Les théorèmes de Gödel

ou les limites du savoir rationnel

Alexandre SAINT-DIZIER

7 février 2019

> *« Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk »*
>
> — Leopold Kronecker, XIX^{ieme} *siècle*

L'objectif de ce projet est de se plonger dans la théorie de la logique fondamentale et de mieux comprendre d'où viennent nos façons de raisonner, quels en sont les mécanismes sous-jacents et comment sont-elles justifiées. Cela va nous amener à définir ce qu'est une preuve, ce qu'est une définition et un problème et nous allons voir ce que ces considérations impliquent, en particulier les deux théorèmes de Gödel, à la limite de la meta-physique.

Théorème 1 (Premier théorème de Gödel)
On peut tout démontrer.

Théorème 2 (Deuxième théorème de Gödel)
On ne peut pas tout démontrer.

Malgré les apparences, ces deux théorèmes ne sont pas incompatibles et dépendent du sens que l'on donne aux mots "tout" et "démontrer". Néanmoins, leur portée philosophique est réelle, et ils représentent deux piliers fondamentale de la logique. Et ils vont entre autre appuyer de manière profonde la citation de Leopold Kronecker, logicien et mathématicien allemand, qui pourrait se traduire par « Dieu a créé les nombres entiers, et l'homme a fait le reste ».

L'objectif de ce projet est de comprendre et d'assimiler les concepts de base de la logique afin d'arriver à redémontrer les deux théorèmes de Gödel et de les pouvoir les expliquer à d'autre personnes ayant un bagage mathématique mais n'ayant de connaissances particulières en logique. Plus que la réponse aux questions, les raisonnements sont importants, car c'est eux qui vont permettre de comprendre les notions impliquées ainsi que *l'essence* des résultats. Beaucoup de fois, vous allez avoir l'impression de démontrer des choses évidentes, mais parfois l'évidence n'est pas toujours aussi évidente que l'on ne le pense. Ainsi, pour éviter de louper des subtilités, il vous faudra écrire rigoureusement toutes les preuves en se basant autant que possible sur les définitions du projets au lieu de l'intuition habituelle, qui a le défaut de ne pas être précise.

1 Préliminaires

1.1 Théorie des ensembles

On utilisera dans ce projet les notation usuelles de la théorie des ensembles et de la logique. Si E est un ensemble et e un élément, on note $e \in E$ pour signifier que e appartient à E. Pour A et B deux ensembles, on note $A \subset B$, $A \cup B$, $A \cap B$, $A \backslash B$ et $A \times B$ pour l'inclusion, l'union, l'intersection, la soustraction et le produit cartésien des ensembles A et B. Si $A \subset E$, A^c désigne les complémentaire de A dans E.

1. Soient A et B parties de E. Montrer les lois de Morgan : $(A \cup B)^c = A^c \cap B^c$ et $(A \cap B)^c = A^c \cup B^c$.

> **Solution:** On procède par double inclusion. Soit $x \in (A \cup B)^c$. Alors $x \notin A \cup B$ et donc $x \notin A$ et $x \notin B$, donc $x \in A^c \cap B^c$. Reciproquement, si $x \in A^c \cap B^c$, alors $x \notin A$ et $x \notin B$ et donc $x \notin A \cup B$ et donc $x \in (A \cup B)^c$. On obtient la deuxième égalité à partir de la première en l'appliquant à A^c et B^c et en utilisant $(A^c)^c = A$.

2. Soit $A \subset E$ et $(B_i)_{i \in I}$ une famille de partie de E. Montrer que

$$A \cup \left(\bigcap_{i \in I} B_i \right) = \bigcap_{i \in I} (A \cup B_i) \text{ et } A \cap \left(\bigcup_{i \in I} B_i \right) = \bigcup_{i \in I} (A \cap B_i) .$$

> **Solution:**
> Soit $x \in A \cup \left(\bigcap_{i \in I} B_i \right)$. Si $x \in A$, alors $\forall i \in I, x \in A \cup B_i$ et donc $x \in \bigcap_{i \in I} (A \cup B_i)$. Si $x \in \bigcap_{i \in I} B_i$ alors $\forall i \in I, x \in B_i$ et donc $\forall i \in I, x \in A \cup B_i$, donc $x \in \bigcap_{i \in I} (A \cup B_i)$. La réciproque est basé sur le même principe.
> Soit $x \in A \cap \left(\bigcup_{i \in I} B_i \right)$. Alors $x \in A$ et $x \in \left(\bigcup_{i \in I} B_i \right)$, et donc $\exists i \in I; x \in B_i$. Donc $\exists i \in I; x \in A \cap B_i$ et donc $x \in \bigcup_{i \in I} (A \cap B_i)$. De même pour la réciproque.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ et $\mathbb{R}$ designeront les ensembles des nombres entiers, relatifs, rationnels et réels. Pour $n \in \mathbb{N}$, on notera $[\![1, n]\!]$ l'ensemble des entiers compris entre 1 et n.

On ensemble E est dit *fini* si il existe un entier $n \in \mathbb{N}$ et une bijection de E dans $[\![1, n]\!]$. L'entier n est unique et est appelé *cardinal* de E, noté $|E|$. Un ensemble est dit *infini* si il n'est pas fini. Un ensemble est dit *dénombrable* si il existe une bijection de E dans $\mathbb{N}$, et est dit *au plus dénombrable* si il est fini ou dénombrable. Un ensemble qui n'est pas au plus dénombrable est dit *indénombrable*.

3. Soit E un ensemble. Montrer que E est au plus dénombrable si et seulement si il existe une surjection de $\mathbb{N}$ dans E.

> **Solution:** Le cas $E = \emptyset$ est trivial. On suppose $E \neq \emptyset$.
> On suppose E au plus dénombrable. Si E est dénombrable, on a une bijection donc une surjection de $\mathbb{N}$ dans E. Si E est fini, alors il existe $n \in \mathbb{N}$ et $\phi : E \to [\![1, n]\!]$ bijective. La fonction ψ :
> $$\begin{cases} \mathbb{N} & \to E \\ k & \to \begin{cases} \phi(k) \text{ si } k \leq n & \text{convient.} \\ \phi(0) \text{ sinon} \end{cases} \end{cases}$$
> Réciproquement, supposons que l'on a une surjection ϕ de $\mathbb{N}$ dans E et que E est infini. Alors on pose $A = \{n \in \mathbb{N} | \forall k < n, \phi(k) \neq \phi(n)\}$. A est clairement dénombrable car E est infini, et par construction on a $\phi_{|A}$ est injective. Donc pour τ une bijection entre $\mathbb{N}$ et A, la fonction $\phi \circ \tau$ convient.

4. Soit A et B deux ensembles, avec $A \subset B$ et B au plus dénombrable. Montrer que A est au plus dénombrable.

Solution: Si $A = \emptyset$, le résultat est évident. Sinon soit $a \in A$. B est au plus dénombrable, donc il existe $\phi : \mathbb{N} \to B$ surjective. De même que précédemment, on pose $X = \phi^{-1}(A)$. Alors $\psi : \begin{cases} \mathbb{N} & \to A \\ n & \to \begin{cases} \phi(n) & \text{si } n \in X \text{ convient.} \\ a & \text{sinon} \end{cases} \end{cases}$

5. Soit $(A_i)_{i\in I}$ une famille au plus dénombrable d'ensemble finis. Montrer que $\bigcup_{i\in I} A_i$ est au plus dénombrable.

Solution: Pour $i \in I$, on pose $n_i = card(A_i)$ et $\phi_i : [\![1, n_i]\!] \to A_i$ une bijection. On pose $\phi_I : \mathbb{N} \to I$ une surjection. Alors pour $n \in \mathbb{N}$, on pose $k(n) = \min\{k \in \mathbb{N} | \sum_{l=0}^{k} n_{\phi_I(l)} > n\}$. On pose $\psi : \begin{cases} \mathbb{N} & \to \bigcup_{i\in I} A_i \\ n & \to \phi_{\phi_I(k(n))}(n - \sum_{l=0}^{k(n)-1} n_{\phi_I(l)}) \end{cases}$. Alors ψ est bien définie et est surjective par définition. Donc $\bigcup_{i\in I} A_i$ est au plus dénombrable.

6. Montrer que $\mathbb{N}^2$ est dénombrable. En déduire que $\mathbb{Q}$ est dénombrable.

Solution: On montre que $\mathbb{N}^2$ est dénombrable. En effet, $\mathbb{N}^2 = \bigcup_{k\in\mathbb{N}} A_k$ avec pour $k \in \mathbb{N}, A_k = \{(i, j) \in \mathbb{N}^2 | \max(i, j) \leq k\}$, l'ensemble fini des points de $\mathbb{N}^2$ dont les coordonnées sont inférieur à k. D'après l'exercice 5, $\mathbb{N}^2$ est dénombrable car infini et donc $\mathbb{Q}$ est dénombrable car $\mathbb{Q} \subset \mathbb{N}^2$ et $\mathbb{Q}$ est infini.
Remarque : On peut facilement construire une bijection explicite entre $\mathbb{N}$ et $\mathbb{N}^2$.

7. Soit $n \in \mathbb{N}$ et $(A_i)_{i\in[\![1,n]\!]}$ une famille finie d'ensemble au plus dénombrable. Montrer $A_1 \times \cdots \times A_n$ est au plus dénombrable.

Solution: Soient A et B deux ensembles au plus dénombrables et ϕ_A, ϕ_B les surjections associées. On pose $\psi : \begin{cases} \mathbb{N}^2 & \to A \times B \\ (i, j) & \to (\phi_A(i), \phi_B(j)) \end{cases}$. ψ est bien définie et clairement surjective par construction. Donc $A \times B$ est au plus dénombrable par dénombrabilité de $\mathbb{N}^2$. Le résultat est une conséquence immédiate par récurrence de ce lemme.

8. Soit $(A_i)_{i\in I}$ une famille au plus dénombrable d'ensemble au plus dénombrable. Montrer que $\bigcup_{i\in I} A_i$ est au plus dénombrable.

Solution: On a donc $\phi_I : \mathbb{N} \to I$ et $\forall i \in I, \phi_i : \mathbb{N} \to A_i$ des surjections. On a en outre, pour tout $i \in I, A_i = \bigcup_{n\in\mathbb{N}} \phi([\![0, n]\!])$. D'où $\bigcup_{i\in I} A_i = \bigcup_{(n,i)\in\mathbb{N}\times I} \phi([\![0, n]\!])$, qui est une union au plus dénombrable d'ensemble finis. Donc $\bigcup_{i\in I} A_i$ est au plus dénombrable.

9. Montrer que $\mathbb{R}$ est indénombrable.

Solution: On suppose $\mathbb{R}$ dénombrable. Alors $[0, 1[\subset \mathbb{R}$ est dénombrable. On a donc une suite $(u_n)_{n\in\mathbb{N}}$ des éléments de $[0, 1[$. Pour $n \in \mathbb{N}$, on écrit u_n en écrire binaire, soit $u_n = 0, u_n^{(0)} \dots u_n^{(k)} \dots$.

On construit $x \in [0,1[$ défini par $\forall k \in \mathbb{N}, x^{(k)} = u_k^{(k)}$. Alors x est bien défini par unicité de l'ecrire binaire et on a $\forall n \in \mathbb{N}, u_n \neq x$. Donc $x \notin \{u_n | n \in \mathbb{N}\} = [0,1[$, ce qui est absurde.

1.2 Linguistiques et induction

On appelera *alphabet* un ensemble fini Σ. Les éléments de Σ sont appelés des *lettres* ou *symboles*. Un *mot* w sur l'alphabet Σ est une suite finie $w_1 w_2 \cdots w_n$ de lettres de Σ. L'entier $n \in \mathbb{N}$ est appelé la longueur de w et est noté $|w|$. On notera le *mot vide* par ϵ, le seul mot de longueur 0. Un *langage* sur Σ est un ensemble de mots sur Σ. L'ensemble de tout les mots sur Σ est noté Σ^*, qui contient par définition le mot vide.
Pour $u = u_1 u_2 \cdots u_n \in \Sigma^*$ et $v = v_1 v_2 \cdots v_m \in \Sigma^*$deux mots, on définit l'opération de concaténation par $u.v = u_1 u_2 \cdots u_n v_1 v_2 \cdots v_m$, que l'on notera aussi uv. Ainsi, uu pourra s'écrire u^2.

10. Ecrire la définition par récurrence de Σ^*.

Solution: Σ^* est défini par :
— $\epsilon \in \Sigma^*$
— $\forall u \in \Sigma^*$ et $\forall v \in \Sigma$, $uv \in \Sigma^*$.

1.3 Induction

Soit E un ensemble. Une *définition inductive* d'une partie X de E consiste à se donner :
— Un sous-ensemble non vide B de E (appelé ensemble de base).
— Un ensemble de règles $R = (r_i)_{i \in I}$ où pour tout $i \in I$, r_i est une fonction de $E^{n_i} \to E$ pour un certain n_i.
La définition inductive est une manière rigoureuse de définir un ensemble, et qui généralise la notion de récurrence. Elle est justifiée par le théorème suivant :

Théorème 3 (Théorème du point fixe)
Soit E un ensemble et (B, R) une définition inductive sur E. Il existe un ensemble X vérifiant :
— $B \subset X$
— *X est stable par R, i.e.* $\forall i \in I$, $\forall x_1, x_2, \ldots, x_{n_i} \in X^{n_i}$, $r_i(x_1, \ldots, x_{n_i}) \in X$.
— *X est le plus petit élément vérifiant (1) et (2), i.e.* $\forall Y \subset E$ *vérifiant (1) et (2),* $X \subset Y$.

11. Ecrire la définition inductive de Σ^* (on suppose donné E tel que $\Sigma^* \subset E$).

Solution: Σ^* est défini par la définition inductive suivante : $B = \{\epsilon\}$ et $R = (r_0)$, où $r_0 : \begin{cases} E \times E & \to E \\ (e, e') & \to ee' \end{cases}$.

12. Ecrire la définition inductive de l'ensemble de nombres non divisible par 4 en utilisant $\{1\}$ comme ensemble de base.

Solution: On prend $E = \mathbb{N}$. On prend $B = \{1\}$ et $R = (r_0, r_1, r_2)$, où $r_0 : \begin{cases} \mathbb{N} & \to \mathbb{N} \\ n & \to n+4 \end{cases}$, $r_1 : \begin{cases} \mathbb{N} & \to \mathbb{N} \\ n & \to 2 \end{cases}$ et $r_2 : \begin{cases} \mathbb{N} & \to \mathbb{N} \\ n & \to 3 \end{cases}$

13. Démontrer le théorème du point fixe.

Solution: Soit $\mathcal{F}$ l'ensemble des parties de E vérifiant les règles de la définition inductive. On a $E \in \mathcal{F}$, donc $\mathcal{F} \neq \emptyset$. On pose $X = \bigcap_{Y \in \mathcal{F}} Y$. X vérifie par construction les règles de l'induction et $\forall Y \in \mathcal{F}, X \subset Y$.

14. Déduire du théorème le principe du raisonnement par induction, généralisant le raisonnement par récurrence, et démontrer sa validité.

Solution: Le raisonnement par induction fonctionne comme suit : Soit $X \subset E$ un ensemble défini par l'induction (B, R), et $\mathcal{P}$ un prédicat défini sur E. Si $\mathcal{P}$ vérifie :
— $\forall b \in B, \mathcal{P}(x)$ est vraie.
— $\forall r_i \in R, x_1, \ldots, x_{n_i} \in E, \mathcal{P}(x_1), \ldots, \mathcal{P}(x_{n_i})$ sont vraies $\implies \mathcal{P}(x)$ est vraie.
Alors $\mathcal{P}(x)$ est vraie pour tout $x \in X$.
Preuve : On pose X' l'ensemble des x tels que $\mathcal{P}(x)$ est vraie. Alors X' vérifie l'induction (B, R), et donc d'après le théorème du point fixe, on a $X \subset X'$.

1.4 Calcul propositionnel

On fixe pour cette section un ensemble fini $\mathcal{P} = \{p_1, \ldots, p_n\}$ de symboles que l'on appelle *variables propositionnelles*. L'ensemble des *formules porpositionnelles* $\mathcal{F}$ est le langage sur l'alphabet $\mathcal{P} \cup \{\neg, \wedge, \vee, \implies, \iff, (,)\}$ par la définition inductive suivante :
— $\mathcal{F}$ contient $\mathcal{P}$
— Si $F \in \mathcal{F}$, alors $\neg F \in \mathcal{F}$
— Si $F, G \in \mathcal{F}$, alors $(F \wedge G) \in \mathcal{F}$, $(F \vee G) \in \mathcal{F}$, $(F \implies G) \in \mathcal{F}$, $(F \iff G) \in \mathcal{F}$.
Une *formule propositionnelle* est donc un mot de ce langage. On appelle *littéral* une formule de la forme p ou $\neg p$ avec $p \in \mathcal{P}$.
On définit une *valuation* comme une distribution de valeur de vérité des éléments de $\mathcal{P}$, i.e. une fonction de $\mathcal{P}$ dans $\{0, 1\}$, où 0 représente FAUX et 1 représente VRAI. Etend donné une valuation v, on peut déduire naturellement la *valeur de vérité* $v(F)$ d'une formule propositionnelle F suivant v en respectant les règles usuelles de la logique. On note $\mathcal{V}$ l'ensemble des valuations.

15. Calculer $|\mathcal{V}|$.

Solution: Pour une valuation donnée, chaque variable propositionnelle peut prendre indépendemment la valeur 0 ou 1. Donc $|\mathcal{V}| = 2^n$.

16. Rappeller les tables de vérité des différents symboles logiques.

Solution:

F	G	$F \vee G$	$F \wedge G$	$F \implies G$	$F \iff G$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

17. Exprimer tout ces symboles en fonction uniquement de $\neg$ et $\wedge$.

Solution: On a $F \vee G = \neg((\neg F) \wedge (\neg G))$, $F \implies G = F \vee (\neg G) = \neg((\neg F) \wedge G)$ et $F \iff G = (F \implies G) \wedge (G \implies F) = (\neg((\neg F) \wedge G)) \wedge (\neg((\neg G) \wedge F))$.

Chaque formule propositionnelle prend les valeurs VRAI et FAUX selon les valuations considérées. Si une formule propositionnelle prend la valeur 1 suivant la valuation v, on dit que v *satisfait* F, et l'on note $v \models F$. Une formule propositionnelle est dite *satisfiable* si elle est satisfaite par au moins une valuation. On appelle *tautologie* une formule propositionnelle satisfaite pour toute valuation, et l'on note $\models F$. Deux formules F et G sont dites *équivalentes* si pour toute valuation v, on a $v(F) = v(G)$.

18. Donner 3 exemples de tautologies, et de formules propositionnelles satisfiable mais non tautologiques.

Solution: Laissé au lecteur.

19. Montrer que toute formule propositionnelle peut s'ecrire uniquement avec les connecteurs $\neg$ et $\wedge$. On dit que $(\neg, \wedge)$ est un système complet de connecteur.

Solution: Il suffit de remplacer la définition inductive par les formules données à la question 17.

20. Donner un connecteur logique binaire constistuant à lui seul un système complet de connecteurs.

Solution: On pose l'opération $\otimes$ défini par :

F	G	$\otimes$
0	0	1
0	1	0
1	0	0
1	1	0

On a alors $\neg F = F \otimes F$ et $F \wedge G = (\neg F) \wedge (\neg G) = (F \otimes F) \wedge (G \otimes G)$. Comme $(\neg, \wedge)$ est un système complet de connecteur, $(\otimes)$ l'est aussi.

21. Démontrer le théorème de complétude fonctionnelle, i.e. que toute fonction de $\mathcal{V}$ dans $\{0,1\}$ est valeur de vérité d'une formule propositionnelle.

Solution: On montre cela par récurrence sur le nombre de variables propositionnelles n. Pour $n = 1$, il y a que 4 fonctions de $\{0,1\}$ dans $\{0,1\}$, qui sont représentées par $p, \neg p, p \wedge (\neg p)$ et $p \vee (\neg p)$. Supposons le résultat pour un entier $n \in \mathbb{N}$. Soit f une fonction de $\{0,1\}^n$ dans $\{0,1\}$. On note f_0 (et f_1) la restriction de f à la valuation telle que $p_{n+1} = 0$ (et $p_{n+1} = 1$). Par l'hypothèse de récurrence, on a une formule $F_0(p_1, \ldots, p_n)$ (et $F_1(p_1, \ldots, p_n)$) telle que f_0 (et f_1) est valeur de vérité de F_0 (et F_1). Alors f peut se faire représenter par $(\neg p_{n+1} \wedge F_0(p_1, \ldots, p_n)) \vee (p_{n+1} \wedge F_0(p_1, \ldots, p_n))$, ce qui conclut la récurrence.

Une *forme normale conjonctive* est une *conjonction* $F_1 \wedge \ldots \wedge F_n$, où chaque F_i est une *disjonction* $G_1 \vee \ldots \vee G_{l_i}$ *de* l_i *littéraux.*

22. Montrer que tout formule propositionnelle peut s'écrire sous forme normale conjonctive.

Solution: On montre par récurrence sur le nombre de variable propositionnelle n. Pour $n = 1$, le résultat est évident. Supposons le résultat pour un entier $n \in \mathbb{N}$. Soit F une formule sur $n+1$ variables propositionnelles et f la fonction de vérité associée à F. D'après la preuve du théorème de complétude, f est représentée par $(\neg p_{n+1} \wedge F_0(p_1, \ldots, p_n)) \vee (p_{n+1} \wedge F_0(p_1, \ldots, p_n))$, avec F_0 et F_1 deux formules sur n variables propositionnelles. Par hypothèse de récurrence, on peut mettre F_0 et F_1 sous forme normale conjonctive et donc F aussi en utilisant les relations entre $\wedge$ et $\vee$.

23. Mettre la formule $F = \neg\,(p \implies (q \implies r)) \vee (r \implies q)$ sous forme normale conjonctive.

> **Solution:** On regarde les valuations pour lesquelles F n'est pas vérifée, et ecrit $\neg F$ comme disjonction de ces valuations. Ici, $\neg F$ est vraie pour $(p = 0, q = 0, r = 1)$ et $(p = 1, q = 0, r = 1)$. D'où $\neg F = (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge r)$, et donc $F = (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee \neg r)$, ce qui se simplifie en $F = q \vee \neg r$.

On se donne pour la suite un ensemble Σ de formules. On dit qu'une valuation v *satisfait* Σ si v satisfait chaque formule de Σ. On dit alors que v est un *modèle* de Σ. Σ est dit *consistant* ou *satisfiable* s'il possède un modèle, et *inconsistant* sinon. Pour F une formule, on dit que F est une *conséquence* de Σ si tout modèle de Σ est un modèle de F. On note alors $\Sigma \models F$.

Théorème de compacité : Soit Σ un ensemble de formules construites sur un ensemble dénombrable $\mathcal{P}$ de variables propositionnelles. Alors Σ est consistant si et seulement si toute partie finie de Σ est consistante.

24. On fixe Σ et $\mathcal{P} = \{p_1, \ldots, p_n, \ldots\}$. Soit $n \in \mathbb{N}$. Supposons qu'il existe une valuation v sur $\{p_1, \ldots, p_n\}$ telle que tout sous-ensemble fini de Σ ait un modèle dans lequel $p_1, \ldots, p_n$ prennent les valeurs $v(p_1), \ldots, v(p_n)$. Alors on peut étendre v à $\{p_1, \ldots, p_{n+1}\}$ avec la même propriété.

> **Solution:** Supposons que $v(p_{n+1}) = 0$ ne convienne pas. Alors il existe un sous-ensemble fini U_0 de Σ qui ne peut être satisfait quand $p_1, \ldots, p_n$ prennent les valeurs $v(p_1), \ldots, v(p_n), 0$. Soit U un sous-ensemble fini de Σ. Alors, par l'hypothèse, $U_0 \cup U$ a un modèle v pour lequel $p_1, \ldots, p_n$ prennent les valeurs $v(p_1), \ldots, v(p_n)$. Alors $v(p_{n+1})$ ne peut pas prendre la valeur 0, donc on a $v(p_{n+1}) = 1$. Autrement dit, tout sous-ensemble fini de Σ possède un modèle prenant les valeurs $v(p_1), \ldots, v(p_n), 1$, ce qui est ce qu'il fallait démontrer.

25. Prouver le théorème de compacité.

> **Solution:** Le sens direct est évident. On suppose que toute partie finie de Σ est consistante. Alors on construit par récurrence la valuation v définit par le lemme de la question 24. Par construction v satisfait tout sous-ensemble fini de Σ, donc tout élément de Σ.
>
> **Remarque :**
> — L'on pourrait ne pas se limiter au cas dénombrable si l'on accepte d'utiliser l'axiome du choix.
> — Le théorème de compacité peut se voir comme un conséquence topologique du théorème de Tychonoff

2 Démonstration

Une *démonstration* est une suite de déductions faites à partir d'axiomes et d'hypothèses et menant à un résultat. Il existe différent type de démonstrations mais elle fonctionnent toutes sur le même principe. Elles partent d'une base, les *axiomes*, et d'une ou plusieurs règles de déduction, un peu comme pour les définitions inductives.

On note $\mathcal{A}$ l'ensemble des axiomes de la la logique boolénne, comme l'ensemble des formules propositionnelles de l'une des formes suivante :

1. $X_1 \implies (X_2 \implies X_1)$
2. $(X_1 \implies (X_2 \implies X_3)) \implies ((X_1 \implies X_2) \implies (X_1 \implies X_3))$
3. $X_1 \implies \neg\neg X_1$
4. $\neg\neg X_1 \implies X_1$
5. $(X_1 \implies X_2) \implies (\neg X_1 \implies \neg X_2)$
6. $X_1 \implies (X_2 \implies (X_1 \wedge X_2))$
7. $(X_1 \wedge X_2) \implies X_1$
8. $(X_1 \wedge X_2) \implies X_2$
9. $X_1 \implies (X_1 \vee X_2)$
10. $X_2 \implies (X_1 \vee X_2)$
11. $(((X_1 \vee X_2) \wedge (X_1 \implies C)) \wedge (X_2 \implies C)) \implies C$

26. Vérifier que tout les éléments de $\mathcal{A}$ sont des tautologies

> **Solution:** Il suffit de faire les tables de vérités.

2.1 Démonstration par modus ponem

La démonstration par modus ponem n'utiliser qu'une seule règle de déduction : la régle du modus ponem qui nous dit que si l'on a montré F et $F \implies G$, alors on a montré G.

On définit ainsi la démonstration par modus ponem de la façon suivante :

Soit T un ensemble de formules propositionnelles, et F une formule propositionnelle. Une *preuve par modus ponem* de F à partir de T est une suite finie $F_1, \dots, F_n$de formules propositionnelles telle que :

— $F_n = F$

— $\forall i \in [\![1, n]\!]$, $F_i \in T \cup \mathcal{A}$ ou F_i s'obtient par modus ponem à partir de F_j, F_k avec $j, k \in [\![1, i-1]\!]$.

On note $T \vdash F$ si F est prouvable à partir de T. Si l'on a $\emptyset \vdash F$, on note $\vdash F$ et on dit que F est *prouvable*.

27. Démontrer $F \implies H$ à partir de $\{F \implies G, G \implies H\}$. par modus ponem.

> **Solution:**
> — $F_1 : G \implies H$, hypothèse.
> — $F_2 : (G \implies H) \implies (F \implies (G \implies H))$, axiome.
> — $F_3 : F \implies (G \implies H)$, modus ponem à partir de F_1 et F_2.
> — $F_4 : (F \implies (G \implies H)) \implies ((F \implies G) \implies (F \implies H))$, axiome.
> — $F_5 : (F \implies G) \implies (F \implies H)$, modus ponem à partir de F_3 et F_4.
> — $F_6 : F \implies G$, hypothèse.
> — $F_7 : F \implies H$, modus ponem à partir de F_5 et F_6.

28. Démontrer $F \implies F$.

Solution: On sait que l'on a montré dans la question 27 $((F \implies G) \wedge (G \implies H)) \implies (F \implies H)$.

- $F_1 : F \implies \neg\neg F$, axiome.
- $F_2 : (\neg\neg F) \implies F$, axiome.
- $F_3 : (F \implies \neg\neg F) \implies (((\neg\neg F) \implies F) \implies ((F \implies \neg\neg F) \wedge (\neg\neg F) \implies F)))$
- $F_4 : ((\neg\neg F) \implies F) \implies ((F \implies \neg\neg F) \wedge (\neg\neg F) \implies F))$, modus ponem à partir de F_1 et F_3.
- $F_5 : (F \implies \neg\neg F) \wedge (\neg\neg F) \implies F)$, modus ponem à partir de F_2 et F_4.
- $F_6 : ((F \implies \neg\neg F) \wedge (\neg\neg F) \implies F)) \implies (F \implies F)$, d'après question 27.
- $F_7 : F \implies F$, par modus ponem à partir de F_5 et F_6.

29. **Validité :** Démontrer que toute formule propositionnelle prouvable par modus ponem est une tautologie.

Solution: On considère une preuve $F_1, \ldots, F_n$ d'une formule F. On montre par récurrence que $\forall i \in [\![1, n]\!]$, F_i est une tautologie. C'est vrai pour $i = 1$ car F_1 est forcement un axiome. On suppose le résultat vrai pour tout $j \leq i$, avec $i \in [\![1, n-1]\!]$. Le résultat est vrai si F_{i+1} est un axiome. On suppose que F_{i+1} s'obtient comme modus ponem à partir de F_j et F_k, avec $j \leq i$ et $k \leq i$. On a donc $F_k = F_j \implies F_{i+1}$. Alors par hypothèse de récurrence, F_j et F_k sont des tautologies et donc par définition de $\implies$, $\neg F_{i+1}$ ne peut satisfaite auquel cas $\neg F_k = \neg(F_j \implies F_{i+1})$ le serait aussi car F_j est une tautologie. Donc F_{i+1} est une tautologie et donc $\forall i \in [\![1, n]\!]$, F_i est une tautologie. En particulier $F_n = F$ est une tautologie, ce qui conclut la preuve de la validité.

30. **Complétude :** On veut démontrer ici la complétude de la preuve par modus ponem, i.e. que toute tautologie est prouvable par modus ponem.
    (a) Soient T une famille de formules et F et G des formules. Montrer que si l'on a à la fois $T \cup \{F\} \vdash G$ et $T \cup \{\neg F\} \vdash G$, alors $T \vdash G$.

Solution: On suppose que F n'est pas de la forme$F_1 \implies F_2$, car sinon on peut se ramener à ce cas en remplacant F par F_2.

Soit $\mathcal{P}_{\mathcal{F}} = (F_1, F_2, \ldots, F_n)$ et $\mathcal{P}_{\neg\mathcal{F}} = (F_1, F_2, \ldots, F_n)$ les formules consituant la preuve de $T \cup \{F\} \vdash G$ et $T \cup \{\neg F\} \vdash G$. On considère l'ensemble $I_F = \{F_i | F_i$ s'obtient par modus ponem à partir de F ou F_j avec $j \in I_F\}$. Alors I_F est bien défini et $I_F \subset \{F_1, \ldots, F_n\}$. Si $I_F = \emptyset$, alors on a directement $T \vdash G$. De même, si $F_n = G \notin I_F$, alors $\{F_1, \ldots, F_n\} \backslash I_F$ est une preuve de $T \vdash G$. On peut donc supposer que $F_n = G \in I_F$, et de même que $G \in I_{\neg F}$. Supposons en outre que $I_F \neq \{G\}$. Soit $F_i \in I_F$ l'élément de I_F d'indice le plus faible. Alors il existe H une formule de la preuve et $j, k \in [\![1, n]\!]$ tels que $F_j = F \implies F_i$ et $F_k = F_i \implies H$ et donc $F_k \in I_F$. Alors par l'exercice 27, on peut montrer $F \implies H$ et donc on peut construire une preuve de $T \cup \{F\} \vdash G$ tel que l'ensemble I'_F associé soit de cardinal strictement inférieur. Ainsi, par récurrence, on peut construire une preuve de $T \cup \{F\} \vdash G$ telle que $I_F = \{G\}$. De même, on construit une preuve de $T \cup \{\neg F\} \vdash G$ tel que $I_{\neg F} = \{G\}$.

On considère alors la preuve $\mathcal{P}$ obtenue en concatenant les preuves $\mathcal{P}_F$ et $\mathcal{P}_{\neg F}$, mais sans les formules F et $\neg F$. On a alors dans la preuve les formules $F \implies G$ et $\neg F \implies G$. En outre, par l'exercice 28, on a $F \implies F$, qui équivaut à $F \vee (\neg F)$. Par l'axiome 11, on a $((F \vee \neg F) \wedge (F \implies G)) \wedge ((\neg F) \implies G)) \implies G$, ce qui permet de compléter $\mathcal{P}$ en une preuve de $T \vdash G$.

Remarque : On a montré au passage que l'on pouvait raisonner par cas.

    (b) On considère X_i une fonction partielle dans $\{0, 1\}$, et on pose $T_V = \{X_i | v(X_i) = 1\} \cup \{\neg X_i | v(X_i) = 0\}$. Montrer que pour toute formule H dont les variables sont dans le domaine de V, la relation $v \models H$ entraîne $T_V \vdash H$ et la relation $v \not\models H$ entraîne $T_V \vdash \neg H$.

Solution: On raisonne par induction, et pour simplifier le raisonnement, on se place dans le cas où les formules sont écrites uniquement à partir de $\neg$ et $\wedge$.
On suppose $H = \neg H'$. Alors $v \models H$ entraîne $v \not\models H'$ et donc par l'hypothèse d'induction, $T_V \vdash \neg H' = H$. De même, $v \not\models H$ entraîne $v \models H'$ et donc $T_V \vdash H'$. Par modus ponem avec l'axione $X \implies \neg\neg X$, on a donc $T_V \vdash \neg lnot H' = \neg H$. On suppose $H = F \wedge G$. Alors $v \models H$ entraîne $v \models F$ et $v \models G$. Alors par hypothèse d'induction, on a $T_V \vdash F$ et $T_V \vdash G$ et donc par 2 modus ponem avec l'axiome $X \implies (Y \implies (X \wedge Y))$, on en déduit $T_V \implies F \wedge G = H$. De même, $v \not\models H$ entraîne $v \not\models F$ ou $v \not\models G$. On suppose sans perte de généralité que c'est F. On a alors $T_V \vdash \neg F$, et donc par modus ponem par l'axiome $X \implies (X \vee Y)$, on en déduit $T_V \vdash (\neg F) \vee (\neg G) = \neg H$.

(c) Montrer la complétude de la preuve par modus ponem.

Solution: Soit F une tautologie, alors toute valutatiion la satidfait et donc pour on a $T_V \vdash F$ pour tout v. Soit $p_1, \ldots, p_n$ les variables propositionnelles intervenant dans F. Alors pour v une valutation, sur $X_1, \ldots, X_{n-1}$, on a alors $T_1 = T_V \cup \{X_n\} \models F$ et $T_2 = T_V \cup \{\neg X_n\} \models F$. Donc par la (b), on a $T_1 \vdash F$ et $T_2 \vdash F$ et donc par disjonction de cas on a $T_V \vdash F$. De même, par une récurrence immédiate, on peut supprimer les variables de T_V jusqu'à avoir $\emptyset \vdash F$.

L'on vient de démontrer que l'on pouvait tout démontrer !
Ici, "tout" fait référence à l'ensemble des tautologies, c'est à dire ce qui est logique, et "démontrer" fait référence à la démonstration par modus ponem. Ainsi, nous avons en quelque sorte montré que la logique est logique ! Mais en fait nous n'avons considéré que les énoncés d'ordre zéro (la logique pure). En mathématique, nous manipulons des propriétés plus compliquées, utilisant des nombres et des variables sur des ensembles quelconques, notamment via les quantificateurs : $\forall$ et $\exists$. Cela va nous amener à définir les formules du premier ordre et à adapter notre méthode de preuve à cette compléxité en espérant préserver ce résultat de complétude. Cependant, cela va faire apparaître la notion de structure, qui va biaiser les choses et permettre le paradoxe des théorèmes de Gödel...

3 Démonstration du premier ordre

Jusqu'à présent nous n'avons considéré que les formules propositionnelle d'ordre 0, c'est à dire sans quantificateur. L'on a vu que tout est prouvable dans la logique, mais si l'on souhaite faire des maths, l'on est très vite limité, car il nous manque les quantificateurs : $\forall$ et $\exists$. Nous allons nous intéresser ici au calcul propositionnel du premier ordre, c'est à dire autorisant les quantificateurs sur les variables. A titre d'information, le calcul du second ordre autorise les quantificateurs sur les fonctions ou les relations, mais cela sort du cadre du projet.

Nous allons donc devoir adapter nos définitions pour inclure les quantificateurs, et se donner la possibilité de travailler avec autre chose que des booléens. Cela va forcement faire apparaître la notion de fonction, ce qui nous force à élargir le champs théorique. Pour définir les formules du premier ordre, nous allons d'abord parler de signatures, de termes et de formules atomiques.
La *signature* $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ d'un langage du premier ordre est la donnée de :
— D'un ensemble de symboles $\mathcal{C}$ appelés *symboles de constantes*.
— D'un ensemble $\mathcal{F}$ de symboles appelé *symboles de fonctions*. A chaque fonction est associé un entier que l'on nomme *arité* (le nombre de variables)
— D'un ensemble $\mathcal{R}$ de symboles appelés *symboles de relations*. A chaque relation est aussi associé une arité.
On fixe pour la suite une signature $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R})$. Les formules du premier ordre seront donc des mots sur l'alphabet $\mathcal{A}(\Sigma) = \mathcal{V} \cup \mathcal{C} \cup \mathcal{F} \cup \mathcal{R} \cup \{\neg, \wedge, \vee, \implies, \iff, (,), \forall, \exists\}$.

L'ensemble des *termes* $\mathcal{T}$ sur la signature Σ est le langage sur l'alphabet $\mathcal{A}(\Sigma)$ défini inductivement par :
— Toute variable et toute constante est un terme, i.e. $\mathcal{V} \cup \mathcal{C} \subset \mathcal{T}$
— Si f est un symbole de fonction d'arité n, et si $t_1, \ldots, t_n$sont des termes, alors $f(t_1, \ldots, t_n)$ est un terme.
Un terme peut être vu un peu comme un nombre. On dira qu'un terme est *clos* si il est sans variable.
Une *formule atomique* sur la signature Σ est un mot sur l'alphabet $\mathcal{A}(\Sigma)$ de la forme $R(t_1, \ldots, t_n)$ où $R \in \mathcal{R}$ est une relation d'arité n et $t_1, \ldots, t_n$sont des termes sur Σ. On peut enfin définir les *formules propositionnelles du premier ordre* $\mathcal{G}$ par induction :
— Toute formule atomique est une formule.
— Si F est une formule, alors $\neg F$ est une formule.
— Si F et G sont des formules, alors $(F \wedge G)$, $(F \vee G)$, $(F \implies G)$, $(F \iff G)$ sont des formules.
— Si F est une formule et $x \in \mathcal{V}$ est une variable, alors $\forall x, F$ est une formule et $\exists x; F$ aussi.
Les variables apparaissent soit dans les formules atomiques, on parle alors de variables libres, soit via les quantificateurs, on parle de variable lié ou muette. Une formule est dite *close* si elle ne possède pas de variable libre.

Nous avons ainsi défini la syntaxe des formules du premier ordre, il faut maintenant définir le sens donné à ces formules (la sémantique). Comme nous prévoyons de sortir des booléen, nous sortons des cadres de la logique, il faut donc interpréter les formules sur une structure externe.
Une *structure* $\mathfrak{M}$ de signature Σ est la donnée :
— D'un ensemble non-vide M, appelé ensemble de base, ou domaine de la structure
— D'un élément, noté $c^{\mathfrak{M}}$, pour chaque symbole de constante $c \in \mathcal{C}$.
— D'une fonction, notée $f^{\mathfrak{M}} : M^n \to M$, pour chaque symbole de fonction $f \in \mathcal{F}$ d'arité n.
— D'une relation, notée $R^{\mathfrak{M}} : M^n \to \{0, 1\}$ pour chaque symbole de relation $R \in \mathcal{R}$ d'arité n.
Ainsi, une structure donne un sens à tout les symboles d'une signature. On parle aussi de *réalisation de signature*. Une valuation v donne maintenant des valeurs non booléennes aux variables, il s'agit donc d'une fonction de l'ensemble des variables $\mathcal{V}$ vers le domaine de la structure M. De même que précédemment, on peut appliquer une valuation v à une formule F. On dit que v *valide* F si $v(F) = 1$. Pour une formule close, la validation de F ne dépend pas de la valuation, mis uniquement de la structure. Dans le cas où F est vraie pour une structure $\mathfrak{M}$, on dit que $\mathfrak{M}$ est un modèle de F et on note $\mathfrak{M} \models F$.

Une *théorie* $\mathfrak{T}$ est un ensemble de formules closes sur une signature donnée. Les formules d'une théorie sont appelés les *axiomes* de cette théorie. Une structure $\mathfrak{M}$ est un modèle de cette théorie $\mathfrak{T}$ si $\mathfrak{M}$ est un modèle de chacune des axiomes de la théorie. Une théorie est dite consistante si elle possède une modèle. Elle est dite *inconsistante* dans le cas contraire. Une formule F est dite être une *conséquence* de la théorie $\mathfrak{T}$ si tout modèle de la théorie $\mathfrak{T}$ est un modèle de F. On note alors $\mathfrak{T} \models F$. On dit qu'une théorie est cohérente, si il n'existe pas de formule F telle que $\mathfrak{T} \vDash F$ et $\mathfrak{T} \vDash \neg F$.

31. Redéfinir les formules propositionnelles d'ordre 0 comme un cas particuliers des formules propositionnelles d'ordre 1 muni d'une strucutre particulière, et relier les différents concepts.

Solution: Laissé au lecteur

32. Définir la théorie des groupes.

Solution: Laissé au lecteur

33. Définir une théorie pour laquelle les graphs non-orientés sont un modèle mais pas les graphs orientés.

Solution: Laissé au lecteur

34. Ecrire dans cette théorie la formule caractérisant les sommet de degré 1, et les triangles.

Solution: Laissé au lecteur

35. Définir une théorie pour laquelle les rationnels sont un modèle mais pas les entiers.

Solution: Laissé au lecteur

36. Définir une théorie pour laquelle les entiers sont un modèle mais pas les rationnels.

Solution: Laissé au lecteur

3.1 Completude

On va adapter la notion de preuve par *modus ponem* aux formules propositionnelles de premier ordre. Il suffit pour cela d'ajouter la règle de généralisation : Si l'on a F une formule et une variable x, alors on a $\forall x, F$. On ajoute aussi les axiomes suivant :

$$\begin{aligned} \exists x; F &\iff \neg\forall x \neg F \\ (\forall x, (F \implies G)) &\implies (F \implies \forall x, G) \\ \forall x, F &\implies F(t/x), \end{aligned}$$

où t désigne un terme que l'on subtitue à x, dans le cas où aucune occurence libre de x ne se trouve dans le champ d'un quantificateur liant une variable de t.
Le premier théorème de Gödel nous dit que si $\mathfrak{T}$ est une théorie, et F une formule close, alors F est une conséquence de $\mathfrak{T}$ si et seulement si F se prouve à partir de $\mathfrak{T}$. En outre, toute théorie cohérente est consistante.
La validité (le sens réciproque), i.e. la véracité de ce que l'on prouve, se montre facilement et la preuve n'est pas particulièrement intéressante, ainsi nous l'admettrons par la suite.

37. Montrer le lemme de déduction. Si $T \cup \{F\} \vdash G$, alors $T \vdash (F \implies G)$.

Solution: On considère une preuve $G_1, \ldots, G_n$ de G à partir de $T \cup \{F\}$.
On construit une preuve de $F \implies G$ à partir de $(F \implies G_1), \ldots, (F \implies G_n)$ en insérant des propositions.

— Si G_i est une tautologie ou F, alors $F \implies G_i$ en est une aussi.
— Si G_i est une axiome ou un élément de $\mathcal{T}$, alors on insère avant G_i (car c'est un axiome) et $G_i \implies (F \implies G_i)$ (c'est une tautologie), ce qui permet de déduire $F \implies G_i$.
— Si G_i est obtenu par modus ponem à partir de G_j et $G_k = (G_j \implies G_i)$. Alors, on insère avant :
  1. $(F \implies G_j) \implies (((F \implies (G_j \implies G_i)) \implies (F \implies G_i))$ car c'est une tautologie
  2. $(F \implies (G_j \implies G_i)) \implies (F \implies G_i)$ obtenu par modus ponem à partir de la formule précédente et de $F \implies G_j$.

  $F \implies G_i$ obtenu par modus ponem à partir de $F \implies G_k$ et la formule précédente.
— Si G_i est obtenu par généralisation de G_j, on ajoute
  1. $\forall x, F \implies G_j$ obtenu par généralisation de $F \implies G_j$.
  2. $(\forall x, (F \implies G_j)) \implies (F \implies \forall x, G_j)$ axiome de quantificateurs, car F est close.

  $F \implies G_i$ se déduit par modus ponem à partir des 2 formules précédentes.

38. Montrer le lemme de substitution. Si T est une théorie et $F(x)$ une formule dont la seule variable libre est x. Si $T \vdash F(c/x)$ alors $T \vdash \forall x, F(x)$.

Solution: On considère une $F_1, \ldots, F_n$ une démonstration de $F(c/x)$. On considère w une variable qui n ?apparaît dans aucune formule F_i et K_i la formule obtenue en remplaçant dans F_i le symbole c par w. On remarque que cela fournit une preuve de $F(w/x)$. Par axiome de quantificateur, on obtient $\forall w, F(w/x) \implies F$, et donc par généralisation $\forall x, (\forall w, F(w/x))$ et donc par le deuxième axiome des quantificateurs, on a $(\forall x, (\forall w, F(w/x)) \implies F) \implies (\forall w, F(w/x) \implies \forall x, F)$, et donc le résultat par modus ponem.

On dit qu'une théorie est *complète* si pour toute formule close F, on a $T \vdash F$ ou $T \vdash \neg F$. On dit qu'une théorie admet des *témoins de Henkin* si pour toute formule $F(x)$ avec une variable libre x, il existe un symbole de constante c dans la signature tel que $\exists x, F(x) \implies F(c)$ soit une formule de la théorie T.

39. Prouver que toute théorie complète avec des témoins de Henkin admet un modèle.

Solution: On construit un modèle comme simplement l'ensemble syntaxique. Notre modèle $\mathfrak{M}$ aura donc comme ensemble de base l'ensemble des termes clos sur la signature de la théorie. Ainsi, si c est une constante, on pose $c^{\mathfrak{M}}$ son interprétation qui est la constante elle-même. Si f est une fonction d'arité n, alors son interprétation $f^{\mathfrak{M}}$ est la fonction qui, à $t_1, \ldots, t_n$ des termes clos associe le terme clos $f(t_1, \ldots, t_n)$. Si R est un symbole de relation d'arité n, alors son interprétation $R^{\mathfrak{M}}$ vaut 1 pour tout les termes clos $(t_1, \ldots, t_n)$ tels que $T \vdash R(t_1, \ldots, t_n)$. On montre par induction $T \vdash F$ si et seulement si $\mathfrak{M}$ est un modèle de F (le modèle a été construit pour ça). Il suffit de le montrer dans les cas du type $F = \neg G$, $F = G \vee H$ et $F = \exists x, G$:
— Si $F = \neg G$, alors par complétude de T, $T \vdash \neg G$ ssi $T \nvdash G$, on donc ssi $\mathfrak{M} \nvDash G$ par hypothèse d'induction, soit $\mathfrak{M} \vDash \neg G$.
— Si $F = G \vee H$. On suppose $\mathfrak{M} \vDash G \vee H$. On peut supposer $\mathfrak{M} \vDash G$, d'où $T \vdash G$ et donc $T \vdash G \vee H$.
  Récirproquement, si $T \vdash G \vee H$. Si $T \vdash G$, alors on a bien $\mathfrak{M} \vDash G$ et donc $\mathfrak{M} \vDash G \vee H$. Sinon, on a $T \nvdash G$ car T est complète, et donc $T \vdash \neg G$ et donc comme $(G \vee H) \implies (\neg G \implies H)$ est une tautologie, on a $T \vdash H$ et donc $\mathfrak{M} \vDash G \vee H$.
— Si $F = \exists x, G(x)$. Supposons $\mathfrak{M} \vDash \exists x, G(x)$, alors il existe un terme clos t tel que $\mathfrak{M} \vDash G(t/x)$ et donc $T \vdash G(t/x)$, ce qui donne facilement une démonstration de $\exists x, G(x)$.
  Réciproquement, si $T \vdash \exists x, G(x)$, alors comme T a des témoins de Henkin, on obtient c tel que $\exists x, G(x) \implies G(c)$ et donc $T \vdash G(c/x)$ et donc $\mathfrak{M} \vDash G(c/x)$ et donc $\mathfrak{M} \vDash F$.

Donc $\mathfrak{M}$ est bien un modèle de T.

40. Prouver que toute théorie cohérente possède une extension complète, cohérente et avec des témoins de Henkin.

Solution: On considère une théorie T cohérente sur une signature Σ. On rajoute à Σ un nombre dénombrable de constante pour former Σ'. On énumère l'ensemble des formules closes de Σ' par $(F_n)_{n\in\mathbb{N}}$. On construit T' par récurrence comme l'union des théories T_n construites par récurrence, par $T_0 = T$ et T_{n+1} comme suit :
Si $T_n \cup F_n$ est cohérente, on pose $G_n = F_n$ et $G_n = \neg F_n$ sinon. On pose alors $T_{n+1} = T_n \cup \{G_n\}$ si $G_n \neq \exists x, H$, et sinon $T_{n+1} = T_n \cup \{G_n, H(c/x)\}$, avec c une constante de Σ' non utilisé dans T_n (existe car seul un nombre fini est utilisé).
Alors on a bien T_{n+1} cohérente. Sinon, on aurait forcement G_n de la forme $\exists x, H$ et on aurait $T_n \cup \{\exists x, H\} \vdash \neg H(c/x)$. Alors par le lemme de substitution démontré à la question 38, on aurait $T_n \cup \{\exists x, H\} \vdash \forall\forall x, \neg H(x)$, ce qui impliquerait que T_n n'est pas cohérente.
On construit donc $T' = \bigcup_n T_n$. T' est bien cohérente car toute partie finie de T' est cohérente. T' est complète car toute formule de Σ' apparaît à un moment dans l'énumération des F_n. Enfin, T' admet des témoins de Henkin. En effet, soit $H(x)$ une formule, il existe n tel que $F_n = \exists x, H(x)$. Alors soit $\neg F_n \in T_{n+1}$, soit il existe une constante c telle que $H(c/x) \in T_{n+1}$. Dans les deux cas, on a $T_{n+1} \vdash \exists x, H(x) \implies H(c/x)$ et donc $\exists x, H(x) \implies H(c)$ est dans T' (sinon on y ajouterait à un moment sa négation, ce qui la rendrait incohérente).

41. Montrer que toute théorie cohérente possède un modèle. En déduire le théorème.

Solution: Soit T une théorie cohérente. Alors il existe une théorie T' extension de T cohérente, complète, avec des témoins de Henkin. Donc T' possède un modèle, qui est donc un modèle de T.
Soit F une formule conséquence de T. Si $T \nvdash F$, alors la théorie $T \cup \{\neg F\}$ est cohérente, et donc possède un modèle par ce qui précède, et donc F n'est pas une conséquence de T, ce qui est absurde. Donc $T \vdash F$.

On voit que la théorie est une tentative de "réduire" une structure à un ensemble d'axiomes. Si il est facile de garantir qu'une structure est bien un modèle de la théorie, il est beaucoup difficile d'empêcher d'autre ensemble plus gros de l'être aussi. On peut se poser la question si il est possible de "capturer" l'essence des entiers, c'est à dire de proposer une théorie qui ne correspond uniquement qu'aux entiers.

3.2 Axiomatisation des entiers

Pour obtenir les entiers, il faut avoir au moins les notions d'addition, de multiplication, de successeur et le raisonnement par récurrence. Nous allons ici définir une axiomatique sur les entiers, appelés *Axiomes de Peano*, qui permet d'attraper tout ces concepts.

On considère une signature composée du symbole de constante 0, d'une fonction unitaire s (qui correspond au successeur), de deux fonctions binaires $+$ et $\times$ et de la relation binaire $=$.

Les axiomes de Peano sont les axiomes de l'égalité (que l'on ne définira pas ici mais qui permettent de définir l'égalité usuelle) ainsi que

$$\begin{aligned}
\forall x, \neg(s(x) = 0) \\
\forall x, \forall y (s(x) = s(y) \implies x = y) \\
\forall x (x = 0 \vee \exists y; s(y) = x) \\
\forall x, 0 + x = x \\
\forall x, s(x) + y = s(x + y) \\
\forall x, 0 \times x = 0 \\
\forall s(x) \times y = x \times y + y
\end{aligned}$$

et toutes les formules de la forme

$$\forall x_1 \dots \forall x_n \left[(F(0, x_1, \dots, x_n) \wedge \forall x_0 F(x_0, x_1, \dots, x_n)) \implies F(s(x_0), x_1, \dots, x_n) \right] \implies \forall x_0 F(x_0, x_1, \dots, x_n)$$

avec $n \in \mathbb{N}$ et F une formule quelconque.

42. Prouver que l'axiome $\forall x (x = 0 \vee \exists y; s(y) = x)$ est inutile, i.e. que c'est une conséquence des autres.

> **Solution:** Laissé au lecteur.

43. Exprimer les concepts suivant à partir des axiomes de Paeno :
    (a) q est le quotient et r le reste de la division euclidienne de x par y.
    (b) y divise x
    (c) x est pair
    (d) x est premier
    (e) x est une puissance de 2

> **Solution:** Laissé au lecteur.

44. Prouver que l'ensemble des formules définissables à partir des axiomes de Paeno est récursivement énumérable, et plus généralement que toute axiomatique récursivement énumérable possède un nombre récursivement énumérable de suite finie de formules.

> **Solution:** Simple corollaire des questions de la partie 1, l'ensemble des suites finies de formules s'obtient comme union dénombrable d'ensemble dénombrables.

45. En déduire que l'on peut définir une bijection de $\mathbb{N}$ dans l'ensemble des suites finies de formules.

Solution: Simple application de la définition.

Cette bijection permet de définir un codage des formules. Ainsi, pour ϕ une formule ou un ensemble de formule, on note $< \phi > \in \mathbb{N}$ son codage.
En réalité, on ne peut pas définir un codage aussi simplement, car il est primordial d'assurer que les formules récursives puissent être représentées par les formules arithmétiques. Une formule $f(x_1, \ldots, x_n)$ est dite *représentée* dans l'axiomatique de Peano si il existe une formule $R(x_1, \ldots, x_n, y)$ vérifiant $\vdash R(< x_1 >, \ldots, < x_n >, y) \Leftrightarrow y =< f(x_1, \ldots, x_n) >$.
On admettra le théorème suivant :
Théorème de représentation : il existe un codage tel que toutes les formules récursives soient représentées dans l'axiomatique de Peano.

3.3 Incomplétude

Il s'agit maintenant de prouver l'incomplétude de l'arithmétique. On rappelle que l'on note $\vdash$ pour prouvable dans l'axiomatique de Peano, et $\models$ pour vrai sur les entiers. On commence par montrer le lemme suivant :
Lemme du point fixe de Gödel Pour toute formule $\psi(x_0)$ avec pour seule variable libre x_0, il existe une formule close τ telle que

$$(\vdash \tau) \Leftrightarrow \psi(< \tau >),$$

On se donne $\psi(y)$ une formule n'ayant que y comme variable libre, et x_0 une autre variable. On admettra que la formule $\text{subst}(< x >, \phi, \pi)$ définie par $\pi = \phi(^{x_0}/_{<x>})$ est récursive. Ainsi, par le théorème de représentation, cela garantit l'existence d'une formule arithmétique $\text{SUBST}(< x >, < \phi >, < \pi >)$ exprimant la propriété suivante : "π est obtenue en substituant la constante $< x >$ dans toutes les occurrences de la variable libre x_0 dans la formules ϕ", i.e. $(\vdash \text{SUBST}(< x >, < \phi >, < \pi >)) \Leftrightarrow (\pi = \phi(^{x_0}/_{<x>}))$.
On pose $\sigma(x)$ la formule définie par $\forall y(\text{SUBST}(x, x, y) \implies \psi(y))$ et on pose $\tau = \sigma(< \sigma(x_0) >)$.
46. Montrer que τ est la solution recherchée. En déduire le lemme.

Solution: On a, par définition,

$$\vdash \text{SUBST}(< \sigma(x_0) >, < \sigma(x_0) >, y) \Leftrightarrow y =< \tau >$$

donc

$$\vdash (\text{SUBST}(< \sigma(x_0) >, < \sigma(x_0) >, y) \implies \psi(y)) \Leftrightarrow (y =< \tau > \implies \psi(y))$$

Et donc

$$\vdash \tau \Leftrightarrow (\vdash \forall y, (\text{SUBST}(< \sigma(x_0) >, < \sigma(x_0) >, y) \implies \psi(y))) \Leftrightarrow (\forall y, (y =< \tau >) \implies \psi(y)) \Leftrightarrow \phi(< \tau >)$$

On admettra que la formule qui, pour π un ensemble de formule et ϕ une formule, est vraie si et seulement si π est une preuve de ϕ, est récursive.
47. Construire la formule PROUVABLE$(< \phi >)$, qui exprime que la formule ϕ est prouvable.

Solution: On a $prouvable(\phi) \Leftrightarrow \exists \pi; preuve(\pi, \phi)$ et cette formule est donc récursive, d'où l'existence de PROUVABLE.

48. Montrer que pour toute formule close ϕ, on a $(\vdash \phi) \Leftrightarrow (\vdash PROUVABLE(< \phi >))$.

Solution: Le sens direct vient du fait que si $\vdash \phi$, alors il existe π un preuve de ϕ et donc $\vdash$ PROUVABLE($< \phi >$). Le sens réciproque est une conséquence de la validité de la preuve dans l'axiomatique de Peano.

49. Utiliser le lemme du point fixe pour construire une formule non prouvable. Montrer que cette formule est vraie.

Solution: On applique le lemme du point fixe à ¬PROUVABLE. Ainsi, on a τ tel que

$$\vdash \tau \Leftrightarrow \neg\text{PROUVABLE}(< \tau >)$$

Par validité de la preuve, on a $\neg\text{PROUVABLE}(< \tau >) \implies \vdash \tau \implies \models \tau$. Réciproquement, si PROUVABLE($< \tau >$), alors $\vdash \neg\tau$ et donc $\models \neg\tau$ par validité. D'où

$$\models \tau \Leftrightarrow \neg\text{PROUVABLE}(< \tau >)$$

Supposons τ fausse. Alors

$$\begin{aligned} \models \neg\tau &\implies \text{PROUVABLE}(< \tau >) \implies \vdash \tau \qquad \text{(par définition de PROUVABLE)} \\ &\implies \models \tau \end{aligned}$$

Donc τ est vraie et non prouvable.

50. En déduire le théorème d'incomplétude.

Solution: On a donc l'existence d'une formule close vraie sur les entiers mais non prouvable par les axiomes de Peano.

4 Conclusion

51. Expliquer pourquoi les deux théorèmes ne sont pas incompatibles.

Solution: Une formule F est démontrable si et seulement si elle est vraie sur **TOUT** les modèles d'une théorie. Mais il existe des formules vraies sur les entiers, qui ne le sont pas sur d'autres modèles de l'axiomatique de Peano. On appelle ces modèles les entiers non standard. La non-incompatibilité vient de l'impossibilité (avec les formules du premier ordre) de définir une axiomatique réservée aux entiers, il y aura toujours des ensembles plus gros d'entiers non standard.
Ainsi dans le théorème 1, *tout* signifie *tout ce qui est vrai sur tout modèle de la théorie* et dans le théorème 2, *tout* signifie *tout ce qui est vrai sur les entiers.*