Chapitre 2

Calcul des Prédicats

2.1 Introduction

Une proposition est un énoncé, un jugement pris en sa totalité.

2.1.1 Exemples

— *Le chat est noir*
— *Il fait beau*
— *Il ne fait pas beau*
— *Il fait beau ou il ne fait pas beau*

Les deux premières propositions sont atomiques c'est-à-dire indécomposables en propositions plus petites contrairement aux deux dernières qui se décomposent comme suit :

— **Non** *il fait beau*
— *il fait beau* **Ou Non** *il fait beau*

Ce découpage en propositions est insuffisant pour rendre compte de tous les types de raisonnement. L'énoncé « le chat est noir » peut faire l'objet d'une analyse plus fine : il relie une propriété **etre noir** et un individu qui possède cette propriété **le chat**.

La propriété **etre noir** s'appelle un prédicat à une place et **le chat** une constante d'individu et ces nouveaux éléments formeront le socle (les objets primitifs) sur lequel on construit les formules du calcul des prédicats.

Les formules atomiques ne sont plus ici la donnée d'un ensemble de symboles de propositions mais seront de la forme **P(t)** où **P(-)** est une symbole de prédicat et **t** un terme (un individu).

L'intérêt de cette decomposition des formule atomique est fondamentale si on veut exprimer des « relations » entres des propriétés d'un même individu.

Par exemple pour exprimer que le « chat est noir », que « tout ce qui est noir, est foncé » et donc que « le chat est foncé » on pourra écrire :

$$(estNoir(chat) \wedge \forall x, estNoir(x) \Rightarrow estFonce(x)) \Rightarrow estFonce(chat)$$

Pour preciser encore un peu les chose avant leur définition formelle voyons un autre exemple issu des mathématiques (très) élémentaires

2.1.2 Un exemple complet

Si on veut énoncer que :

si « x est paire » alors « x + 1 est impaire »

On peut etre tenté d'écrire en logique des propositions,

$$\mathbf{x\_est\_paire} \Rightarrow \mathbf{x\_plus\_un\_est\_impaire}$$

, ou *x_est_paire* et *x_plus_un_est_impaire* sont des propositions atomiques (indécomposables) que l'on aurait aussi bien pu appeller A et B. Mais, cette formalisation a un inconvénient majeur (encore plus évident si on écrit $A \Rightarrow B$), elle masque le lien entre les 2 x de l'énoncé initial.

Pour conserver ce lien entre les 2 x de l'énoncé, on va donc changer de formalisme et passer au calculs des prédicats. On écrit alors :

$$\mathbf{Paire}(\mathbf{x}) \Rightarrow \mathbf{Impaire}(\mathbf{Plus}(\mathbf{x}, \mathbf{1}))$$

Cette nouvelle formulation comportes différents éléments :

— Des variables d'individu, ici x
Elles servent a representé les objets dont on va « parler ».

— Des constantes d'individu, ici 1
Elles servent representé des objects particulier.

— Des **symboles de Prédicat** : ici $Paire$, $Impaire$
Ils vont servir a exprimer des propriétés des individu. C'est propriétés dite atomiques seront les brique de base du nouveau formalisme ; comme les propositions atomique de la logique des propositions.

— Des **symboles de Fonction**, ici $plus$
Ils vont permettre de former de nouveaux individus à partir d'individu(s) existant(s), ici a partir des individus x et 1 on va former l'individu $plus(x, 1)$

Enfin comme on veut pouvoir exprimer que cet énoncé est vrai « pour tout x » on va introduire des nouveaux elements, **les quantificateurs** (ici $\forall$).

On peut alors enfin écrire : $\forall x, Paire(x) \Rightarrow Impaire(plus(x, 1))$

2.2 Définir le langage

2.2.1 L(es)'alphabet(s)

Le(s) langage(s) du calcul des prédicats est (sont) formé(s) des symboles suivants :

- un ensemble de symboles de constante : $a, b, c, O, 1, e, \ldots$
- un ensemble de symboles de prédicats d'arité (nombre d'argument) fixée : $A, B, P, Q, R, \leq, Paire, Premiere, Frere$ [1], $\ldots$
- un ensemble de variables d'individus : $x, y, z, \ldots$
- un ensemble de symboles de fonctions d'arité fixée : $f, g, h, s, +, frere$ [2], $\ldots$

2.2.2 les termes

Les termes sont formés inductivement à partir des règles suivantes :

1. Les constantes et les variables sont des termes.
2. Si f est un symbole de fonction d'arité n et si $t_1 \ldots t_n$ sont des termes, alors $f(t_1, \ldots, t_n)$ est un terme.

2.2.3 les formules atomiques

Les formules atomiques sont formées à partir de la règle suivante :

1. Si P est un symbole de prédicat d'arité n et si $t_1 \ldots t_n$ sont des termes, alors $P(t_1, \ldots, t_n)$ est une formule atomique.

2.2.4 les formules

En passant des propositions aux prédicats, nous avons augmenté le pouvoir d'expression de notre langage. Nous pouvons comme dans le calcul des propositions combiner les formules au moyen des connecteurs pour former des formules plus complexes. Mais nous allons aussi ajouter deux nouveaux

1. D'arité 2, $Frere(x, y)$ exprimera par exemple que l'individu x est le frère de l'individu y
2. D'arité 1, $frere(x)$ designera l'individu qui est le frère de l'individu x

constructeurs de formules qui permettent de dire quelque chose sur les termes dont parlent les formules. Ce sont les quantificateurs. Le quantificateur universel ($\forall$) permettra d'exprimer le fait que tout les individus possèdent une propriété et le quantificateur existenciel ($\exists$) permettra d'exprimer le fait qu'il existe un individu qui possèdent une propriété.

Les formules sont formées inductivement à partir des règles suivantes :

— Les formules atomiques sont des formules
— Si ϕ et ψ sont des formules alors $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, (ϕ) et $\neg\phi$ sont des formules
— Si ϕ est une formule et x une variable alors $\forall x\phi$ et $\exists x\phi$ sont des formules.

2.3 Sémantique : validité, satisfaisabilité (réalisabilité)

Comme pour le calcul des propositions,il s'agit ici de définir la notion de vérité, en nous appuyant sur la notion d'interprétation. Mais, les formules faisant intervenir des individus, les *termes*, cela sera plus complexe.

Prenons un premier exemple :

$$\exists x \forall y P(x, y)$$

Cette formule est elle valide (vraie dans tous les mondes possibles), réalisable (vraie dans au moins un monde) ou jamais vérifiée ?

— Si on se donne comme domaine de référence pour les individus l'ensemble $\mathbb{N}$ des entiers Naturels , et si P signifie dans $\mathbb{N}$, $\leq$,alors la formule signifie :

il existe un entier plus petit ou égal a tous les autres entiers

, et cette formule est « vraie », car 0 est le plus petit élément sur cet ensemble.
— Si on se donne comme domaine de référence pour les individus les entiers naturels, et si P signifie dans $\mathbb{N}$, $\geq$, alors cette formule est fausse car il n'y a pas de plus grand élément sur cet ensemble
— Si on se donne comme domaine de référence $\{a, b, c\}$ pour les individus et si P est la relation définie par les couples $\{(a, b), (b, c)(c, c)\}$, alors cette formule est aussi vraie.

Cette formule est donc satisfiable (on dira aussi, réalisable) mais pas universellement valide.

On voit au travers de cet exemple que pour **interpréter** une formule du calcul des prédicats, il faut se donner à la fois **un domaine pour interpréter les termes** et **une interprétation dans ce domaine pour**

chacuns des symboles de prédicats. Une fois ceci effectué, on peut interpréter la formule. Une formule de la forme $\forall x P(x)$ sera vraie dans une interprétation si tous les elements du domaine sont dans l'interpretation de P. Une formule de la forme $\exists x P(x)$ sera vraie dans une interprétation si au moins un element du domaine est dans l'interpretation de P.

Il faut faire attention à l'alternance des quantificateurs dans une formule : $\exists x \forall y P(x, y)$ n'a pas le même sens que $\forall x \exists y P(x, y)$. La première sera vraie si un même élément est en relation P avec tous les autres. La seconde sera vraie si pour chaque élément du domaine, il existe un élément avec qui il est dans la relation P. Ce dernier peut être différent à chaque fois. Par exemple, elle sera vraie dans la seconde interprétation de notre premier exemple : l'interprétation où on se donne comme domaine de référence pour les individus les entiers Naturels, et où P signifie $\geq$. En effet, pour chaque entier naturel, on peut trouver un autre entier naturel qui lui soit supérieur.

2.3.1 Definition de la validité, de la réalisabilité

Comme pour le calcul des propositions, nous allons définir la notion de vérité, en nous appuyant sur la notion d'interprétation. Mais, les formules faisant intervenir des individus, les *termes*, cela sera plus complexe. Nous définirons d'abord la notion de *réalisation* (on parle aussi de structure), qui permet d'interpréter les termes et les prédicats, puis celle d'*interprétation* permettant de donner une valeur aux variables, et finalement celles de *satisfaction* et de *validité*.

Définition 1 *Soit $\mathcal{L}$ un langage du calcul des prédicats. Une* réalisation *de $\mathcal{L}$ est la donnée de :*

- *Un ensemble D non vide appelé domaine.*
- *Un élément de D pour chaque constante de L*
- *Une application de $D^n \to D$ pour chaque symbole de fonction de L*
- *Un ensemble de n-uplets pour chaque symbole de prédicat d'arité n.*

Définition 2 *Soit $\mathcal{L}$ un langage du calcul des prédicats et M une réalisation de $\mathcal{L}$. Une* interprétation *pour M et L est une fonction de l'ensemble des variables de L vers le domaine de M.*

Nous noterons parfois $\bar{c}$ l'element associé à l'objet c de L par l'interprétation.

Définition 3 *On définit par récurrence sur la formation des formules la relation de* satisfaction *d'une formule* par une interprétation *et une réalisation (notée $M \models_I F$)*

- *Si $F = P(t_1, \ldots t_n)$ alors $M \models_I F$ ssi $(t_1, \ldots t_n) \in \bar{P}$*

— *Si* $F = \phi \vee \psi$ *alors* $M \models_I F$ *ssi* $M \models_I \phi$ *ou* $M \models_I \psi$
— *Si* $F = \phi \wedge \psi$ *alors* $M \models_I F$ *ssi* $M \models_I \phi$ *et* $M \models_I \psi$
— *Si* $F = \phi \rightarrow \psi$ *alors* $M \models_I F$ *ssi* $M \not\models_I \phi$ *ou* $M \models_I \psi$
— *Si* $F = \neg\phi$ *alors* $M \models_I F$ *ssi* $M \not\models_I \phi$
— *Si* $F = \forall x P$ *alors* $M \models_I F$ *ssi pour tout* $c \in D$, $M \models_I P[x/c]$
— *Si* $F = \exists x P$ *alors* $M \models_I F$ *ssi il existe* $c \in D$ *tel que* $M \models_I P[x/c]$

remarque : L'interprétation I ne sert que pour les variables libres des formules, c'est à dire les variables qui ne sont pas sous la portée d'un quantificateur.

Définissons précisemment les notions de variables libres et liées :

Définition 4 *Soit x une variable et F une formule.*
— *Si* $F = P(t_1, \ldots t_n)$ *alors toutes les occurrences de x dans F sont libres.*
— *Si* $F = \phi * \psi$ *(où $*$ représente un connecteur binaire), alors les occurrences libres de x dans F sont les occurrences libres de x dans ϕ et les occurrences libres de x dans ψ.*
— *Si* $F = \neg\phi$ *alors les occurrences libres de x dans F sont les occurrences libres de x dans ϕ.*
— *Si* $F = \forall x P$ *ou* $\exists x P$ *alors x n'a aucune occurrence libre dans F.*
— *Si* $F = \forall y P$ *ou* $\exists y P$ *avec* $y \neq x$*, alors les occurrences libres de x dans F sont les occurrences libres de x dans P*

Exemple 1 $\forall_1 x(A(x,y) \rightarrow ((\forall_2 x B(x)) \vee \exists_3 y C(x,y)))$
Les première et troisième occurrences de x sont liées par le premier quantificateur, la seconde par le second. La première occurrence de y est libre, la seconde liée.

Définition 5 *Soit x une variable et F une formule.*
Les occurrences liées *de x dans F, sont les occurrences non libres de x dans F.*

Une variable libre *de F est une variable de F dont au moins une occurrence est libre.*

Une variable liée *de F est une variable non libre de F, (ie dont toutes les occurrences sont liées).*

Une formule close *est une formule dont toutes les variables sont liée (*ie. *qui n'a pas de variable libre).*

remarque : Comme le nom d'une variable liée n'a pas d'importance, on peut toujours s'arranger pour qu'une variable n'ait pas à la fois des occurrences libres et liées. Par exemple la formule :
$\forall_1 x(A(x,y) \rightarrow ((\forall_2 x B(x)) \vee \exists_3 y C(x,y)))$ est logiquement équivalente à
$\forall_1 x(A(x,y) \rightarrow ((\forall_2 z B(z)) \vee \exists_3 v C(x,v)))$

Définition 6 *Soit F une formule, x une variable et t un terme.*
$F[x/t]$ (parfois aussi noté $F[x := t]$) désigne la formule F dans laquelle chaque occurrence libre *de x a été remplacée par t.*

par exemple :si $F = \forall x(A(x,y) \rightarrow ((\forall x B(x)) \vee \exists y C(x,y)))$ alors
$F[x/v] = F$ et
$F[y/v] = \forall x(A(x,v) \rightarrow ((\forall x B(x)) \vee \exists y C(x,y)))$

Définition 7 *Une réalisation M est un modèle d'une formule F ssi pour toute interprétation I on a : $M \models_I F$ (noté $M \models F$)*

Définition 8 *Une formule F est* satisfaisable *ssi il existe une réalisation M telle que $M \models F$*

Définition 9 *Une formule F est* valide *(ou est une* tautologie*) ssi pour toute réalisation M on a : $M \models F$ (noté $\models F$)*

2.4 La notion de Déduction

2.4.1 Utilisation d'une hypothèse universelle

On va pouvoir rendre compte d'un nouveau type de raisonnement dont l'exemple canonique est le suivant :
Socrate est un homme,
tous les hommes sont mortels
donc socrate est mortel.
En calcul des propositions, chacune des trois lignes précédentes correspondraient à trois propositions, et les règles d'inférence connues ne nous permettent pas d'inférer la dernière des deux premières. Pourtant le raisonnement est correct. Ce sont les règles d'inférence concernant les quantificateurs qui vont nous permettre de déduire "Socrate est mortel" à partir des deux premiers faits. Formalisons cet exemple en calcul des prédicats :
donnons nous tout d'abord deux symboles de prédicat unaire

— "Etre-un-homme" (que nous ecrirons H(-)),

— "Etre-mortel" (que nous ecrirons M(-))
et une constante : socrate.
"Socrate est un homme" correspond à $H(socrate)$ qui est une formule atomique.
"tous les hommes sont mortels" correspond à la formule : $\forall x(H(x) \rightarrow M(x))$
"Socrate est mortel" correspond à $M(socrate)$.
Intuitivement le résultat permettant de déduire $M(socrate)$ à partir de $H(x)$ et $\forall x(H(x) \rightarrow M(x))$ est le suivant :
de $\forall x(H(x) \rightarrow M(x))$ qui vaut pour tout individu, on déduit en particulier : $(H(socrate) \rightarrow M(socrate))$. De ce fait et de l'hypothèse $H(socrate)$ on déduit par modus ponens : $M(socrate)$

Cet exemple illustre donc la figure de raisonnement liée à l'*utilisation d'une hypothèse universelle* (i.e. de la forme $\forall x P(x)$) :l'*instanciation* qui applique un fait qui vaut pour tout individu à un individu particulier.

Instanciation

Si on a en hypothèse que $\forall x P(x)$ alors on peut ajouter en hypothèse $P(a)$ pour n'importe quel individu a. Autrement dit : si P vaut pour tout le monde, alors P vaut en particulier pour n'importe quel a.	«Par instanciation de l'hypothèse sur a nous obtenons $P(a)$ »(nouvelle hypothèse)

2.4.2 Démonstration d'une hypothèse universelle

Imaginons maintenant que nous ayons montré :
Soient n, m et p des entiers. $n * (m + p) = (n * m) + (n * p)$
Nous pouvons nous srvir de ce résultat pour réécrire 2∗(4+3) en (2∗4)+(2∗3) mais aussi pour réécrire $2 * (x + 4)$ en $(2 * x) + (2 * 4)$
Autrement dit, nous utilisons cet énoncé comme un énoncé universel :
$(\forall m \forall n \forall p(n \in \mathbb{N} \wedge m \in \mathbb{N} \wedge p \in \mathbb{N} \rightarrow n * (m + p) = (n * m) + (n * p)))$ en l'instanciant à des cas particuliers chaque fois que nous le désirons.
Ceci est correct parceque, lors de la démonstration de l'énoncé, nous avons raisonné sur n m et p en ne sachant rien sur eux. Ils ont tenu le rôle d'entiers absolument quelconque.

Ainsi si nous avons montré $P(x)$ pour x quelconque, nous avons montré $\forall x P(x)$. Ceci revient à dire : pour démontrer $\forall x P(x)$ il suffit de démontrer P pour un individu quelconque x_0.
Ceci est la figure de raisonnement élémentaire liée à la démonstration d'une formule universelle.

démontrer un $\forall$

Pour démontrer $\forall x P(x)$ il suffit de démontrer P pour un individu quelconque x_0.	«Soit x_0 ; Montrons $P(x_0)$ »

2.4.3 Démonstration d'une formule existencielle

Montrer qu'une formule de la forme $\exists x P(x)$ est vraie est plus facile que montrer la vérité d'une formule universelle : il suffit de trouver quelqu'un qui

vérifie la formule. Par exemple, pour montrer qu'il existe un entier pair, il suffit de choisir un entier, 0 par exemple et de montrer que 0 est pair.

démontrer un $\exists$

Pour démontrer $\exists x P(x)$ il suffit d'exhiber un terme t, un *témoin* et de montrer qu'il verifie P.	«Nous allons montrer que (terme de votre choix) verifie P »

Il faut bien faire la différence entre les modes de raisonnement liés à la démonstration d'une formule universelle et à celle d'une formule existencielle. Dans le premier cas, on démontre P pour un individu que l'on nomme mais dont on ne connait rien. Dans le second, on choisit quelqu'un que l'on connait, un individu existant particulier et on montre la propriété pour cet individu connu.

2.4.4 Utilisation d'une hypothèse existencielle

Comment utiliser une hypothèse de la forme $\exists x P(x)$? Cette hypothése nous dit qu'il existe quelqu'un qui vérifie P, mais ne nous dit pas qui est cet individu. Nous ne savons rien d'autre sur cet individu que le fait qu'il vérifie cette propriété P. Utiliser cette hypothèse, c'est nommer l'individu quelconque vérifiant P.

utiliser un $\exists$

Si on a en hypothèse que $\exists x P(x)$ alors on peut ajouter en hypothèse $P(x_0)$ pour un individu x_0 quelconque.	«l'hypothèse nous dit qu'il existe quelqu'un vérifiant P. Nommons x_0 l'individu vérifiant P »(nouvelle hypothèse)

2.4.5 Quantificateurs et négation

$\neg \forall x P(x) \leftrightarrow \exists x \neg P(x)$ $\neg \exists x P(x) \leftrightarrow \forall x \neg P(x)$

2.5 Les résultats fondamentaux

Comme pour le calcul des Propositions, la notion de démonstration d'une formule peut se définir formellement. Une démonstration est un arbre de formule dont les noeuds sont des formules, la racine est la formule à démontrer . Le passage d'un niveau à l'autre dans l'arbre de preuve se fait en appliquant des règles d'inférences qui formalisent pour l'essentiel les figures de raisonnement que nous avons explicité dans ce cours. On progresse ainsi jusqu'a appliquer des règles qui ne produisent pas de sous arbres. Si toutes les branches sont ainsi fermées, la démonstration est achevée. On note le fait d'avoir une démonstration d'une formule $F \vdash F$.

Théorème 1 (Correction) *Soit F une formule alors :*
Si $\vdash F$ alors $\models F$

Théorème 2 (Complétude) *Soit F une formule alors :*
Si $\models F$ alors $\vdash F$

Théorème 3 (Indécidabilité) *Le calcul des prédicats est indécidable i.e. il n'existe pas d'algorithme qui s'arrête toujours et qui reussit si et seulement si son entrée est un théorème du calcul des prédicats.*

2.6 Quelques propriétés

Vous pouvez chercher à démontrer ces théorèmes utiles du Calcul des Prédicats

$\vdash \forall x(P(x) \wedge Q(x)) \leftrightarrow \forall x P(x) \wedge \forall x Q(x)$
$\vdash \exists x(P(x) \vee Q(x)) \leftrightarrow \exists x P(x) \vee \exists x Q(x)$
$\vdash \forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x))$
$\vdash \forall x(\exists y Q(x,y) \rightarrow P(x)) \rightarrow \forall x \forall y(Q(x,y) \rightarrow P(x))$

2.7 Exercices

Exercice 1 *Formaliser en Calcul des prédicats les phrases suivantes :*

1. *Les baleines sont des mammifères.*
2. *Les entiers sont pairs ou impairs.*
3. *Il existe un entier pair*

Corrigé :

1. $\forall x(Baleine(x) \rightarrow Mamm(x))$
2. $\forall x(Entier(x) \rightarrow (Pair(x) \vee Impair(x)))$
3. $\exists x(Entier(x) \wedge Pair(x))$

Exercice 2 *Il s'agit de construire un modèle partiel du fonctionnement d'une banque. Considérons les règles informelles suivantes. :*

- *Une banque gère pour ses clients deux types de comptes : les comptes* courant *et les comptes* épargne.
- *Chaque compte appartient à un unique client.*
- *Un client peut posséder plusieurs comptes courants mais un seul compte épargne.*

Formaliser les règles précédentes en Calcul des Prédicats

Il s'agit donc de se donner des symboles de prédicats et d'énoncer les règles au moyen de ceux ci. l'utilisation du connecteur $\exists!$ *est autorisée.*

- $\forall x(C(x) \rightarrow Courant(x) \vee Epargne(x))$
  $\forall x(Courant(x) \rightarrow C(x) \wedge \neg Epargne(x))$
  $\forall x(Epargne(x) \rightarrow C(x) \wedge \neg Courant(x))$

- $\forall x(C(x) \rightarrow \exists! y(Client(y) \wedge possede(y, x)))$
- $\forall x \forall y(Client(x), Epargne(y), possede(x, y) \rightarrow \exists! y(Epargne(y) \wedge possede(x, y)))$

Exercice 3 *Prouver :* $\vdash \forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x))$

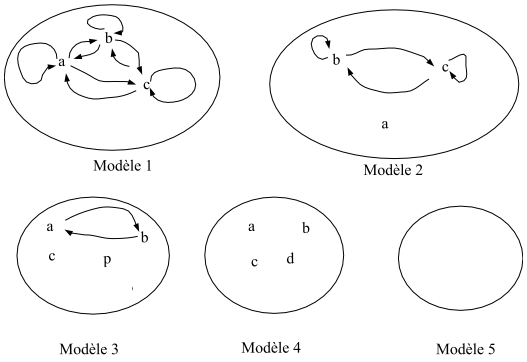
Corrigé : il est assez fréquent de montrer des énoncés universels en procédant par l'absurde. C'est ce que noius allons faire.

Supposons $\forall x(P(x) \rightarrow Q(x))$ *(h1) et* $\forall x P(x)$ *(h2) et montrons* $\forall x Q(x))$
Raisonnons par l'absurde : supposons $\neg \forall x Q(x)$ *, c'est à dire* $\exists x \neg P(x)$ *et montrons qu'on arrive à une contradiction.*
Nommons z l'individu ne vérifiant pas Q. On a donc $\neg Q(z)$ *(h3).*
Par instanciation de h2 sur z on a $P(z)$ *(h4).*
Par instanciation de h1 sur z on a $P(z) \rightarrow Q(z)$ *(h5).*
Donc, par Modus Ponens on a $Q(z)$ *ce qui contredit h3.*

Exercice 4 *prouver :* $\forall x(\exists y Q(x,y) \rightarrow P(x)) \rightarrow \forall x \forall y(Q(x,y) \rightarrow P(x))$
Corrigé : Nous allons faire une preuve directe.
Supposons $\vdash \forall x(\exists y Q(x,y) \rightarrow P(x))$ *(h1) et montrons* $\forall x \forall y(Q(x,y) \rightarrow P(x))$.
Soient a, b et c ; Montrons $Q(a,b) \rightarrow P(a)$.
Supposons $Q(a,b)$ *(h2) et montrons* $P(a)$.
Comme h2 est vraie, on a aussi $\exists y Q(a,y)$ *(h3). Par instanciation de h1 sur a on a :* $\exists y Q(a,y) \rightarrow P(a)$ *(h4), donc on déduit* $P(a)$ *par Modus Ponens.*

Exercice 5 *On se pose la question de savoir si le fait qu'une relation soit symétrique (A) et transitive (B) implique qu'elle soit aussi reflexive (C). Ce n'est pas le cas, et les modèles qui suivent permettent de comprendre pourqoui. Le but de cet exercice est d'ajouter une condition supplémentaire (D) telle que* $A \wedge B \wedge D \rightarrow C$

1. *traduire en calcul des prédicats les phrases suivantes :*
   — *R est symetrique(A)*
   — *R est transitive (B)*
   — *R est reflexive (C)*
   en modélisant la relation binaire R par un prédicat binaire $R(,)$.
2. *parmis ces modèles, lesquels rendent vrais A et B ?*



3. *même question pour C .*
4. *même question pour* $(A \wedge B) \rightarrow C$.
5. *Expliquer ce qui se passe pour les modèles 2 4 et 5*
6. *Compléter la formule suivante pour qu'elle soit valide.* $A \wedge B \wedge \ldots \rightarrow C$
7. *Démontrer cette nouvelle formule*

Corrigé :

1. — $\forall x \forall y(R(x,y) \rightarrow R(y,x))(A)$
   — $\forall x \forall y \forall z(R(x,y) \wedge R(y,z) \rightarrow R(x,z))(B)$
   — $\forall x R(x,x)$ *(C)*

2. *1,2 ,4 et 5 rendent vraies A et B. Le modèle 3 ne verifie pas la transitivité.*
3. *Seul 1 rend vraie C*
4. *1 et 3 rendent vraie $(A \wedge B) \rightarrow C$.*
5. *Dans 2 4 et 5, la relation est transitive et symetrique mais pas reflexive. Ceci est du au fait que la relation R ne concerne pas tous les éléments de l'ensemble.*
6. *Il suffit donc d'ajouter le fait que tous les éléments sont touchés par la relation : $A \wedge B \wedge \forall x \exists y(R(x,y) \vee R(y,x)) \rightarrow C$ En fait il suffit d'ajouter que tous les éléments de l'ensemble sont dans le domaine de R (on dit que la relation est totale). $\forall x \exists y R(x,y)$*
7. *Soit R symetrique, transitive et totale. Soit e un individu quelconque. Montrons que $R(e,e)$.*
   R est totale donc $\exists y R(e,y)$. Appelons f l'individu tel que $R(e,f)$. Comme R est symetrique on a $R(f,e)$. Comme elle est aussi transitive, le fait d'avoir $R(e,f)$ et $R(f,e)$ implique qu'on ait aussi $R(e,e)$, ce qui était le but de notre démonstration.

Chapitre 3

La théorie de l'égalité

3.1 Qu'est ce qu'une théorie ?

Les formules valides ou démontrables en calcul des prédicats sont les pures vérités logiques, les énoncés vrais dans tous les mondes possibles. Si l'on veut utiliser la logique pour modéliser des domaines d'application, la programmation par exemple, cela est insuffisant. On aura par exemple besoin de parler des types de données comme les entiers, les tableaux ..., d'énoncer des faits qui sont relatifs à ces données.
La notion de *théorie* permet cela. Prenons un exemple : imaginons que nous ayons besoin d'un prédicat particulier P qui à la propriété d'être une relation transitive et anti reflexive. La théorie permettant de définir ce prédicat sera constituée des formules : $\forall x \forall y \forall z (P(x,y) \wedge P(y,z) \rightarrow P(x,z))$ et $\forall x \neg P(x,x)$.
Nous pouvons maintenant nous intéresser non pas à tous les mondes possibles, mais uniquement aux mondes dans lequel ces deux formules sont vraies, c'est à dire les univers qui admettent une relation d'ordre stricte.
D'un point de vue sémantique, cela signifie que l'on va s'intéresser à tous les *modèles de cette théorie*. On aura par exemple que tous ces modèles vérifient que P est anti symétrique.
D'un point de vue syntaxique, on s'intéressera aux formules *démontrables dans cette théorie* c'est à dire démontrable en Calcul des Prédicats dans lequel on suppose vraies ces deux formules. Ces formules ne sont pas des théorèmes, car elles ne sont pas démontrées, ce sont des *axiomes*. Mise a part cette différence fondamentale, elles s'utilisent dans les preuves exactement de la même façon.

Définition 10 *Une* théorie *est un ensemble T de formules closes.*
Une réalisation $\mathcal{M}$ est un modèle d'une théorie *T ssi $\mathcal{M} \models \mathcal{F}$ pour chaque formule F de T.*

Une formule ϕ est une conséquence *de T ssi tous modèles de T est un modèle de ϕ (noté $T \models \phi$).*
Une formule ϕ est démontrable dans une théorie T ssi elle est démontrable en Calcul des Prédicats plus la possibilité de supposer vrais les les axiomes de la théorie.

3.2 les axiomes de la théorie de l'égalité

Nous allons exprimer les propriétés d'un prédicat particulier : l'égalité (=). L'égalité est un prédicat qui est reflexif, symétrique, transitif, et qui a la propriété de substitution des égaux par les égaux dans n'importe quel prédicat. Cette dernière propriété est appelée *loi de Leibniz*. En fait seules la reflexivité et la loi de Leibniz suffisent à définir l'égalité. La symétrie et la transitivité seront démontrables à partir de ces deux axiomes.
La théorie de l'égalité est donc constituée des deux axiomes suivants :

1. (refl :) $\forall e(e = e)$
2. (leibniz :) Pour tout prédicat P , $\forall x \forall y(x = y \wedge P(x) \rightarrow P(y))$

L'égalité est un prédicat indispensable à toutes modélisations. C'est pourquoi la majeure partie des théories contiennent les axiomes de l'égalité. C'est le cas par exemple de la théorie des ensembles. Nous parlerons alors de théories du Calcul des Prédicats *avec égalité*.

3.3 Raisonner avec l'égalité

L'égalité est un simple prédicat, défini par des axiomes. Mais l'axiome de Leibniz lui confère un statut tout a fait particulier : si deux éléments sont en relation d'égalité, alors ils se comportent exactement de la même façon pour n'importe quel autre prédicat du langage.
Ainsi, dès qu'une égalité entre 2 individus a et b est connue (une hypothèse ou un théorème), alors on peut à chaque instant dans une démonstration remplacer a par b et inversement.
L'égalité est aux individus, ce que l'équivalence est aux formules.
utiliser une égalité

S'il est vrai que $a = b$, alors partout où a apparait, on peut le remplacer par b et inversement.	≪Comme $a = b$ et $P(a)$ on a aussi $P(b)$ ≫(nouvelle hypothèse) ≪Comme $a = b$ pour démontrer $P(a)$ il suffit de démontrer $P(b)$ ≫

3.4 quelques propriétés

Symétrie	$\forall x \forall y (x = y \rightarrow y = x)$
Transitivité	$\forall a \forall b \forall c (a = b \wedge b = c \rightarrow a = c)$

3.5 Exercices

Exercice 6 *On veut modéliser le fonctionnement d'une bibliothèque : On observe les règles suivantes :*

1. *Un exemplaire est toujours associé à un livre. Celui ci est unique.*
2. *Un même exemplaire de livre ne peut etre emprunté par différents abonnés.*
3. *Un même abonné ne peut emprunter plus d'un exemplaire d'un même livre*

formaliser les règles en Calcul des prédicats.

On se donne :
$Ex(\_)$*(etre un exemplaire),*
$L(\_)$ *(etre un livre)*
$A(\_)$ *(etre un abonné)*
$Emp(a, e)$ *(a emprunte l'exemplaire e) et*
$Exde(e, l)$ *(e est un exemplaire du livre l)*

1. $\forall e(Ex(e) \rightarrow \exists! y(L(y) \wedge Exde(e, l)))$
2. $\forall e, aa, ab(Ex(e), A(aa), A(ab), Emp(aa, e) \wedge Emp(ab, e) \rightarrow aa = ab)$
3. *Si deux exemplaires sont empruntés par un même abonnés, ils concernent des livres différents :*
   $\forall ea, eb((Ex(ea) \wedge Ex(eb) \wedge ea \neq eb \wedge \exists a(A(a) \wedge Emp(a, ea) \wedge Emp(a, eb))) \rightarrow$
   $\forall la, lb(Exde(ea, la) \wedge Exde(eb, lb) \wedge L(la) \wedge L(lb) \rightarrow la \neq lb))$

Exercice 7 *Dans cet exercice, on va faire un peu d'arithmétique. On veut montrer que l'addition de 2 entiers pairs est un entier pair.*
On a besoin des prédicat et théorèmes suivants :

— $\mathbb{N}(x)$ *: x est un entier naturel.*
— $Pair(x)$ *: x est un entier pair*
— *(r1) :* $Pair(a) \leftrightarrow \exists n(a = 2 * n)$

— *(r2)* : $\forall a \forall b \forall c a * (b + c) = (a * b) + (a * c)$

1. *Formaliser l'enoncé à montrer en Calcul des prédicats.*
2. *Montrer l'énoncé*

Corrigé :L'énoncé se traduit par :
$\forall n \forall m(\mathbb{N}(n) \wedge \mathbb{N}(m) \wedge Pair(m) \wedge Pair(n) \rightarrow Pair(n + m))$
Démonstration : Soient a et b deux entiers pairs.
Comme a est pair, on a par r1 : $a = 2 * p$ *pour un certain p.*
Comme b est pair, on a par r1 : $b = 2 * q$ *pour un certain q.*
Donc $a + b = (2 * p) + (2 * q)$.
Or par r2 $(2 * p) + (2 * q) = 2 * (p + q)$.
Donc $a + b = 2 * (p + q)$ *. Il existe donc n tel que* $a + b = 2 * n$ *et donc* $a + b$ *est pair par r1.*

Exercice 8 *On veut montrer que si l'addition de 2 entiers est impaire alors exactement un nombre parmi n et m est impair. Vous avez le droit de vous servir du résultat montré dans l'exercice précédent. On a en plus*
(r3) $Impair(n) \leftrightarrow \exists k(n = (2 * k) + 1)$ *et*
(r4) $\neg(Impair(n)) \leftrightarrow Pair(n)$
et (r5) $(Impair(n) \leftrightarrow Pair(n + 1))$ *ainsi que l'associativité et la reflexivité de l'addition.*

1. *Formaliser l'enoncé à montrer en Calcul des prédicats.*
2. *Montrer l'énoncé par l'absurde.*

Corrigé
enoncé :$\forall n \forall m(\mathbb{N}(n) \wedge \mathbb{N}(m) \wedge Impair(m+n) \rightarrow ((Impair(m) \vee Impair(n)) \wedge \neg(Impair(m) \wedge Impair(n))))$

Démonstration : raisonnons par l'absurde : supposons qu'il existe n et m entiers tels que $Impair(n + m)$*(h1) et*
$\neg((Impair(m) \vee Impair(n)) \wedge \neg(Impair(m) \wedge Impair(n)))(h2)$ *et montrons que c'est impossible.*
Par hypothèse $(n + m)$ *est impair donc par r3* $n + m = (2 * k) + 1$ *pour un certain k.*
Par ailleurs : h2 $\leftrightarrow$
$\neg(Impair(m) \vee Impair(n)) \vee \neg\neg(Impair(m) \wedge Impair(n))) \leftrightarrow$
$(\neg Impair(m) \wedge \neg Impair(n)) \vee (Impair(m) \wedge Impair(n)) \leftrightarrow (r4)$
$(Pair(m) \wedge Pair(n)) \vee (Impair(m) \wedge Impair(n))$
En d'autres termes h2 signifie : n et m sont tous les deux pairs ou tous les deux impairs.

Raisonnons donc par cas sur h2 :
Premier cas : si n et m sont tous les deux pairs, alors l'exercice precedent nous dit que $n + m$ aussi ce qui contredit h1.
Second cas : si n et m sont impairs : alors $n = (2 * a) + 1$ et $m = (2 * b) + 1$ pour un certain a et un certain b (par r3).
Donc $n + m = ((2 * a) + 1) + ((2 * b) + 1) = ((2 * a) + (2 * b) + 1) + 1 = ((2 * (a + b)) + 1 + 1)$ par r2.
Il résulte de r3 que $2 * (a + b)) + 1$ est impair et donc par r5 que $(2 * (a + b)) + 1 + 1)$ est pair donc $n + m$ aussi ce qui contredit h1.

Chapitre 4

La théorie des ensembles

La théorie des ensembles a pour but de définir la notion d'ensemble.

Elle est constituée de 6 axiomes, qui postulent tous l'existence d'ensembles particuliers. Ces six axiomes reviennent à définir le prédicat d'appartenance $\in$. La notoriété et l'utilité de cette théorie viennent du fait qu'elle suffit à modéliser l'ensemble des mathématiques.

Grace a son haut pouvoir d'expression, cette théorie met à notre disposition un langage très utile pour décrire de nombreux concepts tant mathématiques qu'informatiques.

Avant de présenter les axiomes proprement dit, nous allons décrire les principales constructions de la théorie des ensembles.

4.1 ensembles et opérations sur les ensembles

Un **ensemble** est une collection d'objets : ses **éléments**.

On peut définir un ensemble en décrivant ses éléments.

Ceci peut se faire de deux façons : par **extension** ou par **comprehension**.

4.1.1 Définition par extension d'un ensemble

$$A = \{Anne, Bertrand, Florence\}$$

$$B = \{2, 5, 1, 9\}$$

Ces exemples définissent deux ensembles (A et B) par la donnée de leurs éléments placés entre **accolades**.

Les ensembles comme leurs éléments sont des individus au sens du Calcul des prédicats.

4.1.2 Définition par compréhension d'un ensemble

On ne peut pas toujours, notemmment lorsque les ensembles sont infinis, donner exhaustivement les éléments d'un ensemble. Heureusement, on peut aussi caractériser les éléments d'un ensemble au moyen d'une propriété :

$$C = \{\text{x}\,;\ \text{x est un entier impair}\}$$

4.1.3 Appartenance

L'expression ≪a est un élément de l'ensemble S ≫s'ecrit $a \in S$. $\in$ est un nouveau prédicat. Les axiomes de la théorie des ensembles auront tous pour objet de le définir.

4.1.4 L'ensemble vide

Un ensemble joue un rôle majeur : l'ensemble qui n'a pas d'éléments. On l'appelle l'**ensemble vide** et on le note $\emptyset$.

4.1.5 Egalité entre ensembles

2 ensembles sont égaux s'ils ont les mêmes éléments :

$$\forall x(x \in A \leftrightarrow x \in B) \rightarrow A = B$$

Ceci nous donne un moyen de démontrer que 2 ensembles sont égaux.

La réciproque, c'est à dire le fait que si 2 ensembles sont égaux alors ils ont les mêmes éléments, est évidemment vraie, mais ceci n'a rien avoir avoir les ensembles : c'est la loi de Leibniz pour l'égalité qui nous le dit, car l'appartenance est un prédicat ordinaire.
On a donc :

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

Ainsi par exemple $\{\emptyset\}$ a un élément :$\emptyset$, alors que $\emptyset$ n'en a pas. On a donc : $\{\emptyset\} \neq \emptyset$ et $\emptyset \in \{\emptyset\}$ et $\emptyset \neq \emptyset$

L'ordre des éléments dans un ensemble n'a pas d'importance. Il est facile de montrer que $\{a, b\} = \{b, a\}$. Il n'y a donc pas moyen de différencier ces deux ensembles.

De même, on ne peut parler du nombre de fois où un élément apparait dans un ensemble. On n'ecrira donc jamais $\{a, b, a\}$ mais plutôt $\{a, b\}$.

Exercice 9 *Donner une définition par extension des ensembles suivants :*
$a = \{x; x est\ un\ mois\ sans\ la\ lettre\ r\}$
$a = \{y; \exists x(y = x^2 \wedge y \leq 20\}$

Corrigé :
$a = \{Mai, Juin, Juillet, Aout\}$
$a = \{0, 1, 4, 9, 16\}$

4.1.6 Inclusion

Un ensemble X est un sous ensemble d'un autre ensemble Y si tous ses éléments sont aussi des élements de Y. On le note $X \subseteq Y$.

$$X \subseteq Y \leftrightarrow \forall x(x \in X \rightarrow x \in Y)$$

On a : $A \subseteq A$ et $\emptyset \subseteq A$ pour out ensemble A

Atention à ne pas confondre $\in$ et $\subseteq$.
Par exemple : $\{4, 6, 2\} \notin \{1, 2, 3, 4, 5, 6\}$ mais
$\{4, 6, 2\} \in \{\{3\}, \{4, 5, 6\}, 7\}$
$\{4, 6, 2\} \subseteq \{1, 2, 3, 4, 5, 6\}$

4.1.7 Ensembles des parties d'un ensemble

A partir d'un ensemble A, on peut construire l'ensemble de tous ses sous ensembles. Cet ensemble s'appelle l'ensemble des parties de A et se note $\mathcal{P}(A)$.

$$\forall a \forall s(a \in \mathcal{P}(s) \leftrightarrow \forall x(x \in a \rightarrow x \in s))$$

Si A a n éléments, alors $\mathcal{P}(A)$ en a 2^n.

Par exemple :
$A = \{a, b, c\}$ alors $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

4.1.8 Union, intersection et différence

Ces trois opérations permettent de combiner des ensembles existants pour en former de nouveaux.

L'**union** de 2 ensembles X et Y est constitué des objets qui sont éléments de X ou qui sont éléments de Y. On le note $X \cup Y$

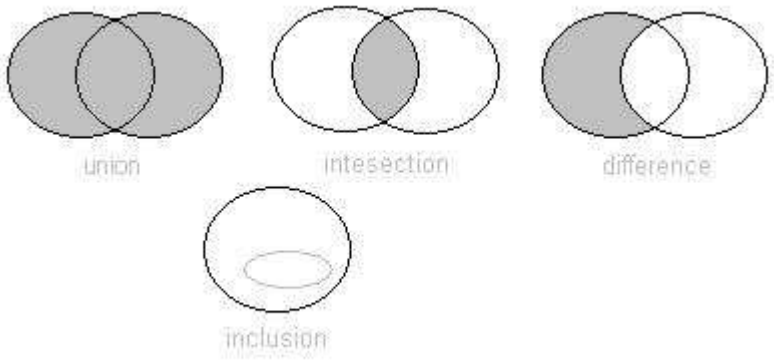
$$x \in X \cup Y \leftrightarrow (x \in X \vee x \in Y)$$

L'**intersection** de 2 ensembles X et Y est constitué des objets qui sont à la fois éléments de X et de de Y. On le note $X \cap Y$

$$x \in X \cap Y \leftrightarrow (x \in X \wedge x \in Y)$$

Le **complément** d'un ensemble Y par rapport à un ensemble X est constitué des éléments de X qui ne sont pas éléments de Y. On le note $X - Y$

$$x \in X - Y \leftrightarrow (x \in X \wedge x \notin Y)$$



4.1.9 Restriction de la définition d'un ensemble par compréhension

On a vu que l'on pouvait d'éfinir un ensemble par comprehension, c'est à dire en donnant la propriétés que ses éléments vérifient. Ceci, utilisé sans garde fou pose problème et produit un paradoxe appelé le *paradoxe de russell* :

Définissons l'ensemble A comme l'ensemble des objets qui ne sont pas éléments d'eux même :

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

Posons nous la question suivante : A appartient il a lui même $(A \in A)$?

- Si non , c'est a dire si $A \notin A$ alors la formule définissant A est vraie et donc $A \in A$
- Si oui, c'est à dire $A \in A$ alors la formule définissant A est fausse et donc $A \notin A$

Pour éviter ce paradoxe, il faut restreindre le principe de définition des ensembles par compréhension. Il aura la forme suivante :

$$A = \{x; \mathbf{x} \in \mathbf{B} \wedge P(x)\}$$

On exige ici que A soit formé à partir d'éléments puisés dans un ensemble préexistant B. Ainsi, on interdit la possibilité que tous le monde soit un ensemble. Par exemple, il n'y aura pas d'ensemble de tous les ensembles. Plus précisemment, cette collection ne sera pas un ensemble au sens de la théorie des ensembles.

4.1.10 couples et produit cartésien

Un *couple* (a, b) est une paire ordonnée, c'est à dire un ensemble dont le premier élément est a et le second b. On peut exprimer cette propriété par :

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$$

La paire $\{a, b\}$ ne vérifie pas cette propriété. On a en effet $\{a, b\} = \{b, a\}$. On ne peut donc pas l'utiliser pour définir le couple. En revanche, l'ensemble $\{\{a, \{a, b\}\}$la vérifie. On définit donc : $(a, b) \stackrel{\text{def}}{=} \{\{a, \{a, b\}\}$.

On peut ensuite définir le produit cartésien de deux ensembles a et b comme l'ensemble des couples dont le premier élément est dans a et le second dans b :

$$a \times b \stackrel{\text{def}}{=} \{(x; y)|(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b)) \wedge x \in a \wedge y \in b\}$$

Pour se convaincre que $(x, y) \in \mathcal{P}(\mathcal{P}(a \cup b))$ prenons un exemple : Posons $a = \{u, v\}$ et $b = \{w\}$. $(u, w) \in a \times b$. Or $(u, w) \stackrel{\text{def}}{=} \{\{u\}, \{u, w\}\}$. $\{u, w\} \subset a \cup b donc \{u, w\} \in \mathcal{P}(a \cup b)$ $\{u\} \subset a \cup b donc \{u\} \in \mathcal{P}(a \cup b)$ donc $\{\{u\}, \{u, w\}\} \subset \mathcal{P}(a \cup b)$ donc $\{\{u\}, \{u, w\}\} \in \mathcal{P}(\mathcal{P}(a \cup b))$ //Ces objets vérifient :

4.2 Les relations binaires

4.2.1 définitions

Une relation de a vers b est un sous-ensemble de $a \times b$.
On définit donc *l'ensemble des relations binaires de a vers b* (noté $a \rightleftharpoons b$) par :

$$a \rightleftharpoons b \stackrel{\text{def}}{=} \mathcal{P}(a \times b)$$

Considérons $R \in a \rightleftharpoons b$: Le *domaine* (dom) de R est l'ensemble des premières composantes des couples de R, et le *codomaine* (ran) l'ensemble des deuxièmes composantes :

$$dom(R) = \{x|x \in a \wedge \exists y(y \in b \wedge (x, y) \in R)\}$$

$$ran(R) = \{y | y \in b \wedge \exists x(x \in a \wedge (x, y) \in R)\}$$

Soit s un sous ensemble de a. La *restriction* de R à s ($s \lhd R$) est l'ensemble des couples de (x, y) de R tels que $x \in a$:

$$s \lhd R \stackrel{\text{def}}{=} \{(x, y) | (x, y) \in R \wedge x \in s\}$$

L' *inverse* de R est définie par :

$$R^{-1} \stackrel{\text{def}}{=} \{(y, x) | (y, x) \in b \times a \wedge (x, y) \in R\}$$

La *composée* de deux relations $R \in a \rightleftharpoons b$ et $T \in b \rightleftharpoons c$ (notée $R; T$) est la relation de a vers c définie par :

$$R; T \stackrel{\text{def}}{=} \{(x, z) | (x, z) \in a \times c \wedge \exists y((x, y) \in R \wedge (y, z) \in T)\}$$

Voici quelques autres constructions sur les relations :
$R \rhd p \stackrel{\text{def}}{=} \{(x, y) | (x, y) \in R \wedge y \in p\}$
$p \lhd R \stackrel{\text{def}}{=} \{(x, y) | (x, y) \in R \wedge x \notin p\}$
$R \rhd p \stackrel{\text{def}}{=} \{(x, y) | (x, y) \in R \wedge y \notin p\}$
$R[p] \stackrel{\text{def}}{=} ran(p \lhd R)$
$R \leftarrow S \stackrel{\text{def}}{=} (dom(S) \lhd R) \cup S$

4.3 Les fonctions

4.3.1 Définitions

Certaines relations sont très utiles : Celles qui ont comme propriétés que tous les éléments de leur domaine ont une image unique. Ce sont les fonctions. Parmi elles on distingue les injections, c'est à dire les fonctions telles que 2 éléments différents de leur domaine ont des images distinctes, les surjections, dont tous les éléments du codomaine sont atteints, et les bijections qui sont à la fois injectives et surjectives. On distingue les fonctions totales, dont tous les éléments de l'ensemble de départ ont une image, des fonctions partielles.

Si f est une fonction, et si $x \in dom(f)$ alors il existe un unique b tel que $(a, b) \in f$. Nous l'appellerons *l'image de x par f* et le noterons $f(x)$.

D'autres part l'ensemble $\{(x, y) | (x, y) \in s \times t \wedge y = e\}$ où e est un terme ne contenant pas d'autre variable que x et tel que $\forall x(x \in s \rightarrow e \in t)$ désigne une unique fonction notée $\lambda x.(x \in s | e)$ telle que $\forall x(x \in s \rightarrow \lambda x.(x \in s | e)(x) = e$.

formellement :

fonction	$a \mathrel{+\!\!\!\rightarrow} b \stackrel{\text{def}}{=}$	$\{r \mid r \in a \rightleftharpoons b \wedge \forall x(x \in dom(r) \rightarrow \exists! y((x,y) \in r))\}$
fonct. totale	$a \rightarrow b \stackrel{\text{def}}{=}$	$\{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge dom(f) = a\}$
injection	$a \rightarrowtail b \stackrel{\text{def}}{=}$	$\{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge$ $\forall x, x'((x \in dom(f) \wedge x' \in dom(f) \wedge x \neq x') \rightarrow f(x) \neq f(x'))\}$
injection totale	$a \rightarrowtail b \stackrel{\text{def}}{=}$	$\{f \mid f \in a \rightarrow b \wedge f \in a \rightarrowtail b\}$
surjection	$a \twoheadrightarrow b \stackrel{\text{def}}{=}$	$\{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge ran(f) = b\}$
surj. totale	$a \twoheadrightarrow b \stackrel{\text{def}}{=}$	$\{f \mid f \in a \rightarrow b \wedge f \in a \twoheadrightarrow b\}$

4.3.2 Propriétés directes

$(fonctpa) : \forall a \forall b(a \mathrel{+\!\!\!\rightarrow} b = \{r \mid r \in a \rightleftharpoons b \wedge$
$\forall x(x \in dom(r) \rightarrow \exists! y((x,y) \in r))\})$
$(fonctpa_1) : \forall f \forall a \forall b(f \in a \mathrel{+\!\!\!\rightarrow} b \leftrightarrow$
$f \in a \rightleftharpoons b \wedge \forall x(x \in dom(f) \rightarrow \exists! y((x,y) \in f)))$

$(fonct) : \forall a \forall b(a \rightarrow b = \{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge dom(f) = a\})$
$(fonct_1) : \forall f \forall a \forall b(f \in a \rightarrow b \leftrightarrow f \in a \mathrel{+\!\!\!\rightarrow} b \wedge dom(f) = a)$

$(injpa) : \forall a \forall b(a \rightarrowtail b = \{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge$
$\forall x, x'(x \in dom(f), x' \in dom(f), x \neq x' \rightarrow f(x) \neq f(x'))\})$
$(injpa_1) : \forall f \forall a \forall b(f \in a \rightarrowtail b \leftrightarrow f \in a \mathrel{+\!\!\!\rightarrow} b \wedge$
$\forall x, x'(x \in dom(f), x' \in dom(f), x \neq x' \rightarrow f(x) \neq f(x')))$

$(inj) : \forall a \forall b(a \rightarrowtail b \stackrel{\text{def}}{=} \{f \mid f \in a \rightarrow b \wedge f \in a \rightarrowtail b\})$
$(inj_1) : \forall f \forall a \forall b(f \in a \rightarrowtail b \leftrightarrow f \in a \rightarrow b \wedge f \in a \rightarrowtail b)$

$(surjpa) : \forall a \forall b(a \twoheadrightarrow b = \{f \mid f \in a \mathrel{+\!\!\!\rightarrow} b \wedge ran(f) = b\})$
$(surjpa_1) : \forall f \forall a \forall b(f \in a \leftrightarrow f \in a \mathrel{+\!\!\!\rightarrow} b \wedge ran(f) = b)$

$(surj) : \forall a \forall b(a \twoheadrightarrow b = \{f \mid f \in a \rightarrow b \wedge f \in a \twoheadrightarrow b\})$
$(surj_1) : \forall f \forall a \forall b(f \in a \leftrightarrow f \in a \rightarrow b \wedge f \in a \twoheadrightarrow b)$

4.4 Les entiers Naturels

4.4.1 Qu'est ce que $\mathcal{N}$?

L'ensemble des entiers naturels est une suite $0, 1, 2 \ldots$.
Plus précisemment, c'est une suite infinie avec un plus petit élément.

On peut atteindre tous les entiers en se donnant 0 et une opération *successeur*. Fondamentalement , $\mathcal{N}$ est le plus petit ensemble contenant 0 et clos par l'opération *successeur*.
Cette structure particulière de $\mathcal{N}$ autorise un type de raisonnement nouveau : le raisonnement par récurrence.
De même, on pourra définir des fonctions par récurrence.

4.4.2 Le raisonnement par récurrence

Le raisonnement par récurrence à la forme suivante : Pour montrer qu'une propriété F vaut pour tout entier, il suffit de montrer que F est vraie de 0, et que si l'on suppose qu'elle est vraie d'un entier n quelconque, alors elle l'est aussi de son successeur. Sa correction est assurée par le fait que tout entier est atteignable par itération de S sur 0.

Formellement le principe de récurrence s'énonce comme suit : Soit F une formule quelconque,

$$Rec \stackrel{\text{def}}{=} (F(0) \wedge \forall y(y \in \mathcal{N} \wedge F(y) \rightarrow F(S(y)))) \rightarrow \forall x(x \in \mathcal{N} \rightarrow F(x))$$

Cette formule est démontrable en théorie des ensembles :

preuve :
Supposons $F(0)$, $(HR) = \forall y(y \in \mathcal{N} \wedge F(y) \rightarrow F(S(y))$,
et montrons $\forall x(x \in \mathcal{N} \rightarrow F(x)$
Supposons que cela ne soit pas le cas : Il y aurait donc un entier n tel que $\neg F(n)$. Considérons le plus petit entier m tel que $\neg F(m)$. Cela ne peut être 0 car on a en hypothèse $F(0)$. m est donc le successeur d'un entier m_1. $m_1 < m$ donc m_1 vérifie F. donc par HR m aussi, ce qui contredit $\neg F(m)$.

4.4.3 Définition de fonctions par récurrence

Nous avons défini un ensemble particulier, l'ensemble des entiers naturels, à l'intérieur de la théorie des ensembles. Nous avons ensuite montré qu'il était possible de raisonner par récurrence pour montrer des propriétés universelles sur cet ensemble. Puisque nous avons aussi défini la notion de fonctions d'ensembles vers d'autres ensembles dans la théorie, nous savons

qu'il existe des fonctions sur les entiers. Nous pouvons montrer par exemple que $S \in \mathcal{N} \rightarrow \mathcal{N}$. Nous pouvons appliquer tous les opérateurs sur les fonctions existantes sur les entiers pour définir de nouvelles fonctions. Par exemple $(S;S) \in \mathcal{N} \rightarrow \mathcal{N}$ et désigne intuitivement la fonction qui a x associe $x+2$. Pour définir de nouvelles fonctions sur les entiers, on a envie de pouvoir procéder de la façon suivante : Supposons que l'on ait à l'esprit une fonction h de $\mathcal{N} \rightarrow A$ (A est un ensemble quelconque) donnée par les deux clauses suivantes :
$h(0) = a$ (pour $a \in A$)
$h(S(n)) = F(h(n))$ (pour une fonction donnée $F \in A \rightarrow A$).

Intuitivement, ces deux clauses permettent de calculer la valeur de h en tout point x. En effet : $h(n) = F(h(n-1)) = F(F(h(n-2))) = \ldots = F^n(a)$. Ce principe de définition de fonction (définition par récurrence) est admissible en théorie des ensembles.

Proposition 1 *Soit A un ensemble, $F \in A \rightarrow A$. Il existe une unique fonction $h \in \mathcal{N} \rightarrow A$ telle que :*
$h(0) = a$ *(pour $a \in A$) et*
$\forall x(x \in \mathcal{N} \rightarrow h(S(x)) = F(h(x)))$

On peut généraliser le principe de définition par récurrence, pour les fonctions à n arguments. Voici le principe pour les fonctions à deux arguments :
Soit A un ensemble, $F_1 \in B \rightarrow A$, $F_2 \in A \times N \times B \rightarrow A$ $F_3 \in B \rightarrow B$. Il existe une unique fonction $h \in \mathcal{N} \times B \rightarrow A$ telle que :
$h(0, y) = F_1(y)$ et
$\forall x, y(x \in \mathcal{N} \wedge y \in B \rightarrow h(S(x), y) = F_2(h(x, F_3(y)), x, y))$

4.4.4 Quelques fonctions sur les entiers

addition	$(+_0) : \forall y(N(y) \rightarrow 0 + y = y)$ $(+_1) : \forall x \forall y(N(x), N(y) \rightarrow s(x) + y = s(x + y))$
multiplication	$(*_0) : \forall y(N(y) \rightarrow 0 * y = 0)$ $(*_1) : \forall x \forall y(N(x), N(y) \rightarrow s(x) * y = (x * y) + y)$
exponentiel	$(exp_0) : \forall m(N(n) \rightarrow m^0 = 1$ $(exp_1) : \forall m \forall n(m^{S(n)} = m \times (m^n)$
soustraction	$\{(m, n, a) \mid m, n, a \in \mathcal{N} \wedge n \leq m \wedge n + a = m\}$
division	$\{(m, n, a) \mid m, n, a \in \mathcal{N} \wedge m \neq 0 \wedge m \times a \leq n \wedge m < m \times S(a)\}$

4.5 Les suites

4.5.1 Définition des suites

Soit A un ensemble. Une suite d'éléments de A de longueur n est une fonction totale de l'intervalle $1..n$ vers A.
Définissons donc d'abord la notion d'intervalle de 1 à n :

$$1..n \stackrel{\text{def}}{=} \{x | x \in \mathcal{N} \wedge 1 \leq x \leq n\}$$

On peut maintenant construire l'ensemble des suites d'éléments de A, noté $seq(A)$ comme l'ensemble des fonctions totales des intervalles d'entiers vers A :

$$\{f | f \in \mathcal{N} \rightarrow\ A \wedge \exists n(n \in \mathcal{N} \wedge f \in 1..n \rightarrow\ A)\}$$

$\emptyset \in seq(A)$ car c'est une fonction totale de $1..0$ vers A. $\emptyset$ désignera dans ce contexte la suite vide et le noterons $[\,]$.
On peut aussi définir la fonction : qui étant donné un élément a de A et une suite $s \in seq(A)$, insère a en tête de s. Il suffit d'augmenter de 1 les indices de s puis d'ajouter le couple $1 \mapsto a$. Pour augmenter de 1 les indices de s, il suffit de composer la fonction prédécesseur ($pred$) avec s comme l'indique la figure suivante :

$$\begin{array}{cccccc} & pred & & s & \\ 2 & \mapsto & 1 & \mapsto & a_1 \\ 3 & \mapsto & 2 & \mapsto & a_2 \\ & & \vdots & & \\ n+1 & \mapsto & n & \mapsto & a_n \end{array}$$

Soit $a \in A$ et $s \in seq(A)$ On définit donc :

$$a : s \stackrel{\text{def}}{=} \{1 \mapsto a\} \cup (pred; s)$$

Proposition 2 $:\in A \times s \in seq(A) \rightarrow\ s \in seq(A)$

4.5.2 Raisonnement par récurrence sur les suites

On se rend compte que l'ensemble des suites est exactement le plus petit ensemble qui contient la suite vide et est clos par la fonction $cons$:

Proposition 3

$$s \in seq(A) \leftrightarrow s = [\,] \vee (\exists y \exists a(y \in seq(A) \wedge a \in A \wedge s = y : a))$$

Preuve :
$\leftarrow$: On a déja montré que $[\,] \in seq(A)$ et le fait que étant donnés $y \in seq(A)$ et $a \in A$ quelconque $a : y \in seq(A)$ découle du fait que : est une fonction totale.

$\rightarrow$: Soit $s \in seq(A)$ montrons :
$s = [\,] \vee (\exists y \exists a(y \in seq(A) \wedge a \in A \wedge s = y : a))$
On a par définition de $seq(A)$:
$s \in \mathcal{N} \nrightarrow A$, $\exists n(n \in \mathcal{N} \wedge s \in 1..n \rightarrow\ A)$
Soit n_0 tel que : $n_0 \in \mathcal{N}$ et $s \in 1..n_0 \rightarrow\ A$
Puisque n_0 est un entier nous pouvons raisonner par cas :
1. $n_0 = 0$: dans ce cas $s = [\,]$ car $1..0 = \emptyset$ et nous concluons en choisissant la première partie de la disjonction qui est notre but.
2. $n_0 = S(n_1)$ pour un certain entier n_1 : en ce cas, puisque $s \in 1..S(n_1) \rightarrow\ A$, on peut construire $s_1 = S; (1 \lhd s)$ telle que $s_1 = \in 1..n_1 \rightarrow\ A$
Il suffit alors de choisir dans notre but la deuxième partie de l'alternative en prenant s_1 comme témoin pour y , et $s(1)$ comme témoin pour a .
On a en effet $s(1) : s_1 = s$.

Gràce au résultat précédent, on déduit qu'il est possible de raisonner par récurrence sur les suites :
pour montrer qu'une propriété F est vraie de toutes les suites, il suffit de montrer que F est vraie de la suite vide, et que si l'on suppose F vraie d'une suite s, alors on sait montrer qu'elle reste vraie de la suite $a : x$ pour a l'un quelconque des éléments de A.
Ceci signifie que la formule suivante est démontrable dans la théorie des ensembles :

$$(F([\,]) \wedge \forall a \forall y(a \in A \wedge y \in seq(A) \wedge F(y) \rightarrow F(a : y))) \rightarrow \forall s(s \in seq(A) \rightarrow F(s))$$

La preuve est identique au cas des entiers naturels. Elle utilise donc aussi une notion de relation d'ordre sur les suites. On prendra bien sur comme relation d'ordre la longueur des suites. On peut aussi définir l'ordre lexicographique sur les suites. On peut aussi définir la fonction d'insertion en queue d'une suite. On aura aussi que $seq(A)$ est le plus petit ensemble contenant la suite vide et clos par insertion en queue. On aura donc un principe de récurrence fondé sur ce résultat. Contrairement aux entiers, où le raisonnement par récurrence est systématique ou presque, de nombreux résultats sur les suites ne se démontrent pas par récurrence mais en utilisant la définition et des résultats sur les fonctions.

4.5.3 Principe de définition par récurrence sur les suites

Soit A un ensemble, $F \in B \times A \rightarrow B$,
Il existe une unique fonction $h \in seq(A) \rightarrow B$ telle que :
$h([\,]) = b$
$h(a : x) = F(h(x), a)$

Soit A un ensemble, $F_1 \in B \rightarrow C$,
$F_2 \in C \times seq(A) \times A \times B \rightarrow C$ et
$F_3 \in B \rightarrow B$.
Il existe une unique fonction $h \in seq(A) \times B \rightarrow C$ telle que :
$h([\,], y) = F_1(y)$ et
$\forall x, y(x \in seq(A) \wedge y \in A \rightarrow h(x : a, y) = F_2(h(x, F_3(y)), x, a, y))$

4.5.4 Quelques fonctions sur les suites

En plus de celles définies dans le chapitre précédent , on peut définir par exemple :

$reverse$	$(rev_0) : reverse([]) = []$ $(rev_1) : \forall a \forall x(N(a), N(x) \rightarrow$ $\quad reverse(a : x) = append(reverse(x), a : []))$
$t \uparrow n$	$t \uparrow n \stackrel{\text{def}}{=} (1..n) \lhd t$

4.5.5 le cardinal d'un ensemble fini

Comment exprimer le fait qu'un ensemble est fini ? Il suffit de pouvoir le mettre en bijection avec un sous ensemble strict de $\mathcal{N}$:

$$Fini(x) \stackrel{\text{def}}{=} \exists f \exists n(n \in \mathcal{N} \wedge f \in 1..n \twoheadrightarrow x \wedge f \in 1..n \rightarrowtail x)$$

Soit maintenant A un ensemble et x un sous ensemble de A.
L'ensemble $card(x) \stackrel{\text{def}}{=} \{(x, m) | x \subseteq A \wedge \exists n \exists f(n \in \mathcal{N} \wedge f \in 1..n \twoheadrightarrow x \wedge f \in 1..n \rightarrowtail x \wedge m = max(dom(f)))\}$ définit une fonction qui associe à chaque sous ensemble fini de A le nombre de ses éléments.
Pour montrer que c'est une fonction, il faut montrer que x a une unique image. Ceci est assuré par le fait que s'il existe n et une bijection de $1..n$ vers x alors ceux ci sont uniques. Le fait qu'elle soit totale sur les sous ensembles finis de A est déduit de la définition de $Fini$.

Exemple 2 *Soit s et t des suites d'éléments de A.*
Ecrire des formules exprimant les faits suivants :

1. *s est ordonnée*
2. *s est une permutation de t*
3. *s est sans répétition*