# (I) GENERALITES

## 1/ Langages et théories

**Déf**: Un langage du premier ordre est un ensemble de symboles de constantes, de fonctions (auquels sont associé une arité) et de prédicats (idem).

**Ex**: $\mathcal{L} = \{0, 1, +, \times\}$ langage de l'arithmétique.

On définit inductivement l'ensemble des termes puis l'ensemble des formules sur un langage $\mathcal{L}$.

**Déf**: Une théorie T est un ensemble de formules closes sur un langage $\mathcal{L}$ fixé. Les éléments de T sont les axiomes de la théorie.

**Exs**:
- Théorie vide $T = \emptyset$ sur $\mathcal{L}$ quelconque
- Théorie des groupes sur $\mathcal{L} = \{e, *, ^{-1}, =\}$

$$\forall x,y,z,\ (x*y)*z = x*(y*z)$$
$$\forall x,\ x*e = x \wedge e*x = x$$
$$\forall x,\ x*x^{-1} = e \wedge x^{-1}*x = e$$

## 2/ Notion de démonstration

**Déf**: On dit qu'une théorie T démontre une formule F ($T \vdash F$) s'il existe une preuve de F dans le système de la déduction naturelle n'utilisant que pour axiomes des formules de T. On dit alors que F est un théorème de T.

**Déf**: T est dite consistante si $T \not\vdash \bot$, dans le cas contraire on dit que T est contradictoire.

**Rq**: On aurait pu choisir un autre système de déduction (Hilbert, séquents, ...) équivalent.

## 3/ Modèles

**Déf**: Un modèle $\mathcal{M}$ sur $\mathcal{L}$ est la donnée :
* d'un ensemble $M_{\mathcal{M}}$ : le domaine de $\mathcal{M}$
* d'un élément non vide $c_{\mathcal{M}}$ de $M_{\mathcal{M}}$ pour chaque symbole c de constante de $\mathcal{L}$
* d'une fonction $f_{\mathcal{M}}$ de $M_{\mathcal{M}}^n \to M_{\mathcal{M}}$ pour chaque f symbole de fonction n-aire de $\mathcal{L}$
* d'un sous-ensemble $P_{\mathcal{M}}$ de $M_{\mathcal{M}}^n$ pour chaque P symbole de prédicat n-aire de $\mathcal{L}$.

On définit la notion de véracité d'une formule close F dans un modèle $\mathcal{M}$ par induction à l'aide d'interprétations des variables. On dit que F est vraie dans $\mathcal{M}$ ou que $\mathcal{M}$ est un modèle de F ($\mathcal{M} \models F$).

**Déf**: $\mathcal{M}$ est un modèle de la théorie T si tout axiome de T est vrai dans $\mathcal{M}$ ($\mathcal{M} \models T$).

**Ex**: $(\mathbb{R}, +)$ et $((\mathbb{Z}/8\mathbb{Z})^*, \times)$ sont des modèles de la théorie des groupes.

On dit que $F$ est <u>conséquence sémantique</u> de $T$ si tout modèle de $T$ est modèle de $F$ ($T \models F$).

Ex: théorie des groupes $\models \forall x,y,z\ (x*y=x*z \Rightarrow y=z)$.

<u>Théorie de l'égalité</u> $\mathcal{L}_= = \{=\} \subseteq \mathcal{L}$

- $\forall x,\ x=x$
- $\forall x,y,\ x=y \Rightarrow y=x$
- $\forall x,y,z,\ (x=y \wedge y=z) \Rightarrow x=z$
- $\forall x_1,\dots x_n, y_1,\dots y_n,\ \left(\bigwedge_{i=1}^{n} x_i=y_i\right) \Rightarrow f(x_1,\dots x_n)=f(y_1,\dots y_n)$ pour chaque symbole de fonction $f$ d'arité $n$
- $\forall x_1,\dots x_n, y_1,\dots y_n,\ \left(\bigwedge_{i=1}^{n} x_i=y_i\right) \Rightarrow (P(x_1,\dots x_n) \to P(y_1,\dots y_n))$ pour chaque ...

Rq: On peut intégrer ces axiomes dans le système de déduction.

On dit qu'un <u>modèle $\mathcal{M}$ est égalitaire</u> si l'égalité est interprétée par $\Delta = \{(x,x) \mid x \in M_U\}$.

<u>Prop</u>: $T$ théorie contenant la théorie de l'égalité
Si $T$ admet un modèle alors elle admet un modèle égalitaire. [Do] p56

## 4/ Lien entre syntaxe et sémantique

<u>Thm de complétude</u> (de la logique classique du 1er ordre)

- $T \vdash F$ ssi $T \models F$
- $T$ consistante ssi $T$ admet un modèle

Rq: $\Rightarrow$ = correction, $\Leftarrow$ = complétude

<u>Cor 1</u> : <u>Thm de compacité</u>

- $T$ admet un modèle ssi pour toute théorie finie $T_0 \subseteq T$, $T_0$ admet un modèle.
- $T$ contradictoire ssi il existe une théorie finie $T_0 \subseteq T$, $T_0$ est contradictoire.

Logre: "être un modèle fini" n'est pas axiomatisable

<u>Cor 2</u>: <u>Thm de Löwenheim-Skolem</u>

$\mathcal{L}$ dénombrable, $T$ théorie sur $\mathcal{L}$, $\kappa$ ensemble infini [Do] p64
Si $T$ admet un modèle alors $T$ admet un modèle quelconque de même cardinal que $\kappa$.

App°: Il existe des groupes de tout cardinal infini.
Il existe des modèles non standard de l'arithmétique de Peano (cf. plus loin).

# II DECIDABILITE, COMPLETUDE

Une théorie $T$ est dite <u>récursive</u> si l'ensemble de ses axiomes est décidable, <u>décidable</u> si l'ensemble de ses théorèmes l'est.

## 1/ La théorie vide

<u>Thm de Church</u>: Si $\mathcal{L}$ contient au moins un prédicat binaire et deux symboles de fonction unaire alors la théorie vide sur $\mathcal{L}$ est indécidable. PCP !

⚠ $T \subseteq T'$ et $T$ indécidable $\not\Rightarrow$ $T'$ indécidable

## 2/ Arithmétique

**Axiomes de Peano $P_0$** $\mathcal{L} = \{0, S(\cdot), +, \times, =\}$

- $\forall x,\ S(x) \neq 0$
- $\forall x, (x = 0 \vee \exists y, x = S(y))$
- $\forall x, y,\ (Sx = Sy \to x = y)$
- $\forall x, y,\ x + 0 = x$
- $\forall x, y,\ (x + S(y) = S(x + y))$
- $\forall x,\ x \times 0 = 0$
- $\forall x, y,\ (x \times S(y) = x \times y + x)$

$PA = P_0$ + le schéma d'axiomes :

$\forall \big[ (F[x:=0] \wedge \forall y, (F[x:=y] \Rightarrow F[x:=Sy])) \Rightarrow \forall x, F \big]$

où F formule dotée universelle.

Ex : $PA \vdash \forall x, y,\ x + y = y + x$

**Thm** : Si $T \supseteq P_0$ et T consistante, alors T est indécidable.

**Déf** : T est dite complète si pour toute formule close, $T \vdash F$ ou $T \vdash \neg F$.

**Thm** : Si T est récursive est complète, T est décidable.

**1er thm de Gödel** Si $T \supseteq P_0$ et T consistante, alors T est incomplète.

**Csqce** : PA est incomplète.

**Arithmétique de Presburger** Si on se restreint au langage $\mathcal{L} = \{0, S, +, =\}$, l'arithétique devient décidable.

**Autre ex d'incomplétude** la théorie des groupes

$\forall x,\ x * x = e$ est vraie dans certains modèles et pas dans d'autres.

## III CONSISTANCE, INDEPENDANCE

**Théorie naïve des ensembles** $\mathcal{L} = \{\in\}$

schéma d'axiomes $\exists a\ \forall y\ (y \in a \Leftrightarrow P(y))$ où P formule avec une variable libre.

**Prop** : Cette théorie est contradictoire (paradoxe de Russell).

**Déf** : Une formule close F est indépendante de T si $T \nvdash F$ et $T \nvdash \neg F$.

**Géométrie**

L'axiome des parallèles d'Euclide est indépendant de ses autres axiomes. ($\rightsquigarrow$ géométries non euclidiennes...).

**Arithmétique**

**2e thm de Gödel** : PA ne peut montrer sa propre consistance : on peut construire une formule close Cons formalisant le fait que PA est consistante, et Cons est indépendante de PA !

**ZF**

C'est la solution au paradoxe de Russell mais c'est plus compliqué. L'axiomes du choix, l'hypothèse du continue et l'axiome de fondation sont indépendants de ZF...

Oubli : le calcul propositionnel (ie. les formules closes sans qtificateurs) est décidable.

Réfs :

[Do] Dowek, les démonstrations et les algorithmes.

[Nour] ...

## Théorème

La théorie logique au premier ordre des entiers munis de l'addition est décidable. Plus précisément, si $\varphi$ est une formule close, le problème de savoir si $(\mathbb{N}, +)$ est un modèle de $\varphi$ indécidable.

On se donne $\varphi$ une formule close qu'on suppose sous forme prénexe :

$$\varphi = Q_1 x_1 Q_2 x_2 \dots Q_n x_n \psi$$

où les $Q_i$ sont des quantificateurs et $\psi$ est sans quantificateurs. On définit, pour $k \in \{0 \dots n\}$, $\varphi_k(x_1, \dots, x_k) = Q_{k+1} x_{k+1} \dots Q_n x_n \psi$.

On peut de plus supposer que tous les atomes de $\psi$ sont de la forme $x_i = x_j + x_k$ ou $x_i = x_j$ : en effet, on peut s'y ramener en ajoutant des variables :

on transforme par exemple $x + y + t = u$ en $v + t = u \wedge v = x + y$ et on ajoute le quantificateur $\exists$.

On construit par récurrence descendante sur $k$ un automate $\mathcal{A}_k$ qui accepte exactement le langage $X_k$ des écriture binaires sur $\Sigma_k = \{0,1\}^k$ des $k$ −uplets d'entiers qui vérifient $\varphi_k$. On ajoute au début des nombres des 0 pour que tous les $x_k$ aient même longueur.

## Construction de l'automate $\mathcal{A}_n$

$\varphi_n$ est combinaison booléenne de clauses de la forme $x_i = x_j$ ou $x_i + x_j = x_k$. Comme on peut construire un automate qui reconnait l'union et l'intersection de langages rationnels, il suffit de construire des automates reconnaissant l'addition et l'égalité sur $\{0,1\}^2$ et $\{0,1\}^3$ respectivement :

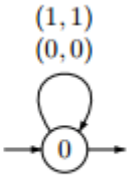


FIG. 3.11 – Automate de égalité

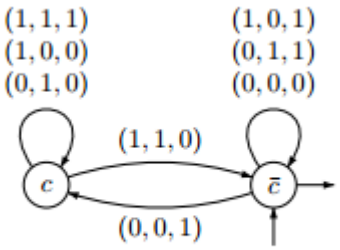


FIG. 3.12 – Automate de l'addition

L'égalité est facile : deux entiers sont égaux si et seulement si ils ont même représentation binaire. Pour l'addition, il faut deux états, l'un correspondant à l'état avec retenue, et l'autre sans retenue : comme on lit les entiers des bits les plus forts aux bits les plus faibles, on effectue le calcul « à l'envers ». On commence nécessairement une addition dans un état sans retenue, et dès qu'un calcul bit à bit ne correspond pas à l'addition bit à bit, soit le calcul est faux, soit on a fait une retenue dans les bits suivants.

## Construction de l'automate $\mathcal{A}_k$ à l'aide de l'automate $\mathcal{A}_{k+1}$

On a $\varphi_k = Q_{k+1} x_{k+1} \varphi_{k+1}$.

Si $Q_{k+1} = \forall$, alors on écrit $\varphi_k = \neg\exists x_{k+1} \neg\varphi_{k+1}$ pour se ramener au cas $Q_{k+1} = \exists$. Il faut pour cela déterminiser $\mathcal{A}_{k+1}$ pour inverser états finaux et non finaux puis faire la construction ci-dessous et à nouveau le déterminiser : c'est très long !

Si $Q_{k+1} = \exists$, on construit l'automate $\mathcal{A}_k$ en oubliant dans l'automate $\mathcal{A}_{k+1}$ la dernière lettre de $\{0,1\}^{k+1}$ : l'automate $\mathcal{A}_k$ a les mêmes états que l'automate $\mathcal{A}_{k+1}$, son alphabet est $\{0,1\}^k$, ses transitions sont de la forme $(p, (x_1, \dots, x_k), q)$ où $(p, (x_1, \dots, x_{k+1}), q)$ est une transition de $\mathcal{A}_{k+1}$. Les états finaux sont les mêmes que ceux de $\mathcal{A}_{k+1}$ et les états initiaux sont ceux qu'on peut atteindre à partir des états initiaux de $\mathcal{A}_{k+1}$ en lisant des lettres de la forme $(0, \dots, 0) \in \{0,1\}^k$.

### Exemple

La relation $x \leq y$ est équivalente à la formule $\exists z: x + z = y$. L'équation $x \equiv 0 \; mod \; 3$ est équivalente à $\exists y, z \; x = y + z \wedge z = y + y$. On peut illustrer la construction de l'automate dans ces cas.

## Théorème

Le système de la déduction naturelle est complet, i.e. si $T$ est une théorie cohérente alors elle est non contradictoire.

Pour cela, on se donne une théorie $T$ sur un langage $\mathcal{L}$ et on va montrer qu'il existe un langage $\mathcal{L}'$ et une théorie $Th$ telle que :

- $T \subset Th$ et $\mathcal{L} \subset \mathcal{L}'$
- $Th$ est complète
- Pour toute formule $G[x]$ à une variable libre, il existe un symbole de constante $c$ tel que $Th \vdash \exists x\, G[x] \rightarrow G[x \coloneqq c]$.

On considère alors le modèle $\mathcal{M}$ dont le domaine est l'ensemble des termes clos sur $\mathcal{L}'$ et l'interprétation est donnée par :

- $f_{\mathcal{M}}(t_1, \dots, t_k) = f(t_1, \dots, t_k)$
- $r_{\mathcal{M}}(t_1, \dots, t_k)$ si et seulement si $Th \vdash r(t_1, \dots, t_k)$

Montrons que l'existence d'une telle théorie implique le résultat du théorème :

Il suffit pour cela de montrer le lemme suivant (on aura le résultat pour $F$ parcourant l'ensemble des formules de $Th$) :

## Lemme

Pour toute formule close $F$, $\mathcal{M} \vDash F$ si et seulement si $Th \vdash F$.

On démontre le lemme par induction sur la formule $F$. On peut supposer que $F$ n'utilise que les connecteurs ∃, ¬ et ∨.

- Si $F = \perp$, le résultat est vrai car $Th$ est cohérente
- Si $F = r(t_1, \dots, t_k)$, le résultat est vrai par définition de $\mathcal{M}$
- Si $F = F_1 \vee F_2$ comme les $F_i$ sont closes, $Th \vdash F_1 \vee F_2$ *ssi* $Th \vdash F_1$ ou $Th \vdash F_2$ et on a le résultat par induction
- Si $F = \neg G$ alors $Th \vdash \neg G$ si et seulement si $Th$ ne démontre pas $G$ par complétude de Th et on en déduit le résultat par induction
- Si $F = \exists x\, G[x]$ alors si on a $Th \vdash F$, comme $Th \vdash \exists x\, G[x] \rightarrow G[x \coloneqq c]$ on a par règle d'élimination de $\rightarrow$ $Th \vdash G[x \coloneqq c]$ et on en déduit que $\mathcal{M} \vDash G[x \coloneqq c]$ et donc $\mathcal{M} \vDash F$. Réciproquement, si $\mathcal{M} \vDash \exists x\, G[x]$, il existe une constante $c$ telle que $\mathcal{M} \vDash G[x \coloneqq c]$ et donc $Th \vdash G[x \coloneqq c]$ et donc $Th \vdash \exists x : G[x]$ par régle d'introduction de ∃.

On a donc le lemme.

Il nous reste à construire $Th$.

Pour cela, on pose $L_0 = \mathcal{L}$ et $T_0 = T$ on construit alors par récurrence $L_n$ :

$$L_{n+1} = L_n \cup \{c_F : F[x]\ est\ une\ formule\ \text{à}\ une\ variable\ libre\ de\ L_n\}$$

$$T_{n+1} = T_n \cup \{\exists x\, F[x] \to F[c_F], F[x]\ est\ une\ formule\ à\ une\ variable\ libre\ de\ L_n\}$$

On pose alors $Th_0 = \cup\, T_n$ et $\mathcal{L}' = \cup\, L_n$.

**Proposition**

Pour toute formule $G[x]$ à une variable libre sur $\mathcal{L}'$, il existe un symbole de constante $c$ tel que $Th_0 \vdash \exists x\, G[x] \to G[x \coloneqq c]$.

C'est direct : si $G[x]$ est une formule à une variable libre sur $\mathcal{L}'$, il existe $n$ tel que $G[x] \in \mathcal{L}_n$ car $G[x]$ utilise un nombre fini de symboles de constantes. Donc $\exists x\, G[x] \to G[c_G] \in T_{n+1} \subset Th_0$.

**Proposition**

$Th_0$ est cohérente.

On démontre par récurrence sur $n$ que $T_n$ est cohérente : $T_0 = T$ est cohérente par hypothèse. Supposons $T_n$ cohérente. Supposons par l'absurde que $T_{n+1}$ n'est pas cohérente : il existe alors $c_1, \dots, c_k$ des symboles de constantes associées à des formules $F_1, \dots F_k$ telles que

$$T_n, \{\exists x, F_i[x] \to F[c_i]\}_{i=1,\dots,k} \vdash \bot$$

On en déduit alors que

$$T_n \vdash \bigwedge_i \exists x\, F_i[x] \to F[c_i] \to \bot$$

car $\Gamma, A \vdash B$ ssi $\Gamma \vdash A \to B$

Comme les variables $c_i$ n'apparaissent nulle part dans $T_n$, on peut facilement vérifier que

$$T_n \vdash \forall y_1, \dots, y_k \left( \bigwedge_i \exists x_i\, F_i[x_i] \to F[y_i] \to \bot \right)$$

donc

$$T_n \vdash \left( \exists y_1, \dots, y_k \bigwedge_i \exists x_i F_i[x_i] \to F[y_i] \right) \to \vdash$$

donc

$$T_n \vdash \left( \bigwedge_i \exists x_i\, F_i[x_i] \to \exists y_i F_i[y_i] \right) \to \vdash$$

or on a clairement $\vdash G \to G$ donc on en déduit

$T_n \vdash \bot$ ce qui est absurde. Donc $T_n$ est cohérente pour tout $n$ et par suite $T$ l'est.

Il reste maintenant à compléter $Th_0$ pour cela, on énumère les formules sur $\mathcal{L}'$ $(F_k)_{k\geq 0}$ . On pose alors $K_0 = Th_0$ et

- Si $K_n$ est complète, alors on pose $K_{n+1} = K_n$

- Sinon, soit $k = \inf k : F_k \; et \; \neg F_k$ ne sont pas prouvables dans $K_n$. On pose alors $K_{n+1} = K_n \cup F_k$.

On pose alors $Th = \cup K_n$ et $Th$ vérifie bien toutes les propriétés voulues.