Exercices de Logique

version 4.1

Isar Stubbe (février 2005)

---

1 Ensembles

1.1 Soit un ensemble X et $\mathscr{P}X$ l'ensemble des parties de X. L'inclusion $A \subseteq B$ définit un ordre partiel sur $\mathscr{P}X$.

(i) Montrez que l'infimum de $A, B \in \mathscr{P}X$ est $A \cap B$, et leur supremum est $A \cup B$. Déduisez-en que $A \subseteq B$ si et seulement si $A \cap B = A$, si et seulement si $A \cup B = B$.

(ii) Notons $A^c = X \setminus A$ pour le complément de $A \in \mathscr{P}X$ dans X. Observez que $A \cup A^c = X$ et $A \cap A^c = \emptyset$, quel que soit A. Et que donc, pour $A, B \in \mathscr{P}X$, $(A \cap A^c) \subseteq B \subseteq (A \cup A^c)$.

(iii) Observez que, pour tout $A, B, C \in \mathscr{P}X$, on a

— $A \cap A = A$ et $A \cup A = A$;
— $A \cap B = B \cap A$ et $A \cup B = B \cup A$;
— $A \cap (B \cap C) = (A \cap B) \cap C$ et $A \cup (B \cup C) = (A \cup B) \cup C$;
— $(A \cap B) \cup B = B$ et $(A \cup B) \cap B = B$;
— $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ et $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
— $(A \cap A^c) \cup B = B$ et $(A \cup A^c) \cap B = B$.

(iv) Vérifiez que, pour tout $A, B \in \mathscr{P}X$,

— $(A \cap B)^c = A^c \cup B^c$ et $(A \cup B)^c = A^c \cap B^c$.

Remarque : On observe ici que, en tant qu'ordre partiel, $(\mathscr{P}X, \subseteq)$ possède des propriétés tout à fait remarquables. Dans 3.8 on étudie une abstraction de ce type d'ordres partiels, appelés *algèbres de Boole*.

1.2 L'application $\{\,\}\colon X \to \mathscr{P}X \colon x \mapsto \{x\}$ est une injection évidente. Montrez qu'il ne peut pas y avoir de surjection $s\colon X \to \mathscr{P}X$. Indication : Considérez

$$Y = \{x \in X \mid x \notin s(x)\},$$

qui devrait être de la forme $s(x_0)$.

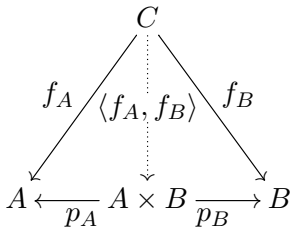
1.3 $A \times B$ dénote le produit cartésien de deux ensembles A et B ; les projections sur les facteurs sont bien sûr

$$p_A\colon A \times B \to A \colon (a, b) \mapsto a,$$

$$p_B \colon A \times B \to B \colon (a, b) \mapsto b.$$

Convenons aussi de noter B^A l'ensemble des applications de A dans B.

(i) Vérifiez que, pour A, B, C donnés, la prescription $f \mapsto (p_A \circ f, p_B \circ f)$ détermine une bijection entre les ensembles $(A \times B)^C$ et $A^C \times B^C$. Indication : Montrez que pour tout couple d'applications $f_A \colon C \to A$, $f_B \colon C \to B$ il existe une unique application $\langle f_A, f_B \rangle \colon C \to A \times B$ faisant commuter le diagramme suivant :



On dit que $\langle f_A, f_B \rangle$ est la factorisation de f_A et f_B à travers le produit.

(ii) Généralisez (i) pour une famille $(A_i)_{i \in I}$ quelconque d'ensembles.

(iii) Trouvez une bijection entre les ensembles $(A^B)^C$ et $A^{B \times C}$.

(iv) Que vaut $A^\emptyset$? Et que vaut $\emptyset \times A$? Et que vaut le produit cartésien d'une famille vide ?

Remarque : La propriété en (i) est la *propriété universelle* de $A \times B$, dans le sens que cette propriété détermine l'ensemble $A \times B$ à bijection près : si un ensemble P et des applications $\pi_A \colon P \to A$, $\pi_B \colon P \to B$ sont tels que, pour tout ensemble C, la prescription $f \mapsto (\pi_A \circ f, \pi_B \circ f)$ détermine une bijection entre P^C et $A^C \times B^C$, alors il existe une unique bijection entre P et $A \times B$, notons-le $b \colon P \to A \times B$, telle que $p_A \circ b = \pi_A$ et $p_B \circ b = \pi_B$.

1.4 Une relation d'équivalence sur un ensemble A est une partie E de $A \times A$ vérifiant la réflexivité, la transitivité et la symétrie.

(i) Vérifiez que si E et E' sont des équivalences sur A, alors leur intersection $E \cap E'$ est également une équivalence. Est-ce vrai pour l'intersection d'une famille quelconque $(E_i)_{i \in I}$ d'équivalences sur A ?

(ii) Pour toute relation R binaire sur A, désignons par $\widetilde{R}$ la plus petite relation d'équivalence sur A qui contient R. Montrez que $\widetilde{R}$ existe et que l'on a $\widetilde{R}(x, y)$ si et seulement si il existe une suite finie d'éléments $z_1, ..., z_r$ telle que $z_1 = x$, $z_r = y$ et pour tout $i \in \{1, ..., r\}$, on ait $R(z_i, z_{i+1})$ ou $R(z_{i+1}, z_i)$ ou $z_i = z_{i+1}$.

1.5 Soit $f \colon A \to B$ une application entre ensembles.

(i) Vérifiez que la clause

$$(a, a') \in E_f \iff fa = fa'$$

définit une relation d'équivalence sur A.

(ii) L'image de f est l'ensemble $\mathsf{im}(f) = \{b \in B \mid \exists a \in A : fa = b\}$. Vérifiez que le quotient de A par E_f est en bijection avec $\mathsf{im}(f)$.

(iii) Montrez que l'application f se factorise en surjection canonique suivie d'une bijection et d'une inclusion canonique.

1.6 On note $s\colon \mathbb{N} \to \mathbb{N}$ pour l'application "successeur" sur l'ensemble des nombres naturels ; c'est-à-dire, $s(n) = n + 1$. Prouvez que, pour tout ensemble A, élément $a \in A$ et application $e\colon A \to A$, il existe une unique application $f\colon \mathbb{N} \to A$ telle que $f(0) = a$ et $f \circ s = e \circ f$.

Cette propriété de l'ensemble $\mathbb{N}$ le caractérise dans le sens suivant : Soit un ensemble N, un élément $z \in N$ et une application $\sigma\colon N \to N$, avec la propriété que, pour tout ensemble A, élément $a \in A$ et application $e\colon A \to A$, il existe une unique application $f\colon N \to A$ telle que $f(z) = a$ et $f \circ s = e \circ f$. Alors il existe une unique bijection $b\colon N \to \mathbb{N}$ telle que $b(z) = 0$ et $b \circ \sigma = s \circ b$. Prouvez ce théorème.

Remarque : On appelle un ensemble N avec un élément $z \in N$ et l'application $\sigma\colon N \to N$ ayant la *propriété universelle* citée ci-dessus, un "objet de nombres naturels" ; on l'écrira tout simplement (N, z, σ). La philosophie est donc qu'un tel ensemble peut toujours "jouer le rôle de $\mathbb{N}$" ; ou autrement dit, que le "contenu mathématique" de l'ensemble $\mathbb{N}$ est exactement exprimé par sa propriété universelle. Nous allons approfondir ce point de vue dans les exercices suivants, en montrant que les "propriétés habituelles" des nombres naturels se déduisent toutes de sa propriété universelle.

1.7 Soit un objet de nombres naturels (N, z, σ).

(i) Prouvez que, si un sous-ensemble $S \subseteq N$ contient l'élément z et est fermé pour la fonction $\sigma\colon N \to N$ (ceci veut dire : $n \in S$ implique $\sigma(n) \in S$), alors $S = N$.

(ii) Déduisez-en que, pour un ensemble A et deux applications $f\colon N \to A$ et $g\colon N \to A$, si $f(z) = g(z)$ et $f(n) = g(n)$ implique que $f(\sigma(n)) = g(\sigma(n))$ pour tout $n \in N$, alors $f = g$.

(iii) Concluez que l'on peut définir une application $\pi\colon N \to N$ en posant que $\pi(z) = z$ et $\pi(\sigma(n)) = n$ (pour tout $n \in N$), et que la composée $\pi \circ \sigma$ est égale

à l'application identité sur N ; observez que cela implique que $\sigma\colon N \to N$ est une injection.

Remarque : Le point (i) prouve que tout objet de nombres naturels admet le principe de preuve par induction. Et l'application $\pi\colon N \to N$ construite en (iii) est l'application "prédécesseur".

1.8 Soit toujours un objet de nombres naturels (N, z, σ). On définit l'addition sur N par récurrence : pour tout $m \in N$ on a

$$m + z = m \text{ et } m + \sigma(n) = \sigma(m + n),$$

quel que soit $n \in N$.

(i) Montrez, par des récurrences appropriées, que $(N, +, z)$ est un monoïde commutatif ; c'est-à-dire, que l'addition est associative et commutative, et que z est son élément neutre.

(ii) Montrez que, de plus, dans ce monoïde la loi de simplification est valide : si $m + n = k + n$ alors $m = k$.

(iii) Et – pour boucler la boucle – montrez que, si on définit $u = \sigma(z)$ dans N, alors pour tout $n \in N$,

$$\sigma(n) = n + u.$$

(Donc les lettres z et u peuvent être lues comme "zéro" et "un(ité)", et le successeur de $n \in N$ est n plus un...)

1.9 La multiplication sur un objet de nombres naturels (N, z, σ) est telle que pour tout $m \in N$ on a

$$m \cdot z = z \text{ et } m \cdot \sigma(n) = m \cdot n + m,$$

quel que soit $n \in N$.

(i) Montrez que la multiplication est distributive par rapport à l'addition...

(ii) ... et que $(N, \cdot, u)$ (où u est toujours la notation pour $\sigma(z)$) est un monoïde commutatif.

1.10 Toujours à propos d'un objet de nombres naturels (N, z, σ), on définit une relation binaire sur N par :

$$m \leq n \text{ si il existe un } k \in N \text{ tel que } m + k = n.$$

Prouvez qu'il s'agit d'un ordre partiel sur N, c'est-à-dire, d'une relation transitive, réflexive et antisymétrique.

1.11 Le théorème de Cantor–Dedekind–Bernstein dit que deux ensembles sont équipotents (donc qu'il existe une bijection entre eux) dès que chacun peut s'injecter dans l'autre. Nous l'admettons.

(i) En utilisant au besoin ce théorème, montrez que tous les intervalles de $\mathbb{R}$ ayant au moins deux éléments sont équipotens.

(ii) Trouvez des injections de $\mathbb{N}$ dans $\mathbb{N} \times \mathbb{N}$ et de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$.

(iii) Trouvez des injections de $\mathbb{Z}$ et de $\mathbb{Q}^+$ dans $\mathbb{N} \times \mathbb{N}$, et déduisez-en que $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}^+$ sont équipotents.

(iv) Utilisez l'équipotence de $\mathbb{N}$ et $\mathbb{Q}^+$ pour démontrer l'équipotence de $\mathbb{Q}$ et $\mathbb{N}$.

(v) Montrez que $\mathbb{R}$ n'est pas dénombrable (c'est-à-dire, n'est pas en bijection avec $\mathbb{N}$). Indication : Montrez que $\mathbb{R}$ et $\mathscr{P}\mathbb{N}$ sont équipotents, et utilisez ensuite 1.2.

Remarque : Le théorème que nous avons utilisé, a été conjecturé par G. Cantor, et R. Dedekind en a donné la première preuve (1887)... mais celle-ci n'a pas été publiée. F. Bernstein fut le premier à avoir publié une preuve, en 1898. Ceci explique pourquoi ce théorème porte ces trois noms.

2 Langages et structures algébriques

2.1 Donnez l'alphabet d'un langage adapté à $\mathbb{N}$ (avec la multiplication, l'addition, les éléments distingués 0 et 1), aux parties ouvertes de $\mathbb{R}^n$ (avec l'intersection, la réunion, les éléments distingués $\emptyset$ et $\mathbb{R}^n$), ou encore aux endomorphismes d'un espace vectoriel sur $\mathbb{R}$ (avec la composition, l'addition, et l'identité et l'application nulle comme éléments distingués).

Décrivez l'interprétation usuelle du langage en question dans chacune des structures indiquées.

2.2 Soit $\mathscr{L}$ un langage algébrique, $x, x' \in V(\mathscr{L})$ et $t, t', t'' \in T(\mathscr{L})$.

(i) Donnez un exemple montrant que l'on n'a pas toujours

$$[t'' \mid x'][t' \mid x]t = [[t'' \mid x']t' \mid x][t'' \mid x']t$$

si x a une occurence dans t''. (On suppose $x' \neq x$.)

(ii) Vérifiez que si x et x' n'ont pas d'occurrence dans t' ni dans t'', alors

$$[t'' \mid x'][t' \mid x]t = [t' \mid x][t'' \mid x']t.$$

2.3 Soit un langage algébrique $\mathscr{L}$, et deux structures $\mathscr{S}_1, \mathscr{S}_2$ avec interprétations $\mathscr{I}_1 : \mathscr{L} \to \mathscr{S}_1$ (et surjections $\sigma_n^1 : O_n \to \mathbb{O}_n$) et $\mathscr{I}_2 : \mathscr{L} \to \mathscr{S}_2$ (et surjections $\sigma_n^2 : O_n \to \mathbb{O}_n$). Une application ensembliste $h : D_1 \to D_2$ entre le domaine de $\mathscr{S}_1$ et le domaine de $\mathscr{S}_2$ est appelée homomorphisme de $\mathscr{L}$-structures si pour tout $n \in \mathbb{N}$, pour tout n-uple $(d_1, ..., d_n) \in D_1^n$ et pour toute opération n-aire $f \in O_n$ de $\mathscr{L}$,

$$h(\sigma_n^1 f(d_1, ..., d_n)) = \sigma_n^2 f(hd_1, ..., hd_n).$$

(i) Montrez que pour deux homomorphismes $h_1 : D_1 \to D_2$ et $h_2 : D_2 \to D_3$ la composition $h_2 \circ h_1 : D_1 \to D_3$ est un homomorphisme ; vérifiez que la composition d'homomorphismes est associative, c'est-à-dire, que pour trois homomorphismes h_1, h_2, h_3 on a toujours que $h_3 \circ (h_2 \circ h_1) = (h_3 \circ h_2) \circ h_1$.

(ii) Montrez que l'application identité $\mathsf{id}_{\mathscr{S}_1} : D_1 \to D_1$ est un homomorphisme, et que pour tout homomorphisme $h : D_1 \to D_2$ on a que $\mathsf{id}_{\mathscr{S}_2} \circ h = h = h \circ \mathsf{id}_{\mathscr{S}_1}$.

Remarque : Ceci indique que les $\mathscr{L}$-structures et leurs homomorphismes forment une *catégorie*. Consultez par exemple "Handbook of Categorical Algebra, vol. 1" [F. Borceux, 1994] pour une introduction à la théorie des catégories.

2.4 Soit un langage algébrique $\mathscr{L}$. Pour deux $\mathscr{L}$-structures $\mathscr{S}_1$ et $\mathscr{S}_2$ telles que $D_1 \subseteq D_2$, on dit que $\mathscr{S}_1$ est une sous-structure de $\mathscr{S}_2$ si l'inclusion $i : D_1 \to D_2$ est un homomorphisme de $\mathscr{L}$-structures.

(i) Expliquez la phrase : $\mathscr{S}_1$ est sous-structure de $\mathscr{S}_2$ si et seulement si $D_1 \subseteq D_2$ et D_1 est "fermé pour les opérations".

(ii) Vérifiez que si $(\mathscr{S}_k)_{k \in K}$ est une famille de sous-structures de $\mathscr{S}$, de domaines respectifs D_k, alors $\bigcap_{k \in K} D_k$ est le domaine d'une sous-structure de $\mathscr{S}$ (notée $\bigcap_{k \in K} \mathscr{S}_k$).

(iii) Montrez par un exemple que si $\mathscr{S}_1$ et $\mathscr{S}_2$ sont deux sous-structures de $\mathscr{S}$, de domaines respectifs D_1 et D_2, il n'est pas vrai en général que $D_1 \cup D_2$ soit le domaine d'une sous-structure.

(iv) Montrez que pour toute partie A de D on peut parler de la plus petite sous-structure de $\mathscr{S}$ dont le domaine contient A (la sous-structure engendrée par A, comme on dit).

2.5 Si $h : D_1 \to D_2$ est un homomorphisme bijectif entre deux structures $\mathscr{S}_1$ et $\mathscr{S}_2$ d'un type fixé, alors la bijection réciproque h^{-1} est également un homomorphisme. Vérifiez. On appelle h un isomorphisme entre $\mathscr{L}$-structures.

Montrez qu'un homomorphisme $h : D_1 \to D_2$ entre deux structures $\mathscr{S}_1$ et $\mathscr{S}_2$ est un isomorphisme si et seulement si il existe un homomorphisme $k : D_2 \to D_1$ satisfaisant $k \circ h = \mathsf{id}_{\mathscr{S}_1}$ et $h \circ k = \mathsf{id}_{\mathscr{S}_2}$.

2.6 Soit $\mathscr{L}$ un langage algébrique. Si $\mathscr{S}_1$ et $\mathscr{S}_2$ sont deux $\mathscr{L}$-structures, de domaines D_1 et D_2, alors le produit cartésien $D_1 \times D_2$ peut être muni naturellement d'une structure du même type, notée $\mathscr{S}_1 \times \mathscr{S}_2$, en définissant, pour tout $n \in \mathbb{N}$, pour tout n-uple $(d_1^1, d_1^2), ..., (d_n^1, d_n^2) \in (D_1 \times D_2)^n$ et pour toute opération n-aire $f \in O_n$ de $\mathscr{L}$, que

$$\sigma_n^{1\times 2} f((d_1^1, d_1^2), ..., (d_n^1, d_n^2)) = (\sigma_n^1 f(d_1^1, ..., d_n^1), \sigma_n^2 f(d_1^2, ..., d_n^2));$$

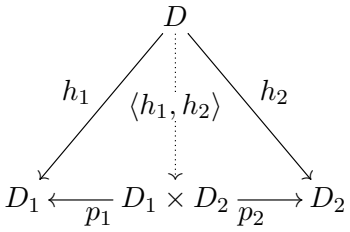
ceci définit à la fois les $\mathbb{O}_j$ et les surjections $\sigma_n^{1\times 2}\colon O_n \to \mathbb{O}_n$ d'une interprétation de $\mathscr{S}_1 \times \mathscr{S}_2$.

(i) Montrez que les projections sur les facteurs

$$p_1\colon D_1 \times D_2 \to D_1\colon (x, y) \mapsto x,$$
$$p_2\colon D_1 \times D_2 \to D_2\colon (x, y) \mapsto y,$$

sont des homomorphismes.

(ii) Montrez que pour toute $\mathscr{L}$-structure $\mathscr{S}$, on a une bijection entre l'ensemble des homomorphismes de $\mathscr{S}$ vers $\mathscr{S}_1 \times \mathscr{S}_2$ et l'ensemble des couples d'homomorphismes de $\mathscr{S}$ vers $\mathscr{S}_1$ et vers $\mathscr{S}_2$, donnée par la préscription $h \mapsto (p_1 \circ h, p_2 \circ h)$. Indication : Par 1.3 on sait que les homomorphismes $h_1\colon D \to D_1$ et $h_2\colon D \to D_2$ déterminent une unique application ensembliste $\langle h_1, h_2\rangle\colon D \to D_1 \times D_2$ faisant commuter le diagramme suivant :

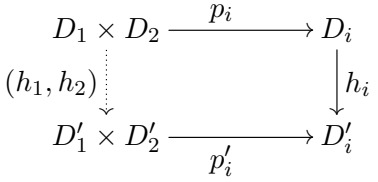


Il suffit donc de montrer que $\langle h_1, h_2\rangle$ est un homomorphisme de $\mathscr{L}$-structures.

(iii) Soient $h_1\colon D_1 \to D_1'$ et $h_2\colon D_2 \to D_2'$ deux homomorphismes, resp. de $\mathscr{S}_1$ à $\mathscr{S}_1'$ et de $\mathscr{S}_2$ à $\mathscr{S}_2'$. Il suit que

$$D_1 \times D_2 \xrightarrow{p_1} D_1 \xrightarrow{h_1} D_1' \qquad \text{et} \qquad D_1 \times D_2 \xrightarrow{p_2} D_1 \xrightarrow{h_2} D_2'$$

déterminent une unique factorisation à travers $D_1' \times D_2'$; on le note (h_1, h_2). Vérifiez que le diagramme suivant commute pour $i = 1, 2$:



(iv) Généralisez ce qui précède au cas où on part d'une famille $(\mathscr{S}_i)_{i\in I}$ quelconque de $\mathscr{L}$-structures.

Remarque : La propriété en (ii) est la *propriété universelle* du produit cartésien de $\mathscr{S}_1$ et $\mathscr{S}_2$, dans le sens que cette propriété détermine le produit cartésien à isomorphisme près.

2.7 Soit $\mathscr{S}$ une $\mathscr{L}$-structure de domaine D. Une congruence E sur $\mathscr{S}$ est par définition une relation d'équivalence E sur D telle que, pour tout $n \in \mathbb{N}$, tout $f \in O_n$ symbole d'opération n-aire du langage $\mathscr{L}$ et tout $(x_1, y_1), ..., (x_n, y_n)$ appartenant à E on a que aussi le couple $(\sigma_n f(x_1, ..., x_n), \sigma_n f(y_1, ..., y_n))$ appartient à E.

(i) Montrez qu'une équivalence E sur D est une congruence si et seulement si E, vue comme partie de $D \times D$, est une sous-structure du produit $\mathscr{S} \times \mathscr{S}$.

(ii) Déduisez-en que l'intersection d'une famille $(E_i)_{i\in I}$ de congruences sur $\mathscr{S}$ est toujours une congruence (cf. 1.4 et 2.4).

2.8 Si $h\colon D_1 \to D_2$ est un homomorphisme quelconque entre $\mathscr{L}$-structures $\mathscr{S}_1$ et $\mathscr{S}_2$, montrez que la relation $hx_1 = hy_1$ est une congruence ; on l'appelle l'équivalence nucléaire associée à h, et on la note E_h.

Montrez que le quotient D_1/E_h peut être muni naturellement d'une $\mathscr{L}$-structure, et que l'application ensembliste $[-]\colon D_1 \to D_1/E_h\colon x \mapsto [x]$ qui envoie un élément sur sa classe d'équivalence, est alors un homomorphisme surjectif.

2.9 Si $h\colon D_1 \to D_2$ est un homomorphisme quelconque entre $\mathscr{L}$-structures $\mathscr{S}_1$ et $\mathscr{S}_2$, montrez que l'ensemble

$$\mathsf{im}(h) = \{y \in D_2 \mid \exists x \in D_1\colon hx = y\}$$

peut être muni naturellement d'une $\mathscr{L}$-structure, et que $\mathsf{im}(h)$ est une sous-structure de $\mathscr{S}_2$. On appelle $\mathsf{im}(h)$ l'image de h.

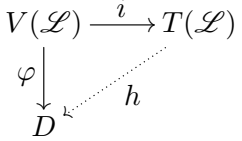
2.10 Montrez qu'un homomorphisme $h\colon D_1 \to D_2$ entre deux structures $\mathscr{S}_1$ et $\mathscr{S}_2$ de type donné se factorise en surjection canonique suivie d'un isomorphisme et d'une inclusion canonique. Indication : Montrez que le diagramme

$$\begin{array}{ccc} D_1 & \xrightarrow{\ h\ } & D_2 \\ {\scriptstyle [-]}\downarrow & & \uparrow{\scriptstyle i} \\ D_1/E_h & \xrightarrow[\overline{h}]{} & \mathsf{im}(h) \end{array}$$

dans lequel $\overline{h}: D_1/E_h \to \mathsf{im}(h)$ est la bijection qui envoie une classe $[x]$ sur hx, est un diagramme commutatif de $\mathscr{L}$-structures et homomorphismes (cf. 1.5, 2.5, 2.8 et 2.9).

2.11 Observez que, pour tout langage algébrique $\mathscr{L}$, l'ensemble des termes $T(\mathscr{L})$ est muni canoniquement d'une $\mathscr{L}$-structure : son domaine est donc $T(\mathscr{L})$, et pour toute opération n-aire $f \in O_n$ du langage $\mathscr{L}$ et tout n-uple $(t_1, ..., t_n) \in T(\mathscr{L})^n$ on pose $\sigma_n f(t_1, ..., t_n) = ft_1...t_n$, ce qui définit à la fois les $\mathbb{O}_j$ et les surjections $\sigma_j: O_j \to \mathbb{O}_j$ d'une interprétation $\mathscr{I}: \mathscr{L} \to T(\mathscr{L})$. Ensuite, observez que l'inclusion $i: V(\mathscr{L}) \hookrightarrow T(\mathscr{L})$ est une valuation.

Soit $\mathscr{S}$ une $\mathscr{L}$-structure de domaine D et $\varphi: V(\mathscr{L}) \to D$ une valuation quelconque. Montrez que le prolongement $\overline{\varphi}: T(\mathscr{L}) \to D$ est l'unique homomorphisme $h: T(\mathscr{L}) \to D$ vérifiant $h \circ i = \varphi$, c'est-à-dire, qui fait commuter le diagramme suivant :



Remarque : Dans le syllabus se trouve une définition inductive du "prolongement d'une valuation". La propriété ci-dessus donne une définition alternative équivalente en termes d'homomorphismes.

2.12 Soient un langage, une structure et une interprétation $\mathscr{I}: \mathscr{L} \to \mathscr{S}$, et une valuation $\varphi: V(\mathscr{L}) \to D$ dans le domaine de $\mathscr{S}$.

(i) Montrez que la relation $t \sim_\varphi t'$ est une congruence sur l'algèbre des termes.

(ii) Montrez que l'équivalence sémantique $t \sim t'$ par rapport à une structure donnée $\mathscr{S}$ est une congruence sur l'algèbre des termes.

Indication : utilisez 2.7, 2.8 et 2.11.

2.13 Soit $\mathscr{L}$ un langage algébrique, $T_{\{x_1,...,x_n\}}(\mathscr{L})$ l'ensemble des termes dont toutes les variables sont contenues dans l'ensemble $\{x_1, ..., x_n\}$, et $\mathscr{S}$ une $\mathscr{L}$-structure de domaine D.

(i) Montrez que $T_{\{x_1,...,x_n\}}(\mathscr{L})$ est (le domaine de) une sous-structure de $T(\mathscr{L})$.

(ii) Montrez que pour tout choix d'un n-uple $\underline{d} = (d_1, ..., d_n)$ d'éléments de D il existe un homomorphisme unique de $T_{\{x_1,...,x_n\}}(\mathscr{L})$ vers D envoyant x_1 sur d_1, ... , x_n sur d_n. On le note $h_{\underline{d}}$.

(iii) Montrez la réciproque de (ii) : que tout homomorphisme de $T_{\{x_1,...,x_n\}}(\mathscr{L})$ vers D détermine un unique n-uple $\underline{d} = (d_1, ..., d_n)$ d'éléments de D.

(iv) Si on choisit p termes dans $T_{\{x_1,...,x_n\}}(\mathscr{L})$, soit $\underline{t} = (t_1, ..., t_p)$, ce choix détermine un homomorphisme de $T_{\{y_1,...,y_p\}}(\mathscr{L})$ vers $T_{\{x_1,...,x_n\}}(\mathscr{L})$, soit $h_{\underline{t}}$. Si on choisit ensuite un n-uple $\underline{d} = (d_1, ..., d_n)$ dans D, ce choix détermine un homomorphisme $h_{\underline{d}}$ de $T_{\{x_1,...,x_n\}}(\mathscr{L})$ vers D. Posons $\underline{t}(\underline{d}) = (h_{\underline{d}}(t_1), ..., h_{\underline{d}}(t_p))$; ce p-uple dans D détermine donc un homomorphisme $h_{\underline{t}(\underline{d})}$ de $T_{\{y_1,...,y_p\}}(\mathscr{L})$ vers D. Justifiez l'égalité $h_{\underline{d}} \circ h_{\underline{t}} = h_{\underline{t}(\underline{d})}$.

(v) Montrez que, si $\{x_{i_1}, ..., x_{i_p}\} \subseteq \{x_1, ..., x_n\}$, alors $T_{\{x_{i_1},...,x_{i_p}\}}(\mathscr{L})$ est une sous-structure de $T_{\{x_1,...,x_n\}}(\mathscr{L})$.

(vi) En particulier on a, pour $1 \leq k \leq n$, des inclusions

$$i_k : T_{\{x_k\}}(\mathscr{L}) \to T_{\{x_1,...,x_n\}}(\mathscr{L})$$

qui sont des homomorphismes. Prouvez que, si on a des homomorphismes $h_k : T_{\{x_k\}}(\mathscr{L}) \to D$ (pour $1 \leq k \leq n$), alors il existe un unique homomorphisme $h : T_{\{x_1,...,x_n\}}(\mathscr{L}) \to D$ tel que $h_k = i_k \circ h$ pour $1 \leq k \leq n$.

(vii) Montrez que $T_{\{y_1,...,y_n\}}(\mathscr{L})$ est isomorphe à $T_{\{x_1,...,x_n\}}(\mathscr{L})$.

Remarque : La $\mathscr{L}$-structure $T_{\{x_1,...,x_n\}}(\mathscr{L})$ est appelée la *$\mathscr{L}$-structure libre sur n générateurs* ; la bijection indiquée en (ii) et (iii) est sa *propriété universelle*. On utilise souvent la notation $T_n(\mathscr{L})$ pour la $\mathscr{L}$-structure des termes avec au plus n variables distinctes, si on ne veut pas spécifier ces variables ; (vii) ci-dessus affirme qu'en effet "le nom des variables n'a pas d'importance". Alors (vi) prouve que "$T_n(\mathscr{L})$ est le *coproduit* (ou *somme*) de n copies de $T_1(\mathscr{L})$" : la *propriété universelle* du coproduit est *duale* à celle du produit—d'où le préfixe "co".

Comparez par exemple avec la notion d'espace vectoriel libre sur un corps k ; les générateurs sont alors les vecteurs de base, et on a l'habitude d'écrire k^n pour un espace vectoriel libre sur n générateurs.

2.14 Soit $\mathscr{L}$ un langage algébrique, et $\mathscr{S}$ une $\mathscr{L}$-structure de domaine D. Avec les notations de 2.13, on définit pour tout $t \in T_n(\mathscr{L})$ l'application ensembliste

$$t^{\mathscr{S}} : D^n \to D : \underline{d} \mapsto h_{\underline{d}}(t).$$

On l'appelle une opération dérivée n-aire.

(i) Montrez qu'une opération dérivée n'est pas toujours un homomorphisme de $\mathscr{L}$-structures. Indication : Pour le langage des groupes, donc avec un symbole binaire ("multiplication"), un symbole unaire ("inverse") et une constante ("unité"), les groupes sont des structures algébriques et les homomorphismes de groupes sont des homomorphismes de structures. Considérez maintenant le terme suivant : $t = x \cdot y$; montrez que, pour un groupe $\mathscr{G} = (G, - \cdot -, (-)^{-1}, 1)$

l'application $t^{\mathscr{G}}: G \times G \to G$ n'est en général pas un homomorphisme de groupes.

(ii) Si on suppose dans (i) que le groupe $\mathscr{G}$ est commutatif, alors qu'est-ce que vous observez ?

(iii) Toujours avec les notations de ci-dessus, vérifiez que

— si $t = x_1 \in V(\mathscr{L})$ (donc t est une variable) alors $t^{\mathscr{S}}: D \to D: d \mapsto d$;

— si $t = f_0 \in O_0$ (donc t est une constante) alors $t^{\mathscr{S}}: \{*\} \to D: * \mapsto \sigma_0 f_0$;

— si $t = f_m t_1 ... t_m$ où $f_m \in O_m$ $(m \geq 1)$ et chaque $t_i \in T_{n_i}(\mathscr{L})$ alors $t^{\mathscr{S}}: D^n \to D$ (avec $n = n_1 + \cdots + n_m$) est égale à la composée

$$D^n = D^{n_1} \times ... \times D^{n_m} \xrightarrow{(t_1^{\mathscr{S}}, ..., t_m^{\mathscr{S}})} D^m \xrightarrow{\sigma_m f_m} D$$

Ceci contient une définition alternative (par induction sur la forme de t) de l'opération dérivée $t^{\mathscr{S}}$.

Remarque : Les points (i) et (ii) contiennent une observation très importante : Une *théorie algébrique* est, essentiellement, la donnée d'un langage algébrique avec un symbole d'égalité et des axiomes qui expriment l'égalité entre certains termes. Pensez par exemple à la théorie des groupes, ou à la théorie des groupes commutatifs ; ces théories sont données par le même langage mais la deuxième théorie a un axiome en plus que la première. Un modèle pour une théorie algébrique est une structure pour le langage dans lequel les axiomes "sont satisfaits" ; un homomorphisme entre modèles est un homomorphisme de structures. Groupes, resp. groupes commutatifs, sont les modèles de la théorie des groupes, resp. de la théorie des groupes commutatifs. En général, une opération dérivée n'est pas un homomorphisme : comme le suggère (i) ci-dessus, la théorie des groupes donne un contre-exemple. Mais pour certaines théories, toutes les opérations dérivées sont des homomorphismes ! Ces théories sont appellées *commutatives* ; la théorie des groupes commutatifs en est un exemple comme le suggère (ii) ci-dessus. Les modèles d'une théorie algébrique commutative forment une catégorie qui a beaucoup de "bonnes propriétés" que la catégorie des modèles d'une théorie algébrique non-commutative n'a pas. Voir "Handbook of Categorical Algebra, vol. 2" [F. Borceux, 1994] pour une introduction très lisible à ce sujet.

2.15 Soit $h: D_1 \to D_2$ un homomorphisme entre $\mathscr{L}$-structures $\mathscr{S}_1$ et $\mathscr{S}_2$.

(i) Justifiez l'égalité $\overline{h \circ \varphi} = h \circ \overline{\varphi}$ pour toute valuation $\varphi: V(\mathscr{L}) \to D_1$.

(ii) Montrez que pour tout $t \in T_n(\mathscr{L})$, les opérations dérivées n-aires $t^{\mathscr{S}_1}$ et

$t^{\mathscr{S}_2}$ font commuter le diagramme suivant :

$$\begin{array}{ccc} D_1^n & \xrightarrow{t^{\mathscr{S}_1}} & D_1 \\ {\scriptstyle (h,...,h)}\downarrow & & \downarrow{\scriptstyle h} \\ D_2^n & \xrightarrow[t^{\mathscr{S}_2}]{} & D_2 \end{array}$$

Les notations sont celles des exercices précédents.

2.16 Soit $\mathscr{L}$ un langage algébrique, et $t \in T_n(\mathscr{L})$. On sait que $T(\mathscr{L})$ est (le domaine de) une $\mathscr{L}$-structure, et donc on a une opération dérivée de t sur $T(\mathscr{L})$. Montrez comment cette opération coïncide avec une substitution simultanée.

3 Calcul des propositions : sémantique

3.1 On notera $\mathbf{2} = (\{0,1\}, \neg_{\mathbf{2}}, \wedge_{\mathbf{2}}, \vee_{\mathbf{2}}, \to_{\mathbf{2}}, \leftrightarrow_{\mathbf{2}})$ pour le domaine des valeurs de vérité. A propos de ces opérations constituant la structure des valeurs de vérité,

(i) montrez qu'elles peuvent toutes s'exprimer à partir de l'opération unique $|_{\mathbf{2}}$ définie par $i_1 \mid_{\mathbf{2}} i_2 = 0$ si et seulement si $i_1 = i_2 = 1$;

(ii) montrez qu'elles peuvent aussi toutes s'exprimer à partir de l'opération $\downarrow_{\mathbf{2}}$ définie par $i_1 \downarrow_{\mathbf{2}} i_2 = 1$ si et seulement si $i_1 = i_2 = 0$.

$|_{\mathbf{2}}$ et $\downarrow_{\mathbf{2}}$ sont appellées opérations de Sheffer et de Peirce.

3.2 Soient P et Q des formules de $\mathscr{L}\mathscr{P}$ dont les variables sont comprises dans $\{p_1, ..., p_n\}$.

(i) Puisque $\mathbf{2}$, le domaine des valeurs de vérité, est une $\mathscr{L}\mathscr{P}$-structure, il existe une opération dérivée $P^{\mathbf{2}}\colon \{0,1\}^n \to \{0,1\}$ (cf. 2.14). Montrez que P est une tautologie si et seulement si $P^{\mathbf{2}}$ est l'application constante à valeur 1.

(ii) Montrez que P et Q sont sémantiquement équivalentes si et seulement si les opérations dérivées respectives coïncident.

3.3 Soit $\mathscr{M}$ une réalisation de $\mathscr{L}\mathscr{P}$. Soit $\mathsf{Th}(\mathscr{M})$ l'ensemble des formules P telles que $\mathscr{M} \models P$. Montrez que $\mathsf{Th}(\mathscr{M})$ a les propriétés suivantes.

(i) Si $P \in \mathsf{Th}(\mathscr{M})$ et si $P' \in \mathsf{Th}(\mathscr{M})$, alors $P \wedge P' \in \mathsf{Th}(\mathscr{M})$.

(ii) Si $P \vee P' \in \mathsf{Th}(\mathscr{M})$ alors $P \in \mathsf{Th}(\mathscr{M})$ ou $P' \in \mathsf{Th}(\mathscr{M})$.

(iii) Si $P \in \mathsf{Th}(\mathscr{M})$ et si $P \to Q \in \mathsf{Th}(\mathscr{M})$, alors $Q \in \mathsf{Th}(\mathscr{M})$.

(iv) Si $P \leftrightarrow P' \in \mathsf{Th}(\mathscr{M})$, alors $[P \mid p]Q \leftrightarrow [P' \mid p]Q \in \mathsf{Th}(\mathscr{M})$.

3.4 Soient $p, q, r \in V(\mathscr{L}\mathscr{P})$. Vérifiez que les formules suivantes sont des tautologies par la méthode des tableaux de vérité.

(i) $p \to (q \to p)$

(ii) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$

(iii) $(\neg q \to p) \to ((\neg q \to \neg p) \to q)$

(iv) $(p \to q) \leftrightarrow (\neg p \vee q)$

(v) $(p \leftrightarrow q) \leftrightarrow \neg((p \wedge \neg q) \vee (q \wedge \neg p))$

(vi) $(p \vee q) \leftrightarrow (\neg p \to q)$

(vii) $(p \wedge q) \leftrightarrow \neg(p \to \neg q)$

Justifiez que ces formules sont toujours des tautologies pour des *formules* P, Q, R de $\mathscr{L}\mathscr{P}$ aux places des *variables* p, q, r (donc $P \to (Q \to P)$, etc.).

3.5 Un "raisonnement" est une suite finie de $n+1$ formules $P_1, ..., P_n, Q$ de $\mathscr{L}\mathscr{P}$, dont les n premières sont appelées "prémisses" et la dernière est appelée "conclusion", et que l'on dispose souvent de la manière suivante :

$$\frac{P_1; ...; P_n}{Q}$$

Le raisonnement est "correct" si la formule $(...(P_1 \wedge P_2) \wedge ... \wedge P_n) \to Q$ est une tautologie. Vérifiez la correction des raisonnements suivants.

(i) $\dfrac{P \to Q; P}{Q}$

(ii) $\dfrac{\neg Q \to \neg P}{P \to Q}$

(iii) $\dfrac{\neg(P \to Q)}{P}$

(iv) $\dfrac{P \to Q; \neg P}{\neg Q}$

(v) $\dfrac{P \to \neg Q; P \to Q}{\neg P}$

3.6 Pour vérifier si une $\mathscr{L}\mathscr{P}$-formule donnée P est une tautologie, on peut éventuellement remplacer le tableau de vérité par une réflexion ou analyse montrant qu'il est impossible que pour une réalisation $\mathscr{M}$ on ait $\overline{\mathscr{M}}(P) = 0$. Appliquez cette méthode pour montrer que les formules suivantes sont des tautologies :

(i) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$;

(ii) $[(((p \to q) \to (\neg r \to \neg s)) \to r) \to u] \to [(u \to p) \to (s \to p)]$ (axiome de Meredith, 1953).

3.7 Montrez que toute formule de $\mathscr{L}\mathscr{P}(\neg, \wedge, \vee, \rightarrow, \leftrightarrow)$ est équivalente à une formule de $\mathscr{L}\mathscr{P}(\neg, \wedge)$, à une formule de $\mathscr{L}\mathscr{P}(\neg, \vee)$, ou encore à une formule de $\mathscr{L}\mathscr{P}(\neg, \rightarrow)$.

3.8 Une *algèbre de Boole* $\mathscr{B}$ est la donnée d'un ensemble B avec deux opérations binaires et une opération unaire, notées

$$\wedge\colon B \times B \to B, \quad \vee\colon B \times B \to B, \quad \neg\colon B \to B$$

satisfaisant certains axiomes. Référence : "Algebra" [S. MacLane et G. Birkhoff, 1967], ou plus spécifiquement "Lattice Theory, 3rd edition" [G. Birkhoff, 1966].

(i) Montrez qu'une algèbre de Boole peut être caractérisée comme étant un ordre partiel $(B, \leq)$ avec un plus grand élément (noté 1) et un plus petit élément (noté 0) dans lequel on peut donner pour chaque paire d'éléments leur supremum et leur infimum, et pour lequel chaque élément admet un orthocomplément. (L'*orthocomplément* d'un élément x d'un ordre partiel avec 0 et 1 est par définition un élément x' tel que le supremum de x et x' égale 1, et l'infimum de x et x' égale 0.) Indication : Soit $\mathscr{B} = (B, \wedge, \vee, \neg)$ une algèbre de Boole comme définie ci-dessus, alors l'ordre partiel sur B est donné par la clause

$$x \leq y \iff x \wedge y = x \quad (\iff x \vee y = y\ ).$$

Réciproquement, si $(B, \leq)$ est un ordre partiel comme décrit ci-dessus, on pose

$$x \wedge y = \text{infimum de } x \text{ et } y,$$

$$x \vee y = \text{supremum de } x \text{ et } y,$$

$$\neg x = \text{orthocomplément de } x.$$

(ii) Est-ce que $(\mathbb{N}, \leq)$ est une algèbre de Boole ? Et, pour un espace vectoriel V, l'ensemble des sous-espaces avec l'inclusion, $(\mathsf{sev}(V), \subseteq)$? Et, pour un espace topologique $(X, \mathscr{T})$, l'ensemble des ouverts avec l'inclusion, $(\mathscr{T}, \subseteq)$? Et, pour un ensemble quelconque X, l'ensemble des sous-ensembles $\mathscr{P}(X)$ avec l'inclusion, $(\mathscr{P}(X), \subseteq)$ (cf. 1.1) ?

(iii) Montrez que toute algèbre de Boole $\mathscr{B} = (B, \wedge, \vee, \neg)$ est munie d'une structure d'algèbre pour le langage des propositions.

(iv) Prouvez que $\mathbf{2} = (\{0, 1\}, \wedge, \vee, \neg)$ (le domaine des valeurs de vérité) est une algèbre de Boole. Prouvez ensuite que, pour une algèbre de Boole $\mathscr{B}$ quelconque, $\mathbf{2}$ est une sous-structure de $\mathscr{B}$.

3.9 Toute algèbre de Boole $\mathscr{B}$, dont le domaine sera noté B, est une $\mathscr{L}\mathscr{P}$-structure, et donc on a une opération dérivée $P^{\mathscr{B}}\colon B^n \to B$ associée à toute formule avec n variables (cf. 2.14). On dira que P est une $\mathscr{B}$-tautologie si $P^{\mathscr{B}}$ est l'application constante à valeur 1 (le plus grand élément de B).

(i) Qu'est-ce qu'une **2**-tautologie ?

(ii) Prouvez que, s'il existe une algèbre de Boole $\mathscr{B}$ telle que P est une $\mathscr{B}$-tautologie, alors P est une **2**-tautologie. Indication : Il suffit de prouver que $P^{\mathbf{2}}$ est l'application constante à valeur 1 si $P^{\mathscr{B}}$ l'est. Mais puisque **2** est une sous-structure de $\mathscr{B}$ (cf. 3.8 (iv)), l'inclusion $i\colon \{0,1\} \to B$ est un homomorphisme. Par 2.15 (ii) on a donc un diagramme commutatif

$$\begin{array}{ccc} \{0,1\}^n & \xrightarrow{P^{\mathbf{2}}} & \{0,1\} \\ {\scriptstyle (i,\ldots,i)}\downarrow & & \downarrow{\scriptstyle i} \\ B^n & \xrightarrow[P^{\mathscr{B}}]{} & B \end{array}$$

et il suit que, si $P^{\mathscr{B}}$ est la constante à valeur 1, alors $P^{\mathbf{2}}$ l'est aussi.

(iii) Considérons une algèbre de Boole $\mathscr{B}$ des sous-ensembles d'un ensemble X—donc $\mathscr{B} = (\mathscr{P}(X), \cap, \cup, (-)^c)$. Prouvez que, pour tout élément $x \in X$, l'application

$$\delta_x\colon \mathscr{P}(X) \to \{0,1\}\colon T \mapsto \begin{cases} 1 \text{ si } x \in T \\ 0 \text{ sinon} \end{cases}$$

est un homomorphisme de $\mathscr{L}\mathscr{P}$-structures. Vérifiez que, pour $T \in \mathscr{P}(X)$,

$$\forall x \in X\colon \delta_x(T) = 1 \iff T = X.$$

Déduisez-en que toute **2**-tautologie est aussi une $\mathscr{B}$-tautologie. Indication : Il suffit de prouver que $P^{\mathbf{2}}$ est l'application constante à valeur 1 seulement si $P^{\mathscr{B}}$ est l'application constante à valeur X. Mais pour tout $x \in X$ l'application $\delta_x\colon \mathscr{P}(X) \to \{0,1\}$ est un homomorphisme et on a un diagramme commutatif

$$\begin{array}{ccc} \{0,1\}^n & \xrightarrow{P^{\mathbf{2}}} & \{0,1\} \\ {\scriptstyle (\delta_x,\ldots,\delta_x)}\uparrow & & \uparrow{\scriptstyle \delta_x} \\ \mathscr{P}(X)^n & \xrightarrow[P^{\mathscr{B}}]{} & \mathscr{P}(X) \end{array}$$

Si $P^{\mathbf{2}}$ est la constante à valeur 1, alors pour tout $x \in X$ l'application $\delta_x \circ P^{\mathscr{B}}$ l'est aussi, et donc $P^{\mathscr{B}}$ envoie chaque $T \subseteq X$ sur X.

Remarque : La propriété en (iii) est aussi vraie pour des algèbres de Boole qui ne sont pas de la forme $(\mathscr{P}(X), \cap, \cup, (-)^c)$. L'exercice 4.1 contient une preuve du cas général, en passant par l'axiomatique du calcul propositionnel.

En somme, l'exercice ci-dessus indique que la sémantique des formules de $\mathscr{L}\mathscr{P}$ – qui dépend a priori de l'algèbre **2** des valeurs de vérité – est également déterminée par toute autre algèbre de Boole à la place de **2**. Exercice 4.1 précisera les choses.

3.10 Si on prend l'algèbre des formules de $\mathscr{L}\mathscr{P}$, l'équivalence sémantique par rapport à la structure des valeurs de vérité est une congruence (cf. 2.12). Observez que l'on a, pour toutes formules P, Q, R,

(o) $P \wedge P \sim P, \quad P \vee P \sim P,$

(i) $P \wedge Q \sim Q \wedge P, \quad P \vee Q \sim Q \vee P,$

(ii) $P \wedge (Q \wedge R) \sim (P \wedge Q) \wedge R, \quad P \vee (Q \vee R) \sim (P \vee Q) \vee R,$

(iii) $(P \wedge Q) \vee Q \sim Q, \quad (P \vee Q) \wedge Q \sim Q,$

(iv) $P \wedge (Q \vee R) \sim (P \wedge Q) \vee (P \wedge R), \quad P \vee (Q \wedge R) \sim (P \vee Q) \wedge (P \vee R),$

(v) $(P \wedge \neg P) \vee Q \sim Q, \quad (P \vee \neg P) \wedge Q \sim Q.$

Concluez que le quotient de l'algèbre des formules par cette congruence (cf. 2.8) – où les relations ci-dessus deviennent des égalités ! – est une algèbre de Boole. L'algèbre quotient est appelée l'*algèbre de Lindenbaum* du calcul propositionnel.

Quelles sont les éléments de la classe d'équivalence qui est le plus grand élément de l'algèbre de Lindenbaum ? Et les éléments de la classe qui est le plus petit élément ?

3.11 Soient $p_1, ..., p_n$ des variables de $\mathscr{L}\mathscr{P}$. Convenons que, pour $\underline{\varepsilon} = (\varepsilon_1, ..., \varepsilon_n) \in \{0,1\}^n$, la notation $p_j^{\varepsilon_j}$ désigne p_j si $\varepsilon_j = 1$ et $\neg p_j$ si $\varepsilon_j = 0$.

(i) Quelle est l'opération dérivée sur $\{0,1\}$ définie par la formule $P = p_1^{\varepsilon_1} \wedge ... \wedge p_n^{\varepsilon_n}$?

(ii) Soit $f\colon \{0,1\}^n \to \{0,1\}$ une opération n-aire quelconque. Quelle est l'opération dérivée sur $\{0,1\}$ définie par la formule

$$P = \bigvee_{\underline{\varepsilon}} (p_1^{\varepsilon_1} \wedge ... \wedge p_n^{\varepsilon_n})$$

pour $\underline{\varepsilon} = (\varepsilon_1, ..., \varepsilon_n)$ parcourant les éléments de $\{0,1\}^n$ pour lesquels $f(\underline{\varepsilon}) = 1$.

(iii) Soit P une formule quelconque de $\mathscr{L}\mathscr{P}$ comprenant les variables $p_1, ..., p_n$. Vous inspirant de (ii), montrez qu'il existe une formule de la forme

$$\bigvee_{\underline{\varepsilon}} (p_1^{\varepsilon_1} \wedge ... \wedge p_n^{\varepsilon_n})$$

qui est sémantiquement équivalente à P.

Remarque : Cet exercice contient le fait que toute formule de $\mathscr{L}\mathscr{P}$ est équivalente à une formule *en forme normale disjonctive*, c'est-à-dire, en forme de disjonction de conjonctions de variables ou négations de variables.

3.12 Soient $P, Q, P_1, ..., P_n$ des formules de $\mathscr{L}\mathscr{P}$.

(i) Vérifiez les équivalences sémantiques

$$\neg(P \wedge Q) \sim (\neg P) \vee (\neg Q) \quad \text{et}$$

$$\neg(P \vee Q) \sim ((\neg P) \wedge (\neg Q)).$$

(ii) Généralisez en

$$\neg(P_1 \wedge ... \wedge P_n) \sim (\neg P_1) \vee ... \vee (\neg P_n) \quad \text{et}$$

$$\neg(P_1 \vee ... \vee P_n) \sim ((\neg P_1) \wedge ... \wedge (\neg P_n)).$$

(iii) Montrez que pour toute formule de $\mathscr{L}\mathscr{P}$ on peut trouver une formule équivalente "en forme nomale conjonctive", c'est-à-dire, en forme de conjonction de disjonctions de variables ou négations de variables.

Remarque : Les équivalences en (i) sont *les lois de De Morgan*. Elles sont vraies dans toute algèbre de Boole $\mathscr{B} = (B, \wedge, \vee, \neg)$: pour tout $a, b \in B$ on a que $\neg(a \wedge b) = \neg a \vee \neg b$ et $\neg(a \vee b) = \neg a \wedge \neg b$.

4 Calcul des propositions : axiomatique

4.1 On considère le calcul des propositions $\mathscr{C}\mathscr{P}$ (cf. syllabus) dont les expressions bien formées sont les formules de $\mathscr{L}\mathscr{P}(\neg, \rightarrow)$, les axiomes sont

$P \rightarrow (Q \rightarrow P)$,
$(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$,
$(\neg Q \rightarrow \neg P) \rightarrow ((\neg Q \rightarrow P) \rightarrow Q)$,

et la seule règle de déduction est le Modus Ponens :

de $\vdash P$ et $\vdash P \rightarrow Q$, déduisez $\vdash Q$.

(i) Prouvez que pour toute algèbre de Boole $\mathscr{B}$, ces trois axiomes sont des $\mathscr{B}$-tautologies, et que le Modus Ponens préserve les $\mathscr{B}$-tautologies (cf. 3.9). Indication : Dans une algèbre de Boole $\mathscr{B} = (B, \wedge, \vee, \neg)$ (cf. 3.8), l'interprétation du symbole $\neg$ est évidente ; pour $\rightarrow$ on interprètera que, pour $a, b \in B$, $a \rightarrow b = \neg(a \wedge \neg b)$ ou, ce qui revient au même par les lois de De Morgan, $a \rightarrow b = \neg a \vee b$. Les lois de De Morgan (cf. 3.12) seront d'ailleurs très utiles pour vérifier que les axiomes ci-dessus sont des $\mathscr{B}$-tautologies !

(ii) Déduisez-en que, pour toute algèbre de Boole $\mathscr{B}$, tout théorème de $\mathscr{C}\mathscr{P}$ est une $\mathscr{B}$-tautologie.

(iii) Concluez à l'aide de 3.9 (ii) que, pour une formule P, les phrases suivantes sont équivalentes :

1. P est une tautologie ;
2. il existe une algèbre de Boole $\mathscr{B}$ pour laquelle P est une $\mathscr{B}$-tautologie ;
3. pour toute algèbre de Boole $\mathscr{B}$, P est une $\mathscr{B}$-tautologie ;
4. P est un théorème du calcul propositionnel.

4.2 Plusieurs auteurs optent pour une axiomatique du calcul des propositions dans laquelle l'axiome

(α) $(\neg Q \to \neg P) \to ((\neg Q \to P) \to Q)$

de 4.1 est remplacé par

(β) $(\neg Q \to \neg P) \to (P \to Q)$.

On peut démontrer l'équivalence des deux systèmes axiomatiques—que l'on notera ici par $\mathscr{C}\mathscr{P}^\alpha$ et $\mathscr{C}\mathscr{P}^\beta$.

(i) Montrez que (β) est un théorème de $\mathscr{C}\mathscr{P}^\alpha$. Indication : Il suffit de montrer que c'est une tautologie, par exemple par un tableau de vérité ; on peut conclure par complétude de $\mathscr{C}\mathscr{P}^\alpha$.

(ii) Vérifiez que le Métathéorème de Herbrand reste valable dans le calcul $\mathscr{C}\mathscr{P}^\beta$. Indication : Notez que la preuve du Métathéorème pour $\mathscr{C}\mathscr{P}^\alpha$ (cf. syllabus) n'utilise pas l'axiome (α).

(iii) Soient P, Q des formules quelconques. Montrez que $\neg P \to (P \to Q)$ est un théorème de $\mathscr{C}\mathscr{P}^\beta$. Attention : On ne sait a priori pas si le calcul $\mathscr{C}\mathscr{P}^\beta$ est complet. Il ne suffit donc pas de montrer que cette formule est une tautologie !

(iv) On considère le calcul $\mathscr{C}\mathscr{P}^\beta$. Soit Γ une théorie et P, Q des formules telles que $\Gamma \cup \{\neg Q\} \vdash \neg P$ et $\Gamma \cup \{\neg Q\} \vdash P$. Montrez qu'alors $\Gamma \vdash Q$. (Un peu plus dur !)

(v) Dans le point précédent, prenez pour Γ la théorie vide. Vérifiez qu'alors on "récupère" (α) comme théorème dans $\mathscr{C}\mathscr{P}^\beta$.

(vi) Concluez que les deux systèmes d'axiomes, $\mathscr{C}\mathscr{P}^\alpha$ et $\mathscr{C}\mathscr{P}^\beta$, sont équivalents : une formule est un théorème dans l'un des systèmes si et seulement si elle est un théorème dans l'autre.

4.3 Certains auteurs optent pour une axiomatisation du calcul des propositions nettement plus riche en axiomes. Par exemple, on prend comme expressions bien formées les termes de $\mathscr{L}\mathscr{P}(\neg, \wedge, \vee, \to)$, et les axiomes sont alors

$P \to (Q \to P)$,

$(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$,
$P \wedge Q \to P$,
$P \wedge Q \to Q$,
$P \to (Q \to (P \wedge Q))$,
$P \to P \vee Q$,
$Q \to P \vee Q$,
$(P \to R) \to ((Q \to R) \to ((P \vee Q) \to R))$,
$(P \to Q) \to ((P \to \neg Q) \to \neg P)$,
$\neg P \to (P \to Q)$,
$\neg P \vee P$.

La règle de déduction est toujours le Modus Ponens. Ce système étant basé sur les travaux de Kleene (1952), on parlera ci-dessous du *système de Kleene*.

(i) Quels axiomes doit-on encore ajouter si on veut disposer du symbole $\leftrightarrow$?

(ii) Montrez que les axiomes ci-dessus sont des théorèmes du calcul propositionnel de 4.1 (ou 4.2), modulo la traduction de $\mathscr{L}\mathscr{P}(\neg, \wedge, \vee, \to)$ à $\mathscr{L}\mathscr{P}(\neg, \to)$ (cf. 3.7).

(iii) Vérifiez que dans ce système on a toujours le Métathéorème de Herbrand.

(iv) Démontrez dans le système de Kleene que $\neg\neg P \to P$. (En fait, en présence des autres axiomes la formule $\neg\neg P \to P$ est équivalente aux deux derniers axiomes donnés ci-dessus.)

(v) Pourquoi aurait-on pu écrire l'axiome $(P \to Q) \to ((P \to \neg Q) \to \neg P)$ aussi comme $(P \to \neg Q) \to ((P \to Q) \to \neg P)$?

(vi) Démontrez que $P \to \neg\neg P$; concluez que $\vdash P \leftrightarrow \neg\neg P$.

(vii) Montrez comment, par "substitution par équivalents" dans un des axiomes ci-dessus, on récupère aussi le troisième axiome du calcul de 4.1 comme théorème.

On peut conclure que le système de Kleene est équivalent aux systèmes de 4.1 et 4.2—modulo la traduction des termes.

4.4 Dans le système de Kleene (cf. 4.3) on peut laisser tomber le dernier axiome. On obtient alors le *calcul propositionnel intuitionniste*. (Ceci indique que "la logique intuitionniste est la logique classique sans tiers exclus", comme les gens disent souvent.) Soit maintenant $(X, \mathscr{T})$ un espace topologique ; pour fixer les idées on peut prendre l'ensemble $X = \mathbb{R}^n$ muni de la topologie habituelle $\mathscr{T} = \mathsf{ouv}(\mathbb{R}^n)$.

(i) Vérifiez que la topologie $\mathscr{T}$ est le domaine d'une $\mathscr{L}\mathscr{P}(\neg, \wedge, \vee, \to)$-structure par les interprétations suivantes (pour $U, U_1, U_2 \in \mathscr{T}$) :

$$\neg(U) = \mathsf{int}(X \setminus U),$$

$$U_1 \wedge U_2 = U_1 \cap U_2,$$
$$U_1 \vee U_2 = U_1 \cup U_2,$$
$$U_1 \to U_2 = \bigcup\{U \in \mathscr{T} \mid U_1 \cap U \subseteq U_2\}.$$

(ii) Montrez que, pour tout $U, U_1, U_2 \in \mathscr{T}$,

$$U \subseteq (U_1 \to U_2) \iff U_1 \wedge U \subseteq U_2.$$

(iii) Inspiré par 3.9 on dira qu'une $\mathscr{L}\mathscr{P}$-formule P est une $(X, \mathscr{T})$-tautologie si l'opération dérivée $P^{(X,\mathscr{T})}$ est l'application constante à valeur X. En d'autres termes, P est une $(X, \mathscr{T})$-tautologie si, pour toute valuation $\varphi\colon V(\mathscr{L}\mathscr{P}) \to \mathscr{T}$, on a que $\overline{\varphi}(P) = X$ (cf. 2.11). Vérifiez que les axiomes du calcul propositionnel intuitionniste sont des $(X, \mathscr{T})$-tautologies, et que le Modus Ponens préserve les $(X, \mathscr{T})$-tautologies. Concluez que tout théorème du calcul propositionnel intuitionniste est une $(X, \mathscr{T})$-tautologie.

(iv) Pourquoi est-ce que tout théorème du calcul propositionnel intuitionniste est aussi un théorème du calcul propositionnel classique ?

(v) Montrez que les formules suivantes – qui sont des tautologies classiques ! – ne sont en général pas des $(X, \mathscr{T})$-tautologies :

— $\neg\neg P \to P$,

— $P \vee \neg P$.

Remarque : Le calcul propositionnel intuitionniste se distingue du calcul propositionnel classique entre autre par son algèbre de Lindenbaum : l'algèbre de Lindenbaum du dernier est une algèbre de Boole (cf. 3.10), et celle du premier est une *algèbre de Heyting*. Une topologie $\mathscr{T}$ est un exemple particulier d'une algèbre de Heyting. Une étude profonde des algèbres de Heyting et leur rôle dans la logique intuitionniste mènerait trop loin du sujet de ce receuil d'exercices. Consultez le "Handbook of Categorical Algebra, vol. 3" [F. Borceux, 1994].

4.5 Prouvez que l'axiomatisation suivante du calcul propositionnel est adéquate et complète : considérant les termes de $\mathscr{L}\mathscr{P}(\neg, \to)$, on n'impose aucun axiome, mais trois règles de déduction :

Modus Ponens : si $\vdash P$ et $\vdash (P \to Q)$ alors $\vdash Q$;

Contradiction : si $\vdash ((\neg P) \to Q)$ et $\vdash ((\neg P) \to (\neg Q))$ alors $\vdash P$;

Déduction : si $\Gamma \cup \{P\} \vdash Q$ alors $\Gamma \vdash (P \to Q)$.

Indication : Il suffit de vérifier la correction de ces trois règles dans le système axiomatique de 4.1, et – réciproquement – de prouver les trois axiomes de 4.1 comme théorèmes dans ce système sans axiomes. (Comment peut-on prouver quelque chose

dans ce système sans axiomes ? Par exemple, on a que $\{P\} \cup \{Q\} \vdash P$ et donc par deux fois la Déduction il suit que $P \to (Q \to P)$ est un théorème.)

Remarque : Il existe une axiomatisation du calcul propositionnel, qui est complète et adéquate, sans règles de déduction : on prend tout simplement toutes les tautologies comme axiomes ! Mais, comme on n'a aucune règle de déduction, il sera impossible dans ce système de donner un sens à l'idée qu'une preuve peut suivre des hypothèses—car on ne peut rien déduire de ces hypothèses !

4.6 Pour le language des propositions, on peut prouver que toute théorie consistante possède un modèle ("complétude générale") et que réciproquement une théorie possédant un modèle est toujours consistante ("adéquation générale")—cf. le syllabus. Ici on va un peu plus loin : on étudie la maximalité d'une telle théorie.

(i) Soit $\mathscr{M} : V(\mathscr{L}\mathscr{P}) \to \{0,1\}$ une réalisation quelconque pour le langage des propositions. Vérifiez que $\{P \in \mathsf{Form}(\mathscr{L}\mathscr{P}) \mid \mathscr{M} \models P\}$ est une théorie maximale consistante. On la note $\mathsf{Th}(\mathscr{M})$.

(ii) Notez que toute théorie maximale consistante est de la forme $\mathsf{Th}(\mathscr{M})$.

(iii) Pour une théorie consistante Γ, indiquez une théorie maximale consistante qui la contient. Cette théorie maximale consistante, est-elle unique ?

5 Calcul des prédicats : sémantique

5.1 On considère, pour fixer les idées, un langage Θ du premier ordre pour lequel $x_1, x_2, ...$ dénotent des variables, f_n $(n = 0, 1, ...)$ des symboles d'opérations n-aires, et r_n $(n = 1, 2, ...)$ des symboles de relations n-aires.

(i) Donnez une définition (inductive) de l'ensemble $VL(P)$ des variables libres d'une formule P. Repérez les variables libres des formules suivantes :

— $(\forall x_2)(r_2 x_1 x_2 \to r_2 x_2 f_0)$,
— $(\forall x_2)(r_2 f_2 x_1 x_2 f_1 x_1) \to \forall x_1(r_2 x_3 f_2 x_2 f_1 x_3)$,
— $(\exists x_2)(r_2 f_0 x_2 \to r_1 x_1) \to (\forall x_1)(r_2 x_1 x_2)$,
— $r_2 x_1 x_2 \to (\exists x_1)(r_2 x_1 x_3)$.

(ii) Le terme $f_2 x_1 x_2$ est-il libre pour x_1 dans les formules suivantes ?

— $r_2 x_1 x_2 \to (\forall x_2) r_1 x_2$,
— $(\forall x_2)(r_2 x_1 x_2) \to r_1 x_1$,
— $(\forall x_3)(r_2 x_1 x_3) \to (\forall x_1) r_1 x_1$,
— $(\exists x_3)(\forall x_1)(r_2 x_1 x_3) \to r_1 x_1$.

5.2 Soit Θ le langage du premier ordre pour lequel $V(\Theta) = \{x_1, x_2, ...\}$, $O_{\Theta,n} = \{f_n\}$ pour $n = 0, 1, 2$ et $O_{\Theta,n} = \emptyset$ pour $n > 2$, $R_{\Theta,n} = \{r_n\}$ pour $n = 1, 2$ et $R_{\Theta,n} = \emptyset$

pour $n \notin \{1, 2\}$. Soit la réalisation $\mathscr{M}$ pour laquelle le domaine est $\mathbb{N}$, et les symboles sont interprétés de manière suivante :

$$\begin{aligned}
&\sigma_0(f_0) = 3,\\
&\sigma_1(f_1)\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto n + 3,\\
&\sigma_2(f_2)\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}\colon (m, n) \mapsto 2mn,\\
&\tau_1(r_1) = 2\mathbb{N},\\
&\tau_2(r_2) = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid m \text{ divise } n\}.
\end{aligned}$$

On considère l'assignation $a\colon V(\Theta) \to \mathbb{N}\colon x_i \mapsto 2i$.

(i) Calculez la valeur des termes suivants :

— $f_2 f_1 x_1 f_0$,
— $f_2 f_1 f_0 f_1 x_3$.

(ii) Les affirmations suivantes ont-elles un sens, et, le cas échéant, sont-elles vraies ou non ?

— $\mathscr{M} \models_a f_0$,
— $\mathscr{M} \models_a r_1 f_0$,
— $\mathscr{M} \models_a r_2 f_0 x_1$,
— $\mathscr{M} \models_a r_2 f_0 x_3$,
— $\mathscr{M} \models_a r_2 x_1 x_2$,
— $\mathscr{M} \models_a r_1 f_1 x_1$,
— $\mathscr{M} \models_a r_1 f_1 f_0$,
— $\mathscr{M} \models_a r_2 x_2 x_1$,
— $\mathscr{M} \models_a (\exists x_1) r_2 x_1 x_3$,
— $\mathscr{M} \models_a (\forall x_2) r_2 x_1 x_2$.

(iii) Les affirmations suivantes sont-elles vraies ? Rappel : $\mathscr{M} \models P$ signifie $\mathscr{M} \models_a P$ pour toute assignation a.

— $\mathscr{M} \models (\forall x_1) r_1 x_1$,
— $\mathscr{M} \models (\exists x_1) r_2 f_0 x_1$,
— $\mathscr{M} \models (\exists x_1) r_1 x_1$,
— $\mathscr{M} \models (\forall x_1)(\exists x_2) r_2 x_1 x_2$,
— $\mathscr{M} \models (\forall x_1)(\forall x_2)[r_1 x_1 \to r_1 f_1 f_1 f_2 x_1 x_2]$.

5.3 On considère un langage Θ comprenant un symbole de constante c, un symbole d'opération unaire f_1, deux symboles d'opérations binaires f_2 et g_2 et un symbole de relation binaire r_2. Soit $V(\Theta) = \{x_1, x_2, ...\}$. On considère la réalisation ayant

comme domaine $\mathbb{N}$ et les interprétations suivantes :

$$\begin{aligned}
&\sigma_0(c) = 0,\\
&\sigma_1(f_1)\colon \mathbb{N} \to \mathbb{N}\colon n \mapsto n+1,\\
&\sigma_2(f_2)\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}\colon (m,n) \mapsto m+n,\\
&\sigma_2(g_2)\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}\colon (m,n) \mapsto mn,\\
&\tau_2(r_2) = \{(m,n) \mid m \leq n\}.
\end{aligned}$$

(i) Pour chacune des formules suivantes, trouvez une assignation qui la satisfait et une assignation qui ne la satisfait pas :

— $r_2 f_1 x_1 x_2 \to r_2 f_1 f_1 x_1 x_2$,
— $(\forall x_1) r_2 g_2 x_1 c x_1 \to r_2 x_1 x_2$,
— $\neg(\forall x_2) r_2 g_2 x_1 x_2 g_2 x_2 x_3$.

(ii) Pour chacune des formules suivantes, examinez si elle est vraie dans la réali-sation considérée :

— $(\forall x_1) r_2 g_2 x_1 c x_1$,
— $r_2 f_1 x_2 x_1 \to \neg r_2 x_1 x_2$,
— $(\forall x_1) r_2 f_2 x_1 x_1 g_2 x_1 f_1 f_1 c$.

5.4 Soit P une formule d'un langage du premier ordre Θ. Montrez que les formules suivantes sont valides. (Rappel : Une formule P est valide – noté $\models P$ – si $\mathscr{M} \models P$ pour toute réalisation $\mathscr{M}$.)

— $(\forall x)(\forall y)P \leftrightarrow (\forall y)(\forall x)P$,
— $(\exists x)(\exists y)P \leftrightarrow (\exists y)(\exists x)P$,
— $(\exists x)(\forall y)P \to (\forall y)(\exists x)P$.

Montrez que l'implication réciproque de la dernière n'est pas valide. Indication : Pour tous les hommes il y a une femme... mais ce n'est pas la même femme pour tous les hommes !

5.5 Soit P une formule d'un langage du premier ordre Θ et t un terme libre pour la variable x dans P, montrez la validité de $[t \mid x]P \to (\exists x)P$.

5.6 Soit P une formule d'un langage du premier ordre, et $VL(P) = \{x_1, ..., x_n\}$. Alors on dit que $\overline{P} = (\forall x_1)...(\forall x_n)P$ est la *clôture universelle* de P (et donc $VL(\overline{P}) = \emptyset$). Montrez que, pour toute réalisation $\mathscr{M}$ du langage, $\mathscr{M} \models P$ si et seulement si $\mathscr{M} \models \overline{P}$.

5.7 Soient P et Q des formules, et x une variable, d'un langage du premier ordre.

(i) Montrez que si x n'est pas libre dans P, alors

— $\models (\forall x)(P \to Q) \leftrightarrow (P \to (\forall x)Q)$,
— $\models (\exists x)(P \to Q) \leftrightarrow (P \to (\exists x)Q)$.

(ii) Montrez que si x n'est pas libre dans Q, alors
— $\models (\forall x)(P \to Q) \leftrightarrow ((\exists x)P \to Q)$,
— $\models (\exists x)(P \to Q) \leftrightarrow ((\forall x)P \to Q)$.

(iii) La clause "x n'est pas libre dans P (Q)" est cruciale : montrez-le avec des (contre-)exemples. Indication : Par exemple, considérez, à propos des nombres entiers, les prédicats

$$P = Q = \text{“}x \text{ est pair”}$$

(notez que $x \in VL(P) = VL(Q)$!). Comparez $(\forall x)(P \to Q)$ et $P \to (\forall x)Q$.

(iv) On considère un langage dont r_1 est un prédicat unaire et r_2 un prédicat binaire ; les x_i sont des variables. Donnez une *formule prénexe* équivalente à

$$(\forall x_1)r_1x_1 \to (\forall x_2)(\exists x_3)r_2x_2x_3.$$

(Une formule prénexe est de la forme $(Q_1x_{i_1})...(Q_kx_{i_k})P$, oú P est sans quantificateurs et où chaque Q_j est $\forall$ ou $\exists$.)
Remarque : Pour indiquer une formule prénexe équivalente à une formule comme

$$[(\forall x_1)r_2x_1x_2 \to (\forall x_2)\neg r_1x_2] \to (\forall x_1)(\forall x_2)s_2x_1x_2$$

on devra faire appel à des résultats concernant le changement de variables liées et le remplacement de sous-formules par des sous-formules équivalentes (cf. exercice 6.5).

5.8 Soit $g\colon X \to Y$ une application. On sait qu'elle induit une application "image réciproque" $g^*\colon \mathscr{P}Y \to \mathscr{P}X$ et une application "image directe" $g_*\colon \mathscr{P}X \to \mathscr{P}Y$.

(i) Vérifiez que g^* respecte les opérations d'intersection, d'union et de prise du complémentaire.

(ii) Vérifiez que g_* respecte la réunion, mais pas les autres opérations.

(iii) Vérifiez que pour $A \subseteq \mathscr{P}X$ et $B \subseteq \mathscr{P}Y$ on a $A \subseteq g^*(B)$ si et seulement si $g_*(A) \subseteq B$, et $g^*(B) \subseteq A$ si et seulement si $B \subseteq (Y \setminus g_*(X \setminus A))$. On définit l'application $g_\forall\colon \mathscr{P}X \to \mathscr{P}Y$ par $g_\forall(A) = (Y \setminus g_*(X \setminus A))$.

(iv) En prenant $g\colon D^{n+1} \to D^n\colon (d_1, ..., d_n, d_{n+1}) \mapsto (d_1, ..., d_n)$ (la projection oubliant la composante d'indice $n+1$), observez que

(a) pour s, une relation n-aire sur D, on a : $(a_1, ..., a_n, a_{n+1}) \in g^*(s)$ si et seulement si $(a_1, ..., a_n) \in s$, sans condition sur a_{n+1} ;

(b) pour r, une relation $(n+1)$-aire sur D, on a : $(a_1, ..., a_n) \in g_*(r)$ si et seulement si il existe $a_{n+1} \in D$ tel que $(a_1, ..., a_n, a_{n+1}) \in r$;

(c) pour r, une relation $(n+1)$-aire sur D, on a : $(a_1, ..., a_n) \in g_\forall(r)$ si et seulement si pour tout $a_{n+1} \in D$ on a $(a_1, ..., a_n, a_{n+1}) \in r$.

Une autre bonne notation pour g_* est donc "$g_\exists$".

Remarque : Etant donné deux ordres partiels $(P, \leq)$ et $(Q, \leq)$, et deux applications croissantes (= préservant l'ordre) $f: P \to Q$ et $g: Q \to P$, on dit que f est l'*adjoint à gauche* de g, et g est l'*adjoint à droite* de f, si on a pour tout $p \in P$ et $q \in Q$ que

$$f(p) \leq q \text{ dans } Q \iff p \leq g(q) \text{ dans } P.$$

On note cette situation souvent comme $f \dashv g$. Ci-dessus on prouve donc que, pour une application $g: X \to Y$ quelconque, $g_\exists \dashv g^* \dashv g_\forall$.

Cette notion d'adjonction – ou mieux dit une généralisation de cette notion pour des foncteurs entre catégories plutôt que des applications croissantes entres ordres partiels – est un point essentiel de la théorie des catégories. Consultez par exemple le "Handbook of Categorical Algebra, vol. 1" [F. Borceux, 1994].

5.9 Soit $\mathscr{M}: \Theta \to \mathscr{S}$ une réalisation d'un langage du premier ordre Θ, désignons par D le domaine de $\mathscr{S}$. Soit P une formule de Θ dont les variables libres sont $x_1, x_2, ..., x_n$.

(i) Expliquez pourquoi, pour une assignation $a: V(\Theta) \to D$, la vérité de l'affirmation $\mathscr{M} \models_a P$ ne dépend que des valeurs par a des variables $x_1, x_2, ..., x_n$.

(ii) Pour un n-uple $\underline{d} = (d_1, ..., d_n) \in D^n$, notons $a_{\underline{d}}: V(\Theta) \to D$ une assignation qui envoie x_1 sur d_1, x_2 sur d_2, ... , x_n sur d_n (et dont la valeur des autres variables n'est pas spécifiée). On définit

$$P^{\mathscr{S}} = \{\underline{d} = (d_1, ..., d_n) \in D^n \mid \mathscr{M} \models_{a_{\underline{d}}} P\}.$$

Vérifiez, à l'aide de (i), que cette relation n-aire sur D est bien définie. On l'appelle une *relation dérivée n-aire*.

(iii) Montrez que,

— si $P = r_m t_1 ... t_m$ alors $P^{\mathscr{S}} = \left(t_1^{\mathscr{S}}, ..., t_m^{\mathscr{S}}\right)^* (\tau_m r_m)$ (bien sûr, r_m dénote un symbôle relationnel m-aire, et les $t_1, ..., t_m$ sont des termes du langage— c'est-à-dire, ce P est une formule atomique) ;

— si $P = \neg Q$ alors $P^{\mathscr{S}} = D^n \setminus Q^{\mathscr{S}}$;

— si $P = Q \wedge R$ alors $P^{\mathscr{S}} = Q^{\mathscr{S}} \cap R^{\mathscr{S}}$;

— si $P = Q \vee R$ alors $P^{\mathscr{S}} = Q^{\mathscr{S}} \cup R^{\mathscr{S}}$;

— si $P = Q \to R$ alors $P^{\mathscr{S}} = (D^n \setminus Q^{\mathscr{S}}) \cup R^{\mathscr{S}}$;

— si $P = \exists x_{n+1} Q$ alors $P^{\mathscr{S}} = g_{\exists}(Q^{\mathscr{S}})$;
— si $P = \forall x_{n+1} Q$ alors $P^{\mathscr{S}} = g_{\forall}(Q^{\mathscr{S}})$.

Les notations sont celles de 2.6 (ii), 2.13 (v) et 5.8 (iv).

(iv) Montrez que l'affirmation $\mathscr{M} \models P$ est vrai si et seulement si $P^{\mathscr{S}} = D^n$.

Remarque : On aurait pu définir la 'relation dérivée n-aire' $P^{\mathscr{S}}$ par induction sur la forme de P comme dans (iii), pour ensuite définir la vérité de $\mathscr{M} \models P$ par l'équivalence de (iv). Cette abstraction permet éventuellement de considérer non seulement des modèles 'ensemblistes' d'un langage du premier ordre Θ (comme nous faisons dans ce cours : le domaine $D_{\mathscr{S}}$ d'une structures $\mathscr{S}$ est un ensemble) mais des modèles dans un 'topos' quelconque ($D_{\mathscr{S}}$ est un objet d'un 'topos'). Référence : "Sheaves in geometry and logic" [S. MacLane et I. Moerdijk, 1992].

5.10 Donnez, par analogie avec 2.3, une (ou plusieurs) "bonne(s) définition(s)" de homomorphisme entre deux Θ-structures $\mathscr{M}_1 \colon \Theta \to \mathscr{S}_1$ et $\mathscr{M}_2 \colon \Theta \to \mathscr{S}_2$. Indication : Consultez éventuellement un livre tel que "Introduction to Model Theory" [Philipp Rothmaler, 2000].

(i) Vérifiez que les propriétés (i) et (ii) de 2.3 sont toujours vraies.

(ii) Que peut-on dire à propos des relations dérivées dans ce contexte, cf. 2.15 (ii) ?

(iii) Quelle est maintenant la "bonne définition" de *sous-structure* (cf. 2.4) ?

(iv) Et qu'est-ce qu'un *isomorphisme* dans ce contexte (cf. 2.5) ?

6 Calcul des prédicats : axiomatique

Dans les exercices suivants, si une formule est de la forme $[P_1 \mid p_1, ..., P_n \mid p_n]T$, où T est une tautologie propositionnelle dont les variables sont dans $\{p_1, ..., p_n\}$, on pourra toujours admettre qu'on dispose d'une démonstration de cette formule (cf. Métathéorème de Transfert).

Dans le Métathéorème de Herbrand pour le calcul des prédicats (cf. syllabus), il y a des restrictions... mais on n'est pas obligé d'y avoir recours ! En effet, on dispose d'une version plus raffinée de ce métathéorème : Soient $\Gamma \subseteq \mathsf{Form}(\Theta)$ une théorie du premier ordre et $P, Q \in \mathsf{Form}(\Theta)$ des formules. Si $\Gamma \cup \{P\} \vdash Q$ et la déduction ne comprend pas de généralisation par rapport à une variable à occurence libre dans P, alors $\Gamma \vdash P \to Q$ ("Logic for Mathematicians (revised edition)" [A. G. Hamilton, 1988]). Nous l'admettons.

6.1 L'axiomatique du calcul des prédicats vue au cours fait intervenir les symboles logiques $\neg, \to$ et $\forall$, et les axiomes sont

— $P \to (Q \to P)$,
— $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$,
— $(\neg Q \to \neg P) \to ((\neg Q \to P) \to Q)$,
— $(\forall x)(P \to Q) \to (P \to (\forall x)Q)$ où x n'a pas d'occurence libre dans P,
— $(\forall x)P \to [t/x]P$ où t est libre pour x dans P.

Les deux règles sont le Modus Ponens et la Généralisation :

de $\vdash P$ et $\vdash P \to Q$, déduisez $\vdash Q$,
de $\vdash P$, déduisez $(\forall x)P$.

Quels axiomes doit-on ajouter si on veut utiliser aussi les symboles $\wedge, \vee, \leftrightarrow$ et $\exists$? Indication : Consultez 4.3.

6.2 Donnez une définition inductive de l'ensemble $SF(P)$ des sous-formules d'une formule P donnée dans un langage du premier ordre Θ donné.

6.3 On considère un langage de premier ordre. Soit P' une sous-formule propre (voir 6.2) de P qu'on remplace à un endroit par P'', et soit P^R le résultat du remplacement.

(i) Prouvez que, si $\{x_1, ..., x_k\}$ comprend toutes les variables libres de P' et/ou P'' qui ont une occurence liée dans P, alors

$$\vdash ((\forall x_1)...(\forall x_k)(P' \leftrightarrow P'') \to (P \leftrightarrow P^R).$$

Indication : La preuve se fait par induction sur la forme de P. Si P est atomique, il n'y a rien à prouver ; ensuite on examine le cas où P est $\neg Q$, le cas où P est $Q \to R$, et finalement le cas où P est $\forall x Q$.

(ii) Déduisez que si $\vdash P' \leftrightarrow P''$, alors $\vdash P \leftrightarrow P^R$.

6.4 Soit P une formule d'un langage du premier ordre Θ telle que $VL(P) = \{x\}$. On suppose que $y \in V(\Theta)$ est libre pour x dans P. Dans ce cas, on dit que la formule $[y \mid x]P$ est *semblable* à P.

(i) Montrez que la relation de similitude est une relation d'équivalence. Remarque : Dans la situation de similitude, telle que décrite ci-dessus, il est d'usage d'écrire $P(x)$ et $P(y)$ au lieu de P (avec $VL(P) = \{x\}$) et $[y \mid x]P$.

(ii) Montrez que si $P(x)$ et $P(y)$ sont semblables, alors

$$\vdash (\forall x)P(x) \leftrightarrow (\forall y)P(y) \quad \text{et} \quad \vdash (\exists x)P(x) \leftrightarrow (\exists y)P(y).$$

6.5 Soit un langage du premier ordre dont P est une formule, les x_i sont des variables, r_1 est un symbole relationnel unaire, et r_2, s_2 sont des symboles relationnels binaires.

(i) Démontrez que $(\forall x_1)(\forall x_2)P \leftrightarrow (\forall x_2)(\forall x_1)P$.

(ii) En utilisant l'exercice 6.4, montrez que

$$(\forall x_1)(\forall x_2)s_2x_1x_2 \leftrightarrow (\forall x_3)(\forall x_4)s_2x_3x_4 \quad \text{et} \quad (\forall x_2)\neg r_1x_2 \leftrightarrow (\forall x_5)\neg r_1x_5.$$

(iii) Trouvez une formule prénexe équivalente à

$$[(\forall x_1)r_2x_1x_2 \rightarrow (\forall x_2)\neg r_1x_2] \rightarrow (\forall x_1)(\forall x_2)s_2x_1x_2$$

(cf. exercice 5.7).

6.6 Une *théorie* Γ *du premier ordre* est, tout simplement, un sous-ensemble des formules d'un langage Θ du premier ordre : $\Gamma \subseteq \mathsf{Form}(\Theta)$. Un *modèle* $\mathscr{M}$ d'une telle théorie est une réalisation $\mathscr{M}\colon \Theta \rightarrow \mathscr{S}$ telle que $\mathscr{M} \models \Gamma$. Pourquoi peut-on, sans perte de généralité, se limiter à l'étude des théories dont tous les éléments sont des formules fermées (c'est-à-dire, sans variables libres) ? Indication : Voir 5.6.

6.7 En principe un langage de premier ordre Θ a des symboles d'opérations et des symboles de relations (en plus des symboles logiques) ; et donc aussi dans une théorie $\Gamma \subseteq \mathsf{Form}(\Theta)$ on dispose de ces symboles. En fait, sans perte de généralité on peut se limiter à l'étude des langages et théories sans symboles d'opérations, comme le suggère cet exercice.

(i) Ecrivez des conditions qui expriment qu'une relation $(n+1)$-aire $R \subseteq D^{n+1}$ est le graphe d'une fonction n-aire $f\colon D^n \rightarrow D$.

(ii) Inspiré par (i), remplacez maintenant dans le langage Θ chaque symbole d'opération n-aire par un symbole de relation $(n+1)$-aire – et appelez le nouveau langage Θ^* – et imposez des axiomes supplémentaires qui disent que les nouvaux symboles de relations sont les "graphes" des anciens symboles d'opérations.

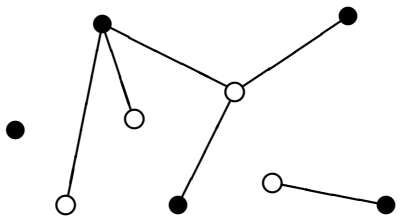
(iii) Soit $\Gamma \subseteq \mathsf{Form}(\Theta)$ une théorie du premier ordre. Indiquez comment on peut construire une théorie $\Gamma^* \subseteq \mathsf{Form}(\Theta^*)$ avec "les mêmes modèles" que Γ.

6.8 Soit un langage du premier ordre Θ, avec un ensemble de variables $V(\Theta) = \{x_1, x_2, ..., x_n, ...\}$, un symbole relationnel binaire, notons $R_2 = \{r\}$, et aucun autre symbole. Soit la théorie de premier ordre $\Gamma = \{P_1, P_2\} \subseteq \mathsf{Form}(\Theta)$, avec

$$\begin{aligned} P_1 &= \forall x_1(rx_1x_1) \\ P_2 &= \forall x_1\forall x_2\forall x_3((rx_1x_2 \wedge rx_2x_3) \rightarrow rx_1x_3) \end{aligned}$$

Qu'est-ce qu'un modèle de Γ ? Qu'est-ce qu'un homomorphisme entre deux modèles de Γ ? De quelle théorie s'agit-il donc ?

6.9 On considère les graphes de type suivant : les points d'un graphe existent en deux couleurs, donc chaque point a une couleur et aucun point a les deux couleurs à la fois, et entre deux points de couleurs différentes il peut exister au maximum un lien. Par exemple :



Donnez une théorie de premier ordre dont les modèles sont ces graphes.

6.10 Une théorie de premier ordre $\Gamma \subseteq \mathsf{Form}(\Theta)$ est *égalitaire* si on dispose d'un symbole relationnel binaire $\mathring{=}$ dans l'alphabet de Θ, et Γ contient les axiomes suivants :

$$
\begin{aligned}
E_1 &= \forall x_1 (x_1 \mathring{=} x_1) \\
E_2 &= \forall x_1 \forall x_2 (x_1 \mathring{=} x_2 \to x_2 \mathring{=} x_1) \\
E_3 &= \forall x_1 \forall x_2 \forall x_3 ((x_1 \mathring{=} x_2 \wedge x_2 \mathring{=} x_3) \to x_1 \mathring{=} x_3) \\
E_4^{f_n} &= \forall x_1 ... \forall x_n, \forall y_1 ... \forall y_n ((x_1 \mathring{=} y_1 \wedge ... \wedge x_n \mathring{=} y_n) \to f_n x_1 ... x_n \mathring{=} f_n y_1 ... y_n) \\
&\qquad\qquad \text{(pour tout } f_n \in O_n) \\
E_5^{r_n} &= \forall x_1 ... \forall x_n \forall y_1 ... \forall y_n ((x_1 \mathring{=} y_1 \wedge ... \wedge x_n \mathring{=} y_n \wedge r_n x_1 ... x_n) \to r_n y_1 ... y_n) \\
&\qquad\qquad \text{(pour tout } r_n \in R_n)
\end{aligned}
$$

Un modèle $\mathscr{M}$ de Γ est *égalitaire* (ou *normal*) si l'interprétation du symbole $\mathring{=}$ dans la structure $\mathscr{S}$ est la diagonale sur le domaine de $\mathscr{S}$: $\tau_2(\mathring{=}) = \{(d, d) \mid d \in D_{\mathscr{S}}\}$.

(i) Par analogie avec 6.8, donnez une théorie égalitaire du premier ordre $\Gamma \subseteq \mathsf{Form}(\Theta)$ dont les modèles égalitaires sont les ordres partiels. Qu'est-ce qu'un homomorphisme dans ce cas ?

(ii) Soit Γ une théorie égalitaire du premier ordre. Montrez comment chaque modèle de Γ détermine un modèle égalitaire. Indication : L'interprétation du symbole $\mathring{=}$ est toujours une relation d'équivalence qui est "compatible" avec les interprétations des symboles d'opérations et de relations du langage. Soit

$\mathscr{M}$ un modèle quelconque, de domaine D disons, alors on peut lui associer le modèle dont le domaine est le quotient de D par l'interprétation de $\stackrel{\circ}{=}$.

6.11 Soient un langage du premier ordre Θ avec un ensemble dénombrable de variables, sans symboles opérationnels et un seul symbole relationnel $\stackrel{\circ}{=} \in R_2$, et la théorie $\Gamma = \{E_1, E_2, E_3\}$ (notations comme dans 6.10 ... pourquoi ne parle-t-on pas de E_4 et E_5 ici ?). Considerons aussi le langage du premier ordre Θ' avec les mêmes variables que Θ, mais sans aucun autre symbole dans son alphabet. Quelle est la diférence entre une réalisation égalitaire de Θ qui est modèle pour Γ, une réalisation de Θ qui est modèle pour Γ (mais pas forcément égalitaire), et une réalisation de Θ' ?

6.12 Soit Θ un langage égalitaire du premier ordre avec un seul prédicat binaire $<$ (autre que l'égalité $\stackrel{\circ}{=}$ et les autres symboles logiques, bien sûr) et considérons la théorie égalitaire $\Gamma \subseteq \mathsf{Form}(\Theta)$ suivante :

$(\forall x)\neg(x < x)$ (anti-reflexivité)
$(\forall x)(\forall y)((x < y) \vee (y < x) \vee (x \stackrel{\circ}{=} y))$ (trichotomie)
$(\forall x)(\forall y)(\forall z)(((x < y) \wedge (y < z)) \rightarrow (x < z))$ (transitivité)
$(\forall x)(\exists y)(\exists z)((y < x) \wedge (x < z))$ (non-borné)
$(\forall x)(\forall y)((x < y) \rightarrow (\exists z)((x < z) \wedge (z < y)))$ (densité)

(plus les axiomes de l'égalité). Observez que $(\mathbb{Q}, <)$ et $(\mathbb{R}, <)$ sont des modèles égalitaires de cette théorie, mais que $(\mathbb{N}, <)$ et $(\mathbb{Z}, <)$ ne le sont pas.

Remarque : On peut prouver que cette théorie n'admet qu'un seul modèle dénombrable (à isomorphisme près) : les nombres rationnels (Cantor, 1895). On dit que la théorie est *catégorique pour les modèles dénombrables*, ou plus simplement qu'elle est *ω-catégorique*. Ceci veut donc dire que les axiomes ci-dessus résument parfaitement le "contenu mathématique" de l'objet mathématique $(\mathbb{Q}, <)$.

6.13 L'*Arithmétique de Peano* est la théorie égalitaire du premier ordre suivante. Le langage que l'on considère est égalitaire et contient (en plus des symboles logiques et l'égalite $\stackrel{\circ}{=}$) un symbole de constante c, un symbole d'opération unaire s et deux symboles d'opérations binaires a et m. La théorie elle-même est donnée par les axiomes suivantes (en plus des axiomes pour l'égalité) :

$(\forall x)\neg(sx \stackrel{\circ}{=} c)$
$(\forall x)(\forall y)((sx \stackrel{\circ}{=} sy) \rightarrow (x \stackrel{\circ}{=} y))$
$(\forall x)(a(x, c) \stackrel{\circ}{=} x)$
$(\forall x)(\forall y)(a(x, sy) \stackrel{\circ}{=} s(a(x, y)))$
$(\forall x)(m(x, c) \stackrel{\circ}{=} c)$

$(\forall x)(\forall y)(m(x, sy) \stackrel{\circ}{=} a(m(x, y), x))$
$(P(c) \wedge (\forall x)(P(x) \to P(sx))) \to (\forall x)P(x)$

Le dernier axiome est en fait un schéma d'axiomes : un pour chaque formule P telle que $VL(P) = \{x\}$ (cf. 6.4). Ce schéma contient donc un Principe d'Induction Mathématique.

(i) Observez que $\mathbb{N}$ est (le domaine d') un modèle de l'Arithmétique de Peano. On l'appelle le *modèle standard*. Indication : Bien sûr, on interprète la constante c comme le nombre zéro, l'opération s comme le successeur, et a et m comme addition et mulitiplication—d'où l'arithmétique !

(ii) Montrez que, dans l'Arithmétique de Peano,

$\vdash (\forall x)(\forall y)(\forall z)(a(a(x, y), z) \stackrel{\circ}{=} a(x, a(y, z)))$
$\vdash (\forall x)(\forall y)(a(x, y) \stackrel{\circ}{=} a(y, x))$
$\vdash (\forall x)(\forall y)(\forall z)(m(m(x, y), z) \stackrel{\circ}{=} m(x, m(y, z)))$
$\vdash (\forall x)(\forall y)(m(x, y) \stackrel{\circ}{=} m(y, x))$
$\vdash (\forall x)(\forall y)(\forall z)(m(x, a(y, z)) \stackrel{\circ}{=} a(m(x, y), m(x, z)))$

Indication : Vous pouvez vous baser sur le travail fait en 1.8 et 1.9.

(iii) Ecrivez dans le langage donné ci-dessus la Conjecture de Goldbach : "Chaque nombre naturel paire plus grand que 2 est la somme de deux nombres premiers." (Jusqu'à présent personne ne sait si $\mathbb{N} \models$ Goldbach.)

(iv) G. Peano (1891) proposait comme Postulat d'Induction : "Si P est une propriété des nombres naturels qui est vraie pour 0, et qui est vrai pour le successeur de x chaque fois qu'elle est vraie pour x, alors P est vraie pour tous les nombres naturels." Peut-on exprimer ce postulat dans un langage du premier ordre ? Quelle est la différence avec l'axiome d'induction ci-dessus ?

Remarque : L'Arithmétique de Peano du premier ordre n'est pas une théorie ω-catégorique : il existe des modèles dénombrables non-isomorphes à $\mathbb{N}$. On les appelle des *modèles non-standards*. (Consultez la litérature.) Si on se permet de travailler avec un langage et une théorie du second ordre, alors on peut parfaitement encoder le Postulat d'Induction de Peano (cf. (iv) ci-dessus). Et la théorie de l'Arithmétique du second ordre que l'on obtient est alors ω-catégorique : son seul modèle dénombrable est $\mathbb{N}$ (à isomorphisme près).

Lié au problème de non-categoricité, est l'incomplétude de l'Arithmétique de Peano. K. Gödel (1930) a prouvé (des métathéorèmes qui impliquent) l'existence d'une formule P telle que ni P ni $\neg P$ est un théorème pour l'Arithmétique de Peano. Pour une construction explicite d'une telle formule, consultez par exemple "Logic for Mathematicians (revised edition)" [A. G. Hamilton, 1988]. Essentiellement, l'idée derrière la construction est d'écrire une formule qui est l'équivalent de la phrase "je

mens toujours" : P dit que "P n'est pas vrai".

6.14 L'Arithmétique de Peano pose des problèmes comme la non-ω-catégoricité et l'incomplétude (cf. 6.13). Certaines personnes pensent qu'à l'origine du mal se trouve la notion d'infini ; les *Finitistes Strictes* vont jusqu'à refuser toute notion d'infini. J.-P. Van Bendegem – un finitiste stricte notoire – propose une modification de l'Arithmétique de Peano ("Classical Arithmetic is Quite Unnatural" [J.-P. Van Bendegem, 2003]) qu'il appelle l'*Arithmétique Strictement Finitiste*.

Soit N un nombre naturel, différent de 0. On considère maintenant le langage Θ_N, égalitaire et du premier ordre, avec

- $N+1$ symboles d'opération nullaire (des constantes) $c_0, c_1, ..., c_N$;
- un symbole d'opération unaire s ;
- deux symboles d'opération binaire : a et m ;
- les symboles logiques et l'égalité.

La théorie égalitaire $\Gamma_N \subseteq \mathsf{Form}(\Theta_N)$ est donnée par les axiomes suivants :

$(\forall x)\neg(sx \mathrel{\mathring{=}} c_0)$
$(\forall x)(\forall y)(\neg(x \mathrel{\mathring{=}} c_N) \wedge \neg(y \mathrel{\mathring{=}} c_N)) \rightarrow ((sx \mathrel{\mathring{=}} sy) \rightarrow (x \mathrel{\mathring{=}} y))$
$(sc_{N-1} \mathrel{\mathring{=}} c_N) \wedge (sc_N \mathrel{\mathring{=}} c_N)$
$(\forall x)(a(x, c_0) \mathrel{\mathring{=}} x)$
$(\forall x)(\forall y)(a(x, sy) \mathrel{\mathring{=}} s(a(x, y)))$
$(\forall x)(m(x, c_0) \mathrel{\mathring{=}} c_0)$
$(\forall x)(\forall y)(m(x, sy) \mathrel{\mathring{=}} a(m(x, y), x))$
$(P(c_0) \wedge (\forall x)(P(x) \rightarrow P(sx))) \rightarrow (\forall x)P(x)$

(plus les axiomes pour l'égalité).

(i) Observez que l'ensemble $D_N = \{0, 1, ..., N\}$ est (le domaine d'un) modèle pour Γ_N. Indication : Toute l'idée est que "le plus grand nombre est fini", et c'est la constante c_N qui jouera le rôle de "plus grand nombre" (à savoir, N). Les constantes $c_0, ..., c_{N-1}$ sont interpretés comme $0, ..., N-1$. On interprète s toujours comme le successeur, et a et m comme addition et multiplication... mais N est "le plus grand nombre qui soit", donc on doit couper ces opérations à N : pour $n, n' \in D_N$,

$$sn = \min\{n+1, N\},$$

$$a(n, n') = \min\{n + n', N\},$$

$$m(n, n') = \min\{n \cdot n', N\}.$$

(ii) Montrez que, dans l'Arithmétique Strictement Finitiste, on a toujours les théorèmes de 6.13 (ii).

Remarque : On peut prouver que Γ_N est consistant et catégorique : chaque modèle a exactement $N+1$ éléments, et est isomorphe au modèle D_N. De plus, les métathéorèmes de Gödel ne s'appliquent pas à la théorie Γ_N ! L'Arithmétique Strictement Finitiste a donc toute une série de bonnes propriétés que l'Arithmétique de Peano n'a pas. En quelque sorte, on peut penser à l'Arithmétique de Peano comme "$\lim_{N\to\infty}\Gamma_N$", et donc $\mathbb{N}$ est "$\lim_{N\to\infty}\{0,...,N\}$". Mais en prenant cette limite, on perd certaines bonnes propriétés.

Table des matières

Ce recueil d'exercices pour le cours SC 1110 de Thierry Lucas trouve son origine dans une liste d'exercices compilée par Jean-Roger Roisin, le titulaire ad interim *de ce cours en 2000–2001 lorsque Thierry Lucas était en congé sabbatique. C'est cette même année que je suis devenu l'assistant pour les séances d'exercices. D'après mes propres goûts et mes expériences en classe, j'ai modifié – au cours des années – cette première liste d'exercices ; et vous tenez le résultat de mon travail etre vos mains ! Je remercie Mathieu Dupont pour avoir corrigé mon orthographe.*

En espérant que l'effort que demandent à l'étudiant ces exercices, portera tôt ou tard ses fruits,

Isar Stubbe.