Structure Discrète
IFT1065
Concepts de logique

Franz Girardin

2 Octobre 2023

Table des matières

11 Chapitre 6
Réfutations

Introduction à la logique

1.1 Concept de logique et proposition

La logique est une façon de raisonner. Simplement, elle permet de **déduire** de nouvelles informations à partir d'information antérieure, tout en déterminant le sens de ce qui a été évoqué à travers l'information.

Définition 1 Proposition

Une proposition est une **phrase** ou une **expression mathématique** qui est soit définitivement vraie ou définitivement fausse.

Exemple 1 Proposition

1. $S : \{0, -1, -2\} \cap \mathbb{N} = \emptyset$ est un proposition **vraie**

Les propositions peuvent contenir des variables. Par exemple, « $P(x)$: **Soit un entier** x, x^2 **sera toujours positif** » est une proposition contenant une variable et cette proposition est vraie. Par contre, une phrase contenant une variable n'est pas nécessairement un proposition : « $Q(x)$: L'entier x est pair » n'est ni définitivement vrai, ni définitivement faux ; cela dépendra de la valeur de x. Ainsi, $Q(x)$ **n'est pas** un proposition.

Définition 2 Phrase ouverte

Une phrase ouverte est une phrase telle que sa véracité dépend d'un contexte.

1.2 Opérateurs logiques

On peut utiliser le mot « **et** » pour combiner deux propositions ; cela engendre une **nouvelle proposition**.

Syntaxe. 1 Opérateur logique $\wedge$

Soit les propositions P, Q et la proposition $R = P \wedge Q$; R est **vraie** si et seulement si à la fois P et Q sont vrais.

Table 1.1 – Table de vérité de $P \wedge Q$

P	Q	$P \wedge Q$
V	V	V
V	F	F
F	V	F
F	F	F

On peut utiliser le mot « **ou** » pour combiner deux propositions ; cela engendre une **nouvelle proposition**.

Syntaxe. 2 Opérateur logique $\vee$

Soit les propositions P, Q et la proposition $R = P \vee Q$; R est **vraie** si au moins P ou Q est vraie.

Table 1.2 – Table de vérité de $P \vee Q$

P	Q	$P \vee Q$
V	V	V
V	F	V
F	V	V
F	F	F

On peut utiliser l'expression « **il n'est pas vrai que** » devant une propositions ; cela engendre une **nouvelle proposition**.

Syntaxe. 3 Opérateur logique $\neg$

Soit la propositions P et la proposition $Q = \neg P$; P est **vraie** si et seulement si Q n'est pas vrai, **et vice versa**.

Table 1.3 – Table de vérité de $\neg P$

P	$\neg P$
V	F
F	V

1.3 Propositions conditionnelles

On peut utiliser l'expression « **si..., alors...** » entre deux propositions ; cela engendre une **nouvelle proposition**.

Syntaxe. 4 Opérateur logique $\Longrightarrow$

Soit la propositions P et la proposition Q ;

$$R = P \implies Q$$

indique que R est **vraie** si le fait que P est vraie **implique nécessairement** que Q soit vraie. Il s'agit d'une proposition conditionnelle, puisque Q sera vraie **sous la condition** que P soit vraie.

TABLE 1.4 – Table de vérité de $P \implies Q$

P	Q	$P \implies Q$
V	V	V
V	F	F
F	V	V
F	F	V

1.4 PROPOSITION BICONDITIONNELLE

Note :

Les proposition suivantes ne sont pas équivalentes

$$P \implies Q \neq Q \implies P$$

D'ailleurs, on dit que l'une est la *réciproque* de l'autre

Deux propositions P et Q peuvent être telles que Q est la réciproque de P et les deux sont à la fois vrai. Puisque ces deux propositions sont vraies, leur conjonction est aussi vraie On obtient alors :

$$(P \implies Q) \wedge (Q \implies P) \quad \textit{Vraie}$$

Nous introduisons alors un nouveau symbole qui illustre la relation entre P et Q; la conjonction suivante engendre une proposition *biconditionnelle* :

1. $Q \implies P$ « *P si Q* »
2. $P \implies Q$ « *P seulment si Q* »

3. $P \Leftrightarrow Q \equiv (P \implies Q) \wedge (Q \implies P)$
4. $P \Leftrightarrow Q$ « *P si et seulement si Q* »

TABLE 1.5 – Table de vérité de $P \Leftrightarrow Q$

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

La proposition biconditionnelle indique que soit les deux propositions qui la composent sont soit toutes deux vraies, ou elles sont soit toutes deux fausses.

1.5 TABLE DE VÉRITÉ DE PROPOSITIONS

Considérons un problème plus complexe où une expression impliques plusieurs propositions combinées. Nous allons essayer déterminer pour quelles valeurs de P et Q une proposition complexe R est vraie.

$$\textit{Soit } R = (P \vee Q) \wedge \neg(P \wedge Q)$$

R indique que *P ou Q est vraie et il n'est pas possible que P et Q soient vrai à la fois.*

TABLE 1.6 – Table de vérité pour $(P \vee Q) \wedge \neg(P \wedge Q)$

P	Q	$(P \vee Q)$	$P \wedge Q)$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge \neg(P \wedge Q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

1.6 ÉQUIVALENCES LOGIQUES

Définition 3 Notion d'équivalence logique

Deux propositions sont dite **logiquement équivalentes** si leurs valeurs correspondent exactement dans une table de vérité.

En utilisant une table de vérité, on peut montrer que les propositions suivantes sont logiquement équivalentes.

1. $P \Leftrightarrow Q = (P \wedge Q) \vee (\neg P \wedge \neg Q)$
2. $P \implies Q = \neg P \implies \neg Q$

TABLE 1.7 – Table de vérité pour $P \implies Q = \neg P \implies \neg Q$

P	Q	$\neg P$	$\neg Q)$	$\neg P \implies \neg Q$	$P \implies Q$
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	V	V	V
F	F	V	V	V	V

1.7 DEMORGAN

Concept. 1 Loi DeMorgan

1. $\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$
2. $\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$

La loi DeMorgan est intuitive. Affirmer $\neg(P \wedge Q)$ revient à dire qu'il n'est pas possible que P et Q soient vrais à la fois.

Or, si P et Q ne peuvent pas être tout deux vrai, soit P est faux, $\neg P$, ou aors Q est faux, $\neg Q$.

Nous résumons ici quelques équivalences logiques importantes.

— Loi de la contraposé

1. $P \implies Q = \neg Q \implies \neg P$

— Loi DeMorgan

1. $\neg(P \wedge Q) = (\neg P) \vee (\neg Q)$
2. $\neg(P \vee Q) = (\neg P) \wedge (\neg Q)$

— Loi commutative

1. $P \wedge Q = Q \wedge P$
2. $P \vee Q = Q \vee P$

— Loi distributive

1. $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$
2. $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \wedge R)$

— Loi associative

1. $P \wedge (Q \wedge R) = (P \wedge Q) \wedge R = P \wedge Q \wedge R$
2. $P \vee (Q \vee R) = (P \vee Q) \vee R = P \vee Q \vee R$

Propositions Quantifiées

2.1 Introduction aux quatificateurs

Certaines propositions peuvent difficilement être symbolisé par un nombre limité **d'opérateurs** logique. Considérons l'ensemble infini d'entiers $S = \{x_1, x_2, x_3, \dots\}$. Pour exprimer l'affirmation *chaque élément de S est impair*, il faudrait procéder de la façon suivante :

$$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \dots$$

Noton ici que $P(x)$ est la phrahse ouverte *x est impair*. Néanmoins, cette approche engendre une expression interminable. Similairement, pour exprimer la proposition selon laquelle *il y a au moins un élément de S qui est impair*, on aurait procéder de la façon suivante :

$$P(x_1) \vee P(x_2) \vee P(x_3) \vee \dots$$

Concept. 2

Nous itroduisons le symbole $\forall$ qui signifie *pour tout*, et le symbole $\exists$ qui signifie *il existe*.

Nous pouvons réécrire les deux expression précédentes de la façon suivante :

1. $\forall x \in S,\ \ P(x)$
2. $\exists x \in S,\ \ P(x)$

Note :

$\forall$ est appelé *quantificateur universel* et $\exists$ est appelé *quantificateur existentiel*. Les propositions qui contiennent l'un ou l'autre sont appeléss *proposition quantifiées*.

2.2 Quantificateur implicite

Concept. 3 Quantificateur implicite

En mathématique, lorsque $P(x)$ et $Q(x)$ sont des phrases ouvertes concernant un élément x appartenant à un certain ensemble S, une expression de la forme $P(x) \implies Q(x)$ est comprise comme étant implicitement $\forall x \in S, P(x) \implies Q(x)$. L'omission du $\forall x \in S$ est un convention. Ce type d'expression revient souvent et on préfère éviter de répéter la portion quantificatrice de l'expression.

Définition 4

Si P et Q sont des proposition ou des phrases ouverte,

$$Si\ P,\ alors\ Q$$

est une proposition.

2.3 Interchangeabilité de l'universellement et de la proposition conditionnelle

Exemple 2 Conjecture de Golbach

La conjecture de Golbach indique que *chaque entier plus grand que 2 est la somme de deux nombres premiers*. Nous pouvons traduire cette proposition de la façon suivante :

— Soit $S = \{x \mid x \geq 2\}$

1. $(n \in S) \implies (\exists p, q \in P, n = p + q)$
2. $\forall n \in S, \exists p, q \in P, n = p + q$

Théorème 1

Suppopsons que S est un ensemble et $Q(x)$ est une proposition par rapport à x pour n'importe quel $x \in S$. Nous savons alors que les deux propositions suivantes veulent dire la même chose

1. $\forall x \in S, Q(x)$
2. $x \in S \implies Q(x)$

2.4 Négation de proposition

Soit une proposition R, la proposition $\neg R$ est la négation de R. Certaines expressions sont plus utiles sous leur forme négative. Le processus pour trouver $-R$ est la **négation de** R

Exemple 3 Négation d'une proposition

Soit la proposition

— R : *Tu peux résoudre le problème en factorisant ou en utilisant le fomule quadratique* .

1. $P =$ *Tu peux résoudre le problème en factorisant*
2. $Q =$ *...avec la formule quadratique.*
3. On a :

$$\neg R = \neg(P \vee Q)$$
$$\neg R = \neg(P) \wedge \neg(Q)$$

2.5 Négation de proposition quantitifée

Considérons une proposition quantitifée :

$$R = \forall x \in \mathbb{N}, P(x)$$

La négation de cette proposition est : *ce n'est pas le cas que pour tout x dans $\mathbb{N}$ $P(x)$ est vrai*. Autrement dit, *il existe un x dans $\mathbb{N}$ tel que $P(x)$ est faux*. Nous pouvons traduire la négation de R de la façon suivante :

$$\neg R = \exists x \in \mathbb{N}, \neg P(x)$$

Nous constatons que la négation d'une proposition universellement quantitifées engendre une proposition existantielle. La réciproque est aussi vraie.

Théorème 2 Négation de proposition universellement ou existentiellement quantitifée

$$\neg(\forall x \in S, P(x) = \exists x \in S, \neg P(x))$$
$$\neg(\exists x \in S, P(x) = \forall x \in S, P(x))$$

2.6 Négation de proposition ayant plusieurs quantificateurs

Lorsqu'un proposition présente plusieurs quantificateurs, il faut décomposer le sens de l'expression itérativement.

Exemple 4 Négation de proposition à plusieurs quantificateurs

Soit la proposition

— S : *pour tout nombre réel x, il existe un nombre réel y pour lequel $y^3 = x$*

1. $S = \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$
2. $\neg S = \neg(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x)$
3. $\neg S = \neg(\forall x \in \mathbb{R}), \forall y \in \mathbb{R}, y^3 \neq x$
4. $\neg S = \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^3 \neq x$

— $\neg S$: *il existe un réel x tel que pour tout réel y, $y^3 \neq x$*

2.7 Négation de proposition conditionnelle

Nous savons que la proposition conditionnelle $P \implies Q$ est fausse uniquement lorsque P est vraie, mais que Q est faux. Ainsi, nous avons :

$$\neg P \implies Q = P \wedge \neg Q$$

Exemple 5 Négation d'une proposition conditionnelle

Soit la proposition

— $R =$ *Si x est impair, x^2 est impair*

1. $\neg R = \neg\Big(\forall x \in \mathbb{Z}, (x \text{ est impair}) \implies x^2 \text{ est impair}\Big)$
2. $\neg R = \exists x \in \mathbb{Z}, (x \text{ est impair}) \implies \neg(x^2 \text{ est impair})$

Techniques de preuve

3.1 Définitions de termes récurrents

Définition 5 Définir un théorème

Est un **théorème** une proposition mathématique qui est vraie et peut être vérifiée comme étant vraie. Une **preuve** d'un théorème est une vérification écrite qui montre que le théorème est, sans équivoque, vrai. Une **définition** est une explication exacte et non ambigue d'une expression mathématique.

Définition 6 Lemme

Il s'agit d'un théorème mineur dont l'objectif est d'aider à montrer la véracité d'un autre théorème.

Définition 7 Corollaire

Il s'agit d'un résultat qui est la conséquence directe d'un autre théorème ou d'une autre proposition.

3.2 DÉFINITION D'ENTITÉS MATHÉMATIQUES

— **Pair et impair**

1. Un **entier** n est **pair** si $n = 2a$ pour un certain entier $a \in Z$
2. Un **entier** n est **impair** si $n = 2a + 1$ pour un certain entier $a \in Z$

— Deux entiers ont **la même parité** s'ils sont tous deux **pairs** ou tout deux **impairs**. Autrement, ils ont une **parité opposée**.

— **Division et multiplication**

1. **Division**. Soit les entier a et b. On dit que a **divise** b si $b = ac$, pour un certain entier $c \in \mathbb{Z}$. On écrit a divise b : $a|b$
2. **Multiplication**. On dit également que a est un **diviseur** de b et que b est un **multiple** de a.
3. Lorsque a **ne divise pas** b, on écrit $a \nmid b$.

— **Nombre premier**

1. Chaque **entier** a un ensemble d'entiers qui peuvent le diviser. Par exemples, les diviseur de 6 sont dans l'ensemble

$$\{a \in Z : a|6\} = \{-6, -3, -2, 0, 2, 3, 6\}$$

2. Un **nombre premier** est un **entier naturel**, n, qui possède exactement deux diviseurs possibles, 1 et n

— Un **entier** n est dit **composé** s'il se factorise en $n = ab, \quad a, b > 1$

— **PGCD et PPMC**

1. **PGCD**. Le **plus grand commun diviseur** des **entiers** a et b, dénoté $pgcd(a, b)$ est le plus grand des entiers qui divise à la fois a et b.
2. **PPMC**. Le **plus petit commun multiple** des entiers **non-nuls** a et b, dénoté $ppcm(a, b)$ est le plus petit entier positif qui est à la fois multiplie de a et b

— **Rationalité**

1. **Nombre rationnel**. Un nombre réel x est **rationnel** si $x = \frac{a}{b}$ pour des entiers $a, b \in mathbbZ$
2. **Nombre irrationnel**. Un nombre réel est **irrationnel** s'il n'est pas rationnel ; c'est-à-dire $x \neq \frac{a}{b}$ pour tous les $a, b \in \mathbb{Z}$

— **Termes indéfinis**

— **Explication** : certains termes ne peuvent nécessitent pas d'être définit ; les termes qu'il faudrait utiliser devraient à leur tour être définit, et ainsi de suite, indéfinement. On accepte donc certains idées comme étant **intuitives et vraies**. Les termes suivants ne sont pas définis.

1. Un **entier**, un **nombre réel**
2. Les opération d'**addtion**, de **soustraction**, de **multiplication** et de **division**.
3. Les lois de **distributivité** et de **commutativité** de l'addtion et de la multiplication.<F35>
4. L'existence des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$.
5. Soient $a, b \in \mathbb{N}$:

$$a + b \in \mathbb{Z}, \quad a - b \in \mathbb{Z} \text{ et } ab \in \mathbb{Z}$$

Théorème 3 L'algorithme de division

Soient deux **entiers** a et b avec $b > 0$, il existe des **entiers** unique q et r tels que $a = qb + r$ et $0 \leq r < b$.

Théorème 4 Factorisation en premiers d'entiers naturels

haque entier naturel $n > 1$ a une **factorisation unique** en nombres premiers. Autrement dit chaque factorisation, peu importe l'ordre engendre les mêmes facteurs et le même nombre de facteurs :

$$1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 \cdot 3 \cdot 7^2$$

$$1176 = 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2 \cdot 7 = 2^3 \cdot 3 \cdot 7^2$$

3.3 PREUVE DIRECTE

1. Identifier l'élément à prouver et le **reformuler** sous forme de proposition conditionnelle

$$P \implies Q$$

2. **Assumer que** P **est vraie** et montrer que cela force Q à être vraie également.

Proposition Si P, alors Q.

Preuve. Supposons P.

⋮

Par conséquent Q. □

Preuve 1 Utilisation de la méthode de preuve directe

Proposition Si x est impair, x^2 est impair.

Preuve. Supposons que x est impair. Dans ce cas, nous savons qu'il existe un nombre $a \in \mathbb{Z}$ tel que $2a + 1 = x$. Or, nous pouvons exprimer x en termes de a :

$$x = 2a + 1 \implies x^2 = (2a + 1)^2 = 4a^2 + 4a + 1$$

Par ailleurs, nous pouvons considérer un nombre b tel que $2b + 1 = x^2$:

$$x^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1 = 2(b) + 1$$

Ainsi, nous avons montré que $x^2 = 2b + 1$ pour un certain nombre $b = 2a^2 + 2a$. Par conséquent, x^2 est impair, *par la définition d'un nombre impair*. □

Preuve 2 Utilisation de la méthode de preuve directe

Proposition Soient a, b et c, des entiers. Si $a|b$ et $b|c$, alors $a|c$.

Preuve. Supposon que $a|b$ et $b|c$. Nous savons alors que b est un multiple de a. Autrement dit, $b = ak_1$ pour un certain nombre $k_1 \in \mathbb{Z}$. Or, *par la définition d'un diviseur*, $c = bk_2 = ak_1k_2$ pour un certain nombre $k_2 \in \mathbb{Z}$. Considérons un nombre $k_3 \in \mathbb{Z}$ tel que $k_3 = k_1k_2$. Or, affirmer $a|c$, revient à exprimer l'équivalence suivante :

$$a|c \implies ak_1k_2 = a \cdot X | X \in \mathbb{Z}$$

Nous savons que X est simplement $k_3 = ak_1k_2$ Ainsi, $c = ak_3$ pour un certain $k_3 \in \mathbb{Z}$.

Par conséquent $a|c$. □

3.4 Preuve par cas

Examiner une proposition implique souvent de considérer tous les scénarios possibles. Ainsi, dans la technique de preuve **preuve par cas**, on décompose la proposition en cas et examine chacun d'eux indivuellement pour déduire une conclusion générale.

Proposition Si $P(c_1, c_2, \cdots, c_n)$, alors Q.

Preuve. Supposons P.

Cas c_1
Cas c_2
⋮
Cas c_n

Par conséquent Q. □

Preuve 3 Utilisation de la technique de preuve par cas

Proposition Si $n \in \mathbb{N}$, alors $1 + (-1)^n(2n - 1)$ est un multiple de 4.

Preuve. Supposons $n \in \mathbb{N}$
Cas 1. Supposons que n est pair. Dans ce cas, il existe un nombre $k \in \mathbb{N}$ tel que $n = 2k$ et $(-1)^n = 1$, peu importe le signe de k. Et ainsi, $1 + (-1)^n(2n - 1) = 1 + 1 \cdot (4k - 1) = 4k$. Dans ce cas, n est un multiple de 4.

Cas 2. Supposons que n est impair. Dans ce cas, il existe un nombre $k \in \mathbb{N}$ tel que $n = 2k + 1$ et $(-1)^n = -1 \cdot 1 = -1$ Et ainsi, $1 + (-1)^n(2n - 1) = 1 + -1(4k + 2 - 1) = -4k$. Dans ce cas, n est un multiple de 4.
Ces cas montrent que $1 + (-1)^n(2n - 1)$ est toujours un multiple de 4. □

Lorsque deux ou plusieurs cas sont similaires, on peut considérer uniquement un des cas et indiquer que la logique pour les autre suit. On utilisera la phrase *Sans perte de généralité* devant l'unique cas qu'on s'apprête à considérer. Cela indique au lecteur que l'écriture explicite de chaque cas serait redondante et que le cas présent suffit à **encapsuler la logique** des autres cas.

Preuve 4 Traitement de cas similaires en un cas

Proposition Si deux entiers sont de parité opposée, alors leur somme est impair.

Preuve. Si deux entiers sont de parité opposée, l'un est pair et l'autre est impair. *Sans perte de généralité*, supposons que l'entier m est pair et l'entier n est impair. Nous allons montrer que leur somme est impair. Ainsi, *par définition d'un nombre pair et par la définition d'un nombre impair*, $m = 2a$ et $n = 2a + 1$ pour un nombre $a \in \mathbb{Z}$. Nous savons que la somme des deux entiers est $m + n = 2a + 2a + 1 = 4a + 1 = 2(2a) + 1$. Cette somme exprime un nombre impair. □

3.5 Preuve par contraposée

Par une table de vérité, nous avons montré plus tôt $P \implies Q$ est **logiquement** éuivalent à $\neg Q \implies \neg P$, la contraposée de $P \implies Q$. Pour évaluer une proposition conditionnelle, on peut donc procéder en évaluant plutôt sa contraposée.

Proposition Si P, alors Q.

Preuve. Supposons $\neg Q$.

⋮

Par conséquent $\neg P$. □

Preuve 5 Utilisation de la technique de preuve par contraposée

Propositions Supposons que $x \in Z$. Si $7x + 9$ est pair, alors x est impair.

Preuve. Supposons que x n'est pas impair (Contraposée). Si x est pair, il existe un nombre $k \in \mathbb{Z}$ tel que $2k = x$. Ansi, $7x + 9 = 7(2k) + 9 = 14k + 8 + 1 = 2(7k + 4) + 1$. Cette expression représente un nombre

impair, *par la définition d'un nombre impair*. Par conséquent, $7x + 9$ n'est pas pair. On a montré que si $\neg Q$ alors $\neg P$. Cela est logiquement équivalent à si P, alors Q. □

Preuve 6 Utilisation de la technique de preuve par contraposée

Proposition Supposons $x, y \in \mathbb{Z}$. Si $5 \nmid xy$, alors $5 \nmid x$ **et** $5 \nmid y$.

Preuve. Supposons qu'il est faux que $5 \nmid x$ et $5 \nmid y$. Par DeMorgan, soit il est faux que $5 \nmid x$ ou il est faux que $5 \nmid y$. Par conséquent, $5|x$ **ou** $5|y$. Nous allons consiédrer les deux cas.
Cas 1. Supposons que $5|x$, alors $x = 5k_1$, pour un entier $k_1 \in \mathbb{Z}$. Ainsi, on obtient $xy = 5(k_1 y)$ et donc 5 divise xy.
Cas 2. Supposons que $5|y$, alors $y = 5k_2$ pour une entier $k_2 \in \mathbb{Z}$. Ainsi, on obtient $xy = 5(k_2 y)$ et donc 5 divise xy.
Dans les deux cas, nous avons montré que $5|xy$. Nous avons montré que la proposition d'origine est vraie en montrant que $\neg Q \implies \neg P$. □

3.6 Preuve par contradiction

L'objectif est supposer qu'une affirmation est fausse, puis de montrer que la supposition engendre une absurdité. Si na négation de l'affirmation est incohérente, l'affirmation elle-même est, en principe cohérente.

Proposition P.
Preuve. Supposons $\neg P$.
⋮
Par conséquent $C \wedge \neg C$. □

Preuve 7 Utilisatation de la technique de preuve par contradiction

Proposition Si $a, b \in \mathbb{Z}$, alors $a^2 - 4ab \neq 2$

Preuve. Supposons qu'il est faux que lorsque $a, b \in \mathbb{Z}$ $a^2 - 4ab \neq 2$. Autrement dit, il existe des entiers a et b tels que $a^2 - 4ab = 2$. De cette équation, nous obtenons $a^2 = 4(ab) + 2 = 2(2ab + 1) = 2k_1, k_1 \in \mathbb{Z}$; et donc a est pair. Nous savons grâce à un lemme que si a^2 est pair a est aussi pair. Et donc $a = 2c$ pour un entier $c \in \mathbb{Z}$. Ainsi, nous avons $(2c)^2 - 4(2c)b = 2$ ou $4c^2 - 8bc = 2$ ou $4(c^2 - 2b) = 2$ ou $2(c^2 - 2b) = 1$. Cela reviendrait à dire que 1 est un nombre impair. Or, 1 n'est pas un nombre impair. La négation de l'affirmation engendre donc une contradiction. Ainsi, l'affirmation doit être vraie. □

3.7 Prouver une proposition conditionnelle par contradiction

L'objectif de la preuve par contradiction d'une proposition conditionnelle est de montré l'absurdité de $\neg(P \implies Q)$. On sait que pour que $P \implies Q$ soit faux, il faut que P soit vrai alors qu Q est faux. La preuve démarre alors en assumant P **et** $\neg Q$

Proposition $P \implies Q$.
Preuve. Supposons P **et** $\neg Q$.
⋮
Par conséquent $C \wedge \neg C$. □

Preuve 8 Utilisation de la technique de preuve par contradiction sur une proposition conditionnelle

Proposition Supposons que $a \in \mathbb{Z}$. Si a^2 est pair, alors a est pair. *Preuve.* Supposons que a^2 est pair alors qu'il est faux que a est pair (a est impair). Nous savons que $a^2 = 2k_1$ pour un entier $k_1 \in \mathbb{Z}$. Or, notre supposition initiale indique qu'il existe un entier $k_2 \in \mathbb{Z}$ tel que $a = 2k_2 + 1$. Selon cette expression, $a^2 = 4{k_2}^2 + 4k_2 + 1 = 2(2{k_2}^2 + 2k_2) + 1$. Ainsi, a^2 serait un nombre impair. Or nous avons la contradiction (a^2est impair) $\wedge$ (a^2est pair) Par conséquent la proposition d'origine doit être vraie. □

Preuves sur les ensembles

4.1 Prouver $a \in A$

Un ensemble est généralement exprimé en notation par compréhension $A = \{x : P(x)\}$ où $P(x)$ est une proposition ou un phrase ouvertre. On comprend par cette notation que A contient tous les éléments pour lesquels $P(x)$ est vraie. Un ensemble peut également être exprimé par $A = \{x \in S : P(x)\}$. Dans cette notation on exprime le fait que A contient tous les éléments de l'ensemble S pour lequel $P(x)$ est vraie.

Les preuves sur les ensembles visent donc à montrer que montrer que certains éléments font effectivement partie de certains ensembles.

Comment monter que $a \in \{x : P(x)\}$

Montrer que $P(a)$ est vraie.

Comment monter que $a \in \{x \in S : P(x)\}$

1. Vérifier que $a \in S$
2. Monter que $P(a)$ est vraie.

4.2 Montrer que $A \subseteq B$

Définition 8 Rappel sur l'appartenance

Si A et B sont des ensembles, $A \subseteq B$ signifie que *tous les éléments dans A se trouvent également dans B.*

Pour prouver l'**appartenance** d'un ensemble à un autre, il suffit de vérifier la proposition conditionnelle :

$$a \in A \implies a \in B$$

Comment monter que $A \subseteq B$ ***Approche Directe***

Preuve. Supposons $a \in A$.
⋮
Par conséquent $a \in A$. □

Comment monter que $A \subseteq B$ ***Approche par Contraposée***

Preuve. Supposons $a \notin B$.
⋮
Par conséquent $a \notin B$. □

Preuve 9 Utilisation de la technique de preuve directeur pour montrer l'appartenance à un ensemble

Proposition $\{x \in \mathbb{Z} : 18|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$

Preuve. Supposons a appartient à l'ensemble des nombres entiers qui peuvent être divisé par 18. Ainsi, il existe un entier $k_1 \in \mathbb{Z}$ tel que $a = 18k_1 = 6(3k_1)$. Si nous considérons $k_2 \in \mathbb{Z}, k_2 = 3k_1$, il s'ensuit que $6|a$. Nous avons montré que si $a \in \{x \in \mathbb{Z} : 18|x\}$, il faut forcément que $a \in \{x \in \mathbb{Z} : 6|x\}$ soit vrai. Ainsi, la proposition d'origine, $\{x \in \mathbb{Z} : 18|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$ est vraie. □

4.3 Prouver que $A = B$

Pour montrer que deux ensembles sont équivalents, il suffit de montrer, dans un premier temps, que tous les éléments se trouvant dans A se trouvent aussi dans B, $A \subseteq B$. Mais cela est insuffisant puisque des éléments autre que ceux de A pourraient se trouver dans B tout en respectant $A \subseteq B$. Or, si on prouve également que $B \subseteq A$, alors cela montre que B ne peut contenir aucun élément qui n'est pas aussi dans A, et donc $A = B$.

Comment monter que $A = B$

Preuve.
[*Prouver que* $A \subseteq B$].
[*Prouver que* $B \subseteq A$].
⋮
Par conséquent, puisque $A \subseteq B$ **et** $B \subseteq A$, il s'ensuit que $A = B$ □

Preuve 10 Utilisation de la technique de preuve directe pour vérifier l'égalité de deux ensembles

Proposition $\{n \in \mathbb{Z} : 35|n\} = \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$.

Preuve. Nous appelleron les trois ensembles S_1, S_2, S_3 respectivement. Nous montrons d'abord que $\{n \in \mathbb{Z} : 35|n\} \subseteq \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. Supposons que $a \in \{a \in \mathbb{Z} : 35|n\}$. Il s'ensuit que $35|a$ et que $a = 35c = 7(5c) = 5(7c)$. Ainsi, nous savons que $5|a$ et $7|a$. Nous avons montré que si $a \in S_1$ cela implique que $a \in S_2$ et $a \in S_3$. Par la définition d'intersection, nous savons alors que $a \in (S_2 \cap S_3)$. Ainsi, nous avons montré que si $a \in S_1$, cela implique que $a \in S_2 \cap S_3$. Par conséquent, $S_1 \subseteq S_2 \cap S_3$

Ensuite, nous allons montrer que $S_2 \cap S_3 \subseteq S_1$. Supposons que $a \in S_2 \cap S_3$. *Par la définition d'intersection*, nous avons alors $5|a$ **et** $7|a$. À partir de ce constat, nous savons qu'il existe des nombres $c, d \in \mathbb{Z}$ tel que $a = 5c$ ou $b = 7c$. Ainsi, nous savons que a a 7 et 5 comme facteur premier; la factorisation de a **doit** inclure 7 et 5. Or, $7 \times 5 = 35$. Cela implique que a est divisible par 7 ou 5 ou 35. Ainsi, nous avons $35|a$ qui implique que $a \in S_1$. Nous venons donc de montrer que $S_2 \cap S_3 \subseteq S_1$.

Finalement, nous avons montré que $\{n \in \mathbb{Z} : 35|n\} \subseteq \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$ **et** $\{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\} \subseteq \{n \in \mathbb{Z} : 35|n\}$. Par conséquent, $A = B$. □

Prouver des propositions conditionnelles

5.1 Preuves si-et-seulement-si

Les proposition **biconditionnelle** renferme deux propositions. Pour évaluer un proposition biconditionnelle, il faut donc évaluer chacune des propositions qu'elle comprend.

Comment monter que $P \Leftrightarrow Q$

Proposition *P si et seulement si Q*

Preuve.
Prouver que $P \implies Q$

Prouverque $Q \implies P$.

⋮

Par conséquent, puisque $P \implies Q$
et $Q \implies P$,
il s'ensuit que $P \Leftrightarrow Q$ □

Preuve 11 Biconditionnelle

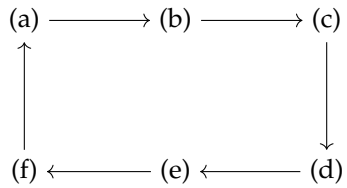
Proposition L'entier n is impair si et seulement si n^2 est impair.

Preuve. Nous allons commencer par montrer, par preuve directe, que si n est impair, alors n^2 est impair. Nous allons appeler cette proposition R. Supposons que n est impair. Dans ce cas, il existe un entier $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Ainsi, nous avons $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Donc, *par la définition d'un nombre impair*, n^2 est **impair**. Nous venons de prouver R.

Nous allons maintenant prouver la réciproque de R par contradiction. Supposons que la réciproque est fausse ; supposons qu'il est faux que lorsque n^2 est impair, n est également impair. Autrement dit, supposons que lorsque n^2 est impair, n est alors pair. Selon cette supposition, il existe $n = 2k$ pour un entier $k \in \mathbb{Z}$. Ainsi, nous avons $n^2 = 4k^2 = 2(2k^2)$. Or, nous déduisons que n^2 est pair, alors que nous savons que n^2 est impair ; il y a contradiction. Par conséquent, la supposition est fausse et la réciproque $\neg R$ est vraie.
En conclusion, nous savons que R est vraie et que la réciproque de R est vraie. Ainsi, nous savons que la proposition d'origine, *l'entier n est impair si et seulement si* n^2 *est impair* est vraie □

5.2 Preuve de proposition équivalentes

Lorsqu'un théorème affirme qu'une liste de propositions $P_1, P_2, \ldots P_n$ sont équivalentes, cela veut dire que soit toutes ces propositions sont vraies, soit elles sont toutes fausses. Autrement dit, il y a une relation d'implication d'une proposition à la suivante, jusqu'à ce que la dernières implique la première également. Pour prouver que les propositions sont équivalentes, il suffit donc de vérifier l'implication pour chacun des termes du cycle.



5.3 Preuve d'existance

La plupart des théorèmes sont sous la forme de propositions conditionnelles ou biconditionnelle. Nous avons vue qu'un proposition conditionnelle $P \implies Q$ se traduit par une proposition universellement quantitifiée, $\forall x \in S, P(x) \implies Q(x)$.

Or, pour **prouver une proposition d'existence**, il suffit de trouver un exemple qui satisfait la proposition associée au théorème. Autrement dit, il faut montrer $\exists x, R(x)$

Preuve 12 Utilisation d'exemple pour une preuve d'existance

Proposition Il existe un nombre premier qui est pair.

Preuve. Observez que 2 est un nombre premier pair.

5.4 Preuve constructive et non-constructive

Une preuve d'existance peut être constructive ou non constructive. La preuve d'existance constructive indique qu'il existe un élément qui respecte la proposition et donne un exemple. La preuve d'existance non-constructive indique simplement qu'il existe un élément qui respecte la proposition, mais ne donne pas d'exemple.

Réfutations

Le processus permettan de montrer qu'une propoisition fausse s'appelle la réfutation. Il existe trois types de propositions :

1. Les propositions qui ont été prouvé. Cela inclus tous les théorèmes, lemmes, corollaires et autres propositions qu'on sait vrai.
2. Les propositions fausses. On ne leur accorde pas de nom particulier et on sait qu'elles sont fausses.
3. Les **conjectures** ; les propositions qu'on *suspecte* être vraies, mais qui n'ont pas encore été prouvées.

Pour montrer qu'une proposition P est fausse, il suffit de montrer que sa réciproque $\neg P$ est vraie, puisque P et $\neg P$ ne peuvent pas être vraie à la fois ; si $\neg P$ est vraie, alors P est fausse.

6.1 Réfutation par contre-exemple

Puisque plusieurs conjectures sont des propositions universellement quantitiées de la forme $\forall x \in S, P(x)$, il suffit d'effectuer la négation :

$$\neg(\forall x \in S, P(x) = \exists x \in S, \neg P(x))$$

Comment réfuter $\forall x \in S, P(x)$

Produire un exemple d'un $x \in S$ qui rend $P(x)$ faux.

Comment réfuter $P(x) \implies Q(x)$

Produire un exemple d'un x qui rend $P(x) \implies Q(x)$ faux.

Définition 9 contre-exemple

Les exemples qui réfutent une proposition sont appellés contre-exemple.

6.2 Réfuter les propositions d'existence

Réfuter une proposition d'existance $\exists x \in S, P(x)$ revient montrer qu'une proposition universellement quantitifée est vraie :

$$\neg(\exists x \in S, P(x)) = \forall x \in S, P(x)$$

6.3 Réfutation par contradiction

Supposon qu'on veut réfuter P. Il faut alors montrer que $\neg P$ est vrai. Or, si on procède par contradiction, on va supposer que la proposition $\neg P$ est fausse, ce qui revient à assumer que $\neg\neg P$ est vrai. Or, $\neg\neg P$ est simplement P. Donc, pour réfuter par contradiction, il suffit d'assumer que P est vrai et déduire une contradiction.

Comment réfuter P **par contradiction**

Assumer que P est vraie, et déduire une *contradiction*.

Lemme 1 Lemme d'Euclide

Si un nombre premier k divise un produit $A = a_1 \cdot a_2 \cdot \cdots \cdot a_n$, alors, k divise au moins une des facteurs de A.

Lemme 2 Factorisation en nombre premer

Si p est un nombre premier et $p|q$, alors p est un facteur premier de q. Autrement dit, la factorisation en nombre

premier de q implique p.