Rentrée de Majeure, École Polytechnique, (Septembre 2005)

E. Bouscaren

Introduction à la Théorie des modèles

Notes complémentaires au cours

1 Introduction

La "théorie des modèles" est une branche de la Logique Mathématique qui est encore assez mal connue, malgré ses nombreuses applications en algèbre et en géométrie.
Nous allons essayer, lors de ces quelques exposés, de donner une introduction aux notions de base de théorie des modèles en évitant le formalisme général abstrait et en regardant tout de suite quelques applications à la théorie des corps algébriquement clos.
Notre "but" principal sera de démontrer, en utilisant la théorie des modèles, un théorème classique:

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

(L'application f est polynomiale c'est-à-dire:

$$f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots f_n(x_1, \ldots, x_n))$$

avec, pour chaque i, $f_i \in \mathbb{C}[X_1, \ldots, X_n]$.)

On va présenter une démonstration de ce théorème qui utilise les notions de base de la théorie des modèles (formules du premier ordre, théorème de compacité) et passe par des théorèmes de transfert de propriétés d'une classe de corps à une autre.

En fait le théorème, énoncé ainsi, est seulement un cas particulier du Théorème d'Ax, qui considère les endomorphismes des variétés algébriques (et en fait des schémas de type fini ([Ax])). Le cas particulier de l'espace affine tout entier, c'est-à-dire $\mathbb{C}^n$ avait déjà été remarqué dans [BB-R]. Il y a eu depuis plusieurs autres démonstrations, par exemple Borel ([Bor]) utilisant la cohomologie et Rudin ([Rud]) qui donne une nouvelle preuve pour $\mathbb{C}^n$.

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

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

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

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

1.1 Les corps finis

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

1.2 Les corps localement finis

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

Lemme 2 *Les corps localement finis satisfont le Théorème d'Ax.*

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

1.3 Clôture algébrique de $\mathbb{F}_p$

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

Nous avons remarqué dans la section précédente que tout corps localement fini satisfaisait Ax, donc, *pour tout premier p, $\overline{\mathbb{F}_p}$ satisfait le théorème d'Ax.*

1.4 Propriétés de transfert

Après ces remarques élémentaires, on invoque la théorie des modèles pour conclure directement car

Théorème 3 *Si une propriété qui s'exprime par un "énoncé du premier ordre" est vraie dans la clôture algébrique de $\mathbb{F}_p$ pour tout p premier, elle est vraie dans $\mathbb{C}$.*

Dans ce petit cours, nous allons essayer de donner un sens précis à tout cela:

- définir précisément ce qu'est un **énoncé du premier ordre** et vérifier que l'énoncé du théorème d'Ax est bien de ce type.
- démontrer ce théorème de transfert, en utilisant les ultraproduits.

Ce théorème est en fait un cas particulier du théorème fondamental de la logique du premier ordre **le théorème de compacité** que l'on montrera après, en utilisant également les ultraproduits.

Il existe d'autres théorèmes de transferts classiques que nous n'aurons pas le temps de voir ici, en particulier "La complétude de la théorie des corps algébriquement clos de caractéristique fixée" : tout énoncé du premier ordre qui est vrai dans un corps algébriquement clos est vrai dans tout corps algébriquement clos de même caractéristique. Ici nous avons choisi une preuve du théorème d Ax qui n'utilise pas directement ce second principe de transfert.

La propriété de complétude de la théorie des corps algébriquement clos de caractéristique fixée est souvent utilisée de manière un peu informelle en géométrie algébrique sous le nom de "Principe de Lefshetz" , par exemple "si on veut montrer "quelque chose" sur un corps algébriquement clos de caractéristique zéro, il suffit de le faire pour $\mathbb{C}$".

Nous n'allons pas donner les définitions dans le cadre général qui est celui de la logique du premier ordre, ni démontrer le théorème de compacité en général. Pour éviter le formalisme et surtout pour essayer de faire tout cela dans le temps qui nous est imparti, nous allons nous placer dès le départ dans le cas particulier qui nous intéresse, c'est à dire définir ce que nous appellerons une formule du premier ordre pour la classe des anneaux commutatifs. Il s'agit là de définitions et d'un cadre "ad hoc" qui permettent d'admettre sans problèmes toute une série de détails techniques qu'il nous faudrait considérer sérieusement autrement.

2 Les formules du premier ordre pour le langage des anneaux

2.1 Définition de l'ensemble des formules

Nous allons nous placer dans la classe de tous les anneaux unitaires commutatifs. Nous avons donc des structures R munies de l' addition $+ : R \times R \mapsto R$, de la soustraction $- : R \mapsto R$, de la multiplication $. : R \times R \mapsto R$ et de deux éléments distingués, 0 et 1.
On va définir par induction l'ensemble $\mathcal{F}orm = \bigcup_n \mathcal{F}_n$, des **formules du premier ordre** du langage des anneaux, et la **satisfaction** d'une telle formule dans la classe à laquelle nous nous sommes restreints, c'est-à-dire les anneaux commutatifs.

On définit tout d'abord l'ensemble des formules **basiques** ou **atomiques**, $\mathcal{F}_0$: ce sont toutes les formules de la forme $P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)$ où P, Q sont des polynômes

dans $\mathbb{Z}[X_1, \ldots, X_n]$.
Les polynômes peuvent être de degré zéro par exemple "$p = 0$" est une formule, pour chaque nombre premier p.

On dira que la variable x_i est **libre** dans la formule ϕ, de la forme $P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)$ si x_i est de degré supérieur ou égal à un dans l'un des deux polynômes P ou Q.

Pour une formule ϕ de $\mathcal{F}_0$, on écrira $\phi(x_1, \ldots, x_n)$ pour indiquer, quand cela sera important, que les variables libres dans ϕ sont parmi $\{x_1, \ldots, x_n\}$.

Si R est un anneau commutatif, si $\phi(x_1, \ldots, x_n)$ est une formule de la forme "$P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)$", et si $a_1, \ldots a_n$ sont des éléments de R, on dira que "R **satisfait** la formule $\phi(a_1, \ldots, a_n)$", ou que la suite $a_1, \ldots, a_n$ satisfait la formule $\phi(x_1, \ldots, x_n)$ dans R, noté

$$R \models \phi(a_1, \ldots, a_n),$$

si, dans R, on a $P(a_1, \ldots, a_n) = Q(a_1, \ldots, a_n)$.

Il y a des formules atomiques sans variables libres: "$p = 0$", par exemple. Une telle formule est vraie ou fausse dans un anneau donné, en l'occurrence celle-ci est vraie exactement dans les anneaux de caractéristique égale à p.

On dira que le sous-ensemble de R^k, $\{(a_1, \ldots, a_k) \in R^k : R \models P(a_1, \ldots, a_k) = 0\}$ est "défini" ou "définissable" par la formule ϕ. Grâce aux formules basiques on obtient, pour chaque anneau R, et pour chaque n, certains fermés de Zariski (de forme particulièrement simple).

On définit maintenant $\mathcal{F}_{n+1}$.
Les formules ϕ de $\mathcal{F}_{n+1}$ sont de l'une des cinq formes suivantes:

- soit $\phi \in \mathcal{F}_n$
- soit ϕ est de la forme $(\phi_1 \wedge \phi_2)$ (lu "ϕ_1 et ϕ_2", ou aussi ϕ_1 conjonction ϕ_2), pour $\phi_1, \phi_2 \in \mathcal{F}_n$,
- soit ϕ est de la forme $(\phi_1 \vee \phi_2)$ (lu "ϕ_1 ou ϕ_2", ou aussi ϕ_1 disjonction ϕ_2) pour $\phi_1, \phi_2 \in \mathcal{F}_n$,
- soit ϕ est de la forme $\neg\psi$ (lu "non ψ", ou aussi négation de ψ), pour $\psi \in \mathcal{F}_n$,
- soit ϕ est de la forme $\exists x\, \psi$ (lu "il existe x ψ", $\exists$ est le quantificateur existentiel), pour $\psi \in \mathcal{F}_n$
- soit ϕ est de la forme $\forall x\, \psi$ (lu "pour tout x ψ", $\forall$ est le quantificateur universel), pour $\psi \in \mathcal{F}_n$.

On dira que x est une *variable libre* de $(\phi_1 \wedge \phi_2)$, ou de $(\phi_1 \vee \phi_2)$, si x est une variable libre de ϕ_1 ou si x est une variable libre de ϕ_2. On dira que x est une variable libre de $\neg\psi$ si x est une variable libre de ψ. On dira que x est une variable libre de $\exists y\psi$, ou de $\forall y\psi$, si x est une variable libre de ψ, mais x n'est jamais une variable libre de $\exists x\psi$, ni de $\forall x\psi$. Par exemple , x et z sont les variables libres de la formule "$\exists y(y^3 = x \wedge \neg(z^5 = x))$", mais z est la seule variable libre de la formule "$\exists x\, \exists y(y^3 = x \wedge \neg(z^5 = x))$".

On définit maintenant *la satisfaction* pour une formule $\phi(x_1, \ldots, x_n)$ de $\mathcal{F}_{n+1}$. Il n'y a pas de surprises, ce sont les définitions que l'on attend. Soit donc R un anneau commutatif, et $a_1, \ldots, a_n$ une suite d'éléments de R:

- $R \models (\phi_1 \wedge \phi_2)(a_1, \ldots, a_n)$ ssi $R \models \phi_1(a_1, \ldots, a_n)$ *et* $R \models \phi_2(a_1, \ldots, a_n)$.
- $R \models (\phi_1 \vee \phi_2)(a_1, \ldots, a_n)$ ssi $R \models \phi_1(a_1, \ldots, a_n)$ *ou* $R \models \phi_2(a_1, \ldots, a_n)$

- $R \models \neg\phi_1(a_1, \ldots, a_n)$ ssi R ne satisfait pas $\phi_1(a_1, \ldots, a_n)$, noté $R \not\models \phi_1(a_1, \ldots, a_n)$
- $R \models \exists y\, \psi(y, a_1, a_2, \ldots, a_n)$ ssi il existe $b \in R$ tel que $R \models \psi(b, a_1, a_2, \ldots, a_n)$
- $R \models \forall y\, \psi(y, a_1, a_2, \ldots, a_n)$ ssi pour tout élément b de R , on a $R \models \psi(b, a_2, \ldots, a_n)$.

L'ensemble des **formules du premier ordre** $\mathcal{F}orm := \bigcup_{n\geq 0} \mathcal{F}_n$. C'est donc la clôture de l'ensemble des formules atomiques par cinq opérations: la conjonction, la négation, la disjonction, la quantification existentielle, la quantification universelle (cette définition est en fait redondante, il suffit d'avoir la négation, la conjonction et le quantificateur existentiel, grâce aux équivalences habituelles qui expriment la disjonction et le quantificateur universel à partir des trois précédents). Au niveau des sous-ensembles définissables cela correspond à clore par intersection finie, réunion finie, complémentaire et projection.

Il est important de remarquer que les formules sont obtenues à partir d'un nombre **fini** d'opérations, et que pour vérifier la satisfaction d'une formule dans un anneau R, on remplace les variables par des **éléments** de R, jamais par des sous-ensembles. Ce sont ces deux propriétés qui caractérisent la logique du **premier ordre**.

Il est également important de réaliser que pour que toutes ces définitions marchent bien, il y aurait un certain nombre de lemmes techniques à vérifier, et de conventions d'écriture à définir. Ici, on se permet de ne pas le faire car on utilise l'intuition que nous avons tous de ce qu'est un polynôme dans un anneau commutatif, et les conventions habituelles de notation sur les indéterminées ou les variables dans ce cas. Mais il faudrait en particulier vérifier que l'on a bien un lemme de "lecture unique" pour les formules, qui permet d'assurer qu'une formule ϕ ne peut pas être obtenue de deux manières différentes dans la construction des $\mathcal{F}_n$. On définit alors la **complexité** de la formule ϕ comme l'unique n tel que $\phi \in \mathcal{F}_n$ et $\phi \notin \mathcal{F}_m$, pour $m < n$. Le lemme de lecture unique nous assure alors que l'on peut définir des fonctions sur $\mathcal{F}orm$ par induction sur la complexité des formules, ou même, tout simplement, que l'ensemble des variables libres d'une formule est vraiment bien défini.

Quelques premiers exemples: $\mathbb{R} \not\models \exists x(x^2 = -1)$, mais $\mathbb{C} \models \exists x(x^2 = -1)$. Un anneau R satisfait la formule $\forall x\,(x = 0) \vee (\exists y\, xy = 1)$ si et seulement si R est un corps.
Si p est un nombre premier, $R \models$ "$p = 0$" ssi R est de caractéristique égale à p.

Il est facile de vérifier, par induction sur la complexité des formules, qu'elles sont préservées par isomorphisme (d'anneau):

Lemme 4 *Si f est un isomorphisme (d'anneau) de R sur R', si $\phi(x_1, \ldots, x_n)$ est une formule, alors pour tous $a_1, \ldots, a_n \in R$,*

$$R \models \phi(a_1, \ldots, a_n) \text{ ssi } R' \models \phi(f(a_1), \ldots, f(a_n)).$$

On introduit quelques notations habituelles:
- on s'autorisera à écrire $P(x_1, \ldots, x_n) \neq Q(x_1, \ldots, x_n)$ à la place de $\neg((P(x_1, \ldots, x_n) = Q(x_1, \ldots, x_n)))$
- On note $(\phi \to \psi)$ la formule $(\neg\phi \vee \psi)$; on note $(\phi \leftrightarrow \psi)$ la formule $((\phi \to \psi) \wedge (\psi \to \phi))$.

Définition: Deux formules, $\phi_1(x_1, \ldots, x_n)$ et $\phi_2(x_1, \ldots, x_n)$ sont **équivalentes** (pour la classe des anneaux commutatifs) si, pour tout anneau commutatif R, et toute suite

$a_1, \ldots, a_n$ d'éléments de R,

$$R \models \phi_1(a_1, \ldots, a_n) \text{ ssi } R \models \phi_2(a_1, \ldots, a_n).$$

On remarque que $\phi_1(x_1, \ldots, x_n)$ et $\phi_2(x_1, \ldots, x_n)$ sont équivalentes si et seulement si, pour tout anneau R,

$$R \models \forall x_1 \ldots \forall x_n \, (\phi_1(x_1, \ldots, x_n) \leftrightarrow \phi_2(x_1, \ldots, x_n)).$$

Les équivalences dont on a l'habitude sont bien sûr vraies, par exemple: $(\phi_1 \vee \phi_2)$ est équivalente à $\neg(\neg\phi_1 \wedge \neg\phi_2)$, $\forall x \phi$ est équivalente à $\neg \exists x \neg\phi$ ...

AUTRES LANGAGES: Comme cela a déjà été dit plus haut, nous nous sommes placés dans un cas particulier qu départ, le langage des anneaux. En théorie des modèles on définit en fait les formules du premier ordre, et la satisfaction pour des langages quelconques. Un langage est la donnée du "type" d'opérations et de relations que l'on s'autorise à utiliser pour construire les formules atomiques. Ensuite l'ensemble de toutes les formules est construit à partir des formules atomiques exactement comme nous l'avons fait ici.

Par exemple, si la classe de structures que l'on veut étudier est celle des anneaux commutatifs ordonnés, en plus des opérations d'addition et de multiplication on utilisera la relation d'ordre. Les formules atomiques dans ce cas sont les expressions de la forme

$$P(X_1, \ldots, X_n) = Q(X_1, \ldots X_n)$$

et aussi celles de la forme

$$P(X_1, \ldots, X_n) < Q(X_1, \ldots X_n).$$

Si l'on s'intéresse aux groupes (non nécessairement commutatifs), on prendra juste la loi de groupe, l'inverse et l'élément neutre. Les formules atomiques à n variables libres seront les identités du type

$$\Pi_{1 \leq i \leq n}(x_i)^{e_{1,i}} \ldots \Pi_{1 \leq i \leq n}(x_i)^{e_{k,i}} = 1$$

avec $k \geq 1$, et $e_{j,i} \in \mathbb{Z}$, pour $1 \leq j \leq k$ et $1 \leq i \leq n$.

Il doit être facile d'imaginer que tous les théorèmes généraux que nous allons démontrer dans la suite (définition des ultraproduits et théorème de Łos, théorème de compacité, critères d'élimination des quantificateurs) sont vrais dans le contexte général avec les mêmes démonstrations.

Nous revenons maintenant au langage des anneaux pour la suite.

2.2 Exemples, théories, modèles

Définitions et remarques: Une formule sans variable libre est appelée un **énoncé**. Un énoncé est soit vrai, soit faux dans un anneau donné (et pas les deux en même temps!). Si l'anneau R satisfait l'énoncé θ, on dira que R est un **modèle** de θ. Si Σ est un ensemble

d'énoncés et si R est modèle de chacun des énoncés de Σ, on dira que R est modèle de Σ, noté $R \models \Sigma$.
Un ensemble (éventuellement infini) d'énoncés qui a un modèle sera appelé **une théorie**.

On dit que θ est **conséquence** de Σ si tout modèle de Σ est également modèle de θ, noté $\Sigma \vdash \theta$.

Regardons tout de suite quelques exemples qui vont permettre de comprendre ce que l'on peut exprimer dans la logique du premier ordre et ce que l'on ne peut pas exprimer. Les modèles de l'énoncé $\Theta_c := \forall x\,(x = 0) \vee (\exists y\, x.y = 1)$ sont exactement les anneaux commutatifs qui sont des corps.

Si p est un nombre premier, les modèles de l'énoncé $\sigma_p :=$ "$p = 0$" sont exactement les anneaux commutatifs de caractéristique p.

Les modèles de $\Sigma := \{\theta_c, \sigma_p\}$ (ou de l'énoncé "$(\theta_c \wedge \sigma_p)$" sont exactement les corps de caractéristique p.

Peut-on trouver un énoncé (du premier ordre) dont les modèles soient exactement tous les anneaux de caractéristique zéro? Si l' on essaye, on voit qu'on ne trouve pas. En revanche on peut trouver un ensemble **infini** d'énoncés qui fait l'affaire:

$$\Sigma_0 = \{\neg\sigma_p : p \text{ premier }\}.$$

Un anneau R est de caractéristique zéro si et seulement si, pour chaque p, $R \models$ "$p \neq 0$" noté $R \models \Sigma_0$.

Pour dire qu'un anneau est de caractéristique zéro, on dit donc qu'il n'est de caractéristique p pour aucun nombre premier p. Et on va voir bientôt que le théorème de compacité prouve que effectivement **il ne peut pas exister** un énoncé (ou un nombre fini d'énoncés, ce qui est la même chose) pour dire qu'un anneau est de caractéristique zéro. D'ailleurs le théorème de transfert que nous allons utiliser (Théorème 3) ne pourrait être vrai s' il existait un énoncé F disant "être de caractéristique zéro". En effet alors $\neg F$ serait vrai dans tous les $\overline{\mathbb{F}_p}$ et par le théorème devrait être vrai dans $\mathbb{C}$.

Le même problème se pose si l'on cherche un énoncé dont les modèles seraient exactement tous les anneaux finis. En revanche on peut facilement dire, pour $n \geq 2$, R a exactement n éléments:

$$G_n := \exists x_1, \ldots \exists x_n[(\bigwedge_{1\leq i<j\leq n} x_i \neq x_j) \wedge (\forall y \bigvee_{1\leq i\leq n} y = x_i)]$$

$$F_n := \exists x_1, \ldots \exists x_n(\bigwedge_{1\leq i<j\leq n} x_i \neq x_j).$$

Un anneau R est de cardinalité égale à n si et seulement si il satisfait l'énoncé G_n. Un anneau R est de cardinalité supérieure ou égale à n si et seulement si il satisfait l'énoncé F_n.

Un anneau R sera infini si et seulement si, pour tout n, $R \models F_n$. À nouveau, le théorème de compacité nous dira que l'on ne peut pas remplacer cet ensemble infini d'énoncés par un nombre fini.

Intuitivement, pour dire que R est fini, on aurait envie de dire "il existe un entier n tel que F_n", mais ceci n'est PAS un énoncé du premier ordre. Dire "il existe un entier n tel que F_n" revient à faire une disjonction infinie $\bigvee_{n\geq 1} F_n$. Ceci n'est pas un énoncé du premier ordre.

2.3 Théorie des corps algébriquement clos, théorème d'Ax

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Ultraproduits et démonstration du théorème de compacité

3.1 Théorème de compacité et conséquences

Nous allons donner la démonstration du théorème de compacité grâce aux ultraproduits un peu plus loin, mais regardons ce qu'il dit et démontrons les premières conséquences que j'ai mentionnées plus haut:

Théorème 5 (Théorème de compacité 1) *Soit Σ un ensemble d'énoncés tel que tout sous ensemble fini de Σ a un modèle. Alors Σ a un modèle.*

Voyons tout de suite une formulation équivalente :

Théorème 6 (Théorème de compacité 2) *Soit Σ un ensemble d'énoncés, et θ un énoncé. Si $\Sigma \vdash \theta$, il existe un sous-ensemble fini F de Σ tel que $F \vdash \theta$.*

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

Corollaire 7 *1. Si T est une théorie qui a des modèles finis de cardinalité arbitrairement grande (c'est-à-dire telle que, pour chaque $n \leq 1$, T a un modèle fini de cardinalité supérieure à n), alors T a un modèle infini.*

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

Corollaire 8 *Si σ est vrai dans tous les corps de caractéristique zéro, alors il existe un nombre premier q tel que σ est vrai dans tous les corps de caractéristique supérieure ou égale à q.*

Preuve: Soit $T = \{\theta_c\} \cup \{p \neq 0 \ : \ p \text{ premier}\}$. Les modèles de T sont tous les corps de caractéristique 0. Si σ est vrai dans tous les corps de caractéristique 0, alors $T \vdash \sigma$. Par le théorème de compacité 2, il existe F fini, $F \subset T$, tel que $F \vdash \sigma$. Puisque F est fini, il existe un nombre premier q tel que $F \subset \{\theta_c\} \cup \{p \neq 0 \ : \ p < q\}$. Si K est un corps de caractéristique $\geq q$, K est modèle de F, et donc aussi modèle de σ. □

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

3.2 Produits cartésiens d'anneaux

Rappelons quelques définitions et fixons quelques notations.

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

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

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

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

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

En revanche, même si les A_i sont des corps, l'anneau $\Pi_{i\in I}A_i$ ne sera jamais intègre dès que I contient au moins deux éléments distincts i_1 et i_2: en effet si on prend, a, b tels que $a(i_1) = 1$ et $a(j) = 0$ pour $j \neq i_1$, et $b(i_1) = 0$ et $b(j) = 1$ pour $j \neq i_1$, on voit que $a.b = 0$.

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

3.3 Filtres et ultrafiltres

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

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

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

Lemme 9 *Si $A \subset I$ est non vide et a la propriété de l'intersection finie, l'ensemble des parties de I qui contiennent une intersection finie d'éléments de A est un filtre, qu'on appelle le filtre engendré par A. Tout filtre a la propriété de l'intersection finie.*

Preuve: Clair □

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

Proposition 10 *1. Un filtre $\mathcal{F}$ est un ultrafiltre si et seulement si, pour tout $X \subset I$, $X \in \mathcal{F}$ ou bien $I \setminus X \in \mathcal{F}$.*
2. Tout filtre est contenu dans un ultrafiltre.

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

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

3.4 Ultraproduits

3.4.1 Cas général

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

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

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

Le lemme suivant sur les cardinalités nous sera utile:

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

Lemme 11 *Soit $(A_i)_{i\in\mathbb{N}}$ une famille d'ensembles non vides, dénombrables infinis. Soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{N}$. Alors $\Pi_{i\in I}A_i/\mathcal{F}$ est de cardinalité égale à $\mathbb{N}^{\mathbb{N}} = |\mathcal{P}(\mathbb{N}|.)$.*

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

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

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

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

Remarque: la famille d'applications E construite dans la preuve ci-dessus a également la propriété que, pour toute $f \in E$, et pour tout n, $f(n) < 2^n$. On peut en déduire de manière très semblable: soit $(A_i)_{i\in\mathbb{N}}$ une famille d'ensembles finis, mais de cardinalités non bornées, c'est-à-dire tels que, pour chaque n, $\{i \in \mathbb{N} : |A_i| \leq n\}$ est fini, et soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{N}$. Alors $\Pi_{i\in I}A_i/\mathcal{U}$ est de cardinalité égale à $|\mathcal{P}(\mathbb{N})|$.

Nous allons maintenant repasser au cas des anneaux.

3.4.2 Produits réduits et ultraproduits d'anneaux

Soit $(R_i)_{i\in I}$ une famille d'anneaux commutatifs. On a vu plus haut que, si l'on définit sur le produit cartésien de la famille, $\mathcal{R} := \Pi_{i\in I}R_i$, une addition et une multiplication coordonnée par coordonnée, $\mathcal{R}$ est un anneau commutatif.
Soit $\mathcal{F}$ un filtre sur I et $\mathcal{R}/\mathcal{F}$ le produit réduit correspondant. On définit une addition et une multiplication sur $\mathcal{R}/\mathcal{F}$ de manière compatible:

$$a_{\mathcal{F}} + b_{\mathcal{F}} := c_{\mathcal{F}} \text{ ssi } \{i \in I : a(i) + b(i) = c(i)\} \in \mathcal{F}$$

$$a_{\mathcal{F}}.b_{\mathcal{F}} := c_{\mathcal{F}} \text{ ssi } \{i \in I : a(i).b(i) = c(i)\} \in \mathcal{F}.$$

On peut vérifier que les deux opérations sont bien définies, c'est-à-dire, ne dépendent pas des représentants des classes d'équivalence, et que $\mathcal{R}/\mathcal{F}$ est toujours une anneau commutatif. Mais dans le cas des anneaux, on peut regarder les choses tout de suite de manière plus algébrique. Considérons

$$J = \{a \in \Pi_{i\in I}R_i : \text{ tels que } \{i \in I; a_i = 0\} \in \mathcal{F}\}.$$

Lemme 12 1. *J est un idéal de $\mathcal{R}$ et pour tous $a, b \in \mathcal{R}$, $a_{\mathcal{F}} = b_{\mathcal{F}}$ si et seulement si $a - b \in J$.*

2. *Si pour chaque i, R_i est un corps, et si $\mathcal{F}$ est un ultrafiltre, alors J est un idéal maximal.*

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

Théorème 13 (Théorème de Łos pour le cas des anneaux commutatifs) *Soit $(R_i)_{i \in I}$ une famille d'anneaux commutatifs et $\mathcal{U}$ un ultrafiltre sur I. Soit $\phi(x_1, \ldots, x_n)$ une formule, et $a_1, \ldots, a_n \in \Pi_{i \in I} R_i = \mathcal{R}$. Alors*

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

Preuve: On va vérifier que cela est vrai par induction sur la complexité des formules.
Pour les formules de complexité zéro, c'est-à-dire les formules atomiques, c'est immédiat si l'on se souvient qu'elles sont de la forme "$P(x_1, \ldots, x_n) = Q(x_1, \ldots x_n)$" et que $P(a_1, \ldots, a_n)(i) = P(a_1(i), \ldots, a_n(i))$. On a donc $P(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}}) = (P(a_1, \ldots, a_n))_\mathcal{U} = (Q(a_1, \ldots, a_n))_\mathcal{U}$ ssi $\{i \in I : [P(a_1, \ldots, a_n)](i) = [Q(a_1, \ldots, a_n)](i)\} \in \mathcal{U}$, c'est-à-dire, ssi

$$\{i \in I : P(a_1(i), \ldots, a_n(i)) = Q(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$$

ssi, par définition de la satisfaction pour les formules atomiques,

$$\{i \in I : R_i \models (P(a_1(i), \ldots, a_n(i)) = Q(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}.$$

On suppose maintenant que cela est vrai pour les formules de complexité k, et soit $\phi(x_1, \ldots, x_n)$ une formule de complexité $k + 1$. On doit considérer cinq cas:

(i) $\phi = \neg\psi$, avec ψ de complexité k. Alors

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

ssi, par définition de la négation,

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

ssi, par hypothèse d'induction,

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

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

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

ssi, par définition de la négation à nouveau,

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

(ii) $\phi = (\phi_1 \wedge \phi_2)$, avec ϕ_1, ϕ_2 de complexité inférieure ou égale à k.

$\mathcal{R}/\mathcal{U} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$ ssi, par définition de la conjonction,

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

ssi, par hypothèse d'induction, $S_j := \{i \in I : R_i \models \phi_j(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$, pour $j = 1, 2$. Ceci, si et seulement si $S_1 \cap S_2 \in \mathcal{U}$, (car $\mathcal{U}$ est un filtre) et

$$S_1 \cap S_2 = \{i \in I : R_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}.$$

(iii) $\phi(x_1, \ldots, x_n) = \exists y\, \psi(y, x_1, \ldots, x_n)$, avec ψ de complexité égale à k.
Si $\mathcal{R}/\mathcal{U} \models \phi(a_{1_\mathcal{U}}, \ldots, a_{n_\mathcal{U}})$, par définition du quantificateur existentiel, il existe $b \in \mathcal{R}$ tel que

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

Par hypothèse d'induction,

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

Mais, si $i \in S$, alors $R_i \models \exists y\, \psi(y, a_1(i), \ldots, a_n(i))$, c'est-à-dire $R_i \models \phi(a_1(i), \ldots, a_n(i))$. Donc, l'ensemble $\{i \in I : R_i \models \phi(a_1(i), \ldots, a_n(i)\}$ contient un élément de $\mathcal{U}$ et $\mathcal{U}$ étant un filtre est donc aussi dans $\mathcal{U}$.
Réciproquement, supposons que $S = \{i \in I : R_i \models \phi(a_1(i), \ldots, a_n(i))\} \in \mathcal{U}$. Pour chaque $i \in S$, il existe $b_i \in R_i$ tel que $R_i \models \psi(b_i, a_1(i), \ldots, a_n(i))$. Soit $b \in \mathcal{R}$ tel que, pour $i \in S$, $b(i) = b_i$, et pour $i \notin S$, $b(i) = 0$. Alors par hypothèse d'induction, puisque $S \in \mathcal{U}$,

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

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

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

On laisse le lecteur vérifier les deux cas restants, disjonction et quantification universelle. On peut remarquer que l'hypothèse de maximalité sur $\mathcal{U}$ n'a été utilisée que pour le cas de la négation. □

Remarque: Si I est infini et si $\mathcal{U}$ est un ultrafiltre principal sur I, $\mathcal{U}$ est engendré par $\{i_0\}$. Alors on peut vérifier que $\mathcal{R}$ est isomorphe à l'anneau R_{i_0}, par l'application $a \in R_{i_0} \mapsto b_\mathcal{U}$, où b est tel que $b(i_0) = a$ et $b(j) = 0$, pour $j \neq i_0$. .

On peut maintenant montrer directement le théorème dont on a besoin:
Preuve du Théorème 3: On considère P l'ensemble des nombres premiers et $\mathcal{U}$ un ultrafiltre non principal sur P. On a remarqué (3.3) que $\mathcal{U}$ doit alors contenir le filtre de Frechet sur P, donc tout ensemble de complémentaire fini. Soit $K_p := \overline{\mathbb{F}_p}$ et $\mathcal{K} := \Pi_{p \in P} K_p/\mathcal{U}$. Quelles sont les propriétés du corps $\mathcal{K}$?

1. $\mathcal{K}$ est de caractéristique zéro: en effet, soit p un premier, alors $\{q \in P : K_q \models p \neq 0\}$ est de complémentaire fini, donc est un élément du filtre de Frechet, donc de $\mathcal{U}$. Par Łos, il suit que $\mathcal{K} \models p \neq 0$ aussi, et cela pour chaque p.

2. $\mathcal{K}$ est algébriquement clos. En effet on a vu (section 2.3 qu' un corps est algébriquement clos si et seulement si, pour chaque $n \geq 1$, il satisfait un certain énoncé θ_n. Par

hypothèse, pour chaque p, K_p est algébriquement clos, donc satisfait θ_n; l'ensemble P est un élément de $\mathcal{U}$, donc par Łos, $\mathcal{K}$ est modèle de θ_n.

3. Quelle est la cardinalité de $\mathcal{K}$? Par le lemme 11, il est de la puissance du continu, c'est à dire a le même cardinal que $\mathcal{P}(\mathbb{N})$, qui est aussi la cardinalité de $\mathbb{R}$ et de $\mathbb{C}$. Nous avons admis (section 1.3) que, à isomorphisme près, il y a un unique corps algébriquement clos de caractéristique zéro et de même cardinalité que $\mathbb{C}$.

Maintenant soit σ un énoncé qui est vrai dans tous les K_p, alors, par Łos, il est vrai dans $\mathcal{K}$ qui est isomorphe à $\mathbb{C}$, donc il est vrai dans $\mathbb{C}$. □

Cela nous donne donc bien le théorème d'Ax.

3.5 Démonstration du théorème de compacité

Théorème 14 Théorème de compacité pour la classe des anneaux commutatifs *Soit* Σ *un ensemble d'énoncés tel que tout sous ensemble fini de* Σ *a un modèle. Alors* Σ *a un modèle.*

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

Nous allons démontrer une deuxième version du théorème de compacité qui nous sera utile pour montrer que la théorie des corps algébriquement clos élimine les quantificateurs, dans la section suivante. La preuve est la même que la précédente, mais nous ne pouvons la déduire de la version précédente à cause des restrictions particulières que nous avons choisies d'imposer dans la définition de l'ensemble des formules, limité au "pur" langage des anneaux).

Théorème 15 (Théorème de compacité avec paramètres) *Soient* T *une théorie,* Σ *un ensemble de formules à variables libres parmi* $\{x_1, \ldots, x_n\}$*, et* $\phi(x_1, \ldots, x_n)$ *une formule. Supposons qu' il n'existe pas de modèle* R *de* T *et de suite* $a_1, \ldots, a_n$ *dans* R *telle que*

- $R \models \phi(a_1, \ldots, a_n)$
- $R \models \sigma(a_1, \ldots, a_n)$ *pour chaque formule* $\sigma(x_1, \ldots, x_n)$ *de* Σ.

Alors il existe $\sigma_1, \ldots, \sigma_k \in \Sigma$ *telles que*

$$T \vdash \forall x_1 \ldots \forall x_n \, (\bigwedge_{1 \leq j \leq k} \sigma_i(x_1, \ldots x_n) \rightarrow \neg \phi(x_1, \ldots, x_n)).$$

Preuve: Supposons que la conclusion n'est pas vraie. Alors pour tout sous-ensemble fini $F \subset \Sigma$, on peut trouver R_F et une suite $a(F)_1, \ldots, a(F)_n \in R_F$ telle que

- $R_F \models T$,
- $R_F \models \sigma(a(F)_1, \ldots a(F)_n)$ pour chaque $\sigma \in F$,
- $R_F \models \phi(a(F)_1, \ldots a(F)_n)$.

Soit I l'ensemble de toutes les parties finies de Σ. Pour chaque formule σ de Σ, soit $V(\sigma) := \{F \in I; \sigma \in F\}$. On remarque que si $F \in V(\sigma)$, $R_F \models \sigma(a(F)_1, \dots a(F)_n)$. La famille $\{V(\sigma); \sigma \in \Sigma\}$ a la propriété de l'intersection finie. Elle est donc contenue dans un ultrafiltre $\mathcal{U}$.

Soit $\mathcal{R}$ l'ultraproduit des R_F, on applique le Théorème de Łos (13): $\mathcal{R}$ est un modèle de la théorie T, car R_F est modèle de T pour chaque $F \in I$, et $I \in \mathcal{U}$,

Soit $a_i = (a(F)_i)_{F \in I}$, pour $1 \leq i \leq n$. Alors pour $\sigma \in \Sigma$, l'ensemble $\{F \in I : R_F \models \sigma(a(F)_1, \dots a(F)_n)\}$ contient $V(\sigma)$ et est donc un élément de $\mathcal{U}$. Il suit que $\mathcal{R} \models \sigma(a_{1\mathcal{U}}, \dots, a_{n\mathcal{U}})$.

Pour chaque F, $R_F \models \phi(a(F)_1, \dots a(F)_n))$, donc on a aussi $\mathcal{R} \models \phi(a_{1\mathcal{U}}, \dots, a_{n\mathcal{U}})$.
On a ainsi trouvé un modèle de T, $\mathcal{R}$, et une suite d'éléments de $\mathcal{R}$, $a_{1\mathcal{U}}, \dots, a_{n\mathcal{U}}$, qui contredisent nos hypothèses. □

4 Suppléments : élimination des quantificateurs et complétude de la théorie des corps algébriquement clos de caractéristique fixée

On considère qu'on maîtrise bien une théorie, ou une classe de structures, si l'on contrôle bien la forme de ses ensembles définissables, par exemple si toute formule est équivalente à une formule sans quantificateurs.

Nous allons montrer que c'est le cas pour la classe des corps algébriquement clos. Il y a de très nombreuses manières de démonter ce résultat, qui est connu, côté géométrie algébrique, sous le nom de théorème de Chevalley ("l'image d'un ensemble constructible par une application polynomiale est un ensemble constructible").

La démonstration choisie ici n'utilise que des notions de théorie des modèles déjà introduites, et en ce qui concerne l'algèbre, n'utilise que l'unicité de la clôture algébrique à isomorphisme près, fait que nous avons admis précédemment.

Nous commençons par quelques définitions , et un critère "local" (formule par formule) d'élimination des quantificateurs qui est très utile.

4.1 Définitions et Critère d'élimination

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

On dit qu'une théorie T **admet l'élimination des quantificateurs** si, pour toute formule $\phi(x_1, \dots, x_n)$, il existe une formule sans quantificateur, $\theta(x_1, \dots, x_n)$ qui lui est équivalente modulo T, c'est-à-dire telle que:

$$T \vdash \forall x_1 \dots \forall x_n \, [(\phi(x_1, \dots, x_n) \leftrightarrow \theta(x_1, \dots, x_n)].$$

Remarque: La notation $\phi(x_1, \dots, x_n)$ indique que les variables libres de ϕ sont parmi $\{x_1, \dots, x_n\}$. Et ce que dit la définition de l'élimination des quantificateurs que nous

avons choisie, c'est qu' on peut trouver une formule équivalente θ, sans quantificateur, qui n'a pas plus de variables libres que ϕ. En particulier, si ϕ est un énoncé, alors ϕ sera équivalent (modulo la théorie T) à un énoncé sans quantificateur.

Si R_1 est un sous-anneau de R_2, si $\phi(x_1, \ldots, x_n)$ est une formule, et si $a_1, \ldots, a_n \in R_1$, il n'y a aucune raison que $R_1 \models \phi(a_1, \ldots, a_n)$ si et seulement si $R_2 \models \phi(a_1, \ldots, a_n)$, ni dans un sens ni dans l'autre.

Par exemple, prenons $\phi(x) = \exists y\, y^2 = x$. Alors $\mathbb{C} \models \phi(-1)$, $\mathbb{R} \models \neg\phi(-1)$, et $\mathbb{R} \models \phi(2)$, alors que $\mathbb{Q} \models \neg\phi(2)$ ....

Mais la formule ϕ de l'exemple comporte un quantificateur. En effet:

Lemme 16 *Soit $\phi(x_1, \ldots, x_n)$ une formule sans quantificateur, R_2 un anneau commutatif, et $R_1 < R_2$, sous-anneau de R_2. Pour tous $a_1, \ldots, a_n \in R_1$,*

$$R_1 \models \phi(a_1, \ldots, a_n) \text{ ssi } R_2 \models \phi(a_1, \ldots, a_n).$$

Preuve: Par induction sur la complexité des formules sans quantificateur. C'est clairement vrai pour les formules atomiques, qui sont des égalités de polynômes. Ensuite il suffit de vérifier que cela reste vrai par conjonction, par négation (et par disjonction). □

Lemme 17 *Soient R_1, R_2 deux anneaux commutatifs. Soient $a_1, \ldots, a_n \in R_1$, et $b_1, \ldots, b_n \in R_2$. Supposons que pour toute formule sans quantificateurs $\phi(x_1, \ldots, x_n)$,*

$$R_1 \models \phi(a_1, \ldots, a_n) \text{ ssi } R_2 \models \phi(b_1, \ldots, b_n).$$

Soit S_1 le sous-anneau de R_1 engendré par $a_1 \ldots, a_n$ et S_2 le sous-anneau de R_2 engendré par $b_1, \ldots, b_n$. Alors si on pose $f(a_i) = b_i$, pour $1 \leq i \leq n$, f se prolonge en un (unique) isomorphisme de S_1 sur S_2.

Preuve: L'hypothèse nous dit que pour tout polynôme $P \in \mathbb{Z}[X_1, \ldots, X_n]$,

$$P(a_1, \ldots, a_n) = 0 \text{ ssi } P(b_1, \ldots b_n) = 0.$$

Il suit bien que $\mathbb{Z}[a_1, \ldots, a_n]$ et $\mathbb{Z}[b_1, \ldots, b_n]$ sont isomorphes. □

Le critère suivant est une sorte de réciproque du lemme 16:

Proposition 18 *Soit $\phi(y_1, \ldots, y_k)$ une formule, et T une théorie. Sont équivalents:*
(i) Il existe une formule sans quantificateurs $\theta(y_1, \ldots, y_n)$ telle que

$$T \vdash \forall y_1 \ldots \forall y_k\, (\phi(y_1, \ldots, y_k) \leftrightarrow \theta(y_1, \ldots, y_k)).$$

(ii) Pour tous les anneaux commutatifs $S_1 < R_1$ et $S_2 < R_2$, tout isomorphisme d'anneau f de S_1 sur S_2 et pour tous $a_1, \ldots a_k \in S_1$,

$$R_1 \models \phi(a_1, \ldots, a_k) \text{ ssi } R_2 \models \phi(f(a_1), \ldots, f(a_k)).$$

Preuve:

(i) implique (ii): Par l'hypothèse (i) nous pouvons supposer que la formule ϕ elle-même est sans quantificateurs. Si $R_1 \models \phi(a_1, \ldots, a_k)$, par le lemme 16, $S_1 \models \phi(a_1, \ldots, a_k)$. Par isomorphisme (Lemme 4), $S_2 \models \phi(f(a_1) \ldots, f(a_k))$ et par le lemme 16 à nouveau, $R_2 \models \phi(f(a_1), \ldots, f(a_k))$.

(ii) implique (i): Considérons l'ensemble de formules suivant

$$\Delta := \{\delta(y_1, \ldots y_k) : T \vdash \forall y_1 \ldots \forall y_k \, (\phi(y_1, \ldots, y_k) \rightarrow \delta(y_1, \ldots, y_k))\}.$$

On va montrer
Claim : Il n'existe pas de modèle R de T et de suite $a_1, \ldots a_k$ dans R telle que :
- $R \models \neg\phi(a_1, \ldots a_k)$
- $R \models \delta(a_1, \ldots, a_k)$ pour chaque $\delta(y_1, \ldots, y_k) \in \Delta$.

Avant de montrer ce Claim, vérifions qu'il nous permet de terminer la démonstration.
On applique le théorème de compacité avec paramètres (Théorème 15). Il existe donc un sous-ensemble fini $\delta_1, \ldots, \delta_m$ de formules de Δ, telles que

$$T \vdash \forall y_1 \ldots \forall y_k \, [\bigwedge_{1 \leq i \leq m} \delta_i(y_1, \ldots, y_k) \rightarrow \phi(y_1, \ldots, y_k)].$$

Posons $\theta(y_1, \ldots, y_k) := \bigwedge_{1 \leq i \leq m} \delta_i(y_1, \ldots, y_k)$. La formule $\theta(y_1, \ldots, y_k)$ est bien sans quantificateur et on a

$$T \vdash \forall y_1 \ldots \forall y_k [\phi(y_1, \ldots, y_k) \leftrightarrow \theta(y_1, \ldots, y_k)].$$

Il ne reste donc plus qu'à prouver le Claim, en utilisant à nouveau la compacité.

Preuve du Claim: Supposons, par l'absurde, qu'il existe un tel modèle R et une telle suite $a_1, \ldots, a_k \in R$.
Soit Γ l'ensemble de toutes les formules sans quantificateur qui sont satisfaites par $(a_1, \ldots, a_k)$ dans R,

$$\Gamma = \{\gamma(y_1 \ldots, y_k) : R \models \gamma(a_1, \ldots, a_k), \, \gamma \text{ sans quantificateur } \}.$$

Par hypothèse, $\Gamma \supset \Delta$. Nous disons qu'il existe aussi un anneau R_1, modèle de la théorie T, et une suite $b_1, \ldots, b_k$ dans R_1 telle que $R_1 \models \phi(b_1, \ldots, b_k)$, et $R_1 \models \gamma(b_1, \ldots, b_k)$ pour chaque $\gamma \in \Gamma$.
Sinon, par la compacité avec paramètres (Proposition 15), il existerait un sous-ensemble fini $\{\gamma_1, \ldots, \gamma_n\}$ de Γ tel que

$$T \vdash \forall y_1 \ldots \forall y_k \, [\bigwedge_{1 \leq i \leq n} \gamma_i(y_1, \ldots, y_k) \rightarrow \neg\phi(y_1, \ldots, y_k)].$$

Par contraposition,

$$T \vdash \forall y_1 \ldots \forall y_k \, [\phi(y_1, \ldots, y_k) \rightarrow \bigvee_{1 \leq i \leq n} \neg\gamma_i(y_1, \ldots y_k)].$$

Mais alors,

$$(\bigvee_{1 \leq i \leq n} \neg\gamma_i(y_1, \ldots, y_k))$$

est une formule de Δ, donc

$$R \models (\mathbb{W}_{1 \leq i \leq n} \neg\gamma_i(a_1, \ldots, a_k)),$$

c'est-à dire, il existe un indice i tel que $R \models \neg\gamma_i(a_1, \ldots, a_k)$, ce qui contredit la définition de Γ.
On a donc d'un coté $(R, a_1, \ldots, a_k)$, de l'autre $(R_1, b_1, \ldots, b_k)$ et pour toute formule sans quantificateurs γ, $R \models \gamma(a_1, \ldots, a_k)$ ssi $R_1 \models \gamma(b_1 \ldots, b_k)$. Par le lemme 17, le sous-anneau engendré par $b_1, \ldots, b_k$ dans R_1 et le sous-anneau engendré par $a_1, \ldots, a_k$ dans R sont isomorphes, par un isomorphisme qui envoie $a_1, \ldots, a_k$ sur $b_1, \ldots, b_k$. Par hypothèse on a donc

$$R \models \phi(a_1, \ldots, a_k) \text{ ssi } R_1 \models \phi(b_1, \ldots, b_k).$$

Ceci est une contradiction et on a donc montré le Claim.

□

Enfin, un dernier lemme facile qui dit que pour éliminer les quantificateurs il suffit de le faire quantificateur par quantificateur:

Lemme 19 *Soit T une théorie telle que, pour toute formule $\phi(x, y_1, \ldots, y_n)$, sans quantificateur, il existe une formule sans quantificateur $\theta(y_1, \ldots, y_n)$ telle que*

$$T \vdash \forall y_1 \ldots \forall y_n \, (\exists x \, \phi(x, y_1 \ldots, y_n) \leftrightarrow \theta(y_1, \ldots, y_n)).$$

Alors T admet l'élimination des quantificateurs.

Preuve: On montre, par induction sur la complexité des formules, que pour toute formule $\psi(y_1, \ldots, y_n)$ il existe une formule sans quantificateur qui lui est équivalente.

Si $\phi(x, y_1 \ldots, y_n)$ est de complexité zéro, c'est-à-dire atomique, elle est déjà elle-même sans quantificateur.

On suppose que c'est vrai pour toutes les formules de complexité inférieure ou égale à k, et on considère $\psi(y_1, \ldots, y_n)$ de complexité égale à $k+1$.

(i) $\psi = \neg\phi$, avec ϕ de complexité k. Par hypothèse d'induction, il existe $\gamma(y_1, \ldots, y_n)$, formule sans quantificateur telle que $T \vdash \forall y_1 \ldots \forall y_n \, (\phi(y_1, \ldots, y_n) \leftrightarrow \gamma(y_1 \ldots, y_n))$. Alors la formule $\neg\gamma(y_1, \ldots, y_n)$ est encore sans quantificateur et

$$T \vdash \forall y_1 \ldots \forall y_n \, (\neg\phi(y_1, \ldots, y_n) \leftrightarrow \neg\gamma(y_1 \ldots, y_n)).$$

(ii) $\psi = (\phi_1 \wedge \phi_2)$ avec ϕ_1 et ϕ_2 de complexité $\leq k$. Alors, par induction, ϕ_1 (resp. ϕ_2) est équivalente a une formule sans quantificateur γ_1 (resp. γ_2). Clairement ϕ est alors équivalente à $(\gamma_1 \wedge \gamma_2)$ qui reste sans quantificateur.

(iii) $\psi(y_1, \ldots, y_n) = \exists x \, \phi(x, y_1, \ldots, y_n)$, avec ϕ de complexité égale à k. Par induction, il existe $\gamma(x, y_1, \ldots, y_n)$ sans quantificateur telle que

$$T \vdash \forall x \forall y_1 \ldots \forall y_n \, (\phi(x, y_1, \ldots, y_n) \leftrightarrow \gamma(x, y_1 \ldots, y_n)).$$

Il est alors évident que

$$T \vdash \forall y_1 \ldots \forall y_n \, (\exists x \, \phi(x, y_1, \ldots, y_n) \leftrightarrow \exists x \, \gamma(x, y_1, \ldots, y_n)).$$

On peut appliquer l'hypothèse du lemme à la formule $\exists x\, \gamma(x, y_1, \ldots, y_n)$, qui est donc équivalente à une formule sans quantificateurs $\theta(y_1, \ldots, y_n)$, qui est également équivalente à $\exists x\, \phi(x, y_1, \ldots, y_n)$.

(iv) Pour la disjonction, on utilise le fait que

$$(\phi_1 \vee \phi_2) \leftrightarrow \neg(\neg\phi_1 \wedge \neg\phi_2).$$

(v) Pour le quantificateur universel, on utilise le fait que

$$(\forall x \phi(x, y_1, \ldots, y_n)) \leftrightarrow \neg(\exists x\, \neg\phi(x, y_1, \ldots, y_n)).$$

□

4.2 Corps algébriquement clos

On va appliquer les résultats de la section précédente à la théorie T_{CAC} dont les modèles sont exactement tous les corps algébriquement clos. Le fait algébrique que nous admettons est l'unicité, à isomorphisme près, de la clôture algébrique (voir section 1.3).

On montre que T_{CAC} satisfait les hypothèses du Lemme 19.

Théorème 20 *Soit T_{CAC} la théorie des corps algébriquement clos et $\phi(x, y_1, \ldots, y_n)$ une formule sans quantificateur. Alors il existe une formule $\theta(y_1, \ldots, y_n)$, sans quantificateur, telle que*

$$T_{CAC} \vdash \forall y_1 \ldots \forall y_n\, (\exists x\, \phi(x, y_1 \ldots, y_n) \leftrightarrow \theta(y_1, \ldots, y_n)).$$

Preuve: On va utiliser le critère d'élimination "local" prouvé dans la Proposition 18.

La formule $\phi(x, y_1, \ldots, y_n)$ est sans quantificateur. Il n'est pas difficile de vérifier qu'elle est équivalente à une disjonction finie de formules du type

$$(\bigwedge_{1 \le i \le m} P_i(x, y_1, \ldots, y_n) = 0) \wedge (Q(x, y_1, \ldots, y_n) \neq 0),$$

avec $P_i, Q \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$. On peut donc supposer que en fait ϕ est égale à l'une de ces conjonctions.

Soient K_1 et K_2 deux corps algébriquement clos, R_1, R_2 deux sous-anneaux respectivement de K_1 et K_2, et un isomorphisme f de R_1 sur R_2. Soit $T_1 < K_1$, corps de fractions de R_1, et $L_1 = \overline{T_1} < K_1$, clôture algébrique de T_1 dans K_1. L'isomorphisme f se prolonge alors en un isomorphisme de L_1 sur $L_2 < K_2$, L_2 une clôture algébrique du corps de fractions de R_2.

Par symétrie, il nous suffit de vérifier que si $a_1, \ldots, a_n \in R_1$ et si $K_1 \models \exists x\, \phi(x, a_1, \ldots, a_n)$, alors $K_2 \models \exists x\, \phi(x, f(a_1), \ldots, f(a_n))$.

On suppose donc que dans K_1 il y a un élément b tel que pour chaque i, $1 \le i \le m$, $P_i(b, a_1, \ldots, a_n) = 0$ et $Q(b, a_1, \ldots, a_n) \neq 0$.

1. Si pour chaque i les polynômes $P_i(X, a_1, \ldots, a_n)$ sont égaux au polynôme nul, il en est de même, par isomorphisme, des polynômes $P_i(X, f(a_1), \ldots, f(a_n))$. Il reste juste la condition $Q(b, a_1, \ldots, a_n) \neq 0$. Considérons le polynôme $Q(X, f(a_1), \ldots, f(a_n)) \in R_2[X]$. Par isomorphisme, il n'est pas égal au polynôme nul. Il a donc dans K_2 un nombre

fini de racines. K_2 étant infini,il existe $c \in K_2$ qui ne l'annule pas, et on a bien $K_2 \models \exists x \phi(x, f(a_1), \ldots, f(a_n))$.

2. Si l'un au moins des $P_i(X, a_1, \ldots, a_n)$ n'est pas nul, alors b est algébrique sur R_1, et donc $b \in L_1$. Par isomorphisme entre L_1 et L_2, on aura que pour chaque i, $P_i(f(b), f(a_1), \ldots, f(a_n)) = 0$ et que $Q(f(b), f(a_1), \ldots, f(a_n)) \neq 0$. □

On en déduit donc par le lemme 19:

Corollaire 21 *La théorie des corps algébriquement clos admet l'élimination des quantificateurs* **dans le langage des anneaux** $(\{+, -, ., 0, 1\})$.

Avoir l'élimination des quantificateurs dans le langage des anneaux est une propriété très forte, et caractérise les corps algébriquement clos parmi les corps.

Théorème 22 [Mac] *Soit K un corps infini tel que, pour toute formule $\phi(x_1, \ldots, x_n)$, il existe une formule sans quantificateur $\theta(x_1, \ldots, x_n)$ telle que*

$$K \models \forall x_1 \ldots \forall x_n \, (\phi(x_1 \ldots, x_n) \leftrightarrow \theta(x_1, \ldots, x_n)).$$

Alors K est algébriquement clos.

Nous n'allons pas donner la démonstration de ce théorème mais pour donner une idée de pourquoi il est vrai, regardons deux exemples. Une formule sans quantificateur en une variable libre, dans le langage des anneaux, définit dans K un sous-ensemble qui est soit fini soit de complémentaire fini (cofini): en effet un tel sous-ensemble de K est une combinaison booléenne finie de fermés de Zariski de K, et un fermé de Zariski de K est l'ensemble des racines dans K d'un nombre fini de polynômes (à une seule variable!).

1. Considérons le corps $\mathbb{R}$, le sous-ensemble suivant $P = \{x \in \mathbb{R} : \exists y \, y^2 = x\}$ (les nombres positifs dans $\mathbb{R}$), n'est ni fini ni cofini. Pour obtenir l'élimination des quantificateurs pour les réels, il faut *agrandir le langage* en rajoutant l'ordre par exemple. Cela consiste à agrandir l'ensemble des formules atomiques et à autoriser aussi les formules du type $P(x_1, \ldots, x_n) < Q(x_1, \ldots, x_n)$ où $P, Q \in \mathbb{Z}[X_1, \ldots, X_n]$. On définit ensuite l'ensemble de toutes les formules à partir des formules atomiques comme nous l'avons fait.

2. Soit K un corps infini de caractéristique $p > 0$, non parfait, c'est-à-dire tel que $K^p \neq K$ (il existe un élément a dans K tel que $b^p \neq a$, pour tout $b \in K$). Alors K^p est infini et de complémentaire infini (c'est un sous-groupe du groupe additif de K qui est d'indice infini dans K). Par exemple, soit t un élément transcendant sur $\mathbb{F}_p$ et $K = \mathbb{F}_p(t)$. Dans K^p il y a $t^p, \ldots, t^{p^n}, \ldots$, et dans $K \setminus K^p$, il y a $\{t^q; q$ premier à $p\}$.

Nous terminerons par la complétude des corps algébriquement clos de caractéristique fixée, qui se déduit rapidement de l'élimination des quantificateurs:

Définition: Deux anneaux commutatifs R_1 et R_2 sont **élémentairement équivalents** si, pour tout énoncé σ,

$$R_1 \models \sigma \text{ ssi } R_2 \models \sigma.$$

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

Proposition 23 *Deux corps algébriquement clos sont élémentairement équivalents si et seulement si ils ont même caractéristique.*

Preuve: Dans un sens si K_1 et K_2 sont élémentairement équivalents, ils doivent être de même caractéristique puisque il y a un énoncé $p = 0$ dont les modèles sont exactement les anneaux de caractéristique p. Dans l'autre sens: soient K_1 et K_2 de même caractéristique, alors chacun contient une copie du corps premier k_0 de la bonne caractéristique. Soit σ un énoncé tel que $K_1 \models \sigma$. Par élimination des quantificateurs pour la théorie des corps algébriquement clos, T_{CAC}, il existe un énoncé θ sans quantificateur tel que $T_{CAC} \vdash (\sigma \leftrightarrow \theta)$. Par le lemme 16,

$$K_1 \models \sigma \text{ ssi } K_1 \models \theta \text{ ssi } k_0 \models \theta \text{ ssi } K_2 \models \theta \text{ ssi } K_2 \models \sigma.$$

□

Quelques suggestions de lecture

Pour ceux qui maintenant ou dans le futur souhaiteraient aller regarder un peu plus de théorie des modèles, quelques références:

Un livre récent de théorie des modèles, dont je me suis très largement inspirée pour la dernière section, qui part de presque zéro et arrive à parler à la fin des interactions entre théorie des modèles et géométrie. Également plein d'exercices et d'exemples intéressants (attention quelques erreurs dans la première édition): **Model Theory: an introduction** de D. Marker, Graduate Texts in Mathematics 217, Springer, 2002.

Si l'on est curieux des applications récentes de la théorie des modèles, il est possible d'aller regarder des articles d'exposition. Par exemple, il y a un volume de Proceedings d'un colloque au MSRI de Berkeley en 1998, en ouverture d'un semestre "Théorie des modèles des corps et applications", colloque destiné a présenter la théorie des modèles aux géomètres et un peu de géométrie aux théoriciens des modèles: **Model theory, algebra, and geometry**, D. Haskell, A. Pillay and C. Steinhorn (Ed.), Mathematical Sciences Research Institute Publications, 39, Cambridge University Press, 2000.

References

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

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

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

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

[Mac] A. Macintyre, *On ω_1-categorical theories of fields*, Fund. Math. **70**, no. 3, 1971, 253-270.

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

Elisabeth Bouscaren
Laboratoire de Mathématiques
Université Paris-Sud, Bat. 425
91405 Orsay, France.
elisabeth.bouscaren@math.u-psud.fr