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 $\mathscr{R}$, 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 $t_1, \dots, t_n$ et un symbole de fonction f d'arité n, alors $f(t_1, \dots, t_n)$ 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

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

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

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

- ▷ Une *formule atomique* est une formule de la forme $\mathscr{R}(t_1,\ldots,t_n)$ où $\mathscr{R}$ 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 $\mathscr{F}_{k+1} = \mathscr{F}_k \cup \left\{ \begin{matrix} (\neg F) \\ (F \to G) \\ (F \vee G) \\ (F \wedge G) \\ \exists x\ F \\ \exists x\ G \end{matrix} \;\middle|\; \begin{matrix} F, G \in \mathscr{F}_k \\ x \in \mathscr{V} \end{matrix} \right\}$;
  - 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 $\exists x\,(x \geq 0 \wedge F)$;

▷ $\forall x \geq 0\,(F)$ au lieu de $\forall x\,(x \geq 0 \to F)$;

▷ $A \leftrightarrow B$ au lieu de $(A \to B) \wedge (B \to A)$;

▷ $t \neq u$ 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 $\wedge$ et $\vee$;
3. le symbole $\to$ (le moins prioritaire).

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

$$(((\forall x\ A) \wedge B) \to ((\neg C) \vee D)).$$

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

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

et alors

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

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 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.

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

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

Quantificateur existentiel.

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

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

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