Une preuve modèle-théorique du théorème d'Ax-Grothendieck

Cédric Rivière

Département de Mathématique
Université de Mons

September 4, 2018

Le théorème d'Ax-Grothendieck

Théorème (Ax (68), Grothendieck (66))

Soit $f : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale. Si f est injective alors f est surjective.

- *The elementary theory of finite fields*, **J. Ax**, Annals of Mathematics, Second Series, 88 (2) (1968).
- *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III.*, **A. Grothendieck**, Inst. Hautes Études Sci. Publ. Math. 28 (1966).
- *Injective morphisms of real algebraic varieties*, **A. Biallyncki-Barula** and **M. Rosenlicht**, Proc. Amer. Math. Soc. 13 (1962).

Théorème (Ax-Grothendieck (66, 68))

Soit $f : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale. Si f est injective alors f est surjective.

Définition

$f : \mathbb{C}^n \to \mathbb{C}^n$ est **polynomiale** *si*
$f(x_1, \ldots, x_n) = (P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$ avec
$P_1, \ldots, P_n \in \mathbb{C}[x_1, \ldots, x_n]$.

Définition

$f : \mathbb{C}^n \to \mathbb{C}^n$ *est* **polynomiale** *si*
$f(x_1, \ldots, x_n) = (P_1(x_1, \ldots, x_n), \ldots, P_n(x_1, \ldots, x_n))$ *avec*
$P_1, \ldots, P_n \in \mathbb{C}[x_1, \ldots, x_n]$.

Exemples/Remarques:

- $f : \mathbb{C} \to \mathbb{C} : x \mapsto x^2$ pas injective, mais surjective.
- Les seules applications polynomiales bijectives de $\mathbb{C}$ dans $\mathbb{C}$ sont celles de degré 1:
  - $f : \mathbb{C} \to \mathbb{C}$ polynomiale non constante est toujours surjective.
  - $f : \mathbb{C} \to \mathbb{C}$ polynomiale injective ssi $deg(f) = 1$.
- $f : \mathbb{C}^2 \to \mathbb{C}^2 : (x_1, x_2) \mapsto (x_1^2 x_2^5, 3x_2^3 - 2x_1^4 x_2)$.

Corps algébriquement clos

- Un corps (comm.) K est **algébriquement clos** si tout polynôme non constant de $K[x]$ admet une racine dans K (ex: $\mathbb{C}$).

- Tout corps algébriquement clos *de caractéristique zéro* et de cardinalité $2^{\aleph_0}$ est isomorphe à $\mathbb{C}$ (Steinitz).

- Soit K un corps (comm.), il existe une extension *algébrique* $\overline{K}$ de K qui est algébriquement close (Zorn, ax. choix, ...).
  Elle est unique (à K-isomorphisme près) et est appelée **la clôture algébrique** de K (e.g. $\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}_p}$).

Corps finis $\mathbb{F}_p$

- Corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \simeq \{0, 1, \ldots, p-1\}$ (p premier).
- $\mathbb{F}_p$ est de **caractéristique p**: $\underbrace{1 + 1 + \cdots + 1}_{p \text{ fois}} = 0$.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^n$ injective $\iff$ f surjective $\iff$ f bijective.

Clôture algébrique des $\mathbb{F}_p$

- $\overline{\mathbb{F}_p}$ est dénombrable (infini) et *localement fini* (i.e. tout sous-corps finiment engendré de $\overline{\mathbb{F}_p}$ est fini).
  - Soit K un corps fini, alors le cardinal de K est de la forme p^n où p est un nombre premier (la caractéristique de K) et $n \in \mathbb{N}_0$.
  - A isomorphisme près, il n'existe qu'un seul corps de cardinal p^n, noté $\mathbb{F}_{p^n}$.
  - Soient $m, n \in \mathbb{N}_0$, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m|n$.
  - $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}_0} \mathbb{F}_{p^{n!}}$.

Principe de transfert et preuve du théorème

Théorème (Lefschetz principle)

Si le théorème d'Ax-Grothendieck est vrai dans $\overline{\mathbb{F}_p}$ pour tout p premier, alors il est vrai dans $\mathbb{C}$.

Il suffit donc montrer que le théorème est vrai dans tout corps localement fini.

Langage et structures

Définition

Un **langage** L *consiste en la donnée:*

- *pour chaque* $n \in \mathbb{N}$*, d'une famille de* **symboles de fonctions** n*-aires* $f(x_1, \ldots, x_n)$*;*
- *pour chaque* $m \in \mathbb{N}$*, d'une famille de* **symboles de relations** m*-aires* $R(x_1, \ldots, x_m)$*;*
- *d'une famille de* **symboles de constantes** c*.*

Langage et structures

Définition

Un **langage** L *consiste en la donnée:*

- *pour chaque* $n \in \mathbb{N}$*, d'une famille de* **symboles de fonctions** n*-aires* $f(x_1, \ldots, x_n)$*;*
- *pour chaque* $m \in \mathbb{N}$*, d'une famille de* **symboles de relations** m*-aires* $R(x_1, \ldots, x_m)$*;*
- *d'une famille de* **symboles de constantes** c*.*

Exemples:

- Langage des anneaux $\boxed{L_A = \{+, -, \cdot, 0, 1\}}$;

Langage et structures

Définition

Un **langage** L *consiste en la donnée:*

- *pour chaque* $n \in \mathbb{N}$*, d'une famille de* **symboles de fonctions** n*-aires* $f(x_1, \dots, x_n)$*;*
- *pour chaque* $m \in \mathbb{N}$*, d'une famille de* **symboles de relations** m*-aires* $R(x_1, \dots, x_m)$*;*
- *d'une famille de* **symboles de constantes** c*.*

Exemples:

- Langage des anneaux $\boxed{L_A = \{+, -, \cdot, 0, 1\}}$;
- Langage des anneaux ordonnés $\boxed{L_R = \{+, -, \cdot, <, 0, 1\}}$.

Langage et structures

Définition

Une L-**structure** $\mathcal{S}$ *consiste en*

- *un ensemble non vide* S *(domaine);*
- *pour chaque symbole de fonction n-aire, une fonction* $f_S : S^n \to S$*;*
- *pour chaque symbole de relation n-aire, une relation* $R_S : S^n \to \{\top, \perp\}$*;*
- *pour chaque symbole de constante, un élément* $c_S \in S$*.*

Les fonctions, relations et constantes dans S sont appelées les **interprétations** des symboles de L dans $\mathcal{S}$.

Langage et structures

Définition

*Une L-**structure** $\mathcal{S}$ consiste en*

- *un ensemble non vide S (domaine);*
- *pour chaque symbole de fonction n-aire, une fonction $f_S : S^n \to S$;*
- *pour chaque symbole de relation n-aire, une relation $R_S : S^n \to \{\top, \bot\}$;*
- *pour chaque symbole de constante, un élément $c_S \in S$.*

Exemples:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{M}_N(K)$ munis de leurs lois usuelles sont des L_A-structures;
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ muni, de plus, de leur ordre usuel sont des L_R-structures.

Termes et Formules atomiques

Soit L un langage.

Définition

*L'ensemble des L-**termes** se définit comme suit:*

- *tout symbole de constante c ou de variable x est un terme;*
- *si f est un symbole de fonction n-aire et $t_1, \ldots, t_n$ sont des termes alors $f(t_1, \ldots, t_n)$ est un terme.*

Définition

*L'ensemble des L-**formules atomiques** se définit comme suit:*

- *si t_1 et t_2 sont des termes alors $t_1 = t_2$ est une formule atomique;*
- *si R est un symbole de relation m-aire et $t_1, \ldots, t_m$ sont des termes alors $R(t_1, \ldots, t_m)$ est une formule atomique.*

Formules atomiques dans L_A

Nous considérons maintenant la classe des anneaux (unitaires) commutatifs, considérés comme L_A structures.

Définition

- *Les* **termes du langage** *sont de la forme*

$$\boxed{P(x_1,\ldots,x_n) \text{ où } P \in \mathbb{Z}[x_1,\ldots,x_n] \text{ et } n \in \mathbb{N}}$$

- L_A-**formules atomiques** $\phi(x_1,\ldots,x_n)$*: équations polynomiales*

$$\boxed{P(x_1,\ldots,x_n) = Q(x_1,\ldots,x_n) \text{ où } P \in \mathbb{Z}[x_1,\ldots,x_n] \text{ et } n \in \mathbb{N}}$$

Exemples:

- $3x^4 - 2x^3 - x + 4 = 0$;
- $x_1^2 x_3 + x_2 = x_4$;
- $1 + 1 \cdots + 1 = 0$.

Formules atomiques dans L_A - Sémantique

Définition

Soient A un anneau et $a_1, \ldots, a_n \in A$, on dit que $a_1, \ldots, a_n$ **satisfont** *la formule atomique $\phi(x_1, \ldots, x_n)$ ci-dessus si $P(a_1, \ldots, a_n) = Q(a_1, \ldots, a_n)$. On note alors* $\boxed{A \models \phi(a_1, \ldots, a_n)}$

Exemples:

- si $\phi(x)$ est la formule $2x = 1$ alors $\mathbb{Q}, \mathbb{R} \models \phi(\frac{1}{2})$ et $\mathbb{F}_3 \models \phi(2)$ mais, pour tout $a \in \mathbb{Z}$, $\mathbb{Z} \not\models \phi(a)$.
- si $\phi(x)$ est la formule $x^2 + 1 = 0$, $\mathbb{C} \models \phi(i)$ mais, pour tout $a \in \mathbb{R}$, $\mathbb{R} \not\models \phi(a)$.

Formules du premier ordre - Syntaxe

- Soit $\mathcal{F}_0$ l'ensemble des formules atomiques.
- $\mathcal{F}$ l'ensemble des formules du premier ordre est la clôture de $\mathcal{F}_0$ sous l'action des connecteurs et quantificateurs: $\vee$, $\neg$, $\exists$ ($\wedge$, $\forall$).

  Soient $\phi_1(x_1, \ldots, x_n), \phi_2(x_1, \ldots, x_m) \in \mathcal{F}$.

  - $\mathcal{F}_0 \subseteq \mathcal{F}$;
  - $\phi_1(x_1, \ldots, x_n) \vee \phi_2(x_1, \ldots, x_m) \in \mathcal{F}$;
  - $\neg\phi_1(x_1, \ldots, x_n) \in \mathcal{F}$;
  - $\exists x_1 \phi_1(x_1, \ldots, x_n) \in \mathcal{F}$.
- On utilisera également les symboles $\implies$ et $\neq$ de façon classique.

Formules du premier ordre - Syntaxe

- $\mathcal{F}$ l'ensemble des formules du premier ordre est la clôture de $\mathcal{F}_0$ pour l'action des connecteurs et quantificateurs: $\vee$, $\neg$, , $\exists$ ($\wedge$, $\forall$).

- Une variable apparaissant dans une formule est dite **libre** si aucun quantificateur n'agit sur elle.

  Exemples:

  - $\exists x \left((xz^2 = y) \wedge (x^3 - z = y^5)\right)$ (y, z libres);
  - $\forall y \exists x \left((xz^2 = y) \wedge (x^3 - z = y^5)\right)$ (z libre);
  - $\forall x \; \exists y \; ((x = 0) \vee (xy = 1))$ (pas de variables libres).

Formules du premier ordre - Syntaxe

- $\mathcal{F}$ l'ensemble des formules du premier ordre est la clôture de $\mathcal{F}_0$ pour l'action des connecteurs et quantificateurs: $\vee$, $\neg$, , $\exists$ ($\wedge$, $\forall$).
- Une variable apparaissant dans une formule est dite **libre** si aucun quantificateur n'agit sur elle.
- Lorsque l'on écrit $\phi(x_1, \dots, x_n)$, on sous-entend que chacune des variables $x_1, \dots, x_n$ est libre.
- Une formule sans variable libre est appelée un **énoncé**.

Formules du premier ordre - Sémantique

Soient $\phi_1(x_1, \dots, x_n), \phi_2(x_1, \dots, x_m)$ des formules ($m \leq n$), A un anneau et $a_1, \dots, a_n \in A$.

- $A \models \phi_1(a_1, \dots, a_n) \vee \phi_2(a_1, \dots, a_m)$ ssi $A \models \phi_1(a_1, \dots, a_n)$ ou $A \models \phi_2(a_1, \dots, a_m)$;
- $A \models \phi_1(a_1, \dots, a_n) \wedge \phi_2(a_1, \dots, a_m)$ ssi $A \models \phi_1(a_1, \dots, a_n)$ et $A \models \phi_2(a_1, \dots, a_m)$;
- $A \models \neg\phi_1(a_1, \dots, a_n)$ ssi $A \not\models \phi_1(a_1, \dots, a_n)$;
- $A \models \exists x_1 \ \phi_1(x_1, a_2, \dots, a_n)$ ssi il existe $b \in A$ tel que $A \models \phi_1(b, a_2, \dots, a_n)$;
- $A \models \forall x_1 \ \phi_1(x_1, a_2, \dots, a_n)$ ssi pour tout $b \in A$ on a que $A \models \phi_1(b, a_2, \dots, a_n)$.

Ensembles définissables

Définition

Soit M une L-structure, un **ensemble L-définissable** *est de la forme*

$$\boxed{\{(a_1, \dots a_n) \in M^n \mid M \models \phi(a_1, \dots, a_n)\}}$$

où $\phi(x_1, \dots, x_n)$ est une L-formule.

Exemples:

- Dans $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$: ensembles constructibles;
- Dans $\langle \mathbb{R}, +, -, \cdot, >, 0, 1 \rangle$: ensembles semi-algébriques.

Théories et modèles

Définition

- *Soit Σ un ensemble (éventuellement infini) d'énoncés, on dit que $A \models \Sigma$ (A est un* **modèle** *de Σ) si $A \models \sigma$ pour tout $\sigma \in \Sigma$. Dans ce cas, Σ est appelé une* **théorie**.

Théories et modèles

Définition

- *Soit Σ un ensemble (éventuellement infini) d'énoncés, on dit que $A \models \Sigma$ (A est un* **modèle** *de Σ) si $A \models \sigma$ pour tout $\sigma \in \Sigma$. Dans ce cas, Σ est appelé une* **théorie**.

- Une théorie ne contient jamais σ et $\neg\sigma$.
- Théorie des corps commutatifs:
  $TF := \left\{ \text{axiomes des anneaux com.} \right\} \cup \left\{ \forall x \ \Big((x = 0) \vee (\exists y \ xy = 1) \Big) \right\}$

Théories et modèles

Définition

- *Soit Σ un ensemble (éventuellement infini) d'énoncés, on dit que $A \models \Sigma$ (A est un* **modèle** *de Σ) si $A \models \sigma$ pour tout $\sigma \in \Sigma$. Dans ce cas, Σ est appelé une* **theorie**.

- Si p premier, $A \models TF_p := TF \cup \{\sigma_p := \underbrace{1 + 1 + \cdots + 1}_{p \text{ fois}} = 0\}$ ssi A est un corps de caractéristique p.

- $A \models TF_0 := TF \cup \{\neg\sigma_2, \neg\sigma_3, \neg\sigma_5, \ldots\}$ ssi A est un corps de caractéristique zéro.

Théories et modèles

Définition

- *Soit Σ un ensemble (éventuellement infini) d'énoncés, on dit que $A \models \Sigma$ (A est un* **modèle** *de Σ) si $A \models \sigma$ pour tout $\sigma \in \Sigma$. Dans ce cas, Σ est appelé une* **theorie**.

- **Théorie des corps algébriquement clos de caractéristique** p (p premier ou nul) $\mathbf{ACF_p} = TF_p \cup \{\theta_n \mid n \in \mathbb{N}_0\}$ où:

$$\boxed{\theta_n := \forall y_0 \ldots \forall y_{n-1} \; \exists x \; \left(x^n + y_{n-1}x^{n-1} + \cdots + y_1 x + y_0 = 0\right)}$$

La théorie ACF_p ($p = 0$ ou p premier)

- La théorie ACF **élimine les quantificateurs** dans le langage L_A.
  - La projection d'un ensemble constructible est constructible (Chevalley, Tarski).
  - Résultats de type "Nullstellensatz".
  - Tout sous-ensemble définissable de $K \models ACF$ est soit fini soit cofini (minimalité).
- La théorie ACF_p est **complète** et ω-**stable**.
  - Un L_A-énoncé est vrai dans un modèle de ACF_p ssi il est vrai dans chacun des modèles de ACF_p.
  - Notion de dimension (rang de Morley) sur les ensembles définissables (dimension algébrique).

"But" : prouver le Principe de transfert

- On voudrait identifier $\mathbb{C}$ à $\prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$.
- Mais $\prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$ est un anneau qui n'est pas même intègre.

"But" : prouver le Principe de transfert

- On voudrait pouvoir "identifier" $\mathbb{C}$ à $\prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$.

- Mais $\prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$ est un anneau qui n'est même pas intègre.

$\longrightarrow$ on va identifier les éléments égaux *"presque partout"* dans $\prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$.

Filtres et ultrafiltres sur I:

Définition

Soit I un ensemble infini (ex: $I = \mathbb{N}$, $I = \mathbb{P}$, $\dots$),un **filtre** *sur I est un sous-ensemble $\mathcal{V}$ de $\mathcal{P}(I)$ tel que*

- $I \in \mathcal{V}$, $\emptyset \notin \mathcal{V}$;
- *si* $A, B \in \mathcal{V}$, $A \cap B \in \mathcal{V}$;
- *si* $A \in \mathcal{V}$ *et* $A \subseteq B$ *alors* $B \in \mathcal{V}$.

Exemples:

- Soit $A \subseteq I$ non vide, $\mathcal{V}_A := \{B \subseteq I \mid A \subseteq B\}$ est un filtre sur I.
- $\mathcal{F}_r := \{A \subseteq I \mid A^c \text{ est fini}\}$ est appelé le **filtre de Fréchet** sur I.
- $I = \mathbb{R}$ et $\mathcal{V} := \{\text{voisinages de } 0\}$.

Filtres et ultrafiltres sur I:

Définition

Soit I un ensemble infini (ex: $I = \mathbb{N}$, $I = \mathbb{P}$, ...),un **filtre** *sur I est un sous-ensemble $\mathcal{V}$ de $\mathcal{P}(I)$ tel que*

- $I \in \mathcal{V}$, $\emptyset \notin \mathcal{V}$;
- *si* $A, B \in \mathcal{V}$, $A \cap B \in \mathcal{V}$;
- *si* $A \in \mathcal{V}$ *et* $A \subseteq B$ *alors* $B \in \mathcal{V}$.

Définition

Un **ultrafiltre** $\mathcal{U}$ *sur I est un filtre sur I tel que pour tout $A \subseteq \mathcal{P}(I)$, soit $A \in \mathcal{U}$, soit $A \notin \mathcal{U}$ (il s'agit d'un filtre maximal pour l'inclusion).*

Filtres et ultrafiltres sur I:

Définition

Un **ultrafiltre** $\mathcal{U}$ *sur* I *est un filtre sur* I *tel que pour tout* $A \subseteq \mathcal{P}(I)$, *soit* $A \in \mathcal{U}$, *soit* $A \notin \mathcal{U}$ *(il s'agit d'un filtre maximal pour l'inclusion).*

Propriété: Tout filtre s'étend en un ultrafiltre (Zorn).

Définition

Un ultrafiltre qui contient le filtre de Fréchet est dit **non principal**.

Ultraproduit des $\overline{\mathbb{F}_p}$

Définition

Soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{P}$. Pour $a, b \in \prod_{p \in \mathbb{P}} \overline{\mathbb{F}_p}$, on définit:

$$\boxed{a \equiv_{\mathcal{U}} b \text{ ssi } \{p \in \mathbb{P} \mid a(p) = b(p)\} \in \mathcal{U}}$$

Ultraproduit des $\overline{\mathbb{F}_p}$

Définition

Soit $\mathcal{U}$ un ultrafiltre non principal sur $\mathbb{P}$. Pour $a, b \in \prod_{p\in\mathbb{P}} \overline{\mathbb{F}_p}$, on définit:

$$\boxed{a \equiv_{\mathcal{U}} b \text{ ssi } \{p \in \mathbb{P} \mid a(p) = b(p)\} \in \mathcal{U}}$$

- $\equiv_{\mathcal{U}}$ est une relation d'équivalence sur $\prod_{p\in\mathbb{P}} \overline{\mathbb{F}_p}$. On note $[a]$ la classe d'équivalence de $a \in \prod_{p\in\mathbb{P}} \overline{\mathbb{F}_p}$.
- $\boxed{\prod_{\mathcal{U}} \overline{\mathbb{F}_\mathbf{p}} := \left(\prod_{p\in\mathbb{P}} \overline{\mathbb{F}_p}\right)/\mathcal{U}}$ est appelé **l'ultraproduit** des $\overline{\mathbb{F}_p}$ (par $\mathcal{U}$).
- On définit: $[a] \pm [b] = [a \pm b]$ et $[a] \cdot [b] = [a \cdot b]$.

Théorème de Łoś (50's)

Théorème

Soient $\phi(x_1, \ldots, x_n)$ *une* L_A*-formule et* $[a_1], \ldots, [a_n] \in \prod_{\mathcal{U}} \overline{\mathbb{F}_p}$ *alors*

$$\boxed{\prod_{\mathcal{U}} \overline{\mathbb{F}_p} \models \phi([a_1], \ldots [a_n]) \iff \{p \in \mathbb{P} \mid \overline{\mathbb{F}_p} \models \phi(a_1(p), \ldots, a_n(p))\} \in \mathcal{U}}$$

Théorème de Łoś (50's)

Théorème

Soient $\phi(x_1, \dots, x_n)$ *une* L_A*-formule et* $[a_1], \dots, [a_n] \in \prod_{\mathcal{U}} \overline{\mathbb{F}_p}$ *alors*

$$\boxed{\prod_{\mathcal{U}} \overline{\mathbb{F}_p} \models \phi([a_1], \dots [a_n]) \iff \{p \in \mathbb{P} \mid \overline{\mathbb{F}_p} \models \phi(a_1(p), \dots, a_n(p))\} \in \mathcal{U}}$$

Cas particuliers:

- Si $\overline{\mathbb{F}_p}$ satisfait un énoncé σ quel que soit $p \in \mathbb{P}$, alors $\prod_{\mathcal{U}} \overline{\mathbb{F}_p} \models \sigma$.
- Si $\overline{\mathbb{F}_p}$ satisfait un énoncé σ pour presque tout $p \in \mathbb{P}$, alors $\prod_{\mathcal{U}} \overline{\mathbb{F}_p} \models \sigma$.

Théorème de Łoś (50's)

Théorème

Soient $\phi(x_1, \ldots, x_n)$ *une* L_A*-formule et* $[a_1], \ldots, [a_n] \in \prod_{\mathcal{U}} \overline{\mathbb{F}_p}$ *alors*

$$\boxed{\prod_{\mathcal{U}} \overline{\mathbb{F}_p} \models \phi([a_1], \ldots [a_n]) \iff \{p \in \mathbb{P} \mid \overline{\mathbb{F}_p} \models \phi(a_1(p), \ldots, a_n(p))\} \in \mathcal{U}}$$

<u>Preuve:</u>

- Par induction sur la complexité des formules.
- La maximalité de $\mathcal{U}$ n'intervient que pour l'étape de la négation.

Retour sur le principe de transfert

Remarque: $\prod_{\mathcal{U}} \overline{\mathbb{F}_p}$ est

- un corps algébriquement clos;
- de caractéristique zéro;
- de cardinalité $2^{\aleph_0}$.

Théorème

$\prod_{\mathcal{U}} \overline{\mathbb{F}_p}$ est isomorphe à $\mathbb{C}$.
En particulier, si un énoncé est vrai dans $\overline{\mathbb{F}_p}$ pour tout p premier, alors il est vrai dans $\mathbb{C}$.

Pour conclure la preuve du Théorème d'Ax-Grothendieck

Théorème (Ax-Grothendieck)

Soit $f : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale. Si f est injective alors f est surjective.

Théorème

Si un énoncé est vrai dans $\overline{\mathbb{F}_p}$ pour tout p premier, alors il est vrai dans $\mathbb{C}$.

Il suffit donc de remarquer que:

- f est injective ssi $\sigma_1 : \ \forall x_1, \dots, x_n \ \ \forall y_1, \dots, y_n$ $\Big(f(x_1, \dots, x_n) = f(y_1, \dots, y_n) \Rightarrow (x_1, \dots, x_n) = (y_1, \dots, y_n)\Big)$;
- f est surjective ssi $\sigma_2 : \ \forall x_1, \dots, x_n \ \ \exists y_1, \dots, y_n \ \ \Big(f(y_1, \dots, y_n) = (x_1, \dots, x_n)\Big)$.

Autre constructions "classiques" :

Soient I un ensemble et $\mathcal{U}$ un ultrafiltre non principal sur I

- Soit $I = \mathbb{N}$, $\prod_{\mathcal{U}} \mathbb{R} := \mathbb{R}^*$ corps des réels non standards.

  $\longrightarrow$ Corps réel clos non archimédien, analyse non standard.

- Soit $I = \mathbb{P}$, $\prod_{\mathcal{U}} (\mathbb{Z}/p\mathbb{Z}, +, 0) \simeq (\mathbb{R}, +, 0)$.

  $\longrightarrow$ "sans torsion" ne s'exprime pas par un énoncé du premier ordre dans le langage des groupes.

- (Ax-Kochen 65) Soit $I = \mathbb{P}$, $\prod_{\mathcal{U}} \mathbb{F}_p((t)) \simeq \prod_{\mathcal{U}} \mathbb{Q}_p$.

  $\longrightarrow$ Pour tout $n \in \mathbb{N}_0$ et tout premier p suffisamment grand, tout polynôme homogène à coefficients dans $\mathbb{Q}_p$ et en au moins $n^2 + 1$ variables admet un zéro non trivial dans $\mathbb{Q}_p$.

Bibliographie:

- *Model Theory, an introduction*, David Marker, Graduate texts in mathematics 217, Springer 2002.
- *Model Theory* ,C.C. Chang and H.J. Keisler, Studies in Logic and the Foundations of Mathematics, 73. North-Holland Publishing Co., Amsterdam, 1990.
- *2010 Summer School in Model Theory*, Peter L. Clark, University of Georgia, notes.
- *Introduction à la théorie des modèles*, Elisabeth Bouscaren, Université Paris-Sud (Orsay), notes 2005.