La logique du premier ordre.

1 Les termes.

On commence par définir les *termes*, qui correspondent à des objets mathématiques. Tandis que les formules relient des termes et correspondent plus à des énoncés mathématiques.

Définition 1. Le langage $\mathscr{L}$ (du premier ordre) est la donnée d'une famille (pas nécessairement finie) de symboles de trois sortes :

- ▷ les symboles de *constantes*, notées c ;
- ▷ les symboles de *fonctions*, avec un entier associé, leur *arité*, notées $f(x_1, \ldots, x_n)$ où n est l'arité ;
- ▷ les symboles de *relations*, avec leur arité, notées R, appelés *prédicats*.

Les trois ensembles sont disjoints.

Remarque 1.
- ▷ Les constantes peuvent être vues comme des fonctions d'arité 0.
- ▷ On aura toujours dans les relations : « $=$ » d'arité 2, et « $\perp$ » d'arité 0.
- ▷ On a toujours un ensemble de variables $\mathscr{V}$.

Exemple 1. Le langage $\mathscr{L}_\mathrm{g}$ de la théorie des groupes est défini par :

- ▷ une constante : c,

- deux fonctions : f_1 d'arité 2 et f_2 d'arité 1 ;
- la relation $=$.

Ces symboles sont notés usuellement e, $*$, $\square^{-1}$ ou bien 0, $+$, $-$.

Exemple 2. Le langage $\mathscr{L}_{\text{co}}$ des corps ordonnés est défini par :

- deux constantes 0 et 1,
- quatre fonctions $+$, $\times$, $-$ et $\square^{-1}$,
- deux relations $=$ et $\leq$.

Exemple 3. Le langage $\mathscr{L}_{\text{ens}}$ de la théorie des ensembles est défini par :

- une constante $\emptyset$,
- trois fonctions $\cap$, $\cup$ et $\square^{\mathsf{c}}$,
- trois relations $=$, $\in$ et $\subseteq$.

Définition 2. Par le haut. L'ensemble $\mathscr{T}$ des termes sur le langage $\mathscr{L}$ est le plus petit ensemble de mots sur $\mathscr{L} \cup \mathscr{V} \cup \{\,(,), ,\,\}$ tel

- qu'il contienne $\mathscr{V}$ et les constantes ;
- qui est stable par application des fonctions, c'est-à-dire que pour des termes $t_1, \ldots, t_n$ et un symbole de fonction f d'arité n, alors $f(t_1, \ldots, t_n)$ est un terme. [1]

Par le bas. On pose

$$\mathscr{T}_0 = \mathscr{V} \cup \{c \mid c \text{ est un symbole de constante de } \mathscr{L}\},$$

puis

$$\mathscr{T}_{k+1} = \mathscr{T}_k \cup \left\{ f(t_1, \ldots t_n) \;\middle|\; \begin{array}{c} f \text{ fonction d'arité } n \\ t_1, \ldots, t_n \in \mathscr{T}_k \end{array} \right\},$$

et enfin
$$\mathscr{T} = \bigcup_{n \in \mathbb{N}} \mathscr{T}_n.$$

Remarque 2. Dans la définition des termes, un n'utilise les relations.

Exemple 4.
- ▷ Dans $\mathscr{L}_{\mathrm{g}}$, $*(*(x, \square^{-1}(y)), e)$ est un terme, qu'on écrira plus simplement en $(x * y^{-1}) * e$.
- ▷ Dans $\mathscr{L}_{\mathrm{co}}$, $(x + x) + (-0)^{-1}$ est un terme.
- ▷ Dans $\mathscr{L}_{\mathrm{ens}}$, $(\emptyset^{\mathsf{c}} \cup \emptyset) \cap (x \cup y)^{\mathsf{c}}$ est un terme.

Définition 3. Si t et u sont des termes et x est une variable, alors $t[x : u]$ est le mot dans lequel les lettres de x ont été remplacées par le mot u. Le mot $t[x : u]$ est un terme (preuve en exercice).

Exemple 5. Avec $t = (x * y^{-1}) * e$ et $u = x * e$, alors on a
$$t[x : u] = ((x * e) * y^{-1}) * e.$$

Définition 4.
- ▷ Un terme *clos* est un terme sans variable (par exemple $(0 + 0)^{-1}$).
- ▷ La *hauteur* d'un terme est le plis petit k tel que $t \in \mathscr{T}_k$.

Exercice 1.
- ▷ Énoncer et prouver le lemme de lecture unique pour les termes.
- ▷ Énoncer et prouver un lemme de bijection entre les termes et un ensemble d'arbres étiquetés.

1. Attention : le « ... » n'est pas un terme mais juste une manière d'écrire qu'on place les termes à côté des autres.

2 Les formules.

Définition 5. ▷ Les formules sont des mots sur l'alphabet

$$\mathscr{L} \cup \mathscr{V} \cup \{\, (,), ,, \exists, \forall, \wedge, \vee, \neg, \rightarrow \}.$$

- ▷ Une *formule atomique* est une formule de la forme $R(t_1, \ldots, t_n)$ où R est un symbole de relation d'arité n et $t_1, \ldots, t_n$ des termes.
- ▷ L'ensemble des *formules* $\mathscr{F}$ du langage $\mathscr{L}$ est défini par
  - on pose $\mathscr{F}_0$ l'ensemble des formules atomiques ;
  - on pose $\mathscr{F}_{k+1} = \mathscr{F}_k \cup \left\{ \begin{array}{c|c} (\neg F) & \\ (F \rightarrow G) & \\ (F \vee G) & F, G \in \mathscr{F}_k \\ (F \wedge G) & x \in \mathscr{V} \\ \exists x\; F & \\ \exists x\; G & \end{array} \right\}$;
  - et on pose enfin $\mathscr{F} = \bigcup_{n\in\mathbb{N}} \mathscr{F}_n$.

Exercice 2. La définition ci-dessus est « par le bas ». Donner une définition par le haut de l'ensemble $\mathscr{F}$.

Exemple 6. ▷ Dans $\mathscr{L}_\mathrm{g}$, un des axiomes de la théorie des groupes s'écrit

$$\forall x\, \exists x\, (x * y = e \wedge y * x = e).$$

- ▷ Dans $\mathscr{L}_\mathrm{co}$, l'énoncé « le corps est de caractéristique 3 » s'écrit
$$\forall x\, (x + (x + x) = 0).$$
- ▷ Dans $\mathscr{L}_\mathrm{ens}$, la loi de De Morgan s'écrit
$$\forall x\, \forall y\, (x^\mathsf{c} \cup y^\mathsf{c} = (x \cap y)^\mathsf{c}).$$

Exercice 3. ▷ Donner et montrer le lemme de lecture unique.
▷ Énoncer et donner un lemme d'écriture en arbre.

Remarque 3 (Conventions d'écriture.). On note :
- ▷ $x \leq y$ au lieu de $\leq(x, y)$;
- ▷ $\exists x \geq 0\ (F)$ au lieu de $\exists x\ (x \geq 0 \land F)$;
- ▷ $\forall x \geq 0\ (F)$ au lieu de $\forall x\ (x \geq 0 \to F)$;
- ▷ $A \leftrightarrow B$ au lieu de $(A \to B) \land (B \to A)$;
- ▷ $t \neq u$ au lieu de $\neg(t = u)$.

On enlèves les parenthèses avec les conventions de priorité

0. les symboles de relations (le plus prioritaire) ;
1. les symboles $\neg, \exists, \forall$;
2. les symboles $\land$ et $\lor$;
3. le symbole $\to$ (le moins prioritaire).

Exemple 7. Ainsi, $\forall x\ A \land B \to \neg C \lor D$ s'écrit

$$(((\forall x\ A) \land B) \to ((\neg C) \lor D)).$$

Remarque 4. Le calcul propositionnel est un cas particulier de la logique du premier ordre où l'on ne manipule que des relations d'arité 0 (pas besoin des fonctions et des variables) : les « variables » du calcul propositionnel sont des formules atomiques ; et on n'a pas de relation « = ».

Remarque 5. On ne peut pas exprimer *a priori* :
- ▷ des quantifications sur en ensemble[2] ;
- ▷ « $\exists n\ \exists x_1 \ldots \exists x_n$ » une formule qui dépend d'un paramètre ;
- ▷ le principe de récurrence : si on a $\mathscr{P}(0)$ pour une propriété $\mathscr{P}$ et que si $\mathscr{P}(n) \to \mathscr{P}(n+1)$ alors on a $\mathscr{P}(n)$ pour tout n.

Quelques définitions techniques qui permettent de manipuler les formules.

Définition 6. L'ensemble des sous-formules de F, noté $\mathrm{S}(F)$ est défini par induction :

- si F est atomique, alors on définit $\mathrm{S}(F) = \{F\}$;
- si $F = F_1 \oplus F_2$ (avec $\oplus$ qui est $\vee$, $\to$ ou $\wedge$) alors on définit $\mathrm{S}(F) = \mathrm{S}(F_1) \cup \mathrm{S}(F_2) \cup \{F\}$;
- si $F = \neg F_1$, ou $F = \mathsf{Q}x\, F_1$ avec $\mathsf{Q} \in \{\forall, \exists\}$, alors on définit $\mathrm{S}(F) = \mathrm{S}(F_1) \cup \{F\}$.

C'est l'ensemble des formules que l'on voit comme des sous-arbres de l'arbre équivalent à la formule F.

Définition 7.

- La *taille* d'une formule, est le nombre de connecteurs ($\neg$, $\vee$, $\wedge$, $\to$), et de quantificateurs ($\forall$, $\exists$).
- La racine de l'arbre est
  - rien su la formule est atomique ;
  - « $\oplus$ » si $F = F_1 \oplus F_2$ avec $\oplus$ un connecteur (binaire ou unaire) ;
  - « Q » si $F = \mathsf{Q}x\, F_1$ avec Q un quantificateur.

Définition 8.

- Une *occurrence* d'une variable est un endroit où la variable apparait dans la formule (*i.e.* une feuille étiquetée par cette variable).
- Une occurrence d'une variable est *liée* si elle se trouve dans une sous-formule dont l'opérateur principal est un quantificateur appelé à cette variable (*i.e.* un $\forall x\, F'$ ou un $\exists x\, F'$).
- Une occurrence d'une variable est *libre* quand elle n'est pas liée.
- Une variable est libre si elle a au moins une occurrence libre, sinon elle est liée.

2. En dehors de $\mathscr{L}_{\text{ens}}$, en tout cas.

Remarque 6. On note $F(x_1, \ldots, x_n)$ pour dire que les variables libres sont F sont parmi $\{x_1, \ldots, x_n\}$.

Définition 9. Une formule est *close* si elle n'a pas de variables libres.

Définition 10 (Substitution). On note $F[x := t]$ la formule obtenue en remplaçant toutes les occurrences libres de x par t, après renommage éventuel des occurrences des variables liées de F qui apparaissent dans t.

Définition 11 (Renommage). On donne une définition informelle et incomplète ici. On dit que les formules F et G sont α-équivalentes si elle sont syntaxiquement identiques à un renommage près des occurrences liées des variables.

Exemple 8. On pose

$$F(x, z) := \forall y\ (x * y = y * z) \land \forall x\ (x * x = 1),$$

et alors

- ▷ $F(z, z) = F[x := z] = \forall y\ (z * y = y * z) \land \forall x\ (x * x = 1)$;
- ▷ $F(y^{-1}, x) = F[x := y^{-1}] = \forall u (y^{-1} * u = u * z) \land \forall x (x * x = 1)$.

On a procédé à un renommage de y à u.

3 Les démonstrations en déduction naturelle.

Définition 12. Un *séquent* est un coupe noté $\Gamma \vdash F$ (où $\vdash$ se lit « montre » ou « thèse ») tel que Γ est un ensemble fini de formules appelé *contexte* (*i.e.* l'ensemble des hypothèses), la formule F est la *conséquence* du séquent.

Remarque 7. Les formules ne sont pas nécessairement closes. Et on note souvent Γ comme une liste.

Définition 13. On dit que $\Gamma \vdash F$ est *prouvable*, *démontrable* ou *dérivable*, s'il peut être obtenu par une suite finie de règles (*c.f.* ci-après). On dit qu'une formule F est *prouvable* si $\emptyset \vdash F$ l'est.

Définition 14 (Règles de la démonstration). Une règle s'écrit

$$\frac{\textit{prémisses} : \text{des séquents}}{\textit{conclusion} : \text{un séquent}}\ \text{nom de la règle}.$$

Axiome.

$$\frac{}{\Gamma, A \vdash A}\ \mathsf{ax}$$

Affaiblissement.

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}\ \mathsf{aff}$$

Implication.

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_{\mathsf{i}} \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \to_{\mathsf{e}}$$ [3]

Conjonction.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\mathsf{i}} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ \vee_{\mathsf{e}}^{\mathsf{g}} \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \vee_{\mathsf{e}}^{\mathsf{d}}$$

Disjonction.

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{i}}^{\mathsf{g}} \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{i}}^{\mathsf{d}}$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_{\mathsf{e}}.$$ [4]

Négation.

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_{\mathsf{i}} \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg_{\mathsf{e}}$$

Absurdité classique.

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \bot_{\mathsf{e}}$$

(En logique intuitionniste, on retire l'hypothèse $\neg A$ dans la prémisse.)

Quantificateur universel.

si x n'est pas libre dans les formules de Γ
$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x\ A}\ \forall_{\mathsf{i}}$$

quitte à renommer les variables liées de A qui apparaissent dans t
$$\frac{\Gamma \vdash \forall x\ A}{\Gamma \vdash A[x := t]}\ \forall_{\mathsf{e}}$$

Quantificateur existentiel.

$$\frac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x\ A}\ \exists_{\mathsf{i}}$$

avec x ni libre dans C ou dans les formules de Γ
$$\frac{\Gamma \vdash \exists x\ A \qquad \Gamma, A \vdash C}{\Gamma \vdash C}\ \exists_{\mathsf{e}}$$

4 La sémantique.

Définition 15. Soit $\mathscr{L}$ un langage de la sémantique du premier ordre. On appelle *interprétation* (ou *modèle*, ou *structure*) du langage $\mathscr{L}$ l'ensemble $\mathscr{M}$ des données suivantes :

- ▷ un ensemble non vide, noté $|\mathscr{M}|$, appelé *domaine* ou *ensemble de base* de $\mathscr{M}$;

3. Aussi appelée *modus ponens*
4. C'est un raisonnement par cas

- pour chaque symbole c de constante, un élément $c_{\mathscr{M}}$ de $|\mathscr{M}|$;
- pour chaque symbole f de fonction n-aire, une fonction $f_{\mathscr{M}} : |\mathscr{M}|^n \to |\mathscr{M}|$;
- pour chaque symbole R de relation n-aire (sauf pour l'égalité « $=$ »), un sous-ensemble $R_{\mathscr{M}}$ de $|\mathscr{M}|^n$.

Remarque 8.
- La relation « $=$ » est toujours interprétée par la vraie égalité :

$$\{(a,a) \mid a \in |\mathscr{M}|\}.$$

- On note, par abus de notation, $\mathscr{M}$ pour $|\mathscr{M}|$.
- Par convention, $|\mathscr{M}|^0 = \{\emptyset\}$.

Exemple 9. Avec $\mathscr{L}_{\text{corps}} = \{0, 1, +, \times, -, \square^{-1}\}$, on peut choisir
- $|\mathscr{M}| = \mathbb{R}$ avec $0_\mathbb{R}$, $1_\mathbb{R}$, $+_\mathbb{R}$, $\times_\mathbb{R}$, $-_\mathbb{R}$ et $\square_\mathbb{R}^{-1}$;
- ou $|\mathscr{M}| = \mathbb{R}$ avec $2_\mathbb{R}$, $2_\mathbb{R}$, $-_\mathbb{R}$, $+_\mathbb{R}$, *etc.*

Définissions la *vérité*.

Définition 16. Soit $\mathscr{M}$ une interprétation de $\mathscr{L}$.
- Un *environnement* est une fonction de l'ensemble des variables dans $|\mathscr{M}|$.
- Si e est un environnement et $a \in |\mathscr{M}|$, on note $e[x := a]$ l'environnement e' tel que $e'(x) = a$ et pour $y \neq x$, $e(y) = e'(y)$.
- La *valeur* d'un terme t dans l'environnement e, noté $\mathscr{V}al_{\mathscr{M}}(t, e)$, est définie par induction sur l'ensemble des termes de la façon suivante :
  - $\mathscr{V}al_{\mathscr{M}}(c, e) = c_{\mathscr{M}}$ si c est une constante ;
  - $\mathscr{V}al_{\mathscr{M}}(c, e) = e(x)$ si x est une variable ;
  - $\mathscr{V}al_{\mathscr{M}}(f(t_1, \ldots, t_n), e) = f_{\mathscr{M}}(\mathscr{V}al_{\mathscr{M}}(t_1, e), \ldots, \mathscr{V}al_{\mathscr{M}}(t_n, e))$.

Remarque 9. La valeur est $\mathscr{V}al_{\mathscr{M}}(t, e)$ est un élément de $|\mathscr{M}|$.

Exemple 10. Dans $\mathscr{L}_{\text{arith}} = \{0, 1, +, \times\}$, avec le modèle

$$\mathscr{M} : \mathbb{N}, 0_{\mathbb{N}}, 1_{\mathbb{N}}, +_{\mathbb{N}}, \times_{\mathbb{N}},$$

et l'environnement

$$e : \quad x_1 \mapsto 2_{\mathbb{N}} \quad x_2 \mapsto 0_{\mathbb{N}} \quad x_3 \mapsto 3_{\mathbb{N}},$$

alors la valeur du terme $t := (1 \times x_1) + (x_2 \times x_3) + x_2$ est $2_{\mathbb{N}} = (1 \times 2) + (0 \times 3) + 0$.

Lemme 1. La valeur $\mathscr{V}al_{\mathscr{M}}(t, e)$ ne dépend que de la valeur de e sur les variables de t. $\square$

Notation.
- ▷ Lorsque cela est possible, on oublie $\mathscr{M}$ et e dans la notation, et on note $\mathscr{V}al(t)$.
- ▷ À la place de $\mathscr{V}al_{\mathscr{M}}(t, e)$ quand $x_1, \dots, x_n$ sont les variables de t et $e(x_1) = a_1, \dots, e(x_n) = a_n$, on note $t[a_1, \dots, a_n]$ ou aussi $t[x_1 := a_1, \dots, x_n := a_n]$. C'est un *terme à paramètre*, mais attention ce n'est ***ni un terme, ni une substitution***.

Définition 17. Soit $\mathscr{M}$ une interprétation d'un langage $\mathscr{L}$. La *valeur* d'une formule F de $\mathscr{L}$ dans l'environnement e est un élément de $\{0, 1\}$ noté $\mathscr{V}al_{\mathscr{M}}(F, e)$ et définie par induction sur l'ensemble des formules par

- ▷ $\mathscr{V}al_{\mathscr{M}}(R(t_1, \dots, t_n), e) = 1$ ssi $(\mathscr{V}al_{\mathscr{M}}(t_1, e), \dots, \mathscr{V}al_{\mathscr{M}}(t_n, e)) \in R_{\mathscr{M}}$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(\bot, e) = 0$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(\neg F, e) = 1 - \mathscr{V}al_{\mathscr{M}}(F, e)$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(F \wedge G, e) = 1$ ssi $\mathscr{V}al_{\mathscr{M}}(F, e) = 1$ et $\mathscr{V}al_{\mathscr{M}}(G, e) = 1$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(F \vee G, e) = 1$ ssi $\mathscr{V}al_{\mathscr{M}}(F, e) = 1$ ou $\mathscr{V}al_{\mathscr{M}}(G, e) = 1$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(F \to G, e) = 1$ ssi $\mathscr{V}al_{\mathscr{M}}(F, e) = 0$ ou $\mathscr{V}al_{\mathscr{M}}(G, e) = 1$;
- ▷ $\mathscr{V}al_{\mathscr{M}}(\forall x\, F, e) = 1$ ssi pour tout $a \in |\mathscr{M}|$, $\mathscr{V}al_{\mathscr{M}}(F, e[x := a]) = 1$;

▷ $\mathscr{V}al_{\mathscr{M}}(\exists x\ F, e) = 1$ ssi il existe $a \in |\mathscr{M}|$, $\mathscr{V}al_{\mathscr{M}}(F, e[x := a]) = 1$.

Remarque 10. ▷ On se débrouille pour que les connecteurs aient leur sens courant, les « mathématiques naïves ».

▷ Dans le cas du calcul propositionnel, si R est d'arité 0, *i.e.* une variable propositionnelle, comme $|\mathscr{M}|^0 = \{\emptyset\}$ alors on a deux possibilité :
  - ou bien $R = \emptyset$, et alors on convient que $\mathscr{V}al_{\mathscr{M}}(R, e) = 0$;
  - ou bien $R = \{\emptyset\}$, et alors on convient que $\mathscr{V}al_{\mathscr{M}}(R, e) = 1$.

Remarque 11. On verra plus tard qu'on peut construire les entiers avec

▷ $0 : \emptyset$,

▷ $1 : \{\emptyset\}$,

▷ $2 : \{\emptyset, \{\emptyset\}\}$,

▷ $\vdots \quad \vdots$

▷ $n + 1 : n \cup \{n\}$,

▷ $\vdots \qquad \vdots$

Notation. À la place de $\mathscr{V}al_{\mathscr{M}}(F, e) = 1$, on notera $\mathscr{M}, e \models F$ ou bien $\mathscr{M} \models F$. On dit que $\mathscr{M}$ *satisfait* F, que $\mathscr{M}$ est un *modèle* de F (dans l'environnement e), que F est est vraie dans $\mathscr{M}$.

Lemme 2. La valeur $\mathscr{V}al_{\mathscr{M}}(F, e)$ ne dépend que de la valeur de e sur les variables libres de F.

Preuve. En exercice. □

Corollaire 1. Si F est close, alors $\mathscr{V}al_{\mathscr{M}}(F, e)$ ne dépend pas de e et on note $\mathscr{M} \models F$ ou $\mathscr{M} \not\models F$.

Remarque 12. Dans le cas des formules closes, on doit passer un environnement à cause de $\forall$ et $\exists$.

Notation. On note $F[a_1, \ldots, a_n]$ pour $\mathscr{V}al_{\mathscr{M}}(F, e)$ avec $e(x_1) = a_1, \ldots, e(x_n) = a_n$. C'est une *formule à paramètres*, mais ce n'est ***pas une formule***.

Exemple 11. Dans $\mathscr{L} = \{S\}$ où S est une relation binaire, on considère deux modèles :

- $\mathscr{N} : |\mathscr{N}| = \mathbb{N}$ avec $S_{\mathscr{N}} = \{(x, y) \mid x < y\}$,
- $\mathscr{R} : |\mathscr{R}| = \mathbb{R}$ avec $S_{\mathscr{R}} = \{(x, y) \mid x < y\}$;

et deux formules

- $F = \forall x\, \forall y\, (S\; x\; y \to \exists z\, (S\; x\; z \wedge S\; z\; y))$,
- $G = \exists x\, \forall y\, (x = y \vee S\; x\; y)$;

alors on a

$$\mathscr{N} \not\models F \quad \mathscr{R} \models F \quad \mathscr{N} \models G \quad \mathscr{R} \not\models G.$$

En effet, la formule F représente le fait d'être un ordre dense, et G d'avoir un plus petit élément.

Définition 18. Dans un langage $\mathscr{L}$, une formule F est un *théorème (logique)* si pour toute structure $\mathscr{M}$ et tout environnement e, on a $\mathscr{M}, e \models F$.

Exemple 12. Quelques théorèmes simples : $\forall x\, \neg\bot$, et $\forall x\, x = x$ et même $x = x$ car on ne demande pas que la formule soit clause.

Dans $\mathscr{L}_{\mathrm{g}} = \{e, *, \square^{-1}\}$, on considère deux formules

- $F = \forall x\, \forall y\, \forall z\, ((x * (y * z) = (x * y) * z) \wedge x * e = e * x = x \wedge \exists t\, (x * t = e \wedge t * x = e))$;
- et $G = \forall e' = \forall e'\, (\forall x\, (x * e' = e' * x = x) \to e = e')$.

Aucun des deux n'est un théorème (il n'est vrai que dans les groupes pour F (c'est même la définition de groupe) et dans les monoïdes pour G (unicité du neutre)), mais $F \to G$ est un théorème logique.

Définition 19. Soient $\mathscr{L}$ et $\mathscr{L}'$ deux langages. On dit que $\mathscr{L}'$ *enrichit* $\mathscr{L}$ ou que $\mathscr{L}$ est une *restriction* de $\mathscr{L}'$ si $\mathscr{L} \subseteq \mathscr{L}'$.

Dans ce cas, si $\mathscr{M}$ est une interprétation de $\mathscr{L}$, et si $\mathscr{M}'$ est une interprétation de $\mathscr{L}'$ alors on dit que $\mathscr{M}'$ est un *enrichissement* de $\mathscr{M}$ ou que $\mathscr{M}$ est une *restriction* de $\mathscr{M}'$ ssi $|\mathscr{M}| = |\mathscr{M}'|$ et chaque symbole de $\mathscr{L}$ a la même interprétation dans $\mathscr{M}$ et $\mathscr{M}'$, *i.e.* du point de vue de $\mathscr{L}$, $\mathscr{M}$ et $\mathscr{M}'$ sont les mêmes.

Exemple 13. Avec $\mathscr{L} = \{e, *\}$ et $\mathscr{L}' = \{e, *, \square^{-1}\}$ alors $\mathscr{L}'$ est une extension de $\mathscr{L}$. On considère

- ▷ $\mathscr{M}$: $\quad |\mathscr{M}| = \mathbb{Z} \quad e_{\mathscr{M}} = 0_{\mathbb{Z}} \quad *_{\mathscr{M}} = +_{\mathbb{Z}}$;
- ▷ $\mathscr{M}'$: $\quad |\mathscr{M}'| = \mathbb{Z} \quad e_{\mathscr{M}'} = 0_{\mathbb{Z}} \quad *_{\mathscr{M}'} = +_{\mathbb{Z}} \quad \square^{-1}_{\mathscr{M}'} = \mathrm{id}_{\mathbb{Z}}$,

et alors $\mathscr{M}'$ est une extension de $\mathscr{M}$.

Proposition 1. Si $\mathscr{M}$ une interprétation de $\mathscr{L}$ est un enrichissement de $\mathscr{M}'$, une interprétation de $\mathscr{L}'$, alors pour tout environnement e,

1. si t est un terme de $\mathscr{L}$, alors $\mathscr{V}\!al_{\mathscr{M}}(t, e) = \mathscr{V}\!al_{\mathscr{M}'}(t, e)$;
2. si F est une formule de $\mathscr{L}$ alors $\mathscr{V}\!al_{\mathscr{M}}(F, e) = \mathscr{V}\!al_{\mathscr{M}'}(F, e)$.

Preuve. En exercice. □

Corollaire 2. La vérité d'une formule dans une interprétation ne dépend que de la restriction de cette interprétation au langage de la formule. □

Définition 20. Deux formules F et G sont *équivalentes* si $F \leftrightarrow G$ est un théorème logique.

Proposition 2. Toute formule est équivalente à une formule n'utilisant que les connecteurs logiques $\neg$, $\vee$ et $\exists$. $\square$

Définition 21. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$.

1. Un *$\mathscr{L}$-morphisme* de $\mathscr{M}$ est une fonction $\varphi : |\mathscr{M}| \to |\mathscr{N}|$ telle que
   - ▷ pour chaque symbole de constante c, on a $\varphi(c_{\mathscr{M}}) = c_{\mathscr{N}}$;
   - ▷ pour chaque symbole f de fonction n-aire, on a
     $$\varphi(f_{\mathscr{M}}(a_1, \ldots, a_n)) = f_{\mathscr{N}}(\varphi(a_1), \ldots, \varphi(a_n)) \; ;$$
   - ▷ pour chaque symbole R de relation n-aire (autre que « $=$ »), on a
     $$(a_1, \ldots, a_n) \in R_{\mathscr{M}} \text{ ssi } (\varphi(a_1), \ldots, \varphi(a_n)) \in R_{\mathscr{N}}.$$
   - ▷ Un *$\mathscr{L}$-isomorphisme* est un $\mathscr{L}$-morphisme bijectif.
   - ▷ Si $\mathscr{M}$ et $\mathscr{N}$ sont *isomorphes* s'il existe un $\mathscr{L}$-isomorphisme de $\mathscr{M}$ à $\mathscr{N}$.

Remarque 13.
1. On ne dit rien sur « $=$ » car si on impose la même condition que pour les autres relations alors nécessairement φ est injectif.
2. La notion dépend du langage $\mathscr{L}$.
3. Lorsqu'on a deux structures isomorphes, on les confonds, ce sont les mêmes, c'est un renommage.

Exemple 14. Avec $\mathscr{L}_{\text{ann}} = \{0, +, \times, -\}$ et $\mathscr{L}' = \mathscr{L}_{\text{ann}} \cup \{1\}$, et les deux modèles $\mathscr{M} : \mathbb{Z}/3\mathbb{Z}$ et $\mathscr{N} = \mathbb{Z}/12\mathbb{Z}$, on considère la fonction définie (on néglige les cas inintéressants) par $\varphi(\bar{n}) = \overline{4n}$.

Est-ce que φ est un morphisme de $\mathscr{M}$ dans $\mathscr{N}$? Oui… et non… Dans $\mathscr{L}$ c'est le cas, mais pas dans $\mathscr{L}'$ car $\varphi(1) = 4$.

Exemple 15. Dans $\mathscr{L} = \{c, f, R\}$ avec f une fonction binaire, et R une relation binaire, on considère

- $\mathscr{M} : \mathbb{R}, 0, +, \le$;
- $\mathscr{N} :]0, +\infty[, 1, \times, \le$.

Existe-t-il un morphisme de $\mathscr{M}$ dans $\mathscr{N}$? Oui, il suffit de poser le morphisme $\varphi : x \mapsto \mathrm{e}^x$.

Proposition 3. La composée de deux morphismes (*resp.* isomorphisme) est un morphisme (*resp.* un isomorphisme). □

Notation. Si φ est un morphisme de $\mathscr{M}$ dans $\mathscr{N}$ et e un environnement de $\mathscr{M}$, alors on note $\varphi(e)$ pour $\varphi \circ e$. C'est un environnement de $\mathscr{N}$.

Lemme 3. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$, et φ un morphisme de $\mathscr{M}$ dans $\mathscr{N}$. Alors pour tout terme t et environnement e, on a

$$\varphi(\mathscr{V}al_{\mathscr{M}}(t, e)) = \mathscr{V}al_{\mathscr{N}}(t, \varphi(e)).$$

□

Lemme 4. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$, et φ un morphisme ***injectif*** de $\mathscr{M}$ dans $\mathscr{N}$. Alors pour toute formule atomique F et environnement e, on a

$$\mathscr{M}, e \models F \text{ ssi } \mathscr{N}, \varphi(e) \models F$$

Lemme 5. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$, et φ un ***isomorphisme***[5] de $\mathscr{M}$ dans $\mathscr{N}$. Alors pour toute formule F et environnement e, on a

$$\mathscr{M}, e \models F \text{ ssi } \mathscr{N}, \varphi(e) \models F$$

Corollaire 3. Deux interprétations isomorphismes satisfont les mêmes formules closes.

Exercice 4. Les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont-ils isomorphes ? Non. En effet, les deux formules

- ▷ $\exists x\,(x \neq e \wedge x * x \neq e \wedge x * (x * x) \neq e \wedge x * (x * (x * x)) = e)$,
- ▷ $\forall x\ (x * x) = e$

ne sont pas vraies dans les deux (pour la première, elle est vraie dans $\mathbb{Z}/4\mathbb{Z}$ mais pas dans $(\mathbb{Z}/2\mathbb{Z})^2$ et pour la seconde, c'est l'inverse).

Remarque 14. La réciproque du corollaire est ***fausse*** : deux interprétations qui satisfont les mêmes formules closes ne sont pas nécessairement isomorphes. Par exemple, avec $\mathscr{L} = \{\le\}$, les interprétations $\mathbb{R}$ et $\mathbb{Q}$ satisfont les mêmes formules closes, mais ne sont pas isomorphes.

Définition 22. Soit $\mathscr{L}$ un langage, $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$. On dit que $\mathscr{N}$ est une *extension* de $\mathscr{M}$ (ou $\mathscr{M}$ est une *sous-interprétation* de $\mathscr{N}$) si les conditions suivants sont satisfaites :

- ▷ $|\mathscr{M}| \subseteq |\mathscr{N}|$;
- ▷ pour tout symbole de constante c, on a $c_\mathscr{M} = c_\mathscr{N}$;
- ▷ pour tout symbole de fonction n-aire f, on a $f_\mathscr{M} = f_\mathscr{N}\big|_{|\mathscr{M}|^n}$ (donc en particulier $f_\mathscr{N}(|\mathscr{M}|^n) \subseteq |\mathscr{M}|$) ;
- ▷ pour tout symbole de relation n-aire R, on a $R_\mathscr{M} = R_\mathscr{N} \cap |\mathscr{M}|^n$.

5. On utilise ici la *surjectivité* pour le « $\exists$ ».

Proposition 4. Soient $\mathscr{M}$ et $\mathscr{N}$ deux interprétations de $\mathscr{L}$. Alors $\mathscr{M}$ est isomorphe à une sous-interprétation $\mathscr{M}'$ de $\mathscr{N}$ si et seulement si, il existe un morphisme injectif de $\mathscr{M}$ dans $\mathscr{N}$.

Exemple 16 (Construction de $\mathbb{Z}$ à partir de $\mathbb{N}$). On pose la relation $(p, q) \sim (p', q')$ si $p + q' = p' + q$. C'est une relation d'équivalence sur $\mathbb{N}^2$. On pose $\mathbb{Z} := \mathbb{N}^2/\sim$ (il y a un isomorphisme $\mathbb{N}^2/\sim \to \mathbb{Z}$ par $(p, q) \mapsto p - q$). Est-ce qu'on a $\mathbb{N} \subseteq \mathbb{N}^2/\sim$? D'un point de vue ensembliste, non. Mais, généralement, l'inclusion signifie avoir un morphisme injectif de $\mathbb{N}$ dans $\mathbb{N}^2/\sim$.

Définition 23. Une *théorie* est un ensemble (fini ou pas) de formules closes. Les éléments de la théorie sont appelés *axiomes*.

Exemple 17. La *théorie des groupes* est

$$
\begin{aligned}
T_{\text{groupe}} := \Big\{ & \forall x\, (x * e = e * x = x),\\
& \forall x\, (x * x^{-1} = e \wedge x^{-1} * x = e),\\
& \forall x\, \forall y\, \forall z\, (x * (y * z) = (x * y) * z) \Big\}
\end{aligned}
$$

dans le langage $\mathscr{L}_{\text{g}}$.

Exemple 18. La *théorie des ensembles infinis* est

$$
\begin{aligned}
T_{\text{ens infinis}} := \Big\{ & \exists x\, (x = x),\\
& \exists x\, \exists y\, (x \neq y),\\
& \exists x\, \exists y\, \exists z\, (x \neq y \wedge y \neq z \wedge z \neq x)\\
& \dots \Big\}
\end{aligned}
$$

dans le langage $\mathscr{L}_{\text{ens}}$.

Définition 24 (Sémantique). ▷ Une interprétation $\mathscr{M}$ *satisfait* T (ou $\mathscr{M}$ est un *modèle* de T), noté $\mathscr{M} \models T$, si $\mathscr{M}$ satisfait toutes les formules de T.

- ▷ Une théorie T est *contradictoire* s'il n'existe pas de modèle de T. Sinon, on dit qu'elle est *non-contradictoire*, ou *satisfiable*, ou *satisfaisable*.

Exemple 19. Les deux théories précédentes, T_{groupes} et $T_{\text{ens infinis}}$, sont non-contradictoires.

Définition 25 (Syntaxique). Soit T une théorie.

- ▷ Soit A une formule. On note $T \vdash A$ s'il existe un sous-ensemble fini T' tel que $T' \subseteq T$ et $T' \vdash A$.
- ▷ On dit que T est *consistante* si $T \nvdash \bot$, sinon T est *inconsistante*.
- ▷ On dit que T est *complète* (« *axiome-complète* ») si T est consistante et, pour toute formule $F \in \mathscr{F}$, on a $T \vdash F$ ou on a $T \vdash \neg F$.

Exemple 20. La théorie des groupes n'est pas complète : par exemple,

$$F := \forall x \, \forall y \, (x * y = y * x)$$

est parfois vraie, parfois fausse, cela dépend du groupe considéré.

Exemple 21. La théorie

$$T = \mathbf{Th}(\mathbb{N}) := \{\text{les formules } F \text{ vraies dans } \mathbb{N}\}$$

est complète mais pas pratique.

De par le théorème d'*incomplétude de Gödel* (c'est un sens différent du « complet » défini avant), on montre qu'on ne peut pas avoir de *joli* ensemble d'axiomes pour $\mathbb{N}$.

Proposition 5. Soit T une théorie complète.

1. Soit A une formule close. On a $T \vdash \neg A$ ssi $T \nvdash A$.
2. Soient A et B des formules closes. On a $T \vdash A \vee B$ ssi $T \vdash A$ ou $T \vdash B$.

Preuve.
- ▷ Si $T \vdash \neg A$ et $T \vdash A$, alors il existe $T', T'' \subseteq_{\text{fini}} T$ tels que $T' \vdash \neg A$ et $T'' \vdash A$. On a donc $T' \cup T'' \vdash \bot$ par :

$$\dfrac{\dfrac{T' \vdash \neg A}{T' \cup T'' \vdash \neg A}\,\textsf{aff} \qquad \dfrac{T'' \vdash A}{T' \cup T'' \vdash A}\,\textsf{aff}}{T' \cup T'' \vdash \bot}\,\neg_{\textsf{e}}$$

  On en conclut que $T \vdash \bot$, absurde car T supposée complète donc consistante. On a donc $T \vdash \neg A$ implique $T \nvdash A$.

  Réciproquement, si $T \nvdash A$ et $T \nvdash \neg A$, alors c'est impossible car T est complète. On a donc $T \nvdash A$ implique $T \vdash \neg A$.
- ▷ Si $T \vdash A$ ou $T \vdash B$, alors par la règle $\vee_{\textsf{i}}^{\textsf{g}}$ ou $\vee_{\textsf{i}}^{\textsf{d}}$, on montre que $T \vdash A \vee B$.

  Réciproquement, si $T \vdash A \vee B$ et $T \nvdash A$ et $T \vdash\nvdash B$ alors, par 1, on a $T \vdash \neg A$ et $T \vdash \neg B$. On montre ainsi (en exercice) que $T \vdash \neg(A \vee B)$ d'où $T \vdash \bot$ par $\neg_{\textsf{e}}$. C'est impossible car T est complète donc consistante, d'où $T \vdash A \vee B$ implique $T \vdash A$ ou $T \vdash B$.

□

5 Théorème de complétude de Gödel.

Théorème 1 (Complétude de Gödel (à double sens)).

Version 1. Soit T une théorie et F une formule close. On a $T \vdash F$ ssi $T \models F$.

Version 2. Une théorie T est consistante (syntaxe) ssi elle est non-contradictoire (sémantique).

Remarque 15. La version 1 se décompose en deux théorèmes :

- ▷ le *théorème de correction* (ce que l'on prouve est vrai)

$$T \vdash F \implies T \models F \; ;$$

- ▷ le *théorème de complétude* (ce qui est vrai est prouvable)

$$T \models F \implies T \vdash F.$$

Pour la version 2, on peut aussi la décomposer en deux théorèmes[6] :

- ▷ la *correction*, T non-contradictoire implique T consistante ;
- ▷ la *complétude*, T consistante implique T non-contradictoire.

Par contraposée, on a aussi qu'une théorie contradictoire est inconsistante.

Proposition 6. Les deux versions du théorème de correction sont équivalentes.

Preuve.

- ▷ D'une part, on montre (par contraposée) « non V2 implique non V1 ». Soit T non-contradictoire et inconsistante. Il existe un modèle $\mathscr{M}$ tel que $\mathscr{M} \models T$ et $T \vdash \bot$. Or, par définition, $\mathscr{M} \not\models \bot$ donc $T \not\models \bot$.
- ▷ D'autre part, on montre « V2 implique V1 ». Soit T et F tels que $T \vdash F$. Ainsi, $T \cup \neg F \vdash \bot$, d'où $T \cup \{\neg F\}$ est inconsistante, et d'où, par la version 2 de la correction, on a que $T \cup \{\neg F\}$ contradictoire, donc on n'a pas de modèle. On a alors que, touts les modèles de T sont des modèles de F, autrement dit $T \models F$.

$\square$

6. On a une négation dans ce théorème, donc ce n'est pas syntaxe implique sémantique pour la correction, mais non sémantique implique non syntaxe.

Proposition 7. Les deux versions du théorème de complétude (sens unique) sont équivalentes.

Preuve.
- Soit T contradictoire. Elle n'a pas de modèle. Ainsi, on a $T \models \bot$ d'où $T \vdash \bot$ par la version 1, elle est donc inconsistante.
- Soit $T \models F$. Considérons $T \cup \{\neg F\}$: cette théorie n'a pas de modèle, donc est contradictoire, donc est inconsistante, et on a donc que $T \cup \{\neg F\} \vdash \bot$ d'où $T \vdash F$ par $\bot_\mathsf{e}$.

$\square$

Remarque 16 (Attention !). On utilise « $\models$ » dans deux sens.
- Dans le sens *modèle* $\models$ *formule*, on dit qu'une formule est vraie dans un modèle, c'est le sens des mathématiques classiques.
- Dans le sens *théorie* $\models$ *formule*, on dit qu'une formule est vraie dans tous les modèles de la théorie, c'est un sens des mathématiques plus inhabituel.

5.1 Preuve du théorème de correction.

Exercice 5. Montrer que le lemme ci-dessous implique la version 1 de la correction.

Lemme 6. Soient T une théorie, $\mathscr{M}$ un modèle et F une formule close. Si $\mathscr{M} \models T$ et $T \vdash F$ alors $\mathscr{M} \models F$.

Preuve. Comme d'habitude, pour montrer quelque chose sur les formules closes, on commence par les formules et même les termes. On commence par montrer que la substitution dans les termes a un sens sémantique.

Lemme 7. Soient t et u des termes et e un environnement. Soient $v := t[x := u]$ et $e' := e[x := \mathscr{Val}(u, e)]$. Alors, $\mathscr{Val}(v, e) = \mathscr{Val}(t, e')$.

Preuve. En exercice. $\square$

Lemme 8. Soit A une formule, t un terme, et e un environnement. Si $e' := e[x := \mathscr{Val}(t, e)]$ alors $\mathscr{M}, e \models A[x := t]$ ssi $\mathscr{M}, e' \models A$.

Preuve. En exercice. $\square$

On termine la preuve en montrant la proposition ci-dessous. $\square$

Montrons cette proposition plus forte que le lemme.

Proposition 8. Soient Γ un ensemble de formules et A une formule. Soit $\mathscr{M}$ une interprétation et soit e un environnement. Si $\mathscr{M}, e \models \Gamma$, et $\Gamma \models A$ alors $\mathscr{M}, e \models A$.

Preuve. Par induction sur la preuve de $\Gamma \vdash A$, on montre la proposition précédente.

- ▷ Cas inductif $\to_\mathsf{i}$. On sait que A est de la forme $B \to C$, et on montre que de $\Gamma, B \vdash C$ on montre $\Gamma \vdash B \to C$. Soient $\mathscr{M}$ et e tels que $\mathscr{M}, e \models \Gamma$. Montrons que $\mathscr{M}, e \models B \to C$. Il faut donc montrer que si $\mathscr{M}, e \models B$ alors $\mathscr{M}, e \models C$. Si $\mathscr{M}, e \models B$ alors $\mathscr{M}, e \models \Gamma \cup \{B\}$. Or, comme $\Gamma, B \vdash C$ alors par hypothèse d'induction, on a que $\mathscr{M}, e \models C$.
- ▷ Cas inductif $\forall_\mathsf{e}$. Si A est de la forme $B[x := t]$, alors de $\Gamma \vdash \forall x\ B$, on en déduit que $\Gamma \vdash B[x := t]$. Soit $\mathscr{M}, e \models \Gamma$ et $a := \mathscr{Val}(t, e)$. Par hypothèse de récurrence, on a que $\mathscr{M}, e \models \forall x\ B$ donc $\mathscr{M}, e[x := a] \models B$ et d'après le lemme précédent, on a que $\mathscr{M}, e \models B[x := t]$.
- ▷ Les autre cas inductifs sont laissé en exercices.

- ▷ Cas de base ax. Si $A \in \Gamma$ et $\mathscr{M}, e \models \Gamma$ alors $\mathscr{M}, e \models A$.
- ▷ Cas de base $=_\mathsf{i}$. On a, pour tout $\mathscr{M}, e$ que $\mathscr{M}, e \models t = t$.

□

Cette proposition permet de conclure la preuve du lemme précédent.

5.2 Preuve du théorème de complétude.

On va montrer la version 2, en ***trois étapes***. Soit T une théorie consistante sur le langage $\mathscr{L}$.

1. On enrichit le langage $\mathscr{L}$ en $\mathscr{L}'$ avec des constantes, appelées *témoins de Henkin*, et qui nous donnerons les éléments de notre ensemble de base : les termes.
2. Pour définir complètement le modèle, on complète la théorie T en une théorie Th sur $\mathscr{L}'$.
3. On quotiente pour avoir la vraie égalité dans le modèle.

Cette construction est assez similaire à la définition de $\mathbb{C}$ comme le quotient $\mathbb{R}[X]/(X^2+1)$.

Proposition 9. On peut étendre $\mathscr{L}$ en $\mathscr{L}'$ et T en T' consistante telle que, pour toute formule $F(x)$ de $\mathscr{L}'$, ayant pour seule variable libre x, il existe un symbole de constante c_F de $\mathscr{L}'$ telle que l'on ait $T' \vdash \exists x\ F(x) \to F(c_F)$, d'où le nom de témoin.

Preuve. On fait la construction « par le bas » :

- ▷ $\mathscr{L}_0 = \mathscr{L}$;
- ▷ $T_0 = T$;
- ▷ $\mathscr{L}_{n+1} = \mathscr{L}_n \cup \{c_F \mid F \text{ formule à une variable libre de } \mathscr{L}_n\}$;
- ▷ $T_{n+1} = T_n \cup \{\exists x\ F \to F(c_F) \mid F \text{ formule de } \mathscr{L}_n\}$;
- ▷ et enfin $\mathscr{L}' = \bigcup_{n\in\mathbb{N}} \mathscr{L}_n$ et $T' = \bigcup_{n\in\mathbb{N}} T_n$.

On commence par montrer quelques lemmes.

Lemme 9. Soient Γ un ensemble de formules et A une formule. Soit c un symbole de constante qui n'apparait ni dans Γ ni dans A. Si $\Gamma \vdash A[x := c]$ alors $\Gamma \vdash \forall x\ A$.

Preuve. Idée de la preuve. On peut supposer que x n'apparait pas dans Γ, ni dans la preuve de $\Gamma \vdash A[x := c]$, sinon on renomme x en y dans l'énoncé du lemme. Alors, de la preuve de $\Gamma \vdash A[x := c]$, on peut déduire une preuve de $\Gamma \vdash A(x)$ en replaçant c par x. Avec la règle $\forall_\mathsf{i}$, on en conclut que $\Gamma \vdash \forall x\ A$. □

Lemme 10. Pour toute formule F à une variable libre x sur le langage $\mathscr{L}'$,

$$T' \vdash \exists x\ F(x) \to F(c_F).$$

Preuve. La formule F a un nombre fini de constantes (car c'est un mot fini), donc F est une formule sur $\mathscr{L}_n$ pour un certain $n \in \mathbb{N}$, donc $(\exists x\ F(x) \to F(c_F)) \in T_{n+1} \subseteq T'$. □

Il nous reste à montrer que la théorie T' est consistante.

Il suffit de montrer que tous les T_n sont consistantes. En effet, si T' est non-consistante, il existe un ensemble fini $T'' \subseteq T'$ et $T'' \vdash \bot$. Comme T'' fini, il existe un certain $n \in \mathbb{N}$ tel que $T'' \subseteq T_n$ et donc $T_n \vdash \bot$.

On montre par récurrence sur n que T_n est consistante.

- On a $T_0 = T$ qui est consistante par hypothèse.
- Supposons T_n consistante et que $T_{n+1} \vdash \bot$. Alors, il existe des formules à une variable libre $F_1, \ldots, F_k$ écrites sur $\mathscr{L}_n$ et
$$T_n \cup \{\, \exists x\ F_i \to F_i(c_{F_i}) \mid 1 \le i \le k \,\} \vdash \bot.$$

Ainsi (exercice)

$$T_n \vdash \Big(\bigwedge_{1 \le i \le k} \big(\exists x\, F_i \to F_i(c_{F_i})\big)\Big) \to \bot.$$

Les c_{F_i} ne sont pas dans T_n d'où, d'après le lemme 9, que

$$T_n \vdash \forall y_1\, \forall y_2\, \ldots \forall y_n \Big(\bigwedge_{1 \le i \le k} \big(\exists x\, F_i \to F_i(y_i)\big)\Big) \to \bot.$$

On peut montrer que (théorème logique)

$$(\star) \qquad \vdash \forall y\, (A(y) \to \bot) \leftrightarrow (\exists y\, A(y) \to \bot),$$

d'où

$$T_n \vdash \Big(\exists y_1\, \exists y_2\, \ldots \exists y_n \bigwedge_{1 \le i \le k} \big(\exists x\, F_i \to F_i(y_i)\big)\Big) \to \bot.$$

On a aussi

$$(\star\star) \qquad \vdash \exists y_1 \exists y_2 \big(A(y_1) \wedge A(y_2)\big) \leftrightarrow \big(\exists y_1 A(y_1)\big) \wedge \big(\exists y_2 A(y_2)\big),$$

et pour y non libre dans A, on a

$$\vdash \exists y\, (A \to B) \leftrightarrow (A \to \exists y\, B).$$

On a donc

$$T_n \vdash \Big(\bigwedge_{1 \le i \le k} (\exists x\, F_i(x) \to \exists y_i\, F_i(y_i))\Big) \to \bot.$$

Or,

$$(\star\star\star) \qquad \vdash \bigwedge_{1 \le i \le k} (\exists x\, F_i(x) \to \exists y_i\, F_i(y_i)).$$

On a donc $T_n \vdash \bot$, ce qui contredit l'hypothèse, d'où T_{n+1} consistante.

En exercice, on pourra montrer les théorèmes logiques $(\star)$, $(\star\star)$, et $(\star\star\star)$.

$\square$

Ensuite, on veut compléter T' en préservant le résultat de la proposition précédente. On cherche Th (axiome-)complète telle que $T' \subseteq \mathrm{Th}$ et pour toute formule à une variable libre F de $\mathscr{L}'$, on a

$$\mathrm{Th} \vdash \exists x\, F \to F(c_F).$$

Faisons le cas dénombrable (sinon, lemme de Zorn) : supposons $\mathscr{L}'$ au plus dénombrable. Soit $(F_n)_{n\in\mathbb{N}}$ une énumération des formules closes de $\mathscr{L}'$. On définit par récurrence

- ▷ $K_0 := T'$;
- ▷ si K_n est complète, alors $K_{n+1} := K_n$;
- ▷ si K_n n'est pas complet, alors soit le plus petit $p \in \mathbb{N}$ tel que l'on ait $K_n \nvdash F_p$ et $K_n \nvdash \neg F_p$, et on pose $K_{n+1} := K_n \cup \{F_p\}$.

Lemme 11. On pose $\mathrm{Th} := \bigcup_{n\in\mathbb{N}} T_n$. La théorie Th a les propriétés voulues.

Preuve.

1. On a $T' \subseteq \mathrm{Th}$.
2. La théorie Th est consistante. En effet, il suffit de montrer que tous les K_n le sont (par les mêmes argument que la preuve précédente). Montrons le par récurrence.
   - ▷ La théorie $K_0 = T'$ est consistante par hypothèse.
   - ▷ Si $K_{n+1} = K_n$ alors K_{n+1} est consistante par hypothèse de récurrence.
   - ▷ Si $K_{n+1} = K_n \cup \{F_p\}$, et si $K_n, F_p \vdash \bot$, alors par la règle $\neg_\mathsf{i}$, on a $K_n \vdash \neg F_p$, ce qui est faux. Ainsi K_{n+1} est consistante.

   On en conclut que Th est consistante.
3. La théorie Th est complète. Sinon, à chaque étape $K_{n+1} =$

$K_n \cup \{F_{q_n}\}$ et il existe F_p telle que $\mathrm{Th} \nvdash F_p$ et $\mathrm{Th} \nvdash \neg F_p$. Ainsi, pour tout $n \in \mathbb{N}$, $K_n \nvdash F_p$ et $K_n \nvdash \neg F_p$, d'où pour tout $n \in \mathbb{N}$, $p_n \leq p$ avec des p_n distincts. C'est absurde, il n'y a qu'un nombre fini d'entiers inférieurs à un entier donné.

□

On construit un quotient avec « = » comme relation d'équivalence, puis on vérifie que les fonctions et relations sont bien définies (ne dépendent pas du représentant choisit, comme pour les groupes quotients).

Soit $\mathscr{E}$ l'ensemble des termes clos de $\mathscr{L}'$, qui n'est pas vide car il contient les termes $c_{x=x}$ (avec la définition de c_F ci-avant). On définit sur $\mathscr{E}$ une relation $\sim$, où $t \sim t'$ ssi $\mathrm{Th} \vdash t = t'$.

Exercice 6. Montrer que $\sim$ est une relation d'équivalence.

On pose enfin $|\mathscr{M}| := \mathscr{E}/{\sim}$. On notera $\bar{t}$ la casse de t. On définit l'interprétation des symboles de $\mathscr{L}'$:

- ▷ si c est une constante, alors $c_{\mathscr{M}} := \bar{c}$;
- ▷ si f est un symbole de fonctions d'arité n,

$$f_{\mathscr{M}}(\bar{t}_1, \ldots, \bar{t}_n) := \overline{f(t_1, \ldots, t_n)}.$$

Lemme 12. La définition de dépend pas des représentants choisis, c'est-à-dire si $\bar{u}_1 = \bar{t}_1, \ldots, \bar{u}_n = \bar{t}_n$ alors

$$\overline{f(t_1, \ldots, t_n)} = \overline{f(u_1, \ldots, u_n)}.$$

Preuve. ▷ On a $\mathrm{Th} \vdash t_i = u_i$ pour tout i par hypothèse

- ▷ donc avec $=_{\mathsf{i}}$, on a $\mathrm{Th} \vdash f(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$
- ▷ donc avec $=_{\mathsf{e}}$, on a $\mathrm{Th} \vdash f(u_1, \ldots, t_n) = f(t_1, \ldots, t_n)$
- ▷ *. . . etc. . .*
- ▷ donc avec $=_{\mathsf{e}}$, on a $\mathrm{Th} \vdash f(u_1, \ldots, u_n) = f(t_1, \ldots, t_n)$

□

[*suite de la définition de l'interprétation*]

- si R est un symbole de relation d'arité n, on définit

$$(\bar{t}_1, \ldots, \bar{t}_n) \in R_{\mathscr{M}} \text{ ssi } \mathrm{Th} \vdash R(t_1, \ldots, t_n).$$

Exercice 7. Montrer que cette définition de dépend pas des représentants choisis.

Lemme 13. Soit F une formule à n variables libres et $t_1, \ldots, t_n$ des termes clos. Alors, $\mathscr{M} \models F[\bar{t}_1, \ldots, \bar{t}_n]$ ssi $\mathrm{Th} \vdash F[t_1, \ldots, t_n]$, où l'on interprète la formule à paramètre dans l'environnement e avec $e(y_i) = \bar{t}_i$ alors $\mathscr{M}, e \models F(y_1, \ldots, y_n)$.

Preuve. Par induction sur F en supposant que F n'utilise que $\neg$, $\vee$, $\exists$ comme connecteurs. En effet, on a pour toute formule G, il existe F qui n'utilise que $\neg$, $\vee$, $\exists$ et $\vdash F \leftrightarrow G$, ce qui permet de conclure directement pour G si le résultat est vrai sur F.

- Pour $F = \bot$, alors on a $\mathrm{Th} \nvdash \bot$ car Th consistante et $\mathscr{M} \models \bot$ par définition.
- Pour $F = R(u_1, \ldots, u_m)$, où les u_i sont des termes non nécessairement clos et où $u_1, \ldots, u_m$ sont des termes à n variables $x_1, \ldots, x_n$. On pose

$$F[t_1, \ldots, t_n] := R(\underbrace{u_1(t_1, \ldots, t_n)}_{v_1}, \ldots, \underbrace{u_m(t_1, \ldots, t_n)}_{v_m})$$

  où l'on définit $v_i := u_i(t_1, \ldots, t_n)$ qui est clos car les t_i sont clos. On veut montrer que

$$\mathscr{M} \models \underbrace{F[\bar{t}_1, \ldots, \bar{t}_n]}_{R(\bar{v}_1, \ldots, \bar{v}_m)} \text{ ssi } \mathrm{Th} \vdash \underbrace{F[t_1, \ldots, t_n]}_{R(v_1, \ldots, v_m)}.$$

Or, on a l'équivalence $\mathscr{M} \models R(\bar{v}_1, \ldots, \bar{v}_m)$ ssi $(\bar{v}_1, \ldots, \bar{v}_m) \in R_{\mathscr{M}}$ ssi $\mathrm{Th} \vdash R(v_1, \ldots, v_m)$.

- ▷ Pour $F = F_1 \vee F_2$, et $t_1, \ldots, t_n$ sont des termes clos, on veut montrer que

$$\begin{aligned} &\mathscr{M} \models F_1[\bar{t}_1, \ldots, \bar{t}_n] \vee F_2[\bar{t}_1, \ldots, \bar{t}_n] \\ \text{ssi } &\mathrm{Th} \vdash F_1[t_1, \ldots, t_n] \vee F_2[t_1, \ldots, t_n]. \end{aligned}$$

Or,

$$\begin{aligned} &\mathscr{M} \models F_1[\bar{t}_1, \ldots, \bar{t}_n] \vee F_2[\bar{t}_1, \ldots, \bar{t}_n] \\ \text{ssi } &\mathscr{M} \models F_1[\bar{t}_1, \ldots, \bar{t}_n] \text{ ou } \mathscr{M} \models F_2[\bar{t}_1, \ldots, \bar{t}_n] \\ \text{ssi } &\mathrm{Th} \vdash F_1[t_1, \ldots, t_n] \text{ ou } \mathrm{Th} \vdash F_2[t_1, \ldots, t_n] \end{aligned}$$

par hypothèse. Ainsi,

  - avec $\vee_\mathsf{i}^\mathsf{g}$ et $\vee_\mathsf{i}^\mathsf{d}$, on a que $\mathrm{Th} \vdash F_1[t_1, \ldots, t_n] \vee F_2[t_1, \ldots, t_n]$;
  - réciproquement, on utilise le lemme 5 car Th est complète.

- ▷ Pour $F = \neg G$, en exercice.
- ▷ Si $F = \exists x\, G$ et $t_1, \ldots, t_n$ des termes clos, on a
  - on a $\mathscr{M} \models \exists x\, G[\bar{t}_1, \ldots, \bar{t}_n, x]$
  - ssi il existe $t \in \mathscr{E}$ tel que $\mathscr{M} \models G[\bar{t}_1, \ldots, \bar{t}_n, \bar{t}]$
  - ssi il existe $t \in \mathscr{E}$ tel que $\mathrm{Th} \vdash G(t_1, \ldots, t_n, t)$

  et donc $\mathrm{Th} \vdash \exists x\, G(t_1, \ldots, t_n, x)$ avec $\exists_\mathsf{i}$. Réciproquement, si $\mathrm{Th} \vdash \exists x G(t_1, \ldots, t_n, x)$ alors $\mathrm{Th} \vdash G(t_1, \ldots, t_n, c_{G(t_1, \ldots, t_n, x)})$, donc il existe un terme t et $\mathrm{Th} \vdash G(t_1, \ldots, t_n, t)$.

□

Lemme 14. On a $\mathscr{M} \models \mathrm{Th}$ (et donc $\mathscr{M} \models T$).

Preuve. On montre que, pour toute formule F de Th, on a que $\mathscr{M} \models F$. Pour cela, on utilise le lemme précédent : si F est close, alors

$$\mathscr{M} \models F \text{ ssi } \mathrm{Th} \vdash F.$$

□

5.3 Compacité.

Théorème 2 (Compacité (sémantique)). Une théorie T et contradictoire ssi elle est finiment contradictoire, *i.e.* il existe $T' \subseteq_{\text{fini}} T$ telle que T' est contradictoire.

Preuve. Soit T contradictoire. On utilise le théorème de complétude. Ainsi T est inconsistante. Il existe donc $T' \subseteq_{\text{fini}} T$ avec T' inconsistante par le théorème de compacité syntaxique ci-dessous (qui est trivialement vrai). On applique de nouveau le théorème de complétude pour en déduire que T' est contradictoire. □

Théorème 3 (Compacité (syntaxique)). Une théorie T est inconsistante ssi elle est finiment inconsistante.

Preuve. Ceci est évident car une preuve est nécessairement finie. □

$$\begin{tikzcd}
\begin{array}{c}\text{vérité syntaxique}\\ \text{dans une théorie finie}\end{array} \arrow[r, bend right, "\text{théorème de correction}"'] \arrow[d, leftrightarrow, "\begin{array}{c}\text{compacité}\\ \text{syntaxique}\end{array}"'] & \begin{array}{c}\text{vérité sémantique}\\ \text{dans une théorie finie}\end{array} \arrow[l, bend right, "\text{théorème de complétude}"'] \arrow[d, leftrightarrow, "\begin{array}{c}\text{compacité}\\ \text{sémantique}\end{array}"] \\
\begin{array}{c}\text{vérité syntaxique}\\ \text{dans une théorie infinie}\end{array} \arrow[r, bend right, "\text{théorème de correction}"'] & \begin{array}{c}\text{vérité sémantique}\\ \text{dans une théorie infinie}\end{array} \arrow[l, bend right, "\text{théorème de complétude}"']
\end{tikzcd}$$

Dans la suite de cette sous-section, on étudie des applications du théorème de compacité.

Théorème 4. Si une théorie T a des modèles finis arbitrairement grands, alors elle a un modèle infini. □

Corollaire 4. Il n'y a pas de théorie des groupes finis *i.e.* un ensemble d'axiomes dont les modèles sont exactement les groupes finis.

Théorème 5 (Löwenheim-Skolem). Soit T une théorie dans un langage $\mathscr{L}$ et κ un cardinal et $\kappa \geq \operatorname{card} \mathscr{L}$ et $\kappa \geq \aleph_0$.[7] Si T a un modèle infini, alors T a un modèle de cardinal κ.

Exemple 22.
- ▷ Avec $T = \mathbf{Th}(\mathbb{N})$, on a $\kappa = \operatorname{card} \mathbb{R}$.
- ▷ Avec $T = \mathbf{ZFC}$, on a $\kappa = \aleph_0 = \operatorname{card} \mathbb{N}$.

7. Ici, $\aleph_0$ est le cardinal de $\mathbb{N}$, on dit donc que κ est infini.