NOM : PECATTE **Prénom :** Timothée **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 924 - Théories et modèles en logique du premier ordre. Exemples.

Autre sujet : Réf : • Dowek, Les démonstrations et les algorithmes
• DNR, Introduction à la logique
• Cori, Logique Mathématique.

I. Introduction et cadre de travail :

I.1. Motivations :

Déf 1 : Un groupe est un ensemble G muni d'une loi interne * vérifiant :
(i) $a*(b*c) = (a*b)*c$
(ii) $\exists e \in G$ tq $\forall a \in G$, $a*e = e*a = a$
(iii) $\forall a \exists b \in G$ tq $a*b = e = c*a$

Ex 2 :
- La propriété (ii) implique $\forall a \exists b$ tq $a*b = b*a = e$
- Il existe des groupes ne vérifiant pas $\forall a \forall b$, $a*b = b*a$, comme $(\mathbb{Z}^2, +)$ et d'autres qui ne vérifient pas cette propriété comme $(\mathcal{M}_n(\mathbb{R}), \times)$.

Bil Définir ce qui est "inscrit dans" les contraintes "hypothèses".
Montrer que ce qui est "inscrit dans" les conséquences "de ces hypothèses ne contient pas ce qui n'est pas "conséquence" de ces hypothèses.

I.2. Formalisation : le langage

Déf 3 : (Langage) Un langage est la donnée d'une famille de symboles de base sont : des constantes, des symboles de fonction et de relation auxquels sont associés un entier $n \in \mathbb{N}^*$, appelé arité.

Ex 4 :
- $\mathcal{L}_{\mathbb{N}_0} = \{0, S_1\}$
- $\mathcal{L}_{groupe} = \{e, *_2, i_1\}$
- $\mathcal{L}_{\mathbb{Z}/2\mathbb{Z}} = \{\bar{0}, n_2, \cup_2, \cap_2, c_1, \mathbb{Z}_2\}$

Déf 5 : (Terme) Soit $\mathcal{L}$ un langage. $T(\mathcal{L})$ est le plus petit ensemble contenant les variables, les constantes et qui est stable par l'application des symboles de fonctions de $\mathcal{L}$.

Ex 6 : $T(\mathcal{L}_{\mathbb{N}}) = \{S_1(S_1(\dots S_1(0)\dots))\}$

Rem 7 : Les constantes peuvent être vues comme des fonctions d'arité 0.

Rem 8 : On préférera écrire $a*b$ plutôt que $*(a,b)$.

Déf 9 : (Formules) Les formules atomiques sont de la forme $R(t_1, \dots, t_n)$, où R est un symbole de relation de $\mathcal{L}$ et $t_1, \dots, t_n \in T(\mathcal{L})$.
L'ensemble des formules est défini par : $F ::= A \mid \top \mid \bot \mid \neg F \mid F \wedge F \mid F \vee F \mid F \Rightarrow F \mid \forall x F \mid \exists x F$

Ex 10 : $\exists e \forall a, *(a,e) = a \wedge *(e,a) = a$

Déf 11 :
- variables libres/liées, formule close.
- α-équivalence

I.3. Formalisation : les preuves/la déduction :

Déf 12 :
- Séquents
- règle de déduction
- preuve d'un séquent

Déf 13 : Déduction naturelle

Ex 14 :

$$\frac{\Gamma \vdash \forall x, x = z \Rightarrow e}{\Gamma \vdash e = e \Rightarrow e' = e} \forall e \qquad \frac{\Gamma \vdash \forall y, e = y \Rightarrow e' = e}{\Gamma \vdash e = e \Rightarrow e' = e} \forall e$$

$\Gamma := \forall x, x*z = z \Rightarrow e = e'$, $\forall y, e = y \Rightarrow e' = e$ $\vdash e = e'$

Rem 15 : On aimerait par preuve n'importe quelle théorie mathématique dans un système de déduction comme les systèmes à la Hilbert, ou les systèmes à plusieurs conclusions.

II. Théories et modèles : de la vérité

II.1. Le point de vue syntaxique :

Déf 16 : (Théorie) Une théorie est un ensemble de formules closes, sur un langage $\mathcal{L}$ appelées axiomes.

Déf 17 : (Théorème) Une formule A est un théorème d'une théorie T si il existe $\Gamma \subseteq T$ tq Γ soit fini et $\Gamma \vdash A$ se démontre.

Ex 18 : Soit $\mathcal{L}_{\mathbb{N}} = \{0, S_1, +_2, \times_2, =_2\}$, on définit PA par :
$F_1 \equiv \forall x \forall y (S(x) = S(y) \Rightarrow x = y)$ / $F_2 \equiv \forall x \neg (0 = S(x))$

$F_3 \equiv \forall y\,(0+y=y)$ | $F_4 \equiv \forall x\forall y\,(S(x)+y=S(x+y))$ | $F_5 \equiv \forall y\,(0\times y=0)$ |

$F_6 \equiv \forall x\forall y\,(S(x)\times y=(x\times y)+y)$

et le schéma d'axiomes de récurrence :

pour $P(x_1,\dots,x_n,y)$ une formule avec une v.l. $F_P \equiv (P(0)\wedge \forall x(P(x)\Rightarrow P(S(x))))\Rightarrow \forall x\,P(x)$

Ex 19 : Théorie naïve des ensembles : pour chaque formule sur $\mathcal{L}_{\in}=\{\in_1,=_2\}$, on a l'axiome : $\forall x_1\dots\forall x_n\exists y\forall y(y\in y \Leftrightarrow P(x_1,\dots,x_n,y))$ ($P(x_1,\dots,x_n,y)$)

Déf 20 : Une théorie T est contradictoire si elle démontre $\bot$

Ex 21 : Le paradoxe de Russel permet de montrer que la théorie naïve des ensembles est contradictoire via : $P(y) \equiv \neg(y\in y)$

Prop 22 : Une théorie est contradictoire ssi $\exists A$ une formule tq $T\vdash A$ et $T\vdash \neg A$

II.2. Le point de vue sémantique :

Déf 23 : ($\mathcal{L}$-structure) Etant donné un langage $\mathcal{L}$, on appelle $\mathcal{L}$-structure l'ensemble $\mathcal{M}$ constitué :
- d'un ensemble non vide $|\mathcal{M}|$, appelé domaine de $\mathcal{M}$
- d'un élément $c_{\mathcal{M}}\in|\mathcal{M}|$ pour chaque constante $c\in\mathcal{L}$
- d'une fonction $f_{\mathcal{M}} : |\mathcal{M}|^n \to |\mathcal{M}|$ pour chaque symbole de fonction n-aire $f\in\mathcal{L}$.
- d'un sous-ensemble $R_{\mathcal{M}} \subseteq |\mathcal{M}|^n$ pour chaque symbole de relation n-aire $R\in\mathcal{L}$.

Ex 24 :
- $(\mathbb{N},0,+,\times,S)$ est une $\mathcal{L}$-structure de $\mathcal{L}_{\mathbb{N}}$
- $(\mathbb{Q},0,+,\times,S)$ ——————
- $(\mathcal{M}_n(\mathbb{R}),0,+,\times,S)$ ——————, où $S(M)=M+I_n$ par exemple

Déf 25 : (Environnement) Etant donné une $\mathcal{L}$-structure $\mathcal{M}$, un environnement est une fonction Θ des variables dans le domaine : $\Theta : X \to |\mathcal{M}|$.

Déf 26 : (Valeur d'un terme) Etant donné un environnement, on définit inductivement $val(t)\in|\mathcal{M}|$.

Ex 27 : Pour $(\mathbb{N},0,+,\times,S)$, on a $val(S(S(0))+S(0)) = 3$

Déf 28 : (Valeur d'une formule) On définit de même la valeur d'une formule par induction et $val(F)\in\{0,1\}$

On notera $\mathcal{M},\Theta\models F$ ou $\mathcal{M}\models F$ si $val(F)=1$ et on dit que $\mathcal{M}$ est un modèle de F

Rem 29 : Pour toute formule F et pour tout $\mathcal{L}$-structure $\mathcal{M}$, on a soit $\mathcal{M}\models F$, soit $\mathcal{M}\models\neg F$.

Déf 30 : (Modèle) On dit qu'une $\mathcal{L}$-structure $\mathcal{M}$ est un modèle de T une théorie si $\mathcal{M}$ est un modèle de tous les axiomes de T (ie $\forall F\in T,\ \mathcal{M}\models F$)

Ex 31 :
- $(\mathbb{N},0,*,\times,\leq)$ est un modèle de PA
- $(\mathbb{Z},0,+,\times,\leq)$ n'est pas un modèle de PA car F_2 est fausse dans cette $\mathcal{L}_{ar}$-structure.

Déf 32 : On dit que F est un théorème logique de la théorie T si pour tout modèle $\mathcal{M}$ de T, on a $\mathcal{M}\models F$.

Ex 33 : $\forall x\forall y\,(x\times y=y\times x)$ n'est pas un théorème logique car il est faux dans le modèle $(\mathcal{M}_n(\mathbb{R}),\times,I_n)$ de la théorie des groupes.

II.3. Une seule et même vérité :

Prop 34 : (Correction) Si on a $T\vdash F$, alors pour tout modèle $\mathcal{M}$ de T, on a $\mathcal{M}\models F$ (ie F est un théorème logique de T)

Coro 35 : S'il existe un modèle de T qui n'est pas un modèle de F, alors F n'est pas démontrable dans T.

Ex 36 : $\forall x\forall y\,(x\times y=y\times x)$ n'est donc pas démontrable dans la théorie des groupes

Th 37 : (Complétude) Si A est valide dans tous les modèles de T, alors $T\vdash A$.

DEV Complétude du calcul propositionnel ← DEV 1

Th 38 : (Compacité) T admet un modèle ssi tout sous-ensemble de T admet un modèle

Th 39 : Si T a des modèles finis de cardinal arbitrairement grand, alors T a aussi un modèle infini

Th 40 : Si T a un modèle infini, alors T a aussi un modèle infini non dénombrable

Ex 41 : PA a $(\mathbb{N},0,s,+,\times)$ comme modèle infini, donc PA a un modèle infini non dénombrable.

DEV2 → DEV | Un groupe (abélien) est totalement ordonnable ssi il est sans torsion

III. Applications de la théorie des modèles :

III.1. Décidabilité :

Prop 42 : Si on peut construire, dans un langage, les propositions N, Null, Succ, Plus, Mult et Eq, alors on peut encoder les programmes dans ce langage

Déf : Théorie T_0

Ex 43 : $\mathcal{L}_{IN}$ permet d'encoder les programmes

Prop 44 : Soit $\mathcal{L}$ un langage qui permet d'encoder des programmes. Pour tout programme f, il existe une proposition F tq $T \vdash F$ ssi f s'arrête sur son entrée.

Prop 45 : La fonction qui à un programme f associe la proposition F est calculable

Cor 46 : Soit $\mathcal{L}$ un langage assez riche et T une théorie tq $Th(T) \supset T_0$, alors $Th(T)$ n'est pas décidable

Cor 47 : Les théorèmes de PA ne sont pas décidables

Rem 48 : La décidabilité n'est pas stable par extension/restriction

Ex 49 : • Les théorèmes de PA sans $\times$ sont décidables
• Les théorèmes de PA $\cup \{\bot\}$ sont décidables

Th 50 : (Church) Soit un langage contenant au moins un symbole de prédicat binaire, alors les théorèmes de la théorie nue sur ce langage est indécidable

III.2. Complétude et indépendance :

Déf 51 : • Une théorie T décide F si $T \vdash F$ ou $T \vdash \neg F$
• T est complète si pour toute formule close F, T décide F

Prop 52 : La théorie nue du calcul propositionnel est complète

Th 53 : Soit T une théorie complète et récursive sur un langage au plus dénombrable. Alors les théorèmes de T sont décidables.

Cor 54 : PA n'est pas complète

Th 55 : (Incomplétude de Gödel) Aucune théorie ne contenant PA, non contradictoire, et récursive n'est complète

Déf 56 : Une formule F est dite indépendante de T si ni $T \vdash F$, ni $T \vdash \neg F$

Ex 57 : • Dans ZF, l'axiome du choix est indépendant
• Dans PA, le théorème de Goodstein

III.3. Modèles standard et définissabilité :

Déf 58 : Modèle standard

Ex 59 : Modèles standards de PA sont de la forme $\{\underbrace{S(S(\dots(0)\dots))}_{n}\}$

Prop 60 : D'après le théorème de compacité, il existe des modèles non-standard

DEV | Modèles non-standard de PA ← DEV3

Déf 61 : (Définissabilité) Soit $\mathcal{M}$ un ensemble, et $R_1, \dots, R_n$ des relations sur cet ensemble. La relation S est définissable s'il existe une formule F dans le langage $\{R_1, \dots, R_n\}$ tq $(a_1, \dots, a_p) \in S \Leftrightarrow \mathcal{M} \models F(a_1, \dots, a_p)$

Ex 62 : • Intersection de deux relations binaires : $F(x,y) \equiv P_1(x,y) \wedge P_2(x,y)$
• Composée de deux relations binaires : $F(x,y) \equiv \exists z,\ P_1(x,z) \wedge P_2(z,y)$
• La clôture réflexive transitive n'est pas définissable

Rem 63 : En théorie des bases de données, les relations définissables correspondent aux requêtes exprimables