Exemples de théories

0. Résumé des épisodes précédents

Les règles de la déduction naturelle

La notion de démonstration

La notion de modèle

Le théorème de correction et le théorème de complétude

Aujourd'hui

La notion de théorie

Propriétés d'une théorie

Quatre exemples de théories :

- La théorie de l'égalité
- L'arithmétique
- La théorie des ensembles
- La théorie des groupes

I. Un exercice : la logique martienne

Quelle hypothèse si les Martiens, avaient la règle de déduction naturelle

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \wedge B}$$

au lieu d'avoir la règle

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

?

Quelle hypothèse si les Martiens, avaient la règle de déduction naturelle

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \wedge B}$$

au lieu d'avoir la règle

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

?

Que, en martien, la disjonction, et non la conjonction, s'écrit $\wedge$

Quelle est la réponse à la question : « Quelle est la signification du symbole “$\wedge$” ? » ?

C'est la règle de déduction

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

(et les autres règles de déduction)

Comment sait-on que l'on peut déduire $A \wedge B$ de A et B ?

La règle

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$$

fait partie de la définition de la signification de $\wedge$

II. La notion de théorie

Pourquoi des théories ?

Un langage : 0 : constante, $=$ symbole de prédicat binaire
Déduction naturelle
Impossible démontrer

$$0 = 0$$

On ne sait pas ce que signifie le symbole $=$
Peut-être signifie-t-il « différent »

Une fusée à deux étages

La logique (règles de déduction) définit la signification des symboles $\top$, $\bot$, $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\forall$, $\exists$

La théorie (axiomes...) définit la signification des symboles 0, $=$, $\leq$, $\in$, point, droite...

Comment utiliser un axiome dans une démonstration ?

Ou bien
on ajoute une règle

$$\frac{}{\Gamma \vdash A}\ A \in \mathcal{T}$$

Ou bien
démonstration de $\Gamma \vdash B$ dans $\mathcal{T}$: démonstration de $\Gamma, \mathcal{T} \vdash B$
Règle axiome de la déduction naturelle

Théories infinies : chaque démonstration n'utilise qu'un nombre fini d'axiomes $\Gamma, \mathcal{T}' \vdash A$, pour $\mathcal{T}'$ sous-ensemble fini de $\mathcal{T}$

Un exercice

Démontrer la proposition $0 = 0$ dans la théorie $\forall x \; (x = x)$

Une grande diversité de théories

- Exprimer une partie des mathématiques : géométrie, arithmétique...
- Exprimer « toutes » les mathématiques : théorie des ensembles, théorie des types...
- Exprimer un savoir spécifique (systèmes experts) : théorie des maladies cryptogamiques des tomates...
- Théories dans lesquelles on n'est pas si intéressé que cela de construire des démonstrations, mais dont les modèles sont intéressants : théorie des groupes...

III. Les propriétés des théories

Contradiction et cohérence

$\mathcal{T}$ contradictoire si (trois définitions équivalentes)
- il existe A telle que A et $\neg A$ démontrables dans $\mathcal{T}$
- $\perp$ démontrable dans $\mathcal{T}$
- toute proposition est démontrable dans $\mathcal{T}$

Exercice : équivalence

$\mathcal{T}$ cohérente sinon (trois définitions possibles)

Complétude et incomplétude

$\mathcal{T}$ complète si pour toute proposition close A, A est démontrable ou $\neg A$ est démontrable

Wir müssen wissen. Wir werden wissen.

Incomplète sinon

Très facile de construire une théorie incomplète

Exercice : langage P, pas d'axiome, P non démontrable, $\neg P$ non démontrable

Décidabilité et indécidabilité

$\mathcal{T}$ décidable s'il existe un algorithme qui décide si une proposition est démontrable dans $\mathcal{T}$

Indécidable sinon

Les propositions de $\mathcal{T}$ peuvent se numéroter : $\ulcorner A \urcorner$ numéro de A

IV. La théorie de l'égalité

Deux axiomes
Réflexivité (identité)

$$\forall x \ (x = x)$$

Substitutivité (Leibniz)
Si deux êtres sont égaux tout ce qui est vrai de l'un est également vrai de l'autre

$$\forall x \forall y \forall c \ (x = y \Rightarrow x \ \epsilon \ c \Rightarrow y \ \epsilon \ c)$$

ϵ ?

Une théorie élémentaire des ensembles (la théorie des classes)
Une infinité d'axiomes (schéma de compréhension)
Pour chaque A ne contenant pas le symbole ϵ, un axiome

$$\overline{\forall}\ \exists c \forall z\ (z\ \epsilon\ c \Leftrightarrow A)$$

Exemple

$$\exists c \forall z\ (z \in c \Leftrightarrow (5 \leq z \wedge z \leq 28))$$

Deux sortes d'objets : individus et classes

Une alternative

Quitte à utiliser un schéma d'axiome
Éviter la notion de classe : un schéma pour l'axiome de Leibniz
Réflexivité (identité)

$$\forall x \ (x = x)$$

Substitutivité (Leibniz)

$$\overline{\forall} \ \forall x \forall y \ (x = y \Rightarrow (x/z)A \Rightarrow (y/z)A)$$

Exemple

$$\forall x \forall y \ (x = y \Rightarrow (5 \leq x \wedge x \leq 28) \Rightarrow (5 \leq y \wedge y \leq 28))$$

Une troisième (et dernière) formulation

Un nombre fini d'instances suffisantes pour schéma entier

Pour chaque symbole de fonction f et pour chaque indice i

$$\forall w_1 ... \forall w_{i-1} \forall w_{i+1} ... \forall w_n \forall x \forall y \ (x = y \Rightarrow f(w_1, ..., w_{i-1}, x, w_{i+1}, ..., w_n) = f(w_1, ..., w_{i-1}, y, w_{i+1}, ..., w_n))$$

Pour chaque symbole de prédicat P et pour chaque indice i

$$\forall w_1 ... \forall w_{i-1} \forall w_{i+1} ... \forall w_n \forall x \forall y \ (x = y \Rightarrow P(w_1, ..., w_{i-1}, x, w_{i+1}, ..., w_n) \Rightarrow P(w_1, ..., w_{i-1}, y, w_{i+1}, ..., w_n))$$

V. L'arithmétique

Un exercice pour commencer : comment exprimer qu'il y a un nombre infini d'objets ?

Un exercice pour commencer : comment exprimer qu'il y a un nombre infini d'objets ?

f, a

$$\forall x\ \forall y\ (f(x) = f(y) \Rightarrow x = y)$$

$$\forall x\ \neg(a = f(x))$$

Une manière de construire les entiers :
$0 = a$, $1 = f(a)$, $2 = f(f(a))$, $3 = f(f(f(a)))$...
Autant appeler a : 0 et f : S

$$\forall x \; \forall y \; (S(x) = S(y) \Rightarrow x = y)$$

$$\forall x \; \neg(0 = S(x))$$

Axiomes 3 et 4 de Peano

Limiter l'univers aux entiers

Ensemble des entiers : seul à contenir 0 et à être clos par S ?

Limiter l'univers aux entiers

Ensemble des entiers : seul à contenir 0 et à être clos par S ?

Non, mais plus petit

$$\forall c\ (0 \epsilon c \Rightarrow \forall x\ (x \epsilon c \Rightarrow S(x) \epsilon c) \Rightarrow \forall y\ y \epsilon c)$$

Axiome 5 de Peano

ϵ ?

Une théorie élémentaires des ensembles (la théorie des classes)
Une infinité d'axiomes (schéma de compréhension)
Pour chaque A ne contenant pas le symbole ϵ, un axiome

$$\overline{\forall}\ \exists c \forall z\ (z\ \epsilon\ c \Leftrightarrow A)$$

Exemple

$$\exists c \forall z\ (z \in c \Leftrightarrow (5 \leq z \wedge z \leq 28))$$

Deux sortes d'objets : entiers et classes

Une alternative

Quitte à utiliser un schéma d'axiome
Éviter la notion de classe : un schéma pour l'axiome 5 de Peano

$$\overline{\forall}\ ((0/z)A \Rightarrow \forall x\ ((x/z)A \Rightarrow (S(x)/z)A) \Rightarrow \forall y\ (y/z)A)$$

Et on est presque au bout : addition et multiplication

$$\forall y\ (0 + y = y)$$

$$\forall x\ \forall y\ (S(x) + y = S(x + y))$$

$$\forall y\ (0 \times y = 0)$$

$$\forall x\ \forall y\ (S(x) \times y = (x \times y) + y)$$

Exercice : démontrer $\forall x\ (x + 0 = x)$?

$0 + 0 = 0$
Si $x + 0 = x$ alors $S(x) + 0 = S(x + 0) = S(x)$
Et ensuite ?

Exercice : démontrer $\forall x\ (x + 0 = x)$?

$0 + 0 = 0$
Si $x + 0 = x$ alors $S(x) + 0 = S(x + 0) = S(x)$
Et ensuite ?

La classe des z tels que $z + 0 = z$ contient 0 et close par successeur
Ou alors

$$0 + 0 = 0 \Rightarrow \forall x\ (x + 0 = x \Rightarrow S(x) + 0 = S(x)) \Rightarrow \forall y\ y + 0 = y$$

Axiome 5 = axiome de récurrence

Une question légitime

Pourquoi $+$ et $\times$ et pas $\uparrow$

Parce que $\uparrow$ (et toutes les fonctions calculables) est définissable
Mais pas $\times$, si $+$ uniquement

Une autre question légitime

Pourquoi 3, 4 et 5 ?
Une autre formulation de l'arithmétique avec un prédicat N qui caractérise les entiers

$$\forall c \ (0 \ \epsilon \ c \Rightarrow \forall x \ (x \ \epsilon \ c \Rightarrow S(x) \ \epsilon \ c) \Rightarrow \forall y \ y \ \epsilon \ c)$$

$$\forall c \ (0 \ \epsilon \ c \Rightarrow \forall x \ (x \ \epsilon \ c \Rightarrow S(x) \ \epsilon \ c) \Rightarrow \forall y \ (N(y) \Rightarrow y \ \epsilon \ c))$$

Dans ce cas

$$N(0)$$

$$\forall x \ (N(x) \Rightarrow N(S(x)))$$

Axiomes 1 et 2

Les 2^2 variantes de l'arithmétique de Peano (PA)

Avec N / sans N, avec c / sans c
Peano : avec, avec, à la mode : sans, sans

VI. La théorie des ensembles

La théorie naïve des ensembles

Dans la théorie des classes ϵ : à gauche un entier, à droite une classe (deux sortes d'objets)
Mais on veut aussi des ensembles d'ensembles : une seule sorte, $\in$ pour chaque A (possiblement contenant $\in$), un axiome

$$\overline{\forall}\ \exists E \forall y\ (y \in E \Leftrightarrow A)$$

Inventée de nombreuses fois : Cantor, Frege...

Le paradoxe de Russell (1902)

Mais

$$\exists R \forall y \; (y \in R \Leftrightarrow \neg y \in y)$$

$$R \in R \Leftrightarrow \neg R \in R$$

Si $R \in R$, alors $\neg R \in R$, donc $\perp$
Donc $\neg R \in R$, donc $R \in R$, donc $\perp$

La théorie des ensembles et la théorie des types

Deux principes :

- n'importe quel prédicat définit un ensemble
- n'importe quel prédicat s'applique à n'importe quel ensemble

Abandon du premier : théorie des ensembles (Zermelo 1908)
Abandon du second : théorie des types (Russell 1903)

La théorie des ensembles de Zermelo

Quatre cas particuliers du schéma de compréhension

Paire :

$$\forall x \forall y \exists z \forall w \; (w \in z \Leftrightarrow (w = x \vee w = y))$$

Réunion :

$$\forall x \exists z \forall w \; (w \in z \Leftrightarrow (\exists v \; (w \in v \wedge v \in x)))$$

Parties :

$$\forall x \exists z \forall w \; (w \in z \Leftrightarrow (\forall v \; (v \in w \Rightarrow v \in x)))$$

Sous-ensemble (séparation, compréhension restreinte) :

$$\overline{\forall} \; \forall x \exists z \forall w \; (w \in z \Leftrightarrow (w \in x \wedge A))$$

À nouveau : classes ou non

Pas de paradoxe de Russell

$$\exists R \forall y \; (y \in R \Leftrightarrow \neg y \in y)$$

Pourquoi ?

L'axiome d'extensionalité

$$\forall E \forall F \; ((\forall x \; (x \in E \Leftrightarrow x \in F)) \Rightarrow E = F)$$

Pas d'ensemble de tous les ensembles

Si un ensemble de tous les ensembles : le schéma de séparation devient le schéma de compréhension

$$\overline{\forall}\ \forall x \exists z \forall w\ (w \in z \Leftrightarrow (w \in x \wedge A))$$

Plus direct : pour chaque ensemble E un ensemble R_E tel que

$$\forall w\ (w \in R_E \Leftrightarrow (w \in E \wedge \neg w \in w))$$

$$R_E \in R_E \Leftrightarrow (R_E \in E \wedge \neg R_E \in R_E))$$

Si $R_E \in R_E$, alors $\neg R_E \in R_E$, donc $\bot$
Donc $\neg R_E \in R_E$
Si $R_E \in E$, alors $R_E \in R_E$, donc $\bot$
Donc $\neg R_E \in E$

Définir les entiers en théorie des ensembles

Trois définitions possibles : Cantor - Peano - Von Neumann

Cantor :
Un axiome qui énonce l'existence d'un ensemble infini B
Cardinaux finis dans B
3 est l'ensemble de tous les ensembles de trois éléments de B
Éléments de l'ensemble des parties de l'ensemble des parties de B

Peano :

Un axiome qui énonce l'existence d'un ensemble infini B

S injection non surjective de B dans B, 0 un élément qui n'est pas dans l'image de S

Von Neumann :

n est l'ensemble des entiers strictement inférieurs à n

$0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$...

Besoin d'un axiome pour l'existence de l'ensemble $\mathbb{N}$

Toujours besoin d'un axiome énonçant l'existence d'un ensemble infini : sinon modèle dans lequel tout ensemble est fini

Les fonctions

Les fonctions comme graphes : ensembles de couples

La théorie des types

Finalement distinguer les individus et les classes une bonne idée
Langage à plusieurs sortes d'objets

Mais on veut aussi des ensembles d'ensembles,
des ensembles d'ensembles d'ensembles,
etc.

Non 2 mais une infinité de sortes, appelées types
ι, $\wp(\iota)$, $\wp(\wp(\iota))$... (aussi notés 0, 1, 2...)
$\in_n$: en argument un terme de sorte n et un terme de sorte $n+1$

Pas de paradoxe de Russell

$$\exists R \forall y \; (y \in R \Leftrightarrow \neg y \in_n y)$$

Pourquoi ?

Les entiers en théorie des types

Cantor, Peano
mais pas Von Neumann ($\{\varnothing, \{\varnothing\}\}$)

De nombreuses autres variantes

En théorie des ensembles et en théorie des types (de Russell)
Ensembles : primitifs, fonctions : ensembles

Autre solution :
Fonctions : primitives, ensembles : fonctions
Pas de symbole $\in$ mais un symbole α

$$\exists f\ \forall x_1\ ...\ \forall x_n\ \alpha(f, x_1, ..., x_n) = t$$

Exemple :

$$\exists f\ \forall x \forall y\ \alpha(f, x, y) = x \times x + y \times y$$

Ensembles : fonctions caractéristiques

VII. La théorie des groupes

$$\forall x \forall y \forall z\ ((x+y)+z) = (x+(y+z))$$

$$\forall x (x+0 = x)$$

$$\forall x (0+x = x)$$

$$\forall x (I(x)+x = 0)$$

$$\forall x (x+I(x) = 0)$$

Peu intéressante en tant que théorie déductive : $I(e) = e$, $\forall x\ I(I(x)) = x$...

Mais ses modèles sont intéressants pour eux-mêmes

La prochaine fois : l'indécidabilité de la démontrabilité