THÉORIE DES MODÈLES
DE L'EXEMPLE AU MODÈLE

KADDAR Younesse

Résumé *On se propose de poser un cadre d'introduction de la théorie des modèles à travers un exemple : le théorème d'Ax, ce qui nous donnera l'occasion d'esquisser une comparaison avec une autre approche - purement algébrique - aboutissant à la démonstration dudit théorème.*

SOMMAIRE

I OBSERVATIONS INITIALES

Le théorème d'Ax stipule que : toute fonction polynomiale injective de $\mathbb{C}^n$ dans $\mathbb{C}^n$ est surjective.

— **Pour $n = 1$:** L'hypothèse "injective" devient **inutile** : c'est le théorème de D'Alembert (modulo les polynômes constants).

— **En substituant un corps fini $\mathbb{K}$ à $\mathbb{C}$:** L'hypothèse "polynomiale" devient **inutile** : cela relève du principe des tiroirs.

Cette observation invite à chercher à "étendre à $\mathbb{C}$" ce qui est évident dans les corps finis, plutôt qu'à entamer une démonstration par récurrence sur $n \in \mathbb{N}$.

II AX : DÉMONSTRATION ALGÉBRIQUE

II.1 NULLSTELLENSATZ FORT

Soient $n \geqslant 1, m \geqslant 0$ et $\mathbb{K}$ un corps.

II.1.1 Lemme de Zariski

Théorème - Lemme de Zariski

Soient $x_1, \dots, x_n \notin \mathbb{K}$ et $A \overset{\text{déf}}{=} \mathbb{K}[x_1, \dots, x_n]$ une $\mathbb{K}$-algèbre de type fini (i.e finiment engendrée, en tant que $\mathbb{K}$-algèbre).

Si A est un corps, alors A est algébrique sur $\mathbb{K}$.

Démonstration: Supposons que $A = \mathbb{K}[x_1, \dots, x_n]$ est un corps. Preuve par récurrence sur $n \in \mathbb{N}^*$:

- Pour $n = 1$: le résultat est évident, puisque $x_1^{-1} \in A = \mathbb{K}[x_1]$
- Si le résultat est acquis pour $n \in \mathbb{N}^*$: Par l'absurde : on peut supposer, sans perte de généralité, que x_1 est transcendant sur $\mathbb{K}$ (sinon, c'est trivial). Comme A est un corps, $\mathbb{K}(x_1) \subset \mathbb{K}[x_1]$ [1], et

$$A = \underbrace{\mathbb{K}(x_1)}_{\overset{\text{déf}}{=} k}[x_2, \dots, x_n]$$

Pour tout $i \in [\![2, n]\!]$: par hypothèse de récurrence, x_i est racine d'un polynôme unitaire $P_i \in k[X]$. En notant $D_i(x_1)$ ($D_i \in \mathbb{K}[X]$) le produit des dénominateurs des coefficients de P_i, et en posant

$$D \overset{\text{déf}}{=} \prod_{j=2}^{n} D_j$$

en multipliant "$P_i(x_i) = 0$" par $D(x_1)^m$, pour un entier m suffisamment grand, il vient que : $D(x_1)x_i$ est entier sur $\mathbb{K}[x_1]$. De plus, comme $\mathbb{K}[a_1] \cong \mathbb{K}[X]$, il existe un polynôme irréductible Q premier avec D.
Donc $(Q(x_1))^{-1} \in A = k[x_2, \dots, x_n]$ (c'est un corps), et $D(x_1)^r (Q(x_1))^{-1} \in k[D(x_1)x_2, \dots, D(x_1)x_n]$ pour un entier r assez grand, d'où $D(x_1)^r (Q(x_1))^{-1}$ est entier sur $\mathbb{K}[x_1]$ (lemme 9).
Or : $\mathbb{K}[x_1]$ est factoriel (en tant qu'anneau principal), donc intégralement clos, et :

$$D(x_1)^r (Q(x_1))^{-1} \in \mathbb{K}[x_1]$$

d'où Q|D, ce qui est absurde.

□

II.1.2 Nullstellensatz faible

Théorème - Nullstellensatz faible

Si $\mathbb{K}$ est algébriquement clos, pour tout idéal J de $\mathbb{K}[X_1, \dots, X_n]$,

$$V(J) = \emptyset \Longrightarrow J = \mathbb{K}[X_1, \dots, X_n]$$

où $\quad V(J) \overset{\text{déf}}{=} \bigcap_{P \in J} P^{-1}(\{0\})$

1. car si $F(x_1) \in \mathbb{K}(x_1)\backslash\{0\}$, il existe $P(x_1) \in \mathbb{K}[x_1]\backslash\{0\}$ tel que $P(x_1)F(x_1) \in \mathbb{K}[x_1]$, d'où $F(x_1) \in \mathbb{K}[x_1]$ puisque $P(x_1)$ est inversible dans $\mathbb{K}[x_1]$.

Démonstration: La fonction

$$\Phi \overset{\text{déf}}{=} \begin{cases} \mathbb{K}^n & \to & \{\text{Idéaux maximaux de } \mathbb{K}[X_1,\dots,X_n]\} \\ (a_1,\dots,a_n) & \mapsto & \langle X_1-a_1,\dots,X_n-a_n\rangle \end{cases}$$

est une bijection.

- **Surjectivité :** Soit I un idéal maximal de $\mathbb{K}[X_1,\dots,X_n]$. On note A le corps $\mathbb{K}[X_1,\dots,X_n]/I$.
  Le morphisme

  $$\phi \overset{\text{déf}}{=} \begin{cases} \mathbb{K} & \to & A \\ \lambda & \mapsto & \overline{\lambda} \end{cases}$$

  est injectif (si $\lambda \in \operatorname{Ker}\phi$, alors $\lambda \in I$, et $\lambda = 0$ car sinon $I = \mathbb{K}[X_1,\dots,X_n]$), d'où $k \overset{\text{déf}}{=} \phi(\mathbb{K})$ est un sous-corps algébriquement clos de A, et $A = k[\overline{X_1},\dots,\overline{X_n}]$.
  Par le lemme de ZARISKI, A est algébrique sur k : c'est donc k (car k est algébriquement clos), et $A \overset{\phi^{-1}}{\cong} \mathbb{K}$. En posant, pour tout $i \in [\![1,n]\!]$, $a_i \overset{\text{déf}}{=} \phi^{-1}(\overline{X_i}) \in \mathbb{K} : X_i - a_i \in I$, d'où $I \supset \langle X_1-a_1,\dots,X_n-a_n\rangle$, et par maximalité de $\langle X_1-a_1,\dots,X_n-a_n\rangle$, $I = \langle X_1-a_1,\dots,X_n-a_n\rangle$.
- **Injectivité :**
  Si $\langle X_1-a_1,\dots,X_n-a_n\rangle = \langle X_1-b_1,\dots,X_n-b_n\rangle$, alors pour tout $i \in [\![1,n]\!]$:

  $$a_i - b_i = X_i - b_i - (X_i - a_i) \in I$$

  d'où $a_i = b_i$, car sinon $I = \mathbb{K}[X_1,\dots,X_n]$.

Par contraposée : si J est un idéal strict de $\mathbb{K}[X_1,\dots,X_n]$, J est inclus dans un idéal maximal $I \supset J$. De fait, par bijectivité de Φ, il existe un élément de $\mathbb{K}^n$ en lequel s'annulent les polynômes de I, et donc de J. □

II.1.3 ASTUCE DE RABINOWITSCH

Théorème - Nullstellensatz fort

Si $\mathbb{K}$ est algébriquement clos, pour tous polynômes $P_1,\dots,P_m \in \mathbb{K}[X_1,\dots,X_n]$, l'idéal $J \overset{\text{déf}}{=} \langle P_1,\dots,P_m\rangle$ vérifie :

$$I(V(J)) = \sqrt{J}$$

où

- $I(V(J))$ est l'idéal des polynômes s'annulant en chacun des éléments de $V(J)$
- $\sqrt{J}$ est le radical de J (i.e l'ensemble des polynômes dont une puissance strictement positive appartient à J)

Démonstration: Soit $J \overset{\text{déf}}{=} \langle P_1,\dots,P_m\rangle \subset \mathbb{K}[X_1,\dots,X_n]$.

- $\sqrt{J} \subset \mathbf{I}(\mathbf{V}(J))$: évident, par intégrité de $\mathbb{K}$.
- $\mathbf{I}(\mathbf{V}(J)) \subset \sqrt{J}$: Soit $P \in \mathbb{K}[X_1,\dots,X_n]$ un polynôme non nul s'annulant en chacun des éléments de $V(J)$. On se place dans $\mathbb{K}[X_0, X_1,\dots,X_n]$, et on pose

  $$\mathfrak{J} \overset{\text{déf}}{=} \langle 1 - X_0 P, P_1,\dots,P_m\rangle$$

Ainsi, $V(\mathfrak{I}) = \emptyset$, et par le Nullstellensatz faible :

$$\mathfrak{I} = \mathbb{K}[X_0, X_1, \dots, X_n] \ni 1$$

c'est-à-dire :

$$1 = (1 - X_0 P)\, Q_0(X_0, \dots, X_n) + \sum_{i=1}^{m} P_i\, Q_i(X_0, \dots, X_n) \quad \circledast$$

pour des polynômes $Q_0, \dots, Q_m \in \mathbb{K}[X_0, X_1, \dots, X_n]$. En prenant l'image des membres de $\circledast$ par le morphisme d'anneaux

$$\begin{cases} \mathbb{K}[X_0, X_1, \dots, X_n] & \to & \mathbb{K}(X_1, \dots, X_n) \\ Q(X_0, X_1, \dots, X_n) & \mapsto & Q(1/P, X_1, \dots, X_n) \end{cases}$$

il vient :

$$1 = \sum_{i=1}^{m} P_i(X_1, \dots, X_n)\, Q_i(1/P, X_1, \dots, X_n)$$

soit, en multipliant par P^r pour un entier r assez grand :

$$P^r = \sum_{i=1}^{m} P_i(X_1, \dots, X_n)\, \widetilde{Q}_i(X_1, \dots, X_n) \in J$$

pour des polynômes $\widetilde{Q}_0, \dots, \widetilde{Q}_m \in \mathbb{K}[X_1, \dots, X_n]$.

□

II.2 Théorème d'Ax

Théorème - Ax - Grothendieck

Toute fonction polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$ qui est injective est bijective.

Démonstration: —

Pour les clôtures algébriques des corps finis

Si $\mathbb{K}$ est un corps fini dont $\overline{\mathbb{K}}$ est une clôture algébrique : toute fonction polynomiale P de $\overline{\mathbb{K}}^n$ dans $\overline{\mathbb{K}}^n$ qui est injective est bijective.

Démonstration: Par l'absurde, si $P = (P_1, \dots, P_n) : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^n$ est injective mais non surjective :

$$\forall x, y \in \overline{\mathbb{K}}^n, P(x) - P(y) = 0 \Longrightarrow x - y = 0$$

d'où, par le Nullstellensatz fort, en considérant la i-ème coordonnée ($i \in [\![1, n]\!]$) :

$$X_i - Y_i \in \sqrt{\left\langle P_i(X_1, \dots, X_n) - P_i(Y_1, \dots, Y_n) \right\rangle} \subset \overline{\mathbb{K}}[X_1, \dots, X_n, Y_1, \dots, Y_n]$$

et il existe une fonction polynomiale $Q : \overline{\mathbb{K}}^n \times \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^n$, $r \in \mathbb{N}^*$ tels que :

$$\forall x, y \in \overline{\mathbb{K}}^n,\ \big(P(x) - P(y)\big) Q(x, y) = (x - y)^r \tag{1}$$

Par non-surjectivité, il existe $x_0 \in \overline{\mathbb{K}}^n$ tel que :

$$\forall x \in \overline{\mathbb{K}}^n, P(x) - x_0 \neq 0$$

Donc

$$\forall x \in \overline{\mathbb{K}}^n,\ \mathrm{P}(x) - x_0 = 0 \implies \underbrace{1}_{\text{fonction constante égale à 1}}(x) = 0$$

et de même, il existe une fonction polynomiale $\mathrm{R} : \overline{\mathbb{K}}^n \to \overline{\mathbb{K}}^n$ telle que :

$$\forall x \in \overline{\mathbb{K}}^n,\ \big(\mathrm{P}(x) - x_0\big)\mathrm{R}(x) = 1 \tag{2}$$

On note k le sous-corps de $\overline{\mathbb{K}}$ engendré par $\mathbb{K}$, x_0, et les coefficients de P, Q, R : il est fini (car finiment engendré et chaque élément de k est algébrique sur $\mathbb{K}$, donc (lemme 6) $\dim_{\mathbb{K}} k < \infty$). Or, P peut être restreinte et corestreinte en une fonction polynomiale $\widetilde{\mathrm{P}} : k^n \to k^n$, qui reste injective et non-surjective. Comme k est fini, c'est absurde. □

Polynôme et fonction polynomiale associée

Comme $\overline{\mathbb{K}}$ est infini (sinon $\prod_{a \in \overline{\mathbb{K}}} \big(\mathrm{X} - a\big) + 1$ n'aurait pas de racines), on peut faire l'abus de langage de pas distinguer un polynôme et sa fonction polynomiale associée, car le morphisme d'anneaux qui à un polynôme associe sa fonction polynomiale associée est injectif (tout Q dans son noyau a une infinité de racines, et est donc nul).

— **Dans $\mathbb{C}$:** Par l'absurde, si $\mathrm{P} = (\mathrm{P}_1, \dots, \mathrm{P}_n) : \mathbb{C}^n \to \mathbb{C}^n$ est surjective mais non injective, on produit de même des fonctions polynomiales $\mathrm{Q} : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$, $\mathrm{R} : \mathbb{C}^n \to \mathbb{C}^n$, un complexe x_0 et un entier $r \in \mathbb{N}^*$ tels que :

$$\forall x, y \in \mathbb{C}^n,\ \begin{cases} \big(\mathrm{P}(x) - \mathrm{P}(y)\big)\mathrm{Q}(x,y) & = (x-y)^r \\ \big(\mathrm{P}(x) - x_0\big)\mathrm{R}(x) & = 1 \end{cases} \qquad \circledast$$

On note $\mathscr{E}$ l'ensemble formé par x_0 et les coefficients de P, Q, R ; et on pose $\mathrm{A} \overset{\text{déf}}{=} \mathbb{Z}[\mathscr{E}]$, dont on note I un idéal maximal.

- Montrons que le corps $\mathrm{A/I} = \mathbb{Z}[\mathscr{E}]/\mathrm{I}$ est fini :
  Supposons, par l'absurde, que le noyau du morphisme d'anneaux

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathbb{Z} & \to & \mathbb{Z}[\mathscr{E}]/\mathrm{I} \\ a & \mapsto & \overline{a} \end{cases}$$

  est trivial : alors on corestreint ϕ à $\phi(\mathbb{Z})$, et $\mathbb{Z} \cong \phi(\mathbb{Z}) \subset \mathrm{A/I}$. Comme A/I est une $\phi(\mathbb{Z})$-algèbre finiment engendrée, c'est aussi une $\mathfrak{Q}$-algèbre finiment engendrée, où $\mathfrak{Q} \cong \mathbb{Q}$.
  Par le lemme de Zariski, A/I est algébrique sur $\mathfrak{Q}$. Si on écrit $\mathrm{A/I} = \phi(\mathbb{Z})[\alpha_1, \dots, \alpha_m]$, on peut choisir $s \in \mathbb{Z}\backslash\{0\}$ tel que toutes les images par ϕ^{-1} des dénominateurs des coefficients des polynômes minimaux des $(\alpha_i)_{i \in [\![1,m]\!]}$ divisent s. Il vient alors que les $(\alpha_i)_{i \in [\![1,m]\!]}$, et donc le corps A/I, sont entiers sur $\phi(\mathbb{Z})[\overline{1}/\phi(s)]$, d'où $\phi(\mathbb{Z})[\overline{1}/\phi(s)]$ est un corps (lemme 10), et $(\overline{1}/(\phi(s) + \overline{1}) \in \phi(\mathbb{Z})[\overline{1}/\phi(s)]$. Donc

$$\overline{1} = (\phi(s) + \overline{1})\mathrm{P}(\overline{1}/\phi(s))$$

  où $\mathrm{P} \in \phi(\mathbb{Z})[\mathrm{X}]$, et pour $q \in \mathbb{N}$ assez grand :

$$\phi(s)^q = (\phi(s) + \overline{1})a$$

  où $a \in \phi(\mathbb{Z})$, ce qui est impossible, parce que tout diviseur irréductible de $\phi(s) + \overline{1}$ divise le membre de droite mais pas de gauche.

Donc $\mathrm{Ker}\,\phi$ est un idéal non trivial de $\mathbb{Z}$, et $\mathrm{Ker}\,\phi = p\mathbb{Z}$, pour un nombre premier p. Donc A/I est de caractéristique p, et il est isomorphe à une algèbre de type fini sur $\mathbb{F}_p$, laquelle est, par le lemme de ZARISKI, algébrique sur $\mathbb{F}_p$. Par le lemme 6, elle est donc un $\mathbb{F}_p$-espace vectoriel de dimension fini, et, de fait, de cardinal fini.

— Les formules $\circledast$ sont encore vraies dans une clôture algébrique de A/I : c'est impossible, car le théorème d'AX est vérifié dans les clôtures algébriques des corps finis, par le lemme introductif.

□

III AX À L'ÉPREUVE DE LA THÉORIE DES MODÈLES

III.1 NOTIONS DE BASE

III.1.1 SYNTAXE

Un système formel (par exemple : le calcul des prédicats (logique du premier ordre), dans lequel on se placera dans la suite) est constitué des éléments ci-après.

Langage : C'est un ensemble de symboles de fonctions et de prédicats (ou relations) d'arités (i.e : de "nombre d'argument") finies, ainsi que de constantes (fonctions d'arité nulle) : dans la suite, on se placera sur le langage des anneaux : $\mathscr{L}_{anneaux} = \{0, 1, +, \times\}$

On se donne un ensemble dénombrable de variables $\{x_i\}_{i\in\mathbb{N}}$.

Terme :

— une variable x_i $(i \in \mathbb{N})$

— OU une constante

— OU une fonction d'arité $n \in \mathbb{N}$ appliquée à n termes

Formule atomique : Un prédicat d'arité $n \in \mathbb{N}$ appliqué à n termes

Formule : Une expression construite par induction à partir des formules atomiques, et des symboles $((,),",")$ / connecteurs $(\to, \leftrightarrow, \neg, \wedge, \vee)$ / quantificateurs $(\forall, \exists)$ de la logique, en l'occurrence, du premier ordre.

Variables liées/libres : Dans une formule, une variable quantifiée est dite liée (libre sinon).

Énoncé/formule close : Une formule ne contenant que des variables liées.

Théorie : un ensemble d'énoncés. Les théories des anneaux commutatifs, des corps, des corps algébriquement clos de caractéristique $p \in \underbrace{\{\text{nombres premiers}\}}_{\text{noté } \mathbb{P}}$, et 0 sont respectivement :

$$
\begin{aligned}
\mathcal{T}_{\text{anneaux comm}} = \ \{ & \\
& \forall x_1, \forall x_2, \forall x_3, && (x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)\,; \\
& \forall x_1, && x_1 = x_1 + 0\,; \\
& \forall x_1, \exists x_2, && x_1 + x_2 = 0\,; \\
& \forall x_1, \forall x_2, && x_1 + x_2 = x_2 + x_1\,; \\
& \forall x_1, \forall x_2, \forall x_3, && (x_1 \times x_2) \times x_3 = x_1 \times (x_2 \times x_3)\,; \\
& \forall x_1, && x_1 \times 1 = 1 \times x_1\,; \\
& \forall x_1, \forall x_2, \forall x_3, && x_1 \times (x_2 + x_3) = x_1 \times x_2 + x_1 \times x_3\,; \\
& \forall x_1, \forall x_2, && x_1 \times x_2 = x_2 \times x_1\,; \\
& \}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{T}_{\text{corps}} = \quad & \{ \ \forall x_1, \exists x_2, && \neg(x_1 = 0) \longrightarrow (x_1 \times x_2 = 1) \ \} \\
\cup \quad & \mathcal{T}_{\text{anneaux comm}}
\end{aligned}
$$

$$
\begin{aligned}
\mathtt{CAC} = \quad & \mathcal{T}_{\text{corps}} \\
\bigcup_{n \in \mathbb{N}^*} \quad & \{ \ \forall x_1, \ldots, \forall x_n, \exists x_0, && x_0^n + x_n x_0^{n-1} + \ldots + x_2 x_0 + x_1 = 0 \ \}
\end{aligned}
$$

$$
\begin{aligned}
\mathtt{CAC}_p = \quad & \mathcal{T}_{\text{corps}} \\
\cup \quad & \mathtt{CAC} \\
\cup \quad & \{ \ p = 0 \ \}
\end{aligned}
$$

$$
\begin{aligned}
\mathtt{CAC}_0 = \quad & \mathcal{T}_{\text{corps}} \\
\cup \quad & \mathtt{CAC} \\
\bigcup_{q \in \mathbb{P}} \quad & \{ \ \neg(q = 0) \ \}
\end{aligned}
$$

III.1.2 Sémantique

Soit $\mathcal{L}$ un langage.

$\mathcal{L}$-structure : Un ensemble $\mathcal{M}$ (appelé domaine du discours) non vide, où on interprète les éléments de $\mathcal{L}$: i.e on choisit

- $c^{\mathcal{M}}$ pour chaque symbole de constante $c \in \mathcal{L}$
- ET $f^{\mathcal{M}} : \mathcal{M}^{n_f} \to \mathcal{M}$ pour chaque symbole de fonction $f \in \mathcal{L}$ d'arité n_f
- ET $\mathrm{P}^{\mathcal{M}} \subset \mathcal{M}^{n_\mathrm{P}}$ pour chaque symbole de prédicat $\mathrm{P} \in \mathcal{L}$ d'arité n_P

On interprète, ainsi, les $\mathcal{L}$-formules atomiques closes, puis les $\mathcal{L}$-énoncés de manière "usuelle" à partir des formules atomiques, par induction. On dit que la $\mathcal{L}$-structure $\mathcal{M}$ satisfait un énoncé θ, qu'on note $\mathcal{M} \vDash \theta$, si et seulement si θ une assertion vraie dans $\mathcal{M}$ (après l'avoir interprété). Pour une théorie $\mathcal{T}$ dont les énoncés sont tous vrais dans $\mathcal{M}$, on note, de même, $\mathcal{M} \vDash \theta$.

Modèle : $\mathcal{M}$ est un modèle de l'énoncé θ (resp. de la théorie $\mathcal{T}$) si, et seulement si, $\mathcal{M} \vDash \theta$ (resp. $\mathcal{M} \vDash \mathcal{T}$). Les modèles de $\mathcal{T}_{\text{anneaux comm}}$ sont les anneaux commutatifs, ceux de $\mathtt{CAC}_0$ sont les corps algébriquement clos de caractéristique nulle.

Satisfaisabilité : une théorie $\mathcal{T}$ est dite : satisfaisable si elle admet au moins un modèle, finiment satisfaisable si toute partie finie de $\mathcal{T}$ est satisfaisable.

Conséquence sémantique : on dit qu'un énoncé θ est une conséquence (sémantique) d'une théorie $\mathcal{T}$ si : pour tout modèle $\mathcal{M}$ de $\mathcal{T}$, $\mathcal{M} \vDash \theta$. On le note $\mathcal{T} \vDash \theta$.

III.2 Théorème de Compacité

III.2.1 Filtres, Ultrafiltres et Ultraproduits

Filtre : un filtre $\mathscr{F}$ sur un ensemble I est une partie de $\mathscr{P}(I)$ vérifiant :

- $\emptyset \notin \mathscr{F}$
- $\forall X \in \mathscr{F}, \forall Y \in \mathscr{P}(I), Y \supset X \Longrightarrow Y \in \mathscr{F}$
- $\forall X, Y \in \mathscr{F}, X \cap Y \in \mathscr{F}$

Ultrafiltre : un filtre maximal (pour l'inclusion).

Ultrafiltre principal/trivial : un ultrafiltre de la forme $\mathscr{U}_{X_0} \overset{\text{déf}}{=} \{Y \in \mathscr{P}(I) \mid Y \supset X_0\}$, pour une partie $X_0 \subset I$.

Filtre de Frechet : Si I est infini, c'est l'ensemble des parties cofinies de I : $\mathtt{Fr} \overset{\text{déf}}{=} \{Y \in \mathscr{P}(I) \mid I\backslash Y \text{ est finie}\}$. Il n'est pas principal (si $Y \in \mathtt{Fr}$, $Y\backslash\{y\} \in \mathtt{Fr}$, pour tout $y \in Y$).

Propriété de l'intersection finie : Une famille $\mathscr{X}$ de parties de I a la "propriété de l'intersection finie" si : $\forall X_1, \dots, X_n \in \mathscr{X}, \bigcap_{i=1}^{n} X_i \neq \emptyset$. Tout filtre a la propriété de l'intersection finie.

Lemmes sur les ultrafiltres

(A) Tout filtre $\mathscr{F}$ sur I est un ultrafiltre si, et seulement si : $\forall X \in \mathscr{P}(I), X \notin \mathscr{F} \Longrightarrow I\backslash X \in \mathscr{F}$.

(B) Tout filtre sur I est inclus dans un ultrafiltre.

(C) Toute famille $\mathscr{X}$ de parties de I ayant la propriété de l'intersection finie est incluse dans un ultrafiltre.

(D) Si I est infini : si $\mathscr{U}$ est un ultrafiltre non principal, il contient le filtre de Fréchet.

(E) **Mesure associée à un ultrafiltre** : tout ultrafiltre sur I correspond à la donnée d'une mesure finiment additive.

Démonstration: (A) Pour tout filtre $\mathscr{F}$ et toute partie X telle $X \notin \mathscr{F}$: $\mathscr{F} \cup \{X\}$ n'a pas la propriété de l'intersection finie si, et seulement si, $I\backslash X \in \mathscr{F}$.

- En effet : $\Longleftarrow$: Si $I\backslash X \in \mathscr{F}$, $(I\backslash X) \cap X = \emptyset$
  $\Longrightarrow$: Si $\mathscr{F} \cup \{X\}$ n'a pas cette propriété, il existe $X_1, \dots, X_n \in \mathscr{F}$ tels que $X_1 \cap \dots \cap X_n \cap X = \emptyset$, d'où $(I\backslash X) \supset X_1 \cap \dots \cap X_n$, et $I\backslash X \in \mathscr{F}$

Donc l'implication directe est acquise, et réciproquement, si "$\forall X \in \mathscr{P}(I), X \notin \mathscr{F} \Longrightarrow I\backslash X \in \mathscr{F}$" : $\mathscr{F} \cup \{X\}$ ne peut être un filtre (et donc avoir la propriété de l'intersection finie) que si $I\backslash X \notin \mathscr{F}$, et donc (par hypothèse) que si $X \in \mathscr{F}$ (i.e $\mathscr{F} \cup \{X\} = \mathscr{F}$).

(B) L'ensemble $E_{\mathscr{F}}$ des filtres sur I contenant $\mathscr{F}$ est tel que tout sous-ensemble E' de $E_{\mathscr{F}}$ totalement ordonné (pour l'inclusion) a un majorant (le filtre qu'est l'union des éléments de E', par exemple), donc, par le lemme de Zorn, $E_{\mathscr{F}}$ a un élément maximal (un ultrafiltre).

(C) $\mathscr{X}$ est incluse dans le filtre $\mathscr{F}_{\mathscr{X}} \overset{\text{déf}}{=} \{Y \in \mathscr{P}(I) \mid \exists X_1, \dots, X_n \in \mathscr{X}; Y \supset X_1 \cap \dots \cap X_n\}$, lui-même inclus dans un ultrafiltre.

(D) Si $\mathscr{U}$ contenait une partie finie X_0, il serait le filtre principal $\mathscr{F}_{X_0}$ qu'elle engendre (il le contiendrait trivialement, et ne pourrait contenir de partie $Y \not\supset X_0$, car $\mathscr{U} \ni (I\backslash Y) \supset X_0$).
Donc, par (A), $\mathscr{U}$ contient toutes les parties cofinies.

(E) À tout ultrafiltre $\mathscr{U}$ sur I, on associe la mesure finiment additive $\mu_{\mathscr{U}} : \mathscr{P}(I) \to \{0,1\}$ définie par :

$$\forall X \in \mathscr{P}(I),\ \mu_{\mathscr{U}}(X) = 1 \iff X \in \mathscr{U}$$

Réciproquement : si $\mu : \mathscr{P}(I) \to \{0,1\}$ est une mesure finiment additive, $\mathscr{U}_\mu \overset{\text{déf}}{=} \mu^{-1}(\{1\})$ est un ultrafiltre.

— En effet : La seule propriété non triviale à vérifier pour montrer que c'est un filtre est la stabilité par intersection : si $\mu(X) = \mu(Y) = 1$, et, par l'absurde, $\mu(X \cap Y) = 0$: $1 = \mu(I) \geqslant \mu(X \cup Y) = \mu(X \backslash (X \cap Y)) + \mu(Y \backslash (X \cap Y)) = 2$.
De plus, pour tout partie $X \notin \mathscr{U}$, $1 = \mu((I \backslash X) \cup X) = \mu((I \backslash X) + \mu(X) = \mu((I \backslash X)$, d'où $\mathscr{U} \ni (I \backslash X)$, et $\mathscr{U}$ est un ultrafiltre, par (A).

Dans la suite, on confondra un ultrafiltre et la mesure finiment additive qui lui est naturellement associée.

□

Ultrafiltres : remarque qualitative

Intuitivement, un ultrafiltre correspond à la donnée des "grandes" parties de I, de telle sorte que toute partie est soit "grande" ($\mathscr{U}$-presque sûre) soit "petite" ($\mathscr{U}$-négligeable). Si I est infini et $\mathscr{U}$ non trivial, on convient que $X \subset I$ est "grande" si, et seulement si, son complémentaire est "petit", que toute intersection finie de parties "grandes" reste "grande" et que I tout entier est "grand".

Soient $(\mathscr{M}_i)_{i \in I}$ une famille de $\mathscr{L}$-structures et $\mathscr{U}$ un ultrafiltre sur I.

Égalité $\mathscr{U}$-presque partout : On définit, sur $\prod_{i \in I} \mathscr{M}_i$, une relation d'équivalence d'"égalité $\mathscr{U}$-presque partout" par :

$$\forall M, N \in \prod_{i \in I} \mathscr{M}_i,\ M \overset{\mathscr{U}\text{-pp}}{=} N \iff \{i \in I \mid M_i = N_i\} \in \mathscr{U} \iff \mu_{\mathscr{U}}\big(\{i \in I \mid M_i = N_i\}\big) = 1$$

Ultraproduit : L'ultraproduit $\mathscr{M}^*$ des $\mathscr{M}_i$ ($i \in I$) par l'ultrafiltre $\mathscr{U}$ est le quotient de $\prod_{i \in I} \mathscr{M}_i$ par la relation d'équivalence $\overset{\mathscr{U}\text{-pp}}{=}$. On le note $\prod_{i \in I} \mathscr{M}_i \Big/ \mathscr{U}$.

L'ultraproduit est une $\mathscr{L}$-structure

$\mathscr{M}^* \overset{\text{déf}}{=} \prod_{i \in I} \mathscr{M}_i \Big/ \mathscr{U}$ est une $\mathscr{L}$-structure.

C'est le cas en interprétant

— $c^{\mathscr{M}^*} \overset{\text{déf}}{=} \overline{(c^{\mathscr{M}_i})_{i \in I}}$ pour chaque symbole de constante $c \in \mathscr{L}$

— $f^{\mathscr{M}^*} : (\mathscr{M}^*)^{n_f} \to \mathscr{M}^*,\ \left(\overline{M^{(1)}}, \dots, \overline{M^{(n_f)}}\right) \mapsto \overline{\left(f^{\mathscr{M}_i}\left(M_i^{(1)}, \dots, M_i^{(n_f)}\right)\right)_{i \in I}}$ pour chaque symbole de fonction $f \in \mathscr{L}$ d'arité n_f

— chaque symbole de prédicat $P \in \mathscr{L}$ d'arité n_P par :

$$\left(\overline{M^{(1)}}, \dots, \overline{M^{(n_P)}}\right) \in P^{\mathscr{M}^*} \subset (\mathscr{M}^*)^{n_P} \iff \left\{i \in I \mid \left(M_i^{(1)}, \dots, M_i^{(n_P)}\right) \in P^{\mathscr{M}_i}\right\} \in \mathscr{U}$$

Ultraproduits : remarques qualitatives

— Ce qui est embêtant, c'est que toutes les formules du premier ordre ne sont pas préservées par passage au produit, en général : le fait que chaque M_i ($i \in \mathrm{I}$) satisfasse une formule ϕ n'implique pas qu'il en est de même pour le produit cartésien.
Par (contre-)exemple, la disjonction "$\vee$" de l'énoncé "$\forall x_1, \underbrace{(x_1 = 0)}_{\text{noté } \mathrm{A}(x_1)} \vee \underbrace{(\exists x_2,\ x_1 \times x_2 = 1)}_{\text{noté } \mathrm{B}(x_1)}$"
condamne l'ensemble des modèles de $\mathscr{T}_{corps}$ à ne par être stable par produit cartésien (le connecteur "$\vee$" est "trop laxiste" : A(0) est vrai et B(0) est faux / A(1) est faux et B(1) est vrai : ce qui condamne $\mathrm{A}\big((0,1)\big)$ ET $\mathrm{B}\big((0,1)\big)$ à être faux !).
En revanche, $\mathscr{T}_{anneaux\ comm}$ a des modèles stables par produit cartésien, car ses énoncés sont des identités algébriques (i.e des clôtures par le quantificateur universel "$\forall$" de formules atomiques).

— Intuitivement, un ultraproduit des structures $\mathscr{M}_i$ ($i \in \mathrm{I}$) est une forme de "moyenne", ou d'"intégrale", des structures calculée par rapport à la mesure "de probabilité" (seulement finiment additive, et pas σ-additive) associée à $\mathscr{U}$, de telle sorte qu'on pourrait le noter :

$$\int_{\mathrm{I}} \mathscr{M}(i)\, \mathrm{d}\mu_{\mathscr{U}}(i)$$

Un ultrafiltre principal associé $\{i_0\}$ est dit "trivial" car il "correspond" à une mesure de Dirac concentrée en $\{i_0\}$: l'"intégrale" vaut simplement $\mathscr{M}_{i_0}$. Si I est infini, un ultrafiltre non principal (contenant donc le filtre de FRÉCHET) correspond à une mesure diffuse : les résultats sont plus riches.

— L'interprétation d'un ultraproduit en tant que que $\mathscr{L}$-structure est une interprétation "presque partout" relativement au produit cartésien : "un élément du produit cartésien est le représentant de l'interprétation d'une constante/de l'image par l'interprétation d'une fonction d'un n_f-uplet" OU "des éléments sont en relation dans l'ultraproduit" si c'est le cas en presque toutes coordonnées.

III.2.2 THÉORÈME DE ŁOŚ

Théorème - Théorème de ŁOŚ

Une formule est vraie dans un ultraproduit si, et seulement si, elle est vraie en presque toutes coordonnées :

Si $\mathscr{M}^* \overset{\text{déf}}{=} \prod_{i\in\mathrm{I}} \mathscr{M}_i \big/ \mathscr{U}$ est un ultraproduit de $\mathscr{L}$-structures, $\phi(x_1, \dots, x_n)$ une $\mathscr{L}$-formule, et $\mathrm{M}^* = \left(\overline{\mathrm{M}^{(1)}}, \dots, \overline{\mathrm{M}^{(n)}}\right) \in (\mathscr{M}^*)^n$, alors :

$$\mathscr{M}^* \vDash \phi(\mathrm{M}^*) \iff \left\{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \phi\big(\mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\big) \right\} \in \mathscr{U}$$

Démonstration: Pour toute $\mathscr{L}$-formule ψ, on note $\mathrm{I}(\psi)$ l'ensemble $\left\{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \psi\big(\mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\big) \right\}$.
Par induction structurelle :

— Si ϕ est atomique, cela résulte de l'interprétation des $\mathscr{L}$-prédicats et $\mathscr{L}$-termes dans la $\mathscr{L}$-structure $\mathscr{M}^*$.

— Si $\phi = \neg\psi$,

$$\mathrm{I}(\phi) \in \mathscr{U} \iff \mathrm{I}\backslash\mathrm{I}(\phi) = \left\{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \psi\left(\mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\right) \right\} \notin \mathscr{U}$$

car $\mathscr{U}$ est un ultrafiltre. On conclut par hypothèse d'induction.

— Si $\phi = \psi \wedge \chi$: pour que $\mathrm{I}(\phi) \in \mathscr{U}$, il faut (car $\mathrm{I}(\phi) \subset \mathrm{I}(\psi), \mathrm{I}(\chi)$) et il suffit (par stabilité par intersection) que $\mathrm{I}(\psi) \in \mathscr{U}$ et $\mathrm{I}(\chi) \in \mathscr{U}$, puisque $\mathscr{U}$ est un filtre. On conclut par hypothèse d'induction.

— Si $\phi(x_1, \dots, x_n) = \exists x_0, \psi(x_0, x_1, \dots, x_n)$:

— $\Longrightarrow$: Si $\mathscr{M}^* \vDash \phi(\mathrm{M}^*)$, il existe $\overline{\mathrm{M}^{(0)}} \in \mathscr{M}^*$ tel que $\mathscr{M}^* \vDash \psi\left(\overline{\mathrm{M}^{(0)}}, \mathrm{M}^*\right)$, et, par hypothèse d'induction :

$$\mathscr{U} \ni \left\{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \psi\left(\mathrm{M}_i^{(0)}, \mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\right) \right\} \subset \left\{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \exists x_0, \psi\left(x_0, \mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\right) \right\} = \mathrm{I}(\phi)$$

Donc $\mathrm{I}(\phi) \in \mathscr{U}$, car $\mathscr{U}$ est un filtre.

— $\Longleftarrow$: Si $\mathrm{I}(\phi) \in \mathscr{U}$, pour tout $i \in \mathrm{I}(\phi)$: par l'axiome du choix, il existe $\mathrm{M}_i^{(0)} \in \mathscr{M}_i$ tel que $\mathscr{M}_i \vDash \psi\left(\mathrm{M}_i^{(0)}, \mathrm{M}_i^{(1)}, \dots, \mathrm{M}_i^{(n)}\right)$. En notant, pour tout $j \in \mathrm{I}\backslash\mathrm{I}(\phi)$, $\mathrm{M}_j^{(0)}$ un élément quelconque de $\mathscr{M}_j \neq \emptyset$ (avec l'axiome du choix), il vient que : $\mathrm{M}^{(0)} \in \prod_{i\in\mathrm{I}} \mathscr{M}_i$ est tel que

$$\mathscr{M}^* \vDash \psi\left(\overline{\mathrm{M}^{(0)}}, \mathrm{M}^*\right)$$

par hypothèse d'induction (comme $\mathrm{I}(\phi) \in \mathscr{U}$), et

$$\mathscr{M}^* \vDash \phi(\mathrm{M}^*)$$

est acquis.

Pour conclure, on utilise le fait que : $\forall x_0, \phi \equiv \neg(\exists x_0, \neg\phi)$; $\phi \vee \psi \equiv \neg(\neg\phi \wedge \neg\psi)$; $\phi \longrightarrow \psi \equiv \neg(\phi \wedge \neg\psi)$; et $\phi \longleftrightarrow \psi \equiv (\phi \longrightarrow \psi) \wedge (\psi \longrightarrow \phi)$. □

III.2.3 Théorème de Compacité

Théorème - Théorème de Compacité

Une théorie est satisfaisable si et seulement si elle est finiment satisfaisable.

Démonstration: Soit $\mathscr{T}$ une théorie finiment satisfaisable, dont on note I l'ensemble des parties finies. Par hypothèse : pour tout $i \in \mathrm{I}$, il existe un modèle $\mathscr{M}_i$ tel que $\mathscr{M}_i \vDash i$.
Pour tout $\theta \in \mathscr{T}$, on pose $\mathrm{I}(\theta) \overset{\text{déf}}{=} \{ i \in \mathrm{I} \mid \mathscr{M}_i \vDash \theta \}$.
La famille $(\mathrm{I}(\theta))_{\theta\in\mathscr{T}}$ est incluse dans un ultrafiltre $\mathscr{U}$, car elle admet la propriété de l'intersection finie ($\forall \theta_1, \dots, \theta_n \in \mathscr{T}, \emptyset \neq \bigcap_{k=1}^{n} \mathrm{I}(\theta_k) \ni \{\theta_1, \dots, \theta_n\}$).
L'ultraproduit $\mathscr{M}^* \overset{\text{déf}}{=} \prod_{i\in\mathrm{I}} \mathscr{M}_i \Big/ \mathscr{U}$ est alors un modèle de $\mathscr{T}$, puisque : si $\theta \in \mathscr{T}$, $\mathrm{I}(\theta) \in \mathscr{U}$, d'où, par Łoś, $\mathscr{M}^* \vDash \theta$.

□

Est-il trop "fort" de recourir à l'axiome du choix ?

Le recours à l'axiome du choix (équivalent au lemme de Zorn) - pour démontrer l'existence, pour tout filtre, d'un ultrafiltre le contenant ET dans le théorème de Łoś - peut paraître trop "fort". Mais il n'en est rien : la démonstration "classique" du théorème de compacité repose sur le théorème de complétude de Gödel ("une théorie est satisfaisable si, et seulement si, elle est cohérente/consistante/non contradictoire"), qui y a aussi recours.

Corollaire 1 du théorème de compacité

Si $\mathscr{T}$ est une théorie, θ un énoncé tels que $\mathscr{T} \vDash \theta$, alors il existe une partie finie $F \subset \mathscr{T}$ telle que $F \vDash \theta$

Démonstration: On montre la contraposée. Si, pour toute partie finie $F \subset \mathscr{T}$: $F \nvDash \theta$, c'est-à-dire qu'il existe un modèle $\mathscr{M}_F$ de F qui satisfait $\neg\theta$, alors $\mathscr{T} \cup \{\neg\theta\}$ est finiment satisfaisable, et, par compacité, est satisfaisable : cela contredit "$\mathscr{T} \vDash \theta$". □

Corollaire 2 du théorème de compacité

Dans le langage des anneaux : si θ est un énoncé qui est vrai dans des corps de caractéristiques $p \in \mathbb{P}$, pour p arbitrairement grand, alors il existe un corps de caractéristique nulle qui satisfait θ.

Démonstration: On montre la contraposée, appliquée à $\neg\theta$: si θ est un énoncé vrai dans tous les corps de caractéristique nulle, alors il existe $q \in \mathbb{P}$ tel que θ est vrai dans tous les corps de caractéristique supérieure à q.
On pose $T \overset{\text{déf}}{=} \mathscr{T}_{corps} \cup \{p \neq 0\}_{p\in\mathbb{P}}$, dont les modèles sont les corps de caractéristique nulle. Par hypothèse, $T \vDash \theta$, donc il existe une partie finie $F \subsetneq T$ telle que $F \vDash \theta$ (par le corollaire 1).
Or, $F \subset \mathscr{T}_{corps} \cup \{p \neq 0\}_{p\in\mathbb{P}\cap[\![0,q-1]\!]}$, pour un $q \in \mathbb{P}$. Par suite, tout corps de caractéristique supérieure à q est un modèle de F, et donc aussi de θ. □

Ce n'est pas fini

Avec ce deuxième corollaire, on pourrait croire qu'on est à deux doigts du théorème d'Ax - modulo la démonstration du fait qu'il se formule comme un ensemble d'énoncés dans le langage des anneaux, et qu'il est vrai dans des corps de caractéristique arbitrairement grande (ces deux derniers points sont vrais). Mais il n'en est rien : il n'est pas dit que le corps de caractéristique nulle satisfaisant le théorème d'Ax - dont l'existence est avérée - est isomorphe à $\mathbb{C}$ (penser à $\mathbb{Q}$).

III.3 Théorème d'Ax

III.3.1 Cardinalité d'un ultraproduit & $2^{\aleph_0}$-catégoricité de $\mathtt{CAC}_p$

Théorème - κ-catégoricité de $\mathtt{CAC}_p$

Tous corps algébriquement clos $\mathbb{K}$, $\mathbb{L}$ de même cardinal κ non dénombrable et de même caractéristique $p \in \{0\} \cup \mathbb{P}$ sont isomorphes.
On dit que $\mathtt{CAC}_p$ est κ-catégorique.

Démonstration: —

Un corps algébriquement clos est déterminé, à isomorphisme près, par sa caractéristique et son degré de transcendance sur son sous-corps premier

Deux corps algébriquement clos K_1, K_2 sont isomorphes si, et seulement si, ils ont la même caractéristique et le même degré de transcendance sur leur sous-corps premier.

Démonstration: L'implication directe est évidente.
Réciproquement, si K_1 est de degré de transcendance k sur son sous-corps premier π, alors pour toute base de transcendance S de cardinalité k, $K_1 \cong \overline{\pi(S)}$. Comme il en est de même de K_2, le résultat est acquis. □

— Comme κ est non dénombrable, $\mathbb{K}$ et $\mathbb{L}$ ont le même degré de transcendance sur leur sous-corps premier au plus dénombrable : κ. En effet, l'ensemble des éléments algébriques sur ce sous-corps premier au plus dénombrable reste dénombrable (l'ensemble des polynômes minimaux est dénombrable). Le lemme introductif conclut.

□

Lemme : Cardinalité de l'ultraproduit d'une famille dénombrable d'ensembles dénombrables.

Soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{N}$.
Si $\mathcal{M}^* \overset{\text{déf}}{=} \prod_{i\in\mathbb{N}} \mathcal{M}_i \Big/ \mathcal{U}$ est un ultraproduit de $\mathcal{L}$-structures dénombrables, alors $\mathcal{M}^*$ est de cardinalité égale à $|\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$

Démonstration: Pour tout $i \in \mathbb{N}$, $\mathcal{M}_i$ est de la forme $\{m_n^{(i)}\}_{n\in\mathbb{N}}$.
On construit un ensemble $\mathrm{F} \subset \mathbb{N}^{\mathbb{N}}$ de fonctions telles que : si $f, g \in \mathrm{F}$ sont différentes, elles sont $\mathcal{U}$-presque partout différentes (i.e $\left\{i \in \mathbb{N} \mid f(i) \neq g(i)\right\} \in \mathcal{U} \iff \left\{i \in \mathbb{N} \mid f(i) = g(i)\right\} \notin \mathcal{U} \iff \left\{i \in \mathbb{N} \mid f(i) = g(i)\right\}$ est fini).
$\mathrm{F} \overset{\text{déf}}{=} \left\{f_\delta \overset{\text{déf}}{=} n \mapsto \sum_{m<n} \delta(m)2^m\right\}_{\delta\in\{0,1\}^{\mathbb{N}}}$ convient, et vérifie $|\mathrm{F}| = 2^{\aleph_0} = |\mathcal{P}(\mathbb{N})|$.
L'application :

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathrm{F} & \to & \prod_{i\in\mathbb{N}} \mathcal{M}_i \Big/ \mathcal{U} \\ f & \mapsto & \overline{\left(m_{f(i)}^{(i)}\right)_{i\in\mathbb{N}}} \end{cases}$$

est injective :

- **En effet :** Pour toutes $f, g \in \mathrm{F}$, si $f \neq g$: $\mathcal{U} \not\ni \left\{i \in \mathbb{N} \mid f(i) = g(i)\right\} = \left\{i \in \mathbb{N} \mid m_{f(i)}^{(i)} = m_{g(i)}^{(i)}\right\}$, d'où : $\overline{\left(m_{f(i)}^{(i)}\right)_{i\in\mathbb{N}}} \neq \overline{\left(m_{g(i)}^{(i)}\right)_{i\in\mathbb{N}}}$.

□

Raffinement

On aurait pu seulement supposer les $(\mathcal{M}_i)_{i\in\mathbb{N}}$ de cardinalités non bornées : en effet, en notant n_i le plus petit entier tel que $|\mathcal{M}_i| \geqslant 2^{n_i} > f(n_i)$,

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathrm{F} & \to & \prod_{i\in\mathbb{N}} \mathcal{M}_i \Big/ \mathcal{U} \\ f & \mapsto & \overline{\left(m_{f(n_i)}^{(i)}\right)_{i\in\mathbb{N}}} \end{cases}$$

convenait.

III.3.2 Théorème de transfert

Théorème - Les $\mathbb{F}_p$ "tendent" vers $\mathbb{C}$

Pour tout $\mathrm{P} \subset \mathbb{P}$ infini, et tout ultrafiltre non principal $\mathcal{U}$ sur P :
L'ultraproduit de la famille des clôtures algébriques des $\left(\mathbb{F}_p\right)_{p\in\mathrm{P}}$ est isomorphe à $\mathbb{C}$.

Démonstration: On note $\mathbb{K}^* \overset{\text{déf}}{=} \prod_{p\in\mathrm{P}} \overline{\mathbb{F}_p} \Big/ \mathcal{U}$ cet ultraproduit, et on pose $\mathbb{K}_p \overset{\text{déf}}{=} \overline{\mathbb{F}_p}$.

(A) $\mathbb{K}^*$ **est un corps algébriquement clos :**
En effet :
Pour tout $p \in \mathbb{P}$, $\mathbb{K}_p$ satisfait CAC, donc par Łoś, $\mathbb{K}^*$ aussi.

(B) $\mathbb{K}^*$ **est de caractéristique nulle :**
En effet :
Pour tout $q \in \mathbb{P}$, $\{p \in \mathrm{P} \mid \mathbb{K}_p \vDash q \neq 0\}$ est cofini, et appartient donc à $\mathscr{U}$. Il s'ensuit, par Łoś, que $\mathbb{K}^* \vDash q \neq 0$.

(C) $\mathbb{K}^*$ **est isomorphe à** $\mathbb{C}$ **:**
En effet :
Par le lemme sur la cardinalité de l'ultraproduit d'une famille dénombrable d'ensembles dénombrables, $\mathbb{K}^*$ a la cardinalité - non dénombrable - de $\mathbb{C}$. Comme ces deux corps sont en plus algébriquement clos et de même caractéristique (nulle), ils sont isomorphes, par le théorème de catégoricité de la section précédente.

□

Remarque
On peut voir $\mathbb{C}$ comme la "limite" des $\mathbb{F}_p$, quand p tend vers l'infini, dans le sens très précis évoqué plus haut.

Théorème - Théorème de Transfert

Toute théorie $\mathscr{T}$ du langage des anneaux est vraie dans $\mathbb{C}$ dès qu'elle est vraie dans les clôtures algébriques des $\mathbb{F}_p$, pour une infinité de nombres premiers p.

Démonstration: On note P l'ensemble des nombres premiers p tels que $\overline{\mathbb{F}_p}$ satisfait $\mathscr{T}$, $\mathscr{U}$ un ultrafiltre non principal sur P.
Par le théorème précédent, $\mathbb{C}$ est isomorphe à $\mathbb{K}^* \overset{\text{déf}}{=} \prod_{p\in\mathrm{P}} \overline{\mathbb{F}_p}\big/\mathscr{U}$, qui est lui-même un modèle de $\mathscr{T}$, par Łoś. Donc $\mathbb{C}$ satisfait $\mathscr{T}$. □

III.3.3 Théorème d'Ax

Lemme : Clôture algébrique de $\mathbb{F}_p$
Soit $p \in \mathbb{P}$.
"La" (à isomorphisme près) clôture algébrique de $\mathbb{F}_p$ est localement finie.

Démonstration:
Pour tous $n < k \in \mathbb{N}^*$, on note f_n^k un plongement de $\mathbb{F}_{p^{n!}}$ dans $\mathbb{F}_{p^{k!}}$ (dont l'existence a été précédemment assurée, puisque $n!|k!$). On note $\overline{\mathbb{F}_p}$ l'ensemble quotient de $\mathrm{E} \overset{\text{déf}}{=} \bigsqcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^{n!}}$ par la relation d'équivalence :

$$\forall x, y \in \mathrm{E}, \forall n, m \in \mathbb{N}^*,\ (p^{n!}, x) \sim (p^{m!}, y) \Leftrightarrow \exists k \in \mathbb{N}^*,\ n \leqslant k,\ m \leqslant k \text{ et } f_n^k(x) = f_m^k(y)$$

Pour tout $n \in \mathbb{N}^*$, $\mathbb{F}_{p^{n!}}$ s'injecte dans $\overline{\mathbb{F}_p}$ par l'application :

$$\phi_{p^{n!}} \overset{\text{déf}}{=} \left\{ \begin{array}{ccc} \mathbb{F}_{p^{n!}} & \to & \overline{\mathbb{F}_p} \\ x & \mapsto & \overline{(p^{n!}, x)} \end{array} \right.$$

$\overline{\mathbb{F}_p}$ intuitivement

Intuitivement, $\overline{\mathbb{F}_p}$ se comprend comme étant la "réunion" de la chaîne croissante[a] :

$$\mathbb{F}_p \subset \mathbb{F}_{p^2} \subset \mathbb{F}_{p^6} \subset \ldots \subset \mathbb{F}_{p^{n!}} \subset \ldots$$

a. "est inclus" étant à comprendre au sens de "s'injecte dans"

Montrons que :

(A) **$\overline{\mathbb{F}_p}$ est une extension algébrique de $\mathbb{F}_p$:**

— $\overline{\mathbb{F}_p}$ est un corps :
Soient $a \in \mathbb{F}_{p^{n!}}, b \in \mathbb{F}_{p^{m!}}$. Or, $\mathbb{F}_{p^{n!}}$ et $\mathbb{F}_{p^{m!}}$ sont isomorphes à deux sous-corps de $\mathbb{F}_{p^{\max(m,n)!}}$, dont a et b peuvent être comme des éléments (par isomorphisme). L'addition et la multiplication se font alors dans $\mathbb{F}_{p^{\max(m,n)!}}$, et, de plus, tout élément non nul (dans $\overline{\mathbb{F}_p}$) admet un inverse.

— $\overline{\mathbb{F}_p}$ est algébrique sur $\mathbb{F}_p$, car tous les $\mathbb{F}_{p^{n!}}$ ($n \in \mathbb{N}^*$) sont des $\mathbb{F}_p$-espaces vectoriels[2] de dimension finie.

(B) **$\overline{\mathbb{F}_p}$ est algébriquement clos :**
Soit $P \in \overline{\mathbb{F}_p}[X]$ un polynôme de degré supérieur à 1.

— **Cas 1 :** P a une racine[3] dans $\mathbb{F}_p$.
Alors P a une racine dans $\overline{\mathbb{F}_p}$, puisque $\mathbb{F}_p$ s'injecte dans $\overline{\mathbb{F}_p}$.

— **Cas 2 :** P est irréductible sur $\mathbb{F}_p$.
Alors, en posant $n \overset{\text{déf}}{=} \deg P$, P a une racine dans $\mathbb{F}_{p^n}$:

- En effet :
L'anneau $K \overset{\text{déf}}{=} \mathbb{F}_p[X]/(P)$ est un corps (car P est irréductible), qui un $\mathbb{F}_p$-espace vectoriel de dimension $\deg P = n$ (car $\mathbb{F}_p[X]$ est euclidien). Par unicité des corps finis, il vient donc que $\mathbb{F}_p[X]/(P) \cong \mathbb{F}_{p^n}$. L'image de X par cet isomorphisme est donc racine du polynôme $X^{p^n} - X$, d'où P divise $X^{p^n} - X$, qui est scindé sur $\mathbb{F}_{p^n}$.

Or, $\mathbb{F}_{p^n}$ s'injecte dans $\mathbb{F}_{p^{n!}}$, qui lui-même s'injecte dans $\overline{\mathbb{F}_p}$: P a une racine dans $\overline{\mathbb{F}_p}$.

Donc $\overline{\mathbb{F}_p}$ **est une clôture algébrique** de $\mathbb{F}_p$, et, de par son expression, tout sous-corps finiment engendré de $\overline{\mathbb{F}_p}$ est fini (puisqu'isomorphe à un sous-corps d'un $\mathbb{F}_{p^{n!}}$, pour n assez grand) : $\overline{\mathbb{F}_p}$ est localement finie. □

Théorème - AX - GROTHENDIECK

Toute fonction polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$ qui est injective est bijective.

Démonstration: — **Pour les clôtures algébriques $\overline{\mathbb{F}_p}$ des $\mathbb{F}_p$**
Soit $p \in \mathbb{P}$.
Toute fonction polynomiale P de $\overline{\mathbb{F}_p}^n$ dans $\overline{\mathbb{F}_p}^n$ qui est injective est bijective.

2. en identifiant leur sous-corps premier avec $\mathbb{F}_p$
3. en voyant P comme polynôme de $\mathbb{F}_p[X]$, ce qui est loisible car $\mathbb{F}_p$ s'injecte dans $\overline{\mathbb{F}_p}$

Démonstration: Soit $P = (P_1, \dots, P_n) : \overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ une fonction polynomiale injective, et $y = (y_1, \dots, y_n) \in \overline{\mathbb{F}_p}^n$.
On note k le sous-corps de $\overline{\mathbb{F}_p}$ engendré par $y_1, \dots, y_n$ et les coefficients de $P_1, \dots, P_n$: il est fini, car $\overline{\mathbb{F}_p}^n$ est localement finie (par le lemme précédent).
L'image de $P_{|k^n}$ est incluse dans k^n (puisque chaque composante est incluse dans $\{k[a]\}_{a\in k} \subset k$). Donc $P_{|k^n}$ est une application injective entre ensembles finis de même cardinal : elle est surjective, et il existe $x \in k^n$ tel que $k^n \ni y = P(x)$.

P est donc surjective. □

— **Le théorème d'**Ax **s'énonce par une infinité d'énoncés du premier ordre** (dans le langage des anneaux) :
On pose, pour tout corps $\mathbb{K}$, fonction polynomiale $P(P_1, \dots, P_n) : \mathbb{K}^n \to \mathbb{K}^n$ de degré $d \in \mathbb{N}^*$:

$$\text{Inj}_d\ (p_{0,0,\dots,0}, p_{1,0,\dots,0}, \dots, p_{d,0,\dots,0}, p_{0,1,\dots,0} \dots, p_{d,d,\dots,d}) \overset{\text{déf}}{=} \text{"}\forall x_1, \dots, x_n, \forall y_1, \dots, y_n,$$
$$\bigwedge_{k=1}^{n} \sum_{i_1+\dots+i_n \leqslant d} p_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n} = \sum_{i_1+\dots+i_n \leqslant d} p_{i_1,\dots,i_n} y_1^{i_1} \cdots y_n^{i_n} \longrightarrow \bigwedge_{k=1}^{n} x_k = y_k\text{"}$$

$$\text{Surj}_d(p_{0,0,\dots,0}, p_{1,0,\dots,0}, \dots, p_{d,0,\dots,0}, p_{0,1,\dots,0} \dots, p_{d,d,\dots,d}) \overset{\text{déf}}{=} \text{"}\forall y_1, \dots, y_n, \exists x_1, \dots, x_n,$$
$$\bigwedge_{k=1}^{n} \sum_{i_1+\dots+i_n \leqslant d} p_{i_1,\dots,i_n} x_1^{i_1} \cdots x_n^{i_n} = y_k\text{"}$$

$$\text{Ax}(d) \overset{\text{déf}}{=} \text{"}\forall p_{0,0,\dots,0}, p_{1,0,\dots,0}, \dots, p_{d,0,\dots,0}, p_{0,1,\dots,0} \dots, p_{d,d,\dots,d},$$
$$\text{Inj}_d(p_{0,0,\dots,0}, \dots, p_{d,d,\dots,d}) \longrightarrow \text{Surj}_d(p_{0,0,\dots,0}, \dots, p_{d,d,\dots,d})\text{"}$$

$$\mathscr{T}_{\text{Ax}} \overset{\text{déf}}{=} \{\text{Ax}(d)\}_{d\in\mathbb{N}^*}$$

$\mathbb{K}$ vérifie alors le théorème d'Ax si, et seulement si, $\mathbb{K} \vDash \mathscr{T}_{\text{Ax}}$

— **Dans $\mathbb{C}$:** Pour tout $p \in \mathbb{P}$, $\overline{\mathbb{F}_p} \vDash \mathscr{T}_{\text{Ax}}$: donc d'après le **théorème de transfert**, $\mathbb{C} \vDash \mathscr{T}_{\text{Ax}}$, et le théorème d'Ax est démontré.

□

ANNEXE

Lemmes pour le Lemme de Zariski

Anneau factoriel : Un anneau commutatif A est dit factoriel si tout élément de A se décompose de manière unique, à ordre et association près, en un produit d'éléments irréductibles et d'un élément inversible.

Anneau intégralement clos : Un anneau intègre A est dit intégralement clos si : pour tous $a, b \in A\backslash\{0\}$, si a/b (élément du corps des fractions de A) est racine d'un polynôme unitaire à coefficients dans A alors $a/b \in A$.

Idéal maximal : Un idéal est dit maximal si tout idéal qui le contient strictement est l'anneau lui-même.

— **Lemme 1 : Caractérisation des idéaux maximaux**
Dans un anneau commutatif A : l'idéal I est maximal si, et seulement si, A/I est un corps.

Démonstration: $\Longrightarrow$: Si I est maximal et $a \in (A/I)\backslash\{0\}$: en notant $a_0 \in A\backslash I$ un représentant de a, $I + a_0 A = A$ (puisque cet idéal contient strictement I). Donc $1 = a_0 b + i$, où $b \in A$, $i \in I$, et x est inversible.

$\Longleftarrow$: Si A/I est un corps et $I \subsetneq J \subset A$: il existe $a_0 \in J\backslash I$, dont la classe a vérifie donc $a \in (A/I)\backslash\{0\}$. Donc $1 = a_0 b + i \in J$, où $b \in A$, $i \in I$, et $J = A$. □

Lemme 2 : Anneau Principal $\Longrightarrow$ Factoriel

Tout anneau principal est factoriel.

Démonstration: Soit a_0 un élément d'un anneau principal A.
EXISTENCE, par l'absurde : si a_0 n'a pas de décomposition, alors $a_0 = a_1 b$ où $a_1 \notin A^*$ et $b \notin A^*$, b n'ayant pas non plus de décomposition (a est irréductible). On construit alors proche en proche une famille $(a_n)_{n\in\mathbb{N}}$ telle que $a_{n+1} \big| a_n$, avec a_{n+1} et a_n non associés. L'idéal $\langle a_n\rangle_{n\in\mathbb{N}}$ est alors de la forme cA, d'où : il existe $N \in \mathbb{N}$ tel que $c \in (a_n)_{n\in[\![0,N]\!]}$, donc $a_N \big| c \big| a_{N+1}$: absurde, car a_N et a_{N+1} ne sont pas associés.

UNICITÉ : Pour chaque élément irréductible p, $\langle p\rangle$ est maximal, car si $\langle p\rangle \subset \langle a\rangle \subset A$, alors $p = ab$ pour un $b \in A$, et a est une unité - d'où $\langle a\rangle = A$ - ou b est une unité - d'où $\langle a\rangle = \langle p\rangle$. Donc par le lemme 1, $A/\langle p\rangle$ est un corps. Si

$$up_1 \cdots p_n = vq_1 \cdots q_m \quad \circledast$$

avec $n, m > 0$ et des notations évidentes, alors en supposant, sans perte de généralité, que $\langle p_1\rangle$ ne contient aucun des $(\langle p_i\rangle)_{i\in[\![0,n]\!]}$ ni $(\langle q_i\rangle)_{i\in[\![0,m]\!]}$: p_1 est nécessairement associé à l'un des q_i, car sinon, par $\circledast$ dans $A/\langle p\rangle$, la classe de zéro est non nulle. On simplifie par l'élément régulier p_1, et on conclut par élimination de proche en proche. □

Lemme 3 : Anneau Factoriel $\Longrightarrow$ Intégralement clos

Tout anneau factoriel est intégralement clos.

Démonstration: Soit A un anneau factoriel, dont on note K le corps des fractions. Soit $u \overset{\text{déf}}{=} a/b \in K$ (où a et b sont premiers entre eux) tel que :

$$u^n + u_{n-1}c^{n-1} + \ldots + c_0 = 0$$

En multipliant par b^n :

$$a^n + c_{n-1}ba^{n-1} + \ldots + c_0 b^n = 0$$

Soit d un diviseur de b premier ou inversible. Si d est premier, $d|a^n$, d'où (par théorème de Gauss) $d|a$: ce qui n'est pas le cas (par hypothèse sur a et b). Donc d est une unité, et $u \in A$. □

Inclusions des théories

Anneaux commutatifs ⊃ Anneaux intègres ⊃ Anneaux intégralement clos ⊃ Anneaux à PGCD ⊃ Anneaux factoriels ⊃ Anneaux principaux ⊃ Anneaux euclidiens ⊃ Corps ⊃ Corps finis

LEMMES POUR LE NULLSTELLENSATZ FAIBLE

Lemme 4 : Extension algébrique d'un corps algébriquement clos

Un corps algébriquement clos $\mathbb{K}$ n'a pas d'extension algébrique propre

Démonstration: Si a est un élément d'une extension de corps de $\mathbb{K}$ algébrique sur $\mathbb{K}$: $P(a)=0$, pour un polynôme P à coefficients dans $\mathbb{K}$. On conclut que $a \in \mathbb{K}$ en utilisant le caractère scindé de P et l'intégrité de $\mathbb{K}$. □

Lemme 5 : Maximalité de $\langle X_1 - a_1, \dots, X_n - a_n \rangle$

Pour tous $a_1, \dots, a_n \in \mathbb{K}$, $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ est un idéal maximal de $\mathbb{K}[X_1, \dots, X_n]$

Démonstration: Le noyau du morphisme d'anneaux surjectif

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathbb{K}[X_1,\dots,X_n] & \to & \mathbb{K} \\ P(X_1,\dots,X_n) & \mapsto & P(a_1,\dots,a_n) \end{cases}$$

est l'idéal $\langle X_1 - a_1, \dots, X_n - a_n \rangle$:

- **En effet :** il le contient évidemment, et si $P \in \mathbb{K}[X_1, X_2]$ a pour racine (a_1, a_2) :

$$P = \underbrace{P(X_1,X_2) - P(X_1,a_2)}_{= (X_2-a_2)Q(X_1,X_2)\text{, où } Q \in \mathbb{K}[X_1,X_2]} + \underbrace{P(X_1,a_2) - P(a_1,a_2)}_{= (X_1-a_1)R(X_1)\text{, où } R \in \mathbb{K}[X_1,X_2]} \in \langle X_1 - a_1, X_2 - a_2 \rangle$$

  On conclut par une récurrence immédiate sur $k \in \mathbb{N}^*$, pour $\mathbb{K}[X_1, \dots, X_k]$

En factorisant ϕ, il vient que $\mathbb{K}[X_1, \dots, X_n] / \langle X_1 - a_1, \dots, X_n - a_n \rangle \cong \mathbb{K}$, d'où $\langle X_1 - a_1, \dots, X_n - a_n \rangle$ est maximal.

□

Lemmes pour le théorème d'Ax

Lemme 6 : Une A-algèbre B de type fini et engendrée par des éléments entiers sur A est un A-module fini

Soit A un anneau commutatif. Une A-algèbre B de type fini (i.e : finiment engendrée en tant qu'algèbre) engendrée par des éléments entiers sur A est un A-module fini (i.e : finiment engendré en tant que module).

Démonstration: Si B est une A-algèbre de type fini de la forme $A[x_1, \dots, x_n]$, où les x_i sont entiers sur A :

- Si $n = 1$: il existe un polynôme unitaire $P \overset{\text{déf}}{=} X^m + \sum_{i=0}^{m-1} p_i X^i \in A[X]$ de degré m tel que $P(x_1) = 0$. Donc $x_1^m = -\sum_{i=0}^{m-1} p_i x_1^i$, et B est finiment engendré par $\left(1, x_1, \dots, x_1^{m-1}\right)$ en tant que A-module.
- Si $n = 2$: il existe des polynômes unitaires $P_1, P_2 \in A[X]$ de degrés m_1, m_2 tels que :

$$P_1(x_1) = 0,\ P_2(x_2) = 0$$

  Montrons que B est finiment engendré, en tant que A-module, par $\left(x_1^i x_2^j\right)_{(i,j) \in [\![0,m_1-1]\!] \times [\![0,m_2-1]\!]}$. Pour tout $P \in B = A[x_1, x_2] = (A[x_1])[x_2]$, P appartient, de même, au $A[x_1]$-module engendré par $\left(1, x_2, \dots, x_2^{m_2-1}\right)$. Or, $A[x_1]$ est engendré, en tant que A-module, par $\left(1, x_1, \dots, x_1^{m_1-1}\right)$, donc le résultat s'ensuit.

On conclut par une récurrence immédiate sur $n \in \mathbb{N}^*$, en montrant que le A-module B est finiment engendré par $\left(x_1^{i_1} \cdots x_n^{i_n}\right)_{(i_1,\dots,i_n) \in [\![0,m_1-1]\!] \times \cdots \times [\![0,m_n-1]\!]}$ (avec des notations analogues).

□

Lemme 7 : Équivalence entre la donnée d'une structure de A[X]-module et la donnée d'un A-module muni d'un endomorphisme.

Tout A[X]-module peut-être associé de manière biunivoque à un couple formé d'un A-module et d'un endomorphisme de ce dernier.

Démonstration: Pour être plus explicite, on notera toute structure de A-module B : $\big(\mathrm{B}, \underbrace{\mathrm{A}}_{\text{anneau des sclaires}}\big)$.

a) On définit une application Φ de la manière suivante :
À tout couple $\big((\mathrm{B},\mathrm{A}),u\big)$, où B est un A-module et $u : \mathrm{B} \to \mathrm{B}$ un endomorphisme de B, on associe le A[X]-module $\Phi\Big(\big((\mathrm{B},\mathrm{A}),u\big)\Big) \overset{\text{déf}}{=} (\mathrm{B},\mathrm{A}[\mathrm{X}])$, où la multiplication externe est définie par :

$$\begin{cases} \mathrm{A}[\mathrm{X}] \times \mathrm{B} & \to & \mathrm{B} \\ (\mathrm{P}, b) & \mapsto & \mathrm{P}(u)(b) \end{cases}$$

(i.e : $\mathrm{P} \cdot b = \mathrm{P}(u)(b)$)
Comme A est un sous-anneau de A[X] et comme la restriction à $\mathrm{A} \times \mathrm{B}$ de la nouvelle multiplication externe coïncide avec l'ancienne multiplication externe, cette structure de A[X]-module prolonge celle de A-module.

b) On définit une application Ψ de la façon suivante :
À tout A[X]-module $(\mathrm{B},\mathrm{A}[\mathrm{X}])$, on associe le couple $\Psi\big((\mathrm{B},\mathrm{A}[\mathrm{X}])\big) \overset{\text{déf}}{=} \big((\mathrm{B},\mathrm{A}),u\big)$ (comme A est un sous-anneau de A[X], B est aussi un A-module), où $u : \mathrm{B} \to \mathrm{B}$ est un endomorphisme de (B,A) défini par :

$$u \overset{\text{déf}}{=} \begin{cases} \mathrm{B} & \to & \mathrm{B} \\ b & \mapsto & \mathrm{X} \cdot b \end{cases}$$

c) Vérifions que Φ et Ψ sont inverses l'une de l'autre :

- $\Psi \circ \Phi = \mathrm{id}$:
  Soit $\big((\mathrm{B},\mathrm{A}),u\big)$ un couple formé d'un A-module B et d'un endomorphisme $u : \mathrm{B} \to \mathrm{B}$ de B.
  On vérifie que :
  $$\Psi\Big(\Phi\big(\big((\mathrm{B},\mathrm{A}),u\big)\big)\Big) = \Psi\big((\mathrm{B},\mathrm{A}[\mathrm{X}])\big) = \big((\mathrm{B},\mathrm{A}),u\big)$$
  En effet, si on pose $\big((\mathrm{B},\mathrm{A}),v\big) \overset{\text{déf}}{=} \Psi\big((\mathrm{B},\mathrm{A}[\mathrm{X}])\big)$: pour tout $b \in \mathrm{B}$, $v(b) = \mathrm{X} \cdot b \overset{\text{a)}}{=} u(b)$, d'où $v = u$.

- $\Phi \circ \Psi = \mathrm{id}$:
  Soit $(\mathrm{B},\mathrm{A}[\mathrm{X}])$ un A[X]-module. On vérifie que :
  $$\Phi\Big(\Psi\big((\mathrm{B},\mathrm{A}[\mathrm{X}])\big)\Big) = \Phi\Big(\big((\mathrm{B},\mathrm{A}),u\big)\Big) = (\mathrm{B},\mathrm{A}[\mathrm{X}])$$
  En effet, avec $u \overset{\text{déf}}{=} \begin{cases} \mathrm{B} & \to & \mathrm{B} \\ b & \mapsto & \mathrm{X} \cdot b \end{cases}$: pour tous $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$, $b \in \mathrm{B}$,
  $$\underbrace{\mathrm{P} \cdot b}_{\text{nouvelle multiplication externe}} = \mathrm{P}(u)(b) = \underbrace{\mathrm{P}(\mathrm{X}) \cdot b}_{\text{ancienne multiplication externe}}$$

□

Lemme 8 : CAYLEY-HAMILTON dans les A-modules finis

Si B est un A-modules de type fini, $u : B \to B$ une application A-linéaire, alors u est annulée par un polynôme (unitaire) de A[X].

Démonstration: B est finiment engendré en tant que A-module, B est donc de la forme : $B = x_1 A + \ldots + x_n A$.

Pour tout $i \in [\![1, n]\!]$, il existe $(\lambda_{i,j})_{j\in[\![1,n]\!]} \overset{\text{déf}}{=} \Lambda_j \in A^n$ tel que :

$$u(x_i) = \sum_{j=1}^{n} \lambda_{i,j} x_j$$

On pose $\Lambda \overset{\text{déf}}{=} \left(\begin{array}{c} \Lambda_1 \\ \hline \vdots \\ \hline \Lambda_n \end{array}\right) \in \mathscr{M}_n(A)$

Dans le A-module $\mathscr{M}_{n,1}(A)$, muni de l'endomorphisme u :

$$\begin{pmatrix} u(x_1) \\ \vdots \\ u(x_n) \end{pmatrix} = \Lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Soit, dans le A[X]-module $\mathscr{M}_{n,1}(A)$ qui lui est biunivoquement associé par le lemme 7 :

$$X \cdot I_n \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} X \cdot x_1 \\ \vdots \\ X \cdot x_n \end{pmatrix} = \Lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

c'est-à-dire :

$$\left(XI_n - \Lambda\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \circledast$$

Soit, en multipliant $\circledast$ à gauche par la transposée de la comatrice de $XI_n - \Lambda$, et en notant P le polynôme $\det(XI_n - \Lambda) \in A[X]$:

$$\begin{aligned} \begin{pmatrix} P(u)(x_1) \\ \vdots \\ P(u)(x_n) \end{pmatrix} &= \det\left(XI_n - \Lambda\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \\ &= {}^t\widetilde{\left(XI_n - \Lambda\right)} \underbrace{\left(XI_n - \Lambda\right) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{=0} \\ &= 0 \end{aligned}$$

Donc $P(u)$ est l'endomorphisme nul (il est nul sur une famille génératrice de B), et $P \in A[X]$ annule u.

□

Lemme 9 : Toute A-algèbre de type fini engendrée par des éléments entiers sur A est entière sur A

Si B est une A-algèbre de la forme $A[x_1, \dots, x_n]$, où $x_1, \dots, x_n$ sont entiers sur A, alors B est entière sur A.

Démonstration: (a) B est un A-module fini, par le lemme 6.

(b) Soit $b \in B$. Montrons que b est entier sur A :
Comme B est un A-module fini, il en est de même du A-module $A[b] \subset B$. L'endomorphisme A-linéaire $u : A[b] \to A[b]$ défini par :

$$u \overset{\text{déf}}{=} \left\{ \begin{array}{ccc} A[b] & \to & A[b] \\ a & \mapsto & ab \end{array} \right.$$

est alors annulé, d'après CAYLEY-HAMILTON (lemme 8), par un polynôme $P \in A[X]$.
En évaluant $0 = P(u)$ en $a = 1_A$, il vient que b est entier sur A.

□

Lemme 10 : Corps entier sur un sous-anneau commutatif

Si B est un corps entier sur un anneau commutatif $A \subset B$, alors A est un corps.

Démonstration: Soit $a \in A \backslash \{0\}$. $a^{-1} \in B$, donc il existe $c_0, \dots, c_{n-1} \in A$ tels que $(a^{-1})^n + \sum_{i=0}^{n-1} c_i (a^{-1})^i = 0$, et $A \ni a^{-1} = -\sum_{i=0}^{n-1} c_i a^{n-i-1}$. □

LEMMES D'ALGÈBRE POUR DÉMONTRER AX VIA LA THÉORIE DES MODÈLES

Clôture algébrique : une clôture algébrique $\overline{\mathbb{K}}$ d'un corps $\mathbb{K}$ est une extension algébrique de $\mathbb{K}$ (i.e : tout élément de $\overline{\mathbb{K}}$ est racine d'un polynôme à coefficients dans $\mathbb{K}$), qui est algébriquement close (i.e : tout polynôme à coefficients dans $\overline{\mathbb{K}}$ a une racine dans $\overline{\mathbb{K}}$).

Corps localement fini : un corps dont tous les sous-corps finiment engendrés sont finis.

Existence et Unicité (à isomorphisme près) de "la" clôture algébrique

(A) Tout corps $\mathbb{K}$ possède une clôture algébrique (i.e une extension algébrique algébriquement close).

(B) Deux clôtures algébriques de $\mathbb{K}$ sont reliées par un isomorphisme fixant les éléments de $\mathbb{K}$.

Démonstration:

(A) **Existence d'une clôture algébrique :**
On note $U \subset \mathbb{K}[X]$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X]$. Pour chaque $P \in U$, on introduit de nouvelles variables $\omega_1^P, \dots, \omega_{\deg P}^P$.

On pose : $C \overset{\text{déf}}{=} \left\{\omega_i^P \mid i \in [\![1, \deg P]\!]\right\}_{P \in U}$, et $R \overset{\text{déf}}{=} \mathbb{K}[C]$.
Ainsi, pour tout $P \in U$,

$$P - \prod_{i=1}^{\deg P}(X - \omega_i^P) = \sum_{j=0}^{\deg P - 1} r_j^P \cdot X^j \in R[X] \quad \circledast$$

pour des coefficients $(r_j^P)_{0 \leqslant j < \deg P} \in R^{\deg P}$.

On note $I \subset R$ l'idéal engendré par $\left\{r_j^P \mid j \in [\![0, \deg P - 1]\!]\right\}_{P \in U}$: il est inclus dans un idéal maximal $M \subset R$ (par le lemme de Zorn).

Le corps R/M est alors une clôture algébrique de $\mathbb{K}$: en effet, il est algébrique sur $\mathbb{K}$ ($\overline{P(\omega_i^P)} = \overline{0}$, pour tous $P \in U, i \in [\![1, \deg P]\!]$), et pour tout $P \in U$, P est scindé, en considérant $\circledast$ modulo M.

(B) **Unicité, à $\mathbb{K}$-isomorphisme près** (isomorphisme de corps laissant invariant chaque élément de $\mathbb{K}$) :

Soient $\mathbb{L}_1, \mathbb{L}_2$ deux clôtures algébriques de $\mathbb{K}$.

L'ensemble des couples (K, f), où K est une extension de $\mathbb{K}$ sur laquelle $\mathbb{L}_1$ est algébrique et $f \in \mathbb{L}_2^K$ un $\mathbb{K}$-homomorphisme de corps, est non vide et inductif (partiellement ordonné et toute partie totalement ordonnée admet un majorant). Par le lemme de Zorn, il existe un élément maximal (K_{max}, f_{max}).

Montrons que $K_{max} = \mathbb{L}_1$: pour tout $x \in \mathbb{L}_1$, x admet un polynôme minimal ($K_{max}[X]$ est principal) $\mu_x(X) \in K_{max}[X]$ irréductible sur $\mathbb{L}_1$ (puisque $\mathbb{L}_1$ est intègre). Donc $K_{max}[x]$ est un corps (sur lequel $\mathbb{L}_1$ reste algébrique). De plus, comme le polynôme [4] $f_{max}(\mu_x)$ admet une racine $y \in \mathbb{L}_2$,

$$\Phi \overset{\text{déf}}{=} \begin{cases} K_{max}[x] & \to & \mathbb{L}_2 \\ P(x) & \mapsto & f_{max}(P)(y) \end{cases}$$

est un $\mathbb{K}$-homomorphisme de corps. Ainsi, par maximalité de (K_{max}, f_{max}), $K_{max}[x] = K_{max}$, et $x \in K_{max}$, d'où $K_{max} = \mathbb{L}_1$.

Comme $f_{max}(\mathbb{L}_1) \subset \mathbb{L}_2$ est algébriquement clos, et $\mathbb{L}_2$ en est une extension algébrique, il vient que $f_{max}(\mathbb{L}_1) = \mathbb{L}_2$: donc le morphisme surjectif $f_{max} : \mathbb{L}_1 \to \mathbb{L}_2$ est non identiquement nul, et, partant, injectif (son noyau est un idéal strict du corps $\mathbb{L}_1$: c'est $\{0\}$).

Ainsi, $f_{max} : \mathbb{L}_1 \to \mathbb{L}_2$ est un $\mathbb{K}$-isomorphisme de corps.

4. par abus de notation, on note encore f_{max} le morphisme qui à $P = \sum_{k=0}^{\deg P} p_k X^k$ associe $f_{max}(P) \overset{\text{déf}}{=} \sum_{k=0}^{\deg P} f_{max}(p_k) X^k$

Clôture algébrique : remarques qualitatives

— Parmi les **extensions de corps** $\mathbb{L} \supset \mathbb{K}$:
  — dans une **extension algébrique** : tous les éléments de $\mathbb{L}$ sont racines d'un polynôme à coefficients dans $\mathbb{K}$.
  — dans une **extension algébriquement close** : tous les polynômes à coefficients dans $\mathbb{L}$ ont une racine dans $\mathbb{L}$.

— "La" (à $\mathbb{K}$-isomorphisme près) **clôture algébrique** est :
  - une "extension algébrique" maximale.
  - une "extension algébriquement close" minimale.
  - une extension algébrique algébriquement close.

— **Intuitivement :** parmi les **extensions de corps**, les **extensions algébriques** sont des *petites* extensions, les **extensions algébriquement closes** des *grandes* extensions. La **clôture algébrique** est la plus grande de ces *petites* extensions, et la plus petite de ces *grandes* extensions.

— Les **extensions algébriquement closes n'ont pas d'extension algébrique propre** : en effet, si $\mathbb{K}$ algébriquement clos a pour extension algébrique $\mathbb{L}$: tout élément de $\mathbb{L}$ est élément de $\mathbb{K}$, car racine d'un polynôme à coefficients dans $\mathbb{K}$, lequel est scindé sur $\mathbb{K}$ ($\mathbb{K}$ AC).

□

— **Existence et unicité (à isomorphisme près) d'un corps fini à p^n éléments**

Soit $p \in \mathbb{P}, n \in \mathbb{N}^*$. Il existe un corps fini à p^n éléments, unique à isomorphisme près.

Démonstration:

(A) **Existence :** On considère le polynôme $P \overset{\text{déf}}{=} X^{p^n} - X \in \mathbb{F}_p[X]$. Il existe un sur-corps $\mathbb{L} \supset \mathbb{F}_p$ tel que P est scindé dans $\mathbb{L}$. De plus, il est à racines simples, puisque $P' = p^n X^{p^n-1} - 1 = -1$ n'a pas de racines.
On vérifie alors aisément que l'ensemble $R_n \subset \mathbb{F}_{p^n}$ des racines de P est un sous-corps de $\mathbb{L}$, car : $\forall x, y \in \mathbb{F}_{p^n}, (x+y)^{p^n} = x^{p^n} + y^{p^n}$ ($\mathbb{L}$ est de caractéristique p), et tout élément non nul $a \in R_n$ a pour inverse a^{p^n-2}. Donc R_n est un corps à p^n éléments.

(B) **Unicité à isomorphisme près :** Soient $\mathbb{K}$, $\mathbb{L}$ deux corps de cardinal p^n. Montrons que $\mathbb{K} \cong \mathbb{L}$.
Soit a un élément primitif (i.e un générateur du groupe cyclique $\mathbb{K}^*$), et $\mu_a(X) \in \mathbb{F}_p[X]$ son polynôme minimal (il existe car l'idéal des polynômes de $\mathbb{F}_p[X]$ annulateurs de a est non trivial (il contient $X^{p^n-1} - 1$) et principal).
Comme $a \in \mathbb{K}$, $X^{p^n} - X$ est un polynôme annulateur de a, et $\mu_a \mid X^{p^n} - X$. Or, $X^{p^n} - X = \prod_{b \in \mathbb{L}} (X - b) \in \mathbb{L}[X]$, donc[5] μ_a est scindé dans $\mathbb{L}$, et il existe $b \in \mathbb{L}$ qui est une racine de μ_a : son polynôme minimal $\mu_b \in \mathbb{F}_p[X]$ divise donc $\mu_a(X)$, et comme $\mu_a(X)$ est irréductible ($\mathbb{F}_p$ est intègre) et unitaire :

$$\mu_a = \mu_b$$

De plus :

$$\mathbb{K} \cong \mathbb{F}_p[X]/(\mu_a)$$

5. en identifiant, par abus de notation, $\mathbb{F}_p[X]$ au sous-corps premier de $\mathbb{L}$ (qui lui est isomorphe), et en exprimant le fait que $\mu_a \mid X^{p^n} - X$ dans $\mathbb{L}[X]$

— En effet : comme $\mu_a(X)$ est irréductible, $(\mu_a) \subset \mathbb{F}_p[X]$ est un idéal maximal de l'ensemble des idéaux principaux propres, i.e (puisque $\mathbb{F}_p[X]$ est principal) de l'ensemble des idéaux propres, et (μ_a) est maximal, d'où $\mathbb{F}_p[X]/(\mu_a)$ est un corps. Le morphisme d'anneaux

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathbb{F}_p[X] & \to & \mathbb{K} \\ P(X) & \mapsto & P(a) \end{cases}$$

se factorise en un morphisme de corps

$$\Phi \overset{\text{déf}}{=} \begin{cases} \mathbb{F}_p[X]/(\mu_a) & \to & \mathbb{K} \\ \overline{P(X)} & \mapsto & P(a) \end{cases}$$

injectif (en tant que morphisme de corps) et surjectif (car son image contient le groupe multiplicatif engendré par a, qui vaut $\mathbb{K}^*$ par hypothèse sur a).

On procède de même avec $\mathbb{L}$: l'homomorphisme de corps

$$\Psi \overset{\text{déf}}{=} \begin{cases} \mathbb{F}_p[X]/(\mu_b) & \to & \mathbb{L} \\ \overline{P(X)} & \mapsto & P(b) \end{cases}$$

injectif (en tant que morphisme de corps), et surjectif, car $|\mathbb{F}_p[X]/(\mu_b)| = |\mathbb{F}_p[X]/(\mu_a)| = |\mathbb{K}| = |\mathbb{L}|$.
Donc

$$\mathbb{K} \cong \mathbb{F}_p[X]/(\mu_a) = \mathbb{F}_p[X]/(\mu_b) \cong \mathbb{L}$$

□

Sous-corps d'un corps fini

Soit $p \in \mathbb{P}, n \in \mathbb{N}^*$.

(A) Tout sous-corps $\mathbb{K}$ de $\mathbb{F}_{p^n}$ est isomorphe à $\mathbb{F}_{p^d}$, pour un entier d divisant n.

(B) Pour tout diviseur d de n, il existe un unique sous-corps de $\mathbb{F}_{p^n}$ isomorphe à $\mathbb{F}_{p^d}$.

Démonstration:

(A) $\mathbb{F}_{p^n}$ est de caractéristique p (son sous-corps premier π est de cardinal p), donc $\mathbb{K}$ aussi, et en posant $d \overset{\text{déf}}{=} \dim_\pi \mathbb{K} : |\mathbb{K}| = p^d$, d'où $\mathbb{K} \cong \mathbb{F}_{p^d}$, par unicité (à isomorphisme près) des corps finis. Or, $\mathbb{F}_{p^n}$ est un $\mathbb{K}$-espace vectoriel, d'où :

$$p^n = |\mathbb{F}_{p^n}| = |\mathbb{K}|^{\dim_{\mathbb{K}} \mathbb{F}_{p^n}} = p^{d \cdot \dim_{\mathbb{K}} \mathbb{F}_{p^n}}$$

et donc $d|n$.

(B) On vérifie aisément que l'ensemble $R_d \subset \mathbb{F}_{p^n}$ des racines de $X^{p^d} - X$ est un sous-corps de $\mathbb{F}_{p^n}$, car : $\forall x, y \in \mathbb{F}_{p^n}, (x+y)^{p^d} = x^{p^d} + y^{p^d}$ ($\mathbb{F}_{p^n}$ est de caractéristique p). De plus, $|R_d| \leqslant p^d$.
En outre, comme $d|n$, $p^d - 1 | p^n - 1$, et $X^{p^d} - X = X(X^{p^d-1} - 1) \,|\, X(X^{p^n-1} - 1) = X^{p^n} - X$

— En effet, en posant $a \overset{\text{déf}}{=} p^d - 1$ et $b \overset{\text{déf}}{=} p^n - 1 = ac$ (où c est entier) : $a|b = ac \implies X^a - 1 \,|\, X^b - 1$:

$$\begin{aligned} X^b - 1 &= (X^a - 1)\frac{X^b - X^{b-ac}}{X^a - 1} \\ &= (X^a - 1)X^{b-a}\frac{X^a - X^{a-ac}}{X^a - 1} \\ &= (X^a - 1)X^{b-a}\frac{1 - (X^{-a})^c}{1 - X^{-a}} \\ &= (X^a - 1)X^{b-a}\sum_{k=0}^{c-1} X^{-ak} \\ &= (X^a - 1)\sum_{k=1}^{c} X^{b-ak} \end{aligned}$$

Par suite, comme $X^{p^n} - X$ est scindé à racines simples dans $\mathbb{F}_{p^n}$, R_d a exactement p^d éléments, et par unicité des corps finis : $R_d \cong \mathbb{F}_{p^d}$.

□

Schéma de Vérité de Tarski

Tout commence avec le constat, faussement trivial :

"Il neige" est vrai si, et seulement si il neige.

À l'aube de la création de la "théorie des modèles" : le problème, millénaire, de la notion de vérité d'un énoncé se pose. Tarski donne un critère caractérisant tout "prédicat de vérité" :

Pour $i \in \mathbb{N}$, on se donne des "ensembles de symboles" (dit langages) $\mathscr{L}_i$ et $\mathscr{L}_{i+1} \supsetneq \mathscr{L}_i$. On se place sur un $\mathscr{L}_i$-système formel (ex : logique du premier ordre) :

— $\mathscr{L}_i$ est appelé Langage-Objet

— $\mathscr{L}_i$ contient (éventuellement) un prédicat de vérité "vrai$_i$"

On se donne un :

— $\mathscr{L}_{i+1}$-système formel, où : $\mathscr{L}_{i+1}$ contient $\mathscr{L}_i$ et est appelé métalangage pour le langage-objet $\mathscr{L}_i$

— $\mathscr{L}_{i+1}$ contient un prédicat de vérité "vrai$_{i+1}$" (n'appartenant pas à $\mathscr{L}_i$)

Propriété - Schéma (V_i)

Pour tout $\mathscr{L}_i$-énoncé p : p est vrai$_{i+1}$ ssi $I_{i+1}(p)$ où : $I_{i+1}(p)$ est l'interprétation de p dans le $\mathscr{L}_{i+1}$-système formel

(V_i) caractérise les "prédicats de vérité", pour tout prédicat appartenant à $\mathscr{L}_{i+1} \setminus \mathscr{L}_i$

De quoi rend compte ce schéma de vérité

— Le schéma (V_i) rend compte, selon Tarski, de notre intuition la plus élémentaire de la notion de vérité : quelle que soit sa position philosophique, personne ne nie l'équivalence du fait que 'Socrate est homme' est vrai, et du fait que Socrate soit un homme.

— Tarski plonge $\mathscr{L}_i$ dans un métalangage $\mathscr{L}_{i+1}$ contenant vrai$_{i+1}$ pour éviter le paradoxe du menteur (dû à l'autoréférence) (ex : l'adjectif "hétérologique" est-il hétérologique ou autologique ? / "Cette phrase est fausse." : faux ou vrai ?)