Table des matières

Principe AKE et notion d'Hensélliennité dans les corps de différence valués

Esther Elbaz sous la direction de Zoé Chatzidakis

17 octobre 2012

La théorie des modèles est une branche de la logique qui a pour objet d'étude les structures mathématiques. Si les applications de la théorie des modèles à l'algèbre ou à d'autres branches des mathématiques n'en constituent bien sûr pas l'essence, celles-ci sont néanmoins nombreuses. En 1995, Hrushowski a par exemple résolu une difficile conjecture de Mordell-Lang sur les corps de fonctions par une preuve dont le noyau fonctionne aussi bien en caractéristique nulle (où les géomètres en connaissaient déjà une) qu'en caractéristique positive (où la preuve de Hrushowski est à ce jour la seule connue). En 1965, une autre conjecture due à Artin a été démontrée par Ax et Kochen. Le principe de leur démonstration a pu être élargi pour montrer un théorème appelé principe AKE et qui dit que la théorie de certaines classes de corps valués est entièrement déterminée par la théorie de leurs corps résiduels et celle de leur groupe de valeurs. Ce principe est bien évidemment précieux pour comprendre la théorie de ces corps, et on a cherché à l'étendre à des classes plus larges de corps valués ou même à d'autres structures. Il a par exemple été récemment démontré un principe AKE pour certains modules. Une théorie souvent étudiée en théorie des modèles est la théorie des corps de différence valués qui sont des corps valués munis d'un automorphisme distingué σ. Pour ces structures la notion d'algébricité n'est pas pertinente et est remplacée par celle de σ-algébricité c'est à dire la propriété d'être racine d'un polynôme en les variables $X, \sigma(X), \sigma^2(X), ...$ En définissant, pour une certaine classe de corps de différence valués, une notion d'Hensélliennité (qui affirme la possibilité de relever certains éléments du corps résiduel en une racine d'un σ-polynôme) Salih Azgin a démontré un principe AKE pour ces corps. Après de brefs rappels sur les notions de base de logique et sur les corps valués, nous énoncerons le principe AKE et en exposerons certaines applications. Dans la section 3, nous essayerons d'expliquer brièvement sur quoi repose la preuve de ce principe. Puis dans la dernière partie, nous tenterons de donner un aperçu de la façon dont les ingrédients clé de cette preuve peuvent être transposés dans le cadre des corps de différence valués grâce à la notion d'Hensélliennité définie par Azgin.

Je tiens à exprimer mes plus vifs remerciements à Zoé Chatzidakis qui a dirigé mon mémoire avec une attention toujours chaleureuse. L'encadrement et la disponibilité dont elle m'a fait bénéficier cette année, malgré toutes ses occupations, ont été pour moi une chance dont je suis très consciente et pour laquelle je lui suis très reconnaissante.

1 Rappels de logique

Commençons par rappeler quelques définitions et notions de logique. Un **langage** L est un ensemble de symboles de fonctions et de relations. Une **L-structure** M est la donnée d'un ensemble M et pour chaque symbole de fonction (resp. de relation) de L d'une fonction (resp. d'une relation), que l'on appelle son interprétation.
Un **morphisme de structure** est alors une fonction qui respecte les interprétations des fonctions et des relations.

Exemple. Soit le langage $L = \{+; -; 0\}$ où $+$ et - sont des fonctions binaires et 0 une fonctions 0-aire, i.e. une constante. Tout anneau est une L-structure.

Toute formule F écrite a l'aide des symboles de L, de variables et de connecteurs logiques $\neg, \wedge, \vee, \forall, \exists$ peut donc être interprétée dans une L-structure M. Les variables d'une formule qui ne sont pas quantifiées sont dites **libres**. Si $x_1, \ldots, x_n$ sont les variables libres d'une formule F, on note cette formule $F(x_1, \ldots, x_n)$; et si $a_1, \ldots, a_n$ sont n éléments de M, on dit que $F(a_1, \ldots, a_n)$ est vraie dans M si la formule obtenue en interprétant x_1 par a_1,. . . , x_n par a_n est vraie dans M.
On dit qu'un sous-ensemble X de M^n est **définissable** s'il existe une formule $F(x_1, \ldots, x_n)$ telle que $P = \{a \in M^n | F(a) \text{ est vraie dans } M\}$. Par exemple, dans le langage $L = \{0; +\}$ l'ensemble défini par la formule $\exists y, y + y = x$ correspond dans $\mathbb{N}$ considéré de façon naturelle comme une L-structure, à l'ensemble des nombres pairs.
Une **théorie** T est un ensemble de L-formules sans variables libres. On dit que M est un **modèle** de T, si M satisfait toutes les formules de T.
On dit qu'une théorie est **décidable** s'il existe un algorithme qui étant donné une formule F permet de déterminer si F est vraie dans tous les modèles de T.
On note $Th(M)$ et on appelle théorie de M l'ensemble des énoncés vrais dans M. Deux L-structures M et N sont dites élémentairement équivalentes si elles ont la même théorie, on le note $M \equiv N$.

Exemple. On peut montrer que deux corps algébriquement clos sont élémentairement équivalents si et seulement si ils ont même caractéristique.

Enfin, si $M \subset N$, sont deux L-structures telles que les interprétations des symboles sur M sont induites par leurs interprétations dans N, on dit que M est une **sous-structure** de N (ou que N est une **extension** de M.). Si de plus, pour toute formule $F(x_1, ..., x_n)$, et tout n-uplet a de M, $F(a)$ est vraie dans M si et seulement si $F(a)$ est vraie dans N, on dit que M est une **sous-structure élémentaire** de N (ou que N est une **extension élémentaire** de M.)

Une **application** f entre deux L-structures M et N est dite **élémentaire** si pour toute formule $F(x_1, \ldots, x_n)$ à n variables libres, pour tout n-uplet $(m_1, \ldots, m_n) \in M$ $F(m_1, \ldots, m_n)$ est vraie dans M ssi $F(f(m_1), \ldots, f(m_n))$ l'est dans N. Ainsi $M \subset N$ est une sous-structure élémentaire de N ssi l'inclusion est une application élémentaire.
Une application **élémentaire partielle** sur M est une application f qui n'est définie que sur une sous-structure A de M et telle que pour toute formule $F(x_1, \ldots, x_n)$ à n variables libres, pour tout n-uplet $(a_1, \ldots, a_n) \in A$, $F(a_1, \ldots, a_n)$ est vraie dans M ssi $F(f(a_1), \ldots, f(a_n))$ l'est dans N.

On dit qu'une théorie **élimine les quantificateurs** si toute formule est équivalente à une formule sans quantificateurs. Ainsi, si une théorie élimine les quantificateurs, tous les ensembles définissables sont engendrés par les intersections, unions et complémentations d'ensembles définis par des formules atomiques.

La propriété d'élimination des quantificateurs dépend du langage considéré et pour toute théorie il existe un langage permettant d'obtenir l'élimination des quantificateurs. Toutefois de tels langages sont en général trop gros pour pouvoir être intéressants. Ce qu'on cherche c'est plutôt une extension minimale du langage qui permette l'élimination des quantificateurs.

Exemple La théorie des corps algébriquement clos admet l'élimination des quantificateurs (dans le langage des corps). Ce fait permet de démontrer un théorème de Chevalley. Soit K un corps algébriquement clos. Soit $X \subset K^n$ un ensemble constructible (c'est à dire une combinaison booléenne de fermés pour la topologie de Zariski). Alors l'image de X par une application polynomiale est elle aussi constructible.
Pour démontrer ce théorème, il suffit de remarquer que par élimination des quantificateurs les ensembles constructibles correspondent exactement aux ensembles définissables et que l'image d'un ensemble définissable par une application polynomiale est elle aussi définissable.

2 Corps valués

2.1 Définitions et exemples.

2.1.1. Définition Soit K un corps et Γ un groupe abélien totalement ordonné. Une **valuation** est une application $v : K \to \Gamma \cup \{\infty\}$ satisfaisant, pour tout $a, b \in K$ et pour tout $\gamma \in \Gamma$:

(i) $v(a) = \infty \Leftrightarrow a = 0$.
(ii) $v(a + b) \geq \min\{v(a), v(b)\}$.
(iii) $v(ab) = v(a) + v(b)$
(iv) $\gamma < \infty$. On pose $\gamma + \infty = \infty$.

Un **corps valué** (K, v) est un corps K muni d'une **valuation** v.

L'ensemble $\{x \in K | v(x) \geq 0\}$ est un anneau et est appelé L'**anneau de valuation** de K. On le note O.
L'ensemble $\{x \in K | v(x) > 0\}$ est l'idéal maximal de O. On le note M.
On appelle **corps résiduel** de K, le corps O/M, noté k.
La projection canonique $O \to k$ sera notés res.

Il existe plusieurs langages qui permettent de parler des corps valués. Ceux-ci sont équivalents à biinterprétabilité près. Nous étudierons la théorie des corps valué dans le **langage à trois sortes** : une structure à trois sortes (K, Γ, k) est constituée de trois univers disjoints : K est l'univers de la sorte "corps", Γ celui de la sorte "groupe" et k celui de la sorte "corps résiduel". Les variables et constantes viennent avec une étiquette de sorte. Chaque sorte vient avec son langage, qui est celui des corps pour les deux corps, et celui des groupes ordonnés pour le groupe ordonné. Le langage contient de plus un symbole ∞ et les fonctions à 1-arité $v : K \to \Gamma \cup \{\infty\}$ et $res : K \to k$. O et M sont des ensembles définissables dans ce langage. Bien évidemment, au corps valué (K, v) nous associerons la structure (K, Γ, k), où Γ est le groupe de valeurs de K.

2.1.2. Exemples

a. Les valuations sur $\mathbb{Q}$. Soit p un nombre premier. On définit la **valuation p-adique** sur $\mathbb{Q}$, de la façon suivante : soit a/b un élément de $\mathbb{Q}$ avec a et b deux entiers premiers entre eux. Soient n le plus grand entier tel que p^n divise a et m le plus grand entier tel que p^m divise b ; on définit

$v(a/b) = n - m$. Le groupe de valeurs de $(\mathbb{Q}, v)$ est isomorphe à $\mathbb{Z}$, son corps résiduel est isomorphe à $\mathbb{F}_p$. Le complété de $\mathbb{Q}$ pour cette valuation est noté $\mathbb{Q}_p$.

b. Corps de Hahn. On dit qu'un ensemble totalement ordonné I est **bien ordonné** si tout sous-ensemble non vide de I admet un plus petit élément, ou, de façon équivalente, si toute suite strictement décroissante d'éléments de I est finie.
Soient k un corps et Γ un groupe abélien ordonné. On définit le **corps de Hahn** $k((\Gamma))$ dont les éléments sont les sommes formelles $f = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ avec $a_\gamma \in k$, pour tout f dont le support Supp(f)=$\{\gamma | a_\gamma \neq 0\}$ est bien ordonné. On définit une addition et une multiplication sur $k((\Gamma))$ en posant

$$\sum_{\gamma \in \Gamma} a_\gamma t^\gamma + \sum_{\gamma \in \Gamma} b_\gamma t^\gamma = \sum_{\gamma \in \Gamma} (a_\gamma + b_\gamma) t^\gamma$$

et

$$(\sum_{\gamma \in \Gamma} a_\gamma t^\gamma)(\sum_{\gamma \in \Gamma} b_\gamma t^\gamma) = \sum_{\gamma \in \Gamma} (\sum_{\gamma' \in \Gamma} a_{\gamma - \gamma'} b_{\gamma'}) t^\gamma$$

Ces opérations munissent bien $k((\Gamma))$ d'une structure de corps.
On définit une valuation sur $k((\Gamma))$ en posant $v(f) = \inf Supp(f)$.
L'anneau de valuation est constitué des séries dont le support ne contient que des éléments strictement positifs.
On notera $k((t))$ le corps de Hahn $k((\mathbb{Z}))$.

2.1.3. Définition. Un corps valué (K, v) est dit **Hensélien** si pour tout polynôme $P(X) \in O[X]$ et tout $a \in O$ tel que $res(P(a)) = 0$ et $res(P'(a)) \neq 0$, il existe $b \in O$ tel que $P(b) = 0$ et $res(a) = res(b)$.
(La propriété d'être Hensélien est donc une propriété du premier ordre.)

2.1.4. Exemple. Tout corps valué sur $\mathbb{Z}$ complet pour la distance associée (comme $\mathbb{Q}_p$) est Hensélien.

2.2 Principe AKE et applications

La classe des corps Henséliens de caractéristique résiduelle nulle forme une classe élémentaire dans le langage considéré qui est particulièrement étudiée en théorie des modèles depuis un théorème démontré en 1965 par Ax et Kochen et de façon indépendante par Ershov :

2.2.1. Théorème. (Ax-Kochen-Ershov) : Soient K et L deux corps valués Henséliens de caractéristique résiduelle nulle. Ils sont élémentairement équivalents si et seulement si leurs groupes de valeurs sont élémentairement équivalents (dans le langage des groupes) et leurs corps résiduels sont élémentairement équivalents (dans le langage des anneaux).

Ce théorème, que nous désignerons dans la suite par "principe AKE", implique que toute propriété du premier ordre exprimable dans le langage considéré est vraie dans un corps valué K qui est

Hensélien et de caractéristique résiduelle 0 si et seulement si elle est vraie dans le corps de Hahn $k((t^\Gamma))$ où k est le corps résiduel de K et Γ son groupe de valeurs.
Il implique également que la théorie d'un corps valué Hensélien de caractéristique résiduelle nulle est décidable si et seulement si la théorie de son groupe de valeurs (dans le langage des groupes) et celle de son corps résiduel (dans le langage des anneaux) le sont.

Ce théorème était motivé par la démonstration d'une conjecture d'Artin qui prévoyait que pour tout $d \in \mathbb{N}$, et pour tout nombre premier p, tout polynôme homogène de degré d dans $\mathbb{Q}_p$ en au moins d^2+1 variables a une racine non triviale. Cette conjecture s'est révélée être fausse. Toutefois, Ax et Kochen ont démontré une version affaiblie de cette conjecture : pour tout d il y a au plus un nombre fini de nombres premiers pour lesquels il existe un polynôme homogène de degré d dans $\mathbb{Q}_p$ en au moins d^2+1 variables qui n'a pas de racine non triviale. Ce résultat a été démontré de façon purement algébrique il y a seulement quelques années.

On définit l'**ultraproduit** des $\mathbb{F}_p((t))$ (respectivement $\mathbb{Q}_p$) comme l'ensemble produit des $\mathbb{F}_p((t))$ (respectivement $\mathbb{Q}_p$) où p parcourt l'ensemble des nombres premiers, quotienté par la relation d'équivalence $x = y \Leftrightarrow$ toutes les composantes de x sont égales à celles de y sauf peut-être pour un nombre fini d'entre elles.
Ces ultraproduits sont des L-structures dans lesquels on considère qu'une formule atomique est vraie si et seulement si elle l'est pour tous les $\mathbb{F}_p((t))$ (respectivement $\mathbb{Q}_p$) sauf peut-être un nombre fini d'entre eux. Le théorème de Los affirme alors qu'une formule quelconque est vraie dans l'ultraproduit des $\mathbb{F}_p((t))$ (respectivement des $\mathbb{Q}_p$) si et seulement si elle l'est dans tous les $\mathbb{F}_p((t))$ (respectivement $\mathbb{Q}_p$) sauf peut-être un nombre fini d'entre eux.
En particulier la conjecture d'Artin est vrai dans l'ultraproduit des $\mathbb{F}_p((t))$ (respectivement des $\mathbb{Q}_p$) si et seulement si elle l'est dans tout les $\mathbb{F}_p((t))$ (respectivement $\mathbb{Q}_p$) sauf peut-être un nombre fini d'entre eux.
Pour démontrer la conjecture d'Artin, Ax et Kochen ont montré (en admettant l'hypothèse du continue) que ces deux ultraproduits sont isomorphes (c'est le "Théorème de transfert").
La conjecture d'Artin étant vraie dans l'ultraproduit de $\mathbb{F}_p((t))$, ils ont alors pu montrer qu'elle l'est aussi dans l'ultraproduit des $\mathbb{Q}_p$ et ainsi obtenir (une version correcte de) la conjecture d'Artin. [1]
Au départ Ax et Kochen avaient simplement énoncé le théorème "de transfert". La méthode permettant de démontrer ce théorème avait été exploitée pour démontrer d'autre résultat sur $\mathbb{Q}_p$, notamment sa décidabilité et une élimination relative des quantificateurs. Dans [2], Simon Kochen a donné une vision unifiée de tous ces résultats qui découlent de ce qu'il a appelé le théorème de l'isomorphisme.
Le principe AKE a depuis été généralisé à une classe plus large que celle des corps Henséliens de caractéristique résiduelle 0. La plus part de ces généralisations repose sur le même principe mais l'une d'elle proposée par F.-V. Kuhlmann pour les corps parfaits de caractéristique non nul et qui sont algébrique maximaux [2] repose sur des méthodes complètement différentes et encore mal comprises.

Le principe AKE (ou le théorème de transfert) permet également de démontrer une conjecture de Lang (pour laquelle il existe aussi une démonstration algébrique, mais difficile) :

1. Si on veut appliquer directement le principe AKE énoncé en 2.2.1, on remarque que les deux ultraproduits sont des corps Henséliens de caractéristique résiduelle 0 qui ont le même corps résiduel et le même groupe de valeurs.

2. Un corps est algébrique maximal s'il ne possède pas d'extension algébrique propre qui ait le même groupe de valeurs et le même corps résiduel que lui. Un corps algébrique maximal est Hensélien, la réciproque est vraie pour certains corps (notamment ceux de caractéristique résiduelle 0) mais ne l'est pas en général.

2.2.2. Théorème Soit d un entier, et P un polynôme homogène de degré d, à coefficients entiers, en d+1 indéterminées. Alors P possède une racine non triviale dans $\mathbb{Q}_p$ pour presque tout p (i.e. tous sauf un nombre fini d'entre eux).
Pour la démonstration, on utilise un théorème de Chevalley d'après lequel pour tout premier p, il existe une racine non triviale de P dans $\mathbb{F}_p$, et donc a fortiori dans $\mathbb{F}_p((t))$. Par le principe AKE, il existe donc aussi une racine non triviale dans l'ultraproduit des $\mathbb{Q}_p$ c'est à dire dans presque tous les $\mathbb{Q}_p$

Si la démonstration de (la version corrigée de) la conjecture d'Artin et de celle de Lang est sans doutes l'un des résultats les plus frappants de l'application du principe AKE, il en existe également d'autres. Mentionons-en deux.

2.2.3. Définition. Soit k un corps. Le **corps des séries de Puiseux** sur K est le corps égal à l'union croissante $\bigcup_{n\in\mathbb{N}} k((t^{1/n}))$. Nous noterons $P(k)$ le corps des séries de Puiseux sur k qui est muni d'une valuation naturelle sur $\mathbb{Q}$.

Certaines propriétés algébriques de k se "transmettent" à $P(k)$. Par exemple, c'est un fait connu que si k est algébriquement clos et de caractéristique résiduelle 0, alors il en est de même de $P(k)$. (Ce résultat tombe en défaut si la caractéristique du corps n'est pas nulle.) Un autre exemple de propriété algébrique dont "hérite" $P(k)$ est la propriété d'être un corps réel clos.

Grâce au principe AKE, on peut montrer que si k est élémentairement équivalent (dans le langage des corps) à $\mathbb{Q}_p$, alors $P(k)$ l'est aussi (dans le langage des corps). [3]
Pour le démontrer, on commence par remarquer grâce au principe AKE, que $P(k)$ muni de sa valuation naturelle est élémentairement équivalent à $P(\mathbb{Q}_p)$. On démontre ensuite l'existence d'une extension (de corps, non de corps valué) élémentaire (dans le langage des corps) de $P(\mathbb{Q}_p)$ qui puisse être munie d'une valuation telle que le corps valué ainsi obtenu est Hensélien avec un corps résiduel élémentairement équivalent à $\mathbb{F}_p$ et un groupe de valeurs élémentairement équivalent à $\mathbb{Z}$ et tel que $v(p) = 1$. Une nouvelle application du principe AKE [4] permet alors de montrer que ce corps est élémentairement équivalent à $\mathbb{Q}_p$.

Soient M et N deux structures d'un même langage L telles que $M \subseteq N$. M est dit **existentiellement clos** dans N si pour tout $a \in N$ qui vérifie une certaine formule sans quantificateurs sur N, on peut trouver un $b \in M$ satisfaisant la même formule.

Il existe des variantes du principe AKE où "être élémentairement équivalent" est remplacé par "être existentiellement clos dans" ou par "être une extension élémentaire de".
La première variante a été mise à profit par F.-V. Kuhlmann pour étudier les espaces de Riemann des corps de fonctions algébriques de caractéristique 0 [3].

---

3. Si un corps est élémentairement équivalent (dans le langage des corps) à $\mathbb{Q}_p$, alors il peut être muni d'une valuation qui le rende élémentairement équivalent (dans le langage des corps valué) à $\mathbb{Q}_p$.

4. Tout corps valué Hensélien de caractéristique 0, de groupe de valeur et de corps résiduel élémentairement équivalents à ceux de $\mathbb{Q}_p$, et tel que $v(p)$ est le plus petit élément non nul de son groupe de valeur, est équivalent à $\mathbb{Q}_p$.

2.3 Élimination des quantificateurs de corps

Soit K un corps valué. Une **section croisée** est une application du groupe de valeurs dans le corps résiduel k qui permet de voir le groupe de valeurs comme un sous-groupe de $(k^*, \times)$. [5] On ajoute au langage à trois sortes un symbole de fonction à une arité s de l'univers de la sorte groupe vers la sorte corps résiduel, pour obtenir le langage $L(s)$.
Le théorème de l'isomorphisme dont le principe AKE est une conséquence permet d'obtenir une élimination relative des quantificateurs pour les corps Henséliens de caractéristique résiduelle 0 munis d'une section croisée.

2.3.1. Théorème. Dans $L(s)$, la théorie T des corps valués Henséliens de caractéristique résiduelle nulle et munis d'une section croisée, élimine les quantificateurs de corps : étant donnée une formule $F(x, \gamma, u)$, où x est un uplet de variables du corps, γ de variables du groupe, et u de variables du corps résiduel, il existe une formule $G(x, \gamma, u)$, dans laquelle les seules variables quantifiées sont celles de corps résiduel ou de groupe, et qui est équivalente à $F(x, \gamma, u)$ modulo T.

3 Principe des preuves

3.1 Méthode du va et vient

Le théorème AKE énoncé en 2.1 est une conséquence du théorème suivant :
3.1.1. Théorème. Soient K et K' deux corps valués Henséliens et de caractéristique résiduelle 0. Supposons que leurs corps résiduels et leurs groupes de valeurs soient élémentairement équivalents. Soit I l'ensemble des isomorphismes partiels dont les domaines de définition sont des sous-corps de K dénombrables et tels que les applications induites sur les corps résiduels et les groupes de valeurs élémentaires partielles. I forme ce qu'on appelle un **système de va-et-vient** : pour tout élément $f \in I$ et pour tout $a \in (K, \Gamma, k)$, il existe $g \in I$ qui prolonge f et dont le domaine de définition contient a ; et pour tout $a' \in (K', \Gamma', k')$, il existe $g \in I$ qui prolonge f et dont l'image contient a'.

Cela suffira à établir le principe AKE. En effet, supposons ce théorème démontré. Soient K et K' deux corps valués Henséliens de caractéristique résiduelle 0. L'ensemble I n'est pas vide : K et K' étant de caractéristique nulle, le corps valué $(\mathbb{Q}, \{0\}, \mathbb{Q})$ est un sous-corps commun à K et K' qui donne l'existence d'un élément de I. Soit F est une formule de la forme $\exists x G(x)$ où G est une formule sans quantificateurs, qui est satisfaite dans K. Soit $a \in K$ tel que $G(a)$ est vrai. Soit $f \in I$ dont le domaine de définition contient a et soit a' l'image de a par f. Alors $G(a')$ est vraie dans K' puisque f est un isomorphisme de son ensemble de définition sur son image. Et donc F est vraie dans K'. Ainsi, et par symétrie des rôles de K et K', $F = \exists x G(x)$ où G est une formule sans quantificateurs est vraie dans K ssi elle est vraie dans K'. (Si F est de la forme $\forall x G(x)$ où G est une formule sans quantificateurs, on remarque qu'elle est fausse dans K ssi la formule $\exists x \neg G(x)$ est vraie dans K donc ssi la formule $\exists x \neg G(x)$ est vraie dans K' donc ssi la formule $\forall x G(x)$ est fausse dans K'.) On fait alors une récurrence sur le nombre de quantificateurs des formules et on montre ainsi que K et K' sont élémentairement équivalents. Cette méthode que nous venons de décrire est classique et connue sous le nom de **technique du va-et-vient**.

Donnons un aperçu de la façon (à quelques inexactitudes près) dont se montre ce théorème : soient $f \in I$, K_0 son ensemble de définition et K'_0 son image. On note k_0 et k'_0 leurs corps résiduels

5. Tout corps valué n'admet pas une section croisée. Il existe néanmoins toujours une extension élémentaire qui puisse être munie d'une section croisée.

respectifs.
Des théorèmes élémentaires de logique permettent de supposer quitte à en prendre des extensions élémentaires que K et K' vérifient une propriété de logique appelée $\aleph_1$-saturation, et qui implique en particulier le fait suivant : Soit $\alpha \in k - k_0$, le fait que les corps résiduels de K et K' sont élémentairement équivalents permet de "reproduire" α dans k', c'est à dire de trouver $\alpha' \in k'$ tel que $k_0(\alpha)$ est isomorphe (par un isomorphisme prolongeant celui induit par f) à $k'_0(\alpha')$. (On a aussi une propriété analogue pour le groupe de valeurs).
Tout le problème est donc de "remonter" aux corps valués c'est-à-dire de trouver $a \in K$ et $a' \in K'$ dont les images résiduelles sont respectivement α et α' et tels que $K_0(a) \cong K'_0(a')$. C'est là que la propriété d'Henséliennité intervient et permet de trouver les élément a et a' cherchés. Cela permet d'étendre les corps résiduels des domaines de définition des éléments f de I (et par symétrie de ceux des images d'éléments f de I.)
(On procède de façon analogue pour les groupe de valeurs.)
Il reste à montrer comment pour tout $x \in K$, on peut prolonger $f \in I$ par un élément $g \in I$ dont le domaine de définition contient x. Cela nécessite une propriété que vérifient les corps de caractéristique résiduelle 0 : l'unicité de l'extension immédiate maximale qui est décrite dans la sous-section suivante. Nous reviendrons sur la démonstration du théorème 3.1.1 dans la section 3.3.

3.2 Unicité de l'extension immédiate maximale

Soit (K, v) un corps valué. On dit qu'un corps valué (L, v') est une **extension du corps valué** (K, v), si le corps L est une extension du corps K et que v' prolonge v.
Soit (L, v') une extension d'un corps valué (K, v). Il est bien évidemment possible que (L, v') ait un groupe de valeurs ou un corps résiduel qui soit strictement plus grand que ceux de (K, v). (Par exemple si k est un corps et k' une extension stricte de k, alors pour tout groupe abélien ordonné Γ, le corps de Hahn $k'((\Gamma))$ a pour corps résiduel k' et est une extension du corps de Hahn $k((\Gamma))$ dont le corps résiduel k est strictement inclus dans k'.)

3.2.1. Définitions. Soit (K, v) un corps valué. Une extension de (K, v) est une **extension immédiate** si son groupe de valeurs et son corps résiduel sont égaux respectivement au groupe de valeurs et au corps résiduel de (K, v).
Un corps est dit **maximal** s'il ne possède pas d'extension propre immédiate.
Un corps est dit **algébrique maximal** s'il ne possède pas d'extension propre immédiate qui soit algébrique.

Irving Kaplansky a donné dans [1] une caractérisation des corps valués maximaux. Les résultats présentés par Irving Kaplansky reposent sur le concept de suite pseudo-convergente. Ils peuvent être réformulés de la façon suivante.

3.2.2. Définitions. Soient K un corps valué et L une extension de K. On dit qu'une suite $(a_k)_{k<\kappa}$ d'éléments de K indexée par un ordinal κ est dite **pseudo-convergente** de **limite** $x \in L$ si la suite $(v(x - a_k))_{k<\kappa}$ est strictement croissante. $x \in L$ une extension de K, algébrique sur K et limite d'une suite $(x_n)_n$ est dit **limite canonique** de $(x_n)_n$ si aucun z avec $[K(z) : K] < [K(x) : K]$ n'est limite de $(x_n)_n$.

3.2.3. Proposition.
a. Un corps valué K est maximal ssi toute suite pseudo-convergente de K a une limite dans K.
b. Un corps valué K est algébrique maximal ssi tout suite pseudo-convergente qui a une limite

algébrique sur K a une limite dans K.
c. Soient M et N deux extensions immédiates de K, $x \in M$ et $y \in N$ deux limites d'une même suite (x_n) de K. Supposons qu'ils sont soit tous deux transcendants sur K, soit de même polynôme minimal et limites canoniques de (x_n). Alors $K(x)$ est K-isomorphe (en tant que corps valué) à $K(y)$.

Krull a démontré qu'un corps valué admet toujours une extension immédiate maximale. Une telle extension s'obtient à partir de K par une série d'adjonctions transfinie de point limites, et, en fait, de point limites canoniques. La question de l'unicité de l'extension maximale revient donc à se demander s'il existe une unique façon de procéder à ces adjonctions, et donc d'après 3.2.2.c, se reformule ainsi :
Soient M et N deux extensions immédiates algébriques maximales de K et $x \in N$ de polynôme minimal P sur K et limite canonique d'une suite $(x_n)_n$ de K. Existe-t-il $y \in M$ de polynôme minimal P sur K et limite canonique de $(x_n)_n$? (*)
En particulier, l'unicité de l'extension immédiate maximale est équivalente à l'unicité de l'extension immédiate algébrique maximale.
Irving Kaplansky a répondu par l'affirmative à (*) pour certains corps valués, et notamment ceux de caractéristique résiduelle zéro.

3.3 Retour à la démonstration du principe AKE.

Nous avions laissé en suspens la question suivante : en gardant les mêmes hypothèses que celle formulées dans la section 3.1, soient $f \in I$ de domaine de définition K_0, et $a \in K - K_0$. On cherche $g \in I$ qui prolonge f et dont le domaine de définition contient a.

L'unicité de l'extension immédiate maximale intervient ici. Soit M une extension immédiate maximale de $K_0(a)$ dans K (l'existence de M est assurée dés que K est $\aleph_1$-saturé.). En étendant les groupes de valeurs et les corps résiduels, il est possible de se ramener à un élément g de I dont le domaine de définition K_1 est inclus dans M et dont M est une extension immédiate. Soient K_1' l'image de K_1 par g et M' une extension immédiate maximale de K_1' dans K'. Par unicité de l'extension immédiate maximale, il existe, entre M et M', un isomorphisme qui prolonge g. Comme $a \in M$ cela termine la démonstration du théorème 3.1.1.

4 Corps de différence valués

Le principe AKE est un outil très puissant. Il a été possible de le généraliser à d'autres structures (par exemple certains modules) et notamment à certains corps de différence valués.

4.1 Définitions

4.1.1. Définitions. Un **corps de différence valué** est un corps valué K muni d'un endomorphisme distingué σ tel que pour tout $x \in K$, si $v(x) = 0$, alors $v(\sigma(x)) = 0$, et si $v(x) > 0$, alors $v(\sigma(x)) > 0$

Soient (K, v, σ) un corps de différence valué, k son corps résiduel et Γ son groupe de valeurs. σ induit un endomorphisme sur k : pour $a \in K$, on associe $res(\sigma(a))$ à $res(a)$. Nous noterons $\bar{\sigma}$ cet endomorphisme.

Si σ est un automorphisme, alors σ induit un automorphisme sur le groupe de valeurs Γ : soient $\gamma \in \Gamma$ et $a \in K$ tels que $v(a) = \gamma$. L'application induite par σ sur Γ associe $v(\sigma(a))$ à γ. Nous noterons encore σ l'application induite par σ sur Γ. Comme $\sigma(O) = O$, cet automorphisme préserve l'ordre.

Pour parler des corps de différence valués, on utilise le langage à trois sortes augmenté d'un symbole σ correspondant à l'endomorphisme distingué.

4.1.2. Définition. Nous dirons que σ est **contractant** si pour tout $n \in \mathbb{N}$, pour tout $a \in K^*$ tel que $v(a) > 0$, $v(\sigma(a)) > nv(a)$.
Nous ne considérerons dans la suite que des corps de différence valués munis d'un automorphisme contractant.

4.1.3. Donnons un exemple d'un corps de différence valué dont l'automorphisme distingué est contractant. Soit le groupe $\Gamma = \mathbb{Z}[\theta, \theta^{-1}]$; on ordonne Γ de la façon suivante :
si $\gamma = \sum\limits_{i=m}^{n} k_i \theta^i$ où $k_n \neq 0$, alors $\gamma > 0$ ssi $k_n > 0$.
Soit σ_v l'automorphisme de Γ défini par : $\forall n \in \mathbb{Z}, \sigma_v(n) = n$ et $\forall i \in \mathbb{Z}, \sigma(\theta^i) = \theta^{i+1}$.
Pour tout entier positif n, pour tout $\gamma \in \Gamma$ strictement positif, $\sigma_v(\gamma)) > n\gamma$.

Soient k un corps et K le corps de Hahn $k((t^\Gamma))$. Munissons K de l'automorphisme σ qui à $\sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma$ associe $\sum\limits_{\gamma \in \Gamma} a_\gamma t^{\sigma_v(\gamma)}$. Vérifions que cet automorphisme est contractant : soit $f = \sum\limits_{\gamma \in \Gamma} a_\gamma t^\gamma \in K$, et soit $\gamma_0 = \min\limits_{\gamma, a_\gamma \neq 0}(\gamma) = v(f)$. Soit n un entier positif. Alors

$$v(\sigma(\sum_{\gamma \in \Gamma} a_\gamma t^\gamma)) = v(\sum_{\gamma \in \Gamma} a_\gamma t^{\sigma_v(\gamma)}) = \min_{\gamma, a_\gamma \neq 0} \sigma_v(\gamma) = \sigma_v(\gamma_0) = \sigma_v(v(\sum_{\gamma \in \Gamma} a_\gamma t^\gamma)) > nv(\sum_{\gamma \in \Gamma} a_\gamma t^\gamma)$$

K est donc un corps de différence valué, dont l'automorphisme distingué est contractant.

On appelle **σ-polynôme** sur un corps de différence valué K un polynôme sur K en les variables $X, \sigma(X), \sigma^2(X), ...$ Dans un corps de différence valué la notion d'algébricité n'est plus pertinente et doit être remplacée par celle de σ-algébricité, c'est à dire le fait d'être racine d'un σ-polynôme. On appelle **ordre** d'un σ-polynôme G, le plus petit entier n tel que G soit un polynôme en les variables $X, \ldots, \sigma^n(X)$, et **complexité** de G, le triplet (n, d, t) où d est le degré de G en $\sigma^n(X)$ et t son degré total. La complexité de deux σ-polynômes est comparée en utilisant l'ordre lexicographique. Soient L une extension de K et $x \in L$ σ-algébrique sur K, le **σ-polynôme minimal** de x est un polynôme de complexité minimale parmi les σ-polynômes sur K qui admettent x comme racine.

4.2 Question de l'unicité de l'extension immédiate maximale

Dans le cas des corps de différence valués munis d'un automorphisme contractant et de caractéristique résiduelle 0, Salih Azgin a retrouvé un analogue de la proposition 3.2.3 :

4.2.1. Proposition.
a. Un corps de différence valué K est maximal ssi pour toute suite pseudo-convergente de K a une limite dans K.
b. Un corps de différence valué K est σ-algébrique maximal ssi tout suite pseudo-convergente qui

qui a une limite σ-algébrique sur K a une limite dans K.
c. Soient M et N deux extensions immédiates de K, $x \in M$ et $y \in N$ deux limites d'une même suite (x_n) de K. Supposons qu'ils sont soit tous deux σ-transcendants sur K, soit de même σ-polynôme minimal et limites canoniques de (x_n). Alors $K(x)$ est K-isomorphe (en tant que corps de différence valué) à $K(y)$.

Un corps de différence valué est donc maximal ssi il est maximal en tant que corps valué. Comme pour les corps valués, la question de l'unicité à K-isomorphisme près de l'extension maximale d'un corps de différence valué K peut être reformulée ainsi :
Soient M et N deux extensions immédiates σ-algébriques maximales de K et $x \in N$ de σ-polynôme minimal G sur K et limite canonique d'une suite $(x_n)_n$ de K. Existe-t-il $y \in M$ de σ-polynôme minimal G sur K et limite canonique de $(x_n)_n$? (**)

Kaplansky répond positivement à la question (*) (correspondante de (**) pour les corps valués) en caractéristique résiduelle 0 en procédant ainsi : Soit $x \in N$ de polynôme minimal P et limite canonique de $(x_n)_n$. Par maximalité de M, (x_n) a une limite $y \in M$. Il s'agit de trouver un tel point qui est racine de P. Kaplansky montre plusieurs lemmes qui mis bout à bout donnent :
Pour $k >> 0 : v(P(x_k)) = v(P'(x_k)) + \gamma_k < v(P_i(x_k)) + i\gamma_k < v(P_j(x_k)) + j\gamma_k$ pour tout $1 < i < j$, et il existe $\gamma > 0$, tel que $v(P(y)) = v(P(x)) + \gamma_k + \gamma < v(P_i(x)) + i\gamma_k + i\gamma < v(P_j(x_k)) + j\gamma_k + j\gamma$ pour tout $1 < i < j$.
Kaplansky montre alors en utilisant simplement ces inégalités qu'il existe $b \in M$ et les propriétés de M que $P(b) = 0$ et $v(y - b) = v(P(a)) - \beta_1 > \gamma_k$. (Cette dernière condition implique en particulier que b est limite de $(x_n)_n$ et permet de répondre positivement à (*)). En fait, bien que cela ne soit pas mis en évidence dans [1], Kaplansky démontre :
Propriété B : Soient M un corps valué, P un polynôme sur M et $a \in M$. On dit que (P, a) est B-Hensélien, si $P_1(a) \neq 0$, et s'il existe $\gamma \in \Gamma$ tel que et $v(P(a)) = v(P_1(a)) + \gamma < v(P_i(a)) + i\gamma < v(P_j(a)) + j\gamma$ pour tout $1 < i < j$ avec P_i non identiquement nul. On note alors $\gamma(P, a) := \gamma$.
i. Si $a \in L - K$ est un point limite de K algébrique sur K et de polynôme minimal P, $(x_k)_k$ une suite canonique de a alors (P, a) et, pour $k >> 0$, (P, x_k) sont B-Henséliens avec $\gamma(P, a) > v(a - x_k)$ et $\gamma(P, x_k) = v(a - x_k)$.
ii. De plus, si M est algébrique maximale, alors pour tout (P, a) B-Hensélien, il existe $b \in M$ tel que $P(b) = 0$ et $v(a - b) = \gamma(P, a)$. (La réciproque est vraie aussi.)
La démonstration de Kaplansky peut se généraliser pour montrer un analogue de B dans les corps de différence valués qui satisfont le schéma d'axiomes suivants noté (A) [6] :
Soit (K, v, σ) un corps de différence valué de corps résiduel k. Toute équation linéaire sur k de la forme

$$1 + a_0 x + ... + a_n \bar{\sigma}^n(x) = 0$$

où $a_0, ..., a_n$ sont des éléments de k non tous nuls, a une solution dans k.
Cet analogue a lui aussi pour conséquence directe l'unicité de l'extension immédiate maximale. Pour les corps de différence valués de caractéristique résiduelle 0, munis d'un automorphisme contractant et qui satisfont (A), on pourrait démontrer directement sans mettre en avant un quelconque concept d'Hensélienneté l'unicité de l'extension σ-algébrique maximale et le principe AKE pour ceux de ces corps de différence valués qui sont σ-algébriques maximaux.

6. Certains corps de différence valués de caractéristique résiduelle 0 et muni d'un automorphisme contractant mais dans lesquels (A) n'est pas satisfait admettent des extensions immédiates maximales non isomorphes.

Dans son article Azgin généralise les preuve exposées dans [1] mais au contraire de Kaplansky qui ne mentionne pas explicitement la propriété B, il met en avant le point ii de la propriété correspondante pour les corps de différence valués et dégage ainsi un concept de "σ-Hensélienneté". Il démontre ensuite qu'un corps de différence valué de caractéristique 0, muni d'un automorphisme contractant, σ-algébrique maximal, et qui satisfait (A) est "σ-Hensélien" [7], puis en démontrant l'analogue (pour les corps de différence valués) du point i, il déduit l'unicité de l'extension immédiate maximale.

4.3 σ-Hensélienneté

On définit l'analogue pour les σ-polynôme des i-ème dérivées formelles. Soient $G(X)$ est un σ-polynôme d'ordre n et $a \in K$. On peut écrire le développement de Taylor de G en a : $G(a+Y) = G(a) + \sum_{(i_0,\ldots,i_n)\in\mathbb{N}^{n+1}} G_{(i_0,\ldots,i_n)}(a)(Y^{i_0}\sigma(Y)^{i_1}...\sigma^n(Y)^{i_n})$ où les $G_{(i_0,\ldots,i_n)}$ sont des σ-polynômes.

4.3.1. Définition. Soient (K, v, σ) un corps de différence valué et $a \in K$.
Soit G un σ-polynôme à coefficients dans K, non constant, et d'ordre n. Nous dirons que (G, a) est en **σ-Hensel configuration** s'il existe $\gamma \in \Gamma$ et $(i_0, \ldots, i_n) \in \mathbb{N}^{n+1}$ dont le seul indice non nul est égal à 1 (on dit que $(i_0, \ldots, i_n)$ est de norme 1).
i) $v(G(a)) = v(G_{(i_0,\ldots,i_n)}(a)) + \sum_{k=0}^n i_k\sigma^k(\gamma)$
ii) Pour tout $(j_0, \ldots, j_n) \in \mathbb{N}^{n+1}$ de norme 1,

$$v(G(a)) = v(G_{(i_0,\ldots,i_n)}(a)) + \sum_{k=0}^{n} i_k\sigma^k(\gamma) \leq v(G_{(j_0,\ldots,j_n)}(a)) + \sum_{k=0}^{n} j_k\sigma^k(\gamma).$$

iii) Pour tous $(j_0, \ldots, j_n), (l_0, \ldots, l_n) \in \mathbb{N}^{n+1}$ non nuls, tels que $G_{(j_0,\ldots,j_n)}$ est non identiquement nul,

$$v(G(a)) < v(G_{(j_0,\ldots,j_n)}(a)) + \sum_{k=0}^{n} j_k\sigma^k(\gamma) < v(G_{(j_0+l_0,\ldots,j_n+l_n)}(a)) + \sum_{k=0}^{n}(j_k + l_k)\sigma^k(\gamma).$$

On note $\gamma(G, a)$ le γ de la définition.

4.3.2. Définition. Un corps de différence valué K est **σ-Hensélien** si pour tout (G, a) en σ-Hensélien, il existe $b \in K$ tel que $G(b) = 0$ et $v(b - a) = \gamma(G, a)$.
On peut montrer qu'un corps de différence valué de caractéristique 0, muni d'un automorphisme contractant et qui satisfait (A) est σ-Hensélien ssi il est σ-algébrique maximal.

4.4 Principe AKE et élimination des quantificateurs de corps

L'unicité de l'extension σ-algébrique maximale et la propriété de σ-Hensélienneté permettent alors de retrouver un analogue du théorème 3.3.1 et ainsi obtenir un principe AKE et une élimination des quantificateurs de corps.

On augmente le langage d'un symbole de fonction s à une aritée qui va de l'univers de la sorte groupe vers celle de la sorte corps résiduel, ce symbole correspondant à une section croisée.

7. La réciproque est également vraie

4.4.1. Théorème. Principe AKE et élimination des quantificateurs de corps. Soit T la $\mathcal{L}(\sigma, s)$-théorie des corps de différence de caractéristique 0, munis d'un automorphisme distingué contractant σ-Henséliens, et munis d'une section croisée. Soient (K, Γ, k) et (K', Γ', k') deux modèles de T. Alors :
1(Principe AKE). $K \equiv K'$ ssi $k \equiv k'$ et $\Gamma \equiv \Gamma'$.
2 (Élimination des quantificateurs de corps). Pour toute $\mathcal{L}(\sigma, s)$-formule $\phi(\mathbf{x})$, il existe une $\mathcal{L}(\sigma, s)$-formule $\psi(\mathbf{x})$ ayant toutes ses occurrences de variables de corps libres, et telle que

$$T - \phi(\mathbf{x}) \longleftrightarrow \psi(\mathbf{x}).$$

(Le point 2 est lui aussi une conséquence de l'existence d'un système de va et vient entre les corps de différence valués considérés.)

4.5 Exemples de paire en σ-Hensel configuration et de corps de différence valués σ-Henséliens

Donnons un exemple simple de paire en σ-Hensel configuration. Soit $G(X)$ un σ-polynôme linéaire (c'est à dire une combinaison linéaire sur K des variables $X, \sigma(X), \sigma^2(X), ...$) non constant. Soit $a \in K$ tel que $v(G(a)) \geq 0$. On peut facilement montrer que pour tout σ-polynôme G et tout $a \in K$, tel qu'il existe $(i_0, \ldots, i_n)$ de norme 1 avec $G_{\mathbf{i}}(a) \neq 0$, il existe un unique $\gamma \in \Gamma$ tel que i) et ii) soient satisfaites. Puisque G est linéaire ce sont les seules conditions à vérifier : (G, a) est en σ-Hensel configuration.
Cet exemple montre qu'un corps de différence valué σ-Hensélien satisfait (A) : toute équation de différence linéaire sur le corps résiduel k, $1 + a_0 x + ... + a_n \bar{\sigma}^n(x) = 0$, où les $a_0, \ldots, a_n \in k$ sont non tous nuls, peut être relevée en une équation linéaire sur K dont tous les coefficients sont de valuation nulle. Le σ-polynôme associé est alors en σ-Hensel configuration avec 0. Ce qui par σ-Henséliennité permet d'en trouver une racine dont l'image résiduelle est racine de l'équation initiale sur k.

Krull a montré que pour tout corps k et tout groupe ordonné Γ, le corps de Hahn $(k((\Gamma)), v)$ est maximal. Ainsi le corps de différence valué de l'exemple 4.1.3 est maximal et si on choisit k algébriquement clos, il satisfait (A) et est donc σ-Hensélien.

Donnons un autre exemple. Soit K_q un corps de caractéristique p, algébriquement clos, muni de l'endomorphisme $\sigma_q : x \mapsto x^q$ où q est une puissance de p. Soit U un ultrafiltre non-principal sur l'ensemble des puissance de p, et soit K^* l'ultraproduit correspondant des K_q. On peut montrer que K^* est également un corps σ-Hensélien.

4.6 Lien entre σ-Henséliennité et Henséliennité

Puisqu'un corps σ-Hensélien est σ-algébrique maximal, il est en particulier algébrique maximal et donc Hensélien. La réciproque n'est pas vraie puisque tout corps de différence valué qui est Hensélien en tant que corps valué ne satisfait pas forcément (A).

4.7 Autre définition d'Henséliennité dans les corps de différence valués.

Hrushovski a proposé une autre définition de l'Henséliennité pour les corps de différence valués muni d'un endomorphisme contractant. Il retrouve un principe AKE : il montre que tous les corps

de différence valué de caractéristique 0, Hensélien (au sens de Hrushovski) et dont le corps résiduel est un modèle de la théorie ACFA ont la même théorie élémentaire. De plus cette théorie admet l'élimination des quantificateurs du corps.
Il serait intéressant de voir si elles sont équivalentes ou si l'une implique l'autre.

Références

[1] I. Kaplansky. Maximal fields with valuations. *Duke Math. J.*, 9 :303–321, 1942.

[2] S. Kochen. The model theory of local fields. In *Logic Conference Kiel 1974 (Proceedings)*, volume 499 of *Lecture Notes in Mathematics*. Springer-Verlag.

[3] F.-V. Kuhlmann and A Prestel. On places of algebraic function fields. *J. reine angew. Math.*, 353 :182–195, 1984.