Le théorème de compacité et son application à l'existence d'une clôture algébrique

Seconde journée 4A – ENS Rennes

Téofil Adamski

vendredi 12 mai 2023

Introduction

La *théorie des modèles* étudie

- les formules logiques d'un langage donné : c'est l'aspect syntaxique ;
- et leurs interprétations dans certaines structures mathématiques sur ce langage : c'est l'aspect sémantique.

Bien que logicienne par nature, cette théorie a de nombreuses applications en algèbre. Nous allons voir comment montrer l'existence d'une clôture algébrique avec des arguments logiques.

Plan

La notion de langage

Définition. —

Un *langage* est la donnée

- de symboles c_h, appelés les *constantes* ;
- de symboles f_i munis d'entiers $n_i \geqslant 1$, appelés les *opérations d'arité* n_i ;
- de symboles R_j munis d'entiers $m_j \geqslant 1$, appelés les *relations d'arité* m_j.

Ce langage sera noté $\mathscr{L} = \{c_h\}_h \cup \{f_i\}_i \cup \{R_j\}_j$, les arités seront implicites.

Définition. —

Un *langage* est la donnée

- de symboles c_h, appelés les *constantes* ;
- de symboles f_i munis d'entiers $n_i \geqslant 1$, appelés les *opérations d'arité* n_i ;
- de symboles R_j munis d'entiers $m_j \geqslant 1$, appelés les *relations d'arité* m_j.

Ce langage sera noté $\mathscr{L} = \{c_h\}_h \cup \{f_i\}_i \cup \{R_j\}_j$, les arités seront implicites.

Exemples. Les langages

$$\mathscr{L}_{\text{anneaux}} := \{0, 1, +, -, \times\} \qquad \text{et} \qquad \mathscr{L}_{k\text{-ev}} := \{0, +\} \cup \{\overline{\lambda}\}_{\lambda \in k}$$

sont respectivement les langages des anneaux et des k-espaces vectoriels.

Formules et phrases sur un langage

Définition. —

Étant donné un langage $\mathscr{L}$, une *formule du premier ordre* sur ce langage est une formule logique faisait intervenir les symboles du langage $\mathscr{L}$ ainsi que les symboles logiques usuels $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, etc. Lorsque dans une formule, toutes les variables apparaissant sont quantifiées, on dit que la formule est une *phrase*.

Formules et phrases sur un langage

Définition. —

Étant donné un langage $\mathscr{L}$, une *formule du premier ordre* sur ce langage est une formule logique faisait intervenir les symboles du langage $\mathscr{L}$ ainsi que les symboles logiques usuels $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, etc. Lorsque dans une formule, toutes les variables apparaissant sont quantifiées, on dit que la formule est une *phrase*.

Exemples. Sur le langage des groupes $\mathscr{L}_{\text{groupes}} := \{e, \cdot, ^{-1}\}$, les deux expressions

$$\forall x \ \exists y \ x \cdot y = e \qquad \text{et} \qquad x \cdot x^{-1} = e$$

sont des formules dont seule la première est une phrase.

Formules et phrases sur un langage

Définition. —

Étant donné un langage $\mathscr{L}$, une *formule du premier ordre* sur ce langage est une formule logique faisait intervenir les symboles du langage $\mathscr{L}$ ainsi que les symboles logiques usuels $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$, etc. Lorsque dans une formule, toutes les variables apparaissant sont quantifiées, on dit que la formule est une *phrase*.

Exemples. Sur le langage des groupes $\mathscr{L}_{\text{groupes}} \coloneqq \{e, \cdot, ^{-1}\}$, les deux expressions

$$\forall x \; \exists y \; x \cdot y = e \qquad \text{et} \qquad x \cdot x^{-1} = e$$

sont des formules dont seule la première est une phrase.

Définition. —

Une *théorie* sur un langage est un ensemble (fini ou non) de phrases sur ce langage.

Définition. —

Une *structure* sur un langage $\mathscr{L}$ est un ensemble A où l'on interprète les constantes (respectivement les opérations et les relations) du langage $\mathscr{L}$ comme des éléments de A (respectivement des opérations et des relations sur A).

Structures

Définition. —

Une *structure* sur un langage $\mathscr{L}$ est un ensemble A où l'on interprète les constantes (respectivement les opérations et les relations) du langage $\mathscr{L}$ comme des éléments de A (respectivement des opérations et des relations sur A).

Exemples.

- Le quadruplet $(\mathbf{Z}, 0, +, -)$ est une structure sur le langage des groupes.
- La suite $(k^n, 0) \cup (x \longmapsto \lambda x)_{\lambda \in k}$ est une structure sur le langage des k-espaces vectoriels. Les symboles d'opérations $\overline{\lambda}$ avec $\lambda \in k$ sont interprétés ici par les multiplications scalaires $x \longmapsto \lambda x$.

Modèles d'une théorie

Définition. —

Soit T une théorie sur un langage $\mathscr{L}$. Un *modèle* de la théorie T est une structure A sur le langage $\mathscr{L}$ dans laquelle toutes les phrases de la théorie T sont vérifiées.

Définition. —

Soit T une théorie sur un langage $\mathscr{L}$. Un *modèle* de la théorie T est une structure A sur le langage $\mathscr{L}$ dans laquelle toutes les phrases de la théorie T sont vérifiées.

Exemples. On considère l'ensemble T_{groupes} des axiomes de la théorie des groupes, c'est-à-dire la théorie formée par les trois phrases

$$\forall x\ \forall y\ \forall z \quad (x \cdot y) \cdot z = x \cdot (y \cdot z), \tag{1}$$

$$\forall x \quad x \cdot e = e \cdot x = x, \tag{2}$$

$$\forall x\ \exists y \quad x \cdot y = e. \tag{3}$$

Alors la structure $(\mathbf{Z}, 0, +, -)$ ou $(\mathfrak{S}_n, \mathrm{id}, \circ, ^{-1})$ en est un modèle mais pas la structure $(\mathbf{N}, 1, +, -)$.

Le théorème de compacité

Théorème de compacité (Gödel, 1930 ; Maltsev, 1936). —

Soit T une théorie sur un langage $\mathscr{L}$. Alors les points suivants sont équivalents :

- le théorie T admet un modèle ;
- pour tout sous-ensemble fini $T' \subset T$, la théorie T' admet un modèle.

Le théorème

Théorème (Steinitz, 1910). —

Soit K un corps. Alors il admet une (unique) clôture algébrique $\overline{\mathrm{K}}$ à isomorphisme près, c'est-à-dire une extension de corps $\overline{\mathrm{K}}/\mathrm{K}$ qui soit algébrique et telle que le corps $\overline{\mathrm{K}}$ soit algébriquement clos.

Le théorème

Théorème (Steinitz, 1910). —

Soit $\mathbf{K}$ un corps. Alors il admet une (unique) clôture algébrique $\overline{\mathbf{K}}$ à isomorphisme près, c'est-à-dire une extension de corps $\overline{\mathbf{K}}/\mathbf{K}$ qui soit algébrique et telle que le corps $\overline{\mathbf{K}}$ soit algébriquement clos.

On va seulement montrer qu'il existe une extension algébriquement close $\mathbf{L}/\mathbf{K}$. Il suffit alors de choisir le corps $\overline{\mathbf{K}}$ des éléments de $\mathbf{L}$ qui sont algébriques sur $\mathbf{K}$.

Le théorème

Théorème (Steinitz, 1910). —

Soit $\mathbf{K}$ un corps. Alors il admet une (unique) clôture algébrique $\overline{\mathbf{K}}$ à isomorphisme près, c'est-à-dire une extension de corps $\overline{\mathbf{K}}/\mathbf{K}$ qui soit algébrique et telle que le corps $\overline{\mathbf{K}}$ soit algébriquement clos.

On va seulement montrer qu'il existe une extension algébriquement close $\mathbf{L}/\mathbf{K}$. Il suffit alors de choisir le corps $\overline{\mathbf{K}}$ des éléments de $\mathbf{L}$ qui sont algébriques sur $\mathbf{K}$.

Dans un premier temps, on veut trouver une extension $\mathbf{L}_0/\mathbf{K}$ telle que tout polynôme de $\mathbf{K}[t]$ admette une racine dans $\mathbf{L}_0$.

Mise en place

Soit $\mathbf{K}$ un corps. On va considérer le langage des anneaux $\mathscr{L}_{\text{anneaux}}$ auquel on rajoute des symboles $\overline{x}$ pour tout élément $x \in \mathbf{K}$. Notons $\mathscr{L}_{\mathbf{K}}$ ce nouveau langage.

Mise en place

Soit $\mathbf{K}$ un corps. On va considérer le langage des anneaux $\mathscr{L}_{\text{anneaux}}$ auquel on rajoute des symboles $\overline{x}$ pour tout élément $x \in \mathbf{K}$. Notons $\mathscr{L}_{\mathbf{K}}$ ce nouveau langage.

On définit la théorie T sur ce langage $\mathscr{L}_{\mathbf{K}}$ dont on veut trouver un modèle, c'est-à-dire la théorie constituée des phrases suivantes :

- les axiomes de la théorie des corps ;
- les tables d'addition et de multiplication de $\mathbf{K}$, c'est-à-dire les phrases
$$\overline{x} + \overline{y} = \overline{z} \qquad \text{et} \qquad \overline{x} \times \overline{y} = \overline{z}$$
lorsque $x + y = z$ et $xy = z$ pour chaque élément $x, y, z \in \mathbf{K}$;
- toute polynôme non constant de $\mathbf{K}[t]$ admet une racine, c'est-à-dire les phrases
$$\exists y \ \overline{a_n} \times y^n + \cdots + \overline{a_0} = 0$$
pour chaque entier $n \geqslant 1$ et élément $a_0, \ldots, a_n \in \mathbf{K}$ avec $a_n \neq 0$.

Qu'est-ce qu'un modèle de la théorie T ?

Un modèle de la théorie T est donc un ensemble $\mathbf{L}$ vérifiant ces phrases où les constantes $\overline{x}$ sont interprétées comme des éléments $x_{\mathbf{L}_0} \in \mathbf{L}_0$. En particulier,

- il s'agit d'un corps ;

Qu'est-ce qu'un modèle de la théorie T ?

Un modèle de la théorie T est donc un ensemble $\mathbf{L}$ vérifiant ces phrases où les constantes $\overline{x}$ sont interprétées comme des éléments $x_{\mathbf{L_0}} \in \mathbf{L_0}$. En particulier,

- il s'agit d'un corps ;
- de plus, comme on a encodé les tables d'additions et de multiplications de $\mathbf{K}$ dans le théorie T, l'application

$$\left| \begin{array}{l} \mathbf{K} \longrightarrow \mathbf{L}_0, \\ x \longmapsto x_{\mathbf{L_0}} \end{array} \right.$$

  est un morphisme de corps puisque, comme le phrase $\overline{x} + \overline{y} = \overline{x+y}$ appartient à la théorie T, on trouve $x_{\mathbf{L_0}} + y_{\mathbf{L_0}} = (x+y)_{\mathbf{L_0}}$ et de même pour la multiplicativité ; on obtient alors une extension $\mathbf{L}_0/\mathbf{K}$;

Qu'est-ce qu'un modèle de la théorie T ?

Un modèle de la théorie T est donc un ensemble $\mathbf{L}$ vérifiant ces phrases où les constantes $\overline{x}$ sont interprétées comme des éléments $x_{\mathbf{L}_0} \in \mathbf{L}_0$. En particulier,

- il s'agit d'un corps ;
- de plus, comme on a encodé les tables d'additions et de multiplications de $\mathbf{K}$ dans le théorie T, l'application

$$\left| \begin{array}{l} \mathbf{K} \longrightarrow \mathbf{L}_0, \\ x \longmapsto x_{\mathbf{L}_0} \end{array} \right.$$

  est un morphisme de corps puisque, comme le phrase $\overline{x} + \overline{y} = \overline{x + y}$ appartient à la théorie T, on trouve $x_{\mathbf{L}_0} + y_{\mathbf{L}_0} = (x + y)_{\mathbf{L}_0}$ et de même pour la multiplicativité ; on obtient alors une extension $\mathbf{L}_0/\mathbf{K}$;
- enfin, tout polynôme non constant de $\mathbf{K}[t]$ admet une racine dans $\mathbf{L}_0$.

Utilisation du théorème de compacité

Trouvons un modèle de la théorie T. Grâce au théorème de compacité, il suffit de trouver un modèle à toute partie finie de cette théorie. Soit $T' \subset T$ une partie finie.

Utilisation du théorème de compacité

Trouvons un modèle de la théorie T. Grâce au théorème de compacité, il suffit de trouver un modèle à toute partie finie de cette théorie. Soit $T' \subset T$ une partie finie.

Dans cette théorie finie T', il n'y a qu'un nombre fini de phrases de la forme

$$\exists y \; \overline{a_{j,n_j}} \times y^{n_j} + \cdots + \overline{a_{j,0}} = 0$$

avec $a_{j,i} \in \mathbf{K}$ et $a_{j,n_j} \neq 0$. Mais avec les corps de décomposition, on peut trouver une extension $\mathbf{L}'$ du corps $\mathbf{K}$ dans lequel les polynômes $a_{j,n_j} t^{n_j} + \cdots + a_{j,0} \in \mathbf{K}[t]$ admettent au moins une racine. Ainsi on trouve

$$\mathbf{L}' \vDash T'.$$

Utilisation du théorème de compacité

Trouvons un modèle de la théorie T. Grâce au théorème de compacité, il suffit de trouver un modèle à toute partie finie de cette théorie. Soit $T' \subset T$ une partie finie.

Dans cette théorie finie T', il n'y a qu'un nombre fini de phrases de la forme

$$\exists y \ \overline{a_{j,n_j}} \times y^{n_j} + \cdots + \overline{a_{j,0}} = 0$$

avec $a_{j,i} \in \mathbf{K}$ et $a_{j,n_j} \neq 0$. Mais avec les corps de décomposition, on peut trouver une extension $\mathbf{L}'$ du corps $\mathbf{K}$ dans lequel les polynômes $a_{j,n_j} t^{n_j} + \cdots + a_{j,0} \in \mathbf{K}[t]$ admettent au moins une racine. Ainsi on trouve

$$\mathbf{L}' \vDash T'.$$

Bilan. Il existe une extension $\mathbf{L}_0/\mathbf{K}$ telle que tout polynôme de $\mathbf{K}[t]$ admette une racine dans $\mathbf{L}_0$.

Fin de la démonstration

En effectuant une récurrence, on trouve une tour d'extensions

$$\cdots/\mathbf{L}_{i+1}/\mathbf{L}_i/\cdots/\mathbf{L}_1/\mathbf{L}_0/\mathbf{K}.$$

telles que tout polynôme de $\mathbf{L}_i[t]$ admette une racine dans $\mathbf{L}_{i+1}$.

Fin de la démonstration

En effectuant une récurrence, on trouve une tour d'extensions

$$\cdots/\mathbf{L}_{i+1}/\mathbf{L}_i/\cdots/\mathbf{L}_1/\mathbf{L}_0/\mathbf{K}.$$

telles que tout polynôme de $\mathbf{L}_i[t]$ admette une racine dans $\mathbf{L}_{i+1}$.

L'union disjointe

$$\mathbf{L} := \bigsqcup_{i\geqslant 0} \mathbf{L}_i$$

est naturellement munie d'une structure de corps et il s'agit d'une extension algébriquement close du corps $\mathbf{K}$.

Perspectives et conclusion

Le théorème de compacité se révèle d'une efficacité redoutable dans cette situation. Avec des arguments similaires, on peut montrer le résultat suivant.

Théorème (finitude uniforme). —

Soit A une structure sur un langage $\mathscr{L}$. Soit $X \subset A^{m+1}$ un ensemble définissable, c'est-à-dire qu'il existe une formule $\phi(x_1, \ldots, x_{m+1})$ sur la langage $\mathscr{L}$ telle que

$$X = \{(x_1, \ldots, x_{m+1}) \in A^{m+1} \mid A \vDash \phi(x_1, \ldots, x_{m+1})\}.$$

On suppose que, pour tout $s \in A^m$, l'ensemble

$$X_s := \{a \in A \mid (s, a) \in X\}$$

est fini. Alors il existe un entier $n \in \mathbf{N}$ tel que

$$\forall s \in A^m, \quad \sharp X_s \leqslant n.$$