Initiation à la logique

Cours de Licence/Maîtrise
Jacques Jayez, ENS-LSH
Jacques.Jayez@ens-lsh.fr

Présentation et niveau Ce cours est une introduction élémentaire à la logique. Il comporte six chapitres.
1. Une introduction à la théorie des ensembles (chapitre 1).
2. Une introduction à la logique propositionnelle classique (chapitre 2).
3. Une introduction à la logique du premier ordre classique (chapitre 3).
4. Une introduction à la théorie des modèles classiques (chapitre 4).
5. Une introduction aux aspects élémentaires du λ–calcul (chapitre 5).
6. Une introduction à la théorie de la preuve avec une discussion de systèmes non–classiques (chapitre 6).

Techniquement, ce cours reste élémentaire. Cela signifie que les objets manipulés ne sont pas physiquement très longs. Par exemple, il n'y a pas de λ–termes de cinq lignes à réduire. En revanche, les notions introduites sont souvent un peu plus complexes que ce qui est introduit dans les manuels de logique «philosophique» et certaines démonstrations de difficulté moyenne sont données *in extenso*.

Mode d'emploi Le plus simple est de lire les chapitres dans l'ordre et de faire les exercices. Ils sont en général assez simples et un peu répétitifs pour permettre de se familiariser de façon mécanique avec la logique. Quelques théorèmes sont délicats. Il faut les aborder avec patience : il est absolument normal de passer du temps à comprendre une démonstration, et ce n'est pas du temps perdu. En général, comme en musique, la répétition seule produit de la maîtrise.

La logique *classique* Exception faite du dernier chapitre, les propriétés logiques décrites ici sont *classiques*. Ce mot ne signifie pas «traditionnel». La logique dite «classique» (LC) est une forme particulière de logique qui a deux principales caractéristiques :

Définition 1 Pour être dite *classique*, une logique doit avoir au moins les deux propriétés suivantes :
1. toute expression est évaluée comme vraie ou comme fausse, mais ni comme indéterminée ni comme vraie et fausse à la fois.
2. Quand on a une expression complexe (par exemple $A \Rightarrow B$, A «implique» B) sa valeur de vérité ne dépend que des valeurs de vérité des composantes (ici A et B), *jamais* de leur sens intuitif ou technique.

La LC est souvent critiquée parce qu'elle donne une image trop simplifiée du raisonnement. Par ex., on lui objecte les difficultés suivantes : • elle pose problème quand on veut représenter l'incertitude ou l'ignorance (par ex., quand on ignore si A ou si non-A),

• Problèmes pour représenter les points de vue (d'un certain pt de vue A, d'un autre pt de vue A). • Problèmes pour construire une déf. intuitive de l'implication (voir ici).
Dans ce cours, je ne discute pratiquement pas de ces problèmes et la LC est prise «telle quelle».

Terminologie de base Les expressions suivantes sont couramment utilisées.[1]

Définition 2 Une *relation* est vraie ou fausse d'un ou de plusieurs objets. Une propriété est une relation qui s'applique à un seul objet à la fois.

Ex. : relation «être plus grand que», notée PG : $PG(a, b)$ est vraie si et seulement si a est plus grand que b ; propriété : «être de nationalité française» (F) ; $F(a)$ est vraie de a si et seulement si a est de nationalité française.

Définition 3 Une *expression* est n'importe quelle suite de signes logiques qui respecte les contraintes de construction du langage logique considéré. Une expression est donc une entité purement formelle.

Ex. : $p \,\&\, q$ («p et q»), $p \Rightarrow (q \;\vee\; s)$ («p implique q ou s»), $\exists x P(x)$ («il existe au moins un x tel que x vérifie P») sont des expressions.

Définition 4 Un *terme* est une expression qui dénote une entité. Un *prédicat* est une expression qui dénote une relation ou une propriété.[2] Une *formule* est une expression qui dénote le vrai ou le faux.

En gros, un terme fonctionne comme un nom ou un groupe nominal (qui désigne quelque chose) ; un prédicat fonctionne comme un verbe ou un adjectif (qui décrit ou qualifie des entités) ; une formule fonctionne comme une phrase assertive (qui est vraie ou fausse).

Définition 5 Un *connecteur* est un signe qui dénote une relation entre des formules.

Ex. : «et» et «ou» sont des connecteurs ; ainsi $A \,\&\, B$ est vraie ssi (abréviation de si et seulement si) A et B sont vraies toutes les deux. L'implication est également exprimée par un connecteur.

Remarque : quand le connecteur porte sur une seule formule, on parle plutôt d'*opérateur*. La négation classique $(\neg)$ et les modalités de possibilité $(\Diamond)$ et de nécessité $(\Box)$ sont des opérateurs.

[1] Toutes ces définitions seront présentées à nouveau dans les chapitres suivants.
[2] Il est normal de ne pas trouver cette définition très claire. Elle ne l'est pas. La question des prédicats est reprise au chapitre 3.

Définition 6 A si et seulement si B signifie que A et B sont équivalents : si A est vraie, B aussi, si A est fausse, B aussi, et inversement

Définition 7 Une *opération* ou *fonction* est n'importe quel mécanisme qui prend plusieurs arguments et renvoie une valeur.

«Opération» $\Rightarrow$ l'ensemble où sont choisis les arguments et celui de la valeur sont le même. Par exemple, l'addition sur les entiers est une opération qui prends deux entiers (= deux éléments de l'ensemble des entiers $\mathbb{N}$) et qui renvoie une entier (leur somme). Cependant, terminologie flottante. En pratique, opération = fonction.
☞ Quand on veut insister sur la structure interne d'une expression ou d'un objet plutôt que sur le résultat d'une fonction/opération, on parle en général de *constructeur*. Par ex., les connecteurs sont des constructeurs.

Chapitre 1

Eléments de théorie des ensembles

1.1 Remarques intuitives

➤ Notion intuitive : ensemble = collection d'objects qui partagent une même propriété ou sont simplement regroupés pour une raison quelconque. Exemples
L'ensemble formé des nombres 1, 2, 3.
L'ensemble des élèves d'une classe.
L'ensemble des entiers naturels (0, 1, 2, etc.).
L'ensemble formé par les quatre premiers nombres pairs + un ticket de métro

➤ Quelques problèmes abordés dans ce cours
• Les intuitions sont relativement claires pour les petits ensembles finis, mais pour les «gros» ensembles finis ou les ensembles infinis ?
• Tout ce qui est défini par une propriété est–il un ensemble ? Autrement dit, la collection des choses qui vérifient la propriété est–elle un ensemble ?
• Réponses
– Pour les ensembles finis (petits ou gros), les outils sont les mêmes ;
– ils sont en partie différents pour les ensembles infinis ;
– tout ce qui est défini par une propriété n'est pas un ensemble.

1.2 Outils de base

➤ $\in$ et $\{x : P(x)\}$

• $a \in A$ note que a est un élément de l'ensemble A.

• $\{x : P(x)\}$ note l'ensemble des objets qui satisfont la propriété P (simple ou complexe).

Ex. :

$1 \in \{2, 1, 3\}$, *Jean* $\in$ {*Jean*, Raphaëlle, *Michèle*}, $* \in \{\circ, \wedge, \vee, \neg, *\}$, etc.

$\{x : x$ est un prénom français$\}$ = l'ensemble des prénoms français.

Soit $\mathbb{N}$ l'ensemble des entiers naturels (= $\{0, 1, 2, 3, \ldots\}$).

$\{x : x = 2$ ou $x = 4\}$ = $\{2, 4\}$.

• Le contraire de $\in$ est note $\notin$, par ex. $a \notin \{b, c, d\}$

• L'ordre n'est pas pertinent pour les ensembles : écrire $\{a, b, c\}$, $\{a, c, b\}$, $\{b, c, a\}$, $\{b, a, c\}$, $\{c, b, a\}$ ou $\{c, a, b\}$, c'est écrire la même chose.

• Il n'y a pas de répétition dans un ensemble. Ecrire $\{a, b, b\}$ est «interdit» (ce n'est pas une écriture qui correspond à un ensemble).

• Les éléments d'un ens. peuvent être eux-mêmes des ens., par ex. : $\{a, \{a, b\}\}$.

☞ La non–répétition est une notion difficile : elle correspond au fait que deux individus en tous points identiques n'en forment qu'un seul.

☞ $\{\}$ est un constructeur : il prend des objets (les éléments d'un ens.) et construit un objet plus complexe, le regroupement de ces éléments en un seul ens.

• On admettra qu'il existe un ensemble vide, noté $\emptyset$. C'est un ens. qui n'a aucun élément. Pour n'importe quel objet x, on peut donc toujours écrire $x \notin \emptyset$.

• L'identité de deux ens. est définie à partir de leurs éléments.

Définition 8 Deux ensembles A et B sont identiques ($A = B$) ssi ils ont les mêmes éléments.

Exercice 1

a. Parmi les expressions suivantes, dire quels sont ceux qui définissent des ensembles : (1) $\{a, b, c, d\}$, (2) $\{a, b, c, a\}$, (3) $\{a, \{a\}\}$, (4) $\{\emptyset, a\}$, (5) $\{\emptyset, \emptyset\}$, (6) $\{\emptyset, \{\emptyset\}\}$, (7) $\{x : x = 2\}$, (8) $\{x : x \neq x\}$, (9) $\{x : x \in \{a, a\}\}$, (10) $\{\{a, b\}, \{b, a\}\}$.

b. Indiquer les éléments des ensembles suivants : (1) $\{a, b, c\}$, (2) $\{a, \{b\}\}$, (3) $\{\emptyset\}$, (4) $\{a, b, \{b, a\}\}$, (5) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{a, \emptyset\}\}$

c. Définissons $\{x : x\,\epsilon^0 X\} =_{df} \{x : x \in X\}$ et $\{x : x\,\epsilon^1 X\} =_{df} \{x :$ il existe au moins un $y \in X$ tel que $x \in y\}$. Indiquez, pour chacun des cinq ens. précédents, quels sont les objets qui entretiennent la relation ϵ^1 avec l'ens. Par ex., $a \in \{a, b\}$ et $b\,\epsilon\{a, \{b\}\}$.

➤ Deux manières de définir un ensemble

• Définition *extensionnelle* : on énumère les éléments

• Défition *intensionnelle* : on indique une propriété caractéristique à travers l'expression $\{x : P(x)\}$. Très pratique pour les ensembles de grande taille ou infinis
Ex. :
déf. extensionnelle : $E = \{0, 2, 4\}$,
déf. intensionnelle : $E = \{x : x \in \mathbb{N} \;\&\; x < 5 \;\&$ il existe un y tel que $y \in \mathbb{N} \;\&\; x = 2y\}$ = $\{0, 2, 4\}$. Voyez–vous pourquoi ?

➤ Un peu plus de notation
«il existe un ...tel que», pas très pratique $\Rightarrow$ deux notations commodes.
• $\exists x(P(x))$ = «il existe au moins un objet qui vérifie P»,
• $\forall x(P(x) \Rightarrow Q(x))$ = «tous les objets qui vérifient P vérifient aussi Q».
• Les symboles $\exists$ et $\forall$ sont appelés des *quantificateurs*. $\exists$: quant. *existentiel*, $\forall$: quant. *universel*.
• On peut les combiner : $\exists x \exists y()$ = «il existe un x tel qu'il existe un y tel que ...», $\exists x \forall y()$ = «il existe un x tel que, pour tout y, ...». Il n'y a pas de limite à ces combinaisons (sauf qu'elles doivent être finies).

➤ Un peu plus de notation
«il existe un ...tel que», pas très pratique $\Rightarrow$ deux notations commodes.
• $\exists x(P(x))$ = «il existe au moins un objet qui vérifie P»,
• $\forall x(P(x) \Rightarrow Q(x))$ = «tous les objets qui vérifient P vérifient aussi Q».
• Les symboles $\exists$ et $\forall$ sont appelés des *quantificateurs*. $\exists$: quant. *existentiel*, $\forall$: quant. *universel*.
• On peut les combiner : $\exists x \exists y()$ = «il existe un x tel qu'il existe un y tel que ...», $\exists x \forall y()$ = «il existe un x tel que, pour tout y, ...». Il n'y a pas de limite à ces combinaisons (sauf qu'elles doivent être finies).

Exercice 2
Dans tout cet exercice, $\mathbb{N}$ désigne l'ens. des entiers naturels, c.à.d. $\{0, 1, 2, 3, \ldots\}$.
a. $\{x : x \in \mathbb{N}\}$ = ?
b. Quelle relation y–a–t–il entre $\emptyset$ et $x : x \in \mathbb{N} \;\&\; x < 0$?
c. Caractérisez l'ens. (i) des entiers inférieurs à 12, (ii) des entiers supérieurs ou égaux à 8, (iii) des entiers pairs, (iv) des entiers impairs, (v) des entiers supérieurs à 100 et inférieurs à 2000, (vi) des 400 000 premiers entiers pairs.
d. Caractérisez l'ens. des multiples de 17[1].
e. Caractérisez l'ens. des multiples entiers d'un entier pair .
☞ Aide,
f. Caractérisez l'ens. des objets plus grands que n'importe quel entier.
g. Caractérisez l'ens. des objets qui sont multiples entiers d'un entier. Quel est cet ensemble ?

h. Caractérisez l'ens. des nombres rationnels[2].
i. Caractérisez l'ens. des solutions du système d'équations suivant :
$$\begin{pmatrix} x + 2y = 3 \\ y - z \geq 2 \end{pmatrix}$$

➤ Sous–ensemble ($\subseteq$)
• Lorsque tous les éléments de A sont également des éléments de B, A est un *sous–ensemble* de B, ou A est *inclus* dans B.

Définition 9 $A \subseteq B$ note la propriété suivante : $\forall x(x \in A \Rightarrow x \in B)$.

Ex. : $\{a, b\} \subset \{a, b, c\}$
• Inclusion stricte ($\subset$) $\neq$ inclusion non–stricte ($\subseteq$) : $A \not\subset A$, $A \subseteq A$.
• Si $A \subseteq B$ et $B \subseteq A$, $A = B$ (tous les éléments de A sont des éléments de B et réciproquement, A et B ont donc les mêmes éléments.
☞ Critère d'identité pour les ensembles : deux ensembles sont identiques ssi[3] ils ont les mêmes éléments.

➤ L'ensemble vide ($\emptyset$)
• Par convention il existe un ensemble «vide», c.à.d. qui n'a aucun élément. Il est noté $\emptyset$.
• Du point de vue du critère intuitif ensemble = collection d'objets, $\emptyset$ est un peu dégénéré, mais . . .
• du point de vue du critère intuitif ensemble = domaine de validité d'une propriété, $\emptyset$ est un bon ensemble.
• $\{x : P(x) = \emptyset\}$ si aucun élément ne vérifie P. Par ex., $\{x : x \in \mathbb{N} \,\&\, x \neq x\} = \emptyset$

Exercice 3
a. Parmi les ens. suivants, dire quels sont ceux qui sont reliés par $\subseteq$, $\supseteq$ ou ni l'un ni l'autre.
1. $X = \{a, b\}$, $Y = \{a, b, c\}$,
2. $X = \{a, b\}$, $Y = \{a, \{b\}, c\}$
3. $X = \{\emptyset, \{a\}\}$, $Y = \{\{a\}\}$
4. $X = \{a, b\}$, $Y = \{b, a\}$
5. $X = \{a, \{a\}, \{\{a\}\}, \{a, \{a\}\}, \{a, \{a\}, \{\{a, \{a\}\}\}\}\}$,
$Y = \{a, \{a\}, \{\{a\}\}, \{a, \{a\}\}, \{a, \{a\}, \{\{a\}\}\}\}$

[2] Un nombre a est un multiple de b s'il existe un nombre c tel que $a = b \times c$. Par ex., 8 (= 4 × 2) est un multiple de 4.
[2] Un nombre est dit *rationnel* quand il peut être exprimé comme une fraction de forme x/y où x et y sont des entiers.
[3] La notation «ssi» abrège *si et seulement si*.

b. L'axiome de fondation dit que tout ens. non–vide a un élément minimal.
(F) $\forall x(x \neq \emptyset \Rightarrow \exists y(y \in x \,\&\, \neg\exists z(z \in x \,\&\, z \in y)))$.
Montrer que (F) implique que $x \notin x$ pour tout x.

➤ La logique classique (LC), $\Rightarrow$ et $\emptyset$
• Pb : déf. en LC de l'implication $\Rightarrow$.
• $A \Rightarrow B$ repose sur 4 possibilités A V(raie) ou F(ausse), B V ou F.
• En LC, une expression est V ou F (def.1).
• Soit un jugement universel de forme $\forall x(P(x) \Rightarrow P'(x)$, par ex. «(à cet endroit) tous les oiseaux volent». En LC c'est V ou F. C'est F si on peut trouver un *contre–exemple*, c.à.d. un oiseau qui ne vole pas.
• dans une situation où il y a un oiseau qui ne vole pas, le jugement est faux.
• dans une situation où tous les oiseaux volent le jugement est vrai.
• Et s'il n'y a pas d'oiseau ? Le jugement ne peut pas être indéterminé (def.1), il est soit V soit F. Il ne peut pas être F, parce qu'il faudrait fournir un contre–exemple = un oiseau qui ne vole pas. Donc le jugement est V.

Proposition 10 Soit ϕ une proposition universelle évaluée en LC, si s est une situation où il n'existe aucun contre-exemple à ϕ, ϕ est vrai dans s.

☞ Approfondissement. Que se passerait–il si on adoptait la convention suivante ?

Définition 11 Un jugement universel de forme «tous les objets qui possèdent la propriété P possèdent aussi la propriété P'» est vrai seulement si on peut trouver des exemples d'objets qui vérifient P', et qui, tous, vérifient Q.

Conséquence : dans une situation où aucun objet ne vérifie P, le jugement est faux. Fig. 1.1 : possibilités d'évaluation en fonction des exemples positifs et des contre–exemples.
Pour la région entourée d'un - - -, *aucun* «grand» système logique ne fait le choix décrit en 1.1 et barré par un $\times$.

☞ Le pb devient :
1. Pqoi la LC fait-elle le choix qu'elle fait ?
2. Pqoi aucun grand système ne fait–il le choix barré par $\times$?
☞ La réponse à 1 dépend de la réponse à 2.

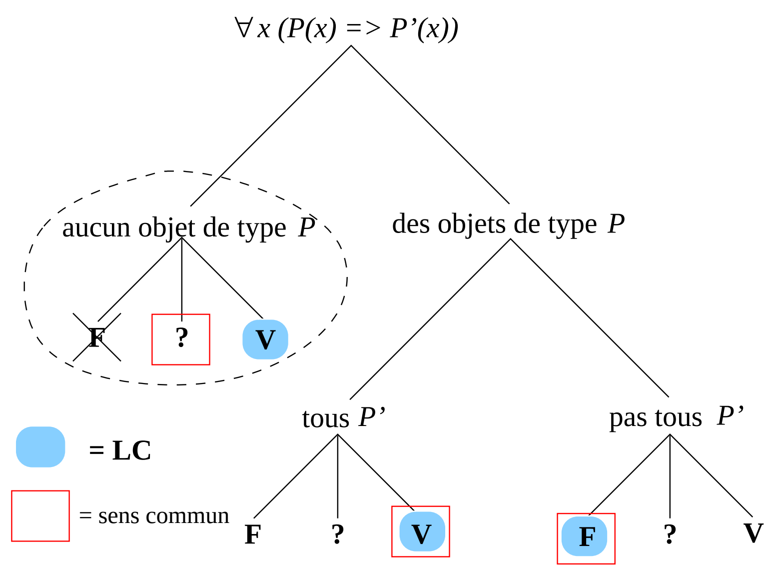

FIG. 1.1 – Exemples et contre–exemples

Réponse à 2 : ce choix serait suicidaire. Par ex. (par définition des entiers) le jugement universel «tout nombre entier pair est inférieur à (au moins) un entier» est vrai (ϕ = $\forall x(x$ est un entier pair $\Rightarrow \exists y(y$ est un entier $\& \ y > x))$.
Ensemble des (contre–)exemples : une feuille où on a écrit quelques entiers, par ex. 1, 3, 7, et 127. La feuille ne contient aucun entier pair. Alors ϕ est fausse ? On n'a pas envie de dire ça, parce qu'un jugement général ne peut pas dépendre de situations particulières (d'ens. de (contre–)exemples particuliers). Il faudrait donc interdire à $\forall$ de porter sur des propriétés générales ou avoir plusieurs $\forall$ (un pour les propriétés générales, un pour les propriétés particulières, etc.).
☞ Plus généralement, ce n'est pas une bonne idée de dire : «si j'ai $p \Rightarrow p'$, et si p est fausse, alors $p \Rightarrow p'$ est fausse». Pourquoi ? Parce que cette règle nous forcerait à admettre comme fausses des implications où il y a une vraie connexion conceptuelle entre p et p'.
Par ex., `Il existe un nombre impair divisible par 2` $\Rightarrow$ `Il existe un nombre divisible par 2` est intuitivement «vrai», parce que s'il y a un nombre impair divisible par 2, disons le nombre 17, alors il existe un nombre divisible par 2 (17 lui-même).
De même `Jean a une voiture` $\Rightarrow$ `Jean a un véhicule` est intuitivement «vrai», même si Jean ne possède aucune voiture.
☞ C'est pourquoi aucune logique n'attribue *systématiquement* la valeur F à une implication dont la partie gauche est fausse. *Mais* il peut arriver (ça dépend des logiques) que l'implication soit fausse pour des propositions données. Elle n'est pas *systématiquement* fausse, c.à.d. qu'elle n'est pas fausse quelle que soit la proposition de gauche.
Par ex. la logique dite «pertinente» (*relevance logics*, Anderson & Belnap 1975) fait dépendre la valeur de vérité de la connexion conceptuelle entre les propositions. En gros $p \rightarrow p'$ est F quand p et p' n'ont pas de rapport. Quand il y a une vraie connexion conceptuelle, $p \rightarrow p'$ est vraie.

`Un nombre impair est divisible par 2` $\rightarrow$ `Il existe un nombre divisible par 2`	V	la proposition de gauche est F
`Un nombre impair est divisible par 2` $\rightarrow$ `La lune est une planète`	F	

dans les deux cas

☞ Si on en revient à 1.1, reste donc ? ou V à l'intérieur de - - -. ? serait possible quand il n'y aucun objet de type P dans *aucune* situation. Par ex., «tout cercle carré est rouge» serait ? parce qu'on est incapable de construire un cercle carré. Mais, en LC, ? n'existe pas, F est suicidaire. Il ne reste que V.
• Finalement, en LC, chaque fois qu'une propriété va décrire l'ensemble vide $\emptyset$, elle va impliquer *n'importe quelle* propriété !
Parce qu'on va retomber sur une forme $\forall x P(x) \Rightarrow P'(x)$ avec $\{x : P(x)\} = \emptyset$.
• Montrer que $\emptyset \subseteq A$ pour tout ensemble A (solution).

➤ Les propriétés de l'implication $\Rightarrow$ en LC
• Si p et p' sont des propositions $p \Rightarrow p'$ n'est fausse que dans un seul cas : si p est vraie et p' fausse.
• Alors quand p est F, $p \Rightarrow p'$ est vraie ? Oui, fondamentalement pour les mêmes raisons que celles qu'on vient de voir à propos de $\emptyset$.
• Table de vérité de l'implication

p	p'	$p \Rightarrow p'$
V	V	V
F	V	V
F	F	V
V	F	F

➤ La démonstration par l'absurde
• Pour démontrer quelque chose en utilisant les val. de vérité, on peut fabriquer des démonstrations par l'absurde. Pour démontrer que $p \Rightarrow p'$, on suppose que p est vrai et que p' est fausse. C'est le seul cas où $p \Rightarrow p'$ peut être fausse. Si ce cas est impossible, alors $p \Rightarrow p'$ est «toujours» vrai. Ici, «toujours» = quelles que soient les val. de vérité de p et de p'.

• Comment est–ce qu'on sait qu'un cas est «impossible» ? Lorsqu'on en arrive à affirmer et à nier une même proposition. En LC, c'est impossible puisqu'une même proposition ne peut pas être à la fois vraie et fausse.
• Exemples. On voudrait démontrer les trois propriétés fondamentales de $\subseteq$.

Proposition 12 $\subset$ est réflexive : $A \subseteq A$ pour tout ens. A
$\subseteq$ est transitive : si $A \subseteq B$ et $B \subseteq C$, alors $A \subseteq C$.
$\subseteq$ est antisymétrique : si $A \subseteq B$ et $B \subseteq B$, alors $A = B$.

Preuve (par l'absurde)
La réflexivité. D'après (9), la réflexivité signifie $\forall x(x \in A \Rightarrow x \in A)$. Donc il faut montrer que, pour n'importe quel x, on a l'implication $x \in A \Rightarrow x \in A$. Il n'y a qu'un seul cas où ça peut être faux : quand $x \in A$ et $x \notin A$. Mais, en LC, on ne peut pas avoir à la fois $x \in A$ et $x \notin A$.
La transitivité. Supposons qu'on ait $A \subseteq B$, $B \subseteq C$, mais pas $A \subseteq C$. Alors il y a un x tel que $x \in A$ mais $x \notin C$. Puisque $x \in A$, $x \in B$ (à cause de $A \subseteq B$). Puisque $x \in B$ $x \in C$ (à cause de $B \subseteq C$). Alors $x \in C$ et $x \notin C$.
L'antisymétrie. Pour que deux ensembles soient égaux (def. 8), il faut et il suffit qu'ils aient les mêmes éléments. Supposons que $A \subseteq B$ et que $B \subseteq$. A et B seraient $\neq$ ssi il y avait un élément qui appartienne à A mais pas à B, ou l'inverse. Mais c'est impossible (à cause de $A \subset B$ et $B \subset A$).

☞ Est-ce que toute démonstration d'une propriété de forme $p \Rightarrow p'$ à base de valeurs de vérité n'est pas une démonstration par l'absurde ? En fait, oui. On aboutit toujours soit à supposer que p est F (et $p \Rightarrow p'$ est alors vrai quelle que soit la valeur de vérité de p'), soit à supposer que p

est vrai et à montrer que p' ne peut pas être faux (parce que ça entraînerait une contradiction). Un exemple un peu déconcertant :
Prouver que $p \Rightarrow p$. Si p est F, c'est V. Si p est V c'est V parce que P ne peut pas être à la fois V et F. La plupart du temps, ces micro-dém. par l'absurde sont faites machinalement, sans qu'on les remarque.

➤ Opérations sur les ensembles
• L'intersection de deux ensembles ($\cap$) est l'ensemble des éléments qu'ils ont en commun.
• L'union de deux ensembles ($\cup$) est l'ensemble des éléments qui figurent dans l'un ou dans l'autre ou dans les deux.

Définition 13 $A \cap B =_{df} \{x : x \in A \,\&\, x \in B\}$.
$A \cup B =_{df} \{x : x \in A \,\vee\, x \in B\}$.

☞ Ces opérations sont définies sur des *ensembles*. On ne peut donc pas les utiliser sur des éléments (qui n'ont eux-mêmes aucun éléments). Par exemple, $\{a, b\} \cup \{c\} = \{a, b, c\}$, mais si $\{x : x \in c\} = \emptyset$, $\{a, b\} \cup c$ n'est pas défini.
☞ Le produit et l'intersection sont des opérations *commutatives*. Autrement dit, $A \cap B = B \cap A$ et $A \cup B = B \cup A$.

Définition 14 Une opération o est commutative lorsque, pour tous les termes a et b auxquelles elle s'applique, $a\; o\; b = b\; o\; a$.

Exercice 4
a. $\{a, b, c\} \cap \{a, d, e, c\}$ = ?, $\{a, b, c\} \cup \{a, d, e, c\}$ = ?
b. Montrer que $A \cap A = A \cup A = A$
c. Montrer que $A \cap B \subseteq A$.
d. Montrer que si $A \subseteq B$, $A \cap C \subseteq B \cap C$.
e. Se servir de (c) et (d) pour montrer que $A \cap B = B$ ssi $B \subseteq A$.
f. Montrer d'une manière analogue que $A \cup B = B$ ssi $A \subseteq B$.

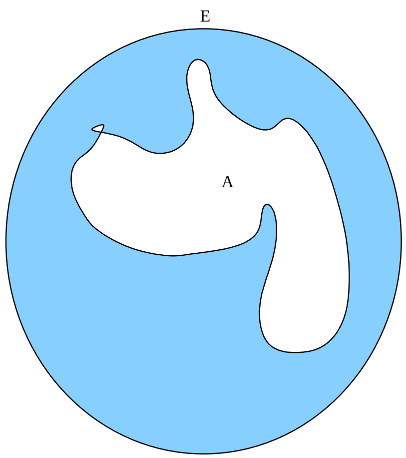

FIG. 1.2 – Le complémentaire de A dans E

Exercice 5
a. Montrer que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ d'une manière «intelligente» (sans procéder par l'absurde).
Suggestion
b. Montrer que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ d'une manière intelligente.
c. Montrer les deux précédents résultats d'une manière mécanique (en procédant par l'absurde).

➤ Complémentaire d'un ens.
• Soit un ensemble E, le *complémentaire* de A dans E est l'ens. des élements qui appartiennent à E mais n'appartiennent pas à A. On note cet ensemble $C_E A$, dans la figure ci-dessus, c'est la zone grisée.

Définition 15 $C_E(A) =_{df} \{x : x \in E \;\&\; x \notin A\}$

Lorsqu'on n'a pas besoin de préciser E, on peut se contenter de noter le complémentaire de A par $-A$.

Définition 16 $-A =_{df} \{x : x \notin A\}$. $A - B = \{x : x \in A \;\&\; x \notin B\}$

Exercice 6
a. quel est le complémentaire de E dans E, autrement dit, $C_E(E) = ?$, de même $C_E(\emptyset) = ?$
b. $-(A \cup B) = ?$ Suggestion
c. $-(A \cap B) = ?$

➤ Ensemble des parties d'un ensemble. Produit cartésien
• L'ens. des parties d'un ens. A, noté $\wp(A)$, $\wp(A)$ est l'ensemble des sous–ensembles de A

Définition 17 $\wp(A) =_{df} \{X : X \subseteq A\}$

. • Attention au fait que $\wp(A)$ est un ens. pas un élément. Etant donné que, pour tout A, $\emptyset \subseteq A$ et $A \subseteq A$, on a toujours $\emptyset \in \wp(A)$ et $A \in \wp(A)$.

Exercice 7
a. $\wp(\{a, b\}) =?$
b. $\wp(\{a\}) =?$
c. $\wp(\{\{a\}\}) =?$
d. $\wp(\emptyset) =?$
e. $\wp(\{\emptyset\}) =?$
f. $\wp(\{\emptyset, \{a\}\}) =?$
g. $\wp(\{a, \{\emptyset\}\}) =?$

Exercice 8
On définit :
. $\wp^0(A) = A$
. $\wp^1(A) = \wp(A)$
. $\wp^n(A) = \wp(\wp^{n-1}(A))$.
a. Calculez $\wp^2(\{a, b\})$.
b. Calculez $\wp^3(\{a\})$.

Exercice 9
a. Montrer que $\wp(A \cap B) = \wp(A) \cap \wp(B)$. Suggestion
b. Est-ce que $\wp(A \cup B) = \wp(A) \cup \wp(B)$. c. Est-ce que $\wp(-A) = -\wp(A)$?

• Paire ordonnée. Bien que les ensembles ne soient pas ordonnées, il est possible de simuler des séquence ordonnées de la manière suivante.

Définition 18 La *paire ordonnée* $\langle a, b\rangle$ est définie comme l'ensemble $\{\{a\}, \{a, b\}\}$.

A partir de la définition 18, on peut définir les séquences ou listes finies : . $\langle\rangle = \emptyset$,
. $\langle x_1 \dots x_n\rangle = \langle x_1, \langle x_2 \dots x_n\rangle\rangle$.
Par exemple $\langle x_1, x_2, x_3\rangle = \langle x_1, \langle x_2, x_3\rangle\rangle = \{\{x_1\}, \{x_1, \langle x_2, x_3\rangle\}\} = \{\{x_1\}, \{x_1, \{\{x_2\}, \{x_2, x_3\}\}\}\}$.

• Produit cartésien. Le *produit cartésien* de deux ensembles est l'ensemble des paires ordonnées composées chacune d'un élément du premier ensemble suivi d'un élément du deuxième ensemble.

Définition 19 Le produit cartésien de A et B, noté $A \times B$ est défini par :
$A \times B =_{df} \{\langle x, y\rangle : x \in A \,\&\, y \in B\}$

• Le p.c. n'est pas commutatif (voir def. 14). Par ex., $\{a, b\} \times \{a\} = \{\langle a, a\rangle, \langle b, a\rangle\}$, mais $\{a\} \times \{a, b\} = \{\langle a, a\rangle, \langle a, b\rangle\}$.

Exercice 10
a. Calculer le p.c. $\{a, b, c\} \times \{b, a\}$.
b. Calculer le p.c. $\{a, b, c\} \times \{a, \{b\}\}$.
c. Calculer le p.c. $\{a, b\} \times \emptyset$.
d. Calculer le p.c. $\{a, b\} \times \{\emptyset\}$.
e. Calculer le p.c. $(\{a, b\} \times \{c\}) \times \{d, e\}$.

➤ Fonction
• En théorie des ens., une fonction n'est pas autre chose qu'un ensemble de paires ordonnées.

Définition 20 Une fonction f de domaine E, où E est un ensemble, est un ensemble f de paires ordonnées tel que chaque élément de E figure une et une seule fois dans une paire $\langle x, y\rangle \in f$.

La déf. correspond à l'idée intuitive de fonction : un même argument ne peut recevoir qu'une seule valeur. Dans les paires ordonnées, le premier élément est l'argument de la fonction, l'élément de droite sa valeur pour l'argument considéré. On ne peut donc pas avoir $f = \{\dots\langle x,y\rangle\dots\langle x,z\rangle\dots\}$ avec $y \neq z$, car, dans ce cas, un même argument (x) aurait deux valeurs distinctes (y et z).
En revanche des arguments différents peuvent avoir la même valeur.

• Il est nécessaire[4] dans un certain nombre de cas de repérer une fonction non seulement par son domaine mais aussi par son *codomaine*. En fait on caractérise ainsi une classe de fonctions.

Définition 21 On écrit $f : E \rightarrow F$ pour indiquer que le domaine de f est E et que pour chaque x_inE, $f(x) \in F$. F est appelé *codomaine* de f. On dit que f est de *type* $E \rightarrow F$.

• Une fonction a en général plusieurs types, puisque si la fonction est de type $E \rightarrow F$, elle est également de type $E \rightarrow F'$ pour tout $F' \supseteq F$.
• Exemples. Soit +2 l'opération qui consiste à ajouter 2 à un nombre. Supposons que la fonction f_{+2} a $\{1,4\} \rightarrow \{3,6,111,5\}$ parmi ses types. Elle a également n'importe quel type $\{1,4\} \rightarrow E$ parmi ses types du moment que $\{3,6,111,5\} \subseteq E$.
☞ On peut définir le type minimal d'une fonction f de domaine E de la manière suivante : c'est le type $E \rightarrow F$ tel que $F = \{y : \exists x(x \in E \;\&\; f(x) = y)\}$. Par exemple, le type minimal de f_{+2} est $\{1,4\} \rightarrow \{3,6\}$.

1.3 Ordinaux et cardinaux

➤ Comment peut–on mesurer des ensembles ?
• Pour des ens. finis, on prendre le nombre d'éléments de l'ens. Le «nombre» d'éléments d'un ens. (qu'il soit fini ou pas) s'appelle le *cardinal* de l'ensemble et se note $CARD$ ou || ||. Par ex., $||\{a,b,c,\{a,f\}\}||$ = 4.

Définition 22 Le *cardinal* d'un ens. A, noté $CARD(A)$ ou $||A||$ est le nombre d'éléments de A.

• Évidemment, (22) est plutôt circulaire car nous n'avons aucune idée, en théorie des ens., de ce que signifie le «nombre» des éléments d'un ens., même fini. Le problème se pose à peu près ainsi : comment définit–on «compter» en théorie des ens. ?
• D'abord on peut remarquer que, pour deux ens. finis, ils ont le même nombre d'éléments si l'on peut définir une correspondance terme à terme entre les deux.

[4] Ça n'est pas une notion techniquement très facile en fait, beaucoup moins qu'elle n'en a l'air.

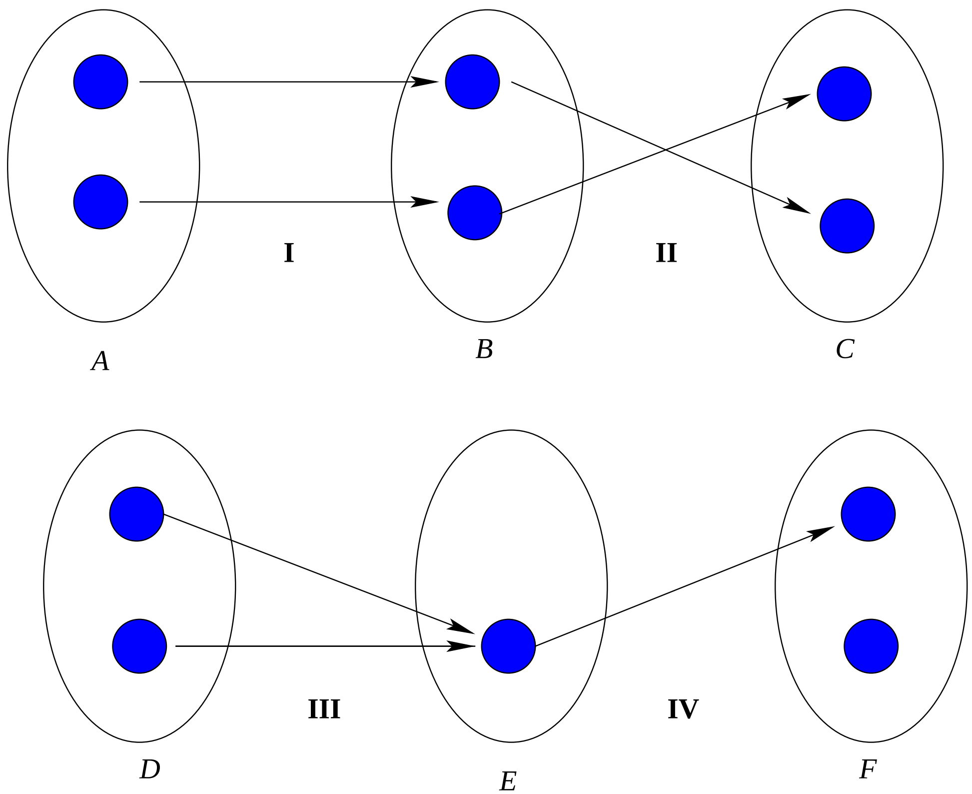

FIG. 1.3 – Un exemple de bijection

➤ Cela nous conduit à la première notion dont nous avons besoin, celle de *bijection*.

• On a vu dans la définition (20) comment on définissait une fonction en théorie des ens. : comme un ens. de paires ordonnées.

• Si nous avons deux ens. $\{a_1 \ldots a_n\}$ et $\{b_1 \ldots b_n\}$, il nous faudrait une fonction qui pour a_1 sélectionne un élément unique b_i de $\{b_1 \ldots b_n\}$, de même pour a_2, a_3, $\ldots a_n$.

• Par simplicité, raisonnons sur deux éléments, nous voulons une situation comme I ou II, pas III ou IV.

III n'est pas une bonne fonction parce qu'elle fait correspondre un ens. plus petit (E) à un ens. plus grand (D). IV n'est pas une bonne fonction parce qu'elle fait correspondre un ens. plus grand (F) à un ens. plus petit (E).

• La cause de ces problèmes est que :
– III associe un même élément de E à deux éléments différents de D,
– IV «oublie» un élément de F.
• une bijection est une fonction qui sépare les éléments de l'ensemble–source et n'oublie aucun élément de l'ensemble–cible.

Définition 23 Soit deux ensembles E et F
1. Une fonction f de type $E \rightarrow F$ est *injective* par rapport à ce type ssi $\forall x, y((x \in E \,\&\, y \in E \,\&\, x \neq y) \Rightarrow f(x) \neq f(y)$. On dit aussi que c'est une injection de E vers F.
2. Elle est *surjective* par rapport à ce type ssi $\forall y(y \in F \Rightarrow \exists x(y \in E \,\&\, f(y) = x))$. On dit que c'est une surjection de E vers F.
3. Elle est *bijective* par rapport à ce type ssi elle est à la fois injective et surjective par rapport à ce type. On dit aussi que c'est une bijection entre E et F.

• Pour les ens. finis, on peut démontrer que l'existence d'une bijection entre deux ens. implique que ces deux ens. ont le «même nombre d'éléments», dans l'acception suivante. Supposons qu'on ait deux ens. E et E' non–vides, si, en retirant un élément de chaque ens. alternativement, on arrive au même moment à l'ensemble vide, les deux ens. ont le même nombre d'éléments.
• Supposons qu'il existe deux ens. E et E' non–vides et une bijection f entre les deux. Considérons E et convenons de retirer à chaque fois un élément de $x \in E$ et son image par la bijection, $f(x) \in E$. Supposons (preuve par l'absurde) qu'on n'arrive pas à vider E et E' au même moment. Il y a deux possibilités.
1. On vide E avant E' ; il va donc rester un $y \in E'$ alors que E est vide. Puisque f est une bijection, c'est en particulier une surjection (23). Cela implique qu'il existe un $x \in E$ tel que $y = f(x)$. Comme on a vidé E, on a, en particulier, supprimé x ; donc y aurait dû être supprimé aussi.
2. On vide E' avant E ; il va donc rester un $x \in E$, alors que E' est vide. Considérons $y = f(x) \in E'$. Il a été supprimé, par hypothèse. Donc, on a, à un certain moment, choisi un $z \in E$ tel que $f(z) = y$. Si $z \neq x$, f n'est pas une bijection, puisqu'elle viole la condition d'injectivité. Donc $z = x$; mais alors x aurait dû être supprimé.

➤ Les ens. infinis
• Peut–on utiliser les bijections pour dire que deux ens. infinis ont «le même nombre» d'éléments ?
• La réponse semblerait plutôt négative. Par exemple, considérons l'ens. des entiers, $\mathbb{N}$, et l'ens. des entiers pairs $\mathbb{N}_p$. Il est clair que $\mathbb{N}p \subset \mathbb{N}$, par exemple $3 \in \mathbb{N}$ mais $3 \notin \mathbb{N}_p$. Cependant, nous pouvons définir une bijection entre $\mathbb{N}$ et $\mathbb{N}_p$, par exemple, la bijection correspondant à $f(x) = 2x$ pour $x \in \mathbb{N}$ (donc $f(0) = 0$, $f(1) = 2$, etc.).

1.4 Solutions des exercices

Exercice 1a
. (1) définit un ens.,
. (2) ne définit pas un ens. (répétition),
. (3) définit un ens.,
. (4) définit un ens.,
. (5) ne définit pas un ens. (répétition),
. (6) définit un ens.,
. (7) définit un ens., l'ens. $\{2\}$,
. (8) définit un ens., l'ens. vide $\emptyset$,
. (9) ne définit pas un ens. (répétition).
. (10) ne définit pas un ens. car $\{a, b\}$ = $\{b, a\}$ (donc répétition).

Exercice 1b
(1) : a, b, c, (2) : $a, \{b\}$, (3) $\emptyset$, (4) $a, b, \{b, a\}$, (5) $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{a, \emptyset\}$

Exercice 1c
(1) : rien n'entretient la relation ϵ avec l'ens., (2) : b, (3) : rien du tout, (4) a et b, (5) : $\emptyset$, $\{\emptyset\}$ et a.

• Si on analyse la formule compliquée à droite du signe :, on voit qu'elle demande de considérer tous les x qui :
1. sont des entiers ($\in \mathbb{N}$),
2. sont inférieurs à 5,
3. tels qu'il existe un autre entier y tel que x vaut deux fois y.

C'est le point (3) qui est un peu difficile : parcourons les entiers dans leur ordre «naturel» et essayons toutes les possibilités pour y et de voir, à chaque fois, si ça nous donne une possibilityé pour x, compte tenu des contraintes qui nous sont imposées.
– $y = 0$, alors $x = 2 \times 0 = 0$, 0 est un entier et est inférieur à 5, donc c'est un des x possibles.
– $y = 1$, alors $x = 2$ et c'est encore un des x possibles,
– $y = 2$, $x = 4$, même remarque,
– $y = 3$, $x = 6$, ça ne va pas parce que x doit être < 5.

Clairement, toutes les valeurs de y supérieures à 2 vont produire des x supérieurs à 5, ce qu'on ne veut pas.
Les trois seuls candidats restant sont donc 0, 2, et 4, les trois premiers nombres pairs.

Exercice 2a

$\mathbb{N}$ lui-même

Exercice 2b
$\emptyset = \{x : x \in \mathbb{N} \,\&\, x < 0\}$.

Exercice 2c
(i) $\{x : x \in \mathbb{N} \,\&\, x < 12\}$
(ii) $\{x : x \in \mathbb{N} \,\&\, x \geq 8\}$
(iii) $\{x : x \in \mathbb{N} \,\&\, \exists y(y \in \mathbb{N} \,\&\, x = 2y)\}$
(iv) $\{x : x \in \mathbb{N} \,\&\, \exists y(y \in \mathbb{N} \,\&\, x = 2y + 1)\}$
(v) $\{x : x \in \mathbb{N} \,\&\, 100 < x < 2000\}$
(vi) $\{x : x \in \mathbb{N} \,\&\, \exists y(y \in \mathbb{N} \,\&\, x = 2y \,\&\, x < 400001\}$

Exercice 2d
$\{x : \exists y(y \in \mathbb{N} \,\&\, x = 17y)\}$
☞ Il n'est pas nécessaire de spécifier que $x \in \mathbb{N}$ parce que tout multiple d'un entier est lui-même un entier. D'ailleurs, on ne le demande pas dans la question.

Aide de 2e
Vous avez besoin de dire quelque chose comme : l'ensemble des objets x tels qu'il existe un objet y qui est pair (vous savez comment dire ça) et un entier u tel que x est le produit de u et de y.

Exercice 2e
$\{x : \exists y(\exists z(z \in \mathbb{N} \;\&\; y = 2z) \;\&\; \exists u(u \in \mathbb{N} \;\&\; x = uy))\}$

Exercice 2f
$\{x : \forall y(y \in \mathbb{N} \Rightarrow x > y\}$

Exercice 2g
$\{x : \exists y \exists z(y \in \mathbb{N} \,\&\, z \in \mathbb{N} \,\&\, x = yz\}$ = $\mathbb{N}$

Exercice 2h
$\{x : \exists y \exists z(y \in \mathbb{N} \,\&\, z \in \mathbb{N} \,\&\, x = y/z\}$

Exercice 2i
$\{\{x, y, z\} : x + 2y = 3 \,\&\, y - z \geq 2\}$

Solution
Il faut se servir de la déf. 9. $x \in \emptyset$ est faux pour tout x, donc $x \in \emptyset \Rightarrow x \in A$ est vrai pour tout x et pour tout Aů Donc, d'après cette déf. $\emptyset \subseteq A$.

Exercice 3a.
1. $X \subseteq Y$
2. ni l'un ni l'autre
3. $Y \subseteq X$
4. les deux ($X = Y$)
5. ni l'un ni l'autre

Exercice 3b.
a. Si $x = \emptyset$, $x \notin x$ (sans quoi $\emptyset$ aurait un élément). b. Supposons que $x \neq \emptyset$. Considérons $\{x\}$. Comme x n'est pas vide, il obéit à l'axiome de fondation (F). Si $x \in x$, l'ensemble $\{x\}$ viole (F). Donc $x \notin x$.

Exercice 4a
$\{a, b, c\} \cap \{a, d, e, c\} = \{a, c\}$, $\{a, b, c\} \cup \{a, d, e, c\} = \{a, b, c, d, e\}$

Exercice 4b
Si $x \in A \cap A$, $x \in A$. Inversement, si $x \in A$, $x \in A \cap A$; donc A et $A \cap A$ ont les mêmes éléments, et, donc, sont identiques (8). Idem pour $A \cup A$

Exercice 4c
Si $x \in A \cap B$, $x \in A$ (par déf.). De même, si $x \in A$, $x \in A \cup B$.

Exercice 4d
Si $x \in A \cap C$, $x \in A$ et $x \in C$, puisque $x \in A$ $x \in B$, donc $x \in B \cap C$.

Exercice 4e
Si $A \cap B = B$, alors comme $A \cap B \subseteq A$ (par (c)), on a $B \subseteq A$. Inversement, si $B \subseteq A$, $B \cap B \subseteq A \cap B$ par (d). Mais $B \cap B = B$.

Exercice 4f
On utilise les deux propriétés (1) $A \subseteq A \cup B$ et (2) si $A \subseteq B$, $A \cup C \subseteq B \cup C$. Si $A \cup B = B$, comme $A \subseteq A \cup B$ par (1), $A \subseteq B$. Inversement, si $A \subseteq B$, par (2) on a $A \cup B \subseteq B \cup B$.

Suggestion pour l'exercice 5a
Vous aurez besoin de la propriété suivante :
Si $X \subseteq Y$, $X \cap Z \subseteq Y \cap Z$.
Démonstration.
Pour l'exercice 5b, vous aurez besoin d'une propriété analogue :
Si $X \subseteq Y$, $X \cup Z \subseteq Y \cup Z$.
Démonstration

Démonstration
Supposons que $X \subseteq Y$. Soit $x \in X \cap Z$, alors $x \in X$ et $x \in Z$. Mais, par hypothèse, si $x \in X$, $x \in Y$. Donc $x \in Y$ et $x \in Z$, donc $x \in Y \cap Z$.

Démonstration de la propriété pour $\cup$.
Supposons que $X \subseteq Y$. Soit $x \in X \cup Z$. Si $x \in X$, alors, par hypothèse, $x \in Y$, donc $x \in Y \cup Z$. Si $x \in Z$, de nouveau, $x \in Y \cup Z$. Donc $x \in Y \cup Z$ dans les deux cas.

Remarque
On peut également prouver (cela sera utile plus tard) que si $X \subset Y$ et $X' \subseteq Z$, $X \cap X' \subseteq Y \cap Z$. Si $x \in X \cap X'$, $x \in X$ et $x \in X'$, donc $x \in Y$ et $x \in Z$, donc $x \in Y \cap Z$.
On prouverait d'une manière analogue que $X \subset Y$ et $X' \subseteq Z$, $X \cup X' \subseteq Y \cup Z$

Exercice 5a
Si $x \in A \cap (B \cup C)$, $a \in A$. S'il n'appartient pas à $(A \cap B) \cup (A \cap C)$, il n'appartient à aucun des deux termes. Comme $\in A$ il faut qu'il n'appartienne ni à B ni à C, mais c'est impossible par hyp.
Inversement On $B \subseteq B \cup C$ et $C \subset B \cup C$. Donc $A \cap B \subseteq A \cap (B \cup C)$ (pourquoi ?, voir page suivante) et la même chose pour $A \cap C$, donc $(A \cap B) \cup (A \cap C) \subseteq (A \cap (B \cup C) \cup A \cap (B \cup C)$ = $A \cap (B \cup C)$.

Pourquoi ?
Parce que, en vertu de ce qu'on a démontré ici, si $B \subseteq B \cup C$ $A \cap B \subseteq A \cap (B \cup C)$ (c'est de la forme : si $X \subseteq Y$, $X \cap Z \subseteq Y \cap Z$.
Retour à l'exercice principal.

Exercice 5b
Puisque $B \cap C \subseteq B, C$ on a $A \cup (B \cap C) \subseteq A \cup B, A \cup C$, donc $(A \cup (B \cap C)) \cap (A \cup (B \cap C)) \subseteq (A \cup B) \cap (A \cup C)$.
Inversement, soit $(A \cup B) \cap (A \cup C)$. Par le résultat précédent cette expression est égale à $((A \cup B) \cap A) \cup ((A \cup B) \cap C))$, et le deuxième terme de cette intersection est égale à $(A \cap B) \cup (B \cap C)$. Or, on a : $(A \cup B) \cap A \subseteq A$ et $A \cap C \subseteq A$, donc :
$((A \cup B) \cap A) \cup (A \cap C) \cup (B \cap C) \subseteq A \cup (B \cap C)$.

Exercice 5c, première partie
Soit $x \in A \cap (B \cup C)$, alors :
1. $x \in A$,
2. $x \in B \cup C$.
Supposons que :
(α) $x \notin (A \cap B) \cup (A \cap C)$, alors :
3. $x \notin A \cap B$, et
4. $x \notin A \cap C$.
Puisque (3), alors :
3a. $x \notin A$ ou,
3b. $x \notin B$, ou,
3c (3a) + (3b).
(3a) est impossible car on a (1) par hyp. De même (3c) est impossible.
Il reste (3b).
Puisque (4), alors :
4a. $x \notin A$ ou,
4b. $x \notin C$, ou,
4c (4a) + (4b).
(4a) et (4c) sont impossibles car on a (1) par hyp. Il reste (4b). Mais (3a) + (3b) produisent $x \notin B \cup C$, ce qui contredit (2). Donc (α) est faux.
On a prouvé que : si $x \in A \cap (B \cup C)$, alors $x \in (A \cap B) \cup (A \cap C)$
On cherche maintenant à prouver l'inverse.
Soit $x \in (A \cap B) \cup (A \cap C)$, alors :
1. $x \in A \cap B$, ou
2. $x \in A \cap C$.
Supposons que :
(β) $x \notin A \cap (B \cup C)$, alors :

3a. $x \notin A$, ou
3b. $x \notin B \cup C$, ou
3c. (3a) + (3b).
Par (1) on a $x \in A$, donc (3a) et (3c) sont impossibles.
Puisque (3b), alors : 4. $x \notin B$, et
5. $x \notin C$.
(4) et (5) entraînent que $x \notin A \cap B$ et que $x \notin A \cap C$, mais on doit avoir l'un des deux au moins car on a (1) ou (2). Donc (β) est faux.

Exercice 5c, deuxième partie
Soit $x \in A \cup (B \cap C)$, alors :
1a. $x \in A$, ou 1b. $x \in B \cap C$, ou
1c. (1a) + (1b).
Supposons que :
(α) $x \notin (A \cup B) \cap (A \cup C)$, alors :
2a. $x \notin A \cup B$, ou
2b. $x \notin A \cup C$, ou
2c. (2a) + (2b). Si (2a) on a $x \notin A$ et $x \notin B$. Puisque $x \notin A$, on n'a ni (1a) ni (1c). Il reste (1b), amis (1b) implique $x \in B$ et nous venons de déduire de (2a) que $x \notin B$. Donc (2a) est impossible.
(2c) est impossible aussi puisqu'il implique (2a).
Reste (2b) qui implique $x \notin A$ et $x \notin C$. Cela exclut (1a) et (1c). Il reste (1b) mais (1b) implique $x \in C$ alors que (2b) implique le contraire.
Donc (α) est contraire à l'hyp.
Inversement, supposons que $x \in (A \cup B) \cap (A \cup C)$, alors :
1. $x \in A \cup B$ et
2. $x \in A \cup C$.
Supposons que :
(β) $x \notin A \cup (B \cap C)$, alors :
3. $x \notin A$ et
4. $x \notin B \cap C$.
(3) et (1) impliquent que $x \in B$. (3) et (2) impliquent que $x \in C$. Donc $x \in B \cap C$, ce qui contredit (4). Donc (β) est impossible.

Exercice 6a
$C_E(E) = \emptyset$, $C_E(\emptyset) = E$.

Suggestion pour 6b
Si vous ne voulez pas une preuve totalement mécanique, montrer que si $A \subseteq B$, $-B \subseteq -A$.

Exercice 6b
On commence par montrer que si $A \subseteq B$, $-B \subseteq -A$.
Si $x \in -B$, $x \notin B$ par définition (16). Supposons que $x \in A$, alors on aurait un objet (x) qui appartient à A mais pas à B. Mais c'est impossible parce qu'on a supposé que $A \subseteq B$.
On a $A \subseteq A \cup B$ et $B \subseteq A \cup B$, donc $-(A \cup B) \subseteq A$ et $-(A \cup B) \subseteq B$. Donc $-(A \cup B) \subseteq -A \cap -B$. Inversement, si $x \in -A \cap -B$, alors $x \in -A$ et $x \in -B$, donc $x \notin A$ et $x \notin B$. Supposons que $x \in A \cup B$, alors $x \in A$ ou $x \in B$ ou le sdeux, mais c'est impossible, donc $x \notin A \cup B$ et $x \in -(A \cup B)$.

Exercice 6c
$-A \subset -(A \cap B)$ et $-B \subseteq -(A \cap B)$, donc $-A \cup -B \subseteq -(A \cap B)$. Inversement si $x \notin A \cap B$, $x \notin A$ ou $x \notin B$. Donc $x \in -A \cup -B$

Exercice 7a
$\{\emptyset, \{a, b\}, \{a\}, \{b\}\}$

Exercice 7b
$\{\emptyset, \{a\}\}$

Exercice 7c
$\{\emptyset, \{\{a\}\}\}$

Exercice 7d
$\{\emptyset\}$

Exercice 7e
$\{\emptyset, \{\emptyset\}\}$

Exercice 7f
$\{\emptyset, \{\emptyset, \{a\}\}, \{\emptyset\}, \{\{a\}\}\}$

Exercice 7g
$\{\emptyset, \{a, \{\emptyset\}\}, \{\emptyset\}, \{a\}, \{\{\emptyset\}\}\}$

Exercice 8a
$\wp^2(\{a, b\}) = \wp(\wp^1(\{a, b\})) = \wp(\wp(\{a, b\}))$ =
$\wp(\{\emptyset, \{a, b\}, \{a\}, \{b\}\})$ =
$\{\emptyset, \{\emptyset, \{a, b\}, \{a\}, \{b\}\},$
$\{\emptyset\}, \{\{a, b\}\}, \{\{a\}\}, \{\{b\}\},$
$\{\emptyset, \{a, b\}\}, \{\emptyset, \{a\}\}, \{\emptyset, \{b\}\},$
$\{\{a, b\}, \{a\}\}, \{\{a, b\}\{b\}\}, \{\{a\}, \{b\}\}\}$

Exercice 8b
$\wp^3(\{a\}) = \wp(\wp^2(\{a\} = \wp(\wp(\wp(\{a\})))$ =
$\wp(\wp(\{\emptyset, \{a\}\})) = \wp(\{\emptyset, \{\emptyset, \{a\}\}, \{\emptyset\}, \{\{a\}\}\})$ =
$\{$
$\emptyset, \{\emptyset, \{\emptyset, \{a\}\}, \{\emptyset\}, \{\{a\}\}\},$
$\{\emptyset, \{\emptyset, \{a\}\}\},$
$\{\emptyset, \{\emptyset\}\},$
$\{\emptyset, \{\{a\}\}\},$

$\{\{\emptyset, \{a\}\}, \{\emptyset\}\},$
$\{\{\emptyset, \{a\}\}, \{\{a\}\}\},$
$\{\{\emptyset\}, \{\{a\}\}\}$
$\}$

Suggestion pour l'exercice 9a
Montrer que si $A \subseteq B$, $\wp(A) \subseteq \wp(B)$
Soit $A \subseteq B$ et $x \in \wp(A)$, alors $x \subseteq A$ par déf. Donc $x \subseteq B$ et $x \in \wp(B)$.

Exercice 9a
On a $A \cap B \subseteq A$ et $A \cap B \subseteq B$. Donc $\wp(A \cap B) \cap \wp(A \cap B) \subseteq \wp(A) \cap \wp(B)$ (se souvenir de cette remarque). Donc $\wp(A \cap B) \subseteq \wp(A) \cap \wp(B)$.
Inversement, soit $x \in \wp(A) \cap \wp(B)$. Alors $x \in \wp(A)$ et $x \in \wp(B)$, donc $x \subseteq A$ et $x \subseteq B$. Soit $y \in x$, alors $y \in A$ et $y \in B$, donc $y \in A \cap B$.
Donc $x \subseteq A \cap B$ et $x \in \wp(A \cap B)$. Si $x = \emptyset$, $x \subseteq A \cap B$.

Exercice 9b
Vu que $A \subseteq A \cup B$ et $B \subseteq A \cup B$, on a $\wp(A) \subseteq \wp(A \cup B)$ et $\wp(B) \subseteq \wp(A \cup B)$. Donc $\wp(A) \cup \wp(B) \subseteq \wp(A \cup B)$ (voir ici).
Inversement, soit $A = \{a\}$ et $B = \{b\}$. On a $A \cup B = \{a, b\}$ et $\wp(A \cup B) = \{\emptyset, \{a, b\}, \{a\}, \{b\}\}$. Mais $\wp(A) \cup \wp(B) = \{\emptyset, \{a\}, \{b\}\}$. Donc, il n'est pas vrai en général que $\wp(A \cup B) \subseteq \wp(A) \cup \wp(B)$.

Exercice 9c
Si $x \in \wp(-A)$, $x \subseteq -A$, donc si $y \in x$, $y \notin A$. Donc $x \nsubseteq A$ et $x \in -\wp(A)$.
L'inverse n'est pas toujours vrai. Si par ex., $x \cap A \neq \emptyset$ et $x \nsubseteq A$, on a $x \in -\wp(A)$. Pour que $x \in \wp(-A)$, il faudrait que, pour tout y, si $y \in x$ $y \notin A$. Mais c'est impossible puisque $x \cap A \neq \emptyset$.

Exercice 10a
$\{\langle a, b\rangle, \langle b, b\rangle, \langle c, b\rangle, \langle a, a\rangle, \langle b, a\rangle, \langle c, a\rangle\}$

Exercice 10b
$\{\langle a, a\rangle, \langle b, a\rangle, \langle c, a\rangle, \langle a, \{b\}\rangle, \langle b, \{b\}\rangle, \langle c, \{b\}\rangle\}$

Exercice 10c
$\emptyset$

Exercice 10d
$\{\langle a, \emptyset\rangle, \langle b, \emptyset\rangle\}$

Exercice 10e
$\{\langle a, c\rangle, \langle b, c\rangle\} \times \{d, e\} = \{\langle\langle a, c\rangle, d\rangle, \langle\langle b, c\rangle, d\rangle, \langle\langle a, c\rangle, e\rangle, \langle\langle b, c\rangle, e\rangle\}$

Chapitre 2

Logique propositionnelle

2.1 Introduction

• En général, une logique propositionnelle porte sur des éléments d'information (les «propositions») considérés comme élémentaires ou inanalysables et que l'on peut nier avec une négation logique ($\neg$) ou combiner à l'aide de connecteurs comme la disjonction ($\vee$), la conjonction ($\&$) ou l'implication ($\Rightarrow$).
• La logique propositionnelle classique a une *syntaxe*, c.à.d. obéit à un ensemble de règles qui déterminent ce qui compte comme expression possible.
• Elle a également une sémantique, donnée en termes de valeurs de vérité (V/F).
• Elle a plusieurs théories de la preuve (chapitre 6).
• La sémantique de la logique propositionnelle classique est simple et élégante. Ses théories de la preuve sont très permissives et très peu «naturelles» quand on les compare au raisonnement quotidien.

2.2 Syntaxe et Sémantique

➤ Syntaxe
• On se donne des propositions atomiques, qui sont les briques élémentaires de la construction syntaxique, et on les combine de diverses

manières.
• La définition d'une proposition est (24). On utilisera les lettres p, q, r, s, p', etc. pour désigner des propositions (atomiques ou non).

Définition 24 Soit P un ensemble de propositions atomiques. Une *proposition* est un des objets suivants :
1. un élément de P (donc une proposition atomique),
2. une expression de forme $\neg p$, p étant une proposition,
3. une expression de forme $p \,\&\, q$, p et q étant des propositions,
4. une expression de forme $p \ \vee\ q$, p et q étant des propositions,
5. une expression de forme $p \ \Rightarrow\ q$, p et q étant des propositions.

On désigne par $\mathcal{L}(P)$ (le «langage» défini sur P) l'ensemble des propositions définies à partir de P.

Exemples :
$p \,\&\, (p \ \vee\ r)$, $\neg(p \ \Rightarrow\ s)$, r avec $r \in P$ sont des propositions. $p \,\&\,, \ \Rightarrow\ q \ \vee\ s$ ne sont pas des propositions.
• On peut représenter une proposition sous forme d'arbre.

➤ Sémantique
• Une interprétation consiste à assigner à chaque proposition atomique une valeur de vérité (V/F) et à assigner à chaque proposition complexe (= non–atomique) une valeur V/F en fonction de certaines règles.
• Les règles traitent la négation et les connecteurs. La définition formelle est la suivante.

Définition 25 Une interprétation sur un ens. de propositions atomiques P est une fonction $\mathcal{I}(\mathcal{L}(P)) \longrightarrow \{V, F\}$ telle que :
1. Pour chaque $p \in P$, $\mathcal{I}(p) = V$ ou F.
2. Pour chaque proposition p de forme $\neg p'$, $\mathcal{I}(p) = V$ si $\mathcal{I}(p') = F$ et $\mathcal{I}(p) = F$ si $\mathcal{I}(p') = V$.
3. Pour chaque proposition p de forme $p_1 \,\&\, p_2$, $\mathcal{I}(p) = V$ si $\mathcal{I}(p_1) = V$ et $\mathcal{I}(p_2) = V$. $\mathcal{I}(p) = F$ dans tout autre cas.
4. Pour chaque proposition p de forme $p_1 \ \vee\ p_2$, $\mathcal{I}(p) = F$ si $\mathcal{I}(p_1) = F$ et $\mathcal{I}(p_2) = F$. $\mathcal{I}(p) = V$ dans tout autre cas.
5. Pour chaque proposition p de forme $p_1 \ \Rightarrow\ p_2$, $\mathcal{I}(p) = F$ si $\mathcal{I}(p_1) = V$ et $\mathcal{I}(p_2) = F$. $\mathcal{I}(p) = V$ dans tout autre cas.

• La définition (25) dit que la négation de p' est vrai ssi p' est fausse, que $p_1 \,\&\, p2$ est vraie ssi les deux sont vraies, que $p_1 \ \vee\ p_2$ est vraie ssi au moins l'une des deux propositions est vraie, et que $p_1 \ \Rightarrow\ p_2$ est fausse ssi p_1 est vraie et p_2 fausse.
• On présente souvent les différentes fonctions d'interprétation sous forme de tables de vérité. Par exemple, (I) pour la négation et (II) pour la disjonction.

(I)

p	$\neg p$
V	F
F	V

(II)

p_1	p_2	$p_1 \vee p_2$
V	V	V
F	V	V
F	F	F
V	F	V

• La représentation par des tables de vérité est sûre, mais elle se révèle vite encombrante. Par ex., pour examiner les différentes possibilités d'assignation de vérité pour la proposition $p \Rightarrow (q \vee r)$, en supposant que p, q et r soient atomiques, on a la table suivante.

p	q	r	$q \vee r$	$p \Rightarrow (q \vee r)$
V	V	V	V	V
V	V	F	V	V
V	F	V	V	V
V	F	F	F	F
F	V	V	V	V
F	V	F	V	F
F	F	V	V	V
F	F	F	F	V

• Bien que cette table soit apparemment compliquée, elle illustre un des principes de base de l'évaluation des propositions. En prêtant attention aux propriétés de structure des fonctions d'assignation, il est souvent possible de simplifier une table compliquée. Ici, on remarque que le connecteur principal est une implication. $p \Rightarrow (q \vee r)$ est de la forme $X \Rightarrow Y$. Une implication ne peut être fausse que si l'antécédent est vrai et le conséquent est faux. Le seul cas ou ceci peut se produire, pour la proposition donnée, est le cas où (a) p est vraie et (b) $q \vee r$ est fausse, c.à.d. où q et r sont toutes deux fausses. Dans tous les autres cas, la proposition est vraie. Il n'y a donc, en réalité, que deux cas importants pour l'évaluation en termes de valeurs de vérité.

➤ Tautologies

• On peut exploiter ce phénomène pour étudier les tautologies et les contradictions.

Définition 26 Une *tautologie* est une proposition qui reçoit la valeur V pour n"importe quelle fonction d'assignation. Une *contradiction* reçoit la valeur F pour n'importe quelle fonction.

Chapitre 3

Logique des prédicats

Chapitre 4

Théorie des modèles

Chapitre 5

Rudiments de lambda–calcul

Chapitre 6

Rudiments de théorie de la preuve

6.1 Introduction

Comme son nom l'indique, la théorie de la preuve s'interroge sur le statut des preuves en logique.

➤ Qu'est-ce qu'une preuve ?
• Intuitivement, une preuve est un objet logique qui permet de mettre en rapport des *prémisses* ou *hypothèses* et une ou plusieurs conclusions.
• La relation entre les hypothèses et les conclusions est variable selon les systèmes logiques utilisés. Autrement dit ce qui compte comme un preuve correcte dans un système ne compte pas forcément comme une preuve correcte dans un autre système.

➤ Notion de *ressource*
• Pour prouver une conclusion, il faut utiliser certaines ressources (les hypothèses). Ces ressources sont en général de deux types.
a. Des ressources globales, utilisables pour n'importe quelle preuve (elles sont toujours disponibles).
b. Des ressources particulières, pas nécessairement toujours utilisables.

• En général, lorsqu'on utilise des hypothèses particulières $H_1 \ldots H_n$ (non–globales) pour prouver une conclusion C, on le note $H_1 \ldots H_n \vdash C$. Cela peut se lire « C est une conséquence de $H_1 \ldots H_n$». Lorsqu'on n'utilise que des ressources globales, $G_1 \ldots G_n$, on peut également écrire $G_1 \ldots G_n \vdash C$, mais on peut aussi écrire $\emptyset \vdash C$, pour souligner le fait que l'ensemble des ressources particulières utilisées est vide. On dit alors que C est un *théorème* du système utilisé (sa prouvabilité dans le système ne dépend pas de ressources particulières).

• L'aspect le plus difficile concerne les règles d'utilisation des ressources ; elles déterminent, par exemple, quelle ressource on a le droit d'utiliser dans quelle situation, si on a le droit d'utiliser une ressource plusieurs fois, une seule fois, etc.

➤ On distingue habituellement trois types généraux de théorie de la preuve. Les systèmes dits «Hilbertiens», les systèmes de *déduction naturelle*, et les systèmes dits «de Gentzen». Je ne considérerai ici que le premier et le troisième type, et uniquement pour la logique classique.

6.2 Systèmes de Hilbert pour la logique classique

➤ Allure générale

• Le nom de «système de Hilbert» ou «système Hilbertien» est attribué couramment au type de système logique que le mathématicien Hilbert développait autour des années 30-40 du XXème siècle. La principale préoccupation de Hilbert était de clarifier le statut de l'infini en mathématiques. Cela l'amena à construire des systèmes axiomatiques qu'il estimait intrinsèquement finis (il y a un nombre fini de ressources).

• Typiquement, un système de Hilbert sous sa forme moderne comprend des schémas d'axiomes et des règle d'inférence.

• Un schéma d'axiome est une forme abstraite dont les termes peuvent être remplacées par n'importe quelles propositions (atomiques ou non). Par exemple, le schéma en (27a) peut recevoir les instanciations en (27b,c,d). On note $p \mapsto X$ le fait que p remplace X.

Illustration 27

a. $X \ \Rightarrow \ (X \ \vee \ Y)$

b. $p \ \Rightarrow \ (p \ \vee \ r)$ $(p \mapsto X, r \mapsto Y)$

c. $(p \,\&\, q) \ \Rightarrow \ ((p \,\&\, q) \ \vee \ p)$ $((p \,\&\, q) \mapsto X, p \mapsto Y)$

d. $((p \,\&\, q) \ \vee \ r) \ \Rightarrow \ (((p \,\&\, q) \ \vee \ r) \ \vee \ (q \ \Rightarrow \ p))$ $(((p \,\&\, q) \ \vee \ r) \mapsto X, q \ \Rightarrow \ p \mapsto Y)$

• Les schémas de règles d'inférence permettent de poser une conclusion à partir d'une ou plusieurs propositions supposées déjà obtenues par le raisonnement. Le plus connu est le *modus ponens*, qui a la forme suivante.

Définition 28 *Modus ponens* (mp)

Le mp est le schéma de règle de la forme suivante :

$$\frac{X \quad X \Rightarrow Y}{Y}$$

$$\frac{c \quad d}{\frac{a}{a}} \ ok$$

6.3 Systèmes de Gentzen

➤ Caractéristiques générales
• Inventé par Gentzen, ce type de système ne manipule pas des schémas d'axiomes et des règles d'inférence mais des preuves.
• Les règles utilisées sont de deux types.
1. Les unes posent des schémas de preuve (elles sont comparables aux schémas d'axiome). Par exemple, $A \vdash A$ signifie que n'importe quelle proposition A est suffisante pour prouver A («si A alors A»).
2. Les autres posent des schémas d'inférence entre preuves. Généralement on n'a qu'un seul type de schéma, de la forme :

Définition 29 [Schéma d'inférence entre preuves]

$$\frac{\Sigma_1 \vdash \Gamma_1 \quad \ldots \quad \Sigma_n \vdash \Gamma_n}{\Sigma_{n+1} \vdash \Gamma_{n+1}}$$

29 signifie que, si on a n preuves, utilisant les hypothèses Σ_i (pour $i = 1 \ldots n$) pour aboutir aux conclusions Γ_i (pour $i = 1 \ldots n$), alors on peut poser qu'on a une preuve utilisant les hypothèses Σ_{n+1} pour aboutir aux conclusions Γ_{n+1}. Par exemple, la règle (32)

Définition 30
a. $A \vdash A$ (A étant n'importe quelle proposition)
b. $\perp \vdash$

Définition 31

a. $\dfrac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$ (AG)

b. $\dfrac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}$ (AD)

c. $\dfrac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}$ (CG)

d. $\dfrac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$ (CD)

Définition 32

a. $\dfrac{A_i, \Gamma \vdash \Delta}{A_0 \,\&\, A_1, \Gamma \vdash \Delta}$ (&G) pour $i = 0$ et $i = 1$

b. $\dfrac{\Gamma \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \,\&\, B}$ (&D)

c. $\dfrac{A, \Gamma \vdash \Delta \quad B, \Gamma \vdash \Delta}{A \;\vee\; B, \Gamma \vdash \Delta}$ $(\vee\mathrm{G})$

d. $\dfrac{\Gamma \vdash \Delta, A_i}{\Gamma \vdash \Delta, A_0 \;\vee\; A_1}$ $(\vee\mathrm{D})$ pour $i = 0$ et $i = 1$

e. $\dfrac{\Gamma \vdash \Delta, A \quad B, \Gamma \vdash \Delta}{A \;\Rightarrow\; B, \Gamma \vdash \Delta}$ $(\Rightarrow \mathrm{G})$

f. $\dfrac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \;\Rightarrow\; B}$ $(\Rightarrow \mathrm{D})$