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-Grothendieck, ce qui nous donnera l'occasion d'esquisser une comparaison (sommaire) avec d'autres approches aboutissant à la démonstration dudit théorème.*

I Prélude et Motivations

II Ax-Grothendieck : 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 $x_1, \ldots, x_n \notin \mathbb{K}$ et $A \overset{\text{déf}}{=} \mathbb{K}[x_1, \ldots, x_n]$ 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 $\mathbb{K}$.

Solution. Supposons que $A = \mathbb{K}[x_1, \ldots, x_n]$ 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 a_1 est transcendant sur $\mathbb{K}$ (sinon, c'est trivial). Comme A est un corps,

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

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 P.

Donc $(Q(x_1))^{-1} \in A = k[x_2, \ldots, x_n]$ (c'est un corps), et $D(x_1)^r (Q(x_1))^{-1} \in k[D(x_1)x_2, \ldots, D(x_1)x_n]$ pour un entier r assez grand, d'où $D(x_1)^r (Q(x_1))^{-1}$ est entier sur $\mathbb{K}[x_1]$.

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.

$\square$

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

Solution. La fonction

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

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

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

  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 appartient à J)

Solution. 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

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

  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 Ax - Grothendieck

Théorème - Ax - Grothendieck

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

Solution. —

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.

Solution. 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 ($i \in [\![1, n]\!]$) :

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

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

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

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

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

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 $\mathrm{P}, \mathrm{Q}, \mathrm{R}$: 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 $\mathrm{P} = (\mathrm{P}_1, \ldots, \mathrm{P}_n) : \mathbb{C}^n \to \mathbb{C}^n$ 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 :

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

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

- Montrons que le corps $\mathrm{A}/\mathrm{I} = \mathbb{Z}[\mathscr{E}]/\mathrm{I}$ 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 $\mathbb{Z} \cong \phi(\mathbb{Z}) \subset \mathrm{A}/\mathrm{I}$. 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 $\mathrm{A}/\mathrm{I} = \phi(\mathbb{Z})[\alpha_1, \ldots, \alpha_m]$, 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 7), 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 $\operatorname{Ker}\phi$ est un idéal non trivial de $\mathbb{Z}$, et $\operatorname{Ker}\phi = p\mathbb{Z}$, 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 ⊛ sont encore vraies dans une clôture algébrique de A/I : c'est impossible, car le théorème d'AX-GROTHENDIECK est vérifié dans les clôtures algébriques des corps finis, par le lemme introductif.

□

III AX-GROTHENDIECK 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 ($\rightarrow, \leftrightarrow, \neg, \wedge, \vee$) / 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 :

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

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

$$\begin{array}{lll}
\mathtt{CAC}_p = & \mathcal{T}_{\textit{corps}} & \\
\bigcup_{n\in\mathbb{N}^*} & \{\ \forall x_1,\ldots,\forall x_n, \exists x_0, & x_0^n + x_n x_0^{n-1} + \ldots + x_2 x_0 + x_1 = 0\ \} \\
\cup & \{\ p = 0\ \} &
\end{array}$$

$$\begin{array}{lll}
\mathtt{CAC}_0 = & \mathcal{T}_{\textit{corps}} & \\
\bigcup_{n\in\mathbb{N}^*} & \{\ \forall x_1,\ldots,\forall x_n, \exists x_0, & x_0^n + x_n x_0^{n-1} + \ldots + x_2 x_0 + x_1 = 0\ \} \\
\bigcup_{q\in\mathbb{P}} & \{\ \neg(q = 0)\ \} &
\end{array}$$

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 $\mathcal{T}_{\textit{anneaux comm}}$ 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 $\mathscr{P}(\mathrm{I})$ vérifiant :

— $\emptyset \notin \mathscr{F}$

— $\forall \mathrm{X} \in \mathscr{F}, \forall \mathrm{Y} \in \mathscr{P}(\mathrm{I}),\ \mathrm{Y} \supset \mathrm{X} \Longrightarrow \mathrm{Y} \in \mathscr{F}$

— $\forall \mathrm{X}, \mathrm{Y} \in \mathscr{F},\ \mathrm{X} \cap \mathrm{Y} \in \mathscr{F}$

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

Ultrafiltre principal/trivial : un ultrafiltre de la forme $\mathscr{U}_{\mathrm{X}_0} \overset{\text{déf}}{=} \{\mathrm{Y} \in \mathscr{P}(\mathrm{I}) \mid \mathrm{Y} \supset \mathrm{X}_0\}$, pour une partie $\mathrm{X}_0 \subset \mathrm{I}$.

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

Propriété de l'intersection finie : Une famille $\mathscr{X}$ de parties de I a la "propriété de l'intersection finie" si : $\forall \mathrm{X}_1, \ldots, \mathrm{X}_n \in \mathscr{X},\ \bigcap_{i=1}^{n} \mathrm{X}_i \neq \emptyset$. 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 : $\forall \mathrm{X} \in \mathscr{P}(\mathrm{I}),\ \mathrm{X} \notin \mathscr{F} \Longrightarrow \mathrm{I}\backslash\mathrm{X} \in \mathscr{F}$.

(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.

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

— En effet : $\Longleftarrow$: Si $\mathrm{I}\backslash\mathrm{X} \in \mathscr{F}$, $(\mathrm{I}\backslash\mathrm{X}) \cap \mathrm{X} = \emptyset$
$\Longrightarrow$: Si $\mathscr{F} \cup \{\mathrm{X}\}$ n'a pas cette propriété, il existe $\mathrm{X}_1, \ldots, \mathrm{X}_n \in \mathscr{F}$ tels que $\mathrm{X}_1 \cap \cdots \cap \mathrm{X}_n \cap \mathrm{X} = \emptyset$, d'où $(\mathrm{I}\backslash\mathrm{X}) \supset \mathrm{X}_1 \cap \cdots \cap \mathrm{X}_n$, et $\mathrm{I}\backslash\mathrm{X} \in \mathscr{F}$

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

(B) L'ensemble $\mathrm{E}_{\mathscr{F}}$ des filtres sur I contenant $\mathscr{F}$ est tel que tout sous-ensemble E' de $\mathrm{E}_{\mathscr{F}}$ 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, $\mathrm{E}_{\mathscr{F}}$ a un élément maximal (un ultrafiltre).

(C) $\mathscr{X}$ est incluse dans le filtre $\mathscr{F}_{\mathscr{X}} \overset{\text{déf}}{=} \{\mathrm{Y} \in \mathscr{P}(\mathrm{I}) \mid \exists \mathrm{X}_1, \ldots, \mathrm{X}_n \in \mathscr{X} ; \mathrm{Y} \supset \mathrm{X}_1 \cap \cdots \cap \mathrm{X}_n\}$, lui-même inclus dans un ultrafiltre.

(D) Si $\mathscr{U}$ contenait une partie finie X_0, il serait le filtre principal $\mathscr{F}_{\mathrm{X}_0}$ qu'elle engendre (il le contiendrait trivialement, et ne pourrait contenir de partie $\mathrm{Y} \not\supset \mathrm{X}_0$, car $\mathscr{U} \ni (\mathrm{I}\backslash\mathrm{Y}) \supset \mathrm{X}_0$).
Donc, par (A), $\mathscr{U}$ contient toutes les parties cofinies.

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

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

Réciproquement : si $\mu : \mathscr{P}(\mathrm{I}) \to \{0, 1\}$ 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 :

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

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 $c \in \mathscr{L}$

— $f^{\mathscr{M}^*} : (\mathscr{M}^*)^{n_f} \to \mathscr{M}^*, \left(\overline{M^{(1)}}, \ldots, \overline{M^{(n_f)}} \right) \mapsto \overline{\left(f^{\mathscr{M}_i}\left(M_i^{(1)}, \ldots, M_i^{(n_f)}\right) \right)_{i \in I}}$ 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 :

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

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 ($i \in I$) satisfasse une formule ϕ n'implique pas qu'il en est de même pour l'ultraproduit.
Par (contre-)exemple, la disjonction "$\vee$" de l'énoncé "$\forall x_1, \underbrace{(x_1 = 0)}_{\text{noté } A(x_1)} \vee \underbrace{(\exists x_2, x_1 \times x_2 = 1)}_{\text{noté } B(x_1)}$" 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 $A\big((0,1)\big)$ ET $B\big((0,1)\big)$ 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 $\mathscr{M}_i$ ($i \in I$) 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 :

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

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

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

Solution. Pour toute $\mathscr{L}$-formule ψ, on note $I(\psi)$ l'ensemble $\left\{ i \in I \mid \mathscr{M}_i \vDash \psi\left(M_i^{(1)}, \ldots, M_i^{(n)}\right) \right\}$.
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 $\phi = \neg\psi$,

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

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 $\phi(x_1, \ldots, x_n) = \exists x_0, \psi(x_0, x_1, \ldots, x_n)$:

— $\Longrightarrow$: 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 :

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

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 $\mathscr{M}_i \vDash \psi\left(\mathrm{M}_i^{(0)}, \mathrm{M}_i^{(1)}, \ldots, \mathrm{M}_i^{(n)}\right)$. 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.

Solution. 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 $(\forall \theta_1, \ldots, \theta_n \in \mathscr{T}, \emptyset \neq \bigcap_{k=1}^n \mathrm{I}(\theta_k) \ni \{\theta_1, \ldots, \theta_n\})$.

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 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 $F \vDash \theta$

Solution. 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 "$\mathscr{T} \vDash \theta$". □

III.3 Löwenheim-Skolem

III.3.1 Löwenheim-Skolem descendant

III.3.2 Löwenheim-Skolem montant

III.4 Ax-Grothendieck

III.4.1 Catégoricité et Complétude

III.4.2 Théorème de transfert

III.4.3 Ax-Grothendieck

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 principal si, et seulement si, A/I est un corps.

Solution. $\Longrightarrow$: 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.

Solution. 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 $\langle p\rangle \subset \langle a\rangle \subset \mathrm{A}$, alors $p = ab$ pour un $b \in \mathrm{A}$, et a est une unité - d'où $\langle a\rangle = \mathrm{A}$ - ou b est une unité - d'où $\langle a\rangle = \langle p\rangle$. Donc par le lemme 1, $\mathrm{A}/\langle p\rangle$ 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 $\mathrm{A}/\langle p\rangle$, 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.

Solution. Soit A un anneau factoriel, dont on note K le corps des fractions. Soit $u \overset{\text{déf}}{=} a/b \in \mathrm{K}$ (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 $u \in \mathrm{A}$. □

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

Solution. Si a est un élément d'une extension de corps de $\mathbb{K}$ algébrique sur $\mathbb{K}$: $\mathrm{P}(a) = 0$, 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 $\left\langle \mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n \right\rangle$

Pour tous $a_1, \ldots, a_n \in \mathbb{K}$, $\left\langle \mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n \right\rangle$ est un idéal maximal de $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$

Solution. Le noyau du morphisme d'anneaux surjectif

$$\phi \overset{\text{déf}}{=} \begin{cases} \mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n] & \to & \mathbb{K} \\ \mathrm{P}(\mathrm{X}_1, \ldots, \mathrm{X}_n) & \mapsto & \mathrm{P}(a_1, \ldots, a_n) \end{cases}$$

est l'idéal $\left\langle \mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n \right\rangle$:

- **En effet :** il le contient évidemment, et si $\mathrm{P} \in \mathbb{K}[\mathrm{X}_1, \mathrm{X}_2]$ a pour racine (a_1, a_2) :

$$\mathrm{P} = \underbrace{\mathrm{P}(\mathrm{X}_1, \mathrm{X}_2) - \mathrm{P}(\mathrm{X}_1, a_2)}_{=(\mathrm{X}_2 - a_2)\mathrm{Q}(\mathrm{X}_1, \mathrm{X}_2)\text{ , où } \mathrm{Q}\in\mathbb{K}[\mathrm{X}_1,\mathrm{X}_2]} + \underbrace{\mathrm{P}(\mathrm{X}_1, a_2) - \mathrm{P}(a_1, a_2)}_{=(\mathrm{X}_1 - a_1)\mathrm{R}(\mathrm{X}_1)\text{ , où } \mathrm{R}\in\mathbb{K}[\mathrm{X}_1,\mathrm{X}_2]} \in \left\langle \mathrm{X}_1 - a_1, \mathrm{X}_2 - a_2 \right\rangle$$

  On conclut par une récurrence immédiate sur $k \in \mathbb{N}^*$, pour $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_k]$

En factorisant ϕ, il vient que $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\langle \mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n\rangle \cong \mathbb{K}$, d'où $\left\langle \mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n \right\rangle$ est maximal.

□

Lemmes pour Ax-Grothendieck

— **Lemme 6 : Une A-algèbre B de type fini et entière 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) et entière sur A est un A-module fini (i.e : finiment engendré en tant que module)

Solution. Toute A-algèbre B de type fini est de la forme $A[x_1, \ldots, x_n]$:

— 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 $\left(1, x_1, \ldots, x_1^{m-1}\right)$ 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 $\left(1, x_2, \ldots, x_2^{m_2-1}\right)$. Or, $A[x_1]$ est engendré, en tant que A-module, par $\left(1, x_1, \ldots, x_1^{m_1-1}\right)$, 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 $\left(x_1^{i_1} \cdots x_n^{i_n}\right)_{(i_1,\ldots,i_n)\in[\![0,m_1-1]\!]\times\cdots\times[\![0,m_n-1]\!]}$ (avec des notations analogues).

□

— **Lemme 7 : 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.

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

□

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 $\mathscr{L}_{i+1} \backslash \mathscr{L}_i$

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 ?)