Une introduction à la théorie des modèles

à travers quelques exemples d'applications

Journée Mathématicienne
Orsay, 26 Septembre 2019

Elisabeth Bouscaren

CNRS - LMO Équipe Arithmétique et Géométrie Algébrique

Introduction

Objectifs:
Utiliser quelques exemples classiques d'applications à l'algèbre (pas forcément très récentes) comme motivation, pour introduire très informellement les outils et concepts de base de la théorie des modèles: structure au sens de la théorie des modèles du premier ordre, ensemble définissables, limites de structures, théorèmes de transfert, théorème de compacité.
Esayer de mettre en lumière ce qui me semble typique de la théorie des modèles et qui fait sa force et son intérêt.

Introduction

Ensuite évoquer des outils et idées plus modernes et quelques uns de leurs domaines d'application plus récents, parmi :

- stabilité, théorie des modèles géométrique et ses applications à la géométrie Diophantienne, dynamique algébrique, combinatoire additive...
- géométrie/topologie modérée (tame) = o-minimalité et NIP et ses applications : combinatoire, lemmes de régularite, théorie des jeux, et géométrie arithmétique...
- la Logique Continue et ses applications à l'analyse fonctionelle, la dynamique topologique...

On pourra retrouver une partie de cet exposé, plus détaillée et avec des références dans l'article "Introduction à la Théorie des modèles", E. Bouscaren, Gazette de la SMF, 2016.
https://smf.emath.fr/publications/la-gazette-des-mathematiciens-149-juillet-2016

Introduction

La **théorie des modèles est une branche de la Logique Mathématique**, plus jeune (vraiment constituée fin des années 40) et moins connue que ses deux soeurs ainées:
La théorie des ensembles (étude des fondements, axiomes, hypothèse du continu, axiome du choix...)
La théorie de la démonstration (étude des notions de "preuves" formelles, liens avec l'informatique théorique.)
La Théorie des Modèles est l'étude des structures et de la famille de leurs ensembles définissables.
Peu concernée par les questions de "fondements". Algèbre abstraite, géométrie abstraite et plus récemment, avec la logique continue, analyse fonctionelle abstraite..... ????.

Motivations : un exemple algébrique très simple et classique

Théorème

(Ax 1969) *Soit f une application polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$ ($n \geq 1$). Si f est injective, f est surjective.*

(L'application f est polynomiale : $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots f_n(x_1, \ldots, x_n))$ avec, pour chaque i, $f_i \in \mathbb{C}[X_1, \ldots, X_n]$.)

En fait démontré par Ax plus généralement pour $f : V^n \mapsto V^n$, V une variété algébrique, ou un schéma de type fini (également par Borel 69, Grothendieck et d'autres depuis...)
L'hypothèse que f est polynomiale est essentielle, il y a par exemple des contre-exemples de fonctions holomorphes

Comment démontrer le théorème d'Ax?

Theorème*(Ax 1969)*: Soit f une application polynomiale de $\mathbb{C}^n$ dans $\mathbb{C}^n$ ($n \geq 1$). Si f est injective, f est surjective.

Preuve modèle-théorique d'Ax:

Pour quels corps est-ce évidemment vrai?

1. Les corps finis Si K est un corps fini, n'importe quelle $f : K^n \mapsto K^n$ qui est injective est surjective.
2. Facile: les corps localement finis : tels que tout sous corps finiment engendré est fini:

on a $f = (f_1, \ldots, f_n) : K^n \mapsto K^n$ injective

$a \in K^n$, $K_0 < K$ finiment engendré par les coefficients des polynomes f_i et $a = (a_1, \ldots a_n)$. $f_0 := f|_{K_0}$ est polynomiale au-dessus de K_0, donc son image est dans K_0 et $f_0 : {K_0}^n \mapsto {K_0}^n$ est injective, K_0 est fini , donc f_0 est surjective et $a = f_0(b)$, $b \in {K_0}^n$.

3.Quels corps localement finis sont utiles? Pour p premier $\widetilde{\mathbb{F}_p}^{alg}$ = clôture algébrique du corps fini $\mathbb{F}_p$.

Donc: Le théorème est vrai pour $\widetilde{\mathbb{F}_p}^{alg}$, pour tout p.

4. On conclut directement que le théorème est vrai pour $\mathbb{C}$ par le théorème suivant très basique de théorie des modèles des corps.

Théorème de transfert: Une propriété qui s'exprime par une formule du premier ordre dans le langage des anneaux est vraie dans $\mathbb{C}$ si et seulement si elle est vraie dans $\widetilde{\mathbb{F}_p}^{alg}$ pour une infinité de premiers p.

Deux choses essentielles

–formule du 1er ordre dans le langage des anneaux (il faut évidemment et vérifier que le théorème d'Ax peut être exprimé ainsi)

– pourquoi on peut transférer? : car la limite quand p tend vers l'infini des corps $\widetilde{\mathbb{F}_p}^{alg}$ est isomorphe au corps $\mathbb{C}$.

Donc - notion générale de "limite" de structures qui permet de transférer les formules du 1er ordre.

ultraproduits ou le théorème fondamental: le théorème de compacité

Autre exemple similaire

On peut exactement de la même manière que pour le théorème d'Ax, démontrer à très peu de frais le résultat classique suivant (remarqué par Bertuccioni en 1992):

Théorème

Soit G un groupe fini d'ordre p^m, pour p premier, et γ une action algébrique de G sur $\mathbb{C}^n$. Alors l'action γ a un point fixe.

Des théorèmes de transfert plus compliqués

Théorème

(Conjecture d'Artin asymptotique)*(Ax-Kochen, 65) Soit un entier* $d \geq 1$. *Il existe un nombre premier* $p_0(d)$ *tel que pour tout* $p \geq p_0(d)$, *tout polynome sur* $\mathbb{Q}_p$, *homogène de degré* d *en* $n > d^2$ *variables, a un zéro non trivial dans* $\mathbb{Q}_p$.

Ce théorème se montre aussi par transfert: Ce résultat avait été montré (Carlitz, Lang) pour tout p, pour les corps des séries formelles à coefficients dans $\mathbb{F}_p$, $\mathbb{F}_p((t))$.

Théorème

(Ax-Kochen) Une propriété qui s'exprime par un énoncé du premier ordre dans le langage des corps (valués) est vraie dans $\mathbb{Q}_p$ pour presque tout p si et seulement si elle est vraie dans $\mathbb{F}_p((t))$ pour presque tout p.

Ce résultat (Artin) est nettement plus compliqué. Il a d'ailleurs fallu attendre plusieurs années pour qu'en soit donnée une démonstration purement géométrique (la preuve "théorie des modèles" date de 1965, il faudra attendre 2011 pour que Jan Denef présente une preuve purement géométrique).
Autres principes de transfert plus compliqués pour des formules qui ne sont plus du premier ordre : par exemple Cuckers-Loeser pour des égalités d'intégrales motiviques ...

Structures, Langage, Ensembles définissables

Ici, pas de définition formelle générale pour une structure abstraite juste des exemples,

– Pour les anneaux (commutatifs unitaires)

R un anneau : on va travailler dans le langage des anneaux: on s'intéresse aux sous ensembles de R^n qu'on peut définir à partir des opérations de base d'un anneau :

Notre structure dans ce cas $\langle R, +, -, ., 0, 1\rangle$

– Si on s'intéresse à la classe des *anneaux ordonnés* , on rajoutera l'ordre $\langle R, +, -, ., 0, 1, <\rangle$

– si on s'intéresse à la classe des groupes nos structures : $\langle G, ., ^{-1}, 1\rangle$

– pour la classe des groupes ordonnés $\langle G, ., ^{-1}, 1, <\rangle$

– anneaux différentiels : $\langle R, +, -, ., 0, 1, \delta\rangle$,

– graphes : $\langle S, E\rangle$ S sera l'ensemble des sommets et E la relation binaire qui relie deux sommets.

Le type d'opérations/relations choisies est le langage de la structure .

Ensembles définissables dans les anneaux (commutatifs unitaires)

La famille des ensembles définissables de la structure $\langle R, +, -., 0, 1\rangle$: pour chaque n on aura une famille de sous-ensembles de R^n , $Def_n(R)$, et $Def(R) := \bigcup_n Def_n(F)$.
On commence par la famille des ensembles basiques définis directement à partir des opérations, $Bas_n(R)$, puis on prendra la clôture par combinaisons booléennes finies (intersection, complémentaire, réunion) et par projection.
$D \subset R^n$ est un sous-ensemble basique si c'est l'ensemble des zéros d'un polynome :
$D(R) = \{(a_1, \ldots a_n) \in R^n : f(a_1, \ldots, a_n) = 0\}$ où $f \in R[X_1, \ldots, X_n]$.

Important On voit les ensembles définissables comme ensembles de solutions d'une "formule".
D est l' ensemble des solutions dans R de "$f(x_1, \ldots, x_n) = 0$, et donc en fait si on a un autre anneau $R' > R$ on peut considérer $D(R)$ et aussi $D(R')$.

Ensuite on définit les ensembles constructibles ou sans quantificateurs: combinaisons booléennes finies de Basiques.
$Cons(R)$ = la plus petite famille contenant $Bas(R)$ et close par complémentaire et intersections finies.
ici pour les anneaux = les ensembles constructibles au sens de la topologie de Zariski.

Ensembles définissables

Maintenant, Def(R): les ensembles définissables=la plus petite famille contenant $Bas(R)$ close par complémentaire, intersection finie et projection.
Au niveau des "formules" complémentaires = négation, intersection = conjonction (et), projection = quantificateur existentiel.

Pour d'autres exemples de structures :

Autres structures

si $\langle R, +, -, 0, 1, < \rangle$ un anneau ordonné on rajoute des ensembles/formules basiques on a aussi $f(x_1, \ldots, x_n) < 0$. alors les ensembles constructibles sont les ensembles semi-algébriques. Si on a $\langle R, +, -, 0, 1, \delta, \rangle$, un anneau différentiel, les ensembles basiques seront les zéros de polynômes différentiels (à nouveau obtenus en composant les opérations de base, addition, multiplication et la dérivation)
dans un groupe $\langle G, .^{-1}, 1 \rangle$, les formules basiques seront de la forme

$$x_1{}^{e_1} \ldots . x_n{}^{en} = 1$$

avec $e_i \in \mathbb{Z}$.

Les énoncés

Les Enoncés : si il n'y a pas de variable, ou si elles sont toutes quantifiées, on obtient des formules qui ne définissent pas des sous ensembles mais sont soit vraies soit fausses
Par exemple, un corps de caractéristique p vérifie $p = 0$, on dit que ce sont les modèles de cet énoncé.
Une théorie (dans un langage fixé) est un ensemble éventuellemnt infini d'énoncés : la théorie des anneaux, des groupes abéliens, des corps de caractéristique 0 algébriquement clos.

Les deux propriétés essentielles de la logique du premier ordre

on ne prend que des intersections finies (logique finitaire)

les variables représentent les éléments de la structure, pas des sous-ensembles (logique du premier ordre)
Les corps de caractéristique p vérifieront l'énoncé "p =0".
Les corps de caractéristique 0 vérifieront, pour chaque p l'énoncé $p \neq 0$. c'est une liste infinie de formules , pas UNE formule (sinon le théorème de transfert serait faux!)

Rapport avec les soeurs ainées

- La théorie des ensembles , au sens des axiomes de Zermelo-Frankel (ZF) ou ZFC (avec l'axiome du choix) c'est quoi?
Une structure a priori très simple $(U, \in)$ avec une seule relation (en plus de l'égalité), une relation binaire "$x \in y$ " , x appartient à y ou x est élément de y. Donc formules basiques : $x \in y$ ou $x = y$ et ensuite on clôt par negation, conjonction finie, et le quantificateur "$\exists$". les axiomes de ZF = des énoncés dans ce cadre, les éléments de U l'univers, sont les ensembles, les sous-parties définissables dans U sont "les classes".
- La théorie de la démonstration: Tout cela marche bien et a du sens parce que dans le background, il y a une notion de démonstration ou preuve formelle et le théorème de complétude de Gõdel qui dit que: " un énoncé ϕ est vrai dans tous les modèles d'un ensemble Σ d'énoncés si et seulement si il existe une "preuve formelle" de ϕ à partir des énoncés de Σ"

Extension, compacité

La bonne notion d'extension pour deux structures de même type/langage, extension élémentaire:
$\langle R, Def(R)\rangle \preceq \langle R', Def(R')\rangle$ si $R \subset R'$ et pour tout D définissable dans$Def_n(R)$, si $D(R')$ non vide alors $D(R)$ non vide. En particulier R et R' vérifient exactement les mêmes énoncés du premier ordre.
ex: $\mathbb{C}$ n'est pas une extension élémentaire de $\mathbb{R}$ car $x^2 = -1$ n'a pas de solution dans $\mathbb{R}$, mais c'est une extension élémentaire de $\mathbb{Q}^{alg}$.

Compacité

Une formulation du théorème de compacité:
Si dans une structure $\langle R, Def(R)\rangle$ on a une famille infinie de sous ensembles définissables $(D_i)_{i\in I}$ de R^n qui a la propriété de l'intersection finie (toute sous famille finie a une intersection non vide), alors il y a une extension élémentaire $\langle R', Def(R')\rangle$ de $\langle R, Def(R)$ dans laquelle l'intersection de tous les D_i est non vide.
= compacité de l'espace de Stone associé à l'algèbre de Boole des ensembles définissables.
Exemple de conséquence: considérons le corps ordonné $\mathbb{R}$ (langage des anneaux et l'ordre) dans $\mathbb{R}$ pour chaque entier $n > 0$ l'ensemble définissable D_n $\{x : 0 < x < 1/n\}$ est non vide mais l'intersection des D_n est vide. Par compacité il existe des corps ordonnés extensions élémentaires de $\mathbb{R}$ avec des éléments infiniment petits. De même pour des infiniment grands. C'est le début de l'analyse non standard....

Elimination des quantificateurs

On s'intéresse à la complexité des ensembles définissables
Théorème classique (Chevalley, Tarski) : Dans un corps algébriquement clos K, la projection d'un ensemble constructible est encore constructible. Donc les ensembles définissables sont les ensembles constructibles.
On dit que les corps algébriquement clos éliminent les quantificateurs
De même
Théorème (Seidenberg, Tarski) Dans le corps ordonné des réels $\mathbb{R}$ la projection d'un semi-algébrique est semi-algébrique.
———> décidabilité, effectivité ...
Et depuis, énormément de résultats de ce type dans des structures beaucoup plus compliquées dans les langages adéquats : corps différentiellement clos, corps valués henséliens, les p-adiques ———> applications à la théorie des nombres, à l'intégration motivique (Denef, Loeser, Cluckers...)

Théorie "moderne"

Dans les exemples plus haut, on part d'une structure donnée et on étudie ses ensembles définissables
mais dans le sens contraire:
Théorème (MacIntyre, 71) Si K est un corps infini tel que les ensembles définissables sont les ensembles constructibles (pour le langage des anneaux) alors K est algébriquement clos.
En passant à un niveau d'abstraction supplémentaire, développement de la théorie des modèles pure, ou théorie de la stabilité.
Le premier vrai résultat de stabilité, le théorème de Morley, en 1965.

Morley

Pour cela revenons aux corps algébriquement clos.
Si on fixe la caractéristique, disons 0, le type d'isomorphisme d'un corps algébriquement clos K est determiné par la cardinalité d'une base de transcendence sur $\mathbb{Q}$ (ensemble maximal d'éléments de K algébriquement indépendants au dessus de $\mathbb{Q}$).

Donc, infinité de corps algébriquement clos dénombrables à isomorphisme près :

$$\mathbb{Q}^{alg}, \mathbb{Q}(t_1)^{alg}, \ldots, \mathbb{Q}(t_1, \ldots, t_n)^{alg}, \ldots, \mathbb{Q}(t_1, \ldots, t_n, \ldots)^{alg}$$

où $t_1, \ldots, t_n, \ldots$ sont algébriquement indépendants.
Mais, pour toute cardinalité λ non dénombrable, il y aura à isomorphisme près un seul corps de cardinalité λ, celui dont une base de transcendence est de cardinalité λ.

Idem pour espaces vectoriels sur un corps k fixé.

Morley

Theorème (Morley 65) Soit Σ une théorie dans un langage fixé, dont tous les modèles sont infinis. Supposons que pour une cardinalité λ non dénombrable, il n'y ait (à isomorphisme près) qu'un seul modèle de Σ. Alors pour toute cardinalité non dénombrable , il y a un unique modèle de Σ à isomorphisme près.

La méthode: de ces hypothèses abstraites, Morley deduit de bonnes propriétés combinatoires de la famille des ensembles définissables, une bonne notion de dimension qui généralise la dimension linéaire ou la dimension algébrique, chaque ensemble définissable a une dimension finie. dans les corps algébriquement clos on retrouve pour les fermés de Zariski la dimension algébrique.

Shelah

La théorie des modèles pure.

Puis, Saharon Shelah.....

depuis 1975 : Théorie de la stabilité ou théorie de la classification . Classer les structures en fonction des objets de combinatoire infinie qu'on peut y définir: ordres, arbres, en déduire des propriétés générales positives et utiles. Si il n'y a pas d' ordre (théorie est stable) ni arbre (théorie est superstable), alors on peut définir une bonne notion d'indépendance, on peut assigner aux ensembles définissables une bonne notion de dimension, pas forcément finie .
Stable : corps algébriquement clos, espaces vectoriels, groupes abéliens
instables: graphe aléatoire, les réels

La stabilité Géométrique, Zilber et Hrushovski

A partir de la fin des années 80:
méthodes et outils inspirés de la géométrie : combinatoire ou algébrique.
première applications remarquées à la géométrie Diophantienne (Manin-Mumford, Mordell-Lang, par Hrushovski en 94).
Typique de la théorie des modèles Géométrique introduite par Zilber et Hrushovski:
– Classifier les structures par les objets algébriques qu'on peut y définir: groupes, corps
– développer de manière abstraite des outils inspirés de la géométrie algébrique ou des géométries combinatoires dans les structures avec bonne notion de dimension. exemple: dans $\mathbb{C}$, géométrie algébrique avec topologie de Zariski, dans $\mathbb{C}$ muni d'une dérivation adéquate, δ, on peut définir une nouvelle topologie, plus fine, la δ-topologie
...(utilisation pour Mordell-Lang)

Conjecture de Zilber

– caractériser de manière abstraite les structures mathématiques classiques .
Par exemple prenons la condition abstraite
(FM): Une théorie T est fortement minimale si dans tout modèle R de T, tout sous ensemble définissable de R (dimension 1) est fini ou alors son complémentaire est fini.
Trois types d'exemples classiques : - les corps algébriquement clos, les espaces vectoriels,
les ensembles sans structure (le langage est réduit à l'égalité).
Conjecture de trichotomie de Zilber: c'est les seuls!
finalement non: (Hrushovski 91) mais presque.

Les Géométries de Zariski

La conjecture de trichotomie est fausse en général: exemples de géométries combinatoires non classiques construites par Hrushovski (91).

Mais, avec des hypothèse supplémentaires sur la structure fortement minimale la trichotomie est vraie (Hrushovski-Zilber , Géométries de Zariski 93) . Outil essentiel dans les preuves originelles de Hrushovski de Mordell-Lang et Manin-Mumford, dans des applications plus récentes à la géométrie Diophantienne ou à la dynamique algébrique.

Généralisations de

– Théorème classique de Géométrie projective : un plan projectif Arguésien (des droites et des points satisfaisant certaines propriétés) est isomorphe au plan projectif associé à un espace vectoriel.

– Théorème de Weil qui reconstruit un groupe algébrique à partir d'une loi rationelle associative donnée génériquement sur une variété.

Supplément : l'o-minimalité

Retour au début :

- stabilité, théorie des modèles géométrique et ses applications à la géométrie Diophantienne, dynamique algébrique, combinatoire additive...
- géométrie/topologie modérée (tame) = o-minimalité et NIP et ses applications : combinatoire, lemmes de régularite, théorie des jeux, et géométrie arithmétique...
- la Logique Continue et ses applications à l'analyse fonctionelle, la dynamique topologique...

o-minimalité

Les réels, corps ordonné, sont instables en particulier pas fortement minimaux mais propriété très forte:
Quels sont les ensembles définissables en dimension 1? les sous-ensembles définissables de $\mathbb{R}$?
réunion finie d'intervalles et de points.
Cela est-il encore vrai si on agrandit la classe des ensembles définissables, c'est à dire si on enrichit le langage, par exemple en s'autorisant à utiliser, pour construire les ensemble basiques de nouvelles fonctions réelles?
Définition (van den Dries, Pillay-Steinhorn) On dit qu'un enrichissement du corps ordonné $\mathbb{R}$ est o-minimal (order minimal) si les seuls ensembles définissables, en dimension 1, dans le nouveau langage sont toujours les réunions finies d'intervalles.
Ce n'est plus vrai si on s'autorise par exemple à rajouter dans le langage la fonction sinus : $\{x : sin\ x = 0\}$ est alors un ensemble définissable infini discret

Quel intérêt? On peut montrer que la pluspart des propriétes des semi-algébriques dans les réels sont vraies pour tous les ensembles définissables dans une structure o-minimale.

Et en 1996, Wilkie a montré l'o-minimalité des les réels avec l'exponentielle : $\mathbb{R}_{exp}$ dans laquelle on autorise aussi les formules basiques du type $f(x_1, \ldots, x_n) = 0$ et $f(x_1, \ldots, x_n) > 0$, où f n'est plus simplement un polynôme mais est un polynôme exponentiel, c'est-à-dire obtenu par composition des opérations basiques, l'addition, l'opposé, la multiplication et la fonction exponentielle réelle.

Ensuite (Van den Dries, Miller) $\mathbb{R}_{an}$, dans laquelle on autorise toutes les fonctions analytiques réelles restreintes, c'est-à-dire, toutes les fonctions $h : \mathbb{R}^m \mapsto \mathbb{R}$ dont la restriction à $[-1, 1]^m$ est analytique réelle et qui sont nulles en dehors, et enfin la structure $\mathbb{R}_{an,exp}$ dans laquelle on peut composer toutes les fonctions précédentes pour définir les formules basiques.

Applications très récentes à la géométrie arithmétique (conjecture d'André-Oort par exemple), à la combinatoire et à la théorie des jeux!