THÉORIE DES MODÈLES ET CORPS PSEUDO FINIS

MERCEDES HAIECH

Table des matières

Introduction

Le présent document a été rédigé dans le cadre d'un stage de M1, à l'université Pierre et Marie Curie, sous la direction de François Loeser, que je tenais à remercier pour son encadrement.

Parfois, pour faciliter l'étude des ensembles qu'il manipule, le mathématicien a besoin de les munir de fonctions et de relations. Bien que naturelle, l'égalité sur un ensemble E n'en demeure pas moins une relation que l'on représente comme la diagonale de E^2. De même, la loi de composition interne dont on munit un groupe G est une fonction de G^2 dans G. Plus généralement, munir un ensemble de relations et de fonctions c'est le munir d'une structure. La logique, et en particulier ici, la théorie des modèles va nous donner un cadre pour penser ces structures de manière uniforme. On s'appuiera, pour ce faire, sur des connaissances intuitives que nous avons, qu'il s'agisse de la notion d'ensembles ou de fonctions. Le propos n'est pas de définir

tous les objets de base des mathématiques, mais d'utiliser ces connaissances afin de formaliser des notions comme les formules, les démonstrations et les structures.

Pour parvenir à cet objectif, on va se fixer un langage, qu'il faut penser comme des briques de base servant à construire des formules mathématiques telles que nous les connaissons. Nous savons que $\exists x\ x^2 + x + 1 = 0$ est une formule formée d'un quantificateur ($\exists$), d'une variable, de constantes, et d'une fonction (l'addition). Tous ces éléments (variables, constantes, fonctions, etc) vont être des éléments de notre langage. Une formule ne sera qu'un mot du langage, construite en suivant quelques règles de syntaxe. Une comparaison, peut-être judicieuse, serait d'imaginer que le langage est un ensemble de mots d'une langue, et qu'une formule est une phrase construite en respectant les règles de grammaires propre à la langue. Nous pourrons alors nous intéresser à des formules particulières que l'on appellera énoncés ; ils seront construits de sorte que toutes les variables qui interviennent soient liées à un quantificateur. Des énoncés classiques sont des formules comme $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$, qui exprime l'associativité dans un ensemble muni d'une loi de composition interne. Une collection d'énoncés formera une théorie, comme par exemple la théorie des groupes où les énoncés sont ceux exprimant l'associativité, l'existence de l'élément neutre et des inverses. Des questions de théorie des modèles seront de savoir si une théorie admet des modèles, c'est-à-dire des structures dans lesquels tous les énoncés de la théorie sont valides. En ce sens, les groupes seront des modèles de la théorie des groupes. Étant donné un ensemble, une formule y est soit vraie, soit fausse (dans un sens à préciser en définissant l'interprétation d'une formule dans une structure), mais cela ne garantit en rien l'existence d'une démonstration qui permet, en partant des énoncés de la théorie et de quelques règles logiques, de savoir si la formule est une conséquence logique de la théorie. Le théorème de complétude de Gödel permet de tisser un lien entre l'existence de modèles qui vérifient une formule et l'existence d'une démonstration formelle.

Certaines théories possèdent des propriétés intéressantes que nous allons un peu développer. Après avoir défini le formalisme nécessaire, le présent document montrera que les corps algébriquement clos admettent l'élimination des quantificateurs. Ce type de propriété permet d'obtenir des théorèmes sur les corps algébriquement clos. On peut l'utiliser pour démontrer le Nullstellensatz de Hilbert ou encore le théorème d'Ax suivant :

Théorème (Ax)**.** *Soit $f\colon \mathbf{C}^n \to \mathbf{C}^n$ une application polynomiale. C'est-à-dire de la forme $f = (f_1, \cdots, f_n)$ avec $f_i \in \mathbf{C}[X_1, \cdots, X_n]$. Si l'application f est injective, alors f est surjective.*

Lorsque l'on disposera d'une famille de modèles d'une théorie, nous verrons une méthode pour construire un nouveau modèle, fondée sur la notion d'ultraproduits. Ce sera l'objet du théorème de Łos, qui montrera que notre construction nous donne bien un modèle. Cette construction permettra de

mettre en évidence que la propriété d'être fini, pour les corps finis, ne peut pas s'exprimer comme un énoncé du langage des anneaux.

1. Structures et théorie

1.1. **Langage et formules.**

1.1.1. *Langage.* Dans ce paragraphe, nous allons formaliser la notion de langage. L'idée étant de se donner des briques de base pour former des mots, ou plus exactement des formules qui ressemblent aux formules rencontrées habituellement en mathématique, comme par exemple $\exists x\ (x^2 + 1 = 0)$.

Définition 1.1.1. Un *langage* est composé des données suivantes :

(1) d'un ensemble infini dénombrable $\mathcal{V} = \{v_i\}_{i\in\mathbf{N}}$ de variables ;

(2) des symboles logiques $\neg$ (négation), $\wedge$ (conjonction), $\vee$ (disjonction), $\Rightarrow$ (implication), $\Leftrightarrow$ (équivalence), $\forall$ (pour tout) et $\exists$ (il existe) ;

(3) pour chaque entier naturel n, un ensemble $\mathcal{F}_n$, dont les éléments sont appelés *symboles de fonctions n-aires* ;

(4) pour chaque entier naturel n, un ensemble $\mathcal{R}_n$, dont les éléments sont appelés *symboles de relations n-aires.*

Un symbole de fonction 0-aire sera appelé une constante. L'on suppose aussi que $\mathcal{R}_0$ contient un élément $\top$ qui sera interprété comme l'énoncé toujours vrai. Un *mot* d'un langage L est une suite finie d'éléments de L. Par exemple, si v_1 et v_2 sont des variables, alors $v_1 \vee v_2$ est un mot, de même que $\vee \vee v_1 \neg$. On remarquera que l'égalité n'est pas nécessairement comprise dans le langage. Elle peut cependant y apparaitre comme symbole de relation 2-aire (on dit aussi d'*arité* 2 ou *binaire*). Par ailleurs, la donnée d'un langage sera souvent notée $L = \{\mathcal{R}, \mathcal{F}\}$, où $\mathcal{R}$ désigne l'ensemble des symboles de relations et $\mathcal{F}$ celui des symboles de fonction. Les variables seront toujours sous-entendues, de même que le symbole $\top$ et l'égalité lorsque cela ne prêtera pas à confusion.

Des exemples classiques de langages qui nous accompagnerons tout le long de ce document sont :

† le langage des anneaux $L_r = \{=, +, -, \cdot, 0, 1\}$. Dans cet exemple $=$ est une relation binaire, les symboles de fonction $+, -, \cdot$ sont d'arité 2, et $0, 1$ sont des constantes (soit encore des symboles de fonction 0-aire). [1]

† Le langage des anneaux ordonnés $L_{r,ord} = L_r \cup \{<\}$, où $<$ est un symbole de relation binaire (ou 2-aire).

† le langage des ensembles $L = \varnothing$. Dans ce cas, il n'y a ni symbole de fonction, ni symbole de relation.

† Le langage des ensembles ordonnés $L_{ord} = \{=, <\}$.

1. Il est à noter que le symbole de fonction $-$ est inutile pour définir le langage des anneaux.

1.1.2. *Termes.* La notion de mot n'est cependant pas très pertinente pour travailler. Une grande majorité des mots ne ressemble pas aux formules que nous avons l'habitude de rencontrer. Pour pallier cela, nous allons introduire la notion de *terme*, qui se construit par induction.

On se fixe un langage L. L'ensemble $\mathcal{T}_0(L)$, que l'on appelle termes de *hauteur* 0, est l'ensemble des variables et des symboles de constantes (ou fonction 0-aires). L'ensemble $\mathcal{T}_{k+1}(L)$ est l'union de $\mathcal{T}_k(L)$ et des $ft_1 \cdots t_n$, où f est un symbole de fonction n-aire, et $t_1, \cdots, t_n$ sont des éléments de $\mathcal{T}_k(L)$. Finalement l'ensemble des termes du langage L, est l'ensemble $\mathcal{T}(L) = \cup_{k\in\mathbf{N}}\mathcal{T}_k(L)$. On appellera *hauteur* d'un terme t, qu'on notera $\mathrm{h}[t]$, le plus petit entier naturel k tel que $t \in \mathcal{T}_k(L)$.

Si v_1 est une variable dans le langage des anneaux L_r, alors $\mathrm{h}[v_1] = 0$, mais $\mathrm{h}[(v_1 + v_1) + v_1] = 2$. De même $\mathrm{h}[(v_1 + v_1) + (v_1 + v_1)] = 2$.

Une application des définitions nous donne la proposition suivante, dite *de lecture unique*.

Proposition 1.1.2 (Propriété de lecture unique)**.** *Étant donné un langage L, un terme t de $\mathcal{T}(L)$ vérifie l'une des trois propriétés suivantes :*

(1) Le terme t est une variable de L ;

(2) Le terme t est un symbole de constante ;

(3) Il existe un entier n strictement positif, un symbole de fonction n-aire f et des termes $t_1, \cdots, t_n$ tels que $t = ft_1 \cdots t_n$.

Désormais, nous utiliserons la notation $f(t_1, \cdots, t_n)$ pour signifier $ft_1 \cdots t_n$ afin de nous rapprocher des notations usitées habituellement. Par ailleurs, dans le langage des anneaux, corps, etc, nous commettrons l'abus de langage en écrivant $v_1 + v_1$ à la place de $+(v_1, v_1)$ comme l'auraient voulu les définitions.

Notation. Lorsqu'un terme t d'un langage L est composé de variables, nous noterons $t(v_{i_1}, \cdots, v_{i_n})$ lorsque les variables v_{i_j} ont au moins une occurrence dans t.

1.1.3. *Formules.* Nous nous approchons maintenant des formules mathématiques telles que nous en rencontrons régulièrement. Pour définir cette notion, nous allons une fois encore procéder par induction. Si $n > 0$ est un entier naturel, et R un symbole de relation n-aire, l'on dira que $Rt_1 \cdots t_n$, où les t_i sont des termes, est une *formule atomique*. Les formules atomiques sont dites de hauteur 0. Si F est une formule de hauteur m alors les mots $\neg F$, $\exists v F$ et $\forall v F$ sont des formules de hauteur $m + 1$. Si G est une autre formule de hauteur m' alors les mots $(F \wedge G)$, $(F \vee G)$,$(F \Rightarrow G)$,$(F \Leftrightarrow G)$ sont des formules de hauteur $\sup(m, m') + 1$.

Définition 1.1.3 (Forme prénexe)**.** On dira qu'une formule $\varphi(\bar{x})$ est sous forme *prénexe* si c'est une formule de la forme $Q_1x_1Q_2x_2 \cdots Q_nx_n\varphi'(\bar{x})$ où $Q_i \in \{\forall, \exists\}$, et où $\varphi'(\bar{x})$ est une formule sans quantificateurs [2].

2. On peut toujours mettre une formule sous cette forme.

Notation. On écrira assez rapidement $R(t_1, \cdots, t_n)$ pour signifier $Rt_1 \cdots t_n$, et on se permettra à nouveau des abus de notation courant comme par exemple $x < y$ à la place de $<(x, y)$.

Une fois encore, il découle des définitions une propriété de lecture unique.

Proposition 1.1.4 (Propriété de lecture unique)**.** *Étant donné un langage L, une formule F énoncée dans le langage L vérifie l'une des cinq propriétés suivantes :*

(1) La formule F est atomique ;

(2) Il existe une unique formule G telle que la formule F soit de la forme $\neg G$;

(3) Il existe deux formules G et H, définies de manière unique, telles que F soit de la forme $G\alpha H$, où $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$;

(4) Il existe une unique variable v_i et une unique formule G telles que F soit de la forme $\exists v_i G$;

(5) Il existe une unique variable v_i et une unique formule G telles que F soit de la forme $\forall v_i G$.

Si l'on se place dans le langage des ensembles ordonnés $L_{ord} = \{=, <\}$, alors les mots suivants sont des formules :

† $\forall x\, \neg(x < x)$;

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

† $\forall x \forall y \forall z\, \neg((x < y \wedge y < z) \wedge (z = x \vee z < x))$.

Ces trois formules décriront une fois interprétées les ordres totaux stricts. Cet exemple est cependant particulier car toutes les variables qui apparaissent sont liées à un quanteur, c'est-à-dire est après un symbole $\forall$ ou $\exists$. Cependant des mots de la forme $x < y$ ou $\forall x(y = x)$ sont aussi des formules.

1.1.4. *Variables libres, liées.* L'on en arrive à la notion de variables libres et liées. En effet, dans les exemples précédents, nous avons remarqué que certaines variables pouvaient être précédées d'un quanteur. Lorsque c'est le cas, on dira que la variable n'est pas libre. Soyons plus précis : si F est une formule atomique toutes les occurrences d'une variable v_i dans F sont dites *libres*. Si F est de la forme $\neg G$, alors les occurrences libres de v_i dans F sont exactement les occurrences libres de v_i dans G. Les occurrences libres de v_i dans $(F\alpha G)$, où $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$ sont celle dans F et celles dans G. Les occurrences libres de v_i dans $F = \exists v_j G$ ou $\forall v_j G$ sont celle de v_i dans G si $i \neq j$. Au contraire si $i = j$ aucune des occurrences de v_i dans F n'est libre. Une variable qui n'a aucune occurrence libre est dite *liée*. Les variables libres dans F sont celles qui admettent au moins une occurrence libre.

Notation. Si F est une formule on notera $F[v_{i_1}, \cdots, v_{i_n}]$ si les variables libres de F sont parmi les v_{i_j}, mais qu'aucun v_{i_j} ne soit une variable liée de F. [3]

3. Cependant il n'est pas demandé que seules les variables libres apparaissent dans la notation. La formule $(u \Rightarrow (u \vee v))$ peut-être notée $F[u, v]$ ou $F[x, u, y, v]$.

Dans la formule $\forall x \forall y\ ((x < y) \vee y < x) \vee x = y)$ les variables x et y sont liées, alors que dans la formule $x < y$ les deux variables sont libres. On peut, bien entendu, avoir des formules en plusieurs variables dont certaines sont liées et d'autres non comme dans l'exemple $\forall x\ (y = x)$ où x est liée mais pas y. Un dernier exemple en considérant le langage $L = \{=, f\}$ avec f une relation unaire. Dans la formule $(f(x) = y \wedge \forall y\ (y = x \vee f(y) \neq f(x))$, la variable y est libre car elle admet au moins une occurrence libre. On aurait tout aussi bien pu écrire la formule de la manière suivante avec une variable supplémentaire $(f(x) = z \wedge \forall y\ (y = x \vee f(y) \neq f(x))$, auquel cas les variables x et z sont libres tandis que la variable y est liée.

Définition 1.1.5 (Énoncé, théorie)**.** Une formule exprimée dans un langage L ne possédant aucune variable libre est appelée un *énoncé*. Un ensemble d'énoncés est appelé une *théorie*.

1.1.5. *Exemple, théorie des groupes.* On se donne le langage des groupes $L = \{=, \cdot, ^{-1}, e\}$, où $\cdot$ est une relation binaire, $^{-1}$ une relation unaire, et e un symbole de constante. La théorie des groupes est constituée des énoncés suivants :

† $\forall x \forall y \forall z\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$;
† $\forall x\ (x \cdot e = e \cdot x)$;
† $\forall x\ (x \cdot x^{-1} = e)$.

Remarquons que l'on aurait pu appauvrir le langage en oubliant la fonction unaire $^{-1}$ et en remplaçant le troisième énoncé par $\forall x \exists y\ (x \cdot y = e)$.

1.1.6. *Substitutions.* On se donne une formule $F[u_1, \cdots, u_n]$ exprimé dans un langage L, où les variables u_i sont libres. Si $t_1, \cdots, t_n$ sont des termes, alors on peut remplacer chaque occurrence libre de u_i par t_i. On l'appellera opération de substitution que l'on notera $F_{t_1/u_1, \cdots, t_n/u_n}$.

On se place par exemple dans le langage des anneaux $L_r = \{=, +, -, \cdot, 0, 1\}$. Considérons la formule $\psi(y) = (y^3 + y - 1 = 0 \wedge \forall y\ (y + 1 \neq y))$ et le terme $x + 1$, alors comme la variable y est libre dans la formule $\psi(y)$ on peut substituer y par $x + 1$ pour aboutir à la formule

$$\psi_{x+1/y} = ((x + 1)^3 + (x + 1) - 1 = 0 \wedge \forall y\ (y + 1 \neq y))$$

1.2. **Structures et modèles.**

1.2.1. *Structures.* Maintenant que nous avons un langage qui nous permet d'écrire des formules qui semblent familière, il faut se donner un moyen de les interpréter. Nous allons pouvoir donner un sens à ces formules dans des ensembles munis de fonctions et de relations, que nous appellerons structures.

Définition 1.2.1. Une *L-structure* $\mathfrak{M}$ est l'ensemble des données suivantes :

(1) Un ensemble non vide M, appelé ensemble sous-jacent à la structure $\mathfrak{M}$;
(2) Pour chaque entier naturel $n \geqslant 0$ et tout symbole de fonction n-aire f, une fonction $f^{\mathfrak{M}} : M^n \to M$;

(3) Pour chaque entier naturel $n \geqslant 0$ et tout symbole de relation n-aire R, un sous-ensemble $R^{\mathfrak{M}}$ de M^n.

On remarque que si l'on se fixe l'entier $n = 0$ on associe à tout symbole de fonction 0-aire c une fonction $c^{\mathfrak{M}} : M^0 \to M$ qui n'est rien d'autre qu'un élément de M. On demande de plus que $\top^{\mathfrak{M}} = M^0$. On appellera $f^{\mathfrak{M}}$ et $R^{\mathfrak{M}}$ les *interprétations* des symboles f et R dans la structure. Une structure sera parfois noté $\mathfrak{M} = \{M, R^{\mathfrak{M}}, f^{\mathfrak{M}} \mid R \in \mathcal{R}, f \in \mathcal{F}\}$.

Les exemples suivants sont des L_r-structures, où L_r désigne le langage des anneaux :

† Une structure dont l'ensemble sous-jacent est l'anneau des entiers relatifs est $\mathfrak{M} = (\mathbf{Z}, =, +, -, \cdot, 0, 1)$. Les symboles de fonctions $+, -, \cdot$ sont les fonctions d'addition, de soustraction, et de multiplication usuels de $\mathbf{Z}$. Les constantes 0 et 1 sont interprétées comme le 0 et le 1 de $\mathbf{Z}$. Enfin, à l'égalité est associé la diagonale de $\mathbf{Z}^2$, c'est à dire l'ensemble des $\{(x, x) \mid x \in \mathbf{Z}\}$.

† Tout corps K est aussi l'ensemble sous-jacent d'une L_r-structure lorsqu'on considère $\mathfrak{M} = \{K, =, +, -, \cdot, 0, 1\}$.

1.2.2. *Interprétation de termes et de formules dans une structure.* Les termes et les formules vont prendre du sens une fois interprétés dans une structure. Si un terme t est une constante c alors son interprétation dans $\mathfrak{M}$ est $c^{\mathfrak{M}}$. Si un terme t est de la forme $t[v_i] = v_i$, avec v_i une variable, alors, si on se fixe un élément a de M, le terme $t[a] = a$ est interprété comme l'élément a. Si $t[u_1, \cdots, u_n]$ est un terme avec u_i des variables, et si $\bar{a} = (a_1, \cdots, a_n)$ est un élément de M^n, alors on note $t[a_1, \cdots, a_n]$ l'interprétation de t en remplaçant les u_i par a_i. En prenant $t[u_1, \cdots, u_n] = f(t_1, \cdots, t_r)$ un symbole de fonction r-aire, où chaque t_i est un terme, alors $t[\bar{a}] = f^{\mathfrak{M}}(t_1[a_1, \cdots, a_n], \cdots, t_r[a_1, \cdots, a_n])$.

Considérons une formule $F[w_1, \cdots, w_n]$ où les w_i sont des variables. Si $\bar{a} = (a_1, \cdots, a_n)$ est un élément de M^n, on dit que $\bar{a}$ satisfait F et on note $\mathfrak{M} \vDash F[a_1, \cdots, a_n]$ si la formule obtenue en interprétant les w_i par les a_i est satisfaite dans F :

(1) Si $F = R(t_1, \cdots, t_r)$ est une formule atomique, alors $\mathfrak{M} \vDash F[a_1, \cdots, a_n]$ si et seulement si $(t_1[a_1, \cdots, a_n], \cdots, t_r[a_1, \cdots, a_n]) \in R^{\mathfrak{M}}$;

(2) $\mathfrak{M} \nvDash F[a_1, \cdots, a_n]$ si et seulement si $\mathfrak{M} \vDash \neg F[a_1, \cdots, a_n]$;

(3) Si $\alpha \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$, alors $\mathfrak{M} \vDash F \alpha G[a_1, \cdots, a_n]$ si et seulement si $(\mathfrak{M} \vDash F[a_1, \cdots, a_n]$ α $\mathfrak{M} \vDash G[a_1, \cdots, a_n])$;

(4) Si $F = (\forall v G)[w_1, \cdots, w_n]$ et si la variable v est différente des w_i, alors $G = G[v, w_1, \cdots, w_n]$ et $\mathfrak{M} \vDash (\forall v G)[a_1, \cdots, a_n]$ si pour tout a dans M on a $\mathfrak{M} \vDash G[a, a_1, \cdots, a_n]$; idem pour $\exists$;

(5) Si $F = (\forall w_i G)[w_1, \cdots, w_n]$ alors $\mathfrak{M} \vDash (\forall w_i G)[a_1, \cdots, a_n]$ si pour tout a dans M on a $\mathfrak{M} \vDash G[a_1, \cdots, a_{i-1}, a, a_{i+1}, \cdots, a_n]$; idem pour $\exists$.

On notera parfois $M \models F[a_1, \cdots, a_n]$ à la place de $\mathfrak{M} \models F[a_1, \cdots, a_n]$. Si $F[v_1, \cdots, v_n]$ est une formule, on notera $\mathfrak{M} \models F[v_1, \cdots, v_n]$ si et seulement si pour tout $(a_1, \cdots, a_n)$ de M^n on a $\mathfrak{M} \models F[a_1, \cdots, a_n]$.

Dans le langage des ensembles ordonnés $L_{ord} = \{=, <\}$, on peut considérer la structure $\{\mathbf{N}, =, <\}$ qui est l'ensemble des entiers naturels uniquement vu comme ensemble ordonné avec l'ordre usuel. Si $F[x]$ désigne la formule $\forall y(x < y \vee x = y)$, alors $N \models F[0]$. La formule indiquant que x est le plus petit élément de l'ensemble $\mathbf{N}$. Par contre, si l'on avait considéré la structure $\{\mathbf{Z}, =, <\}$, il n'y aurait pas eu d'élément a de $\mathbf{Z}$ tel que $\mathbf{Z} \models F[a]$.

1.2.3. *Remarques sur l'égalité.* Lorsque le langage L contient le symbole de relation binaire $=$, on appellera *structure égalitaire* toute structure $\mathfrak{M}$ dans laquelle la relation $=^{\mathfrak{M}}$ est interprétée comme la vraie égalité dans M. Ainsi $=^{\mathfrak{M}}$ sera le sous-ensemble $\{(x, x) \in M^2\} \subset M^2$. *Dans tout ce document, toutes nos structures seront supposées égalitaires.*

Par ailleurs, lorsque $\mathfrak{M}$ est le modèle d'une théorie T exprimée dans un langage L contenant le symbole $=$, on pourra aussi définir l'égalité en supposant que les énoncés suivants font partie de la théorie T :

(1) $\forall v \ (v = v)$;
(2) $\forall v_0 \forall v_1 \ (v_0 = v_1 \Rightarrow v_1 = v_0)$;
(3) $\forall v_0 \forall v_1 \forall v_2 \ ((v_0 = v_1 \wedge v_1 = v_2) \Rightarrow v_0 = v_2)$;
(4) pour chaque symbole de fonction n-aire f, si pour tout entier i on a $v_i = v_{n+i}$, alors $f(v_1, \cdots, v_n) = f(v_{n+1}, \cdots, v_{2n})$;
(5) pour chaque symbole de relation n-aire R, si pour tout entier i on a $v_i = v_{n+i}$, alors $R(v_1, \cdots, v_n) \Leftrightarrow R(v_{n+1}, \cdots, v_{2n})$.

1.2.4. *Modèles.* On rappelle qu'une théorie est un ensemble d'énoncés (une formule sans variables libres). Si T est une théorie exprimée dans un langage L et si $\mathfrak{M}$ est une L-structure, on dit que $\mathfrak{M}$ est un *modèle* de la théorie T si tout énoncé de T est satisfait dans $\mathfrak{M}$. Si une théorie T admet au moins un modèle, on dit qu'elle est *consistante*.

La théorie des groupes développée dans le paragraphe 1.1.5 admet des modèles que l'on appelle usuellement des groupes. Comme il existe des groupes, cette théorie est consistante.

On dit qu'une théorie T exprimée dans un langage L est *complète* si pour toute formule φ de F soit φ soit $\neg\varphi$ est vérifiée dans tout modèle de T.

Notation. Si $\mathfrak{M}$ est une L-structure, on note $\mathrm{Th}(\mathfrak{M})$ l'ensemble des énoncés vrais dans $\mathfrak{M}$. Il est clair que la structure $\mathfrak{M}$ est un modèle de la théorie $\mathrm{Th}(\mathfrak{M})$.

De plus, pour $\mathfrak{M}$ une L-structure et A un sous-ensemble de $\mathfrak{M}$, on peut considérer l'expansion $\mathfrak{M}_A$ de $\mathfrak{M}$ par des constantes dans A, c'est-à-dire la L_A-structure $\{M, L, a : a \in A\}$ où $L_A = L \cup \{a : a \in A\}$. Ce qui signifie qu'on rajoute à $\mathfrak{M}_A$ des constantes correspondants aux éléments de A. On note $\mathrm{Th}(\mathfrak{M}, A)$ la théorie de $\mathfrak{M}_A$ qui correspond donc à l'ensemble des énoncés à paramètres dans A qui sont vrais dans $\mathfrak{M}$.

1.3. **Démonstrations formelles.** Le but de ce paragraphe est de donner un sens à "la formule F est démontrable à partir de la théorie T". Pour ce faire, il y aura des règles formelles qui permettront, en un sens à préciser, de passer d'une formule à l'autre, mais aussi un ensemble d'axiomes logiques qui contient en particulier les tautologies. Intuitivement, une tautologie est un énoncé qui est "toujours vrai", comme $F \vee \neg F$. Une autre manière de le dire est "peu importe la valeur de vérité que prend F, la formule est toujours vraie". Nous allons cependant nous attarder un peu sur ces notions de valeurs de vérité.

1.3.1. *Tables de vérité, tautologies.* Dans toute la suite, la notion de vrai ou faux sera exprimée grâce aux chiffres 0 et 1. La valeur 1 signifiera que l'énoncé est vrai tandis que la valeur 0 impliquera que l'énoncé est faux. [4] On appellera ce nombre la *valeur de vérité* de la formule. Si l'on se donne des formules F et G exprimées dans un langage L, on voudra déterminer quelle valeur de vérité donner aux formules $\neg F$ ou $F \alpha G$ avec $\alpha \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$. Il est entendu que la réponse dépendra de la valeur de vérité de F, et il est attendu que la réponse coïncide avec l'intuition. Dans le cas où notre formule F serait vraie, l'on s'attend à ce que la formule $\neg F$ (**non** F) prenne la valeur faux, et réciproquement. Pour une formule du type $F \vee G$ (respectivement $F \wedge G$), on demandera qu'elle soit vraie si une des deux formules F **ou** G soit vraie (respectivement si F **et** G) sont vraies.

On peut résumer nos attentes par les tableaux suivants que l'on appellera *tables de vérité* :

F	$\neg F$
0	1
1	0

F	G	$F \vee G$
0	0	0
0	1	1
1	0	1
1	1	1

F	G	$F \wedge G$
0	0	0
0	1	0
1	0	0
1	1	1

Une constatation rassurante est que la formule $\neg\neg F$ et F possèdent la même table de vérité.

Il nous faut maintenant régler le cas des formules $F \Rightarrow G$ et $F \Leftrightarrow G$. Comme le veut l'usage en mathématique, nous imposerons que $F \Leftrightarrow G$ et $F \Rightarrow G \vee G \Rightarrow F$ aient la même table de vérité, de même que $F \Rightarrow G$ et $\neg F \vee G$. Ce deuxième cas est un peu moins intuitif qu'il en a l'air. En effet, si tout un chacun acquiescera que $F \Rightarrow G$ permet d'affirmer si F est vraie alors G est vraie, qu'en est-il des cas où F est fausse ? Ou plutôt, quelle valeur de vérité donner à la formule $F \Rightarrow G$ lorsque F est fausse et G est vraie ? Pour donner un exemple, la formule "2 est divisible par 4 implique 2 pair" est-elle vraie ou fausse ? A priori, on peut se sentir gêné pour répondre intuitivement puisque la première partie de la formule est fausse. Par contre, il nous aurait été beaucoup plus simple de répondre oui si l'on avait demandé si la formule "n est divisible par 4 implique n pair" est vraie. Peut-être que

4. Ce choix est arbitraire, on aurait très bien pu choisir la convention inverse.

de telles remarques peuvent justifier intuitivement pourquoi "faux implique vrai" est considéré comme vrai.

Une dernière remarque à propos de l'implication. Elle ne correspond pas nécessairement au verbe "impliquer" auquel on peut s'attendre. Pour étayer ce propos, disons que le théorème de Pythagore et le théorème de Thalès sont deux formules vraies, ainsi d'après les définitions précédentes la formule "le théorème de Pythagore implique le théorème de Thalès" est vraie sans pour autant que le théorème de Pythagore soit utilisé effectivement pour démontrer le théorème de Thalès.

Résumons à nouveau nos remarques sur l'implication et l'équivalence à travers deux tableaux.

F	G	$F \Rightarrow G$
0	0	1
0	1	1
1	0	0
1	1	1

F	G	$F \Leftrightarrow G$
0	0	1
0	1	0
1	0	0
1	1	1

Donnons quelques exemples supplémentaires de formules et de tables de vérité.

F	G	H	$F \Rightarrow G \vee H \Rightarrow G$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

F	G	$F \Rightarrow (G \Rightarrow F)$
0	0	1
0	1	1
1	0	1
1	1	1

La deuxième table de vérité de cet exemple est particulièrement intéressante, car la formule $F \Rightarrow (G \Rightarrow F)$ prend toujours la valeur 1, peut importe les valeurs de vérité de F et G.

Définition 1.3.1. On appellera *tautologie* une formule dont la valeur de vérité est toujours 1.

1.3.2. *Démonstrations formelles.* Les tautologies seront des briques permettant de construire des démonstrations. Voyons maintenant les méthodes permettant de transformer et combiner des formules pour démontrer un résultat. Règles formelles. Il y en a deux,

† Le *modus ponens* : à partir de formule F et de $F \Rightarrow G$ le modus ponens nous permet de déduire G ;

† La règle de généralisation : à partir de la formule F, on déduit $\forall v F$.

Axiomes logiques. Il sont de deux types :

† Les tautologies ;

† Les axiomes des quantificateurs :

(1) Si F est une formule : $(\exists v\ F) \Leftrightarrow (\neg \forall v\ \neg F)$;

(2) Pour des formules F et G et une variable v n'ayant pas d'occurrence libre dans F : $\forall v(F \Rightarrow G) \Rightarrow (F \Rightarrow \forall vG)$;

(3) Pour une formule F, une variable v et un terme t tel qu'aucune occurrence libre de v dans F n'apparait dans le champ d'un quantificateur liant une variable de t : $\forall vF \Rightarrow F_{t/v}$.

La restriction sur les occurrences libres de v dans (3) est nécessaire. En effet, prenons la formule $F = \exists v_1 R(v, v_1)$ et $t = v_1$, alors $F_{v_1/v} = (\exists v_1 R(v_1, v_1))$ tandis que $\forall vF = \forall v \exists v_1 R(v, v_1)$. Ainsi, l'implication $\forall vF \Rightarrow F_{v_1/v}$ n'est pas vraie en général.

Définition 1.3.2. Soit T une théorie et F une formule de L. On dit que F est *démontrable* à partir de la théorie T si et seulement s'il existe une suite finie $F_1, \cdots F_n$ de formules de L avec $F_n = F$ telles que pour tout entier $i \in \{1, \cdots, n\}$, soit $F_i \in T$, soit F_i est un axiome logique, soit F_i se déduit à partir d'une ou deux formules précédentes dans la suite par l'une des règles formelles.

On appelle aussi la suite des F_i une *démonstration formelle* de F. Lorsqu'une telle démonstration existe, on note $T \vdash F$ et on dit que F est une *conséquence syntaxique* de T. D'autre part, si pour tout modèle $\mathfrak{M}$ de la théorie T l'on a $\mathfrak{M} \vDash F$, alors on dit que F est une *conséquence sémantique* de T et l'on note $T \vDash F$.

Lemme 1.3.3. *Soit T une théorie et F une formule de $\mathcal{L}$. Si $T \vdash F$ alors $T \vDash F$.*

Démonstration. Procédons par récurrence sur la longueur de la démonstration formelle, à savoir l'entier n de la définition. L'énoncé de récurrence sera $P(n)$ = "pour toute démonstration formelle $(F_1, \cdots, F_n)$ et pour tout $i \in \{1, \cdots, n\}$, on a $\mathfrak{M} \vDash F_i$". Lorsque l'entier n vaut 1, alors $F = F_1$ ne peut pas se déduire de règles formelles impliquant les formules précédentes puisqu'il n'y en a pas. Ainsi, nécessairement F est un axiome logique. Or, les axiomes logiques sont vrais dans n'importe quel modèle $\mathfrak{M}$ d'une théorie T. Supposons que pour un entier n la propriété $P(n)$ est vérifié. On considère une démonstration formelle avec $n+1$ formules $(F_1, \cdots, F_n, F_{n+1})$ de F_{n+1}. Alors $(F_1, \cdots, F_n)$ est aussi une démonstration formelle, mais de F_n. L'hypothèse de récurrence nous assure que pour tout $i \in \{1, n\}$ l'on a $\mathfrak{M} \vDash F_i$. Il nous reste à montrer que $\mathfrak{M} \vDash F_{n+1}$. Soit F_{n+1} est un axiome logique auquel cas l'on a bien le résultat voulu. Soit F_{n+1} se déduit d'une autre formule, disons F_k, avec $k < n+1$ par généralisation, auquel cas si $\mathfrak{M} \vDash F_k$ alors $\mathfrak{M} \vDash \forall vF_k$. Soit F_{n+1} se déduit d'une autre formule, disons F_k avec $k < n+1$, par le modus ponens. Or si $\mathfrak{M} \vDash F_k$ et $\mathfrak{M} \vDash (F_k \Rightarrow F_{n+1})$, alors par définition $\mathfrak{M} \vDash F_{n+1}$. L'hypothèse de récurrence étant héréditaire, notre propriété $P(n)$ est vérifiée à chaque rang n. □

Il est aussi vrai que si F est conséquence sémantique de T alors il est conséquence syntaxique. Ceci résulte du théorème de complétude de Gödel,

et justifie a posteriori les règles pour définir la conséquence syntaxique. On pourra trouver une preuve de ce fait dans les notes de cours de François Loeser [7].

2. Sous-structure, morphismes, théories modèles complètes

À l'instar des ensembles, où nous sommes parfois amenés à considérer des sous-ensembles, nous allons nous intéresser à la notion de sous-structure, et aux morphismes entre structures qui conservent les interprétations de L.

2.1. **Morphismes entre structures.** Soit L un langage. On se donne $\mathfrak{M}$ et $\mathfrak{N}$ deux L-structures. Soit $F\colon M \to N$ une application entre les ensembles sous-jacent des L-structures.

On dit que F est un *morphisme de L-structures*, si pour tout n-uplet $\bar{a}$ de M, tout symbole de fonction n-aire f et tout symbole de relation n-aire R,

$$\mathfrak{M} \vDash R(\bar{a}) \Rightarrow \mathfrak{N} \vDash R(F(\bar{a})) \quad \text{et} \quad f^{\mathfrak{N}}(F(\bar{a})) = F(f^{\mathfrak{M}}(\bar{a})).$$

Définition 2.1.1 (Plongement)**.** Si F est un morphisme de L-structures injectif et vérifie de plus, que pour tout n-uplet $\bar{a}$ de M et tout symbole de relation n-aire R,

$$\mathfrak{M} \vDash R(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash R(F(\bar{a}))$$

où $F(\bar{a})$ désigne $(F(a_1), F(a_2), \cdots, F(a_n))$, alors on appelle F un *plongement*.

Supposons que F soit un morphisme vérifiant l'équivalence de la définition précédente. Alors, si x et y sont des éléments de M vérifiant $F(x) = F(y)$, on a $\mathfrak{N} \vDash (F(x) = F(y))$, et par l'équivalence, on a nécessairement $\mathfrak{M} \vDash (x = y)$. En d'autres termes, un tel morphisme est nécessairement injectif lorsque l'égalité est un symbole de relation du langage.

Lorsque $M \subset N$ et que l'inclusion ensembliste est un plongement de $\mathcal{L}$-structures, on dit que $\mathfrak{M}$ est une *sous-structure* de $\mathfrak{N}$.

Donnons quelques exemples :

- † Dans le langage des groupes, la structure $(\mathbf{Z}, =, +, 0)$ est une sous-structure de $(\mathbf{R}, =, +, 0)$. En effet, l'addition (symbole de fonction binaire), et 1 (symbole de fonction 0-aire) coïncident qu'elles soient vues dans $\mathbf{Z}$ ou dans $\mathbf{R}$. Il en va de même pour l'égalité (symbole de relation binaire). Il est par ailleurs intéressant de relever que $\mathbf{Z}$ est un sous-groupe de $\mathbf{R}$.
- † On considère le morphisme $\exp\colon \mathbf{Z} \to \mathbf{R}$. Il s'agit d'un plongement de la structure $(\mathbf{Z}, =, +, 0)$ dans $(\mathbf{R}, =, \cdot, 1)$.

Proposition 2.1.2. *Soit L un langage, et soit $\mathfrak{M}$ une sous-structure de $\mathfrak{N}$. Si $\bar{a}$ est un élément à coordonnées dans M et que $\varphi(\bar{x})$ est une L-formule sans quantificateurs, alors $\mathfrak{M} \vDash \varphi(\bar{a})$ si et seulement si $\mathfrak{N} \vDash \varphi(\bar{a})$.*

Démonstration. En procédant par récurrence, il est clair que si $\bar{b}$ est un élément à coordonnées dans M, et si $t(\bar{x})$ est un terme, alors $t^{\mathfrak{M}}(\bar{b}) = t^{\mathfrak{N}}(\bar{b})$. On va montrer la proposition par récurrence sur la hauteur des formules.

Si φ est une formule atomique $R(t_1, \cdots, t_n)$, comme pour tout entier $i \in \{1, \cdots, n\}$, on a $t_i^{\mathfrak{M}}(\bar{a}) = t_i^{\mathfrak{N}}(\bar{a})$, alors par définition des sous-structures

$$\mathfrak{M} \vDash R(t_1^{\mathfrak{M}}(\bar{a}), \cdots, t_n^{\mathfrak{M}}(\bar{a})) \Leftrightarrow \mathfrak{N} \vDash R(t_1^{\mathfrak{N}}(\bar{a}), \cdots, t_n^{\mathfrak{N}}(\bar{a})).$$

On suppose que la proposition est vraie pour $\psi(\bar{x})$ et que la formule $\varphi(\bar{x})$ est $\neg\psi(\bar{x})$, alors

$$\mathfrak{M} \vDash \neg\psi(\bar{a}) \Leftrightarrow \mathfrak{M} \nvDash \psi(\bar{a}) \Leftrightarrow \mathfrak{N} \nvDash \psi(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash \neg\psi(\bar{a}).$$

Enfin si la proposition est vraie pour ψ_0 et ψ_1 et que φ est la formule $\psi_0 \wedge \psi_1$, alors $\mathfrak{M} \vDash \varphi(\bar{a})$ si et seulement si $\mathfrak{M} \vDash \psi_0(\bar{a})$ et $\mathfrak{M} \vDash \psi_1(\bar{a})$ si et seulement si $\mathfrak{N} \vDash \psi_0(\bar{a})$ et $\mathfrak{N} \vDash \psi_1(\bar{a})$. □

Vocabulaire.

(1) Un morphisme F de L-structures est un *isomorphisme* si F est un plongement surjectif.

(2) Un morphisme F de L-structures est un *plongement élémentaire* si pour toute formule $\varphi(\bar{x})$ et tout uplet $\bar{a}$ de M,

$$\mathfrak{M} \vDash \varphi(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash \varphi(F(\bar{a}))$$

Lorsque $M \subset N$ et que l'inclusion ensembliste est un plongement élémentaire, alors on dit que $\mathfrak{M}$ est une *sous-structure élémentaire* de $\mathfrak{N}$ et l'on note $\mathfrak{M} \prec \mathfrak{N}$.

(3) Un *isomorphisme partiel* g entre $\mathfrak{M}$ et $\mathfrak{N}$ est une bijection entre un sous-ensemble M_0 de M et N_0 de N qui vérifie que pour toute formule $\varphi(\bar{x})$ sans quantificateurs et tout uplet $\bar{a}$ de M_0, on a

$$\mathfrak{M} \vDash \varphi(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash \varphi(g(\bar{a})).$$

(4) Si $\mathfrak{M}$ et $\mathfrak{N}$ sont deux L-structures, on dit qu'elles sont *élémentairement équivalentes*, et on note $\mathfrak{M} \equiv \mathfrak{N}$ si les deux structures vérifient les mêmes formules. Soit encore si $\mathrm{Th}(\mathfrak{M}) = \mathrm{Th}(\mathfrak{N})$. En particulier si $\mathfrak{M}$ est une sous-structure élémentaire de $\mathfrak{N}$, alors $\mathfrak{M} \equiv \mathfrak{N}$.

Une sous-structure n'est pas nécessairement uns sous-structure élémentaire élémentaire. En effet, dans le langage des groupes, on a vu que $(\mathbf{Z}, =, +, 0)$ est une sous-structure de $(\mathbf{R}, =, +, 0)$, néanmoins la formule $\exists y\ (y+y = 1)$ est vérifiée dans $\mathbf{R}$ par $1/2$, mais pas dans $\mathbf{Z}$.

Par ailleurs, il est possible, étant donné un modèle infini $\mathfrak{M}$ d'une théorie, de construire des extensions élémentaires $\mathfrak{N}$ de $\mathfrak{M}$. Pour le démontrer nous admettrons provisoirement le théorème suivant qui sera démontré dans le paragraphe 3.2.2.

Théorème 2.1.3 (Compacité)**.** *Soit Σ un ensemble d'énoncé, tel que sous-ensemble fini de Σ admet un modèle. Alors Σ admet un modèle.*

On appellera *cardinal* d'une structure le cardinal de son ensemble sous-jacent.

Lemme 2.1.4. *Soit une théorie T et $\mathfrak{M}$ un modèle infini de cette théorie, si l'on se donne un cardinal κ, il existe un modèle $\mathfrak{N}$ de T, de cardinal supérieur ou égal à κ tel que $\mathfrak{M} \prec \mathfrak{N}$.*

Démonstration. Considérons des nouveaux symboles de constantes $(c_i)_{i\in\kappa}$ et l'ensemble d'énoncés :

$$\Sigma := \mathrm{Th}(\mathfrak{M}, M) \cup \{c_i \neq c_j \mid i \neq j\}.$$

Chaque sous-ensemble fini de Σ ne fait intervenir qu'un nombre fini de constantes, qui peuvent donc être interprétée par des éléments distincts de M puisque l'ensemble est infini. Donc la théorie Σ est finiement consistance puisque la structure M est un modèle de toute partie finie de Σ, donc la théorie Σ est consistance par le théorème 2.1.3 de compacité. Elle admet donc un modèle $\mathfrak{N}$ de cardinal supérieur ou égal à κ (puisqu'il faut interpréter toutes les constantes), qui est une extension élémentaire de $\mathfrak{M}$ par définition des énoncés de $\mathrm{Th}(\mathfrak{M}, M)$. □

2.2. **Théorie modèles complètes, et élimination des quantificateurs.**

2.2.1. *Théories modèles complètes.* Soit T une théorie exprimée dans un langage L.

(1) On dit que la théorie T est *modèle complète* si pour tous modèles A et B tels que $A \subset B$, on a $A \prec B$.

(2) On dit que la théorie T admet *l'élimination des quantificateurs* si pour toute formule $\varphi(\bar{x})$, il existe une formule $\psi(\bar{x})$ sans quantificateurs telle que :

$$T \vdash \forall \bar{x}(\varphi(\bar{x}) \Leftrightarrow \psi(\bar{x})).$$

Ces deux notions ne sont pas sans liens. Une théorie qui admet l'élimination des quantificateurs est aussi modèle complète. Prenons, en effet, deux modèles $\mathfrak{M} \subseteq \mathfrak{N}$ d'une théorie T qui admet l'élimination des quantificateurs. Soit $\varphi(\bar{x})$ une L-formule, et soit $\bar{a}$ un élément de M. Puisque la théorie T admet l'élimination des quantificateurs, il existe une formule $\psi(\bar{x})$ sans quantificateurs telle que :

$$T \vdash \forall \bar{x}\ (\varphi(\bar{x}) \Leftrightarrow \psi(\bar{x})).$$

Comme les formules sans quantificateurs sont préservées par sous-structures (voir la proposition 2.1.2), on a :

$$\mathfrak{M} \vDash \varphi(\bar{a}) \Leftrightarrow \mathfrak{M} \vDash \psi(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash \psi(\bar{a}) \Leftrightarrow \mathfrak{N} \vDash \varphi(\bar{a}).$$

Théorème 2.2.1. *Soit langage L qui contient le symbole $=$. Soit T une théorie exprimée dans le langage L, et soit $\varphi(\bar{x})$ une formule à m variables libres. Alors les deux conditions suivantes sont équivalentes :*

(1) Il existe une formule sans quantificateurs $\psi(\bar{x})$ telle que $T \vdash \forall \bar{x}\ (\varphi(\bar{x}) \Leftrightarrow \psi(\bar{x}))$;

(2) Si $\mathfrak{A}$ est une $\mathcal{L}$-structure, et $\mathfrak{M}, \mathfrak{N}$ deux modèles de T contenant $\mathfrak{A}$, pour tout uplet a de $\mathfrak{A}$, on a $\mathfrak{M} \vDash \varphi(\bar{a})$ si et seulement si $\mathfrak{N} \vDash \varphi(\bar{a})$.

Démonstration. L'implication de (1) vers (2) est claire puisqu'une formule sans quantificateurs est vérifiée dans un modèle si et seulement si elle est vérifiée dans une sous-structure. Pour la réciproque, on on considère l'ensemble $\Gamma(\bar{x})$ formé des formules sans quantificateurs $\psi(\bar{x})$ telles que $T \vdash \forall \bar{x}\ (\varphi(\bar{x}) \Rightarrow \psi(\bar{x})$. On rajoute des nouvelles constantes de symbole $d_1, \cdots, d_m$.

Montrons que $T \cup \Gamma(\bar{d}) \vDash \varphi(\bar{d})$. Sinon il existerait une structure $\mathfrak{M}$ telle que $\mathfrak{M} \vDash T \cup \Gamma(\bar{d}) \cup \{\neg\varphi(\bar{d})\}$. Considérons la sous-structure $\mathfrak{A}$ de $\mathfrak{M}$ engendrée par les symboles de constante $\bar{d}$. On notera $\Delta(\mathfrak{A})$ l'ensemble des formules sans quantificateurs vérifiées dans la structure $\mathfrak{A}$. On considère $\Sigma = T \cup \Delta(\mathfrak{A}) \cup \{\varphi(\bar{d})\}$. Montrons que Σ admet un modèle. En effet, si Σ n'a pas de modèle, alors ce n'est pas une théorie consistante, donc il existe (par le théorème de compacité 2.1.3) $g_1(\bar{d}), \cdots, g_n(\bar{d})$ dans $\Delta(\mathfrak{A})$ telles que :

$$T \vDash \wedge_i g_i(\bar{d}) \Rightarrow \neg\varphi(\bar{d}).$$

Comme les symboles de constantes d_i n'apparaissent pas dans la théorie T ni dans le langage $\mathcal{L}$, il s'ensuit que :

$$T \vDash \forall \bar{x}\ (\wedge_i g_i(\bar{x}) \Rightarrow \neg\varphi(\bar{x})).$$

Mais alors

$$T \vDash \forall \bar{x}\ (\varphi(\bar{x}) \Rightarrow \vee_i \neg g_i(\bar{x}))$$

et $\vee_i \neg g_i(\bar{x})$ appartient à $\Gamma(\bar{x})$, et donc $\mathfrak{A} \vDash \vee_i \neg g_i(\bar{x})$, ce qui est absurde. Il existe donc un modèle $\mathfrak{N}$ de Σ contenant $\mathfrak{A}$. On a donc $\mathfrak{M} \vDash \neg\varphi(\bar{d})$ tandis que $\mathfrak{N} \vDash \varphi(\bar{d})$ ce qui contredit (2). On a donc montré que $T \cup \Gamma(\bar{d}) \vDash \varphi(\bar{d})$. Il existe par compacité des formules sans quantificateurs $g_1(\bar{d}), \cdots, g_n(\bar{d})$ dans $\Gamma(\bar{d})$ telles que

$$T \vDash \wedge_i g_i(\bar{d}) \Rightarrow \varphi(\bar{d})$$

ils s'ensuit que

$$T \vDash \forall \bar{x}\ (\wedge_i g_i(\bar{x}) \Rightarrow \varphi(\bar{x})).$$

Mais alors

$$T \vDash \forall \bar{x}\ (\wedge_i g_i(\bar{x}) \Leftrightarrow \varphi(\bar{x})).$$

Et la formule $\wedge_i g_i(\bar{x})$ est sans quantificateurs. □

On remarque si le langage L est dénombrable (c'est-à-dire que l'ensemble de toutes les formules que l'on peut écrire dans le langage L est dénombrable), alors on peut demander à ce que $\mathfrak{A}$ dans (2) soit seulement dénombrable, puisqu'une sous-structure de $\mathfrak{M}$ engendré par une partie dénombrable, est dénombrable.

2.2.2. *La méthode du va et vient.* Soient $\mathfrak{M}$ et $\mathfrak{N}$ deux L-structures. Supposons qu'il existe une famille $\mathcal{I}$ d'isomorphismes partiels entre $\mathfrak{M}$ et $\mathfrak{N}$ satisfaisant aux deux conditions suivantes :

(1) Pour tout isomorphisme partiel $f \in \mathcal{I}$, et pour tout $a \in M$, il existe $f' \in \mathcal{I}$ qui prolonge f ayant a dans son domaine ;

(2) Pour tout isomorphisme partiel $f \in \mathcal{I}$, et pour tout $b \in N$, il existe $f' \in \mathcal{I}$ qui prolonge f ayant b dans son image.

Alors $\mathfrak{M}$ est élémentairement équivalent à $\mathfrak{N}$ ($\mathfrak{M} \equiv \mathfrak{N}$).

Démonstration. Nous allons montrer le théorème du va-et-vient. On prouve par induction sur le nombre de quantificateurs d'une formule $\varphi(\bar{x})$ prénexe que : si $\bar{a}$ est un uplet dans le domaine d'un élément f de $\mathcal{I}$ alors :

$$M \vDash \varphi(\bar{a}) \Leftrightarrow N \vDash \varphi(f(\bar{a})).$$

Pour les formules sans quantificateurs, c'est par définition d'isomorphisme partiel. Considérons la formule $\varphi(\bar{x}) = \exists y\ \psi(\bar{x}, y)$, et supposons le résultat vrai pour la formule $\psi(\bar{x}, y)$. Supposons que $\bar{a}$ est dans le domaine de la fonction $f \in \mathcal{I}$, et que $M \vDash \exists y\ \psi(\bar{a}, y)$. Soit $b \in M$ tel que $M \vDash \psi(\bar{a}, b)$. Par hypothèse, il existe $f' \in \mathcal{I}$ étendant f et ayant b dans son domaine. Pat hypothèse d'induction, on a $N \vDash \psi(f'(a), f'(b))$, et qui montre bien que $N \vDash \varphi(\bar{a})$.

On procède de la même façon pour montrer l'autre direction. □

2.2.3. *Les corps algébriquement clos.* Nous allons montrer que la théorie des corps algébriquement clos admet l'élimination des quantificateurs, et est donc modèle complète. On se place dans le langage des anneaux $L_r := \{=, +, -, \cdot, 0, 1\}$, et on considère la théorie suivante notée ACF et axiomatisée par :

- † Les énoncés de la théorie des anneaux intègres commutatifs avec unité 0 et 1 ;
- † L'énoncé $\forall x \exists y\ (x = 0 \vee xy = 1)$;
- † Pour tout entier naturel $n > 1$, l'énoncé : $\forall x_1 \cdots \forall x_n \exists y\ y^n + x_1 y^{n-1} + \cdots + x_n = 0$.

Les modèles de ACF sont des corps algébriquement clos. Un exemple en caractéristique nulle est le corps $\mathbf{C}$, et en caractéristique $p > 0$ la clôture algébrique $\tilde{\mathbf{F}}_p$ du corps fini à p éléments $\mathbf{F}_p$. On notera, de plus, pour p un nombre premier, $ACF_p = ACF \cup \{p = 0\}$, et $ACF_0 = ACF \cup \{n \neq 0 \mid n \in \mathbf{N}, n > 0\}$.

Lemme 2.2.2. *Soient K et L des corps algébriquement clos, et supposons que $f : A \to B$ soit un isomorphisme entre des sous-structures de K et L respectivement. Soit $a \in K$ un élément algébrique sur A. Alors il existe un isomorphisme f' étendant f et ayant a dans son domaine.*

Démonstration. Quitte à passer au corps des fractions, on peut supposer que A et B sont des corps. Soit $a \in K$ un élément algébrique sur A, et soit $P(X)$ son polynôme (unitaire) minimal sur A. On note $f(P)(X)$ le polynôme de $B[X]$ obtenu en appliquant f aux coefficients du polynôme P. Puisque le corps L est algébriquement clos, il existe $b \in L$, racine du polynôme $f(P)(X)$. Nous avons donc des isomorphismes canoniques, grâce à la propriété universelle du quotient

$$A(a) \simeq_A A[X]/\langle P(X)\rangle \quad \text{et} \quad B(b) \simeq_B B[X]/\langle f(P)(X)\rangle.$$

Donc f s'étend naturellement en un isomorphisme $f' \colon A(a) \to B(b)$ qui envoie a sur b. □

Théorème 2.2.3. *La théorie ACF admet l'élimination des quantificateurs et est donc modèle complète.*

Démonstration. Pour cette preuve, nous allons utiliser la caractérisation du théorème 2.2.1. Soit φ une formule du langage $\mathcal{L}$. Soit C une $\mathcal{L}$-structure dénombrable, et soit K et L deux corps algébriquement clos qui contiennent C. Ces corps sont de même caractéristique puisque si la formule $1+\cdots+1=0$ (pour p fois 1) est vraie dans C, alors elle est vraie dans K et L puisqu'il s'agit d'une formule atomique. De plus, quitte à passer à des extensions élémentaires de K et L (ce qui est possible grâce au lemme 2.1.4), on peut supposer que K et L sont non dénombrables. On va maintenant montrer qu'il existe un va-et-vient entre les structures K et L

Considérons la famille $\mathcal{I}$ d'isomorphismes f entre des sous-structures dénombrables de K et L contenant C. Nous allons montrer que cette famille satisfait la condition du va-et-vient : Soit a un élément de K, et f un isomorphisme partiel de $\mathcal{I}$, A le domaine de f et $B = f(A)$. Si l'élément a est algébrique sur A alors le lemme 2.2.2 nous donne un isomorphisme partiel $f' \in \mathcal{I}$ ayant a dans son domaine (en effet, la construction de l'isomorphisme f' dans le lemme nous montre que ses domaines de départ et d'arrivé sont toujours des sous-structures dénombrables de K et L). Supposons que a n'est pas algébrique sur A, puisque la cardinalité de L est plus grande que celle de B, il existe $b \in L$ qui n'est pas algébrique sur B (en effet, l'ensemble des éléments algébrique sur B est dénombrable alors que L ne l'est pas). En posant $f'(a) = b$ on peut alors étendre f en un isomorphisme $f' : A[a] \to B[b]$.

Si b est un élément de L, on raisonne de la même façon avec f^{-1} pour obtenir l'autre direction. Le théorème du va-et-vient nous donne donc que les structures K et L sont élémentairement équivalentes. C'est-à-dire que pour tout élément $\bar{a}$ de C, la formule $\varphi(\bar{a})$ est vraie dans K si et seulement si elle est vraie dans L. Donc par le théorème 2.2.1, la formule φ est équivalente à une formule sans quantificateur. Donc la théorie ACF admet bien l'élimination des quantificateurs. □

Corollaire 2.2.4. *Les théories ACF_0 et ACF_p sont complètes.*

Démonstration. Nous allons montrer ce résultat pour ACF_p, le raisonnement pour obtenir la complétude ACF_0 étant similaire, en remplaçant $\tilde{\mathbf{F}}_p$ par $\mathbf{Q}$.

Soit φ une formule du langage des anneaux L_r. Notons $\tilde{\mathbf{F}}_p$ la clôture algébrique du sous-corps premier $\mathbf{F}_p$. La formule φ est soit vraie, soit fausse dans $\tilde{\mathbf{F}}_p$. Sans perte de généralité, on peut supposer que φ est vraie dans $\tilde{\mathbf{F}}_p$. Soit K un corps algébriquement clos de caractéristique p (qui vérifie donc la théorie ACF_p). Il contient alors le sous-corps premier $\mathbf{F}_p$ et aussi sa clôture algébrique que nous noterons $\tilde{\mathbf{F}}_p$. Comme ACF admet l'élimination des quantificateurs d'après le théorème 2.2.3, la théorie est aussi modèle complète. En particulier $\tilde{\mathbf{F}}_p$ est une sous-structure élémentaire de K, donc la formule φ, puisqu'elle est vérifiée dans $\tilde{\mathbf{F}}_p$, l'est aussi dans K. On en déduit en particulier que pour tout modèle K de la théorie ACF_p, on a $K \vDash \varphi$. La

formule φ est donc une conséquence syntaxique de T, ce qui implique $T \vdash \varphi$. Donc la théorie ACF_p est complète. □

Nous allons voir une application de l'élimination des quantificateurs.

Théorème 2.2.5 (Principe de Lefschetz)**.** *Soit φ un énoncé du langage des anneaux. Les propriétés suivantes sont équivalentes :*

(1) L'énoncé φ est vérifié dans $\mathbf{C}$;

(2) L'énoncé φ est vérifié dans un corps algébriquement clos de caractéristique 0 ;

(3) L'énoncé φ est vérifié dans tout corps algébriquement clos de caractéristique 0 ;

(4) L'énoncé φ est vérifié dans tout corps algébriquement clos de caractéristique p avec p suffisamment grand ;

(5) Il existe un ensemble infini de nombre premiers P tel que que pour chaque p dans P, la formule φ est vérifiée pour au moins un corps algébriquement clos de caractéristique p.

Démonstration. Il est clair que (1) implique (2) et que (3) implique (1). Montrons que (2) implique (3). Soit K un corps algébriquement clos de caractéristique 0 tel que $K \models \varphi$. Comme c'est un corps de caractéristique 0, alors K contient $\mathbf{Q}$. Comme K est algébriquement clos, alors K contient la clôture algébrique de $\mathbf{Q}$ notée $\bar{\mathbf{Q}}_{alg}$. Enfin, d'après le théorème 2.2.3, comme la théorie des corps algébriquement clos est modèle complète, alors $\bar{\mathbf{Q}}_{alg} \models \varphi$. Soit L un autre corps de caractéristique nulle. Comme $\bar{\mathbf{Q}}_{alg} \subset L$ alors $\bar{\mathbf{Q}}_{alg} \prec L$, et en particulier $L \models \varphi$. Donc les énoncés (1), (2) et (3) sont équivalents. Montrons maintenant que (3) implique (4) Puisque pour tout modèle $\mathfrak{M}$ de la théorie des corps algébriquement clos de caractéristique 0 (notée ACF_0) on a $\mathfrak{M} \models \varphi$, alors il existe une démonstration formelle de φ ; on note $ACF_0 \vdash \varphi$. En particulier il existe une partie finie Δ de ACF_0 telle que $\Delta \vdash \varphi$. Comme il faut une infinité d'énoncés pour décrire qu'on est en caractéristique nulle, pour tout nombre premier p suffisamment grand on a $ACF_p \vdash \varphi$. On en déduit bien (4). Comme (4) implique (5), il ne reste plus qu'à montrer que (5) implique (3). Supposons qu'il existe un ensemble infini de nombres premiers $\mathcal{P}$ tel que la formule φ est vérifiée pour p dans $\mathcal{P}$ pour au moins un corps algébriquement clos de caractéristique p. Si $ACF_0 \nvdash \varphi$, alors $ACF_0 \vdash \neg\varphi$ car la théorie ACF_0 est complète par 2.2.4. Dans ce cas, la formule $\neg\varphi$ est vérifiée dans tout corps algébriquement clos de caractéristique p assez grande, ce qui est absurde. □

Grâce à ce principe nous allons pouvoir démontrer le théorème d'Ax dont nous parlions dans l'introduction.

Théorème 2.2.6 (Ax)**.** *Soit $f\colon \mathbf{C}^n \to \mathbf{C}^n$ une application polynomiale. C'est-à-dire de la forme $f = (f_1, \cdots, f_n)$ avec $f_i \in \mathbf{C}[X_1, \cdots, X_n]$. Si l'application f est injective, alors f est surjective.*

Démonstration. D'après le principe de Lefschetz 2.2.5, il suffit de démontrer l'énoncé pour la clôture algébrique $\bar{\mathbf{F}}_p$ du corps $\mathbf{F}_p$ pour tout entier p premier. En effet pour toute paire d'entier (n, d), il existe un énoncé du langage des anneaux, noté $\psi_{n,d}$, exprimant dans un corps K que pour toute famille $(f_1, \cdots, f_n)$ de polynômes en n variables de degré inférieur ou égal à d, si l'application associée $K^n \to K^n$ est injective, alors elle est surjective. Si $\psi_{n,d}$ est une conséquence de ACF_p pour tout entier p, alors c'est une conséquence de ACF_0. Pour tout entier k strictement positif, l'ensemble des racines du polynôme $X^{p^k} - X$ dans $\bar{\mathbf{F}}_p$ est un sous-corps $\mathbf{F}_{p^k}$ de cardinal p^k de $\bar{\mathbf{F}}_p$, de plus $\mathbf{F}_{p^k}$ est un sous-corps de $\mathbf{F}_{(p^k)^r}$ et $\bar{\mathbf{F}}_p$ est la réunion de ses sous-corps $\mathbf{F}_{p^k}$. En particulier, toute partie finie de $\bar{\mathbf{F}}_p$ est contenue dans un sous-corps fini de $\bar{\mathbf{F}}_p$. Soit $f = (f_1, \cdots, f_n) : \bar{\mathbf{F}}_p{}^n \to \bar{\mathbf{F}}_p{}^n$ une application polynomiale injective. On suppose qu'il existe b dans $\bar{\mathbf{F}}_p$ qui n'est pas dans l'image de f. Soit k le sous-corps fini de $\bar{\mathbf{F}}_p$ contenant les composantes de b ainsi que les coefficients des polynômes f_i. L'application f induit une application $k^n \to k^n$ qui est injective et non surjective, ce qui est absurde vu que k^n est un corps fini. □

3. Ultraproduits

Dans cette section nous allons voir une méthode pour construire un modèle à partir d'une famille de modèles. Une idée naïve, lorsqu'on se donne une famille de modèles $(\mathfrak{M}_i)_i$ d'une théorie T serait de considérer une structure dont l'ensemble sous-jacent serait le produit cartésien $\prod_i M_i$. Cependant, on voit vite les limites de cette idée : en général le produit de deux corps (qui vérifient les énoncés de la théorie des corps) n'est pas un corps puisqu'on peut y trouver des diviseurs de zéros. Pour pallier à ce problème nous allons quotienter par une relation compatible aux fonctions et relations de la structure. Cette relation sera construire à partir de filtres et ultrafiltres que nous allons développer dans le paragraphe à venir.

3.1. **Filtres et ultrafiltres.**

3.1.1. *Filtres.*

Définition 3.1.1. On appelle *filtre* sur un ensemble E un ensemble $\mathcal{F}$ de parties de E qui vérifie les propriétés suivantes :

- (F_1) Si $F \in \mathcal{F}$ alors tout sous-ensemble E de X qui contient F est un élément de $\mathcal{F}$;
- (F_2) L'ensemble $\mathcal{F}$ est stable par intersection finies ;
- (F_3) L'ensemble vide n'appartient pas à $\mathcal{F}$.

Des deux dernières propriétés on déduit qu'une intersection finie d'éléments de $\mathcal{F}$ est non vide.

Lorsqu'un ensemble E est muni d'un filtre $\mathcal{F}$, il est appelé *ensemble filtré par le filtre* $\mathcal{F}$.

Donnons quelques exemples canoniques de filtres.

† L'ensemble $\mathcal{F} = \{E\}$ est un filtre sur E.
† On fixe X_0 un sous-ensemble de E. L'ensemble $\mathcal{F}_{X_0} := \{A \subset E \mid X_0 \subset A\}$ est un filtre sur E. Dans le cas où $X_0 = x_0$ est réduit à un élément, on l'appelle *filtre principal* sur E.
† Lorsque E est un espace topologique, et x un élément de E, l'ensemble des voisinages de x est un filtre.
† Si E est un ensemble infini, l'ensemble des complémentaire des parties finies de E est un filtre sur E appelé *filtre de Fréchet*.

Montrons rapidement que le dernier exemple est bien un filtre. Soit E un ensemble infini, et soit Y un élément de filtre de Fréchet. (F_1)Si $Y \subset X$, alors par passage au complémentaire $\complement_E X \subset \complement_E Y$. Comme le complémentaire de Y est fini, l'inclusion précédente permet de montrer que le complémentaire de X est fini, et donc que X est un élément de filtre de Fréchet. (F_2) Le complémentaire d'une intersection est inclus dans l'union des complémentaires. Ainsi l'intersection de deux éléments du filtre de Fréchet est toujours de complémentaire fini. (F_3) Le vide n'est pas un élément du filtre car son complémentaire est l'ensemble E qui est infini.

3.1.2. *Comparaisons de filtres.* Certains filtres semblent intuitivement moins précis que d'autres. Le filtre $\mathcal{F} = \{E\}$ est, par exemple, contenu dans tous les autres, dans le sens où E est toujours un élément de n'importe quel filtre. Nous allons préciser ceci, en établissant une relation d'ordre sur les filtres.

Définition 3.1.2. Étant donné deux filtres $\mathcal{F}$ et $\mathcal{F}'$ sur un même ensemble E, on dit que $\mathcal{F}'$ est *plus fin* que $\mathcal{F}$, ou que $\mathcal{F}$ est moins fin que $\mathcal{F}'$, si $\mathcal{F} \subset \mathcal{F}'$. De plus si $\mathcal{F} \neq \mathcal{F}'$, on dit que $\mathcal{F}'$ est *strictement plus fin* que $\mathcal{F}$.

Ainsi, si $X_0 \subset E$ et si $x_0 \in X_0$, le filtre $\mathcal{F}_{x_0}$ est plus fin que $\mathcal{F}_{X_0}$. De plus, comme on l'a déjà fait remarquer au début de ce paragraphe, le filtre $\mathcal{F} = \{E\}$ est moins fin que n'importe quel autre filtre sur E.

Deux filtres dont l'un est plus fin que l'autre sont dit *comparables*, et comme souhaité la relation "être plus fin que" est une relation d'ordre sur l'ensemble des filtres définis sur un même ensemble E.

Soit I un ensemble non vide. Considérons une famille de filtre $\{\mathcal{F}_i\}_{i\in I}$ sur un ensemble E. L'ensemble $\mathcal{F} := \bigcap_i \mathcal{F}_i$ est non vide puisque $E \in \mathcal{F}$, et ne contient pas l'ensemble vide car il n'est contenu dans aucun des filtres $\mathcal{F}_i$ (F_3). De plus si A et B sont des éléments de $\mathcal{F}$, ils appartiennent à chaque $\mathcal{F}_i$, donc leur intersection aussi, et en particulier $A \cap B \in \mathcal{F}$ (F_2). Enfin, si X est un élément de $\mathcal{F}$, et si l'ensemble Y est tel que $X \subset Y$, alors comme chaque $\mathcal{F}_i$ est un filtre, l'ensemble Y est dans chaque $\mathcal{F}_i$ et en particulier dans leur intersection (F_1). Ceci prouve que $\mathcal{F}$ est un filtre que l'on nomme *filtre intersection* de la famille des $\mathcal{F}_i$, et il est par construction moins fin que chacun des $\mathcal{F}_i$.

Proposition 3.1.3. *L'ensemble ordonné des filtres sur un ensemble non vide E est inductif.*

Démonstration. Soit I un ensemble non vide. Considérons une chaîne de filtre $\{\mathcal{F}_i\}_{i\in I}$ sur un ensemble E, c'est-à-dire que l'ensemble des filtres $\{\mathcal{F}_i\}_{i\in I}$ est totalement ordonné pour la relation "être plus fin que". Intéressons-nous à l'ensemble $\mathcal{F} := \bigcup_i \mathcal{F}_i$. Soit $X \in \mathcal{F}$, alors il existe $j \in I$ tel que $X \in \mathcal{F}_j$. Soit Y un sous-ensemble de E vérifiant $X \subset Y$. Puisque l'ensemble $\mathcal{F}_j$ est un filtre, alors $Y \in \mathcal{F}_j$, et en particulier l'ensemble Y est un élément de $\mathcal{F}$, ce qui montre (F_1). Par ailleurs, on se donne X et Y deux éléments de $\mathcal{F}$. Il existe $j, k \in I$ tels que $X \in \mathcal{F}_j$ et $X \in \mathcal{F}_k$. Comme la famille de filtre est totalement ordonnée, quitte à échanger j et k on peut supposer $\mathcal{F}_k \subset \mathcal{F}_j$, auquel cas X et Y sont des éléments de $\mathcal{F}_j$. Leur intersection est donc aussi un élément de $\mathcal{F}_j$ et en particulier de $\mathcal{F}$, ce qui montre (F_2). Comme les filtres $\mathcal{F}_i$ sont non vides et que l'ensemble I est aussi non vide, alors $\mathcal{F}$ est non vide, ce qui montre (F_3). □

3.1.3. *Ultrafiltres.* Nous venons de montrer que l'ensemble ordonné des filtres sur un ensemble non vide E est inductif. Le lemme de Zorn nous assure l'existence d'un élément maximal dans l'ensemble ordonné des filtres sur un ensemble non vide E.

Définition 3.1.4. Un élément maximal de l'ensemble des filtres sur un ensemble non vide E est appelé un *ultrafiltre*.

Autrement dit, un ultrafiltre est un filtre qui n'est plus fin que n'importe quel autre filtre qui lui est comparable. Une autre caractérisation utile des ultrafiltres est la suivante : le filtre $\mathcal{F}$ est un ultrafiltre si et seulement s'il satisfait de plus la formule suivante notée (F_4) :

$$\forall X \subset E,\ X \in \mathcal{F} \Leftrightarrow (E\backslash X) \notin \mathcal{F}.$$

Supposons, en effet, que $\mathcal{F}$ est un ultrafiltre. Si $X \in \mathcal{F}$, on a bien $(E\backslash X) \notin \mathcal{F}$ sinon, en considérant leur intersection, l'ensemble vide serait dans $\mathcal{F}$. Supposons maintenant que l'ensemble X soit tel que $(E\backslash X) \notin \mathcal{F}$. On remarque que si $Y \in \mathcal{F}$, alors $X \cap Y \neq \varnothing$. Sinon, on aurait $Y \subset E\backslash X$, ce qui est absurde par la propriété (F_1). On peut alors considérer le filtre $\mathcal{F}'$ engendré par $\mathcal{F} \cup \{X\}$, qui est composé de $\mathcal{F}$ de X, de tous les ensembles inclus dans X, et de toutes les intersections, entre $Y \subset X$ et $\mathcal{F}$. Alors on a $\mathcal{F} \subset \mathcal{F} \cup \{X\}$. Mais par maximalité du filtre $\mathcal{F}$, on a $\mathcal{F} = \mathcal{F}'$, et donc en particulier $X \in \mathcal{F}$.

Réciproquement, soit un filtre $\mathcal{F}$ vérifiant la propriété (F_4). Soit $\mathcal{F}'$ un filtre tel que $\mathcal{F} \subset \mathcal{F}'$. S'ils étaient distincts, on pourrait trouver $X \in \mathcal{F}'$ tel que $X \notin \mathcal{F}$. Mais alors $E\backslash X \in \mathcal{F}$, et par inclusion $E\backslash X \in \mathcal{F}'$, ce qui est absurde. Donc $\mathcal{F}$ est un ultrafiltre.

Proposition 3.1.5. *Un ultrafiltre est soit principal, soit il contient le filtre de Fréchet.*

Démonstration. Soit $\mathcal{F}$ un ultrafiltre. On suppose que $\mathcal{F}$ ne contient pas le filtre de Fréchet. Donc il existe un ensemble $X \subset E$ de complémentaire fini, tel que $X \notin \mathcal{F}$. Comme $\mathcal{F}$ est un ultrafiltre, alors $E\backslash X \in \mathcal{F}$, d'après la propriété ($\mathrm{F}_4$) que vérifient les ultrafiltres. Notons $E\backslash X = \{x_1, \cdots, x_n\}$.

Alors il existe un entier $i_0 \in \{1, \cdots, n\}$ tel que $\{x_{i_0}\} \in \mathcal{F}$. En effet, si tel n'était pas le cas, comme $\mathcal{F}$ est un ultrafiltre, on aurait $E\backslash\{x_i\} \in \mathcal{F}$, pour tout entier $i \in \{1, \cdots, n\}$. En particulier, leur intersection $\cap_i(E\backslash\{x_i\})$ serait dans $\mathcal{F}$. Or cette intersection est exactement X. On aurait donc $X \in \mathcal{F}$, ce qui est absurde par hypothèse, donc il existe un entier $i_0 \in \{1, \cdots, n\}$ tel que $\{x_{i_0}\} \in \mathcal{F}$. Alors $\mathcal{F}_{i_0} := \{X \mid x_{i_0} \in X\} \subset \mathcal{F}$. Cependant $\mathcal{F}_{i_0}$ est un ultrafiltre, on a donc $\mathcal{F}_{i_0} = \mathcal{F}$, ce qui prouve que $\mathcal{F}$ est un ultrafiltre principal. □

3.2. **Ultraproduits.**

3.2.1. *Ultraproduits.* On se fixe un langage L et un ensemble non vide I. Nous allons voir dans ce paragraphe comment construire une L-structure à partir d'une famille $(\mathfrak{M}_i)_{i\in I}$ de L-structures.

L'ensemble sous-jacent de notre future structure $\mathfrak{N}$ est $N = \prod_{i\in I} M_i$, à savoir le produit cartésien des M_i que l'on peut encore voir comme les fonctions a de I dans la réunion disjointe des M_i, où si $i \in I$ alors $a(i) \in M_i$. Une telle fonction est aussi notée $(a(i))_{i\in I}$. Si f est un symbole de fonction n-aire du langage, on lui associe une fonction $f^{\mathfrak{N}}$ définie coordonnée par coordonnée par $f^{\mathfrak{N}}(a_1, \cdots, a_n)(i) = f^{\mathfrak{M}_i}(a_1(i), \cdots, a_n(i))$. Si c est un symbole de constante et $c(i)$ son interprétation dans M_i, alors l'interprétation de c dans N est $(c(i))_{i\in I}$. Enfin si R est un symbole de relation n-aire, alors $\prod_{i\in I} M_i \vDash R(a_1, \cdots, a_n)$ si et seulement si $M_i \vDash R(a_1(i), \cdots, a_n(i))$. Ces diverses définitions font $\mathfrak{N}$ une L-structure d'ensemble sous-jacent N.

Soit $\mathcal{F}$ un filtre sur I, on définit une relation sur l'ensemble $\prod_{i\in I} M_i$ de la façon suivante, pour $a, b \in N$:

$$a \equiv_{\mathcal{F}} b \Leftrightarrow \{i \in I \mid a(i) = b(i)\} \in \mathcal{F}.$$

Proposition 3.2.1. *La relation $\equiv_{\mathcal{F}}$ définit une relation d'équivalence sur l'ensemble $\prod_{i\in I} M_i$.*

Démonstration. La symétrie de la relation est claire. Comme $I \in \mathcal{F}$, la relation $\equiv_{\mathcal{F}}$ est réflexive, c'est–à–dire $a \equiv_{\mathcal{F}} a$. Soit maintenant a, b, c trois éléments de $\prod_{i\in I} M_i$ qui vérifient $a \equiv_{\mathcal{F}} b$ et $b \equiv_{\mathcal{F}} c$. Autrement dit $\{i \in I \mid a(i) = b(i)\} \in \mathcal{F}$ et $\{i \in I \mid b(i) = c(i)\} \in \mathcal{F}$. Or, si pour un certain $i \in I$, on a $a(i) = b(i)$ et $b(i) = c(i)$, alors $a(i) = c(i)$. On en déduit l'inclusion suivante :

$$\{i \in I \mid a(i) = b(i)\} \bigcap \{i \in I \mid b(i) = c(i)\} \subset \{i \in I \mid a(i) = c(i)\}.$$

Comme $\mathcal{F}$ est un filtre sur I, l'on en déduit que $\{i \in I \mid a(i) = c(i)\} \in \mathcal{F}$, ce qui montre que la relation est transitive. Finalement, nous avons montré que $\equiv_{\mathcal{F}}$ est une relation d'équivalence. □

On peut dire mieux, cette relation d'équivalence est aussi compatible avec les fonctions et les relations de la L-structure $\mathfrak{N}$. Si f est un symbole de fonction n-aire, que $a_1, \cdots, a_n$ et $b_1, \cdots, b_n$ sont des éléments de N de telle sorte que pour tout $j \in \{1, \cdots, n\}$ on ait $a_j \equiv_{\mathcal{F}} b_j$. Remarquons

que si $i \in I$ vérifie que pour tout $j \in \{1, \cdots, n\}$ on ait $a_j(i) = b_j(i)$, alors $f(a_1, \cdots, a_n)(i) = f(b_1, \cdots, b_n)(i)$. On en déduit l'inclusion suivante :

$$\bigcap_{k=1}^{n} \{i \in I \mid a_k(i) = b_k(i)\} \subset \{i \in I \mid f(a_1, \cdots, a_n)(i) = f(b_1, \cdots, b_n)(i)\}.$$

On déduit des propriétés (F_1) et (F_2) des filtres que $f(a_1, \cdots, a_n) \equiv_{\mathcal{F}} f(b_1, \cdots, b_n)$. Soient R est un symbole de relation n-aire, et $a_1, \cdots, a_n$ et $b_1, \cdots, b_n$ des éléments de M équivalent deux à deux, comme précédemment. Supposons de plus que $\{i \in I \mid M_i \vDash R(a_1(i), \cdots, a_n(i))\} \in \mathcal{F}$. Remarquons maintenant que si $i \in I$ vérifie $M_i \vDash R(a_1(i), \cdots, a_n(i))$ et si pour tout entier $j \in \{1, \cdots, n\}$, on a $a_j(i) = b_j(i)$, alors $M_i \vDash R(b_1(i), \cdots, b_n(i))$. On en déduit, en notant

$$X := \{i \in I \mid M_i \vDash R(a_1(i), \cdots, a_n(i))\} \cap \bigcap_{k=1}^{n} \{i \in I \mid a_k(i) = b_k(i)\}$$

que $X \subset \{i \in I \mid M_i \vDash R(b_1(i), \cdots, b_n(i))\}$. Par symétrie de l'énoncé et par les propriétés (F_1) et (F_2) des filtres on déduit que $\{i \in I \mid M_i \vDash R(a_1(i), \cdots, a_n(i))\} \in \mathcal{F}$ si et seulement si $\{i \in I \mid M_i \vDash R(b_1(i), \cdots, b_n(i))\} \in \mathcal{F}$. Nous venons donc de démontrer la proposition suivante :

Proposition 3.2.2. *La relation d'équivalence $\equiv_{\mathcal{F}}$ est compatible avec les fonctions et les relations de la L-structure $\mathfrak{M}$.*

Finalement, on peut définir une L-structure sur l'ensemble $\prod_{i \in I} M_i/\mathcal{F}$ des classes d'équivalences modulo $\equiv_{\mathcal{F}}$. L'égalité est donnée par $\equiv_{\mathcal{F}}$; en effet si $[a_1]_{\mathcal{F}}, \cdots, [a_n]_{\mathcal{F}} \in \prod_{i \in I} M_i/\mathcal{F}$, alors $f([a_1]_{\mathcal{F}}, \cdots, [a_n]_{\mathcal{F}}) = [f(a_1, \cdots, a_n)]_{\mathcal{F}}$ et $\prod_{i \in I} M_i/\mathcal{F} \vDash R([a_1]_{\mathcal{F}}, \cdots, [a_n]_{\mathcal{F}})$ si et seulement si $\{i \in I \mid M_i \vDash R(a_1(i), \cdots, a_n(i))\} \in \mathcal{F}$. Enfin, l'interprétation de c est donnée par $[c(i)_{i \in I}]$. La proposition 3.2.2 assure que les diverses définitions qui munissent l'ensemble $\prod_{i \in I} M_i/\mathcal{F}$ d'une L-structure ne dépendent pas du représentant choisi.

Définition 3.2.3. Si $\mathcal{F}$ est un ultrafiltre, la L-structure $\prod_{i \in I} M_i/\mathcal{F}$ est appelée *ultraproduit*. Si de plus toutes les structures M_i sont toutes égales à une même structure M, on parle d'*ultrapuissance* de M.

Nous avons vu dans la proposition 3.1.5 qu'il y a essentiellement deux types d'ultrafiltres : les ultrafiltres principaux et ceux qui contiennent le filtre de Fréchet. Soit $(M_i)_{i \in I}$ une famille de L-structure et soit $\mathcal{F}_{i_0} := \{J \subset I \mid i_0 \in J\}$ un ultrafiltre principal. Si on note $p_{i_0} \colon \prod_{i \in I} M_i \to M_{i_0}$ la projection canonique, ce morphisme est compatible à la relation d'équivalence $\equiv_{\mathcal{F}_{i_0}}$. En effet, si a, b sont des éléments de $\prod_{i \in I} M_i$ équivalents, alors $a(i_0) = b(i_0)$, en particulier leur image par p_{i_0} est la même. Le morphisme p_{i_0} induit donc un morphisme $\tilde{p}_{i_0} \colon \prod_{i \in I} M_i/\mathcal{F}_{i_0} \to M_{i_0}$, qui reste clairement surjectif, et est injectif puisque $a(i_0) = b(i_0)$ implique $[a]_{\mathcal{F}_{i_0}} = [b]_{\mathcal{F}_{i_0}}$. On en conclu que les deux ensembles $\prod_{i \in I} M_i/\mathcal{F}_{i_0}$ et M_{i_0} sont isomorphes. Ils sont aussi isomorphes en tant que structures, ce qui est un cas particulier du théorème suivant. Avec ce choix d'ultrafiltre, nous n'avons rien construit de nouveau.

Notre seul espoir d'avoir une nouvelle structure par cette méthode est donc de considérer des ultrafiltres qui contiennent le filtre de Fréchet.

Une conséquence importante du théorème de Łos, que nous allons énoncer, est que si tous les M_i sont des modèles d'une théorie T, et que $\mathcal{F}$ est un ultrafiltre alors la L-structure $\prod_{i\in I} M_i/\mathcal{F}$ est aussi un modèle de la théorie T.

Théorème 3.2.4 (Théorème de Łos)**.** *Soit $\mathcal{F}$ un filtre, $(M_i)_{i\in I}$ une famille de L-structures, et $M = \prod_{i\in I} M_i/\mathcal{F}$.*

(1) Soit $\bar{x} = (x_1, \cdots, x_n)$ un uplet de n variables, $\varphi(\bar{x})$ une formule construite uniquement à l'aide des relations atomiques et des symboles logiques $\wedge$ et $\exists$, et soit $\bar{a} = [(\bar{a}(i))_{i\in I}]_{\mathcal{F}}$ un n-uplet de M. Alors

$$M \vDash \varphi(\bar{a}) \Leftrightarrow \{i \in I \mid M_i \vDash \varphi(\bar{a}(i))\} \in \mathcal{F}.$$

(2) Si maintenant $\mathcal{F}$ est un ultrafiltre. Si $\bar{x} = (x_1, \cdots, x_n)$ un uplet de n variables, $\varphi(\bar{x})$ une formule, et $\bar{a} = [(\bar{a}(i))_{i\in I}]_{\mathcal{F}}$ un n-uplet de M. Alors

$$M \vDash \varphi(\bar{a}) \Leftrightarrow \{i \in I \mid M_i \vDash \varphi(\bar{a}(i))\} \in \mathcal{F}.$$

Démonstration. Soit $\mathcal{F}$ un filtre. La démonstration se fait par induction sur les termes et les formules. Nous allons dans un premier temps démontrer que si $t(\bar{x})$ est un terme, et $\bar{a} = (a_1, \cdots, a_n)$ un n-uplet de M, alors

$$t^{\mathfrak{M}}(\bar{a}) = [t^{\mathfrak{M}_i}(a_1(i), \cdots, a_n(i))]_{i\in I}.$$

Si le terme $t(\bar{x})$ est une constante, ou une variable, l'égalité précédente est vraie par définition. Soient $t_1(\bar{x}), \cdots, t_k(\bar{x})$ des termes pour lesquels la propriété est vérifiée, et soit f un symbole de fonction k-aire. Alors, pour $\bar{a}$ uplet de M, en notant $\bar{a}(i) = (a_1(i), \cdots, a_n(i))$

$$f^{\mathfrak{M}}(t_1^{\mathfrak{M}}(\bar{a}), \cdots, t_n^{\mathfrak{M}}(\bar{a})) \quad = [f^{\mathfrak{M}_i}(t_1^{\mathfrak{M}_i}(\bar{a}(i)), \cdots, t_n^{\mathfrak{M}_i}(\bar{a}(i)))]_{i\in I}.$$

On a donc prouvé comment les termes s'interprétaient dans la structure $\mathfrak{M}$. Nous allons maintenant procéder par induction sur les formules pour montrer le théorème de Łos. Si φ est une formule, alors le critère

$$M \vDash \varphi(\bar{a}) \Leftrightarrow \{i \in I \mid M_i \vDash \varphi(\bar{a}(i))\} \in \mathcal{F},$$

que nous nommerons (c), est vrai pour les formules atomiques par définition des ultraproduits. Si φ et ψ sont deux formules qui vérifient le critère (c), alors $\mathfrak{M} \vDash (\varphi \wedge \psi)(\bar{a})$ si et seulement si $X := \{i \in I \mid M_i \vDash \varphi(\bar{a}(i))\} \in \mathcal{F}$ et $Y := \{i \in I \mid M_i \vDash \psi(\bar{a}(i))\} \in \mathcal{F}$. Or comme $\mathcal{F}$ est un filtre, $X \cap Y \in \mathcal{F}$ si et seulement $X \in \mathcal{F}$ et $Y \in \mathcal{F}$. Or

$$X \cap Y := \{i \in I \mid M_i \vDash (\varphi \wedge \psi)(\bar{a}(i))\} \in \mathcal{F}.$$

Donc la formule $\varphi \wedge \psi$ vérifie le critère (c). Supposons maintenant le critère vérifié pour une formule $\varphi(y, \bar{x})$. Soit

$$X := \{i \in I \mid M_i \vDash \exists y\ \varphi(y, \bar{a}(i))\}.$$

Si $\mathfrak{M} \models \exists y\ \varphi(y, \bar{a})$, alors il existe $b \in M$ tel que $\mathfrak{M} \models \varphi(b, \bar{a})$. Alors par hypothèse

$$Y := \{i \in I \mid M_i \models \varphi(b(i), \bar{a}(i))\} \in \mathcal{F}.$$

Or comme $Y \subset X$, on a $X \in \mathcal{F}$. Réciproquement, si $X \in \mathcal{F}$, choisissons pour tout $i \in I$, un élément $b(i) \in M_i$, tel que si $\mathfrak{M}_i \models \exists y\ \varphi(y, \bar{a}(i))$, alors $\mathfrak{M}_i \models \varphi(b(i), \bar{a}(i))$. Alors

$$\{i \in I \mid M_i \models \varphi(b(i), \bar{a}(i))\} = X \in \mathcal{F}.$$

En posant $b = (b(i))_{i \in I} \in M$ [5], alors $\mathfrak{M} \models \varphi(b, \bar{a})$. On a donc démontré que la formule $\exists y\ \varphi(y, \bar{x})$ vérifie le critère (c). Ces considérations terminent la preuve du point (1).

Si maintenant $\mathcal{F}$ est un ultrafiltre. Pour montrer le résultat du point (2), il suffit de montrer que si $\varphi(\bar{x})$ est une formule qui vérifie le critère (c), alors il en va de même pour la formule $\neg\varphi(\bar{x})$. Posons $X = \{i \in I \mid M_i \models \varphi(\bar{a}(i))\}$, alors $\mathfrak{M} \models \neg\varphi(\bar{a})$ si et seulement si $X \notin \mathcal{F}$. Or comme $\mathcal{F}$ est un ultrafiltre [6], $X \notin \mathcal{F}$ si et seulement si $I \backslash X \in \mathcal{F}$. Or $I \backslash X = \{i \in I \mid M_i \models \neg\varphi(\bar{a}(i))\}$. Donc la formule $\neg\varphi(\bar{x})$ vérifie le critère. □

La condition d'être un ultrafiltre et non simplement un filtre est très importante dans le théorème de Łos pour garantir que toutes les formules sont vérifiées dans l'ultraproduit. En effet, si $I = \{1, 2\}$ que $\mathcal{F} = \{I\}$ (c'est bien un filtre), et que l'on choisit K et L deux corps, vérifiant en particulier la théorie des corps, alors l'énoncé $\forall x \exists y\ (x = 0 \vee xy = 1)$ est vrai dans K et L, mais pas dans $K \times L / \mathcal{F} \equiv K \times L$ qui possède des diviseurs de zéros.

3.2.2. *Compacité.* Nous allons utiliser les ultraproduits pour démontrer un théorème utilisé quelques fois dans ce document, à savoir le théorème de compacité.

Théorème 3.2.5 (Compacité)**.** *Soit Σ un ensemble d'énoncés, tel que sous-ensemble fini de Σ admette un modèle. Alors Σ admet un modèle.*

Démonstration. Considérons un ensemble Σ d'énoncés dont toute partie finie admet un modèle. Pour toute partie finie i de Σ, on note $\mathfrak{M}_i$ un modèle de i. Nous allons construire un ultraproduit à l'aide de ces $\mathfrak{M}_i$ qui vérifiera tous les énoncés de Σ. Soit I l'ensemble des parties finies de Σ et pour tout $i \in I$ notons I_i l'ensemble $\{j \in I \mid i \subset j\}$. Alors $\mathcal{F} := \{X \subset I \mid \exists i \in I; I_i \subset X\}$ est un filtre. En effet, $\varnothing \notin \mathcal{F}$, puisque pour tout $i \in I$, l'ensemble I_i n'est jamais vide. Soit X et Y des éléments de $\mathcal{F}$, de sorte que $I_i \subset X$ et $I_j \subset Y$. Alors $I_{i \cup j} \subset X \cap Y$. Enfin, si $X \subset Z$, alors $I_i \subset Z$, donc $Z \in \mathcal{F}$. L'ensemble $\mathcal{F}$ vérifie bien les propriétés des filtres. Soit $\mathcal{U}$ un ultrafiltre contenant $\mathcal{F}$. Considérons l'ultraproduit $M = \prod_{i \in I} M_i / \mathcal{U}$. Soit φ un énoncé de Σ. Alors

$$I_{\{\varphi\}} \subset \{i \in I \mid \mathfrak{M}_i \models \varphi\} \in \mathcal{F}.$$

5. On a besoin de l'axiome du choix ici.
6. C'est ici qu'être un filtre ne suffit pas

Donc par le théorème de Łos 3.2.4, on a $\mathfrak{M} \vDash \varphi$. Donc la structure $\mathfrak{M}$ est un modèle de Σ. □

4. Corps pseudo-finis

Dans ce paragraphe, nous allons étudier la théorie des corps finis. Il sera intéressant de remarquer que la propriété d'être fini ne s'exprime pas au premier ordre. En effet la formule que l'on utiliserait a priori :

$$\exists n \forall x_1 \cdots \forall x_{n+1}(x_1 = x_2 \vee x_1 = x_3 \vee \cdots \vee x_n = x_{n+1}),$$

qui signifie qu'il existe un entier n tel que si on prend $n+1$ éléments on pourra toujours en trouver deux égaux, fait intervenir un entier n qui n'a pas d'interprétation dans le modèle. De fait, la théorie des corps finis n'a pas d'énoncés exprimant que les corps considérés sont finis. On pourra donc construire des corps infinis qui satisfont la théorie des corps finis et que l'on nommera *corps pseudo-finis*. Cette construction prouvera alors que la propriété "d'être fini" n'est pas un énoncé de la théorie des corps finis. Par la suite, on donnera trois propriétés, telles que tout corps vérifiant ces trois propriétés est un corps pseudo-fini.

4.1. **Modèles de la théorie des corps finis.**

4.1.1. *Théorie des corps finis.* On considère le langage des anneaux $L_r = \{=, +, -, \cdot, 0, 1\}$. Les énoncés suivants décrivent la théorie des corps.

(1) $\forall x \forall y \forall z((x + y) + z = x + (y + z))$;

(2) $\forall x(x + 0 = 0 + x = x)$;

(3) $\forall x(x - x = 0)$;

(4) $\forall x \forall y(x + y = y + x)$;

(5) $\forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$;

(6) $\forall x(x \cdot 1 = 1 \cdot x = x)$;

(7) $\forall x \forall y \forall z(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$;

(8) $\forall x \forall y(x \cdot y = y \cdot x)$;

(9) $\forall x \exists y(x \cdot y = 1)$.

Les trois premiers énoncés décrivent la théorie des groupes, en rajoutant le quatrième on obtient la théorie des groupes abéliens. Les sept premiers énoncés décrivent la théorie des anneaux, avec le huitième on obtient les anneaux commutatifs et rajouter le dernier énoncé permet de définir la théorie des corps.

La théorie des corps finis est en fait composée de l'ensemble de tous les énoncés satisfaits dans tous les corps finis, de fait on ne donnera pas de liste explicte d'énoncés qui décrivent les corps finis.

Définition 4.1.1. Nous appellerons *corps pseudo-fini* tout modèle **infini** de la théorie des corps finis.

Rappelons maintenant deux propriétés des corps finis qui nous seront utiles pour caractériser les corps pseudo-finis.

Proposition 4.1.2. *Soit F un corps fini.*

(P_1) Le corps F est parfait.

(P_2) Pour tout entier n strictement positif, le corps F possède exactement une extension algébrique de degré n.

Démonstration. (P_1) On note $q = p^m$ le cardinal du corps fini F. Alors le corps F est isomorphe à $\mathbf{F}_q$. On sait que le corps $\mathbf{F}_q$ est parfait, car le morphisme de Frobenius de $\mathbf{F}_q$ dans $\mathbf{F}_q$ défini par $x \mapsto x^p$ est surjectif. (P_2) Une extension de degré n de $\mathbf{F}_q$ est isomorphe à $\mathbf{F}_{q^n}$. Donc le corps F a bien une unique extension algébrique de degré n. □

4.1.2. *Exemple de corps pseudo-fini.* Cet exemple est naturel une fois le théorème de Łos connu. On note $\mathcal{Q}$ l'ensemble des nombres premiers et de leurs puissances. Soit $\mathcal{U}$ un ultrafiltre **non principal** sur $\mathcal{Q}$. On considère l'ultraproduit dont l'ensemble sous-jacent est $\prod_{q\in\mathcal{Q}} \mathbf{F}_q/\mathcal{U}$. On a vu dans le paragraphe 3.2.1 que cet ultraproduit est une structure du langage des anneaux et le théorème de Łos nous assure qu'il vérifie tous les énoncés de la théorie des corps finis. Il s'agit donc d'un corps pseudo-fini, à condition qu'il soit infini.

Proposition 4.1.3. *Avec les notations précédentes, si $\mathcal{U}$ est un ultrafiltre non principal alors le corps $\prod_{q\in\mathcal{Q}} \mathbf{F}_q/\mathcal{U}$ est infini.*

Démonstration. On se fixe un entier naturel $n > 1$. La formule qui énonce qu'il existe au moins n éléments distincts est vérifiée dans tous les corps $\mathbf{F}_q$ sauf pour un nombre fini de q. Comme un ultrafiltre non principal contient le filtre de Frechet, alors

$$\{q \in \mathcal{Q} \mid \mathbf{F}_q \text{ contient au moins } n \text{ éléments distincts}\} \in \mathcal{U}.$$

Par le théorème de Łos, cela implique que le corps $\prod_{q\in\mathcal{Q}} \mathbf{F}_q/\mathcal{U}$ vérifie aussi cet énoncé. Ainsi, en choisissant des entiers n de plus en plus grand, on en déduit que le corps $\prod_{q\in\mathcal{Q}} \mathbf{F}_q/\mathcal{U}$ contient une infinité d'éléments. □

4.2. **Propriétés des corps pseudo-finis.** Nous allons donner trois propriétés que vérifient les corps pseudo-finis. Nous verrons de plus que ces trois propriétés sont des formules du langage des anneaux. Soit F un corps pseudo-fini, alors il vérifie :

(P_1) Le corps F est parfait ;

(P_2) Pour tout entier n strictement positif, le corps F a exactement une extension algébrique de degré n ;

(P_3) Toute variété V définie sur F a un point F-rationnel, c'est-à-dire un point dont toutes les coordonnées sont dans F.

La notion de variété est définie dans l'annexe 4.3 mais dans le cadre qui nous intéresse on pourra se contenter de la remarque 2 de cette annexe.

Dans la suite, nous allons démontrer qu'un modèle infini de la théorie des corps pseudo-finis vérifie les trois propriétés. Il existe aussi une réciproque, que nous nous contenterons d'énoncer.

Théorème 4.2.1. *Soit F un corps vérifiant les propriétés (P_1), (P_2) et (P_3). Alors, F est un modèle infini de la théorie des corps finis. De plus, il est élémentairement équivalent à un ultraproduit de corps finis.*

Démonstration. Une référence pour ce théorème est le livre de James Ax [1], *The Elementary Theory of Finite Fields.* □

Pour ce qui est des propriétés (P_1) et (P_2), elles sont vérifiés par tous les corps finis, donc elles sont aussi vérifiées par tout corps pseudo-fini F, puisque les corps pseudo-fini sont des modèles infini de la théorie des corps finis.

La propriété (P_3) n'est pas vérifié pour les corps finis. Si $\mathbf{F}_q$ est un corps fini, alors la variété définie par l'équation

$$y \prod_{0 \leqslant i < j \leqslant q} (x_i - x_j) = 1,$$

n'a pas de point $\mathbf{F}_q$ rationnel, puisque tout $q+1$-uplet de $\mathbf{F}_q$ possède au moins deux coordonnées égales. Pour montrer que tout corps pseudo-fini vérifie (P_3) nous aurons besoin du théorème de Lang-Weil.

Théorème 4.2.2 (Théorème de Lang-Weil)**.** *Soient m, n, e des entiers positifs. Il existe une constante positive $C = C(m,n,e)$ telle que pour tout corps fini $F = \mathbf{F}_q$ et polynômes $f_1(\bar{Y}), \cdots, f_m(\bar{Y}) \in F[\bar{Y}]$ de degré total plus petit ou égal à e, avec $\bar{Y} = (Y_1, \cdots Y_n)$, si les polynômes engendrent $f_1(\bar{Y}), \cdots, f_m(\bar{Y})$ l'idéal définissant une variété V de dimension d, alors*

$$|\mathrm{card}(V \cap F^n) - q^d| \leqslant C q^{d-1/2}.$$

Remarquons en particulier que si q est supérieur à C^2, alors $V \cap F^n$ est non vide puisque

$$0 < -Cq^{d-1/2} + q^d \leqslant \mathrm{card}(V \cap F^n) \leqslant Cq^{d-1/2} + q^d.$$

Démonstration. On trouvera la démonstration de ce résultat dans l'article *Number of points of varieties in finite fields* [8] de S. Lang et A. Weil. □

Grâce à la remarque, formulons une conséquence du théorème de Lang-Weil. On se fixe un corps F (non nécessairement fini) et des entiers positifs m, n, e. Soit V une variété dont l'idéal est engendré par des polynômes $f_1(\bar{Y}), \cdots, f_m(\bar{Y})$ de degré inférieur ou égal à e à coefficients dans F. On se donne C la constante qui apparait dans le théorème de Lang-Weil alors la formule

$$(\mathrm{card}(F) < C^2) \vee (V \cap F^n \neq \varnothing)$$

est vérifiée dans tous les corps finis, c'est donc un énoncé de la théorie des corps finis. Par conséquent, elle est aussi vérifié dans les corps pseudo-finis. Ceci signifie que les corps pseudo-finis vérifient la propriété (P_3).

Remarque 1. Il est vrai que, tel quel, l'énoncé

$$(\mathrm{card}(F) < C^2) \vee (V \cap F^n \neq \varnothing)$$

n'est pas une formule du langage des anneaux. On peut cependant exprimer la première partie en disant que "tout C^2-uplet de F possède au moins deux coordonnées égales". Quant à la deuxième partie de l'énoncé, on verra dans la suite comment exprimer que l'on est une variété irréductible dans le langage des anneaux.

4.2.1. *Formules du premier ordre.* On va maintenant voir que les énoncés (P_1), (P_2) et (P_3) sont des formules qui s'expriment dans le langage des anneaux. Une première subtilité est que, si des énoncés du type "$\exists n \ldots$", lorsque n n'est pas un élément du modèle, nous sont interdits, il est parfaitement possible de fixer un entier n à l'avance et de demander qu'une propriété s'applique. En effet, on peut alors décomposer un énoncé du type "pour tout n, on peut trouver n éléments distincts" (qui est un énoncé de la théorie des corps infinis) en une infinité d'énoncés, dont les premiers seraient "on peut trouver 1 élément distinct" et "on peut trouver 2 éléments distincts" et "on peut trouver 3 éléments distincts", etc. Une théorie pouvant être composée par une infinité d'énoncés.

Ainsi, l'énoncé (P_1) peut se reformuler ainsi : pour chaque nombre premier p on considère l'énoncé "$p \neq 0 \vee \forall x \exists y (y^p - x = 0)$", qui dit que si la caractéristique est p alors tout élément admet une racine p-ième. Rappelons simplement qu'en caractéristique $p > 0$ être parfait est équivalent à la surjectivité du morphisme de Frobenius.

Pour la propriété (P_2), fixons un entier $n > 0$. Il existe une formule, que l'on notera $Irr(\bar{x})$ avec $\bar{x} = (x_1, \cdots, x_n)$, qui dans un corps F décrit les n-uplets $\bar{a}$ tels que le polynôme $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ soit irréductible. En effet, si $f(X) = g(X) \cdot h(X)$, alors les polynômes g et h sont de degré inférieur ou égal à n, et on a des relations entre les coefficients qui s'expriment dans le corps F.

Supposons montré le résultat suivant (il le sera dans le paragraphe 4.2.2) : à toute formule $\theta(\bar{y})$ avec $\bar{y} = (y_1, \cdots, y_m)$ on peut associer une formule $\theta^*(\bar{x}, \bar{y})$ avec $\bar{x} = (x_1, \cdots, x_n)$, telle que pour tout corps F et tout n-uplet $\bar{a}$ de F, si le polynôme $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ est irréductible et si $b \in F^m$ alors

$$F[X]/\langle f(X) \rangle \vDash \theta(\bar{b}) \Leftrightarrow F \vDash \theta^*(\bar{a}, \bar{b}).$$

Soit $\theta(\bar{y})$, avec $\bar{y} = (y_1, \cdots, y_n)$, l'énoncé $\exists z \; z^n + y_1 z^{n-1} + \cdots + y_n = 0$, alors on peut lui associer une formule $\theta^*(\bar{x}, \bar{y})$ comme ci-dessus. Alors considérons l'énoncé suivant :

$$\exists \bar{x} \; Irr(\bar{x}) \wedge (\forall y \; Irr(\bar{y}) \Rightarrow \theta^*(\bar{x}, \bar{y}))$$

Cet énoncé traduit le fait qu'il existe un polynôme irréductible sur F de degré n, donc une extension du corps F degré n notée E_1, et que tout autre polynôme irréductible de F de degré n admet une racine dans E_1. Ceci implique que F n'a qu'une unique extension de degré n. En effet, soit E_2 une extension de F de degré n. Comme le corps F est parfait, toute extension est séparable et le théorème de l'élément primitif implique que E_2 est engendrée par la racine α d'un polynôme irréductible g de degré n. Or d'après l'énoncé le polynôme g admet une racine dans E_1. Donc le corps E_2 s'injecte dans E_1, ils sont donc isomorphe car de même degré.

4.2.2. *Codage des extensions algébriques finies.* Soit F un corps et soit $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme irréductible à coefficients dans F. On note α une racine de ce polynôme dans une clôture algébrique. Nous allons montrer comment interpréter F dans une structure isomorphe à $F[\alpha]$. Prenons comme base du F-espace vectoriel $F(\alpha)$ la base $\{1, \alpha, \cdots, \alpha^{n-1}\}$. L'addition est donc définie coordonnée par coordonnée. Pour la multiplication, remarquons déjà que la multiplication par α est une transformation linéaire de l'espace vectoriel $F(\alpha)$ donnée par la matrice :

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

La multiplication par α^i est décrite par la matrice M_α^i. Nous définissons donc la multiplication de deux n-uplets de la manière suivante :

$$(x_1, \cdots, x_n)\tilde{\times}(y_1, \cdots, y_n) = (x_1\mathrm{I}_n + x_2M_\alpha + \cdots + x_nM_\alpha^{n-1}) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

La définition de $\tilde{\times}$ fait intervenir les paramètres $(a_1, \cdots, a_n)$ mais est uniforme en ces paramètres. On remarque que l'interprétation de F dans cette structure isomorphe à $F(\alpha)$ est l'ensemble des n-uplets $(a, 0, \cdots, 0)$.

On se donne une formule $\theta(\bar{y}, \alpha)$, avec $\bar{y} = (y_1, \cdots, y_m)$. Considérons la formule $\theta^*(\bar{y}, \bar{a})$, avec $\bar{x} = (x_1, \cdots, x_n)$, qui est $\theta(\bar{y}, z)$ où l'on a remplacé toutes les occurrences de α par $\bar{a}$, et où toutes les variables sont remplacés par des n-uplets de variables. Les symboles d'additions sont interprété comme l'addition coordonnée par coordonnée et la multiplication comme la multiplication $\tilde{\times}$. Enfin, les symboles de constante 0 et 1 sont remplacés par les n-uples $(0, \cdots, 0)$ et $(1, 0, \cdots, 0)$. On a alors $F(\alpha) \vDash \theta(\bar{b}, \alpha)$ si et seulement si $F \vDash \theta^*(\bar{b}, \bar{a})$.

Ainsi à l'énoncé $\theta(\bar{y})$, avec $\bar{y} = (y_1, \cdots, y_n)$, qui exprime $\exists z\ z^n + y_1z^{n-1} + \cdots + y_n = 0$, on associe l'énoncé $\theta^*(\bar{y}, \bar{a})$ qui exprime

$$\exists \bar{z} = (z_1, \cdots, z_n)\ \bar{z}^{\tilde{\times}n} + (y_1, 0, \cdots, 0)\tilde{\times}\bar{z}^{\tilde{\times}n-1} + \cdots + (y_n, 0, \cdots, 0) = (0, \cdots, 0)$$

où la notation $\bar{z}^{\tilde{\times}n}$ exprime la multiplication $\tilde{\times}$ de $\bar{z}$ par lui-même n fois.

Nous avons donc démontré le résultat suivant :

Théorème 4.2.3. *Soit n un entier naturel. Soit $\mathcal{L}_r$ le langage des anneaux. À toute $\mathcal{L}_r$ formule $\theta(\bar{y}, z)$, avec $\bar{y} = (y_1, \cdots, y_m)$, on peut associer une autre $\mathcal{L}_r$ formule $\theta(\bar{y}, \bar{x})$, avec $x = (x_1, \cdots, x_n)$, telle que pour tout corps F et tout n-uplet $\bar{a}$ de F, si le polynôme $X^n + a_1 X^{n-1} + \cdots + a_n$ est irréductible sur F, avec α une racine de ce polynôme, et $\bar{b} \in F^m$, alors*

$$F(\alpha) \vDash \theta(\bar{b}, \alpha) \Leftrightarrow F \vDash \theta^*(\bar{b}, \bar{a}).$$

Annexes

4.3. **Variétés.** Nous parlerons de variétés au sens algébrique. Le but n'étant pas l'étude précise des variétés, mais seulement de préciser le sens de la propriété (P_3) du paragraphe 4.2 nous nous contenterons d'une définition de la géométrie algébrique classique.

Dans tout ce qui suit A désignera un anneau commutatif unitaire, sauf s'il s'agit de l'anneau nul auquel cas ce sera précisé.

4.3.1. *Ensembles algébriques.* Si A est un anneau (commutatif), nous noterons $\mathrm{Spec}(A)$ l'ensemble des idéaux premiers de A. Si x est un élément de $\mathrm{Spec}(A)$, il sera parfois plus commode de noter $\mathfrak{p}_x$ au lieu de x. Soit E un sous-ensemble de A. On définit les *ensembles algébriques*

$$V(E) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid S \subset \mathfrak{p}\}.$$

Si Y est un sous-ensemble de $\mathrm{Spec}(A)$, on définit

$$\mathcal{J}(Y) := \bigcap_{y \in Y} \mathfrak{p}_y.$$

4.3.2. *Topologie de Zariski.* On peut munir l'ensemble $\mathrm{Spec}(A)$ d'une topologie en définissant les fermés comme étant les $V(E)$ pour E sous-ensemble de A. Les $V(E)$ vont se comporter comme des fermés comme l'indique la proposition suivante, où $\langle E \rangle$ désignera l'idéal engendré par E.

Proposition 4.3.1. *Si A est un anneau et que E et E' sont des sous-ensembles de A, on a :*

(1) $V(\{0\}) = \mathrm{Spec}(A)$; $V(\{1\}) = \varnothing$

(2) Si $E \subset E'$ *alors* $V(E') \subset V(E)$

(3) Pour toute famille $(E_\lambda)_\lambda$ *de parties de A, on a* $V(\cup_\lambda E_\lambda) = \cap_\lambda V(E_\lambda)$

(4) $V(\sqrt{\langle E \rangle}) = V(\langle E \rangle) = V(E)$

(5) $V(\langle E \rangle \cap \langle E' \rangle) = V(E) \cup V(E')$

Si I est un idéal la notation $\sqrt{I}$ désigne l'idéal $\{a \in A \mid \exists n \in \mathbf{N}, a^n \in I\}$ que l'on appelle le *radical* de I.

Démonstration. (1) Pour tout élément $\mathfrak{p}$ de $\mathrm{Spec}(A)$, on a $0 \in \mathfrak{p}$, et $1 \notin \mathfrak{p}$.

(2) Soit $\mathfrak{p} \in V(E')$, alors $E \subset E' \subset \mathfrak{p}$, donc $\mathfrak{p} \in V(E)$.

(3) Soit $\mathfrak{p} \in \mathrm{Spec}(A)$, alors $\mathfrak{p} \in V(\cup_\lambda E_\lambda)$ si et seulement si $\cup_\lambda E_\lambda \subset \mathfrak{p}$ si et seulement si pour tout λ on a $E_\lambda \subset \mathfrak{p}$, si et seulement si $\mathfrak{p} \in \cap_\lambda V(E_\lambda)$.

(4) Comme $\mathfrak{p}$ est un idéal, il est équivalent de demander $E \subset \mathfrak{p}$ ou $\langle E \rangle \subset \mathfrak{p}$. De plus, comme l'idéal $\mathfrak{p}$ est premier, on a $\sqrt{\mathfrak{p}} = \mathfrak{p}$, ce qui prouve qu'il est équivalent de demander $\langle E \rangle \subset \mathfrak{p}$ ou $\sqrt{\langle E \rangle} \subset \mathfrak{p}$.

(5) Par (2), on sait $V(E) \cup V(E') \subset V(\langle E \rangle \cap \langle E' \rangle)$. Réciproquement si $\mathfrak{p} \in V(\langle E \rangle \cap \langle E' \rangle)$ et si $\mathfrak{p} \notin V(E)$ et $\mathfrak{p} \notin V(E')$, alors il existe $x, y \notin \mathfrak{p}$ avec $x \in \langle E \rangle$ et $y \in \langle E' \rangle$ mais alors $xy \in \langle E \rangle \cap \langle E' \rangle$, donc $xy \in \mathfrak{p}$. Or l'idéal $\mathfrak{p}$ est premier, donc $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Contradiction. □

Définition 4.3.2. La topologie sur $\mathrm{Spec}(A)$ où les fermés sont les $V(E)$ lorsque E parcourt les parties de A s'appelle la *topologie de Zariski*.

4.3.3. *Espaces irréductibles.* Soit X un espace topologique, alors il est dit *irréductible* s'il n'est pas la réunion de deux fermés propres (c'est-à-dire strictement inclus dans X). Par passage au complémentaire, c'est équivalent de demander que deux ouverts non vide de X ne soient jamais disjoints.

Définition 4.3.3 (Variété)**.** Si A est un anneau, on appellera *variété* tout fermé irréductible de $\mathrm{Spec}(A)$. C'est-à-dire un ensemble $V(I)$, où I est un idéal de A, tel que si $V(I) \subset Y \cup Y'$ avec Y et Y' deux fermés de $\mathrm{Spec}(A)$, alors $V(I) \subset Y$ ou $V(I) \subset Y'$.

4.3.4. *Cas des anneaux de polynômes.* Dans tout ce qui suit F désignera un corps et K un corps algébriquement clos qui contient F.

Soit l'anneau de polynômes $F[X_1, \cdots, X_n]$ en n variables et donnons-nous un idéal I de cet anneau. Considérons

$$Z(I) = \{x \in K^n \mid f(x) = 0,\ \forall f \in I\}$$

le sous-ensemble de K^n, lieu d'annulation de tous les polynômes de I. C'est intuitivement ainsi qu'on a l'habitude de se représenter des courbes. Par exemple, si I est l'idéal engendré par le polynôme $X - Y$ de $K[X, Y]$, cela est usuellement représenté par une droite lorsque F est le corps des réels $\mathbf{R}$.

Le Nullstellensatz va nous permettre de faire le lien entre l'ensemble $V(I)$ défini précédemment et $Z(I)$.

Lemme 4.3.4. *Soit I un idéal propre de $K[X_1, \cdots, X_n]$, alors $Z(I)$ est non vide.*

Démonstration. Soit M un idéal maximal contenant I. Le théorème de Krull en assure l'existence puisque l'idéal I est propre. Alors $K[X_1, \cdots, X_n]/M$ est une extension du corps K. On peut plonger le corps $K[X_1, \cdots, X_n]/M$ dans un corps algébriquement clos, que nous noterons L. Il existe dans le corps $K[X_1, \cdots, X_n]/M$, et donc dans L, un uplet $(a_1, \cdots, a_n)$ qui annule tous les polynômes dans M, et en particulier dans I. Comme l'anneau $K[X_1, \cdots, X_n]$ est noéthérien, l'idéal M est engendré par un nombre fini d'éléments, disons

$f_1, \cdots, f_m$. La formule $\psi : \exists \bar{a}\ (\wedge_i (f_i(\bar{a}) = 0))$ est vérifié dans L. Comme la théorie ACF est modèle complète, alors $K \prec L$, donc la formule ψ est aussi vérifiée dans K. Ce qui signifie l'ensemble $Z(M) = \{x \in K^n \mid f(x) = 0,\ \forall f \in M\}$ est non vide. □

Théorème 4.3.5 (Nullstellensatz)**.** *Soit K un corps algébriquement clos. Soit M un idéal maximal de l'anneau de polynômes $K[X_1, \cdots, X_n]$, alors il existe un uplet $a_1, \cdots, a_n$ d'éléments de K tel que M soit l'idéal $\langle X_1 - a_1, \cdots, X_n - a_n \rangle$.*

Démonstration. Soit M un idéal maximal de $K[X_1, \cdots, X_n]$. D'après le lemme 4.3.4, il existe un élément $(a_1, \cdots, a_n)$ de $Z(M)$. Soit f un polynôme dans M. Par division euclidienne successives, il existe des polynômes $(h_i)_{1 \leqslant i \leqslant n}$ de $K[X_1, \cdots, X_n]$ et une constante c de K tels que l'on puisse écrire $f = \sum_{i=1}^{n} (X_i - a_i)h_i + c$. Le polynôme f s'annule sur tous les éléments de $Z(M)$, en particulier il s'annule sur $(a_1, \cdots, a_n)$. L'on en déduit que la constante c est nulle, donc on a l'inclusion d'idéaux $M \subset \langle X_1 - a_1, \cdots, X_n - a_n \rangle$. Par maximalité de l'idéal M, cette inclusion est une égalité. On a bien $M = \langle X_1 - a_1, \cdots, X_n - a_n \rangle$. □

On déduit du Nullstellensatz, que si K est un corps algébriquement clos, et I un idéal propre $K[X_1, \cdots, X_n]$, alors il existe une bijection entre K^n et les idéaux maximaux de $K[X_1, \cdots, X_n]$. De manière plus forte, on peut aussi en déduire l'existence d'une bijection entre $Z(I)$ et les idéaux maximaux de $K[X_1, \cdots, X_n]/I$.

Remarque 2. Bien qu'on perde en généralité, on pourra voir, dans le cas des anneaux de polynômes, une variété, comme étant le lieu d'annulation d'un ensemble de polynômes S de $K[X_1, \cdots, X_n]$, dont l'idéal engendré par S est premier.

On dira aussi que la variété $Z(\langle S \rangle)$ est définie sur F (où F est un sous-corps de K) si $Z(\langle S \rangle \cap F[X_1, \cdots, X_n]) = Z(\langle S \rangle)$.

4.4. **Bornes pour les idéaux de polynômes.** Ce paragraphe concerne l'existence de bornes pour les idéaux de polynômes. Les théorèmes énoncés ici nous permettrons d'exprimer par une formule du premier ordre qu'un idéal est premier, ou qu'une variété est irréductible.

Nous commencerons par définir la notion de degré d'un polynôme à n variables. Pour cela définissons le degré du monôme $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ comme égal à $i_1 + i_2 + \cdots i_n$. Un polynôme f en plusieurs variables est une somme finie de monômes. On définira le degré du polynôme f comme étant le maximum du degré des monômes qui apparaissent dans l'expression de f avec un coefficient non nul.

Théorème 4.4.1. *Soient n, e des entiers positifs, et $\bar{X} = (X_1, \cdots, X_n)$.*

(1) Il existe une constante $A = A(n, e)$ telle que pour tout corps K et tous polynômes $f_1(\bar{X})), \cdots, f_m(\bar{X}), g(\bar{X}) \in K[\bar{X}]$ de degré inférieur ou égal

à e, si $g(\bar{X}) \in \langle f_1(\bar{X})), \cdots, f_m(\bar{X})\rangle$ *(l'idéal de* $K[\bar{X}]$ *engendré par les polynômes* $f_1(\bar{X})), \cdots, f_m(\bar{X})$*), alors*

$$g(\bar{X}) = f_1(\bar{X})h_1(\bar{X}) + \cdots + f_m(\bar{X})h_m(\bar{X})$$

avec des polynômes $h_1(\bar{X}), \cdots, h_m(\bar{X})$ *de degré inférieur ou égal à* A*.*

(2) Il existe une constante $B = B(n, e)$ *telle que pour tout corps* K *et pour tout idéal* I *de* $K[\bar{X}]$ *engendré par des polynômes de degré inférieur ou égal à* e*, s'il existe* k *tel que* $g(\bar{X})^k \in I$*, alors* $g(\bar{X})^B \in I$*.*

(3) Il existe une constante $C = C(n, e)$ *telle que pour tout corps* K *et pour tous idéaux* I *et* J *de* $K[\bar{X}]$ *engendrés par des polynômes de degré inférieur ou égal à* e*, les idéaux* $I \cap J$ *et* $I : J := \{f \in K[\bar{X}] \mid fJ \subset I\}$ *sont engendrés par des polynômes de degré inférieur ou égal à* C*.*

(4) Il existe une constante $D = D(n, e)$ *telle que pour tout corps* K *et pour tout idéal* I *de* $K[\bar{X}]$ *engendré par des polynômes de degré inférieur ou égal à* e*, si l'idéal* I *n'est pas premier, alors il existe des polynômes* $g(\bar{X}), h(\bar{X})$ *de degré inférieur ou égal à* D *tels que* $g(\bar{X}) \notin I$ *et* $h(\bar{X}) \notin I$ *mais* $g(\bar{X})h(\bar{X}) \in I$*.*

(5) Il existe une constante $E = E(n, e)$ *telle que pour tout corps* K *et pour tout idéal* I *de* $K[\bar{X}]$ *engendré par des polynômes de degré inférieur ou égal à* e*, il existe au plus* E *idéaux premiers minimaux contenant* I *et tous sont engendrés par des polynômes de degré inférieur ou égal à* E*.*

Démonstration. On trouvera une démonstration de ces énoncés dans l'article [6] de L. van den Dries et K. Schmidt. □

Ces résultats vont permettre d'exprimer à l'aide de formules dont les variables sont les coefficients des polynômes l'appartenance d'un polynôme à un idéal, le fait que cet idéal soit premier, radical, etc. On se fixe r, n, e des entiers positifs et on note $M(n, e)$ l'ensemble des monômes de $K[\bar{X}]$ de degré inférieur ou égal à e. Donnons deux applications du théorème précédent

Proposition 4.4.2. *Soient* n, r, e *des entiers naturels.*

(1) Il existe une formule $\alpha(\bar{x}_1, \cdots, \bar{x}_r, \bar{x}_{r+1})$ *avec* $\bar{x}_i = (x_{i,m})_{m \in M(n,e)}$*, telle que pour tout corps* K*, si* $f_i(\bar{X}) = \sum_{m \in M(n,e)} a_{i,m} m \in K[\bar{X}]$ *alors*

$$f_{r+1}(\bar{X}) \in \langle f_1(\bar{X}), \cdots, f_r(\bar{X})\rangle \Leftrightarrow K \vDash \alpha(\bar{a}_1, \cdots, \bar{a}_r, \bar{a}_{r+1}).$$

(2) Il existe une formule $\beta(\bar{x}_1, \cdots, \bar{x}_r, \bar{x}_{r+1})$ *avec* $\bar{x}_i = (x_{i,m})_{m \in M(n,e)}$*, telle que pour tout corps* K *si* $f_i(\bar{X}) = \sum_{m \in M(n,e)} a_{i,m} m \in K[\bar{X}]$ *alors*

$$\langle f_1(\bar{X}), \cdots, f_r(\bar{X})\rangle \text{ est premier} \Leftrightarrow K \vDash \beta(\bar{a}_1, \cdots, \bar{a}_r, \bar{a}_{r+1}).$$

Démonstration. (1) Le polynôme $f_{r+1}(\bar{X})$ est dans l'idéal $\langle f_1(\bar{X}), \cdots, f_r(\bar{X})\rangle$ si et seulement s'il existe des polynômes $h_1(\bar{X}), \cdots, h_r(\bar{X})$ de degré inférieur ou égal à A, par le théorème 4.4.1, tels que $f_{r+1}(\bar{X}) = f_1(\bar{X})h_1(\bar{X}) + \cdots + f_r(\bar{X})h_r(\bar{X})$. On peut traduire cette égalité en terme de coefficients apparaissant devant chaque monôme. Les monômes apparaissant sont de degré

inférieur ou égal à $e + A$, ce qui permet de traduire l'égalité polynômiale comme une conjonction d'équations à vérifier dans K. Il existe donc une formule $\psi(\bar{x}_1, \cdots, \bar{x}_r, \bar{x}_{r+1}, \bar{y}_1, \cdots, \bar{y}_r)$ qui est une conjonction d'équations, telle que pour tout corps K et uplets $\bar{a}_1, \cdots, \bar{a}_r, \bar{a}_{r+1}$ et $\bar{b}_1, \cdots, \bar{b}_r$, où $\bar{a}_i = (a_{i,m})_{m \in M(n,e)}$ et $\bar{b}_i = (b_{i,m})_{m \in M(n,A)}$, on a, pour $f_i(\bar{X}) = \sum_{m \in M(n,e)} a_{i,m} m$ et $h_i(\bar{X}) = \sum_{m \in M(n,A)} b_{i,m} m$,

$$\begin{array}{c} f_{r+1}(\bar{X}) = f_1(\bar{X})h_1(\bar{X}) + \cdots + f_r(\bar{X})h_r(\bar{X}) \\ \Updownarrow \\ K \vDash \psi(\bar{a}_1, \cdots, \bar{a}_r, \bar{a}_{r+1}, \bar{b}_1, \cdots, \bar{b}_r) \end{array}$$

Nous prendrons pour α la formule $\exists (\bar{y}_i)_{1 \leqslant i \leqslant r}\ \psi(\bar{x}_1, \cdots, \bar{x}_r, \bar{x}_{r+1}, \bar{y}_1, \cdots, \bar{y}_r)$.

(2) Les formules construites en (1) dépendant en fait des entiers n, e, r, pour le signifier, on notera la formule α aussi $\alpha_{n,e,r}$. Soit D la constante du point (4) du théorème 4.4.1. La formule $\beta(\bar{x}_1, \cdots, \bar{x}_r, \bar{x}_{r+1})$ est obtenue en traduisant au premier ordre : Pour tout $\bar{y} = (y_m)_{m \in M(n,D)}$, pour tout $\bar{z} = (z_m)_{m \in M(n,D)}$, si $\bar{t} = (t_m)_{m \in M(n,2D)}$ est la suite des coefficients du polynôme $(\sum_{m \in M(n,D)} y_m m)(\sum_{m \in M(n,D)} z_m m)$, alors

$$\alpha_{n,2D,r}(\bar{x}_1, \cdots, \bar{x}_r, \bar{t}) \Rightarrow (\alpha_{n,D,r}(\bar{x}_1, \cdots, \bar{x}_r, \bar{y}) \vee \alpha_{n,D,r}(\bar{x}_1, \cdots, \bar{x}_r, \bar{z})).$$

La formule signifiant qu'en notant I l'idéal considéré, si $\sum_{m \in M(n,2D)} t_m m \in I$ implique que $\sum_{m \in M(n,D)} y_m m \in I$ ou $\sum_{m \in M(n,D)} z_m m \in I$. □

Références

1. J. Ax, *The elementary theory of finite fields*, vol. 88, Annals of Mathematics, September 1968.
2. Zoé Chatzidakis, *Cours de 3ème cycle : Théorie des modèles des corps finis et pseudo-finis*, 1996.
3. Lascar D. Cori R., *Logique mathematique, tome 1. calcul propositionnel, algebre de boole, calcul des predicats*, Dunod, 2003.
4. ———, *Logique mathematique, tome 2. fonctions recursives, theorie des modeles*, Dunod, 2003.
5. Marker D., *Model theory an introduction*, Springer, 2002.
6. K. Schmidt L. van den Dries, *Bounds in the theory of polynomial rings over fields. a nonstandard approach.*, Inventiones mathematicae **76** (1984), 77–92.
7. François Loeser, *Notes de cours : un premier cours de logique*, 2010.
8. A. Weil S. Lang, *Number of points of varieties in finite fields*, J. of Math **76** (1954), 819 –827.