \min(a, b)$$

Définition 1.12. Soit B une partie d'un treillis $(A, \leqslant)$. On dit que B est un sous treillis de A si et seulement si, pour tous x et y de B, $x \wedge y$ et $x \vee y$ sont dans B.

Remarque. Toute partie d'un treillis qui est elle même un treillis pour la restriction de l'ordre du treillis, n'est pas forcément un sous treillis du treillis initial.

Exemple.



$(A, \leqslant)$ $\quad$ $B = \{a, b, c, 0\}$ $\quad$ $C = \{1, a, b, 0\}$

$(A, \leqslant)$ est un treillis, B est un treillis et un sous treillis de A, et C est un treillis mais pas un sous treillis de A.

Définition 1.13.

1. Soient $(A_1, \leqslant_1)$ et $(A_2, \leqslant_2)$ deux treillis. On dit qu'une fonction f de A_1 dans A_2 est un $\wedge$-morphisme si :
$$\forall x \in A_1, \forall y \in A_1 \quad f(x \wedge y) = f(x) \wedge f(y)$$
2. On dit que f est un $\vee$-morphime si :
$$\forall x \in A_1, \forall y \in A_1 \quad f(x \vee y) = f(x) \vee f(y)$$
3. On dira que f est un morphisme de treillis si f est à la fois un $\wedge$-morphisme et un $\vee$-morphisme. Si de plus f est bijective, on parle d'isomorphisme de treillis.

Remarque. Un morphisme de treillis est un morphisme d'ordre, mais la réciproque est fausse.

Théorème 1.7. *Soient $(A_1, \leqslant_1)$ et $(A_2, \leqslant_2)$ deux ensembles ordonnés de même type. Si l'un est un treillis, il en est de même de l'autre et les deux treillis sont isomorphes.*

Démonstration. Par hypothèse, il existe une bijection f de A_1 dans A_2 telle que :
$$\forall x \in A_1, \forall y \in A_1 \quad x \leqslant_1 y \Rightarrow f(x) \leqslant_2 f(y)$$
On peut faire la preuve en supposant que A_1 est le treillis sans diminuer sa généralité.

A_1 étant un treillis, x et y étant deux éléments de A_1, $x \wedge y$ existe. Nous allons montrer que $f(x) \wedge f(y)$ existe et que $f(x \wedge y) = f(x) \wedge f(y)$.

1. $f(x \wedge y)$ est un minorant de $\{f(x), f(y)\}$:
$$x \wedge y \leqslant_1 x \Rightarrow f(x \wedge y) \leqslant_2 f(x)$$
$$x \wedge y \leqslant_1 y \Rightarrow f(x \wedge y) \leqslant_2 f(y)$$
2. Soit m un minorant de la partie $\{f(x), f(y)\}$ dans A_2. Alors $m \leqslant_2 f(x)$ et $m \leqslant_2 f(y)$. f étant bijective, m admet un antécédent dans A_1, z et $f(z) = m$. Alors $z \leqslant_1 x$ (sinon $m = f(z) > f(x)$, contraire à l'hypothèse), et $z \leqslant_1 y$. D'où z est un minorant de $\{x, y\}$ donc $z \leqslant x \wedge y$ (qui est le plus grand des minorants). D'où :
$$f(z) \leqslant_2 f(x \wedge y)$$
$$m \leqslant_2 f(x \wedge y)$$
Donc $f(x \wedge y)$ est le plus grand des minorants de $\{f(x), f(y)\}$.

On montre de même que $f(x \vee y) = f(x) \vee f(y)$. □

Définition 1.14. Soit $(A, \leqslant)$ un treillis.

1. On dit que $(A, \leqslant)$ est borné s'il admet un plus petit et un plus grand élément (généralement on les note 0 et 1).
2. On dit que $(A, \leqslant)$ est complet si toute partie non vide de A admet une borne supérieure et une borne inférieure dans A.
3. Si $(A, \leqslant)$ est un treillis borné et $a \in A$, on dit que a' est un complément de a si $a \wedge a' = 0$ et $a \vee a' = 1$.
4. On dit que $(A, \leqslant)$ est un treillis complémenté si chaque élément de A possède un complément.

Définition 1.15. Soit $(A, \leqslant)$ un ensemble ordonné.

1. On dit que A satisfait à la condition de chaîne ascendante, ou encore que A est noetherien, si toute suite ordonnée $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n \leqslant \ldots$ d'éléments de A est stationnaire à partir d'un certain rang :
$$\exists k \in \mathbb{N}^* \quad a_k = a_{k+1} = \cdots = a_n = \ldots$$
2. On dit que A satisfait à la condition de chaîne descendante, ou encore que A est artinien si toute suite ordonnée $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n \geqslant \ldots$ d'éléments de A est stationnaire à partir d'un certain rang :
$$\exists k \in \mathbb{N}^* \quad a_k = a_{k+1} = \cdots = a_n = \ldots$$

Théorème 1.8.

1. *Soit* $(A, \leqslant)$ *un ensemble noetherien. Alors toute partie non vide de* A *admet au moins un élément maximal.*
2. *Soit* $(A, \leqslant)$ *un ensemble artinien. Alors toute partie non vide de* A *admet au moins un élément minimal.*

Démonstration.

1. Soient B une partie non vide de A et a_1 un élément de B.
   – si a_1 est maximal, c'est fini. Sinon, il existe $a_2 \in B$ tel que $a_1 \leqslant a_2$ et $a_1 \neq a_2$.
   – Si a_2 est maximal, c'est fini. Sinon, il existe $a_3 \in B$ tel que $a_1 \leqslant a_2 \leqslant a_3$ et $a_2 \neq a_3 \neq a_1$.

   Au bout d'un nombre fini d'opérations de ce type, on aboutit à un élément maximal dans B, sinon B, donc A, contiendrait une suite infinie strictement croissante et A ne serait pas noetherien.

2. Aux étudiants.

□

Remarque. Si $(A, \leqslant)$ est un ensemble ordonné tel que toute partie non vide possède un élément maximal, alors A est noetherien : s'il ne l'était pas, il contiendrait une suite infinie croissante, donc une partie sans élément maximal.

De même, si toute partie non vide de A contient un élément minimal, A est artinien.

Exemples.

1. $(\mathbb{N}, |)$ est artinien mais pas noetherien.
2. Si E est un ensemble infini, $(\mathscr{P}(E), \subseteq)$ n'est ni noetherien, ni artinien.

Théorème 1.9. *Tout treillis à la fois noetherien et artinien est complet.*

Démonstration. Soit $(T, \leqslant)$ un treillis noetherien et artinien. Montrons que A, partie non vide quelconque de T, possède une borne inférieure.

Soit a_0 un élément de A. Si a_0 est un minorant de A, alors a_0 est un minimum de A et $\inf(A) = a_0$. Sinon, il existe $a_1 \in A$ tel que $a_1 \wedge a_0 < a_0$: si $a_1 \wedge a_0$ est un minorant de A, alors $\inf(A) = a_1 \wedge a_0$ car tout minorant y de A vérifie $y \leqslant a_0$ et $y \leqslant a_1$ donc on a $y \leqslant a_1 \wedge a_0$, d'où $a_1 \wedge a_0$ est le plus grand des minorants de A. Sinon, si $a_1 \wedge a_0$ n'est pas un minorant de A, il existe $a_2 \in A$ tel que $a_0 \wedge a_1 \wedge a_2 \leqslant a_0 \wedge a_1 < a_0 \ldots$. A étant artinien, ce procédé aboutit en un nombre fini d'étapes, mettant en évidence $\inf(A)$.

Une démonstration analogue nous donne $\sup(A)$. □

Théorème 1.10. *Tout treillis fini est complet.*

Démonstration. Soit $T = \{a_1, \ldots, a_n\}$ un treillis. Soit $A = \{a_{i_1}, \ldots, a_{i_k}\}$ une partie non vide de T. Alors :

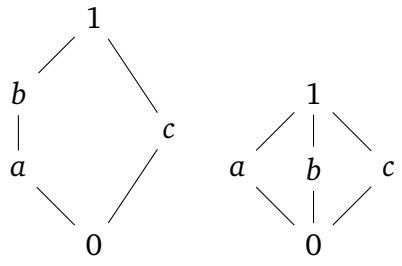
$$\inf(A) = a_{i_1} \wedge a_{i_2} \wedge \cdots \wedge a_{i_k}$$
$$\sup(A) = a_{i_1} \vee a_{i_2} \vee \cdots \vee a_{i_k}$$

□

Définition 1.16. Soit $(T, \leqslant)$ un treillis. On dit qu'il est modulaire si :

$$\forall x, y, z \in T \quad x \leqslant z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$$

Exemples.



Treillis K Treillis N

Le treillis K n'est pas modulaire, car $a \leqslant b$ mais :

$$a \vee (c \wedge b) = a \vee 0 = a$$
$$(a \vee c) \wedge b = 1 \wedge b = b$$

Le treillis N est modulaire : on peut tout de suite remarquer que la définition est automatiquement vérifiée si deux des trois élément x, y, z sont égaux. De même si l'un des éléments est égal à 0 ou à 1. Il ne reste à vérifier que la cas où $\{x, y, z\} = \{a, b, c\}$. Or, ces éléments n'étant pas comparables, $x \leqslant z$ sera faux et l'implication sera vraie.

Remarques.

1. Tout sous treillis d'un treillis modulaire est modulaire.
2. Dans un treillis quelconque, l'inégalité modulaire est toujours observée :

$$\forall x, y, z \in \mathrm{T} \quad x \leqslant z \Rightarrow x \vee (y \wedge z) \leqslant (x \vee y) \wedge z$$

3. Les treillis N et K de l'exemple ci-dessus sont complémentés :
   – Dans K, a et b sont tous deux compléments de c.
   – Dans N, chacun des éléments a, b, c est complément des deux autres.

Théorème 1.11. *Un treillis* $(\mathrm{T}, \leqslant)$ *est modulaire si et seulement si quelques soient* a, b, c *dans* T *:*

$$[(a \leqslant b) \textit{ et } (a \wedge c = b \wedge c) \textit{ et } (a \vee c = b \vee c)] \Rightarrow a = b$$

Démonstration. Supposons que $a, b, c \in \mathrm{T}$ et que :

$$(a \leqslant b) \text{ et } (a \wedge c = b \wedge c) \text{ et } (a \vee c = b \vee c)$$

Alors si T est modulaire :

$$\begin{aligned} a &= a \vee (c \wedge a) \\ &= a \vee (c \wedge b) \quad \text{(hypothèse)} \\ &= (a \vee c) \wedge b \quad \text{(T modulaire)} \\ &= (b \vee c) \wedge b \quad \text{(hypothèse)} \\ &= b \end{aligned}$$

Réciproquement, supposons que T ne soit pas modulaire. Montrons que l'on peut trouver dans T des éléments a, b, c tels que a et b soient comparables et distincts et $a \wedge c = b \wedge c$ et $a \vee c = b \vee c$.

T n'étant pas modulaire, il existe des éléments x, y, z tels que $x \leqslant z$ et

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

D'après la remarque 2 précédente, on a $x \vee (y \wedge z) < (x \vee y) \wedge z$. Posons $a = x \vee (y \wedge z)$, $b = (x \vee y) \wedge z$ et $c = y$. Alors on a :

1. $a < b$
2. $$\begin{aligned} a \wedge c &= \big(x \vee (y \wedge z)\big) \wedge y \geqslant \big(x \vee (y \wedge z)\big) \wedge (y \wedge z) = (y \wedge z) \\ b \wedge c &= \big((x \vee y) \wedge z\big) \wedge y \leqslant (y \wedge z) \quad \text{car } y \wedge z \leqslant y \leqslant x \vee y \end{aligned}$$

   D'où $a \wedge c \geqslant b \wedge c$. Or $a < b$, donc $a \wedge c \leqslant b \wedge c$. D'où l'égalité $a \wedge c = b \wedge c$.
3. $$\begin{aligned} a \vee c &= \big(x \vee (y \wedge z)\big) \vee y \geqslant x \vee y \quad \text{car } y \wedge z \leqslant y \leqslant x \vee y \\ b \vee c &= \big((x \vee y) \wedge z\big) \vee y \leqslant \big((x \vee y) \wedge z\big) \vee (x \vee y) = (x \vee y) \end{aligned}$$

   d'où $a \vee c \geqslant b \vee c$. Mais $a < b$ donc $a \vee c \leqslant b \vee c$. D'où l'égalité $a \vee c = b \vee c$.

□

Corollaire 1.1. *Un treillis* T *est modulaire si et seulement si* T *n'admet pas de sous treillis du type* K *de l'exemple plus haut.*

Démonstration. Si T est modulaire, tout ses sous treillis sont modulaires ; K ne l'étant pas, il ne peut être isomorphe à un sous treillis de T.

Si T n'est pas modulaire, il existe a, b, c dans T tels que $a \leqslant b$ et $a \wedge c = b \wedge c$ et $a \vee c = b \vee c$. Alors les éléments $a \wedge c, a, b, c$ et $b \wedge c$ forment un sous treillis de T du type K. □

Définition 1.17. Soit $(T, \leqslant)$ un treillis. On dit que T est distributif si :

$$\forall x, y, z \in T \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{1.1}$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \tag{1.2}$$

Remarques.

1. On peut montrer que (1.1) $\Rightarrow$ (1.2).
2. Toute chaîne est un treillis distributif.
3. Tout sous treillis d'un treillis distributif est distributif.

Théorème 1.12. *Tout treillis distributif est modulaire.*

Démonstration. $\forall x, y, z \in T$ treillis distributif. Si $x \leqslant z$ alors :

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) && \text{car T est distributif} \\ &= (x \vee y) \wedge z && (x \leqslant z) \end{aligned}$$

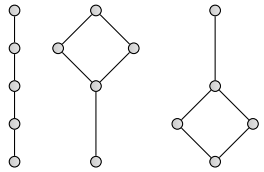
□

Exemples.

1. Pour tout ensemble E, $(\mathscr{P}(E), \subseteq)$ est un treillis distributif.
2. Le treillis K n'est ni distributif, ni modulaire.
3. N est modulaire, mais n'est pas distributif :

$$\begin{aligned} a \wedge (b \vee c) &= a \wedge 1 = a \\ (a \wedge b) \vee (a \wedge c) &= 0 \vee 0 = 0 \end{aligned}$$

4. Les seuls treillis distributifs à cinq éléments sont :



Théorème 1.13. *Un treillis* $(T, \leqslant)$ *est distributif si et seulement si :*

$$\forall a, b, c \in T \quad [(a \wedge c = b \wedge c) \text{ et } (a \vee c = b \vee c)] \Rightarrow (a = b)$$

Démonstration. Supposons $(T, \leqslant)$ distributif, a, b, c quelconques dans T tels que :

$$a \wedge c = b \wedge c \quad \text{et} \quad a \vee c = b \vee c$$

Alors :

$$\begin{aligned} a = a \wedge (a \vee c) &= a \wedge (b \vee c) \\ &= (a \wedge b) \vee (a \wedge c) \\ &= (b \wedge a) \vee (b \wedge c) \\ &= b \wedge (a \vee c) \\ &= b \wedge (b \vee c) \\ &= b \end{aligned}$$

Réciproquement, soit T un treillis tel que :

$$\forall a, b, c \in \mathrm{T} \quad [(a \vee c) = (b \vee c) \text{ et } (a \wedge c) = (b \wedge c)] \Rightarrow a = b$$

Remarquons que le treillis T est modulaire d'après le théorème 1.11. Soient x, y, z des éléments quelconques de T. Posons :

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

Alors :

$$\begin{aligned} a \wedge c &= \big((x \wedge y) \vee z\big) \wedge (x \vee y) \wedge y \\ &= \big((x \wedge y) \vee z\big) \wedge y \quad \text{car } y \leqslant x \vee y \\ &= (x \wedge y) \vee (z \wedge y) \quad \text{car } x \wedge y \leqslant y \text{ et T modulaire} \end{aligned}$$

De même, on a :

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

D'autre part :

$$a \vee c = (x \wedge y) \vee \big(z \wedge (x \vee y)\big) \vee y = b \vee c$$

D'après l'hypothèse de départ, $a = b$. Donc $a \wedge x = b \wedge x$. Or :

$$\begin{aligned} a \wedge x &= \big((x \wedge y) \vee y\big) \wedge (x \vee y) \wedge x \\ &= \big((x \wedge y) \vee z\big) \wedge x \quad \text{car } x \leqslant x \vee y \\ &= (x \wedge y) \vee (z \wedge x) \quad \text{car } x \wedge y \leqslant x \text{ et T modulaire} \\ b \wedge x &= (y \vee z) \wedge \big((y \wedge z) \vee x\big) \wedge x \\ &= (y \vee z) \wedge x \end{aligned}$$

Donc $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ et T est distributif. □

Théorème 1.14. *Un treillis est distributif s'il n'admet aucun sous treillis de type* K *et aucun sous treillis de type* N.

Démonstration. Si T est distributif, ses sous treillis le sont aussi ; K et N ne l'étant pas, T ne peut contenir de sous treillis de ce type.

Réciproquement, si T est non distributif, on sait qu'il existe a, b, c tels que $a \wedge c = b \wedge c$, $a \vee c = b \vee c$ et $a \neq b$.

- Si a et b sont comparables, on peut mettre en évidence un sous treillis de type K (corollaire du théorème 1.11).
- Si a et b ne sont pas comparables, on peut montrer, en exploitant le fait que T est modulaire, que T contient un sous treillis de type N.

□

Théorème 1.15. *Dans un treillis distributif complémenté, chaque élément possède un unique complément.*

Démonstration. Si a' et a'' sont des compléments de a, alors :

$$a \wedge a' = 0 = a \wedge a'' \text{ et } a \vee a' = 1 = a \vee a''$$

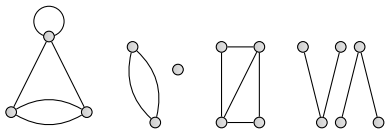
Comme T est distributif, le théorème 1.13 dit que $a' = a''$. □

1.2 Graphes et arbres

Définition 1.18. Un graphe c'est un triplet ordonné (S, A, f), où :

- S est un ensemble non vide, de cardinal fini, dont les éléments sont appelés sommets, ou nœuds,
- A est un ensemble fini dont les éléments sont appelés arêtes, ou côtés, ou arcs,
- f est une fonction qui à toute arête a associe une paire non ordonnée de sommets appelés extrémités de A.

Exemples.



(a) (b) (c) (d) (e) (f)

Remarques. 1. et  sont le même graphe.

2. Les arêtes peuvent se couper en des points qui ne sont pas des sommets.
3. La paire de sommets affectés à chaque arête par f n'est pas forcément constituée de deux sommets distincts.

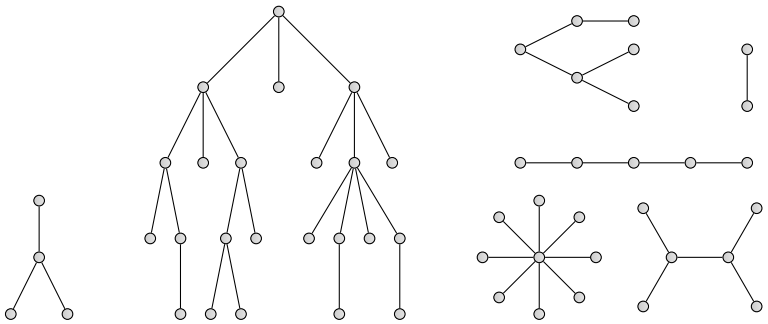
Définition 1.19.
- Deux sommets d'un graphe sont dits adjacents s'ils sont extrémités d'une même arête.
- Une boucle est une arête dont les deux extrémités sont un seul et même sommet.
- Deux arcs sont dits parallèles s'ils ont les mêmes extrémités. Un ensemble d'arcs parallèles de mêmes extrémités est appelé un arc multiple, ou une arête multiple.
- Un graphe simple est un graphe sans boucle, ni arête multiple.
- On dit qu'un nœud est isolé s'il n'est adjacent à aucun autre sommet.
- Le degré d'un nœud est le nombre d'arêtes arrivant à ce nœud.
- Un graphe est dit complet si deux nœuds distincts sont toujours adjacents quelques soient ces deux nœuds.
- Un chemin du nœud n_0 au nœud n_k est une suite n_0, a_0, n_1, a_1, …, n_{k-1}, a_{k-1}, n_k de nœuds et d'arêtes où : $\forall i \in \mathbb{N}_{k-1}$ n_i et n_{i+1} sont les extrémités de a_i. La longueur d'un chemin est le nombre d'arête qu'il contient.
- Un graphe est dit connexe si, quelque soit le couple de sommets choisis dans le graphe, il y a toujours un chemin de l'un vers l'autre.
- Un cycle, ou circuit simple, dans un graphe est un chemin qui relie un sommet à lui même, où aucun arc n'apparaît plus d'une fois et aucun sommet autre que n_0 n'y apparaît plus d'une fois.
- Un graphe sans cycle est appelé acyclique.

Remarque. Un graphe acyclique est simple, mais la réciproque est fausse.

Définition 1.20. Un arbre est un graphe acyclique et connexe.

Remarque. Un arbre n'a ni arêtes multiples, ni boucles.

Exemples.



(1) (2) (3)

(1) et (2) sont des arbres, mais (3) est une forêt.

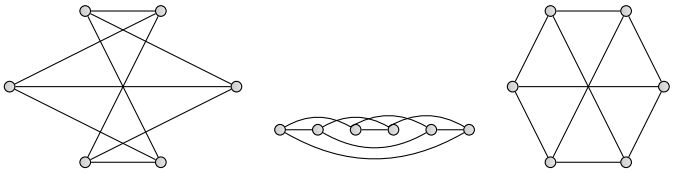
Définition 1.21.

1. Les sommets d'un arbre sont appelés des nœuds, et les arêtes des branches.
2. Un nœud de degré 1 est appelé une feuille.
3. Tout nœud d'un arbre peut être désigné par le terme « racine ».
4. Tout nœud autre que la racine ou qu'une feuille est un nœud de branche.
5. Un ensemble d'arbres disjoints est appelé une forêt.

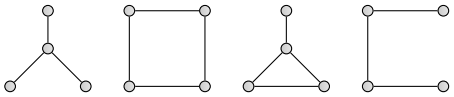
Définition 1.22.

1. On dira que deux graphes $G = (S, A, f)$ et $G' = (S', A', f')$ sont isomorphes si et seulement s'il existe une bijection φ de S dans S' telle que :
$$\forall x, y \in S \quad (x, y) \in \mathrm{Im}\, f \Rightarrow (\varphi(x), \varphi(y)) \in \mathrm{Im}\, f'$$
C'est à dire que tout couple d'images d'éléments de S correspond à une arête de G'.
2. Un graphe est dit planaire si et seulement s'il est isomorphe à un graphe tracé sur un plan sans que ses arêtes se coupent en dehors des sommets.
3. Soit G un graphe planaire. On appelle région planaire, ou face, de G toute partie F du plan possédant la propriété suivante : $\forall x, y \in F$ on peut tracer une courbe allant de x à y sans traverser une arête de G. Une arête d'un graphe G sera une arête frontière si tout segment qui la traverse contient des points dans plus d'une face de G.

Exemples. 1. Les graphes suivants sont isomorphes :



2. Quelque soit le choix d'une paire parmi ces graphes, les graphes choisis ne sont pas isomorphes.



Théorème 1.16 (Théorème d'Euler)**.** *Soit* G *un graphe planaire connexe ayant s sommets et a arêtes. Alors toute représentation planaire de* G *(dessin de* G *sans croisement d'arêtes hors des sommets) découpe le plan en f faces où* $f = a - s + 2$.

Démonstration. Supposons que la relation ci-dessus ne soit pas vérifiée pour un certain graphe planaire connexe G. Alors l'ensemble A des valeurs de a, où a est le nombre d'arêtes d'un graphe planaire connexe pour lequel le théorème d'Euler n'est pas vérifié, n'est pas vide. $A \subset \mathbb{N}, A \neq \emptyset$ donc A possède un plus petit élément m.

Tous les graphes planaires connexes pour lesquels le nombre d'arêtes est plus petit que m vérifient donc le théorème d'Euler. Il existe au moins un graphe ayant m arêtes, G, et tel que $f - m + s \neq 2$. Considérons une arête $\{a, b\}$ de G. Deux cas :

- Si $\{a, b\}$ est une arête frontière de G, soit G_1 le graphe obtenu en effaçant l'arête $\{a, b\}$ mais en gardant les sommets a et b dans G_1. Alors G_1 est planaire car G l'est, connexe car $\{a, b\}$ étant une arête frontière, c'est une arête d'un cycle de G. Soient f_1, a_1, s_1 les nombres de faces, d'arêtes et de sommets de G_1. Alors :

$$s_1 = s, \quad a_1 = m - 1, \quad f_1 = f - 1$$

  Comme $a_1 < m$, l'équation d'Euler s'applique à G_1 :

$$\begin{aligned} f_1 - a_1 + s_1 &= 2 \\ (f-1) - (m-1) + s &= 2 \\ f - m + s &= 2 \end{aligned}$$

  Ce qui contredit notre choix de G.
- Si $\{a, b\}$ n'est pas une arête frontière. Alors le retrait de l'arête $\{a, b\}$ sépare G en deux graphes planaires G_2 et G_3, chacun d'entre eux étant

connexe et ayant moins de m arêtes. D'après la définition de m, chacun des deux graphes G_2 et G_3 vérifie la relation :

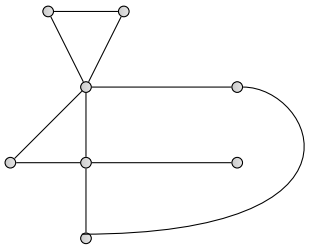
$$\begin{aligned} f_2 - a_2 + s_2 &= 2 \\ f_3 - a_3 + s_3 &= 2 \\ (f_2 + f_3) - (a_2 + a_3) + (s_2 + s_3) &= 4 \end{aligned}$$

Or $s = s_2 + s_3$ car G_2 et G_3 sont deux graphes disjoints contenant tous les sommets de G ; $m - 1 = a_2 + a_3$ car G_2 et G_3 sont disjoints et contiennent toutes les arêtes de G sauf $\{a, b\}$; $f + 1 = f_2 + f_3$ car on compte deux fois la face non bornée, une fois avec G_2 et une fois avec G_3. D'où :

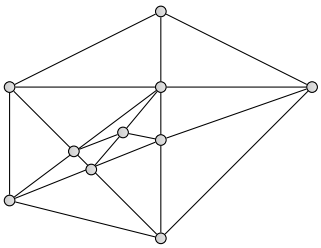
$$\begin{aligned} 4 &= (f_2 + f_3) - (a_2 + a_3) + (s_2 + s_3) = (f + 1) - (m - 1) + s \\ &= f - m + s + 2 \end{aligned}$$

D'où $f - m + s = 2$: contradiction.
L'hypothèse par laquelle la relation d'Euler pourrait ne pas être vérifiée n'aboutit qu'a des contradictions. Donc son contraire est vrai. □

Exemples.



$f = 4$, $a = 10$, $s = 8$
$4 - 10 + 8 = 2$



$f = 14$, $a = 22$, $s = 10$
$14 - 22 + 10 = 2$

Remarques.

1. On peut généraliser le théorème aux graphes planaires sans qu'ils soient connexes : si c est le nombre de composantes connexes du graphe :

$$f - a + s = c + 1$$

2. Appliqué aux arbres, qui ne possèdent pas de circuits et donc pas de faces autre que la face externe, d'où $f = 1$, la formule d'Euler devient :

$$\begin{aligned} 1 - a + s &= 2 \\ s - a &= 1 \\ a &= s - 1 \end{aligned}$$

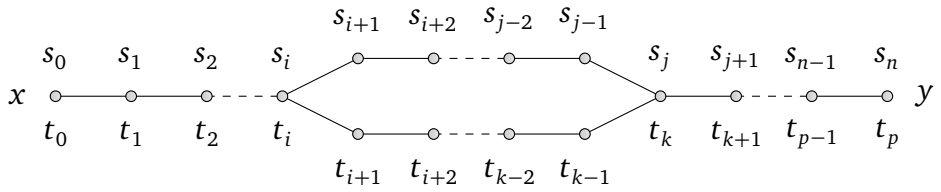
Théorème 1.17. *Soit* T *un arbre avec au moins* 2 *sommets, alors :*

1. *Pour chaque paire* (x, y) *de sommets de* T*, il y a un chemin unique dans* T *qui relie* x *à* y*.*
2. *Le graphe obtenu à partir de* T *en ôtant une arête quelconque a deux composantes connexes dont chacune est un arbre.*
3. *Si* F *est une forêt, dont le nombre total d'arêtes est* a*, le nombre total de sommets est* s *et le nombre total d'arbres est* c*, alors :*

$$a = s - c$$

Démonstration. 1. Tout arbre étant un graphe connexe, pour chaque paire de sommets (x, y) il existe un chemin dans T qui relie x à y.

Supposons que pour un couple de sommets (x, y) donné, il y ait deux chemins reliant x à y. Puisqu'il n'y a ni arêtes multiples, ni boucles dans un arbre, on peut représenter un chemin par une suite de sommets uniquement. Désignons par $x = s_0, s_1, \ldots, s_n = y$ et $x = t_0, t_1, \ldots, t_p = y$ nos deux chemins.



Soit i le plus petit indice tel que $s_{i+1} \neq t_{i+1}$. Puisque les chemins se terminent en y, ils vont se croiser à nouveau. Soit j le plus petit indice tel que $j > i$ et $s_j = t_k$ pour un certain k.

Alors s_i, s_{i+1}, …, s_{j-1}, s_j, t_{k-1}, …, t_{i+1}, t_i est un cycle dans T, ce qui contredit la structure d'arbre de T. Donc pour tout couple (x, y) de sommets de T, il existe un chemin unique qui relie x à y.

2. Soient s et t deux sommets adjacents de T. Désignons par st l'unique branche joignant s à t. Si $\mathrm{T} = (\mathrm{N}, \mathrm{B}, f)$, soit $\mathrm{T}' = (\mathrm{N}, \mathrm{B} \setminus \{st\}, g)$ où $g = f_{|(\mathrm{B}\setminus\{st\})}$.

Soit N_1 l'ensemble des nœuds x de T pour lesquels l'unique chemin de x à t passe par s. Alors il est clair que ce chemin se termine par st, sinon T contiendrait un cycle. Désignons par N_2 le complémentaire de N_1 dans N. Tout sommet de N_1 est relié par un chemin de T′ à s et chaque sommet de N_2 est relié à t dans T′, mais on ne peut aller de s à t.

Les ensembles N_1 et N_2 sont donc constitués des sommets des deux composantes connexes de T′. Aucune des composantes ne contient de cycle, car T n'en contient pas. Donc ces deux composantes sont des arbres.

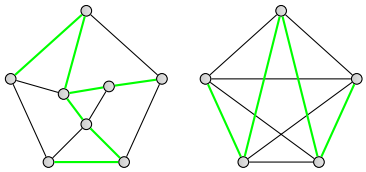
3. Supposons que $F = \{T_1, T_2, \ldots, T_c\}$ et désignons par a_i le nombre de branches de l'arbre T_i, s_i le nombre de nœuds de l'arbre T_i. Alors $\forall i \in \mathbb{N}_c^* \quad a_i = s_i - 1$. Or :

$$a = \sum_{i=1}^{c} a_i = \sum_{i=1}^{c} (s_i - 1) = \sum_{i=1}^{c} s_i - \sum_{i=1}^{c} 1 = s - c$$

□

Définition 1.23. Soit $G = (S, A, f)$ un graphe. On appelle arbre couvrant de G tout sous graphe T de G qui est un arbre et tel que son ensemble de nœuds est égal à S.

Exemples. En vert les arbres couvrants :

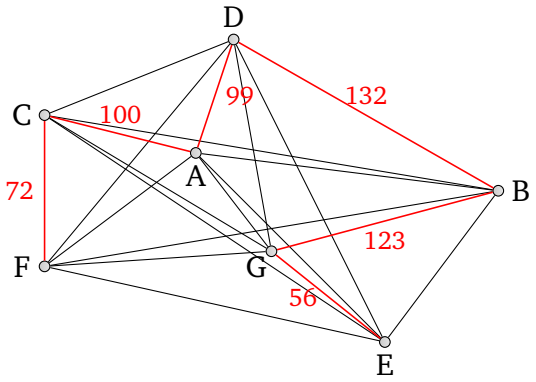


Définition 1.24.

1. On appelle graphe pondéré tout graphe $G = (S, A, f)$ tel qu'il existe une application de A dans un ensemble de nombres. Le nombre affecté à une arête s'appelle poids de l'arête, on le note $p(a)$, $a \in A$. On appelle poids de G la somme $\sum_{a \in A} p(a)$.
2. On appelle arbre couvrant minimal d'un graphe pondéré tout arbre couvrant dont le poids est minimum dans l'ensemble des poids des arbres couvrants du graphe.

Exemple. Vous possédez une petite compagnie aérienne et vous avez décroché le marché du transport spécial du siège principal d'une entreprise à ses 6 filiales en France. Le tableau des distances entre les sites est donné par :

	A	B	C	D	E	F	G
A	0	132	100	99	179	102	132
B	132	0	234	132	127	205	123
C	100	234	0	168	258	72	204
D	99	132	168	0	238	188	204
E	179	127	258	238	0	204	56
F	102	205	72	188	204	0	146
G	132	123	204	204	56	146	0



On suppose que le siège principal est en F. Évidemment vous n'avez pas assez d'avions disponibles pour en placer 6 en F. Pour réduire vos frais au maximum, vous voulez trouver un chemin qui couvre toute les villes.

Vous vous placez en F : le site le plus proche est en C. En C, le site le plus proche qui n'est ni F ni C est A, et ainsi de suite jusqu'à épuisement des sites. Le chemin obtenu est un arbre couvrant minimal.

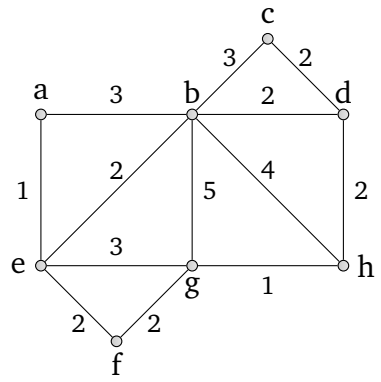
Algorithme de l'arbre couvrant minimal (R.C. Prim, 1957)

1. Choisir un sommet quelconque s_1 du graphe pondéré G, et poser T $=$ $\{s_1\}$.
2. Choisir dans l'ensemble des arêtes ayant un sommet dans T et un hors de T une arête a de poids minimum, et remplacer T par T $\cup \{a\}$ extrémités comprises.
3. Répéter 2 jusqu'à ce que tous les sommets de G soient des sommets de T.

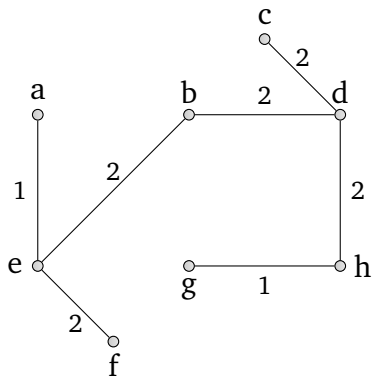
Remarques.

1. Cette méthode est aussi valable pour obtenir un arbre couvrant d'un graphe non pondéré : il suffit d'affecter 1 à chaque arête et d'utiliser l'algorithme de Prim.
2. Si le graphe de départ est complet, l'arbre couvrant minimal est un chemin (voir l'exemple précédent).

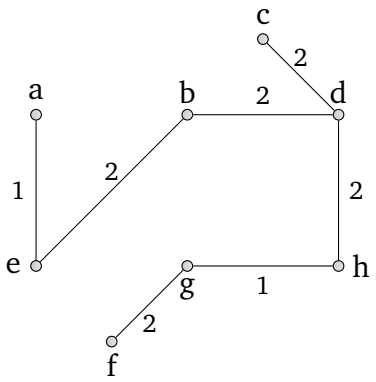
Exemple.



Graphe G = (S, A, f)



En partant de a
Poids de l'arbre : 12



En partant de g
Poids de l'arbre : 12

Théorème 1.18. *Soit* G *un graphe pondéré et* T *un arbre couvrant construit avec l'algorithme de Prim. Alors quelque soit le graphe couvrant* U *de* G*, le poids de* T *sera inférieur ou égal au poids de* U.

Démonstration. Notons $a_1, \ldots, a_n$ les arêtes de T, les indices indiquant leur ordre de construction dans l'algorithme de Prim. Si U = T, le résultat est une évidence. Si U $\neq$ T, il y a des arêtes de T qui ne sont pas arêtes de U. Soit a_k la première arête de T qui ne soit pas dans U.

Soit N l'ensemble des nœuds de l'arbre partiel obtenu dans l'exécution de l'algorithme juste avant l'adjonction de a_k. Posons $a_k = xy$ où $x \in$ N et $y \notin$ N. Puisque U est un arbre couvrant, il existe un chemin dans U allant de x à y et lorsque nous allons nous déplacer le long de ce chemin, nous allons parcourir une branche a^* qui a un nœud dans N et l'autre hors de N.

Lorsque a_k est sélectionne par l'algorithme, a^* est aussi candidate mais n'est pas retenue : donc le poids de a^* est supérieur ou égal au poids de a_k. Notons $p(a)$ le poids d'une arête a. Si $a^* \in$ T c'est qu'elle est choisie après a_k. En remplaçant a^* par a_k dans U, on obtient un arbre couvrant de G, U_1, pour

lequel :

$$p(\mathrm{U}_1) = p(\mathrm{U}) - p(a^*) + p(a_k) \leqslant p(\mathrm{U})$$

La première branche qui apparaît dans T sans être dans U_1 se trouve après a_k dans l'ordre de départ. On répète la même procédure pour obtenir une suite d'arbres couvrants $\mathrm{U}_1, \mathrm{U}_2, \ldots, \mathrm{U}_s = \mathrm{T}$ tels que :

$$p(\mathrm{T}) = p(\mathrm{U}_s) \leqslant p(\mathrm{U}_{s-1}) \leqslant \cdots \leqslant p(\mathrm{U}_1) \leqslant p(\mathrm{U})$$

□

1.3 Semi-groupes et monoïdes

Définition 1.25.

1. On appelle semi-groupe tout ensemble non vide E, muni d'une loi associative.
2. On appelle monoïde tout semi-groupe possédant un élément neutre.
3. Si la loi de composition interne est commutative, on dit que le semi-groupe ou le monoïde est commutatif.

Exemples.

1. $(\mathbb{N}, +)$ est un monoïde d'élément neutre 0.
2. $(\mathbb{R}, \times)$ est un monoïde d'élément neutre 1.
3. Soit $(\mathrm{A}, \leqslant)$ un treillis ; alors $(\mathrm{A}, \wedge)$ est un semi-groupe commutatif. Si A est borné et possède pour élément maximum 1, alors $(\mathrm{A}, \wedge)$ est un monoïde d'élément neutre 1.

Définition 1.26.

1. On appelle sous semi-groupe d'un semi-groupe $(\mathrm{A}, \cdot)$ toute partie B stable non vide de A : $\forall x, y \in \mathrm{B} \quad xy \in \mathrm{B}$.
2. On appelle sous monoïde d'un monoïde $(\mathrm{A}, \cdot)$ tout sous semi-groupe de A qui contient l'élément neutre.

Exemples.

1. $(\mathbb{Z}, \times)$ est un sous monoïde de $(\mathbb{R}, \times)$.
2. $(2\mathbb{Z}, +)$ est un sous monoïde de $(\mathbb{Z}, +)$
3. $(2\mathbb{Z}, \cdot)$ est un sous semi-groupe de $(\mathbb{Z}, \times)$ mais pas un sous monoïde car $1 \notin 2\mathbb{Z}$.

4. Soient X et Y deux parties de E telles que $X \neq \emptyset$, $X \neq Y$ et $X \subseteq Y$. Alors $\mathscr{P}(X)$ est un sous monoïde de $(\mathscr{P}(Y), \cup)$ et un sous semi-groupe de $(\mathscr{P}(Y), \cap)$. Notons que $(\mathscr{P}(X), \cap)$ est un monoïde d'élément neutre X.

Définition 1.27.

1. Soit $(A, *)$ un semi-groupe et a un élément quelconque de A. Pour tout $n \in \mathbb{N}^*$, on pose $a^1 = a, \ldots, a^n = a^{n-1} * a$
2. Si $(A, *)$ est un monoïde, on pose de plus : $a^0 = e$ l'élément neutre de A.
3. On appelle sous semi-groupe engendré par l'élément a dans le semi-groupe $(A, *)$ la partie $S_a = \{a^n / n \in N^*\}$.
4. On appelle sous monoïde engendré par l'élément a dans le monoïde $(A, *)$, la partie $M_a = \{a^n / n \in N\}$.

Remarques.

1. Il est clair que $a^n * a^p = a^{n+p}$ et $(a^n)^p = a^{np}$
2. Si la loi n'est pas commutative, $(a * b)^n \neq a^n * b^n$ en général.

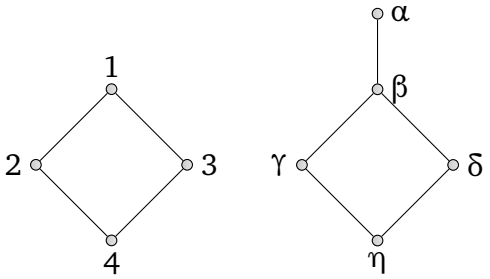
Définition 1.28.

1. Soient $(S_1, *_1)$ et $(S_2, *_2)$ deux semi-groupes. On dit que l'application f de S_1 dans S_2 est un homomorphisme de semi-groupes si :
$$\forall x \in S_1, \forall y \in S_1 \quad f(x *_1 y) = f(x) *_2 f(y)$$
2. Soient $(M_1, *_1)$ et $(M_2, *_2)$ deux monoïdes d'éléments neutres respectifs e_1 et e_2. On dit que l'application f de M_1 dans M_2 est un homomorphisme de monoïdes si :
   (a) $\forall x \in S_1, \forall y \in S_1 \quad f(x *_1 y) = f(x) *_2 f(y)$
   (b) $f(e_1) = e_2$
3. Dans le cas où l'application f est bijective, on parle d'isomorphisme de semi-groupes ou de monoïdes.

Exemples.

1. Soit A un ensemble non vide. $(\mathscr{P}(A), \cup)$ et $(\mathscr{P}(A), \cap)$ sont deux monoïdes d'éléments neutres respectifs $\emptyset$ et A. Alors $f : \mathscr{P}(A) \to \mathscr{P}(A)$ définie par : $X \mapsto \complement_A X$ est un homomorphisme de monoïde :
$$f(X \cup Y) = \complement_A(X \cup Y) = \complement_A X \cap \complement Y = f(X) \cap f(Y)$$
$$f(\emptyset) = \complement_A \emptyset = A$$

2. Soient $(M, *)$ un monoïde et $f : (\mathbb{N}, +) \to (M, *)$ définie par $n \mapsto a^n$ où a est un élément fixé dans M. Alors f est un homomorphisme de monoïde.
3. Considérons les deux treillis suivants A et C :



A C

$$\begin{aligned} f :& A \to C \\ & 1 \mapsto \beta \\ & 2 \mapsto \gamma \\ & 3 \mapsto \delta \\ & 4 \mapsto \eta \end{aligned}$$

f est un morphisme de treillis, donc un morphisme de semi groupes de $(A, \wedge)$ dans $(C, \wedge)$. Mais ce n'est pas un morphisme de monoïdes de $(A, \wedge)$ dans $(C, \wedge)$ car l'élément neutre de A est 1, celui de C est α et $f(1) = \beta \neq \alpha$.

Théorème 1.19.

1. *Soient* $(S, *)$ *et* $(T, \Diamond)$ *des semi-groupes, et* f *un homomorphisme surjectif de* S *dans* T. *Si* S *est commutatif,* T *l'est aussi.*
2. *Soient* $(S, *)$ *et* $(T, \Diamond)$ *des semi-groupes et* S' *un sous semi-groupe de* S. *Si* f *est un homomorphime de semi-groupes de* S *dans* T, *alors* $\widehat{f}(S') = \{f(s)/s \in S'\}$ *est un sous semi-groupe de* T.
3. *Soient* $(M, *)$ *et* $(N, \Diamond)$ *des monoïdes. Si* $f : M \to N$ *est surjective et est un homomorphisme de semi-groupes, alors* f *est un homomorphisme de monoïdes.*
4. *Soient* $(M, *)$ *et* $(N, \Diamond)$ *des monoïdes. Si* M' *est un sous monoïde de* M, *et* f *un homomorphisme de monoïdes, alors* $\widehat{f}(M')$ *est un sous monoïde de* N.

Démonstration.

1. $\forall t_1, t_2 \in T = \widehat{f}(S)$, $\exists s_1, s_2 \in S$ tels que $t_1 = f(s_1)$ et $t_2 = f(s_2)$. D'où :

$$\begin{aligned} t_1 \Diamond t_2 = f(s_1) \Diamond f(s_2) &= f(s_1 * s_2) \\ &= f(s_2 * s_1) = f(s_2) \Diamond f(s_1) = t_2 \Diamond t_1 \end{aligned}$$

Donc T est commutatif.

2. $\forall t_1, t_2 \in \widehat{f}(\mathrm{S}')$, $\exists s_1, s_2 \in \mathrm{S}'$ tels que $f(s_1) = t_1$ et $f(s_2) = t_2$. D'où :

$$t_1 \Diamond t_2 = f(s_1) \Diamond f(s_2) = f(s_1 * s_2) \in \widehat{f}(\mathrm{S}')$$

Donc $\widehat{f}(\mathrm{S}')$ est stable pour $\Diamond$, c'est donc un semi-groupe de T.

3. Il reste à montrer que $f(e_{\mathrm{M}}) = e_{\mathrm{N}}$. Soit y un élément quelconque de N et x l'un de ses antécédents par f. Alors :

$$y \Diamond f(e_{\mathrm{M}}) = f(x) \Diamond f(e_{\mathrm{M}}) = f(x * e_{\mathrm{M}}) = f(x) = y$$
$$f(e_{\mathrm{M}}) \Diamond y = f(e_{\mathrm{M}}) \Diamond f(x) = f(e_{\mathrm{M}} * x) = f(x) = y$$

Donc $f(e_{\mathrm{M}})$ est l'élément neutre de N, c'est à dire $f(e_{\mathrm{M}}) = e_{\mathrm{N}}$.

4. D'après 2, $\widehat{f}(\mathrm{M}')$ est un sous semi-groupe de N et d'après 3 appliqué à $f' : \mathrm{M}' \to \widehat{f}(\mathrm{M}')$ définie par $x \mapsto f(x)$ qui est une surjection.

□

Exemples.

1. $f : \mathbb{Z} \to 2\mathbb{Z} : x \mapsto 2x$ est un homomorphisme de monoïdes de $(\mathbb{Z}, +)$ dans $(2\mathbb{Z}, +)$.
2. $f : \mathscr{P}(\mathrm{A}) \to \mathscr{P}(\mathrm{A}) : \mathrm{X} \mapsto \complement_{\mathrm{A}}\mathrm{X}$ est un homomorphisme de monoïdes de $(\mathscr{P}(\mathrm{A}), \cup)$ dans $(\mathscr{P}(\mathrm{A}), \cap)$, et on a aussi $f = f^{-1}$.

Définition 1.29. Soient $(\mathrm{S}, *)$ et $(\mathrm{T}, \Diamond)$ des semi-groupes. On appelle semi groupe produit de $(\mathrm{S}, *)$ et $(\mathrm{T}, \Diamond)$ le semi groupe $(\mathrm{S} \times \mathrm{T}, \otimes)$ défini par :

$$\forall s_1, s_2 \in \mathrm{S}, \forall t_1, t_2 \in \mathrm{T} \quad (s_1, t_1) \otimes (s_2, t_2) = (s_1 * s_2, t_1 \Diamond t_2)$$

Remarques.

1. On vérifie facilement que $(\mathrm{S} \times \mathrm{T}, \otimes)$ est un semi-groupe.
2. Si S et T sont des monoïdes d'éléments neutres respectifs e_{S} et e_{T}, alors $(\mathrm{S} \times \mathrm{T}, \otimes)$ est un monoïde d'élément neutre $(e_{\mathrm{S}}, e_{\mathrm{T}})$.

Exemple. Soient $(\mathbb{N}, +)$ et $(\mathbb{Z}, \times)$. Alors dans $(\mathbb{N} \times \mathbb{Z}, \otimes)$, $(0, 1)$ est élément neutre et $(3, 7) \otimes (12, -2) = (15, -14)$.

Définition 1.30. Soient $(\mathrm{S}, *)$ un semi-groupe et R une relation d'équivalence sur S. On dit que R est compatible avec $*$ (ou encore que R est une congruence sur $(\mathrm{S}, *)$) si :

$$\forall s_1, s_2, s_1', s_2' \in \mathrm{S} \quad s_1 \mathrm{R} s_1' \text{ et } s_2 \mathrm{R} s_2' \Rightarrow s_1 * s_2 \mathrm{R} s_1' * s_2'$$

Théorème 1.20.

1. *Soient* $(S, *)$ *un semi-groupe et* R *une congruence sur* $(S, *)$. *Alors* $(S/R, \dot{*})$ *où* $\dot{*}$ *est définie par :*

$$\forall \dot{x}, \dot{y} \in \frac{S}{R} \quad \dot{x} \dot{*} \dot{y} = \dot{\widehat{x * y}}$$

   est un semi-groupe qu'on appelle semi-groupe quotient de S *par* R.

2. *Si de plus* $(S, *)$ *est un monoïde d'élément neutre* e_S, $(S/R, \dot{*})$ *est un monoïde d'élément neutre* $\dot{e}_S$.

Démonstration. Soient A, B, C trois éléments quelconques de S/R et a, b, c trois représentants respectifs de ces classes. Alors :

$$\begin{aligned}
(A \dot{*} B) \dot{*} C = (\dot{a} \dot{*} \dot{b}) \dot{*} \dot{c} = \dot{\widehat{(a * b)}} \dot{*} \dot{c} &= \dot{\widehat{(a * b) * c}} \\
&= \dot{\widehat{a * (b * c)}} \\
&= \dot{a} \dot{*} \dot{\widehat{(b * c)}} \\
&= \dot{a} \dot{*} (\dot{b} \dot{*} \dot{c}) \\
&= A \dot{*} (B \dot{*} C)
\end{aligned}$$

Donc $(S/R, \dot{*})$ est un semi-groupe.

Il nous reste à prouver l'existence d'un élément neutre pour $\dot{*}$. Soit $E = \dot{e}_S$ et X une classe quelconque de S/R de représentant x :

$$\begin{aligned}
X \dot{*} E = \dot{x} \dot{*} \dot{e}_S = \dot{\widehat{x * e_S}} = \dot{x} = X \\
E \dot{*} X = \dot{e}_S \dot{*} \dot{x} = \dot{\widehat{e_S * x}} = \dot{x} = X
\end{aligned}$$

Donc E est un élément neutre pour $\dot{*}$ et S/R est un monoïde. □

Théorème 1.21. *Soient* $(S, *)$ *et* $(T, \Diamond)$ *des semi-groupes (resp. monoïdes), et* $f : S \to T$ *un homomorphisme de semi-groupes (resp. monoïdes). Soit* R *la relation définie sur* S *par :*

$$\forall x, y \in S \quad x R y \iff f(x) = f(y)$$

Alors :

1. R *est une congruence sur* S.
2. *Les semi-groupes (resp. monoïdes)* $(S/R, \dot{*})$ *et* $(\widehat{f}(S), \Diamond)$ *sont isomorphes.*

Démonstration. R est la relation d'équivalence associée à f (voir TD). D'après le théorème de décomposition canonique d'une application, f se décompose en $f = i \circ b \circ s$ où :

- $s : \mathrm{S} \to \mathrm{S/R} : x \mapsto \dot{x}$ est une surjection.
- $b : \mathrm{S/R} \to \widehat{f}(\mathrm{S}) : \dot{x} \mapsto f(x)$ est une bijection.
- $i : \widehat{f}(\mathrm{S}) \to \mathrm{T} : f(x) \mapsto f(x)$ est une injection.

1. $\forall s_1, s_2, s_1', s_2' \in \mathrm{S}$ tels que $s_1 \mathrm{R} s_1'$ et $s_2 \mathrm{R} s_2'$. Alors $f(s_1) = f(s_1')$ et $f(s_2) = f(s_2')$.

$$f(s_1) \Diamond f(s_2) = f(s_1') \Diamond f(s_2')$$
$$f(s_1 * s_2) = f(s_1' * s_2')$$
$$s_1 * s_2 \mathrm{R} s_1' * s_2'$$

   Donc R est une congruence sur S.

2. Il suffit de prouver que b est un homomorphisme de semi-groupes. Pour tous $\mathrm{X}, \mathrm{Y} \in \mathrm{S/R}$ de représentants respectifs x et y :

$$b(\mathrm{X} \dot{*} \mathrm{Y}) = b(\dot{x} \dot{*} \dot{y}) = b(\dot{\widehat{x * y}}) = f(x * y) = f(x) \Diamond f(y) = b(\mathrm{X}) \Diamond b(\mathrm{Y})$$

   Pour les monoïdes, $\widehat{f}(\mathrm{S})$ est un monoïde d'après le théorème 1.19, $(\mathrm{S/R}, \dot{*})$ est un monoïde d'après le théorème 1.20 et b un homomorphisme de monoïdes d'après le théorème 1.19.

□

Définition 1.31. Soit A un ensemble non vide appelé alphabet dont les éléments sont appelés lettres. On appelle mot sur A toute suite finie non vide de lettres.

Remarque. Un mot est donc une application w de $\mathbb{N}_n^*$ dans A pour un n qui varie dans $\mathbb{N}^*$. L'égalité entre deux mots en découle : pour que deux mots soient égaux il faut qu'ils aient même ensemble de départ (même longueur) et même ensemble d'arrivée (c'est A), et même graphe :

$$\forall k \in \mathbb{N}_k^* \quad \text{si } w = w' \quad w(k) = w'(k)$$

Théorème 1.22. *On considère l'ensemble des mots sur un alphabet* A*. La loi de composition interne $\cdot$ définie sur cet ensemble par :*

$$(x_1 \dots x_n) \cdot (y_1 \dots y_n) = x_1 \dots x_n y_1 \dots y_n$$

est associative.

Définition 1.32. La loi du théorème 1.22 est appelée concaténation, et on note A^+ le semi-groupe des mots de A. On l'appelle semi-groupe libre sur A (ou engendré par A).

Démonstration. Soient u, v et w trois mots sur A. Alors il existe $n, m, p \in \mathbb{N}^*$, $x_1, \ldots, x_n,\ y_1, \ldots, y_m,\ z_1, \ldots, z_p \in A$ tels que $u = x_1 \ldots x_n$, $v = y_1 \ldots y_m$ et $w = z_1 \ldots z_p$. Alors :

$$\begin{aligned}
(uv) &= (x_1 \ldots x_n)(y_1 \ldots y_m) \\
&= x_1 \ldots x_n y_1 \ldots y_m \\
(uv)w &= (x_1 \ldots x_n y_1 \ldots y_m)(z_1 \ldots z_p) \\
&= x_1 \ldots x_n y_1 \ldots y_m z_1 \ldots z_p \\
(vw) &= (y_1 \ldots y_m)(z_1 \ldots z_p) \\
&= y_1 \ldots y_m z_1 \ldots z_p \\
u(vw) &= (x_1 \ldots x_n)(y_1 \ldots y_m z_1 \ldots z_p) \\
&= x_1 \ldots x_n y_1 \ldots y_m z_1 \ldots z_p
\end{aligned}$$

□

Théorème 1.23. *Soit* A *un ensemble non vide et* S *un semi groupe. Si* φ *est une application de* A *dans* S*, il existe un homomorphisme unique* Φ *du semi groupe libre* A^+ *dans* S *tel que* $\forall x \in A, \Phi(x) = \varphi(x)$*. De plus,* Φ *est surjective si et seulement si* $\widehat{\varphi}(A)$ *est un ensemble de générateurs de* S*.*

X *est un ensemble de générateurs de* S *si tout élément de* S *s'écrit sous la forme d'un produit fini d'éléments de* X*.*

Démonstration. On a $\varphi : A \to S$. Soit Φ l'application de A^+ dans S définie par :

$$\begin{aligned}
&\forall x \in A \quad \Phi(x) = \varphi(x) \\
&\forall u \in A^+ \quad \exists x_1, \ldots, x_n \in A / u = x_1 \ldots x_n \quad \Phi(u) = \varphi(x_1) \ldots \varphi(x_n)
\end{aligned}$$

On va montrer que Φ est un homomorphisme de semi-groupes. Soit $u, v \in A^+$. Il existe $x_1, \ldots, x_n, y_1, \ldots, y_p$ dans A tels que $u = x_1 \ldots x_n$, $v = y_1 \ldots y_p$. Donc :

$$\begin{aligned}
\Phi(uv) &= \Phi\left[(x_1 \ldots x_n)(y_1 \ldots y_p)\right] \\
&= \Phi\left[x_1 \ldots x_n y_1 \ldots y_p\right] \\
&= \varphi(x_1) \ldots \varphi(x_n)\varphi(y_1) \ldots \varphi(y_p) \\
&= \left[\varphi(x_1) \ldots \varphi(x_n)\right]\left[\varphi(y_1) \ldots \varphi(y_p)\right] \\
&= \Phi(x_1 \ldots x_n)\Phi(y_1 \ldots y_p) \\
&= \Phi(u)\Phi(v)
\end{aligned}$$

Supposons à présent qu'il existe un homomorphisme de semi-groupe Φ' de A^+ dans S tel que $\Phi'_{|A} = \varphi$. Alors pour tout $u \in A^+$, il existe $x_1, \ldots, x_n \in A$ tels que $u = x_1 \ldots x_n$. D'où :

$$\begin{aligned}
\Phi'(u) &= \Phi'(x_1 \ldots x_n) \\
&= \Phi'(x_1) \ldots \Phi'(x_n) \quad \text{car } \Phi' \text{ est un homomorphisme} \\
&= \varphi(x_1) \ldots \varphi(x_n) \quad \text{car } \Phi'_{|A} = \varphi \\
&= \Phi(x_1) \ldots \Phi(x_n) \quad \text{car } \Phi_{|A} = \varphi \\
&= \Phi(x_1 \ldots x_n) = \Phi(u) \quad \text{car } \Phi \text{ est un homomorphisme}
\end{aligned}$$

D'où $\Phi = \Phi'$ et Φ est l'unique homomorphisme de A^+ dans S qui prolonge φ.

Supposons que $\widehat{\varphi}(A)$ soit un ensemble de générateurs de S, et soit s un élément quelconque de S. Alors il existe $s_1, \ldots, s_p \in \widehat{\varphi}(A)$ tels que $s = s_1 \ldots s_p$. Or $\forall i \in \mathbb{N}_p^*$, $s_i \in \widehat{\varphi}(A)$ donc $\forall i \in \mathbb{N}_p^*$, il existe $x_i \in A$ tel que $s_i = \varphi(x_i)$. Donc :

$$s = \varphi(x_1) \ldots \varphi(x_p) = \Phi(x_1 \ldots x_p) \in \widehat{\Phi}(A+)$$

Donc Φ est surjective.

Réciproquement, supposons Φ surjective : alors $\forall s \in S$, $\exists u \in A^+$ tel que $\Phi(u) = s$. Or, si $u \in A^+$, il existe $x_1, \ldots, x_n \in A$ tels que $u = x_1 \ldots x_n$. D'où $s = \Phi(u) = \varphi(x_1) \ldots \varphi(x_n)$. Donc tout élément de S est un produit fini d'éléments de $\widehat{\varphi}(A)$. $\widehat{\varphi}(A)$ engendre donc S. □

Exemple. Soient A un alphabet et $\ell : A \to \mathbb{N}$ définie par $x \mapsto 1$. On sait que ℓ admet un unique prolongement sur A^+, $L : A^+ \to \mathbb{N}$ définie par $u = x_1 \ldots x_n \mapsto L(u) = n$.

Théorème 1.24. *Soit* S *un semi-groupe et* A *un ensemble de générateurs de* S. *Alors* S *est l'image homomorphe du semi-groupe libre* A^+.

Démonstration. Soit $i : A \to S$ définie par $x \mapsto x$. Alors $\widehat{i}(A)$ est surjective et on applique le théorème 1.23. □

1.4 Algèbre de Boole

Définition 1.33. Soit B un ensemble contenant au moins deux éléments notés 0 et 1, et muni :

1. d'une loi de composition interne appelée addition et notée $+$,
2. d'une loi de composition interne appelée multiplication et notée $\cdot$,
3. d'une application appelée complémentation et notée $\bar{}$.

On dit que B possède une structure d'algèbre de Boole s'il a les propriétés suivantes :

1. $+$ et $\cdot$ sont associatives et commutatives.
2. 0 est élément neutre pour $+$, 1 est élément neutre pour $\cdot$.
3. $+$ est distributive par rapport à $\cdot$, et $\cdot$ est distributive par rapport à $+$.
4. $\forall a \in \mathrm{B}$, $a + \bar{a} = 1$ et $a \cdot \bar{a} = 0$.

Exemples.

1. $\left(\mathscr{P}(\mathrm{E}), \cup, \cap, \complement_{\mathrm{E}}\right)$
2. $\left(\mathrm{D}_{10} = \{1, 2, 5, 10\}, +, \times, \bar{}\right)$ où $x + y = \mathrm{ppcm}(x, y)$, $xy = \mathrm{pgcd}(x, y)$, $\bar{x} = 10/x$ et 1 est élément neutre pour $+$, 10 est élément neutre pour $\cdot$.
3. $(\{1, 0\}, +, \times, \bar{})$ où $+, \times, \bar{}$ sont définis par les tables :

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

x	$\bar{x}$
0	1
1	0

4. $(\mathscr{F}(\mathrm{E}, \{0, 1\}), +, \cdot, \bar{})$ où $\mathscr{F}(\mathrm{E}, \{0, 1\})$ est l'ensemble des applications de l'ensemble E dans l'algèbre de Boole $\{0, 1\}$. On parle aussi de l'ensemble des applications caractéristiques des parties de E : si $\mathrm{A} \in \mathscr{P}(\mathrm{E})$, $\varphi_{\mathrm{A}} : \mathrm{E} \to \{0, 1\}$ est définie par $\varphi_{\mathrm{A}}(x) = 1$ si $x \in \mathrm{A}$ et $\varphi_{\mathrm{A}}(x) = 0$ si $x \notin \mathrm{A}$. Alors $\varphi_{\mathrm{A}} + \varphi_{\mathrm{B}} = \varphi_{\mathrm{A} \cup \mathrm{B}}$, $\varphi_{\mathrm{A}} \cdot \varphi_{\mathrm{B}} = \varphi_{\mathrm{A} \cap \mathrm{B}}$ et $\bar{\varphi_{\mathrm{A}}} = \varphi_{\bar{\mathrm{A}}}$ où $\bar{\mathrm{A}} = \complement_{\mathrm{E}}\mathrm{A}$.

Remarque. La parfaite symétrie des rôles des deux lois de composition interne nous amène à penser que tout théorème se présentera sous deux formes duales. L'énoncé de théorème dual s'obtiendra en permutant systématiquement dans l'énoncé du théorème initial les symboles $+$ et $\cdot$, et les éléments 0 et 1.

Théorème 1.25. *Soit* B *une algèbre de Boole. Pour tout a de* B*, $\bar{a}$ est l'unique élément de* B *vérifiant :*

$$a + \bar{a} = 1 \quad \textit{et} \quad a \cdot \bar{a} = 0$$

Il en découle que $\bar{1} = 0$, $\bar{0} = 1$ et que pour tout a de B*, $\bar{\bar{a}} = a$.*

Démonstration. Par la définition 1.33, $\forall a \in \mathrm{B}$, $a + \bar{a} = 1$ et $a \cdot \bar{a} = 0$. Supposons qu'il existe $a' \in \mathrm{B}$ tel que $a + a' = 1$ et $a \cdot a' = 0$. Alors :

$$\begin{aligned} \bar{a}(a + a') &= \bar{a} \cdot 1 = \bar{a} \\ &= \bar{a}a + \bar{a}a' = 0 + \bar{a}a' = \bar{a}a' \\ (a + \bar{a})a' &= 1a' = a' \\ &= (aa' + \bar{a}a') = 0 + \bar{a}a' = \bar{a}a' \end{aligned}$$

D'où $\bar{a} = a'$.

D'après la définition 1.33 on a $1 + 0 = 1$ et $1 \cdot 0 = 0$ donc $\bar{1} = 0$ et $\bar{0} = 1$.

De plus, $\forall a \in \mathrm{B}$:

$$\begin{aligned} a + \bar{a} = 1 \quad &\text{et} \quad a\bar{a} = 0 \\ \bar{\bar{a}} + \bar{a} = 1 \quad &\text{et} \quad \bar{\bar{a}}\bar{a} = 0 \end{aligned}$$

D'où $\bar{\bar{a}} = a$ d'après l'unicité. □

Théorème 1.26. *Soit* B *une algèbre de Boole. Alors quelques soient les éléments* a, b, x, y *de* B *on a les propriétés suivantes :*

1. $a + a = a \quad et \quad aa = a$.
2. 1 *est absorbant pour l'addition et* 0 *pour la multiplication.*
3. $a + (ax) = a$ *(absorption)*.
4. $(ax) + (\bar{a}y) = ax + \bar{a}y + xy$ *(redondance)*.
5. $\overline{a + b} = \bar{a} \cdot \bar{b}$ *et* $\overline{ab} = \bar{a} + \bar{b}$ *(De Morgan)*.

Démonstration.

1.

$$\begin{aligned} (a\bar{a}) + a &= 0 + a = a \\ &= (a + a)(\bar{a} + a) \\ &= (a + a)1 \\ &= a + a \end{aligned}$$

$aa = a$ est l'écriture duale de la première.

2.

$$\begin{aligned} 1 + a &= (a + \bar{a}) + a \\ &= a + a + \bar{a} \\ &= a + \bar{a} \\ &= 1 \end{aligned}$$

$0a = 0$ est l'écriture duale de la précédente.

3.

$$\begin{aligned} a + (ax) &= (a1) + (ax) \\ &= a(1 + x) \\ &= a1 \\ &= a \end{aligned}$$

4.

$$ax = ax + axy \quad \text{et} \quad \bar{a}y = \bar{a}y + \bar{a}xy$$

$$\begin{aligned} ax + \bar{a}y &= ax + \bar{a}y + axy + \bar{a}xy \\ &= ax + \bar{a}y + (a + \bar{a})xy \\ &= ax + \bar{a}y + xy \end{aligned}$$

5. Montrons que $\overline{a+b} = \bar{a}\bar{b}$, la seconde égalité étant duale de la première.

$$\begin{aligned} \bar{a}\bar{b} + (a+b) &= (\bar{a}\bar{b} + a1) + b \\ &= (\bar{a}\bar{b} + a1 + \bar{b}1) + b \\ &= \bar{a}\bar{b} + a + (\bar{b} + b) \\ &= \bar{a}\bar{b} + a + 1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} (\bar{a}\bar{b})(a+b) &= \bar{a}\bar{b}a + \bar{a}\bar{b}b \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

Donc d'après le théorème 1.25, $\bar{a}\bar{b}$ est le complément de $a+b$.

□

Théorème 1.27. *Soit* B *une algèbre de Boole. La relation* $\leqslant$ *définie sur* B *par :*

$$\forall a, b \in \mathrm{B} \quad a \leqslant b \iff ab = a$$

est une relation d'ordre sur B *compatible avec les deux lois de* B.

Démonstration. Réflexivité : $\forall a \in \mathrm{B} \quad aa = a$ donc $a \leqslant a$.

Antisymétrie : $\forall a \in \mathrm{B}, \forall b \in \mathrm{B}$ supposons $a \leqslant b$ et $b \leqslant a$. Alors $ab = a$ et $ba = b$. Or $\cdot$ est commutative, d'où $ab = ba$ et $a = b$.

Transitivité : $\forall a \in \mathrm{B}, \forall b \in \mathrm{B}, \forall c \in \mathrm{B}$, $a \leqslant b$ et $b \leqslant c \Rightarrow ab = a$ et $bc = b$. D'où $a = ab = a(bc) = (ab)c = ac$, et $a \leqslant c$.

On peut remarquer que si B a plus de deux éléments, cet ordre n'est pas total car il existe $a \in \mathrm{B} \setminus \{0, 1\}$; son complément $\bar{a}$ est alors aussi autre que 0 et 1. Comme $a\bar{a} = 0$, on n'a ni $a \leqslant \bar{a}$, ni $\bar{a} \leqslant a$. Cet ordre est aussi défini par :

$$a \leqslant b \iff a + b = b$$

Compatibilité : les lois de B étant commutatives, il n'est nécessaire de le montrer qu'à gauche. Soient a, b, c des éléments quelconques de B tels que $a \leqslant b$. Comparons ca et cb :

$$(ca)(cb) = (cc)(ab) = ca$$

d'où $ca \leqslant cb$. Comparons $c + a$ et $c + b$:

$$\begin{aligned}(c+a)(c+b) &= cc + ac + cb + ab \\ &= c + cb + a + ac \\ &= c + a\end{aligned}$$

□

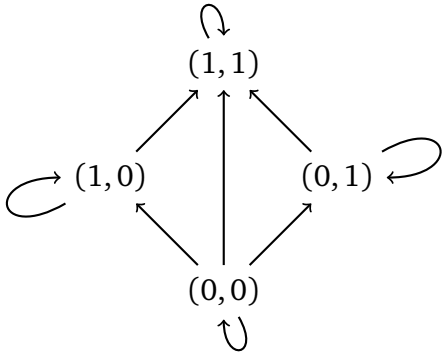
Remarque. Dans tout algèbre de Boole, pour tout $a \in \mathrm{B}$, $0a = 0$ donc $0 \leqslant a$ et $a1 = a$ donc $a \leqslant 1$. En particulier, $0 \leqslant 1$.

Exemples.

1. Dans $\left(\mathscr{P}(\mathrm{E}), \cup, \cap, \complement\right)$, $\leqslant$ est l'inclusion $\subseteq$:

$$\begin{aligned}\mathrm{A} \leqslant \mathrm{B} &\iff \mathrm{A} \cap \mathrm{B} = \mathrm{A} \\ &\iff \mathrm{A} \subseteq \mathrm{B}\end{aligned}$$

2. Dans $(\{0,1\}, +, \cdot, \bar{})$, $0 \leqslant 0$, $0 \leqslant 1$ et $1 \leqslant 1$.
3. Dans $\left(\{0,1\}^2, +, \cdot, \bar{}\right)$: $(0,1)(1,1) = (0,1)$ donc $(0,1) \leqslant (1,1)$.



$(0,1)$ et $(1,0)$ ne sont pas comparables.

Définition 1.34. Soit B une algèbre de Boole finie. Un atome de B est un élément non nul de B n'ayant que deux éléments inférieurs par la relation $\leqslant$: 0 et lui-même.

Exemples.

1. Dans $\left(\mathscr{P}(\mathrm{E}), \cup, \cap, \complement\right)$, $\leqslant$ est l'inclusion et les atomes sont les singletons.
2. Dans $(\{0,1\}, +, \cdot, \bar{})$, 1 est le seul atome.
3. Dans $\left(\{0,1\}^2, +, \times, \bar{}\right)$ les atomes sont $(0,1)$ et $(1,0)$.

Théorème 1.28. *Soit a un élément non nul d'une algèbre de Boole* B *finie. Le sous ensemble* I_a *des éléments de* B *inférieurs à a contient au moins un atome.*

Démonstration. I_a est une partie d'un ensemble fini, donc elle est finie et non vide car 0 et a sont dans I_a.

- 1^{er} cas : $\mathrm{I}_a = \{0, a\}$ alors a est un atome et le théorème est vérifié.
- 2^{e} cas : $\mathrm{I}_a \neq \{0, a\}$, il existe donc $a_1 \in \mathrm{I}_a$ autre que 0 et a. Considérons $\mathrm{I}_{a_1} : \mathrm{I}_{a_1} \subseteq \mathrm{I}_a$.
  - 1^{er} cas : $\mathrm{I}_{a_1} = \{0, a_1\}$ et a_1 est un atome. D'où $a_1 \in \mathrm{I}_{a_1} \subseteq \mathrm{I}_a$ et le théorème est vérifié.
  - $\mathrm{I}_{a_1} \neq \{0, a_1\}$ et $\mathrm{I}_{a_1} \subsetneq \mathrm{I}_a$ car $a \in \mathrm{I}_a$ mais $a \notin \mathrm{I}_{a_1}$ on choisit alors $a_2 \in \mathrm{I}_{a_1}$ autre que a_1 et 0, ...

On obtient ainsi une chaîne $\mathrm{I}_a \supsetneq \mathrm{I}_{a_1} \supsetneq \mathrm{I}_{a_2} \supsetneq \cdots \supsetneq \mathrm{I}_{a_n}$. I_a étant fini, cette chaîne s'arrête à un certain $\mathrm{I}_{a_n} = \{0, a_n\}$ et a_n est un atome de B. Comme $\mathrm{I}_{a_n} \subseteq \mathrm{I}_a$, le théorème est vérifié. □

Théorème 1.29. *Soit* B *une algèbre de Boole finie.*

1. *L'ensemble des atomes est non vide.*
2. *Le produit de deux atomes distincts de* B *est nul.*
3. *La somme de tous les atomes de* B *est égale à* 1.
4. *Tout élément de* B *s'écrit d'une manière unique sous la forme d'une somme d'atomes différents.*
5. *Si $a \in$ B, et s'il s'écrit sous forme d'une somme d'atomes, $\bar{a}$ s'écrit comme somme de tous les autres atomes.*
6. *Si* B *a p atomes, alors* $\operatorname{card} \mathrm{B} = 2^p$.

Démonstration.

1. Conséquence immédiate du théorème 1.28.
2. Soient a, a' deux éléments quelconques de B. Alors $aa' \leqslant a$ et $aa' \leqslant a'$. Supposons de plus que a et a' soient des atomes distincts et que $aa' \neq 0$. D'après la définition d'un atome, $aa' = a$ et $aa' = a'$ d'où $a = a'$ contraire à l'hypothèse. Donc $aa' = 0$.

3. Soient $a_1, \ldots, a_p$ tous les atomes de B. Posons $a = \sum_{i=1}^{p} a_i$ et supposons que $a \neq 1$. Alors $\bar{a} \neq 0$. D'après le théorème 1.28, $\mathrm{I}_{\bar{a}}$ contient au moins un atome a_k. D'où $a_k \leqslant \bar{a}$ et $a_k \bar{a} = a_k$. Or :

$$\begin{aligned} a_k a &= a_k \sum_{i=1}^{p} a_i \\ &= \sum_{i=1}^{p} a_k a_i \\ &= a_k a_k \\ &= a_k \end{aligned}$$

Donc $a_k \bar{a} = a_k a$.

$$\begin{aligned} (a_k \bar{a})(a_k a) &= (a_k a_k)(\bar{a} a) = 0 \\ &= a_k a_k = a_k \end{aligned}$$

Absurde car a_k est un atome. L'hypothèse $a \neq 1$ est fausse et donc $\sum_{i=1}^{p} a_i = 1$.

6. Il y a autant d'éléments dans B que de sommes finies d'atomes différents.

n	Nombre de sommes à n atomes
0	$1 = \binom{p}{0}$ c'est le 0 de B
1	$p = \binom{p}{1}$
2	$\binom{p}{2}$
$\vdots$	$\vdots$
p	$1 = \binom{p}{p}$ le 1 de B

Soit au total $\binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p} = \sum_{k=0}^{p} \binom{p}{k} = 2^p$.

□

Définition 1.35.

1. Un isomorphisme f d'une algèbre de Boole $(\mathrm{B}, +, \cdot, \bar{})$ vers une algèbre de Boole $(\mathrm{B}', \boxplus, \boxdot, \breve{})$ est une bijection de B vers B′, telle que :

$$\begin{aligned} \forall a \in \mathrm{B}, \forall b \in \mathrm{B}', \quad f(a+b) &= f(a) \boxplus f(b) \\ f(ab) &= f(a) \boxdot f(b) \\ f(\bar{a}) &= f\breve{(a)} \end{aligned}$$

2. Si B et B′ sont deux algèbres de Boole, et qu'il existe un isomorphisme de B dans B′ (ou de B′ dans B), on dit que B et B′ sont isomorphes.

Remarques.

1. Si f est un isomorphisme d'algèbre de Boole de $(\mathrm{B}, +, \cdot, \bar{})$ dans $(\mathrm{B}', \boxplus, \boxdot, \bar{})$, f^{-1} est un isomorphisme d'algèbre de Boole de $(\mathrm{B}', \boxplus, \boxdot, \bar{})$ dans $(\mathrm{B}, +, \cdot, \bar{})$.
2. Si f est un isomorphisme d'algèbre de Boole de $(\mathrm{B}, +, \cdot, \bar{})$ dans $(\mathrm{B}', \boxplus, \boxdot, \bar{})$, alors :

$$\forall a \in \mathrm{B}, \forall b \in \mathrm{B} \quad a \leqslant b \Rightarrow f(a) \leqslant f(b)$$

Théorème 1.30 (Stone)**.** *Toute algèbre de Boole finie* $(\mathrm{B}, +, \cdot, \bar{})$ *est isomorphe à l'algèbre de Boole* $\left(\mathscr{P}(\mathbb{N}_p^*), \cup, \cap, \complement\right)$ *où* p *est le nombre d'atomes de* B.

Démonstration. D'après le théorème 1.29, l'ensemble des atomes de B est non vide. B étant fini, cet ensemble lui même est fini. Désignons par $a_1, \ldots, a_p$ ($p \geqslant 1$) les atomes de B.

Nous savons que tout élément $a \in \mathrm{B}$ s'écrit de manière unique sous la forme : $a = \sum_{i \in \mathrm{I}} a_i$ où $\mathrm{I} \subseteq \mathbb{N}_p^*$.

Considérons l'algèbre de Boole $\left(\mathscr{P}(\mathbb{N}_p^*), \cup, \cap, \complement\right)$ et :

$$\begin{aligned} f &: \mathrm{B} \to \mathscr{P}(\mathbb{N}_p^*) \\ 0 &\mapsto \emptyset \\ a_i &\mapsto \{i\} \quad \forall i \in \mathrm{N}_p^* \\ a &\mapsto \mathrm{I} \quad \text{si } a = \sum_{i \in \mathrm{I}} a_i \end{aligned}$$

Montrons que f est surjective. Soit F une partie quelconque de $\mathbb{N}_p^*$.

- Si $\mathrm{F} = \emptyset$, alors $f(0) = \mathrm{F}$.
- Sinon, si $\mathrm{F} \neq \emptyset$, soit a l'élément de B défini par $a = \sum_{i \in \mathrm{I}} a_i$. Par définition de f, $f(a) = \mathrm{F}$, f est donc surjective.

Or B ayant p atomes, $\operatorname{card} \mathrm{B} = 2^p$ et $\operatorname{card} \mathscr{P}(\mathbb{N}_p^*) = 2^p$. Donc f est une bijection.

Considérons a et b deux éléments de B tels que :

$$a = \sum_{i \in \mathrm{I}} a_i, b = \sum_{j \in \mathrm{J}} a_j$$

Alors $a + b = \sum_{k \in \mathrm{I} \cup \mathrm{J}} a_k$ et :

$$f(a+b) = \mathrm{I} \cup \mathrm{J} = f(a) \cup f(b)$$

$$ab = \left(\sum_{i \in \mathrm{I}} a_i\right)\left(\sum_{j \in \mathrm{J}} a_j\right) = \sum_{(i,j) \in \mathrm{I} \cup \mathrm{J}} a_i a_j = \sum_{k \in \mathrm{I} \cup \mathrm{J}} a_k$$

car $a_i a_j = 0$ si $i \neq j$: ce sont des atomes.
Alors $f(ab) = \mathrm{I} \cap \mathrm{J} = f(a) \cap f(b)$.

$$\bar{a} = \overline{\sum_{i \in \mathrm{I}} a_i} = \sum_{i \in \complement \mathrm{I}} a_i$$

d'après le théorème 1.29. D'où $f(\bar{a}) = \complement \mathrm{I} = \complement f(a)$. f est bien un homomorphisme d'algèbre de Boole de $(\mathrm{B}, +, \cdot, \bar{})$ dans $\left(\mathscr{P}(\mathbb{N}_p^*), \cup, \cap, \complement\right)$. □

Définition 1.36. Soit B une algèbre de Boole.

1. On appelle expression booléenne de deux éléments a et b de B, tout élément de B obtenu en combinant a et b à l'aide d'un nombre fini d'additions, de multiplications et de complémentation. On définit de même des expressions booléennes de trois, quatre, ..., n éléments.
2. Un littéral est une expression booléenne formée d'un seul élément, complémenté ou non.
3. Un monôme est un produit d'un ou de plusieurs littéraux.
4. Un monal est une somme d'un ou de plusieurs littéraux.
5. Une expression $\Sigma\Pi$ est une somme d'un ou plusieurs monômes.
6. Une expression $\Pi\Sigma$ est un produit d'un ou plusieurs monaux.
7. Un minterme des n éléments $a_1, \ldots, a_n$ est un monôme à n littéraux obtenu, en choisissant dans chacun des n couples $(a_i, \bar{a}_i)$ un élément et un seul.
8. Un maxterme des n éléments $a_1, \ldots, a_n$ est un monal à n littéraux, obtenu en choisissant dans chacun des n couples $(a_i, \bar{a}_i)$ un élément et un seul.

Exemples. Soient a et b deux éléments d'une algèbre de Boole B.

1. Expressions booléennes : $\overline{a + ab}$, $\overline{\bar{a} + b}$, $ab + a$, ...
2. Littéraux : a,b, $\bar{a}$, $\bar{b}$, ...
3. Monômes : $ab\bar{c}$, $\bar{a}b\bar{c}\bar{d}$, ...
4. Monaux : $a + \bar{b}$, $a + b + \bar{d}$, $\bar{a} + \bar{d}$, ...
5. Expressions $\Sigma\Pi$: $a\bar{b} + \bar{a}\bar{b}c$, $ab\bar{c} + b + \bar{c}\bar{d}$, ...
6. Expressions $\Pi\Sigma$: $(a + b)(\bar{a} + c)$, $\bar{a}(c + \bar{d})(\bar{a} + b + \bar{c})$, ...
7. Mintermes de a et de b, il y en a 4 : ab, $\bar{a}b$, $a\bar{b}$, $\bar{a}\bar{b}$. Mintermes de a, b et de c, il y en a 8 : $abc, \bar{a}bc, a\bar{b}c, \bar{a}\bar{b}c, ab\bar{c}, \bar{a}b\bar{c}, \bar{a}\bar{b}\bar{c}, a\bar{b}\bar{c}$.
8. Maxtermes de a et de b, il y en a 4 : $a + b$, $a + \bar{b}$, $\bar{a} + b$, et $\bar{a} + \bar{b}$.

Remarques.

1. Il y a exactement 2^n mintermes (resp. maxtermes) de n éléments $a_1, \ldots, a_n$ (n choix successifs entre deux termes : a_i ou $\bar{a}_i$).
2. On peut numéroter les mintermes (resp. maxtermes) grâce à l'astuce suivante : quand on choisit a_i on le note 1 et quand on choisit $\bar{a}_i$ on le note 0.

   Par exemple, $\bar{a}bc \rightsquigarrow 011$. $a\bar{b}c\bar{d} \rightsquigarrow 1010$. Ensuite on convertit le nombre binaire obtenu en base 10 et on l'affecte en indice à m pour les mintermes et à M pour les maxtermes.

   $$\bar{a}bc = m_3 \quad a + \bar{b} + c + \bar{d} = \mathrm{M}_{10}$$

   Grâce à cette numérotation, on obtient facilement les complémentaires des mintermes et des maxtermes. Si m_i est un minterme de $a_1, \ldots, a_n$, $0 \leqslant i \leqslant 2^n - 1$ on a :

   $$\overline{m_i} = \mathrm{M}_j, \quad \overline{\mathrm{M}_i} = m_j \quad \text{où } j = 2^n - 1 - i$$

   Par exemple, $m_3 = \overline{a_1}a_2a_3$. Alors :

   $$\overline{m_3} = \overline{\overline{a_1}a_2a_3} = a_1 + \overline{a_2} + \overline{a_3} = \mathrm{M}_4$$

   Or $4 = 2^3 - 1 - 3$.

Définition 1.37. Soit B une algèbre de Boole. On appelle sous algèbre de Boole de B, toute partie $\mathscr{A}$ non vide de B telle que les restrictions des trois opérations $+, \cdot, \bar{}$ confèrent à $\mathscr{A}$ une structure d'algèbre de Boole.

1. $\mathscr{A} \neq \emptyset$
2. $\forall a, b \in \mathscr{A}$, $a + b \in \mathscr{A}$, $ab \in \mathscr{A}$ et $\bar{a} \in \mathscr{A}$.

Remarque. Toute partie non vide de B stable pour les 3 opérations est une sous algèbre de Boole de B.

Exemples.

1. Soit $\mathrm{B} = \left(\mathscr{P}(\mathbb{N}_2^*), \cup, \cap, \complement\right)$. Les seules sous algèbres de B sont $\left(\emptyset, \mathbb{N}_2^*\right)$ et $\mathscr{P}(\mathbb{N}_2^*)$ lui même. Notons que $\{\emptyset\}$ n'est pas une sous algèbre de B car $\bar{\emptyset} = \mathbb{N}_2^* \notin \{\emptyset\}$.
2. Soient $a_1, \ldots, a_n$ des éléments d'une algèbre de Boole de B. Le sous-ensemble $\mathscr{G}(a_1, \ldots, a_n)$ des expressions booléennes de $a_1, \ldots, a_n$ est une sous algèbre de Boole de B.

   Si $a, b \in \mathrm{B}$, $\mathscr{G}(a, b) = \{0, 1, a, b, \bar{a}, \bar{b}, a + b, a + \bar{b}, \bar{a} + b, \bar{a} + \bar{b}, ab, a\bar{b}, \bar{a}b, \bar{a}\bar{b}, \bar{a}b + a\bar{b}, ab + \bar{a}\bar{b}\}$

Théorème 1.31. *Soient* B *une algèbre de Boole finie,* $a_1, \ldots, a_n$ *des éléments quelconques de* B. *Les atomes de* $\mathscr{G}(a_1, \ldots, a_n)$ *sont les mintermes non nuls de ces éléments.*

Démonstration. Montrons tout d'abord que $\mathscr{G}(a_1, \ldots, a_n)$ est l'ensemble de toutes les sommes finies de monômes à littéraux pris parmi $a_1, \ldots, a_n, \bar{a_1}, \ldots, \bar{a_n}$. On rappelle que par convention 0 est la somme de zéro atome et que chaque atome est la somme d'un seul atome, lui même.

Soit S le sous ensemble de $\mathscr{G}(a_1, \ldots, a_n)$ formé de toutes les sommes finies de monômes à littéraux pris parmi $a_1, \ldots, a_n, \bar{a_1}, \ldots, \bar{a_n}$. S contient tous les éléments $a_1, \ldots, a_n$ car chaque a_i peut être constitué comme somme du seul monôme a_i. De plus :

- S est stable pour l'addition (par définition).
- S est stable pour la multiplication car le produit de deux sommes finies de monômes est une somme finie de monômes (à cause de la distributivité de $\cdot$ par rapport à $+$).
- S est stable pour la complémentation car le complément d'une somme finie de monômes est encore une somme finie de monômes (De Morgan et distributivité de $\cdot$ par rapport à $+$).

Montrons à présent l'égalité entre S et $\mathscr{G}(a_1, \ldots, a_n)$.

Soit a un élément quelconque de $\mathscr{G}(a_1, \ldots, a_n)$: a s'obtient en faisant un nombre fini d'opérations $+, \cdot, \bar{}$ à partir d'éléments pris dans $\{a_1, \ldots, a_n\}$. On reste donc dans S en procédant de cette façon. Donc $a \in$ S et $\mathscr{G}(a_1, \ldots, a_n) \subseteq$ S. On en déduit l'égalité : S $= \mathscr{G}(a_1, \ldots, a_n)$.

Passons à présent à la démonstration du théorème et montrons que tout minterme non nul de $a_1, \ldots, a_n$ est un atome de $\mathscr{G}(a_1, \ldots, a_n)$. Soit $m \neq 0$ un minterme de $a_1, \ldots, a_n$. D'après le théorème 1.28, il existe au moins un atome $a \in \mathscr{G}(a_1, \ldots, a_n)$ tel que $a \leqslant m$. Or a est une somme de monôme (d'après la première partie de la démonstration) : $a = \sum_{i=1}^{p} u_i$ où chaque u_i est un monôme. Supposons que les u_i soient distincts avec $p \geqslant 2$. Alors $a = u_1 + \cdots + u_p$. On ne peut avoir $a = u_1$ ou $a = 0$ donc :

$$u_1 a = u_1 \left(u_1 + \cdots + u_p\right) = u_1 u_1 + u_1 u_2 + \cdots + u_1 u_p = u_1$$

et $u_1 \leqslant a$ ce qui est absurde pour un atome. L'hypothèse $p \geqslant 2$ est fausse et $p = 1$ d'où $u_1 = a$.

Considérons à présent am : on a soit $am = 0$ (il existe dans a un littéral complémenté dans m), soit $am = m$ (tous les littéraux de a sont dans m). Or le cas $am = 0$ est impossible car $a \leqslant m$ donc $am = a \neq 0$. D'où $a = m$.

Il reste à prouver que tout atome de $\mathscr{G}(a_1, \ldots, a_n)$ est un minterme non nul de $a_1, \ldots, a_n$.

Soit a un atome de $\mathscr{G}(a_1, \ldots, a_n)$. Nous avons vu précédemment que a était obligatoirement un monôme. Supposons que a ne soit pas un minterme : alors il existe un littéral a_i tel que ni a_i, ni $\bar{a}_i$ ne figure dans a. Les éléments $a_i a$ et $\bar{a}_i a$ sont strictement inférieurs à l'atome a, donc ils sont nuls : $a_i a = a$ et $\bar{a}_i a = 0$. D'où :

$$0 = a_i a + \bar{a}_i a = (a_i + \bar{a}_i)a = 1a = a$$

Absurde. Donc a est un minterme de $a_1, \ldots, a_n$. □

Remarque. Les propriétés des atomes du théorème 1.29 s'appliquent aux mintermes de $\mathscr{G}(a_1, \ldots, a_n)$ et les propriétés duales aux maxtermes :

1. Le produit de deux mintermes distincts est nul. La somme de deux maxtermes distincts est égale à 1.
2. La somme de tous les mintermes est égale à 1. Le produit de tous les maxtermes est égal à 0.
3. Tout élément de $\mathscr{G}(a_1, \ldots, a_n)$ s'écrit de manière unique sous la forme d'une somme de mintermes distincts, non nuls et sous la forme d'un produit de maxtermes distincts différents de 1.

   En conséquence, deux sommes de mintermes sont égales si et seulement si les mintermes qui ne sont pas communs aux deux sommes valent 0.
4. Lorsqu'un élément a de $\mathscr{G}(a_1, \ldots, a_n)$ est écrit sous la forme de somme de mintermes distincts (resp. de produit de maxtermes distincts), son complément $\bar{a}$ est la somme de tous les autres mintermes (resp. le produit de tous les autres maxtermes).
5. Le nombre total d'éléments de $\mathscr{G}(a_1, \ldots, a_n)$ est 2^p où p est le nombre de mintermes non nuls de $a_1, \ldots, a_n$, ou encore le nombre de maxtermes de $a_1, \ldots, a_n$ différents de 1.

Définition 1.38.

1. On appelle décomposition canonique disjonctive d'un élément a de $\mathscr{G}(a_1, \ldots, a_n)$ la somme de mintermes (distincts et non nuls) de $a_1, \ldots, a_n$ égale à cet élément.
2. On appelle décomposition canonique conjonctive d'un élément a de $\mathscr{G}(a_1, \ldots, a_n)$ le produit des maxtermes (distincts et différents de 1) de $a_1, \ldots, a_n$ et égal à cet élément.

Exemple. Soient $a, b, c \in (\mathrm{B}, +, \cdot, \bar{})$ et $e \in \mathscr{G}(a, b, c)$.

$$e = \overline{\overline{ab}c + b\bar{a}} + a + \bar{b}c$$

Calculons sa décomposition canonique disjonctive.

1. On transforme e en une expression $\Sigma\Pi$ qu'il est inutile de simplifier complètement.

$$e = \overline{\overline{ab}c} \cdot \overline{b\bar{a}} + a + \bar{b}c = (ab + \bar{c})(\bar{b} + a) + a + \bar{b}c = a + \bar{b}c + \bar{b}\bar{c}$$

2. On introduit pour chaque mônome les littéraux manquants, puis on développe et on élimine les mintermes superflus.

$$\begin{aligned} e &= a(b + \bar{b})(c + \bar{c}) + (a + \bar{a})\bar{b}c + (a + \bar{a})\bar{b}\bar{c} \\ &= abc + ab\bar{c} + a\bar{b}c + a\bar{b}\bar{c} + a\bar{b}c + \bar{a}\bar{b}c + a\bar{b}\bar{c} + \bar{a}\bar{b}\bar{c} \\ &= abc + ab\bar{c} + a\bar{b}c + a\bar{b}\bar{c} + \bar{a}\bar{b}c + \bar{a}\bar{b}\bar{c} \end{aligned}$$

   Lorsque certains termes sont nuls, on simplifie en conséquence.

Définition 1.39.

1. Une partie $S = \{a_1, \ldots, a_n\}$ de n éléments d'une algèbre de Boole est libre lorsque les 2^n mintermes de $a_1, \ldots, a_n$ sont différents de 0. On dit aussi que $a_1, \ldots, a_n$ sont booléennement indépendants. Dans le cas contraire, on dit liée ou booléennement dépendants.
2. Une partie $S = \{a_1, \ldots, a_n\}$ de n éléments d'une algèbre de Boole B est génératrice de B lorsque la sous algèbre $\mathscr{G}(a_1, \ldots, a_n)$ est égale à B. On dit encore que $\{a_1, \ldots, a_n\}$ est un système de générateurs de B.
3. Une base d'une algèbre de Boole est une partie libre et génératrice de cette algèbre.

Théorème 1.32.

1. *Lorsqu'une partie finie* S *de l'algèbre de Boole* B *est libre, toute partie* S′ *obtenue en remplaçant un nombre quelconque d'éléments de* S *par leurs compléments est aussi libre.*
2. *Soient* S *et* S′ *deux parties finies de* B *telles que* $S \subseteq S'$ *: alors si* S′ *est libre,* S *est libre et si* S *est liée,* S′ *est liée.*

Démonstration.

1. Par définition, les 2^n mintermes des n éléments de S′ sont identiques aux 2^n mintermes des n éléments de S. Ils sont donc tous différents de 0.
2. Posons $S = \{a_1, \ldots, a_n\}$ et $S' = S \cup \left\{a'_1, \ldots, a'_p\right\}$. Supposons S′ libre. Soit m un minterme de S. Considérons $ma'_1 \ldots a'_p$: c'est un minterme de S′. Or S′ étant libre, ce minterme est non nul. Donc $m \neq 0$. Tout minterme de S est donc non nul et S est libre.

   La seconde propriété est la contraposée.

□

Théorème 1.33. *Soit* B *une algèbre de Boole ayant un nombre* 2^n *éléments. Soit* p *le plus grand entier tel que* $2^p \leqslant n$. *Toute partie libre de* B *admet au plus* p *éléments et il existe au moins une partie libre de* B *ayant* p *éléments.*

Démonstration. Supposons qu'une partie libre $\{a_1, \ldots, a_q\}$ possède plus que p éléments : $q > p$. Par définition de p, $n < 2^q$. Les 2^q mintermes de $a_1, \ldots, a_q$ sont tous non nuls. Or d'après la remarque 5 suivant le théorème 1.31, on doit avoir conjointement que $\operatorname{card} \mathscr{G}(a_1, \ldots, a_q) = 2^{2^q} > 2^n = \operatorname{card} \mathrm{B}$. Ceci est absurde car $\mathscr{G}(a_1, \ldots, a_q) \subseteq \mathrm{B}$.

Montrons l'existence d'une partie libre à p éléments.

1. Montrons d'abord que si n est une puissance de 2, $n = 2^p$, il existe une partie libre de B ayant p éléments. Grâce au théorème de Stone, il suffit de le prouver pour les algèbres de Boole de la forme $\mathscr{P}(\mathrm{E}_{2^p})$ où $\mathrm{E}_k = \mathbb{N}_k^*$. Procédons par récurrence sur p.
   - Si $p = 1$, $\mathscr{P}(\mathrm{E}_2) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. $\{1\}$ est une partie libre de $\mathscr{P}(\mathrm{E}_2)$ à un élément.
   - Supposons si $n = 2^p$ que $\mathscr{P}(\mathrm{E}_n)$ admette une partie libre à p éléments. Considérons $n' = 2^{p+1}$. Par hypothèse de récurrence, il existe dans $\mathscr{P}(\mathrm{E}_n)$ une partie libre à p éléments : S. Or $n' = 2n$. Construisons la partie S′ de $\mathscr{P}(\mathrm{E}_{n'})$ de la façon suivante : considérons les p éléments de S : ce sont des parties de E_n. À chacune de ces parties, rajoutons des éléments avec le procédé suivant : si $i \in \mathbb{N}_n^*$ est dans S, on rajoute $i + n$, ceci pour tout i de la partie. On obtient ainsi p parties de $\mathrm{E}_{n'}$. À ces p parties on rajoute une $(p+1)^{\mathrm{e}}$, E_n lui même. On désigne par S′ l'ensemble de ces $(p+1)$ parties de $\mathrm{E}_{n'}$. Montrons que S′ est une partie libre de $\mathscr{P}(\mathrm{E}_{n'})$.
     Les 2^p mintermes des p premiers éléments de S′ contiennent au moins un $i \in \mathbb{N}_n^*$, et donc un $j \in \complement_{\mathbb{N}_{2n}^*} \mathbb{N}_n^*$, $j = i+n$, car S est libre par hypothèse de récurrence.
     Les 2^{p+1} mintermes des $(p+1)$ éléments de S′ sont obtenus en faisant l'intersection d'un minterme précédent avec $\mathrm{E}_n = \{1, \ldots, n\}$ ou son complément dans E_{2n}, $\{n+1, \ldots, n+n\}$. Cette intersection contient soit i, soit $i + n$: elle n'est donc pas vide, et par conséquent S′ est libre.
2. Supposons que n ne soit pas une puissance de 2 et soit p le plus grand entier tel que $2^p < n$. Montrons qu'il existe une partie libre de $\mathscr{P}(\mathrm{E}_n)$ ayant exactement p éléments. Remarquons que $\mathrm{E}_{2^p} = \mathbb{N}_{2^p}^* \subseteq \mathrm{E}_n = \mathbb{N}_n^*$. Or d'après ce qui précède, $\mathscr{P}(\mathrm{E}_{2^p})$ contient une partie libre S ayant p éléments. Or tout élément de S est une partie de E_{2^p}, donc de E_n. Donc S est une partie libre de $\mathscr{P}(\mathrm{E}_n)$.

□

Exemple. Considérons $E_4 = \{1,2,3,4\}$ et $S = \{a,b\}$ où $a = \{1,2\}$, et $b = \{1,3\}$. Les 2^2 mintermes de S sont :

$$\begin{aligned} a \cap b &= \{1\} \\ a \cap \bar{b} &= \{2\} \\ \bar{a} \cap b &= \{3\} \\ \bar{a} \cap \bar{b} &= \{4\} \end{aligned}$$

Aucun n'est nul, donc S est libre. Alors :

$$\begin{aligned} E_{2\times 4} = E_8 &= \{1,2,3,4,1+4,2+4,3+4,4+4\} \\ &= \{1,2,3,4,5,6,7,8\} \\ S' &= \{\{1,2,5,6\},\{1,3,5,7\},\{1,2,3,4\}\} \end{aligned}$$

Notons $A = \{1,2,5,6\}$, $B = \{1,3,5,7\}$ et $C = \{1,2,3,4\}$. Les 2^3 mintermes de S' sont :

$$\begin{aligned} A \cap B \cap C &= \{1\} \\ A \cap B \cap \bar{C} &= \{5\} \\ A \cap \bar{B} \cap C &= \{2\} \\ A \cap \bar{B} \cap \bar{C} &= \{6\} \\ \bar{A} \cap B \cap C &= \{3\} \\ \bar{A} \cap B \cap \bar{C} &= \{7\} \\ \bar{A} \cap \bar{B} \cap C &= \{4\} \\ \bar{A} \cap \bar{B} \cap \bar{C} &= \{8\} \end{aligned}$$

Cette partie est donc libre dans $\mathscr{P}(E_8)$.

Théorème 1.34. *Soit* $S = \{a_1, \ldots, a_n\}$ *une partie d'une algèbre de Boole* B. *Les propositions suivantes sont équivalentes :*

1. S *est une partie génératrice de* B.
2. *Les mintermes non nuls de* $a_1, \ldots, a_n$ *sont les atomes de* B.
3. *Tout élément de* B *s'écrit d'une manière unique sous la forme d'une somme de mintermes (distincts, non nuls) de* $a_1, \ldots, a_n$.

Démonstration. $1 \Rightarrow 2$. Les mintermes non nuls de $a_1, \ldots, a_n$ sont les atomes de $\mathscr{G}(a_1, \ldots, a_n)$ (théorème 1.31). Or par hypothèse $B = \mathscr{G}(a_1, \ldots, a_n)$, donc les mintermes non nuls de $a_1, \ldots, a_n$ sont les atomes de B.

$2 \Rightarrow 3$. Conséquence immédiate du 4 du théorème 1.29.

$3 \Rightarrow 1$. $a_1, \ldots, a_n \in \mathrm{B}$ donc $\mathscr{G}(a_1, \ldots, a_n) \subseteq \mathrm{B}$. Inversement, toute somme de mintermes de $a_1, \ldots, a_n$ appartient à $\mathscr{G}(a_1, \ldots, a_n)$. Donc tout élément de B appartient à $\mathscr{G}(a_1, \ldots, a_n)$. D'où l'égalité. □

Théorème 1.35.

1. *Lorsqu'une partie* S *est génératrice, toute partie* S′ *obtenue en remplaçant un nombre quelconque d'éléments de* S *par leurs compléments est aussi génératrice.*
2. *Soient* S *et* S′ *deux parties d'une algèbre de Boole* B *telles que* $\mathrm{S} \subseteq \mathrm{S}'$. *Si* S *est génératrice,* S′ *l'est aussi.*

Démonstration.

1. L'ensemble des 2^n mintermes des éléments de S′ est égal à l'ensemble des 2^n mintermes des éléments de S (si $\operatorname{card} \mathrm{S} = n$). Les atomes de B sont donc les mintermes non nuls des éléments de S′. D'après le théorème 1.34, S′ engendre B.
2. Soient $\mathrm{S} = \{a_1, \ldots, a_n\}$ et $\mathrm{S}' = \mathrm{S} \cup \left\{a'_1, \ldots, a'_p\right\}$. Alors $\mathscr{G}(a_1, \ldots, a_n) \subseteq \mathscr{G}(a_1, \ldots, a_n, a'_1, \ldots, a'_p) \subseteq \mathrm{B}$. Or S est une partie génératrice de B, donc $\mathscr{G}(a_1, \ldots, a_n) = \mathrm{B}$. Les inclusions deviennent donc des égalités et $\mathscr{G}(a_1, \ldots, a_n, a'_1, \ldots, a'_p) = \mathrm{B}$. Donc S′ engendre B.

□

Théorème 1.36. *Soit* B *une algèbre de Boole finie ayant* 2^n *éléments. Soit* q *le plus petit entier tel que* $n \leqslant 2^q$. *Toute partie génératrice de* B *admet au moins* q *éléments, et il existe au moins une partie génératrice de* B *à* q *éléments.*

Démonstration. Montrons d'abord que toute partie génératrice de B admet a au moins q éléments. Supposons que $\mathrm{S} = \{a_1, \ldots, a_r\}$ soit une partie génératrice de B avec $r < q$. Alors le nombre de mintermes non nuls m est inférieur ou égal à 2^r. Or nous savons que $\mathrm{B} = \mathscr{G}(a_1, \ldots, a_r)$ et que $\operatorname{card} \mathscr{G}(a_1, \ldots, a_r) = 2^m \leqslant 2^{2^r}$. Or $r < q$, ce qui contredit la définition de q.

Montrons qu'il existe une partie génératrice de B à q éléments.

1. Supposons tout d'abord que $n = 2^q$ et montrons qu'il existe une partie génératrice de B ayant q éléments. Nous savons d'après le théorème 1.33 que B possède une partie libre à q éléments, $\mathrm{S} = \left\{a_1, \ldots, a_q\right\}$. Les 2^q mintermes non nuls de $a_1, \ldots, a_q$ sont les atomes de la sous algèbre $\mathscr{G}(a_1, \ldots, a_q)$. D'où $\operatorname{card} \mathscr{G}(a_1, \ldots, a_q) = 2^{2^q} = 2^n = \operatorname{card} \mathrm{B}$. D'où $\mathscr{G}(a_1, \ldots, a_q) = \mathrm{B}$ et S est une partie génératrice de B.

2. Si n n'est pas une puissance de 2, soit q le plus petit entier tel que $n < 2^q$. Montrons qu'il existe au moins une partie génératrice avec q éléments. D'après le théorème de Stone, il suffit de le prouver pour les algèbres de Boole de la forme $\mathscr{P}(\mathbb{N}_n^*)$. Posons $E_n = \mathbb{N}_n^*$. Alors $\operatorname{card}\mathscr{P}(E_n) = 2^n$ et $\operatorname{card}\mathscr{P}(E_{2^q}) = 2^{2^q}$ avec $n < 2^q$. D'après 1, $\mathscr{P}(E_{2^q})$ admet une partie génératrice à q éléments, $S = \{A_1, \ldots, A_q\}$. Montrons que $S' = \{A_1 \cap E_n, \ldots, A_q \cap E_n\}$ est une partie génératrice de $\mathscr{P}(E_n)$.
Toute partie A de E_n est aussi une partie de E_{2^q}, donc A peut s'écrire sous forme de réunion de mintermes $A_1, \ldots, A_q$: $A = \bigcup_j m_j$ avec m_j un minterme non nul de $A_1, \ldots, A_q$. Donc $A = A \cap E_n = \left(\bigcup_j m_j\right) \cap E_n = \bigcup_j \left(m_j \cap E_n\right)$. Or l'intersection de E_n avec un minterme de $A_1, \ldots, A_q$ est un minterme de $A_1 \cap E_n, \ldots, A_q \cap E_n$:
Supposons que $B_1 \cap \cdots \cap B_q$ soit un minterme de $A_1, \ldots, A_q$. Alors $E_n \cap \left(B_i \cap \cdots \cap B_q\right)$ peut se réecrire de la façon suivante :

$$\bigcap_{j=1}^{q} \left(F_j +_j B_j\right)$$

où

$$F_j = E_n \quad \text{et} \quad +_j = \cap \quad \text{si } B_j = A_j$$
$$F_j = \emptyset \quad \text{et} \quad +_j = \cup \quad \text{si } B_j = \overline{A_j}$$

D'où

$$E_n \cap \left(B_1 \cap \cdots \cap B_q\right) = \bigcap_{j=1}^{q} K_j$$

où

$$K_j = E_n \cap A_j \quad \text{si } B_j = A_j$$
$$K_j = \overline{E_n \cap A_j} \quad \text{si } B_j = \overline{A_j}$$

Donc $S' = \{A_1 \cap E_n, \ldots, A_q \cap E_n\}$ est une partie génératrice de $\mathscr{P}(E_n)$.

□

Exemples.

1. $\left(\mathscr{P}(E_3), \cup, \cap, \bar{}\right)$ contient $2^3 = 8$ éléments. $q = 2$ est le plus petit entier $\mathbb{N}$ tel que $3 < 2^q$. Toute partie génératrice de $\mathscr{P}(E_3)$ possède au moins deux éléments :

$$\{\{1\}, \{2\}\}; \{\{1\}, \{1,2\}\}; \{\{1\}, \{2\}, \{1,3\}\}$$

sont des parties génératrices.

2. $\left(\mathscr{P}(\mathrm{E}_4), \cup, \cap, \bar{}\right)$ contient $2^4 = 16$ éléments. $q = 2$ est le plus petit entier tel que $2 \leqslant 2^q$. Toute partie génératrice de $\mathscr{P}(\mathbb{N}_4^*)$ possède au moins 2 éléments : $\{\{1,2\},\{2,3\}\}$ est une partie génératrice de $\mathscr{P}(\mathbb{N}_4^*)$.

Théorème 1.37. *Une algèbre de Boole ayant 2^n éléments admet une base si et seulement si l'exposant n est une puissance de 2 ($n = 2^p$). Dans ce cas, toutes les bases ont p éléments.*

Démonstration. Soit B une algèbre de Boole ayant 2^n éléments et admettant une base S contenant p éléments. Alors $2^p \leqslant n$ car S est libre et $2^p \geqslant n$ car S est génératrice. D'où $n = 2^p$. Au cours de la démonstration du théorème 1.36 nous avons montré que si n était de la forme $n = 2^p$, il existe une partie libre de B qui est aussi génératrice, donc c'est une base de B. □

Théorème 1.38. *Soit* B *une algèbre de Boole ayant 2^n éléments avec $n = 2^p$. Alors*

1. *Toute partie libre de p éléments de* B *est une base de* B.
2. *Toute partie génératrice de p éléments de* B *est une base de* B.

Démonstration.

1. C'est toujours le théorème 1.36.
2. Soit $\mathrm{S} = \{a_1, \ldots, a_p\}$ une partie génératrice de B. Supposons qu'il y ait un minterme nul parmi les 2^p mintermes de $a_1, \ldots, a_p$. Le nombre de mintermes non nuls m est donc strictement inférieur à 2^p. Or $\operatorname{card} \mathscr{G}(a_1, \ldots, a_p) = 2^m = \operatorname{card} \mathrm{B} = 2^{2^p}$ d'où $m = 2^p$. Contradiction, il n'y a donc pas de minterme nul et S est une partie libre de B, donc une base de B.

□

Définition 1.40. Une fonction booléenne de n variables binaires est une application de $\{0,1\}^n$ vers $\{0,1\}$.

Exemples.

1. Soit $f : \{0,1\}^2 \to \{0,1\}$ définie par

$$\begin{aligned}(0,0) &\mapsto 0\\ (0,1) &\mapsto 1\\ (1,0) &\mapsto 1\\ (1,1) &\mapsto 0\end{aligned}$$

f est une fonction booléenne à deux variables binaires. On peut l'écrire de façon littérale $f(x,y) = \bar{x}y + x\bar{y}$, où x, y et $f(x,y)$ sont dans l'algèbre de Boole $(\{0,1\}, +, \cdot, \bar{})$.

2. Toute expression booléenne des éléments $x_1, \ldots, x_n$ de l'algèbre $(\{0,1\}, +, \cdot, \bar{})$ définit une fonction booléenne. Ainsi l'expression $\bar{x} + \bar{y}z$ donne la fonction à trois variables $f : \{0,1\}^3 \to \{0,1\}$ définie par $(x, y, z) \mapsto \bar{x} + \bar{y}z$. On lui associe la table

x	y	z	$\bar{x} + \bar{y}z$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Remarque. L'ensemble $\mathscr{F}_n$ des fonctions booléennes de n variables contient 2^{N} éléments ($\mathrm{N} = 2^n$). On y définit trois opérations : $\check{+}, \check{\cdot}, \check{\bar{}}$ de la façon suivante

$$\begin{aligned}(f \check{+} g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n)\\ (f \check{\cdot} g)(x_1, \ldots, x_n) &= f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)\\ \check{\bar{f}}(x_1, \ldots, x_n) &= \overline{f(x_1, \ldots, x_n)}\end{aligned}$$

Muni de ces trois opérations, $\mathscr{F}_n$ a une structure d'algèbre de Boole induite par celle de $(\{0,1\}, +, \cdot, \bar{})$. D'après le théorème de Stone, $(\{0,1\}^{\mathrm{N}}, +, \cdot, \bar{})$ et $(\mathscr{F}_n, \check{+}, \check{\cdot}, \check{\bar{}})$ sont isomorphes à $(\mathscr{P}(\mathrm{E}_{\mathrm{N}}), \cup, \cap, \complement)$ donc isomorphes entre elles.

Théorème 1.39. *Soit $\{a_1, \ldots, a_n\}$ une base de $\{0,1\}^{\mathrm{N}}$ ($\mathrm{N} = 2^n$) et prenons un élément quelconque de $\{0,1\}^{\mathrm{N}}$ ($= \mathscr{G}(a_1, \ldots, a_n)$) qui a été écrit sous la forme d'une expression booléenne $f(a_1, \ldots, a_n)$. Soit $\Psi : \{0,1\}^{\mathrm{N}} \to \mathscr{F}_n$ qui à cet élément associe la fonction booléenne f de $\{0,1\}^{\mathrm{N}}$ dans $\{0,1\}$*

$$\begin{aligned}\Psi :&\{0,1\}^{\mathrm{N}} \to \mathscr{F}_n\\ &f(a_1, \ldots, a_n) \mapsto f\end{aligned}$$

Alors Ψ est un isomorphisme d'algèbre de Boole.

Démonstration. Soient $\{a_1, \ldots, a_n\}$ une base de $\{0,1\}^{\mathrm{N}}$ et $a = f(a_1, \ldots, a_n)$, $b = g(a_1, \ldots, a_n)$. Si $a \neq b$, leurs décompositions disjonctives sont donc différentes donc f et g sont différentes et Ψ est injective. Or $\mathrm{card}\{0,1\}^{\mathrm{N}} = 2^{\mathrm{N}} = \mathrm{card}\,\mathscr{F}_n$. D'où Ψ est bijective. La propriété d'homomorphisme se montre facilement. □

Remarques.

1. Il existe 2^N fonctions booléennes à n variables ($N = 2^n$), ce nombre croît très vite avec la valeur de n.

$$\begin{aligned} n &= 2 & 2^{2^2} &= 16 \\ n &= 3 & 2^{2^3} &= 256 \\ n &= 4 & 2^{2^4} &= 65536 \\ n &= 5 & 2^{2^5} &= 4294967296 \end{aligned}$$

2. On définit pour les fonctions booléennes, comme pour les expressions booléennes, une forme normale disjonctive (F.N.D.) et une forme normale conjonctive (F.N.C.). On utilise, pour les écrire à partir de la table des valeurs de la fonction, le procédé suivant :
   - Pour la F.N.D. : on repère les vecteurs binaires correspondant aux valeurs 1 de la fonction. Ensuite on écrit le minterme correspondant et enfin on fait la somme de ces mintermes. Pour $f(x,y,z) = \bar{x} + \bar{y}z$

$$f(x,y,z) = \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}z$$

   - Pour la F.N.C. : on repère les vecteurs binaires ayant pour image 0. Ensuite on écrit le maxterme correspondant, puis on fait le produit de ces maxtermes. Pour écrire le maxterme correspondant au vecteur dont l'image est 0, on écrit le littéral correspondant s'il est égal à 0 et son complément s'il est égal à 1. Pour $f(x,y,z) = \bar{x} + \bar{y}z$

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

Chapitre 2

Logique

2.1 Calcul propositionnel

Définition 2.1. Une proposition est un énoncé déclaratif susceptible de vérité ou de fausseté.

Exemple. « Il pleut » est une proposition. « Quelle heure est-il ? » n'est pas une proposition, « Apprenez vos leçons ! » non plus.

Notation. Si p et q sont deux propositions quelconques, p : V (ou $p : \not{1}$) se lira : la valeur de vérité de la proposition p est « vrai ». p : F (ou $p : \not{0}$) se lira : la valeur de vérité de la proposition p est « faux ». V et F s'appellent les valeurs de vérité.

Remarque. Dans la logique classique, il n'y a que ces deux valeurs de vérité. Dans les logiques contemporaines (logique floue) il peut y en avoir plusieurs et même une infinité organisée en treillis.

2.1.1 Les formules

Définition 2.2. On appelle variable propositionnelle tout élément d'un ensemble P non vide, fini ou infini. En général on utilisera les lettres de l'alphabet, éventuellement affectées d'indices.

On appelle symbole de connecteur propositionnel tout élément d'un ensemble $S = \{\neg, \vee, \wedge, \Rightarrow, \Longleftrightarrow\}$ qu'on lit « non », « ou », « et », « implique », « équivaut à » et que l'on suppose ne pas appartenir à P.

On appelle « parenthèse ouvrante » et « parenthèse fermante » les deux symboles « (» et «) » que l'on suppose ne pas appartenir à $P \cup S$.

Définition 2.3. 1. Toute variable propositionnelle est une formule.

2. Si F est une formule, ¬(F) est une formule.
3. Si F et G sont des formules, (F ∧ G), (F ∨ G), (F ⇒ G) et (F ⟺ G) sont aussi des formules.
4. Rien n'est une formule, sauf ce qu'on a obtenu par application des règles 1, 2, 3.

Exemple.

1. $\neg(p \Rightarrow q)$ est une formule.
2. $\big((\neg p \Rightarrow q) \vee (p \Rightarrow \neg q)\big) \wedge \big((p \wedge q) \vee (\neg p \wedge \neg q)\big)$ est une formule.
3. (n'est pas une formule.
4. $pq\vee ==\Rightarrow)($ n'est pas une formule.

2.1.2 Règles de simplification de l'écriture

1. Suppression des parenthèses placées de part et d'autre d'une variable propositionnelle : ¬(A) s'écrit ¬A, (A) ∨ (B) s'écrit A ∨ B.
2. Suppression des parenthèses qui séparent des négations consécutives.

$$\neg(\neg(\neg(\neg(\neg(A \vee B))))) \quad \text{s'écrit} \quad \neg\neg\neg\neg\neg(A \vee B)$$

3. Règle de préséance entre les connecteurs : on convient que ∨ et ∧ dominent ¬, on convient que ⇒ et ⟺ dominent ∨ et ∧. Par exemple : ¬A ∨ B ⇒ C doit se lire (¬(A) ∨ (B)) ⇒ (C).

$$\begin{array}{c} (((\neg(A) \vee (B)) \Rightarrow (C)) \iff ((\neg(\neg(B))) \wedge (\neg(C))) \\ \downarrow \\ (\neg A \vee B \Rightarrow C) \iff (\neg\neg B \wedge \neg C) \end{array}$$

2.1.3 Notation polonaise (de Łukasienviez)

Cette notation permet de ne pas utiliser de parenthèse. On utilise les connecteurs comme des symboles de fonction à une ou deux places : elle réduit le nombre de symbole mais ne facilite pas la lecture.

Exemple.

1. (A ∨ B) ⇒ (¬B ⇒ (C ∨ D)) s'écrira ⇒ ∨AB ⇒ ¬B ∨ CD
2. (¬A ∨ B ⇒ C) ⟺ (¬¬B ∧ ¬C) devient ⇒ ∨¬ABC ∧ ¬¬B¬C

2.1.4 Valeur de vérité d'une formule

On va définir les valeurs de vérité des formules élémentaires. Le mode de construction des formules plus complexes permettra toujours de s'y ramener.

1. La négation.

p	$\not 0$	$\not 1$
$\neg p$	$\not 1$	$\not 0$

2. La conjonction.

p	q	$p \wedge q$
$\not 0$	$\not 0$	$\not 0$
$\not 0$	$\not 1$	$\not 0$
$\not 1$	$\not 0$	$\not 0$
$\not 1$	$\not 1$	$\not 1$

3. La disjonction.

p	q	$p \vee q$
$\not 0$	$\not 0$	$\not 0$
$\not 0$	$\not 1$	$\not 1$
$\not 1$	$\not 0$	$\not 1$
$\not 1$	$\not 1$	$\not 1$

4. L'implication,

p	q	$p \Rightarrow q$
$\not 0$	$\not 0$	$\not 1$
$\not 0$	$\not 1$	$\not 1$
$\not 1$	$\not 0$	$\not 0$
$\not 1$	$\not 1$	$\not 1$

5. La double implication,

p	q	$p \wedge q$
$\not 0$	$\not 0$	$\not 1$
$\not 0$	$\not 1$	$\not 0$
$\not 1$	$\not 0$	$\not 0$
$\not 1$	$\not 1$	$\not 1$

Le nombre de tables de vérité que l'on peut construire ne dépend que du nombre de variables utilisées : si une formule a n variables, sa table correspondra à l'une des 2^{2^n} applications de $\{\not 0, \not 1\}^n$ dans $\{\not 0, \not 1\}$. Le nombre de formules à n variables est infini. Par contre le nombre de tables possibles est fini. On en profite pour « classer » ces formules en comparant leurs tables de vérité.

Définition 2.4. Deux formules F et G du calcul propositionnel (C.P.) sont dites synonymes si elles contiennent les mêmes variables et que leurs tables de vérité sont identiques.

Remarque. On peut élargir cette définition à des formules qui n'ont pas exactement le même nombre de variables, à condition qu'il y en ait une qui contient l'ensemble des variables de l'autre, si toute distribution de valeurs de vérité appliquée aux variables communes donne la même valeur aux formules.

Notation. F synonyme de G s'écrira $F \equiv G$.

Exemples. $p \Rightarrow q \equiv \neg p \vee q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$, $\neg(p \wedge q) \equiv \neg p \vee \neg q$.

Définition 2.5. On dira qu'une formule est une tautologie si quelques soient les valeurs de vérité affectées à ses variables, la valeur de vérité de cette formule est toujours « vrai » ($\mathcal{V}$).

Exemple. $p \vee \neg p$, $(p \Rightarrow q) \iff (\neg p \vee q)$

Définition 2.6. On dira qu'une formule est une contradiction, ou une antilogie, si quelques soient les valeurs de vérité affectées à ses variables, la valeur de vérité de cette formule est toujours « faux » ($\mathcal{F}$).

Exemple. $p \wedge \neg p$, $\neg((p \Rightarrow q) \iff (\neg q \Rightarrow \neg p))$.

2.1.5 Formes normales, disjonctives et conjonctives

Définition 2.7. Soit F une formule.

1. On appellera forme disjonctive (resp. conjonctive) de F, toute formule synonyme de F qui sera écrite avec les mêmes variables sous forme de disjonctions de conjonctions de ces variables ou de leurs négations (resp. de conjonctions de disjonctions des ces variables ou de leurs négations).
2. On appellera forme normale disjonctive (distinguée) de la formule F, que l'on notera F.N.D. toute forme disjonctive de F dont tous les membres conjonctifs contiennent une fois et une seule chaque variable figurant dans F, précédée du signe $\neg$ ou pas. On définit la forme normale conjonctive dans le même tonneau.

Remarque. Si F a pour variables propositionnelles $A_1, \ldots, A_n$ alors sa forme normale disjonctive a pour allure $\bigvee_{i\in I}(\bigwedge_{j\in\mathbb{N}_n^*} B_j)$ où $B_j \in \{ A_1, \ldots, A_n, \neg A_1, \ldots, \neg A_n \}$, et sa forme normale conjonctive a pour allure $\bigwedge_{i\in I}(\bigvee_{j\in\mathbb{N}_n^*} B_j)$.

Théorème 2.1. *Toute formule* F *admet une forme normale disjonctive et une forme normale conjonctive.*

Démonstration. Toute formule possède un nombre fini de variables propositionnelles. Sa table de vérité est donc la table d'une fonction booléenne. L'algorithme décrit dans la deuxième remarque suivant le théorème 1.39 du chapitre I nous donne sa forme normale disjonctive et sa forme normale conjonctive. Il suffit de remplacer $+$ par $\vee$, $\cdot$ par $\wedge$ et $\bar{}$ par $\neg$. □

2.1.6 Conséquence tautologique et compacité

Définition 2.8. Soient A et B deux ensembles de formules du calcul propositionnel.

1. On dit que A est satisfiable s'il existe une distribution de valeurs de vérité qui satisfait A, c'est à dire qui donne la valeur « vrai » à toute formule de A. Cette distribution est alors appelée modèle de A. On dit aussi que A est compatible. Dans le cas contraire on dit que A est incompatible.
2. On dit que A est finiment satisfiable si tout sous ensemble fini de A est satisfiable.
3. On dit que la formule G est une conséquence tautologique de A, ce que l'on notera $A \models G$, si tout modèle de A est un modèle de G.
4. On dit que A et B sont équivalents si toute formule de A est conséquence tautologique de B, et toute formule de B conséquence tautologique de A.

Remarque. Au lieu de « compatible » et « incompatible » on dit aussi « consistant » et « inconsistant » (« contradictoire »).

Théorème 2.2. *Pour tout ensemble* A *de formules du calcul propositionnel,* A *est satisfiable si et seulement si* A *est finiment satisfiable.*

Démonstration. Hors programme, nécessite le théorème de Tychonoff. □

On pourrait énoncer ce théorème de deux autres façons :

1. Pour tout ensemble A de formules du calcul propositionnel, A est contradictoire si et seulement si A admet un sous ensemble fini contradictoire.
2. Pour tout ensemble A de formules du calcul propositionnel et pour toute formule F, F est une conséquence tautologique de A si et seulement si F est une conséquence tautologique d'une partie finie de A.

2.1.7 Déduction formelle en calcul propositionnel

On écrira $\Sigma \vdash A$ si l'on peut obtenir la formule A à partir de l'ensemble de formules Σ par simple application de ces règles, que l'on nomme en général « règles primitives ».

Par convention, Σ est un ensemble de propositions appelées prémisses, A et B des propositions, et les ensembles $\Sigma \cup \{A\}$ et $\Sigma \cup \Sigma'$ seront notés respectivement Σ, A et Σ, Σ'. Le signe $\vdash$ se lit « produit » ou « donne ». L'écriture $\Sigma \vdash A$ n'est pas une formule du langage, mais une proposition du métalangage.

1. (Ref) Réflexivité :
   $A \vdash A$.
2. $(+)$ Addition des prémisses :
   Si $\Sigma \vdash A$,
   alors $\Sigma, \Sigma' \vdash A$.
3. $(\neg -)$ $\neg$-élimination :
   Si $\Sigma, \neg A \vdash B$,
   $\Sigma, \neg A \vdash \neg B$,
   alors $\Sigma \vdash A$.
4. $(\Rightarrow -)$ $\Rightarrow$-élimination :
   Si $\Sigma \vdash A \Rightarrow B$,
   $\Sigma \vdash A$,
   alors $\Sigma \vdash B$.
5. $(\Rightarrow +)$ $\Rightarrow$-introduction :
   Si $\Sigma, A \vdash B$,
   alors $\Sigma \vdash A \Rightarrow B$.
6. $(\wedge -)$ $\wedge$-élimination :
   Si $\Sigma \vdash A \wedge B$,
   alors $\Sigma \vdash A$,
   $\Sigma \vdash B$.
7. $(\wedge +)$ $\wedge$-introduction :
   Si $\Sigma \vdash A$,
   $\Sigma \vdash B$,
   alors $\Sigma \vdash A \wedge B$.
8. $(\vee -)$ $\vee$-élimination :
   Si $\Sigma, A \vdash C$,
   $\Sigma, B \vdash C$,
   alors $\Sigma, A \vee B \vdash C$.
9. $(\vee +)$ $\vee$-introduction :
   Si $\Sigma \vdash A$,

alors $\Sigma \vdash A \vee B$,
$\Sigma \vdash B \vee A$.

10. $(\Longleftrightarrow -) \Longleftrightarrow$-élimination :
Si $\Sigma \vdash A \Longleftrightarrow B$,
$\Sigma \vdash A$,
alors $\Sigma \vdash B$.
Si $\Sigma \vdash A \Longleftrightarrow B$,
$\Sigma \vdash B$,
alors $\Sigma \vdash A$.
11. $(\Longleftrightarrow +) \Longleftrightarrow$-introduction :
Si $\Sigma, A \vdash B$,
$\Sigma, B \vdash A$,
alors $\Sigma \vdash A \Longleftrightarrow B$.
12. $(\in)$ appartenance :
Si $A \in \Sigma$,
alors $\Sigma \vdash A$.

Définition 2.9. On dit que A se déduit formellement de Σ, ce que l'on notera $\Sigma \vdash A$, si et seulement si $\Sigma \vdash A$ est obtenu en appliquant un nombre fini de fois les règles de déduction formelles.

Autrement dit, $\Sigma \vdash A$ si et seulement s'il existe une suite finie $\Sigma_1 \vdash A_1$, $\Sigma_2 \vdash A_2$, ..., $\Sigma_n \vdash A_n$ telle que chaque terme $\Sigma_k \vdash A_k$ $(k = 2, \ldots, n)$ est engendré à partir d'une règle de déduction formelle à partir d'un ou de plusieurs termes le précédant, et que $\Sigma_n = \Sigma$ et $A_n = A$. La suite $\Sigma_1 \vdash A_1$, ..., $\Sigma_n \vdash A_n$ s'appelle preuve formelle de $\Sigma \vdash A$.

Exemples.

1. Prouvons $(\in)$: si $A \in \Sigma$ alors $\Sigma \vdash A$. Soit $\Sigma' = \Sigma - \{A\}$.
   (a) $A \vdash A$
   (b) $A, \Sigma' \vdash A$
2. Supposons $\Sigma = \{A \Rightarrow B, B \Rightarrow C\}$. On voudrait $\Sigma \vdash A \Rightarrow C$.
   (a) $\Sigma, A \vdash A \Rightarrow B$ d'après $(\in)$
   (b) $\Sigma, A \vdash A$ d'après $(\in)$
   (c) $\Sigma, A \vdash B$ d'après $(\Rightarrow -)$ et (a), (b)
   (d) $\Sigma, A \vdash B \Rightarrow C$ d'après $(\in)$
   (e) $\Sigma, A \vdash C$ d'après $(\Rightarrow -)$ et (c), (d)
   (f) $\Sigma \vdash A \Rightarrow C$ d'après $(\Rightarrow +)$ et (e)

2.1.8 Complétude du calcul propositionnel

Théorème 2.3. *Dans le calcul propositionnel, si* $\Sigma \vDash A$ *alors* $\Sigma \vdash A$ *et réciproquement.*

Démonstration. Hors programme. □

2.2 La logique du premier ordre

2.2.1 Introduction

Examinons le raisonnement suivant : Si Napoléon était mexicain, il aurait été américain ; il n'était pas américain donc il n'était pas mexicain. Si on pose P = Napoléon mexicain et Q = Napoléon américain, ce raisonnement pourrait être schématisé par : $P \Rightarrow Q, \neg Q \Rightarrow \neg P$.

Par contre : Titi est un canari, les canaris ne sont pas migrateurs, donc Titi n'est pas migrateur. Ce raisonnement ne peut s'écrire que sous la forme $P, Q \vdash R$ en calcul propositionnel, ce qui ne peut faire l'objet d'une démonstration. Le raisonnement ici a la forme suivante : m a la propriété F, aucun n'ayant la propriété F n'a la propriété G, donc m n'a pas la propriété G.

On a donc la nécessité d'introduire des symboles de relation décrivant le fait d'avoir une propriété. On les appellera des « prédicats ». De plus, pour décrire les situations où certains possèdent une propriété, ou bien où tous possèdent cette propriété, nous utiliserons des symboles appelés « quantificateurs ».

2.2.2 La syntaxe

Définition 2.10. Le langage du premier ordre, ou langage des prédicats, est un ensemble L de symboles qui se compose de deux parties :

1. La première est constituée :
   - d'un ensemble infini dénombrable $\mathcal{V} = \{v_0, v_1, \ldots, v_n, \ldots\}$ dont les éléments sont appelés variables,
   - des parenthèse « (» et «) »,
   - des symboles de connecteurs $\{\neg, \vee, \wedge, \Rightarrow, \Longleftrightarrow\}$,
   - de deux nouveaux symboles :
     - $\forall$ appelé quantificateur universel, et qui se lit « quelque soit », ou « pour tout »,
     - $\exists$ appelé quantificateur existentiel, et qui se lit « il existe », ou « pour au moins un ».

2. La seconde est la réunion d'un ensemble $\mathscr{C}$ et de deux suites $(\mathrm{F}_n)_{n\in\mathbb{N}}$ et $(\mathrm{R}_n)_{n\in\mathbb{N}}$ d'ensembles deux à deux disjoints et tous deux disjoints de $\mathscr{C}$.
   – Les éléments de $\mathscr{C}$ sont appelés symboles de constantes.
   – Pour chaque entier $n \geqslant 1$, les éléments de F_n sont appelés symboles de fonctions (ou symboles fonctionnels) à n places (ou à n argument, ou n-aires, ou d'arité n), et les éléments de R_n sont appelés symboles de relations (ou symboles de prédicats, ou symboles relationnels) à n places (ou à n arguments, ou n-aire, ou d'arité n).

Remarque. Le plus souvent on distingue un symbole $\simeq$, ou $\approx$, appelé symbole d'égalité ; c'est un élément de R_2.

Définition 2.11. L'ensemble $\mathscr{T}(\mathrm{L})$ des termes du langage L est le plus petit sous ensemble de $\mathscr{M}(\mathrm{L})$, l'ensemble des mots de L (ou suite finie de symboles de L), qui :

1. contient les variables et les symboles de constantes ($\mathscr{V} \cup \mathscr{C}$),
2. est stable, pour chaque entier $n \geqslant 1$ et chaque $f \in \mathrm{F}_n$ pour l'opération $(m_1, \ldots, m_n) \mapsto f\, m_1 \ldots m_n$ où $m_1, \ldots, m_n$ sont des termes.

Définition 2.12. L'ensemble $\mathscr{A}(\mathrm{L})$ des formes atomiques du langage L est constitué de deux types de formules :
– Si R est une relation n-aire, $t_1, \ldots, t_n$ sont des termes du langage, $\mathrm{R}t_1 \ldots t_n$ est une formule atomique.
– Si t_1 et t_2 sont deux termes de L, $\simeq (t_1, t_2)$ est une formule atomique (en général on écrit $t_1 \simeq t_2$).

Définition 2.13. L'ensemble $\mathscr{F}(\mathrm{L})$ des formules du premier ordre est le plus petit sous ensemble de $\mathscr{M}(\mathrm{L})$ qui :
– contient toutes les formules atomiques.
– chaque fois qu'il contient deux mots M et N, contient également les mots : $\neg$M, (M $\wedge$ N), (M $\vee$ N), (M $\Rightarrow$ N), (M $\iff$ N), et pour tout entier n, les mots $\forall v_n$M et $\exists v_n$M.

Définition 2.14. Soient $\mathrm{F} \in \mathscr{F}(\mathrm{L})$, $k \in \mathbb{N}$, et v_k une variable de L.
– Si F est atomique, toutes les occurrences de v_k dans F sont libres.
– Si F = $\neg$G, les occurrences libres de v_k dans F sont les occurrences libres de v_k dans G.
– Si F = (GαH), $\alpha \in \{\wedge, \vee, \Rightarrow, \iff\}$, les occurrences libres de v_k dans F sont les occurrences libres de v_k dans G et les occurrences libres de v_k dans H.
– Si F = $\forall v_h$G ou $\exists v_h$G ($h \neq k$), les occurrences libres de v_k dans F sont les occurrences libres de v_k dans G.

– Si F $= \forall v_k$G ou $\forall v_k$F, aucune des occurrences de v_k dans F est une occurrence libre.

Remarque.

1. Les occurrences de v_k dans F qui ne sont pas libres sont appelées occurrences liées.
2. Dans le passage de la formule G à la forme $\forall v_k$G (resp. $\exists v_k$G) on dit que la variable v_k a été quantifiée universellement (resp. existentiellement) ou encore que G a subi une quantification universelle (resp. existentielle) pour la variable v_k.

Exemple. Considérons le langage L $= \{$R, $c, f\}$ où R est un symbole de relation binaire, c un symbole de constante, f un symbole de relation unaire. Soit F $= \forall v_0(\exists v_1 \forall v_0(\mathrm{R}v_1v_0 \Rightarrow \neg v_0 \approx v_3) \wedge \forall v_2(\exists v_2(\mathrm{R}v_1v_2 \wedge f\,v_0 \approx c) \wedge (v_2 \approx v_2)))$. Toutes les occurrences de v_0 et v_2 sont liées. Les deux premières occurrences de v_1 sont liées tandis que la troisième est libre. L'unique occurrence de v_3 est libre.

Définition 2.15. Les variables libres dans une formule F $\in \mathscr{F}$(L) sont les variables qui admettent au moins une occurrence libre dans F.

Une formule close est une formule dans laquelle aucune variable n'est libre.

Notation. On notera $\mathscr{S}$(L) l'ensemble des formules closes du langage L.

Définition 2.16. On appelle champ d'un quantificateur la formule à laquelle il s'applique.

Exemple. $\forall x[\mathrm{H}(x) \wedge \mathrm{G}(b,x) \Rightarrow \exists y \exists z(\mathrm{F}(y) \wedge \mathrm{F}(z) \wedge x \approx f(y,z))]$

Le champ de $\forall x$ est $[\,]$. Le champ de $\exists y$ est $\exists()$. Le champ de $\exists z$ est $()$.

2.2.3 La sémantique

Définition 2.17. Une interprétation I du langage du premier ordre consiste en un domaine D et une fonction notée I, dont le domaine de définition sera l'ensemble des symboles non logiques et telle que a^{I}, F^{I} et f^{I} représentent $\mathrm{I}(a)$, I(F) et I(f) où a est un symbole de variable ou de constante, F un symbole de prédicat, et f un symbole de fonction, on ait :

1. $a^{\mathrm{I}} \in \mathrm{D}$
2. $\mathrm{F}^{\mathrm{I}} \subseteq \mathrm{D}^n$
3. $f^{\mathrm{I}} : \mathrm{D}^n \to \mathrm{D}$

Notation. On notera t^{I} la valeur d'un terme clos dans l'interprétation I, et A^{I} la valeur de la formule close A dans l'interprétation I.

Définition 2.18. La valeur d'un terme clos dans l'interprétation I de domaine D est définie comme suit par récurrence :

1. Si $a \in \mathscr{V} \cup \mathscr{C}$, $a^{\mathrm{I}} \in \mathrm{D}$
2. $(f(t_1, \ldots, t_n))^{\mathrm{I}} = f^{\mathrm{I}}(t_1^{\mathrm{I}}, \ldots, t_n^{\mathrm{I}})$ où $t_1, \ldots, t_n$ sont des termes clos.

Définition 2.19. La valeur d'une formule close dans l'interprétation I de domaine D est définie comme suit par récurrence :

1. $\mathrm{F}(t_1, \ldots, t_n)^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } (t_1^{\mathrm{I}}, \ldots, t_n^{\mathrm{I}}) \in \mathrm{F}^{\mathrm{I}} \\ \emptyset \text{ sinon} \end{cases}$ $t_1, \ldots, t_n$ étant des termes clos.

   $(t_1 \approx t_2)^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } t_1^{\mathrm{I}} = t_2^{\mathrm{I}} \\ \emptyset \text{ sinon} \end{cases}$
2. $(\neg \mathrm{A})^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } \mathrm{A}^{\mathrm{I}} = \emptyset \\ \emptyset \text{ sinon} \end{cases}$
3. $(\mathrm{A} \wedge \mathrm{B})^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } \mathrm{A}^{\mathrm{I}} = \mathrm{B}^{\mathrm{I}} = \mathit{1} \\ \emptyset \text{ sinon} \end{cases}$
4. $(\mathrm{A} \vee \mathrm{B})^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } \mathrm{A}^{\mathrm{I}} = \mathit{1} \text{ ou } \mathrm{B}^{\mathrm{I}} = \mathit{1} \\ \emptyset \text{ sinon} \end{cases}$
5. $(\mathrm{A} \Rightarrow \mathrm{B})^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } \mathrm{A}^{\mathrm{I}} = \mathit{1} \text{ ou si } \mathrm{B}^{\mathrm{I}} = \mathit{1} \\ \emptyset \text{ sinon} \end{cases}$
6. $(\mathrm{A} \iff \mathrm{B})^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si } \mathrm{A}^{\mathrm{I}} = \mathrm{B}^{\mathrm{I}} \\ \emptyset \text{ sinon} \end{cases}$
7. $\forall x \mathrm{A}(x)^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si pour tout } \alpha \in \mathrm{D} \text{ quand on affecte } \alpha \text{ à } u, \mathrm{A}(u)^{\mathrm{I}} = \mathit{1}, \\ u \text{ n'ayant pas d'occurrence dans } \mathrm{A}(x) \\ \emptyset \text{ sinon} \end{cases}$
8. $\exists x \mathrm{A}(x)^{\mathrm{I}} = \begin{cases} \mathit{1} \text{ si pour un } \alpha \in \mathrm{D} \text{ quand on affecte } \alpha \text{ à } u, \mathrm{A}(u)^{\mathrm{I}} = \mathit{1}, \\ u \text{ n'ayant pas d'occurrence dans } \mathrm{A}(x) \\ \emptyset \text{ sinon} \end{cases}$

Remarques.

1. On peut montrer, par récurrence sur la complexité de t et de A, que si I est une interprétation de domaine D, t un terme clos et A une formule close, on a : $t^{\mathrm{I}} \in \mathrm{D}$, et $\mathrm{A}^{\mathrm{I}} \in \{\not\emptyset, \not 1\}$.
2. Les définitions 2.18 et 2.19 règlent les cas des termes clos et des formules closes, mais ne disent pas comment interpréter les termes non clos et les formules contenant des symboles de variables libres.
   – Un terme contenant n symboles de variables libres sera interprété non comme un élément de D, mais comme une fonction n-aire sur D.
   – Une formule contenant n symboles de variables libres, ne sera pas interprétée en terme de $\not 1$ ou $\not\emptyset$, mais comme une fonction propositionnelle n-aire sur D.

   Ainsi les valeurs des termes et formules non clos dépenderont non seulement des interprétations, mais aussi des affectations des symboles de variables libres qui y figurent.

Définition 2.20. Une affectation dans une interprétation I de domaine D est un remplacement, lors de l'interprétation d'une formule, de ses symboles de variables libres par des éléments de D.

Notation. On utilisera la lettre s pour désigner une affectation, et u^s l'élément de D affecté au symbole de variable u par s. La valeur d'un terme t dans l'interprétation I avec l'affectation s et la valeur d'une formule A dans l'interprétation I avec s seront notés $t^{\mathrm{I},s}$ et $\mathrm{A}^{\mathrm{I},s}$ respectivement.

Définition 2.21. La valeur des termes dans l'interprétation I avec l'affectation s est définie par récurrence comme suit :

1. $a^{\mathrm{I},s} = a^{\mathrm{I}} \in \mathrm{D}$ si $a \in \mathscr{C}$.
2. $u^{\mathrm{I},s} = u^s \in \mathrm{D}$ si $u \in \mathscr{V}$.
3. $f(t_1, \ldots, t_n)^{\mathrm{I},s} = f^{\mathrm{I}}(t_1^{\mathrm{I},s}, \ldots, t_n^{\mathrm{I},s})$

Notation. Soit $\alpha \in \mathrm{D}$. On notera $s(u/\alpha)$ l'affectation qui coïncide avec s sauf en u où $u^{s(u/\alpha)} = \alpha$. Par conséquent pour tout symbole de variable libre v,

$$v^{s(u/\alpha)} = \begin{cases} \alpha \text{ si } v = u \\ v^s \text{ sinon} \end{cases}$$

Définition 2.22. La valeur des formules dans l'interprétation I de domaine D, avec l'affectation s est définie comme suit par récurrence :

1. $\mathrm{F}(t_1, \ldots, t_n)^{\mathrm{I},s} = \begin{cases} \not 1 \text{ si } (t_1^{\mathrm{I},s}, \ldots, t_n^{\mathrm{I},s}) \in \mathrm{F}^{\mathrm{I}} \\ \not\emptyset \text{ sinon} \end{cases}$

   $(t_1 \approx t_2)^{\mathrm{I},s} = \begin{cases} \not 1 \text{ si } t_1^{\mathrm{I},s} = t_2^{\mathrm{I},s} \\ \not\emptyset \text{ sinon} \end{cases}$

2. $(\neg \mathrm{A})^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si } \mathrm{A}^{\mathrm{I},s} = \emptyset \\ \emptyset \text{ sinon} \end{cases}$
3. $(\mathrm{A} \wedge \mathrm{B})^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si } \mathrm{A}^{\mathrm{I},s} = \mathrm{B}^{\mathrm{I},s} = \mathcal{1} \\ \emptyset \text{ sinon} \end{cases}$
4. $(\mathrm{A} \vee \mathrm{B})^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si } \mathrm{A}^{\mathrm{I},s} = \mathcal{1} \text{ ou } \mathrm{B}^{\mathrm{I},s} = \mathcal{1} \\ \emptyset \text{ sinon} \end{cases}$
5. $(\mathrm{A} \Rightarrow \mathrm{B})^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si } \mathrm{A}^{\mathrm{I},s} = \emptyset \text{ ou si } \mathrm{B}^{\mathrm{I},s} = \mathcal{1} \\ \emptyset \text{ sinon} \end{cases}$
6. $(\mathrm{A} \iff \mathrm{B})^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si } \mathrm{A}^{\mathrm{I},s} = \mathrm{B}^{\mathrm{I},s} \\ \emptyset \text{ sinon} \end{cases}$
7. $\forall x \mathrm{A}(x)^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si pour tout } \alpha \in \mathrm{D},\ \mathrm{A}(u)^{\mathrm{I},s(u/\alpha)} = \mathcal{1}, \\ u \text{ n'ayant pas d'occurrence dans } \mathrm{A}(x). \\ \emptyset \text{ sinon} \end{cases}$
8. $\exists x \mathrm{A}(x)^{\mathrm{I},s} = \begin{cases} \mathcal{1} \text{ si pour un } \alpha \in \mathrm{D},\ \mathrm{A}(u)^{\mathrm{I},s(u/\alpha)} = \mathcal{1}, \\ u \text{ n'ayant pas d'occurrence dans } \mathrm{A}(x). \\ \emptyset \text{ sinon} \end{cases}$

Remarques.

1. On montre par récurrence sur la complexité du terme t ou de la formule A, que si I est une interprétation de domaine D et s une affectation de I, $t^{\mathrm{I},s} \in \mathrm{D}$, et $\mathrm{A}^{\mathrm{I},s} \in \{\emptyset, \mathcal{1}\}$.
2. Dans l'évaluation de t ou de A dans l'interprétation I avec l'affectation s, on a seulement besoin d'un nombre fini d'informations concernant $a^{\mathrm{I}}, \mathrm{F}^{\mathrm{I}}, f^{\mathrm{I}}$ et u^s où a, F et f représentent les symboles non logiques et les symboles de variables libres figurant dans t ou dans A.
3. Dans le cas où t et A sont clos, l'affectation s des définitions 2.21 et 2.22 n'intervient pas du tout.

Exemples.

$$t = f(g(a), f(b, c)),$$
$$t_1 = f(g(u), f(v, c)),$$
$$\mathrm{A} = f(g(b), g(u)) \equiv g(v),$$
$$\mathrm{B} = \forall x \exists y (\mathrm{F}(y) \wedge \mathrm{G}(x, y)),$$
$$\mathrm{C} = \forall x [\mathrm{H}(x) \wedge \mathrm{G}(b, x) \Rightarrow \exists y \exists z (\mathrm{F}(y) \wedge \mathrm{F}(z) \wedge x \equiv f(x, y))]$$

Supposons que I soit une interprétation de domaine $\mathbb{N}$ et s une affectation de I dans laquelle :

- $a^{\mathrm{I}} = 1$, $b^{\mathrm{I}} = 2$, $c^{\mathrm{I}} = 3$,
- $u^{\mathrm{I},s} = 4$, $v^{\mathrm{I},s} = 5$,
- $\mathrm{F}^{\mathrm{I}}(x)$: « x est premier »,
- $\mathrm{G}^{\mathrm{I}}(x, y)$: « $x < y$ »,
- $\mathrm{H}^{\mathrm{I}}(x)$: « x est pair »,
- f^{I} : l'addition,
- g^{I} : élever au carré.

Alors :

- $t^{\mathrm{I}} : 1^2 + (2+3) = 6$, $t_1^{\mathrm{I},s} : 16 + (5+3) = 24$,
- $\mathrm{A}^{\mathrm{I},s} : 2^2 + 4^2 = 5^2$, ce qui a pour valeur $\emptyset$,
- $\mathrm{B}^{\mathrm{I},s}$: « pour chaque entier naturel on peut trouver un entier premier plus grand », valeur $\mathbb{1}$,
- $\mathrm{C}^{\mathrm{I},s}$: « tout entier pair plus grand que 2 (strictement) est égal à la somme de deux entiers premiers », conjecture de Goldbach.

2.2.4 Conséquence logique

Définition 2.23. Soit Σ un ensemble de formules du langage L ($\Sigma \subseteq \mathscr{F}(\mathrm{L})$). On dira

$$\Sigma^{\mathrm{I},s} = \begin{cases} \mathbb{1} \text{ si pour tout B de } \Sigma,\ \mathrm{B}^{\mathrm{I},s} = \mathbb{1} \\ \emptyset \text{ sinon} \end{cases}$$

Remarque. Si $\Sigma \subseteq \mathscr{S}(\mathrm{L})$, alors s n'intervient pas.

Définition 2.24 (Satisfiabilité)**.** $\Sigma \subseteq \mathscr{S}(\mathrm{L})$ est satisfiable si et seulement s'il existe une interprétation I telle que $\Sigma^{\mathrm{I}} = \mathbb{1}$.

$\Sigma \subseteq \mathscr{F}(\mathrm{L})$ est satisfiable si et seulement s'il existe une interprétation I avec une affectation s telle que $\Sigma^{\mathrm{I},s} = \mathbb{1}$.

Lorsque $\Sigma \subseteq \mathscr{S}(\mathrm{L})$ et $\Sigma^{\mathrm{I}} = \mathbb{1}$ on dit que I satisfait Σ ou que I est un modèle de Σ, ou que Σ est vrai dans I. On le note $\mathrm{I} \vDash \Sigma$.

Lorsque $\Sigma \subseteq \mathscr{F}(\mathrm{L})$ et $\Sigma^{\mathrm{I},s} = \mathbb{1}$, on dit que I satisfait Σ avec s, ou s satisfait Σ dans I et on le note $\mathrm{I} \vDash_s \Sigma$.

Définition 2.25 (Validité)**.** On dit que $\mathrm{A} \in \mathscr{S}(\mathrm{L})$ est valide si et seulement si, pour toute interprétation I, $\mathrm{I} \vDash \mathrm{A}$. On dit que $\mathrm{A} \in \mathscr{F}(\mathrm{L})$ est valide si et seulement si, pour toute interprétation I et toute affectation $s \in \mathrm{I}$, $\mathrm{I} \vDash_s \mathrm{A}$.

Remarques.

1. On dit parfois « universellement valide » au lieu de « valide ».

2. Une formule valide est donc une formule vraie de par sa forme, indépendamment du sens qu'on peut donner aux symboles non logiques qui y figurent et aux affectations possibles de ses variables libres.
3. Une formule satisfiable est une formule qui est vraie dans une interprétation et une affectation données.
4. Les formules valides du langage du premier ordre jouent le rôle des tautologies du calcul propositionnel, avec toutefois une différence sensible : pour savoir si une formule du calcul propositionnel est une tautologie on dispose d'algorithmes (par exemple les tables de vérité), pour les formules du premier ordre, on doit examiner toutes les interprétations, et affectations dans ces interprétations, dans des ensembles de cardinaux infinis : il est clair qu'en général il n'y a pas de méthode pour évaluer $\forall x \mathrm{A}(x)^{\mathrm{I},s}$ en un nombre fini d'étapes si le domaine D de I est infini.

   Il est parfois possible de le faire, mais Alonzo Church a montré en 1936 qu'il existait des formules du premier ordre pour lesquelles on n'a pas d'algorithme montrant la validité ou l'invalidité.

Définition 2.26. Une tautologie du langage du premier ordre est une formule obtenue à partir d'une tautologie du calcul propositionnel en substituant des formules du premier ordre aux variables propositionnelles.

Exemples. $\mathrm{A} \Rightarrow \mathrm{A} \vee \mathrm{B}$ est une tautologie du premier ordre. $\mathrm{F}(u) \Rightarrow \mathrm{F}(u) \vee \mathrm{G}(b, v)$, $\exists \mathrm{F}(x) \Rightarrow \exists \mathrm{F}(x) \vee \forall y \mathrm{H}(y)$ en sont également. En revanche, $\forall x(\mathrm{F}(x) \Rightarrow \mathrm{F}(x))$ est valide mais n'est pas une tautologie du premier ordre.

Définition 2.27 (Conséquence logique)**.** Si $\Sigma \subseteq \mathscr{F}(\mathrm{L})$ et $\mathrm{A} \in \mathscr{F}(\mathrm{L})$, on dit que A est une conséquence logique de Σ, et on le note $\Sigma \vDash \mathrm{A}$, si et seulement si pour toute interprétation I et toute affectation s dans I,

$$\mathrm{I} \vDash_s \Sigma \text{ entraîne } \mathrm{I} \vDash_s \mathrm{A}$$

Remarques.

1. Dans le cas où $\emptyset \vDash \mathrm{A}$, A est valide.
2. Les notations $\nvDash$ et $\models\!\!\models$ signifient respectivement que l'on a pas $\Sigma \vDash \mathrm{A}$, et que si A et B sont deux formules on a $\mathrm{A} \vDash \mathrm{B}$ et $\mathrm{B} \vDash \mathrm{A}$. Dans ce dernier cas, on dit que A et B sont logiquement équivalents.

Exemple. $(\forall x)(\neg \mathrm{A}(x)) \nvDash \neg((\exists x)\mathrm{A}(x))$ signifie qu'il existe une interprétation I de domaine D et une affectation s dans I tels que :

1. $(\forall x)(\neg \mathrm{A}(x))^{\mathrm{I},s} = \mathbb{1}$
2. $\neg((\exists x)\mathrm{A}(x))^{\mathrm{I},s} = \emptyset$

Considérons $A(u)$ obtenu à partir de $A(x)$ en substituant à u, qui ne figure pas dans $A(x)$, à x. Par 1 nous avons : $(\neg(A(u)))^{I,s(u/\alpha)} = \mathbb{1}$ pour tout $\alpha \in D$. D'où pour tout $\alpha \in D$,

3. $A(u)^{I,s(u/\alpha)} = \emptyset$

Or 2 le contredit : $(\exists x A(x)) = \mathbb{1}$. D'où $(\forall x(\neg A(x))) \vDash \neg((\exists x)A(x))$.

Théorème 2.4. *Supposons* $A \models\!\models A'$, $B \models\!\models B'$, $C(u) \models\!\models C'(u)$. *Alors*

1. $\neg A \models\!\models \neg A'$
2. $A \wedge B \models\!\models A' \wedge B'$
3. $A \vee B \models\!\models A' \vee B'$
4. $A \Rightarrow B \models\!\models A' \Rightarrow B'$
5. $A \iff B \models\!\models A' \iff B'$
6. $\forall x C(x) \models\!\models \forall x C'(x)$
7. $\exists x C(x) \models\!\models \exists x C'(x)$

Démonstration. De 1 à 5, comme dans le calcul propositionnel. Montrons 6. Soient I une interprétation de domaine D et s une affectation dans I. Supposons $\forall x C(x)^{I,s} = \mathbb{1}$ (1). Considérons $C(u)$ et $C'(u)$ où u n'a d'occurrence ni dans $C(x)$ ni dans $C'(x)$. De (1) on déduit que pour tout α de D, $C(u)^{I,s(u/\alpha)} = \mathbb{1}$ (2). D'après le (2) et les hypothèses du théorème 2.4, on obtient que pour tout $\alpha \in$ D, $C'(u)^{I,s(u/\alpha)} = \mathbb{1}$ et par conséquent $\forall x C'(x)^{I,s} = \mathbb{1}$. D'où $\forall x C(x) \vDash \forall x C'(x)$.

La réciproque et 7 s'obtiennent parallèlement. □

Théorème 2.5. *Supposons que* $B \models\!\models C$ *et que l'on ait obtenu* A' *à partir de* A*, en remplaçant certaines occurrences de* B *dans* A*, mais pas nécessairement toutes, par* C*. Alors* $A \models\!\models A'$.

Démonstration. Raisonnement par récurrence sur la complexité de A. □

Théorème 2.6. *Soient* A *une formule composée d'atomes de* L*, des connecteurs* $\neg, \wedge, \vee$ *et des deux quantificateurs, et* A' *obtenue à partir de* A *en échangeant* $\wedge$ *avec* $\vee$*,* $\forall$ *avec* $\exists$*, et chaque atome avec sa négation. Alors* $A' \models\!\models \neg A$.

Démonstration. Par récurrence sur la complexité de A. □

2.2.5 Déduction formelle

La déduction formelle en logique du premier ordre ressemble à la déduction formelle en calcul propositionnel à ceci près qu'on introduit des règles supplémentaires concernant les quantificateurs.

Définition 2.28 (Déduction formelle)**.** Soit $\Sigma \subseteq \mathscr{F}(\mathrm{L})$ et $\mathrm{A} \in \mathscr{F}(\mathrm{L})$. On dit que A est formellement déductible de Σ en logique du premier ordre si et seulement si $\Sigma \vdash \mathrm{A}$ peut être obtenu à partir des 17 (ou 18) règles de déduction formelle.

Remarque. En notant $\forall x_1 x_2 \dots x_n$ l'écriture $\forall x_1 \forall x_2 \dots \forall x_n$ et $\exists x_1 x_2 \dots x_n$ l'écriture $\exists x_1 \exists x_2 \dots \exists x_n$, on peut généraliser les nouvelles règles de déduction que l'on vient d'ajouter. Par exemple :

$$(\forall -) \quad \text{Si } \Sigma \vdash \forall x_1 \dots x_n \mathrm{A}(x_1, \dots, x_n) \text{ alors } \Sigma \vdash \mathrm{A}(t_1, \dots, t_n)$$

Théorème 2.7. *Dans la logique du premier ordre, si* $\Sigma \subseteq \mathscr{F}(\mathrm{L})$ *et* $\mathrm{A} \in \mathscr{F}(\mathrm{L})$*,* $\Sigma \vDash \mathrm{A}$ *si et seulement si* $\Sigma \vdash \mathrm{A}$*.*

Démonstration. Par cas sur l'utilisation des règles. □

2.2.6 Mise sous forme prénexe

Théorème 2.8. *Supposons* $\mathrm{B} \vdash\!\dashv \mathrm{C}$ *et que l'on obtienne* A' *à partir de* A *en remplaçant quelques occurrences de* B *par* C *dans* A*. Alors* $\mathrm{A} \vdash\!\dashv \mathrm{A}'$*.*

Démonstration. Récurrence sur la complexité de A. □

Théorème 2.9. *Soit* A *une formule composée d'atomes de* L*, de connecteurs* $\neg, \wedge, \vee$ *et des deux quantificateurs respectant les règles de formation des formules. Soit* A' *la formule duale de* A *(on échange* $\wedge$ *et* $\vee$*,* $\exists$ *et* $\forall$*, chaque atome avec sa négation). Alors* $\neg\mathrm{A} \vdash\!\dashv \mathrm{A}'$*.*

Démonstration. Récurrence sur la complexité de A. □

Définition 2.29. On dit qu'une formule est sous forme prénexe si elle est de la forme $\mathrm{Q}_1 x_1 \dots \mathrm{Q}_n x_n \mathrm{B}$ où pour tout $i \in \mathbb{N}^*$, Q_i est soit $\exists$, soit $\forall$, et B est sans quantificateur. $\mathrm{Q}x_1 \dots \mathrm{Q}_n x_n$ est appelé le préfixe et B la matrice.

Théorème 2.10. *Supposons qu'on obtienne* A' *à partir de* A*, en remplaçant dans* A*, quelques occurrences de* $\mathrm{Q}x\mathrm{B}(x)$ *par* $\mathrm{Q}y\mathrm{B}(y)$*. Alors* $\mathrm{A} \models\!\!\dashv \mathrm{A}'$ *et* $\mathrm{A} \vdash\!\dashv \mathrm{A}'$*.*

Démonstration. Par récurrence sur la complexité de A. □

Théorème 2.11. *Toute formule est équivalente à une formule sous forme prénexe.*

Démonstration. Nous avons :

1. $\mathrm{A} \Rightarrow \mathrm{B} \models\!\!\dashv \neg\mathrm{A} \vee \mathrm{B}$

2. $A \iff B \models\!\!\models (\neg A \vee B) \wedge (A \vee \neg B)$
3. $A \iff B \models\!\!\models (A \wedge B) \vee (\neg A \wedge \neg B)$
4. $\neg\neg A \models\!\!\models A$
5. $\neg Q x A(x) \models\!\!\models \check{Q} x \neg A(x)$, où $\check{\exists}$ est $\forall$ et $\check{\forall}$ est $\exists$.
6. $A \wedge Q x B(x) \models\!\!\models Q x (A \wedge B(x))$ si x n'a pas d'occurrence dans A.
7. $A \vee Q x B(x) \models\!\!\models Q x (A \vee B(x))$
8. $\forall x A(x) \wedge \forall x B(x) \models\!\!\models \forall x (A(x) \wedge B(x))$
9. $\exists x A(x) \vee \exists x B(x) \models\!\!\models \exists x (A(x) \vee B(x))$
10. $Q_1 x A(x) \wedge Q_2 y B(y) \models\!\!\models Q_1 x Q_2 y (A(x) \wedge B(y))$
11. $Q_1 x A(x) \vee Q_2 y B(y) \models\!\!\models Q_1 x Q_2 y (A(x) \vee B(y))$

où les notations $\models\!\!\models$ peuvent être remplacées par $\vdash\!\!\dashv$.

Grâce aux théorèmes de remplacement des formules équivalentes et à 1, 2, et 3, on peut remplacer $\Rightarrow$ et $\iff$ par $\neg, \vee, \wedge$. Grâce à 4 on peut supprimer les doubles négations et simplifier les formules. Les règles 5 à 11 permettent de bouger les quantificateurs vers la gauche. Lorsqu'une formule prenexe a été obtenue par application des règles 1 à 11, elle est équivalente à la formule de départ. □

Exemple.

$$
\begin{aligned}
&\neg \left[\forall x \exists y F(u,x,y) \Rightarrow \exists x (\neg \forall y G(y,v) \Rightarrow H(x))\right] \\
&\neg \left[\neg \forall x \exists y F(u,x,y) \vee \exists x (\neg\neg \forall y G(y,v) \vee H(x))\right] \\
&\neg\neg \forall x \exists y F(u,x,y) \wedge \neg \exists x (\forall y G(y,v) \vee H(x)) \\
&\forall x \exists y F(u,x,y) \wedge \neg \exists x \forall y (G(y,v) \vee H(x)) \\
&\forall x \exists y F(u,x,y) \wedge \exists x \forall y \neg (G(y,v) \vee H(x)) \\
&\forall x \exists y F(u,x,y) \wedge \exists x \forall y (\neg G(y,v) \wedge \neg H(x)) \\
&\forall x (\exists y F(u,x,y) \wedge \exists y (\neg G(y,v) \wedge \neg H(x))) \\
&\forall x (\exists y F(u,x,y) \wedge \exists z (\neg G(z,v) \wedge \neg H(x))) \\
&\forall x \exists y \exists z (F(u,x,y) \wedge \neg (G(z,v) \wedge \neg H(x)))
\end{aligned}
$$

Index