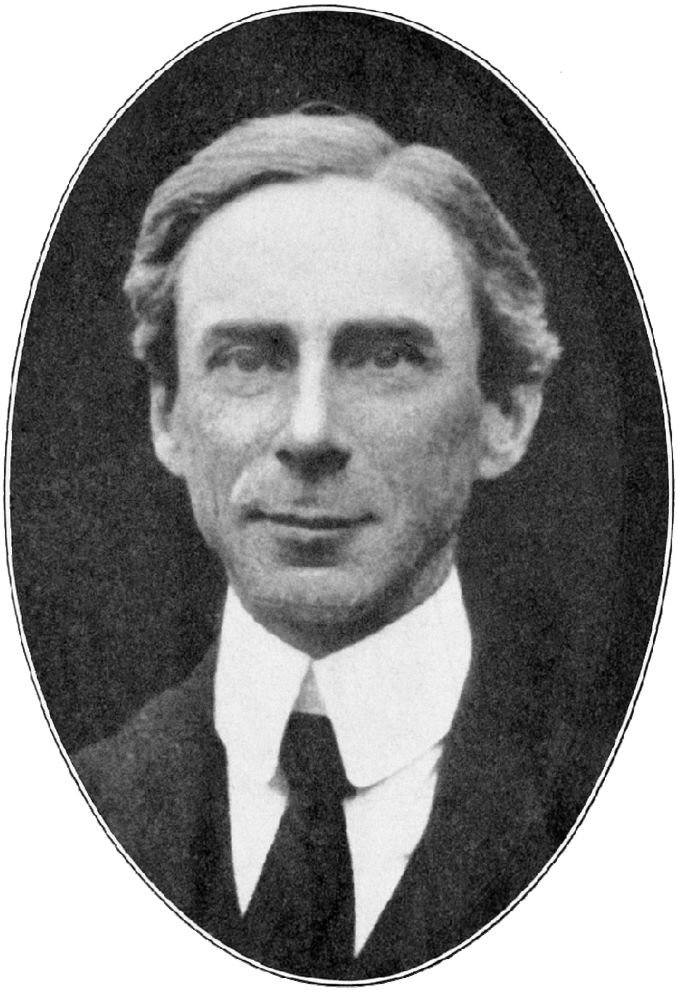
جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Polycopié de Logique mathématique

A l'usage des étudiants de
2ème année Licence de Mathématiques



Bertrand Russell
L'un des fondateurs de la logique contemporaine

Rezki Chemlal

Université A. Mira de Béjaia - Algérie

Préface

Ce polycopié est issu du cours de Logique Mathématique de la $2^{ème}$ année Licence de Mathématiques que j'ai eu à assumer d'abord à l'université de Guelma durant les années 2006 à 2008 et ensuite à l'université de Béjaia entre 2014 et 2018.

Le volume horaire alloué à ce cours est passé de 3 heures hebdomadaires quand j'ai commencé à 1h30 (1 cours seulement) pour revenir à 3 heures hebdomadaires à la faveur d'une proposition transmise au comité national des programmes.

Le programme couvre la logique propositionnelle ainsi que des éléments de la théorie des ensembles.

Le chapitre 1 est consacré au calcul propositionnel et au calcul des prédicats, on y aborde notamment les règles d'inférences éléments de base du raisonnement mathématique.

Pour palier à certaines lacunes constatés chez les étudiants de 2ème année licence mathématiques, on a opté pour l'ajout d'une section "éléments du langage mathématique" et une section "bonnes habitudes de rédaction".

Le chapitre 2 est consacré à la théorie des ensembles, après un rappel de la théorie naïve des ensembles on aborde le paradoxe de Russel. Ce paradoxe permet une transition naturelle vers la théorie de Zermelo Fraenkel noté théorie ZF. Si le polycopié aborde la théorie ZF il est néanmoins possible de passer aux sections suivantes sans préjudice.

Deux concepts importants en théorie des ensembles sont abordés en fin de chapitre, l'hypothèse du continu et l'axiome du choix.

Le chapitre 3 est consacré aux ensembles bien ordonnés et à la preuve par le principe du bon ordre.

On y aborde la version la plus simple de la preuve par le principe du bon qu'est la preuve par récurrence. On généralise ce principe au début à des ensembles où la relation du bon ordre est facile à trouver.

La preuve par le principe du bon est souvent utilisés en informatique théorique pour démontrer la finitude de certains algorithmes par exemple.

La dernière section concerne la preuve du théorème de Zermelo sur l'existence d'une relation de bon ordre pour n'importe quel ensemble.

Chaque chapitre est suivi d'exercices dont certains avec solutions dans le but de permettre aux étudiants de maitriser les différents concepts développés.

Table des matières

Chapitre 1

Logique

1.1 Calcul propositionnel

1.1.1 Proposition

Définition 1.1 *Un énoncé ne possédant que deux valeurs vrai (1) ou faux (0) sans aucune ambiguité et indépendament du contexte de l'énnoncé est dit proposition.*

On note généralement les propositions par les lettres $p, q, r \ldots$ou encore p_1, p_2,..

Exemple 1.1 *"4 n'est pas un carré parfait" est une proposition fausse.*

Exemple 1.2 *"La promotion de 2ème année licence mathématiques de l'université de Béjaia comporte 60 étudiants" n'est pas une proposition.*

Exemple 1.3 *"La promotion de 2ème année licence mathématiques de l'université de Béjaia 2015-2016 comporte 60 étudiants" est une proposition.*

Exemple 1.4 *"Steven Gerrard est un bon joueur" ne constitue pas une proposition.*

1.1.2 Connecteurs fondamentaux

Les connecteurs permettent de lier des propositions entre elles. Un connecteur se définit en donnant sa table de vérité. Définir un connecteur binaire consiste simplement à remplir la troisième colonne de la table de vérité :

p	q	$p \boxdot q$
0	0	
0	1	
1	0	
1	1	

Il existe ainsi 2^4 possibilités de remplir la dernière colonne de la table de vérité, il y a donc 16 connecteurs binaires possibles mais dont certains ne présentent aucun intéret, d'autres correspondent à des constructions logiques courantes.

La négation

Définition 1.2 *Si p est une proposition, sa négation est notée par $\neg p$, ou bien $\overline{p}$ et prend la valeur contraire de celle de p, la négation est définie par la table de vérité*

p	$\neg p$
0	1
1	0

Remarque 1.1 *Le connecteur $\neg$ est un connecteur unaire autrement dit qui lie une seule proposition.*

Disjonction (ou) / Conjonction (et)

Définition 1.3 *Les connecteurs binaires conjonction et disjecontion, notés respectivement* $\wedge$ *et* $\vee$ *sont définis par les tables de vérité :*

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

La proposition composée $p \wedge q$ *se lit "*p *et* q*" est vraie si* p *et* q *sont vraies toutes deux et fausse dans les autres cas.*
La proposition composée $p \vee q$ *se lit "*p *ou* q*" est vraie si l'une au moins des propositions* p *et* q *est vraie et fausse si* p *et* q *sont fausses.*

Remarque 1.2 *La conjonction et la disjonction sont des connecteurs associatifs.*
c'est à dire qu'on peut écrire $p \wedge (q \wedge r)$ *ou* $(p \wedge q) \wedge r$ *ou simplement* $p \wedge q \wedge r$*.*
De même $p \vee (q \vee r)$ *ou* $(p \vee q) \vee r$ *ou simplement* $p \vee q \vee r$*.*

Distributivité et lois de Morgan

Distribution de la conjonction sur la disjonction

- Les propositions $p \wedge (q \vee r)$ et $(p \wedge q) \vee (q \wedge r)$ sont équivalentes (possèdent la même table de vérité).

Distribution de la disjonction sur la conjonction.

- Les propositions $p \vee (q \wedge r)$ et $(p \vee q) \wedge (q \vee r)$ sont équivalentes (possèdent la même table de vérité).

Lois de Morgan

- La négation de la proposition $(p \wedge q)$ est la proposition $\neg p \vee \neg q$.
- La négation de la proposition $(p \vee q)$ est la proposition $\neg p \wedge \neg q$.

Disjonction exclusive (xor)

Définition 1.4 *: Soient p et q deux propositions, la proposition composée $(p \vee q) \vee^{\neg} (p \wedge q)$ s'écrit $p \oplus q$. Le connecteur binaire $\oplus$ est appelé disjonction exclusive, la proposition $p \oplus q$ est vraie si une et une seule des propositions est vraie et la table de vérité est donnée par :*

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Remarque 1.3 *xor est une abréviation de e**x**clusive **or.***

Implication logique (si ... alors...)

Définition 1.5 *Soient p et q deux propositions, la proposition "Si p Alors q" se note $p \Rightarrow q$ le connecteur binaire s'appelle **implication** et il est défini par la table de vérité.*

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

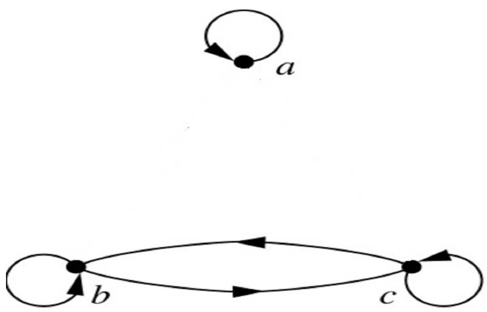
*p est dit **antécédent** et q est dit **conséquent.***

Remarque 1.4 *Il existe d'autres expressions gramaticales qui ont la même intérpétation* *que l'expression "Si...Alors...".*

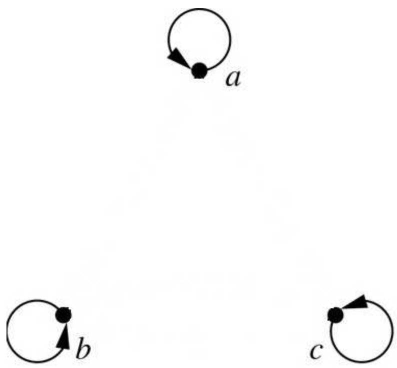
$$\left.\begin{array}{l} q \text{ si } p \\ p \text{ est une condition suffisante pour } q \\ \text{Pour } q \text{ il suffit que } p \\ q \text{ est une condition nécéssaire pour } p \\ p \text{ seulement si } q \end{array}\right\} : p \Rightarrow q$$

Exemple 1.5 *Une enseignante dit à ses élèves "Si vous répondez juste à la question que je vais poser alors je vous rajouterai un point en plus", l'enseignante pose sa question et aucun élève ne trouve la réponse juste, l'enseignante rajoute un point à chaque élève et ces derniers ne comprennent pas."*
Si on note $P =$ *"répondre juste à la question" et* $Q =$ *" Rajouter un point".*
L'implication logique $P \Rightarrow Q$ *est vraie dans les deux situations (que l'enseignante distribue des points ou pas) car* P *est fausse.*

Exemple 1.6 *On se donne les relations suivantes définies sur un ensemble* $E = \{a, b, c\}$ *par les graphes :*



Relation $n^\circ = 1$



Relation $n^\circ = 2$

Les relations $n^\circ = 1$ *et* $n^\circ = 2$ *sont symétriques.*

La définition d'une relation symétrique est donnée par :

$$\forall (x, y) \in \mathbb{E}^2 : xRy \Rightarrow yRx \qquad (*)$$

Relation n° = 1 :

- Dans le cas de l'élément a les relations aRb, bRa, cRa, aRc sont fausses ce qui entraine que l'implication logique $(*)$ est vraie.

Relation n° = 2 :

Toutes les relations de type xRy où $x \neq y$ sont fausses ce qui entraine que l'implication logique $(*)$ est toujours vraie.

Définition 1.6 *L'implication $q \Rightarrow p$ est appelée réciproque de $p \Rightarrow q$. L'implication $\neg q \Rightarrow \neg p$ est appelée contraposée de $p \Rightarrow q$*

Remarque 1.5 *Une implication a toujours la même table de vérité que sa contraposée en effet on a :*

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$\neg q \Rightarrow \neg p$
0	0	**1**	1	1	**1**
0	1	**1**	0	1	**1**
1	0	**0**	1	0	**0**
1	1	**1**	0	0	**1**

Remarque 1.6 *Une implication n'a pas la même table de vérité que sa réciproque.*

p	q	$p \Rightarrow q$	$q \Rightarrow p$
0	0	**1**	***1***
0	1	**1**	***0***
1	0	**0**	***1***
1	1	**1**	***1***

Proposition 1.1 *La négation de la proposition $p \Rightarrow q$ est la proposition $p \wedge^{\neg} q$.*

Preuve. On a recours à la table de vérité.

p	q	$p \Rightarrow q$	$^{\neg}(p \Rightarrow q)$	p	$^{\neg}q$	$p \wedge^{\neg} q$
0	0	1	**0**	0	1	**0**
0	1	1	**0**	0	0	**0**
1	0	0	**1**	1	1	**1**
1	1	1	**0**	1	0	**0**

■

Equivalence (si et seulement si)

Définition 1.7 *Soient p et q deux propositions, la proposition composée $(p \Rightarrow q) \wedge (q \Rightarrow p)$ est dite "p si et seulement si q".*
On note $p \Leftrightarrow q$ et la table de vérité est donnée par :

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

1.1.3 Formules propositionnelles

Définition 1.8 *Une formule propositionnelle est dite atomique si elle ne peut pas s'écrire en fonction d'autres formules propositionnelles à l'aide des connecteurs fondamentaux.*

Exemple 1.7 *La formule propositionnelle p : "4 est un carré parfait" est une formule atomique.*
La forumule "4 est un carré parfait alors 4 est un nombre pair " n'est pas une formule atomique.

Définition 1.9 *Une formule propositionnelle se définit par :*
i) Toute formule atomique est une formule propositionnelle.
ii) Si $\mathcal{A}$ est une formule alors $\urcorner\mathcal{A}$ est aussi une formule.
iii) Si $\mathcal{A}$ et $\mathcal{B}$ sont des formules alors $(\mathcal{A} \wedge \mathcal{B}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \Rightarrow \mathcal{B})$ sont aussi des formules.
iv) Rien d'autres n'est une formule.

1.1.4 Système complet de connecteurs

Définition 1.10 *On dit qu'un ensemble de connecteurs C est un système complet de connecteurs si toute formule propositionnelle est équivalente à une formule n'utilisant que les connecteurs de C.*

Proposition 1.2 *L'ensemble $\{\urcorner, \vee\}$ est un système complet de connecteurs.*

Preuve. Il suffit de montrer que les propositions $(p \wedge q), (p \Rightarrow q), (p \Leftrightarrow q)$ peuvent s'écrire en utilisant seulement les connecteurs $\urcorner, \vee$.
i) On a $(p \wedge q) \Leftrightarrow \urcorner(\urcorner p \vee \urcorner q)$.
ii) On a $(p \Rightarrow q) \Leftrightarrow \urcorner p \vee q$.
iii) On a $(p \Leftrightarrow q) \Leftrightarrow (\urcorner p \vee q) \wedge (\urcorner q \vee p)$. ■

1.1.5 Tautologie et antilogie

Définition 1.11 *Une tautologie est une formule (proposition composée) dont la valeur de vérité est toujours 1*
- Pour signifier qu'une formule est une tautologie on note : $\vdash F$.
- Une proposition qui est toujours fausse est une antilogie ou une contradiction.

Exemple 1.8 *Soit p une proposition, la formule $p \vee \urcorner p$ est une tautologie.*

p	$\urcorner p$	$p \vee \urcorner p$
0	1	1
1	0	1

Exemple 1.9 *Soit* p *une proposition, la formule* $p \wedge^{\neg} p$ *est une contradiction.*

p	$^{\neg}p$	$p \wedge^{\neg} p$
0	*1*	*0*
1	*0*	*0*

1.2 Calcul des prédicats

1.2.1 Quantificateur universel et existentiel

Définition 1.12 *Un prédicat est un énnoncé dépendant d'une ou plusieurs variables. La valeur de vérité du prédicat dépend ainsi de la (les) variable(s) le composant.*

Exemple 1.10 $p(x) : x^2 + 1 = 2x$ *est un prédicat. On ne peut connaitre sa valeur de vérité qu'en remplaçant la valeur de* x.
Ainsi le prédicat est vrai pour $x = 1$ *et faux pour* $x \neq 1$.

Définition 1.13 *Soit* $p(x)$ *un prédicat dépendant de la variable* x. *On introduit les propositions :*
1- $\forall x\ (p(x))$ *: Par définition cette proposition est vraie si toute valeur de* x *rend vrai le prédicat* $p(x)$.
2- $\exists x\ (p(x))$ *: Par définition cette proposition est vraie s'il existe au moins une valeur de* x *pour laquelle le prédicat* $p(x)$ *est vrai.*
Les symboles $\forall$ *et* $\exists$ *s'appellent respectivement quantificateur universel et quantificateur existentiel.*

Exemple 1.11 *"tous les étudiants possèdent un tél portable" peut se formaliser de la façon suivante :*

$$\forall x\ (x \text{ est un étudiant } \Longrightarrow x \text{ possède un tél portable}).$$

Exemple 1.12 *"Un pays d'Afrique au moins est en guerre" peut se formaliser de la façon suivante :*

$$\exists x\ (x \textit{ est un pays d'Afrique } \wedge\ x \textit{ est en guerre}).$$

Dans la plupart des cas les variables sur lesquels portent les quantificateurs sont prises dans des ensembles. On adopte ainsi les notations suivantes :

- $\forall x \in A : p(x)$ est utilisée pour désigner la formule $\forall x((x \in A \Longrightarrow p(x)))$.
- $\exists x \in A : p(x)$ est utilisée pour désigner la formule $\exists x((x \in A) \wedge p(x))$.

Remarque 1.7 *La formule $\forall x \in \phi : p(x)$ est toujours vraie.*
Comme la formule $\forall x \in \phi : p(x)$ est une notation abrégée de $\forall x((x \in \phi \Longrightarrow p(x)))$.
La proposition $x \in \phi$ étant fausse pour toutes les valeurs de x la proposition $x \in \phi \Longrightarrow p(x)$ est donc vraie pour toutes les valeurs de x.

1.2.2 Quantificateurs multiple

Lorsque un prédicat à plusieurs variables est quantifié universellement et existentiellement, l'ordre dans lequel apparaissent les quantificateurs est important. Ainsi pour un prédicat $p(x, y)$ les formules $\forall x$, $\exists y$, $p(x, y)$ et $\exists x$,$\forall y$,$p(x, y)$ n'ont pas le même sens.

Exemple 1.13 *Soit G un ensemble muni d'une loi interne notée $*$.*
La formule $\exists e \in G, \forall x \in G : e * x = x * e = x$ et différente de la formule $\forall x \in G, \exists e \in G : e * x = x * e = x$.
Dans la première formule l'existence de e est indépendante de la variable x.
Dans la seconde formule pour chaque élément x il existe un élément e.

Remarque 1.8 *Il est possible de permuter les quantificateurs lorsqu'ils sont de même nature et consécutifs.*

Exemple 1.14 *Les deux formules ci dessous sont équivalentes :*

$$\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x^2 + y^2 \geq 0.$$

$$\forall y \in \mathbb{R}, \forall x \in \mathbb{R} : x^2 + y^2 \geq 0.$$

1.2.3 Négation d'un quantificateur

Les règles fondamentales de négation des formules sont données par :

$$\neg \forall x : p(x) \Longleftrightarrow \exists x : \neg p(x) \qquad \neg \exists x : p(x) \Longleftrightarrow \forall x : \neg p(x)$$

Ces règles sont appliquées succesivement a plusieurs quantificateurs.

1.2.4 Quantificateurs et connecteurs

Dans des formules faisant une utilisation simultanée de quantificateurs et des connecteurs de conjonction et de disjonction il faut faire attention à la signification des formules.

Ainsi les formules : $\forall x : (p(x) \wedge q(x))$ et $(\forall x : p(x)) \wedge (\forall x : q(x))$ sont équivalentes.

Par contre les formules $\forall x : (p(x) \vee q(x))$ et $(\forall x : p(x)) \vee (\forall x : q(x))$ ne sont pas équivalentes, la seconde implique la première.

De même $\exists x : (p(x) \vee q(x))$ et $(\exists x : p(x)) \vee (\exists x : q(x))$ sont équivalentes, alors que $\exists x : (p(x) \wedge q(x))$ implique $(\exists x : p(x)) \wedge (\exists x : q(x))$.

Exemple 1.15 *Soit x une variable prenant ses valeurs dans l'alphabet habituel et soient les prédicats :*

$$cons(x) : x \text{ est une consonne}$$
$$voy(x) : x \text{ est une voyelle}$$

La formule $\forall x(cons(x) \vee voy(x))$ affirme que toute lettre de l'alphabet est une consonne ou une voyelle.

Exemple 1.16 *La formule* $(\forall x\ cons(x)) \vee (\forall x\ voy(x))$ *affirme que toute les lettres de l'alphabet sont soit toutes des consonnes soit toutes des voyelles.*

Exemple 1.17 *La formule* $(\exists x\ cons(x)) \wedge (\exists x\ voy(x))$ *exprime qu'il existe dans l'alphabet au moins une consonne et au moins une voyelle.*

Exemple 1.18 *La formule* $\exists x(cons(x) \wedge voy(x))$ *affirme qu'il existe une lettre qui est à la fois une voyelle et consonne.*

1.2.5 Le quantificateur d'unique existence

Le quantificateur $\exists!$ signife "il existe un et un seul", la formule $\exists!\ x : p(x)$ affirme l'existence d'une unique valeur de la variable x rendant vrai le prédicat $p(x)$, cette affirmation peut s'exprimer par les quantificateurs $\forall$ et $\exists$:

$$(\exists x, p(x)) \wedge (\forall y, \forall z, (p(y) \wedge p(z)) \Longrightarrow y = z)$$

1.2.6 Clôture d'un prédicat

Définition 1.14 *Une variable qui apparait à la suite d'un quantificateurest dite liée. Une variable qui n'est pas liée est dite libre.*

Exemple 1.19 $\exists x \in \mathbb{R} : x^2 = \alpha$. *Ici la variable* x *est liée et la variable* α *est libre.*

Définition 1.15 *Une formule qui ne comporte aucune variable libre est dit close. Une formule close est une proposition.*

Exemple 1.20 *La formule* $\forall \alpha \in \mathbb{R}^+, \exists x \in \mathbb{R} : x^2 = \alpha$ *est une formule close (toutes les variables sont liées).*
C'est une proposition vraie.

Définition 1.16 *La clôture universelle (resp. clôture existentielle) d'une formule est la formule obtenue en adjoignant au début de cette formule les quantificateurs* $\forall$ *(resp.* $\exists$*) à toutes les variables libres de la formule.*

Exemple 1.21 *Soit le prédicat* $P(x,y) : x^2 = -y^2 - 1$.
La clôture universelle de ce prédicat est donnée par $\forall x \in \mathbb{R}, \forall y \in \mathbb{R} : x^2 = -y^2 - 1$.
La clôture existentielle de ce prédicat est donnée par $\exists x \in \mathbb{R}, \exists y \in \mathbb{R} : x^2 = -y^2 - 1$.

Définition 1.17 *Une formule est dite valide si sa clôture universelle est valide (vraie dans toutes les situations).*
Une formule est dite inconsistente si sa négation est valide.

1.3 Règles de déduction (d'inférences)

Les règles d'inférences sont des règles basées sur des tautologies , elles constituent la base des preuves mathématiques.

1.3.1 Modus Ponens (Preuve directe)

On dit qu'une proposition q découle logiquement d'une proposition vraie p si l'implication $p \Rightarrow q$ est vraie on écrit dans ce cas :

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline \therefore q \end{array}$$

où le signe $\therefore$ se lit " Par conséquent".

La proposition p est appelée hypothèse et q est appelée thèse.

La règle du Modus Ponenes est basée sur la tautologie $(p \wedge (p \Rightarrow q)) \Rightarrow q$. En effet on a :

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
0	0	1	0	**1**
0	1	1	0	**1**
1	0	0	0	**1**
1	1	1	1	**1**

Rédaction

La rédaction d'une preuve directe prend souvent la forme suivante :

> **Proposition** : Si p alors q.
>
> *Preuve :* Supposons p
>
> ...
>
> Par conséquent (D'où...) q.

Exemple 1.22 *Montrer que pour tout entier naturel impair n l'entier $3n+7$ est pair.*

$$\underbrace{\forall n \text{ entier impair}}_{P} \Rightarrow \underbrace{\exists k \in N : n = 2k+1}_{P1}$$

$$\underbrace{\exists k \in N : n = 2k+1}_{P1} \Rightarrow \underbrace{\exists k \in N : 3n+7 = 3\,(2k+1)+7}_{P2}$$

$$\underbrace{\exists k \in N : 3n+7 = 6k+8 = 2\,(3k+4)}_{P3} \Rightarrow \underbrace{3n+7 \text{ est pair}}_{Q}$$

Par transitivité de l'implication logique on obtient : $P \Rightarrow P1 \Rightarrow P2 \Rightarrow P3 \Rightarrow Q$ donc la proposition $P \Rightarrow Q$ est également vraie.
On a alors :

$$\begin{array}{l} \underbrace{\forall n \text{ entier impair}}_{P} \\ \underbrace{\forall n \text{ entier impair} \Rightarrow 3n+7 \text{ est pair}}_{P\Rightarrow Q} \\ \hline \therefore 3n+7 \text{ est pair} \end{array}$$

Remarque 1.9 *Dans une preuve directe on ne commence jamais avec une proposition fausse sinon on ne peut rien conclure. En effet si la proposition p est fausse la proposition $p \Rightarrow q$ est vraie. On ne peut obtenir aucune conclusion sur la nature de q qui peut être vraie ou fausse.*

1.3.2 Preuve par contraposé

La preuve par contraposé est basée sur l'équivalence tautologique suivante $(p \Rightarrow q) \Longleftrightarrow (\neg q \Rightarrow \neg p)$.

Elle permet dans certains cas de simplifier une démonstration.

Exemple 1.23 *L'exemple classique de l'utilisation de la preuve par contraposé concerne l'injectivité d'une application.*
Ainsi pour montrer qu'une fonction $f : E \to F$ est injective on peut montrer l'implication logique :

$$\forall x_1, x_2 \in E : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

Mais souvent il est plus simple de montrer la contraposé

$$\forall x_1, x_2 \in E : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

1.3.3 Preuve par l'absurde

La preuve par l'absurde repose sur la tautologie suivante

$$(\neg p \Rightarrow F) \Leftrightarrow p : (F : \text{proposition fausse (contradiction)})$$

p	$\neg p$	F	$\neg p \Rightarrow F$	$(\neg p \Rightarrow F) \Leftrightarrow p$
0	1	0	0	1
1	0	0	1	1

Elle consiste à démontrer qu'une implication logique ayant pour antécédent $\neg p$ et pour conséquent une contradiction est vraie.

Ainsi la seule possibilité est que la proposition $\neg p$ soit fausse ce qui entraine que la proposition p est vraie.

Cette démonstration commence en général par :"supposons $\neg p$ et cherchons une contradiction". La contradiction apparait sous forme d'une proposition et son contraire vraie en même temps.

Exemple 1.24 *Montrer que $\sqrt{2}$ est un nombre irrationel.*

Supposons que $\sqrt{2}$ est un nombre rationel. Il existe donc deux entiers m, n premiers entre eux tels que $\sqrt{2} = \dfrac{m}{n}$ avec $n \neq 0$.
En élevant au carré on obtient $2 = \dfrac{m^2}{n^2}$ on obtient donc $2n^2 = m^2$ et on déduit que m^2 est pair et par conséquent m est pair.
Puisque 2 divise m alors 4 divise m^2.
Comme le résultat de la division de m^2 par n^2 est 2 alors n aussi est pair.
On conclut donc que m et n sont pairs tous les deux ce qui constitue une contradiction avec le fait qu'ils soient premiers entre eux.

Exemple 1.25 *On va revoir la preuve de l'exemple précédent plus en détail.*

On souhaite prouver p : $\sqrt{2}$ est un nombre irrationel.
$\neg p : \exists\,(m, n) \in (\mathbb{N} \times \mathbb{N}^*) : (m \wedge n = 1) \wedge \sqrt{2} = \dfrac{m}{n}.(\sqrt{2}\textit{n'est pas un nombre irrationel})$
$\neg p \Rightarrow \exists\,(m, n) \in (\mathbb{N} \times \mathbb{N}^*) : \underbrace{(m \wedge n = 1)}_{C} \wedge \sqrt{2} = \dfrac{m}{n} \wedge \underbrace{(m \textit{ et } n \textit{ pair})}_{\neg C}$
$\neg p \Rightarrow C \wedge (\neg C)$

Exemple 1.26 *Si $a, b \in \mathbb{Z}$ alors $a^2 - 4b \neq 2$.*
Supposons que la proposition est fausse.
Il existe par conséquent deux entiers a et b tel que $a^2 - 4b = 2.\,(*)$
De cette équation on obtient $a^2 = 4b + 2 = 2\,(2b + 1)$ ainsi a^2 est pair.
Comme a^2 est pair on déduit que a est également pair, il existe un entier c tel que $a = 2c$.
En remplçant dans les termes de l'équation $(*)$ on obtient $(2c)^2 - 4b = 2$.
En divisant par 2 on obtient $2c^2 - 2b = 1$ d'où $2\,(c^2 - b) = 1$.
On déduit que l'entier 1 est pair ce qui constitue une contradiction.

1.3.4 Preuve par contre-exemple.

La preuve par contre exemple repose sur la tautologie suivante

$$\neg \forall x P\,(x) \Leftrightarrow \exists x \neg P\,(x)$$

Pour démontrer que la propostion $\forall x : P(x)$ est fausse on trouve x_0 tel que $\neg P(x_0)$ soit vraie.

1.3.5 Preuve par séparation des cas.

Soient $P_1, P_2, ...P_n$ des propositions. On souhaite prouver une proposition Q sachant que la proposition $P_1 \vee P_2 \vee ... \vee P_n$ est vraie.

Il suffit alors de prouver séparement que $\forall\ 1 \leq i \leq n$ si P_i est vraie alors Q est vraie

Exemple 1.27 *Montrer que si $n \in \mathbb{N}$ alors $1 + (-1)^n (2n-1)$ est un multiple de 4.*

Preuve : *Supposons $n \in \mathbb{N}$, ainsi n est soit pair soit impair. Considérant chaque cas séparément.*

Cas n°1 : *Supposons n pair alors il existe un entier k tel que $n = 2k$. On obtient alors :*

$$1 + (-1)^n (2n-1) = 1 + 1(2.2k - 1) = 4k$$

Cas n°2 : *Supposons n impair alors il existe un entier k tel que $n = 2k+1$. On obtient alors :*

$$1 + (-1)^n (2n-1) = 1 + -(2(2k+1) - 1) = -4k$$

1.3.6 Autres règles d'inférences

Les règles d'inférences suivantes sont moins utilisées dans les preuves mathématiques sous leurs formes directes mais permettent souvent de faire des conclusions.

$$\begin{array}{c} p \Rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array} \; , \; \begin{array}{c} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

1.4 Preuves constructives et non constructives

1.4.1 Preuves non constructives (Preuves existentielles)

Proposition 1.3 *Il existe deux nombres irrationnels x et y tels que x^y soit rationnel.*

Preuve. Nous savons que $\sqrt{2}$ est irrationnel. On considère alors le nombre $\sqrt{2}^{\sqrt{2}}$ qui est soit rationnel soit irrationnel.

Si $\sqrt{2}^{\sqrt{2}}$ est rationnel, la proposition est démontrée en considérant $x = y = \sqrt{2}$.
Si $\sqrt{2}^{\sqrt{2}}$ est irrationnel alors en posant $x = \sqrt{2}^{\sqrt{2}}$ et $y = \sqrt{2}$ on obtient $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = 2$ et la proposition est démontrée. ■

La preuve de l'existence de deux nombres x et y irrationnels tels que x^y est rationnel est faite sans qu'on puisse être capable de donner un exemple de deux nombres irrationnels qui vérifient $x^y \in Q$.

Ce type de preuves est appelé "preuve non constructive" dans le langage mathématiques.

1.4.2 Preuves constructives

Proposition 1.4 *Il existe deux nombres irrationnels x et y tels que x^y soit rationnel.*

Preuve. Soit $x = \sqrt{3}$ et $y = \log_3(4)$.
x et y sont irrationnels [1] et on a :

$$x^y = \sqrt{3}^{\log_3(4)} = 3^{\frac{1}{2}\log_3(4)} = 3^{\log_3(4)^{\frac{1}{2}}} = 3^{\log_3 2} = 2$$

■

[1] A faire comme exercice : Montrer que $\log_3(4)$ est bien irrationnel.

1.5 Rédaction d'une preuve mathématiques

Les bonnes habitudes

1. **Ne pas commencer une phrase par un symbôle mathématiques.**

Une phrase commence par une lettre majuscule alors que les variables mathématiques sont sensibles aux majuscules et minuscules.

Exemple 1.28

n étant un entier alors $4n+1$ est impair	*Mauvais*
Comme n est un entier alors $4n+1$ est impair	*Bon*
$x^2+3x+2=0$ possède deux solutions	*Mauvais*
$X^2+3x+2=0$ possède deux solutions	*Pire*
L'équation $x^2+3x+2=0$ possède deux solutions	*Bon*

2. **Terminer la phrase par un point.**

Ceci est valable même si la fin de la phrase est une expression mathématiques.

Exemple 1.29

Euler a démontré la formule $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p\in P} \frac{1}{1-\frac{1}{p^s}}$ *Mauvais*

Euler a démontré la formule $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p\in P} \frac{1}{1-\frac{1}{p^s}}.$ *Bon*

3. **Séparer les expressions mathématiques et les symbôles par des mots.**

Ne pas faire ceci peut entrainer une confusion.

Exemple 1.30

Comme $x^2-1=0, x=1$ ou $x=-1$. *Mauvais*

Comme $x^2-1=0$ on obtient $x=1$ ou $x=-1$. *Bon*

4. **Eviter l'usage abusif des symbôles mathématiques.**

Les symbôles mathématiques comme $\leq$, $\subset$, $\in$, $\Rightarrow$ ne sont pas des mots. Les utiliser hors contexte est inapproprié.

Exemple 1.31

Comme a est pair et x pair$\Rightarrow x^2$ pair, a^2 est pair.	*Mauvais*
Comme a est pair et que tout entier pair elevé au carré est pair alors a^2 est pair.	*Bon*

5. **Eviter l'usage de symbôles ou notations superflues**

Eviter d'utiliser des symbôles mathématiques quand leurs rôle n'est pas nécéssaire.

Exemple 1.32

Aucun ensemble X ne possède de cardinal négatif.	*Mauvais*
Aucun ensemble ne possède de cardinal négatif.	*Bon*

;

6. **Utiliser la première personne du pluriel**

Dans la rédaction mathématiques on s'exprime en utilisant la première personne du pluriel (on, nous, notre,...).

Je vais démontrer que ...	Mauvais
On démontre que...	Bon

7. **Expliquer chaque nouveau symbôle**

Il faut expliquer l'introduction de chaque nouveau symbôle mathématique.

Exemple 1.33

Comme a divise b on obtient : $b = ac$.	*Mauvais*
Comme a divise b il existe une constante c tel que : $b = ac$.	*Bon*

8. **Eviter la confusion**

La rédaction d'une preuve mathématiques doit éviter la confusion chez le lecteur.

Exemple 1.34 *Comme* $X \subset Y$ *et* $Card\,(X) > 0$ *on voit qu'il n'est pas vide.*
Est ce que "Il" désigne l'ensemble X *ou bien* Y.
Comme $X \subset Y$ *et* $Card\,(X) > 0$, *on déduit que l'ensemble* Y *n'est pas vide.*

9. **Eviter les preuves longues**

Si la démonstration est trop longue, on la structure en plusieurs éléments à l'aide de lemmes.

10. **Ne pas céder aux tentations**

Ne pas essayer de camoufler les passages qu'on a du mal à justifier.

11. **Traitement de cas similaires : (l'expression : sans perte de généralité)**

Il arrive que deux ou plusieurs cas dans une preuve soient similaires et que les écrire séparément paraisse répétitif ou inutile.

Exemple 1.35 *Montrer que si deux entiers sont de parités*[2] *différentes alors leurs somme est un entier impair.*
Preuve : *Soient m et n deux entiers de parités opposés*
On doit montrer que m+n est impair on alors deux cas .
Cas n$^\circ 1$: *Supposons que* m *est impair et* n *est pair. Il existe alors deux entiers* a, b *tels que* $m = 2a + 1$ *et* $n = 2b$.
D'où on obtient $m + n = 2\,(a + b) + 1$ *qui est impair.*
Cas n$^\circ 2$: *Supposons que* m *est pair et* n *est impair. Il existe alors deux entiers* a, b *tels que* $m = 2a$ *et* $n = 2b + 1$.
D'où on obtient $m + n = 2\,(a + b) + 1$ *qui est impair.*

On constate que les deux cas se traite de la même manière et que seul l'ordre dans lequel apparaissent les termes change. En général en mathématiques on évite cette répé-

[2] *Parité d'un entier : pair ou impair*

tition en utilisant l'expression *"sans perte de généralité"* la preuve précédente serait par exemple :

Exemple 1.36 *Montrer que si deux entiers sont de parités*[3] *différentes alors leurs somme est un entier impair.*

Preuve : *Soit* m *et* n *deux entiers de parités opposés*

On doit montrer que m+n est impair on a alors deux cas .

Sans perte de généralité ***s****upposons que* m *est impair et* n *est pair. Il existe alors deux entiers* a, b *tels que* $m = 2a + 1$ *et* $n = 2b$.

D'où on obtient $m + n = 2(a + b) + 1$ *qui est impair.*

[3] *Parité d'un entier : pair ou impair*

1.6 Eléments du langage mathématique

Théorème : Un théorème est un énnoncé qui a été démontré.

Lemme : Un lemme, en mathématiques et en logique mathématique, est un résultat intermédiaire sur lequel on s'appuie pour conduire la démonstration d'un théorème plus important.

Conjecture : Proposition dont on ignore encore la valeur de vérité mais qu'on soupçonne d'être vraie. (souvent en l'absence de contre exemple).

Exemple 1.37 *Conjecture de Golbach.*
Tout entier pair strictement plus grand que 2 est la somme de deux nombres premiers.

Exemple 1.38 *Conjecture de Collatz.*
Soit la suite $(u_n)_{n\in\mathbb{N}}$ définie par

$$u_{n+1} = \begin{cases} \dfrac{u_n}{2} \text{ si } u_n \text{ est pair} \\ 3u_n + 1 \text{ si } u_n \text{ est impair.} \end{cases}$$

Alors, pour tout $u_0 \in \mathbb{R}$, la suite $(u_n)_{n\in\mathbb{N}}$ tend vers la période 4,2,1.

Axiome : Un axiome est un énnoncé qui est supposé vrai.

Si au début des mathématiques le mot axiome avait tendance à désigner un énnoncé évident. Le terme axiome est utilisé désormais en logique mathématique, pour désigner une vérité première, à l'intérieur d'une théorie.

L'ensemble des axiomes d'une théorie est appelé axiomatique ou théorie axiomatique. Cette axiomatique doit être non contradictoire ; c'est sa seule contrainte.

Exemple 1.39 *La définition axiomatique des entiers naturels de Peano est usuellement décrite informellement par cinq axiomes :*
1- L'élément appelé zéro et noté 0, est un entier naturel.
2- Tout entier naturel n a un unique successeur, noté $s(n)$ ou Sn.

3- Aucun entier naturel n'a 0 *pour successeur.*

4- Deux entiers naturels ayant le même successeur sont égaux.

5- Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à $\mathbb{N}$.

Exemple 1.40 *Axiomes d'Euclide.*

1- Un segment de droite peut être tracé en joignant deux points quelconques distincts ;

2- Un segment de droite peut être prolongé indéfiniment en une ligne droite ;

3- Étant donné un segment de droite quelconque, un cercle peut être tracé en prenant ce segment comme rayon et l'une de ses extrémités comme centre ;

4- Tous les angles droits sont congruents ;

5- Si deux lignes sont sécantes avec une troisième de telle façon que la somme des angles intérieurs d'un côté est strictement inférieure à deux angles droits, alors ces deux lignes sont forcément sécantes de ce côté.

1.7 Exercices

Exercice 1.1 *Soient* p, q, r *des propositions, donner la table de vérité de chacune des propositions composées suivantes :*

$$p \Rightarrow (p \Rightarrow q)\,; \quad q \vee (\neg q \wedge p)\,; \quad (p \vee q) \Rightarrow r.$$

Exercice 1.2 *Réécrire chaque phrase en utilisant la notation d'implication logique "Si ...Alors...".*

1- Pour qu'une fonction soit continue, il suffit qu'elle soit dérivable.

2- Un entier est divisible par 8 seulement s'il est divisible par 4.

Exercice 1.3 *Montrer que les ensembles* $\{\urcorner, \wedge\}$ *et* $\{\urcorner, \Rightarrow\}$ *sont des systèmes complets de connecteurs.*

Exercice 1.4 *Donner les valeurs des entiers* $n, m \in \mathbb{N}$ *vérifiant*

$$Si\ n^2 + m^2 = 25\ alors\ n < m.$$

Exercice 1.5 *On se donne la "définition" suivante d'un nombre quadruple :*

"On dit qu'un entier n est quadruple s'il vérifie la proposition suivante : si 2 divise n alors 4 divise n"

Selon cette définition est ce que les nombres 12,2,5,6 sont quadruples ou pas.

Solution :

Notons P : 2 divise n Q : 4 divise n. Ainsi nous avons ici l'implication logique $P \Rightarrow Q$

n	P : 2 divise n	Q : 4 divise n	$P \Rightarrow Q$	Application de la définition
12	V	V	V	12 est quadruple.
2	V	F	F	2 n'est pas quadruple
5	F	F	V	5 est quadruple
6	V	F	F	6 n'est pas quadruple

Ainsi selon cette définition seuls les nombres 2 et 6 ne sont pas quadruples.

Exercice 1.6 *Montrer que la relation de l'ordre strict $<$ sur l'ensemble $\mathbb{R}$ est antisymétrique.*

Solution : Notons $P : x < y$ et $Q : y < x$ enfin $S : x = y$

	$x < y$	$y < x$	$P \wedge Q$	$P \wedge Q \Rightarrow S$
Si $x < y$	V	F	F	V
Si $x > y$	F	V	F	V
Si $x = y$	F	F	F	V

Exercice 1.7 *Soit $\mathcal{R}$ une relation définie sur un ensemble E.*
1) *Est ce qu'une relation peut être en même temps anti réflexive et transitive ?*
2) Est ce qu'une relation peut être en même temps anti réflexive, transitive et vérifier la condition ci dessous ?

$$\forall x \in E, \exists y \in E : x\mathcal{R}y$$

Exercice 1.8 *Un étudiant pense que dans la définition de la relation d'équivalence la réflexivité n'est pas nécéssaire*

Voici son argument :

Puisque la relation R est symétrique alors on a

$\forall (x, y) \in E \times E : xRy \Rightarrow yRx.$

Par transitivité on a : $xRy \wedge yRx \Rightarrow xRx$

Donc R est réflexive.

Que pensez-vous de ce raisonnement mathématique ?

Exercice 1.9 *Montrer que $\sqrt{3}$ est irrationnel.*

Exercice 1.10 *Montrer que si $\frac{2n}{1+n^2}$ est irrationel alors n est irrationnel.*

Exercice 1.11 *Montrer que pour tout nombre réel a, si $a^2 > 0$ alors $a \neq 0$.*

Exercice 1.12 *Pour modéliser l'expression courante « Ni ... Ni... » on introduit le connecteur binaire Ni qui associe à p, q propositions atomiques la formule qu'on notera $Ni(p, q)$ qui est vraie seulement si p et q sont fausses en même temps.*
1. Donnez la table de vérité de $Ni(p, q)$.
2. Montrer qu'on peut exprimer la négation à l'aide de $Ni(p, q)$.
3. Montrer qu'on peut exprimer la disjonction à l'aide de $Ni(p, q)$.
4. Que pouvez vous déduire ?

Solution :

1. Table de vérité de $Ni(p, q)$.

p	q	$Ni(p,q)$
0	**0**	**1**
1	0	0
0	1	0
1	**1**	**0**

2. De la table de vérité précédente on remarque que $Ni(p,p) \Leftrightarrow \neg p$

p	$Ni(p,p)$
0	**1**
1	**0**

3. De la table de vérité de $Ni(p,q)$.on remarque que c'est la négation de la disjonction ainsi on peut écrie

$$Ni\left(Ni(p,q), Ni(p,q)\right) \Leftrightarrow p \vee q$$

Montrer qu'on peut exprimer la disjonction à l'aide de $Ni(p,q)$.

4. On déduit que $\{Ni\}$ constitue un système complet de connecteurs.

Exercice 1.13 *Soient les connecteurs $\mid$ et $\downarrow$ définies par*

P	Q	$P \mid Q$	$P \downarrow Q$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

Montrer que l'ensemble des connecteurs $\{\mid, \downarrow\}$ est un ensemble complet de connecteurs.

Solution : Il suffit de montrer que les connecteurs $\{\urcorner, \vee\}$ peuvent s'exprimer en fonction des connecteurs $\{\mid, \downarrow\}$.

– On commence par constater que la table de vérité de $P \mid P$ est donnée par

P	P	$P \mid P$
0	0	1
1	1	0

Ainsi $\urcorner P = P \mid P$.

– On constate ensuite que la table de vérité de $P \downarrow Q$ correspond à la négation de celle de $P \vee Q$

P	Q	$P \vee Q$	$P \downarrow Q$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

Ainsi $P \vee Q = (P \vee Q) \shortmid (P \vee Q)$

Exercice 1.14 *Formalisez les propositions suivantes en utilisant uniquement les prédicats indiqués, les connecteurs et les quantificateurs :*

1. Personne n'est parfait : $[p(x) : x \text{ est parfait}]$.

2 . L'entier 0 *est multiple de chaque nombre entier*

$$[m(x,y) : x \text{ est multiple de } y; e(x) : x \text{ est un entier}].$$

3. Les absents n'ont pas tous tort $[a(x) : x \text{ est absent}\,;\, t(x) : x \text{ a tort}]$.

Exercice 1.15 *Ecrivez la négation des formules suivantes :*

1.	$\forall x\,(p(x) \Rightarrow q(x))$	***2.***	$\exists x\,(p(x) \wedge q(x))$
3.	$\forall x\,(p(x) \Leftrightarrow q(x))$	***4.***	$\exists x \forall y\,(q(x,y) \Rightarrow p(x,y) \vee r(x,y))$
5.	$\forall x\ \exists y\ (p(x,y) \Leftrightarrow q(x,y))$	***6.***	$\forall x\,(\exists y\ p(x,y) \Rightarrow r(x))$
7.	$\forall x \exists y\ p(x,y) \Rightarrow \forall z\ r(z)$	***8.***	$\forall x\,(r(x) \Rightarrow \exists y p(x,y))$

Exercice 1.16 *Soient les prédicats :*

$Etudiant\,(x) : (x \text{ est un étudiant})\,, vélo\,(y) : (y \text{ est un vélo})\,,\ possède\,(x,y) : (x \text{ possède } y)$

Traduisez en language courant les propositions suivantes :

1. $\forall x\,(\textit{vélo}\,(x) \Rightarrow \exists z\,(\textit{Etudiant}\,(z) \wedge \textit{possède}\,(z,x)))\,.$

2. $\forall x\,(\textit{Etudiant}\,(x) \Rightarrow \forall y \forall z\,(\textit{vélo}\,(z) \wedge \textit{vélo}\,(y) \wedge (z \neq y) \Rightarrow \neg\textit{possède}\,(x,z) \vee \neg\textit{possède}\,(x,y)))\,.$

3. $\exists x\,(\textit{Etudiant}\,(x) \wedge \forall y\,(\textit{vélo}\,(y) \Rightarrow \neg\textit{possède}\,(x,y)))\,.$

Exercice 1.17 *Même question pour :*

1. $\forall x(F(x) \Rightarrow G(x))$.

2. $\forall x(F(x) \Rightarrow \neg G(x))$.

3. $\exists x(F(x) \wedge G(x))$.

Exercice 1.18 *Soit x une variable prenant ses valeurs dans l'alphabet habituel et soient les prédicats :*

$$\begin{aligned} \textit{cons}\,(x) &\;:\; x \text{ est une consonne.} \\ \textit{voy}\,(x) &\;:\; x \text{ est une voyelle} \end{aligned}$$

Expliquer dans chaque cas l'affirmation donnée par les propositions suivantes :

1. $\forall x\ (\textit{cons}\,(x) \vee \textit{voy}\,(x))$

2. $(\forall\ x\ \textit{cons}\,(x)) \vee (\forall x\ \textit{voy}\,(x))$

3. $(\exists x\ \textit{cons}\,(x)) \wedge (\exists x\ \textit{voy}\,(x))$

4. $\exists x\ (\textit{cons}\,(x) \wedge \textit{voy}\,(x))$.

Exercice 1.19 *Les deux formules suivantes sont elles équivalentes ?*

$$\begin{aligned} F1 &\;:\; \exists m,n \in \mathbb{N} : m \wedge n = 1 \wedge \sqrt{2} = \frac{m}{n} \\ F2 &\;:\; (\exists m,n \in \mathbb{N} : m \wedge n = 1) \wedge \left(\exists m,n \in \mathbb{N} : \sqrt{2} = \frac{m}{n}\right) \end{aligned}$$

Exercice 1.20 *Soit Q la proposition $\forall x\,(p\,(x) \vee q\,(x))$ et P la proposition $(\forall x\ p\,(x)) \vee (\forall x\ q\,(x))$*

1. Démontrer que $P \Rightarrow Q$.

2. Est ce qu'on a $Q \Rightarrow P$? Justifier votre réponse.

Exercice 1.21 *Montrer que si r est irrationnel alors $\sqrt{r}$ est aussi irrationnel.*

Exercice 1.22 *Montrer que la proposition $(p \Rightarrow q) \Longleftrightarrow (\neg q \Rightarrow \neg p)$ est une tautologie.*

Exercice 1.23 *Montrer que tout entier multiple de 4 s'écrit sous la forme* $1+(-1)^n(2n-1)$.

Exercice 1.24 *Montrer que pour tout réel $x \in \left[0, \frac{\pi}{2}\right]$ on a* $\sin(x) + \cos(x) \geq 1$.

Exercice 1.25 *Ci dessous deux preuves de la proposition : $\sqrt{2}$ est un nombre irrationnel.*

Lire chaque preuve et répondre aux questions suivantes :

1. Quel est le mode de raisonement utilisé pour chaque preuve.

2. Dire pour chaque preuve s'il s'agit d'une preuve constructive ou pas.

***Preuve n°**1 :*

Supposons que $\sqrt{2}$ est un nombre rationel. Il existe donc deux entiers m, n premiers entre eux tel que $\sqrt{2} = \frac{m}{n}$.

En élevant au carré on obtient $2 = \frac{m^2}{n^2}$ on obtient donc $2n^2 = m^2$ et on déduit que m^2 est pair et par conséquent m est pair.

Puisque 2 divise m alors 4 divise m^2.

Comme le résultat de la division de m^2 par n^2 est 2 alors n aussi est pair.

On conclut donc que m et n sont pairs tous les deux ce qui constitue une contradiction avec le fait qu'ils soient premiers entre eux.

***Preuve n°**2 :*

Pour toute valeur de $a \in \mathbb{Z}$ et toute valeur $b \in \mathbb{Z}^*$ on a :

$$\left|\sqrt{2} - \frac{a}{b}\right| = \left|\frac{\sqrt{2}b - a}{b}\right| = \left|\frac{\sqrt{2}b - a}{b} \times \frac{\sqrt{2}b + a}{\sqrt{2}b + a}\right| = \left|\frac{2b^2 - a^2}{\sqrt{2}b^2 + ab}\right| = \frac{|2b^2 - a^2|}{\sqrt{2}b^2 + ab}$$

On peut écrire a et b sous la forme $a = 2^n x$ et $b = 2^m y$ où n et m sont des entiers naturels et x et y sont impairs.

On obtient : $a^2 = 2^{2n}x^2$ et $2b^2 = 2^{2m+1}y^2$ ainsi dans les factorisations en nombres premiers de a^2 et $2b^2$ ne sont pas identiques et par conséquent $|2b^2 - a^2| \geq 1$.

Si $\dfrac{a}{b} = \sqrt{2}$ *alors* $\dfrac{a}{b} + \sqrt{2} \leq 3$ *(Car* $\sqrt{2} \leq \frac{3}{2}$*).En multipliant par* b *on obtient* $a + \sqrt{2} \leq 3b$ *d'où* $\dfrac{1}{a+\sqrt{2}} \geq \dfrac{1}{3b}$.
On a finalement :

$$\frac{|2b^2 - a^2|}{\sqrt{2}b^2 + ab} \geq \frac{1}{b\,(3b)} = \frac{1}{3b^2} > 0.$$

D'où il n'existe aucun rationnel égal à $\sqrt{2}$.

Chapitre 2

Introduction à la théorie des ensembles

2.1 Théorie naive des ensembles

Dans la théorie naïve des ensembles les notions d'ensemble et d'appartenance jugés intuitives ne sont pas définis de façon précise.

On note $x \in E$ le fait que x soit un élément de E. Deux ensembles sont égaux lorsqu'ils ont les mêmes éléments.

L'ensemble vide est noté par $\{\}$ ou $\varnothing$.

En général on décrit un ensemble ou bien en donnant la liste de tous ses éléments. Par exemple, l'ensemble des étudiants de 2ème année licence Analyse promotion 2016-2017 ou bien en caractérisant ses éléments parmi ceux d'un ensemble déjà connu. Par exemple $E = \{n \in \mathbb{N} \,|\, (\exists m \in \mathbb{N}) \ (n = 2m)\}$.

On dit que F est un *sous-ensemble* de E, ou bien F est contenu dans E, et on note $F \subset E$, si tout élément de F appartient aussi à E. On dit aussi que F est une *partie* de E.

La réunion de deux ensembles notée $E \cup F$ est l'ensemble de tous les éléments de E et de F. L'intersection de deux ensembles noté $E \cap F$ est l'ensemble de tous les éléments qui appartiennent à la fois à E et à F.La différence de deux ensembles noté $E\backslash F$ est l'ensemble de tous les éléments de E qui n'appartiennent pas à F.

Si $F \subset E$ alors nous notons $C_E F = E\backslash F$ l'ensemble complément de F dans E. Enfin la différence symétrique $E\Delta F$ est l'ensemble défini par $E\Delta F = (E\backslash F) \cup (F\backslash E)$.

2.1.1 Le produit cartésien

Définition 2.1 *Soient E et F deux ensembles et soient $x \in E$ et $y \in F$. Alors on définit le couple ordonné (x, y) par*

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Lemme 2.1 *On a $(x, y) = (x', y')$ si et seulement si $x = x'$ et $y = y'$.*

Preuve. On a :

$$(x, y) = (x', y') \Leftrightarrow \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}.$$

On a deux situations :
1- $\{x\} = \{x'\} \Rightarrow x = x'$ d'où $\{x, y\} = \{x', y'\}$ ainsi on obtient $y = y'$.
2- $\{x\} = \{x', y'\} \Rightarrow x = x' = y'$ comme $\{x, y\} = \{x'\}$ on obtient $x = x' = y' = y$. ■

2.1.2 Ensembles des parties

Définition 2.2 *Soit E un ensemble. On appelle ensemble des parties de E l'ensemble, noté $\mathcal{P}(E)$ constitué de touts les sous-ensembles de E.*

Exemple 2.1 *Soit $E = \{a, b, c\}$ alors*

$$\mathcal{P}(E) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

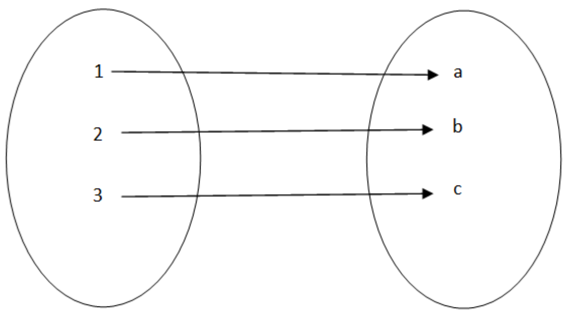
2.1.3 Relation binaire

Une relation binaire $\mathcal{R}$ d'un ensemble E vers un ensemble F est définie par une partie $G_{\mathcal{R}}$ de $E \times F$. Les composantes d'un couple appartenant au graphe d'une relation $\mathcal{R}$ sont dit en relation par $\mathcal{R}$

Si $(x, y) \in G$, on dit que x est en relation avec y et on note $x\mathcal{R}y$.

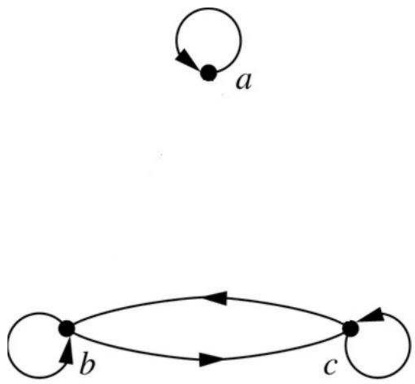
Quand une relation binaire est définie d'un ensemble E vers lui-même, on l'appelle relation interne sur E, ou simplement relation sur E.

Exemple 2.2 *Soient les ensembles* $E = \{1, 2, 3\}$ *et* $F = \{a, b, c\}$ *et la relation* $\mathcal{R}$ *définie par* $\{(1, a), (2, b), (3, c)\}$.
On peut représenter la relation $\mathcal{R}$ *par le graphe suivant dit représentation* sagittale *:*



Exemple 2.3 *Soit l'ensemble* $E = \{a, b, c\}$ *et la relation* $\mathcal{R}$ *définie par* $\{(a, a), (b, b), (b, c), (c, b), (c$
Comme l'ensemble de départ et d'arrivée sont identiques on se contente de représenter

la relation par un graphe orienté *:*



Définition 2.3 *1- Soit $\mathcal{R}$ une relation de E sur F et $\mathcal{S}$ une relation de E dans G, on définit la relation de composition $\mathcal{S} \circ \mathcal{R}$ de E sur G par :*

$$G_{\mathcal{S}\circ\mathcal{R}} = \{(x, y) \in E \times G : \exists z \in F \ \ (x, z) \in G_{\mathcal{R}} \ \textit{et} \ \ (z, y) \in G_{\mathcal{S}}\}.$$

2- Soit $\mathcal{R}$ une relation de E sur F, on peut définir une relation $\mathcal{R}^{-1}$ de F sur E dite relation inverse ou réciproque par :

$$G_{\mathcal{R}^{-1}} = \{(x, y) \in F \times E : (y, x) \in G_{\mathcal{R}}\}.$$

3- Soit $\mathcal{R}$ une relation de E sur F, on peut définir une relation $\mathcal{R}$ de F sur E dite relation complémentaire par :

$$G_{\overline{\mathcal{R}}} = \{(x, y) \in F \times E : (x, y) \notin G_{\mathcal{R}}\}.$$

4- La diagonale Δ_E d'un ensemble E et la diagonale $\left|\overline{\mathcal{R}}\right|$ d'une relation interne $\mathcal{R} \subset E \times E$ sont définis par :

$$\Delta_E = \{(x, x) : x \in E\}, \qquad \left|\overline{\mathcal{R}}\right| = \{x \in E, (x, x) \in G_{\mathcal{R}}\}.$$

Définition 2.4 *Soit $\mathcal{R}$ une relation binaire sur E.*
- $\mathcal{R}$ est réflexive si $\Delta_E \subset G_{\mathcal{R}}$.
- $\mathcal{R}$ est irréflexive si $\Delta_E \cap G_{\mathcal{R}} = \varnothing$.
- $\mathcal{R}$ est symétrique si $G_{\mathcal{R}} = \mathcal{G}_{\mathcal{R}^{-\infty}}$.
- $\mathcal{R}$ est anti-symétrique si $\mathcal{G}_{\mathcal{R}} \cap \mathcal{G}_{\mathcal{R}^{-\infty}} = \Delta_E$.
- $\mathcal{R}$ est transitive si $G_{\mathcal{R}\circ\mathcal{R}} \subset \mathcal{G}_{\mathcal{R}}$.

La définition précédente peut se traduire sous la forme suivante plus pratique lors des démonstrations.

Définition 2.5 *Soit $\mathcal{R}$ une relation binaire sur E.*
- On dit que $\mathcal{R}$ est réflexive quand : $\forall x \in E, x\mathcal{R}x$.
- On dit que $\mathcal{R}$ est irréflexive ou antiréflexive si aucun élément de E n'est en relation avec lui-même.
- On dit que $\mathcal{R}$ est symétrique quand : $\forall (x,y) \in E^2, x\mathcal{R}y \Rightarrow y\mathcal{R}x$.
- On dit que $\mathcal{R}$ est anti-symétrique quand : $\forall (x,y) \in E^2, (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$.
- On dit que $\mathcal{R}$ est transitive quand : $\forall (x,y,z) \in E^3, x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z$.

Exemple 2.4 *- La relation d'ordre usuel sur $\mathbb{R}$ est réflexive, antisymétrique et transitive.*
- La relation d'ordre strict sur $\mathbb{R}$ est antiréflexive, antisymétrique et transitive.

2.1.4 Les applications

Définition 2.6 *Un triplet $f = (E, F, G)$ avec une relation binaire $G \subset E \times F$ est une application s'il vérifie*

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

Si $E = F = \emptyset$ alors la fonction $f = (\emptyset, \emptyset, \emptyset)$ est appelée la fonction vide.

Définition 2.7 *Soient E et F deux ensembles. On dit qu'une fonction f de E dans F est :*

- *injective si*

$$\forall x, y \in E, (f(x) = f(y) \Rightarrow x = y)$$

- *surjective si*

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

- *Une bijection est une application qui est injective et surjective.*

Les définitions de relation et d'application que nous venons de voir font appel au produit cartésien et par conséquent à la notion d'ensemble. On dit dans ce cas que les définitions sont ensemblistes.

Les ensembles sont d'une importance fondamentale en mathématiques. La mécanique interne des mathématiques (nombres, relations, fonctions, etc.) peut se définir en termes d'ensembles.

2.2 Paradoxe liés à la théorie naive des ensembles

Un paradoxe, d'après l'étymologie (du grec paradoxos : « contraire à l'opinion commune », de para : « contre », et doxa : « opinion »), est une idée ou une proposition à première vue surprenante ou choquante, c'est-à-dire allant contre le sens commun.

En mathématique un paradoxe (ou antinomie) est un énoncé ou un raisonnement qui contient ou semble contenir une contradiction logique.

Plusieurs paradoxes apparaissent dans la théorie naive des ensembles où justement les notions d'ensemble et d'apprtenance ne sont pas définies clairement.

Russell décrivit le paradoxe portant son nom dans une lettre adressée en 1902 à Gottlob Frege, où il montrait à ce dernier que l'une des règles introduite dans ses Grundgesetze der Arithmetik, la compréhension non restreinte, rendait la théorie de Frege contradictoire.

Frege affirmait que n'importe quel énnoncé dépendant d'une ou plusieurs variables permet de définir un ensemble. C'est ce qui est appelé le schéma de compréhension non restreint.

2.2.1 Le paradoxe de Russell (1901)

Le paradoxe de Russell résulte de la question suivante :

"*L'ensemble de tous les ensembles qui ne s'appartiennent pas eux mêmes appartient il à lui même ?*"

L'ensemble peut se traduire par la notation suivante :

$$E = \{x : \ x \notin x\}$$

Nous avons alors deux possibilités :

1. Supposons que l'ensemble E appartient à lui même donc il vérifie le prédicat $x \notin x$ et par conséquent $E \notin E$.
2. Supposons à présent que l'ensemble E n'appartient pas à lui même on a alors :$E \notin E$ donc par définition $E \in E$.

2.2.2 Autres versions du paradoxe de Russell

Le paradoxe de Russell peut être énnoncé sous des formes plus ludiques, nous proposons ici certaines de ces formes.

Le paradoxe du barbier

Le barbier du village décide de raser tous les hommes du village qui ne se rasent pas eux-mêmes, et seulement ceux-là.

On se pose alors la question : qui rase le barbier ? Nous avons dans ce cas deux possibilités :

1. S'il se rase lui-même, alors il rase quelqu'un qui ne se rase pas lui-même.
2. S'il ne se rase pas lui-même alors il devrait se raser en respectant sa décision.

Le paradoxe du menteur crêtois

Le crétois Épiménide (entre 600 et 550 av. J.-C.) a écrit un vers à l'origine de ce paradoxe :

"Les Crétois sont toujours menteurs, de méchantes bêtes, des ventres paresseux." On se pose alors la question suivante : Est ce qu'Épiménide dit la vérité ?

Nous avons dans ce cas deux possibilités :

1. L'affirmation :"Les Crétois sont toujours menteurs" est vraie dans ce cas Épiménide dit la vérité or Épiménide est crêtois donc il ment.
2. L'affirmation :"Les Crétois sont toujours menteurs" est fausse dans ce cas Épiménide dit la vérité.

Le paradoxe du bibliothécaire

Le catalogue de tous les catalogues qui ne se mentionnent pas eux-mêmes doit il se mentionner lui même ?

1. Si le catalogue ne se mentionne pas lui même alors il devra dès lors figurer dans la liste des catalogues ne se mentionnant pas eux-mêmes.
2. Si le catalogue se mentionne lui même c'est que c'est un catalogue qui ne se mentionne pas par définition.

2.2.3 Paradoxe de Berry

L'idée de départ est de décrire les entiers naturels par des énoncés (en français).Par exemple :

1. Deux est une expression d'un mot décrivant un entier naturel.
2. Un plus deux est une expression de trois mots décrivant un entier naturel.
3. Un plus deux plus trois plus...plus neuf est une expression de 17 mots décrivant un entier naturel.

Comme le vocabulaire disponible est fini -Les dictionnaires français les plus complets atteignent 90 000 mots- les énoncés de N mots peuvent décrire au plus 90000^N entiers naturels.

Considérons à présent l'ensemble des entiers naturels non descriptibles par une expression de quinze mots ou moins.Cet ensemble possède un plus petit élément.[1] Ce plus petit élément devrait donc être exprimé par seize mots et plus or l'énoncé :

«Le plus petit entier naturel non descriptible par une expression de quinze mots ou moins.»

contient quinze mots justement d'où le paradoxe.

2.2.4 Ensemble bien défini :

Un ensemble E est bien défini si pour tout objet x l'énoncé "$x \in E$ et $x \notin E$" est faux.

2.3 Théorie de Zermelo-Fraenkel

Nous présentons une version simplifiée de la théorie de Zermelo Fraenkel. Cette théorie repose sur les axiomes suivants :

Axiome de l'égalité (ou Extensionalité)

Deux ensembles sont égaux si et seulement si ils ont les mêmes éléments.

$$\forall x \; \forall y \;\; [\forall z (z \in x \Longleftrightarrow z \in y) \Longrightarrow x = y]$$

[1] Pourquoi est ce vrai ?

Axiome de compréhension (ou de séparation).

Étant donné un ensemble U et un prédicat $P(x)$ il existe un ensemble E dont les éléments sont ceux, parmi les éléments de U, qui ont la propriété $P(x)$.

$$E = \{x \in U : P(x)\}$$

Remarque 2.1 *Cet axiome est également appelé axiome de compréhension restreint par opposition à l'axiome de compréhension universel qui mène au paradoxe de Russel.*

Proposition 2.1 *Il n'y a pas d'ensemble ayant pour éléments tous les ensembles.*

Preuve. On raisonne par l'absurde et on suppose qu'il existe un ensemble de tous les ensembles noté E.
Dans ce cas l'écriture suivante est correcte

$$F = \{x \in E : x \notin x\}.$$

Or cette écriture mène au paradoxe de Russel et donc à une contradiction.
Ainsi il n'existe pas d'ensemble contenant tous les ensembles. ■

Remarque 2.2 *On parle dans ce cas de collection de tous les ensembles.*

Axiome de la paire

Étant donnés deux ensembles a et b, il existe un ensemble c qui contient a et b et eux seulement.

$$\forall a\ \forall b\ \exists c\ \forall t\ [t \in c \Longleftrightarrow (t = x \vee t = y)]$$

L 'ensemble c dont les seuls éléments sont a et b est noté $\{a, b\}$.

Si $a \neq b$ l'ensemble$\{a, b\}$ est appelé une paire. Si $a = b$ l'ensemble $\{a, b\}$ est appelé un singleton, on le note $\{a\}$.

Axiome de la réunion (ou de la somme)

Pour tout ensemble a il existe un ensemble b dont les éléments sont exactement les éléments des éléments de a. La formule correspondante est :

$$\forall a\ \exists b\ \ (\forall x, x \in b \Longleftrightarrow \exists y\ , y \in a \wedge x \in y)\,.$$

Cet ensemble est unique, on l'appelle la réunion des éléments de x et on le note $\cup_{y\in x} y$.

Axiome de l'ensemble des parties

A tout ensemble on peut associer un ensemble qui contient exactement les parties du premier.

$$\forall a \exists b\,(\forall x, x \in b \Rightarrow x \subset a)$$

Remarque 2.3 *La notation* $x \subset a$ *est une abbréviation pour* $\forall y, y \in x \Leftrightarrow y \in a$.

Remarque 2.4 *L'ensemble des parties de l'ensemble* a *est noté* $\mathfrak{P}\,(a)\,.$

2.3.1 Axiome de l'infini

Il existe un ensemble $\mathbb{M}$ dont $\emptyset$ est élément et tel que pour tout x appartenant à $\mathbb{M}$ l'ensemble $\{x\}$ appartient aussi à $\mathbb{M}$.

Remarque 2.5 *Cet axiome construit indirectement les entiers naturels. Aini* $\emptyset$ *correspond à 0 et pour chaque entier* n *l'entier* $n+1$ *correspond à* $n \cup \{n\}\,.$

Exemple 2.5

Entier naturel	*Notation ensembliste*
0	$\emptyset$
1	$\emptyset \cup \{\emptyset\} = \{\emptyset\}$
2	$\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$
3	$\{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}\,, \{\emptyset, \{\emptyset\}\}\}$

Axiome de fondation

Tout ensemble non vide contient un élément avec lequel il n'a aucun élément en commun.

$$\forall x, (x \neq \emptyset \Longrightarrow \exists y \ (y \in x, x \cap y = \emptyset).$$

Corollaire 2.1 *Aucun ensemble ne s'auto-appartient.*

2.4 Hypothèse du continu

2.4.1 Equipotence

Définition 2.8 *Deux ensembles E et F sont équipotents si et seulement il existe une application bijective entre E et F.*
Un ensemble E est dit subpotent à un ensemble F s'il existe une injection de E dans F

Proposition 2.2 *L'équipotence est une relation d'équivalence notée $\sim$.*

Preuve. Exercice. ■

Exemple 2.6 *L'application $f :]-1,1[\to \mathbb{R}$ définie par $f(x) = \dfrac{x}{1-|x|}$ est une bijection et nous avons donc $]-1,1[\sim \mathbb{R}$.*

2.4.2 Ensembles finis / infinis

Définition 2.9 *Pour tout entier naturel n, on va noter $\mathbb{N}_n = \{x \in \mathbb{N} : x < n\} = \{0, \dots , n-1\}$ l'ensemble des n premiers entiers naturels*

Définition 2.10 *On dit que E est un ensemble fini de cardinal n, quand E est équipotent à $\mathbb{N}_n$. Un ensemble qui n'est pas fini est dit fini.*

Remarque 2.6 *L'ensemble vide est l'unique ensemble fini de cardinal 0.*

Proposition 2.3 *Toute injection d'un ensemble fini dans lui-même est une bijection.*

Preuve. Il suffit de montrer le résultat pour les ensembles $\mathbb{N}_n$.
On raisonne par récurrence sur $n \geq 1$.

Pour $n = 1$ l'ensemble $\mathbb{N}_n$ est réduit au singleton $\{1\}$ et la seule application de $\{1\}$ dans lui même est l'identité qui est une bijection.

Soit $n \geq 2$ et f une injection de $\mathbb{N}_n$ dans lui même. Soit $m = f(n-1)$, on définit l'application g de $\mathbb{N}_{n-1}$ dans lui même par :

$$g(i) = \begin{cases} f(i) \text{ si } f(i) < m \\ f(i) - 1 \text{ si } f(i) > m \end{cases}.$$

Alors g est injective puisque $n-1$ n'appartient pas à $\mathbb{N}_{n-1}$.
Par hypothèse de récurrence g est surjective. Par construction on a $\mathrm{Im}(f) = \mathrm{Im}(g) \cup \{n-1\}$ d'où $\mathrm{Im}(f) = \{0, 1, ..., n-1\}$. ■

Corollaire 2.2 *Tout ensemble fini est en bijection avec un unique intervalle* $\{1, ..., n\}$ *de* $\mathbb{N}$.

2.4.3 Ensemble dénombrable

Définition 2.11 *Un ensemble est dit dénombrable si et seulement s'il appartient à la classe d'équivalence de* $\mathbb{N}$.

Exemple 2.7 *Soit* $P = \{2k, k \in \mathbb{N}\}$ *l'ensemble des entiers pairs. Soit l'application* $f : \mathbb{N} \to P$ *qui a tout entier* k *associe* $2k$.
L'application f *est bijective, l'ensemble* P *est dénombrable.*

Exemple 2.8 *L'ensemble* $\mathbb{Z}$ *est dénombrable ainsi que* $\mathbb{Q}$.

2.4.4 Puissance du continu

Définition 2.12 *Un ensemble a la puissance du continu s'il appartient à la classe d'équivalence de* $\mathbb{R}$.

Exemple 2.9 *L'application* $f :]-1,1[\to \mathbb{R}$ *définie par* $f(x) = \dfrac{x}{1-|x|}$ *est une bijection et nous avons donc* $]-1,1[\sim \mathbb{R}$.

Théorème 2.1 (Cantor) *Pour tout ensemble* E *on a* $|E| < |P(E)|$.

Preuve. Soit f une application d'un ensemble E dans son ensemble des parties $P(E)$. Notons par D le sous-ensemble des éléments de E qui n'appartiennent pas à leur image par f :

$$D = \{x \in E : x \notin f(x)\}$$

On va montrer que l'ensemble D n'a pas d'antécédant par l'application f.
Supposons qu'il existe $y \in E$ tel que $D = f(y)$ on alors deux situations :
1- Soit $y \in D$, mais par construction de D on a $y \notin f(y) = D$ d'où $y \notin D$.
2- Soit $y \notin D = f(y)$, d'où par définition on a $y \in D$.
Par conséquent, f n'est pas surjective. ■

Hypothèse du continu : Tout sous-ensemble de l'ensemble des nombres réels est soit fini, soit infini dénombrable, soit possède la puissance du continu.

La proposition suivante est admise sans preuve.

Proposition 2.4 (Paul Cohen 1963) *L'hypothèse du continu est indépendante de la théorie axiomatique des ensembles.*

La proposition de Paul Cohen montre qu'on peut accepter ou rejeter l'hyothèse du continu sans tomber en contradiction avec les axiomes de la théorie des ensembles.

2.5 Axiome du choix

Axiome : Pour tout ensemble E, il existe une fonction qui à chaque partie non vide de E associe un élément de cette partie autrement dit :

$$\begin{aligned} f : \mathcal{P}(E) \setminus \{\emptyset\} &\to \mathcal{P}(E) \setminus \{\emptyset\} \\ X &\mapsto f(X) \in E. \end{aligned}$$

Il existe d'autres formulations équivalentes comme :

- Pour toute relation d'équivalence $\mathcal{R}$, il existe un système de représentants des classes de $\mathcal{R}$.
- Le produit d'une famille d'ensembles non vides est non vide.

L'axiome du choix ne fait pas partie du jeu d'axiomes de la théorie des ensembles ZF. On appelle théorie ZFC, la théorie ZF munie en plus de l'axiome du choix.

Les deux propositions ci dessous démontrés en 1938 et 1963 affirment qu'on peut accepter ou non l'axiome du choix sans être en contradiction avec la théorie des ensembles.

Proposition 2.5 (Kurt Godel 1938) *ZF + AC est une théorie cohérente si ZF l'est.*

Proposition 2.6 (Paul Cohen 1963) *ZF +(non) AC est une théorie cohérente si ZF l'est.*

2.6 Exercices

Exercice 2.1 *Vérifier si la définition ensembliste suivante peut convenir pour la notion de couple :*

$$(a, b) = \{\{\emptyset, a\}, \{\emptyset, b\}\}$$

Exercice 2.2 *Montrer que l'équipotence est une relation d'équivalence.*

Exercice 2.3 *Trouver une application injective de* $]0, 1[$ *vers* $]0, 1[\times]0, 1[$.

Exercice 2.4 *Trouver une application injective de* $]0,1[\times]0,1[$ *vers* $]0,1[$.

Exercice 2.5 *Trouver une application injective de* $\mathcal{P}(\mathbb{N})$ *vers* $\mathbb{R}$.

Exercice 2.6 *Soit* E *un ensemble et* $\mathcal{R}$ *une relation d'équivalence sur* E. *Soit* $a,b\in E$ *montrer qu'on a soit* $\widetilde{a}=\widetilde{b}$ *ou* $\widetilde{a}\cap\widetilde{b}=\emptyset$. *Où* $\widetilde{a}$ *désigne la classe d'équivalence de* a.

Exercice 2.7 *Que pensez vous du raisonnement suivant :*

> *Soit* X *un ensemble. L'ensembe vide n'est pas inclus dans* X.
> *Preuve : Pour que l'ensemble vide soit un sous ensemble de X,*
> *il faut que chaque élément de l'ensemble vide soit un élément de X.*
> *Comme l'ensemble vide n'a aucun élément cette condition n'est pas*
> *satisfaite. Alors l'ensemble vide n'est pas un sous ensemble de X.*

Exercice 2.8 *Soient* E,F *deux ensembles et* f *une application de* E *dans* F. *Démontrer que :*

1. $\forall(A,B)\in\mathcal{P}(E)^2, f(A\cup B)=f(A)\cup f(B)$.
2. $\forall(A,B)\in\mathcal{P}(E)^2, f(A\cap B)\subset f(A)\cap f(B)$.
3. $\forall B\in\mathcal{P}(E), f(f^{-1}(B))\subset B$.

Démontrer les équivalences suivantes :

1. f est injective $\Leftrightarrow\forall(A,B)\in\mathcal{P}(E)^2, f(A\cap B)=f(A)\cap f(B)$.
2. f est surjective $\Leftrightarrow\forall B\in\mathcal{P}(E), f(f^{-1}(B))=B$.

Exercice 2.9 *Soient* E,F *deux ensembles et* f *une application de* E *dans* F.*On pose*

$$\begin{aligned}\overline{f}&:\mathcal{P}(E)\to\mathcal{P}(E)\\ X&\longmapsto\overline{f}(X)=f(X)\end{aligned}$$

Montrer que :

1. $\overline{f}$ injective $\Leftrightarrow f$ injective.

2. $\overline{f}$ surjective $\Leftrightarrow f$ surjective.

Exercice 2.10 *Soit E un ensemble, A et B deux parties de E. Soit l'application :*

$$\begin{aligned} f : \mathcal{P}(E) &\to \mathcal{P}(A) \times \mathcal{P}(B) \\ X &\longmapsto (X \cap A, X \cap B) \end{aligned}$$

1. Démontrer que : f injective $\Leftrightarrow A \cup B = E$.

2. Démontrer que : f surjective $\Leftrightarrow A \cap B = \emptyset$.

3. A quelle condition f est-elle bijective ? Expliciter alors f^{-1}.

Exercice 2.11 *Montrer que $\mathbb{R} \backslash \mathbb{Q}$ n'est pas dénombrable.*

Chapitre 3

Bon ordre et preuve par récurrence

3.1 Preuve par récurrence

3.1.1 Preuve par récurrence simple

Théorème 3.1 *Soit $\mathcal{P}(n)$ un prédicat dépendant d'un élément n de $\mathbb{N}$.*
On suppose que $\mathcal{P}(0)$ est vraie. ***(Initialisation)***
On suppose également que pour tout entier n l'implication $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ est vraie. ***(Hérédité)***
Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier n.

Preuve. On raisonne par l'absurde.
Soit $E = \{n \in N, \mathcal{P}(n) \text{ est faux}\}$.
En tant que partie non vide de $\mathbb{N}$, l'ensemble E a un plus petit élément n_0.
n_0 est différent de 0 car on a supposé $P(0)$ vraie comme $0 < n_0$ on sait que $n_0 - 1 \in \mathbb{N}$.
$P(n_0 - 1)$ est vraie car $n_0 - 1 \notin E$.
Par hypothèse $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$ d'où $\mathcal{P}(n_0)$ est vraie ce qui contredit le fait que $n_0 \in E$.
Cette méthode de démonstration utilise le principe dit :**"principe du bon ordre".** ■

Exemple 3.1 *Soit la suite définie par la relation de récurrence :*

$$\begin{cases} u_0 = \dfrac{1}{2} \\ u_{n+1} = \dfrac{1+u_n^2}{2}, \forall n \geq 0. \end{cases}$$

On va montrer par récurrence que $(u_n)_{n\in\mathbb{N}}$ *est majorée par 1.*
Pour $n = 0$ *on a* $u_0 = \dfrac{1}{2} \leq 1$.
On suppose ensuite que la proposition est vraie pour n *et on la démontre pour* $n+1$.
On remarquera que les termes de la suite sont positifs.

$$0 \leq u_n \leq 1 \Rightarrow u_n^2 \leq 1 \Rightarrow u_n^2 + 1 \leq 1 + 1 \Rightarrow \frac{1+u_n^2}{2} \leq \frac{2}{2} = 1.$$

3.1.2 Schéma de preuve par le principe du bon ordre

1. Définir l'ensemble $E = \{n \in \mathbb{N} : P(n) \text{ est faux}\}$
2. Supposer que E est non vide comme base pour une preuve par contradiction.
3. Comme $\mathbb{N}$ est bien ordonné , il y a un plus petit élément n_0 dans E.
4. Le plus petit élément ne peut pas être celui de la proposition de départ. Utiliser l'hérédité pour arriver à la contradiction.

Exemple 3.2 *Soit la suite définie par la relation de récurrence :*

$$\begin{cases} u_0 = \dfrac{1}{2} \\ u_{n+1} = \dfrac{1+u_n^2}{2}, \forall n \geq 0. \end{cases}$$

On va montrer par le principe du bon ordre que $(u_n)_{n\in\mathbb{N}}$ *est majorée par 1.*
On raisonne par l'absurde.
Soit $E = \{n \in \mathbb{N},\ u_n > 1\}$
En tant que partie non vide de $\mathbb{N}$ *l'ensemble* E *a un plus petit élément* n_0.

On a n_0 *différent de* 0 *car on a* $u_0 = \frac{1}{2} \leq 1$.
Comme $0 < n_0$ *on sait que* $n_0 - 1 \in \mathbb{N}$ *et* $n_0 - 1 \notin E$.

$$0 \leq u_{n_0-1} \leq 1 \Rightarrow u_{n_0-1}^2 \leq 1 \Rightarrow u_{n_0-1}^2 + 1 \leq 1+1 \Rightarrow \frac{1+u_{n_0-1}^2}{2} \leq \frac{2}{2} = 1 \Rightarrow u_{n_0} \leq 1 \Rightarrow u_{n_0} \notin E.$$

Ce qui contredit le fait que $n_0 \in E$.

Exemple 3.3 ***Importance de l'initialisation***
Est ce que $3^{2n+4} - 2^n$ *est un multiple de* 7 *?*
Supposons que $3^{2n+4} - 2^n$ *est un multiple de* 7.
On va montrer que $3^{2(n+1)+4} - 2^{n+1}$ *est un multiple de* 7.
On a

$$\begin{aligned} 3^{2n+6} - 2^{n+1} &= 9 \times 3^{2n+4} - 2 \times 2^n = (7+2) \times 3^{2n+4} - 2 \times 2^n \\ &= 7 \times 3^{2n+4} + 2 \times 3^{2n+4} - 2 \times 2^n \end{aligned}$$

On a par conséquent la somme de deux multiples de 7 qui est donc un multiple de 7.
Ici l'initialiation est impossible pour $n = 0$ *on a* $3^4 - 2^0 = 80$ *qui n'est pas divisible par 7.*
On peut démontrer en utilisant le calcul par congruences que $3^{2n+4} - 2^n$ *n'est pas un multiple de* 7.
En effet on a :

$$3^2 \equiv 2\,[7] \Rightarrow 3^{2n} \equiv 2^n\,[7] \text{ de plus on a } 3^4 \equiv 4\,[7] \text{ d'où } 3^{2n+4} \equiv 4.2^n\,[7]$$
$$\text{On a également } 2^n \equiv 2^n\,[7] \text{ d'où } 3^{2n+4} - 2^n \equiv 3.2^n\,[7]$$

Comme 7 *ne divise pas 3 ni 2 alors* 7 *ne divise pas* $3^{2n+4} - 2^n$.

Remarque 3.1 *Pour montrer qu'une proposition* $\mathcal{P}(n)$ *est vraie pour tout entier* $n \geq n_0$, *on remplace l'hypothèse d'initialisation par* $\mathcal{P}(n_0)$ *est vraie.*

Exemple 3.4 *Preuve par récurrence simple (avec un pas supérieur à 1)*

La suite de Fibonnaci[1] *est donnée par*

$$\begin{cases} F_0 = 0. \\ F_1 = 1. \\ \forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n. \end{cases}$$

Soient $\varphi = \dfrac{1+\sqrt{5}}{2}$ *et* $\varphi' = \dfrac{1-\sqrt{5}}{2}$ *(*φ *est appelé le nombre d'or). On a* φ *et* φ' *sont solution de l'équation* $x^2 - x - 1 = 0$.

Question : Montrer que pour tout $n \geq 1$ *nous avons* $F_n \leq \varphi^{n-1}$.

Réponse :Pour $n = 1$ *on a* $F_1 = 1 \leq 1 = \varphi^0$.

Pour $n = 2$ *on a* $F_2 = F_1 + F_0 = 1 \leq \dfrac{1+\sqrt{5}}{2} = \varphi^1$.

On doit ensuite démontrer que :

$$\forall n \geq 1 : P(n) \wedge P(n+1) \Rightarrow P(n+2)$$

On a par définition

$$\forall n \in \mathbb{N} : F_{n+2} = F_{n+1} + F_n \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^n + \varphi^{n-1} \text{ (Par hypothèses de récurrence)}$$
$$\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}(\varphi + 1) \Rightarrow \forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n-1}\left(\varphi^2\right) \text{ (Car } \varphi^2 - \varphi - 1 = 0\text{)}$$

Donc $\forall n \in \mathbb{N} : F_{n+2} \leq \varphi^{n+1}$.

3.1.3 Preuve par récurrence généralisée

Théorème 3.2 *Soit* $\mathcal{P}(n)$ *une proposition dépendant d'un élément* n *de* $\mathbb{N}$.

On suppose que $\mathcal{P}(0)$ *est vraie.* ***(Initialisation)***

On suppose également que pour tout entier n *que l'implication* $(\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n)) \Rightarrow$

[1] *Leonardo Fibonacci (1175-1250 Pise, Italie) est un mathématicien italien qui a fait ses études à Béjaia.*

$\mathcal{P}(n+1)$ *est vraie.* ***(Hérédité)***

Alors la proposition $\mathcal{P}(n)$ *est vraie pour tout entier* n.

Preuve. Soit la proposition $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n) = Q(n)$.
On va montrer que $Q(n)$ est vraie pour toute valeur de $\mathbb{N}$ si et seulement si $\mathcal{P}(n)$ est vraie pour toute valeur de $\mathbb{N}$.
Ici il s'agit de montrer une équivalence, on doit donc montrer deux implications.

Implication n°1

On va montrer que si $Q(n)$ est vraie pour toute valeur de $\mathbb{N}$ alors $\mathcal{P}(n)$ est vraie pour toute valeur de $\mathbb{N}$.
On a $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n)$ Vrai, par conséquent $\mathcal{P}(0)$ Vrai et $\mathcal{P}(1)$ Vrai ...et $\mathcal{P}(n)$ Vrai donc $\mathcal{P}(n)$ est vrai.

Implication n°2

On va montrer que si $\mathcal{P}(n)$ est vrai pour toute valeur de $\mathbb{N}$, alors $Q(n)$ est vrai pour toute valeur de $\mathbb{N}$.
Comme $P(n)$ est vraie pour toute valeur de $\mathbb{N}$ par conséquent $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n)$ est également vrai et donc $Q(n)$ est vrai pour toute valeur de $\mathbb{N}$. ■

Exemple 3.5 *Démontrer que tout entier n entier supérieur ou égal à 2 peut se décomposer de façon unique en produit de facteurs premiers.*

Démonstration :

Notons P(n) la propriété : tout entier k *de* $\{2; 3; 4.....; n-1; n\}$ *peut se décomposer en produit de facteurs premiers.*

i) On a P(2) est vraie car 2 = 2.

ii) Supposons que $P(k)$ *est vraie pour tout entier naturel* $2 \leq k \leq n$. *Il faut prouver que* $P(n+1)$ *est vraie.*

- Si n + 1 est premier on peut écrire n + 1 = n + 1.

- Si n + 1 n'est pas premier il admet donc un diviseur premier p et on a : n +1= q.p

On a nécessairement $q \leq n$ *et donc selon (ii) q se décompose en produit de facteurs* *premiers.*

Par conséquent, P(n + 1) est vraie.

3.1.4 Preuve par récurrence forte

Théorème 3.3 *Soit $\mathcal{P}$ une proposition dépendant d'un élément n de $\mathbb{N}$.*

Si pour tout n on a : $\forall k < n : \mathcal{P}(k) \Rightarrow \mathcal{P}(n)$

Alors la proposition $\mathcal{P}(n)$ est vraie pour tout entier n.

Preuve. On effectue la preuve par récurrence généralisée sur n.

On a pour $n = 0$.

$\forall k < 0 : \mathcal{P}(k)$ Cette proposition est vraie car k appartient à l'ensemble vide.

On suppose que la proposition $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n)$ est vraie et on démontre que $\mathcal{P}(n+1)$.

Comme $\mathcal{P}(0) \wedge \mathcal{P}(1) \wedge .... \wedge \mathcal{P}(n)$ est vraie alors $\forall k < n+1 : \mathcal{P}(k)$ est vraie.

D'où on obtient $\mathcal{P}(n+1)$ est vraie. ■

3.1.5 Cas particulier de preuve par récurrence (récurrence de Cauchy)

Proposition 3.1 *Soit $P(n)$ un prédicat qui vérifie :*

$$\begin{cases} (i) : P(1) \ \textit{ est vraie.} \\ (ii) : \forall n \in \mathbb{N} : P(n) \Rightarrow P(2n) \\ (iii) : \forall n \in \mathbb{N} : P(n+1) \Rightarrow P(n) \end{cases}$$

Alors $P(n)$ est vraie pour toute valeur de n.

3.1.6 Preuve de l'inégalité de Cauchy Scwhartz par récurrence.

Théorème 3.4 *Moyenne harmonique, géométrique et arithmétique.*
Soient $a_1, a_2, ..., a_n$ des nombres réels positifs, alors :

$$\frac{n}{\frac{1}{a_1} + ... + \frac{1}{a_n}} \leq \sqrt[n]{a_1.a_2...a_n} \leq \frac{a_1 + a_2... + a_n}{n}$$

L'égalité ayant lieu si et seulement si tous les a_i sont égaux.

Preuve. Pour $n = 2$, il faut établir que $a_1 a_2 \leq \left(\frac{a_1+a_2}{2}\right)^2$ c'est à dire $(a_1 - a_2)^2 \geq 0$ ce qui est vrai.

On va montrer $P(n) \Rightarrow P(n-1)$ Posons $A = \sum\limits_{k=1}^{n-1} \frac{a_k}{n-1}$ alors :

$$\left(\prod_{k=1}^{n-1} a_k\right) A \overset{P(n)}{\leq} \left(\sum_{k=1}^{n-1} \frac{a_k + A}{n}\right)^n = \left(\frac{(n-1)A + A}{n}\right)^n = A^n$$

Donc $\prod\limits_{k=1}^{n-1} a_k \leq A^{n-1} = \left(\sum\limits_{k=1}^{n-1} \dfrac{a_k}{n-1}\right)^{n-1}$.

On démontre à présent que $P(n) \Rightarrow P(2n)$

$$\prod_{k=1}^{2n} a_k = \left(\prod_{k=1}^{n} a_k\right)\left(\prod_{k=n+1}^{2n} a_k\right) \overset{P(n)}{\leq} \left(\sum_{k=1}^{n} \frac{a_k}{n}\right)^n \left(\sum_{k=n+1}^{2n} \frac{a_k}{n}\right)^n$$

$$\overset{P(2)}{\leq} \left(\frac{\sum\limits_{k=1}^{2n} \frac{a_k}{n}}{2}\right)^{2n} = \left(\frac{\sum\limits_{k=1}^{2n} a_k}{2n}\right)^{2n}$$

L'inégalité de gauche se déduit de la précédente en considérant $\dfrac{1}{a_1}, ..., \dfrac{1}{a_n}$ ■

3.2 Ordre bien fondé

3.2.1 Ordre et ordre strict

Définition 3.1 *Soit $\mathcal{R}$ une relation binaire sur E.*

- On dit que $\mathcal{R}$ est réflexive quand : $\forall x \in E,\ x\mathcal{R}x.$

- On dit que $\mathcal{R}$ est symétrique quand : $\forall (x,y) \in E^2,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x.$

- On dit que $\mathcal{R}$ est anti-symétrique quand : $\forall (x,y) \in E^2,\ x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y.$

- On dit que $\mathcal{R}$ est transitive quand : $\forall (x,y,z) \in E^3,\ x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z.$

Définition 3.2 *Une relation binaire est une relation d'ordre si elle est réflexive, antisymétrique et transitive.*

Exemple 3.6 *L'ensemble $\mathbb{R}$ muni de la relation d'ordre usuel $(\leq)$.*

Exemple 3.7 *Sur l'ensemble des parties d'un ensemble, la relation $\subset$ est une relation d'ordre.*

Définition 3.3 *Une relation binaire est une relation d'ordre strict si elle est transitive et anti réflexive.*

$$\mathcal{R} \text{ anti réflexive : } \forall x \in E : x \not\mathcal{R} x$$

Exemple 3.8 *L'ensemble $\mathbb{R}$ muni de la relation $<$.*

Proposition 3.2 *Une relation d'ordre strict est antisymétrique.*

Preuve. $\mathcal{R}$ est par définition transitive et anti réflexive.
Une relation est antisymétrique si elle vérifie

$$\forall (x,y) \in E^2,\ \ (x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$$

On va montrer que dans une relation d'ordre strict la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est toujours fausse.

On raisonne par l'absurde.

On suppose qu'il existe $(x, y) \in E^2$ tel que la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est vraie. Alors par transitivité on obtient $x\mathcal{R}x$ vraie ce qui contredit le fait que $\mathcal{R}$ est anti réflexive.

Par conséquent, la proposition $x\mathcal{R}y \wedge y\mathcal{R}x$ est toujours fausse et donc l'implication logique $(x\mathcal{R}y \wedge y\mathcal{R}x) \Rightarrow x = y$ est toujours vraie. $\blacksquare$

Définition 3.4 *Soit $(E, \mathcal{R})$ un ensembe ordonné. Deux éléments x et y sont dits comparables si on a $x\mathcal{R}y$ ou $y\mathcal{R}x$. Dans le cas contraire on dit que x et y sont incomparables.*

Exemple 3.9 *Soit l'ensemble $\mathcal{P}(\{a, b, c\})$ -l'ensemble des parties de $\{a, b, c\} -$ muni de la relation d'ordre $\subset$.*

Les éléments $\{a, b\}, \{b, c\}$ sont incomparables.

Définition 3.5 *Un ordre $\mathcal{R}$ sur E est dit total si deux éléments sont toujours comparables*

$$\forall (x, y) \in E, \ x\mathcal{R}y \text{ ou } y\mathcal{R}x.$$

Un ordre qui n'est pas total est dit partiel.

Définition 3.6 *Un ordre strict est dit strict total si deux éléments distincts sont toujours comparables*

$$\forall (x, y) \in E, x \neq y \Rightarrow x\mathcal{R}y \text{ ou } y\mathcal{R}x.$$

Remarque 3.2 *Dans ce qui suit nous noterons une relation d'ordre par $\preceq$ une relation d'ordre stricte par $\prec$.*

3.2.2 Minorants, majorants, minimaux et maximaux

Définition 3.7 *Soit $(E, \preceq)$ un ensemble ordonné et F une partie non vide de E.*

On dit que $x \in E$ est un ***minorant*** *de F si on a :*

$$\forall y \in F, x \preceq y.$$

Si le minorant de F est un élément de F on dit que c'est le ***plus petit élément*** *ou* ***le minimum*** *de F.*
On dit que $x \in E$ est ***un majorant*** *de F si on a :*

$$\forall y \in F, y \preceq x.$$

Si le majorant de F est un élément de F on dit que c'est le ***plus grand élément*** *ou* ***le maximum*** *de F.*

Définition 3.8 *Soit $(E, \preceq)$ un ensemble ordonné et F une partie non vide de E.*
- Un élément x est un élément ***minimal*** *de F quand aucun élément de F n'est strictement plus petit que x :*

$$\forall y \in F, y \preceq x \Rightarrow x = y.$$

- Un élément x est un élément ***maximal*** *dans de F quand aucun élément de F n'est strictement plus grand que x :*

$$\forall y \in F, x \preceq y \Rightarrow x = y.$$

Remarque 3.3 *Si la relation est d'ordre total alors les notions d'élément minimal et et de minimum coincident. (Même remarque pour la notion d'élément maximal et de maximum).*

Exemple 3.10 0 *est un élément minimal de $(\mathbb{N}, \leq)$ c'est également son minimum.*

Exemple 3.11 *Soit l'ensemble $\mathcal{P}(\{a, b, c\}) \setminus \{\varnothing\}$ muni de la relation d'ordre partiel $\subset$. Les éléments $\{a\}, \{b\}, \{c\}$ sont des éléments minimaux mais il n y a pas de minimum.*

3.2.3 Produit d'ordre (ordre lexicographique)

Soit $(E, \preceq_E)$ et $(F, \preceq_F)$ deux ensembles ordonnés. On considère l'ensemble produit $E \times F$ et on définit l'ordre lexicographique $\preceq_{lex}$par

$$\forall (x, y) \in E \times F, \forall (x', y') \in E \times F, (x, y) \preceq_{lex} (x', y') \Leftrightarrow \begin{cases} x \preceq_E x' \\ ou \\ x = x' \text{ et } y \preceq_F y'. \end{cases}$$

Si $\preceq_E$ et $\preceq_F$ sont des relations d'ordres totals alors l'ordre lexicographique l'est également.

Exemple 3.12 *L'ordre lexicographique sur l'ensemble $\mathbb{N}^2$ est défini par*

$$\forall (x, y) \in \mathbb{N}^2, \forall (x', y') \in \mathbb{N}^2, (x, y) \preceq_{lex} (x', y') \Leftrightarrow \begin{cases} x \leq x' \\ ou \\ x = x' \text{ et } y \leq y'. \end{cases}$$

3.2.4 Ordre bien fondé

Définition 3.9 *Soit $(E, \preceq)$ un ensemble ordonné par une relation d'ordre total.*
On dit que $\preceq$ est bien fondé quand il n'existe pas de suite infinie strictement décroissante d'éléments de E.

Remarque 3.4 *On dit également que l'ensemble E est bien ordonné.*

Exemple 3.13 *L'ordre usuel sur $\mathbb{N}$ est bien fondé mais pas sur $\mathbb{Z}$ ni $\mathbb{R}^+$.*

Exemple 3.14 *L'ordre lexicographique sur $\mathbb{N}^2$ est bien fondé.*

Théorème 3.5 *Soit $(E, \preceq)$ un ensemble ordonné. L'ordre $\preceq$ est bien fondé si et seulement si toute partie non vide $F \subset E$ admet un minimum.*

Remarque 3.5 *Soit $(E, \preceq)$ on peut associer à la relation d'ordre $\preceq$ une relation d'ordre strict par la définition suivante :*

$$x \prec y \text{ si et seulement si } x \preceq y \text{ et } x \neq y$$

Remarque 3.6 *Soit* $(E, \prec)$ *on peut associer à la relation d'ordre* $\prec$ *une relation d'ordre par la définition suivante :*

$$x \preceq y \text{ si et seulement si } x \prec y \text{ ou } x = y$$

3.3 Preuve par induction

La preuve par induction permet de généraliser la preuve par récurrence à tout ensemble bien ordonné. Le principe de la preuve est le suivant :

Principe Soit $(E, \preceq)$ un ensemble bien ordonné. Notons par e l'élément minimal de E.

Soit $\mathcal{P}(x)$ une proposition dépendant des éléments $x \in E$.

i) On suppose que $\mathcal{P}(e)$ est vraie. **(Initialisation)**

ii) On suppose également que $\forall y \prec x : \mathcal{P}(y) \Rightarrow \mathcal{P}(x)$ est vraie. **(Hérédité)**

Alors la proposition $\mathcal{P}(x)$ est vraie pour tout $x \in E$.

Théorème 3.6 *Soit* $(E, \preceq)$ *un ensemble ordonné. L'ordre* $\preceq$ *est bien fondé si et seulement si le principe d'induction est correct.*

Preuve. Nous allons seulement démontrer que si l'ordre est bien fondé alors le principe d'induction est correct.
On raisonne par l'absurde, on suppose que $\mathcal{P}(x)$ vérifie les propriétés **(i)** et **(ii)** et qu'il existe des éléments de E qui ne vérifie pas $\mathcal{P}(x)$.

Soit $A = \{x \in E, \mathcal{P}(x) \text{ est fausse}\}$
A est par conséquent un sous ensemble non vide de E.
Comme l'ordre est bien fondé l'ensemble A possède un élément minimal x_0.
Par conséquent pour tout élément $y \prec x_0$ on a $\mathcal{P}(y)$ vraie par définition.
En appliquant le principe d'hérédité on obtient $\mathcal{P}(x_0)$ vraie ce qui constitue une contradiction. ■

Exemple 3.15 *On considère la suite $S_{m,n}$ définie sur $\mathbb{N}^2$ par $S_{0,0} = 0$ et la relation suivante :*

$$S_{m,n} = \begin{cases} S_{m-1,n} + 1 \text{ si } n = 0 \\ S_{m,n-1} + 1 \text{ sinon.} \end{cases}$$

On va montrer que pour toute paire $(m,n) \in \mathbb{N}^2, S_{m,n} = m + n$.

Initialisation : *On commence par prouver la propriété pour l'élément $(0,0)$*

On a $S_{0,0} = 0 = 0 + 0$ Vérifié.

Hérédité

On montre que si la propriétée est vraie pour toute paire $(m', n') \prec (m,n)$ alors elle est vraie pour (m,n).

On suppose donc qu'on a

$$\forall (m', n') \prec (m,n) : S_{m',n'} = m' + n'$$

On distingue deux cas :

Cas 1 : Si $n = 0$

Dans ce cas nous avons par définition $S_{m,0} = S_{m-1,0} + 1 \overset{Hypothèse}{=} m - 1 + 1 = m + 0$.

Cas 2 : Si $n \neq 0$

Dans ce cas nous avons par définition $S_{m,n} = S_{m,n-1} + 1$. On a également $(m, n-1) \prec (m,n)$ donc par hypothèse on a $S_{m,n-1} = m + n - 1$. D'où

$$S_{m,n} = S_{m,n-1} + 1 = m + n - 1 + 1 = m + n.$$

3.4 Théorème du bon ordre général de Zermelo

3.4.1 Préordre

Définition 3.10 *Un ensemble* préordonné *est un ensemble E muni d'une relation binaire $\mathcal{R}$ qui est réflexive et transitive. On dit que la relation $\mathcal{R}$ est une relation de* préordre..

- *Un ensemble* préordonné *est totalement prordonné si on a $x\mathcal{R}y$ ou $y\mathcal{R}x$ pour tout x et y de E.*

Exemple 3.16 *L'ensemble des entiers relatifs $\mathbb{Z}$ muni de la relation de divisibilité entre entiers :*

$$x\mathcal{R}y \Leftrightarrow x \text{ divise } y.$$

La relation $\mathcal{R}$ est une relation de préordre mais n'est pas une relation d'ordre. La preuve est laissée en exercice.

Exemple 3.17 *Entre fonctions réelles d'une variable réelle, la domination est un préordre.*

Nous utiliserons la notation $\preceq$ pour la relation de préordre.

Définition 3.11 *Deux éléments x et y d'un ensemble préodonné E qui sont tels que $x \preceq y$ et $y \preceq x$ sont dits équivalents.*

La notion d'équivalence définie précédement est en fait une relation d'équivalence sur E. Ainsi à chaque relation de préordre est associée une relation d'équivalence.

Définition 3.12 *Soit A une partie d'un ensemble préordonné E.*
La cloture de A noté A^+ est l'ensemble défini par

$$A^+ = \{x \in E : \exists y \in A, x \preceq y \wedge y \preceq x\}$$

l'ensemble A est dit clos si $A = A^+$.

Définition 3.13 *Soient x et y deux éléments ensemble préordonné E. On dit que x est strictement plus petit que y si*

$$x \preceq y \text{ et si } x \text{ n'est pas équivalent à } y.$$

Définition 3.14 *Soit $(E, \preceq)$ un ensemble préordonné et A une partie non vide de E. On dit que $m \in E$ est un* ***minorant*** *de A si tout élément de A est plus grand que x.*

$$\forall y \in F, m \preceq y$$

Si le minorant de A est un élément de A on dit que c'est le ***plus petit élément*** *ou* ***minimum*** *de F.*
On dit que $M \in E$ est ***un majorant*** *de A si tout élément de A est plus petit que M.*

$$\forall y \in F, y \preceq M$$

Si le majorant de A est un élément de A on dit que c'est le ***plus grand élément*** *ou* ***maximum*** *de F.*

Remarque 3.7 *Si le maximum (resp. le minium) quand il existe est unique dans le cas d'une relation d'ordre ce n'est pas le cas pour une relation de préordre. En effet il peut y avoir plusieurs minimums équivalents.*

Exemple 3.18 *Soit la relation de prépordre de divisibilité entre entiers relatifs et l'ensemble $A = \{-2, 2, 4, 8, -8\}$.*
Nous avons deux minimums 2 et -2 et deux maximums 8 et -8.

Définition 3.15 *Une « borne supérieure » (resp. « borne inférieure ») (si elle existe) d'une partie A de E est un plus petit élément de l'ensemble des majorants de A (resp. un plus grand élément de l'ensemble des minorants de A).*

Remarque 3.8 *Plusieurs bornes supérieurs (resp. inférieures) équivalentes peuvent exister.*

Lemme 3.1 *Soit E un ensemble préordonné fini. Alors il existe une application injective croissante $f : E \to \mathbb{N}$.*

Preuve. On procède par récurrence sur le nombre d'éléments de E.
Pour $n = 1$ la proposition est vérifiée.
Supposons que la proposition est vérifiée pour $n - 1$ et on démontre pour n.
Comme E est fini et non vide il existe nécéssairement un élément minimal a de E. Posons $F = E - \{a\}$.
Par hypothèse de récurrence, il existe une application injective croissante $\varphi : E \to \mathbb{N}$.
On définit $f : E \to \mathbb{N}$ en posant $f(a) = 0$ et $f(y) = \varphi(y) + 1$ pour tout $y \in Y$. Cette application est injective et croissante. ■

Définition 3.16 *Un ensemble préordonné E est bien préordonné si toute partie non vide de E admet un plus petit élément.*

Noter qu'un ensemble bien préordonné est totalement préordonné, et que tout sous-ensemble d'un ensemble bien préordonné est bien préordonné. Un exemple fondamental d'ensemble bien préordonné (en fait bien ordonné) est l'ensemble $\mathbb{N}$ des entiers naturels (ordonné de la manière usuelle).

Définition 3.17 *Un ensemble préordonné est dit « inductif » si toute partie bien ordonnée de E admet un majorant.*

Remarque 3.9 *Un ensemble préordonné inductif ne peut pas être vide, puisque la partie vide de cet ensemble, qui est bien ordonnée, doit avoir un majorant.*

Définition 3.18 *Un* crible *sur un ensemble préordonné E est une partie A de E telle que $x \in A$ et $y \preceq x$ entraînent $y \in A$ (pour tous x et y de E). Le fait que A soit un crible sur E sera noté $A \lhd E$.*

Il est immédiat que l'intersection d'une famille quelconque de cribles sur E est encore un crible sur E. De même, l'union d'une famille quelconque de cribles sur E est un crible sur E. Par ailleurs, il est clair que tout crible est clos.

Lemme 3.2 *Soient A, B deux cribles sur un ensemble E totalement préordonné, alors ou bien $A \lhd B$ ou $B \lhd A$.*

Preuve. En effet, supposons par exemple qu'il existe $x \in A$ tel que $x \notin B$. Soit $y \in B$. On ne peut pas avoir $x \preceq y$ sinon on aurait $x \in B$. On a donc $y \leq x$ donc $y \in A$ et $B \subset A$. On a donc montré $A \subset B$ ou $B \subset A$ mais comme il s'agit de cribles, alors ou bien $A \lhd B$ ou $B \lhd A$. ■

Définition 3.19 *Soit A une partie d'un ensemble préordonné E et soit $a \in A$. On note $a_A^{\prec}$ le plus petit crible sur A contenant a.*

Il est clair que $a_A^{<}$ n'est autre que l'ensemble $\{x \in A : x \prec a\}$ des éléments de A strictement plus petits que a.

3.4.2 Lemme de Zorn et théorème du bon ordre général

Lemme 3.3 *Soit E un ensemble préordonné, A et B deux parties de E. Si $A \lhd B \lhd E$, alors pour tout $a \in A$ on a $a_A^{\prec} = a_B^{\prec}$.*

Théorème 3.7 (lemme de Zorn) *Tout ensemble préordonné inductif a un élément maximal.*

Théorème 3.8 (Zermelo) *Sur tout ensemble il existe un bon ordre.*

Preuve. Soit E un ensemble. Notons E l'ensemble des couples (A, R) où A est une partie de E et R une relation de bon ordre sur A. Notons $(A, R) \preceq (B, R')$ le fait que $A \subset B$ et R' prolonge R . E est alors un ensemble ordonné inductif (pour toute partie bien ordonnée de E, prendre la réunion de ses éléments). Il résulte donc du lemme de Zorn que E a un élément maximal (A, R). Un tel élément doit nécessairement vérifier $A = E$ (sinon, ajouter un élément à A et décider qu'il est plus grand que tous ceux de A). ■

Remarque 3.10 *Ce bon ordre est difficile à expliciter dans la plupart des ensembles. Par exemple l'ensemble des nombres rationnels peut être bien ordonné par l'ordre lexicographique. Pour les réels aucune relation de bon ordre n'a été établie.*

3.5 Exercices

Exercice 3.1 *Montrer en utilisant le principe du bon ordre que*

$$\forall n \in \mathbb{N} : \sum_{i=}^{n} i = \frac{n(n+1)}{2}$$

Solution :

On raisonne par l'absurde on suppose que la proposition n'est pas vérifiée pour toutes les valeurs de $n \in \mathbb{N}^*$.

Notons A l'ensemble des valeurs de n pour lesquels l'identitée n'est pas vérifiée

$$A = \left\{ n \in \mathbb{N}^* : \sum_{i=1}^{n} i \neq \frac{n(n+1)}{2} \right\}$$

Comme $A \subset \mathbb{N}^*$ alors il possède un minimum noté n_0.
On sait que $n_0 \neq 1$ car l'identité est vérifiée pour 1 en effet on a

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$$

Ainsi comme $n_0 \geq 2$ on obtient que $n_0 - 1 \geq 1$ et par conséquent l'identitée est vérifiée pour $n_0 - 1$.

On a alors

$$\begin{aligned} \sum_{i=1}^{n_0-1} i &= \frac{(n_0-1)(n_0-1+1)}{2} = \frac{(n_0-1)(n_0)}{2} \Rightarrow \left(\sum_{i=1}^{n_0-1} i \right) + n_0 = \frac{(n_0-1)(n_0)}{2} + n_0 \\ &\Rightarrow \sum_{i=1}^{n_0} i = \frac{(n_0-1)(n_0)}{2} + n_0 = \frac{n_0(n_0+1)}{2} \end{aligned}$$

Ce qui constitue une contradiction avec le fait que n_0 ne vérifie par l'identité.

Exercice 3.2 *On considère la suite définie par :*

$$\begin{cases} u_0 = 2 \\ u_{n+1} = 1 + \dfrac{1}{1+u_n} \end{cases}$$

En utilisant le principe du bon ordre montrer que pour tout entier naturel on a : $1 \leq u_n \leq 2$.

Solution :

On raisonne par l'absurde on suppose que la proposition n'est pas vérifiée pour toutes les valeurs de $n \in \mathbb{N}$.

Notons A l'ensemble des valeurs de n pour lesquels l'identitée n'est pas vérifiée

$$A = \{n \in \mathbb{N} : u_n > 2 \text{ ou } u_n < 1\}$$

Comme $A \subset \mathbb{N}$ alors il possède un minimum noté n_0.
On sait que $n_0 \neq 0$ car l'identité est vérifiée pour 0
Ainsi comme $n_0 \geq 1$ on obtient que $n_0 - 1 \geq 0$ et par conséquent l'identitée est vérifiée pour $n_0 - 1$.

On a alors

$$\begin{aligned} 1 &\leq u_{n_0-1} \leq 2 \Rightarrow 2 \leq 1 + u_{n_0-1} \leq 3 \Rightarrow \frac{1}{3} \leq \frac{1}{1+u_{n_0-1}} \leq \frac{1}{2} \\ &\Rightarrow 1 + \frac{1}{3} \leq 1 + \frac{1}{1+u_{n_0-1}} \leq 1 + \frac{1}{2} \Rightarrow \frac{4}{3} \leq u_{n_0} \leq \frac{3}{2} \Rightarrow 1 \leq u_{n_0} \leq 2 \end{aligned}$$

Ce qui constitue une contradiction avec le fait que n_0 ne vérifie par l'identité.

Exercice 3.3 *Supposons que R est un ordre partiel sur un ensemble E. Montrer que chaque sous ensemble fini $E \subset A$ possède un élément minimal.*

Solution :

On suppose que $(E, \prec)$ est une relation d'ordre partiel :

On va effectuer une preuve par récurrence sur le cardinal de l'ensemble.

$$\forall A \subset E : Card\,(A) = n \Rightarrow A \text{ possède au moins un élément minimal}$$

Pour $n = 1$ on $A = \{x\}$ est un élément minimal.

Supposons la proposition vraie pour n et on démontrer pour $(n+1)$

Soit A un ensemble de $(n+1)$ éléménts qu'on notera $A = \{x_1, x_2, ...x_n, x_{n+1}\}$.

On peut écrire A comme

$$A = \{x_1, x_2, ...x_n\} \cup \{x_{n+1}\}$$

L'ensemble $\{x_1, x_2, ...x_n\}$ ayant n éléments possède par conséquent un élément minimal qu'on notera m.

On ensuite 3 cas

Cas n° $= 1$: Les éléments m et x sont incomparables alors m est toujours un élément minimal de l'ensemble A.

Cas n° $= 2$: Les éléments m et x sont comparables et on a $m \prec x_{n+1}$ dans ce cas m est un élément minimal de l'ensemble A.

Cas n° $= 3$: Les éléments m et x sont comparables et on a $x_{n+1} \prec m$ dans ce cas x_{n+1} un élément minimal de l'ensemble A.

Exercice 3.4 *On considère la suite S définie sur $\mathbb{N}^2$ par $S_{1,1} = 5$ et la relation suivante :*

$$S_{m,n} = \begin{cases} S_{m-1,n} + 2 \; si \; n = 1 \\ S_{m,n-1} + 2 \; Sinon \end{cases}$$

Montrer que pour toute paire $(m, n) \in \mathbb{N}^2, S_{m,n} = 2\,(m+n) + 1$.

Solution :

On commence par montrer que la proposition est vraie pour le minimum c'est à dire $(1,1)$.

On a en effet $S_{1,1} = 5 = 2(1+1)+1$.

On suppose à présent que la proposition est vraie pour toute valeur $(m', n') \prec (m,n)$ et on montre qu'elle est vraie pour (m,n).

D'après la définition de $S_{m,n}$ on a deux cas :

Cas n$^\circ = 1$ **: si** $n = 1$.

$$S_{m,n} \overset{définition}{=} S_{m-1,n} + 2 \overset{Hypothèse}{=} 2(m-1+n)+1+2 = 2m+2n+1 \text{ (Vérifié)}$$

Cas n$^\circ = 2$ **: si** $n \neq 1$.

$$S_{m,n} \overset{définition}{=} S_{m,n-1} + 2 \overset{Hypothèse}{=} 2(m+n-1)+1+2 = 2m+2n+1 \text{ (Vérifié)}$$

Exercice 3.5 *1. Soit* $(E, \prec)$ *un ensemble muni d'une relation d'ordre strict.*
Montrer qu'on peut définir sur E *une relation d'ordre.*
2. Soit $(E, \preceq)$ *un ensemble muni d'une relation d'ordre.*
Montrer qu'on peut définir sur E *une relation d'ordre strict.*

Exercice 3.6 *Soit* $(E, \prec)$ *un ensemble muni d'une relation d'ordre strict. Montrer que la relation d'ordre lexicographique induite par* $\prec$ *sur l'ensemble* E^n *est une relation d'ordre strict.*

Exercice 3.7 *En utilisant le principe du bon ordre montrer que*

$$\forall n \in \mathbb{N} : 3/\left(n^3 - n\right). \quad \textit{(3 est un diviseur de } \left(n^3 - n\right)\textit{)}.$$

Exercice 3.8 *Est ce qu'il existe une relation d'ordre pour laquelle les ensembles suivants sont bien ordonnés ?*

$$(1)\ \mathbb{N}^3. \qquad (2)\ \mathbb{Q}.$$

Exercice 3.9 *Soient les prédicats ci dessous prenant leurs valeurs dans* $\mathbb{Z}$ *et qui vérifient :*

$$\begin{cases} P1(0) \ \ Vrai \\ \forall n \in \mathbb{Z} : P1(n) \Rightarrow P1(-n) \end{cases}, \begin{cases} P2(0) \ \ Vrai \\ \forall n \in \mathbb{Z} : P2(n) \Rightarrow P2(n-1) \end{cases}$$

$$\begin{cases} P3(0) \ \ Vrai \\ \forall n \in \mathbb{Z} : P3(n) \Rightarrow P3(n+2) \\ \forall n \in \mathbb{Z} : P3(n+1) \Rightarrow P3(n) \end{cases}, \begin{cases} P4(0) \ \ Vrai \\ \forall n \in \mathbb{Z} : P4(n) \Rightarrow P4(n+1) \\ \forall n \in \mathbb{Z} : P4(n+2) \Rightarrow P4(n) \end{cases}$$

Dire dans chaque cas si le prédicat est vrai pour toutes les valeurs de $\mathbb{Z}$ *? Démontrer votre affirmation.*

Exercice 3.10 *Dans chaque cas donner une relation d'ordre pour laquelle les ensembles suivants sont bien ordonnés.*

$$\left\{\frac{n}{n+1}, n \in \mathbb{N}\right\}, \ \mathbb{N} \times \mathbb{Z}, \ \left\{\frac{1}{n}, n \in \mathbb{Z}^*\right\}, \ \{2n, n \in \mathbb{N}\} \cup \{-2n-1, n \in \mathbb{N}\}$$

Exercice 3.11 .

Soit A *un ensemble fini muni d'une relation d'ordre et* f *une fonction monotone de* A *dans* A.

1. Montrer que la fonction f *admet au moins un point fixe. (C'est à dire un point* $r \in A$ *qui vérifie* $f(r) = r$).

2. Montrer que s'il existe plusieurs points fixes alors il existe un plus petit point fixe qui s'écrit sous la forme $f^k(x)$ *où* $x \in A$ *et* $k \leq Card(A)$.

Exercice 3.12 *Montrer qu'un préordre est un ordre si et seulement si la relation d'équivalence associée est l'équivalence.*

Annexe : Alphabet grec

A	α		alpha
B	β		beta
Γ	γ		gamma
Δ	δ		delta
E	ϵ	ε	epsilon
Z	ζ		zeta
H	η		eta
Θ	θ	ϑ	theta
I	ι		iota
K	κ		kappa
Λ	λ		lambda
M	μ		mu
N	ν		nu
O	o		omicron
Ξ	ξ		xi
Π	π	ϖ	pi
P	ρ	ϱ	rho
Σ	σ	ς	sigma
T	τ		tau
Υ	υ		upsilon
Φ	ϕ	φ	phi
X	χ		chi
Ψ	ψ		psi
Ω	ω		omega

Bibliographie

[1] Herbet B Enderton, Introduction to Logic, Harcourt academic press, New York, 2013.

[2] Gary Chartrand et al, Mathematical Proofs A Transition to Advanced Mathematics, Pearson, New York, 2013.

[3] Christopher C. Leary, A Friendly Introduction to Mathematical Logic, Prentice Hall, New Jersey, 2000.

[4] Paul Halmos, Introduction à la théorie des ensembles, Gauthier-Villars, Paris 1970.

[5] Daniel J.Velleman, How to prove it, second edition, Cambridge university press, Cambridge 2006.