M2 - Orsay , Mars 2007

E. Bouscaren

Introduction à la Théorie des modèles (version préliminaire 1 - couvrant la seconde moitié de la séance du 15 mars et la séance du 22 mars 07)

1 Quelques définitions

Si ϕ est une formule close ou **énoncé**, , c'est à dire sans aucune variable libre, la valeur de vérité de ϕ dans $\mathcal{M}$ ne dépend pas du n-uple auquel on l'applique: la formule est toujours soit vraie, soit fausse dans $\mathcal{M}$. Donc on écrira simplement $\mathcal{M} \models \phi$ et on dira que $\mathcal{M}$ est un **modèle** de ϕ.

• **Connecteurs supplémentaires**:
On utilisera les notations suivantes, si ϕ, ψ sont des formules:
– $(\phi \to \psi)$ pour la formule $(\neg\phi \vee \psi)$
– $(\phi \leftrightarrow \psi)$ pour la formule $((\phi \to \psi) \wedge (\psi \to \phi))$

Une formule close ϕ du langage L est dite *universellement valide* si elle est satisfaite par toute L-structure.

• **Équivalence, conséquence sémantique**
Deux formules $\phi(v_0, \ldots, v_n)$ et $\psi(v_0, \ldots, v_n)$ sont dites *équivalentes* si la formule

$$\forall v_0 \ldots \forall v_n(\phi(v_0, \ldots, v_n) \leftrightarrow \psi(v_0? \ldots, v_n))$$

est universellement valide. Cela revient à dire que, dans toute L-structure $\mathcal{M}$, pour tout $n+1$-uple $(a_0, \ldots, a_n) \in |\mathcal{M}|^n$, on a $\mathcal{M} \models \phi(a_0, \ldots, a_n$ si et seulement si $\mathcal{M} \models \psi(a_0, \ldots, a_n)$.

Soit Σ un ensemble d'énoncés de L. On dit qu'une L-structure $\mathcal{M}$ est un modèle de Σ si $\mathcal{M}$ est modèle de chaque énoncé ϕ de l'ensemble Σ et on écrit $\mathcal{M} \models \Sigma$.

On dit que un énoncé ϕ est *conséquence sémantique* (ou, plus simplement, *conséquence*) de Σ si tout modèle de Σ satisfait ϕ. La notation est $\Sigma \vdash F$. Un énoncé ϕ est universellement valide si et seulement si il est conséquence de $\emptyset$, donc noté $\vdash \phi$.

• Quelques équivalences habituelles

On peut vérifier que l'on a bien les équivalences habituelles, quelles que soient les formules ϕ, ψ:
– $\phi \vee \psi$ équivaut à $\neg(\neg\phi \wedge \neg\psi)$;

– $\exists v\,(\phi \vee \psi)$ équivaut à $(\exists v\,\phi \vee \exists v\,\psi)$;
– $\forall v\,(\phi \wedge \psi)$ équivaut à $(\forall v\,\phi \wedge \forall v\,\psi)$
– $Qv\,(\phi * \psi)$ équivaut à $(Qv\,\phi) * \psi)$ si la variable v n'est pas libre dans ψ; quand Q est soit $\forall$, soit $\exists$, et $*$ est soit $\wedge$, soit $\vee$;
– $\forall v\,\forall w\,\phi$ équivaut à $\forall w\,\forall v\,\phi$;
– $\exists v \exists w\,\phi$ équivaut à $\exists v\,\exists w\,\phi$;
– $\exists v\,\phi$ équivaut à $\neg\forall v\,\neg\,\phi$.

En particulier, on voit que toute formule est équivalente à une formule qui ne contient que les connecteurs $\neg$ et $\wedge$ et le quantificateur $\exists$, ou plus généralement que l'on peut se contenter pour définir l'ensemble des formules de deux connecteurs $\{\neg, \wedge\}$ ou bien $\{\neg, \vee\}$ et d'un seul quantificateur, $\exists$ ou bien $\forall$.

2 Élémentaire équivalence - Théories complètes

On appelle ici **théorie** de L un ensemble d'énoncés de L qui a un modèle.
Définition: Soient L un langage, $\mathcal{M}$ et $\mathcal{N}$ deux L-structures. On dit que $\mathcal{M}$ et $\mathcal{N}$ sont **élémentairement équivalents**, noté $\mathcal{M} \equiv_L \mathcal{N}$, si $\mathcal{M}$ et $\mathcal{N}$ satisfont exactement les mêmes énoncés (= formules sans variables libres) de L, c'est-à-dire si, pour tout énoncé σ de L,

$$\mathcal{M} \models \sigma \text{ si et seulement si } \mathcal{N} \models \sigma.$$

Définition: Soient L un langage et T une théorie de L. On dit que la théorie T est **complète** si, pour tous modèles $\mathcal{M}$ et $\mathcal{N}$ de T, $\mathcal{M}$ et $\mathcal{N}$ sont élémentairement équivalents.

Proposition 1 *(Exercice) Soit T une théorie de $\mathcal{L}$, alors les conditions suivantes sont équivalentes:*

1. *T est complète,*
2. *pour tout énoncé σ de L, $T \vdash \sigma$ si et seulement si il existe un modèle de T qui satisfait σ,*
3. *pour tout énoncé σ de L, $T \vdash \sigma$ ou bien $T \vdash \neg\sigma$.*

Si $\mathcal{M}$ est une $\mathcal{L}$-structure, alors la théorie suivante, appelée **Théorie de la structure** $\mathcal{M}$ est complète:

$$Th(\mathcal{M}) = \{\sigma; \sigma \text{ énoncé de } L \text{ tel que } \mathcal{M} \models \sigma\}.$$

2.1 Exemples de théories

2.1.1 Les groupes libres finiment engendrés

On considère le langage des groupes $L = \{., ^{-1}, 1\}$.

Il est facile de voir que si $n \neq m$, le groupe commutatif libre sur n générateurs $\mathbb{Z}^n$ et le groupe commutatif libre sur m générateurs $\mathbb{Z}^m$ ne sont pas élémentairement équivalents dans L: on remarque que $\mathbb{Z}^n/2\mathbb{Z}^n$ est de cardinalité égale à 2^n et que cela peut se "dire".

La situation est beaucoup plus compliquée pour les groupes libres non commutatifs. La question suivante avait été posée par (ou bien est traditionnellement attribuée à) A. Tarski vers 1945: pour chaque $n \geq 2$ on appelle F_n le groupe (non commutatif) libre sur n générateurs. Si $n \neq m$, les groupes F_n et F_m sont-ils élémentairement équivalents dans L?

On a montré assez rapidement que pour tout n, m, F_n et F_m satisfont les mêmes énoncés universels de L. Puis les mêmes énoncés positifs (1966), puis les mêmes énoncés à deux alternances de quantificateurs (annoncé en 1973).

Mais la question générale restait ouverte. Récemment une réponse *positive* à la question de Tarski a été annoncée de deux sources différentes: première annonce datée de 1998 de O. Kharlampovich et A. Myasnikov, deuxième annonce (2000), avec des méthodes différentes, de Z. Sela. (Dans les deux cas, le résultat est le point culminant d'une série de 5 ou 6 articles, dont les derniers ont je crois été enfin publiés il y a un ou deux ans.)

Le travail de Z. Sela (" Diophantine geometry over groups") en particulier fait bien plus que répondre à la question initiale. Il montre que le plongement canonique de F_n dans F_m, pour $n \leq m$ est un plongement élémentaire (voir section 6) et surtout donne une caractérisation de tous les groupes finiment engendrés qui sont élémentairement équivalents à cette classe de groupes (voir l'exposé n° 922 du Séminaire Bourbaki, Juin 2003, "Sur la théorie élémentaire des groupes libres [d'après Sela]", par F. Paulin).

3 Énoncé du théorème de compacité

Nous allons donner la démonstration du théorème de compacité grâce aux ultraproduits un peu plus loin, mais regardons ce qu'il dit et donnons deux premiers exemples d'applications immédiates.

Théorème 2 (Théorème de compacité 1) *Soit Σ un ensemble d'énoncés tel que tout sous ensemble fini de Σ a un modèle. Alors Σ a un modèle.*

Voyons tout de suite une formulation équivalente :

Théorème 3 (Théorème de compacité 2) *Soit Σ un ensemble d'énoncés, et θ un énoncé. Si $\Sigma \vdash \theta$, il existe un sous-ensemble fini F de Σ tel que $F \vdash \theta$.*

Montrons que les deux formulations sont équivalentes:
Preuve: $2 \rightarrow 1$: Supposons par contradiction que Σ n'a pas de modèle. Alors pour tout énoncé θ, il est vrai que $\Sigma \vdash \theta$. Par exemple $\Sigma \vdash (\forall x\, x \neq x)$. Par 2., il existe F fini sous-ensemble de Σ tel que $F \vdash (\forall x\, x \neq x$. Mais alors, F ne peut pas avoir de modèle non plus, car $\forall x\, x \neq x$ n'en a pas.
$1 \rightarrow 2$: A nouveau par contradiction, supposons que $\Sigma \vdash \theta$ mais que pour chaque F fini, $F \subset \Sigma$, il existe un modèle de F, $\mathcal{M}_F$, qui n'est pas modèle de θ, c'est-à-dire, $\mathcal{M}_F$ est modèle de $F \cup \{\neg\theta\}$. Par 1., il existe donc un modèle $\mathcal{M}$ de l'ensemble d'énoncés $\Sigma \cup \{\neg\theta\}$. Cela contredit l'hypothèse: tout modèle de Σ est également modèle de θ. $\square$

Corollaire 4 *1. Si T est une théorie qui a des modèles finis de cardinalité arbitrairement grande (c'est-à-dire telle que, pour chaque $n \geq 1$, T a un modèle fini de cardinalité supérieure à n), alors T a un modèle infini.*

Preuve: Considérons l'énoncé $F_n := \exists x_1, \ldots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$. Un modèle de F_n est de cardinalité au moins n. Soit $T' := T \cup \{F_n : n \geq 2\}$. Un modèle de T', s'il en existe, est un modèle de T de cardinalité supérieure à n pour chaque n, donc infini. Si F est un sous-ensemble fini de T', alors il existe k tel que $F \subset T \cup \{F_n : 2 \leq n \leq k\}$. Par hypothèse, T a un modèle de cardinalité au moins égale à k, $\mathcal{M}_k$. Celui-ci est un modèle de $T \cup \{F_n : 2 \leq n \leq k\}$ et donc de F. Le théorème de compacité entraîne bien que T' a un modèle. □

Corollaire 5 *Si σ est un énoncé du langage des anneaux qui est vrai dans tous les corps de caractéristique zéro, alors il existe un nombre premier q tel que σ est vrai dans tous les corps de caractéristique supérieure ou égale à q.*

Preuve: Soit θ_c l'ensemble fini d'énoncés du langage des anneaux dont les modèles sont exactement tous les corps commutatifs, et $T = \{\theta_c\} \cup \{p \neq 0 : p \text{ premier}\}$. Les modèles de T sont tous les corps de caractéristique 0. Si σ est vrai dans tous les corps de caractéristique 0, alors $T \vdash \sigma$. Par le théorème de compacité 2, il existe F fini, $F \subset T$, tel que $F \vdash \sigma$. Puisque F est fini, il existe un nombre premier q tel que $F \subset \{\theta_c\} \cup \{p \neq 0 : p < q\}$. Si K est un corps de caractéristique $\geq q$, K est modèle de F, et donc aussi modèle de σ. □

Remarque: Le corollaire précédent s'énonce aussi de manière équivalente: *si σ est un énoncé qui est vrai dans des corps de caractéristique p, pour p arbitrairement grand, alors il existe un corps de caractéristique zéro dans lequel σ est vrai.*

4 Produits réduits, ultraproduits et démonstration du théorème de compacité

4.1 Filtres et ultrafiltres

Définitions: Soit I un ensemble non vide, un **filtre** $\mathcal{F}$ sur I est un sous-ensemble de $\mathcal{P}(I)$ (l'ensemble des parties de I), tel que :
- $I \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$
- si $X, Y \in \mathcal{F}$, alors $X \cap Y \in \mathcal{F}$
- si $X \in \mathcal{F}$ et $X \subset Z \subset I$, alors $Z \in \mathcal{F}$.

Exemples: 1. Si $\emptyset \neq X_0 \subset I$, $\mathcal{F}_{X_0} = \{Y \subset I : X_0 \subset Y\}$. Un tel filtre est appelé *filtre principal*.
2. Si I est infini, l'ensemble des parties cofinies de X, $\mathcal{FR} = \{X \subset I \,;\, I \setminus X \text{ est fini }\}$, est un filtre, appelé le *filtre de Frechet*, qui n'est jamais principal. En effet, soit Y quelconque dans $\mathcal{FR}$, et $a \in Y$, alors $Y \setminus \{a\}$ est encore dans $\mathcal{FR}$, mais ne contient pas Y.

On dit qu'un ensemble non vide de parties de I, A, a la **propriété de l'intersection finie** si, pour tous $X_1, \ldots, X_n \in A$, $X_1 \cap \ldots \cap X_n \neq \emptyset$.

Lemme 6 *Si $A \subset I$ est non vide et a la propriété de l'intersection finie, l'ensemble des parties de I qui contiennent une intersection finie d'éléments de A est un filtre, qu'on appelle le filtre engendré par A. Tout filtre a la propriété de l'intersection finie.*

Preuve: Clair □

Un **ultrafiltre** est un filtre maximal pour l'inclusion (remarquez que d'après notre définition, tout filtre est propre, c'est-à-dire différent de $\mathcal{P}(I)$).

Proposition 7 *1. Un filtre $\mathcal{F}$ est un ultrafiltre si et seulement si, pour tout $X \subset I$, $X \in \mathcal{F}$ ou bien $I \setminus X \in \mathcal{F}$.*
2. Tout filtre est contenu dans un ultrafiltre.

Preuve: 1. Si $\mathcal{F}$ est un filtre et que $A \notin \mathcal{F}$ alors $\mathcal{F} \cup \{A\}$ a la propriété de l'intersection finie ssi $I \setminus A$ n'est pas dans $\mathcal{F}$: Si $I \setminus A \in \mathcal{F}$, $A \cap (I \setminus A) = \emptyset$. Si $\mathcal{F} \cup \{A\}$ n'a pas la propriété de l'intersection finie, il existe $B_1 \cap \ldots \cap B_n \in \mathcal{F}$ tels que $B_1 \cap \ldots B_n \cap A = \emptyset$, c'est-à-dire, $B_1 \cap \ldots \cap B_n \subset I \setminus A$, et donc $I \setminus A \in \mathcal{F}$.
2. Par le lemme de Zorn[1]: Soit $\mathcal{F}$ un filtre, on considère l'ensemble de tous les filtres sur I qui contiennent $\mathcal{F}$, ordonné par l'inclusion. Si $(\mathcal{F}_j)_{j\in J}$ est une chaîne de tels filtres, alors $\cup_{j\in J}\mathcal{F}_j$ est un filtre qui contient chaque $\mathcal{F}_j$ et majore donc tout élément de la chaîne. On peut appliquer Zorn, il existe donc un filtre maximal pour l'inclusion qui contient $\mathcal{F}$. □

Exemples importants: Un filtre principal $\mathcal{F}$ est un ultrafiltre si et seulement si il existe $i_0 \in I$ tel que $\mathcal{F} = \{X \subset I : \{i_0\} \subset X\}$.
Si I est infini, un ultrafiltre de I est non principal si seulement si il contient le filtre de Frechet.

4.2 Produits réduits, ultraproduits

4.2.1 Produits réduits et ultraproduits d'ensembles

Soit $(A_i)_{i\in I}$ une famille d'ensembles non vides, $\mathcal{A} = \Pi_{i\in I}A_i$. Soit $\mathcal{F}$ un filtre sur I, et $\equiv_{\mathcal{F}}$ la relation suivante sur $\mathcal{A}$:

$$a \equiv_{\mathcal{F}} b \text{ ssi } \{i \in I;\, a(i) = b(i)\} \in \mathcal{F}.$$

On vérifie facilement que $\equiv_{\mathcal{F}}$ est une relation d'équivalence. On notera $a_{\mathcal{F}}$ la classe de a. L'ensemble quotient, $\Pi_{i\in I}A_i/\mathcal{F} = \{a_{\mathcal{F}} : a \in \Pi_{i\in I}A_i\}$ est appelé le **produit réduit** des A_i (par $\mathcal{F}$). Si $\mathcal{F}$ est un ultrafiltre on appelle $\Pi_{i\in I}A_i/\mathcal{F}$, **l'ultraproduit** des A_i (par $\mathcal{F}$). Dans ce cas, si a et b sont équivalents pour la relation $\equiv_{\mathcal{F}}$, on dira qu'ils sont égaux presque partout.

Le lemme suivant sur les cardinalités nous sera utile:

Lemme 8 *Soit $(A_i)_{i\in\mathbb{N}}$ une famille d'ensembles non vides, dénombrables infinis. Soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{N}$. Alors $\Pi_{i\in I}A_i/\mathcal{F}$ est de cardinalité égale à $\mathbb{N}^{\mathbb{N}} = |\mathcal{P}(\mathbb{N}|.)$.*

[1]Lemme de Zorn: Soit A un ensemble ordonné tel que tout sous-ensemble totalement ordonné a un majorant. Alors A a un élément maximal

Preuve: On commence par construire un ensemble E d'applications de $\mathbb{N}$ dans $\mathbb{N}$, de cardinalité $|\mathcal{P}(\mathbb{N})|$ et tel que si $f, g \in E$, et $f \neq g$, alors $\{i \in \mathbb{N} : f(i) = g(i)\}$ est fini. Pour chaque application δ de $2^{\mathbb{N}}$ ($\delta : \mathbb{N} \mapsto \{0,1\}$), on définit une application f_δ de $\mathbb{N}$ dans $\mathbb{N}$ en posant

$$f_\delta(n) = \Sigma_{m<n}\, \delta(m) 2^m.$$

La famille $E = \{f_\delta : \delta \in 2^{\mathbb{N}}\}$ a la propriété requise. Maintenant, pour chaque $i \in \mathbb{N}$, on fixe une énumération de $A_i = (e_{i,n})_{n\in\mathbb{N}}$.

Ensuite, pour chaque $f \in E$, on définit un élément a_f dans $\Pi_{i\in\mathbb{N}} A_i$: $a_f(i) := e_{i,f(i)}$. Alors si $f \neq g$, $\{i \in \mathbb{N} : a_f(i) = b_g(i)\} = \{i \in \mathbb{N} : f(i) = g(i)\}$ est fini et n'est donc pas dans $\mathcal{U}$, ultrafiltre non principal. Donc, si $f \neq g$, $(a_f)_{\mathcal{U}} \neq (b_f)_{\mathcal{U}}$. □

En fait, on a plus généralement:

Lemme 9 *Soit $(A_i)_{i\in\mathbb{N}}$ une famille d'ensembles non vides finis, mais de cardinalités non bornées, c'est-à-dire tels que, pour chaque n, $\{i \in \mathbb{N} : |A_i| \leq n\}$ est fini, et soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{N}$. Alors $\Pi_{i\in I} A_i/\mathcal{U}$ est de cardinalité égale à $|\mathcal{P}(\mathbb{N})|$.*

Preuve: On reprend la famille d'applications E construite dans la preuve ci-dessus. Elle a également la propriété que, pour toute $f \in E$, et pour tout n, $f(n) < 2^n$. Pour chaque $i \in \mathbb{N}$, on définit $n(i)$ comme le plus grand entier tel que $card(A_i) \geq 2^{n(i)}$. Pour chaque i on peut donc trouver dans A_i une suite d'éléments distincts $(e_{i,k})_{k<2^{n(i)}}$. Pour chaque $f \in E$, on définit a_f dans $\Pi_{i\in\mathbb{N}} A_i$: $a_f(i) := e_{i,f(n(i))}$. Comme au-dessus, si $f \neq g$, $\{i \in \mathbb{N} : a_f(i) = b_g(i)\} = \{i \in \mathbb{N} : f(n(i)) = g(n(i))\}$ est fini et n'est donc pas dans $\mathcal{U}$, ultrafiltre non principal. □

4.2.2 Produits cartésiens de L-structures

Si $(A_i)_{i\in I}$ est une famille d'ensembles non vides, on note $\mathbb{A} := \Pi_{i\in I} A_i$, le produit cartésien de la famille, qui est égal à l'ensemble des applications a de I dans la réunion $\bigcup_{i\in I} A_i$, telles que, pour chaque $i \in I$, $a(i) \in A_i$. Nous noterons donc un élément a de $\Pi_{i\in I} A_i$, $a = (a(i))_{i\in I}$.

Soit L un langage du premier ordre à une seule sorte. Si chacun des $\mathcal{M}_i$ est une L-structure, on définit une L-structure sur le produit cartésien, $\mathbb{M} := \Pi_{i\in I} |\mathcal{M}_i|_i$, "coordonnée par coordonnée":

– Si c est un symbole de constante dans L, on pose $c^{\mathbb{M}} := (c^{\mathcal{M}_i})_{i\in I}$;

– Si f est un symbole de fonction d'arité n de L, on définit la fonction $f^{\mathbb{M}}$ en posant, si $(a_1, \ldots, a_n) \in \mathbb{M}$,

$$f^{\mathbb{M}}(a_1, \ldots, a_n)(i) := f^{\mathcal{M}_i}(a_1(i), \ldots, a_n(i));$$

– Si R est un symbole de relation d'arité n, on pose

$$(a_1, \ldots, a_n) \in R^{\mathbb{M}} \text{ ssi pout tout } i \in I,\ (a_1(i), \ldots, a_n(i)) \in R^{\mathcal{M}_i}.$$

Exemples : 1. Si chacun des $\mathcal{M}_i$ est un groupe, alors $\mathbb{M}$ est un groupe.

2. Si chacun des $\mathcal{M}_i$ est un anneau commutatif, noté A_i, on définit, coordonnée par coordonnée, une addition et une multiplication sur $\Pi_{i\in I} A_i$, en posant

$$(a+b)(i) := a(i) + b(i) \text{ et } (a.b)(i) := a(i).b(i).$$

Muni de ces deux opérations $\Pi_{i\in I}A_i$ est un anneau commutatif, avec $0 = (0, ..., 0, ...)$ et $1 = (1, ..., 1, ...)$.
Si $P(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, alors pour chaque i, et chaque $a_1, \ldots, a_n \in \Pi_{i\in I}A_i$,

$$P(a_1, \ldots, a_n)(i) = P(a_1(i), \ldots, a_n(i)).$$

En revanche, même si les A_i sont des corps, l'anneau $\Pi_{i\in I}A_i$ ne sera jamais intègre dès que I contient au moins deux éléments distincts: en effet si on prend, a, b tels que $a(i_1) = 1$ et $a(j) = 0$ pour $j \neq i_1$, et $b(i_1) = 0$ et $b(j) = 1$ pour $j \neq i_1$, on voit que $a.b = 0$.

Pour éviter cela, si I est infini, on va quotienter de manière à identifier à 0 les uples a tels que $a(i)$ est égal à zéro "presque partout".

4.2.3 Produits réduits et ultraproduits de L-structures

Soit L un langage à une seule sorte, $(\mathcal{M}_i)_{i\in I}$ une famille de L-structures et $\mathcal{F}$ un filtre sur I. On va définir une L-structure sur le produit réduit $\mathcal{M} := \Pi_{i\in I}\mathcal{M}_i/\mathcal{F}$. On rappelle que si $a, b \in \Pi_{i\in I}\mathcal{M}_i$, a et b seront égaux dans $\mathcal{M}$, noté $a =_{\mathcal{F}} b$ ssi $\{i \in I : a(i) = b(i)\} \in \mathcal{F}$. On note la classe de $a = (a(i))_{i\in I}$, $a_{\mathcal{F}}$.

Il faut donner une interprétation pour chaque symbole du langage, compatible avec le quotient:

– si c est un symbole de constante, $c^{\mathcal{M}}$ est la classe d'équivalence de $(c^{\mathcal{M}_i})_{i\in I}$,

– si R est un symbole de relation d'arité n, si $((a_1)_{\mathcal{F}}, \ldots, (a_n)_{\mathcal{F}}) \in \mathcal{M}$,

$$((a_1)_{\mathcal{F}}, \ldots, (a_n)_{\mathcal{F}}) \in R^{\mathcal{M}} \text{ iff } \{i \in I : \mathcal{M}_i \models R(a_1(i), \ldots, a_n(i))\} \in \mathcal{F},$$

– si f est un symbole de fonction d'arité n, si $((a_1)_{\mathcal{F}}, \ldots, (a_n)_{\mathcal{F}}) \in \mathcal{M}$, on pose

$$f^{\mathcal{M}}((a_1)_{\mathcal{F}}, \ldots, (a_n)_{\mathcal{F}})) := (f^{\mathcal{M}_i}(a_1(i), \ldots, a_n(i)))_{i\in I}.$$

On vérifie facilement que ces défintions sont indépendantes du choix des représentants pour les $(a_j)_{\mathcal{F}}$.

On remarque également que lorsque l'on a défini la relation d'équivalence $=_{\mathcal{F}}$, on a bien défini l'interprétation dans $\mathcal{M}$ du symbole de relation distingué $R_=$.

4.2.4 Cas des langages à plusieurs sortes

Si L est un langage à plusieurs sortes, $(S_j)_{j\in J}$, on veut que $\mathcal{M}$, le produit réduit, soit la réunion disjointe des sortes ${S_j}^{\mathcal{M}}$. Donc si $(\mathcal{M}_i)_{i\in I}$ est une famille de L-structures, et $\mathcal{F}$ est un filtre sur I, on définit la L-structure $\mathcal{M}$ de la façon suivante: l'ensemble de base $|\mathcal{M}|$ sera la réunion disjointe des ensembles ${S_j}^{\mathcal{M}}$, où

$${S_j}^{\mathcal{M}} := \Pi_{i\in I}{S_j}^{\mathcal{M}_i}/\mathcal{F}.$$

Autrement dit ${S_j}^{\mathcal{M}}$ est le quotient de $\{(a \in \Pi_{i\in I}|\mathcal{M}_i| : a(i) \in {S_j}_i^{\mathcal{M}} \text{ pour tout } i \in I\}$ par la relation d'équivalence $=_{j,F}$, où $a =_{j,F} b$ ssi $\{i \in I : a(i) = b(i)\} \in \mathcal{F}$. La relation $=_{j,F}$ induit la relation d'égalité attachée à la sorte S_j dans $\mathcal{M}$.

Ensuite on définit l'interprétation des autres symboles du langage L dans $\mathcal{M}$ comme plus haut, en quotientant sorte par sorte à chaque fois par la relation d'équivalence adéquate.

Pour unifier la notation on se permettra d'écrire quand même dans ce cas aussi que $\mathcal{M} = \Pi_{i\in I}\mathcal{M}_i/\mathcal{F}$.

4.2.5 Le théorème de Łos

On va maintenant montrer le théorème fondamental de préservation des formules du premier ordre:

Théorème 10 (Théorème de Łos) *Soient L un langage, $(M_i)_{i\in I}$ une famille de L-structures, $\mathcal{U}$ un ultrafiltre sur I et $\mathcal{M} = \Pi_{i\in I}\mathcal{M}_i/\mathcal{U}$. Soit $\phi(x_1,\ldots,x_n)$ une formule, et $a_{1_\mathcal{U}},\ldots,a_{n_\mathcal{U}} \in \mathcal{M}$. Alors*

$$\mathcal{M} \models \phi(a_{1_\mathcal{U}},\ldots,a_{n_\mathcal{U}}) \ \ ssi \ \ \{i\in I : \mathcal{M}_i \models \phi(a_1(i),\ldots,a_n(i))\} \in \mathcal{U}.$$

Preuve: La preuve est identique pour le cas à une ou plusieurs sortes.

On vérifie (immédiat, par induction sur l'ensemble des termes du langage) que tout se passe bien pour les termes de L, c'est-à-dire que si $t(v_1,\ldots,v_n)$ est un terme de L, alors pour tout $((a_1)_\mathcal{U},\ldots,(a_n)_\mathcal{U}) \in \mathcal{M}$,

$$t^\mathcal{M}(((a_1)_\mathcal{U},\ldots,(a_n)_\mathcal{U})) = [(t^{\mathcal{M}_i}(a_1(i),\ldots,a_n(i)),\ldots,a_n(i)))_{i\in I}]_\mathcal{U}.$$

On fait maintenant la démonstration par induction sur l'ensemble des formules de L.

Pour les formules de complexité zéro, c'est-à-dire les formules atomiques, c'est vrai par la définition que l'on a donnée de l'interprétation des symboles de relation dans $\mathcal{M}$: une formule atomique est de la forme $R(t_1(x_1,\ldots,x_k),\ldots,t_n(x_1,\ldots,x_k))$, pour R symbole de relation de L d'arité n, et les t_j termes en (au plus) k variables.

Par définition de la L-structure mise sur $\mathcal{M}$, et de la satisfaction pour les formules atomiques, on aura

$$\mathcal{M} \models R(t_1(a_{1_\mathcal{U}},\ldots,a_{k_\mathcal{U}}),\ldots,t_n(a_{1_\mathcal{U}},\ldots,a_{k_\mathcal{U}}))$$

ssi

$$({t_1}^\mathcal{M}(a_{1_\mathcal{U}},\ldots,a_{k_\mathcal{U}}),\ldots,{t_n}^\mathcal{M}(a_{1_\mathcal{U}},\ldots,a_{k_\mathcal{U}})) \in R^\mathcal{M}$$

ssi

$$\{i\in I : ({t_1}^{\mathcal{M}_i}(a_1(i),\ldots,a_k(i)),\ldots,{t_n}^{\mathcal{M}_i}(a_1(i),\ldots,a_k(i)) \in R^{\mathcal{M}_i}\} \in I$$

ssi

$$\{i\in I : \mathcal{M}_i \models (t_1(a_1(i),\ldots,a_k(i))\ldots,t_n(a_1(i),\ldots,a_k(i))\} \in \mathcal{F}.$$

Par induction, on doit maintenant considérer trois cas:

(i) $\phi = \neg\psi$, Alors

$$\mathcal{M} \models \phi(a_{1_\mathcal{U}},\ldots,a_{n_\mathcal{U}})$$

ssi, par définition de la négation,

$$\mathcal{M} \not\models \psi(a_{1_\mathcal{U}},\ldots,a_{n_\mathcal{U}})$$

ssi, par hypothèse d'induction,

$$\{i\in I : M_i \models \psi(a_1(i),\ldots,a_n(i))\} \notin \mathcal{U}$$

ssi, puisque $\mathcal{U}$ est un ultrafiltre, le complémentaire est dans $\mathcal{U}$, c'est-à-dire

$$\{i\in I : \mathcal{M}_i \not\models \psi(a_1(i),\ldots,a_n(i))\} \in \mathcal{U}$$

ssi, par définition de la négation à nouveau,

$$\{i \in I : \mathcal{M}_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}.$$

(ii) $\phi = (\phi_1 \wedge \phi_2)$,
$\mathcal{M} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$ ssi, par définition de la conjonction,

$$\mathcal{M} \models \phi_1(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) \text{ et } \mathcal{M} \models \phi_2(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$$

ssi, par hypothèse d'induction, $X_j := \{i \in I : R_i \models \phi_j(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$, pour $j = 1, 2$. Ceci, si et seulement si $X_1 \cap X_2 \in \mathcal{U}$, (car $\mathcal{U}$ est un filtre) et

$$X_1 \cap X_2 = \{i \in I : \mathcal{M}_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}.$$

(iii) $\phi(x_1, \ldots, x_n) = \exists y\, \psi(y, x_1, \ldots, x_n)$.
Si $\mathcal{M} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$, par définition du quantificateur existentiel, il existe $b \in \mathcal{M}$ tel que

$$\mathcal{M} \models \psi(b_\mathcal{U}, a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}).$$

Par hypothèse d'induction,

$$X = \{i \in I : \mathcal{M}_i \models \psi(b(i), a_1(i), \ldots, a_n(i))\} \in \mathcal{U}.$$

Mais, si $i \in X$, alors $\mathcal{M}_i \models \exists y\, \psi(y, a_1(i), \ldots, a_n(i))$, c'est-à-dire $\mathcal{M}_i \models \phi(a_1(i), \ldots, a_n(i))$. Donc, l'ensemble $\{i \in I : \mathcal{M}_i \models \phi(a_1(i), \ldots, a_n(i)\}$ contient un élément de $\mathcal{U}$ et $\mathcal{U}$ étant un filtre, est donc aussi dans $\mathcal{U}$.
Réciproquement, supposons que $X = \{i \in I : \mathcal{M}_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$. Pour chaque $i \in X$, il existe $b_i \in \mathcal{M}_i$ tel que $\mathcal{M}_i \models \psi(b_i, a_1(i), \ldots, a_n(i))$. Soit $b \in \mathcal{M}$ tel que, pour $i \in X$, $b(i) = b_i$, et pour $i \notin X$, $b(i)$ est un élément quelqconque de $\mathcal{M}_i$. Alors par hypothèse d'induction, puisque $X \in \mathcal{U}$,

$$\mathcal{M} \models \psi(b_\mathcal{U}, a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}),$$

c'est-à-dire, par définition de $\exists$,

$$\mathcal{M} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}).$$

□

On peut remarquer que l'hypothèse de maximalité sur $\mathcal{U}$ n'a été utilisée que pour le cas de la négation.

Remarque: Si I est infini et si $\mathcal{U}$ est un ultrafiltre principal sur I, $\mathcal{U}$ est engendré par $\{i_0\}$. Alors on peut vérifier que, pour toute formule $\phi(v_1, \ldots, v_n)$, $\mathcal{M} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$ si et seulement si $\mathcal{M}_{i_0} \models \phi(a_1(i_0), \ldots, a_n(i_0)$. En fait si g est l'application : $a \in \mathcal{M}_{i_0} \mapsto b_\mathcal{U}$, où b est tel que $b(i_0) = a$ et $b(j)$ est égal à n'importe quel élément de $\mathcal{M}_j$, pour $j \neq i_0$, g est une bijection et

$$\mathcal{M}_{i_0} \models \phi(a_1, \ldots, a_n) \text{ ssi } \mathcal{M} \models \phi(g(a_1), \ldots, g(a_n)).$$

L'application g est ce qu'on applelle un L-isomorphisme (voir section 6).

Ultrapuissance et plongement diagonal: Si pour chaque $i \in I$, $\mathcal{M}_i = \mathcal{N}$, alors on note $\mathcal{N}^\mathcal{U} := \Pi_{i \in I} \mathcal{M}_i / \mathcal{U} = \mathcal{N}^I / \mathcal{U}$ et on l'appelle l'ultra puissance de $\mathcal{N}$. Si on définit l'application d de $\mathcal{N}$ dans $\mathcal{N}\mathcal{U}$, par $d(a) := (a^I)_\mathcal{U}$, on appelle d le plongement diagonal. On vérifie facilement que l'image de $\mathcal{N}$ par d, $d(\mathcal{N})$, est une L-sous-structure de $\mathcal{N}\mathcal{U}$. En fait d est un L-plongement élémentaire (voir section 6).

4.3 Démonstration du théorème de compacité

On rappelle l'énoncé du théorème de compacité (voir section 3)

Théorème 11 (Théorème de compacité) *Soit L un langage et soit Σ un ensemble d'énoncés de L tel que tout sous ensemble fini de Σ a un modèle. Alors Σ a un modèle.*

Preuve: Par hypothèse, tout sous-ensemble fini F de Σ a un modèle $\mathcal{M}_F$. Soit I l'ensemble de toutes les parties finies de Σ. Pour chaque énoncé θ de Σ, soit $V(\theta) := \{F \in I; \theta \in F\}$. On remarque que si $F \in V(\theta)$, $\mathcal{M}_F \models \theta$. La famille $\{V(\theta); \theta \in \Sigma\}$ a la propriété de l'intersection finie: l'ensemble fini $\{\theta_1, \ldots, \theta_n\} \in V(\theta_1) \cap \ldots \cap V(\theta_n)$. Elle est contenue dans un filtre et donc dans un ultrafiltre $\mathcal{U}$. On vérifie que $(\Pi_{F \in I} \mathcal{M}_F)/\mathcal{U}$, l'ultraproduit des $\mathcal{M}_F$, est, par le théorème de Łos, un modèle de Σ. En effet, soit $\theta \in \Sigma$, alors $\{F \in I; \mathcal{M}_F \models \theta\} \supset V(\theta)$, comme nous l'avons remarqué au-dessus. Cet ensemble contenant un élément de $\mathcal{U}$, est aussi un élément de $\mathcal{U}$. □

5 Applications algébriques des ultraproduits

5.1 Les corps algébriquement clos

Rappels algébriques sur les corps algébriquement clos (voir par exemple [La]):
1. Un corps K est *algébriquement clos* si tout polynôme de $K[X]$ de degré ≥ 1 a une racine dans K.
2. Soit k un corps, il existe un corps algébriquement clos K qui est une extension de k.
3. Soit k un corps, il existe une extension de k qui est algébriquement close et algébrique sur k, qu'on appellera une *clôture algébrique* de k et qu'on notera $\bar{k}$. Deux clôtures algébriques de k sont isomorphes au-dessus de k.
4. Cas de la caractéristique p: fixons une clôture algébrique du corps fini $\mathbb{F}$, $\overline{\mathbb{F}_p}$. Dans cette clôture algébrique, $\mathbb{F}_p$ a une seule extension de degré n, $\mathbb{F}_p < \mathbb{F}_{p^n}$. De plus, $\mathbb{F}_{p^n} < \mathbb{F}_{p^m}$ ssi n divise m, appelons $i_{n,m}$ ce plongement. On obtient donc $\overline{\mathbb{F}_p}$ comme limite inductive de la famille $(\mathbb{F}_{p^n})_{n \geq 1}$, munie des plongements $i_{n,m}$. En particulier, tout sous-corps finiment engendré de $\overline{\mathbb{F}_p}$ est fini, c'est-à-dire, $\overline{\mathbb{F}_p}$ est un corps localement fini .
5. Cas de la caractéristique 0. On utilisera une seule propriété qu'on admet: tout corps algébriquement clos de caractéristique zéro et de cardinalité identique à celle de $\mathbb{C}$ (c'est-à-dire de cardinalité le continu, la cardinalité de $\mathcal{P}(\mathbb{N})$) est isomorphe à $\mathbb{C}$.

Théorie des corps algébriquement clos On travaille avec le langage des anneaux, $L_{ann} = \{+, -, ., 0, 1\}$. Soit θ_c l'énoncé (ou le nombre fini d'énoncés) du langage des anneaux dont les modèles sont exactement les corps et soit σ_p l'énoncé $p = 0$, pour p un nombre premier (p est la notation pour $1 + \ldots + 1$ p fois).

Il existe une théorie, c'est-à-dire un ensemble d'énoncés, dont les modèles sont exactement les corps algébriquement clos.
Soit $n \geq 1$ un entier fixé, on peut écrire un énoncé, θ_n, tel que un corps K satisafit θ_n ssi tout polynôme unitaire de degré n à coefficients dans R a une solution dans R:

$$\forall y_0 \ldots \forall y_{n-1} \exists x \, (x^n + \Sigma_{i=0}^{n-1} y_i . x^i) = 0.$$

Les corps algébriquement clos sont alors exactement les modèles de la théorie

$$T_{CAC} := \{\theta_c\} \cup \{\theta_n; n \geq 1\}.$$

Pour p premier, on note T_{CAC_p} la théorie des corps algébriquement clos de caractéristique p, c'est-à-dire $T_{CAC} \cup \{\sigma_p\}$. Et T_{CAC_0} sera la théorie des corps algébriquement clos de caractéristique zéro, c'est-à-dire $T_{CAC} \cup \{\neg\sigma_p : p \text{ premier}\}$.

Les ultraproduits permettent de montrer que la théorie de $\mathbb{C}$ est la "limite" de celle des $\mathbb{F}_p$ quand p tend vers l'infini, dans un sens très précis:

Proposition 12 *Soit S un ensemble infini de nombres premiers et $\mathcal{U}$ un ultrafiltre non principal sur S. Soit $\mathcal{K} := \Pi_{p\in S}\overline{\mathbb{F}_p}/\mathcal{U}$, l'ultraproduit de la famille des clôtures algébriques de $\mathbb{F}_p$, pour $p \in S$. Alors $\mathcal{K}$ est isomorphe à $\mathbb{C}$.*

Preuve: Notons $K_p := \overline{\mathbb{F}_p}$. Rappellons (4.1) que $\mathcal{U}$ doit contenir le filtre de Frechet sur S, donc tout sous-ensemble de S de complémentaire fini.
1. $\mathcal{K}$ est de caractéristique zéro: en effet, soit p un premier, alors $\{q \in S : K_q \models p \neq 0\}$ est de complémentaire fini, donc est un élément du filtre de Frechet, donc de $\mathcal{U}$. Par Łos, il suit que $\mathcal{K} \models p \neq 0$ aussi, et cela pour chaque p.

2. $\mathcal{K}$ est un corps algébriquement clos. En effet on vient de voir qu' une L_{ANN}-structure est un corps algébriquement clos ssi elle est modèle de T_{CAC}. Pour chaque $p \in S$, K_p est modèles de T_{CAC}, donc Par Łos, $\mathcal{K}$ aussi

3. Quelle est la cardinalité de $\mathcal{K}$? Par le lemme 8, il est de la puissance du continu, c'est à dire a le même cardinal que $\mathcal{P}(\mathbb{N})$, qui est aussi la cardinalité de $\mathbb{C}$. Nous avons admis que, à isomorphisme près, il y a un unique corps algébriquement clos de caractéristique zéro et de même cardinalité que $\mathbb{C}$. □

Corollaire 13 *Si un énoncé du premier ordre du langage des anneaux L_{ann} est vrai dans la clôture algébrique de $\mathbb{F}_p$ pour une infinité de premiers p, il est vrai dans $\mathbb{C}$.*

Preuve: Soit S l'ensemble infini des nombres premiers p tels que $\overline{\mathbb{F}_p}$ est modèle de σ. Par la proposition précédente, $\mathbb{C}$ est isomorphe au corps $\mathcal{K}$, ultraproduit des $\overline{\mathbb{F}_p}$ pour $p \in S$. Par Łos, $\mathbb{C}$ est donc modèle de σ. □

On va donner deux exemples d'applications directes de ce résultat de transfert.

5.1.1 Le théorème d'Ax sur les applications polynomiales

L'une des premières applications de ce type:

Théorème 14 (Ax 1969) *Soit f une application polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$, $(n \geq 1)$. Si f est injective, f est surjective.*

(L'application f est polynomiale c'est-à-dire: $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots f_n(x_1, \ldots, x_n))$ avec, pour chaque i, $f_i \in \mathbb{C}[X_1, \ldots, X_n]$.)

En fait le théorème, énoncé ainsi, est seulement un cas particulier du Théorème d'Ax, qui considère les endomorphismes des variétés algébriques (et en fait des schémas de type

fini ([Ax])). Le cas particulier de l'espace affine tout entier, c'est-à-dire $\mathbb{C}^n$ avait déjà été remarqué dans [BB-R]. Il y a eu depuis plusieurs autres démonstrations, par exemple Borel ([Bor]) utilisant la cohomologie et Rudin ([Rud]) qui donne une nouvelle preuve pour $\mathbb{C}^n$.

Après avoir vu la démonstration via la théorie des modèles, dans le cas de $\mathbb{C}^n$, le lecteur devrait pouvoir refaire sans aucune difficulté le cas où f est une application polynomiale de V^n dans V^n, avec V un fermé de Zariski dans C^k

$$V = \{a \in \mathbb{C}^k : P_1(a) = P_2(a) = \ldots = P_m(a) = 0\}$$

pour $P_1, \ldots, P_m \in \mathbb{C}[X_1, \ldots, X_k]$.

On veut utiliser le théorème de transfert, de façon à ne démontrer vraiment le théorème que dans des cas très faciles. La première question est donc: *Quels sont les corps qui vérifient évidemment le théorème d'Ax?*

Les corps finis

Soit K un corps fini ($K = \mathbb{F}_{p^r}$, pour p premier et $r \geq 1$).
Alors si g est *n'importe quelle* application injective de K^n dans K^n, g est surjective, simplement car il s'agit d'une application injective d'un ensemble fini dans lui-même.

Les corps localement finis

Un corps K est **localement fini** si tout sous-corps finiment engendré de K est fini. Un corps localement fini est donc nécessairement de caractéristique $p > 0$, car tout corps de caractéristique zéro contient $\mathbb{Q}$.

Lemme 15 *Les corps localement finis satisfont le Théorème d'Ax.*

Preuve: Soient $f = (f_1, \ldots, f_n)$ une application polynomiale injective de K^n dans K^n, et $a = (a_1, \ldots, a_n)$ un élément de K^n, avec K localement fini. Soit K_0 le sous-corps de K engendré par $\{a_1, \ldots, a_n\}$ et tous les coefficients des polynômes $f_1, \ldots, f_n$ (qui sont en nombre fini). K étant localement fini, le corps K_0 est fini. On peut considérer la restriction f_0 de f à ${K_0}^n$. Il s'agit de polynômes à coefficients dans K_0, donc l'image de f_0 est aussi contenue dans ${K_0}^n$. L'application f_0 est injective de ${K_0}^n$ dans ${K_0}^n$, K_0 est fini, donc f_0 est surjective et il existe $e_1, \ldots, e_n \in {K_0}^n$ tels que $f_0(e_1, \ldots, e_n) = f(e_1, \ldots, e_n) = a$. □

En particulier, *pour tout premier p, $\overline{\mathbb{F}_p}$ satisfait le théorème d'Ax.*

Enfin, il nous faut vérifier que *le théorème d'Ax s'énonce par une infinité d'énoncés du premier ordre.* Ce que l'on peut dire, par une formule $J_{n,d}$, c'est que, si K est un corps, pour n et d fixés, toute application polynomiale de K^n dans K^n, de degré inférieur ou égal à d, qui est injective, est surjective. Comme toujours, il va falloir quantifier sur les coefficients des polynômes, pour dire "pour tout polynôme de degré $\leq d$", c'est donc un peu fastidieux à écrire. Je l'écris ici dans un cas simple $f = (f_1, f_2)$, application de degré ≤ 2 de $\mathbb{K}^2$ dans $\mathbb{K}^2$.
On a $f_1(x_1, x_2) = \Sigma_{i+j=2}\ y_{ij} {x_1}^i {x_2}^j$ et $f_2(x_1, x_2) = \Sigma_{i+j=2}\ z_{ij} {x_1}^i {x_2}^j$.

Soit $I(\bar{y}, \bar{z})$ la formule :

$$\forall x_1 \forall x_2 \forall x'_1 \forall x'_2 [((\Sigma_{i+j=2}\ y_{ij} {x_1}^i {x_2}^j = \Sigma_{i+j=2}\ y_{ij} {x'_1}^i {x'_2}^j) \wedge$$

$$(\Sigma_{i+j=2}\ z_{ij}{x_1}^i{x_2}^j = \Sigma_{i+j=2}\ z_{ij}{x'_1}^i{x'_2}^j)) \rightarrow (x_1 = x'_1 \wedge x_2 = x'_2)].$$

Alors $K \models I((\bar{y}, \bar{z})$ ssi f est injective.
Soit $S(\bar{y}, \bar{z})$ la formule

$$\forall v \forall w\, \exists x_1 \exists x_2((\Sigma_{i+j=2}\ y_{ij}{x_1}^i{x_2}^j = v) \wedge (\Sigma_{i+j=2}\ z_{ij}{x_1}^i{x_2}^j = w)).$$

Alors $K \models S(\bar{y}, \bar{z})$ ssi f est surjective.
Maintenant soit

$$J_{2,2} := (\forall \bar{y}\, \forall \bar{z}\, (I(\bar{y}, \bar{z}) \rightarrow S(\bar{y}, \bar{z}))).$$

Alors $K \models J_{2,2}$ si et seulement si toute application polynomiale de degré inférieur ou égal à 2, de K^2 dans K^2, qui est injective, est surjective.

Pour chaque p premier , et chaque n, d, $\overline{\mathbb{F}_p}$ est modèle de l'énoncé $J_{n,d}$. Par le corollaire 13, $\mathbb{C}$ l'est aussi et satisfait donc bien le théorème d'Ax.

5.1.2 Une deuxième application: Action algébrique d'un groupe fini d'ordre p^m sur $\mathbb{C}^n$

On peut exactement de la même manière que pour le théorème d'Ax, démontrer à peu de frais le résultat classique suivant [Be]:

Théorème 16 *Soit G un groupe fini d'ordre p^m, pour p premier, et γ une action algébrique de G sur $\mathbb{C}^n$. Alors l'action γ a un point fixe.*

On fixe donc un groupe G d'ordre p^m L'action γ est algébrique veut dire que

$$\gamma : G \times \mathbb{C}^n \mapsto \mathbb{C}^n$$

et pour chaque $g \in G$, il existe $f_{g_1}, \ldots, f_{g_n} \in \mathbb{C}[X_1, \ldots, X_n]$, tels que pour tout $(x_1, \ldots, x_n) \in \mathbb{C}^n$,

$$\gamma(g, (x_1, \ldots, x_n) = g.(x_1, \ldots, x_n) = (f_{g_1}(x_1, \ldots, x_n), \ldots, f_{g_n}(x_1, \ldots, x_n).$$

On dira que l'action est de degré inférieur ou égal à d si chacun des polynômes f_{g_i} est de degré inférieur ou égal à d.

Maintenant, une famille de polynômes $(f_{g_i})_{g \in G, 1 \leq i \leq n}$ dans $\mathbb{C}[X_1, \ldots, X_n]$, définira une action (algébrique) de G sur $\mathbb{C}^n$ si et seulement si: (on note $x = (x_1, \ldots, x_n)$)
– $\forall x\, f_{e_i}(x) = x$, pour e l'identité de G et $1 \leq i \leq n$,
– $\forall x\, f_{g'_i}(f_{g_1}(x), \ldots, f_{g_n}(x)) = f_{h_i}(x)$ pour $h, g, g' \in G$ tels que $h = g'g$ et $1 \leq i \leq n$.
En quantifiant, comme dans l'application précédente, sur les coefficients des polynômes, on voit qu'il existe , pour chaque entier d une formule $\psi_{(d,n)}(\overline{y}$ du langage des anneaux tel que, si K est un corps, $K \models \psi_{(d,n)}(\overline{a})$ si et seulement si il existe une suite de polynômes $(f_{g_i})_{g \in G, 1 \leq i \leq n}$ dans $K[X_1, \ldots, X_n]$, de degré inférieur ou égal à d, dont les $\overline{a}$ sont les coefficients, et qui définit une action algébrique de G sur K^n.

Toujours par une formule du premier ordre sur les coefficients des polynômes, on peut également dire que cette action a un point fixe: G étant fini, il suffit de considérer la

formule $\phi(\overline{y})$, disjonction finie, sur les éléments g de G différents de l'élément neutre , des formules

$$\exists x \, (f_{g_1}(x), \ldots, f_{g_n}(x)) = x.$$

Donc il existe un énoncé du premier ordre:

$$\theta_{n,d} := \forall \overline{y} (\psi_{(d,n)} (\overline{y} \, \rightarrow \, \phi(\overline{y})$$

tel que si K est un corps, $K \models theta$ si et seulement si toute action algébrique de G sur K^n, de degré inférieur ou égal à d, a un point fixe.

Par le corollaire 13, pour vérifier que $\mathbb{C} \models \theta_{n,d}$, il suffit de vérifier que pour un nombre infini de nombres premiers q, $K_q := \overline{\mathbb{F}_q} \models \theta_{n,d}$, c'est-à-dire que toute action algébrique de G (de degré au plus d) sur $K_q = \overline{\mathbb{F}_q}$ a un point fixe.

Cela est facile à vérifier: si le groupe G est d'ordre p^n, soit q un nombre premier différent de p. Soit k sous corps de K_q engendré par les coefficients des polynômes qui définissent l'action algébrique de G sur ${K_q}^n$. Alors l'action de G restreinte aux éléments de k définit une action de G sur k. Le corps k étant finiment engendré dans K_q est un sous-corps corps fini donc isomorphe à un $\mathbb{F}_{q^r}$. C"est un simple calcul sur le nombre d'orbites de vérifier que si un groupe G de cardinalité p^m agit sur un ensemble fini de cardinalité q^r, avec q et p premiers distincts, alors il doit y avoir un point fixe.

5.2 Rapport avec les constructions algébriques habituelles

1. Si on a une famille $(G_i)_{i \in I}$ de *groupes*, si on note $\mathcal{G} := \Pi_{i \in I} G_i$, le produit cartésien des G_i, pour $g \in \mathcal{G}$, on appelle $Z(g)$ l'ensemble des i dans I tels que $g(i) = e_i$, où e_i est l'élément neutre du groupe G_i. Alors si $g, h \in \mathcal{G}$, $Z(g^{-1}) = Z(g)$ et $Z(gh) \supset Z(g) \cap Z(h)$. Il est alors facile de vérifier que si $\mathcal{F}$ est un filtre sur I et si $N = \{g \in \mathbb{G} : \text{ tels que } Z(g) \in \mathcal{F}\}$, N est un sous-groupe normal et que si $g, h \in \mathbb{G}$, $g_{\mathcal{F}} = h_{\mathcal{F}}$ si et seulement si $h^{-1} g \in N$. On vérifie immédiatemment que $\mathcal{G}/\mathcal{F}$ est isomorphe au groupe $\mathcal{G}/\mathcal{N}$.

2. Soit $(R_i)_{i \in I}$ une famille d'anneaux commutatifs. Considérons

$$J_{\mathcal{F}} := \{a \in \Pi_{i \in I} R_i \, : \text{ tels que } Z(a) (:= \{i \in I; a_i = 0\}) \in \mathcal{F}\}.$$

Lemme 17 1. *$J_{\mathcal{F}}$ est un idéal de $\mathcal{R}$ et pour tous $a, b \in \mathcal{R}$, $a_{\mathcal{F}} = b_{\mathcal{F}}$ si et seulement si $a - b \in J$.*

3. *Si pour chaque i, R_i est un corps, $\mathcal{F}$ est un ultrafiltre ssi $J_{\mathcal{F}}$ est un idéal maximal.*

Preuve: 1. Si $a, b \in J_{\mathcal{F}}$, $\{i \in I; a(i) = 0\} \in \mathcal{F}$ et $\{i \in I; b(i) = 0\} \in F$. $\mathcal{F}$, étant un filtre, est stable par intersection finie, donc $\{i \in I; a(i) = b(i) = 0\} \in \mathcal{F}$ et est contenu dans $\{i \in I \, : a(i) + b(i) = 0\}$. Donc $a + b \in J_{\mathcal{F}}$. Si $c \in \mathcal{R}$, $a \in J_{\mathcal{F}}$, $\{i \in I; c(i) a(i) = 0\} \supset \{i \in I; a(i) = 0\}$ et, toujours par les propriétés des filtres, est aussi dans $\mathcal{F}$, donc $ca \in J_{\mathcal{F}}$.
2. Supposons que les R_i sont des corps et que $\mathcal{F}$ est un ultrafiltre. Soit $b \notin J_{\mathcal{F}}$, alors $\{i; b(i) = 0\} \notin \mathcal{F}$, mais par maximalité de $\mathcal{F}$, $\{i; b(i) \neq 0\} \in \mathcal{F}$. Soit a tel que $a(i) = 1$ si $b((i) = 0$, et $a(i) = 0$ si $b(i) \neq 0$. Alors $a \in J_{\mathcal{F}}$. Soit c tel que $c(i) = 0$ si $b(i) = 0$ et

$c(i) = 1/b(i)$ sinon. Alors $a + cb = 1$, donc $J_{\mathcal{F}}$ est bien maximal. Réciproquement si $J_{\mathcal{F}}$ est maximal, soit $X \subset I$ tel que $X \notin \mathcal{F}$. Soit $a \in \mathcal{R}$ tel que $Z(a) = X$. Donc, $a \notin J_{\mathcal{F}}$. Par maximalité, il existe c tel que $1 - ca \in J_{\mathcal{F}}$ et $Z(1 - ca) \subset I \setminus X$, donc $(I \setminus X) \in \mathcal{F}$. □

Si $\mathcal{F}$ est un ultrafiltre, $\mathcal{R}/\mathcal{F}$ est isomorphe au corps $\mathcal{R}/J_{\mathcal{F}}$. On pourrait vérifier "à la main" que si $\mathcal{F}$ est un ultrafiltre non principal, et si les caractéristiques des R_i sont finies non bornées, alors $\mathcal{R}/\mathcal{F}$ est de caractéristique 0, ou alors que si tous les R_i sont algébriquement clos, alors $\mathcal{R}/\mathcal{F}$ est aussi algébriquement clos, mais ce sont là juste des cas particuliers du fait général que le passage à un ultraproduit de L-structures "préserve" tous les énoncés du premier ordre qui sont vrais "presque partout".

6 Morphismes et Extensions élémentaires

6.1 Premières définitions

Soient L un langage, $\mathcal{M}$ et $\mathcal{N}$ deux L-structures et h une application de $|\mathcal{M}|$ dans $|\mathcal{N}|$. L'application h est un L-**homomorphisme** de $\mathcal{M}$ dans $\mathcal{N}$ si h vérifie:

– (0) pour toute sorte S de L, $h(S^{\mathcal{M}}) \subset S^{\mathcal{N}}$,

– (1) pour tout symbole c de constante de L, $h(c^{\mathcal{M}}) = c^{\mathcal{N}}$,

– (2) pour tout symbole f de fonction de L, d'arité k, pour tout $(m_1, \ldots, m_k) \in |M|^k$, $h(f^{\mathcal{M}}(m_1, \ldots, m_k)) = f^{\mathcal{N}}(h(m_1), \ldots, h(m_k))$.

– (3) pour tout symbole R de relation de L, d'arité k, pour tout $(m_1, \ldots, m_k) \in |M|^k$, si $(m_1, \ldots, m_k) \in R^{\mathcal{M}}$, alors $(h(m_1), \ldots, h(m_k)) \in R^{\mathcal{N}}$.

L'application h est un L-**plongement** de $\mathcal{M}$ dans $\mathcal{N}$ si h est un L-homomorphisme et satisfait en plus que pour tout symbole R de relation de $\mathcal{L}$, d'arité k, pour tout $(m_1, \ldots, m_k) \in M^k$, $(m_1, \ldots, m_k) \in R^{\mathcal{M}}$, **si et seulement si** $(h(m_1), \ldots, h(m_k)) \in R^{\mathcal{N}}$.

En particulier, dans le cas de langages et de structures égalitaires, un L-plongement est injectif.

Un L-plongement surjectif est appelé un L-**isomorphisme**. Un L-isomorphisme de $\mathcal{M}$ dans $\mathcal{M}$ est appelé un L-**automorphisme** de $\mathcal{M}$.

Remarque: un L-homomorphisme injectif n'est pas forcément un L-plongement. C'est le cas si le langage L ne comprend pas de symbole de relation (autre que l'égalité), mais si on considère par exemple le langage L d'une relation binaire, et les deux L-structures $\mathcal{M}_1 = <\mathbb{Z}, \equiv_6>$ et $\mathcal{M}_2 = <\mathbb{Z}, \equiv_3>$, où $\equiv_n$ est la congruence modulo n, alors l'identité est un L-homomorphisme bijectif de $\mathcal{M}_1$ dans $\mathcal{M}_2$ mais n'est pas un L-plongement.

On voit que $\mathcal{M}$ est une L-sous-structure de $\mathcal{N}$ si et seulement si l'inclusion est un L-plongement.

On peut caractériser les morphismes par le type de formules qu'ils préservent:

On dit qu'une formule est **sans quantificateur** si elle ne contient ni le symbole $\exists$, ni le symbole $\forall$. On vérifie facilement que l'ensemble des formules sans quantificateurs peut être défini par induction: c'est la clôture, à l'intérieur de l'ensemble de toutes les formules, de l'ensemble des formules atomiques par la négation, la conjonction (et la disjonction).

Proposition 18 *Soit h une application de $|\mathcal{M}|$ dans $|\mathcal{N}|$.*

L'application h est un L-plongement de $\mathcal{M}$ dans $\mathcal{N}$ si et seulement si, pour toute formule $\phi(v_1, \ldots, v_n)$ de L, **sans quantificateurs**, *pour tout $(m_1, \ldots, m_n) \in |\mathcal{M}|^n$, $\mathcal{M} \models \phi(m_1, \ldots, m_n)$ ssi $\mathcal{N} \models \phi(h(m_1), \ldots, h(m_n))$.*

Preuve: Dans un sens supposons que l'application h préserve toutes les formules sans quantificateurs. Soit c un symbole de constante du langage, et $\phi(v)$ la formule (sans quantificateurs) "v = c". Alors pour tout $a \in \mathcal{M}$, $\mathcal{M} \models \phi(a)$ ssi $a = c^{\mathcal{M}}$ ssi $\mathcal{N} \models h(a)$ ssi $h(a) = c^{\mathcal{N}}$, donc $h(c^{\mathcal{M}}) = c^{\mathcal{N}}$. Si f est un symbole de fonction d'arité n, alors $\mathcal{M} \models f(a_1, \ldots, a_n) = b$ (formule sans quantificateurs), ssi $\mathcal{N} \models f(h(a_1), \ldots, h(a_n) = h(b)$. Donc $h \circ f^{\mathcal{M}} = f^{\mathcal{N}} \circ h$. Si R est un symbole de fonction d'arité n alors $\mathcal{M} \models R(a_1, \ldots, a_n))$ (formule sans quantificateurs), ssi $\mathcal{N} \models R(h(a_1), \ldots, h(a_n))$. L'application h est bien un L-plongement.

Dans l'autre sens supposons que h est un L-plongement. On vérifie facilement que, plus généralement si h est un L-homomorphisme, alors h commute avec tous les $t^{\mathcal{M}}$, c'est-à-dire, pour $t(v_1, \ldots, v_n)$ un terme de L, pour $a \in \mathcal{M}^n$, $h(t^{\mathcal{M}}(a)) = t^{\mathcal{N}}h(a))$ (par induction sur l'ensemble des termes de L).

Ensuite, induction sur l'ensemble des formules sans quantificateurs. Vrai immédiatement pour les formules atomiques par définition d'un plongement.
Si $\phi = \neg\Psi(v_1, \ldots, v_n)$, avec ψ sans quantificateurs, $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ ssi $\mathcal{M} \not\models \psi(a_1, \ldots, a_n)$ ssi, par hypothèse d'induction, $\mathcal{N} \not\models \psi(h(a_1, \ldots, h(a_n))$.
Si $\phi = (\phi_1 \wedge \phi_2)(v_1, \ldots, v_n)$, avec ϕ_1 et ϕ_2 sans quantificateurs. $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ ssi

$$\mathcal{M} \models \phi_1(a_1, \ldots, a_n) \text{ et } \mathcal{M} \models \phi_2(a_1, \ldots, a_n)$$

ssi par hypothèse d'induction pour ϕ_1 et pour ϕ_2,

$$\mathcal{N} \models \phi_1(h(a_1), \ldots, h(a_n)) \text{ et } \mathcal{M} \models \phi_2(h(a_1), \ldots, h(a_n)$$

ssi

$$\mathcal{N} \models \phi(h(a_1), \ldots, h(a_n)).$$

□

Définition L'application h est un **L-plongement élémentaire** si pour **toute formule** $\psi(v_1, \ldots, v_n)$ de L, et pour tout $(m_1, \ldots, m_n) \in |\mathcal{M}|^n$,

$$\mathcal{M} \models \psi(m_1, \ldots, m_n) \text{ ssi } \mathcal{N} \models \psi(h(m_1), \ldots, h(m_n)).$$

On écrit $\mathcal{M} \preceq_L \mathcal{N}$.

Si $|\mathcal{M}| \subset |\mathcal{N}|$ on dit que $\mathcal{M}$ est une **sous-structure élémentaire** de $\mathcal{N}$ (ou que $\mathcal{N}$ est une **extension élémentaire** de $\mathcal{M}$) si l'inclusion est un $\mathcal{L}$-plongement élémentaire (noté $\mathcal{M} <_L \mathcal{N}$).
Exemple: Considérons les deux structures $\mathcal{M} =< \mathbb{N} \setminus \{0\}, \leq >$ et $\mathcal{N} =< \mathbb{N}, \leq >$ dans le langage $\mathcal{L}$ avec un symbole de relation binaire.

L'identité $i : \mathbb{N} \setminus \{0\} \mapsto \mathbb{N}$ est un $\mathcal{L}$-plongement mais n'est pas un $\mathcal{L}$-plongement élémentaire: en effet les conditions de la définition d'un $\mathcal{L}$-plongement sont satisfaites,

il faut et il suffit que i préserve l'égalité et la relation d'ordre. Mais si on considère la formule $\psi(v) = \forall w\ v \leq w$, on a:

$$\mathcal{M} \models \psi(1) \text{ mais } \mathcal{N} \models \neg\psi(1).$$

En revanche si on considère $h : \mathbb{N} \setminus \{0\} \mapsto \mathbb{N}$, définie par $h(n) = n - 1$, alors pour la formule $\psi(v)$ donnée au-dessus on a bien que:

$$\mathcal{M} \models \psi(1) \text{ et } \mathcal{N} \models \psi(h(1)).$$

En fait ce deuxième plongement h est, lui, élémentaire, comme le dit la proposition suivante:

Proposition 19 *Soit h un $\mathcal{L}$-plongement de $\mathcal{M}$ dans $\mathcal{N}$ qui est surjectif, alors h est un plongement élémentaire.*

Preuve: Par induction on montre que si $\phi(v_1, \ldots, v_n)$ est une formule et $a_1, \ldots, a_n \in \mathcal{M}$,

$$\mathcal{M} \models \phi(a_1, \ldots, a_n) \text{ ssi } \mathcal{N} \models \phi(h(a_1) \ldots, h(a_n)).$$

Vrai pour les formules atomiques car h est un plongement.
Si $\phi = \neg\psi$ ou $\phi = \phi_1 \wedge \phi_2$, vrai directement par l'hypothèse d'induction et les défintions respectives de $\neg$ et de $\wedge$.
Si $\phi = \exists v\, \psi(v, v_1, \ldots, v_n)$, $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ ssi il existe $b \in \mathcal{M}$ tel que $\mathcal{M} \models \psi(b, a_1, \ldots, a_n)$. Par induction sur ψ, ssi $\mathcal{N} \models \psi(h(b), h(a_1), \ldots, h(a_n))$. Si h est surjective cela est équivalent à $\mathcal{N} \models \exists v\, \psi(v, h(a_1), \ldots, h(a_n))$. □

Quelques remarques

Si $\mathcal{M}$ et $\mathcal{N}$ sont L-isomorphes, alors $\mathcal{M}$ et $\mathcal{N}$ sont élémentairement équivalents. Plus généralement s'il existe un L-plongement élémentaire de $\mathcal{M}$ dans $\mathcal{N}$, alors $\mathcal{M}$ et $\mathcal{N}$ sont élémentairement équivalents. Mais il ne suffit pas d'avoir $\mathcal{M} \subset_L \mathcal{N}$ et $\mathcal{M} \equiv_L \mathcal{N}$, pour que $\mathcal{M}$ soit une sous-structure élémentaire de $\mathcal{N}$: dans l'exemple donné plus haut de $\mathcal{M} =< \mathbb{N} \setminus \{0\}, \leq >$ et $\mathcal{N} =< \mathbb{N}, \leq >$, on a bien $\mathcal{M} \subset_L \mathcal{N}$, $\mathcal{M}$ et $\mathcal{N}$ sont élémentairement équivalentes pusiqu'on a pu construire un L-isomorphisme entre elles, mais $\mathcal{M}$ n'est pas sous-structure élémentaire de $\mathcal{N}$.

Comme on le verra un peu plus loin, dès que $\mathcal{M}$ est infinie, il existe $\mathcal{N}$ qui lui est élémentairement équivalente mais qui ne lui est pas isomorphe. Ce n'est en revanche pas le cas pour les structures finies :

Proposition 20 *(Exercice) Soit $\mathcal{L}$ un langage fini, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures élémentairement équivalentes. Si M, l'ensemble de base de $\mathcal{M}$ est fini, alors $\mathcal{M}$ et $\mathcal{N}$ sont $\mathcal{L}$-isomorphes.*

6.2 Critère de Tarski-Vaught

Proposition 21 (Tarski-Vaught) *Soit $\mathcal{N}$ une L-structure et $A \subset |\mathcal{N}|$ tel que pour toute formule $\phi(v_0, \ldots, v_{n-1}, v_n)$ de L, pour tous $a_0, \ldots, a_{n-1} \in A$,*

$$\text{si } \mathcal{N} \models \exists v_n \ \phi(a_0, \ldots, a_{n-1}, v_n), \text{ il existe } b \in A \text{ tel que } \mathcal{N} \models \phi(a_0, \ldots, a_{n-1}, b).$$

Alors, A est l'ensemble de base d'une L-sous-structure élémentaire de $\mathcal{N}$.

Preuve: On vérifie d'abord que A est l'ensemble de base d'une L-sous-structure, c'est-à-dire que A contient les interprétations des constantes dans $\mathcal{N}$ et est clos pour les fonctions de $\mathcal{L}$, et dans le cas d'un langage à plusieurs sortes, que pour chaque sorte S, $S^{\mathcal{N}} \cap A \neq \emptyset$. Soit S une sorte, et v une variable de sorte S. Alors $\mathcal{N} \models \exists v \, (v =_S v)$, avec v une variable de sorte S, donc il existe $b \in A \cap S^{\mathcal{N}}$ (tel que $b =_S b$). Soit c un symbole de constante, et $\phi(v_0)$ la formule $v_0 = c$. Alors $\mathcal{N} \models \exists v \, \phi(v)$. Par la propriété de A, il existe $a \in A$ tel que $\mathcal{N} \models \phi(a)$, c'est-à-dire, tel que dans $|\mathcal{N}|$, on $a = c^{\mathcal{N}}$.
Si f est un symbole de fonction d'arité k, soient $a_1, \ldots a_k \in A$. Soit $\psi(v_1, \ldots, v_k, w)$ la formule $f(v_1, \ldots, v_k) = w$. Alors $\mathcal{N} \models \exists w \, \psi(a_1, \ldots, a_k, w)$. Par hypothèse il doit donc exister $b \in A$ tel que $\mathcal{N} \models \psi(a_1, \ldots, a_k, b)$, c'est-à-dire $f^{\mathcal{N}}(a_1, \ldots, a_k) = b$.

Maintenant on montre que la L-sous-structure A est une sous-structure élémentaire, c'est-à-dire que pour toute formule $\phi(v_1, \ldots, v_n)$ et pour tous $a_1, \ldots, a_n \in A$

$$A \models \phi(a_1, \ldots, a_n) \text{ ssi } \mathcal{M} \models \phi(a_1, \ldots, a_n).$$

Par induction sur l'ensemble des formules:

- si $\phi(v_1, \ldots, v_n)$ est une formule atomique c'est vrai parceque A est une L-sous-structure (l'inclusion est donc un L-plongement).

- si $\phi = \neg\psi$ ou $\phi = \phi_1 \wedge \phi_2$ cela découle directement de l'hypothèse d'induction.

- si $\phi = \exists v \, \psi(v, v_1, \ldots, v_n)$; si $A \models \phi(a_1, \ldots, a_n)$, par définition, il existe $b \in A$ tel que $A \models \psi(b, a_1, \ldots, a_n)$. Par induction, $\mathcal{M} \models \psi(b, a_1, \ldots, a_n)$ et donc $\mathcal{M} \models \phi(a_1, \ldots, a_n)$. Réciproquement, si $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ c'est à dire $\mathcal{M} \models \exists v \, \psi(v, a_1, \ldots, a_n)$, par l'hypothèse, il existe $b \in A$ tel que $\mathcal{M} \models \psi(b, a_1, \ldots, a_n)$. Par hypothèse d'induction sur ψ, alors $A \models \psi(b, a_1, \ldots, a_n)$, et donc $A \models \phi(a_1, \ldots, a_n)$. □

Remarque: Soit $\mathcal{M}$ une L-structure. Soit $\phi(v_1, \ldots, v_n, w_1, \ldots w_k))$ une formule, et $a_1, \ldots, a_k$ des éléments dand $\mathcal{M}$. On note $\phi(\mathcal{M}) := \{(b_1, \ldots, b_n) \in |\mathcal{M}|^n : \mathcal{M} \models \phi(b_1, \ldots, b_n, a_1, \ldots a_k)$.
Soent $\mathcal{M} \subset_L \mathcal{N}$. Alors, par définition, $\mathcal{M}$ est une sous-structure élémentaire de $\mathcal{N}$ si et seulement si pour toute formule $\phi(v_1, \ldots, v_n, w_1, \ldots w_k))$ et toute suite $a_1, \ldots, a_k \in \mathcal{M}$,

$$\phi(\mathcal{M}) = \phi(\mathcal{N}) \cap |M|^n.$$

Le critère de Tarski-vaught nous dit que la condition suivante, apparement plus faible est en fait équivalente: tout sous-ensemble non vide de $|\mathcal{N}|$, définissable à paramètres dans $\mathcal{M}$, a un point dans $|\mathcal{M}|$.

7 Petit supplément "culturel", un exemple "classique" de théorie du premier ordre: la théorie des ensembles

La théorie axiomatique des ensembles dite de Zermelo Frankel est une théorie dans un langage égalitaire du premier ordre. Le langage est celui d'une relation binaire, Nous notons cette relation $\in$ et le langage $\mathcal{L}_\in = \{\in\}$. Nous considérons des $\mathcal{L}_\in$-structures, $\mathcal{U} =< U, \in >$, qu'on appelle **univers**.

Un *élément* de la $\mathcal{L}_\in$-structure $\mathcal{U}$ est appelé **un ensemble**.

La relation binaire $\in$ met donc en relation deux ensembles, nous l'écrirons $x \in y$, lu "l'ensemble x **appartient** à l'ensemble y" ou "l'ensemble x est **élément** de l'ensemble y".

Les axiomes habituels sont les suivants:

AX(1) L'axiome d'extensionnalité

$$\forall x\ \forall y\ (\forall z\ (z \in x \leftrightarrow z \in y)) \rightarrow (x = y)$$

Si $\mathcal{U} \models AX(1)$, alors deux ensembles dans $\mathcal{U}$ sont égaux si et seulement si ils ont les mêmes éléments.

AX(2) L'axiome de la paire

$$\forall x\ \forall y\ \exists z\ \forall u\ (u \in z \leftrightarrow (u = x \vee u = y)$$

C'est-à-dire, si $\mathcal{U} \models AX(1) \wedge AX(2)$, pour tous a, b ensembles de $\mathcal{U}$, il existe un (unique) ensemble c qui a comme seuls éléments les ensembles a et b. On l'appelle **la paire** $\{a, b\}$. Si $a = b$, on l'appelle **le singleton** $\{a\}$.

AX(3) L'axiome de la réunion

$$\forall x\ \exists y\ \forall z\ (z \in y\ \leftrightarrow\ \exists t(t \in x \wedge z \in t)$$

C'est-à-dire, si $\mathcal{U} \models AX(1) \wedge AX(3)$, pour tout ensemble a, il existe un (unique) ensemble, noté $\bigcup a$, ou $\bigcup_{x \in a} x$, appelé **réunion de** a, dont les éléments sont exactement les éléments des éléments de a.

AX(4) L'axiome de l'ensemble des parties

Si a, b sont des ensembles, on écrit $a \subset b$ pour la formule $\forall x\ (x \in a \rightarrow x \in b)$, lu "$a$ est un sous-ensemble de b".

$$\forall x\ \exists y\ \forall z\ (z \in y\ \leftrightarrow\ z \subset x)$$

C'est-à-dire, si a est un ensemble, il existe un ensemble, noté $\mathcal{P}(a)$ dont les éléments sont exactement les sous-ensembles de a.

SC Schéma de compréhension

Pour chaque formule $\phi(x, w_1, \ldots, w_k)$ de $\mathcal{L}_\in$, on a l'énoncé suivant:

$$\forall w_1, \ldots \forall w_k \forall t \exists y \forall x \ (x \in y \leftrightarrow (x \in t \wedge \phi(x, w_1, \ldots, w_k)).$$

C'est-à-dire, si $a_1, \ldots, a_n$ sont des ensembles, si t est un ensemble, alors la collection des ensembles x de $\mathcal{U}$, qui sont éléments de t et qui sont tels que $\mathcal{U} \models \phi(x, a_1, \ldots, a_n)$ forme un ensemble c, qu'on note $c = \{x \in t \,;\, \mathcal{U} \models \phi(x, a_1, \ldots, a_n)\}$.

On ne peut pas supprimer l'ensemble t (paradoxe de Russel): la collection S des ensembles x dans $\mathcal{U}$ tels que $\mathcal{U} \models x \notin x$ ne forme pas un ensemble. Sinon, soit c cet ensemble alors $\mathcal{U} \models c \notin c$ si et seulement si $\mathcal{U} \models c \in c$, ce qui est impossible.

Cela entraine que l'univers $\mathcal{U}$ lui-même ne forme pas un ensemble, c'est-à-dire, il n'existe pas d'ensemble c dans $\mathcal{U}$ telque $\forall x \ x \in c$: sinon, on pourrait, par le schéma de compréhension appliqué à cet ensemble c, déduire que la collection S au-dessus est un ensemble.

SR Schéma de remplacement ou de substitution

Pour chaque formule $\phi(x, y, w_1, \ldots, w_k)$ de $\mathcal{L}_\in$, on a l'énoncé:

$$\forall w_1, \ldots w_k \ (\forall x \forall y \forall z (\phi(x, y, w_1, \ldots, w_k) \wedge \phi(x, z, w_1, \ldots, w_k) \rightarrow y = z)$$

$$\rightarrow (\forall t \ \exists u \forall y \ (y \in u \leftrightarrow \exists x (x \in t \wedge \phi(x, y, w_1, \ldots, w_k)))).$$

C'est-à-dire, si $a_1, \ldots, a_k$ sont des ensembles, si la formule $\phi(x, y, a_1, \ldots, a_k)$ définit une relation fonctionelle (pour chaque x, il existe au plus un y tel que $\phi(x, y, a_1, \ldots, a_k)$), alors, si b est un ensemble, la collection des ensembles y qui sont image d'un élément x de b forme un ensemble.

Lemme 22 *Le schéma de remplacement implique le schéma de compréhension.*

Preuve: Soit $\phi(x, w_1, \ldots, w_k)$ une formule de $\mathcal{L}_\in$. On applique le schéma de remplacement à la formule $\psi(x, y, w_1, \ldots, w_k) = \phi(x, w_1, \ldots, w_k) \wedge x = y$, qui est bien fonctionelle.

On appelle $\mathbf{ZF}^-$ la théorie formée des Axiomes 1 à 4 et du Schéma de Remplacement.

Si $\mathcal{U}$ est un modèle de ZF^-, alors il existe un (unique) ensemble qui n'a auncun élément, qu'on note $\emptyset$: soit a un ensemble quelconque dans $\mathcal{U}$, alors

$$\emptyset = \{x \in a \ ; \ x \neq x\}.$$

Enfin, **la théorie ZF** est formée de ZF^- et du dernier axiome, **l'axiome de l'infini, AI** :

$$\exists x \ (\emptyset \in x \wedge \forall y \ (y \in x \rightarrow y \cup \{y\} \in x)).$$

Certains auteurs incluent dans ZF, un axiome supplémentaire, **l'axiome de fondation, AF**.

$$\forall x \ (x \neq \emptyset \ \rightarrow \ \exists y(y \in x \ \wedge y \cap x = \emptyset)).$$

En travaillant un peu plus, on voit que l'axiome du choix , AC, est également un énoncé du premier ordre du langage.

Le fait que l'axiome du choix soit "indépendant de ZF" signifie que $ZF \nvdash AC$ et que $ZF \nvdash \neg AC$, autrement dit qu'il y a un modèle de ZF qui vérifie l'axiome du choix et un autre modèle de ZF qui ne vérifie pas l'axiome du choix. De même, l'hypothèse du continu, HC, s'exprime par un énoncé du premier ordre, $ZFC\,(= ZF + AC) \nvdash HC$ et $ZFC \nvdash \neg HC$. (On suppose pour tout ceci qu'il y a un modèle de ZF)

References

[Ax] J. Ax, *Injective endomorphisms of varieties and schemes*, Ann. Math. **88**(2), 1969, 239-271.

[Be] I. Bertuccioni, *Algebraic actions of p-groups*, Arch. Math. **58**, 1992, 329.

[BB-R] A. Bialyncki-Barula and M. Rosenlicht, *Injective morphisms of real algebraic varieties*, Proc. Amer. Math. Soc. **13**, 1962, 1-7.

[Bor] A. Borel, *Injective endomorphisms of algebraic varieties*, Arch. Math. (Basel) **20**, 1969, 531-537.

[La] S. Lang, **Algebra**, Addison-Wesley.

[Rud] W. Rudin, *Injective polynomial maps are automorphisms*, Am. Math. Mon. **102**, 1995, 540-543.