Modèles de la théorie des corps

Théories consistantes

Soit $\mathbf{T}$ une $\mathcal{L}$-théorie.

- Une *preuve* de $\mathbf{T}$ est une suite finie de $\mathcal{L}$-formules $\phi_1, \ldots, \phi_n$ telle que soit $\phi_i \in \mathbf{T}$, soit ϕ_i est un axiome logique, soit ϕ_i est une conséquence de $\phi_1, \ldots, \phi_{i-1}$ en appliquant les règles d'inférence.
- Un *théorème* de $\mathbf{T}$ est une $\mathcal{L}$-formule ϕ telle qu'il existe une preuve $\phi_1, \ldots, \phi_n$ de $\mathbf{T}$ où $\phi_n = \phi$.

La théorie $\mathbf{T}$ est qualifiée d'*inconsistante* s'il existe une $\mathcal{L}$-formule ϕ telle que ϕ et $\neg\phi$ soient deux théorèmes de $\mathbf{T}$. Dans le cas contraire $\mathbf{T}$ est dite *consistante*.

Théories consistantes

Lemme

Dans une théorie inconsistante, toute formule est un théorème.

En effet, quelles que soient les formules ϕ et ψ, la formule $\phi \to (\neg\phi \to \psi)$ est une tautologie. Appelant ϕ une formule d'une théorie inconsistante $\mathbf{T}$ telle que $\mathbf{T} \vdash \phi$ et $\mathbf{T} \vdash \neg\phi$, il suffit d'appliquer deux fois de suite le modus ponens à l'axiome précédent.

Théories consistantes

Proposition

Toute théorie ayant un modèle est consistante.

D'après le lemme une théorie inconsistante prouverait en particulier l'énoncé $\exists x,\ x \neq x$ qui est faux dans toutes les structures.

Théorie des corps algébriquement clos

Un corps k est *algébriquement clos* dès que tout polynôme à coefficients dans k possède une racine dans k.

Définition

CAC est l'ensemble des $\mathcal{L}_{an}$[1]-énoncés suivant,

- Les axiomes de corps commutatifs,
- Pour tout entier naturel n,

$$\forall a_1,\, \forall a_2,\, \ldots,\, \forall a_n,\, \exists x,\, \sum_{i=0}^{n} a_i x^i + x^{n+1} = 0.$$

$$\mathbf{CAC}_0 := \mathbf{CAC} \cup \{\underbrace{1 + \ldots + 1}_{p \text{ termes}} \neq 0,\ p \in \mathcal{P}\}$$

$$\mathbf{CAC}_p := \mathbf{CAC} \cup \{\underbrace{1 + \ldots + 1}_{p \text{ termes}} = 0,\ p \in \mathcal{P}\},\ p \in \mathcal{P}.$$

1. $\mathcal{L}_{an} := \{+,\ -,\ .,\ 0,\ 1\}$.

Théorie des corps algébriquement clos

Soit L/k une extension de corps.

- Un élément a de L est *algébrique sur k* lorsqu'il existe un polynôme non nul à coefficients dans k dont a est une racine.
- L'extension L est dite *algébrique sur k* si c'est le cas pour tous ses éléments.
- On appelle L une *clôture algébrique de k* si elle est algébrique sur k et algébriquement close.

Théorie des corps algébriquement clos

Théorème (Steinitz)

Tout corps commutatif admet une (« unique ») clôture algébrique.

Soit k un corps commutatif. Le lemme de Zorn fournit une extension algébrique maximale de k que l'on note $\overline{k}$, reste à montrer que celle-ci est algébriquement close.

Théorie des corps algébriquement clos

Soit $P \in \overline{k}[X]$ que l'on peut supposer irréductible dans $\overline{k}$. Soit $A := {}^{\overline{k}[X]}\!\big/_{(P)}$: c'est un corps. Ceci découle du théorème de Bachet-Bézout et de la principalité de $\overline{k}[X]$. On obtient

$$\overline{k} \hookrightarrow A$$

et comme A est une extension algébrique finie de $\overline{k}$ par transitivité algébrique A est une extension algébrique de k donc $A = \overline{k}$. Or P possède une racine dans A.

Théorie des corps algébriquement clos

Corollaire

Les théories $\mathbf{CAC}_0$ et $\mathbf{CAC}_p$ sont consistantes.

Théorème d'Ax-Grothendieck

Soit k un corps de caractéristique $p > 0$. *L'endomorphisme de Frobenius* est l'application

$$F : \begin{array}{ccc} k & \longrightarrow & k \\ x & \longmapsto & x^p \end{array} .$$

Lemme

La clôture algébrique de $\mathbf{F}_p$ est une union de corps finis, laissés invariants par le Frobenius.

On a

$$\overline{\mathbf{F}_p} = \bigcup_{n \in \mathbf{N}} \mathrm{Fix}_{\overline{\mathbf{F}_p}}(F^n)$$

et les $\mathrm{Fix}_{\overline{\mathbf{F}_p}}(F^n)$ sont bien des corps finis car composés des éléments x de $\overline{\mathbf{F}_p}$ qui vérifient $x^{p^n} - x = 0$.

Théorème d'Ax-Grothendieck

Théorème (Łoś)

Soient $\mathcal{U}$ un ultrafiltre non principal sur I, $\mathcal{A}_i$ des $\mathcal{L}$-structures, $[a_{1i}],\ \ldots,\ [a_{ni}]$ n éléments de $\prod_{i\in I} \mathcal{A}_i/\mathcal{U}$ et $\phi(x_1,\ \ldots,\ x_n)$ une $\mathcal{L}$-formule. Alors $\prod_{i\in I} \mathcal{A}_i/\mathcal{U} \models \phi([a_{1i}]_{\mathcal{U}},\ \ldots,\ [a_{ni}]_{\mathcal{U}})$ si et seulement si $\{i \in I,\ \mathcal{A}_i \models \phi(a_{1i},\ \ldots,\ a_{ni})\} \in \mathcal{U}$.

En particulier, pour tout ultrafiltre $\mathcal{U}$ non principal sur $\mathcal{P}$, $\prod_{p\in\mathcal{P}} \overline{\mathbf{F}_p}/\mathcal{U}$ est un modèle de la théorie $\mathbf{CAC}_0$.

Théorème d'Ax-Grothendieck

Définition

Une application

$$f : \begin{array}{ll} \mathbb{C}^n & \longrightarrow \mathbb{C}^n \\ (x_1, \ldots, x_n) & \longmapsto (f_1(\overline{x}), \ldots, f_n(\overline{x})) \end{array}$$

où les f_i sont des éléments de $\mathbb{C}[X_1, \ldots, X_n]$ est appelée *polynomiale*.

Théorème d'Ax-Grothendieck

Théorème (Ax, Grothendieck)

Toute application polynomiale injective est surjective.

L'énoncé ϕ du théorème pour les applications polynomiales de degré borné s'exprime dans $\mathcal{L}_{an}$ avec les quantificateurs $\forall\exists$.

Toute application injective d'un ensemble fini dans lui-même est surjective.

Dans chacun des $\mathrm{Fix}_{\overline{\mathbf{F}_p}}(F^n)$, ϕ est vrai. On en déduit qu'il est aussi vrai dans $\overline{\mathbf{F}_p}$.

D'après le théorème de Łoś, ϕ est vrai dans $\prod_{p\in\mathcal{P}} \overline{\mathbf{F}_p} / \mathcal{U}$.

Théorème d'Ax-Grothendieck

Théorème (Ax, Grothendieck)

Toute application polynomiale injective est surjective.

D'après ce que l'on a vu plus haut, $\prod_{p \in \mathcal{P}} \overline{\mathbf{F}_p} \big/ \mathcal{U}$ est un corps algébriquement clos de caractéristique nulle et de cardinalité $2^{\aleph_0}$. Or, d'après Steinitz, il y a unicité d'un tel corps : ϕ est donc vrai dans $\mathbb{C}$.