Introduction à la Logique Mathématique et Théorème de Gödel

Benjamin Druart

Institut Fourier

14 mars 2012

Plan

Plan

Notion de Langage

Définition

Un **langage** $\mathcal{L}$ est un ensemble de symboles constitué :

- d'un ensemble de symboles logiques $\{\neg; \vee; \wedge; \Rightarrow; \Leftrightarrow; \forall; \exists; (;)\}$;
- d'un ensemble de variables $\{x_1; x_2; ....; x_n; ....\}$;
- d'un ensemble $\mathcal{C}$ de constantes (ex : 0, 1, e ...) ;
- d'un ensemble $\mathcal{F}$ de fonctions (ex: $+$, $\cdot$, exp ...) ;
- d'un ensemble $\mathcal{R}$ de relations (ex: $=$, $\leq$ ...).

Formule du premier ordre

On peut ainsi définir une **formule du premier ordre** comme une suite finie de symboles d'un langage obéissant à certaines règles, telle que :

- '$\forall \vee x_1 + = ((\exists$' ne soit pas une formule ;
- '$\forall x (x \geq 0 \Rightarrow \exists y \quad x = y^2)$' soit une formule.

Formule du premier ordre

On peut ainsi définir une **formule du premier ordre** comme une suite finie de symboles d'un langage obéissant à certaines règles, telle que :

- '$\forall \vee x_1 + = ((\exists$' ne soit pas une formule ;
- '$\forall x (x \geq 0 \Rightarrow \exists y \quad x = y^2)$' soit une formule.

Dans une formule du premier ordre les quantificateurs ne portent que sur les variables et pas sur des ensembles ou des nombres entiers :

- on ne peut pas dire, a priori, avec une formule du premier ordre qu'un groupe G est simple, il faudrait pouvoir exprimer que tout sous-groupe distingué est soit G soit $\{e\}$.
- on ne peut pas dire, a priori, qu'un élément d'un groupe est d'ordre fini.

Structures

Une $\mathcal{L}$- structure $\mathfrak{M}$ est constituée d'un ensemble de base M, où l'on peut interpréter chaque symbole du langage $\mathcal{L}$.

Structures

Une $\mathcal{L}$- structure $\mathfrak{M}$ est constituée d'un ensemble de base M, où l'on peut interpréter chaque symbole du langage $\mathcal{L}$.

Exemples :

- $\langle \mathbb{R}, 0, 1, +, -, \cdot, \leq \rangle$;
- $\langle \mathbb{R}, < \rangle$;
- $\langle \mathbb{C}, 0, 1, +, -, \cdot \rangle$;
- $\langle G, e, \cdot \rangle$.

Structures

Une $\mathcal{L}$- structure $\mathfrak{M}$ est constituée d'un ensemble de base M, où l'on peut interpréter chaque symbole du langage $\mathcal{L}$.

Exemples :

- $\langle \mathbb{R}, 0, 1, +, -, \cdot, \leq \rangle$;
- $\langle \mathbb{R}, < \rangle$;
- $\langle \mathbb{C}, 0, 1, +, -, \cdot \rangle$;
- $\langle G, e, \cdot \rangle$.

Notation : Si la formule φ est vraie dans $\mathfrak{M}$, on note $\mathfrak{M} \models \varphi$.

- $\langle \mathbb{R}, 0, 1, +, -, \cdot, \geq \rangle \models \forall x (x \geq 0 \Rightarrow \exists y \quad x = y^2)$
- $\langle \mathbb{Q}, 0, 1, +, -, \cdot, \geq \rangle \not\models \forall x (x \geq 0 \Rightarrow \exists y \quad x = y^2)$

Théorie

Définition

Une **théorie** T est un ensemble de formules.

Exemple : La théorie des groupes T dans le langage $\mathcal{L} = \{e, \cdot\}$ est l'ensemble des 3 formules suivantes :

- $\forall x \forall y \forall z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \quad e \cdot x = x \cdot e = x$
- $\forall x \exists y \quad x \cdot y = y \cdot x = e$

Théorie

Définition

Une **théorie** T est un ensemble de formules.

Exemple : La théorie des groupes T dans le langage $\mathcal{L} = \{e, \cdot\}$ est l'ensemble des 3 formules suivantes :

- $\forall x \forall y \forall z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \quad e \cdot x = x \cdot e = x$
- $\forall x \exists y \quad x \cdot y = y \cdot x = e$

Vocabulaire : Si $\mathfrak{M} \models T$, on dit que $\mathfrak{M}$ est un **modèle** de T.

Théorie

Définition

Une **théorie** T est un ensemble de formules.

Exemple : La théorie des groupes T dans le langage $\mathcal{L} = \{e, \cdot\}$ est l'ensemble des 3 formules suivantes :

- $\forall x \forall y \forall z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \quad e \cdot x = x \cdot e = x$
- $\forall x \exists y \quad x \cdot y = y \cdot x = e$

Vocabulaire : Si $\mathfrak{M} \models T$, on dit que $\mathfrak{M}$ est un **modèle** de T.

Définition

On dit qu'une théorie T est consistante si elle admet au moins un modèle.

Conséquence sémantique

Définition

Soit T une théorie et φ une formule.
On dit que φ est une conséquence sémantique de T, et on note $T \vdash \varphi$, si pour tout $\mathfrak{M} \models T$, on a $\mathfrak{M} \models \varphi$.

Conséquence sémantique

Définition

Soit T une théorie et φ une formule.
On dit que φ est une conséquence sémantique de T, et on note $T \vdash \varphi$, si pour tout $\mathfrak{M} \models T$, on a $\mathfrak{M} \models \varphi$.

Exemple : Si T est la théorie des groupes, on a

$$T \quad \vdash \quad \forall y (\forall x \quad x \cdot y = y \cdot x = x \quad \Rightarrow \quad y = e)$$

Démonstration

Soit T une théorie, et φ une formule.
On dit que T démontre φ si il existe une suite finie de formules $\psi_1, \psi_2, ..., \psi_n$ telle que $\psi_n = \varphi$ et que ψ_i est :

- soit une formule de T;
- soit une tautologie ;
- soit obtenue à partir à partir des ψ_j (pour $j < i$) par des règles de déduction élémentaires.

Démonstration

Soit T une théorie, et φ une formule.
On dit que T démontre φ si il existe une suite finie de formules $\psi_1, \psi_2, ..., \psi_n$ telle que $\psi_n = \varphi$ et que ψ_i est :

- soit une formule de T;
- soit une tautologie ;
- soit obtenue à partir à partir des ψ_j (pour $j < i$) par des règles de déduction élémentaires.

Théorème de complétude de Gödel

T démontre φ si et seulement si $T \vdash \varphi$.

Démonstration

Soit T une théorie, et φ une formule.
On dit que T démontre φ si il existe une suite finie de formules $\psi_1, \psi_2, ..., \psi_n$ telle que $\psi_n = \varphi$ et que ψ_i est :

- soit une formule de T;
- soit une tautologie ;
- soit obtenue à partir à partir des ψ_j (pour $j < i$) par des règles de déduction élémentaires.

Théorème de complétude de Gödel

T démontre φ si et seulement si $T \vdash \varphi$.

Remarque : T n'est pas consistante *ssi* il existe une formule φ telle que $T \vdash \varphi$ et $T \vdash \neg\varphi$.

Théories complètes

Définition

On dit qu'une théorie T est **complète** si elle est consistante et si elle vérifie l'une des deux conditions équivalentes suivantes :
(i) Tous les modèles de T vérifient les mêmes formules.
(ii) Pour toute formule φ, $T \vdash \varphi$ ou $T \vdash \neg\varphi$.

Théories complètes

Définition

On dit qu'une théorie T est **complète** si elle est consistante et si elle vérifie l'une des deux conditions équivalentes suivantes :
(i) Tous les modèles de T vérifient les mêmes formules.
(ii) Pour toute formule φ, $\quad T \vdash \varphi$ ou $T \vdash \neg\varphi$.

Exemples:

- La théorie des corps algébriquement clos de caractéristique donnée est complète.
- La théorie des groupes abélien infini divisible sans torsion est complète.

Le théorème de compacité

Théorème de compacité

1. T est consistante *ssi* toute partie finie de T est consistante.
2. T est inconsistante *ssi* il existe une partie finie T_0 de T inconsistante.
3. $T \vdash \varphi$ *ssi* il existe une partie finie $T_0 \subseteq T$ telle que $T_0 \vdash \varphi$.

Plan

Fonctions récursives primitives

Définition

On considère $\mathcal{F}$ l'ensembles des fonctions $f : \mathbb{N}^p \longrightarrow \mathbb{N}$.
L'ensemble des **fonctions récursives primitives** est le plus petit sous-ensemble de $\mathcal{F}$ qui contient :

- la fonction *nulle* ($0 : \mathbb{N} \longrightarrow \mathbb{N}$);
- la fonction *successeur* ($s : \mathbb{N} \longrightarrow \mathbb{N}$) ;
- les fonctions *projections* ($p_k^i : \mathbb{N}^k \longrightarrow \mathbb{N}$ telles que $p_k^i(x_1, ..., x_k) = x_i$).

et qui est clos par :

- *composition* : si $h : \mathbb{N}^p \longrightarrow \mathbb{N}$ et $g_1, ..., g_p : \mathbb{N}^n \longrightarrow \mathbb{N}$ sont récursives primitives, alors $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ définie par $f(x_1, ..., x_n) = h(g_1(x_1, ..., x_n), ..., g_p(x_1, ..., x_n))$ est récursive primitive.
- récurrence : si $g : \mathbb{N}^p \longrightarrow \mathbb{N}$ et $h : \mathbb{N}^{p+2} \longrightarrow \mathbb{N}$ sont récursives primitives alors $f : \mathbb{N}^{p+1} \longrightarrow \mathbb{N}$ est récursive primitive où :

$$f(a_1, ..., a_p, 0) = g(a_1, ..., a_p)$$
$$f(a_1, ..., a_p, x+1) = h(a_1, ..., a_p, x, f(a_1, ..., a_p, x))$$

Exemples :

1. L'addition : on la définit par récurrence

$$\begin{aligned} x + 0 &= x \\ x + (y+1) &= (x+y) + 1 = s(p_3^3(x, y, x+y)) \end{aligned}$$

Exemples :

1. L'addition : on la définit par récurrence

$$\begin{aligned} x + 0 &= x \\ x + (y+1) &= (x+y) + 1 = s(p_3^3(x, y, x+y)) \end{aligned}$$

2. La multiplication :

$$\begin{aligned} x \cdot 0 &= 0 \\ x \cdot (y+1) &= (x \cdot y) + y \end{aligned}$$

Exemples :

1. L'addition : on la définit par récurrence

$$
\begin{aligned}
x + 0 &= x \\
x + (y+1) &= (x+y) + 1 = s(p_3^3(x, y, x+y))
\end{aligned}
$$

2. La multiplication :

$$
\begin{aligned}
x \cdot 0 &= 0 \\
x \cdot (y+1) &= (x \cdot y) + y
\end{aligned}
$$

3. Les fonctions polynômes ;
4. La division euclidienne ;
5. La fonction qui à $n \in \mathbb{N}$ associe la n^{ieme} décimale de π ou de e.

Ensembles récursifs primitifs

Définition

Un ensemble (ou un prédicat) $E \subseteq \mathbb{N}^p$ est dit récursif primitif si sa fonction caractéristique est récursive primitive.

Ensembles récursifs primitifs

Définition

Un ensemble (ou un prédicat) $E \subseteq \mathbb{N}^p$ est dit récursif primitif si sa fonction caractéristique est récursive primitive.

Exemples :

1. Les ensembles finis ;
2. L'ensembles des nombres premiers ;
3. Les prédicats $\leq, \geq, =, \neq, ...$(ie. les ensembles $\{(x; y) \in \mathbb{N}^2 \mid x \leq y\}$...)

Définition

Un ensemble (ou un prédicat) $E \subseteq \mathbb{N}^p$ est dit récursif primitif si sa fonction caractéristique est récursive primitive.

Exemples :

1. Les ensembles finis ;
2. L'ensembles des nombres premiers ;
3. Les prédicats $\leq, \geq, =, \neq, ...$(ie. les ensembles $\{(x; y) \in \mathbb{N}^2 \mid x \leq y\}...$)

Proposition

L'ensemble des prédicats récursifs primitifs est clos par $\neg, \wedge, \vee$ et par quantification bornée (ie si $P(x_1, ..., x_n, y)$ est récursif primitif, alors le prédicat $Q(x_1, ..., x_n) = \forall y \leq k \quad P(x_1, ..., x_n)$ est récursif primitif).

Fonction d'Ackermann

On considère la fonction $A : \mathbb{N}^2 \longrightarrow \mathbb{N}$ définie par :
$A(0, x) = x + 2$
$A(1, 0) = 0$ et $A(n + 2, 0) = 1$
$A(n + 1, x + 1) = A(n, A(n + 1, x))$

Fonction d'Ackermann

On considère la fonction $A : \mathbb{N}^2 \longrightarrow \mathbb{N}$ définie par :
$A(0, x) = x + 2$
$A(1, 0) = 0$ et $A(n + 2, 0) = 1$
$A(n + 1, x + 1) = A(n, A(n + 1, x))$

On peut démontrer que :
$A(0, x) = x + 2$
$A(1, x) = 2x$
$A(2, x) = 2^x$

Cette fonction est a priori calculable...

Fonction d'Ackermann

On considère la fonction $A : \mathbb{N}^2 \longrightarrow \mathbb{N}$ définie par :
$A(0, x) = x + 2$
$A(1, 0) = 0$ et $A(n + 2, 0) = 1$
$A(n + 1, x + 1) = A(n, A(n + 1, x))$

On peut démontrer que :
$A(0, x) = x + 2$
$A(1, x) = 2x$
$A(2, x) = 2^x$

Cette fonction est a priori calculable...
... MAIS ELLE N'EST PAS RECURSIVE PRIMITIVE !

Fonctions récursives

Définition

On considère $\mathcal{F}$ l'ensembles des fonctions $f : \mathbb{N}^p \longrightarrow \mathbb{N}$.
L'ensemble des **fonctions récursives** est le plus petit sous-ensemble de $\mathcal{F}$ qui contient :

- la fonction *nulle* ($0 : \mathbb{N} \longrightarrow \mathbb{N}$);
- la fonction *successeur* ($s : \mathbb{N} \longrightarrow \mathbb{N}$) ;
- les fonctions *projections* ($p_k^i : \mathbb{N}^k \longrightarrow \mathbb{N}$ telles que $p_k^i(x_1, ..., x_k) = x_i$).

et qui est clos par :

- *composition* : si $h : \mathbb{N}^p \longrightarrow \mathbb{N}$ et $g_1, ..., g_p : \mathbb{N}^n \longrightarrow \mathbb{N}$ sont récursives, alors $f : \mathbb{N}^n \longrightarrow \mathbb{N}$ définie par
  $f(x_1, ..., x_n) = h(g_1(x_1, ..., x_n), ..., g_p(x_1, ..., x_n))$ est récursive.
- *récurrence* : si $g : \mathbb{N}^p \longrightarrow \mathbb{N}$ et $h : \mathbb{N}^{p+2} \longrightarrow \mathbb{N}$ sont récursives alors $f : \mathbb{N}^{p+1} \longrightarrow \mathbb{N}$ est récursive où :

$$f(a_1, ..., a_p, 0) = g(a_1, ..., a_p)$$
$$f(a_1, ..., a_p, x+1) = h(a_1, ..., a_p, x, f(a_1, ..., a_p, x))$$

- *opérateur μ* : si $g : \mathbb{N}^{p+1} \longrightarrow \mathbb{N}$ est récursive alors la fonction $f : \mathbb{N} \longrightarrow \mathbb{N}$ est récursive, où

$$f(a_1, ..., a_p) = \mu t[g(a_1, ..., a_p, t) = 0] = \text{le plus petit } t \text{ tel que } g(a_1, ..., a_p, t) = 0$$

Ensembles récursifs

Définition

Un ensemble $E \subseteq \mathbb{N}^p$ est dit récursif si sa fonction caractéristique est une fonction récursive totale (ie. définie partout).

Ensembles récursivement énumérables

Définition

Un ensemble $E \subseteq \mathbb{N}^p$ est dit **récursivement énumérable** si il est vide ou si il est l'image d'une fonction récursive totale (ie. il existe une fonction récursive totale $f : \mathbb{N} \longrightarrow \mathbb{N}^p$ telle que $E = \{f(x) \mid x \in \mathbb{N}\}$).

Définition

Un ensemble $E \subseteq \mathbb{N}^p$ est dit **récursivement énumérable** si il est vide ou si il est l'image d'une fonction récursive totale (ie. il existe une fonction récursive totale $f : \mathbb{N} \longrightarrow \mathbb{N}^p$ telle que $E = \{f(x) \mid x \in \mathbb{N}\}$).

Remarque : Tout ensemble récursif est récursivement énumérable.

Proposition

Un ensemble $E \subseteq \mathbb{N}^p$ est récursif *ssi* E et E^c sont récursivement énumérables.

Ensembles récursivement énumérables

Définition

Un ensemble $E \subseteq \mathbb{N}^p$ est dit **récursivement énumérable** si il est vide ou si il est l'image d'une fonction récursive totale (ie. il existe une fonction récursive totale $f : \mathbb{N} \longrightarrow \mathbb{N}^p$ telle que $E = \{f(x) \mid x \in \mathbb{N}\}$).

Remarque : Tout ensemble récursif est récursivement énumérable.

Proposition

Un ensemble $E \subseteq \mathbb{N}^p$ est récursif *ssi* E et E^c sont récursivement énumérables.

Proposition

Un ensemble $E \subseteq \mathbb{N}$ est récursivement énumérable *ssi* il est définie par une formule de la forme $\exists x_1 ... \exists x_k \varphi$ où φ est sans quantificateur non borné.

Machines de Turing et thèse de Church

De son côté, A. Turing a donné un modèle de machine abstraite pour définir ce qui calculable.
Ce sont des machines capables de n'effectuer que certaines opérations très élémentaires. On entre les données initiale et on obtient le résultat.

Machines de Turing et thèse de Church

De son côté, A. Turing a donné un modèle de machine abstraite pour définir ce qui calculable.
Ce sont des machines capables de n'effectuer que certaines opérations très élémentaires. On entre les données initiale et on obtient le résultat.

Proposition

Ce qui est calculable à partir de fonction récursive est calculable avec des machines de Turing et vice-versa.

Machines de Turing et thèse de Church

De son côté, A. Turing a donné un modèle de machine abstraite pour définir ce qui calculable.
Ce sont des machines capables de n'effectuer que certaines opérations très élémentaires. On entre les données initiale et on obtient le résultat.

Proposition

Ce qui est calculable à partir de fonction récursive est calculable avec des machines de Turing et vice-versa.

Thèse de Church

$\{\text{Fonctions calculables}\} = \{\text{Fonctions récursives}\} = \{\text{Machine de Turing}\}$

Codage des machines de Turing

Une fonction récursive, considérée comme une machine de Turing, peut être vue comme une suite d'instructions (qui déterminent entièrement ma fonction).
Je peux associer à chaque instruction un nombre entier naturel, et ainsi coder chaque fonction par un entier naturel.
A partir du code, je peux retrouver la suite d'instruction.

Codage des machines de Turing

Une fonction récursive, considérée comme une machine de Turing, peut être vue comme une suite d'instructions (qui déterminent entièrement ma fonction).
Je peux associer à chaque instruction un nombre entier naturel, et ainsi coder chaque fonction par un entier naturel.
A partir du code, je peux retrouver la suite d'instruction.

Un code ne représente qu'une seule fonction.
Une fonction peut être représentée par plusieurs codes.

Fonction universelle

Théorème

Pour tout entier p.
Il existe une fonction récursive $\varphi^p : \mathbb{N}^{p+1} \longrightarrow \mathbb{N}$ telle que

$$\forall x_1, ..., x_p \quad \varphi^p(\alpha, x_1, ..., x_p) = f(x_1, ..., x_p)$$

où f est la fonction de code α.

Fonction universelle

Théorème

Pour tout entier p.
Il existe une fonction récursive $\varphi^p : \mathbb{N}^{p+1} \longrightarrow \mathbb{N}$ telle que

$$\forall x_1, ..., x_p \quad \varphi^p(\alpha, x_1, ..., x_p) = f(x_1, ..., x_p)$$

où f est la fonction de code α.

Exemples d'ensembles non récursifs :

- $\{\alpha \in \mathbb{N} \mid \alpha \text{ code la fonction } f\}$ où f est une fonction récursive donnée.
- $\{x \in \mathbb{N} \mid \varphi^1(x, x) \text{ est défini}\}$.

Plan

Arithmétique de Péano

On cherche à axiotamiser les propriétés de $\mathbb{N}$:
On se place dans le langage $\mathcal{L}_{Ar} = \{0, s, +, \cdot, <\}$.
On considère la théorie P constituée des axiomes suivants :

1. $\forall v_0 \quad \neg s(v_0) = 0$
2. $\forall v_0 \forall v_1 \quad (s(v_0) = s(v_1) \Rightarrow v_0 = v_1)$
3. $\forall v_0 \quad v_0 + 0 = v_0$
4. $\forall v_0 \forall v_1 \quad v_0 + s(v_1) = s(v_0 + v_1)$
5. $\forall v_0 \quad v_0 \cdot 0 = 0$
6. $\forall v_0 \forall v_1 \quad v_0 \cdot s(v_1) = v_0 \cdot v_1 + v_0$
7. $\forall v_0 \quad \neg v_0 < 0$
8. $\forall v_0 \forall v_1 \quad (v_0 < v_1 \vee v_0 = v_1 \vee v_1 < v_0)$
9. $\forall v_0 \forall v_1 \quad (v_0 < s(v_1) \Rightarrow (v_0 < v_1 \vee v_0 = v_1))$

Arithmétique de Péano

On cherche à axiotamiser les propriétés de $\mathbb{N}$:
On se place dans le langage $\mathcal{L}_{Ar} = \{0, s, +, \cdot, <\}$.
On considère la théorie P constituée des axiomes suivants :

1. $\forall v_0 \quad \neg s(v_0) = 0$
2. $\forall v_0 \forall v_1 \quad (s(v_0) = s(v_1) \Rightarrow v_0 = v_1)$
3. $\forall v_0 \quad v_0 + 0 = v_0$
4. $\forall v_0 \forall v_1 \quad v_0 + s(v_1) = s(v_0 + v_1)$
5. $\forall v_0 \quad v_0 \cdot 0 = 0$
6. $\forall v_0 \forall v_1 \quad v_0 \cdot s(v_1) = v_0 \cdot v_1 + v_0$
7. $\forall v_0 \quad \neg v_0 < 0$
8. $\forall v_0 \forall v_1 \quad (v_0 < v_1 \vee v_0 = v_1 \vee v_1 < v_0)$
9. $\forall v_0 \forall v_1 \quad (v_0 < s(v_1) \Rightarrow (v_0 < v_1 \vee v_0 = v_1))$
10. $\forall \bar{v} \quad [\varphi(0, \bar{v}) \wedge \forall w \ (\varphi(w, \bar{v}) \Rightarrow \varphi(s(w), \bar{v}))] \Rightarrow \forall w \ \varphi(w; \bar{v})$

Codage des formules

$$\varphi = \quad \forall n \quad \exists m \quad (\exists k \quad m = k \cdot k \quad \wedge \quad n < m)$$

Codage des formules

$$\varphi = \quad \forall n \quad \exists m \quad (\exists k \quad m = k \cdot k \quad \wedge \quad n < m)$$

$$\downarrow$$

11 0 13 2 15 13 4 2 21 4 27 4 5 0 29 2 17

Codage des formules

$$\varphi = \quad \forall n \quad \exists m \quad (\exists k \quad m = k \cdot k \quad \wedge \quad n < m)$$

$$\downarrow$$

11 0 13 2 15 13 4 2 21 4 27 4 5 0 29 2 17

$$\downarrow$$

$$\ulcorner \varphi \urcorner = 2^{11+1} \cdot 3^{0+1} \cdot 5^{13+1} \cdot 7^{2+1} \cdot \ldots . \cdot 59^{17+1}$$

Remarques sur le codage

Proposition

L'ensemble $\{\ulcorner \varphi \urcorner \mid \varphi \text{ est une formule}\}$ est récursif primitif.

Remarques sur le codage

Proposition

L'ensemble $\{\ulcorner\varphi\urcorner \mid \varphi \text{ est une formule}\}$ est récursif primitif.

Les démonstrations sont des suites finies de formules, on peut donc coder les preuves. A chaque démonstration D, on va associé son code $\ulcorner D\urcorner$.

Remarques sur le codage

Proposition

L'ensemble $\{\ulcorner \varphi \urcorner \mid \varphi \text{ est une formule}\}$ est récursif primitif.

Les démonstrations sont des suites finies de formules, on peut donc coder les preuves. A chaque démonstration D, on va associé son code $\ulcorner D \urcorner$.

Proposition

L'ensemble $\{\ulcorner D \urcorner \mid D \text{ est une démonstration}\}$ est récursif primitif.

Théories décidables

Définition

Soit T une théorie.

1. On dit que T est **récursivement axiomatisée** si $\{\ulcorner\varphi\urcorner \mid \varphi \in T\}$ est un ensemble récursif.

Théories décidables

Définition

Soit T une théorie.

1. On dit que T est **récursivement axiomatisée** si $\{\ulcorner\varphi\urcorner \mid \varphi \in T\}$ est un ensemble récursif.
2. On dit que T est **décidable** si $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ est récursif.

Théories décidables

Définition

Soit T une théorie.

1. On dit que T est **récursivement axiomatisée** si $\{\ulcorner\varphi\urcorner \mid \varphi \in T\}$ est un ensemble récursif.
2. On dit que T est **décidable** si $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ est récursif.

Théorème

Si T est récursivement axiomatisable, alors

- $\{(d, f) \in \mathbb{N}^2 \mid d$ est le code d'une démonstration qui prouve la formule codée par f à partir de $T\}$ est récursif primitif.
- $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ est récursivement énumérable.

Indécidabilité de l'arithmétique

On voit facilement que P est récursivement axiomatisée.

Indécidabilité de l'arithmétique

On voit facilement que P est récursivement axiomatisée.

Théorème d'indécidabilté de Church

- P est indécidable.
- Toute théorie de $\mathcal{L}_{Ar}$ contenant P est indécidable.

Incomplétude

Théorème

Soit T une théorie de $\mathcal{L}_{Ar}$.
Si T est récursivement axiomatisée et complète alors T est décidable.

Incomplétude

Théorème

Soit T une théorie de $\mathcal{L}_{Ar}$.
Si T est récursivement axiomatisée et complète alors T est décidable.

Théorème d'incomplétude de Gödel

Soit T une théorie récursivement axiomatisable, consistante qui contient P, alors T est incomplète.

Incomplétude

Théorème

Soit T une théorie de $\mathcal{L}_{Ar}$.
Si T est récursivement axiomatisée et complète alors T est décidable.

Théorème d'incomplétude de Gödel

Soit T une théorie récursivement axiomatisable, consistante qui contient P, alors T est incomplète.

On considère ZF la théorie des ensembles de Zermelo-Fraenkel.

Corollaire

Toute théorie consistante contenant ZF est incomplète.

Merci !