Noé de Rancourt
Bureau T9A, toits du DMA

noe.de.rancourt@ens.fr
http://webusers.imj-prg.fr/~noe.de-rancourt/

TD de Logique 10 : Indécidabilité, incomplétude, arithmétique

8 et 11 décembre 2017

Les exercices marqués du symbole ⧫ sont importants, ce sont ceux que je prévois d'aborder en TD (je ne garantis pas qu'on aura le temps de tous les faire). Ceux d'entre eux qu'on aura eu le temps d'aborder sont à connaître. Les exercices sans symbole sont moins importants, on les abordera en TD si le temps le permet, et sinon je vous conseille de les faire chez vous pour approfondir. Les exercices marqués du symbole ♣ sont facultatifs, en général plus difficiles, et sont destinés à vous faire découvrir des notions en marge du cours ou des applications des notions vues en cours. N'hésitez pas à me demander des précisions à leur propos si ça vous intéresse.

L'exercice 2 est à préparer avant le TD et sera corrigé tout au début de la séance.

Ayez avec vous l'énoncé du TD 9, on finira l'exercice sur l'exponentielle.

I. Indécidabilité, incomplétude

⧫ Exercice 1.

On travaille dans le langage des anneaux $\mathcal{L} = \{0, 1, +, -, \times\}$. Montrer que toute théorie ayant $\mathbb{Z}$ pour modèle est indécidable.

On pourra utiliser le théorème suivant, dû à Lagrange : tout entier naturel peut d'écrire comme une somme de quatre carrés d'entiers naturels.

⧫ Exercice 2.

On travaille dans le langage de l'arithmétique. Soit $T \supseteq \mathcal{Q}_0$ une théorie telle que $\mathbb{N} \models T$. On note $\mathrm{Dem}_T(x, y)$ une formule Σ_1 qui définit dans $\mathbb{N}$ l'ensemble (récursif) des couples (a, b) tels que a code un énoncé et b code une preuve dans T de cet énoncé. Parmi les affirmations suivantes, lesquelles sont vraies pour tous les énoncés φ ?

1. $\mathbb{N} \models \exists x\ \mathrm{Dem}_T(\#\varphi, x) \to \varphi$;
2. $T \vdash \exists x\ \mathrm{Dem}_T(\#\varphi, x) \to \varphi$;
3. $\mathbb{N} \models \varphi \to \exists x\ \mathrm{Dem}_T(\#\varphi, x)$;
4. $T \vdash \varphi \to \exists x\ \mathrm{Dem}_T(\#\varphi, x)$.

♦ **Exercice 3** (Examen 2017)**.**

Le but de cet exercice est de donner une preuve alternative (due à Chaitin) au premier théorème d'incomplétude. Étant donnée une machine de Turing τ et un entier k, on définit la complexité de (τ, k) comme étant le nombre d'états de τ plus $\log_2 k$. La *complexité* (de Kolmogorov) d'un entier n (notée par $C(n)$) est la complexité minimale d'un couple (τ, k) tel que la machine de Turing τ avec l'entrée k (écrit en binaire) termine et renvoie n en sortie. (L'alphabet des machines de Turing est fixé à $\{0, 1, b\}$ et le nombre de bandes est également fixé. On peut interpréter la complexité de Kolmogorov d'un entier n comme le plus petit nombre de bits suffisant pour décrire n.)

Soit T une théorie récursive, cohérente, contenant $\mathcal{Q}_0$.

1. Justifier qu'il existe une formule $\phi(x, y)$ qui est Σ_1 et telle que pour $L, n \in \mathbb{N}$, $\phi(L, n)$ exprime que $C(n) < L$. (On pourra utiliser le codage de machines de Turing fait en cours ; il n'est pas nécessaire d'entrer trop dans les détails.)
2. Montrer que si $T \vdash \neg\phi(n, L)$, alors $\mathbb{N} \models \neg\phi(n, L)$ (*N.B.* : On ne suppose pas que $\mathbb{N} \models T$.)
3. Montrer qu'il existe un entier L tel qu'aucun énoncé de la forme $\neg\phi(n, L)$ ne soit prouvable dans T. (*Indication :* Raisonner par l'absurde et construire une fonction récursive qui prenant L en entrée renvoie un n de complexité L.)
4. Montrer qu'il existe un énoncé qui est vrai dans $\mathbb{N}$ mais qui n'est pas démontrable dans T.

Exercice 4 (Fonctions prouvablement totales)**.**

On travaille dans le langage de l'arithmétique. On fixe T une théorie cohérente, récursive, et contenant $\mathcal{Q}_0$.

Soit $f : \mathbb{N}^p \longrightarrow \mathbb{N}$ une fonction récursive totale ; on rappelle qu'il existe une formule $F(\bar{x}, y)$ Σ_1 qui *représente* f, c'est-à-dire telle que pour tous $\bar{a} \in \mathbb{N}^p$ et $b \in \mathbb{N}$, on ait $f(\bar{a}) = b$ si et seulement si $\mathcal{Q}_0 \vdash F(\underline{\bar{a}}, \underline{b})$. On dira que f est *prouvablement totale dans* T s'il existe une telle formule qui satisfait de plus $T \vdash \forall \bar{x}\, \exists y\, F(\bar{x}, y)$.

1. Montrer qu'il existe une fonction récursive partielle $h : \mathbb{N}^2 \longrightarrow \mathbb{N}$ telle que pour tous $a, n \in \mathbb{N}$, on ait :
   – si $a = \#F(x_0, x_1)$ où $F(x_0, x_1)$ est Σ_1 et qu'il existe $m \in \mathbb{N}$ tel que $T \vdash F(\underline{m}, \underline{n})$, alors $T \vdash F(\underline{m}, \underline{h(a, n)})$;
   – si $a = \#F(x_0, x_1)$ où $F(x_0, x_1)$ est Σ_1 et qu'il n'existe pas de $m \in \mathbb{N}$ tel que $T \vdash F(\underline{m}, \underline{n})$, alors $h(a, n)$ n'est pas défini ;
   – Sinon, $h(a, n) = 0$.
2. On définit une fonction partielle $g \in \mathcal{F}_3^*$ par, pour tout $a, b, n \in \mathbb{N}$:
   – si $a = \#F(x_0, x_1)$ où $F(x_0, x_1)$ est Σ_1 et si b est le code d'une preuve dans T de $\forall x_0\, \exists x_1 F(x_0, x_1)$, alors $g(a, b, n) = h(a, n)$;
   – sinon $g(a, b, n) = 0$.
   Montrer que g est récursive totale.
3. Montrer que la fonction g est universelle pour les fonctions $\mathbb{N} \longrightarrow \mathbb{N}$ récursives totales et prouvablement totales dans T, c'est-à-dire que pour toute telle fonction $u : \mathbb{N} \longrightarrow \mathbb{N}$, il existe $a, b \in \mathbb{N}$ tels que $u = g(a, b, \cdot)$.
4. Montrer qu'il existe une fonction récursive totale qui n'est pas prouvablement totale dans T. En déduire l'existence d'un énoncé satisfait dans $\mathbb{N}$ mais pas prouvable dans T.

II. La hiérarchie arithmétique

Dans tout cette partie TD, on travaillera dans le langage de l'arithmétique $\mathcal{L} = \{0, \mathrm{s}, +, \times, <\}$.

Une $\mathcal{L}$-formule est dite Σ_0, ou encore Π_0, si elle appartient au plus petit ensemble contenant les formules atomiques et clos par :

- conjonction finie, disjonction finie, négation ;
- quantification universelle bornée : si φ est Σ_0, si t est un terme, et x une variable n'apparaissant pas dans t, alors $\forall x \leqslant t\ \varphi$ est Σ_0 (ici, $\forall x \leqslant t\ \varphi$ est une abréviation pour $\forall x\ (x \leqslant t \longrightarrow \varphi)$).
- quantification existentielle bornée, qu'on définit de façon similaire.

Pour $n \in \mathbb{N}$, on dit d'une $\mathcal{L}$-formule qu'elle est :

- Σ_{n+1} si elle est de la forme $\exists x\ \varphi$ pour φ une $\mathcal{L}$-formule Π_n ;
- Π_{n+1} si elle est de la forme $\forall x\ \varphi$ pour φ une $\mathcal{L}$-formule Σ_n ;

Étant donné $p \in \mathbb{N}^*$, et $n \in \mathbb{N}$, on dit qu'un ensemble $A \subseteq \mathbb{N}^p$ est Σ_n (resp. Π_n) s'il est définissable par une $\mathcal{L}$-formule Σ_n (resp. Π_n). On dit qu'il est Δ_n s'il est à la fois Σ_n et Π_n. On notera $\Sigma_n(\mathbb{N})$ (resp. $\Pi_n(\mathbb{N})$, $\Delta_n(\mathbb{N})$) l'ensemble des ensembles qui sont des parties Σ_n (resp. Π_n, Δ_n) d'un $\mathbb{N}^p$ pour un certain $p \in \mathbb{N}^*$.

Pour $A \subseteq \mathbb{N}^{p+1}$ et $i \in \mathbb{N}$, on notera A_i l'ensemble $\{\bar{x} \in \mathbb{N}^p \mid (i, \bar{x}) \in A\}$.

Pour tout $p \in \mathbb{N}$, on notera W^p le domaine de Φ^p (la fonction récursive universelle), et conformément à la notation précédente, pour tout $i \in \mathbb{N}$, W_i^p désignera le domaine de φ_i^p. Les ensembles W^p et W_i^p sont donc des sous-ensembles récursivement énumérables de $\mathbb{N}^{p+1}$ et $\mathbb{N}^p$ respectivement.

Exercice 5.

1. Montrer que le complémentaire d'un ensemble Σ_n est Π_n, et que $\Delta_n(\mathbb{N})$ est clos par passage au complémentaire.
2. Montrer que pour tout $n \in \mathbb{N}$, on a $\Sigma_n(\mathbb{N}) \cup \Pi_n(\mathbb{N}) \subseteq \Delta_{n+1}(\mathbb{N})$.
3. Montrer que $\Sigma_n(\mathbb{N})$, $\Pi_n(\mathbb{N})$ et $\Delta_n(\mathbb{N})$ sont clos par :
   - union et intersection finies ;
   - quantification universelle bornée et quantification existentielle bornée : par exemple, si $A \subseteq \mathbb{N}^{p+1}$ est Σ_n, alors $B = \{(\bar{x}, y) \in \mathbb{N}^{p+1} \mid \forall z \leqslant y\ (\bar{x}, z) \in A\}$ est Σ_n.
4. Montrer que $\Sigma_n(\mathbb{N})$ est clos par quantification existentielle (c'est-à-dire que si $A \subseteq \mathbb{N}^{p+1}$ est Σ_n, alors $B = \{\bar{x} \in \mathcal{M}^p \mid \exists y\ (\bar{x}, y) \in A\}$ l'est aussi), et que Π_n est clos par quantification universelle (se définit de façon analogue).

Exercice 6 (Représentabilité)**.**

1. Montrer qu'une partie de $\mathbb{N}^p$ est Σ_1 si et seulement si elle est récursivement énumerable.
2. En déduire que $\Delta_1(\mathbb{N})$ est exactement l'ensemble des ensembles récursifs.
3. Montrer la réciproque du théorème de représentabilité : toute fonction totale $f : \mathbb{N}^p \longrightarrow \mathbb{N}$ représentée par une formule Σ_1 est récursive. (Indication : on pourra montrer que le graphe de f est Δ_1.)

Exercice 7 (Ensembles universels)**.**

Soit Γ une classe de sous-ensembles des $\mathbb{N}^p$ pour $p \in \mathbb{N}^*$. On dit qu'un ensemble $U \subseteq \mathbb{N}^{p+1}$ est Γ-*universel* s'il est dans Γ et si pour tout $A \subseteq \mathbb{N}^p$ qui est dans Γ, il existe $i \in \mathbb{N}$ tel que $A = U_i$.

1. Donner, pour tout $p \in \mathbb{N}^*$, un exemple de sous-ensemble Σ_1-universel de $\mathbb{N}^{p+1}$.
2. Montrer que pour tout $n \in \mathbb{N}^*$ et pour tout $p \in \mathbb{N}^*$, il existe un sous-ensemble Σ_n-universel et un sous-ensemble Π_n-universel de $\mathbb{N}^{p+1}$.
3. Montrer que pour tout $n \in \mathbb{N}^*$, les inclusions $\Delta_n(\mathbb{N}) \subseteq \Sigma_n(\mathbb{N})$ et $\Delta_n(\mathbb{N}) \subseteq \Pi_n(\mathbb{N})$ sont strictes.

⧫ **Exercice 8** (Réduction *many-one*)**.**

Soient $A \subseteq \mathbb{N}^p$, $B \subseteq \mathbb{N}^q$ deux ensembles. On dit que A *se réduit* à B s'il existe $f : \mathbb{N}^p \to \mathbb{N}^q$ récursive totale telle que $A = f^{-1}(B)$. On notera ceci $A \leqslant_m B$.

1. Soit $n \in \mathbb{N}^*$. Montrer que si $A \leqslant_m B$ et si B est Σ_n (resp. Π_n, Δ_n), alors A l'est également.

Soit Γ une classes de sous-ensembles des $\mathbb{N}^p$ pour $p \in \mathbb{N}^*$, qui est close par image réciproque récursive. On dit qu'un ensemble $A \in \Gamma$ est Γ-*complet* si tout ensemble de Γ s'y réduit.

2. Quels sont les ensembles Δ_1-complets ?
3. Soit $n \in \mathbb{N}^*$. Montrer qu'un ensemble Σ_n-universel (resp. Π_n-universel) est Σ_n-complet (resp. Π_n-complet). En particulier, de tels ensembles existent.
4. Soit $n \in \mathbb{N}^*$. Montrer qu'un ensemble Σ_n-complet n'est pas Δ_n, et de même pour un ensemble Π_n.

⧫ **Exercice 9** (Exemples d'ensembles complets)**.**

1. Montrer que l'ensemble $\{x \in \mathbb{N} \mid \phi^1(x, x) \downarrow\}$ est Σ_1-complet.
2. Soit $p \in \mathbb{N}$. Montrer que l'ensemble des $i \in \mathbb{N}$ tels que la fonction ϕ_i^p soit totale est Π_2-complet. (Indication : on pourra utiliser la propriété smn.)
3. Montrer que l'ensemble des $i \in \mathbb{N}$ tels que W_i^1 est fini est Σ_2-complet.

Exercice 10.

Soit $\mathcal{M} \models \mathcal{PA}$. On peut définir la notion de sous-ensemble Σ_n, Π_n, et Δ_n de $\mathcal{M}^p$, pour $p \in \mathbb{N}^*$ et $n \in \mathbb{N}$, de la même façon que pour $\mathbb{N}$. Montrer que tous les résultats montrés dans l'exercice 8 restent vrais dans ce cadre.

III. Modèles non-standards de l'arithmétique

Exercice 11 (Préservation)**.**

On travaille dans le langage de l'arithmétique (avec symbole d'ordre). Si $\mathcal{M}$ est une structure et $\mathcal{N}$ une sous-structure de $\mathcal{M}$, on dira que $\mathcal{N}$ est un *segment initial* de $\mathcal{M}$ si pour tout $y \in \mathcal{N}$ et tout $x \in \mathcal{M}$, si $\mathcal{M} \models x \leqslant y$, alors $x \in \mathcal{N}$.

1. Montrer que si $\mathcal{M}$ est une structure et $\mathcal{N}$ une sous-structure de $\mathcal{M}$ qui est est un segment initial de $\mathcal{M}$, alors pour toute formule Δ_0 $\varphi(\bar{x})$ et tout uplet $\bar{a} \in \mathcal{N}^p$, on a $\mathcal{N} \models \varphi(\bar{a}) \Leftrightarrow \mathcal{M} \models \varphi(\bar{a})$.
2. Montrer que si $\mathcal{M}$ est une structure et $\mathcal{N}$ une sous-structure de $\mathcal{M}$ qui est est un segment initial de $\mathcal{M}$, alors pour toute formule Σ_1 $\varphi(\bar{x})$ et tout uplet $\bar{a} \in \mathcal{N}^p$, on a $\mathcal{N} \models \varphi(\bar{a}) \Rightarrow \mathcal{M} \models \varphi(\bar{a})$.
3. En déduire que pour tout $\mathcal{L}$-énoncé Σ_1 φ, on a $\mathbb{N} \models \varphi \Leftrightarrow \mathcal{P}_0 \vdash \varphi$.

♣ **Exercice 12.**

On fixe $\mathcal{M}$ un modèle de $\mathcal{PA}$. *L'ensemble des nombres premiers de* $\mathcal{M}$ est l'ensemble $\mathcal{P}^{\mathcal{M}}$ défini par la formule $\mathcal{P}(x)$ suivante : $\forall y, z\ (x = yz \to y = 1 \vee z = 1)$.

1. Montrer qu'il existe une unique bijection strictement croissante et définissable $\mathrm{Pr} : \mathcal{M} \longrightarrow \mathcal{P}$. (On pourra s'inspirer de la construction de l'exponentielle.)
2. Soit $f : \mathcal{M} \longrightarrow \mathcal{M}$ une fonction définissable avec paramètres. Montrer qu'il existe une unique fonction $F : \mathcal{M} \longrightarrow \mathcal{M}$ définissable avec paramètres telle que $F(0) = 0$ et pour tout $a \in \mathcal{M}$, $F(a+1) = f(a)F(a)$. Vérifier que de plus, F est définissable avec les mêmes paramètres que f. Dans la suite, $F(a)$ sera noté $\prod_{x<a} f(x)$.
3. Soit $f : \mathcal{M} \longrightarrow \mathcal{M}$ définissable avec paramètres ; on suppose que $\mathrm{supp}(f) = \{x \in \mathcal{M} \mid f(x) \neq 1\}$ est majoré dans $\mathcal{M}$. Montrer que la valeur de $\prod_{x<a} f(x)$ ne dépend pas de $a \in \mathcal{M}$ tant que a est un majorant strict de $\mathrm{supp}(f)$. Cette valeur sera notée $\prod_{x \in \mathcal{M}} f(x)$.
4. Soient $p \in \mathcal{P}^{\mathcal{M}}$ et $a \in \mathcal{M}$. Montrer que l'ensemble des $x \in \mathcal{M}$ tels que $p^x \mid a$ possède un plus grand élément. On le notera $v_p(a)$. L'application $\begin{array}{ccc} \mathcal{P}^{\mathcal{M}} \times \mathcal{M} & \longrightarrow & \mathcal{M} \\ (p, a) & \longmapsto & v_p(a) \end{array}$ est alors définissable.
5. Soit $a \in \mathcal{M}$. Montrer que l'ensemble des $x \in \mathcal{M}$ tels que $v_{\mathrm{Pr}(x)}(a) > 0$ est majoré. Montrer que $a = \prod_{x \in \mathcal{M}} \mathrm{Pr}(x)^{v_{\mathrm{Pr}(x)}(a)}$. C'est l'existence de la décomposition en facteurs premiers.
6. Soit $f : \mathcal{M} \longrightarrow \mathcal{M}$ une fonction définissable avec paramètres telle que $\{x \in \mathcal{M} \mid f(x) > 0\}$ est majoré dans $\mathcal{M}$, et $a = \prod_{x \in \mathcal{M}} \mathrm{Pr}(x)^{f(x)}$. Montrer que pour tout $x \in \mathcal{M}$, $v_{\mathrm{Pr}(x)}(a) = f(x)$. C'est l'unicité de la décomposition en facteurs premiers.

♣ **Exercice 13** (Théorème de Tennenbaum)**.**

Le but de cet exercice est de montrer que $\mathcal{PA}$ n'a pas de modèle non-standard récursif, autrement dit que si un modèle dénombrable et non-standard de $\mathcal{PA}$ a $\mathbb{N}$ pour ensemble de base, alors l'addition de ce modèle n'est pas récursive.

On commence par fixer un modèle non-standard quelconque $\mathcal{M} = (M, \dot{0}, \mathfrak{s}, \oplus, \otimes, <)$ de $\mathcal{PA}$; pour éviter les confusions dans la suite, le modèle standard sera noté $\mathcal{N} = (\mathbb{N}, 0, \mathrm{s}, +, \times, <)$, et on notera $i : \mathcal{N} \longrightarrow \mathcal{M}$ l'unique plongement.

1. On se donne, pour cette question et la suivante, $A, B \subseteq \mathbb{N}$ récursivement énumérables et disjoints. Montrer qu'il existe deux formules Δ_0, $\varphi(x, \bar{y})$ et $\psi(x, \bar{y})$, sans paramètre et à $p+1$ variables libres (pour un certain $p \in \mathbb{N}^*$), telles que pour tout $n \in \mathbb{N}$, on ait $n \in A$ si et seulement s'il existe $\bar{a} \in \mathbb{N}^p$ tel que $\mathcal{M} \models \varphi(i(\bar{a}), i(n))$, et $n \in B$ si et seulement s'il existe $a \in \mathbb{N}^p$ tel que $\mathcal{M} \models \psi(i(\bar{b}), i(n))$.
2. En déduire qu'il existe $C \subseteq M$ définissable dans $\mathcal{M}$ avec paramètres, tel que $A \subseteq i^{-1}(C)$ et $B \cap i^{-1}(C) = \varnothing$.

On supposera maintenant que $M = \mathbb{N}$ et que $\oplus : \mathbb{N}^2 \longrightarrow \mathbb{N}$ est récursive dans le but d'aboutir à une contradiction.

3. Montrer que i est récursive. Montrer que l'application :

$$\begin{array}{ccc} \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (n, x) & \longmapsto & i(n) \otimes x \end{array}$$

   est récursive.

4. Montrer que l'ensemble $D = \{(n, x) \in \mathbb{N}^2 \mid \mathcal{M} \models i(n) \mid x\}$ est récursif.

5. On note $(p_n)_{n \in \mathbb{N}}$ l'énumeration strictement croissante des nombres premiers de $\mathcal{N}$. Soit $A \subseteq M$ définissable dans $\mathcal{M}$ avec paramètres. Montrer qu'il existe $a \in M$ tel que pour tout $n \in \mathbb{N}$, $\mathcal{M} \models i(p_n) \mid a$ si et seulement si $i(n) \in A$.

6. En déduire que si $A \subseteq M$ est définissable dans $\mathcal{M}$ avec paramètres, alors $i^{-1}(A)$ est récursif.

7. En utilisant les deux premières questions, aboutir à une contradiction.