Emmanuel Jeandel

Théorie des modèles

Notes du cours de Frank Wagner

NOTATIONS

ND	non démontré (i)
$\mathfrak{M} \models \phi(\overline{m})$	$\mathfrak{M}$ satisfait $\phi(\overline{m})$ (4)
$\mathrm{Th}(\mathfrak{M}, A)$	Ensemble des énoncés à paramètres dans A satisfaites par $\mathfrak{M}$ (7)
$\mathfrak{M} \equiv \mathfrak{N}$	M et N sont élementairement équivalents (11)
$\mathfrak{M} \subseteq \mathfrak{N}$	$\mathfrak{M}$ est une sous-structure de $\mathfrak{N}$ (12)
$\mathfrak{M} \prec \mathfrak{N}$	$\mathfrak{M}$ est une sous-structure élémentaire de $\mathfrak{N}$ (12)
ω	Cardinal des entiers (17)
$S_n(\overline{a})$	Ensemble des types en n- variables à paramètres dans $\overline{a}$ (51)

Table des matières

INTRODUCTION

Ces notes de cours correspondent au cours de maitrise donné par Frank Wagner, les TDs ayant été assurés par Bruno Poizat. Certains points ont été ajoutés, lorsqu'il s'agit de corollaires immédiats et faciles du cours, comme le test de Vaught. Certains énoncés très durs sont quant à eux énoncés en exercice, sans qu'il soit indispensable pour le lecteur d'essayer de les prouver.

Nous supposerons le lecteur habitué aux raisonnements par induction et à la logique classique, et à quelques notions d'algèbre élémentaires, celles-ci étant uniquement utilisé ici pour fournir des exemples d'application des différents théorèmes.
Dans la suite, nous noterons par ND les points des exemples, dont la démonstration est difficile avec les éléments dont on dispose dans l'état d'avancement du cours. Le lecteur, s'il tient à s'assurer de la véracité des faits, devra faire la démonstration après avoir lu les chapitres suivants. Il est néanmoins important, pour des raisons de pédagogie, de posséder assez tôt quelques exemples, même si les nombreux faits rapportés sont délicats à démontrer.

Lex exercices sont accompagnés quelquefois d'une notation indicative de leur difficulté :

$\star$ Il faut travailler un peu

$\star\star$ Difficile sans indications

$\star\star\star$ Vraiment pas facile

Chapitre 1

LANGAGES ET STRUCTURES

On introduira ici les définitions de base, qui permettront de formaliser les notions intuitives de relations, de termes, et de modèles.

1.1 Syntaxe

Définition 1.1 (*Langage*)

Un *langage* $\mathcal{L}$ est la donnée

- D'un ensemble $\mathcal{C}$ de symboles appelés *constantes*
- D'un ensemble $\mathcal{F}$ de symboles appelés *fonctions* et d'une application de $\mathcal{F}$ dans $\mathbb{N}$, qui associe à chaque fonction son *arité*. On peut donc écrire $\mathcal{F} = \cup \mathcal{F}_n$, où $\mathcal{F}_n$ est l'ensemble des fonctions d'arité n.
- D'un ensemble $\mathcal{R}$ de symboles appelés *relations* et d'une application de $\mathcal{R}$ dans $\mathbb{N}$, qui associe à chaque relation son *arité*. $\mathcal{R}$ contient toujours un élément privilégié, noté $=$, d'arité 2. On définit comme ci-dessus $\mathcal{R}_n$.

les ensembles considérés étant disjoints.

Au lieu de dire que l'arité de f est 1 (resp. 2) on dit souvent que f est une fonction *unaire* (resp. *binaire*)[1]. On travaille souvent également avec l'alphabet des *variables* $\mathcal{V}$. Celui-ci ne fait pas explicitement partie d'un langage, et sera souvent considéré comme préexistant.

♦ **Exemple**

Le langage des groupes $\mathcal{L}_{gp}$ notés multiplicativement est défini par $\mathcal{C} = \{1\}$, $\mathcal{F} = \left\{{}^{-1}, \circ\right\}$, les deux fonctions étant respectivement unaires et binaires.

Lorsqu'il n'y a qu'un nombre fini de fonctions, constantes ou relations, on dénotera souvent $\mathcal{L}$ directement par ses symboles. Par exemple, on écrira quelquefois $\mathcal{L}_{gp} = \{1, {}^{-1}, \circ\}$

Remarque : Cette définition ne donne encore aucun sens aux objets qu'on manipule, il ne faut y voir pour l'instant qu'une façon de fixer l'alphabet avec lequel on va travailler.

Définissons maintenant les termes et les formules, qui correspondent aux propriétés que l'on veut pouvoir énoncer.

[1] On trouve dans quelques textes des fonctions d'arité 0, qu'on identifie alors naturellement à des constantes

Définition 1.2 (*Termes*)

Soit $\mathcal{L}$ un langage. L'ensemble des $\mathcal{L}$-*termes* $\mathcal{T}$ est le plus petit ensemble qui vérifie

- $\mathcal{T}$ contient les constantes : $\forall c \in \mathcal{C}, c \in \mathcal{T}$
- $\mathcal{T}$ contient les variables : $\forall v \in \mathcal{V}, v \in \mathcal{T}$
- $\mathcal{T}$ est clos par les fonctions :

$$\forall n, \forall f \in \mathcal{F}_n, \forall (t_i)_{i \leq n} \in \mathcal{T}^n, f(t_1, \ldots, t_n) \in \mathcal{T}$$

Concrètement, c'est l'ensemble de tout ce qu'on peut construire en prenant les constantes, les variables et les fonctions.

♦ **Exemple**

Dans le langage des groupes, $^{-1}(\circ(1, x))$ est un terme, mais $= (x, x)$ n'en est pas un.

Remarque : Suivant le contexte, certaines fonctions unaires seront notées de façon préfixe ou suffixe, et certaines relations et fonctions binaires de façon infixe. On écrira donc plutôt $(x \circ 1)^{-1}$, mais on s'éloigne ici de la théorie, on change juste l'écriture des termes.

Définition 1.3 (*Formules*)

Soit $\mathcal{L}$ un langage, $\mathcal{T}$ l'ensemble des termes sur $\mathcal{L}$. L'ensemble des $\mathcal{L}$-*formules* $\mathfrak{F}$ est le plus petit ensemble qui vérifie

- $\mathfrak{F}$ contient les formules atomiques, de la forme $R(t_1 \ldots t_n)$:

$$\forall n, \forall R \in \mathcal{R}_n, \forall (t_i)_{i \leq n} \in \mathcal{T}^n, R(t_1, \ldots, t_n) \in \mathfrak{F}$$

- $\mathfrak{F}$ est clos par combinaisons booléennes :

$$\forall \phi, \psi \in \mathfrak{F}, (\phi \wedge \psi) \in \mathfrak{F}$$

$$\forall \phi, \psi \in \mathfrak{F}, (\phi \vee \psi) \in \mathfrak{F}$$
$$\forall \phi \in \mathfrak{F}, \neg \phi \in \mathfrak{F}$$

- $\mathfrak{F}$ est clos par quantificateurs existentiels et universels : Quelles que soient $x \in \mathcal{V}$ et $\phi \in \mathfrak{F}$, $\exists x \phi$ et $\forall x \phi$ sont dans $\mathfrak{F}$

L'ajout des parenthèses pour les quantificateurs est là pour avoir unicité de l'écriture : Il y a plusieurs façons de comprendre la formule $\phi \wedge \psi \wedge \theta$, mais une seule façon de lire $((\phi \wedge \psi) \wedge \theta)$. Ceci fait l'objet du **Théorème de lecture unique**, dont nous ne donnerons pas la démonstration, celle-ci présentant peu d'intérêt dans ce cours. Ce théorème permet entre autres de faire des raisonnements (et des définitions) par *induction* sur la structure des formules et des termes.

Certaines des variables que nous manipulons peuvent être libres, c'est à dire qui ne sont pas associées à un quantificateur. Définissons cette notion :

Définition 1.4 (*Variables libres*)

On définit inductivement la notion de variable libre d'une formule ϕ par

- Les variables libres d'une formule atomique sont les variables apparaissant dans cette formule
- Si $\phi = \psi \vee \theta$, ou $\phi = \psi \wedge \theta$, les variables libres de ϕ sont celles libres dans ψ ou dans θ
- Si $\phi = \neg\psi$, les variables libres de ϕ sont celles de ψ.
- Si $\phi = \exists x\psi$ (resp. $\forall x\psi$) les variables libres de ϕ sont celles de ψ privées de la variable x.

Notation Dans la suite du cours, on notera $\phi(\overline{x}) \in \mathfrak{F}$ pour dire que ϕ est une formule dont les variables libres sont précisément celles du n-uplet $\overline{x}$. On notera également ϕ plutôt que $\phi()$. On appelle *énoncé* une formule sans variable libre.

♦ Exemple

$\exists x = (x, y)$ est une formule dont la seule variable libre est y.

1.2 Sémantique, $\mathcal{L}$-structures

Nous n'avons défini pour l'instant que des mots sans signification, il faut pouvoir les interpréter dans différents cadres. La définition de $\mathcal{L}$-structures est le cadre naturel de cette interprétation

Définition 1.5 (*$\mathcal{L}$-structures*)

Soit $\mathcal{L}$ un langage. Une *$\mathcal{L}$-structure* $\mathfrak{M}$ est la donnée d'un ensemble M **non vide**, appelé domaine de $\mathfrak{M}$ et des élements suivants :

- Une fonction de $\mathcal{C}$ dans M, qui associe à chaque constante c un élement $f(c)$ du langage, plus souvent noté $c^{\mathfrak{M}}$
- Des fonctions de $\mathcal{F}_n$ dans M^{M^n}, qui associe à chaque fonction f n-aire une application de M^n dans M, notée $f^{\mathfrak{M}}$.
- Des fonctions de $\mathcal{R}_n$ dans M^n, qui associe à chaque relation R n-aire un sous-ensemble de M^n noté $R^{\mathfrak{M}}$. Cette fonction associe **toujours** à $=$ le sous-ensemble $\{(x, x), x \in M\}$

On associe grâce à la définition précédente un sens aux différents symboles. Il faut maintenant voir comment cela se généralise aux termes et aux formules

Définition 1.6 (*Interprétation d'un terme*)

Soit $\mathcal{L}$ un langage et $\mathfrak{M}$ une $\mathcal{L}$-structure. Soit $\overline{m}$ un uple d'élement de M. L'*interprétation* d'un terme $t(\overline{x})$ de *paramètre* $\overline{m}$, est définie inductivement par

- L'interprétation de $c \in \mathcal{C}$ est $c^{\mathfrak{M}}$.
- L'interprétation de $x \in \mathcal{V}$ est l'élement de $\overline{m}$ correspondant
- L'interprétation de $f(t_1, \dots t_n)$ est $f^{\mathfrak{M}}(t_1^{\mathfrak{M}} \dots t_n^{\mathfrak{M}})$, où $t_i^{\mathfrak{M}}$ désigne l'interprétation de t_i.

Cette définition est beaucoup plus simple qu'elle n'y paraît : elle veut simplement dire qu'il suffit de remplacer les variables par $\overline{m}$, et d'évaluer le terme en utilisant les règles valables dans $\mathfrak{M}$

♦ **Exemple**

Dans le langage $\mathcal{L}_{gp}$ des groupes :
- Avec $M = \mathbb{Z}$, 1 interprété par 0, $^{-1}$ comme opposé, et $\circ$ comme addition, l'interprétation de $t(x,y) : x^{-1} \circ y$ avec le paramètre $(2,3)$ est $-2+3$
- Avec $M = \mathbb{Z}$, 1 interprété par -4, $^{-1}$ la fonction identité, et $\circ$ la multiplication, l'interprétation de $t(x,y) : x^{-1} \circ y$ avec le paramètre $(2,3)$ est 2×3

De même qu'on a noté $\mathcal{L}_{gp} = \{1,^{-1}, \circ\}$, on notera souvent un modèle par son domaine et ses interprétations, de sorte que les exemples s'écriraient $\mathfrak{M} = (\mathbb{Z}, 0, -, +)$ et $\mathfrak{M} = (\mathbb{Z}, -4, \mathrm{id}, \times)$.

Comme le second exemple l'indique bien, il ne s'agit ici pour l'instant que d'un langage des groupes, pas d'une théorie des groupes, il est donc naturel qu'on puisse interpréter à notre convenance les deux opérateurs. Pour que la $\mathcal{L}$-structure soit un groupe, il faudrait rajouter des conditions, comme $\forall x, x \circ 1 = x$. La *théorie* nous permettra bientôt de préciser la manière de procéder.

Définissons maintenant la satisfaction d'une formule :

Définition 1.7 (*Satisfaction d'une formule*)

Soit $\mathcal{L}$ un langage et $\mathfrak{M}$ une $\mathcal{L}$-structure. Soit $\overline{m}$ un uple d'élement de M. La *satisfaction* d'une formule $\phi(\overline{x})$ de *paramètre* $\overline{m}$, est définie inductivement par :

- Si $\phi(\overline{m})$ est une formule atomique $R(t_1, \dots t_m)$, $\phi(\overline{m})$ est satisfaite si et seulement si $(t_1^{\mathfrak{M}}, \dots t_m^{\mathfrak{M}}) \in R$, où $t_i^{\mathfrak{M}}$ désigne l'interprétation de t_i avec le paramètre $\overline{m}$
- Si $\phi = \phi_1 \wedge \phi_2$, ϕ est satisfaite si et seulement si ϕ_1 et ϕ_2 sont satisfaites.
- Si $\phi = \phi_1 \vee \phi_2$, ϕ est satisfaite si et seulement si ϕ_1 ou ϕ_2 est satisfaite.
- Si $\phi = \neg\psi$, ϕ est satisfaite si et seulement si ψ n'est pas satisfaite.
- Si $\phi(\overline{x}) = \exists y \psi(\overline{x}, y)$, ϕ est satisfaite dans $\mathfrak{M}$ pour le paramètre $\overline{m}$ si et seulement si il existe $y \in M$ tel que ψ soit satisfaite pour le paramètre $\overline{m}, y$.
- Si $\phi(\overline{x}) = \forall y \psi(\overline{x}, y)$, ϕ est satisfaite pour le paramètre $\overline{m}$ si et seulement si quel que soit $y \in M$, ψ est satisfaire pour le paramètre $\overline{m}, y$.

Lorsque $\phi(\overline{x})$ est satisfaite dans $\mathfrak{M}$ avec le paramètre $\overline{m}$, on utilise la notation $\mathfrak{M} \models \phi(\overline{m})$, qui se lit : $\mathfrak{M}$ satisfait $\phi(\overline{m})$.

Là encore, cette définition donne juste le sens souhaité aux formules : on interprète les symboles booléens de façon usuelle, on interprète les relations, et on regarde si la formule finale est vérifiée.

♦ **Exemple**

- Dans la première structure, $\forall x, x \circ 1 = x$ est vérifiée, mais$\exists x, \exists y, (x \circ x = x) \wedge (y \circ y = y) \wedge \neg(x = y)$ n'est pas vérifiée.
- Dans la seconde structure, $\forall x, x \circ 1 = x$ n'est pas vérifiée, mais$\exists x, y, (x \circ x = x) \wedge (y \circ y = y) \wedge \neg(x = y)$ est vérifiée.

Dès ce premier exemple qui utilise les symboles booléens, on remarque tout de suite que certains parenthèses ont été supprimées. Elles sont, en toute rigueur, obligatoires, mais lorsque la formule est compréhensible sans celles-ci (i.e Tout être humain sensé l'interprétera de la même façon), on les supprimera.

Lorsqu'on travaille dans une structure donnée $\mathfrak{M}$, on peut également définir la notion de formule ϕ a paramètres : on s'autorise alors l'utilisation d'éléments de M dans la formule. Par exemple la formule $\phi(x)\,:\,3 \circ x = 9$ est une formule dans $\mathbb{Z}$ utilisant les paramètres 3 et 9. On écrit souvent $\phi(\overline{x}, \overline{a})$ pour une formule dont les variables libres sont $\overline{x}$ et les paramètres $\overline{a}$.

Définissons maintenant la notion de *formules équivalentes*

Définition 1.8 (*Formules équivalentes*)

> Deux formules $\phi(\overline{x})$ et $\psi(\overline{x})$ sont équivalentes, si et seulement si quelque soit la $\mathcal{L}$-structure $\mathfrak{M}$, et $\overline{m}$ un paramètre dans M, $\mathfrak{M}$ satisfait $\phi(\overline{m})$ si et seulement si $\mathfrak{M}$ satisfait $\psi(\overline{m})$.

Cette définition est typique des procédés utilisés en théorie des modèles : L'équivalence entre formule logique n'est ici pas un critère syntaxique, mais défini à travers les modèles. De sorte qu'il n'est pas évident a priori de décider si deux formules équivalentes.

Après toutes ces définitions, la première proposition, triviale il est vrai, peut enfin être énoncée :

Proposition 1.1

> Pour tout ϕ et ψ,les couples de formules suivants sont équivalents :
>
> - ϕ et $\neg\neg\phi$
> - $\neg(\phi \wedge \psi)$ et $(\neg\phi \vee \neg\psi)$
> - $\neg(\phi \vee \psi)$ et $(\neg\phi \wedge \neg\psi)$
> - $\neg\exists x\phi$ et $\forall x\neg\phi$
> - $\neg\forall x\phi$ et $\exists x\neg\phi$

Cette proposition est relativement évidente, et sera laissée en exercice. Remarquons toutefois que les deux dernières propositions ne peuvent s'établir qu'en supposant que les $\mathcal{L}$-structures sont non vides, ce qui est bien le cadre dans lequel nous nous sommes placés.

Notation Dans la suite, nous utiliserons les notations abrégées $\phi \implies \psi$ pour $\psi \vee \neg\phi$ et $\phi \iff \psi$ pour $(\phi \implies \psi) \wedge (\psi \implies \phi)$. Il ne s'agit, là encore, que d'une convention d'écriture.

1.3 Théorie et modèles d'une théorie

Le cadre est maintenant fixé pour définir ce qu'est précisément un modèle.

Définition 1.9 (*Théorie*)

> Soit $\mathcal{L}$ un langage, T un ensemble d'énoncés sur $\mathcal{L}$. T est une *théorie* si et seulement si il existe une $\mathcal{L}$-structure $\mathfrak{M}$ telle que
>
> $$\forall \phi \in T, \mathfrak{M} \models \phi$$
>
> Dans ce cas, $\mathfrak{M}$ est appelé un modèle de T.

En d'autres termes, une théorie est un ensemble d'énoncés *cohérent*, au sens où il existe une structure qui les réalisent simultanément.

♦ **Exemple**

La première structure est un modèle de la *théorie des groupes*, c'est à dire la théorie constituée des énoncés :
- $\forall x, x \circ 1 = x$
- $\forall x, x \circ x^{-1} = 1$
- $\forall x, x^{-1} \circ x = 1$
- $\forall x, y, z (x \circ y) \circ z = x \circ (y \circ z)$

Une autre théorie qui sera souvent utilisée dans les exemples est la *théorie des ordres*, dont le langage ne contient qu'une relation $<$ et dont les énoncés sont :
- $\forall x \neg(x < x)$
- $\forall x, y\ (x < y) \implies \neg(y < x)$
- $\forall x, y, z\ (x < y) \wedge (y < z) \implies (x < z)$

La *théorie des ordres totaux* est la théorie des ordres enrichie de l'axiome

$$\forall x, y (x < y) \vee (y < x) \vee (y = x)$$

On appelle *chaîne* tout modèle de cette théorie.

Notation $T \models \phi$ si et seulement si $\mathfrak{M} \models \phi$ pour tout modèle $\mathfrak{M}$ de T.

En d'autres termes, $T \models \phi$ si le fait que ϕ soit vraie ne dépend que de la théorie et non pas du modèle de la théorie.

La proposition suivante, dont la démonstration est immédiate, sera utile par la suite :

Proposition 1.2

Avec les mêmes notations que précédemment, $\phi \in T \implies T \models \phi$

Attention $T \not\models \phi$ est différent de $T \models \neg\phi$. Le premier signifie qu'il existe un modèle de T qui ne satisfait pas ϕ (donc qui satisfait $\neg\phi$), le second signifie que tous les modèles de T satisfont $\neg\phi$. La distinction disparaît pour une *théorie complète*

Définition 1.10 (*Théorie complète*)

Soit T une théorie. T est une théorie complète ssi

$$\forall \phi, T \models \phi \text{ ou } T \models \neg\phi$$

ou, de façon équivalente

$$\forall \phi, T \not\models \phi \implies T \models \neg\phi$$

1.4 Diagrammes

À chaque $\mathcal{L}$-structure, on peut associer l'ensemble des formules vraies dans cette structure, c'est le sens de la définition suivante

Définition 1.11 (*$\mathcal{L}(A)$-théorie*)

Soit $\mathfrak{M}$ une $\mathcal{L}$-structure, et A un sous-ensemble de M. On appelle $\mathcal{L}(A)$-théorie de $\mathfrak{M}$, notée $\mathrm{Th}(\mathfrak{M}, A)$ l'ensemble des formules à paramètres dans A satisfaites par $\mathfrak{M}$.

Dans le cas où $A = M$, $\mathrm{Th}(\mathfrak{M}, A)$ est appelé le *diagramme élémentaire* de $\mathfrak{M}$.

On appelle *diagramme* de $\mathfrak{M}$, noté $\Delta_{\mathfrak{M}}$, les formules du diagramme élémentaire sans quantificateurs.

Remarque : Il faut faire très attention à bien comprendre la définition : La théorie $\mathrm{Th}(\mathfrak{M}, A)$ est dans le langage $\mathcal{L}(A)$ et non dans le langage $\mathcal{L}$: On a ajouté au langage tous les éléments de A, considérés comme des constantes c_a, et on les interprète dans $\mathfrak{M}$ par les éléments de A correspondants (on note quelquefois $\mathfrak{M}_A$ la nouvelle structure).

On s'aperçoit ainsi immédiatement $\mathfrak{M}_A$ est un modèle de $\mathrm{Th}(\mathfrak{M}, A)$ (ce qui justifie l'apppellation de théorie).

Notation on écrit $\mathrm{Th}(\mathfrak{M})$ au lieu de $\mathrm{Th}(\mathfrak{M}, \emptyset)$.

On a enfin la première proposition intéressante :

Proposition 1.3

Soit $\mathfrak{M}$ une $\mathcal{L}$-structure, et A un sous-ensemble de M. La $\mathcal{L}(A)$-théorie de $\mathfrak{M}$ est une théorie complète.

Preuve : Soit ϕ une formule. Supposons que $\mathrm{Th}(\mathfrak{M}, A) \not\models \phi$. On veut montrer que $\mathrm{Th}(\mathfrak{M}, A) \models \neg\phi$. Comme $\mathrm{Th}(\mathfrak{M}, A) \not\models \phi$, $\phi \notin \mathrm{Th}(\mathfrak{M}, A)$. Par définition de $\mathrm{Th}(\mathfrak{M}, A)$, $\mathfrak{M}_A \not\models \phi$. Donc $\mathfrak{M}_A \models \neg\phi$, et finalement $\neg\phi \in \mathrm{Th}(\mathfrak{M}, A)$ ce qui entraîne $\mathrm{Th}(\mathfrak{M}, A) \models \neg\phi$. ■

Exercices

(1 - 1) Démontrer la proposition 1.1

(1 - 2) Ecrire les formules signifiant :

- ϕ_n : La structure a au moins n éléments
- ψ_n : La structure a au plus n éléments
- E_n : La formule a exactement n éléments

(1 - 3) Montrer qu'une théorie qui admet (au moins) deux modèles finis dont le cardinal est différent n'est pas complète.

(1 - 4) Soit $n > 1$ un entier. Montrer que la théorie des groupes finis à n^2 éléments dans le vocabulaire $(1, \cdot, ^{-1})$ n'est pas complète.

(1 - 5) On se place dans le langage des groupes. Soit G un groupe, $g \in G$ et ϕ une formule telle que $G \models \phi(g)$.

Q 1) Montrer que $G \models \phi(g^{-1})$.

Q 2) Soit $p \in G$. Montrer que $G \models \phi(pgp^{-1})$.

(1 - 6) On considère le langage $\{R, a, b\}$ où R est un prédicat binaire et a, b des constantes, et la théorie :

- $\forall x, y\ R(x, y) \iff R(y, x)$
- $\forall x\ R(x, x)$
- $\forall x\ R(a, x) \vee R(b, x)$
- $\exists x, y\ \neg R(a, x) \wedge \neg R(x, y) \wedge \neg R(y, b)$
- $a \neq b$
- $R(a, b)$

Q 1) Montrer que tout modèle de la théorie a au moins 4 éléments.

Q 2) Donner un modèle de cardinal n pour tout $n \geq 4$.

Q 3) Montrer que la formule $\forall c, d\ \exists x, y\ R(c, x) \wedge R(x, y) \wedge R(y, d)$ est une conséquence de la théorie.

(1 - 7) On se place dans le langage contenant tous les $\{V_i\}$ (prédicats zero-aires) et dans la théorie $E_n \iff V_n$ où E_n est défini comme plus haut.

Q 1⋆) Soit $\phi(\overline{x}, y)$ une formule sans quantificateurs. Montrer que $\exists y \phi(\overline{x}, y)$ est équivalente à une formule sans quantificateurs.

Q 2) En déduire que toute formule $\phi(\overline{x})$ est équivalente à une formule sans quantificateurs.

Q 3) En déduire que s'il existe une infinité de n tel que ϕ est vraie pour tout modèle de cardinal n, alors il existe n_0 tel que ϕ est vrai pour tout modèle de cardinal $m > n_0$ (en particulier pour un modèle infini).

On se place maintenant dans le langage vide (on a donc juste l'égalité)

Q 4) Montrer que toute formule ϕ est équivalente à une combinaison booléenne de E_i.

Q 5) En déduire que l'ensemble des cardinaux (finis) des modèles qui vérifient ϕ est soit fini soit cofini.

(1 - 8) Soit Φ et Ψ deux théories.

Q 1) Construire une théorie Θ tel que $\mathfrak{M}$ est modèle de Θ si et seulement si $\mathfrak{M}$ est modèle de Φ et modèle de Ψ.

Q 2) Construire une théorie Θ tel que $\mathfrak{M}$ est modèle de Θ si et seulement si $\mathfrak{M}$ est modèle de Φ ou modèle de Ψ.

Q 3) Montrer qu'il n'existe pas toujours de Θ tel que $\mathfrak{M}$ est modèle de Θ si et seulement si $\mathfrak{M}$ n'est pas modèle de Φ (on pourra utiliser l'exercice précédent)

(1 - 9) On considère le langage (R, B, f), où R et B sont des prédicats unaires et f une fonction unaire. Considérons la théorie donnée par les axiomes :

- $\forall x, R(x) \iff \neg B(x)$
- $\forall x, y, f(x) = f(y) \implies x = y$
- $\forall x, R(x) \iff B(f(x))$

Q 1) Trouver un modèle de la théorie

Q 2) Montrer $\forall x, B(x) \iff R(f(x))$

Q 3) Montrer que tout modèle fini de la théorie est de cardinal pair

Q 4) Montrer que la théorie n'est pas complète

(1 - 10) *(Définissabilité)* On se place dans la structure des entiers naturels $\mathbb{N}$. Les différents symboles du langage auront leur interprétation habituelle. On se place dans le langage $\{\times, <\}$ et dans la structure $\mathbb{N}$ où les symboles sont interprétés de la manière usuelle.

Q 1$\star$) Dans le langage $\{\times, S\}$, où S désigne la fonction successeur, montrer qu'il existe une formule $\phi(x, y, z)$ telle que $\mathbb{N} \models \phi(a, b, c)$ si et seulement si $a + b = c$.

Q 2) Même question dans le langage $\{\times, <\}$

(1 - 11) On considère le langage $\{\top, \nabla, \oplus, \otimes\}$, les deux premiers symboles étant des constantes et les deux derniers des fonctions d'arité 2, représentées de façon infixe. Considérons la théorie formée des axiomes :

- $\forall x, \forall y, x \oplus y = y \oplus x$
- $\forall x, \forall y, x \otimes y = y \otimes x$
- $\forall x, \forall y, \forall z (x \oplus y) \oplus z = x \oplus (y \oplus z)$
- $\forall x, \forall y, \forall z (x \otimes y) \otimes z = x \otimes (y \otimes z)$
- $\forall x, \forall y, \forall z, x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$
- $\forall x, (x \oplus x) \oplus x = \top$
- $\forall x, x \otimes x = \nabla$

Q 1) Trouver un modèle de cette théorie (Chercher un modèle à un seul élément)

Q 2) Montrer que tout modèle de cette théorie vérifie :
- $\top \oplus \top = \top$
- $\top \oplus \nabla = \nabla$
- $\top = \nabla$
- $\forall x, x \otimes \top = \top$

Q 3) Considérons la structure $(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$, où les symboles sont interprétés par :
- $\top = \nabla = (0, 0)$
- $\forall x_1, x_2, \forall y_1, y_2, (x_1, x_2) \oplus (y_1, y_2) = (x_1 + y_1, 0)$
- $\forall x_1, x_2, \forall y_1, y_2, (x_1, x_2) \otimes (y_1, y_2) = (0, x_2 \times y_2)$

Montrer que cette structure est bien modèle de la théorie

Q 4) En déduire que la théorie n'est pas complète.

(1 - 12) On se place dans le langage $\{+, -, \times, 0, 1, <\}$ et on considère un modèle $\mathfrak{M} \supsetneq \mathbb{R}$ du diagramme élémentaire de $\mathbb{R}$. Il s'agit donc d'une structure qui contient $\mathbb{R}$ et qui vérifie exactement les mêmes énoncés à paramètres dans $\mathbb{R}$. L'existence d'un tel modèle sera prouvé dans le chapitre 3.

On appelle réel non standard un élément de $M - \mathbb{R}$.

Q 1) Montrer qu'il existe un réel non standard $\epsilon > 0$ vérifiant

$$\forall x \in \mathbb{R}, x > 0 \to \epsilon > x$$

On appelle un tel nombre un infinitésimal.

Q 2) Montrer que la somme de deux infinitésimaux est soit 0 soit un infinitésimal

Q 3) Montrer que le produit d'un réel et d'un infinitésimal est soit 0 soit un infinitésimal

Q 4) Soit p un polynôme à coefficients dans $\mathbb{R}$. Soit x un réel, et ϵ un infinitésimal. Montrer qu'il existe un infinitésimal α tel que

$$\frac{p(x+\epsilon) - p(x)}{\epsilon} = p'(x) + \alpha$$

Chapitre 2

EQUIVALENCES ENTRE MODÈLES

Lorsqu'on dispose de deux modèles d'une même théorie, il est souvent intéressant de savoir quelles propriétés ils partagent. Nous allons également introduire ici les définitions communes à presque tous les formalismes mathématiques : La notion de sous-structure, et la notion de morphisme.

2.1 Équivalence élémentaire

Définition 2.1 (*Equivalence élémentaire*)

Deux $\mathcal{L}$-structures $\mathfrak{M}$ et $\mathfrak{N}$ sont dites *élementairement équivalentes* , ce qu'on note $\mathfrak{M} \equiv \mathfrak{N}$ si ces structures satisfont les mêmes énoncés, c'est à dire :

$$\forall \phi,\ \mathfrak{M} \models \phi \iff \mathfrak{N} \models \phi$$

La notion de $\mathcal{L}$-théorie vue plus haut permet de donner un autre point de vue :

Proposition 2.1

Deux $\mathcal{L}$-structures sont élémentairement équivalentes si et seulement si $Th(\mathfrak{M}) = Th(\mathfrak{N})$

La démonstration est immédiate.

2.2 Lien avec la complétude des théories

Le fait que deux $\mathcal{L}$-structures soient élementairement équivalentes est très lié avec le fait que la théorie sous-jacente soit complète. Nous avons en effet la proposition suivante :

Proposition 2.2

Deux $\mathcal{L}$-structures sont élémentairement équivalentes si et seulement si elles sont deux modèles d'une même théorie complète

Preuve : [$\Rightarrow$] Si deux structures $\mathfrak{M}$ et $\mathfrak{N}$ sont élementairement équivalentes, elles sont modèles de la théorie $Th(\mathfrak{M}) = Th(\mathfrak{N})$ (2.1) qui est complète d'après la proposition (1.3).
[$\Leftarrow$] Soit deux structures $\mathfrak{M}$ et $\mathfrak{N}$ modèles de T complète. Soit ϕ tel que $\mathfrak{M} \models \phi$. Alors $\mathfrak{M} \models \neg\neg\phi$, donc $\mathfrak{M} \not\models \neg\phi$. Alors $T \not\models \neg\phi$, donc $T \models \neg\neg\phi$, puisque T est complète. Comme $\mathfrak{N}$ est un modèle de cette théorie, on en déduit $\mathfrak{N} \models \neg\neg\phi$, et $\mathfrak{N} \models \phi$. La seconde implication est analogue. ■

Cette proposition peut aussi s'énoncer, d'un point de vue dual, sous la forme

Proposition 2.3

Une théorie est complète si et seulement si tous ses modèles sont élémentairement équivalents.

L'intérêt de la proposition est considérable, en effet la principale méthode pour démontrer que deux modèles sont élementairement équivalents est justement de trouver une théorie dont elles sont modèle, et de montrer que la théorie est complète.

♦ **Exemple**

- Pour le langage des ordres, $(\mathbb{Q},<)$ et $(\mathbb{R},<)$ sont élementairement équivalents ND . On démontre pour cela que la théorie des ordres denses sans extrêmité est complète ND .
- Pour le langage des ordres, $(\mathbb{Q},<)$ et $(\mathbb{Z},<)$ ne sont pas élementairement équivalents. En effet,la formule

$$\phi : \forall x, y\ (x < y) \implies \exists z x < z \wedge z < y$$

  est vraie dans la première structure et non dans la seconde. On en déduit que la théorie T des ordres n'est pas complète puisque $T \not\models \phi$ et $T \not\models \neg\phi$.

Comme on le voit dans ces exemples, il est souvent assez facile de prouver que deux modèles ne sont pas élémentairement équivalents mais il est plus difficile de montrer qu'une théorie est complète, puisqu'il faut à priori chercher pour toutes les formules si celles-ci sont vérifiées ou non.

2.3 Sous-structures

On définit de façon assez naturelle les sous-structures

Définition 2.2 (*Sous-structure*)

Soit $\mathfrak{N}$ une $\mathcal{L}$-structure. Une *sous-structure* de $\mathfrak{N}$ est la $\mathcal{L}$-structure $\mathfrak{M}$ définie par

- M est un sous-ensemble de N.
- L'interprétation des fonctions et des relations est la restriction à M de leur interprétation dans $\mathfrak{N}$. Bien entendu, cela implique que M est stable par les fonctions.

On écrit alors $\mathfrak{M} \subseteq \mathfrak{N}$.

Définition 2.3 (*Sous-structure élémentaire*)

$\mathfrak{M} \subseteq \mathfrak{N}$ est une sous-structure élémentaire si et seulement si pour toute formule $\phi(\overline{m})$ à paramètres dans $\mathfrak{M}$, $\mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\overline{m})$. On note alors $\mathfrak{M} \prec \mathfrak{N}$

Bien entendu, une sous-structure élémentaire $\mathfrak{M}$ d'une structure $\mathfrak{N}$ est une sous-structure qui est élémentaire équivalente à $\mathfrak{N}$, mais la condition exprimée ci-dessus est même plus forte. Par exemple, $(\mathbb{Z}\times\mathbb{Z},<_{\text{lex}})$ et $(\mathbb{Z}\times 1,<_{\text{lex}})$ sont deux structures élémentairement équivalentes ND , la seconde est une sous-structure de la première, et pourtant elle n'est pas une sous-structure élémentaire, puisque la formule $\phi : \exists x, x < (0,1)$ est vraie dans la première structure mais pas dans la seconde.

2.4 Morphismes

2.4.1 Définition

Il s'agit ici de la notion habituelle de morphisme, semblable à toutes celles rencontrées habituellement en mathématiques.

Définition 2.4 (*$\mathcal{L}$-morphisme*)

Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathcal{L}$-structures. Un *$\mathcal{L}$-morphisme* de $\mathfrak{M}$ dans $\mathfrak{N}$ est une application σ de M dans N qui est stable par les différentes opérations, c'est à dire :

- Stabilité pour les constantes :

$$\forall c \in \mathcal{C}, \sigma(c^{\mathfrak{M}}) = c^{\mathfrak{N}}$$

- Stabilité pour les fonctions :

$$\forall f \in \mathcal{F}_n, \forall m_i \in M^n, \sigma\left(f^{\mathfrak{M}}(m_1, \ldots m_n)\right) = f^{\mathfrak{N}}(\sigma(m_1) \ldots \sigma(m_n))$$

- Stabilité pour les relations :

$$\forall R \in \mathcal{R}_n, \forall m_i \in M^n, (m_1, \ldots m_n) \in R^{\mathfrak{M}} \iff \sigma(m_1 \ldots m_n) \in R^{\mathfrak{N}}$$

♦ **Exemple**

Les morphismes de deux $\mathcal{L}$-modèles de la théorie des groupes sont les morphismes de groupes injectifs ND , Les morphismes de deux $\mathcal{L}$-modèles de la théorie des ordres sont les fonctions strictement croissantes.

Pourquoi ce "injectif" dans l'exemple ? Cela provient de la préservation de la relation =, et c'est l'objet de la proposition suivante

Proposition 2.4

Tout $\mathcal{L}$-morphisme est injectif

Preuve : Soit $m, m' \in M$ tel que $\sigma(m) = \sigma(m')$. Alors $(\sigma(m), \sigma(m')) \in =^{\mathfrak{N}}$, donc par définition d'un $\mathcal{L}$-morphisme, $(m, m') \in =^{\mathfrak{M}}$, et $m = m'$. ∎

La notion assez naturelle d'isomorphisme apparaît alors

Définition 2.5 (*$\mathcal{L}$-isomorphisme*)

Un $\mathcal{L}$-isomorphisme est un $\mathcal{L}$-morphisme surjectif.

2.4.2 Morphismes élémentaires

Les morphismes ne préservent pas nécessairement la satisfaction des formules. Ainsi, il existe une injection canonique de $(\mathbb{Z}, <)$ dans $(\mathbb{Q}, <)$, mais $(\mathbb{Z}, <)$ n'en est pas pour autant restriction élémentaire de $(\mathbb{Q}, <)$. On introduit alors la notion de *morphisme élémentaire*.

Définition 2.6 (*Morphisme élémentaire*)

Un $\mathcal{L}$-morphisme entre $\mathfrak{M}$ et$\mathfrak{N}$ est élémentaire si et seulement si

$$\forall \phi \in \mathfrak{F}, \forall \overline{m} \in M, \mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\sigma(\overline{m}))$$

Une autre caractérisation des sous-structures élémentaires se déduit de la définition :

Proposition 2.5

Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathcal{L}$-structures telles que $M \subset N$. Alors $\mathfrak{M}$ est une sous-structure élémentaire de $\mathfrak{N}$ si et seulement si l'injection canonique $M \hookrightarrow N$ est un $\mathcal{L}$-morphisme élémentaire.

Nous avons alors la proposition fondamentale suivante

Proposition 2.6

Un $\mathcal{L}$-isomorphisme est élémentaire.

Preuve : C'est notre première preuve par induction, écrivons donc là proprement.Montrons donc par induction sur la structure de $\phi(\overline{m})$ que

$$\mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\sigma(\overline{m}))$$

- Si ϕ est atomique, $\phi = R(m_1 \dots m_n)$. Alors

$$\begin{aligned} \mathfrak{M} \models \phi(m_1 \dots m_n) &\iff (m_1 \dots m_n) \in R^{\mathfrak{M}} \\ &\iff (\sigma(m_1) \dots \sigma(m_n)) \in R^{\mathfrak{N}} \\ &\iff \mathfrak{N} \models \phi(\sigma(m_1), \sigma(m_n)) \end{aligned}$$

- Si $\phi = \phi_1 \wedge \phi_2$. Alors

$$\begin{aligned} \mathfrak{M} \models \phi &\iff \mathfrak{M} \models \phi_1 \text{ et } \mathfrak{M} \models \phi_2 \\ &\iff \mathfrak{N} \models \phi_1 \text{ et } \mathfrak{N} \models \phi_2 \quad \text{Par hypothèse d'induction} \\ &\iff \mathfrak{N} \models \phi \end{aligned}$$

- Si $\phi = \phi_1 \vee \phi_2$, la preuve est similaire
- Si $\phi = \neg\psi$,

$$\begin{aligned} \mathfrak{M} \models \phi &\iff \mathfrak{M} \not\models \psi \\ &\iff \mathfrak{N} \not\models \psi \quad \text{Par hypothèse d'induction} \\ &\iff \mathfrak{N} \models \phi \end{aligned}$$

- Si $\phi = \exists x \psi(x)$. Supposons $\mathfrak{M} \models \phi$. Alors il existe $x \in \mathfrak{M}$, tel que $\mathfrak{M} \models \psi(x)$. Alors $\mathfrak{N} \models \psi(\sigma(x))$ par hypothèse d'induction, donc $\mathfrak{N} \models \phi$. Réciproquement, si $\mathfrak{N} \models \phi$, il existe $x \in \mathfrak{N}$, $\mathfrak{N} \models \psi(x)$. Alors $\mathfrak{M} \models \phi(\sigma^{-1}(x))$, donc $\mathfrak{M} \models \phi$.
- Le cas du quantificateur universel est similaire au précédent. ■

Notons que les premiers points de la démonstration n'utilisent pas la bijectivité de σ on en déduit

Proposition 2.7

Un $\mathcal{L}$-morphisme préserve les formules sans quantificateurs.

2.4.3 Diagrammes

On peut réécrire la proposition précédente de la façon suivante :

Proposition 2.8

Si σ est un $\mathcal{L}$-morphisme de $\mathfrak{M}$ dans $\mathfrak{N}$, alors $\mathfrak{N}$ est un modèle de $\Delta_{\mathfrak{M}}$, le diagramme de $\mathfrak{M}$.

Mieux :

Lemme 2.9 (*Premier lemme du diagramme*)

Il existe un $\mathcal{L}$-morphisme de $\mathfrak{M}$ dans $\mathfrak{N}$ si et seulement si $\mathfrak{N}$ peut être étendue en un modèle de $\Delta_{\mathfrak{M}}$, le diagramme de $\mathfrak{M}$

Il faut comprendre dans l'expression "peut être étendue" le fait qu'on étende la structure $\mathfrak{N}$ en donnant des interprétations à toutes les constantes c_i pour $i \in M$.

Preuve : Si σ est un $\mathcal{L}$-morphisme de $\mathfrak{M}$ dans $\mathfrak{N}$, il suffit d'interpréter chaque constante c_i pour i dans M par $\sigma(i)$. Réciproquement, si $\mathfrak{N}$ es tun modèle de $\Delta_{\mathfrak{M}}$, l'application $\sigma : i \mapsto c_i$ est un $\mathcal{L}$-morphisme. ■

On a un résultat similaire en ce qui concerne les morphismes élémentaires :

Lemme 2.10 (*Second lemme du diagramme*)

Il existe un $\mathcal{L}$-morphisme élémentaire de $\mathfrak{M}$ dans $\mathfrak{N}$ si et seulement si $\mathfrak{N}$ peut être étendue en un modèle de $\mathrm{Th}(\mathfrak{M}, M)$, le diagramme élémentaire de $\mathfrak{M}$.

La preuve est laissée au lecteur.

2.5 Test de Tarski

Vérifier qu'une sous-structure est élémentaire revient à montrer qu'une même formule est vérifiée dans deux structures différentes. Le test de Tarski est là pour obtenir une condition plus facile d'utilisation

Théorème 2.11 (*Test de Tarski*)

Soit $\mathfrak{M}$ une sous-structure de $\mathfrak{N}$. $\mathfrak{M}$ est une sous-structure élémentaire de $\mathfrak{N}$ si et seulement si pour toute formule $\phi(x)$ à paramètres dans $\mathfrak{M}$ telle que $\mathfrak{N} \models \exists x \phi(x)$, il existe $m \in \mathfrak{M}$ tel que $\mathfrak{N} \models \phi(m)$.

Ce théorème signifie qu'une sous-structure est élémentaire si à chaque fois que je veux prouver une formule dans $\mathfrak{N}$ qui contient un $\exists x$, je peux prendre x dans la sous-structure.

Preuve : [$\Rightarrow$] Si $\phi(x)$ est à paramètres dans $\mathfrak{M}$ et vérifie $\mathfrak{N} \models \exists x \phi(x)$, alors comme $\mathfrak{M}$ est une sous-structure élémentaire, $\mathfrak{M} \models \exists x \phi(x)$, donc il existe m dans $\mathfrak{M}$ telle que $\mathfrak{M} \models \phi(m)$, et donc $\mathfrak{N} \models \phi(m)$. On peut représenter graphiquement cette preuve de la façon suivante :

$$\begin{array}{ccc}
\mathfrak{N} \models \exists x\phi(x) & \xrightarrow{\mathfrak{M}\prec\mathfrak{N}} & \mathfrak{M} \models \exists x\phi(x) \\
 & & \text{Définition de}\Big\downarrow\text{la satisfaction} \\
\text{il existe } m \in M, \mathfrak{N} \models \phi(m) & \xleftarrow{\mathfrak{M}\prec\mathfrak{N}} & \text{il existe } m \in M, \mathfrak{M} \models \phi(m)
\end{array}$$

[$\Leftarrow$] Montrons donc par induction sur la structure de $\phi(\overline{m})$ que

$$\mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\overline{m})$$

Pour tous les cas qui ne prennent pas en compte de quantificateurs, on peut reprendre la démonstration de la proposition 2.6. Ecrivons la preuve pour le quantificateur existentiel.

– $\mathfrak{M} \models \exists x\phi(x) \implies \mathfrak{N} \models \exists x\phi(x)$. On utilise l'hypothèse d'induction :

$$\begin{array}{ccc}
\mathfrak{M} \models \exists x\phi(x) & \xrightarrow[\text{la satisfaction}]{\text{Définition de}} & \text{il existe } m \in M, \mathfrak{M} \models \phi(m) \\
 & & \text{Hypothèse}\Big\downarrow\text{d'induction} \\
\mathfrak{M} \models \exists x\phi(x) & \xleftarrow[\text{la satisfaction}]{\text{Définition de}} & \text{il existe } m \in M, \text{ donc dans } N, \mathfrak{N} \models \phi(m)
\end{array}$$

– $\mathfrak{N} \models \exists x\phi(x) \implies \mathfrak{M} \models \exists x\phi(x)$. On utilise l'hypothèse du théorème.

$$\begin{array}{ccc}
\mathfrak{N} \models \exists x\phi(x) & \xrightarrow[\text{test de Tarski}]{\text{Hypothèse du}} & \text{il existe } m \in M, \mathfrak{N} \models \phi(m) \\
 & & \text{Hypothèse}\Big\downarrow\text{d'induction} \\
\mathfrak{M} \models \exists x\phi(x) & \xleftarrow[\text{La satisfaction}]{\text{Définition de}} & \text{il existe } m \in M, \mathfrak{M} \models \phi(m)
\end{array}$$

Le quantificateur universel se traite de manière similaire. ■

2.6 Skolemisation

Pour chaque formule $\exists x\phi(x)$ qui est vraie dans un modèle, on a l'existence d'un élément m de ce modèle tel que $\phi(m)$ soit satisfaite. La skolemisation revient en fait à faire rentrer ces éléments dans le langage.

Définition 2.7 (*Skolemisation d'une théorie*)

Soit T une $\mathcal{L}$-théorie. On considère, pour chaque formule $\phi(x, \overline{y})$ un nouveau symbole de fonction $f_\phi(\overline{y})$. On pose alors

$$\mathcal{L}_{\text{Skolem}} = \mathcal{L} \cup \{f_\phi : \phi \in \mathfrak{F}\}$$

La *skolemisation* T_{Skolem} de la théorie T est l'ensemble d'énoncés

$$T_{\text{Skolem}} = T \cup \{\exists x\phi(x, \overline{y}) \to \phi(f_\phi(\overline{y}), \overline{y}) : \phi \in \mathfrak{F}\}$$

En fait, les symboles qu'on rajoutent signifient : Si une formule $\exists x, \phi(x, \overline{y})$ est vraie, alors je peux trouver un tel x, c'est $f_\phi(\overline{y})$.

On a évidemment la propriété essentielle suivante :

Proposition 2.12

La skolémisation d'une théorie est bien une théorie. Plus précisément, tout modèle de T nous donne un modèle de T'.

La démonstration est intuitive, elle revient à dire que dès qu'on a une formule $\exists x, \phi(x, \overline{y})$ qui est vraie, on peut choisir un x qui la vérifie et alors on pose $f_\phi(\overline{y}) = x$. Si elle n'est pas vraie, on pose $f_\phi(\overline{y}) = m_0$, m_0 quelconque. Bien évidemment, cette démonstration est entièrement dépendante de l'*axiome du choix*.

Après un petit lemme, nous allons enfin pouvoir arriver au théorème intéressant.

Lemme 2.13

Soit $\mathfrak{N}$ une structure modèle de la théorie T_{skolem} et $A \subset N$. La clôture M de A par toutes les constantes, les fonctions de $\mathcal{F}$ et par les fonctions de Skolem est une sous-structure élémentaire pour le langage $\mathcal{L}$ de $\mathfrak{N}$. Si A ou $\mathcal{L}$ est infini, son cardinal est $|A| + |\mathcal{L}|$.

Preuve : M est évidemment une sous-structure. Elle vérifie le test de Tarski : En effet, supposons $\mathfrak{N} \models \exists x, \phi(x, y)$, alors $f_\phi(y) \in M$ est l'élément recherché. La preuve de cardinalité nécessite quelques connaissances de cardinaux infinis, et ne sera pas faite ici. ■

On en vient alors au premier théorème important

Théorème 2.14 (*Löwenheim-skolem descendant*)

Soit $\mathfrak{N}$ une $\mathcal{L}$-structure infinie, et $A \subset N$. Soit λ un cardinal infini tel que $|A|+|\mathcal{L}| \leq \lambda \leq |N|$. Alors il existe une sous-structure élémentaire $\mathfrak{M} \prec \mathfrak{N}$ contenant A de cardinal λ

Preuve : Quitte à augmenter A, on peut choisir $|A| = \lambda$. On choisit une skolemisation de $\mathfrak{N}$. Alors la clotûre de A est une sous-structure élémentaire de $\mathfrak{N}$, dont le cardinal est précisément λ, d'après le lemme précédent. ■

Remarque : Pour des cardinaux α, β infinis $\alpha + \beta = \alpha\beta = \max(\alpha, \beta)$

Une conséquence importante de ce théorème est la suivante :

Corollaire 2.15

Si une théorie de langage fini a un modèle infini, elle a un modèle dénombrable.

Et plus encore :

Théorème 2.16

Une théorie de langage fini ou dénombrable, dont tous les modèles dénombrables sont infinis et isomorphes et complète.

Une théorie dont tous les modèles dénombrables sont isomorphes est dite ω-catégorique. Cette proposition se généralise à la κ-catégoricité, comme nous le verrons au chapitre suivant.

Preuve : Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de la théorie. Ils sont infinis, donc en prenant $A = \emptyset$ et $\lambda = \omega$, on en déduit l'existence de structures $\mathfrak{M}' \prec \mathfrak{M}$ et $\mathfrak{N}' \prec \mathfrak{N}$. Par ω-catégoricité, $\mathfrak{M}'$ et $\mathfrak{N}'$ sont isomorphes, donc élémentairement équivalents, et donc $\mathfrak{M}$ et $\mathfrak{N}$ sont élémentairement équivalents. ■

2.7 Complétude des ordres denses avec extrêmités

Appliquons la proposition précédente pour établir une complétude.

Nous étudions ici la théorie des ordres totaux auquel on ajoute deux constantes $\top$ et $\perp$ et les axiomes :

- $\forall x, \forall y, x < y \implies \exists z, x < z \wedge z < y$
- $\forall x, x \neq \top \implies x < \top$
- $\forall x, x \neq \perp \implies \perp < x$
- $\perp < \top$

La première proposition précise que l'ordre est dense, les deux suivantes donnent les extrêmités. Enfin la dernière précise qu'il y a au moins deux éléments et, par densité, une infinité.

$([0,1], <)$ est l'exemple classique d'ordre dense avec extrêmités. Toutefois, nous utiliserons ici le *modèle dyadique*. Il s'agit de l'ensemble $\mathbb{D}$ des rationnels $\frac{p}{2^n} \in [0,1]$, p impair ou $p = 0$, $\perp$ interprété par 0, $\top$ par 1, et $<$ par $<$. Il s'agit bien entendu d'un ordre dense (prendre $z = \frac{x+y}{2}$) avec extrêmités (0 et 1).

Proposition 2.17

Tout ordre dense avec extrêmités dénombrable est isomorphe au modèle dyadique.

Corollaire 2.18

La théorie des ordres denses avec extrêmités est ω-catégorique.

Corollaire 2.19

La théorie des ordres denses avec extrêmités est complète.

Le corollaire est immédiat par application du précédent théorème. Construisons maintenant l'isomorphisme.

Preuve : Soit $\mathfrak{M}$ un modèle dénombrable de la théorie. On note

$$M = \{m_i, i \in \mathbb{N}\}$$

avec $m_0 = \perp$, $m_1 = \top$. On pose $d_0 = 0$ et $d_1 = 1$.

- Construisons par récurrence $d_i \in \mathbb{D}$ tels que

$$\forall i, j \leq n, d_i <^{\mathfrak{D}} d_j \iff m_i <^{\mathfrak{M}} m_j$$

Pour $n = 0, 1$, la relation est évidemment vérifiée. Sinon, soit $x = m_n$. Il existe alors deux indices $\lhd, \rhd < n$ tel que $m_\lhd$ soit le plus grand élément de

$$\left\{m_k <^{\mathfrak{M}} m_n, k < n\right\}$$

et $m_\triangleright$ est le plus petit élément de

$$\left\{m_n <^{\mathfrak{M}} m_k, k < n\right\}$$

(les ensembles considérés ne sont jamais vides, puisqu'ils contiennent au moins $\perp = m_0$ (resp $\top = m_1$)). On pose alors

$$d_n = \frac{d_\triangleleft + d_\triangleright}{2}$$

Evidemment $d_n \in \mathbb{D}$. Remarquons de plus que $d_\triangleleft < d_\triangleright$. Montrons que la propriété est vérifiée. En fait il y a juste à vérifier

$$\forall i < n, d_i <^{\mathfrak{D}} d_n \iff m_i <^{\mathfrak{M}} m_n$$

et

$$\forall i < n, d_n <^{\mathfrak{D}} d_i \iff m_n <^{\mathfrak{M}} m_i$$

Montrons la première propriété, la seconde se montrant de façon similaire.

- Supposons $m_i <^{\mathfrak{M}} m_n$. Alors $m_i \leq^{\mathfrak{M}} m_\triangleleft$. Par hypothèse de récurrence $d_i \leq^{\mathfrak{D}} d_\triangleleft$. Comme $d_\triangleleft < d_\triangleright$, on a alors $d_i <^{\mathfrak{D}} \frac{d_\triangleleft + d_\triangleright}{2}$, et on a terminé.
- Supposons $\neg(m_i <^{\mathfrak{M}} m_n)$. $m_i = m_n$ est impossible puisque $i \neq n$. On a donc $m_n <^{\mathfrak{M}} m_i$. Donc $m_\triangleright \leq^{\mathfrak{M}} m_i$. Par hypothèse de récurrence, on a alors $d_\triangleright \leq^{\mathfrak{D}} d_i$. Comme $d_\triangleleft < d_\triangleright$, on a alors $\frac{d_\triangleleft + d_\triangleright}{2} <^{\mathfrak{D}} d_i$, et donc on en déduit $\neg(d_i <^{\mathfrak{D}} \frac{d_\triangleleft + d_\triangleright}{2})$

- On pose alors

$$\phi : \begin{array}{ccc} M & \to & D \\ m_i & \mapsto & d_i \end{array}$$

Par construction, ϕ est un morphisme élémentaire de $\mathfrak{M}$ dans $\mathfrak{D}$. Il reste à montrer qu'il est surjectif. La preuve de surjectivité est technique mais relativement sans intérêt, nous laissons le lecteur s'en convaincre. ■

2.8 Définissabilité

Les formules du premier ordre permettent assez facilement de parler de parties définissables, ou de fonctions définissables.

Définition 2.8 (*Fonction définissable*)

Une fonction f est dite *définissable* pour la structure $\mathfrak{M}$ s'il existe une formule $\phi(\overline{a}, \overline{x}, y)$ telle que

$$f(\overline{x}) = y \iff \mathfrak{M} \models \phi(\overline{a}, \overline{x}, y)$$

On définit de même

Définition 2.9 (*Partie définissable*)

$I \subset M^n$ est une *partie définissable* s'il existe une formule $\phi(\overline{a}, \overline{x})$ tel que

$$\overline{x} \in M^n \iff \mathfrak{M} \models \phi(\overline{a}, \overline{x})$$

En fait, on peut donc introduire ces fonctions dans le langage, sans changer l'expressivité. (on peut cependant ainsi avoir des raccourcis d'écriture, ce qui peut-être important pour l'élimination des quanteurs, comme on le verra)

Exercices

(2 - 1) Montrer que $\prec$ est transitive.

(2 - 2) Soit $\mathfrak{M}$, $\mathfrak{N}$ et $\mathfrak{P}$ trois structures sur le même langage vérifiant

- $\mathfrak{M} \prec \mathfrak{P}$
- $\mathfrak{N} \prec \mathfrak{P}$
- $M \subset N$

Montrer que $\mathfrak{M} \prec \mathfrak{N}$

(2 - 3) Soit G_1, G_2 et G trois groupes. Montrer que si G_1 et G_2 sont élémentairement équivalents, il en est de même de $G_1 \times G$ et $G_2 \times G$. Montrer que la réciproque n'est pas toujours vraie.

(2 - 4) Montrer qu'on peut avoir $\mathfrak{M}_1 \prec \mathfrak{N}, \mathfrak{M}_2 \prec \mathfrak{N}$ avec $M_1 \cap M_2 \neq \emptyset$ sans avoir $\mathfrak{M}_1 \cap \mathfrak{M}_2 \prec \mathfrak{N}$.

(2 - 5) Donner un exemple d'une théorie *non complète* qui à n modèles dénombrables non élémentairement équivalentes (prendre un langage qui n'a que des constantes).

(2 - 6) On se place dans un langage vide (donc sans fonctions et dont le seul prédicat est l'égalité)

Q 1) Ecrire l'énoncé ϕ_n qui traduit l'existence d'au moins n éléments distincts.

Q 2) Montrer que la théorie $\{\phi_n, n > 0\}$ est complète.

(2 - 7) On se place dans un langage ne contenant qu'un prédicat binaire $\mathcal{R}$, représentant une relation et noté de manière infixe (on notera donc $x\mathcal{R}y$ plutôt que $\mathcal{R}(x, y)$)

Q 1) Ecrire les formules

- χ : $\mathcal{R}$ est une relation d'équivalence.
- $\phi_n(x)$: La classe d'équivalence de x a au moins n éléments.
- ψ_n : Il y a au moins n classes d'équivalence distinctes.

Q 2) A l'aide des formules précédentes, écrire un ensemble d'énoncés désignant une théorie qui a une infinité de classes d'équivalences, chacune d'entre elles étant infinie.

Q 3) On pose $\mathfrak{M} = (\mathbb{N} \times \mathbb{N}, \mathcal{R})$, où $\mathcal{R}$ est interprété par

$$(a, b)\mathcal{R}(c, d) \iff a = c$$

Montrer que $\mathfrak{M}$ est un modèle de la théorie considérée

Q 4) Montrer que cette théorie n'a qu'un modèle dénombrable
(ou encore : tous les modèles dénombrables sont isomorphes)

Q 5) En déduire que la théorie est complète.

On se donne dans la suite un entier $p > 0$.

Q 6) Ecrire les énoncés

- α_p : Chaque classe d'équivalence a exactement p éléments
- β_p : Il y a exactement p classes d'équivalence.

Q 7) Pour chacune des théories suivantes :

1. Ecrire les énoncés correspondant
2. Donner un modèle de la théorie
3. Expliquer (brièvement) pourquoi la théorie est complète

- Une relation d'équivalence qui a une infinité de classes, toutes de cardinal p.
- Une relation d'équivalence qui a p classes, toutes infinies.

(2 - 8) On se place dans la théorie des ordres denses sans extrêmités dans le langage $\{<, (c_i)_{i\in\mathbb{N}}\}$ auquel on a ajouté les axiomes $\{c_i < c_{i+1}\}$

Q 1⋆) Montrer que cette théorie a exactement trois modèles dénombrables à isomorphisme près.

Q 2) Montrer que cette théorie est complète. (Commencer par montrer que si on n'ajoute qu'un nombre fini d'axiomes $\{c_i < c_{i+1}\}$, la théorie est complète. Utilisez ensuite le fait que toute formule n'utilise qu'un nombre fini de constantes)

Remarque : cet exemple dû à Ehrenfeucht est très important, puisqu'il montre l'existence d'une théorie complète à exactement 3 modèles infinis dénombrables. Par un théorème de Vaught, on peut en effet montrer que toute théorie complète qui n'est pas $\aleph_0$ catégorique a au moins 3 modèles infinis dénombrables (on ne peut donc pas trouver de théorie complète ayant exactement 2 modèles infinis dénombrables). L'exemple montre donc que 3 est la meilleure borne possible.

Remarque : On peut trouver un exemple dans un langage fini.

On ajoute maintenant une nouvelle constante c à la théorie et les axiomes $\{c_i < c\}$

Q 3) Montrer que cette nouvelle théorie a toujours trois modèles dénombrables à isomorphisme près. Quels sont les modèles de la théorie précédente qu'on peut interpréter comme des modèles de cette théorie ?

Q 4) Montrer que cette nouvelle théorie est complète.

On revient à la théorie initiale, et on ajoute une relation unaire P, les axiomes $\{P(c_i)\}$ et les axiomes suivants

$$\begin{array}{l}
\forall x, \exists y, P(y) \wedge y > x \\
\forall x, \exists y, P(y) \wedge y < x \\
\forall x, y\ x \neq y \rightarrow \exists z, P(z) \wedge x < z \wedge z < x \\
\forall x, \exists y, \neg P(y) \wedge y > x \\
\forall x, \exists y, \neg P(y) \wedge y < x \\
\forall x, y\ x \neq y \rightarrow \exists z, \neg P(z) \wedge x < z \wedge z < x
\end{array}$$

Q 5⋆) Montrer que cette théorie est complète.

Q 6) Montrer qu'elle a exactement 4 modèles dénombrables à isomorphisme près.

Q 7) Construire une théorie complète qui a n modèles dénombrables pour $n > 3$. (Colorier les points avec plus de 2 couleurs)

Problème 1

Comme nous sommes encore dans le début du cours, il est délicat d'offrir un problème traitant uniquement de théorie des modèles. Celui-ci nécessite donc quelques notions d'algèbre linéaire et, pour la première partie, un peu de théorie des nombres.

On s'intéresse ici à démontrer le théorème suivant, du à Mal'cev

Théorème 2.20

Soit $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps de caractéristiques nulles, et $n, m \geq 2$. $GL_n(\mathbb{K}_1)$ et $GL_m(\mathbb{K}_2)$ sont élémentairement équivalents dans le langage des groupes si et seulement si :
- $n = m$
- $\mathbb{K}_1$ et $\mathbb{K}_2$ sont élementairement équivalents dans le langage des corps

Mal'cev a en fait prouvé un théorème valable pour d'autres classes de groupe qu'uniquement le groupe linéaire.

Commençons par le sens facile

Q 1) Montrer que si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont élémentairement équivalents, alors $GL_n(\mathbb{K}_1)$ et $GL_n(\mathbb{K}_2)$ sont élémentairement équivalents.

PARTIE 1 - $n = 1$

Q 1) Trouver une formule ϕ tel que $GL_n(\mathbb{K}_1) \models \phi$ si et seulement si $n = 1$.

Q 2) Montrer que $GL_1(\mathbb{K}_1)$ et $GL_m(\mathbb{K}_2)$ sont élémentairement équivalents si et seulement si $m = 1$ et les groupes multiplicatifs $\mathbb{K}_1^\times$ et $\mathbb{K}_2^\times$ sont élémentaires équivalents

On donne maintenant un exemple de deux corps $\mathbb{K}_1$ et $\mathbb{K}_2$ ayant des groupes multiplicatifs isomorphes mais $\mathbb{K}_1$ et $\mathbb{K}_2$ ne sont pas élémentairement équivalents.

On considère le corps $\mathbb{K} = \mathbb{Q}[i\sqrt{-2}] = \{a + ib\sqrt{2}, (a, b) \in \mathbb{Q}\}$. On peut soit considérer que $\mathbb{Z}[i\sqrt{2}]$ est factoriel, dont les seuls inversibles sont 1 et -1, ou utiliser les premières questions ci-dessous pour le prouver.

On définit $N(a + ib\sqrt{2}) = a^2 + 2b^2$. N est bien défini.

Q 3) Vérifier que $\mathbb{K}$ est bien un corps (en particulier que l'inverse d'un element de $\mathbb{K}$ est dans $\mathbb{K}$)

Q 4) Montrer que N vérifie $N(xy) = N(x)N(y)$ et $N(x + y) \leq N(x) + N(y)$.

Q 5) Quels sont les $x \in \mathbb{K}$ tel que $N(x) = 1$?

Q 6) Montrer que pour tout $x \in \mathbb{K}$, il existe $y \in \mathbb{Z}[i\sqrt{-2}]$ tel que $N(x - y) < 1$.

Q 7) Montrer que pour tout $p, q \in \mathbb{Z}[i\sqrt{-2}]$, $q \neq 0$, il existe $r, s \in \mathbb{Z}[i\sqrt{-2}]$ tel que $p = qr + s$ et $N(s) < N(q)$.

Q 8) En déduire que $\mathbb{Z}[i\sqrt{2}]$ est factoriel (tout élément s'écrit, au signe près, de façon unique comme un produit de nombres premiers)

On peut maintenant admettre ce qu'on a prouvé juste au dessus et passer à la partie théorie des modèles.

Q 9) Montrer que $\mathbb{Q}^\times$ et $\mathbb{K}^\times$ sont isomorphes

Q 10) Montrer l'existence de deux corps $\mathbb{K}_1$ et $\mathbb{K}_2$ de caractéristique nulle tel que $\mathbb{K}_1^\times$ et $\mathbb{K}_2^\times$ sont élémentairement équivalents en tant que groupes, mais $\mathbb{K}_1$ et $\mathbb{K}_2$ ne sont pas élémentairement équivalents en tant que corps.

PARTIE 2 - $n = m$

On s'intéresse à l'ensemble $E = \{X \in GL_n(\mathbb{K}) | X^2 = 1\}$ muni de la relation d'équivalence $X \sim Y \iff \exists P, PXP^{-1} = Y$.

Q 1) Déterminer le nombre de classes d'équivalence.

Q 2) Donner l'existence d'une formule ϕ_k tel que $GL_n(\mathbb{K}) \models \phi_k$ si et seulement si $n = k$.

Q 3) Par un procédé similaire, obtenir une formule ϕ_k tel que $SL_n(\mathbb{K}) \models \phi_k$ si et seulement si $n = k$.

On sait maintenant que si $GL_n(\mathbb{K}_1)$ et $GL_m(\mathbb{K}_2)$ sont élémentairement équivalents, $n = m$.

PARTIE 3 - $n = 2 \implies (\mathbb{K}_1 \equiv \mathbb{K}_2)$

On suppose dans toute cette partie $n = 2$.

Q 1) Ecrire une formule $\pi(x)$ tel que $GL_2(\mathbb{K}) \models \pi(X)$ si et seulement si X, dans une certaine base, se met sous la forme

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Q 2) Donner une formule $\xi(x, y)$ telle que $GL_2(\mathbb{K}) \models \xi(X, M)$ si et seulement si X (sans changement de base) est de la forme

$$N(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

Q 3) Vérifier que $N(\lambda)N(\delta) = N(\lambda + \delta)$

Q 4) Soit U tel que $N(\lambda) = UN(1)U^{-1}$. Calculer $UN(\delta)U^{-1}$.

Q 5) Montrer l'existence de deux formules α et β telles que

$$\begin{aligned} GL_2(\mathbb{K}) \models \alpha(N(\lambda), N(\delta), N(x)) &\iff x = \lambda + \delta \\ GL_2(\mathbb{K}) \models \beta(N(\lambda), N(\delta), N(x)) &\iff x = \lambda\delta \end{aligned}$$

Faire attention au cas $\lambda = 0$.

Q 6) Montrer que $GL_2(\mathbb{K}_1)$ et $GL_2(\mathbb{K}_2)$ sont élémentairement équivalents si et seulement si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont élementairement équivalents dans le langage des corps.

PARTIE 4 - $n > 2$

On admettra le résultat suivant : $SL_n(\mathbb{K}) = \{XYX^{-1}Y^{-1}, X, Y \in GL_n(\mathbb{K})\}$

Q 1) Montrer que si $GL_n(\mathbb{K}_1)$ et $GL_n(\mathbb{K}_2)$ sont élémentairement équivalents, alors $SL_n(\mathbb{K}_1)$ et $SL_n(\mathbb{K}_2)$ le sont également.

Soit M une matrice de $SL_n(\mathbb{K})$ telle que $M^2 = 1$.

Q 2) Montrer que l'ensemble E des matrices de $GL_n(\mathbb{K})$ qui commutent avec M est de la forme $GL_k(\mathbb{K}) \times GL_{n-k}(\mathbb{K})$ pour un certain k.

On vérifiera que E est un groupe.

On s'intéresse à l'ensemble des $X \in E \cap SL_n(\mathbb{K})$ tel que $X^2 = 1$ muni de nouveau de la relation d'équivalence $X \sim Y \iff \exists P \in E \cap SL_n(\mathbb{K}), PXP^{-1} = Y$.

Q 3) Donner le nombre de classes d'équivalence en fonction de n et k.

Q 4) En déduire une formule ϕ telle que $E \models \phi$ si et seulement si $k = 1$ (ou $k = n - 1$)

Q 5) Montrer que si $SL_n(\mathbb{K}_1)$ et $SL_n(\mathbb{K}_2)$ sont élémentairement équivalents, alors $GL_{n-1}(\mathbb{K}_1)$ et $GL_{n-1}(\mathbb{K}_2)$ sont élémentairement équivalents.

Q 6) Prouver le théorème de Mal'cev (dans la version donnée ci-dessus).

Interlude ℵ

ORDRES

ℵ.1 Définitions

Définition ℵ.1 (*structure ordonnée*)

Une structure $\mathfrak{M}$ sur le langage $<$ est ordonnée si elle vérifie les formules

- Antiréflexivité : $\forall x, \neg(x < x)$
- Antisymétrie : $\forall x, y(x < y) \implies \neg(y < x)$
- Transitivité : $\forall x, y, z(x < y) \wedge (y < z) \implies (x < z)$

L'ordre est dit total si la structure vérifie $\forall x, y, (x < y) \wedge (x = y) \wedge (y < x)$

Dans une structure ordonnée, on définit $\leq^{\mathfrak{M}}$, par $\{(x, y) \in M, (x, y) \in <^{\mathfrak{M}}$ ou $x = y\}$, et $>^{\mathfrak{M}}$ par $\{(x, y) \in M, (y, x) \in <^{\mathfrak{M}}\}$.

Définition ℵ.2 (*Ordres denses et discrets*)

Soit $\mathfrak{M}$ une structure ordonnée totale

- $\mathfrak{M}$ est un *ordre dense*énoncé si elle vérifie $\forall x, y, x < y \implies \exists z, x < z \wedge z < y$
- On note $S(x, y) = x < y \wedge \forall z, x < z \implies y \leq z$ Cette formule signifie y est le successeur de x.
- On note $P(x, y) = y < x \wedge \forall z, z < x \implies z \leq y$ Cette formule signifie y est le prédecesseur de x.
- $\mathfrak{M}$ est un *ordre discret* si elle vérifie : $\forall x, \exists y, S(x, y) \wedge \exists z, P(x, z)$
- $\mathfrak{M}$ est sans extrêmités si elle vérifie $\forall x, \exists y, x < y \wedge \exists z, z < x$

ℵ.2 Coupures

Définition ℵ.3 (*Coupure*)

Soit $\mathfrak{M}$ une structure ordonnée totalement. On appelle coupure un segment initial de M, c'est à dire un ensemble I tel que $\forall x \in I, \forall y < x, y \in I$

Proposition ℵ.1

Les coupures de $\mathbb{N}$ sont les $[0, n]$, $n \in \mathbb{N} \cup \{\infty\}$

En fait, les coupures sont toujours ordonnées :

Proposition ℵ.2

Les coupures d'un ordre total, munies de la relation $\not\subseteq$, forment une structure ordonnée totale.

Preuve : Il suffit juste de montrer que l'ordre est total. Soit X, Y deux coupures. Si $X \neq Y$, on peut supposer qu'il existe $x \in X - Y$. Prenons maintenant $y \in Y$. Alors $y < x$ (sinon $x \in Y$). Donc $y \in X$. Et finalement $Y \subseteq X$. ■

Les ordres denses forment la base de tous les ordres, on a en effet la proposition :

Proposition ℵ.3

Tout ordre I total de cardinal λ infini se plonge dans un ordre dense de cardinal λ.

Preuve : Commençons par ajouter un élément 0 qui est inférieur à tous les éléments de I. On considère alors l'ensemble des suites dans $I \cup \{0\}$ de support fini. (i.e l'ensemble des $n, u_n \neq 0$ est fini)

On pose alors

$$x < y \iff \exists i, x_1 \dots x_{i-1} = y_1 \dots y_{i-1}, x_i < y_i$$

On vérifie aisément que c'est une relation d'ordre. Remarquons que c'est également une relation d'ordre sur l'ensemble des suites de support non nécessairement fini. Montrons que l'ordre est dense. Soit $x_1 \dots x_n < y_1 \dots y_m$. Il existe i tel que $x_1 \dots x_{i-1} = y_1 \dots y_{i-1}, x_i < y_i$. Posons j (resp k) le dernier indice où $x_j \neq 0$ (resp y_k) Deux cas se produisent :

– $j < k$. Dans ce cas, on prend $z = y_1 \dots y_{k-1} 0 a 0 \dots$, où a est un élément quelconque. z convient.
– $j \geq k$. On prend $z = xa$, où a est un élément quelconque, qui convient.

Et on a fini.

Il reste maintenant à injecter I dans cet ensemble, ce qui se fait aisément. ■

On a même plus puissant :

Proposition ℵ.4

Tout ordre I total de cardinal λ se plonge dans un ordre dense de cardinal λ avec 2^λ coupures.

Preuve : Il suffit de vérifier que l'ordre établi précédemment à 2^λ coupures. C'est clairement une borne supérieure.

Chaque suite $(x_n)_{\{n \in \mathbb{N}\}}$ (non nécessairement de support fini) définit une coupure $I(x) = \{y, y < x\}$

Prenons maintenant deux suites x et y distinctes, et considérons $I(x)$ et $I(y)$. On peut supposer $x < y$. Alors $x \in I(y)$, mais $x \notin I(x)$. Donc $I(x) \neq I(y)$. La fonction I est injective, et il y a donc au moins 2^λ coupures. On a terminé ■

Chapitre 3

LA COMPACITÉ

Après toutes ces définitions, il était indispensable que le premier théorème vraiment important arrive. En effet, la compacité est le théorème fondamental de la théorie des modèles, on ne s'étonnera pas de la difficulté de sa démonstration

3.1 Énoncé

Théorème 3.1 (*Théorème de compacité*)

Φ un ensemble d'énoncés a un modèle si et seulement si toute partie finie de Φ a un modèle.

Remarque : Le sens direct est immédiat, c'est la réciproque qui présente vraiment de l'intérêt.

Ce théorème est très puissant. Il est en effet souvent assez facile de trouver un modèle d'un ensemble fini d'énoncé, mais construire un modèle pour tout l'ensemble est relativement délicat. Avant de donner la démonstration, examinons quelques exemples d'utilisation

♦ **Exemple**

Existence d'un modèle Prenons le langage de l'arithmétique $(0, 1, +, -, \times)$. Ajoutons une constante c et considérons l'ensemble constitué des formules vraies dans $\mathbb{N}$ auquel on ajoute :

$$\phi_n : \exists x \underbrace{x + \cdots + x}_{n \text{ fois}} = c$$

et

$$\neg(c = 0)$$

Si on prend un nombre fini d'énoncés de cet ensemble, il ne mentionne qu'un nombre fini de ϕ_i, disons avec $i < n$, et un modèle est alors donné par $\mathbb{N}$ dans lequel on interprète c par $n!$. Mais si on prend tous les énoncés ? On obtient une structure qui a les mêmes propriétés que $\mathbb{N}$, sauf qu'il possède un élément divisible par tous les autres... Est-ce possible ? La compacité nous assure de son existence. Un tel modèle est alors appelé un modèle des *entiers non standards*.

Non existence d'une théorie La compacité permet de montrer qu'il n'y a pas de théorie dont les modèles soient exactement les groupes finis. En effet, supposons qu'il existe une telle théorie T. Si on ajoute dans T

$$\phi_n : \exists x_1 \ldots \exists x_n, x_1 \neq x_2 \ldots x_1 \neq x_n, x_2 \neq x_3, \ldots x_{n-1} \neq x_n$$

c'est à dire une formule du premier ordre qui signifie que le groupe a au moins n éléments. Il est aisé de trouver des modèles de n'importe quel sous-ensemble fini de cet ensemble d'énoncés, il suffit de prendre un groupe de cardinal suffisament grand. Mais dans ce cas, la compacité nous assure l'existence d'un modèle qui vérifie tous les axiomes. Ce modèle est alors aussi un modèle de T, donc un groupe fini, ce qui est en contradiction avec le fait qu'il vérifie ϕ_n pour tout n !

3.2 Démonstration

3.2.1 Prélude

Que vérifie l'ensemble des formules d'une structure donnée ou, autrement dit, que peut-on dire de $Th(\mathfrak{M})$?

On vérifie aisément les propriétés :

- $\forall\phi \in Th(\mathfrak{M}), \psi \in Th(\mathfrak{M}), \phi \wedge \psi \in Th(\mathfrak{M})$
- $\forall\phi, \psi \in Th(\mathfrak{M}), \phi \vee \psi \in Th(\mathfrak{M})$ (aucune hypothèse sur ϕ)
- $\forall\phi, (\phi \in Th(\mathfrak{M}) \vee \neg\phi \in Th(\mathfrak{M}))$

Les filtres et les ultrafiltres correspondent à la version ensembliste de ces propriétés.

3.2.2 Filtres et ultrafiltres

Définition 3.1 (*Filtre*)

Soit E un ensemble. Un filtre $\mathcal{U}$ sur E est un sous-ensemble de $\mathcal{P}(E)$ (donc un ensemble de parties de E) vérifiant :

1. $\emptyset \notin \mathcal{U}$
2. $\forall X, Y \in \mathcal{U}, X \cap Y \in \mathcal{U}$
3. $\forall X \in \mathcal{U}, \forall Y \supseteq X, Y \in \mathcal{U}$

La dernière propriété est équivalente à l'axiome $\forall X \in \mathcal{U}, \forall Y, X \cup Y \in \mathcal{U}$, où on reconnaît deux des trois règles vues dans le paragraphe précédent.

Le fait que l'ensemble vide ne soit pas dans le filtre signifie en fait que tous les éléments du filtre possède une propriété en commun : leur intersection (finie) est toujours non vide. D'ailleurs, cette condition est presque en fait la seule condition suffisante, puisqu'on a la proposition suivante :

Proposition 3.2

Si A est un sous-ensemble de parties de E stable par intersection, et qui ne contient pas le vide, il existe un filtre qui contient cette partie.

Preuve : On va montrer que l'ensemble $\mathcal{U} = \{X \cup Y, X \in A, Y \subseteq E\}$ est un filtre. Remarquons que, par construction, il sera le filtre minimal contenant la partie A.

1. $\emptyset \notin \mathcal{U}$.
2. Soit Z_1 et Z_2 dans $\mathcal{U}$, donc de la forme $X_1 \cup Y_1$ et $X_2 \cup Y_2$. Alors

$$\begin{aligned} Z_3 &= Z_1 \cap Z_2 \\ &= (X_1 \cap X_2) \cup ((X_1 \cap Y_2) \cup (X_2 \cup Y_1) \cup (Y_1 \cup Y_2)) \\ &= (X_3) \cup Y_3 \end{aligned}$$

avec $X_3 = X_1 \cap X_2$, donc dans A, et Y_3 un ensemble quelconque donc $Y_3 \subseteq E$, et finalement $Z_3 \in \mathcal{U}$

3. Soit $Z = X \cup Y$ dans A et $Z' \supseteq Z$. Alors $Z' = X \cup Z'$ est bien dans $\mathcal{U}$ ■

On a alors deux corollaires importants.

Corollaire 3.3

Si A est un ensemble de parties de E telles que toutes les intersections finies soient non vides, alors il existe un filtre qui contient A.

La preuve est immédiate.

Corollaire 3.4

Si $\mathcal{U}$ est un filtre et X tel que $\forall Y \in \mathcal{U}, X \cap Y \neq \emptyset$, alors il existe un filtre qui contient $\mathcal{U}$ et X.

Preuve : Utiliser la propriété précédente avec $\{X \cap Y, Y \in \mathcal{U}\}$. ■

En général, l'union de deux filtres n'est pas un filtre, puisqu'elle n'est à priori pas stable par intersection. Nous avons tout de même la proposition suivante :

Proposition 3.5

Soit $\mathfrak{U}$ un ensemble de filtres, tel que $\forall \mathcal{U}, \mathcal{V} \in \mathfrak{U}, \mathcal{U} \subset \mathcal{V}$ ou $\mathcal{V} \subset \mathcal{U}$. Alors $\bigcup_{\mathcal{U} \in \mathfrak{U}} \mathcal{U}$ est un filtre.

La démonstration est immédiate.

Prenons maintenant une partie A stable par intersection. Il existe un filtre qui la contient. L'ensemble des filtres qui la contiennent est, d'après la proposition précédente, un ensemble ordonné inductif et le lemme de Zorn nous donne alors l'existence d'un filtre $\mathcal{U}$ maximal pour l'inclusion. Prenons alors un élément X qui n'est pas dans ce filtre. D'après le corollaire, dans sa forme contraposée, la proposition $\forall Y \in \mathcal{U}, X \cap Y \neq \emptyset$ est fausse, sinon on pourrait trouver un filtre plus grand. Donc il existe Y tel que $X \cap Y = \emptyset$. Donc $Y \subset E - X$. Par définition d'un filtre, on a alors $E - X \in \mathcal{U}$. Un filtre qui vérifie cette propriété est alors appelé un ultrafiltre.

Définition 3.2 (*Ultrafiltre*)

Un filtre qui vérifie

$$\forall X, X \in \mathcal{U} \text{ ou } E - X \in \mathcal{U}$$

est appelé un *ultrafiltre*

Remarque : Le “ou” de la définition est bien entendu exclusif, puisque $\emptyset \notin \mathcal{U}$, et un filtre est stable par intersection...

En fait, toute cette partie a donc montré :

Théorème 3.6 (*Existence d'un ultrafiltre*)

Soit A un ensemble de parties de E stable par intersection. Alors il existe un ultrafiltre qui la contient.

3.2.3 Ultraproduit

L'ultraproduit est l'élément clé qui nous donnera le modèle recherché.

Définition 3.3 (*Ultraproduit*)

Soit I un ensemble. À tout $i \in I$, on associe une structure $\mathfrak{M}_i$. Soit $\mathcal{U}$ un ultrafiltre sur I. On définit l'*ultraproduit* $\mathfrak{M} = \prod_{i \in I} \mathfrak{M}_i/\mathcal{U}$ par

- Son domaine est le produit cartésien $\times_{i \in I} M_i$ quotienté par la relation d'équivalence
$$(m_i) \sim (n_i) \iff \{i \in I, m_i = n_i\} \in \mathcal{U}$$
On notera $[x_i]$ la classe d'équivalence d'un élément (x_i).
- $\forall c \in \mathcal{C}, c^{\mathfrak{M}} = [c^{\mathfrak{M}_i}]$
- Pour chaque f dans $\mathcal{F}_n$, on définit $f^{\mathfrak{M}}([m_i]) = [f^{\mathfrak{M}_i}(m_i)]$ On vérifiera que cette définition est cohérente.
- Pour chaque R dans $\mathcal{R}_n$, on définit
$$([m^1], \dots [m^n]) \in R^{\mathfrak{M}} \iff \left\{i, (m_i^1 \dots m_i^n) \in R^{\mathfrak{M}_i}\right\} \in \mathcal{U}$$

C'est l'ultraproduit qui va nous servir de modèle pour la démonstration. Pour cela, nous avons besoin d'un dernier théorème

Théorème 3.7 (*Critère de Łoś*)

Pour toute formule $\phi(\overline{x})$ et uple $\overline{m} = ([m_1], \dots [m_n]) \in M^k$, on a
$$\mathfrak{M} \models \phi([m_1], \dots [m_k]) \iff \{i \in I, \mathfrak{M}_i \models \phi(m_1, \dots m_k)\} \in \mathcal{U}$$

Preuve : Par induction sur la structure de ϕ.

- Si ϕ est une formule atomique $R(m_1 \dots m_n)$, la démonstration est immédiate par définition de R.
- Si $\phi = \psi \vee \theta$.

  [⇒] Supposons $\mathfrak{M} \models \phi$. Alors par définition de la satisfaction, $\mathfrak{M} \models \psi$ ou $\mathfrak{M} \models \theta$ Par hypothèse d'induction, on a alors $\{i \in I, \mathfrak{M}_i \models \psi\} \in \mathcal{U}$ ou $\{i \in I, \mathfrak{M}_i \models \theta\} \in \mathcal{U}$. Comme on a un filtre, on peut écrire
  $$\{i \in I, \mathfrak{M}_i \models \psi\} \cup \{i \in I, \mathfrak{M}_i \models \theta\} \in \mathcal{U}$$
  ou encore
  $$\{i \in I, \mathfrak{M}_i \models \psi \text{ ou } \mathfrak{M}_i \models \theta\} \in \mathcal{U}$$
  donc par définition de la satisfaction $\{i \in I, \mathfrak{M}_i \models \psi \vee \theta\} \in \mathcal{U}$

  [⇐] Si $\{i \in I, \mathfrak{M}_i \models \psi \vee \theta\} \in \mathcal{U}$. Supposons que $\mathfrak{M} \not\models \psi$. Par hypothèse d'induction, $\{i \in I, \mathfrak{M}_i \models \psi\} \notin \mathcal{U}$, ou encore, par propriété d'un ultrafiltre :

$\{i \in I, \mathfrak{M}_i \not\models \psi\} \in \mathcal{U}$. Dans ce cas

$$\{i \in I, \mathfrak{M}_i \not\models \psi\} \cap \{i \in I, \mathfrak{M}_i \models \psi \vee \theta\} \in \mathcal{U}$$

C'est à dire

$$\{i \in I, \mathfrak{M}_i \not\models \psi \text{ et } \mathfrak{M}_i \models \psi \vee \theta\} \in \mathcal{U}$$

ce qui se réécrit

$$\{i \in I, \mathfrak{M}_i \not\models \psi \text{ et } \mathfrak{M}_i \models \theta\} \in \mathcal{U}$$

Comme cet ensemble est inclus dans $\{i \in I, \mathfrak{M}_i \models \theta\}$, on en déduit

$$\{i \in I, \mathfrak{M}_i \models \theta\} \in \mathcal{U}$$

Donc par hypothèse d'induction, $\mathfrak{M} \models \theta$. Et finalement on a montré que $\mathfrak{M} \models \psi$ ou $\mathfrak{M} \models \theta$. Ouf !

- Si $\phi = \psi \wedge \theta$, la démonstration est similaire.
- Si $\phi = \neg\psi$.

$$\begin{array}{rcl} \mathfrak{M} \models \phi & \iff & \mathfrak{M} \not\models \psi \\ & \iff & \{i \in I, \mathfrak{M}_i \models \psi\} \notin \mathcal{U} \\ & \iff & \{i \in I, \mathfrak{M}_i \not\models \psi\} \in \mathcal{U} \\ & \iff & \{i \in I, \mathfrak{M}_i \models \neg\psi\} \in \mathcal{U} \end{array}$$

  Ce point est très important, puisque c'est ici que l'on utilise le fait que $\emptyset \notin \mathcal{U}$, ou, plus exactement : $X \in \mathcal{U} \implies I - X \notin \mathcal{U}$

- Si $\phi = \exists x \psi(x)$.
  - Supposons $\mathfrak{M} \models \phi$. Alors il existe $[m_i] \in M$ tel que $\mathfrak{M} \models \psi(m)$. Par hypothèse d'induction, $\{i, \mathfrak{M}_i \models \psi(m_i)\} \in \mathcal{U}$. Cet ensemble etant inclus dans $\{i, \mathfrak{M}_i \models \exists x \psi(x)\}$, ce dernier est dans $\mathcal{U}$.
  - Supposons

    $$\{i, \mathfrak{M}_i \models \exists x \psi(x)\} \in \mathcal{U}$$

    On se donne, pour chaque i tel que $\mathfrak{M}_i \models \exists x \psi(x)$, un n_i tel que $\mathfrak{M}_i \models \psi(n_i)$, et on prend n_i quelconque sinon. Bien entendu, on a besoin ici de l'axiome du choix pour trouver ces éléments. Alors $[n_i]$ vérifie $\{i, \mathfrak{M}_i \models \psi(n_i)\} \in \mathcal{U}$, puisque l'ensemble en question contient, par construction, $\{i, \mathfrak{M}_i \models \exists x \psi(x)\}$. Ainsi, par hypothèse d'induction, $\mathfrak{M} \models \psi([n_i])$, donc $\mathfrak{M} \models \exists x \psi(x)$.
- Si $\phi = \forall x \psi(x)$, la démonstration est similaire. ■

On a maintenant tous les éléments nécessaires pour démontrer la compacité.

3.2.4 Démonstration de la compacité

On choisit pour I l'ensemble des parties finies de Φ, et pour chaque $i \in I$ un modèle $\mathfrak{M}_i$ de i. On pose, à $\phi \in \Phi$ donné, $I_\phi = \{i \in I, \phi \in i\}$

Proposition 3.8

Il existe un ultrafiltre $\mathcal{U}$ qui contient les I_ϕ.

Preuve : Les intersections finies de I_ϕ sont non vides. ■

Alors, par construction, on a $\forall \phi \in \Phi, I_\phi \in \mathcal{U}$, c'est à dire $\forall \phi, \mathfrak{M} \models \phi$, et donc $\mathfrak{M}$ est bien un modèle de Φ. La preuve est enfin terminée !

3.3 Löwenheim-Skolem ascendant

La compacité va nous permettre d'établir un théorème analogue au théorème de Löwenheim-Skolem, mais dans l'autre sens.

Proposition 3.9

Soit $\mathfrak{M}$ une $\mathcal{L}$-structure infinie. Alors pour tout cardinal λ, il existe une $\mathcal{L}$-structure $\mathfrak{N}$ de cardinal $|N| \geq \lambda$ telle que $\mathfrak{M} \prec \mathfrak{N}$.

Preuve : On ajoute au langage des constantes c_i, pour $i < \lambda$. Il suffit alors de considérer la théorie $Th(\mathfrak{M}, M)$ enrichie des énoncés $c_i \neq c_j$, pour $j \neq i$. Chaque sous-ensemble fini admet $\mathfrak{M}$ comme modèle, puisque ce sous-ensemble ne mentionne qu'un nombre fini de constantes c_i, que l'on peut interpréter dans M. On en déduit par compacité que l'ensemble d'énoncés à un modèle, et celui-ci est bien une sur-structure élémentaire de $\mathfrak{M}$. ■

Cette proposition nous donne une sur-structure de cardinal supérieur à λ, comment faire si on veut avoir exactement λ ?

Théorème 3.10 (*Löwenheim-Skolem ascendant*)

Soit $\mathfrak{M}$ une $\mathcal{L}$-structure infinie, alors pour tout $\lambda > |M| + |\mathcal{L}|$, il existe une sur-structure élémentaire $\mathfrak{N}$ de $\mathfrak{M}$ de cardinal λ.

Preuve : Avec le lemme précédent, on a l'existence de $\mathfrak{N}'$ tel que $\mathfrak{M} \prec \mathfrak{N}'$, $|N| \geq \lambda$, il suffit alors d'utiliser Löwenheim-Skolem descendant pour obtenir $\mathfrak{N}$ tel que $\mathfrak{N} \prec \mathfrak{N}'$ de cardinal λ exactement. Il reste alors à prouver que

$$\mathfrak{M} \prec \mathfrak{N}', \mathfrak{N} \prec \mathfrak{N}', M \subset N \implies \mathfrak{M} \prec \mathfrak{N}$$

ce qui est laissé au lecteur ■

3.4 Axiomatisation

On va donner ici une conséquence du théorème de compacité qui montre assez bien pourquoi ce nom lui a été donné.

Définition 3.4 (*Axiomatisation*)

Soit T une théorie. Une *axiomatisation* d'une théorie est un ensemble de formules Φ tels que Φ et T aient les mêmes modèles. On dit que T est finiment axiomatisable si elle a une axiomatisation finie.

Proposition 3.11

Une théorie est finiment axiomatisable si et seulement si de toute axiomatisation, on peut extraire une axiomatisation finie.

Preuve : Le sens indirect est trivial.

Soit T finiment axiomatisable, et Φ une axiomatisation finie de T.Quitte à considérer l'axiomatisation dont le seul énoncé est $\bigwedge_{\phi\in\Phi}\phi$, on peut supposer que Φ est réduite à un simple élément ϕ. Soit Ψ une axiomatisation de T. Alors $\Psi \cup \{\neg\phi\}$ n'admet pas de modèle, puisque tout modèle de Ψ est un modèle de $\{\phi\}$. Donc il existe un sous-ensemble fini qui n'admet pas de modèle. Ce sous-ensemble ne peut pas ne contenir que des formules de Ψ. Donc on a un sous-ensemble Θ de Φ tel que $\Theta\cup\{\neg\phi\}$ n'ait pas de modèle. Ceci implique que tout modèle de Θ vérifie ϕ. Or tout modèle de ϕ est un modèle de T donc vérifie les énoncés de Θ. Ainsi, les modèles de Θ sont exactement les modèles de T. ■

3.5 κ-catégoricité

Les théorèmes de Löwenheim-Skolem permettent de donner une première manière de montrer qu'une théorie est complète.

Définition 3.5 (*κ-catégoricité*)

Une théorie T est dite *κ-catégorique*, κ infini, si tous les modèles de cardinal κ sont isomorphes.

Théorème 3.12 (*Test de Łoś-Vaught*)

Une théorie κ-catégorique sans modèles finis, avec $\kappa \geq |\mathcal{L}|$, est complète.

Preuve : Montrons que deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ quelconques sont élémentairement équivalents. Deux cas se présentent :

- $|M| \geq \kappa$. Dans ce cas, on peut appliquer Löwenheim-descendant pour obtenir $\mathfrak{M}' \prec \mathfrak{M}$ avec $|\mathfrak{M}'| = \kappa$
- $|M| < \kappa$ Comme $\kappa > |\mathcal{L}|$, et $\mathfrak{M}$ infini, on déduit $\kappa > |\mathcal{L}| + |M|$. Comme $\mathfrak{M}$ est infini, on peut appliquer Löwenheim-Skolem ascendant pour trouver $\mathfrak{M} \prec \mathfrak{M}'$ avec $|\mathfrak{M}'| = \kappa$

Dans tous les cas, on a $\mathfrak{M}$ élémentairement équivalent à $\mathfrak{M}'$ de cardinal κ. On effectue la même procédure avec $\mathfrak{N}$, et l'hypothèse de catégoricité conclut à $\mathfrak{M}'$ isomorphe (donc élémentairement équivalent) à $\mathfrak{N}'$, et on en déduit $\mathfrak{M}$ élémentairement équivalent à $\mathfrak{N}$. ■

Exercices

(3 - 1) *(Compacité et théories)*

Q 1) Soit T une théorie, et ϕ tel que $T \models \phi$. Montrer qu'il existe une partie finie $T' \subset T$ tel que $T' \models \phi$. (Aide : $T \cup \{\neg\phi\}$ n'a pas de modèle)

Q 2) Soit $(T_i)_{i\in\mathbb{N}}$ une suite croissante de théories tel qu'il existe un modèle de T_i qui n'est pas un modèle de T_{i+1}. Montrer que $\cup T_i$ est une théorie, et qu'elle n'est pas finiment axiomatisable.

Q 3) Soit T une théorie finiment axiomatisable sur un langage L fini. Montrer qu'il y a équivalence entre :
- Il y a un nombre fini de théories complètes $T' \supseteq T$;
- Il y a un nombre fini de théories $T' \supseteq T$;
- Toute théorie $T' \supseteq T$ est finiment axiomatisable.

(3 - 2) Montrer qu'une théorie T qui a des modèles de cardinaux finis arbitrairement grands a un modèle infini. Donner l'exemple d'une théorie qui a des modèles de cardinaux finis arbitrairement grands et dont tous les modèles infinis sont au moins de cardinal $\aleph_1$.

(3 - 3) *(Amalgamation)*

Q 1⋆) Soit $\mathfrak{M}$, $\mathfrak{N}_1$ et $\mathfrak{N}_2$ trois structures telles que $\mathfrak{M} \prec \mathfrak{N}_1$, et $\mathfrak{M} \prec \mathfrak{N}_2$. Montrer qu'il existe $\mathfrak{N}$ telle que $\mathfrak{N}_1 \prec \mathfrak{N}$, et $\mathfrak{N}_2$ s'injecte élémentairement dans $\mathfrak{N}$ (autrement dit, il existe $\mathfrak{N}_2' \prec \mathfrak{N}$, où $\mathfrak{N}_2'$ est une structure isomorphe à $\mathfrak{N}_2$)

On dit que deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ sont équivalents s'il existe un modèle $\mathfrak{P}$ tel que $\mathfrak{M}$ et $\mathfrak{N}$ s'injectent élémentairement dans $\mathfrak{P}$.

Q 2) Montrer qu'il s'agit bien d'une relation d'équivalence.

(3 - 4) On se place dans la théorie des graphes non orientés, c'est à dire dans le langage contenant uniquement une relation $\mathcal{R}$ et dans la théorie contenant l'axiome $\forall x, y, \mathcal{R}(x, y) \iff \mathcal{R}(y, x)$. Si $\mathfrak{M}$ est un modèle, on appelle sommet un élément de M.

Soit G un modèle de la théorie. On dit qu'un sous-ensemble S est stable si pour tout $x, y \in S$, on a $(x, y) \notin \mathcal{R}$. On dit qu'il est complet si au contraire, on a pour tout $x, y \in S$, $(x, y) \in \mathcal{R}$.

Q 1⋆) Soit G un graphe infini. Montrer qu'il contient soit une sous-partie infinie stable, soit une sous-partie infinie complète.

Q 2) Montrez ce théorème de Ramsey : Pour tout entier n, il existe un entier k tel que tout graphe à au moins k sommets admet une sous-partie complète de taille n ou une sous-partie stable de taille n.

(3 - 5) *(Non-théories)*

Q 1) Montrer qu'il n'existe pas de langage $\mathcal{L}$ contenant $<$ et de théorie T telle que les modèles de T soient précisément les bons ordres (un bon ordre est un ordre total tel que toute partie non vide a un plus petit élément).

Q 2) Montrer qu'il n'existe pas de théorie dont les modèles soient les groupes abéliens finiment engendrés.

(3 - 6) Soit $\mathcal{L}$ un langage. On note K l'ensemble des théories complètes.

A tout ensemble de formules sans paramètres Φ on associe $T_\Phi = \{T \in K | \Phi \subseteq T\}$

On dira que $X \subseteq K$ est fermé si $X = T_\Phi$ pour un certain Φ. Un ouvert est le complémentaire d'un fermé.

Q 1) Montrer qu'on a défini ainsi une topologie, c'est à dire :
- L'ensemble vide est un fermé ;
- K est fermé ;
- L'union de deux fermés est un fermé ;
- Une intersection quelconque de fermés est un fermé ;

Q 2) Soit V_i une famille de fermés tels que toute intersection finie est non vide. Montrer que $\cap V_i$ est non vide. (On vient en fait de montrer que K est compact).

Q 3) Montrer que K est Hausdorff : Si $X, Y \in K$, alors il existe des ouverts disjoints U_1, U_2 tels que $X \in U_1, Y \in U_2$.

Q 4) Montrer que tout fermé s'écrit comme intersection d'ouverts-fermés (on dit alors que K est totalement discontinu).

Q 5) Montrer que les théories T finiment axiomatisables sont les points isolés (C'est à dire $\{T\}$ est un ouvert).

(3 - 7) *(Théorème de Robinson)*

On s'intéresse au théorème suivant

Théorème 3.13 (*Théorème de Robinson*)

Soient $\mathcal{L}_1$ et $\mathcal{L}_2$ deux langages, et $\mathcal{L}$ leur intersection. Soient T_1 et T_2 des théories sur $\mathcal{L}_1$ et $\mathcal{L}_2$. On suppose qu'il n'existe pas de formule de $\mathcal{L}$ tel que $T_1 \models \phi$ et $T_2 \models \neg\phi$. Alors $T_1 \cup T_2$ a un modèle.

Q 1$\star\star\star$) Montrer le théorème. (Idée : Construire une suite de modèles $\mathfrak{M}_i, \mathfrak{N}_i$ de T_1 et T_2 et des $\mathcal{L}$-morphismes f_i de $\mathfrak{M}_i$ dans $\mathfrak{N}_i$ tels que l'image de f_{i+1} contienne $\mathfrak{N}_i$)

Remarque : Ce théorème est sans doute trop dur et il est donné uniquement ici comme exemple. Si jamais vous voulez tout de même essayer, commencez par les questions suivantes, elle vous donneront quelques indications.

Q 2) Montrer le théorème suivant

Théorème 3.14 (*Théorème d'interpolation de Craig*)

Si ϕ et ψ sont des formules telles que tout modèle de ϕ est un modèle de ψ, alors il existe une formule θ qui n'utilise que les symboles apparaissant simultanémént dans ϕ et ψ et tel que tout modèle de ϕ est un modèle de θ, et tout modèle de θ est un modèle de ψ.

et montrer le théorème de Robinson à partir de ce théorème.

Q 3$\star$) Montrer que le théorème suivant est équivalent au théorème de Robinson

Théorème 3.15

Soient T_1 et T_2 des théories sur $\mathcal{L}_1$ et $\mathcal{L}_2$ et $T \subseteq T_1 \cap T_2$ une théorie complète de $\mathcal{L}$. Alors $T_1 \cup T_2$ est satisfaisable.

Chapitre 4

CHAÎNES

La chaîne est un outil souvent utilisé pour construire un nouveau modèle d'une théorie, en 'itérant' un procédé. Nous expliquons ici ce qu'est une chaîne, et comment exploiter le principe

4.1 Chaînes élémentaires

Définition 4.1 (*chaîne*)

Une *chaîne* est un ensemble $\mathfrak{M}_\mathfrak{i}$ de structures sur le même langage vérifiant $\forall i, \mathfrak{M}_\mathfrak{i} \subseteq \mathfrak{M}_{\mathfrak{i}+1}$

Proposition 4.1

Si $\mathfrak{M}_\mathfrak{i}$ est une chaîne, il existe une (et une seule) structure $\mathfrak{M} = \cup \mathfrak{M}_\mathfrak{i}$ vérifiant

- $M = \cup M_i$
- $\forall i, \mathfrak{M}_\mathfrak{i} \subseteq \mathfrak{M}$

Preuve : Montrons l'existence de la structure. L'ensemble M est donc défini comme $\cup M_i$. Soit f une fonction du langage. Soit $(x_1, \ldots, x_n) \in \cup M_i$. Donc $x_1 \in M_{i_1}, \ldots x_n \in M_{i_n}$. En posant $i = max\ i_j$, on a donc $x_1, \ldots x_n \in M_i$. On pose alors $f^{\mathfrak{M}}(\overline{x}) = f^{\mathfrak{M}_\mathfrak{i}}(\overline{x})$. Le lecteur vérifiera aisément que cette définition ne dépend pas du choix de $i_1, \ldots i_n$. On définit de manière similaire les relations. Il est immédiat que la structure obtenue vérifie bien les conditions recherchées. Les faits de la construction sont nécessaires, d'où l'unicité. ■

Définition 4.2 (*chaîne élémentaire*)

Une chaîne $\mathfrak{M}_\mathfrak{i}$ est une *chaîne élémentaire* si $\forall i, \mathfrak{M}_\mathfrak{i} \prec \mathfrak{M}_{\mathfrak{i}+1}$

Théorème 4.2 (*Principe de la chaîne élémentaire de Tarski-Vaught*)

Si $\mathfrak{M}_\mathfrak{i}$ est une chaine élémentaire, en posant $\mathfrak{M} = \cup \mathfrak{M}_\mathfrak{i}$

$$\forall j, \mathfrak{M}_\mathfrak{j} \prec \mathfrak{M}$$

Preuve : On montre par induction sur la structure de ϕ que

$$\text{Pour tout } j, \text{ pour tous } a_1, \ldots a_n \in \mathfrak{M}_\mathfrak{j}$$

$$\mathfrak{M}_\mathfrak{j} \models \phi(\overline{a}) \iff \mathfrak{M} \models \phi(\overline{a})$$

La preuve ne présente aucune difficulté et ne sera donc pas effectuée ici. ■

4.2 Morphismes élémentaires

L'utilisation des chaînes permet entre autres de construire un automorphisme à partir d'un morphisme élémentaire partiel.

Proposition 4.3

Soit σ un isomorphisme élémentaire partiel de $\mathfrak{M}$. Alors il existe une extension élementaire $\mathfrak{N}$ de $\mathfrak{M}$ tel que σ soit la restriction d'un automorphisme de $\mathfrak{N}$.

La preuve va utiliser le lemme délicat :

Lemme 4.4

Soit σ un isomorphisme élémentaire partiel de $\mathfrak{M}$. Alors il existe $\mathfrak{N}$ extension de $\mathfrak{M}$ et un isomorphisme élémentaire τ extension de σ tel que M soit dans le domaine de τ.

Preuve : Commençons par donner une idée de la preuve. Supposons que τ existe. Alors pour tout $\overline{m} \in M$, on aura

$$\begin{aligned} \mathfrak{N} \models \phi(\tau(\overline{m})) \quad &\iff \quad \mathfrak{N} \models \phi(\overline{m}) \\ &\iff \quad \mathfrak{M} \models \phi(\overline{m}) \end{aligned}$$

Prenons maintenant $\overline{m} \in M$ et $\overline{n}$ dans le domaine de σ. On a alors, comme ci-dessus :

$$\mathfrak{N} \models \phi(\tau(\overline{m}), \tau(\overline{n})) \iff \mathfrak{M} \models \phi(\overline{m}, \overline{n}))$$

Et comme τ est une extension de σ :

$$\mathfrak{N} \models \phi(\tau(\overline{m}), \sigma(\overline{n})) \iff \mathfrak{M} \models \phi(\overline{m}, \overline{n}))$$

Ceci nous donne une idée de comment construire τ. Prenons des nouvelles constantes m' pour chaque élément $m \in \mathfrak{M}$. Considérons

$$Th(\mathfrak{M}, M) \cup \left\{ \phi(\overline{m}', \sigma(\overline{n})) | \mathfrak{M} \models \phi(\overline{m}, \overline{n}), \overline{n} \in dom(\sigma) \right\}$$

On considère donc que m' représente en fait $\tau(m)$. Toute partie finie ne mentionne qu'un nombre fini des formules ϕ, notées ϕ_i. Par construction, $\mathfrak{M} \models \phi_i(\overline{m}_i, \overline{n}_i)$ Ceci implique :

$$\mathfrak{M} \models \exists \overline{x}_1, \ldots \overline{x}_i \bigwedge \phi_i(\overline{x}_i, \overline{n}_i)$$

L'intérêt de la démarche est d'avoir passé les constantes $\overline{m}$ en variables. Comme σ est élémentaire, on a alors

$$\mathfrak{M} \models \exists \overline{x}_1, \ldots \overline{x}_i \bigwedge \phi_i(\overline{x}_i, \sigma(\overline{n}_i))$$

Et donc il existe des uples $\overline{m}_1 \ldots \overline{m}_i$ qui conviennent, ce qui permet de fixer les valeurs pour les constantes m' (Le lecteur attentif remarquera qu'il y a une petite arnaque dans cette preuve, mais il saura la rectifier aisément). Toute partie finie a un modèle, et l'ensemble total à un modèle. L'application $\tau : m \mapsto m'$ convient alors. On remarque en effet aisément que c'est une prolongation de σ, et la construction assure que c'est bien un isomorphisme élémentaire. ■

On peut maintenant prouver la proposition

Preuve : On va construire une chaîne $\mathfrak{M}_i$ et des morphismes élementaires σ_i de sorte que

- $\mathfrak{M}_0 = \mathfrak{M}$
- $\sigma_0 = \sigma$
- $\mathfrak{M}_{2i} \subset dom(\sigma_{2i+1})$
- l'image de σ_{2i+2} contient $\mathfrak{M}_{2i+1}$

Par construction, $\cup\mathfrak{M}_i$ et $\cup\sigma_i$ conviendront. Le lemme précédent permet de régler les étapes impaires, et les étapes paires se font de même en considérant σ_{2i}^{-1} ■

Interlude ב

L'INFINI

Le but de ce chapitre est de donner quelques notions sur les cardinaux et les ordinaux, utiles pour certaines démonstrations. Il ne s'agit pas ici de définir ce qu'est un ensemble, nous supposons en effet que le lecteur connaît, uniquement de façon élémentaire, les axiomes de Zermelo-Frankel.

ב.1 Les entiers

Rappelons que dans la théorie des ensembles, on peut représenter les entiers de la façon suivante :
– $[0] = \emptyset$
– $[n+1] = [n] \cup \{[n]\}$
Et on a donc $[1] = \{\emptyset\}$, $[2] = \{\emptyset, \{\emptyset\}\}$, et caetera. On note alors $\omega = \{[n], n \in \mathbb{N}\}$.
Les propriétés suivantes se démontrent alors immédiatement :

Proposition ב.1

- ◦ $[n] \subsetneq [m]$ si et seulement si $n < m$
- ◦ si $[n] \in [m]$, $[n] \subsetneq [m]$

La seconde proposition est encore valable si on remplace $[m]$ par ω.
La proposition suivante donnera en fait sa justification au principe de récurrence :

Proposition ב.2

Tout sous ensemble de $[n]$ (resp ω) admet un élément minimal pour $\in$ (qui est une relation d'ordre totale)

Autrement dit la relation $\in$ est une relation de bon ordre sur ω.
Les ordinaux se définissent par analogie.

ב.2 Les ordinaux

Définition ב.1 (*Ordinal*)

Un ensemble λ est un *ordinal* si

- ◦ La relation $\in$ est une relation de bon ordre sur λ, c'est à dire
  1. $\in$ est totale : $\forall x, y \in \lambda, x \in y \text{ou} y \in x \text{ou} x = y$
  2. $\in$ est bien fondée : Tout sous ensemble de λ admet un plus petit élément.
- ◦ $\forall x \in \lambda, x \subset \lambda$

Les ensembles vus précédemment ($[n]$ et ω) sont des ordinaux. On s'aperçoit de même que l'ensemble $\omega \cup \{\omega\}$, noté $\omega + 1$ est aussi est un ordinal. On peut de même définir $\omega + 2, \ldots, \omega + n$, et même $\omega + \omega$, noté $\omega \cdot 2$, puis même $\omega \cdot \omega$ noté ω^2.

On remarque alors :

Proposition ב.3

Si α est un ordinal, et $\beta \in \alpha$, alors β est un ordinal.

Preuve : Soit B un sous ensemble de β. Comme $\beta \in \alpha$, $\beta \subset \alpha$, et donc $B \subset \beta$, donc B admet un plus petit élément. De même, soit $x \in \beta$. Comme $\beta \subset \alpha$, $x \in \alpha$. Soit maintenant $y \in x$. Comme $x \subset \alpha$, $y \in \alpha$. Donc comme l'ordre est total, on a $y \in \beta$ ou $\beta \in y$ ou $y = \beta$.

- $\beta \in y$ est impossible, puisqu'il donne $\beta \in y \in x \in \beta$
- $\beta = y$ est impossible pour la même raison : $\beta \in x \in \beta$
- Ainsi $y \in \beta$

$\forall y \in x, y \in \beta$, et donc $x \subset \beta$. ■

La proposition suivante est immédiate :

Proposition ב.4

Si α est un ordinal, $\emptyset \in \alpha$ ou $\alpha = \emptyset$

Preuve : Supposons $\alpha \neq \emptyset$. α a un plus petit élément pour $\in$ que l'on note x. Supposons qu'il existe $y \in x$. Alors $y \in \alpha$, comme $x \subset \alpha$. Ceci est en contradiction avec le fait que x soit le plus petit élément. Donc $x = \emptyset$, et $\emptyset \in \alpha$ ■

ב.3 Récurrence transfinie

Toutes ses réflexions nous permettent d'introduire le procédé de récurrence transfinie, qui est une généralisation du procédé de récurrence classique

Théorème ב.5 (*Récurrence transfinie*)

Soit $\mathcal{P}$ une propriété sur les ensembles. On suppose

- (Initialisation) $P(\emptyset)$
- (Récurrence). Si $\forall \alpha \in \beta, P(\alpha)$, alors $P(\beta)$.

Alors pour tout ordinal λ, on a $P(\lambda)$

Remarquons que la première hypothèse est superflue puisqu'elle est conséquence de la deuxième.

Preuve : Soit λ un ordinal. Supposons que $P(\lambda)$ ne soit pas vraie. Alors $\{\alpha \in \lambda, P(\alpha) \text{est faux}\}$ est non vide, d'après le principe de récurrence, donc admet un plus petit élément β. Alors $P(\beta)$ est faux, donc il existe $x \in \beta$, $P(x)$ est faux. Or, $\beta \subset \lambda$, donc $x \in \lambda$, et ceci contredit la minimalité de β. ■

Cette propriété permet de démontrer aisément la proposition suivante :

Proposition ב.6

Pour tous ordinaux α et β, on a $\alpha \in \beta$, $\beta \in \alpha$, ou $\beta = \alpha$

Preuve : On montre la proposition par récurrence sur α. On pose donc $P(\lambda) =' \forall \beta \text{ordinal}, \beta \in \lambda, \lambda = \beta, \lambda \in \beta'$.

Supposons $P(\alpha')$ pour tout $\alpha' \in \alpha$. Montrons maintenant P par récurrence sur β . On pose donc $Q(\lambda) =' \alpha \in \lambda, \alpha = \lambda, \lambda \in \alpha'$. On suppose $Q(\beta')$ pour $\beta' \in \beta$, et on veut montrer $Q(\beta)$.

On sait donc que $\forall \alpha' \in \alpha, \beta \in \alpha', \alpha' = \beta \text{ou} \alpha' \in \lambda$. Il y a deux cas :

1. $\exists \alpha' \in \alpha, \beta \in \alpha' \text{ou} \alpha' = \beta$ Dans les deux cas, on en déduit $\beta \in \alpha$
2. Sinon, on sait donc que $\forall \alpha' \in \alpha, \alpha' \in \beta$. On distingue maintenant deux cas similaires au précédents
   (a) il existe $\beta' \in \beta$, $\alpha \in \beta'$ ou $\beta' = \alpha$. Là encore on peut conclure.
   (b) Sinon, en résumé, on a eu :
      – $\forall \alpha' \in \alpha, \alpha' \in \beta$
      – $\forall \beta' \in \beta, \beta' \in \alpha$
      donc $\alpha = \beta$

La preuve est terminée par récurrence transfinie. ■

La récurrence transfinie permet de faire des preuves sur tous les ensembles, on a en effet le théorème suivant (non prouvé)

Théorème ב.7

Tout ensemble est en bijection avec un ordinal

Ainsi, si on veut faire une preuve pour un ensemble quelconque, il suffit de faire la preuve pour les ordinaux.

ב.4 Ordinaux limites

Le schéma de récurrence transfinie n'est pas utilisable aisément. On utilise donc souvent plutôt un autre schéma relativement semblable. Nous devons pour cela définir d'abord les ordinaux limites

Définition ב.2 (*Ordinal limite et Ordinal successeur*)

Un ordinal α est un *ordinal successeur* s'il s'écrit $\beta \cup \{\beta\}$ pour un certain β. Un ordinal est un *ordinal limite* s'il n'est pas un ordinal successeur.

On a alors la proposition importante suivante :

Proposition ב.8

Un ordinal α est un ordinal limite si et seulement si $\alpha = \cup_{\beta \in \alpha} \beta$

Preuve : Remarquons que $\cup_{\beta \in \alpha} \beta \subset \alpha$, puisque $\beta \in \alpha \implies \beta \subset \alpha$.

– [$\Leftarrow$] Si α est un ordinal successeur, $\alpha = \beta \cup \{\beta\}$. $\cup_{\gamma \in \alpha} \gamma = \beta$.

– [⇒] Supposons α ordinal limite. Posons $\beta = \cup_{\gamma\in\alpha}\gamma$. Supposons $\beta \neq \alpha$. Par définition de la limite $\beta + 1 = \beta \cup \{\beta\} \in \alpha$ (puisque cet ensemble ne peut être égal à α (α est un ordinal limite) et qu'il ne peut le contenir. Mais alors, par définition de β, on a $\beta + 1 \subset \beta$, donc en particulier $\beta \in \beta$, contradiction, et finalement $\alpha = \beta$ ■

Ceci peut se reformuler en

Proposition ב.9

Tout cardinal α s'écrit :
- Soit $\beta + 1 = \beta \cup \{\beta\}$
- Soit $\cup_{\beta\in\alpha}\beta$

On en déduit le principe de récurrence transfinie usuel :

Théorème ב.10 (*Récurrence transfinie usuelle*)

Soit $\mathcal{P}$ une propriété sur les ensembles. On suppose
- ∘ Si $P(\alpha)$, alors $P(\alpha + 1)$
- ∘ Si $\forall\beta \in \alpha, P(\beta)$, alors $P(\cup_{\beta\in\alpha}\beta)$.

Alors pour tout ordinal λ, on a $P(\lambda)$

Preuve : Les hypothèses du théorème entraînent les hypothèse du principe de récurrence transfinie évoqué avant. ■

ב.5 Cardinaux

Définition ב.3 (*Cardinaux*)

Le *cardinal* d'un ensemble A est le plus petit ordinal équipotent (en bijection) avec A. On le note $|A|$.

Cet ordinal existe bien : l'axiome du choix nous assure que tout ensemble est en bijection avec un ordinal λ, et il suffit alors de prendre le plus petit ordinal inférieur à λ (qui existe) en bijection avec l'ensemble considéré.

Avec cette définition, le cardinal d'un ensemble de n éléments est bien $[n]$, celui de $\mathbb{N}$ est ω.

Un théorème, que nous ne développerons pas ici, assure que toute classe bien ordonnée qui n'est pas un ensemble est isomorphe à la classe des ordinaux. Ceci assure en particulier que la classe des cardinaux infinis est isomorphe à la classe des ordinaux. On peut donc numéroter les cardinaux par des ordinaux, d'où la fonction $\aleph(x)$ qui associe à chaque ordinal x, un cardinal. On note usuellement plutôt $\aleph_x$, ce qui donne lieu aux fameux $\aleph_0$, $\aleph_1$, etc...

Chapitre 5

VA ET VIENT

Le Va et Vient est la méthode qui va enfin pouvoir permettre de répondre à la fameuse question : Comment montrer qu'une théorie est complète, ou de façon équivalente : Comment montrer que deux structures sont élémentairement équivalentes. Nous allons en effet voir ici une caractérisation qui permettra de donner assez facilement une méthode pratique de preuve des propriétés précédemment énoncées.

Nous allons introduire pour cela les k-isomorphismes, pour k ordinal quelconque, et les ∞-isomorphismes. Cette deuxième notion étant plus visuelle, et puisqu'elle ne fait pas intervenir de cardinal, il paraît plus pratique de commencer par celle-ci

5.1 ∞-isomorphismes

5.1.1 Définitions

Commençons d'abord par énoncer la notion d'isomorphisme local.

Définition 5.1 (*Isomorphisme local*)

> Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux $\mathcal{L}$-structures. Soit (a_i) et (b_i) deux n-uplets de M et de N. L'application σ de a_i dans b_i est un *isomorphisme local* si elle s'étend en un isomorphisme de la $\mathcal{L}$-structure engendrée par les a_i sur la $\mathcal{L}$-structure engendrée par les b_i.

Cette définition est assez obscure, et il faut donc la commenter. On peut l'écrire en disant que les a_i et les b_i satisfont les mêmes formules atomiques (sans quantificateurs) dans leur structure respective. Par exemple, $f^{\mathfrak{M}}(a_1) = f^{\mathfrak{M}}(a_2)$ si et seulement si $f^{\mathfrak{N}}(b_1) = f^{\mathfrak{N}}(b_2)$. Il est en général assez facile de voir qu'une application est un isomorphisme local.

♦ **Exemple**

- Plaçons nous dans le langage des ordres et considérons deux modèles de la théorie des ordres. Comme il n'y a aucune fonction, l'application qui à a_i fait correspondre b_i sera un isomorphisme local si elle préserve les relations. Comme il n'y a qu'une relation $<$, il suffit que $a_i < a_j \iff b_i < b_j$. Les isomorphismes locaux sont donc ici les fonctions strictement croissantes définies sur une partie finie.
- Considérons les deux modèles finis $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/4\mathbb{Z}, +)$. On va chercher tous les isomorphismes locaux. Comme c'est un morphisme, il envoie 0 sur 0. Comme on a $= (1+1, 0)$ dans la première structure, l'élément sur lequel on envoie 1 doit aussi vérifier cette propriété. On vérifie alors que l'application qui à $(0, 1)$ associe $(0, 2)$ est bien un isomorphisme local. Les isomorphismes locaux sont alors toutes les restrictions de cet isomorphisme.

Il arrive assez souvent que l'on considère l'isomorphisme local qui à $\emptyset$ associe $\emptyset$. Pour vérifier que c'est bien un isomorphisme, il faut bien entendu penser que la $\mathcal{L}$-structure engendrée n'est pas toujours vide, puisqu'elle contient toutes les interprétations des constantes, et donc ensuite la clotûre par les fonctions !

Définissons alors la notion fondamentale, celle de famille karpienne :

Définition 5.2 (*Famille karpienne*)

Un ensemble K d'isomorphismes locaux entre M et N est une *famillekarpienne* si et seulement si

- $K \neq \emptyset$
- K satisfait la propriété de *va* :
  Pour tout $\sigma \in K$, pour tout $a \in M$, il existe $\tau \in K$ tel que
  - $\tau_{|dom\,\sigma} = \sigma$
  - $a \in dom\,\tau$
- K satisfait la propriété de *vient* :
  Pour tout $\sigma \in K$, pour tout $b \in N$, il existe $\tau \in K$ tel que
  - $\tau_{|dom\,\sigma} = \sigma$
  - $b \in im\,\tau$

La proposition ci-dessous donne une caractéristique intéressante d'une famille karpienne.

Proposition 5.1

- L'union de deux familles karpiennes est une famille karpienne.
- Si K est une famille karpienne, l'ensemble des fonctions restrictions de fonctions de K est une famille karpienne.

On en déduit que s'il existe une famille karpienne, il en existe une plus grande (pour l'inclusion), et que celle-ci est stable par restriction.

Définition 5.3 (∞-*isomorphismes*)

S'il existe une famille karpienne K de $\mathfrak{M}$ dans $\mathfrak{N}$, on dit que $\mathfrak{M}$ et $\mathfrak{N}$ sont des *structures* ∞*-équivalentes*. Soit K_{opt} la plus grande famille karpienne de $\mathfrak{M}$ dans $\mathfrak{N}$. Tout élément de K_{opt} est alors appelé un ∞-*isomorphisme*, et les n-uplets $\overline{a}$ et $\overline{b}$ supports de cet isomorphisme sont dits ∞-équivalents.

La notion d'∞-isomorphisme est relativement simple à concevoir : L'application qui envoie $\overline{a}$ sur $\overline{b}$ est un ∞-isomorphisme si pour chaque $a \in M$ je peux trouver un $b \in M$ (et réciproquement) de façon à conserver l'isomorphisme local, et même de façon à trouver un isomorphisme qui vérifie cette définition.

♦ **Exemple**

- Considérons le langage des ordres, et les structures $(\mathbb{N}, <)$ et $(\mathbb{Z}, <)$. L'application qui envoie 0 sur 0 n'est pas un ∞-isomorphisme, bien que ce soit un isomorphisme local. En effet, si je prends -1 dans $\mathbb{Z}$, il me faut trouver, pour satisfaire la propriété de vient, un élément a dans $\mathbb{N}$ tel qu'on ait toujours un ∞-isomorphisme. Mais un ∞-isomorphisme est un isomorphisme local, donc $(0, a)$ et $(0, -1)$ doivent vérifier les mêmes propriétés. Mais $-1 < 0$, et on ne peut avoir $a < 0$, et on a une contradiction.

- Considérons maintenant toujours le même langage, et les structures $(\mathbb{Q}, <)$ et $(\mathbb{R}, <)$. Montrons que l'ensemble des fonctions strictement croissantes de $\mathbb{Q}$ dans $\mathbb{R}$ à support fini est une famille karpienne (donc que ces fonctions sont des ∞-isomorphismes). Soit σ une fonction strictement croissante de $\mathbb{Q}$ dans $\mathbb{R}$, c'est à dire la donnée de $m_i \in \mathbb{Q}$ et $n_i \in \mathbb{R}$, telles que $\forall i, m_i < m_{i+1}, n_i < n_{i+1}$. On veut montrer la propriété de va. On prend donc un $q \in \mathbb{Q}$, et on va essayer de trouver un $r \in \mathbb{R}$ de façon à vérifier les mêmes propriétés, c'est à dire que l'application qui à (m_i, q) associe (n_i, r) est aussi une fonction strictement croissante.
  - Si q est un des m_i, on prend pour r le n_i correspondant.
  - Si $\forall i, q < m_i$, il faut trouver un $r \in \mathbb{R}$ inférieur à tous les n_i. On peut prendre par exemple $\inf n_i - 1$.
  - Si $\forall i, q > m_i$, on peut prendre par exemple $\max n_i + 1$.
  - Le dernier cas est maintenant $m_i < q < m_{i+1}$, pour un certain i. Il suffit alors de prendre $r = \frac{n_i + n_{i+1}}{2}$.

  La démonstration de vient est identique, et on voit que $\mathbb{Q}$ et $\mathbb{R}$ sont ∞-isomorphes.

5.1.2 Structures isomorphes

Les deux propositions suivantes, dont les démonstrations sont relativement simples, ont toutefois un intérêt appréciable.

Proposition 5.2

Deux structures isomorphes sont ∞-isomorphes

Preuve : Soit σ un isomorphisme entre les deux structures. Alors les restrictions finies de σ forment une famille karpienne. ■

Proposition 5.3

Deux structures ∞-isomorphes infinies dénombrables sont isomorphes

Preuve : Soit $\{m_i\}$ et $\{n_i\}$ les deux structures ∞-isomorphes. Construisons par récurrence un ∞-isomorphisme σ_n telle que

- $\forall i \leq n, m_i \in dom\,(\sigma_n)$
- $\forall i \leq n, n_i \in im(\sigma_n)$

- L'amorce de récurrence est immédiate puisque l'application qui à $\emptyset$ associe $\emptyset$ est un ∞-isomorphisme (c'est la restriction d'un ∞-isomorphisme).
- Supposons construit σ_n. En utilisant l'hypothèse de va avec m_{n+1} puis l'hypothèse de vient avec n_{n+1}, le résultat est démontré.

La limite des σ_n est alors un isomorphisme. ■

5.1.3 Équivalence élémentaire

La notion d'∞-isomorphisme est surtout importante pour la propriété suivante :

Proposition 5.4

Deux structures ∞-équivalentes sont élémentairement équivalentes.

Remarque : La réciproque est fausse, mais on verra plus loin dans quel cas elle est valide

Preuve : Par induction sur ϕ, montrons que si $\overline{a}$ et $\overline{b}$ sont ∞-équivalents, alors

$$\mathfrak{M} \models \phi(\overline{a} \iff \mathfrak{N} \models \phi(\overline{b})$$

Il suffira alors d'utiliser la proposition avec $a = \emptyset$ et $b = \emptyset$. Les seuls cas vraiment intéressants sont $\phi = \exists x\psi$, et $\phi = \forall x\psi$. Ils se traitent de façon symétrique, examinons $\phi = \exists x\psi$.

$\mathfrak{M} \models \exists x\phi(\overline{a}, x)$ $\xrightarrow[\text{la satisfaction}]{\text{Définition de}}$ il existe $m \in M, \mathfrak{M} \models \phi(\overline{a}, m)$

Hypothèse $\downarrow$ de **va**

Il existe $n \in N$ tel que $\overline{a}, m$ et $\overline{b}, n$ soient ∞-isomorphes, et $\mathfrak{M} \models \phi(\overline{a}, m)$

Hypothèse $\downarrow$ d'induction

$\mathfrak{N} \models \exists x\phi(\overline{b}, x)$ $\xleftarrow[\text{la satisfaction}]{\text{Définition de}}$ $\mathfrak{N} \models \phi(\overline{b}, n)$

Réciproquement :

$\mathfrak{N} \models \exists x\phi(\overline{b}, x)$ $\xrightarrow[\text{la satisfaction}]{\text{Définition de}}$ il existe $n \in N, \mathfrak{N} \models \phi(\overline{b}, n)$

Hypothèse $\downarrow$ de **vient**

Il existe $m \in M$ tel que $\overline{a}, m$ et $\overline{b}, n$ soient ∞-isomorphes, et $\mathfrak{N} \models \phi(\overline{b}, n)$

Hypothèse $\downarrow$ d'induction

$\mathfrak{M} \models \exists x\phi(\overline{a}, x)$ $\xleftarrow[\text{la satisfaction}]{\text{Définition de}}$ $\mathfrak{M} \models \phi(\overline{a}, m)$

$\blacksquare$

Remarque : Cette démonstration montre tout de suite l'intérêt des ∞-isomorphismes : Ils sont prévus pour que le seul point ennuyeux de la démonstration puisse se résoudre sans difficultés.

L'exemple précédemment étudié nous donne alors le corollaire suivant

Corollaire 5.5

$(\mathbb{R}, <)$ et $(\mathbb{Q}, <)$ sont élémentairement équivalents.

On a (enfin) pu démontrer que deux structures sont élémentairement équivalentes !

5.2 Modèles ω-saturés

La proposition précédente nous permet aisément de montrer que deux structures ∞-isomorphes sont élémentairement équivalentes. La réciproque est fausse, on introduit alors les modèles ω-saturés, pour laquelle on a cette réciproque.

Introduisons auparavant la notion de type.

Définition 5.4 (*Type*)

Un *type* dans $\mathfrak{M}$ est un ensemble de formules $\phi(\overline{a}, \overline{x})$ finiment réalisable, i.e pour tout sous ensemble fini, on peut trouver $\overline{x}$ dans M tel que $\mathfrak{M} \models \phi(\overline{a}, \overline{x})$ pour toutes les formules ϕ considérés. On note $S_n(\overline{a})$ l'ensemble des types en n variables à paramètres dans $\overline{a}$.

♦ **Exemple**

Dans la structure des entiers naturels, l'ensemble des $\phi_n(x)\ :\ x > \underbrace{1 + \cdots + 1}_{n \text{ fois}}$ est finiment satisfaisable : Si on se donne un nombre fini d'entiers, on peut en trouver un plus grand que tous ceux-là.

Comme l'exemple précédent l'indique bien, un type peut être finiment satisfaisable, sans pour autant être satisfaisable : il n'existe pas d'entier supérieur à tous les entiers.

La compacité nous assure tout de même :

Proposition 5.6

Tout type de $S_1(\overline{a})$ est réalisé dans une extension élémentaire de $\mathfrak{M}$

Preuve : Soit $\Phi(x)$ le type considéré. On considère le langage enrichi de la constante c. Alors, tout fragment fini de $Th(M) \cup \Phi(c)$ a comme modèle $\mathfrak{M}$, où on interprète c comme nécessaire, donc cet ensemble a un modèle qui est par construction isomorphe à une extension élémentaire de $\mathfrak{M}$. ■

La notion d'ω-saturation correspond à une réalisation dans la structure elle même :

Définition 5.5 (*Structure ω-saturée*)

$\mathfrak{M}$ est une *structure ω-saturée* si pour tout uple $\overline{a} \in M$, tout type $\Phi(x) \in S_1(\overline{a})$ est réalisé dans M, c'est à dire il existe $m \in M$ tel que pour tout $\phi(x) \in \Phi(x)$, $\mathfrak{M} \models \phi(m)$.

L'exemple ci-dessus nous montre donc que $(\mathbb{N}, <, +)$ n'est pas une structure ω-saturée.

On a vu plus haut qu'il était possible de trouver, pour un type donné, une extension qui réalisait ce type. On a même le fait plus important :

Proposition 5.7

Toute structure a une extension ω-saturée.

Preuve : Soit $\mathfrak{M}$ la structure initiale. On introduit pour chaque type $\Phi(\overline{a}, x)$ une nouvelle constante c_Φ. On considère alors l'ensemble

$$Th(\mathfrak{M}, M) \cup \bigcup_{\Phi} \bigcup_{\phi \in \Phi} \{\phi(\overline{a}, c_\Phi)\}$$

Tout sous-ensemble fini admet $\mathfrak{M}$ comme modèle, donc il existe un modèle de l'ensemble, noté $\mathfrak{M}_1$ tel que tout type de support porté par M soit réalisé dans M_1. En itérant, on obtient alors une suite $\mathfrak{M}_1 \prec \mathfrak{M}_2 \prec \mathfrak{M}_3 \ldots$. On appelle $\mathfrak{N}$ la limite de cette suite. Soit alors $\Phi \in S_1(\overline{a})$ un type. $\overline{a}$ est un ensemble fini, donc il est inclus dans un des $\mathfrak{M}_i$, disons $\mathfrak{M}_n$. Alors ce type est réalisé dans $\mathfrak{M}_{n+1}$, donc dans $\mathfrak{N}$. ■

La relation avec l'élémentaire équivalence est alors la suivante :

Théorème 5.8

Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux structures ω-saturées.

$$\mathfrak{M} \text{ et } \mathfrak{N} \text{ sont élémentairement équivalents } \iff \mathfrak{M} \text{ et } \mathfrak{N} \text{ sont } \infty\text{-équivalents.}$$

Preuve : Il suffit de montrer la réciproque, le sens direct ayant déjà été observé. Il suffit de montrer que l'ensemble F des morphismes qui à $\overline{a}$ associe $\overline{b}$ tels que $\overline{a}$ et $\overline{b}$ satisfont les mêmes formules est une famille karpienne.

- $F \neq \emptyset$, puisque $\emptyset \in F$.
- Montrons la propriété de **va**. Soit $\sigma \in F$ qui à $\overline{a}$ associe $\overline{b}$. Soit $\alpha \in M$. Prenons

$$A = \{\phi(\overline{a}, x), \mathfrak{M} \models \phi(\overline{a}, \alpha)\}$$

  Soit $\phi_1, \ldots, \phi_n$ une partie finie de A satisfaite par α. On a alors

$$\mathfrak{M} \models \exists x \phi_1(\overline{a}, x) \wedge \cdots \wedge \phi_n(\overline{a}, x)$$

  Comme $\sigma \in F$,

$$\mathfrak{N} \models \exists x \phi_1(\overline{b}, x) \wedge \cdots \wedge \phi_n(\overline{b}, x)$$

  Donc $B(x) = \left\{\phi(\overline{b}, x), \phi \in A\right\}$ est finiment réalisable, donc par ω-saturation, $B(x)$ est réalisée pour un certain β. Alors, par construction, l'application qui à $\overline{a}\alpha$ associe $\overline{b}\beta$ est dans F.
- La propriété de **vient** se démontre de manière similaire. ■

On en déduit la propriété fondamentale suivante :

Proposition 5.9

Une théorie est complète si et seulement si tout ses modèles ω-saturés sont ∞-équivalents.

Preuve : $[\Rightarrow]$ est évident, d'après la proposition précédente. Sinon, soit deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T. Ils ont deux extensions élémentaires ω-saturées $\mathfrak{M}'$ et $\mathfrak{N}'$ qui sont ∞-équivalents donc élémentairement équivalentes. Ainsi $\mathfrak{M}$ et $\mathfrak{N}$ sont élémentairement équivalents. ■

On en déduit une méthode pour montrer qu'une théorie est complète.

Méthode 5.10

Pour montrer qu'une théorie T est complète :
- Trouver une famille A qui contient les modèles ω-saturées de T.
- Montrer que deux éléments quelconques de A sont ∞-équivalents.

Il semble à priori difficile d'exhiber exactement les modèles ω-saturés, on donne donc plutôt une famille qui les contient. En effet, comme la famille A contient les modèles ω-saturés de T, on a en particulier montré que deux modèles ω-saturés sont élémentairement équivalents.

On a même plus fort :

Proposition 5.11

Toute structure ∞-équivalente à une structure ω-saturée est ω-saturée.

Ainsi, A est exactement l'ensemble des modèles ω-saturés.

Preuve : Soit $\mathfrak{M}$ ∞-équivalent à $\mathfrak{N}$ ω-saturée. Soit $\overline{a}$ et $\overline{b}$ ∞-équivalents Considérons alors un type $A(x) = \{\phi(\overline{a}, x)\}$. On veut montrer qu'il est réalisé dans $\mathfrak{M}$.

On choisit $\overline{b}$ ∞-équivalent à $\overline{a}$. Par hypothèse, $A(x)$ est finiment consistant. Prenons donc une partie ϕ_i quelconque. Alors

$$\mathfrak{M} \models \exists x \wedge \phi_i(\overline{a}, x)$$

Par ∞-équivalence, donc élémentaire équivalence, on a alors

$$\mathfrak{N} \models \exists x \wedge \phi_i(\overline{b}, x)$$

Donc $B(x) = \left\{\phi(\overline{b}, x), \phi \in A\right\}$ est finiment satisfaisable, donc satisfaisable par β. On utilise alors la propriété de **vient** pour obtenir α tel que $\overline{b}\beta$ et $\overline{a}\alpha$ vérifient les mêmes propriétés, donc en particulier, α satisfait $A(x)$. ∎

5.3 Applications à la complétude

5.3.1 Les ordres denses sans extrêmités

Théorème 5.12

Deux ordres denses sans extrêmités sont ∞-isomorphes

Corollaire 5.13

La théorie des ordres denses sans extrêmités est complète

Démontrons le théorème. Soit deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T. Nous allons montrer que l'ensemble des fonctions strictement croissantes de M dans N est une famille karpienne. Remarquons tout d'abord que ces fonctions sont bien des isomorphismes locaux, et que l'ensemble n'est pas vide.

- Propriété de **va** : Soit σ fonction strictement croissante qui envoie $\overline{a}$ sur $\overline{b}$. Soit α dans M. Il y a plusieurs cas suivant α

- Si α est l'un des $\overline{a}$, σ convient.
- Si α est inférieur à tous les $\overline{a}$. Alors, comme $\mathfrak{N}$ est sans extrêmités, il existe un élément β inférieur à tous les $\overline{b}$, et l'application $\sigma \cup \{\alpha \mapsto \beta\}$ convient.
- Si α est supérieur à tous les $\overline{a}$, la démonstration est identique.
- Si α est entre deux a_i, disons entre a_i et a_{i+1}. Alors, comme $\mathfrak{N}$ est dense, il existe un élément β entre b_i et b_{i+1}, et l'application $\sigma \cup \{\alpha \mapsto \beta\}$ convient.

Dans tous les cas, la propriété de **va** est vérifiée

– On procède de même pour la propriété de **vient**.

La démonstration est terminée.

5.3.2 Les ordres discrets sans extrêmités

La démonstration est ici un peu plus pénible, et va utiliser les modèles ω-saturés. Dans un ordre discret, chaque élément a un successeur et un prédécesseur, que l'on notera $s(x)$ et $p(x)$. Attention : s et p n'appartiennent pas au langage ni à la théorie.

Définition 5.6 (*Distance*)

On appelle distance de x à y, noté $d(x, y)$ la quantité

$$d(x,y) = \begin{cases} \text{Card}\,\{w, x < w \leq y\} & \text{si } x \leq y \\ d(y,x) & \text{sinon} \end{cases}$$

Par exemple, dans $\mathbb{Z}$, la distance de 3 à -5 est 8.

Dans $\{0,1\} \times_{\text{lex}} \mathbb{Z}$, la distance de $(0,4)$ à $(0,6)$ est 2 , mais celle de $(0,0)$ à $(1,0)$ est infinie.

Proposition 5.14

Il existe une formule $\phi_n(x, y)$ qui dit si x et y sont à distance supérieure à n.

Proposition 5.15

Un modèle est ω-saturé si il existe une infinité de points x_i tel

1. Pour tout $i \neq j$ la distance de x_i à x_j est infinie.
2. L'ensemble des x_i forme une chaine dense sans extrêmités.

Preuve : Prenons un modèle $\mathfrak{M}$ ω-saturé.

1. Il suffit de vérifier que si $x_1 \dots x_n$ sont à distance infinie les uns des autres, alors il existe x_{n+1} à distance infinie des n premiers. Pour cela, considérons l'ensemble de formules
$$A(x) = \{\phi_m(x, x_i), m \in \mathbb{N}, i \leq n\}$$
Cet ensemble est finiment satisfaisable. En effet, une partie finie n'évoque qu'un nombre fini de distance majorée par M, et il faut alors trouver un élément à une distance supérieure de M de tous les x_i, ce qui est faisable puisque l'ordre est infini. Comme le modèle est ω-saturé, le type $A(x)$ est satisfait par un x_{n+1}, et on a montré la proposition.

2. Chaine sans extrêmités Il suffit de montrer que pour tout x, il existe y à distance infinie de x supérieure (resp inférieure) à x. En remarquant que
$$A(y) = \{\phi_m(x,y) \wedge x < y, m \in \mathbb{N}\}$$
est un type, on peut conclure

Chaine dense Il suffit de montrer que pour tout $x < x'$, il existe y à distance infinie de x et x' avec $x < y < x'$. Puisque
$$A(y) = \left\{\phi_m(x,y) \wedge \phi_m(x',y) \wedge x < y < x', m \in \mathbb{N}\right\}$$
est un type, on peut aussi conclure. ■

Ainsi, un ordre discret sans extrêmités ω-saturé quotienté par la relation être à distance finie donne un ordre dense sans extrêmités.

Proposition 5.16

Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles qui vérifient la propriété ci-dessus. Alors l'ensemble des applications finies de M et N strictement croissantes qui préservent les distances est une famille karpienne

La démonstration est laissée au lecteur.

Corollaire 5.17

La théorie des ordres discrets sans extrêmités est complète.

5.4 Va et vient fini

Les ∞-isomorphismes ne marchent qu'entre structures saturées. On définit alors naturellement les k-isomorphismes, plus restreints, mais qui permettent de traiter plus de cas

Définition 5.7 (*k-isomorphisme*)

On définit par récurrence sur k le terme k-isomorphisme :

- Tout isomorphisme local est un 0-isomorphisme
- σ est un $k+1$ isomorphisme s'il satisfait :
  - la propriété de *k-va* :
    Pour tout $a \in M$, il existe τ k-isomorphisme tel que :
    - $\tau_{|dom\,\sigma} = \sigma$
    - $a \in dom\,\tau$
  - la propriété de *k-vient* :
    Pour tout $b \in N$, il existe τ k-isomorphisme tel que
    - $\tau_{|dom\,\sigma} = \sigma$
    - $b \in im\,\tau$
- σ est un λ isomorphisme, où λ est un ordinal limite, si c'est un κ isomorphisme pour tout $\kappa < \lambda$

Définition 5.8

Deux structures $\mathfrak{M}$ et $\mathfrak{N}$ sont k-isomorphes si l'application qui envoie $\emptyset(\in M^0)$ sur $\emptyset(\in N^0)$ est un k-isomorphisme.

5.4.1 Lien avec les ∞ isomorphismes

Cette définition est compatible avec la définition donnée précédemment d'un ∞-isomorphisme. On a en effet :

Proposition 5.18

Si σ est un ∞-isomorphisme, c'est un λ-isomorphisme pour tout λ.

Preuve : Soit K une famille karpienne. Montrons par récurrence (transfinie) sur λ que tout élément de K est un λ isomorphisme.
- $\lambda = 0$: Tout élément d'une famille karpienne est un isomorphisme local
- $\lambda = \alpha + 1$. Prenons $\sigma \in K$. Montrons que σ vérifie la propriété de va. Prenons $a \in M$. Alors on sait qu'on peut prolonger σ en $\tau \in K$ de domaine contenant a. $\tau \in K$, donc τ est un α isomorphisme par hypothèse de récurrence. Donc σ vérifie bien la propriété de α-va, de même elle vérifie la propriété de α-vient et c'est bien un $\alpha + 1$ isomorphisme.
- λ ordinal limite : évident ■

La réciproque nécessite un lemme technique :

Lemme 5.19

Soit $\mathfrak{M}$ et $\mathfrak{N}$ deux structures. Il existe λ tel que tout λ-isomorphisme est un κ isomorphisme pour tout κ.

Preuve : Remarquons tout d'abord que tout κ isomorphisme est un λ isomorphisme, pour $\lambda < \kappa$ (preuve par récurrence transfinie sur κ) Ainsi si σ n'est pas un κ isomorphisme, ce n'est pas non plus un λ isomorphisme, pour $\lambda > \kappa$.

À chaque isomorphisme σ on associe A_σ le plus petit ordinal tel que σ ne soit pas un A_σ-isomorphisme, lorsqu'il existe, et sinon $A_\sigma = \infty$. Prenons maintenant λ un cardinal strictement supérieur à tous les A_σ, pour $A_\sigma \neq \infty$. Un tel cardinal existe, il suffit de prendre un cardinal supérieur à $\cup_\sigma A_\sigma$ qui est un ordinal, donc admet un cardinal qui lui est supérieur. Alors on peut voir que λ convient. ■

On a alors la réciproque

Proposition 5.20

Si σ est un κ isomorphisme pour tout κ, c'est un ∞ isomorphisme.

Preuve : Soit λ donné par le lemme précédent. Montrons que l'ensemble K des isomorphismes locaux κ isomorphismes pour tous κ forment une famille karpienne. Soit $\sigma \in K$ et $a \in M$. σ est un $\lambda + 1$-isomorphisme donc il existe τ λ-isomorphisme extension de σ.

Mais alors τ est un λ-isomorphisme, donc κ isomorphisme pour tout κ et $\tau \in K$, on a fini la démonstration. ∎

5.4.2 Equivalence élémentaire

La notion d'∞ isomorphisme est très forte, mais l'ω isomorphisme permet de déterminer aisément l'équivalence élémentaire. Commençons par une définition intuitive :

Définition 5.9 (*Rang de quantification*)

On définit par induction sur ϕ le *rang de quantification* de ϕ par
- Si ϕ est atomique, $r(\phi) = 0$
- $r(\neg\phi) = \phi$, $r(\phi \wedge \psi) = r(\phi \vee \psi) = \max(r(\phi), r(\psi))$
- $r(\exists x\phi) = r(\forall x\phi) = r(\phi) + 1$

Intuitivement, si on représente ϕ par un arbre, c'est le nombre maximal de quantificateurs que l'on rencontre d'une feuille à la racine.

Lemme 5.21

Si σ est un k-isomorphisme (k fini) entre $\overline{m} \in \mathfrak{M}$ et $\overline{n} \in \mathfrak{N}$, alors pour toute formule ϕ de rang de quantification k :

$$\mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\overline{n})$$

Preuve : La preuve se fait par récurrence sur k.
- $k = 0$: C'est la définition d'un isomorphisme local
- $k \to k+1$. On fait une induction sur ϕ, les cas ϕ atomique, $\phi = \neg\psi$, $\phi = \psi\perp\psi'$ étant évidents par hypothèse d'induction. On peut supposer que ϕ commence par $\exists$, le cas $\forall$ étant similaire. Supposons donc $\mathfrak{M} \models \exists x\psi(\overline{m}, x)$, avec ψ de rang de quantification k. Donc il existe a tel que $\mathfrak{M} \models \psi(\overline{m}, a)$. σ est un $k+1$-isomorphisme, donc en utilisant la propriété de va, il existe τ k isomorphisme entre $\overline{m}a$ et $\overline{n}b$ pour un certain b. Mais alors, par hypothèse de récurrence, $\mathfrak{N} \models \psi(\overline{n}, b)$, et donc $\mathfrak{N} \models \exists x\psi(\overline{n}, x)$. La démonstration est identique pour démontrer l'autre implication. ∎

On en déduit le corollaire :

Corollaire 5.22

Deux structures ω-isomorphes sont élémentairement équivalentes

Preuve : Soit σ l'ω isomorphisme en question. Supposons $\mathfrak{M} \models \phi$. Soit k le rang de quantification de ϕ $\mathfrak{M} \models \phi$ et σ est un k-isomorphisme, donc $\mathfrak{N} \models \phi$, et ainsi pour toute formule ϕ,

$$\mathfrak{M} \models \phi \implies \mathfrak{N} \models \phi$$

et on a terminé. ∎

5.4.3 Vers un changement du langage

Le théorème précédent n'admet pas de réciproque immédiate. Le principal problème est la grande complexité des formules mises en jeu. Il suffit qu'il y ait une seule fonction pour que déjà le nombre de formules explose. Il existe deux manières de surmonter le problème :

- Ne considérer, dans le lemme ci dessus, que les formules effilées, c'est à dire tels que tous les arguments des fonctions et des relations présentes sont des variables (on interdit ainsi les $f(f(f\dots(x))))$
- Transformer toutes les fonctions en relations, ce qui a en somme le même résultat.

Les deux transformations permettent de ne pas perdre de pouvoir d'expressivité. Ici, nous utiliserons la deuxième transformation.

La preuve est basé sur le lemme essentiel (appelé Théorème d'Hintinka-Fraïssé dans une de ses variantes)

Lemme 5.23

> Dans un langage qui n'a que des relations (et en nombre fini) et pas de fonctions, pour n donné, il n'y a qu'un nombre fini de n-uples deux à deux non p-isomorphes, chacun de ces uples étant caractérisé par une formule de rang de quantification inférieure à p.

Preuve : Par induction sur k.

- $k = 0$. Il n'y a qu'un nombre fini de relations, donc un nombre fini de formules atomiques à n variables. On les appelle ϕ_i. Mais alors la classe d'isomorphisme local d'un uple $\overline{a}$ qui vit dans un modèle $\mathfrak{M}$ est donné entièrement par la formule :
$$\bigwedge_{i|\mathfrak{M}\models\phi_i(\overline{a})} \phi_i(\overline{x}) \wedge \bigwedge_{i|\mathfrak{M}\models\neg\phi_i(\overline{a})} \neg\phi_i(\overline{x})$$
Et il y a un nombre fini de telles formules.
- $k \to k+1$ Prenons un uple $\overline{a}$, et notons ϕ_i les différentes formules de rang de quantification k qui caractérisent des $n+1$ uples. Alors
$$\bigwedge_{i|\mathfrak{M}\models\exists y\phi_i(\overline{a},y)} \exists y\phi_i(\overline{x},y) \wedge \bigwedge_{i|\mathfrak{M}\models\forall y\neg\phi_i(\overline{a},y)} \forall y\neg\phi_i(\overline{x},y)$$
caractérise les n uples $p+1$-isomorphes à $\overline{a}$, et il y a un nombre fini de telles formules. ■

On en déduit la réciproque d'un des lemmes précédents :

Théorème 5.24

> Dans un langage fini relationnel, deux uples sont k-isomorphes si et seulement si ils satisfont les mêmes formules de rang de quantification inférieure à k.

Preuve : $[\Rightarrow]$ a été fait précédemment.
$[\Leftarrow]$ Deux uples $\overline{m}$ et $\overline{n}$ qui satisfont les mêmes formules de rang de quantifications inférieur à k satisfont en particulier la formule qui caractérise la classe de k-isomorphisme de $\overline{m}$, donc $\overline{n}$ appartient à la classe de k-isomorphisme de $\overline{m}$ et, dit autrement, $\overline{m}$ et $\overline{n}$ sont k isomorphes. ■

On en déduit le corollaire important :

Corollaire 5.25

Deux structures sur un langage fini relationnel sont ω-isomorphes si et seulement si elles sont élémentairement équivalentes

Preuve : [$\Rightarrow$] a été fait précédemment
[$\Leftarrow$] Deux structures élémentairement équivalentes satisfont les mêmes formules de rang de quantification inférieures à k, pour tout k, donc sont k-isomorphes pour tout k, donc sont ω-isomorphes. ■

Exercices

(5 - 1) *(Sur la complétude des ordres discrets sans extrêmités)*
On se place dans le langage contenant uniquement l'ordre $<$. Nous utilisons ici la méthode des k-isomorphismes pour montrer la complétude des ordres discrets sans extrêmités.

Q 1) Montrer que deux isomorphismes locaux sont des $k+1$ isomorphismes si et seulement si les distances inférieures à 2^k sont conservées.

Q 2) En déduire que deux modèles quelconques $\mathfrak{M}$ et $\mathfrak{N}$ sont k-isomorphes pour tout k.

Q 3) En déduire que la théorie est complète.

Q 4) Montrer que $\mathbb{Z}$ et $\{0, 1\} \times \mathbb{Z}$ sont ω isomorphes mais non ∞ isomorphes.

(5 - 2) *(Partiel 2001)*
On se place dans un langage muni de deux relations unaires U et V, et d'une relation binaire R. La structure est censée représenter un graphe biparti : U et V sont les deux ensembles de sommets, et $R(x, y)$ signifie x est relié à y, avec $x \in U$ et $y \in V$.

Q 1) Écrire les formules qui indiquent que la structure est bien un graphe biparti.

On suppose que notre graphe vérifie les propriétés $E_{k,l}$: Pour chaque ensemble fini X_1 de cardinal k et X_2 de cardinal l de sommets dans U (resp. dans V), il existe un sommet dans V (resp. dans U) relié à tous les sommets de X_1 et à aucun sommet de X_2.

Q 2) Écrire les formules $E_{k,l}$ correspondant au comportement indiqué

Q 3) Montrer que U et V sont nécessairement infinis.

Q 4) Montrer que pour chaque ensemble finis X_1 et X_2 de sommets dans U (resp. V) il existe une infinité de sommets dans V (resp U) reliés à tous les sommets de X_1 et à aucun sommet de X_2.

Q 5) Montrer que tout isomorphisme local est un ∞-isomorphisme.

Q 6) Conclure que la théorie est complète et que tous les modèles sont ω-saturés.

Le fait que la théorie est complète a une conséquence inattendue. On appelle B_n l'ensemble des graphes bipartis à n sommets dont les sommets sont étiquetés de 1 à n. Si ϕ est une formule, on note $\phi(B_n)$ l'ensemble des graphes de B_n qui vérifient ϕ, et on note $l(\phi) = \lim_n |\phi(B_n)|/|B_n|$ lorsque la limite existe.

Q 7) Montrer que pour tous k, l on a $l(E_{k,l}) = 1$ (C'est une question de probabilité)

Q 8) En déduire que pour toute formule ϕ, $l(\phi) = 1$ ou $l(\phi) = 0$

(5 - 3) On se place dans le langage contenant uniquement une relation R, et la théorie contenant les axiomes :
– $\forall x, \neg R(x, x)$
– $\forall x, y R(x, y) \implies R(y, x)$
donc dans la théorie des graphes. On appelle G_n l'ensemble des graphes bipartis à n sommets dont les sommets sont étiquetés de 1 à n. Si ϕ est une formule, on note $\phi(G_n)$ l'ensemble des graphes de G_n qui vérifient ϕ, et on note $l(\phi) = \lim_n |\phi(G_n)|/|G_n|$ lorsque la limite existe.

Q 1) En procédant comme dans l'exercice précédent, montrer que pour toute formule ϕ, $l(\phi) = 0$ ou $l(\phi) = 1$. Vérifier que $\{\phi | l(\phi) = 1\}$ est une théorie complète.

(5 - 4) *(Groupes divisibles sans torsions)* On se place dans le langage $\{+, 0\}$ et on s'intéresse aux groupes commutatifs qui vérifient de plus les formules

$$\begin{array}{rl} \phi_n : & nx = 0 \implies x = 0 \\ \psi_n : & \forall x, \exists y, ny = x \end{array}$$

où nx signifie $\underbrace{x + \cdots + x}_{n \text{ fois}}$.

Q 1) Montrer que tout modèle de cette théorie est canoniquement isomorphe à un $\mathbb{Q}$-espace vectoriel. Plus précisément, montrer comment associer de façon canonique à tout modèle de cette théorie un $\mathbb{Q}$-espace vectoriel, et comment tout $\mathbb{Q}$-espace vectoriel peut s'interpréter comme un modèle de cette théorie.

Q 2) Montrer que cette théorie est λ-catégorique pour tout $\lambda > \aleph_0$. Décrire les modèles de cardinal $\aleph_0$.

Q 3) Que manque-t-il à cette théorie pour qu'elle soit complète ?

Q 4) Montrer que cette théorie n'est pas finiment axiomatisable.

Q 5) Montrer que la relation "être colinéaire" n'est pas définissable.

Q 6) Décrire le modèle ω-saturé de cardinal $\aleph_0$.

(5 - 5) *(Théorie des modèles finis)*

Q 1) Dans le langage vide, montrer que deux structures de cardinal supérieur à m sont m-isomorphes.

Q 2) Montrer qu'il n'existe pas de formule de rang de quantification inférieure (strictement) à m qui exprime que le cardinal de la structure est supérieur à m.

Q 3) Dans le langage $<$, montrer qu'il n'existe pas de formule de rang de quantification inférieure à k pour traduire le fait que le cardinal de la structure est supérieur à 2^m.

Q 4) Construire une formule de rang de quantification $O(m)$ qui implique que le cardinal est supérieur à 2^m, lorsque $<$ est interprété comme une relation d'ordre total.

Chapitre 6

ÉLIMINATION DES QUANTEURS

Dans $\mathbb{R}$, la formule

$$\phi(a,b,c) = \exists x, ax^2 + bx + c = 0$$

est équivalente à

$$\psi(a,b,c) = ((a \neq 0) \land b^2 - 4ac \geq 0) \lor (a = 0 \land b = 0 \rightarrow c = 0)$$

De même, la formule

$$\phi(a,b) = \forall x, x > 0 \rightarrow ax + b > 0$$

est équivalente à

$$\psi(a,b) = (ab > 0) \lor (a = 0 \land b > 0)$$

Dans les deux cas, on a pu obtenir une formule équivalente sans $\forall$ ni $\exists$, c'est ce qu'on appelle **L'élimination des quanteurs**.

6.1 Ensemble d'élimination

Définition 6.1 (*Ensemble d'élimination*)

Un ensemble E de formules (avec éventuellement des paramètres) est appelé un *ensemble d'élimination* d'une théorie T si toute formule ϕ est équivalente à une combinaison booléene de formules dans E.
Dit autrement :

Pour toute formule ϕ, il existe ψ combinaison booléenne de formules dans E, tel que pour tout modèle $\mathfrak{M}$ de T et tout n-uplet $\overline{m}$,

$$\mathfrak{M} \models \phi(\overline{m}) \leftrightarrow \psi(\overline{m})$$

Théorème 6.1

Un ensemble E est un ensemble d'élimination si et seulement si pour tous modèles $\mathfrak{N}$ et $\mathfrak{M}$ et tout uples $\overline{n}$ et $\overline{m}$,

Si $\overline{n}$ et $\overline{m}$ satisfont les mêmes formules dans E, $\overline{n}$ et $\overline{m}$ satisfont les mêmes formules

Preuve : On va montrer le théorème en trois étapes :

1. Etant donné une formule ϕ, il existe un ensemble fini Θ de formules combinaisons booléennes de formules de E tel que dans chaque modèle $\mathfrak{M}$, ϕ soit équivalente à une formule $\psi_{\mathfrak{M}}$ de Θ.

2. Etant donné une formule ϕ et un modèle $\mathfrak{M}$, il existe un ensemble $\Sigma_{\mathfrak{M}}$ d'énoncés de E telle que tout modèle $\mathfrak{N}$ de $\Sigma_{\mathfrak{M}} \cup T$ vérifie $\mathfrak{N} \models \phi \leftrightarrow \psi_{\mathfrak{M}}$
3. Etant donné une formule ϕ, il existe une formule ψ combinaison booléenne de formules de E tel que dans chaque modèle, ϕ soit équivalente à une formule de ψ.

1. Considérons une formule ϕ quelconque et considérons

$$\Phi = T \cup \left\{\psi(\overline{c}) \leftrightarrow \psi(\overline{d})\right\} \cup \{\phi(\overline{c})\} \cup \left\{\neg\phi(\overline{d})\right\}$$

pour c et d des nouvelles constantes.

Φ n'a pas de modèles, puisque sinon les interprétation des uplets $\overline{c}$ et $\overline{d}$ vérifieraient les mêmes formules dans E, mais pas les mêmes formules.

Par compacité, il existe donc une sous-partie de Φ qui n'admet pas de modèle, notons là Φ_0. Plusieurs cas se présentent suivant Φ_0 :

   - Si Φ_0 ne contient ni $\phi(\overline{c})$ et $\neg\phi(\overline{d})$, alors tout modèle de T est un modèle de Φ_0, en prenant une interprétation quelconque pour $\overline{c} = \overline{d}$, ce qui est contradictoire.
   - Si Φ_0 ne contient que $\phi(\overline{c})$ et non $\neg\phi(\overline{d})$. Alors, si Φ_0 n'a pas de modèles, celà signifie que dans chaque modèle $\mathfrak{M}$, on a $\forall\overline{x}, \neg\phi(\overline{x})$ (sinon,on pourrait prendre un uplet $\overline{m}$ qui contredit la propriété comme interprétation de $\overline{c}$ et $\overline{d}$).

     Dans ce cas, $\phi \leftrightarrow$ faux, qui est bien une combinaison booléene de formules dans E.
   - Sinon, Φ_0 contient $\phi(\overline{c})$ et $\neg\phi(\overline{d})$. Ainsi, la sous-famille contradictoire est de la forme

$$\Phi_0 = T_0 \cup \left\{\psi_i(\overline{c}) \leftrightarrow \psi_i(\overline{d}), i < n\right\} \cup \{\phi(\overline{c})\} \cup \left\{\neg\phi(\overline{d})\right\}$$

     avec $T_0 \subset T$.

     Soit $\mathfrak{M}$ un modèle de T. Soit $\overline{x}$ et $\overline{y}$ deux uples. En interprétant $\overline{c}$ par $\overline{x}$ et $\overline{d}$ par $\overline{y}$, on sait que $\mathfrak{M}$ n'est pas un modèle de Φ_0, donc si $\forall i < n, \psi_i(\overline{x}) \leftrightarrow \psi_i(\overline{y})$, alors $\phi(\overline{x}) \leftrightarrow \phi(\overline{y})$. Ainsi, ϕ est équivalente à une des combinaisons booléennes obtenue à partir des $\{\psi_i, i < n\}$, et il y en a un nombre fini, à équivalence près.

   On a pu conclure dans tous les cas, la première partie est démontrée.
2. Considérons l'ensemble

$$\Phi = T \cup \{\psi, \psi \in E, \mathfrak{M} \models \psi\} \cup \neg(\forall x, \psi_{\mathfrak{M}}(\overline{x}) \leftrightarrow \phi(\overline{x}))$$

   Montrons que Φ n'a pas de modèle. Si $\mathfrak{N}$ est un modèle de Φ, alors il vérifie les mêmes énoncés dans E que $\mathfrak{M}$, donc il est élémentairement équivalent à $\mathfrak{M}$, par hypothèse appliquée au uple vide. Donc, comme

$$\mathfrak{M} \models \forall x, \psi_{\mathfrak{M}}(\overline{x}) \leftrightarrow \phi(\overline{x})$$

On en déduit
$$\mathfrak{N} \models \forall x, \psi_{\mathfrak{M}}(\overline{x}) \leftrightarrow \phi(\overline{x})$$
et $\mathfrak{N}$ n'est donc pas un modèle de Φ. Ainsi, Φ n'a pas de modèle, donc une sous-partie Φ_0 n'a pas de modèle, et cette sous partie est de la forme
$$\Phi_0 = T_0 \cup \{\psi_i, \psi_i \in E, \mathfrak{M} \models \psi_i, i < n\} \cup \neg(\forall x, \psi_{\mathfrak{M}}(\overline{x}) \leftrightarrow \phi(\overline{x})$$
(Le dernier terme est forcément présent, sinon $\mathfrak{M}$ serait un modèle de Φ_0) Ainsi, en prenant
$$\Sigma_{\mathfrak{M}} = \{\psi_i, \psi_i \in E, \mathfrak{M} \models \psi_i, i < n\}$$
on a montré la deuxième partie.

3. On pose $\sigma_{\mathfrak{M}}$ la conjonction des éléments de $\Sigma_{\mathfrak{M}}$. Le nombre d'énoncé dans E est majoré par $|\mathcal{L}| + \omega$, il est donc cohérent de parler de l'ensemble :
$$\{\sigma_{\mathfrak{M}}, \mathfrak{M} \models T\}$$
Considérons
$$\Phi = T \cup \{\neg\sigma_{\mathfrak{M}}, \mathfrak{M} \models T\}$$
Par construction, Φ n'a pas de modèle, donc une sous-partie finie Φ_0 n'a pas de modèle, avec
$$\Phi_0 = T_0 \cup \{\neg\sigma_{\mathfrak{M}i}, i < n\}$$
Ainsi tout modèle de T vérifie $\vee\sigma_{\mathfrak{M}_i}$, et comme pour chaque $\mathfrak{M}_i$, on a
$$\sigma_{\mathfrak{M}_i} \rightarrow (\phi \leftrightarrow \psi_{\mathfrak{M}_i})$$
on en déduit
$$\phi \leftrightarrow \vee(\psi_{\mathfrak{M}_i} \wedge \sigma_{\mathfrak{M}_i})$$
Le théorème est (enfin) prouvé.

■

6.2 Élimination des quanteurs

Définition 6.2 (*Élimination des quanteurs*)

Une théorie T élimine les quanteurs si l'ensemble des formules atomiques est un ensemble d'élimination.

Afin de prouver qu'une théorie élimine les quanteurs, nous allons utiliser du lemme suivant :

Lemme 6.2

Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux structures ω-saturées. On suppose que deux uples qui satisfont les mêmes formules atomiques satisfont les mêmes formules de la forme $\exists x\phi(x, \overline{y})$, où ϕ est sans quanteurs. Alors tout isomorphisme local est un ∞-isomorphisme (Donc tout isomorphisme local est un morphisme élémentaire).

Preuve : Soit σ un isomorphisme local qui envoie $\overline{m}$ sur $\overline{n}$. Montrons la propriété de va, la propriété duale se montrant de façon analogue. Considérons donc α dans M. On note $\Phi(\overline{m}, x)$ l'ensemble des formules atomiques satisfaites par α dans $M\mathfrak{M}$. On veut en fait montrer $\Phi(\overline{n}, x)$ est un type sur $\mathfrak{N}$.

Pour chaque sous-ensemble Φ_0 fini de $\Phi(\overline{n}, x)$, auquel correspond un sous-ensemble Ψ_0 de $\Phi(\overline{m}, x)$, on a

$$\mathfrak{M} \models \exists x \wedge \Psi_0(\overline{m}, x)$$

En utilisant l'hypothèse, on a alors :

$$\mathfrak{N} \models \exists x \wedge \Phi_0(\overline{n}, x)$$

Donc $\Phi(\overline{n}, x)$ est bien un type, et on peut trouver β dans N tel que $\mathfrak{N} \models \Phi(\overline{n}, \beta)$. ■

On peut alors donner une caractérisation des théories qui éliminent les quanteurs :

Proposition 6.3

Une théorie T élimine les quanteurs si pour tous modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T, deux uples qui satisfont les mêmes formules atomiques satisfont les mêmes formules de la forme $\exists x\phi(x, \overline{y})$, ϕ sans quanteurs.

Preuve : Prenons deux modèles $\mathfrak{M}$ et $\mathfrak{N}$, et $\overline{m}$ et $\overline{n}$ deux uples satisfaisant les mêmes formules atomiques. On veut montrer que $\overline{m}$ et $\overline{n}$ satisfont les mêmes formules, et le théorème de la section précédente permettra de conclure.

Considérons deux extensions ω-saturées $\mathfrak{M}_0$ et $\mathfrak{N}_0$ de $\mathfrak{M}$ et $\mathfrak{N}$. Alors $\overline{m}$ et $\overline{n}$ satisfont les mêmes formules atomiques dans $\mathfrak{M}_0$ et $\mathfrak{N}_0$, donc en utilisant le lemme précédent, on sait que $\overline{m}$ et $\overline{n}$ sont ∞-équivalents dans $\mathfrak{M}_0$ et $\mathfrak{N}_0$, donc satisfont les mêmes formules dans $\mathfrak{M}_0$ et $\mathfrak{N}_0$, donc dans $\mathfrak{M}$ et $\mathfrak{N}$ par sous-structure élémentaire. ■

6.3 Modèle-complétude

Définition 6.3 (*Modèle-complétude*)

Une théorie T est une *théorie modèle-complète* si toute inclusion de modèles est élémentaire.

Le rapport avec l'élimination des quanteurs est le suivant :

Proposition 6.4

Une théorie qui élimine les quanteurs est modèle-complète.

Preuve : Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux modèles de T, avec $\mathfrak{M} \subset \mathfrak{N}$. Soit $\phi(\overline{m})$ une formule à paramètres dans $\mathfrak{M}$. Par élimination, ϕ est équivalente dans tout modèle à une formule $\psi(x)$ sans quanteurs. Comme ψ est sans quanteurs, on a

$$\mathfrak{M} \models \psi(\overline{m}) \iff \mathfrak{N} \models \psi(\overline{m})$$

Donc
$$\mathfrak{M} \models \phi(\overline{m}) \iff \mathfrak{N} \models \phi(\overline{m})$$

■

La réciproque est malheureusement fausse : La théorie de $\mathbb{R}$ considéré comme anneau est modèle complète, mais n'élimine pas les quanteurs. En effet, $\exists y, y^2 = x$ n'est pas équivalente à une formule sans quanteurs ND . Pourtant, si on rajoute l'ordre à $\mathbb{R}$, on peut démontrer que la théorie obtenue élimine alors les quanteurs.

Ainsi, la propriété d'élimination dépend (hélas) du langage.

Le dernier théorème important, et dont la preuve est remarquablement compliquée, est le suivant

Théorème 6.5

> Une théorie est modèle-complète si et seulement si toute formule est équivalente à une formule existentielle.

Preuve :

– [$\Leftarrow$] est relativement simple, et laissé au lecteur à titre d'exercice.
– [$\Rightarrow$] Nous procéderons en plusieurs points :

1. **Toute formule est équivalente à une combinaison booléenne de formules existentielles.** Une fois que ce fait aura été établi, il ne restera plus qu'à montrer qu'une formule universelle est équivalente à une formule existentielle. En effet, le $\wedge$ et le $\vee$ de deux formules existentielles donne une formule existentielle, mais le $\neg$ nous donne une formule universelle, qu'il faudrait transformer en formule existentielle.
2. **Toute formule universelle est équivalente à une formule existentielle**

1. On va en fait montrer que l'ensemble des formules existentielles est un ensemble d'élimination. Prenons deux modèles $\mathfrak{M}$ et $\mathfrak{N}$ de T et deux uples $\overline{m}$ et $\overline{n}$ qui vérifient les mêmes formules existentielles. On veut montrer qu'ils satisfont les mêmes formules.

   On note $c_m, m \in M$ des nouvelles constantes. Il s'agit donc d'une copie de M. Considérons
$$\Phi = Th(\mathfrak{N}, N) \cup \{\phi(c_{m_1}, \ldots, c_{m_n}, \overline{n}), \mathfrak{M} \models \phi(m_1, \ldots, m_k, \overline{m}, \phi\text{atomique}\}$$

   Prenons un sous-ensemble fini de Φ. Il n'évoque qu'un nombre fini de propositions $\phi(c_{m_1}, \ldots, c_{m_n}, \overline{n})$ Quitte à prendre leur conjonction, on peut supposer qu'il n'y en a qu'une seule. Alors, par construction de Φ,
$$\mathfrak{M} \models \phi(m_1, \ldots, m_k, \overline{m})$$

   donc
$$\mathfrak{M} \models \exists x_1, \ldots x_k, \phi(x_1, \ldots, x_k, \overline{m})$$

   Comme $\overline{n}$ et $\overline{m}$ satisfont les mêmes formules existentielles,
$$\mathfrak{N} \models \exists x_1, \ldots x_k, \phi(x_1, \ldots, x_k, \overline{n})$$

Donc il existe $n_1, \dots n_k$ tel que

$$\mathfrak{N} \models \phi(n_1, \dots, n_k, \overline{n})$$

Alors $\mathfrak{N}$ dans lequel on interprète $c_{m_1}, \dots, c_{m_n}$ par $n_1, \dots n_k$ est un modèle de la sous-partie finie. Par compacité, on en déduit que Φ a un modèle, appelé $\mathfrak{N}'$. Comme Φ contient $Th(\mathfrak{N}, N)$, on en déduit qu'en fait $\mathfrak{N}'$ est une extension élémentaire de $\mathfrak{N}$. De plus, par construction, $\mathfrak{N}'$ contient une copie de $\mathfrak{M}$, notée $\mathfrak{M}'$. On remarquera que l'image du uplet $\overline{m}$ est le uple $\overline{n}$ en considérant par exemple la formule atomique

$$\phi(c_{m_1}, \dots c_{m_k}, \overline{m}) = c_{m_1} = m_1 \wedge \dots c_{m_k} = m_k$$

Comme $\mathfrak{M}' \subset \mathfrak{N}'$, on en déduit par hypothèse de modèle complétude que $\mathfrak{M}'$ est élémentairement équivalente à $\mathfrak{N}'$.

On peut maintenant finir, en démontrant que $\overline{m}$ et $\overline{n}$ satisfont les mêmes formules. Prenons une formule $\psi(\overline{x})$.

Alors

$$\begin{tikzcd}
\mathfrak{M} \models \psi(\overline{m}) \arrow[r, leftrightarrow, "\mathfrak{M}' \text{ est une}", "\text{copie de } \mathfrak{M}"'] & \mathfrak{M}' \models \psi(\overline{n}) \arrow[d, leftrightarrow, "\text{modèle}"', "\text{complétude}"] \\
\mathfrak{N} \models \psi(\overline{n}) \arrow[r, leftrightarrow, "\mathfrak{N}' \text{ extension}", "\text{élémentaire de } \mathfrak{N}"'] & \mathfrak{N}' \models \psi(\overline{n})
\end{tikzcd}$$

Ainsi l'hypothèse nécessaire à l'application du théorème est prouvé, et l'ensemble des formules existentielles est bien un ensemble d'élimination

2. On va maintenant prendre une formule universelle $\phi(\overline{y})$ et montrer qu'elle est équivalente à une formule existentielle. Notons $\Phi(\overline{x})$ l'ensemble des formules existentielles ψ qui impliquent $\phi(\overline{x})$, c'est à dire

$$\forall \mathfrak{M}, \mathfrak{M} \models (\forall \overline{x} \psi(\overline{x}) \to \phi(\overline{x}))$$

Remarquons que Φ est stable par $\vee$. Et notons $\Psi(\overline{x}) = \{\neg\psi, \psi \in phi(\overline{x})\}$

On pose

$$\Theta = T \cup \Psi(\overline{c}) \cup \{\phi(\overline{c})\}$$

On va montrer

(a) Θ n'a pas de modèles.

(b) ϕ est équivalente à une formule existentielle.

Effectuons maintenant les deux preuves.

(a) Supposons que Θ ait un modèle $\mathfrak{M}$. Appelons $\Phi_0(\overline{x})$ l'ensemble des formules existentielles vérifiées par $\overline{c}^{\mathfrak{M}}$, l'interprétation de $\overline{c}$. Alors

$$T \cup \Phi_0(\overline{d}) \cup \{\neg\phi(\overline{d})\}$$

ne peut avoir de modèles ($\overline{c}$ et $\overline{d}$ vérifieraient en effet les mêmes formules existentielles, donc les mêmes formules, ce qui est impossible)

On a donc un sous-ensemble fini contradictoire qui contient nécessairement $\{\neg\phi(\overline{d})\}$, donc de la forme

$$T_0 \cup \Phi'_0(\overline{d}) \cup \{\neg\phi(\overline{d})\}$$

pour un certain Φ'_0 fini. En posant $\psi = \wedge\Phi'_0$, on voit que tout modèle de T qui vérifie $\psi(\overline{m})$ pour un certain uplet vérifie également $\phi(\overline{m})$, ce qui signifie que $\psi \in \Phi$. Donc par construction du modèle $\mathfrak{M}$, $\mathfrak{M} \models \neg\psi(\overline{c})$ Pourtant, comme $\psi \in \Phi_0$, on a $\mathfrak{M} \models \psi(\overline{c})$. La contradiction est flagrante !

(b) Ainsi l'ensemble Θ n'a pas de modèle, et admet une partie finie contradictoire de la forme $T_0 \cup \Psi_0 \cup \{\phi(\overline{c})\}$. Notons $\theta = \wedge\Psi_0$ Mais dans ce cas, dans tout modèle $\mathfrak{M}$ de T, $\mathfrak{M} \models \forall x, \phi(\overline{x}) \to \neg\theta(x)$ Et

$$\neg\theta = \vee\{\neg\psi, \psi \in \Psi_0\} = \vee\{\neg\neg\psi, \psi \in \Phi\}$$

Donc $\neg\theta$ est équivalente à une formule dans Φ, c'est à dire dans tout modèle $\mathfrak{M}$ de T, on a $\mathfrak{M} \models \forall x, \neg\theta(\overline{x}) \to \phi(x)$ Donc ϕ est équivalente à la formule $\neg\theta$, qui est bien équivalente à une formule existentielle.

Le théorème est (enfin !) prouvé. ■

Exercices

(6 - 1) On se place dans le langage des groupes, et on s'intéresse à la théorie des groupes vérifiant $(\forall x, x^5 = x)$. Eliminer les quanteurs dans les formules :

- $\theta(x) = \exists y, x = y \cdot x$
- $\xi(x) = \forall y, y = y \cdot x$
- $\tilde{\xi}(x) = \exists y, y = y \cdot x$
- $\phi(x) = \exists y, x = y \cdot y$
- $\psi(x) = \exists z, x \neq z \wedge \forall y, x = y \cdot x$
- $\alpha(x) = \exists y, x = y \cdot y \cdot y$

(6 - 2) Donner un exemple d'une théorie modèle-complète non complète

Remarque : On verra dans le chapitre suivant que la théorie des corps algébriquement clos est modèle-complète sans être complète (il manque uniquement la caractéristique du corps). Nous demandons évidemment ici un autre exemple.

(6 - 3) Soit T une théorie. On ajoute au langage $\mathcal{L}$ les relations n-aires R_ϕ pour toute $\mathcal{L}$ formule ϕ n-aire, obtenant ainsi le langage $\mathcal{L}'$. On considère la théorie T' :

$$T' = T \cup \{\forall x_1 \dots x_n, \phi(x_1 \dots x_n) \iff R_\phi(x_1 \dots x_n), \phi\ \mathcal{L} - \text{formule}\}$$

Q 1) Montrer que tout modèle $\mathfrak{M}$ s'étend de façon unique en un modèle de $\mathfrak{M}'$.

Q 2) Montrer que tout $\mathcal{L}'$-formule est équivalente modulo T' à une $\mathcal{L}$ formule.

Q 3) Montrer que T' élimine les quanteurs

Q 4) Montrer que T est modèle complète si et seulement si

$$M \subset N \implies M' \subset N'$$

(6 - 4) On se place dans la théorie des ordres.

Q 1) Donner un exemple d'une chaîne avec maximum ayant une restriction sans maximum.

Q 2) Donner un exemple d'une chaîne sans maximum ayant une restriction avec maximum.

Q 3) Montrer que l'énoncé $\forall x \exists y, x < y$ n'est synonyme d'aucun énoncé universel ni d'aucun énoncé existentiel.

Problème 2

On s'intéresse ici à la notion de modèle-complétion et à la différence précise entre élimination des quantificateurs et modèle-complétude.

PARTIE 1 - Préliminaires

Q 1) On se place dans le langage $\{<\}$. Soit T une théorie qui contient les axiomes spécifiant que $<$ est un ordre total et que tout modèle contient au moins 2 éléments. Montrer que T élimine les quantificateurs si et seulement si T est la théorie des ordres denses sans extrêmités.

Q 2) Soit T et T' deux théories modèles-complètes. On suppose que tout modèle de T s'injecte élémentairement dans un modèle de T' et réciproquement. Montrer que T et T' sont équivalentes (tout modèle de T est un modèle de T'). (on pourra utiliser une chaîne de modèles).

PARTIE 2 - Modèle complétion

Définition 6.4

On appelle modèle-complétion d'une théorie T une théorie $T^\star$ avec $T \subset T^\star$ telle que pour tout modèle $\mathfrak{M}$ de T

- Il existe un modèle de $T^\star$ qui contient $\mathfrak{M}$
- Tous les modèles de $T^\star$ qui contiennent $\mathfrak{M}$ sont élémentairement équivalents.

Q 1) Montrer que $T^\star$ est modèle-complète

Q 2) Montrer en utilisant une question précédente qu'il n'existe qu'une seule modèle-complétion (c'est à dire : deux modèle-complétions d'une même théorie ont les mêmes modèles). En déduire que si T est modèle-complète, c'est sa propre modèle-complétion.

Q 3) Montrer qu'une théorie complète non modèle-complète n'admet pas de modèle-complétion. En donner un exemple.

PARTIE 3 - Modèle complétion - Application

Q 1) Montrer que la théorie des ordres denses sans extrêmités est la modèle complétion de la théorie des ordres totaux avec au moins 2 éléments.

On se place dans le langage des corps. On admet que la théorie des corps algébriquement clos élimine les quantificateurs, et que deux corps algébriquement clos sont équivalents si et seulement si ils ont même caractéristique.

Q 2) Montrer que la théorie des corps algébriquement clos est la modèle complétion de la théorie des corps infinis.

Q 3) Soit T une théorie contenant les axiomes signifiant que tout modèle est un corps, et tout modèle est infini. Montrer que si T élimine les quantificateurs, tout modèle de T est un corps algébriquement clos.

PARTIE 4 - Sous-modèle complétude

On va supposer (c'est un point de détail) que toutes les théories qu'on manipule ont au moins une constante.

Définition 6.5

> On dit qu'une théorie T est sous-modèle complète si tous modèles $\mathfrak{M}_1, \mathfrak{M}_2$ de T qui possèdent une sous-**structure** commune $\mathfrak{N}$ sont élémentairement équivalents dans le langage $\mathcal{L} \cup \{c_i, i \in N\}$.

Q 1) Montrer qu'une théorie qui élimine les quantificateurs est sous-modèle complète.

Q 2) Montrer qu'une théorie sous-modèle complète est modèle-complète.

Si $\overline{m}$ est un tuple d'une structure $\mathfrak{M}$, on note $\langle \overline{m} \rangle$, la structure *engendrée* par $\overline{m}$, la plus-petite sous-structure de $\mathfrak{M}$ qui contient $\overline{m}$.

Q 3) Montrer que si $\overline{m}$ et $\overline{n}$ satisfont les mêmes formules atomiques, elles engendrent des sous-structures isomorphes.

Q 4) Montrer qu'une théorie sous-modèle complète élimine les quantificateurs.

Chapitre 7

LES CORPS ALGÉBRIQUEMENT CLOS ET RÉEL CLOS

Les exemples précedemment étudiés, comme les ordres denses sans extrêmités, étaient relativement faciles, et ne montraient pas vraiment la puissance de la théorie des modèles. Nous allons ici nous intéresser à des théories bien plus proches de l'algèbre. Là encore la théorie des modèles va nous permettre bien souvent de démontrer facilement des propriétés intéressantes.

7.1 Les corps algébriquement clos (ACF)

On s'intéresse ici à la théorie ACF donnée par les axiomes :

- La théorie des corps (structure de groupe vis-à-vis de la loi $+$, et de la loi $\times$, distributivité de $\times$ sur $+, \ldots$) (Noter que l'inverse pour $\times$ n'est pas dans le language)
- Tout polynôme unitaire a une racine : Cela correspond aux énoncés ϕ_n :

$$\phi_n : \forall a_1, \ldots a_n, \exists x, x^n + a_1 x^{n-1} + \ldots a_n = 0$$

Notons que cette théorie n'est pas complète : En effet, on ne dit rien sur la caractéristique des corps (i.e, la formule $\forall x, x + x = 0$ n'est pas conséquence de la théorie, ni sa négation). Le modèle le plus connu est bien entendu le corps des complexes, qui est même ω-saturé ND.

Néanmoins, nous avons la propriété d'élimination

Théorème 7.1

La théorie ACF élimine les quanteurs.

Preuve : Prenons deux corps ACF $\mathbb{K}$ et $\mathbb{L}$, et deux uples $\overline{a} \in \mathbb{K}$, $\overline{b} \in \mathbb{L}$ qui satisfont les mêmes formules atomiques. Prenons une formule $\phi(x, \overline{y})$ sans quanteurs. On veut démontrer

$$\mathbb{K} \models \exists x \phi(x, \overline{a}) \iff \mathbb{L} \models \exists x \phi(x, \overline{b})$$

Le théorème d'élimination nous permettra alors de conclure.

$\overline{a}$ et $\overline{b}$ engendrent deux sous-corps $\mathbb{A}$ et $\mathbb{B}$ isomorphes. Examinons la formule ϕ. C'est une combinaison booléenne d'égalités de termes atomiques, ceux-ci étant en fait des polynômes en les variables $x, y_1 \ldots y_n$ à coefficients dans $\mathbb{Z}$. Toute formule atomique est donc équivalente à une disjonction finie de formules de la forme $\wedge f_i(x, \overline{y}) = 0 \wedge g(x, \overline{y}) \neq 0$ f_i et g polynômes dans $\mathbb{Z}$. La formule $\mathbb{K} \models \exists x \phi(x, \overline{a})$ est donc vraie si une des formules ci-dessus est vraie. On va donc montrer

$$\mathbb{K} \models \exists x \wedge f_i(x, \overline{a}) = 0 \wedge g(x, \overline{a}) \neq 0 \iff \mathbb{L} \models \exists x \wedge f_i(x, \overline{b}) = 0 \wedge g(x, \overline{b}) \neq 0$$

Le résultat sera alors démontré.

- Si $\wedge f_i(x,\overline{a}) = 0$ définit un ensemble fini de $\mathbb{K}$, Ses solutions sont dans $\tilde{\mathbb{A}}$, la clotûre algébrique de $\mathbb{A}$. Comme celle-ci est isomorphe à $\tilde{\mathbb{B}}$, $g(x,\overline{a}) \neq 0$ a une solution dans cet ensemble fini pour $\mathbb{K}$ si et seulement si $g(x,\overline{a}) \neq 0$ a une solution dans l'ensemble fini isomorphe.
- Si $\wedge f_i(x,\overline{a}) = 0$ définit un ensemble infini de $\mathbb{K}$, c'est à dire : tous les f_i sont triviaux, donc tout x est solution. Il y a deux cas suivant g :
  - g est trivial (c'est une constante non nulle). Dans ce cas, il ne peut y avoir de solutions dans $\mathbb{L}$ ou dans $\mathbb{K}$.
  - Sinon $g(x) \neq 0$ désigne un ensemble co-fini. Donc $g(x) \neq 0$ admet une solution dans $\mathbb{K}$ et dans $\mathbb{L}$

Dans tout les cas, $\mathbb{K} \models \exists x\phi(x,\overline{a}) \iff \mathbb{L} \models \exists x\phi(x,\overline{b})$, et on a terminé. ■

Bien que la théorie ACF ne soit pas complète, elle y est presque, puisqu'on a le théorème :

Théorème 7.2

- La théorie ACF$_p$ des corps algébriquement clos de caractéristique p donné est complète. De plus, tout énoncé à paramètres $\overline{a}$ est soit vrai dans tout corps, soit faux dans tout corps algébriquement clos qui contient le sous corps engendré par $\overline{a}$.
- Un énoncé est vrai dans tout corps de caractéristique nulle si et seulement si il est vrai dans tout corps de caractéristique p première , sauf un nombre fini

Preuve :

- Il suffit de montrer la seconde propriété, qui implique la première en prenant $\overline{a} = 0, 1$, puisque tout corps contient le sous-corps engendré par 0 et 1.
  Prenons donc une formule $\phi(\overline{a})$ et $\mathbb{K}$ et $\mathbb{L}$ deux corps qui contiennent le corps engendré par $\phi(\overline{a})$, noté $\mathbb{A}$. Alors $\overline{a}$ satisfait les mêmes formules sans quanteurs dans $\mathbb{K}$ et dans $\mathbb{A}$, les mêmes formules sans quanteurs dans $\mathbb{L}$ et dans $\mathbb{A}$, donc par transitivé les mêmes formules dans $\mathbb{K}$ et dans $\mathbb{L}$. Par élimination des quanteurs, on sait alors que $\overline{a}$ vérifie les mêmes formules dans $\mathbb{K}$ et dans $\mathbb{L}$. Donc $\mathbb{K} \models \phi(\overline{a}) \iff \mathbb{L} \models \phi(\overline{a})$.
- Prenons ϕ un énoncé, et supposons ϕ vraie dans tout corps algébriquement clos de caractéristique p, sauf un nombre fini. Il existe donc p' tel que ϕ soit vraie dans tout corps de caractéristique $p > p'$.
  considérons
  $$\Phi = ACF_0 \cup \{\phi\}$$
  Où ACF_0 est la théorie ACF agrémenté des axiomes $1 + \ldots 1 \neq 0$. Toute partie finie de Φ n'utilise qu'un nombre fini d'axiomes de la forme précédente, donc a un modèle, en choisissant une caractéristique suffisament grande. Ainsi Φ a un modèle, donc ϕ est vraie dans un corps de caractéristique 0 , donc dans tout corps de caractértistique 0 par complétude.
  Pour la réciproque, il suffit de considérer $\neg\phi$. ■

Examinons maintenant quelques applications de la complétude et de la modèle-complétude. L'élimination des quanteurs nous donne la modèle-complétude, et permet de retrouver, en particulier, ce fameux théorème.

Théorème 7.3 (*Théorème des Zéros de Hilbert*)

Soit $\mathbb{K}$ est un corps algébriquement clos, et $\phi(\overline{x})$ un système d'équations et d'inéquations à coefficients dans $\mathbb{K}$. Si le système a une solution, il en a une dans $\mathbb{K}$.

Ainsi, ce théorème permet de ramener l'existence d'une solution à un système d'équations polynomiales dans $\tilde{\mathbb{Q}}$ à l'existence d'une solution dans le corps des complexes.

Preuve : Soit $\mathbb{L}$ l'extension de corps dans lequel ϕ a une solution. On a donc $\mathbb{L} \models \exists \overline{x} \phi(\overline{x})$. Par modèle-complétude, comme $\mathbb{K} \subset \mathbb{L}$, on en déduit $\mathbb{K} \prec \mathbb{L}$, donc $\mathbb{K} \models \exists x \phi(\overline{x})$. ■

Le théorème des Zéros de Hilbert permet alors d'obtenir assez facilement le théorème suivant

Théorème 7.4 (*NullStellenSatz*)

Soit $\mathbb{K}$ un corps algébriquement clos, et $f_1(\overline{x}), \dots f_m(\overline{x}), , g(\overline{x})$ des polynômes sur $\mathbb{K}$. Si tout zéro commun de $f_1, \dots f_m$ est aussi un zéro de g, alors il existe k tel que g^k soit dans l'idéal engendré par $f_1, \dots, f_m$.

On reconnaît ici l'analogue du célèbre théorème d'algèbre linéaire :

$f_1, \dots f_n, g$ formes linéaires telles que

$$\mathrm{Ker} g \supset \cap \mathrm{Ker} f_i$$

Alors $g \in \mathrm{Vect}(f_1, \dots f_n)$.

Preuve : On pose $f_0(\overline{x}, z) = 1 - g(\overline{x})z$. On considère alors l'idéal I engendré par $f_0, \dots f_m$ vu maintenant comme des polynômes en $\overline{x}, z$ (on a donc ajouté une variable). Il suffit alors de montrer que $I = \mathbb{K}[x, z]$. En effet, dans ce cas, on aura l'existence de polynômes p_i tels que

$$\Sigma p_i f_i = 1$$

En substitutant z par $1/g(\overline{x})$, et en multipliant l'expression par une puissance de g convenable, on aura alors le résultat souhaité.

Supposons donc $I < \mathbb{K}[\overline{x}, z]$. Alors I est contenu dans un idéal propre maximal M, et $\mathbb{L} = \mathbb{K}[\overline{x}, z]/M$ est un corps. Comme M est un idéal propre, l'application $a \to \overline{a}$ de $\mathbb{K}$ dans $\mathbb{L}$ qui associe à un élément sa classe d'équivalence est un morphisme injectif (Si $\overline{a} = 0$, $a \in M$, donc $a = 0$, car $\mathbb{K} \cap M = \{0\}$)

Considérons maintenant le système d'équations polynômiales

$$\phi(\overline{X}, Z) = \wedge f_i(\overline{X}, Z)$$

ϕ a une solution dans $\mathbb{L}$, par exemple $\overline{x_1}, \dots \overline{x_m}, \overline{z}$ (les classes d'équivalence des monômes). En effet

$$f_i(\overline{x_1}, \dots, \overline{x_m}, \overline{z}) = \overline{f_i(x_1, \dots, x_m, z)} = \overline{0}$$

puisque $f_i(x_1 \dots x_m, z) \in I \subset M$.

Le théorème des zéros nous assure alors qu'on a déjà une solution dans $\mathbb{K}$, mais ceci est impossible, puisque tout zéro dans $\mathbb{K}$ des $f_i, i \geq 1$ ne est zéro de g, donc ne peut l'être de f_0. Nous avons donc une contradiction, et $I = \mathbb{K}[\overline{x}, z]$. ■

Définissons maintenant les fonctions pseudo-rationnelles.

Définition 7.1 (*Fonction pseudo-rationnelle*)

Une fonction $f(x)$ d'un corps algébriquement clos $\mathbb{K}$ est une *fonction pseudo-rationnelle* si elle est de la forme $\sqrt[p^n]{g(x)/h(x)}$, où p est la caractéristique du corps (si $p = 0$, $n = 0$).

Remarquons qu'une telle définition est cohérente : Dans un corps de caractéristique p, il y a une seule racine p-ième. On parle de même de fonction pseudo-rationnelle par morceaux s'il existe une partition du domaine en un nombre fini de parties définissables, et f est pseudo-rationnelle sur chaque partie.

L'élimination des quanteurs nous fournit

Proposition 7.5

Toute fonction définissable dans un corps algébriquement clos est pseudo-rationnelle par morceaux.

Preuve : Par élimination des quanteurs, on peut supposer que la fonction définissable est définie par ϕ sans quanteurs. On montre alors par induction sur la structure de ϕ qu'elle définit bien une fonction pseudo-rationnelle par morceaux. ND ■

On peut alors démontrer cette curieuse propriété :

Théorème 7.6 (*Principe d'Ax*)

Si $\mathbb{K}$ est un corps algébriquement clos et $A \subset \mathbb{K}^n$ une partie définissable, alors toute fonction définissable injective est surjective.

La réciproque est bien entendu fausse, il suffit de considérer la fonction $x \mapsto x^2$ de $\mathbb{C}$ dans $\mathbb{C}$.

Preuve : Soit $f : A \to A$ une fonction injective non surjective. Soit $\psi(\overline{a}, \overline{x}, \overline{y})$ la formule qui définit f. La formule :

$$\forall \overline{x}, \forall \overline{y}, \forall \overline{z}, \psi(\overline{a}, \overline{x}, \overline{z}) \wedge \psi(\overline{a}, \overline{y}, \overline{z}) \to \overline{x} = \overline{y}$$

nous dit que f est injective, et

$$\exists \overline{y}, \forall \overline{x}, \neg\psi(\overline{a}, \overline{x}, \overline{y})$$

que f n'est pas surjective. On a donc une formule $\phi(\overline{a})$ qui nous dit que f est injective et non surjective. En particulier, $\mathbb{K} \models \exists x \phi(\overline{x})$. Cet énoncé est vrai dans un corps algébriquement clos de caractéristique première (prendre $\mathbb{K}$ lui même si la caractérique est non nulle, utiliser une caractérisation précédente sinon). Ainsi, il existe donc un nombre premier p tel que la clôture algébrique $\mathbb{K}_p$ de $\mathbb{F}_p$ satisfasse $\exists x \phi(\overline{x})$ Prenons alors $\overline{b}$ dans $\mathbb{K}_p$ tel que $\mathbb{K}_p \models \phi(\overline{b})$. On a ainsi démontré qu'on pouvait se restreindre au cas où la fonction est d'une partie $B \subset \mathbb{K}_p^n$ dans B pour un certain p. Notons g cette fonction.

On sait alors qu'il existe une partition définissable de B en $B_1, \ldots B_m$, telle que g soit une fonction pseudo-rationnelle g_i sur chacun des B_i. Chaque B_i est défini par une formule $\phi_i(\overline{c}_i, \overline{x})$ chaque g_i par une formule $\psi_i(\overline{d}_i, \overline{x}$ Notons $C = \cup \overline{c}_i \cup \overline{d}_i$. Considérons un sous-corps fini F contenant C. Ceci est possible, puisque la caractéristique est fini.

De plus, $\mathbb{K}_p = \cup_{F \supset C} F$. Alors la restriction de g sur $F^n \cap B$ est à valeurs dans $F^n \cap B$. En effet, si $x \in F^n$, alors pour toute fraction rationnelle R, $R(x) \in F$, et la racine p-ième sera encore dans F. Mais sur $F^n \cap B$, g est injective donc surjective, puisque $F^n \cap B$ est fini. Comme $B = \cup_{F \supset C} F^n \cap B$, on en déduit que g est surjective, ce qui est en contradiction avec l'hypothèse. ∎

7.2 Corps réel clos

Les corps réel clos sont ce qu'est $\mathbb{R}$ à $\mathbb{C}$. Ils sont donc donnés par les axiomes

- La théorie des corps
- $\leq$ est un ordre total qui satisfait :
  - $x \leq y \implies x + z \leq y + z$
  - $x \leq y \wedge 0 \leq z \implies xz \leq yz.$
  - $x \leq y \wedge z \leq 0 \implies yz \leq xz.$
- Le théorème des valeurs intermédiaires pour les polynômes :

  Si $f \in \mathbb{K}[X], a \leq b, f(a)f(b) \leq 0$, alors il existe x dans $[a, b]$ avec $f(x) = 0$.

  Ceci se traduit par un énoncé par degré du polynôme.

$\mathbb{R}$ est le prototype de corps réel clos, on vérifiera de plus que la majorité des propriétés de $\mathbb{R}$ se transposent aux corps réel clos ($0 \leq 1, 0 \leq x^2, \ldots$). On remarquera également que tout corps ordonné est nécessairement de caractéristique 0 ($1 > 0 \to 1 + \ldots 1 > 0$), l'ordre doit également être dense sans extrêmités.

Bien que $\mathbb{R}$ soit l'exemple canonique, il n'est pas ω-saturé. Il suffit en effet de considérer le type $\Phi(x) = \{x > n, n \in \mathbb{N}\}$, qui est finiment réalisé et non réalisé. Un corps réel clos est exactement ce qu'est $\mathbb{R}$ à $\mathbb{C}$. Nous avons en effet la propriété :

Théorème 7.7

Si $\mathbb{K}$ est un corps réel clos, alors $\mathbb{K}[X]/(X^2 + 1)$ est un corps algébriquement clos.

Dit autrement, il ne manque que l'adjonction de $i = \sqrt{-1}$ au corps pour obtenir un corps algébriquement clos. Ce théorème sera admis.
Les deux premiers points de la théorie caractérise les corps ordonnés. Ils ne sont pas nécessairement clos.

Donnons quelques propriétés des corps réels clos :

Proposition 7.8

Si $f \in \mathbb{K}[X]$ satisfait la propriété des valeurs intermédiaires sur $[a, b]$, c'est à dire :

$$\forall [x, y] \subset [a, b], f(x)f(y) \geq 0 \implies \exists z \in [x, y], f(z) = 0$$

Alors f change de signe un nombre fini de fois sur $[a, b]$.

Preuve : On peut supposer $f \neq 0$. Soit $n = \deg f$. Supposons que f change de signe plus de n fois. On a donc $x_0 < \dots x_n < x_{n+1}$ dans $[a, b]$ tel que $f(x_0) > 0, f(x_1) < 0, \dots f(x_n) < 0, f(x_{n+1}) > 0$. On a alors un zéro dans chaque intervalle, donc f a au moins $n + 1$ zéros, donc est nulle, contradiction. ■

On a de plus

Propriété 7.9

Soit $\mathbb{K}$ un corps réel clos. Soit f un polynôme. On suppose que $f' > 0$ sur $[a, b]$. Alors f est croissante sur $[a, b]$.

Remarque : le résultat est en fait vrai dans tout corps ordonné, mais plus pénible à prouver.

Preuve : Commençons par montrer que si $f'(x) > 0$, alors il existe $\epsilon > 0$ tel que $f(y) > f(x)$ pour $x < y < x + \epsilon$. C'est une conséquence directe de l'écriture $f(x) = \sum_i \frac{f^{(i)}(e)(x-e)^i}{i!}$ qui est vraie dans tout corps.

On peut alors maintenant utiliser la proposition précédente, ou encore la méthode suivante. Il suffit de démontrer que $f' > 0$ sur $[a, b]$ entraine $f(b) \geq f(a)$. Quitte à prendre $f(x) - f(a)$, on peut supposer $f(a) = 0$. Supposons $f(b) < 0$. Comme f' est positive autour de a, on peut prendre $c \in [a, b]$ tel que $f(c) > f(a)$. Dans ce cas, comme $f(b) < 0 < f(c)$ on sait comme on est dans un corps réel clos qu'il existe $a_1 \in [c, b]$ tel que $f(a_1) = 0$. En recommençant le raisonnement sur l'intervalle $[a_1, b]$ et en itérant, on prouve que f a en fait une infinité de racines dans l'intervalle $[a, b]$, une contradiction. ■

Les deux propriétés montrent qu'en fait un corps ordonné se comporte de la même façon que $\mathbb{R}$. On peut maintenant démontrer la propriété importante :

Proposition 7.10

Tout corps ordonné $\mathbb{K}$ se plonge dans un corps réel clos $\mathbb{L}$ algébrique sur $\mathbb{K}$.

Preuve : Notons $\mathbb{M}$ la clotûre algébrique de $\mathbb{K}$. ($\mathbb{M}$ n'est pas réel clos, puisque -1 y est un carré). L'ensemble des extensions $\mathbb{L} \subset \mathbb{M}$ de corps ordonnés de $\mathbb{K}$ est ordonné inductif, donc admet un élément maximal $\mathbb{L}$, par le lemme de Zorn. Montrons que $\mathbb{L}$ est réel clos.
Prenons f minimale (en degré), $a < b$ tel que $f(a) > 0 > f(b)$, et f n'a pas de racines dans $[a, b]$. Notons que f est nécessairement irréductible. f' ne change de signe qu'un nombre fini de fois (f' est de degré inférieur strictement à celui de f, donc vérifie la propriété des valeurs intermédiaires sur $[a, b]$). On peut donc supposer que f' ne change pas de signe sur $[a, b]$, donc f monotone sur $[a, b]$ ne change de signe qu'une seule fois. Notons

$$A =]-\infty, a] \cup \{a' \in [a, b], f(a') > 0\}$$

Remarquons que A n'a pas d'élément maximal. Notons α une racine de f dans $\mathbb{M}$. $\mathbb{L}[\alpha] = \mathbb{L}[X]/f(X)$, chaque élément s'identifie avec un polynôme de degré inférieur à celui de f. On va définir un ordre sur $\mathbb{L}[\alpha]$ qui prolonge l'ordre de $\mathbb{L}$ et en déduire une contradiction. Il suffit pour cela de poser

$$g \leq g' \iff g - g' \leq 0 \text{ près de } A$$

C'est à dire :

$$\exists B \subset A, \forall x \in A, \forall y \in B, x > y \to x \in B \text{ et } g - g' \leq 0 \text{ sur } B$$

Il suffit maintenant de vérifier que $\leq$ définit un ordre total sur $\mathbb{L}[\alpha]$ pour obtenir la contradiction. La seule proposition un peu délicate est le fait que l'ordre soit total. Il suffit pour cela de s'apercevoir que la dérivée de $g - g'$ est de degré inférieur strictement à celui de f, donc ne change de signe qu'un nombre fini de fois, donc que $g - g'$ est monotone sur un segment final de A, donc de signe constant. ■

Remarquons qu'il n'y a pas unicité de la clotûre réelle : On peut trouver $\mathbb{L}_1$ et $\mathbb{L}_2$ différents dans $\mathbb{M}$ tels que $\mathbb{L}_1$ et $\mathbb{L}_2$ soient des corps réels clos algébriques sur $\mathbb{K}$. Cependant $\mathbb{L}_1$ et $\mathbb{L}_2$ sont isomorphes :

Corollaire 7.11

Tout isomorphisme de corps ordonnés s'étend en un isomorphisme de corps réel clos.

Preuve : Soit $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps ordonnés et $\mathbb{L}_1$, $\mathbb{L}_2$ une de leurs clotûres réelles, et σ un isomorphisme de $\mathbb{K}_1$ dans $\mathbb{K}_2$. Soit $\alpha \in \mathbb{L}_1$. Il existe $[a, b] \subset \mathbb{K}_1$ et f polynôme tel que $f(a)f(b) < 0$ et $\alpha \in [a, b]$. Alors $\sigma(f)(\sigma(a))\sigma(f)(\sigma(b)) < 0$. Donc $\sigma(f)$ a une racine α' dans $[\sigma(a), \sigma(b)]$, et on peut prolonger σ de $\mathbb{K}_1(\alpha)$ dans $\mathbb{K}_2(\alpha')$. Réciproquement, si on prend $\alpha' \in \mathbb{L}_2$, on peut trouver $\alpha \in \mathbb{L}_1$ de façon similaire. Ainsi, on peut construire en itérant le procédé un isomorphisme de $\mathbb{L}_1$ dans $\mathbb{L}_2$.

Pour être plus précis, il suffit de considérer :

$$\left\{\sigma', \sigma \text{ isomorphisme de } \mathbb{K}'_1 \supset \mathbb{K}_1 \text{ dans } \mathbb{K}'_2 \supset \mathbb{K}_2, \sigma'_{|\mathbb{K}_1} = \sigma\right\}$$

C'est un ensemble ordonné inductif, qui possède un élément maximal σ' , et les quelques lignes précédentes montrent que σ' est nécessairement total. ■

On peut alors enfin démontrer l'important théorème :

Théorème 7.12

La théorie des corps réel clos est complète et élimine les quanteurs.

Preuve : Il suffit de montrer qu'elle élimine les quanteurs. En effet, dans ce cas, $\mathbb{R} \cap \tilde{\mathbb{Q}}$, la clotûre réelle des rationnels, s'injecte dans tout modèle, et ainsi par modèle complétude, tout modèle est élémentairement équivalent à $\mathbb{R} \cap \tilde{\mathbb{Q}}$.

Prenons $\mathbb{K}_1$ et $\mathbb{K}_2$ réel clos ω-saturés, $\overline{a}$ et $\overline{b}$ deux uples qui satisfont les mêmes formlules atomiques. Prenons une formule $\exists x \phi(\overline{a}, x)$ vérifiée par $\overline{a}$,avec ϕ atomique. On veut montrer qu'elle est vérifiée par $\overline{b}$. Prenons donc a_0 tel que $\mathbb{K}_1 \models \phi(\overline{a}, a_0)$. Les sous corps A et B engendrés par $\overline{a}$ et $\overline{b}$ sont isomorphes, et par la proposition précédente, il existe σ isomorphisme de $\mathbb{K}_1 \cap A$ dans $\mathbb{K}_2 \cap B$. Deux cas se produisent :

– a_0 est algébrique sur A. Alors on trouve aisément $b_0 = \sigma(a_0) \in \mathbb{K}_2$ tel que $\overline{a}a_0$ et $\overline{b}b_0$ engendrent des corps ordonnés isomorphes, donc en particulier satisfont les mêmes formules. Ainsi $\mathbb{K}_2 \models \exists x \phi(\overline{b}, x)$

- a_0 est transcendant sur A, c'est à dire $A(a_0)$ est isomorphe au corps des fonctions rationnelles, l'ordre étant déterminé par la coupure $C = \{a \in A, a < a_0\}$. Par ω-saturation, on peut donc trouver b_0 dans $\mathbb{K}_2$ qui réalise la même coupure, puisque $\{x > b, b \in \sigma(C)\}$ est un type. Comme la coupure détermine l'ordre, on est sur que $A(a_0)$ et $B(b_0)$ sont isomorphes, donc en particulier $\overline{a}a_0$ et $\overline{b}b_0$ satisfont les mêmes formules atomiques, donc $\mathbb{K}_2 \models \phi(\overline{b}, b_0)$, et $\mathbb{K}_2 \models \exists x \phi(\overline{b}, x)$.

Dans tous les cas,
$$\mathbb{K}_1 \models \exists x \phi(\overline{a}, x) \implies \mathbb{K}_2 \models \exists x \phi(\overline{b}, x)$$
pour ϕ atomique. L'autre implication se montre de manière similaire, et on a donc bien la condition d'application du théorème d'élimination des quanteurs. ■

Exercices

(7 - 1) **Q 1)** Montrer que dans la théorie des corps algébriquement clos sur le langage $(+, \times, =, 0, 1)$, toute formule $\phi(x)$ est équivalente à une formule $\psi(x)$ qui n'utilise pas les symboles $\forall, \neg$ (et donc qui n'utilise pas non plus $\neq$, qui n'est qu'une abréviation).

Q 2) Montrer que dans la théorie des corps réels clos dans le langage $(+, \times, <, =, 0, 1)$ toute formule $\phi(x)$ est équivalente à une formule $\psi(x)$ sans quantificateurs ni négation, mais que ce n'est pas le cas si on prend la théorie des corps réels clos dans le langage $(+, \times, \leq, =, 0, 1)$

(7 - 2) *(Sur l'ω-saturation)*

Q 1) Montrer que $\tilde{\mathbb{Q}}$ n'est pas ω-saturé

- En trouvant un type finiment satisfait et non satisfait
- En trouvant un corps algébriquement clos dénombrable non isomorphe à $\tilde{\mathbb{Q}}$. Pourquoi ceci implique-t-il que $\tilde{\mathbb{Q}}$ n'est pas ω-saturé ?

Q 2) Mêmes questions avec $\tilde{\mathbb{Q}} \cap \mathbb{R}$.

Q 3) Montrer que $\mathbb{R}$ n'est pas ω-saturé.

La même question, avec $\mathbb{C}$, admet cette fois-ci une réponse positive : $\mathbb{C}$ est ω-saturé, mais nous n'allons pas le démontrer

Q 4) Montrer qu'il n'existe pas de formule $\phi(x)$ telle que $\mathbb{C} \models \phi(n)$ si et seulement si n est une racine de l'unité (Construire à partir d'un tel ϕ un type non satisfait)

(7 - 3) Il s'agit de prouver que K est réel clos si et seulement si le corps quotient $K[X]/\left[X^2+1\right]$ est algébriquement clos (ou encore $\left\{a + ib, (a, b) \in K^2\right\}$, où i est tel que $i^2 = -1$). En fait, nous ne prouverons pas le sens direct, le lecteur se reportera à tout manuel d'algèbre, où il trouvera une preuve du théorème de d'Alembert-Gauss qui n'utilise que des propriétés de corps réel clos. Prenons donc K corps ordonné. On note $\mathbb{K} = \left\{a + ib, (a, b) \in K^2\right\}$. On veut montrer que tout polynôme P qui change de signe a une racine dans K. On considère ici K comme un sous-corps de $\mathbb{K}$, grâce à l'injection canonique $a \mapsto a + i0$.

Q 1) (Préliminaire) Montrer que $X^2 + 1$ est bien irréductible dans K,et donc que, comme nous l'annonçons, $K[X]/\left[X^2+1\right]$ est bien un corps.

Q 2) Montrer qu'on peut se restreindre au cas où P est irréductible dans K, de degré supérieur à 2. (Dans la suite, nous dirons simplement : P est irréductible, sans préciser que son degré est supérieur à 2).

Q 3) On définit dans $\mathbb{K}$ l'application : $f : a + ib \mapsto a - ib$. Montrer que cette application est un automorphisme.

Q 4) Montrer que si ζ est racine de P, $f(\zeta)$ est également racine, et que, si P est irréductible dans $K, \zeta \neq f(\zeta)$.

Q 5) Montrer que tout polynôme P irréductible dans K s'écrit $P(X) = \alpha(X - \zeta)(X - f(\zeta))$, où $\alpha \in K$.

Q 6) En déduire que P est de signe constant sur K.

Q 7) Conclure.

Problème 3

On s'intéresse ici aux anneaux de polynômes et à leurs théories. On se place dans le langage $\mathcal{L} = \{0, 1, +, \times\}$ de la théorie des anneaux. Dans tout le problème, les corps considérés sont de caractéristique nulle.

Partie 1 - Préliminaire

Q 1) Montrer qu'il existe une formule $\phi(x)$ telle que pour tout polynôme $P \in \mathbb{K}[X], \mathbb{K}[X] \models \phi(P)$ si et seulement si $P \in \mathbb{K}$ (c'est à dire P est un polynôme constant)

Q 2) En déduire que si $\mathbb{K}[X]$ et $\mathbb{L}[X]$ sont élémentairement équivalents, $\mathbb{K}$ et $\mathbb{L}$ sont élémentairement équivalents.

Q 3$\star$) Montrer que si $\mathbb{K}$ et $\mathbb{L}$ sont ∞-équivalents, $\mathbb{K}[X]$ et $\mathbb{L}[X]$ sont ∞-équivalents.
Remarque : cette question n'est pas nécessaire pour la suite.

Partie 2 - Entiers et rationnels

On s'autorise le raccourci $P|Q := \exists R, PR = Q$ pour dire que P divise Q.

Q 1) Soit $\alpha \in \mathbb{K}$ et P et Q deux polynômes (non constants) tels que $P|Q$. On suppose que la propriété suivante est vraie :

$$\forall x \in \mathbb{K}, P + x|Q \implies ((P + x + 1|Q) \vee (x = \alpha))$$

Montrer que α est un entier positif

Q 2) Montrer que si α est un entier positif, on peut trouver P et Q tels que la propriété précédente soit vraie.

Q 3) En déduire qu'il existe un prédicat $\psi(x)$ tel que pour tout polynôme $P \in \mathbb{K}[X], \mathbb{K}[X] \models \psi(P)$ si et seulement si $P \in \mathbb{N}$.

Q 4) En déduire qu'il existe un prédicat similaire pour $P \in \mathbb{Q}$.

Q 5) En déduire que si $\mathbb{L}[X]$ est élémentairement équivalent à $\mathbb{Q}[X]$, alors $\mathbb{L} = \mathbb{Q}$. Pourquoi ce résultat n'est pas en contradiction avec le théorème de Lowenheim-Skolem ?

Partie 3 - Transcendance

Q 1) Soit $\mathbb{K} \subset \mathbb{L}$ deux corps, $P \in \mathbb{L}[X]$ et $Q \in \mathbb{L}[X]$ deux polynômes non constants vérifiant

$$\forall \alpha \in \mathbb{K}, \exists \beta \in \mathbb{K}, P - \alpha | Q - \beta$$

Montrer qu'il existe un polynôme $R \in \mathbb{K}[X]$ tel que $Q = R(P)$ (utiliser le théorème d'interpolation de Lagrange).

Q 2) Montrer réciproquement que si $Q = R(P)$ avec $R \in \mathbb{K}[X]$, la propriété précédente est vérifiée.

Q 3) Soit $\alpha, \beta \in \mathbb{L}$. On se donne trois polynômes (non constants) $Q, P \in \mathbb{L}[X]$ et $R \in \mathbb{K}[X]$ tel que $Q = R(P)$. On suppose de plus que $P - \alpha | Q - \beta$. En écrivant $Q = R((P - \alpha) + \alpha)$, montrer que $R(\alpha) = \beta$.

Q 4) En déduire l'existence d'une formule $\theta(x)$ telle que si $\alpha \in \mathbb{L} \subset \mathbb{L}[X]$, $\mathbb{L}[X] \models \theta(\alpha)$ si et seulement si α est algébrique (il existe $P \in \mathbb{Q}[X], P(\alpha) = 0$).

Dans toutes les questions suivantes, les corps sont supposés algébriquement clos. Le degré de transcendance d'un corps algébriquement clos $\mathbb{K}$ est le plus petit n tel qu'il existe $\alpha_1 \dots \alpha_n$ tel que pour tout $x \in \mathbb{K}$, $P(\alpha_1 \dots \alpha_n, x) = 0$ pour un certain polynôme P. Il n'est pas nécessaire de connaître une quelconque propriété du degré de transcendance. On dira que deux corps algébriquement clos sont de même degré de transcendance si et seulement ils sont tous les deux de degré de transcendance infini, ou leur degré de transcendance est fini et le même.

Q 5) Montrer que si $\mathbb{L}[X]$ est élémentairement équivalent à $\tilde{\mathbb{Q}}[X]$, alors $\mathbb{L} = \tilde{\mathbb{Q}}$

Q 6) En généralisant le raisonnement précédent, montrer que si $\mathbb{L}[X]$ et $\mathbb{K}[X]$ sont élémentairement équivalents, $\mathbb{L}$ et $\mathbb{K}$ ont même degré de transcendance.

Q 7) Montrer que $\mathbb{L}$ et $\mathbb{K}$ sont ∞-équivalents si et seulement si ils ont même degré de transcendance

Remarque : Puisqu'à isomorphisme près il n'y a qu'un corps algébriquement clos de degré de transcendance p, il suffit de prouver que $\mathbb{L}$ est ∞-équivalent a un corps algébriquement clos de degré de transcendance infini si et seulement si $\mathbb{L}$ est de degré de transcendance infini

On en déduit que si $\mathbb{L}$ et $\mathbb{K}$ sont deux corps algébriquement clos, $\mathbb{L}[X]$ et $\mathbb{K}[X]$ sont élementairement équivalents si et seulement si $\mathbb{L}$ et $\mathbb{K}$ sont ∞-équivalents, ce qui conclut le problème.

Problème 4

On donne ici une solution positive au dix-septième problème de Hilbert

Théorème 7.13

> Tout polynôme réel à plusieurs variables qui est toujours positif s'écrit comme une somme de carrés de fractions rationnelles.

En fait, la définition d'un corps réel clos a justement été donné pour démontrer ce théorème, il serait donc bête de ne pas le faire. On notera qu'en fait techniquement seules les deux dernières questions utilisent la théorie des modèles. L'idée est en fait sensiblement la même que celle utilisée précédemment pour prouver le NullStellenSatz.

PARTIE 1 - Préliminaires

Q 1) Montrer le résultat pour $P \in \mathbb{R}[X]$, c'est à dire pour une seule variable.

Q 2) Montrer que le polynôme $X^4Y^2 + X^2Y^4 - X^2Y^2 + 1$ est toujours positif, mais qu'il ne s'écrit pas comme une somme de carrés de polynômes (donc qu'il faut bien des fractions rationnelles)

PARTIE 2 - Cônes

Si $\mathbb{K}$ est un corps, un cône est un sous-ensemble de $\mathbb{K}$ stable par addition et multiplication, et contenant tous les carrés. On note P un cône. Un cône propre est un cône tel que $-1 \notin P$.

Q 1) Soit P un cône propre. Soit x tel que $x \notin P$. Définir un cône propre qui contient $-x$.

Q 2) Soit P un cône propre maximal. Vérifier que la relation $x \leq y \iff y - x \in P$ définit bien un ordre tel que $\mathbb{K}$ est un corps ordonné

Q 3) En déduire que si x n'est pas une somme de carrés dans $\mathbb{K}$ il existe un ordre sur $\mathbb{K}$ tel que $x < 0$.

PARTIE 3 - La fin

On se donne maintenant un polynôme P de $\mathbb{R}[X_1 \dots X_n]$. On note $P = \sum_{\alpha \in \mathbb{N}^n} p_\alpha \overline{X}^\alpha$. On travaille dans le corps $\mathbb{K} = \mathbb{R}(X_1 \dots X_n)$ c'est à dire les fractions rationnelles. On suppose que P ne s'écrit pas comme somme de carrés. On peut donc se donner un ordre sur $\mathbb{K}$ tel que $P < 0$. Soit M la cloture réelle de $\mathbb{K}$. On remarque que $\mathbb{R} \subset \mathbb{K} \subset M$, donc on peut voir en fait P comme un polynôme de M.

Q 1) Expliquer pourquoi la formule $\exists x_1 \dots x_n \sum_{\alpha \in \mathbb{N}^n} p_\alpha \overline{x}^\alpha < 0$ est vraie dans M.

Q 2) En deduire que P en tant que polynôme de $\mathbb{R}[X_1 \dots X_n]$ n'est pas toujours positif.

Q 3) Soit $P \in \mathbb{Q}[X_1 \dots X_n]$ tel que P est toujours positif. Montrer que P est une somme de carrés de fractions rationnelles à coefficients dans $\mathbb{Q}$. On pourra utiliser
- $\mathbb{Q}$ est dense dans $\mathbb{R}$
- Tout élément positif de $\mathbb{Q}$ est une somme de carrés.

Annexe A

LISTE DES DÉFINITIONS

Annexe B

LISTE DES THÉORÈMES

Annexe C

INDEX