École normale supérieure de Rennes

Rapport de stage de deuxième année

Théorie des modèles et intégration motivique

Téofil Adamski

Encadrant : George Comte

Laboratoire de Mathématiques (LAMA) de l'Université Savoie Mont Blanc

Le Bourget-du-Lac, mai-juin 2021

Résumé

Dans ce mémoire, je vais comprendre la construction d'une intégrale motivique dans les corps valués tels que $\mathbf{C}(\!(t)\!)$ ou $\mathbf{Q}_p$. Cette construction se base sur l'article [9] que je suivrais linéairement. Pour commencer, je développerai les bases de la théorie des modèles qui permettront ensuite de se placer dans un cadre modéré utile à la construction ; je donnerai les théorèmes principaux de cette théorie et notamment le théorème de Gödel. Dans un second temps, je construirai pas à pas l'intégrale motivique de Cluckers et Loeser, permettant d'intégrer des objets géométriques dans les corps valués. Je donnerai également quelques démonstrations omises dans l'article et admettrai les derniers lemmes.

Remerciements

Je souhaite remercier avant tout Georges Comte qui a sû aiguiser ma curiosité pour ce domaine passionnant des mathématiques et qui m'a accompagné tout au long de ma compréhension du sujet. Je remercie également Raf Cluckers de m'avoir éclairé sur une partie de son article.

Sommaire

Notations principales

– Les ensembles des réels, des rationnels, des entiers relatifs et des entiers naturels sont respectivement notés $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{Z}$ et $\mathbf{N}$.
– Les lettres gothiques ($\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{M}$, ...) sont réservées aux structures.
– Les notations $k[t]$, $k[\![t]\!]$ et $k(\!(t)\!)$ désigneront respectivement les anneaux des polynômes, des séries formelles et des séries de Laurent à coefficients dans un corps k.
– Pour un corps valué discret K, sa valuation sera toujours notée $\mathrm{ord}\colon K \longrightarrow \mathbf{Z} \cup \{\infty\}$ et sa composante angulaire $\overline{\mathrm{ac}}\colon K^\times \longrightarrow k_K$ où l'ensemble $k_K \coloneqq \mathscr{O}_K/\mathfrak{m}_K$ est son corps résiduel.

Bibliographie

[1] Yvette Amice. *Les nombres p-adiques*. Presse universitaire de France, 1975.

[2] Serge Cantat. « Nombres p-adiques ». École normale supérieure de Rennes, 2020. url : https://perso.univ-rennes1.fr/serge.cantat/Documents/Cours_ENS_2020.pdf.

[3] Zoé Chatzidakis. « Introductory notes on the model theory of valued fields ». *Motivic integration and its interactions with model theory and non-Archimedean geometry*. T. I. 383. Cambridge University Press, 2011, p. 35-79.

[4] Zoé Chatzidakis. *Notes on motivic integration*. 2015. url : http://www.math.ens.fr/~chatzidakis/papiers/Lyon-11.pdf.

[5] Raf Cluckers. « Presburger sets and p-minimal fields ». *Journal of Symbolic Logic* 68.1 (2003), p. 153-162.

[6] Raf Cluckers et Leonard Lipshitz. « Fields with analytic structure ». *Journal of the European Mathematical Society* 13.4 (2011), p. 1147-1223.

[7] Raf Cluckers et François Loeser. « Constructible motivic functions and motivic integration ». *Inventiones mathematicae* 173 (2008), p. 23-121.

[8] Raf Cluckers et François Loeser. « Fonctions constructibles et intégration motivique I ». *Comptes rendus de l'Académie des Sciences* 339 (2004), p. 411-416.

[9] Raf Cluckers et François Loeser. « Motivic integration in all residue field characteristics for Henselian discretely valued fields of characteristic zero ». *Journal für die reine und angewandte Mathematik* 701 (2015), p. 1-31.

[10] George Comte. « Géométrie algébrique ». Université Savoie Mont Blanc, 2016. url : http://gcomte.perso.math.cnrs.fr/M2/CoursM2RGeometrieAlgebrique.pdf.

[11] Danilov. *Hensel ring - Encyclopedia of Mathematics*. url : https://encyclopediaofmath.org/wiki/Hensel_ring.

[12] David Marker. *Model Theory: An Introduction*. Graduate texts in mathematics. 217. Springer-Verlag New York, 2002.

[13] Lou van den Dries. *Tame Topology and O-minimal Structures*. London Mathematical Society. 248. Cambridge University Press, 1998.

Chapitre 1

Introduction à la théorie des modèles

Avant de travailler sur l'intégration motivique, nous avons besoin de développer les rudiments de la *théorie des modèles*. Considérée comme une discipline à part entière dans les années 1950, elle tente de formaliser la notion de satisfaisabilité de formules et de prouvabilité dans des ensembles munis d'un langage. Nous verrons quelques résultats importants de cette théorie comme le théorème de complétude de Gödel. Enfin, dans l'annexe A, nous donnerons un exemple de théorie éliminant les quantificateurs, celle des corps réels clos.

Ce chapitre s'appuiera principalement sur le cours [10, Chapitre 3] et quelques rajouts ont été rapportés du livre [12].

1.1. Structure et langage

Dans un premier temps, introduisons la notion de langage. Ces derniers permettent de définir les symboles que l'on pourra utiliser dans nos formules.

Définition 1.1. Un *langage* est un triplet constitué

– d'une famille $(c_h)_{h\in H}$ de symboles c_h, appelés les *constantes* ;

– d'une famille $(f_i, n_i)_{i\in I}$ de symboles f_i, appelés les *opérations*, associés à des entiers $n_i \in \mathbf{N}^*$; pour tout indice $i \in I$, l'entier n_i est appelé l'*arité* de l'opération f_i ;

– d'une famille $(R_j, m_j)_{j\in J}$ de symboles R_j, appelés les *relations*, associés à des entiers $m_j \in \mathbf{N}^*$; pour tout indice $j \in J$, l'entier m_j est appelé l'*arité* de la relation R_j.

Bien souvent, les arités seront sous-entendues car la notation des symboles en elle-même nous suffira à déterminer leurs arités. De plus, afin de ne pas alourdir les notations, un langage

$$\mathscr{L} \coloneqq ((c_h)_{h\in H}, (f_i, n_i)_{i\in I}, (R_j, m_j)_{j\in J})$$

sera tout simplement noté sous la forme de l'ensemble

$$\mathscr{L} = \{c_h\}_{h\in H} \cup \{f_i\}_{i\in I} \cup \{R_j\}_{j\in J}.$$

Exemples. Le langage des groupes est constitué de trois symboles :

– une constante e, représentant l'élément neutre ;

– une opération binaire $\cdot$, représentant la loi de groupe ;

– une opération unaire $^{-1}$, représentant le passage à l'inverse.

Avec nos conventions d'écriture, ce langage s'écrit $\mathscr{L}_{\text{groupes}} \coloneqq \{e, \cdot, ^{-1}\}$. De même, en associant aux symboles leurs arités et natures bien connues, le langage des anneaux ordonnées est

$$\mathscr{L}_{\text{ord}} \coloneqq \{0, 1, +, \times, -, <\}.$$

Donnons un dernier exemple. Soit k un corps. Le langage des k-espaces vectoriels est

$$\mathscr{L}_{k\text{-ev}} \coloneqq \{0, +\} \cup \{\lambda\}_{\lambda\in k}$$

où chaque symbole λ est une opération unaire, représentant la multiplication par le scalaire $\lambda \in k$.

Remarque. Les symboles logiques comme $\wedge$, $\longrightarrow$ ou $\exists$ ne sont pas inclus dans les langages. Dans tous les cas, ils seront ajoutés aux symboles pouvant apparaître dans les formules lorsque ces dernières seront définies.

À présent, on peut interpréter les différents symboles d'un langage $\mathscr{L}$ dans un ensemble quelconque A en terme d'éléments, de lois ou de relations sur cet ensemble. Rappelons qu'une loi d'arité $n \in \mathbf{N}^*$ sur A est une application de A^n dans A et qu'une relation d'arité n sur A est une partie de A^n.

Notations. Soit R une relation n-aire sur A avec $n \in \mathbf{N}^*$. Pour un n-uplet $(a_1, \dots, a_n) \in A^n$, on note $R(a_1, \dots, a_n)$ lorsque ce n-uplet appartient à $R \subset A^n$. Si $n = 2$, pour un couple $(a, b) \in A^2$, on notera simplement $a\ R\ b$ pour signifier $R(a, b)$, c'est-à-dire $(a, b) \in R$. Ce dernier point s'appliquera également pour une loi binaire.

Définition 1.2. Soit $\mathscr{L} \coloneqq ((c_h)_{h\in H}, (f_i, n_i)_{i\in I}, (R_j, m_j)_{j\in J})$ un langage. Une *$\mathscr{L}$-structure* est un quadruplet $\mathfrak{A}$ constitué

- d'un ensemble A, appelé l'*univers* ou le *domaine* de la structure et noté $\mathrm{Dom}(\mathfrak{A})$;
- d'une famille $(c_h^{\mathfrak{A}})_{h\in H}$ d'éléments de A ;
- d'une famille $(f_i^{\mathfrak{A}})_{i\in I}$ dont chaque élément $f_i^{\mathfrak{A}}$ est une opération n_i-aires sur A ;
- d'une famille $(R_j^{\mathfrak{A}})_{j\in J}$ dont chaque élément $R_j^{\mathfrak{A}}$ est une relation m_j-aires sur A.

Si $\mathfrak{A}$ est une $\mathscr{L}$-structure, on dit que les objets $c_h^{\mathfrak{A}}$, $f_i^{\mathfrak{A}}$ et $R_j^{\mathfrak{A}}$ sont respectivement les *interprétations* des symboles c_h, f_i et R_j dans A.

Dans la plupart des cas, les ensembles H, I et J seront au plus dénombrables. Lorsqu'ils s'écriront respectivement $[\![1, p]\!]$, $[\![1, q]\!]$ et $[\![1, r]\!]$ avec $p, q, r \in \mathbf{N}$, cette structure $\mathfrak{A}$ sera notée

$$(A, c_1^{\mathfrak{A}}, \dots, c_p^{\mathfrak{A}}, f_1^{\mathfrak{A}}, \dots, f_q^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \dots, R_r^{\mathfrak{A}}).$$

On adaptera les notations si un ou deux des trois ensembles est infini, etc.

Exemples. – Le septuplet $(\mathbf{R}, 0, 1, +, \times, -, <)$ est une $\mathscr{L}_{\mathrm{ord}}$-structure où les symboles apparaissant sont les constantes, les opérations et les relations usuelles sur $\mathbf{R}$.
– Le quadruplet $(\mathbf{Z}, 0, +, -)$ est une $\mathscr{L}_{\mathrm{groupes}}$-structures où la constante $0 \in \mathbf{Z}$ a été associée au symbole e, l'opération $+$ au symbole $\cdot$ et l'opération $-$ au symbole $^{-1}$.
– Bien que $(\mathbf{Z}, \times)$ ne soit pas un groupe, le triplet $(\mathbf{Z}, 1, \times, ^{-1})$ est une $\mathscr{L}_{\mathrm{groupes}}$-structure.

Maintenant, on peut donner un sens à la notion de formule sur un langage $\mathscr{L}$. C'est ici qu'on va implémenter le symbole $=$ et les symboles logiques. On supposera que ces derniers symboles et les symboles comme (ou , ne sont pas dans les langages.

Dans les formules, on utilisera des variables. Ces dernières peuvent être n'importe quels symboles non utilisés. Notons X un ensemble, dit l'ensemble des variables. La plupart du temps, les variables seront notées x_0, x_1, … ou encore x, y, z, …

Définition 1.3. Soit $\mathscr{L}$ un langage.

- Un *$\mathscr{L}$-terme* est une suite finie de symboles engendrée par les règles suivantes :
  - les variables et les constantes sont des $\mathscr{L}$-termes ;
  - si f est une opération n-aire et t_1, …, t_n sont des $\mathscr{L}$-termes, alors $f(t_1, \dots, t_n)$ est un $\mathscr{L}$-terme.
- Un *$\mathscr{L}$-formule atomique* est une suite finie de symboles de la forme
  - soit $t = s$ pour des $\mathscr{L}$-termes t et s ;
  - soit $R(t_1, \dots, t_m)$ pour une relation m-aires R et des $\mathscr{L}$-termes t_1, …, t_m.

Dans les deux cas, on pourra écrire ces $\mathscr{L}$-formules atomiques sous la forme

$$t(x_1, \dots, x_\ell) = s(x_1, \dots, x_\ell) \quad \text{et} \quad R_j(t_1(x_1, \dots, x_\ell), \dots, t_m(x_1, \dots, x_\ell))$$

§1. On pourrait définir cette notation plus rigoureusement en utilisant les mêmes règles qui définissent les $\mathscr{L}$-termes, mais on voit très bien ce qu'il se passe.

pour signifier qu'elles font intervenir au moins les variables x_1, …, x_ℓ [§1].

– Une *$\mathscr{L}$-formule* est une suite finie de symboles engendrée par les règles suivantes :
  - une $\mathscr{L}$-formule atomique est une $\mathscr{L}$-formule ;
  - si ϕ et ψ sont deux $\mathscr{L}$-formules, alors $\neg\phi$, $\phi \wedge \psi$ et $\phi \vee \psi$ sont trois $\mathscr{L}$-formules ;
  - si ϕ est une $\mathscr{L}$-formule et x est une variable, alors $\exists x\ \phi$ et $\forall x\ \phi$ sont des $\mathscr{L}$-formules.

Les formules construites sans la dernière règle sont dites *sans quantificateur*. On écrira $\phi(x_1, \dots, x_\ell)$ pour indiquer que les variables x_1, …, x_ℓ apparaissant dans une $\mathscr{L}$-formule ϕ ne sont pas assujetties à des quantificateurs $\forall$ ou $\exists$, qualifiées de *libres*.

– Les formules dans lesquelles toutes les variables sont sujets à des quantificateurs sont les *$\mathscr{L}$-phrases*.

Exemple. Pour le langage des groupes $\mathscr{L}_{\text{groupes}}$, avec $X = \{x, y, z, a, b\}$, des formules sont

$$(x \cdot y = z) \wedge (y = e) \qquad \text{ou} \qquad \forall a\ \exists b\ (a \cdot b = e).$$

En revanche, l'expression $(x \vee y) = e$ n'est pas une formule. Dans la suite, on ne précisera jamais l'ensemble des variables X.

Remarque. On pourra utiliser les parenthèses ou les crochets pour délimiter nos formules. On introduit également les symboles d'implication et d'équivalence à partir des symboles déjà définis. En effet, pour deux $\mathscr{L}$-formules ϕ et ψ, on notera

$$(\phi \longrightarrow \psi) \coloneqq (\neg\phi \vee \psi) \qquad \text{et} \qquad (\phi \longleftrightarrow \psi) \coloneqq ([\phi \longrightarrow \psi] \wedge [\psi \longrightarrow \phi])$$

qui sont des $\mathscr{L}$-formules.

1.2. Interprétation des formules

Fixons un langage $\mathscr{L}$ et une $\mathscr{L}$-structure $\mathfrak{A}$ d'univers A. On souhaite interpréter les $\mathscr{L}$-formules dans la structure $\mathfrak{A}$. Dans un premier temps, étendons le langage $\mathscr{L}$ en ajoutant un symbole a, vu comme une constantes, pour tout élément $a \in A$. On obtient un nouveau langage $\mathscr{L}_A$ dont $\mathfrak{A}$ est une structure. Remarquons qu'un $\mathscr{L}_A$-terme t peut alors être vu comme un élément $t^{\mathfrak{A}} \in A$.

Notation. Étant donnés une $\mathscr{L}_A$-formule $\phi(x_1, \dots, x_\ell)$ et des éléments $a_1, \dots, a_\ell \in A$, on définit la $\mathscr{L}_A$-phrase $\phi(a_1, \dots, a_\ell)$, parfois notée $\phi(x_1/a_1, \dots, x_\ell/a_\ell)$, comme la $\mathscr{L}$-formule $\phi(x_1, \dots, x_\ell)$ où toutes les variables libres x_i sont respectivement remplacées par les constantes $a_i \in A$. Souvent, le ℓ-uplet $(x_1, \dots, x_\ell)$ sera noté $\overline{x}$.

1.2.1. L'interprétation

Définition 1.4. On définit la notation $\mathfrak{A} \models \sigma$, qui se lit « $\mathfrak{A}$ satisfait σ », pour une $\mathscr{L}_A$-phrase σ par les règles suivantes :

– si t et s sont des $\mathscr{L}_A$-termes, alors $\mathfrak{A} \models t = s$ si $t^{\mathfrak{A}} = s^{\mathfrak{A}}$;
– si R est une relation m-aire et $t_1, \dots, t_m$ des $\mathscr{L}_A$-termes, alors $\mathfrak{A} \models R(t_1, \dots, t_m)$ si $R^{\mathfrak{A}}(t_1^{\mathfrak{A}}, \dots, t_m^{\mathfrak{A}})$;
– si ϕ est un $\mathscr{L}_A$-phrase, alors $\mathfrak{A} \models \neg\phi$ si on n'a pas $\mathfrak{A} \models \phi$;
– si ϕ et ψ sont deux $\mathscr{L}_A$-phrases, alors
  - $\mathfrak{A} \models \phi \wedge \psi$ si $\mathfrak{A} \models \phi$ et $\mathfrak{A} \models \psi$;
  - $\mathfrak{A} \models \phi \vee \psi$ si $\mathfrak{A} \models \phi$ ou $\mathfrak{A} \models \psi$;
– si $\phi(\overline{x})$ est une $\mathscr{L}_A$-formule avec ℓ variables libres, alors
  - $\mathfrak{A} \models \forall\overline{x}\ \phi(\overline{x})$ si $\mathfrak{A} \models \phi(\overline{a})$ pour tout ℓ-uplet $\overline{a} \in A^\ell$;
  - $\mathfrak{A} \models \exists\overline{x}\ \phi(\overline{x})$ si $\mathfrak{A} \models \phi(\overline{a})$ pour un ℓ-uplet $\overline{a} \in A^\ell$.

Exemple. On considère de langage des anneaux $\mathscr{L}_{\text{anneaux}} \coloneqq \{0, 1, +, \times, -\}$. On munit les ensembles $\mathbf{Z}$ et $\mathbf{R}$ de leurs $\mathscr{L}_{\text{anneaux}}$-structures naturelles, respectivement notées $\mathfrak{Z}$ et $\mathfrak{R}$. L'expression

$$\forall x\ \big(x = 0 \vee [\exists y\ (x \times y = 1)]\big)$$

est une phrase qui est satisfaite dans $\mathfrak{R}$ et non satisfaite dans $\mathfrak{Z}$.

Définition 1.5. Un ensemble de $\mathscr{L}$-phrases Σ *prouve* une $\mathscr{L}$-phrase ϕ si cette dernière est une conséquence des phrases de Σ, *i. e.* on peut construire une suite finie de $\mathscr{L}$-formules qui sont soit dans Σ, soit déduites de la formule précédente de la suite par les règles logiques usuelles et qui permettent de déduire ϕ. On notera $\Sigma \vdash \phi$.

On dira que la phrase ϕ est une *conséquence syntaxique* de Σ ou que l'on peut *formellement prouver* la phrase ϕ dans Σ. Dans ce cas, la phrase ϕ sera satisfaite dans toute $\mathscr{L}$-structure $\mathfrak{A}$ dans laquelle toutes les phrases $\sigma \in \Sigma$ sont vraies (il suffit d'utiliser les règles d'inférences qui prouvent ϕ formellement à partir de T et les règles d'inférences qui prouvent l'interprétation de ϕ dans A).

Exemple. On considère l'ensemble Σ_{groupes} des $\mathscr{L}_{\text{groupes}}$-phrases suivantes :
- $\forall x \ (x \cdot e = x) \wedge (e \cdot x = x)$
- $\forall x \ \exists y \ (x \cdot y = e)$;
- $\forall x \ \forall y \ \forall z \ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$

qui axiomatisent la théorie des groupes. Alors il est facile de voir que

$$\Sigma_{\text{groupes}} \vdash \Big[\forall y \ (\forall x \ (x \cdot y = x) \wedge (y \cdot x = x)) \longrightarrow y = e\Big].$$

Définition 1.6. – Une *$\mathscr{L}$-théorie* est un ensemble de $\mathscr{L}$-phrases.
– Un *modèle* d'une $\mathscr{L}$-théorie Σ est une $\mathscr{L}$-structure $\mathfrak{A}$ dans laquelle toutes les phrases de Σ sont vraies, c'est-à-dire

$$\mathfrak{A} \models \sigma \qquad \text{pour toute } \mathscr{L}\text{-phrase } \sigma \in \Sigma.$$

Soit Σ une théorie. On dira qu'une $\mathscr{L}$-phrase ϕ est une *conséquence sémantique* de Σ si elle est satisfaite dans tout modèle de Σ. D'après ce qui précède, une conséquence syntaxique de Σ est une conséquence sémantique de Σ. En fait, le théorème de complétude de Gödel assurera la réciproque.

Définition 1.7. Soit $\mathscr{C}$ une classe de $\mathscr{L}$-structures. La *théorie engendrée* par la classe $\mathscr{C}$ est l'ensemble des $\mathscr{L}$-phrases vraies dans toutes les $\mathscr{L}$-structures de $\mathscr{C}$, noté $\mathrm{Th}(\mathscr{C})$. Dans le cas où la classe $\mathscr{C}$ est réduite à une $\mathscr{L}$-structure $\mathfrak{A}$, cet ensemble sera simplement noté $\mathrm{Th}(\mathfrak{A})$.

Donnons quelques définitions supplémentaires permettant de qualifier une théorie.

Définition 1.8. Une $\mathscr{L}$-théorie T est
- *non contradictoire* ou *cohérente* si elle admet un modèle ;
- *complète* si, pour toute $\mathscr{L}$-phrase ϕ, soit ϕ est vraie dans tous les modèles de T, soit $\neg\phi$ est vraie dans tous les modèles de T ;
- *axiomatisée* par une $\mathscr{L}$-théorie Σ si, pour toute $\mathscr{L}$-phrase $\phi \in T$, on a $\Sigma \vdash \phi$; on dira que T est une conséquence de Σ ;
- *consistante* si elle ne permet pas de prouver une $\mathscr{L}$-phrase et sa négation.

De plus, une $\mathscr{L}$-phrase ϕ est *indécidable* dans T si cette dernière ne prouve ni ϕ ni $\neg\phi$.

Exemple. On reprend la théorie Σ_{groupes} de l'exemple précédent. Elle est cohérente puisqu'un modèle est $(\mathbf{R}, 0, +, -)$. En revanche, elle n'est pas complète puisque la phrase

$$\forall x \ \forall y \ (x \cdot y = y \cdot x)$$

est vraie dans $(\mathbf{R}, 0, +, -)$ et fausse dans $(\mathrm{M}_n(\mathbf{R}), I_n, \times, ^{-1})$: il existe des groupes non abéliens.

Proposition 1.9. Soit $\mathfrak{A}$ une $\mathscr{L}$-structure. Alors la théorie $\mathrm{Th}(\mathfrak{A})$ est complète.

Preuve Soit ϕ une $\mathscr{L}$-phrase. Alors dans la $\mathscr{L}$-structure $\mathfrak{A}$, elle est soit vraie soit fausse, donc la phrase ϕ ou sa négation $\neg\phi$ appartient à $\mathrm{Th}(\mathfrak{A})$. Supposons être dans le premier cas. Soit $\mathfrak{M}$ un modèle de $\mathrm{Th}(\mathfrak{A})$. Par définition d'un modèle, on a $\mathfrak{M} \models \phi$. Par conséquent, la phrase ϕ est vraie dans tous les modèles de $\mathrm{Th}(\mathfrak{A})$. On procède identiquement dans le second cas. Finalement, la théorie $\mathrm{Th}(\mathfrak{A})$ est complète. $\square$

Proposition 1.10. Un $\mathscr{L}$-théorie cohérente est consistante.

Preuve Soit T une $\mathscr{L}$-théorie cohérente. Raisonnons par l'absurde et supposons qu'elle n'est pas consistante. Alors il existe une $\mathscr{L}$-phrase ϕ telle que $T \vdash \phi$ et $T \vdash \neg\phi$. Puisque la théorie est cohérente, elle admet un modèle $\mathfrak{A}$. Alors $\mathfrak{A} \models \phi$ et $\mathfrak{A} \models \neg\phi$. Une $\mathscr{L}$-phrase étant soit vraie soit fausse dans $\mathfrak{A}$, on obtient une contradiction. Donc la théorie T est consistante. □

1.2.2. Le théorème de complétude de Gödel et ses conséquences

Dans le paragraphe précédent, on a vu qu'une conséquence syntaxique est une conséquence sémantique pour une $\mathscr{L}$-théorie T. Le théorème suivant, qu'on admet, nous donne la réciproque.

Théorème 1.11 *(de complétude de Gödel).* Soient Σ une $\mathscr{L}$-théorie et ϕ une $\mathscr{L}$-phrase. Alors les deux points suivants sont équivalents :

- la théorie Σ prouve la phrase ϕ ;
- le phrase ϕ est vraie dans tout modèle de Σ, on notera $\Sigma \models \phi$.

Autrement dit, pour une $\mathscr{L}$-théorie Σ, une $\mathscr{L}$-phrase en est une conséquence syntaxique si et seulement si elle en est un conséquence sémantique.

De ce théorème, on peut en déduire un corollaire qui va faire le lien entre les différents adjectifs utilisés pour qualifier une théorie.

Corollaire 1.12.
- Les notions de cohérence et de consistance sont équivalentes.
- Une $\mathscr{L}$-théorie admettant une $\mathscr{L}$-phrase indécidable est incomplète.

Définissons une notion de cardinal sur les langages.

Définition 1.13. Le *cardinal* d'un langage $\mathscr{L}$ est le plus petit cardinal infini supérieure ou égal au cardinal de l'ensemble de ses symboles S, c'est-à-dire le cardinal

$$\sharp\mathscr{L} := \max(\sharp S, \aleph_0).$$

Le cardinal d'une $\mathscr{L}$-structure est celui de son univers.

La preuve du théorème de complétude de Gödel montre, au passage, le corollaire suivant.

Corollaire 1.14.
- Toute $\mathscr{L}$-théorie consistante admet un modèle de cardinal inférieur ou égal à celui de l'union $\mathscr{L} \cup \mathbf{N}$.
- Toute $\mathscr{L}$-théorie consistante s'étend en une théorie complète sur un langage ayant les mêmes symboles que $\mathscr{L}$ et des constantes supplémentaires.

Montrons à présent le théorème de compacité qui s'appuie sur le théorème de complétude de Gödel. Il va se révéler très utile dans la suite (cf. les preuves des résultats 1.24 ou 2.27)

Théorème 1.15 *(de compacité).* Soit T une $\mathscr{L}$-théorie. Si tout sous-ensemble fini de T admet un modèle, alors T admet un modèle.

Preuve Raisonnons par contraposée et supposons que la $\mathscr{L}$-théorie T n'admet pas de modèle. Considérons la $\mathscr{L}$-phrase $\phi_0 := [\exists x\ (x \neq x)]$. Comme T n'admet pas de modèle, le théorème de complétude de Gödel assure $T \vdash \phi_0$. Or une preuve formelle de ϕ_0 dans $\mathscr{L}$ à partir de T repose sur un nombre fini de $\mathscr{L}$-phrases de T. Notons T' l'ensemble de ces $\mathscr{L}$-phrases. Alors $T' \vdash \phi_0$ et l'ensemble fini $T' \subset T$ ne peut admettre de modèle car la $\mathscr{L}$-phrase ϕ_0 est clairement fausse dans toute $\mathscr{L}$-structure et *a fortiori* dans tout modèle de T. Finalement, il existe un sous-ensemble fini de T n'admettant pas de modèle. On a montré la contraposée. □

Corollaire 1.16 *(théorème de compacité avec paramètres).* Soient T une $\mathscr{L}$-théorie et Σ un ensemble de $\mathscr{L}$-formules de variables libres x_1, …, x_n. Soit $\Phi(x_1, \dots, x_n)$ une $\mathscr{L}$-formule. On suppose qu'il n'existe pas de modèle $\mathfrak{M}$ de T et de n-uplet $(a_1, \dots, a_n) \in (\operatorname{Dom} \mathfrak{M})^n$ tel que

$$\begin{aligned} &\mathfrak{M} \models \Phi(a_1, \dots, a_n), \\ &\mathfrak{M} \models \sigma(a_1, \dots, a_n) \qquad \text{pour toute } \mathscr{L}\text{-formule } \sigma \in \Sigma. \end{aligned}$$

Alors il existe un entier $\ell \in \mathbf{N}^*$ et des $\mathscr{L}$-formules $\sigma_1, \dots, \sigma_\ell \in \Sigma$ tels que

$$T \vdash \Big(\forall x_1 \cdots \forall x_n \quad \bigwedge_{i=1}^{\ell} \sigma_i(x_1, \dots, x_n) \quad \Longrightarrow \quad \neg\Phi(x_1, \dots, x_n) \Big).$$

Preuve Soit $\Sigma' \coloneqq \{\sigma_1, \dots, \sigma_\ell\} \subset \Sigma$ un sous-ensemble fini. On note $\sigma_{\Sigma'}$ la $\mathscr{L}$-formule

$$\forall x_1 \cdots \forall x_n \quad \bigwedge_{i=1}^{\ell} \sigma_i(x_1, \dots, x_n) \quad \Longrightarrow \quad \neg\Phi(x_1, \dots, x_n).$$

Raisonnons par l'absurde et supposons que notre conclusion n'est pas vérifiée. Dans ce cas, on n'a pas $T \vdash \sigma_{\Sigma'}$. Soit $T' \subset T$ un sous-ensemble fini. On n'a pas $T' \vdash \sigma_{\Sigma'}$ de telle sorte que la $\mathscr{L}$-théorie

$$T' \cup \{\forall \overline{x}\ \phi(\overline{x}) \mid \phi(\overline{x}) \in \Sigma' \cup \{\Phi\}\}$$

ne permet pas de montrer $\forall \overline{x}\ \neg\Phi(\overline{x})$. Cette dernière est donc consistante [§2]. Par le corollaire 1.14, elle admet un modèle. Ainsi tout sous-ensemble fini de la $\mathscr{L}$-théorie

$$T \cup \{\forall \overline{x}\ \phi(\overline{x}) \mid \phi(\overline{x}) \in \Sigma \cup \{\Phi\}\}$$

admet un modèle. Le théorème de compacité assure que cette dernière admet un modèle ce qui contredit notre hypothèse. □

Théorème 1.17 *(Löwenheim-Skolem).* Soit T une $\mathscr{L}$-théorie admettant un modèle infini. Alors pour tout cardinal $\kappa \geqslant \sharp\mathscr{L}$, il existe un modèle de T de cardinal κ.

Preuve Soit $\mathfrak{M}$ un modèle infini de T. Soient κ un cardinal infini tel que $\kappa \geqslant \sharp\mathscr{L}$ et E un ensemble disjoint du l'ensemble $\mathscr{L}$ de cardinal κ. On adjoint les éléments $i \in E$, vu comme des constantes e_i, au langage $\mathscr{L}$. Notons $\mathscr{L}'$ le langage obtenu. Considérons la $\mathscr{L}'$-théorie

$$T' \coloneqq T \cup \{e_i \neq e_j \mid i, j \in E, i \neq j\}.$$

Alors elle admet un modèle. En effet, par le théorème de compacité, il suffit de montrer que tout sous-ensemble fini de T' admet un modèle. Soit donc $T'' \subset T'$ un sous-ensemble fini. Alors ses phrases ne font intervenir qu'un nombre fini de constantes e_i et, comme $\mathfrak{M}$ est infini, on peut les interpréter comme des constantes dans la $\mathscr{L}$-structure $\mathfrak{M}$, quitte à les confondre avec des constantes déjà existantes de $\mathfrak{M}$. Cela nous donne une $\mathscr{L}'$-structure $\mathfrak{M}'$ vérifiant $T' \models \mathfrak{M}'$.

Comme la consistance et la cohérence sont équivalentes, la $\mathscr{L}'$-théorie T' est donc consistante. Le corollaire 1.14 assure alors l'existence d'un modèle $\mathfrak{M}'$ de T' tel que $\sharp\mathfrak{M}' \leqslant \sharp\mathscr{L}' + \aleph_0$. Puisque les formules $e_i \neq e_j$ avec $i \neq j$ sont vraies dans $\mathfrak{M}'$, on obtient $\sharp\mathfrak{M}' \geqslant \kappa$. Par hypothèse, on a $\kappa \geqslant \sharp\mathscr{L}$ et le cardinal κ est infini, donc

$$\sharp\mathscr{L}' = \sharp\mathscr{L} + \kappa \leqslant \kappa \leqslant \sharp\mathfrak{M}' \leqslant \sharp\mathscr{L}' + \aleph_0 = \sharp\mathscr{L}'$$ [§3]

ce qui implique $\sharp\mathfrak{M}' = \kappa$. Comme $\mathfrak{M}$ est un modèle de $T' \supset T$, c'est un modèle de T. □

1.2.3. Élimination des quantificateurs

Définition 1.18. Une $\mathscr{L}$-théorie T *élimine les quantificateurs* si, pour toute $\mathscr{L}$-formule $\psi(\overline{x})$, il existe une $\mathscr{L}$-formule $\phi(\overline{x})$ sans quantificateur telle que

$$T \models \forall \overline{x}\ (\psi(\overline{x}) \longleftrightarrow \phi(\overline{x})).$$

§2. Un $\mathscr{L}$-théorie non consistante permet de prouver toutes les $\mathscr{L}$-phrases. En effet, soit T une $\mathscr{L}$-théorie non consistante. Alors il existe une $\mathscr{L}$-phrase ϕ telle que $T \vdash \phi$ et $T \vdash \neg\phi$. Pour toute $\mathscr{L}$-phrase ψ, comme

$$\phi \longrightarrow (\neg\phi \longrightarrow \psi) \equiv \neg\phi \vee (\neg\phi \longrightarrow \psi) \equiv \neg\phi \vee (\phi \vee \psi) \equiv \psi$$

on obtient $T \vdash \psi$.

§3. Pour deux cardinaux infinis λ et μ, on a $\lambda + \mu = \max(\lambda, \mu)$. Dans la première inégalité, on utilisé $\kappa + \kappa = \kappa$.

Dans ce cas, on dit que les $\mathscr{L}$-formules ϕ et ψ sont *équivalentes modulo* T.

Exemple. Donnons simplement une formule équivalente à une autre formule sans quantificateur dans un modèle. On considère le langage des corps ordonnés $\mathscr{L}_{\text{corps}} := \{0, 1, +, -, \times, {}^{-1}, <\}$. On munit la droite réelle $\mathbf{R}$ de sa $\mathscr{L}_{\text{corps}}$-structure $\mathfrak{R}$. Dans cette structure, la phrase

$$\exists x \; ax^2 + bx + c = 0$$

est équivalente à la phrase sans quantificateur

$$(a \neq 0 \wedge b^2 - 4ac > 0) \vee (a = 0 \wedge [b \neq 0 \vee c = 0]).$$

Définition 1.19. Soient $\mathfrak{A}$ et $\mathfrak{B}$ deux $\mathscr{L}$-structures. On dit que

– l'une est une *sous-structure* de l'autre si $\operatorname{Dom}(\mathfrak{A}) \subset \operatorname{Dom}(\mathfrak{B})$ et l'interprétation des symboles du langage $\mathscr{L}$ dans $\mathfrak{A}$ est la restriction de celle dans $\mathfrak{B}$. On note $\mathfrak{A} \subset \mathfrak{B}$;

– l'une est une sous-structure *élémentaire* de l'autre si $\mathfrak{A} \subset \mathfrak{B}$ et, pour toute $\mathscr{L}$-formule $\phi(\overline{x})$ et tout n-uplet $\overline{a} \in (\operatorname{Dom} \mathfrak{A})^n$, on a $\mathfrak{A} \models \phi(\overline{a})$ si et seulement si $\mathfrak{B} \models \phi(\overline{a})$. On note $\mathfrak{A} \prec \mathfrak{B}$;

– elles sont *élémentairement équivalentes* si elles satisfont les mêmes $\mathscr{L}$-phrases. On note $\mathfrak{A} \sim \mathfrak{B}$.

Remarque. Une $\mathscr{L}$-théorie est complète si et seulement si tous ses modèles sont élémentairement équivalents. Une sous-structure élémentaire de $\mathfrak{A}$ est élémentairement équivalente à $\mathfrak{A}$.

Exemple. Le $\mathscr{L}_{\text{ord}}$-structure $\mathbf{Z}$ est une sous-structure de $\mathbf{R}$. Mais, elles ne sont pas élémentairement équivalentes puisque la phrase $\exists x \; x^2 = 2$ est vraie dans $\mathbf{R}$ et fausse dans $\mathbf{Z}$.

Définition 1.20. Une $\mathscr{L}$-théorie T est *modèle-complète* si elle admet un modèle et, pour tous modèles $\mathfrak{A}$ et $\mathfrak{B}$ de T vérifiant $\mathfrak{A} \subset \mathfrak{B}$, on a $\mathfrak{A} \prec \mathfrak{B}$.

Remarque. Une $\mathscr{L}$-théorie complète T éliminant les quantificateurs est modèle-complète. Montrons cela. Soient $\mathfrak{A}$ et $\mathfrak{B}$ deux modèles de T vérifiant $\mathfrak{A} \subset \mathfrak{B}$. Soient $\phi(x_1, \dots, x_n)$ une $\mathscr{L}$-formule et $\overline{a} \in (\operatorname{Dom} \mathfrak{A})^n$. Soit $\varphi(x_1, \dots, x_n)$ une $\mathscr{L}$-formule sans quantificateur équivalente à $\phi(x_1, \dots, x_n)$. Si $\mathfrak{B} \models \phi(\overline{a})$, alors $\mathfrak{B} \models \varphi(\overline{a})$ et, comme $\varphi(x_1, \dots, x_n)$ n'a pas de quantificateur et $\mathfrak{A}$ est une sous-structure de $\mathfrak{B}$, on a $\mathfrak{A} \models \varphi(\overline{a})$, donc $\mathfrak{A} \models \phi(\overline{a})$. Réciproquement, si $\mathfrak{A} \models \phi(\overline{a})$, alors $\mathfrak{B} \models \phi(\overline{a})$ clairement. D'où le résultat.

Cependant, la réciproque de cette remarque est fausse. En effet, on peut montrer que le théorie de la $\mathscr{L}_{\text{anneaux}}$-structure $\mathbf{R}$ est modèle-complète et n'élimine pas les quantificateurs.

Définition 1.21. Soit $\mathfrak{A}$ une $\mathscr{L}$-structure d'univers A. Une partie $X \subset A^\ell$ est $\mathfrak{A}$-*définissable* s'il existe une $\mathscr{L}$-formule $\phi(x_1, \dots, x_\ell, y_{\ell+1}, \dots, y_{\ell+k})$ et un élément $\overline{b} \in A^k$ tels que

$$X = \{\overline{a} \in A^\ell \mid \mathfrak{A} \models \phi(\overline{a}, \overline{b})\}.$$

Lorsque la $\mathscr{L}$-formule est sans quantificateur, on dit que la partie X est $\mathfrak{A}$-*constructible*.

Exemple. On munit l'ensemble $\mathbf{R}$ de sa structure de corps ordonné. Alors l'ensemble

$$\{(a, b, c) \in \mathbf{R}^3 \mid \exists x \in \mathbf{R},\ ax^2 + bx + c = 0\}$$

est $\mathbf{R}$-définissable et même $\mathbf{R}$-constructible.

Définition 1.22. Dans le langage des corps ordonnés, les ensembles $\mathbf{R}$-constructibles sont appelés les *ensembles semi-algébriques*. Il s'agit simplement des sous-ensembles des espaces $\mathbf{R}^n$ dont les éléments sont solutions d'un système d'équations et d'inéquations polynomiales strictes.

Remarque. Une théorie élimine les quantificateurs si et seulement si, pour tout modèle $\mathfrak{A}$, tout ensemble $\mathfrak{A}$-définissable est $\mathfrak{A}$-constructible.

1.3. Complément : l'o-minimalité

Définition 1.23. Une structure ordonnée $\mathfrak{A} \coloneqq (A, <, \dots)$ est *o-minimale* ou *minimale pour l'ordre* si, pour toute ensemble $\mathfrak{A}$-définissable $X \subset A$, il existe un sous-ensemble fini $X_0 \subset X$ et des intervalles $I_1, \dots, I_n$ d'extrémités dans $A \cup \{\pm\infty\}$ tels que

$$X = X_0 \cup I_1 \cup \cdots \cup I_n.$$

Exemple. La théorie des corps réels clos est o-minimale. En effet, si R est un corps réel clos, tout ensemble R-définissable de R est une union finie d'intersections finies d'ensembles de la forme

$$\{x \in R \mid P(x) = 0\} \quad \text{ou} \quad \{x \in R \mid Q(x) > 0\} \quad \text{avec} \quad P, Q \in R[X].$$

Le premier est un ensemble fini ou $R = \left]-\infty, +\infty\right[$ tout entier. Le second est une union d'intervalles.

Donnons un résultat qui utilise la puissance du théorème de compacité. Ce lemme, dit de finitude uniforme, sert principalement dans la géométrie o-minimale. On peut retrouver un preuve dans le livre [13] qui n'utilise pas la théorie des modèles.

Proposition 1.24 *(finitude uniforme).* Soient $\mathscr{L}$ un langage et $\mathfrak{A}$ une $\mathscr{L}$-structure. Soit $X \subset A^{m+1}$ un ensemble $\mathfrak{A}$-définissable. On suppose que, pour tout $s \in A^m$, l'ensemble

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

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

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

Preuve Comme X est $\mathfrak{A}$-définissable, il existe une $\mathscr{L}$-formule $\phi(x_1, \dots, x_{m+1}, y_1, \dots, y_k)$ et un élément $y^{\mathfrak{A}} \coloneqq (y_1^{\mathfrak{A}}, \dots, y_k^{\mathfrak{A}}) \in A^k$ tels que $X = \{x \in A^{m+1} \mid \mathfrak{A} \models \phi(x, y^{\mathfrak{A}})\}$.

Raisonnons par l'absurde et supposons que, pour tout $n \in \mathbf{N}$, il existe $s \in A^m$ tel que $\sharp X_s > n$. Ajoutons au langage $\mathscr{L}$ des symboles de constantes $s_1, \dots, s_m, y_1, \dots, y_k$. Notons

$$\tilde{\mathscr{L}} \coloneqq \mathscr{L} \cup \{s_1, \dots, s_m, y_1, \dots, y_k\}$$

le langage obtenu, $s \coloneqq (s_1, \dots, s_m)$ et $y \coloneqq (y_1, \dots, y_k)$. Pour $n \in \mathbf{N}$, on considère la $\tilde{\mathscr{L}}$-phrase

$$\phi_n \coloneqq [\sharp X_s > n] = \Big[\exists a_1 \cdots \exists a_{n+1} \ \Big(\bigwedge_{i<j} (a_i \neq a_j) \wedge \bigwedge_{i=1}^{n+1} \phi(s, a_i, y)\Big)\Big].$$

Montrons que la $\tilde{\mathscr{L}}$-théorie

$$\Gamma \coloneqq \operatorname{Th}(\mathfrak{A}) \cup \{\phi_n\}_{n \in \mathbf{N}}$$

est consistante. Soient $I \subset \mathbf{N}$ et $T \subset \operatorname{Th}(\mathfrak{A})$ deux parties finies. Montrons que la $\tilde{\mathscr{L}}$-théorie

$$\Gamma' \coloneqq T \cup \{\phi_n\}_{n \in I}$$

est consistante. Grâce à notre hypothèse absurde, il existe un m-uplet $s^{\mathfrak{A}} \coloneqq (s_1^{\mathfrak{A}}, \dots, s_m^{\mathfrak{A}}) \in A^m$ tel que $\sharp X_{s^{\mathfrak{A}}} > \max I$. Ainsi, on munit la $\mathscr{L}$-structure $\mathfrak{A}$ d'une structure sur le langage $\tilde{\mathscr{L}}$ en interprétant les symboles s_i par les éléments $s_i^{\mathfrak{A}} \in A$ et les symboles y_i par les éléments $y_i^{\mathfrak{A}} \in A$. Notons $\tilde{\mathfrak{A}}$ la $\tilde{\mathscr{L}}$-structure obtenue. Elle est construite de telle sorte que

$$\tilde{\mathfrak{A}} \models T \quad \text{et} \quad \tilde{\mathfrak{A}} \models \phi_n, \quad n \in I.$$

Finalement, la $\tilde{\mathscr{L}}$-structure $\tilde{\mathfrak{A}}$ est un modèle de la théorie Γ'. Ainsi toute partie finie de Γ est consistante. Par le théorème de compacité, la théorie Γ est consistante. Soit $\mathfrak{M}$ un modèle de Γ.

Dans cette structure, les symbole $s_i \in \tilde{\mathscr{L}}$ s'interprètent comme des constantes $s_i^{\mathfrak{M}} \in \operatorname{Dom} \mathfrak{M}$. De même, les symboles y_j s'interprètent comme des constantes $y_j^{\mathfrak{M}} \in \operatorname{Dom} \mathfrak{M}$. Comme $\mathfrak{M} \models \operatorname{Th}(\mathfrak{A})$, la structure $\mathfrak{M}$ satisfait la finitude de la fibre $Y_{s^{\mathfrak{M}}}$ avec

$$Y \coloneqq \{x \in (\operatorname{Dom} \mathfrak{M})^{m+1} \mid \mathfrak{M} \models \phi(x, y_1^{\mathfrak{M}}, \dots, y_k^{\mathfrak{M}})\}.$$

Comme pour les phrases ϕ_n, cette finitude peut se traduire sous la forme d'une $\tilde{\mathscr{L}}$-phrases. Dans le même temps, les phrases ϕ_n y sont toutes vraies ce qui est contradictoire. $\square$

Remarque. En adaptant la preuve, on montre facilement que la borne est même uniforme par rapport à la structure $\mathfrak{A}$.

Chapitre 2

Intégration motivique

Grâce à ce premier chapitre, nous sommes maintenant en mesure de définir l'intégrale motivique au sens de l'article [9]. En fait, ce dernier est un raffinement d'un article antérieur [7], résumé dans l'article [8], que nous utiliserons également.

2.1. Corps valués

Dans toute cette section, on considère un corps K et on va définir la notion de valuation. Pour des exemples intuitifs de corps valué, on pourra penser aux corps $\mathbf{C}((t))$ ou $\mathbf{Q}_p$ qui sont munis d'une valuation naturelle. On s'est servi des références [2], [1] et [3].

2.1.1. Définitions et quelques propriétés

Définition 2.1. Soit Γ un groupe abélien totalement ordonné, c'est-à-dire muni d'une relation d'ordre total $\leqslant$ telle que

$$w \geqslant 0 \quad \Longrightarrow \quad uw \leqslant vw, \qquad u, v, w \in \Gamma.$$

Une *valuation* sur le corps K est une application surjective $\operatorname{ord}\colon K \longrightarrow \Gamma \cup \{\infty\}$ telle que

- pour tout élément $x \in K$, on a $\operatorname{ord} x = \infty \Leftrightarrow x = 0$;
- pour tous éléments $x, y \in K$, on a $\operatorname{ord}(xy) = \operatorname{ord} x + \operatorname{ord} y$;
- pour tous éléments $x, y \in K$, on a $\operatorname{ord}(x+y) \geqslant \min(\operatorname{ord} x, \operatorname{ord} y)$.

Lorsque $\Gamma = \mathbf{Z}$, on dit que la valuation est *discrète*.

Remarque. Avec le deuxième axiome, la valuation de l'élément neutre multiplicatif est nulle et les valuations d'un élément et de son opposé sont égales.

Proposition 2.2. Soit $\operatorname{ord}\colon K \longrightarrow \Gamma \cup \{\infty\}$ une valuation sur le corps K. Alors l'ensemble

$$\mathscr{O}_K \coloneqq \{x \in K \mid \operatorname{ord} x \geqslant 0\}$$

est un anneau, appelé l'*anneau de valuation* du corps K. De plus, l'ensemble

$$\mathfrak{m}_K \coloneqq \{x \in K \mid \operatorname{ord} x > 0\}$$

est l'unique idéal maximal de l'anneau $\mathscr{O}_K$, appelé l'*idéal de valuation* du corps K. Enfin, le corps quotient $k_K \coloneqq \mathscr{O}_K/\mathfrak{m}_K$ est le *corps résiduel* du corps K.

Preuve Grâce aux trois axiomes vérifiés par l'application ord, l'ensemble $\mathscr{O}_K$ est bien un anneau : le deuxième axiome garantit que le neutre multiplicatif appartient à cet ensemble et les deuxième et troisième axiomes assurent qu'il est stable par somme et produit.

Avec le deuxième axiome, l'ensemble $\mathfrak{m}_K$ est clairement un idéal de l'anneau $\mathscr{O}_K$. Montrons qu'il est l'unique idéal maximal. Tout d'abord, vérifions que, pour tout élément $x \in K$, soit $x \in \mathscr{O}_K$ soit $x^{-1} \in \mathscr{O}_K$. En effet, supposons que $x \notin \mathscr{O}_K$. Le deuxième axiome permet d'écrire

$$\operatorname{ord} 1 = 0 \quad \text{et} \quad \operatorname{ord} 1 = \operatorname{ord} x + \operatorname{ord} x^{-1}$$

donc $\operatorname{ord} x^{-1} = -\operatorname{ord} x > 0$, donc $x^{-1} \in A$. On peut maintenant montrer que

$$\mathfrak{m}_K = \mathscr{O}_K \setminus \mathscr{O}_K^\times$$

En effet, si $x \in \mathscr{O}_K \setminus \mathscr{O}_K^\times$, alors $x \in \mathscr{O}_K$ et $x^{-1} \notin \mathscr{O}_K$, donc $\operatorname{ord} x \geqslant 0$ et $-\operatorname{ord} x < 0$, donc $\operatorname{ord} x > 0$, donc $x \in \mathfrak{m}_K$. Réciproquement, si $x \in \mathfrak{m}_K$, alors $x \in \mathscr{O}_K$, donc $x^{-1} \notin \mathscr{O}_K$, donc $x \in \mathscr{O}_K \setminus \mathscr{O}_K^\times$. Cela nous montre l'égalité et conclut la preuve. □

Exemple *(un corps valué utile).* Soit k un corps. On munit l'ensemble $k^{\mathbf{N}}$ de sa structure d'anneau naturelle : on obtient l'anneau des séries formelles $k[\![t]\!]$. Son corps des fractions qu'on note $K := k(\!(t)\!)$ est le *corps des séries de Laurent* et un élément $f \in K$ s'écrit sous la forme

$$f = \sum_{n=N}^{+\infty} a_n t^n \quad \text{avec} \quad N \in \mathbf{Z},\ a_n \in k,\ a_N \neq 0\ ;$$

l'entier N est noté $\operatorname{ord} f$ [§1]. Le corps K est ainsi muni d'une valuation discrète et son corps résiduel est isomorphe au corps k.

Définition 2.3. Soit K un corps valué. Tout élément $\pi \in K$ de valuation une est *uniformisant.*

Notation. Pour un corps valué K, on choisit un élément uniformisant $\pi_K \in \mathfrak{m}_K$. Par exemple, pour le corps $k(\!(t)\!)$, l'élément t est uniformisant.

Définition 2.4. Soit $n \geqslant 1$ un entier. La *composante angulaire d'ordre n* est l'application

$$\overline{\mathrm{ac}}_n : \left| \begin{array}{rcl} K^\times & \longrightarrow & \mathscr{O}_K/\mathfrak{m}_K^n, \\ x & \longmapsto & [\pi_K^{-\operatorname{ord} x} x]. \end{array} \right.$$

On note $\overline{\mathrm{ac}} := \overline{\mathrm{ac}}_1$. Cette application coïncide avec la projection $\mathscr{O}_K \longrightarrow \mathscr{O}_K/\mathfrak{m}_K^n$.

Exemple. En choisissant $\pi_{k(\!(t)\!)} := t$, la composante angulaire $\overline{\mathrm{ac}} \colon k(\!(t)\!)^\times \longrightarrow k$ s'écrit

$$\overline{\mathrm{ac}}\, f = a_N \quad \text{avec} \quad f := \sum_{n=N}^{+\infty} a_n t^n \in k(\!(t)\!),\ a_N \neq 0.$$

Proposition 2.5 *(topologie sur un corps valué).* Soit K un corps de valué discret.

1. Quelque soit le réel $q \in]0,1[$, l'application $d \colon (x,y) \in K^2 \longmapsto q^{\operatorname{ord}(x-y)} \in \mathbf{R}_+$ est une distance ultramétrique sur K, c'est-à-dire vérifiant

$$d(x,y) \leqslant \max(d(x,z), d(z,y)), \qquad x, y, z \in K.$$

Elle induit une topologie appelée la *topologie de valuation.*

2. Une boule ouverte de K est un ensemble de la forme

$$\mathrm{B}_K(a,z) := \{x \in K \mid \operatorname{ord}(x-a) > z\}$$

avec $a \in K$ et $z \in \Gamma$. Les boules ouvertes sont ouvertes et fermées pour la topologie de valuation.

Preuve Le premier point est assez évident grâce à la remarque p. 9. Le second découle du fait que la distance est ultramétrique : une boule $\mathrm{B}_K(a,z)$ est fermée puisque, pour tout $b \in K \setminus \mathrm{B}_K(a,z)$, on a $\mathrm{B}_K(b,z) \cap \mathrm{B}_K(a,z) = \emptyset$. □

Remarque. Soient $z \in \Gamma$, $a \in K$, $n \geqslant 1$ et $\xi \in \mathscr{O}_K/\mathfrak{m}_K^n$. Alors l'ensemble

$$B := \{t \in K \mid \overline{\mathrm{ac}}_n(x-a) = \xi,\ \operatorname{ord}(x-a) = z\}$$

§1. Par convention, on pose $\operatorname{ord} 0 = \infty$.

est une boule. En effet, on prend un élément $u \in K$ tel que $\overline{\mathrm{ac}}_n\, u = \xi$ et on trouve

$$B = \mathrm{B}_K(a + u\pi_K^z, z + n - 1)$$

Dans la suite, quand on parlera d'une topologie sur le corps K, on prendra cette base d'ouverts. On introduit maintenant la notion d'anneau hensélien (voir le site [11]).

Définition 2.6. Un anneau local A d'idéal maximal $\mathfrak{m}$ est *hensélien* si, pour tout polynôme unitaire $P \in A[X]$ et tout élément $a_0 \in A$ tels que $P(a_0) \equiv 0 \mod \mathfrak{m}$ et $P'(a_0) \not\equiv 0 \mod \mathfrak{m}$, il existe un élément $a \in A$ tel que $P(a) = 0$ et $a \equiv a_0 \mod \mathfrak{m}$.

Définition 2.7. Soit p un nombre premier ou nul. Un $(0,p)$*-corps* est un corps valué discret K de caractéristique 0 dont l'anneau de valuation $\mathscr{O}_K$ est hensélien et le corps résiduel k_K est de caractéristique p.

Exemple. Le corps des nombres p-adiques $\mathbf{Q}_p$ est un $(0,p)$-corps pour la valuation p-adique ord_p. En effet, son corps résiduel est le corps $\mathbf{F}_p$ qui est de caractéristique p. Tout élément $x \in \mathbf{Q}_p^\times$ s'écrit de manière unique sous la forme

$$x = \sum_{n=N}^{+\infty} a_n p^n \quad \text{avec} \quad a_n \in [\![0, p-1]\!], a_N \neq 0.$$

Pour un tel élément $x \in \mathbf{Q}_p^\times$, on a $\mathrm{ord}_p\, x = N$ et $\overline{\mathrm{ac}}\, x = a_N$. On peut également montrer que le corps $\mathbf{Q}_p$ est bien hensélien.

Notation. On note $T_{(0,p)}$ la $\mathscr{L}_{\mathrm{DP}}$-théorie des $(0,p)$-corps.

2.1.2. Le langage de Denef-Pas

On étend le langage des corps $\mathscr{L}_{\mathrm{corps}}$ en ajoutant les symboles $+$, $-$, 0, ∞, $<$ et ord associés respectivement aux bonnes opérations et constantes sur Γ, formant le langage $\mathscr{L}_{\mathrm{val}}$. Une $\mathscr{L}_{\mathrm{val}}$-structure est la donnée d'un corps K, d'un groupe abélien ordonné Γ et d'une valuation ord. Lorsqu'on aura $\Gamma = \mathbf{Z}$, on ajoutera à ce langage les symboles $\equiv_n$ de congruence modulo n pour tout entier $n \geqslant 1$, formant ainsi le *langage de Presburger*.

De même, on peut re-étendre ce langage avec les symboles $+$, $-$, $\times$, 0, 1 et $\overline{\mathrm{ac}}$ associés respectivement aux opérations et constantes sur k, pour former le langage $\mathscr{L}_{\mathrm{DP}}$, dit de Denef-Pas. Par exemple, le triplet $(k(\!(t)\!), k, \mathbf{Z} \cup \{\infty\})$ associé aux bonnes constantes et opérations est une structure[§2] sur le langage $\mathscr{L}_{\mathrm{DP}}$ et c'est un modèle de la théorie des corps valués et résiduels. On remplacera $\mathbf{Z} \cup \{\infty\}$ par $\mathbf{Z}$ quitte à remplacer une condition $\mathrm{ord}\, x = \infty$ par $x = 0$.

Exemple. Soit $\mathfrak{K} \coloneqq (K, k, \mathbf{Z})$ une $\mathscr{L}_{\mathrm{DP}}$-struture. Tout ensemble $\mathfrak{K}$-définissable est de la forme

$$\phi(\mathfrak{K}) \coloneqq \{(\overline{x}, \overline{u}, \overline{z}) \in K^n \times k^m \times \mathbf{Z}^r \mid \phi(\overline{x}, \overline{u}, \overline{z})\}$$

pour une $\mathscr{L}_{\mathrm{DP}}$-formule $\phi(\overline{x}, \overline{u}, \overline{z})$. Par exemple, l'ensemble

$$\{(x, y, u, z) \in K^2 \times k \times \mathbf{Z} \mid x^2 = y,\ \mathrm{ord}(xy) = z,\ \overline{\mathrm{ac}}\, x = u,\ z \equiv_2 0\}$$

est définissable et même constructible.

2.2. Modérations géométriques sur les théories des corps valués

Soit p un nombre premier ou nul. Dans toute cette section, on considère un $(0,p)$-corps K dont le groupe des valeurs est Γ.

§2. On dit que le langage $\mathscr{L}_{\mathrm{DP}}$ possède trois *sortes* : celle pour le corps valué, celle pour le corps résiduel et celle pour le groupe des valeurs. Les deux dernières sont qualifiés d'*auxiliaires*. Remarquons qu'une structure (K, k, Γ) sur les trois sortes peut bien être vue comme une $\mathscr{L}_{\mathrm{DP}}$-structure définie dans le chapitre 1 : on peut prendre, par exemple, la $\mathscr{L}_{\mathrm{DP}}$-structure $K \cup k \cup \Gamma$ et lui associer correctement les symboles de constantes, de relations et d'opérations.

VOCABULAIRE. Soit $\mathfrak{A}$ une structure sur un langage $\mathscr{L}$. Pour un sous-ensemble $B \subset \operatorname{Dom} \mathfrak{A}$, le terme « B-définissable » qualifiera les objets qui sont $\mathfrak{A}$-définissable dans le langage $\mathscr{L}$ auquel on a ajouté comme constantes les éléments de l'ensemble B, c'est-à-dire dans le langage $\mathscr{L}_B$. En particulier, l'ancienne $\mathfrak{A}$-définissabilité est la nouvelle $\emptyset$-définissabilité. Par abus, on pourra également écrire $\mathfrak{B}$-définissable pour une sous-structure $\mathfrak{B} \subset \mathfrak{A}$.

DÉFINITION 2.8. Soient $B, B' \subset K$ deux parties quelconques. Une fonction $F\colon B \longrightarrow B'$ est *jacobienne* si elle satisfait les points suivants :

(i) la fonction F est une bijection et les ensembles B et B' sont des boules de K ;

(ii) la fonction F est de classe $\mathscr{C}^1$ sur B de dérivée F' ;

(iii) la fonction F' ne s'annule pas et la fonction $x \in B \longmapsto \operatorname{ord} F'(x)$ est constante égale à $c \in \Gamma$;

(iv) pour tous éléments $x, y \in B$ avec $x \neq y$, on a $c + \operatorname{ord}(x-y) = \operatorname{ord}(F(x) - F(y))$.

De plus, elle est *1-jacobienne* si

(v) la fonction $x \in B \longmapsto \overline{\mathrm{ac}}\, F'(x)$ est constante égale à $c' \in k_K$;

(vi) pour tous éléments $x, y \in B$, on a $c'\,\overline{\mathrm{ac}}(x-y) = \overline{\mathrm{ac}}(F(x) - F(y))$.

Une $\mathscr{L}_{\mathrm{DP}}$-théorie T sera dite jacobienne si, pour tout modèle $\mathfrak{K}$ de cette théorie de domaine (K, k, Γ), toute sous-structure $\mathfrak{A} \subset \mathfrak{K}$, tout entier $n \geqslant 1$ et toute fonction $\mathfrak{A}$-définissable $F\colon K \longrightarrow K$, il existe une fonction $\mathfrak{A}$-définissable $f\colon K \longrightarrow S$ avec $S \coloneqq k^m \times \Gamma^r$ telle que toute fibre infinie $f^{-1}(\{s\})$ soit une boule sur laquelle la fonction F est soit constante soit jacobienne.

On définit maintenant les deux notions centrales qui vont nous permettre de construire l'intégrale motivique sur les $(0,p)$-corps. En fait, il s'agit de conditions de modérations géométriques.

DÉFINITION 2.9. Une $\mathscr{L}_{\mathrm{DP}}$-théorie est *divisée* si tout modèle $\mathfrak{K}$ de domaine (K, k, Γ) vérifie les points suivants :

(i) tout ensemble $\mathfrak{K}$-définissable de Γ^r est Γ-définissable (pour le langage $\{+, -, 0, <\}$) ;

(ii) pour tout ensemble fini $A \subset \operatorname{Dom} \mathfrak{K}$, tout ensemble A-définissable $X \subset k_K^m \times \Gamma^r$ s'écrit sous la forme $X = \bigcup_{i=1}^{\ell} U_i \times Z_i$ où les ensembles $U_i \subset k_K^m$ et $Z_i \subset \Gamma^r$ sont $\mathfrak{A}$-définissables.

Autrement dit et informellement, lorsque une théorie est divisée, les ensembles définissables dans les sortes auxiliaires peuvent se décomposer en une union disjointe de rectangles dont les côtés sont respectivement dans k_K et Γ.

DÉFINITION 2.10. Une $\mathscr{L}_{\mathrm{DP}}$-théorie est *finiment b-minimale* si tout modèle $\mathfrak{K}$ de domaine (K, Γ, k) vérifie les points suivants :

(i) l'image de toute fonction $\mathfrak{K}$-définissable localement constante $g\colon K^\times \longrightarrow K$ est finie ;

(ii) pour toute sous-structure finie $\mathfrak{A} \subset \mathfrak{K}$ et tout ensemble $\mathfrak{A}$-définissable $X \subset K$, il existe

– une fonction $\mathfrak{A}$-définissable $f\colon X \longrightarrow S$ où l'ensemble $S \subset k_K^m \times \Gamma^r$ est définissable,

– une fonction $\mathfrak{A}$-définissable $c\colon S \longrightarrow K$

telles que toute fibre $f^{-1}(\{s\})$ non vide avec $s \in S$ soit

– ou bien égale au singleton $\{c(s)\}$,

– ou bien égale à la boule

$$\{x \in K \mid \overline{\mathrm{ac}}(x - c(s)) = \xi(s),\ \operatorname{ord}(x - c(s)) = z(s)\}$$

pour certains éléments $\xi(s) \in k_K$ et $z(s) \in \Gamma$.

La notion de b-minimalité pour les corps valués est l'analogue de l'o-minimalité dans les structures sur un langage : il s'agit d'une notion de modération géométrique. On énonce maintenant une conséquence importante de la b-minimalité finie. Ce lemme est essentiel dans l'article [9].

LEMME 2.11. Soit $\mathfrak{K}$ un modèle d'une $\mathscr{L}_{\mathrm{DP}}$-théorie finiment b-minimale T. Notons (K, Γ, k) son domaine. Soient S un produit cartésien de sortes auxiliaires et $h\colon S \longrightarrow K$ une fonction $\mathfrak{K}$-définissable. Alors son image $\operatorname{Im} h \subset K$ est finie. La conclusion est également vraie pour des fonctions définissables localement constantes $X \subset K^\ell \longrightarrow K$.

Preuve Si $S = \emptyset$, il n'y a rien à montrer. On suppose désormais $S \neq \emptyset$. On écrit $S \subset S_1 \times \cdots \times S_\ell$ avec $S_i \in \{\Gamma, k_K\}$. On raisonne par récurrence sur l'entier ℓ.

• *Initialisation.* On considère le cas $\ell = 1$. Montrons que l'image de la fonction h est finie. On peut distinguer deux cas.

– On suppose $S \subset \Gamma$. On considère l'application $g\colon K^\times \longrightarrow K$ définie par la relation

$$g(x) = \begin{cases} h(\operatorname{ord} x) & \text{si } \operatorname{ord} x \in S, \\ 0 & \text{sinon.} \end{cases}$$

Tout d'abord, elle est clairement $\mathfrak{K}$-définissable. De plus, elle est localement constante sur $K^\times$ puisque, pour tout point $x \in K^\times$, l'ensemble

$$V \coloneqq \{y \in K^\times \mid \operatorname{ord} y = \operatorname{ord} x\} = \mathrm{B}_K(0, \operatorname{ord} x) \setminus \mathrm{B}_K(0, \operatorname{ord} x - 1).$$

est un voisinage du point x et ce dernier vérifie $g = g(x)$ sur V. Comme la théorie est b-minimale, cette application g est d'image finie. Comme la valuation est surjective, la fonction h est également d'image finie.

– On suppose $S \subset k_K = \mathscr{O}_K/\mathfrak{m}_K$. De même, l'application $g\colon K^\times \longrightarrow K$ définie par la relation

$$g(x) = \begin{cases} h(\overline{\operatorname{ac}}\, x) & \text{si } \overline{\operatorname{ac}}\, x \in S, \\ 0 & \text{sinon} \end{cases}$$

est localement constante et définissable. Comme précédemment, cela conclut la finitude de l'image de la fonction h.

• *Hérédite.* On suppose $\ell > 1$ et que la propriété est vraie au rang $\ell - 1$. Considérons la projection $p\colon S \longrightarrow S' \coloneqq S_1 \times \cdots \times S_{\ell-1}$. Pour tout $s \in p(S)$, la fonction $h(s, \cdot)\colon S_\ell \longrightarrow K$ est définissable et notre hypothèse de récurrence nous assure donc que l'ensemble $h(p^{-1}(\{s\}))$ est finie. En procédant comme dans la preuve de la proposition 1.24, les ensembles $h(p^{-1}(\{s\}))$ avec $s \in p(S)$ sont alors uniformément finis. Quitte à considérer une partition finie de l'ensemble X, on peut supposer que les ensembles $h(p^{-1}(\{s\}))$ non vide sont tous de même cardinal $t \in \mathbf{N}^*$. Pour un élément $s \in p(S)$ tel que $h(p^{-1}(\{s\})) \neq \emptyset$, on note alors

$$h(p^{-1}(\{s\})) = \{a_{s,1}, \dots, a_{s,t}\}.$$

Considérons les polynômes symétriques élémentaires $g_0, \dots, g_{t-1} \in K[X_1, \dots, X_t]$, c'est-à-dire ceux vérifiant

$$\prod_{i=1}^{t} (T + X_i) = \sum_{k=0}^{t-1} g_k(X_1, \dots, X_t) T^{t-k} + 1.$$

Pour $j \in [\![0, t-1]\!]$, on définit alors la fonction $h_j\colon S' \longrightarrow K$ telle que

$$h_j(s) = \begin{cases} g_j(a_{s,1}, \dots, a_{s,t}) & \text{si } h(p^{-1}(\{s\})) \neq \emptyset, \\ 0 & \text{sinon.} \end{cases}$$

Par notre hypothèse de récurrence, chaque fonction h_j doit avoir une image finie. On en déduit que l'image de la fonction h est finie.

Montrons la seconde partie du lemme. Soient $X \subset K^\ell$ un ensemble $\mathfrak{K}$-définissable et $h\colon X \longrightarrow K$ une fonction définissable localement constante. On procède également par récurrence sur l'entier ℓ.

• *Initialisation.* On suppose $\ell = 1$. Avec la b-minimalité finie de la théorie, il existe un ensemble définissable $S \subset k_K^m \times \Gamma^r$ et deux fonctions $\emptyset$-définissables $f\colon X \longrightarrow S$ et $c\colon S \longrightarrow K$ tels que toute fibre $f^{-1}(\{s\})$ non vide avec $s \in S$ soit

– ou bien égale au singleton $\{c(s)\}$;

– ou bien égale à la boule

$$B_s \coloneqq \{x \in K \mid \overline{\operatorname{ac}}(x - c(s)) = \xi(s),\ \operatorname{ord}(x - c(s)) = z(s)\}$$

pour certains éléments $\xi(s) \in k_K$ et $z(s) \in \Gamma$.

D'après la première partie du lemme, l'image de la fonction c est finie. Quitte à faire une partition finie de l'ensemble X, on peut supposer que la fonction c est constante égale à un élément $c_0 \in K$ et que chaque fibre $f^{-1}(\{s\})$ non vide avec $s \in S$ est égale à la boule B_s. Quitte à translater la fonction f par l'élément c_0, on peut supposer que $c_0 = 0$.

On étend maintenant la fonction h par zéro en une fonction $\tilde{h} \colon K^\times \longrightarrow K$. D'après les hypothèses faites précédemment, cette extension est localement constante. Par la b-minimalité finie, son image est finie. On en déduit que l'image de la fonction h est finie ce qui termine l'initialisation.

• *Hérédite.* On suppose $\ell > 1$ et que la propriété est vrai au rang $\ell - 1$. Pour tout $y \in K^{\ell-1}$, en notant $X_y := \{t \in K \mid (y,t) \in X\}$ la fibre selon y, la fonction

$$h(y,\cdot) \colon \left| \begin{array}{l} X_y \longrightarrow K, \\ \quad t \longmapsto h(y,t) \end{array} \right.$$

est définissable et localement constante (puisque la projection $K^\ell \longrightarrow K$ est ouverte), donc elle possède une image finie d'après le cas $\ell = 1$. Notons $p \colon K^\ell \longrightarrow K^{\ell-1}$ la projection sur les $\ell - 1$ premières coordonnées. Par le même argument que précédemment, on peut supposer que les images des fonctions $h(y,\cdot)$ avec $y \in p(X)$ sont toutes de même cardinal $t \in \mathbf{N}$. On procède alors comme dans la première partie de la preuve et cela conclut. □

Comme on l'a dit, la b-minimalité finie et la divsion vont nous servir dans la suite. Le théorème suivant est montré dans l'article [6].

THÉORÈME 2.12. Le $\mathscr{L}_{\mathrm{DP}}$-théorie des $(0,p)$-corps est divisée, finiment b-minimale et jacobienne.

2.3. Définition de l'intégrale motivique

Soit p un nombre premier ou nul. Dans la suite, on notera Field_p l'ensemble des $(0,p)$-corps, c'est-à-dire des modèles de la théorie des $(0,p)$-corps.

2.3.1. Sous-assignations définissables et morphismes définissables

2.3.1.1. Définition

DÉFINITION 2.13. Soient $n,m,r \geqslant 0$ trois entiers. Pour un $(0,p)$-corps K, on pose

$$h[n,m,r](K) := K^n \times k_K^m \times \mathbf{Z}^r.$$

Une *sous-assignation définissable* est une famille de sous-ensembles $X(K) \subset h[n,m,r](K)$ pour des corps $K \in \mathrm{Field}_p$ tels qu'il existe une $\mathscr{L}_{\mathrm{DP}}$-formule $\phi(\overline{x},\overline{u},\overline{z})$ vérifiant

$$X(K) = \{(\overline{x},\overline{u},\overline{z}) \in h[n,m,r](K) \mid (K,k_K,\mathbf{Z}) \models \phi(\overline{x},\overline{u},\overline{z})\}, \quad \forall K \in \mathrm{Field}_p.$$

Pour deux sous-assignations définissables X et Y, on note $Y \subset X$ lorsque

$$Y(K) \subset X(K), \quad \forall K \in \mathrm{Field}_p.$$

Un *point* d'une sous-assignation définissable X est un couple (x_0, K) avec un corps $K \in \mathrm{Field}_p$ et un point $x_0 \in X(K)$. L'ensemble des points de X est noté $|X|$.

Parfois, on fera disparaître l'adjectif « définissable » pour des raisons de lisibilité.

EXEMPLE. La famille $X = (X(K))_{K \in \mathrm{Field}_p}$ définie par la relation

$$X(K) := \{x \in K \mid (K,k_K,\mathbf{Z}) \models \exists y \ x = y^2\}$$

est une sous-assignation définissable de $h[1,0,0]$. Les couples $(1,\mathbf{Q}_p)$ et $(t^2, \mathbf{C}(\!(t)\!))$ sont des points de cette dernière.

NOTATION. Pour une fonction $f \colon A \longrightarrow B$, on note $\Gamma(f) \subset A \times B$ son graphe.

DÉFINITION 2.14. Soient X et Y deux sous-assignations définissables. Un *morphisme définissable* est la donnée d'une famille de fonctions $f_K : X(K) \longrightarrow Y(K)$ pour des corps $K \in \mathrm{Field}_p$ telles que la famille $(\Gamma(f_K))_{K\in\mathrm{Field}_p}$ soit une sous-assignation définissable. On le notera $f : X \longrightarrow Y$.

Notation. Pour une sous-assignation définissable $Y \subset h[n,m,r]$ et trois entiers $n', m', r' \geqslant 0$, on définit la sous-assignation $Y[n',m',r'] \subset h[n+n', m+m', r+r']$ par les égalités

$$Y[n',m',r'](K) := \{(\overline{x},\overline{x}',\overline{u},\overline{u}',\overline{z},\overline{z}') \in K^n \times K^{n'} \times k_K^m \times k_K^{m'} \times \mathbf{Z}^r \times \mathbf{Z}^{r'} \mid (\overline{x},\overline{y},\overline{z}) \in Y(K)\}.$$

On notera également $h := h[0,0,0]$ de sorte que la notation précédente coïncide avec celle pour désigner $h[n,m,r]$.

2.3.1.2. Notion de dimension

Définition 2.15. Soient $n,m,r \geqslant 0$ trois entiers et K un $(0,p)$-corps. On définit la *dimension* d'un ensemble définissable non vide $X \subset h[n,m,r](K)$ comme ce qui suit.

- Lorsque $n = 0$, la dimension de l'ensemble X vaut zéro.
- Lorsque $n \geqslant 1$, la dimension de l'ensemble X vaut
  - s'il existe, l'entier maximal $d \in [\![1,n]\!]$ tel qu'en notant $p : h[n,m,r](K) \longrightarrow K^d$ une projection sur d coordonnées, l'image $p(X)$ contienne un produit cartésien de d boules ;
  - zéro sinon.

Le dimension d'une sous-assignation définissable $X \subset h[n,m,r]$ est le maximum des dimensions des ensembles $X(K)$ pour $K \in \mathrm{Field}_p$. On la note $\dim X$.

Lemme 2.16. Soit K un $(0,p)$-corps. Alors toute boule $\mathrm{B}_K(a,z)$ est infinie.

Preuve Soient $a \in K$ un point et $z \in \mathbf{Z}$ un entier. Une récurrence immédiate assure alors que, pour tout entier $n \in \mathbf{N}^*$, on a $\operatorname{ord} n\pi_K^{z+1} \geqslant z+1 > z$. Ceci permet de définir l'application

$$\left|\begin{aligned} \mathbf{N}^* &\longrightarrow \mathrm{B}_K(a,z), \\ n &\longmapsto a + n\pi_K^{z+1} \end{aligned}\right.$$

qui est injective puisque le corps K est de caractéristique nulle. □

Proposition 2.17 *(caractérisation des ensembles de dimension zéro).* Soient $n,m,r \geqslant 0$ trois entiers avec $n \geqslant 1$ et K un $(0,p)$-corps. Notons $p : h[n,m,r](K) \longrightarrow K^n$ la projection sur les n premières coordonnées. Alors un ensemble définissable non vide $X \subset h[n,m,r](K)$ est de dimension zéro si et seulement sa projection $p(X)$ est finie.

Preuve On suppose que l'ensemble $p(X) \subset K^n$ est fini. Montrons que l'ensemble X est de dimension zéro. Soient $d \in [\![1,n]\!]$ un entier et $p_1 : h[n,m,r](K) \longrightarrow K^d$ une projection sur d coordonnées. Lorsque $d = 1$, la b-minimalité (cf. théorème 2.12) et le lemme précédent assurent que l'image $p_1(X)$ ne contient aucune boule. En particulier, pour tout entier $d > 1$, la projection $p_1(X)$ ne contient pas de produit cartésien de d boules. Ainsi l'ensemble X est de dimension zéro.

On veut maintenant montrer la réciproque. On procède par récurrence sur l'entier n. Initialisons la récurrence. Lorsque $n = 0$, le résultat est immédiat. Traitons le cas $n = 1$. Soit $X \subset h[1,m,r](K)$ un ensemble définissable non vide de dimension zéro. Alors son image $p(X)$ ne contient aucune boule. La b-minimalité et les lemmes 2.11 et 2.16 assurent que cette image $p(X)$ est finie.

Passons à l'hérédité. Soit $n \geqslant 1$ un entier. On suppose que le résultat est vrai pour des ensembles définissables $Y \subset h[n,m,r](K)$. Soit $X \subset h[n+1,m,r](K)$ un ensemble définissable non vide de dimension zéro. Notons $p_1 : h[n+1,m,r](K) \longrightarrow h[n,m,r](K)$ la projection. Comme X est de dimension zéro, l'ensemble définissable $p_1(X) \subset h[n,m,r](K)$ est de dimension zéro, donc sa projection $X' \subset K^n$ est finie d'après l'hypothèse de récurrence. De plus, en considérant la projection de X sur la $n+1$-ième coordonnée, on obtient un sous-ensemble $X'' \subset K$ de dimension zéro également qui est donc fini d'après le cas $n = 1$. Donc l'ensemble $p(X) \subset X' \times X''$ est fini. □

2.3.2. Intégration sur le groupe des valeurs

Définition 2.18. Soit $\mathbb{L}$ un symbole formel, appelé le *symbole de Lefschetz*. On définit l'anneau

$$\mathbb{A} \coloneqq \mathbf{Z}\left[\mathbb{L}, \mathbb{L}^{-1}, \left(\frac{1}{1-\mathbb{L}^{-i}}\right)_{i\geqslant 1}\right].$$

C'est un sous-anneau des fonctions rationnelles en la variable $\mathbb{L}$. Chaque réel $q > 1$ induit un morphisme d'anneaux

$$\vartheta_q\colon \left|\begin{aligned} \mathbb{A} &\longrightarrow \mathbf{R}, \\ r(\mathbb{L}) &\longmapsto r(q). \end{aligned}\right.$$

Exemple. Prenons $q = 2$ et $r(\mathbb{L}) \coloneqq 2\mathbb{L} + 4\mathbb{L}^{-1} + 5/(1-\mathbb{L}^{-1})$. Alors $\vartheta_2(r(\mathbb{L})) = 16$.

Dans la suite de cette section, on fixe une sous-assignation définissable S.

Notation. Un morphisme définissable $\alpha\colon S \longrightarrow h[0,0,1]$ induit l'application

$$\tilde{\alpha}\colon \left|\begin{aligned} |S| &\longrightarrow \mathbf{Z} \subset \mathbb{A}, \\ (s,K) &\longmapsto \alpha_K(s). \end{aligned}\right.$$

Il induit également l'application

$$\mathbb{L}^{\tilde{\alpha}}\colon \left|\begin{aligned} |S| &\longrightarrow \mathbb{A}, \\ (s,K) &\longmapsto \mathbb{L}^{\tilde{\alpha}(s,K)}. \end{aligned}\right.$$

Définition 2.19. On définit le sous-anneau $\mathscr{P}(S)$ de l'anneau des fonctions $|S| \longrightarrow \mathbb{A}$ généré par

- les fonctions constantes $|S| \longrightarrow \mathbb{A}$;
- les fonctions $\tilde{\alpha}\colon |S| \longrightarrow \mathbb{A}$ pour des morphismes définissables $\alpha\colon S \longrightarrow h[0,0,1]$;
- les fonctions $\mathbb{L}^{\tilde{\beta}}\colon |S| \longrightarrow \mathbb{A}$ pour des morphismes définissables $\beta\colon S \longrightarrow h[0,0,1]$.

Les éléments de l'anneau $\mathscr{P}(S)$ sont appelés les *fonctions constructibles de Presburger* sur S.

Notation. Pour un élément $r(\mathbb{L}) \in \mathbb{A}$, on note $r(\mathbb{L}) \geqslant 0$ si

$$\forall q > 1, \quad \vartheta_q(r(\mathbb{L})) \geqslant 0.$$

Notons $\mathbb{A}_+$ l'ensemble des éléments positifs de $\mathbb{A}$. On définit également l'ensemble $\mathscr{P}_+(S)$ des fonctions constructibles positives de Presburger constitué des fonctions $f \in \mathscr{P}(S)$ qui sont positives en tout point de $|S|$.

Définition 2.20. Une fonction $\varphi \in \mathscr{P}(S[0,0,r])$ est *S-intégrable* si, pour tout réel $q > 1$ et tout point $(s,K) \in |S|$, la famille $(\vartheta_q(\varphi(s,i,K)))_{i\in\mathbf{Z}^r}$ est sommable. On note $\mathrm{I}_S\mathscr{P}(S[0,0,r])$ l'ensemble des fonctions S-intégrables. C'est un $\mathscr{P}(S)$-module. On définit également l'ensemble $\mathrm{I}_S\mathscr{P}_+(S[0,0,r])$.

Exemples. – Considérons la sous-assignation définissable $S \coloneqq h[1,0,0]$ et les fonctions

$$\alpha_K\colon \left|\begin{aligned} K \times \mathbf{Z} &\longrightarrow \mathbf{Z}, \\ (s,i) &\longmapsto i \operatorname{ord} s \end{aligned}\right.$$

pour tout corps $K \in \mathrm{Field}_p$. On obtient un morphisme $\alpha\colon S[0,0,1] \longrightarrow h[0,0,1]$ et ainsi une fonction de Presburger $\tilde{\alpha} \in \mathscr{P}(S[0,0,1])$. Regardons si cette dernière est S-intégrable. Soit $q > 1$ un réel. On considère le corps $\mathbf{Q}_p$ et l'élément $p \in \mathbf{Q}_p$. Pour tout entier $i \in \mathbf{Z}$, on a

$$\vartheta_2(\tilde{\alpha}(p,i,K)) = \vartheta_2(i \operatorname{ord} p) = i \operatorname{ord} p = i,$$

donc la famille $(\vartheta_2(\alpha(s,i,K)))_{i\in\mathbf{Z}}$ n'est pas sommable : la fonction $\tilde{\alpha}$ n'est pas S-intégrable.

– Considérons la sous-assignation $S \coloneqq h = h[0,0,0]$. Les applications

$$\alpha_K\colon \left|\begin{aligned} \mathbf{Z} &\longrightarrow \mathbf{Z}, \\ i &\longmapsto \mathbb{1}_{\mathbf{N}}(i) \end{aligned}\right. \quad \text{et} \quad \beta_K\colon \left|\begin{aligned} \mathbf{Z} &\longrightarrow \mathbf{Z}, \\ i &\longmapsto -i \end{aligned}\right.$$

donnent deux morphismes $\alpha, \beta\colon h[0,0,1] \longrightarrow h[0,0,1]$. On peut alors définir la fonction de Presburger $\tilde{\alpha}\mathbb{L}^{\tilde{\beta}} \in \mathscr{P}(h[0,0,1])$ qui est h-intégrable puisque, pour tout réel $q > 1$, tout $(0,p)$-corps K et tout entier $i \in \mathbf{Z}$, on a

$$\vartheta_q(\tilde{\alpha}\mathbb{L}^{\tilde{\beta}}(i,K)) = \vartheta_q(\mathbb{1}_{\mathbf{N}}(i)\mathbb{L}^{-i}) = \frac{\mathbb{1}_{\mathbf{N}}(i)}{q^i}$$

avec $0 < 1/q < 1$. Ceci montre également que $\tilde{\alpha}\mathbb{L}^{\tilde{\beta}} \in \mathrm{I}_S\mathscr{P}_+(S[0,0,1])$.

Dans la suite, pour un morphisme définissable $\alpha\colon S \longrightarrow h[0,0,1]$, on le confondra avec l'application $\tilde{\alpha}\colon |S| \longrightarrow \mathbf{Z}$ puisqu'ils se déterminent mutuellement. On peut maintenant définir l'intégrale sur le groupe des valeurs pour une fonction S-intégrable.

THÉORÈME 2.21. Soit $\varphi \in \mathrm{I}_S\mathscr{P}(S[0,0,r])$ une fonction S-intégrable. Alors il existe une unique fonction $\mu_S(\varphi) \coloneqq \psi \in \mathscr{P}(S)$ telle que

$$\forall q > 1,\ \forall (s,K) \in |S|, \quad \vartheta_q(\psi(s,K)) = \sum_{i \in \mathbf{Z}^r} \vartheta_q(\varphi(s,i,K)).$$

De plus, l'application

$$\mu_S\colon \left| \begin{aligned} \mathrm{I}_S\mathscr{P}(S[0,0,r]) &\longrightarrow \mathscr{P}(S), \\ \varphi &\longmapsto \mu_S(\varphi) \end{aligned} \right.$$

est un morphisme de $\mathscr{P}(S)$-modules.

EXEMPLE. On reprend le dernier exemple et on veut calculer la fonction $\mu_S(\alpha\mathbb{L}^\beta)$. Soient $q > 1$ un réel et $(s,K) \in |S|$ un point. On a

$$\sum_{i \in \mathbf{Z}} \vartheta_q(\alpha\mathbb{L}^\beta(s,i,K)) = \sum_{i=0}^{+\infty} q^{-i} = \frac{1}{1-q^{-1}}.$$

Ainsi la fonction $\mu_S(\alpha\mathbb{L}^\beta)$ est la fonction constante $1/(1-\mathbb{L}^{-1}) \in \mathbb{A}$.

NOTATION. Pour un morphisme définissable $f\colon Z \longrightarrow Y$, on définit son *tiré en arrière*

$$f^*\colon \left| \begin{aligned} \mathscr{P}(Y) &\longrightarrow \mathscr{P}(Z), \\ \varphi &\longmapsto [(z,K) \in |Z| \longmapsto \varphi(f_K(z),K)]. \end{aligned} \right.$$

Démonstration du théorème 2.21

La seconde partie du théorème est évidente. Pour la première, on va synthétiser la démonstration présente dans l'article [7, Theorem-Definition 4.5.1].

DÉFINITION 2.22. Soient S un ensemble $\mathscr{L}_{\mathrm{DP}}$-définissable et $X \subset S \times \mathbf{Z}^r$ un sous-ensemble définissable. Une fonction $f\colon X \longrightarrow \mathbf{Z}$ est S-*linéaire* s'il existe une fonction définissable $\gamma\colon S \longrightarrow \mathbf{Z}$ et trois r-uplets $(a_1,\dots,a_r), (c_1,\dots,c_r), (n_1,\dots,n_r) \in \mathbf{Z}^r$ d'entiers tels que

– pour tout $i \in [\![1,r]\!]$, on ait $0 \leqslant c_i < n_i$;
– pour tout $x \coloneqq (s,x_1,\dots,x_r) \in X \subset S \times \mathbf{Z}^r$, on ait

$$\forall i \in [\![1,r]\!],\ n_i \mid x_i - c_i \qquad \text{et} \qquad f(x) = \sum_{i=1}^r a_i \frac{x_i - c_i}{n_i} + \gamma(s).$$

On aura ensuite besoin d'un théorème de décomposition cellulaire sur les ensembles de Presburger qui est démontré dans l'article [5, Theorem 1].

DÉFINITION 2.23. On définit les S-*cellules* par induction.

– Une S-cellule de type (0) est le graphe d'une fonction S-linéaire $S' \longrightarrow \mathbf{Z}$ pour un ensemble définissable $S' \subset S$. Une S-cellule de type (1) est un ensemble de la forme

$$A \coloneqq \{(s,x) \in S' \times \mathbf{Z} \mid \alpha(s) \mathrel{\square_1} x \mathrel{\square_2} \beta(s),\ x \equiv c \mod n\}$$

où un ensemble définissable $S' \subset S$, deux fonctions S-linéaires $\alpha, \beta \colon S' \longrightarrow \mathbf{Z}$, deux entiers $c, n \in \mathbf{Z}$ tels que $0 \leqslant c < n$ et deux symboles $\square_i \in \{\leqslant, \emptyset\}$ vérifient que les fibres $A_s \coloneqq \{x \in \mathbf{Z} \mid (s,x) \in A\}$ ne soient pas uniformément bornées par rapport à la variable $s \in S'$.

– Soient $r \geqslant 1$ un entier et $(i_1, \dots, i_r) \in \{0,1\}^r$ un r-uplet. Une S-cellule du type $(i_1, \dots, i_r, 1)$ est un ensemble de la forme

$$A \coloneqq \{(s,x) \in S \times \mathbf{Z}^{r+1} \mid s \in D,\ \alpha(s) \square_1 x \square_2 \beta(s),\ x \equiv c \mod n\}$$

où une S-cellule $D \subset S \times \mathbf{Z}^r$ du type $(i_1, \dots, i_r)$, deux fonctions S-linéaires $\alpha, \beta \colon D \longrightarrow \mathbf{Z}$, deux entiers $c, n \in \mathbf{Z}$ tels que $0 \leqslant c < n$ et deux symboles $\square_i \in \{\leqslant, \emptyset\}$ vérifient que les fibres $A_s \subset \mathbf{Z}$ ne soient pas uniformément bornées par rapport à la variable $x \in D$. Une S-cellule du type $(i_1, \dots, i_r, 0)$ est un ensemble de la forme

$$\{(s,x) \in S \times \mathbf{Z}^{r+1} \mid s \in D,\ \alpha(s) = x\}$$

pour une S-cellule $D \subset S \times \mathbf{Z}^r$ du type $(i_1, \dots, i_r)$ et une fonction S-linéaire $\alpha \colon D \longrightarrow \mathbf{Z}$.

Théorème 2.24 *(de décomposition cellulaire pour les fonctions de Presburger).* Soient S un ensemble $\mathscr{L}_{\mathrm{DP}}$-définissable, $X \subset S \times \mathbf{Z}^r$ un sous-ensemble définissable et $f \colon X \longrightarrow \mathbf{Z}$ une fonction définissable. Alors il existe une partition finie $\mathscr{P}$ de l'ensemble X en S-cellules telle que chaque restriction $f|_A \colon A \longrightarrow \mathbf{Z}$ avec $A \in \mathscr{P}$ soit S-linéaire.

Preuve du théorème 2.21 Quitte à utiliser le théorème de Fubini pour les familles sommables, on ne traitera que le cas $r = 1$. Soit $\varphi \in \mathrm{I}_S\mathscr{P}(S[0,0,1])$. On va, au cours du prochain paragraphe, se ramener à une expression simple de la fonction φ.

Avec la définition 2.19, cette fonction φ est une somme de termes $a\alpha_1 \cdots \alpha_\ell \mathbb{L}^\beta$ avec $a \in \mathbb{A}$ et des morphismes $\alpha_i, \beta \colon S[0,0,1] \longrightarrow h[0,0,1]$. En utilisant la linéarité des familles sommables, on peut donc supposer que $\varphi = a\alpha_1 \cdots \alpha_\ell \mathbb{L}^\beta$. Soit $K \in \mathrm{Field}_p$. Quitte à appliquer le théorème de décomposition aux fonctions $\alpha_{j,K}$ et β_K, on peut supposer que le support de ces fonctions est inclus dans une $S(K)$-cellule $A_K \subset S(K) \times \mathbf{Z}$ et que ces fonctions sont $S(K)$-linéaires. Si la cellule A_K est du type (0), le résultat du théorème est immédiat. On peut donc supposer qu'elle est de la forme

$$A_K = \{(s,i) \in S'(K) \times \mathbf{Z} \mid \alpha_K(s) \square_1 i \square_2 \beta_K(s),\ i \equiv c_K \mod N_K\}$$

où l'on a adopté les notations de la définition 2.23. Soit $s \in S(K)$ un point désormais fixé. Quitte à poser $\alpha_K(s) = -\infty$ ou $\beta_K(s) = +\infty$, on peut supposer $\square_1 = \square_2 = <$. Par ailleurs, comme les fonctions $\alpha_{j,K}$ et β_K sont $S(K)$-linéaires, on les écrit sous les formes

$$\alpha_{j,K}(s,i) = a_{j,K}\frac{i - c_{j,K}}{n_{j,K}} + \gamma_{j,K}(s) \quad \text{avec} \quad i \equiv c_{j,K} \mod n_{j,K}$$

et

$$\beta_K(s,i) = a_{0,K}\frac{i - c_{0,K}}{n_{0,K}} + \gamma_{0,K}(s) \quad \text{avec} \quad i \equiv c_{0,K} \mod n_{0,K}$$

pour tout couple $(s,i) \in A_K$ où, lorsque les congruences ne sont pas satisfaites, les fonctions valent zéro [§3]. Quitte à faire des sommes, il suffit donc de prouver le théorème dans le cas où la fonction φ s'écrit sous la forme

$$\varphi_K(s,i) = ah_K(s)\mathbb{L}^{a_{0,K}(i-c_{0,K})/n_{0,K}} \prod_{j=1}^{b} \frac{i - c_{j,K}}{n_{j,K}}, \quad i \in (A_K)_s \tag{2.1}$$

pour un entier $b \in [\![1, \ell]\!]$ et une fonction définissable $h_K \colon A_K \longrightarrow \mathbf{Z}$. On note $(A_K)_s$ la fibre de l'ensemble A_K au point s, c'est-à-dire $(A_K)_s \coloneqq \{i \in \mathbf{Z} \mid \alpha_K(s) \leqslant i \leqslant \beta_K(s),\ i \equiv c_K \mod N_K\}$. Rappelons que l'on veut calculer les sommes

$$\sum_{i \in (A_K)_s} \vartheta_q(\varphi(s,i,K)), \qquad q > 1. \tag{2.2}$$

On peut donc supposer $(A_K)_s \neq \emptyset$ car sinon on pose $\psi(s,K) \coloneqq 0$. Soit $\tilde{c}_K \in (A_K)_s$ un entier fixé. Soit $j \in [\![0, b]\!]$ un indice. Comme $(s, \tilde{c}_K) \in A_K$, on a $\tilde{c}_K \equiv c_{j,K} \mod n_{j,K}$. Ainsi quitte à écrire

$$\frac{i - c_{j,K}}{n_{j,K}} = \frac{i - \tilde{c}_K}{n_{j,K}} - \frac{c_{j,K} - \tilde{c}_K}{n_{j,K}} \quad \text{avec} \quad i \equiv \tilde{c}_K \mod n_{j,K}, \quad i \in (A_K)_s$$

§3. On ne reprécisera jamais ceci pour ne pas alourdir la rédaction et à faire des sommes, on peut supposer que les entiers $c_{j,K}$ avec $j \in [\![0, b]\!]$ sont tous égaux à un entier $c_K \in (A_K)_s$. Maintenant, pour tous $i \in \mathbf{Z}$ et $j \in [\![0, b]\!]$, on a

$$i \in (A_K)_s \quad \Longrightarrow \quad i \equiv c_K \mod n_{j,K}.$$

Par conséquent, quitte à multiplier par une bonne constante, on peut supposer que les entiers $n_{j,K}$ sont tous égaux à un entier $N_K \in \mathbf{N}^*$. Enfin, comme on somme sur les entiers $i \in (A_K)_s$, on peut oublier la constante multiplicative en facteur dans l'expression (2.1). Finalement, on peut supposer que la fonction φ s'écrit sous la forme

$$\varphi_K(s,i) = \mathbb{L}^{a_K(i-c_K)/N_K}\left(\frac{i-c_K}{N_K}\right)^b, \quad i \in (A_K)_s \tag{2.3}$$

avec

$$i \equiv c_K \mod N_K, \qquad i \in (A_K)_s \tag{2.4}$$

pour certains entiers $a_K \in \mathbf{Z}$ et $c_K, N_K, b \in \mathbf{N}$ tels que $c_K < N_K$.

Grâce à ces deux dernières expressions, on est maintenant en mesure de calculer la somme (2.2) Posons [§4]

$$\alpha'_K(s) \coloneqq \left\lceil \frac{\alpha_K(s) - c_K}{N_K} \right\rceil \quad \text{et} \quad \beta'_K(s) \coloneqq \left\lfloor \frac{\beta_K(s) - c_K}{N_K} \right\rfloor$$

de telle sorte que

$$(A_K)_s = \{\ell N_K + c_K \mid \ell \in \mathbf{Z},\ \alpha'_K(s) \leqslant \ell \leqslant \beta'_K(s)\}.$$

On obtient alors

$$\sum_{i\in(A_K)_s} \vartheta_q(\varphi(s,i,K)) = \sum_{i\in(A_K)_s} q^{a_K(i-c_K)/N_K}\left(\frac{i-r_K}{N_K}\right)^b = \sum_{\ell=\alpha'_K(s)}^{\beta'_K(s)} (q^{a_K})^\ell \ell^b.$$

Comme la fonction φ est S-intégrable, cela implique $\alpha'_K(s) > -\infty$ ou $\beta'_K(s) < +\infty$ selon le signe de l'entier a_K. Par symétrie, on peut supposer $\alpha'_K(s) > -\infty$ ce qui implique $a_K < 0$. Quitte à ajouter ou retirer un nombre fini de termes, on peut supposer $\alpha'_K(s) = 0$. Le cas $\beta'_K(s) < +\infty$ étant alors trivial puisque la somme a un nombre fini de termes, on suppose $\beta'_K(s) = +\infty$. Il s'agit donc de calculer la somme

$$\sum_{i\in(A_K)_s} \vartheta_q(\varphi(s,i,K)) = \sum_{\ell=0}^{+\infty} (q^{a_K})^\ell \ell^b$$

avec $a_K < 0$. On souhaite montrer qu'elle est de la forme $\vartheta_q(r)$ pour un élément $r \in \mathbb{A}$. D'après le lemme 2.25, la dernière somme s'écrit

$$\sum_{\ell=0}^{+\infty} (q^{a_K})^\ell \ell^b = \sum_{j=0}^{b} \frac{\lambda_j (q^{a_K})^j}{(1-q^{a_K})^{j+1}}$$

pour des constantes $\lambda_j \in \mathbf{R}$ indépendantes du réel q. Il suffit alors de poser

$$\psi(s,K) \coloneqq \sum_{j=0}^{b} \lambda_j \mathbb{L}^{a_K j}\left(\frac{1}{1-\mathbb{L}^{a_K}}\right)^{j+1} \in \mathbb{A}$$

et la fonction $\psi \in \mathscr{P}(S)$ [§5] vérifie bien les conditions du théorème.

Quant à elle, l'unicité se montre par un argument polynomiale. En effet, soit $\psi' \in \mathscr{P}(S)$ une autre telle fonction. Soit $(s,K) \in |S|$ un point fixé. Alors

$$\forall q > 1, \qquad \vartheta_q(\psi(s,K) - \psi'(s,K)) = 0 \tag{2.5}$$

Quitte à multiplier l'élément $r(\mathbb{L}) \coloneqq \psi(s,K) - \psi'(s,K)$ par des termes de la forme $\mathbb{L}^k$ ou $(1-\mathbb{L}^{-i})^k$ ce qui ne change pas la condition (2.5), on peut supposer $r \in \mathbf{Z}[\mathbb{L}] \subset \mathbf{R}[\mathbb{L}]$. La condition (2.5) dit alors que le polynôme r admet une infinité de racines, donc $r = 0$. Finalement, ceci étant vrai pour tout point $(s,K) \in |S|$, on obtient $\psi = \psi'$. □

§4. On pose les conventions adéquates lorsque l'un des deux entiers $\alpha_K(s)$ et $\beta_K(s)$ vaut l'infini.

§5. Notons que la fonction ψ est bien de Presburger. En effet, le théorème 2.24 fonctionne pour des fonctions de Presburger et, sur chaque cellule, les constantes c_K, n_K, … peuvent être prises indépendantes du corps K. Ce fait, qu'on admet, se montre avec le théorème de compacité comme dans la preuve de la proposition 1.24.

Lemme 2.25. Soit A un anneau. On considère l'application A-linéaire

$$\Delta\colon \left|\begin{array}{rcl} A[X] & \longrightarrow & A[X], \\ P & \longmapsto & P(X+1)-P(X). \end{array}\right.$$

Soient $d, a \in \mathbf{N}$ deux entiers et $P \in A[X]$ un polynôme de degré d. Alors l'égalité

$$\sum_{n=a}^{+\infty} P(n)T^n = \sum_{j=0}^{d} \frac{\Delta^j P(a) T^{a+j}}{(1-T)^{j+1}}$$

est vraie dans $A[\![T]\!]$.

Preuve On raisonne par récurrence sur le degré d. Pour $d=0$, la formule résulte simplement de la relation bien connue

$$\sum_{n=0}^{+\infty} T^n = \frac{1}{1-T} \qquad \text{dans } A[\![T]\!].$$

Soit $d \in \mathbf{N}$. On suppose que la formule est vérifiée pour des polynômes de degré d. Soit $P \in A[X]$ un polynôme de degré $d+1$. Alors

$$\begin{aligned}(1-T)\sum_{n=a}^{+\infty} P(n)T^n &= \sum_{n=a}^{+\infty} P(n)T^n - \sum_{n=a}^{+\infty} P(n)T^{n+1} \\ &= \sum_{n=a-1}^{+\infty} P(n+1)T^{n+1} - \sum_{n=a}^{+\infty} P(n)T^{n+1} \\ &= P(a)T^a - T\sum_{n=a}^{+\infty} \Delta P(n)T^n.\end{aligned}$$

Comme le polynôme ΔP est de degré d, l'hypothèse de récurrence nous donne

$$\begin{aligned}(1-T)\sum_{n=a}^{+\infty} P(n)T^n &= P(a)T^a - T\sum_{j=0}^{d} \frac{\Delta^{j+1} P(a) T^{a+j}}{(1-T)^{j+1}} \\ &= \Delta^0 P(a)T^a - \sum_{j=1}^{d+1} \frac{\Delta^j P(a) T^{a+j}}{(1-T)^j} \\ &= \sum_{j=0}^{d} \frac{\Delta^j P(a) T^{a+j}}{(1-T)^j}\end{aligned}$$

puisque $\Delta^{d+1}P = 0$. En divisant cette dernière égalité par le polynôme $1-T$, on obtient l'égalité au rang $d+1$ ce qui conclut la preuve. □

2.3.3. Intégration sur le corps résiduel

Soit Z une sous-assignation. On définit le demi-groupe[§6] $\mathscr{Q}_+(Z)$, également noté $SK_0(\mathrm{Def}_Z)$, comme le demi-groupe abélien libre sur les symboles $[Y]$ pour une sous-assignation $Y \subset Z[0,m,0]$ avec un entier $m \geqslant 0$ où l'on impose les relations suivantes :

(i) on a $[\emptyset] = 0$ où $\emptyset := (\emptyset)_{K \in \mathrm{Field}_p}$ est la sous-assignation vide ;

(ii) si $f\colon Y \longrightarrow Y'$ est un isomorphisme commutant avec les injections $Y \longrightarrow Z$ et $Y' \longrightarrow Z$, alors

$$[Y] = [Y'] ;$$

(iii) si $Y_1, Y_2 \subset [0,m,0]$, alors

$$[Y_1 \cup Y_2] + [Y_1 \cap Y_2] = [Y_1] + [Y_2].$$

Pour une sous-assignation $Y \subset Z[0,m,0]$, on notera toujours $[Y] \in \mathscr{Q}_+(Z)$ sa classe.

§6. Un *demi-groupe* est un magma associatif.

NOTATION. Soient $Y_1 \subset h[n,m,r]$, $Y_2 \subset h[n',m',r']$ et X trois sous-assignations et $f_1 \colon Y_1 \longrightarrow X$ et $f_2 \colon Y_2 \longrightarrow X$ deux morphismes. Le *produit fibré* de Y_1 et Y_2 au-dessus de X est la sous-assignation

$$Y_1 \times_X Y_2 \subset h[n+n', m+m', r+r']$$

définie par les égalités

$$(Y_1 \times_X Y_2)(K) \coloneqq \{(\overline{x}_1, \overline{x}_2, \overline{u}_1, \overline{u}_2, \overline{z}_1, \overline{z}_2) \in h[n+n', m+m', r+r'](K) \mid \\ (\overline{x}_1, \overline{u}_1, \overline{z}_1) \in Y_1(K),\ (\overline{x}_2, \overline{u}_2, \overline{z}_2) \in Y_2(K),\ f_{1,K}(\overline{x}_1, \overline{u}_1, \overline{z}_1) = f_{2,K}(\overline{x}_2, \overline{u}_2, \overline{z}_2)\}.$$

Lorsque les sous-assignations Y_1 et Y_2 sont respectivement incluses dans $X[n,m,r]$ et $X[n',m',r']$ et que l'on considère les projections $Y_1 \longrightarrow X$ et $Y_2 \longrightarrow X$, le produit fibré $Y_1 \times_X Y_2$ sera identifié à la sous-assignation correspondante de $X[n+n', m+m', r+r']$.

STRUCTURE DE DEMI-ANNEAU. Pour deux sous-assignations $Y \subset Z[0,m,0]$ et $Y' \subset Z[0,m',0]$, on pose

$$[Y] \times [Y'] \coloneqq [Y \times_Z Y']$$

où le produit fibré est pris selon les projections $Y \longrightarrow Z$ et $Y' \longrightarrow Z$. Avec cette définition, on munit le demi-groupe $\mathscr{Q}_+(Z)$ d'une structure de demi-anneau, dit *de Grothendieck*. Remarquons que cette loi est bien définie en vertu du point (ii). On pose

$$1 \coloneqq [Z] \in \mathscr{Q}_+(Z) \quad \text{et} \quad \mathbb{L} \coloneqq [Z[0,1,0]] \in \mathscr{Q}_+(Z).$$

REMARQUES. – Le symbole $\mathbb{L}$ fait référence à deux objets à la fois, le premier dans $\mathbb{A}$ et le second dans $\mathscr{Q}_+(Z)$. Cependant, aucune confusion n'est possible ce qui justifie leur notation commune.

– Montrons que, pour tout entier $m \geqslant 0$, on a $\mathbb{L}^m = [Z[0,m,0]]$. Traitons uniquement le cas $m = 2$. Par définition, on a $\mathbb{L}^2 = [Z[0,1,0] \times_Z Z[0,1,0]]$ où, en notant $p \colon Z[0,1,0] \longrightarrow Z$ la projection, pour tout corps $K \in \mathrm{Field}_p$, on a $(Z[0,1,0] \times_Z Z[0,1,0])(K) \cong Z[0,2,0](K)$. Il suffit alors d'utiliser le point (ii) ce qui montre $\mathbb{L}^2 = [Z[0,2,0]]$. On peut alors faire une récurrence sur l'entier m.

DÉFINITION 2.26. Soient $m \geqslant 0$ un entier et X une sous-assignation. Considérons la sous-assignation $Z \coloneqq X[0,m,0]$. L'*intégrale dans la fibre selon la projection* $Z \longrightarrow X$ est l'application

$$\mu_X \colon \left| \begin{array}{r@{\ }c@{\ }l} \mathscr{Q}_+(Z) & \longrightarrow & \mathscr{Q}_+(X), \\ [Y] & \longmapsto & [Y]. \end{array} \right.$$

Explicitons quelque peu cette définition. Un élément de $\mathscr{Q}_+(Z)$ est de la forme $[Y]$ pour une sous-assignation $Y \subset Z[0,m',0]$. Comme $Z = X[0,m,0]$, on a $Y \subset X[0, m+m', 0]$ et on considère donc la classe $[Y] \in \mathscr{Q}_+(X)$.

NOTATION. Pour un morphisme définissable $f \colon Z_1 \longrightarrow Z_2$, on définit également son tiré en arrière

$$f^* \colon \left| \begin{array}{r@{\ }c@{\ }l} \mathscr{Q}_+(Z_2) & \longrightarrow & \mathscr{Q}_+(Z_1), \\ [Y] & \longmapsto & [Y \times_{Z_2} Z_1]. \end{array} \right.$$

2.3.4. INTÉGRATION SUR LE GROUPE DES VALEURS ET LE CORPS RÉSIDUEL

Soit Z une sous-assignation définissable. On définit le sous-demi-anneau $\mathscr{P}_+^0(Z) \subset \mathscr{P}_+(Z)$ engendré par

– les fonctions $\mathbb{1}_Y \colon (z,K) \in |Z| \longmapsto \mathbb{1}_{Y(K)}(z) \in \mathbb{A}$ pour des sous-assignations Y de Z ;
– la fonction constante $(z,K) \in |Z| \longmapsto \mathbb{L} - 1 \in \mathbb{A}$.

Avec l'inclusion $\mathscr{P}_+^0(Z) \longrightarrow \mathscr{P}_+(Z)$ et le morphisme canonique de demi-anneaux $\mathscr{P}_+^0(Z) \longrightarrow \mathscr{Q}_+(Z)$ qui envoie les fonctions $\mathbb{1}_Y$ sur les classes $[Y]$ et la fonction constante $\mathbb{L}-1$ sur la classe $\mathbb{L}-1$, les demi-anneaux $\mathscr{Q}_+(Z)$ et $\mathscr{P}_+(Z)$ sont alors munis d'une structure de $\mathscr{P}_+^0(Z)$-demi-modules. On définit alors le demi-anneau

$$\mathscr{C}_+(Z) \coloneqq \mathscr{P}_+(Z) \otimes_{\mathscr{P}_+^0(Z)} \mathscr{Q}_+(Z).$$

Bien qu'ils ne soient pas des fonctions, les éléments du demi-anneau $\mathscr{C}_+(Z)$ sont appelés les *fonctions motiviques constructibles positives sur* Z.

NOTATION. Pour un morphisme définissable $f\colon Z \longrightarrow Y$, on définit également son tiré en arrière

$$f^*\colon \left| \begin{array}{l} \mathscr{C}_+(Y) \longrightarrow \mathscr{C}_+(Z), \\ \displaystyle\sum_{i=1}^{r} a_i \otimes b_i \longmapsto \sum_{i=1}^{r} f^*(a_i) \otimes f^*(b_i) \end{array} \right.$$

en utilisant les notations définies précédemment.

Avant de définir l'intégrale sur le groupe des valeurs et le corps résiduel, on a besoin d'un lemme préliminaire qui découle de la division de la théorie. Pour sa preuve, on va procéder comme pour la proposition 1.24 et utiliser le théorème de compacité.

LEMME 2.27 *(division des sous-assignations).* Soient S et $X \subset S[0,m,r]$ deux sous-assignations. Alors il existe des sous-assignations définissables $U_1, \dots, U_\ell \subset S[0,m,0]$ et $Z_1, \dots, Z_\ell \subset S[0,0,r]$ telles que

$$X = \bigsqcup_{i=1}^{\ell} U_i \times_S Z_i$$

où le produit fibré est pris selon les projections $S[0,m,0] \longrightarrow S$ et $S[0,0,r] \longrightarrow S$.

Preuve Raisonnons par l'absurde et supposons le contraire. On note $S \subset h[n,m',r']$. Soit Φ la formule définissant la sous-assignation X. On rajoute $n'+m'+r'$ symboles de constantes, notés c_i, au langage $\mathscr{L}_{\mathrm{DP}}$, formant le langage $\tilde{\mathscr{L}}_{\mathrm{DP}}$. Notons $c := (c_1, \dots, c_{n'+m'+r'})$. Pour ℓ phrases

$$\phi_j(x_1, \dots, x_{n'}, u'_1, \dots, u'_{m'}, z'_1, \dots, z'_{r'}, u_1, \dots, u_m) \quad \text{avec} \quad j \in [\![1,\ell]\!]$$

avec des variables libres dans les bonnes sortes [§7] et pour ℓ phrases

$$\psi_j(x_1, \dots, x_{n'}, u'_1, \dots, u'_{m'}, z'_1, \dots, z'_{r'}, z_1, \dots, z_r) \quad \text{avec} \quad j \in [\![1,\ell]\!]$$

avec la même convention, on considère la $\tilde{\mathscr{L}}_{\mathrm{DP}}$-phrase [§8] $\Psi_{\phi_1,\dots,\phi_\ell,\psi_1,\dots,\psi_\ell}$

$$\neg\Big\{\forall u_1 \cdots \forall u_m \forall z_1 \cdots \forall z_r \qquad \Phi(c, u_1, \dots, u_m, z_1, \dots, z_r) \longleftrightarrow$$
$$\Big([\phi_1(c,u_1,\dots,u_m) \wedge \psi_1(c,z_1,\dots,z_r)] \otimes \cdots \otimes [\phi_\ell(c,u_1,\dots,u_m) \wedge \psi_\ell(c,z_1,\dots,z_r)]\Big)\Big\}.$$

où le symbole $\otimes$ désigne la disjonction exclusive. Alors la théorie des $(0,p)$-corps à laquelle on ajoute les phrases $\Psi_{\phi_1,\dots,\phi_\ell,\psi_1,\dots,\psi_\ell}$ est consistante : on utilise le théorème de compacité comme dans la preuve de la proposition 1.24. Pour être plus précis, on applique notre hypothèse absurde aux formules $\phi_{i,j}$ et $\psi_{i,j}$ et cela nous donne un $(0,p)$-corps K et une interprétation pour la constante c dans ce dernier qui va satisfaire toutes les phrases. Ainsi cette nouvelle théorie admet un modèle : les phrases $\Psi_{\phi_1,\dots,\phi_\ell,\psi_1,\dots,\psi_\ell}$ y sont vraies ce qui contredit la division de cette nouvelle théorie, la théorie des $(0,p)$-corps l'étant. □

PROPOSITION 2.28. Soit S une sous-assignation. Notons $p\colon S[0,0,r] \longrightarrow S$ et $q\colon S[0,m,0] \longrightarrow S$ les projections. On considère les morphismes composés

$$\mathscr{P}^0_+(S) \longrightarrow \mathscr{P}_+(S) \xrightarrow{p^*} \mathscr{P}_+(S[0,0,r]) \qquad \text{et} \qquad \mathscr{P}^0_+(S) \longrightarrow \mathscr{Q}_+(S) \xrightarrow{q^*} \mathscr{Q}_+(S[0,m,0])$$

qui confèrent aux demi-anneaux $\mathscr{P}_+(S[0,0,r])$ et $\mathscr{Q}_+(S[0,m,0])$ des structures de $\mathscr{P}^0_+(S)$-demi-modules. Alors le morphisme canonique

$$\Phi\colon \left| \begin{array}{r} \mathscr{P}_+(S[0,0,r]) \otimes_{\mathscr{P}^0_+(S)} \mathscr{Q}_+(S[0,m,0]) \longrightarrow \mathscr{C}_+(S[0,m,r]), \\ a \otimes b \longmapsto p_1^*(a) \otimes p_2^*(b) \end{array} \right.$$

est un isomorphisme de demi-anneaux où $p_1\colon S[0,m,r] \longrightarrow S[0,0,r]$ et $p_2\colon S[0,m,r] \longrightarrow S[0,m,0]$

§7. Les variables avec les lettres x, u et z sont respectivement dans les sortes du corps valué, du corps résiduel et du groupe des valeurs.

§8. Cette phrase signifie, réinterprétée dans le corps K, que la fibre $X(K)_c \subset k_K^m \times \mathbf{Z}^r$ ne peut pas être écrite comme une union disjointe de fibres $(U_i \times_{X(K)} Z_i)_c$ où les ensembles définissables $U_i \subset S(K) \times k_K^m$ et $Z_i \subset S(K) \times \mathbf{Z}^r$ sont respectivement définis par les phrases ϕ_i et ψ_i.

sont les projections.

Preuve Tout d'abord, l'application Φ est clairement un morphisme de demi-anneaux puisqu'elle est induite par l'application $\mathscr{P}^0_+(S)$-bilinéaire

$$\tilde{\Phi}\colon \left| \begin{array}{rcl} \mathscr{P}_+(S[0,0,r]) \times \mathscr{Q}_+(S[0,m,0]) & \longrightarrow & \mathscr{P}_+(S[0,m,r]) \times \mathscr{Q}_+(S[0,m,r]), \\ (a,b) & \longmapsto & (p_1^*(a), p_2^*(b)). \end{array} \right.$$

Cette dernière fait commuter le diagramme

$$\begin{tikzcd} \mathscr{P}_+(S[0,0,r]) \times \mathscr{Q}_+(S[0,m,0]) \arrow[r, "\tilde{\Phi}"] \arrow[d] & \mathscr{P}_+(S[0,m,r]) \times \mathscr{Q}_+(S[0,m,r]) \arrow[d] \\ \mathscr{P}_+(S[0,0,r]) \otimes_{\mathscr{P}^0_+(S)} \mathscr{Q}_+(S[0,m,0]) \arrow[r, "\Phi"] & \mathscr{C}_+(S[0,m,r]) \end{tikzcd}$$

Construisons une application

$$\Psi\colon \mathscr{C}_+(S[0,m,r]) \longrightarrow \mathscr{P}_+(S[0,0,r]) \otimes_{\mathscr{P}^0_+(S)} \mathscr{Q}_+(S[0,m,0])$$

qui sera l'isomorphisme réciproque. Définissons-le sur les éléments $a \otimes b$. Soit $a \otimes b \in \mathscr{C}_+(S[0,m,r])$. En utilisant la linéarité, on peut supposer $b = [Y]$ pour une sous-assignation $Y \subset S[0,m+m',r]$ et un entier $m' \geqslant 0$. Grâce au lemme 2.27, il existe des sous-assignations $U_1, \dots, U_\ell \subset S[0,m+m',0]$ et $Z_1, \dots, Z_\ell \subset S[0,0,r]$ telles que

$$Y = \bigsqcup_{i=1}^{\ell} U_i \times_S Z_i. \tag{2.6}$$

Par ailleurs, avec la définition 2.19, en utilisant la même linéarité, on peut se ramener au cas où la fonction $a \in \mathscr{P}_+(S[0,m,r])$ s'écrit sous la forme $\alpha_1 \cdots \alpha_k \mathbb{L}^{\alpha_0}$ pour certains morphismes définissables $\alpha_0, \alpha_1, \dots, \alpha_k\colon S[0,m,r] \longrightarrow h[0,0,1]$. Soit $j \in [\![0,k]\!]$ un indice. La fonction α_j étant définissable, son graphe $\Gamma(\alpha_j) \subset S[0,m,r+1]$ est une sous-assignation définissable, donc il s'écrit sous la forme

$$\Gamma(\alpha_j) = \bigsqcup_{i=1}^{\ell'_j} U'_{j,i} \times_S Z'_{j,i} \tag{2.7}$$

pour des ensembles définissables $U'_{j,i} \subset S[0,m,0]$ et $Z'_{j,i} \subset S[0,0,r+1]$. On peut donc écrire

$$\alpha_{j,K}(s,u,z) = \sum_{i=1}^{\ell'_j} \mathbb{1}_{U'_{j,i}(K)}(s,u)\beta_{j,i,K}(s,z) \tag{2.8}$$

où l'on a considéré les morphismes définissables $\beta_{j,i}\colon S[0,0,r] \longrightarrow h[0,0,1]$ dont le graphe est la sous-assignation $Z'_{j,i}$ §9. Remarquons qu'on peut choisir les entiers ℓ'_j égaux quitte à prendre leur maximum et à rajouter à la décomposition (2.7) des sous-assignations vides. Notons $\ell' \in \mathbf{N}$ leur valeur commune. En condensant l'écriture, on peut mettre la fonction a sous la forme

$$a = \Big(\sum_{i=1}^{\ell'} p_2^*(\mathbb{1}_{U'_i})p_1^*(\beta_i)\Big) \prod_{i=1}^{\ell'} \mathbb{L}^{p_2^*(\mathbb{1}_{V'_i})p_1^*(\gamma_i)}$$

pour des sous-assignations $U'_i, V'_i \subset S[0,m,0]$ et des morphismes $\beta_i, \gamma_i\colon S[0,0,r] \longrightarrow h[0,0,1]$. Quitte à écrire

$$\mathbb{L}^{p_2^*(\mathbb{1}_{V'_i})p_1^*(\gamma_i)} = p_2^*(1 - \mathbb{1}_{V'_i})\mathbb{L}^0 + p_2^*(\mathbb{1}_{V'_i})\mathbb{L}^{p_1^*(\gamma_i)}, \qquad i \in [\![1,\ell']\!]$$

§9. Forgeons notre intuition de l'égalité (2.8) grâce à la remarque suivante. Soit $(s,u,z) \in S[0,m,r](K)$ un point fixé avec $s \in S(K)$ et $(u,z) \in k_K^m \times \mathbf{Z}^r$. Par définition, on a $(s,u,z,\alpha_{j,K}(s,u,z)) \in \Gamma(a_{j,K})$. Ainsi, grâce à la décomposition (2.7), on peut exhiber un indice $i \in [\![1,\ell'_j]\!]$ tel que

$$(s,u,z,a_{j,K}(s,u,z)) \in U'_{j,i}(K) \times_{S(K)} Z'_{j,i}(K).$$

Avec la définition du produit fibré $U'_{j,i}(K) \times_{S(K)} Z'_{j,i}(K)$, cela se récrit

$$(s,u) \in U'_{j,i} \quad \text{et} \quad (s,z,\alpha_{j,K}(s,u,z)) \in Z'_{j,i}.$$

Cette égalité (2.8) est alors vraie puisque les graphes de deux fonctions coïncident.

et à faire des sommes, on peut supposer qu'il existe des sous-assignations $W_1, \ldots, W_\ell \subset S[0,m,0]$ et un morphisme $\gamma\colon S[0,0,r] \longrightarrow h[0,0,1]$ vérifiant

$$a = \sum_{i=1}^{\ell'} p_2^*(\mathbb{1}_{W_i}) p_1^*(\beta_i \mathbb{L}^\gamma). \tag{2.9}$$

En résumé, on a obtenu les décompositions (2.6) et (2.9). En utilisant les morphismes

$$\mathscr{P}_+^0(S[0,m,r]) \longrightarrow \mathscr{P}_+(S[0,m,r]) \quad \text{et} \quad \mathscr{P}_+^0(S[0,m,r]) \longrightarrow \mathscr{Q}_+(S[0,m,r])$$

définissant la structure de $\mathscr{P}_+^0(S[0,m,r])$-demi-module, on peut ainsi écrire

$$\begin{aligned} a \otimes b &= \Big(\sum_{i=1}^{\ell'} p_2^*(\mathbb{1}_{W_i}) p_1^*(\beta_i \mathbb{L}^\gamma)\Big) \otimes \Big[\bigsqcup_{j=1}^{\ell} U_j \times_S Z_j\Big] \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} p_2^*(\mathbb{1}_{W_i}) p_1^*(\beta_i \mathbb{L}^\gamma) \otimes [U_j] \times [Z_j] \\ &= \sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} p_1^*(\mathbb{1}_{U_j} \beta_i \mathbb{L}^\gamma) \otimes p_2^*([Z_j \times_S W_i]). \end{aligned}$$

En posant

$$\Psi(a \otimes b) \coloneqq \sum_{i=1}^{\ell} \sum_{j=1}^{\ell'} p_1^*(\mathbb{1}_{U_j} \beta_i \mathbb{L}^\gamma) \otimes p_2^*([Z_j \times_S W_i]) \in \mathscr{P}_+(S[0,0,r]) \otimes_{\mathscr{P}_+^0(S)} \mathscr{Q}_+(S[0,m,0]),$$

on a ainsi définit l'application

$$\Psi\colon \mathscr{C}_+(S[0,m,r]) \longrightarrow \mathscr{P}_+(S[0,0,r]) \otimes_{\mathscr{P}_+^0(S)} \mathscr{Q}_+(S[0,m,0])$$

qui, par sa définition, est l'isomorphisme réciproque du morphisme Φ. Ceci conclut la preuve. $\square$

DÉFINITION 2.29. Une fonction $\varphi \in \mathscr{C}_+(X[0,m,r])$ est X-*intégrable* si on peut écrire

$$\Phi^{-1}(\varphi) = \sum_{i=1}^{\ell} a_i \otimes b_i \quad \text{avec} \quad a_i \in \mathrm{I}_X \mathscr{P}_+(X[0,0,r]) \quad \text{et} \quad b_i \in \mathscr{Q}_+(X[0,m,0])$$

où l'on utilise l'isomorphisme de la proposition précédente.

On peut maintenant définir l'intégrale sur le groupe des valeurs et le corps résiduel.

LEMME 2.30. Soit $\varphi \in \mathscr{C}_+(X[0,m,r])$ une fonction X-intégrable s'écrivant comme précédemment. Alors la fonction

$$\mu_X(\varphi) \coloneqq \sum_{i=1}^{\ell} \mu_X(a_i) \otimes \mu_X(b_i) \in \mathscr{C}_+(X)$$

ne dépend pas des éléments a_i et b_i et elle est appelée l'*intégrale de la fonction φ sur les fibres de la projection $X[0,m,r] \longrightarrow Y$.*

Preuve Considérons le groupe libre W sur l'alphabet $\mathrm{I}_X \mathscr{P}_+(X[0,0,r]) \times \mathscr{Q}_+(X[0,m,0])$. Avec la proposition précédente, il suffit de montrer que l'application

$$w\colon \left| \begin{array}{rcl} W & \longrightarrow & \mathscr{C}_+(X), \\ \displaystyle\sum_{i=1}^{\ell} (a_i, b_i) & \longmapsto & \displaystyle\sum_{i=1}^{\ell} \mu_X(a_i) \otimes \mu_X(b_i) \end{array} \right.$$

se factorise en une application

$$\mathrm{I}_X \mathscr{P}_+(X[0,0,r]) \otimes_{\mathscr{P}_+^0(X)} \mathscr{Q}_+(X[0,m,0]) \longrightarrow \mathscr{C}_+(X). \tag{2.10}$$

Pour cela, vérifions qu'elle est bilinéaire. Soient $(a,b), (a',b') \in W$ et $c \in \mathscr{P}_+^0(X)$. La linéarité des applications $\mu_X\colon \mathrm{I}_X \mathscr{P}_+(X[0,0,r]) \longrightarrow \mathscr{P}_+(X)$ et $\mu_X\colon \mathscr{Q}_+(X[0,m,0]) \longrightarrow \mathscr{Q}_+(X)$ donne

$$w(a+a', b) = w(a,b) + w(a',b) \quad \text{et} \quad w(a, b+b') = w(a,b) + w(a,b').$$

Il reste à vérifier l'égalité $cw(a,b) = w(ca,b) = w(a,cb)$. On peut facilement se ramener au cas où l'on écrit $b = [Y]$ pour une sous-assignation $Y \subset X[0, m+m', 0]$. Comme la fonction c a sa variable dans X, on a

$$\begin{aligned} w(ca,b) &= \mu_X(ca) \otimes \mu_X(b) \\ &= c\mu_X(a) \otimes \mu_X(b) = cw(a,b). \end{aligned}$$

Avec la définition du sous-demi-anneau $\mathscr{P}^0_+(X)$, il suffit de traiter les deux cas suivants. Si $c = \mathbb{1}_Z$ pour une sous-assignation $Z \subset X$, alors

$$\begin{aligned} w(ca,b) &= \mathbb{1}_Z \mu_X(a) \otimes [Y] \\ &= \mu_X(a) \otimes [Z] \times [Y] \\ &= \mu_X(a) \otimes \mu_X([Z] \times [Y]) = w(a,cb). \end{aligned}$$

où l'on a utilisé le morphisme $\mathscr{P}^0_+(X) \longrightarrow \mathscr{Q}_+(X)$. On procède de même lorsque $c = \mathbb{L} - 1$. Ainsi l'application w est bien bilinéaire. Par conséquent, elle se factorise en une unique application (2.10) ce qui termine la preuve. $\square$

Exemple. Reprenons le même exemple. Pour rappel, avec $X = h$, on considère la fonction

$$\mathrm{I}_X \mathscr{P}_+(h[0,0,1]) \ni a \colon \left| \begin{aligned} |g[0,0,1]| &\longrightarrow \mathbb{A}, \\ (i,K) &\longmapsto \mathbb{1}_{\mathbf{N}}(i)\mathbb{L}^{-i}. \end{aligned} \right.$$

L'intégrale de la fonction $a \otimes \mathbb{L} \in \mathscr{C}_+(h[0,1,1])$ vaut

$$\mu_X(a \otimes \mathbb{L}) = \frac{1}{1-\mathbb{L}} \otimes \mathbb{L}.$$

Lemme 2.31. Soit Z une sous-assignation. Considérons l'injection

$$\left| \begin{aligned} \mathscr{P}_+(Z) &\longrightarrow \mathscr{C}_+(Z), \\ \psi &\longmapsto \psi \otimes [Z]. \end{aligned} \right.$$

Soit $\varphi \in \mathscr{C}_+(Z)$ une fonction. Alors il existe une fonction $\psi \in \mathscr{P}_+(Z[0,m,0])$ telle que $\varphi = \mu_Z(\psi)$.

Preuve Encore une fois, la division de la théorie va intervenir. En utilisant la linéarité, il suffit de montrer le lemme lorsque la fonction φ est de la forme $a \otimes [Y]$ avec $a \in \mathscr{P}_+(Z)$ et $Y \subset Z[0,m,0]$ pour un entier $m \geqslant 0$. Notons $p \colon Z[0,m,0] \longrightarrow Z$ la projection et considérons la fonction

$$\psi \coloneqq \mathbb{1}_Y p^*(a) \in \mathscr{P}_+(Z[0,m,0]) \subset \mathscr{C}_+(Z[0,m,0]).$$

En utilisant l'isomorphisme $\mathscr{P}^+_0(Z[0,m,0]) \longrightarrow \mathscr{Q}_+(Z[0,m,0])$ et le lemme 2.30, cette dernière fonction vérifie bien l'égalité souhaitée. $\square$

2.3.5. Intégration sur une variable du corps valué

Soit K un $(0,p)$-corps. Pour une boule $B \coloneqq \mathrm{B}_K(a,z) \subset K$ et un réel $q > 1$, le *q-volume* de la boule B est le réel

$$\mathrm{vol}_q(B) \coloneqq q^{-z}.$$

Un *domaine étagé*, ou simplement un domaine, est une famille $S \coloneqq \{B_i\}_{i \in I}$ de boules de K, indexées par un ensemble I au plus dénombrable, telle que

$$\mathrm{vol}_q(B_i) \neq \mathrm{vol}_q(B_j), \qquad i \neq j,\ q > 1. \tag{2.11}$$

Il sera identifié avec l'union $S^\cup \coloneqq \bigcup_{i \in I} B_i$.

Une fonction $f \colon K \longrightarrow \mathbf{R}_+$ est *étagée* s'il existe un unique domaine S et un élément $a_0 \in K$ tels que la fonction f soit

– une constante strictement positive sur chaque boule de S ;
– nulle sur $K \setminus (S^\cup \cup \{a_0\})$.

Soit $q > 1$ un réel. Une fonction étagée $f \colon K \longrightarrow \mathbf{R}_+$ associée à un domaine S est *q-intégrable* sur K si

$$\mathrm{I}_q(f) \coloneqq \sum_{B \in S} \mathrm{vol}_q(B) c_B < +\infty$$

où, pour chaque boule $B \in S$, le réel $c_B > 0$ est la valeur de la fonction f sur la boule B. Dans ce cas, cette dernière quantité $\mathrm{I}_q(f) \in \mathbf{R}$ est appelée la *q-intégrale* de la fonction f sur K.

DÉFINITION 2.32. Soit X une sous-assignation. Une fonction $\varphi \in \mathscr{P}_+(X[1,0,0])$ est *une famille de fonctions étagées X-intégrables* si, pour tout point $(x,K) \in |X|$, il existe un domaine S tel que, pour tout réel $q > 1$, il existe une partie finie $S_q \subset S$ que la fonction

$$\vartheta_q(\varphi(x,\cdot,K)) \colon \left| \begin{aligned} K &\longrightarrow \mathbf{R}_+, \\ t &\longmapsto \vartheta_q(\varphi(x,t,K)) \end{aligned} \right.$$

soit une fonction étagée de domaine $S \setminus S_q$ et q-intégrable sur K.

EXEMPLE. La fonction $\varphi \in \mathscr{P}_+(h[1,0,0])$ définie par la relation

$$\varphi(t,K) \coloneqq \begin{cases} (\mathbb{L}-2)^2 & \text{si } t \in \mathscr{O}_K = \mathrm{B}_K(0,-1), \\ 0 & \text{sinon.} \end{cases}$$

est une famille de fonctions étagées h-intégrables. Pour tout $(0,p)$-corps K et tout réel $q > 1$, le domaine de la fonction $\vartheta_q(\varphi(\cdot,K))$ est

$$\begin{cases} \{\mathscr{O}_K\} & \text{si } q \neq 2, \\ \emptyset & \text{sinon} \end{cases}$$

et sa q-intégrale vaut

$$\mathrm{I}_q(\vartheta_q(\varphi(\cdot,K))) = q^{-1}(q-2)^2.$$

On a envie de dire que l'intégrale de la fonction φ par rapport à la sous-assignation h est la fonction constante $\mathbb{L}^{-1}(\mathbb{L}-2)^2$.

On définit maintenant l'intégrale par rapport à des variables du corps valué K. Pour une seule variable, la condition « étagée » va nous permettre de nous ramener à intégrer une autre fonction sur le groupe des valeurs.

LEMME 2.33. Soit $\varphi \in \mathscr{P}_+(X[1,0,0])$ une famille de fonctions étagées X-intégrables. Alors il existe une unique fonction $\psi \in \mathscr{P}_+(X)$ telle que, pour tout point $(x,K) \in |X|$ et tout réel $q > 1$, on ait

$$\vartheta_q(\psi(x,K)) = \mathrm{I}_q(\vartheta_q(\varphi(x,\cdot,K))).$$

La fonction $\mu_X(\varphi) \coloneqq \psi$ est l'*intégrale de la fonction φ sur les fibres de la projection* $X[1,0,0] \longrightarrow X$.

Preuve Soit $(x,K) \in |X|$. Notons $S_{x,K}$ le domaine « commun », comme dans la définition, des fonctions $\vartheta_q(\varphi(x,\cdot,K))$ avec $q > 1$. Pour un entier $z \in \mathbf{Z}$, on pose

$$\varphi_0(x,z,K) \coloneqq \begin{cases} \mathbb{L}^{-z}\varphi(x,t,K) & \text{s'il existe une boule } \mathrm{B}_K(t,z) \text{ dans } S_{x,K}, \\ 0 & \text{sinon.} \end{cases}$$

Avec la condition (2.11), cette fonction $z \in \mathbf{Z} \longmapsto \varphi_0(x,z,K) \in \mathbb{A}$ est bien définie. Par ailleurs, la fonction φ_0 appartient à $\mathscr{P}_+(X[0,0,1])$: en effet, elle est bien définissable puisqu'un domaine peut-être retrouvé par le biais d'une formule du premier ordre, la notion de fonction constante étant donnée par une telle formule. Ainsi la fonction $\psi \coloneqq \mu_X(\varphi_0)$, comme étant définie dans le théorème 2.21, convient. L'unicité étant évidente, ceci conclut la preuve. □

On admet la preuve du lemme suivant, cette dernière étant technique. Elle utilise la b-minimalité de la théorie et le lemme 2.11.

LEMME 2.34. Soient X une sous-assignation et $Z \coloneqq X[1,0,0]$. On dit qu'une fonction $\varphi \in \mathscr{C}_+(Z)$ est *X-intégrable* s'il existe un entier $m \geqslant 0$ et une fonction $X[0,m,0]$-intégrable $\psi \in \mathscr{P}_+(Z[0,m,0])$, au sens de la définition 2.32, telle que

$$\mu_Z(\psi) = \varphi\,^{\S 10}.$$

§10. Il faut comprendre cette égalité comme dans le lemme 2.31.

Dans ce cas, la fonction

$$\mu_X(\varphi) \coloneqq \mu_X(\mu_{X[0,m,0]}(\psi)) \in \mathscr{C}_+(X)$$

est indépendante du choix de l'entier m et de la fonction ψ. On l'appelle l'*intégrale de la fonction φ sur les fibres de la projection $Z \longrightarrow X$.*

2.3.6. INTÉGRATION GÉNÉRALE

DIMENSION RELATIVE. Pour un morphisme $f\colon X \longrightarrow Y$, la *dimension relative* de X sur Y selon le morphisme f est l'entier

$$\dim_Y X \coloneqq \max_{(y,K)\in|Y|} \big[\dim f_K^{-1}(\{y\})\big].$$

On va définir l'intégrale sur un nombre fini quelconque de variables du corps valué. Pour cela, on procède par récurrence. Soient $n, m, r \geqslant 0$ trois entiers et $\varphi \in \mathscr{C}_+(X[n,m,r])$ une fonction constructible. Lorsque $n = 0$, si la fonction φ est X-intégrable, alors on a déjà défini son intégrale avec le lemme 2.30. Le lemme suivant traite le cas général où l'on suppose $n \geqslant 1$.

LEMME 2.35. Soient X une sous-assignation et $Z \coloneqq X[n,m,r]$. On dit qu'une fonction $\varphi \in \mathscr{C}_+(Z)$ est *X-intégrable* s'il existe une sous-assignation $Z' \subset Z$ et une permutation des n premières coordonnées telles que

- on ait $\dim_X(Z \setminus Z') < n$ où l'on a considéré la projection $Z \setminus Z' \longrightarrow X$;
- la fonction $\varphi' \coloneqq \mathbb{1}_{Z'}\varphi$ soit $X[n-1,m,r]$-intégrable au sens du lemme 2.34 ;
- la fonction $\mu_{X[n-1,m,r]}(\varphi') \in \mathscr{C}_+(X[n-1,m,r])$ soit X-intégrable où l'on vérifie les hypothèses de ce lemme au rang $n-1$.

Alors la fonction

$$\mu_X(\varphi) \coloneqq \mu_X(\mu_{X[n-1,m,r]}(\varphi')) \in \mathscr{C}_+(X)$$

est indépendante de la sous-assignation Z'. On l'appelle l'*intégrale de la fonction φ sur les fibres de la projection $Z \longrightarrow X$.*

On admet la preuve et on renvoie le lecteur au papier [9, Lemma-Definition 9.1] qui utilise le fait que la théorie des $(0,p)$-corps est jacobienne et b-minimale. Finalement, on est en mesure de définir l'intégrale motivique d'une fonction quelconque du semi-anneau $\mathscr{C}_+(Z)$.

DÉFINITION 2.36. Soit $Z \subset X[n,m,r]$ une sous-assignation. Une fonction $\varphi \in \mathscr{C}_+(Z)$ est *X-intégrable* si son extension par zéro en une fonction $\tilde{\varphi} \in \mathscr{C}_+(X[n,m,r])$ est X-intégrable. Dans ce cas, son intégrale sur les fibres de la projection $Z \longrightarrow X$ est la fonction

$$\mu_X(\varphi) \coloneqq \mu_X(\tilde{\varphi}) \in \mathscr{C}_+(X).$$

Lorsque $X = h[0,0,0]$, la fonction μ_X sera simplement notée μ et la fonction $\mu(\varphi)$ est l'intégrale de la fonction φ sur Z.

Annexe A

La théorie des corps réels clos

Dans la suite, on va introduire la notion de corps réels clos et notre but sera de montrer que cette théorie élimine les quantificateurs. Le théorème de Tarski-Seidenberg, découlant du théorème de Sturm, va nous permettre d'établir ce résultat.

A.1. Le théorème de Sturm

Soit $P \in \mathbf{R}[X]$ un polynôme réel. En effectuant l'algorithme d'Euclide dans $\mathbf{R}[X]$, il existe une suite finie $(P_1, \dots, P_k)$ de $\mathbf{R}[X]$ telle que

- on ait $P_0 = P$ et $P_1 = P'$;
- pour $i \in [\![2, k]\!]$, le polynôme P_i soit l'*opposé* du reste de la division euclidienne de P_{i-2} par P_{i-1} ;
- le dernier polynôme P_k ne soit pas nul.

Définition A.1. La *suite de Sturm* associée au polynôme P est cette suite finie $(P_0, \dots, P_k)$.

Exemple. Considérons le polynôme $P := (X-1)(X-2)(X-3)$. Alors sa suite de Sturm est constituée des polynômes

$$\begin{aligned} P_0 &= X^3 - 6X^2 + 11X - 6, \\ P_1 &= 2X^2 - 12X + 11, \\ P_2 &= \tfrac{2}{3}X - \tfrac{4}{3}, \\ P_3 &= 1. \end{aligned}$$

Définition A.2. Soit $a \in \mathbf{R}$ un réel tel que $P(a) \neq 0$. Le nombre de changements de signe dans la suite $(P_0(a), \dots, P_k(a))$ est l'entier

$$\mathfrak{s}_P(a) := \sharp \{ i \in [\![1, k]\!] \mid P_{i-1}(a) P_i(a) < 0 \}.$$

Exemple. Reprenons l'exemple précédent. On a $\mathfrak{s}_P(-1) = 3$ et $\mathfrak{s}_P(4) = 0$ puisque

$$\begin{aligned} (P_0(-1), P_1(-1), P_2(-1), P_3(-1)) &= (-24, 26, -2, 1), \\ (P_0(4), P_1(4), P_2(4), P_3(4)) &= (6, 11, 4/3, 1). \end{aligned}$$

Dans la suite, on va étudier les variations de la fonction $\mathfrak{s}_P \colon \mathbf{R} \setminus R \longrightarrow \mathbf{N}$ où on a noté R l'ensemble des racines réelles de P.

Lemme A.3. Soient $P \in \mathbf{R}[X]$ un polynôme réel sans racine réelle multiple et $a, b \in \mathbf{R}$ deux réels qui ne sont pas des racines de P tels que $a < b$. Alors le nombre de racines réelles de P sur $[a, b]$ vaut

$$\mathfrak{s}_P(b) - \mathfrak{s}_P(a).$$

Preuve Tout d'abord, regardons le comportement des signes des termes $P_0(x)$ et $P_1(x)$ lorsque x passe par une racine $r \in \mathbf{R}$ de $P_0 = P$. Comme P n'a pas de racine multiple, on a $P_1(r) = P'(r) \neq 0$. Au voisinage de r, la fonction P' garde donc un signe constant ce qui induit un changement de signe pour la fonction P. Ainsi les fonctions P_0 et P_1 sont de signe opposé avec le passage en r et de signe identique après. On est alors dans une des situations représentées par les tableaux suivants.

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_0(x) & - & 0 & + \\ \operatorname{sgn} P_1(x) & + & + & + \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_0(x) & + & 0 & - \\ \operatorname{sgn} P_1(x) & - & - & - \end{array}$$

Soit $i \in [\![1, k-1]\!]$. Faisons de même avec les termes $P_{i-1}(x)$, $P_i(x)$ et $P_{i+1}(x)$ lorsque x passe par une racine $r \in \mathbf{R}$ de P_i. Comme $P_i(r) = 0$, on a nécessairement $P_{i-1}(r) \neq 0$ et $P_{i+1}(r) \neq 0$ car sinon, en remontant l'algorithme d'Euclide, comme $P_{i-1}(r) = P_i(r) = 0$, on obtiendrai $P_0(r) = P_1(r) = 0$ ce qui est impossible car, le polynôme P n'admettant aucune racine multiple, les polynômes $P_0 = P$ et $P_1 = P'$ sont premiers entre eux. De plus, on peut écrire $P_{i-1} = P_i Q_i - P_{i+1}$ avec $Q_i \in \mathbf{R}[X]$, donc $P_{i-1}(r) = -P_{i+1}(r)$. Ceci implique qu'au voisinage de r, les signes des fonctions P_{i-1} et P_{i+1} sont opposés. En conclusion, on se trouve dans un des cas suivants.

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_{i-1}(x) & + & + & + \\ \operatorname{sgn} P_i(x) & \star & 0 & \star \\ \operatorname{sgn} P_{i+1}(x) & - & - & - \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P_{i-1}(x) & - & - & - \\ \operatorname{sgn} P_i(x) & \star & 0 & \star \\ \operatorname{sgn} P_{i+1}(x) & + & + & + \end{array}$$

On a ainsi traité tous les cas intéressants puisqu'au voisinage d'un réel qui n'est racine d'aucun polynôme P_i, la fonction $\mathfrak{s}_P$ est clairement constante. Finalement, la fonction $\mathfrak{s}_P$ ne varie qu'au voisinage d'une racine de P et elle y diminue d'une unité. Ceci assure le résultat du lemme. □

EXEMPLE. En reprenant l'exemple précédent, le polynôme P admet $\mathfrak{s}_P(-1) - \mathfrak{s}_P(4) = 3 - 0 = 3$ racines sur le segment $[-1, 4]$.

THÉORÈME A.4 *(Sturm).* Soient $P \in \mathbf{R}[X]$ un polynôme réel et $a, b \in \mathbf{R}$ deux réels qui ne sont pas des racines de P tels que $a < b$. Alors le nombre de racines réelles de P sur $[a, b]$ vaut

$$\mathfrak{s}_P(b) - \mathfrak{s}_P(a).$$

Preuve Le polynôme P_k divise tous les autres polynômes P_i et, puisque $P_k = \operatorname{pgcd}(P, P')$, les polynômes P_0 et P_0/P_k ont les mêmes racines et ce dernier n'admet aucune racine réelle multiple. D'après le lemme, l'entier $\mathfrak{s}_{P_0/P_k}(a) - \mathfrak{s}_{P_0/P_k}(b)$ est le nombre de racines réelles de P_0/P_k sur $[a, b]$, *i. e.* le nombre de racines réelles de P sur $[a, b]$. Mais comme le nombre de changements de signe de la suite

$$(P_0(a)/P_k(a), \ldots, P_{k-1}(a)/P_k(a), 1)$$

est égal à celui de la suite $(P_0(a), \ldots, P_1(a))$, on conclut le théorème de Sturm. □

COROLLAIRE A.5. Soit $P \in \mathbf{R}[X]$. On note $\mathfrak{s}_P(+\infty)$ et $\mathfrak{s}_P(-\infty)$ le nombre de changements de signe dans les suites des coefficients dominants des suites

$$(P_0(X), \ldots, P_k(X)) \quad \text{et} \quad (P_0(-X), \ldots, P_k(-X)).$$

Alors le nombre de racines réelles de P vaut $\mathfrak{s}_P(-\infty) - \mathfrak{s}_P(+\infty)$.

Preuve Comme la fonction $\mathfrak{s}_P$ ne varie qu'au voisinage d'une racine de P et le polynôme P n'admet qu'un nombre fini de racines, il existe un réel $a \in \mathbf{R}$ tel que la fonction $\mathfrak{s}_P$ soit constante sur $]-\infty, a[$. De même, on peut trouver un réel $b > a$ tels qu'elle soit constante sur $]b, +\infty[$. Par le théorème de Sturm, la quantité $\mathfrak{s}_P(b) - \mathfrak{s}_P(a)$ comptant le nombre de racines réelles de P sur $[a, b]$, elle compte le nombre de racines réelles de P sur $\mathbf{R}$. Quitte à choisir des réels a et b plus grand ou plus petit, on peut supposer que le signe des polynômes P_i ne change plus sur $]-\infty, a]$ et $[b, +\infty[$. Dans ce cas, pour tout $i \in [\![1, k]\!]$, le signe du polynôme P_i sur $]-\infty, a]$ (respectivement sur $[b, +\infty[$) est celui du coefficient dominant du polynôme $P_i(-X)$ (respectivement $P_i(X)$). Par conséquent, on obtient

$$\mathfrak{s}_P(a) = \mathfrak{s}_P(-\infty) \quad \text{et} \quad \mathfrak{s}_P(b) = \mathfrak{s}_P(+\infty)$$

ce qui conclut. □

A.2. Le théorème de Tarski-Seidenberg

A.2.1. Le cas d'un système simple

Théorème A.6. Soient $P, Q \in \mathbf{R}[X]$ et $a, b \in \mathbf{R}$ deux réels qui ne sont pas des racines de P tels que $a < b$. On note $p \in \mathbf{N}$ le nombre de solutions sur $[a, b]$ du système

$$\begin{cases} P(x) = 0, \\ Q(x) > 0 \end{cases}$$

et on note $n \in \mathbf{N}$ le nombre de solutions sur $[a, b]$ du système

$$\begin{cases} P(x) = 0, \\ Q(x) < 0. \end{cases}$$

On note $(P_1, \dots, P_k)$ la suite de Sturm avec $P_0 = P$ et $P_1 = P'Q$ et, pour $a \in \mathbf{R}$, on note $\mathfrak{s}_{P,Q}(a)$ le nombre de changements de signe dans la suite $(P_0(a), \dots, P_k(a))$. Alors

$$\begin{aligned} p - n &= \mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b), \\ p &= \tfrac{1}{2}[\mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b) + \mathfrak{s}_{P,Q^2}(a) - \mathfrak{s}_{P,Q^2}(b)]. \end{aligned}$$

De plus, les mêmes relations sont valables en remplaçant le couple (a, b) par le couple $(-\infty, +\infty)$.

Preuve On va étudier les variations de la fonction $\mathfrak{s}_{P,Q}$ au voisinage d'une racine $r \in \mathbf{R}$ de P.

• *Première égalité.* Dans un premier temps, on suppose que les polynômes P et $P'Q$ sont premiers entre eux. Soit $r \in \mathbf{R}$ une racine de P. Alors ce n'est ni une racine de P' ni de Q, donc le signe du polynôme $P_1 = P'Q$ est constant au voisinage de r. Cela implique que le signe du polynôme $P_0 = P$ change nécessairement. Ainsi lorsque $Q > 0$ au voisinage de r, on est dans un des deux cas

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & - & 0 & + \\ \operatorname{sgn} P'(x) & + & + & + \\ \operatorname{sgn} P'Q(x) & + & + & + \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & + & 0 & - \\ \operatorname{sgn} P'(x) & - & - & - \\ \operatorname{sgn} P'Q(x) & - & - & - \end{array}$$

et lorsque $Q < 0$ au voisinage de r, on est dans les deux autres cas

$$\begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & - & 0 & + \\ \operatorname{sgn} P'(x) & + & + & + \\ \operatorname{sgn} P'Q(x) & - & - & - \end{array} \qquad \begin{array}{l|ccc} x & & r & \\ \operatorname{sgn} P(x) & + & 0 & - \\ \operatorname{sgn} P'(x) & - & - & - \\ \operatorname{sgn} P'Q(x) & + & + & + \end{array}$$

Maintenant, soit $r \in \mathbf{R}$ une racine d'une polynôme P_i. Comme dans la preuve du lemme A.3 et grâce à l'hypothèse, le nombre de changements de signe dans la suite $(P_{i-1}(x), P_i(x), P_{i+1}(x))$ est constant au voisinage de r.

En conclusion, la fonction $\mathfrak{s}_{P,Q}$ ne varie qu'au voisinage des racines de P et

– décroît d'une unité pour une racine $r \in \mathbf{R}$ de P telle que $Q(r) > 0$;
– croît d'une unité pour une racine $r \in \mathbf{R}$ de P telle que $Q(r) < 0$;

On peut alors conclure la première égalité

$$p - n = \mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b).$$

Dans le cas où les polynômes P et $P'Q$ ne sont pas premiers entre eux, on procède de la même façon que pour la preuve du théorème de Sturm.

• *Seconde égalité.* D'après ce qui précède, remarquons que la quantité $\mathfrak{s}_{P,Q^2}(a) - \mathfrak{s}_{P,Q^2}(b)$ correspond au nombre $n + p$ de racines de P sur $[a, b]$ qui ne sont pas des racines de Q sur $[a, b]$. En trouvant une bonne combinaison linéaire, on trouve finalement

$$p = \tfrac{1}{2}[\mathfrak{s}_{P,Q}(a) - \mathfrak{s}_{P,Q}(b) + \mathfrak{s}_{P,Q^2}(a) - \mathfrak{s}_{P,Q^2}(b)].$$

Pour finir, les égalités avec $\pm\infty$ se montre comme dans le corollaire A.5. $\square$

A.2.2. Un procédé algorithmique pour des systèmes plus généraux

On va trouver une procédure qui permet déterminer si un système d'équations et d'inéquations polynomiales admet des solutions. Soient $R_1, \dots, R_m, Q_1, \dots, Q_\ell \in \mathbf{R}[X]$. On considère le système

$$\begin{cases} R_i(x) = 0, & i \in [\![1, m]\!], \\ Q_j(x) \diamond_j 0, & j \in [\![1, \ell]\!] \end{cases} \tag{S}$$

d'inconnue $x \in \mathbf{R}$ où chaque symbole $\diamond_j$ est un des quatre relations $<$, $\leqslant$, $>$ et $\geqslant$.

Tout d'abord, montrons que l'on peut se ramener au cas $m = 1$ et où les symboles $\diamond_j$ sont $>$. Quitte à remplacer les polynômes Q_j par $-Q_j$, on peut supposer que les symboles $\diamond_j$ sont $>$ ou $\geqslant$. Lorsque $\geqslant$ apparaît, il suffit de remarquer que, pour tout $x \in \mathbf{R}$, l'inégalité $Q_j(x) \geqslant 0$ équivaut à une des égalités $Q_j(x) = 0$ et $Q_j(x) > 0$ de sorte que décider si l'inéquation $Q_j(x) \geqslant 0$ admet des solutions revient à décider si l'inéquation $Q_j(x) > 0$ ou l'équation $Q_j(x) = 0$ admet des solutions. On peut donc se ramener dans le cas où les symboles $\diamond_j$ sont $>$. Enfin, quitte à remplacer les premières équations par l'équation $R_1^2(x) + \cdots + R_m^2(x) = 0$ si $m > 0$ ou l'équation $0 = 0$ si $m = 0$, on peut supposer $m = 1$.

Soit $P \in \mathbf{R}[X]$. Finalement, on est ramené à étudier l'existence de solutions au système

$$\begin{cases} P(x) = 0, \\ Q_j(x) > 0, & j \in [\![1, \ell]\!]. \end{cases} \tag{Σ}$$

Soit $\mu := (\mu_1, \dots, \mu_\ell) \in \{0, 1\}^\ell$ un ℓ-uplet. On pose

$$s^\mu := \mathfrak{s}_{P,Q^\mu}(-\infty) - \mathfrak{s}_{P,Q^\mu}(+\infty) \quad \text{avec} \quad Q^\mu := Q_1^{2-\mu_1} \cdots Q_\ell^{2-\mu_\ell}.$$

D'après le théorème A.6, on sait calculer cette quantité s^μ et il s'agit du nombre de solutions réelles du système

$$\begin{cases} P = 0, \\ Q^\mu > 0 \end{cases}$$

moins le nombre de solutions réelles du système

$$\begin{cases} P = 0, \\ Q^\mu < 0 \end{cases}.$$

En raisonnant par récurrence sur l'entier $\ell \in \mathbf{N}^*$, on va trouver une formule donnant le nombre de solutions σ^μ du système

$$\begin{cases} P(x) = 0, \\ (-1)^{\mu_j} Q_j(x) > 0, & j \in [\![1, \ell]\!]. \end{cases} \tag{Σ^μ}$$

pour $\mu \in \{0, 1\}^\ell$ en fonction des quantités s^λ avec $\lambda \in \{0, 1\}^\ell$. Une fois cette formule obtenue, on pourra calculer la quantité $\sigma^{(0,\dots,0)}$ qui nous intéresse.

Effectuons alors cette récurrence. On commence par le cas $\ell = 1$. Dans la suite, on note $R \subset \mathbf{R}$ l'ensemble des racines réelles de P. Alors on peut écrire

$$\begin{aligned} s^0 &= \sharp\{r \in R \mid Q_1^2(r) > 0\} - \sharp\{r \in R \mid Q_1^2(r) < 0\} = \sharp\{r \in R \mid Q_1(r) \neq 0\}, \\ s^1 &= \sharp\{r \in R \mid Q_1(r) > 0\} - \sharp\{r \in R \mid Q_1(r) < 0\}, \\ \sigma^0 &= \sharp\{r \in R \mid Q_1(r) > 0\}, \\ \sigma^1 &= \sharp\{r \in R \mid Q_1(r) < 0\}. \end{aligned}$$

On obtient donc $s^0 = \sigma^0 + \sigma^1$ et $s^1 = \sigma^0 - \sigma^1$. Matriciellement, cela s'écrit

$$\begin{pmatrix} s^0 \\ s^1 \end{pmatrix} = A_1 \begin{pmatrix} \sigma^0 \\ \sigma^1 \end{pmatrix} \quad \text{avec} \quad A_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}).$$

Ainsi les quantités σ_0 et σ^1 s'expriment linéairement en fonction de s^0 et s^1.

Pour illustrer, traitons le cas $\ell = 2$ avant de faire l'hérédité. Bien que les calculs soient lourds, cela nous donne une piste pour la suite. De même, on peut écrire les égalités

$$s^{(0,0)} = \sharp\{r \in R \mid Q_1^2(r) Q_2^2(r) > 0\} - \sharp\{r \in R \mid Q_1^2(r) Q_2^2(r) < 0\}$$

$$
\begin{aligned}
&= \sharp\{r \in R \mid Q_1(r)Q_2(r) \neq 0\},\\
s^{(0,1)} &= \sharp\{r \in R \mid Q_1^2(r)Q_2(r) > 0\} - \sharp\{r \in R \mid Q_1^2(r)Q_2(r) < 0\}\\
&= \sharp\{r \in R \mid Q_1(r) \neq 0, Q_2(r) > 0\} - \sharp\{r \in R \mid Q_1(r) \neq 0, Q_2(r) < 0\},\\
s^{(1,0)} &= \sharp\{r \in R \mid Q_1(r) > 0, Q_2(r) \neq 0\} - \sharp\{r \in R \mid Q_1(r) < 0, Q_2(r) \neq 0\},\\
s^{(1,1)} &= \sharp\{r \in R \mid Q_1(r)Q_2(r) > 0\} - \sharp\{r \in R \mid Q_1(r)Q_2(r) < 0\},\\
\sigma^{(0,0)} &= \sharp\{r \in R \mid Q_1(r) > 0, Q_2(r) > 0\},\\
\sigma^{(0,1)} &= \sharp\{r \in R \mid Q_1(r) > 0, Q_2(r) < 0\},\\
\sigma^{(1,0)} &= \sharp\{r \in R \mid Q_1(r) < 0, Q_2(r) > 0\},\\
\sigma^{(0,1)} &= \sharp\{r \in R \mid Q_1(r) < 0, Q_2(r) < 0\}.
\end{aligned}
$$

On obtient alors

$$
\begin{pmatrix} s^{(0,0)} \\ s^{(0,1)} \\ s^{(1,0)} \\ s^{(1,1)} \end{pmatrix} = A_2 \begin{pmatrix} \sigma^{(0,0)} \\ \sigma^{(0,1)} \\ \sigma^{(1,0)} \\ \sigma^{(1,1)} \end{pmatrix} \quad \text{avec} \quad A_2 \coloneqq \begin{pmatrix} A_1 & A_1 \\ A_1 & -A_1 \end{pmatrix} \in \mathrm{GL}_4(\mathbf{Z}).
$$

Passons maintenant à l'hérédité. Soit $\ell \geqslant 2$. On suppose qu'il existe une matrice $A \in \mathrm{GL}_{2^\ell}(\mathbf{Z})$ telle que $(s^\mu)_{\mu \in \{0,1\}^\ell} = A_\ell (\sigma^\mu)_{\mu \in \{0,1\}^\ell}$ où l'on range les éléments de $\{0,1\}^\ell$ par ordre lexicographique. Pour trouver une telle matrice au rang $\ell + 1$, il suffit de poser

$$
A_{\ell+1} \coloneqq \begin{pmatrix} A_\ell & A_\ell \\ A_\ell & -A_\ell \end{pmatrix} \in \mathrm{GL}_{2^{\ell+1}}(\mathbf{Z})
$$

dont l'inverse est

$$
A_{\ell+1}^{-1} = \frac{1}{2} \begin{pmatrix} A_\ell^{-1} & A_\ell^{-1} \\ A_\ell^{-1} & -A_\ell^{-1} \end{pmatrix}.
$$

Ceci termine la récurrence. En conclusion, les quantités σ^μ se calculent linéairement en fonction des quantités s^μ et on peut donc trouver la quantité $\sigma^{(0,\dots,0)}$. Finalement, on a trouvé un procédé calculatoire permettant de savoir si un système de la forme (Σ) admet des solutions et, dans le cas où il admet un nombre fini de solutions, de calculer ce nombre.

A.2.3. Le théorème de Tarski-Seidenberg

On peut à présent passer à la preuve du théorème de Tarski-Seidenberg. De celui-ci, on va pouvoir déduire deux résultats très importants qui concluront notre annexe.

Théorème A.7 *(Tarski-Seidenberg)*. Soient $n, m \in \mathbf{N}^*$ des entiers, $S_1, \dots, S_m \in \mathbf{R}[T_1, \dots, T_n, X]$ des polynômes réels à $n+1$ variables et $\diamond_1, \dots, \diamond_n \in \{>, =\}$ des symboles. Alors il existe des systèmes d'équations et d'inéquations polynomiales $R_1(T)$, …, $R_k(T)$ d'inconnue $T \coloneqq (T_1, \dots, T_n)$ tels que, pour tout vecteur $t \in \mathbf{R}^n$, on ait l'équivalence

$$
(\exists x \in \mathbf{R},\ \forall j \in [\![1, m]\!],\quad S_i(t, x) \diamond_i 0) \quad\Longleftrightarrow\quad R_1(t) \vee \dots \vee R_k(t).
$$

Preuve En appliquant la procédure calculatoire du dernier paragraphe, on peut se ramener à un système simple comme dans le théorème A.6. On calcule alors toutes les suites de Sturm et les quantités $\mathfrak{s}_{P,Q}(-\infty) - \mathfrak{s}_{P,Q}(+\infty)$ nécessaires pour décider, si ce système admet des solutions. Ce calcul se fait dans l'anneau $\mathbf{R}(T)[X]$: en distinguant selon les signes des coefficients dominants de ces dernières quantité, on va pouvoir affirmer l'existence ou non d'une solution, produisant ainsi, quitte à multiplier par leurs dénominateurs, des systèmes d'équations et d'inéquations polynomiales. □

Exemple. On va donner un exemple, permettant de clarifier la preuve. Soient $t_1, t_2, t_3 \in \mathbf{R}$ trois réels. On considère l'équation

$$
t_1 x^2 + t_2 x + t_3 = 0 \tag{E}
$$

d'inconnue $x \in \mathbf{R}$. Cette équation est bien connue et on peut directement donner une condition sur les réels t_i pour que celle-ci admette une solution. Cependant, utilisons notre procédé pour retrouver le résultat. Pour cela, on pose

$$P_0 \coloneqq t_1 X^2 + t_2 X + t_3 \in \mathbf{R}[X].$$

• *Premier cas.* On suppose $t_1 \neq 0$. Alors la suite de Sturm associée au polynôme P_0 est la suite donnée par les deux autres polynômes

$$P_1 \coloneqq \frac{\mathrm{d}P}{\mathrm{d}X} = 2t_1 X + t_2 \quad \text{et} \quad P_2 \coloneqq \frac{t_2^2 - 4t_1 t_3}{4t_1}.$$

Dans un premier temps, on suppose $P_2 \neq 0$. Pour connaître si l'équation (E) admet des solutions, on étudie le signe de la quantité $\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty)$ en fonction des signes des termes t_1 et $t_2^2 - 4t_1 t_3$. On obtient les tableaux suivants[§1] avec $\Delta = t_2^2 - 4t_1 t_3$.

$\operatorname{sgn}(\Delta)$	$+$	$-$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_0(-X))] = \operatorname{sgn}(t_1)$	$+$	$+$	$-$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(-X))] = \operatorname{sgn}(-2t_1)$	$-$	$-$	$+$	$+$
$\operatorname{sgn}[\operatorname{cd}(P_2(-X))] = \operatorname{sgn}(\Delta/4t_1)$	$+$	$-$	$-$	$+$
$\mathfrak{s}_{P_0}(-\infty)$	2	1	2	1

$\operatorname{sgn}(\Delta)$	$+$	$-$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_0(+X))] = \operatorname{sgn}(t_1)$	$+$	$+$	$-$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(+X))] = \operatorname{sgn}(2t_1)$	$+$	$+$	$-$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_2(+X))] = \operatorname{sgn}(\Delta/4t_1)$	$+$	$-$	$-$	$+$
$\mathfrak{s}_{P_0}(+\infty)$	0	1	0	1

On remarque alors que

$$\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty) > 0 \iff t_2^2 - 4t_1 t_3 > 0.$$

Donc l'équation (E) admet des solutions si et seulement si $t_2^2 - 4t_1 t_3 > 0$.

Dans un second temps, on suppose $P_2 = 0$. La suite de Sturm est donnée par les polynômes P_0 et P_1 et on obtient les tableaux suivants.

$\operatorname{sgn}[\operatorname{cd}(P_0(-X))] = \operatorname{sgn}(t_1)$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(-X))] = \operatorname{sgn}(-2t_1)$	$-$	$+$
$\mathfrak{s}_{P_0}(-\infty)$	1	1

$\operatorname{sgn}[\operatorname{cd}(P_0(+X))] = \operatorname{sgn}(t_1)$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(+X))] = \operatorname{sgn}(2t_1)$	$+$	$-$
$\mathfrak{s}_{P_0}(+\infty)$	0	0

Dans tous les cas, on a $\mathfrak{s}_{P_0}(-\infty) - \mathfrak{s}_{P_0}(+\infty) = 1 > 0$, donc l'équation (E) admet des solutions.

• *Second cas.* On suppose désormais $t_1 = 0$. Alors la suite de Sturm est donnée par les polynômes

$$P_0 = t_2 X + t_3 \quad \text{et} \quad P_1 \coloneqq t_2.$$

Dans un premier temps, on suppose $t_2 \neq 0$. On obtient les tableaux suivants.

$\operatorname{sgn}[\operatorname{cd}(P_0(-X))] = \operatorname{sgn}(-t_2)$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(-X))] = \operatorname{sgn}(t_2)$	$-$	$+$
$\mathfrak{s}_{P_0}(-\infty)$	1	1

$\operatorname{sgn}[\operatorname{cd}(P_0(+X))] = \operatorname{sgn}(t_2)$	$+$	$-$
$\operatorname{sgn}[\operatorname{cd}(P_1(+X))] = \operatorname{sgn}(t_2)$	$+$	$-$
$\mathfrak{s}_{P_0}(+\infty)$	0	0

De même, on conclut que l'équation (E) admet des solutions.

Dans un second temps, on suppose $t_2 = 0$ et il est évident que l'équation (E) admet des solutions si et seulement si $t_3 = 0$.

• *Conclusion.* Notre disjonction a amené à traiter tous les cas. Finalement, l'équation (E) admet des solutions si et seulement si

$$(t_1 \neq 0 \wedge t_2^2 - 4t_1 t_2 > 0) \vee (t_1 = 0 \wedge t_2 \neq 0) \vee (t_1 = 0 \wedge t_2 = 0 \wedge t_3 = 0).$$

On retrouve le résultat qu'on connaît sur les racines réelles d'un polynôme réel de degré deux.

Corollaire A.8 *(Tarski-Seidenberg, forme projetée).* Soit $A \subset \mathbf{R}^{n+1}$ un ensemble semi-algébrique. On note $p\colon \mathbf{R}^{n+1} \twoheadrightarrow \mathbf{R}^n$ la projection sur les n premières coordonnées. Alors l'image $p(A) \subset \mathbf{R}^n$ est un ensemble semi-algébrique de $\mathbf{R}^n$.

Preuve C'est une conséquence immédiate du théorème de Tarski-Seidenberg. □

Corollaire A.9 *(Tarski-Seidenberg, forme logique).* Dans le langage des corps ordonnés, les ensembles **R**-définissables sont **R**-constructibles, *i. e.* le $\mathscr{L}_{\mathrm{ord}}$-théorie de l'ensemble **R** élimine les quantificateurs.

§1. La notation $\operatorname{cd}(P)$ désigne le coefficient dominant d'un polynôme $P \in \mathbf{R}[X]$.

Preuve On considère une $\mathscr{L}_{\text{ord}}$-formule $\Psi(x_1, \dots, x_n)$ de la forme

$$\Box_1 x_{n+1} \cdots \Box_m x_{n+m} \ \Phi(x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m})$$

où la formule Φ n'a pas de quantificateur et les symboles $\Box_j$ sont des quantificateurs $\forall$ ou $\exists$. Quitte à prendre la négation de cette formule, on peut supposer $\Box_1 = \exists$. Le théorème de Tarski-Seidenberg assure alors que cette formule est équivalente, dans $\mathbf{R}$, à une formule de la forme

$$\Box'_2 x_{n+2} \cdots \Box'_m x_{n+m} \ \Phi'(x_1, \dots, x_n, x_{n+2}, \dots, x_{n+m})$$

où la formule Φ' n'a pas de quantificateur et les symboles $\Box'_j$ sont des quantificateurs $\forall$ et $\exists$. Ainsi on procède par récurrence sur le nombre m de variables quantifiés dans la formule Ψ et cette dernière est donc équivalente à une formule sans quantificateur. Ceci termine la preuve. $\Box$

A.3. Les corps réels clos

Définition A.10. Un *corps réels clos* est un corps R muni d'une relation totale $<$ qui vérifie
- les axiomes des corps ordonnés :
  - pour tous $x, y, z \in R$, si $x < y$, alors $x + z < y + z$;
  - pour tous $x, y, z \in R$, si $x < y$ et $0 < z$, alors $xz < yz$;
- les axiomes des corps réels clos :
  - pour tout $x \in R$, si $x > 0$, alors il existe $y \in R$ tel que $x = y^2$;
  - pour tous $n \in \mathbf{N}$ et $x_0, \dots, x_{2n+1} \in R$, il existe $y \in R$ tel que $y^{2n+1} + x_{2n}y^{2n} + \cdots + x_0 = 0$.

On note CRC la $\mathscr{L}_{\text{ord}}$-théorie des corps réels clos.

Exemples. Le corps $\mathbf{R}$ est réel clos. Les corps des réels algébriques sur $\mathbf{C}$ en est également un.

Théorème A.11. Le théorie des corps réels clos est modèle-complète et élimine les quantificateurs.

Preuve Le fait qu'elle élimine les quantificateurs provient du théorème de Tarski-Seidenberg qui reste vrai pour des corps réels clos. Par conséquent, elle est modèle-complète. $\Box$

Lemme A.12. 1. Un corps ordonné est de caractéristique nulle.
2. Tout corps de caractéristique nulle contient une copie de $\mathbf{Q}$.

Preuve 1. Soit k un corps ordonné. Dans un premier temps, on suppose $0 < 1$. Alors l'unique morphisme $\varphi \colon \mathbf{Z} \longrightarrow k$ est croissant. Raisonnons par l'absurde et supposons que le corps k est de caractéristique $p > 0$. Alors $0 = \varphi(0) < \varphi(p) = 0$, donc $\varphi(p-1) = 0$ avec $p > p - 1 > 0$ ce qui est impossible. Le corps étant totalement ordonné, l'autre cas est lorsque $1 < 0$ qui se traite de la même manière.
2. Soit k un corps de caractéristique nulle. Alors l'unique morphisme $\mathbf{Z} \longrightarrow k$ est injectif, donc le corps k contient une copie de $\mathbf{Z}$. Comme k est un corps, il contient une copie de $\operatorname{Frac} \mathbf{Z} = \mathbf{Q}$. $\Box$

Théorème A.13 *(principe de transfert de Tarski).* Soit $\mathfrak{A}$ une $\mathscr{L}_{\text{ord}}$-structure d'univers A. Alors l'ensemble $(A, <)$ est un corps réel clos si et seulement si la structure $\mathfrak{A}$ est élémentairement équivalente à la structure $\mathbf{R}$.

Preuve Si $\mathfrak{A}$ et $\mathbf{R}$ sont élémentaires équivalentes, alors $\mathfrak{A}$ satisfait les mêmes phrases que $\mathbf{R}$ et, en particulier, les axiomes des corps réels clos, donc A est un corps réel clos.

On suppose que $\mathfrak{A}$ est un modèle de la théorie des corps réels clos. Montrons qu'il est élémentairement équivalent à $\mathbf{R}$. Soit φ une $\mathscr{L}_{\text{ord}}$-phrase telle que $\mathfrak{A} \models \varphi$. Montrons que $\mathbf{R} \models \varphi$. Comme la théorie des corps réels clos élimine les quantificateurs, il existe une $\mathscr{L}_{\text{ord}}$-phrase Φ sans quantificateur telle que $\text{CRC} \models (\varphi \longleftrightarrow \Phi)$. Comme $\mathfrak{A} \models \varphi$, on a $\mathfrak{A} \models \Phi$. L'ensemble A étant un corps réel clos, le lemme assure qu'il contient une copie de $\mathbf{Q}$, donc la structure $\mathbf{Q}$ une sous-structure de $\mathfrak{A}$. Mais comme Φ est sans quantificateur, on a $\mathbf{Q} \models \Phi$, donc $\mathbf{R} \models \Phi$. Enfin, comme $\mathbf{R}$ est un corps réel clos, on obtient $\mathbf{R} \models \varphi$. Par symétrie, si $\mathbf{R} \models \varphi$, alors $\mathfrak{A} \models \varphi$. Ceci conclut notre preuve. $\Box$