Fiche résumée du cours de Logique

1 Apprendre à compter, ordinaux et cardinaux

1.1 Théorèmes de Cantor-Bernstein et de Cantor

1.1.1 *Théorème* ***(Cantor-Bernstein)***

Soient deux ensembles A et B tels qu'il existe une injection de A dans B et une injection de B dans A. Alors, il existe une bijection de A dans B.

1.1.2 *Théorème* ***(Cantor)***

Soit X un ensemble, il n'existe pas de surjection de X dans $\mathcal{P}(X)$.

1.2 Ensembles ordonnés

1.2.1 *Définition* ***(Ordre)***

Soit X un ensemble. Une **relation d'ordre** sur X est une relation antiréflexive ($\forall x \in X, x \nless x$) et transitive ($\forall x, y, z \in X, (x < y et y < z) \Rightarrow x < z$). Si tous les éléments sont comparables sur X, on dit que l'ordre est **total**.

1.2.2 *Définition* ***(Plus petit élément, élément minimal)***

Soit $(X, <)$ un ensemble ordonné, et $Y \subset X$.

i) Un **plus petit élément** (resp. **plus grand élément** de Y est un élément y tel que, $\forall x \in Y$, $y \leq x$ (resp. $y \geq x$).

ii) Un élément y de Y est **minimal** (resp.**maximal**) si, $\forall x \in Y, x \nless y$ (resp. $x \ngtr y$).

iii) Un **minorant** (resp.**majorant** de Y est un élément $x \in X$ tel que $x \leq y \forall y \in Y$ (resp. $x \leq y \forall y \in Y$).

iv) Une **borne inférieure** (resp.**borne supérieure**) de Y est un élément maximal (resp. minimal) de l'ensemble des minorants (resp. majorants).

1.2.3 *Définition* ***(Bon ordre)***

Un ordre $<$ sur X est un **bon ordre** si toute partie non vide admet un plus petit élément. (Un bon ordre est toujours total) On appellera également bon ordre un ensemble muni d'un bon ordre.

1.3 Ordinaux

1.3.1 *Définition* ***(Ensemble transitif, ordinal)***

i) Un ensemble X est **transitif** si $\forall x \in X$, $x \subset X$.

ii) Un **ordinal** est un ensemble transitif sur lequel $\in$ est un bon ordre.

1.3.2 *Propriétés des ordinaux*

i) $\emptyset$ est un ordinal.

ii) Si α est un ordinal non vide, $\emptyset \in \alpha$

iii) Si α est un ordinal, $\alpha \notin \alpha$.

iv) Si α est un ordinal et $\beta \in \alpha$, alors β est un ordinal.

v) Si β est un ordinal et $\beta \in \alpha$, alors $\beta = \delta_{<\beta}$, où $\beta = \delta_{<\beta}$ est l'ensemble des éléments plus petits que β (pour $\in$)

vi) α, β deux ordinaux, $\beta \subset \alpha \Leftrightarrow (\beta \in \alpha$ ou $\beta = \alpha)$

vii) α un ordinal, $\alpha^+ = \alpha \cup \{\alpha\}$ est un ordinal

1.3.3 *Théorème*

Soient α et β deux ordinaux, l'un des énoncés suivants est vérifié :

$$\alpha \in \beta \qquad \alpha = \beta \quad \text{ou} \quad \beta \in \alpha$$

1.3.4 *Proposition*

Soit A un ensemble non vide d'ordinaux, il possède un plu petit élément $\underset{\alpha \in A}{cap} \alpha$, qui est un ordinal.

1.3.5 *Proposition*

Soit A un ensemble non vide d'ordinaux,$a = \underset{\alpha \in A}{\cup} \alpha$ est un ordinal, et, si $\beta < a$, $\exists \alpha \in A$, $\beta \in \alpha$, avec β un ordinal.

1.3.6 *Définition **(Ordinal limite)***

Un **ordinal limite** est non vide, et n'est pas de la forme α^+

1.3.7 *Proposition*

Soit λ un ordinal limite, on a l'équivalence :

$$\lambda \text{ est un ordinal limite } \Leftrightarrow \lambda = \underset{\alpha \in \lambda}{\cup} \alpha$$

1.3.8 *Définition **(Ordinal fini)***

Un ordinal est **fini** si ni lui, ni aucun de ses éléments n'est limite.

1.3.9 *Théorème*

Tout ensemble bien ordonné X est isomorphe comme ensemble ordonné à un ordinal α. De plus, α et l'isomorphisme sont uniques. En particulier, on assimile tout ordinal fini à un $n \in \mathbb{N}$ de la manière suivante : $\emptyset = 0$, et $\forall n \in \ltimes$, $n + 1 = n^+$. On note $\omega = \mathbb{N} = \underset{n \in \mathbb{N}}{\cup} n$ le plus petit ordinal limite.

1.3.10 *Proposition*

Pour tout $x \in X$, il existe un isomorphisme $f_x : S_{\leq x} \to \alpha_x$, avec α_x ordinal. ($S_{\leq x} = \{y \in X, y \leq x\}$)

1.4 Opérations sur les ordinaux

1.4.1 *Sommme de deux ensembles ordonnés*

Soit $A + B = \{(x, y) \in \{A \times \{1\} \cup B \times \{2\}\}$, muni de l'ordre :

$$\begin{cases} (a,1) < (b,2) \quad \forall (a,b) \in A \times B \\ (a,1) < (a',1) \Leftrightarrow a < a' \quad \forall (a,a') \in A^2 \\ (b,2) < (b',2) \Leftrightarrow b < b' \quad \forall (b,b') \in B^2 \end{cases}$$

Si A et B sont totalement (resp. bien) ordonnés, alors $A + B$ est totalement (resp. bien) ordonné. Notons que $(A + B) + C$ est isomorphe à $A + (B + C)$

1.4.2 *Produit de deux ensembles ordonnés*

Si A, B sont des ensembles ordonnés, on munit $A \times B$ de l'ordre antilexicographique :

$$(a, b) < (a', b') \Leftrightarrow b < b' \text{ ou } b = b' \text{ et } a < a'$$

Si A et B sont totalement (resp. bien) ordonnés, alors $A \times B$ est totalement (resp. bien) ordonné. Notons que $(A \times B) \times C$ est isomorphe à $A \times (B \times C)$, et$A \times (B + C)$ est isomorphe à $(A \times B) + (A \times C)$

1.4.3 exponentiation

Si A, B sont des ensembles ordonnés, et si A a un plus petit élément, noté 0, on considère l'ensemble $A^{(B)}$ dse fonctions de B dans A à support fini, ie $\{f \in A^B \mid \{x \mid f(x) \neq 0\}$est fini$\}$. Sur cet ensemble, on pose alors

$$f < g \Leftrightarrow \exists b \in B \mid f(b) < g(b) \text{ et } f(x) = g(x) \quad \forall x > b$$

Si A et B sont bien ordonnés, alors $A^{(B)}$ l'est aussi.

Remarque : Si f à valeur dans un bon ordre est à support fini, alors son support admet un plus grand élément.

1.4.4 Arithmétique sur les ordinaux

Si α et β sont des ordinaux, on note $\alpha + \beta$ (resp. $\alpha.\beta, \alpha^{\beta}$) l'unique ordinal isomorphe à $\alpha + \beta$ (resp. $\alpha.\beta, \alpha^{(\beta)}$)

1.4.5 Propriétés de l'addition

Pour tout α, β, ordinaux, on a :

i) $\alpha + 0 = 0 + \alpha = \alpha$
ii) $\alpha + 1 = \alpha^+$
iii) $\alpha < \beta \Leftrightarrow \exists \gamma \neq 0, \beta = \alpha + \gamma$
iv) si $\beta < \beta'$, alors pour tout $\alpha, \alpha + \beta < \alpha + \beta'$. En particulier, si $\alpha + \beta = \alpha + \beta'$, alors $\beta = \beta'$
v) Si λ est un ordinal limite, $\alpha + \lambda = \bigcup\limits_{\beta \in \lambda} \alpha + \beta$
vi) $1 + \alpha = \alpha + 1 = \alpha^+$ si α est fini, et $1 + \alpha = \alpha$ sinon.

L'addition sur les ordinaux est associative.

1.4.6 Propriétés de la multipliation

i) $\alpha.0 = 0.\alpha = 0$
ii) $\alpha.1 = 1.\alpha = 1$
iii) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ et $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$
iv) $2\omega = \omega$, tandis que $\omega 2 = \omega + \omega$
v) Si $\alpha \neq 0$ et $\beta < \beta'$, alors $\alpha\beta < \alpha\beta'$
vi) Si λ est limite, alors $\alpha\lambda$ est la borne supérieure des $\alpha\beta$, pour $\beta \in \lambda$

1.4.7 Lemme

Si $\gamma < \alpha\beta$, alors, il existe $\rho < \alpha$ et $\sigma < \beta$, $\gamma = \alpha\sigma + \rho$

1.4.8 Propriétés de l'exponentiation

i) On a $\alpha^0 = 1$, $\alpha^1 = \alpha$, $1^{\alpha} = 1$ si $\beta \neq 0$, $0^{\beta} = 0$
ii) $\alpha^{\beta+\gamma} = \alpha^{\beta}\alpha^{\gamma}$, et $\alpha^{\beta\gamma} = (\alpha^{\beta})^{\gamma}$
iii) Si $\alpha > 1$, et $\beta < \beta'$, alors $\alpha^{\beta} < \alpha^{\beta'}$
iv) Si λ est limite, et si $\alpha > 1$, alors $\alpha^{\lambda} = \bigcup\limits_{\beta \in \lambda} \alpha^{\beta}$

1.5 Suites de Goodstein

1.5.1 Définition *(**Développement itéré en base p**)*

Soit p un entier ≥ 2. Soit n un entier, $n = \sum\limits_{i=1}^{r} p^{n_i}.c_i$ le développement de n en base p, avec $n_1 > n_2 ... > n_r$, et $c_i \in \{0..p-1\} \quad \forall i$. On peut également développer les n_i en base p et itérer le processus. On obtient le **développement itéré en base p** de n.

1.6 Axiome du choix

Soit $(X_i)_{i \in I}$ une famille d'ensembles, on note $\prod(X_i)_{i \in I} = \underset{i \in I}{X_i}$ l'ensemble des fonctions $f : I \to \bigcup\limits_{i \in I} X_i$ telles que, $\forall i \in I$, $f(i) \in X_i$

1.6.1 Axiome du choix

Si $(X_i)_{i \in I}$ est une famille d'ensembles non vides, alors $\prod(X_i)_{i \in I}$ est non vide.

Modulo les axiomes de Zermelo-Fraenckel, l'axiome du choix est équivalent au lemme de Zorn et au théorème de Zermelo.

*1.6.2 Définition **(Ensemble inductif)***

Un ensemble ordonné $(X, <)$ est **inductif** si toute partie Y de X qui est totalement ordonnée par $<$ est majorée dans X. **Tout ensemble inductif est non vide.**

*1.6.3 Lemme **(Zorn)***

Tout ensemble inductif admet un élément maximal.

1.6.4 Théorème (Zermelo)

Tout ensemble admet un bon ordre.

ON SUPPOSE DÉSORMAIS L'AXIOME DU CHOIX

1.7 Cardinal

*1.7.1 Définition **(Ensembles équipotents)***

Deux ensembles A et B sont dits **équipotents** s'il existe une bijection entre A et B.

*1.7.2 Définition **(Cardinal)***

Un ordinal α est un **cardinal**, si $\forall \beta < \alpha$, β n'est pas équipotent à α.

1.7.3 Proposition

Tout ensemble A est équipotent à un unique cardinal, noté card(A)

1.7.4 Proposition

Soient A et B deux ensembles, on suppose A non vide. Les énoncés suivants sont équivalents :

i) $card(A) \leq card(B)$

ii) Il existe une injection $A \to B$

iii) Il existe une surjection $B \to A$

1.7.5 Lemme

Si A est un ensemble de cardinaux, alors $\beta = \bigcup\limits_{\alpha \in A} \alpha$ est un cardinal.

1.7.6 Lemme

Si $f : \beta \to \alpha$ est une application strictement croissante entre ordinaux, alors, $\forall \lambda \in \beta,\ f(\lambda) \geq \lambda$

1.7.7 Proposition

Remarque : ne pas confondre les incrémentations de cardinaux et d'ordinaux. On notera $\alpha + 1$ celle sur les ordinaux, et α^+ celle sur les cardinaux. Ainsi, $(\aleph_\alpha)^+ = \aleph_{\alpha+1}$.

1.7.8 Proposition

Tout cardinal infini est de la forme $\aleph_\alpha$.

1.8 Opérations sur les ordinaux

1.8.1 Proposition

i) Si $\lambda \leq \mu$ et $\nu \leq \kappa$, alors $\lambda + \nu \leq \mu + \kappa$, $\lambda\nu \leq \mu\kappa$, et si $\mu \neq \emptyset$, $\lambda^\nu \leq \mu^\kappa$

ii) L'addition et le produit de cardinaux sont commutatifs et associatifs. Le produit est distributif par rapport à l'addition. De plus,

$$\lambda^{\mu+\nu} = \lambda^{\nu}.\lambda^{\mu} \qquad \lambda^{\nu}, \mu^{\nu} = (\lambda\mu)^{\nu} \qquad (\lambda^{\mu})^{\nu} = \lambda^{\mu\nu}$$

1.8.2 Proposition

$$card(\mathbb{R}) = 2^{\aleph_0}$$

1.8.3 Proposition

Si α est un ordinal infini, alors $card(\alpha) = card(\alpha + 1)$.

1.8.4 Proposition

Si λ est un cardinal infini, alors $\lambda.\lambda = \lambda$.

1.8.5 Proposition

i) Si λ est un cardinal infini, $\lambda + \lambda = \lambda$

ii) Si X, Y sont des ensembles non vides, dont l'un au moins est infini, on a :

$$card(X \cup Y) = card(X \times Y) = sup(card(X), card(Y))$$

iii) Si $(X_i)_{i\in I}$ est une famille d'ensembles dont l'un au moins est infini, alors $card(\underset{i\in I}{\cup} X_i) \leq \sup\limits_{i\in I}(card(X_i), card(I))$.

Application : Une union dénombrable d'ensembles dénombrables est dénombrables.

1.8.6 Théorème (Koenig)

Soient $(X_i)_{i\in I}$ e t$(Y_i)_{i\in I}$ deux familles d'ensembles, tels que $card(X_i) < card(Y_i)$ $\forall i \in I$. Alors,

$$card(\cup X_i) < card(\cup Y_i)$$

1.9 Cofinalité, montrer que $2^{\aleph_0} \neq \aleph_\omega$

*1.9.1 Définition **(Cofinalité)***

i) Une partie $B \subset A$ est dite cofinale dans A si elle est non bornée dans le sens suivant :

$$\forall a \in A, \quad \exists b \in B, \quad b \geq a$$

ii) Une application $f : \alpha \to \beta$ entre ordinaux est dite cofinale se son image dans α est cofinale dans α.

iii) Soit α un ordinal. la cofinalité de α, notée $cf(\alpha)$ est le plus petit ordinal β tel qu'il existe $f : \beta \to \alpha$, strictement croissante, et cofinale.

1.9.2 Lemme

Soit α un ordinal. $cf(\alpha)$ ets le plus petit ordinal β tel qu'il existe une application $f : \beta \to \alpha$ cofinale

1.9.3 Proposition

Pour tout ordinal α, on a

i) $cf(\alpha) \leq \alpha$

ii) $cf(cf(\alpha)) = cf(\alpha)$

iii) $cf(\alpha)$ est un cardinal

1.9.4 Proposition

Si λ est un ordinal limite, alors $cf(\aleph_\lambda) = cf(\lambda)$

*1.9.5 Définition **(Cardinal régulier)***

Un cardinal est dit **régulier** si il est infini et si $cf(\alpha) = \alpha$.

1.9.6 *Proposition*

Tout cardinal successeur infini, de la forme $\aleph_{\lambda+1}$ est régulier.

1.9.7 *Proposition*

Pour tout cardinal $\kappa \geq 2$ et tout cardinal infini λ, on a $cf(\kappa^{\lambda} > \lambda$.

1.9.8 *Corollaire*

$\aleph_{\omega} \neq 2^{\aleph_0}$. En effet, $cf(\aleph_{\omega}) = \omega$ et $cf(2^{\aleph_0}) > \aleph_0 = \omega$.

2 Théorie des modèles

2.1 languages

2.1.1 *Définition* ***(Languages formels)***

Un language est composé :

i) D'un ensemble infini dénombrable de variables, $V = \{v_0, v_1..\}$

ii) De symboles logiques $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \forall, \exists$

iii) de suites $(\mathcal{F}_n)_{n\in\mathbb{N}}$, et $(\mathcal{R}_n)_{n\in\mathbb{N}}$, où les éléments de $\mathcal{F}_n$ sont des symboles de fonctions n-aires, les éléments de $\mathcal{F}_0$ sont des symboles de constantes, et où les éléments de $\mathcal{R}_n$ sont des symboles de relations n-aires. De plus, on demande quee le symbole "toujours vrai", T, appartienne à $\mathcal{R}_0$

Un language L est la réunion de ces ensembles. On note $L^* = \underset{n\in\mathbb{N}}{L^k}$

2.2 Termes

2.2.1 *Définition* ***(termes)***

L'ensemble $T(L)$ des termes du language L est le plus petit sous-ensemble de L^* contenant :

i) V, l'ensemble des variables

ii) $\mathcal{F}_0$, l'ensemble des constantes

iii) $\{ft_1..t_n, \forall f \in \mathcal{F}_n, \forall (t_1..t_n) \in T(L)^n\}$

On a de plus $T(L) = \underset{k\in\mathbb{N}}{\cup} T_k(L)$, avec $T_0(L) = \mathcal{F}_0 \cup V$ et $T_{k+1}(L) = T_k(L) \cup (\underset{n\in\mathbb{N}}{\cup}\{ft_1..t_n, \forall f \in \mathcal{F}_n, \forall (t_1..t_n) \in T_k(L)^n\}$

On dit qu'un terme t est de hauteur k si $t \in T_k(L) - T_{k-1}(L)$

2.2.2 *Proposition* ***(Lecture unique d'un terme)***

Tout terme t vérifie une et une seule des propriétés suivantes :

$\star$ $t \in \mathcal{F}_0$ $\quad\star$ $t \in V$ $\quad\star$ $t = ft_1..t_n$, avec f et les t_i uniques.

2.3 Formules

2.3.1 *Définition* ***(Formule atomique)***

Une formule atomique est un élément de $\mathcal{R}_n \times T(L)^n$. On note $F_0(L)$ l'ensemble des formules atomiques. On définit

$$F_{n+1}(L) = F_n(L) \cup \{\neg F, F \in F_n(L)\} \cup \{\forall v_i F, F \in F_n(L)\}$$

$$\cup \{\exists v_i F, F \in F_n(L)\} \cup \{F\alpha G, F, G \in F_n(L), \alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}\}$$

Enfin, on pose $F(L) = \underset{n\in\mathbb{N}}{\cup} F_n(L)$. Si $G \in F_n(L) - F_{n-1}(L)$, on dit que G est de hauteur n. F est l'ensemble des formules sur L.

2.3.2 *Proposition*

Toute formule F vérifie une et une seule des propriétés suivantes :

i) F est atomique, $F = Rt_1..t_n$, avec R, et les t_i uniques.
ii) $F = \neg G$, avec G unique
iii) $F = \forall v_n G$, avec v_n et G uniques
iv) $F = \exists v_n G$, avec v_n et G uniques
v) $F = \alpha GH$, α unique dans $\{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, G,H uniques.

2.3.3 *Définition* ***(Variables libres, liées)***

Soit v_k une variable. On définit les occurences libres de v_k dans F par :

i) Si F est atomique, toutes les occurences sont libres
ii) Si $F = \neg G$, les occurences libres de F sont celles de G. De même, si $F = \alpha GH$, avec $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$, les occurences libres de F sont celles de G et H.
iii) Si $F = \forall v_i G$, ou $\exists v_i G$:

Si $i \neq k$, les occurences libres de v_k de F sont celles de G

Si $i = k$, aucune occurence libre de $v_k$dans F

Les occurences non libres de v_k sont dites liées. Les variables de F sont celles ayant au moins une occurence libre dans F. Une formule sans variable libre est appellée **énoncé**.

2.4 Substitution dans les formules

2.4.1 *Définition* ***(Substitution)***

Soit $F \in F(L)$, $(u_1..u_n) \in V^n$ distinctes, $(t_1..t-n) \in T(L)^n$. On définit la formule $F_{t_1/u_1..t_n/u_n}$ en remplacant u_i par t_i dans les occurences libres de u_i dans F

2.5 Structures

2.5.1 *Définition* ***(Structure)***

Soit L un language. une L structure m est un ennsemble M non vide, muni, pour chaque $f \in \mathcal{F}_n$, d'une fonction $f^m : M^m \to M$, et, pour chaque $R \in \mathcal{R}_n$, d'un sous ensemble $R^m \subset M^n$. par ailleurs, on demande que $T^m = M^0$

2.5.2 *Interprétation des termes*

Soit $t\,[u_1..u_n]$ un terme de L et m une L-structure. Soient $(a_1..a_n) \in M^n$, on note $t\,[a_1..a_n] \in M$ obtenue en interprétant les symboles de fonctions, et en remplaçant u_i par a_i.

- Si t est un symbole de constante c, $t\,[u_1..u_n] = c^m$
- Si t est un symbole de variable u_i, $t\,[u_1..u_n] = a_i$
- Si $t = f(t_1..t_n)$, on interprète t par $f^m(t_1^m..t_n^m)$.

2.6 Satisfaction d'une formule dans une structure

Soit F une formule, $F = F\,[u_1..u_n]$. Si $(a_1.;a_n) \in M^n$, on dit que $F\,[a_1..a_n]$ est satisfait dans m, noté $m \vDash F\,[a_1..a_n]$

i) Pour $F = R\,[t_1..t_n]$, si $(t_1\,[a_1..a_n]\,..t_n\,[a_1..a_n]) \in R^m \subset M^n$

ii) Pour $F = \neg G$, si $m \nvDash G\,[a_1..a_n]$, ie si G n'est pas satisfait dans m

iii) Pour $F = G \wedge H$, si $m \vDash H\,[a_1..a_n]$, et $m \vDash G\,[a_1..a_n]$

iv) Idem pour $F = G \vee H$

v) Pour $F =\Rightarrow FG$ si $m \vDash G\,[a_1..a_n]$ entraîne $m \vDash H\,[a_1..a_n]$

vi) Pour $F =\Leftrightarrow FG$ si $m \vDash G\,[a_1..a_n]$ est équivalent à $m \vDash H\,[a_1..a_n]$

vii) Pour $F = (\forall v G)\,[u_1..u_n]$, si pour $v \notin \{u_1..u_n\}$, $\forall a \in M$, $G\,[a_1..a_n]$, et si pour $v \in \{u_1..u_n\}$, $v = u_{i0}$, $\forall a \in M$, $G\,[a_1..a_{i_0-1}, a_{i-0}, a_{i_0+1}..a_n]$

viii) Idem pour $F = \exists v G$

2.6.1 *Définition* ***(validité universelle)***

Un énoncé F de L est universellement valide si, pour toute structure m de L, $m \vDash F$. Une formule est universellement valide su une (donc toute) clôture universelle l'est. Deux formules F et G sont logiquement équivalentes si $F \Leftrightarrow G$ est universellement valide. une théorie dans un language L est un ensemble d'énoncés. Une L-structure m est un modèle de T si tout énoncé de T est satisfait dans m (on note $m \vDash T$). Une théorie est consistante si elle admet au moins un modèle.

2.7 Tautologies

2.7.1 Définition ***(Tautologies du calcul propositionnel)***

Une tautologie du calcul propositionnel est une formule de L_p quelque soient les valeurs de vérité associées aux p_i. Soit $J[p_1..p_n]$ une tautologie de L_p, $F_1..F_n$ des formules de L. La formule $J[F_1..F_n]$, obtenue en substituant les F_i aux p_i est appellée tautologie de E.

2.8 Démonstration formelle

$t[u_1..u_n]$

i)

ii)

iii)

2.8.1 Proposition

2.8.2 Définition ***()***