N° d'ordre : 1915

Université de Rennes I
Institut de recherche mathématique

Thèse de doctorat

Spécialité : mathématiques

Étude modèle-théorique d'anneaux satisfaisant un principe de Hasse non singulier

par

Luck DARNIÈRE

Thèse soutenue le 6 Janvier 1998

Directeur : F. Delon
Co-directeur : L. Moret-Bailly

Rapporteurs : L. van den Dries
A. Prestel

Composition du jury :

M. Coste
F. Delon
A. Macintyre
L. Moret-Bailly
A. Prestel

Remerciements

Je remercie Mme Delon pour m'avoir guidé tout au long de cette thèse en me faisant profiter de son sens mathématique aigu ainsi que de sa vaste culture en théorie des modèles.

M Moret-bailly a assumé le rôle ambigu de co-directeur d'une thèse dans une sous-discipline qui n'était pas la sienne. Il s'est acquitté de cette tâche ingrate en m'ouvrant d'autres horizons mathématiques, avec une gentillesse et une disponibilité qui ont toute ma reconnaissance.

Je tiens également à remercier toute l'équipe de l'institut de recherche mathématique de Rennes, qui m'a accueilli pendant trois ans. J'y ai rencontré des gens formidables, humainement et/ou mathématiquement, à qui je dois pour beaucoup d'aimer de nouveau les maths aujourd'hui. Parmi eux, j'ai une pensée particulière pour Jean-Pierre Escofier, qui a partagé avec moi son bureau mais surtout son experience de mathématicien et d'enseignant, et pour Bas Edixhoven notre directeur d'école doctorale, qui est tout simplement épatant.

Enfin je remercie tout ceux qui, à Rennes ou à Paris, m'ont soutenu de leur sympathie ou de leur amitié, ainsi que Mme Lanneau et Mme Orieux, les plus efficaces et les plus compréhensives des secrétaires !

Sommaire

Abstract

Local-global principles (LGP) like non singular Hasse's principle have interested model-theoretists for a while (pseudo algebraically closed fields (PAC), pseudo real closed fields (PRC), pseudo p-adically closed fields... *etc.*). In this thesis, we introduce a new local-global principle, concerned with integral rings in place of fields. This LGP generalizes the preceding ones, and remains first order in the usual language of rings.

This leads us to study model theoretic properties of PAC, PRC or PC_M rings (these are natural generalisation of the analogous notions for fields). In particular, we give necessary and sufficient conditions for such rings to have a decidable complete theory. As an application, we obtain that the integral closure of the ring of integers in the field of p-adic numbers (resp. of totally p-adic numbers) is decidable. The same result is established for the integral closure of $\mathbb{F}_p[T]$ in any separable closure of its fraction field.

We also give a contribution to algebra, by studying polynomials in $n+1$ variables with coefficients in the integral closure of $\mathbb{Z}$ (resp. $\mathbb{F}_p[T]$) in the algebraic closure of its fraction field. We prove that when given a finite set of such polynomials having a commun zero in A for every value of the first n parameters ranging among A, there exists a polynomial with coefficients in A dividing all the members of this family, wich is monic in the last variable

Introduction

Petit historique

– 1986 : [Ru 86] Rumely démontre que l'anneau $\widetilde{\mathbb{Z}}$ de tous les entiers algébriques satisfait un principe local-global (LGP) analogue au principe de Hasse non singulier. Il en déduit une réponse positive au dixième problème de Hilbert pour $\widetilde{\mathbb{Z}}$: cet anneau a une théorie équationnelle décidable.

– 1988 : [VdD 88] Van den Dries revisite la partie logique du résultat de Rumely, et démontre un théorème d'élimination des quantificateurs pour $\widetilde{\mathbb{Z}}$ qui donne la décidabilité de $\widetilde{\mathbb{Z}}$. Une axiomatisation de cet anneau par des conditions "algébriques" continue cependant à faire défaut.

– 1989 : [MB 89] Moret-Bailly généralise grandement le théorème de Rumely, permettant des investigations comparables à celles de Rumely sur de nombreux anneaux naturels autres que $\widetilde{\mathbb{Z}}$.

– 1990 : [VdD-M], [P-S 90] Van den Dries et Macintyre d'une part, Prestel et Schmid de l'autre, publient indépendamment deux axiomatisations "algébriques" de $\widetilde{\mathbb{Z}}$. Les premiers englobent dans leur étude des anneaux de caractéristique positive (ils utilisent déja le théorème de Moret-Bailly) tandis que les seconds introduisent dans leur article une notion nouvelle de relation radicale. Ils ont en commun de centrer leurs axiomatisations sur des LGP, apparemment assez différents.

– 1991 : [P-S 91] Prestel et Schmid adaptent leur idée de relation radicale et axiomatisent l'anneau $\widetilde{\mathbb{Z}} \cap \mathbb{R}$ des entiers algébriques réels (en recourant eux-aussi au théorème de Moret-Bailly).

– 1992 et au-delà : Ershov publie une série d'articles faisant intervenir un LGP d'anneau. Il n'utilise pas de relation radicale, mais se base sur la notion d'anneau booléen, qu'il a introduite, et dont nous retiendrons qu'elle exclut les anneaux dont le radical de Jacobson est nul, comme $\widetilde{\mathbb{Z}}$ ou $\widetilde{\mathbb{Z}} \cap \mathbb{R}$. Son étude comprend également une remarquable synthèse des LGP classiques de corps, baptisée "clôture régulière relative."

Buts de cette thèse

Les LGP de corps ont une longue histoire en théorie des modèles appliquée à l'algèbre, et la très fameuse thèse de Van den Dries, tout comme l'introduction des corps pseudo réels clos par Prestel, et le détail de leur étude par Ershov, en ont été des tournants. Mais avec les articles cités plus haut, parus depuis 1986, il semble qu'un nouveau type de LGP spécifique aux anneaux soit apparu. Nous avons essayé de dégager un cadre assez vaste pour englober les approches actuelles que nous venons de rappeler, cadre qui pourrait s'intituler, en paraphrasant [VdD-M] : "le contenu modèle-théorique du principe local-global de Moret-Bailly." Le but, en unifiant et généralisant ces approches, était de découvrir par les voies de la théorie des modèles de nouvelles propriétés (logiques ou algébriques) des anneaux qui sont l'objet du théorème de Moret-Bailly.

Vue d'ensemble et résultats

Parmi les candidats naturels à des applications il y avait bien sûr les anneaux déjà étudiés (et notamment $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_p$, dont la décidabilité avait échappé de peu aux tentatives de [P-S 91]) mais aussi des anneaux *a priori* plus "difficiles" comme celui des entiers algébriques absolument p-adiques, voire des analogues en caractéristique positive. Il n'était pas évident d'élaborer une étude théorique dont ils auraient tous été des cas particulier immédiats, et je ne prétends pas y avoir réussi totalement. Il est clair aussi que les applications algébriques, même s'il y en a, restent assez marginales.

D'un autre côté nous avons exhibé un LGP unique, dont tous les autres ne sont que des cas (très) particuliers, et qui pourtant reste axiomatisable au premier ordre (condition essentielle à une utilisation par la théorie des modèles du théorème de Moret-Bailly). De plus les principaux anneaux "naturels" que visait notre étude sont bien au rendez-vous : on retrouve les résultats antérieurs de [VdD-M] et [P-S 91] avec en prime l'axiomatisation de $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_p$, et on démontre la décidabilité de la clôture intégrale de $\mathbb{F}_p[T]$ dans tout corps séparablement clos, ainsi que de divers sur-anneaux des entiers algébriques absolument réels, et (modulo un résultat de Pop encore à confirmer) de l'anneau des entiers algébriques absolument p-adiques.

Revue détaillée

Le premier chapitre présente le principe local-global qui est au coeur de cette thèse, nous le noterons LGPH. Pour cela on commence par présenter une adaptation naturelle au cadre des anneaux de la notion de clôture régulière introduite pour les corps par Ershov. Celle-ci permet d'expliciter la profonde signification logique des LGP, qu'ils soient de corps ou d'anneaux, à l'aide la notion auxiliaire d'anneau géométriquement clos : on appelle ainsi tout anneau intègre A tel que pour toute variété V définie sur le corps des fractions de A et ayant un point lisse à coordonnées dans A, le plongement de A dans $A[V]$ soit existentiellement clos. Il se trouve que tout anneau de valuation hensélien, tout corps valué hensélien, tout corps réel clos ou algébriquement clos est géométriquement clos (§ I.1) et l'on a :

Proposition
Soit A un anneau intègre de corps des fractions K et soit $\mathcal{R}$ une famille d'anneaux inclus dans une clôture algébrique de K et contenant tous A. Si tous les éléments de $\mathcal{R}$ sont géométriquement clos, alors les propriétés suivantes sont équivalentes :

(i) *A est existentiellement clos dans tout anneau intègre B le contenant tel que l'extension $\mathrm{Fr}(B)|\mathrm{Fr}(A)$ soit régulière et que pour tout $R \in \mathcal{R}$ le plongement de R dans $R \otimes_A B$ soit existentiellement clos ;*

(ii) *pour toute variété non vide V définie sur K, et pour tout polynôme g à coefficients dans A n'appartenant pas à $I(V)$, si V possède un point lisse dans tout $R \in \mathcal{R}$,* *alors V possède dans A un point n'annulant pas g.*

On définit alors au § I.2 les anneaux satisfaisant le LGPH. Ce sont les anneaux de Prüfer A tels que toute variété non vide définie sur le corps de fraction de A et ayant un point lisse à coordonnées dans le hensélisé de $A_{\mathfrak{m}}$ pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, possède (en conséquence) un point lisse à coordonnées dans A. Le théorème de Moret-Bailly, rappelé au § I.2, donne de nombreux exemples algébriques d'anneaux satisfaisant le LGPH. La suite du chapitre est consacrée à la comparaison du LGPH avec celui de Rumely et avec les LGP de corps (§ I.3 et I.4). Il faudra attendre la fin du chapitre 3 pour faire de même avec le LGP plus sophistiqué de Prestel et Schmid (qui lui aussi apparaîtra comme un cas particulier du LGPH). Nous terminons par une digression d'intérêt plus général sur le principe de spécialisation locale (une terminologie que nous empruntons à Lang) au cours de laquelle nous démontrons par exemple :

Proposition
Soit F un corps valué henselien, F^c le complété de F relativement à cette valuation, et V une variété définie sur F.
Alors $V^\circ(F)$ est dense dans $V^\circ(F^c)$ (pour la topologie produit de la valuation).
En particulier, si V a un point lisse dans F^c alors elle en a un dans F.

Le contenu du chapitre 2 est élémentaire. On y démontre que le LGPH est axiomatisable au premier ordre dans le langage des anneaux. Ce résultat assez technique est fondamental pour pouvoir appliquer au LGPH les outils de la théorie des modèles. La vérification aurait pu être faite plus directement, mais sous l'influence des articles de Ershov sur les anneaux booléens, nous avons situé notre étude dans un cadre homogène, englobant le sien : celui des anneaux localement booléens. Nous les définissons comme les anneaux intègres A tels que pour tout élément a de A, non nul et non inversible, le localisé $S_a^{-1}A$ (où S_a est le complémentaire dans A de la réunion des idéaux maximaux de A contenant a) est booléen. Nous vérifions qu'ils conservent les propriétés les plus remarquables des anneaux booléens, comme d'être stables par clôture intégrale (un résultat que nous avons reporté au § III.2) ou de former une classe élémentaire (§ II.2). Signalons aussi que pour un anneau localement booléen, les notions classiques d'approximation par blocs (BAP) et de bonne factorisation (BF) que nous avons empruntées à la littérature sont respectivement équivalentes à l'indépendance (la localisation par deux idéaux maximaux distincts donne des anneaux de valuation indépendants, *cf.* § II.3) et à la propriété de Bezout (tout idéal de type fini est principal, § II.4). C'est dans ce genre de réduction que réside tout le charme des anneaux localement booléens. Ils ont en outre l'avantage d'être considérablement plus répandus, puisque nous montrons par exemple aux § II.1 et II.3 :

Proposition
Tout anneau intégralement clos inclus dans une clôture algébrique de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$ est localement booléen.
Tout anneau de Dedekind est localement booléen.

À titre de comparaison, les anneaux booléens inclus dans $\mathbb{Q}$ ou dans $\mathbb{F}_p(T)$ sont seulement les anneaux n'ayant qu'un nombre fini d'idéaux premiers. Nous n'avons pas exploité très à fond la notion d'anneau localement booléen, et il ne paraît pas douteux que l'on pourrait en poursuivant dans cette voie obtenir des résultats de théorie des modèles semblables à ceux bien connus sur les produits booléens de structures. Cependant, cela nous aurait emmené trop loin des préoccupations liées à notre sujet. La lecture de ce chapitre n'est du reste pas indispensable à la compréhension de notre travail, pour qui est familier des propriétés d'approximation par blocs et de bonne factorisation (les définitions sont rappelées aux § II.3 et II.4).

Le chapitre suivant culmine dans le théorème de clôture existentielle pour les anneaux satisfaisant le LGPH qui est le noeud gordien de notre thèse (§ III.3). L'idée est que le LGPH, bien que purement géométrique dans sa définition, peut s'interpréter comme une propriété de clôture existentielle dans certaines extensions non seulement au sens des anneaux, comme le montrait la première proposition citée dans cette introduction, mais même au sens d'une structure enrichie : celles des r-anneaux, ou anneaux munis d'une relation radicale (une notion due à Prestel et Schmid). Toute la partie syntaxique de notre travail, à l'exception de l'axiomatisation, est concentrée dans ce théorème de clôture existentielle. L'avantage est que dans les preuves qui suivront, l'essentiel des arguments (hormis ce théorème) seront de nature algébrique. L'inconvénient est que sa démonstration est longue, et assez pénible. Nous conseillons au lecteur de la passer dans un premier temps, avec celles des lemmes qui l'accompagnent, pour aller d'abord voir dans les chapitres suivants la manière dont il intervient, et d'y revenir ensuite.

En application immédiate de ce résultat, nous vérifions au § IV.4 que le LGP de Prestel et Schmid est bien un cas particulier du LGPH. Il n'est pas inutile ici de rendre à César ce qui lui appartient : le LGP de Prestel et Schmid est en fait notre point de départ, et c'est la lecture de l'article de van den Dries et Macintyre [VdD-M] qui nous a montré la voie pour éliminer les conditions suplémentaires sur la relation radicale, et prouver que le LGP de Prestel et Schmid pouvait être ramené à quelque chose de purement algébrique (*i.e.* sans relation radicale).

En amont de ce résultat, et presqu'à titre de récréation, nous démontrons au § III.2 que le LGPH est stable par clôture intégrale, tout comme ses ancêtres les LGP de corps étaient stables par clôture algébrique. La preuve est cependant un peu plus délicate, car on ne dispose plus de bases pour les extensions d'anneaux comme on en avait pour les extensions de corps.

Avec le chapitre 4 on aborde le second versant de cette thèse : celui des applications. On commence par introduire les notions d'anneaux PAC, PRC et PC_M, généralisations immédiates des définitions homonymes pour les corps (§ IV.1). Après quelques rappels et vérifications élémentaires (§ IV.1 et IV.2) nous formulons pour ces anneaux des théorèmes de plongement (§ IV.3 et IV.4) qui nous permettent au § IV.5 d'élucider totalement les propriétés modèles-théoriques fondamentales de ces anneaux sous la forme de conditions nécessaires et suffisantes simples, caractérisant les plongements existentiellement clos, les plongements élémentaires, et la décidabilité. Pour cette partie, nous avons largement pioché dans la littérature classique sur les corps PAC, PRC ou PC_M, et il serait vain de vouloir faire la liste des nombreux auteurs envers qui nous avons ainsi contracté une dette (cette liste est à peu près égale à notre bibliographie). C'est en application de ces théorèmes que nous obtenons au § IV.6 les résultats annoncés plus haut de décidabilité de la clôture intégrale de $\mathbb{F}_p[T]$ dans tout corps séparablement clos, ainsi que de divers sur-anneaux des entiers algébriques absolument réels, et (modulo un résultat de Pop encore non publié) de l'anneau des entiers algébriques absolument p-adiques. Nous avons aussi regroupé à la fin de ce quatrième chapitre les applications à l'algèbre que nous avons pu trouver, et notamment :

Proposition
Notons A la clôture intégrale de $\mathbb{Z}$ ou de $\mathbb{F}_p[T]$ dans un corps algébriquement clos. Alors pour tous $f_1, \ldots, f_m \in A[X_1, \ldots, X_n, Y]$ les assertions suivantes sont équivalentes :
(i) *$\forall a \in A^n$, les $f_i(a, Y)$ ont un zéro commun dans A ;*
(ii) *il existe $f \in A[X_1, \ldots, X_n, Y]$, unitaire en Y, qui divise simultanément tous les f_i (dans $A[X_1, \ldots, X_n, Y]$).*

Le chapitre 5 qui termine ce travail regroupe d'autres résultats analogues à ceux du chapitre 4, mais nécessitant un formalisme plus détaillé. Ils montrent qu'avec le LGPH on peut axiomatiser des classes d'anneaux dont on a fixé les théories locales (sous des hypothèses satisfaites par tous les exemples envisageables), et obtenir pour les anneaux algébriquement maximaux appartenant à ces classes, des caractérisations simples des plongements existentiellement clos ou élémentaires, et de la décidabilité. En application nous obtenons le résultat qui fut l'un des premiers objectifs de notre thèse : la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_p$ est décidable.

La plupart de nos résultats de décidabilité viennent de ce qu'on ramène la théorie de l'anneau considéré à celle de structures plus simples, dont des treillis distributifs d'un genre particulier : les quasi-algèbres de Boole. Encore faut-il pour les applications connaître des quasi-algèbres de Boole décidables. Comme aucune référence publiée n'existe sur la question, nous avons dû nous fendre d'une annexe pour vérifier que les quasi-algèbres de Boole denses étaient décidables (la démonstration est essentiellement la même que pour le résultat analogue bien connu sur les algèbres de Boole). Bien que nous n'ayons pas voulu l'inclure ici par souci de concision, signalons tout de même le résultat suivant : toute quasi-algèbre de Boole peut être représentée comme le treillis résiduel (notion définie dans les prérequis) d'un anneau satisfaisant le LGPH, et l'on peut imposer à peu près ce que l'on veut sur le corps des fractions. Comme il existe bien évidemment des quasi-algèbres de Boole indécidables, cela signifie qu'il existe des anneaux qui satisfont le LGPH et sont néanmoins indécidables (c'est une remarque triviale pour un logicien, mais qui peut paraître surprenante à un algébriste).

Notations et conventions

La numérotation des énoncés démontrés repart de 1 au début de chaque paragraphe. Les références sont à comprendre ainsi :

- §1 renvoie au paragraphe 1 du chapitre courant ;
- §II.1 au paragraphe 1 du chapitre 2 ;
- théorème 1 au théorème 1 du paragraphe courant ;
- théorème 2.1 au théorème 1 du §2 ;
- théorème III.2.1 au théorème 1 du §III.2.

Anneaux et valuations

Tous nos anneaux sont commutatifs et unitaires.

Si R est un anneau de valuation sur un corps K, je note :

- $m(R)$ l'idéal maximal de R ;
- v_R la valuation associée à R ;
- k_R son corps résiduel ;
- Γ_R son groupe des valeurs, qui sera noté en général multiplicativement.

Pour tout x de K, le module de x suivant R sera noté $|x|_R$, c'est-à-dire que :

$$|x|_R \leq |y|_R \quad \Longleftrightarrow \quad \exists z \in R,\ x = yz.$$

Si R' est un anneau de valuation prolongeant R, et si $x \in \mathrm{Fr}(R')$, je note aussi bien $|x|_R$ que $|x|_{R'}$, chaque fois qu'il n'y a pas d'ambiguïté (et notamment quand R' est le hensélisé de R).

Si A est un anneau intègre, et $\mathfrak{p}$ un idéal premier de A tel que $A_\mathfrak{p}$ soit un anneau de valuation, je noterai "$X_\mathfrak{p}$" tout ce que j'ai noté ci-dessus "$X_{A_\mathfrak{p}}$".

Extensions algébriques et hensélisations

Étant donnée une extension galoisienne L d'un corps K, je note $Gal(L|K)$ ou $G(L|K)$ le groupe de Galois associé.

Si K est un corps quelconque, je note $G(K)$ le groupe absolu de Galois de K, *i.e.* l'ensemble des K-automorphismes d'une clôture séparable de K.

En ce qui concerne "le" henselisé d'un anneau de valuation, j'adopte les conventions suivantes : chaque fois que dans un énoncé je me donne un anneau intègre A, je sous-

entends qu'il est plongé dans son corps des fractions K, qui est lui même plongé dans une clôture algébrique K^a fixée, et que **pour tout anneau de valuation R de K je me suis donné un hensélisé R^h de R, fixé dans K^a**.
Cela étant posé, je noterai :
- $H_R(K) := \mathrm{Fr}(R^h)$ (dans K^a) ;
- K^s la clôture séparable de K dans K^a ;
- R^s (resp. R^a) l'unique prolongement de R^h à K^s (resp. K^a).

Remarque: Quand je me donne une famille W d'anneaux de valuation sur un corps K et que j'énonce une propriété faisant appel aux hensélisés des éléments de W, la satisfaction de cette propriété dépend a priori du choix des hensélisés que j'ai fait en me donnant W. Toutes les propriétés qui nous intéressent sont en fait, de manière évidente, indépendantes de ce choix, et je laisserai au lecteur le soin de s'en convaincre par lui-même en chaque occasion.

Anneaux de Prüfer et parties constructibles

Étant donné un anneau intègre A, de corps des fractions K, je note :
- W_A la famille des anneaux de valuation R de K tels que $m(R) \cap A \in \mathrm{Spm}(A)$;
- pour tout $I \subseteq A$, $M(I) := \{\mathfrak{m} \in \mathrm{Spm}(A) \,/\, I \subseteq \mathfrak{m}\}$ et si $I = \{a\}$, $M(a) := M(\{a\})$;
- sauf indication contraire, pour tout $a \in A$, $S_a := A \setminus \bigcup M(a)$;
- enfin le complémentaire d'une partie du type $M(I)$ ou $M(a)$ que nous noterons $M(I)^c$ (resp. $M(a)^c$) sera toujours pris dans $\mathrm{Spm}(A)$ (et pas, par exemple, dans $\mathrm{Sp}(A)$).

On remarquera que $0 \in S_a$ si et seulement si a est inversible.

Si W est une famille d'anneaux de valuation sur K, je note :
- $A_W := \bigcap W$ l'anneau d'holomorphie de W ;
- pour tout x de K, $W(x) := \{R \in W \,/\, x \in m(R)\}$;
- $\mathrm{L}(W) := \{W(x) \,/\, x \in K\}$.

Rappelons qu'un anneau A est **de Prüfer** s'il est intègre et si son localisé par tout idéal premier est un anneau de valuation. Il suffit que cela soit vérifié pour les idéaux maximaux de A. En particulier, A de Prüfer si et seulement si $W_A = \{A_\mathfrak{m} \,/\, \mathfrak{m} \in \mathrm{Spm}(A)\}$.

Les anneaux **de Bezout** constituent un cas particulier important d'anneaux de Prüfer. On appelle ainsi les anneaux dont tout idéal de type fini est principal *i.e.* (par une récurrence triviale) tels que pour tous $a, b \in A$ il existe $d \in A$ tel que $aA + bA = dA$. Un tel élément d est appelé un **pgcd** de a et b (dans A) et par abus de notations on écrit $d = (a, b)$ pour "d est un pgcd de a et b dans A".

Définitions
(1) Avec les notations ci-dessus, la **topologie de Zariski sur W** est la topologie définie en prenant $\mathrm{L}(W)$ comme sous-base de fermés. Les **parties constructibles de W** sont les combinaisons booléennes d'éléments de $L(W)$
(2) J'appelle parties **constructibles de $\mathrm{Spm}(A)$** les combinaisons booléennes de parties du spectre maximal de A de la forme $M(a)$ ($a \in A$).

Propriété 1
Soit A un anneau de Prüfer, et K son corps des fractions.

(1) *Pour tout $x \in K$, il existe $a_1, \ldots, a_n \in A$ tels que* $W_A(x) = \bigcap_{1 \leq i \leq n} W_A(a_i)$.

(2) *L'application* $\mathfrak{m} \mapsto A_\mathfrak{m}$ *est un homéomorphisme de* $\mathrm{Spm}(A)$ *sur* W_A. *Elle établit une correspondance bijective entre les parties constructibles de* $\mathrm{Spm}(A)$ *et celles de* W_A.

Preuve:

(1) Soit $x \in K$, on peut supposer $x \neq 0$ sinon $x \in A$ et c'est trivial. Pour tout $y \in K$, notons $M(y) := \{\mathfrak{m} \in \mathrm{Spm}(A) \,/\, y \in m(A_\mathfrak{m})\}$. Il est clair que $W_A(y) = \{A_\mathfrak{m} \,/\, \mathfrak{m} \in M(y)\}$.

Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, soient $a_\mathfrak{m}, b_\mathfrak{m} \in A \neq 0$ tels que $x = a_\mathfrak{m}/b_\mathfrak{m}$. Si $\mathfrak{m} \in M(x)$ alors $x \in m(A_\mathfrak{m})$ donc on peut imposer que $a_\mathfrak{m} \in \mathfrak{m}$ et que $b_\mathfrak{m} \notin \mathfrak{m}$; sinon $x^{-1} \in A_\mathfrak{m}$ et on peut imposer que $a_\mathfrak{m} \notin \mathfrak{m}$. Dans les deux cas, on a :

$$M(a_\mathfrak{m}) = M(b_\mathfrak{m} x) \supseteq M(x) \qquad (\text{car } b_\mathfrak{m} \in A).$$

L'ensemble $\{M(b_\mathfrak{m})^c\}_{\mathfrak{m} \in M(x)} \cup \{M(a_\mathfrak{m})^c\}_{\mathfrak{m} \in M(x)^c}$ constitue un recouvrement ouvert de $\mathrm{Spm}(A)$, dont on sait qu'il est quasi-compact, donc on peut en extraire un recouvrement fini $\{M(b_{\mathfrak{m}_i})^c\}_{1 \leq i \leq r} \cup \{M(a_{\mathfrak{m}_i})^c\}_{r+1 \leq i \leq s}$. Posons $\mathcal{M} := \bigcap_{i=1}^s M(a_{\mathfrak{m}_i})$

– Par construction $M(x)$ est inclus dans $M(a_{\mathfrak{m}_i})$ pour tout $i \in [\![1, s]\!]$ donc $M(x)$ est inclus dans $\mathcal{M}$.

– Inversement $\bigcap_{i=1}^r M(b_{\mathfrak{m}_i}) \cap \mathcal{M} \subseteq \bigcap_{i=1}^r M(b_{\mathfrak{m}_i}) \cap \bigcap_{i=r+1}^s M(a_{\mathfrak{m}_i}) = \emptyset$, donc pour tout $\mathfrak{m} \in \mathcal{M}$ il existe $i \in [\![1, r]\!]$ tel que $\mathfrak{m} \notin M(b_{\mathfrak{m}_i})$. Or x s'écrit $a_{\mathfrak{m}_i}/b_{\mathfrak{m}_i}$ avec $b_{\mathfrak{m}_i} \notin \mathfrak{m}$ et $a_{\mathfrak{m}_i} \in \mathfrak{m}$ (car $\mathfrak{m} \in \mathcal{M} \subseteq \bigcap_{i=1}^r M(a_{\mathfrak{m}_i})$) donc $x \in m(A_\mathfrak{m})$ *i.e.* $\mathfrak{m} \in M(x)$.

On a donc $M(x) = \bigcap_{i=1}^s M(a_{\mathfrak{m}_i})$ d'où $W_A(x) = \bigcap_{i=1}^s W_A(a_{\mathfrak{m}_i})$.

(2) A étant de Prüfer cette application, disons φ, est une bijection de $\mathrm{Spm}(A)$ sur W_A, de réciproque $R \mapsto m(R) \cap A$. De plus elle envoie toute partie de la forme $M(a)^c$ sur $W_A(a)^c$ donc est ouverte. Pour vérifier que c'est un homéorphisme, il suffit donc de montrer qu'elle est continue.

L'ensemble des $W_A(a)^c$, pour a décrivant A, est une base d'ouverts de la topologie de Zariski de W_A. En effet c'est une famille d'ouverts de W_A, stable par intersection finie puisque pour tous $a, b \in A$ on a $W_A(a)^c \cap W_A(b)^c = W_A(ab)^c$, et tout ouvert de base $W_A(x)^c$, avec $x \in K$, est recouvert par des $W_A(a_i)^c$ donnés par le (1). Quel que soit $a \in A$, $\varphi^{-1}[W_A(a)] = M(a)$ est un ouvert de $\mathrm{Spm}(A)$, donc cette application est bien continue.

Enfin, montrons que l'application image directe associée à φ, notons-la φ^*, envoie bijectivement les constructibles de $\mathrm{Spm}(A)$ sur les constructibles de W_A. L'application φ étant étant bijective, φ^* commute aux opérations de combinaisons booléennes, il s'ensuit qu'elle conserve la constructibilité. De plus φ étant injective on sait que φ^* est injective, et *a fortiori* sa restriction aux parties constructibles de $\mathrm{Spm}(A)$. Il ne reste donc plus qu'à montrer que pour tout $x \in K$, $W_A(x)$ est l'image directe d'une partie constructible de $\mathrm{Spm}(A)$. Or étant donné un tel x le (1) fournit des éléments $a_1, \ldots, a_n$ de A qui donnent la conclusion puisque :

$$W_A(x) = \bigcap_{i=1}^n W_A(a_i) = \bigcap_{i=1}^n \varphi^*(M(a_i)) = \varphi^*\left(\bigcap_{i=1}^n M(a_i)\right)$$

■

Quelques notations vectorielles (plus rares)

Etant donnés $x = (x_1, \ldots, x_m)$ et $y = (y_1, \ldots, y_n)$ dans un corps valué (K, R), je note :

$$|x|_R \leq |y|_R \quad\iff\quad \max_{1\leq i\leq m} |x_i|_R \leq \min_{1\leq j\leq n} |y_j|_R$$

Si W est une famille d'anneaux de valuation sur un corps K, et $x, y \in K$, je note :

$$|x|_W \leq |y|_W \quad\iff\quad \forall R \in W,\ |x|_R \leq |y|_R$$

Enfin, si $\mathcal{P}$ est une partie du spectre d'un anneau intègre A, de corps des fractions K, et si $W_{\mathcal{P}}$ désigne l'ensemble des anneaux de valuation R de K tels que $m(R) \cap A \in \mathcal{P}$, je noterai simplement $|x|_{\mathcal{P}}$ au lieu de $|x|_{W_{\mathcal{P}}}$.

Prérequis

L'approche de Ershov : les anneaux booléens

Définition
Soit W une famille d'anneaux de valuation sur un corps K.
W est **booléenne** si et seulement si :
– $\mathrm{L}(W)$ est stable par combinaisons booléennes ;
– W est un espace booléen pour la topologie de Zariski (*i.e.* compact totalement déconnecté, la première hypothèse implique qu'il suffit pour cela que W soit quasi-compact).

Exemples:
(1) Une famille finie d'anneaux de valuation sur un corps K est booléenne si et seulement si ses éléments sont deux à deux incomparables pour l'inclusion.
Dans une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$, les familles booléennes d'anneaux de valuation sont exactement les familles finies.
(2) Soit K un corps, et π un élément de K différent de 0 et 1. Soit W_π l'ensemble des anneaux de valuation R de K dont le groupe des valeurs (noté additivement) possède un plus petit élément strictement positif qui soit précisément $v_R(\pi)$. Ershov a montré que toute famille du type W_π est booléenne.

L'une des propriétés caractéristiques des familles booléennes d'anneaux de valuation est de pouvoir être reconstruites à partir de leur anneau d'holomorphie.

Théorème 1 (Ershov)
Soit W une famille booléenne d'anneaux de valuation sur un corps K. Alors :
(a) $\mathrm{Fr}(A_W) = K$;
(b) *A_W est de Prüfer ;*
(c) $W_{A_W} = W$;
(d) *pour tout $x \in K$, il existe $a \in A_W$ tel que $W(x) = W(a)$.*

Ershov appelle alors **anneaux booléens** les anneaux d'holomorphie des familles booléennes d'anneaux de valuation, donc les anneaux A de Prüfer tels que W_A soit booléenne. Il démontre également :

Théorème 2 (Ershov)
Soit A un anneau booléen, de corps des fractions K. Soit L une extension algébrique

de K. Alors la clôture intégrale de A dans L est encore un anneau booléen.

Remarque: Ershov donne en fait une définition différente des anneaux booléens, qui montre qu'il s'agit d'une propriété du premier ordre, puis il démontre qu'elle est équivalente à la définition que je viens de donner.

L'approche de Prestel et Schmid

Définitions
Un **r-anneau** est un anneau A muni d'un préordre $\leq$ vérifiant, pour tous $a, b, c \in A$:
(i) $1 \leq a$;
(ii) $a \leq b$ et $a \leq c \Longrightarrow a \leq b + c$;
(iii) $a \leq b \Longrightarrow ac \leq bc$;
(iv) $a \leq b^2 \Longrightarrow a \leq b$.
Un tel préordre est appelé une **relation radicale** sur A.
Si de plus $(A, \leq)$ satisfait l'axiome
(o) $\forall a\,(0 \leq a \Longrightarrow 0 = a)$,
alors $(A, \leq)$ est un **$r_\circ$-anneau.**
Un **r-domaine** est un r-anneau intègre, et de même pour un **$r_\circ$-domaine**.

Remarque: Un r-anneau quelconque $(A, \leq)$ satisfait toujours l'axiome : $\forall a,\ a \leq 0$. En effet, si $a \in A$, on a $a \leq a$ (par réflexivité) et $1 \leq 1 = (-1)^2 \underset{\text{(iv)}}{\Longrightarrow} 1 \leq -1 \underset{\text{(iii)}}{\Longrightarrow} a \leq -a$, d'où, vu (ii), $a \leq a + (-a) = 0$.

Exemple: Étant donnés un anneau A et $\mathcal{P} \subseteq \mathrm{Sp}(A)$, la relation suivante se trouve être une relation radicale :

$$\forall a, b \in A, \qquad a \leq_{\mathcal{P}} b \iff \forall \mathfrak{p} \in \mathcal{P}\ (a \in \mathfrak{p} \Longrightarrow b \in \mathfrak{p}).$$

Si $\mathcal{P} = \mathrm{Sp}(A)$, $\quad a \leq_{\mathcal{P}} b \iff b \in \sqrt{(a)}$.
Si $\mathcal{P} = \mathrm{Spm}(A)$, $\quad a \leq_{\mathcal{P}} b \iff b \in \mathrm{Jac}(a)$ (le radical de Jacobson de (a).)

Définitions
La relation radicale $\leq_{\mathcal{P}}$ introduite ci-dessus sera appelée **relation radicale induite** par $\mathcal{P}$. La relation radicale induite sur un anneau A par son spectre maximal sera notée $\boldsymbol{\leq_A}$. Nous y recourrons souvent, sous le nom de **relation radicale associée** à A.

NB : Chaque fois que la définition sera donnée d'une propriété de r-anneau, on dira d'un anneau A qu'il a cette propriété si et seulement si le r-anneau associé $(A, \leq_A)$ la satisfait.

Prestel et Schmid ont montré que toute relation radicale sur un anneau A était de la forme $\leq_{\mathcal{P}}$, pour un certain $\mathcal{P} \subseteq \mathrm{Sp}(A)$. Pour cela, il faut introduire les définitions suivantes :

Définitions
Soit $(A, \leq)$ un r-anneau, et X une partie de A.
(1) X est dite **r-close** si et seulement si pour tous $a, b \in A$:

$$a \in X \text{ et } a \leq b \Longrightarrow b \in X.$$

(2) Il est clair que $\boldsymbol{[X]_{\leq}} := \{a \in A \,/\, \exists x \in X \text{ tel que } x \leq a\}$ est la plus petite partie r-close de $(A, \leq)$ contenant X. On l'appellera donc la **r-clôture** de X.

(3) Le **r-radical** de X est la partie $\mathbf{(X)_{\leq}}$ de A définie par :
$X_0 = X, \quad \forall n \in \mathbb{N},\ X_{n+1} =$ l'idéal engendré par $[X_n]_{\leq}, \quad (X)_{\leq} = \bigcup_{n\in\mathbb{N}} X_n.$
Autrement dit $(X)_{\leq}$ est le plus petit idéal r-clos de $(A, \leq)$ contenant X.
(4) Le **spectre r-clos** de $(A, \leq)$, est l'ensemble des idéaux premiers r-clos de $(A, \leq)$. On le note $\mathbf{Sp(A, \leq)}$.

Remarques:
(1) Les $\mathrm{r}_\circ$-anneaux sont exactement les r-anneaux dont l'idéal nul est r-clos.
(2) Il va de soi que $\mathrm{Sp}(A, \leq)$ est une partie quasi-compacte de $\mathrm{Sp}(A)$ (nous utiliserons parfois cette propriété sans nous y référer, sa vérification est laissée en exercice au lecteur).

Notations: Soit $(A, \leq)$ un r-anneau. Pour toute partie X de A, on note :

$$P_{(A,\leq)}(X) := \{\mathfrak{p} \in \mathrm{Sp}(A, \leq) \,/\, X \subseteq \mathfrak{p}\}.$$

Chaque fois que c'est possible sans ambiguïté, on écrit simplement $P(X)$ ou $P_A(X)$ pour $P_{(A,\leq)}(X)$. Enfin si X est réduit à un singleton, on note $P(x)$ pour $P(\{x\})$.

Théorème 3 (Prestel-Schmid).
Soit $(A, \leq)$ un r-domaine.
(a) $\forall X \subseteq A, \quad (X)_{\leq} = \bigcap P(X)$ *(par convention, si $P(X) = \emptyset$ on prend $\bigcap P(X) = A$).*
(b) *La relation radicale de $(A, \leq)$ est précisément celle induite sur A par* $\mathrm{Sp}(A, \leq)$.

Remarque: Prestel et Schmid interdisaient à une relation radicale d'être définie par la partie vide, en imposant en axiome $0 \not\leq 1$. Pourtant, ce cas particulier de r-anneau est parfois utile, et marche aussi bien que les autres. Comme dirait Poizat : "je ne comprends pas cette horreur du vide, si peu logique." Aussi ai-je pris la liberté de modifier un peu leur définition des r-anneaux en éliminant cet axiome parasite, mais il est clair que ça n'enlève rien à la validité du théorème ci-dessus.

De même j'ai cru bon de distinguer les parties r-closes des idéaux r-clos en appelant r-radical ce qu'ils appelaient "$\leq$-clôture."

Définitions
Soit $(A, \leq)$ un r-anneau.
(1) On considère dans [P-S 90] l'ensemble $\mathbf{L(A, \leq)}$ $:=\{P(a) \,/\, a \in A\}$. Cet ensemble, ordonné par l'inclusion, est stable par la réunion ($P(a) \cup P(b) = P(ab)$) et possède un plus grand élément $\mathbf{1} = P(0)$ et un plus petit élément $\mathbf{0} = P(1)$. C'est donc un demi-treillis supérieur avec extrémités. Nous l'appellerons le **TSUP résiduel** de $(A, \leq)$.
(2) $(A, \leq)$ sera dit **$\cap$-stable** si $\mathrm{L}(A, \leq)$ est stable par intersection (finie). Conformément à nos conventions, nous dirons d'un anneau B qu'il est $\cap$-stable si et seulement si $(B, \leq_B)$ est $\cap$-stable. Si $(A, \leq)$ est $\cap$-stable, alors $\mathrm{L}(A, \leq)$ est un treillis distributif avec extrémités nous l'appellerons le **treillis résiduel** de $(A, \leq)$.
(3) Les **parties constructibles** de $\mathrm{Sp}(A, \leq)$ sont les combinaisons booléennes d'éléments de $\mathrm{L}(A, \leq)$.

Exemples:
(1) Si un anneau A est de Bezout, pour tous $a, b \in A$, pour tout $\mathfrak{p} \in Sp(A)$, et pour tout pgcd d de a et b on a : $\ d \in \mathfrak{p} \iff (a \in \mathfrak{p}$ et $b \in \mathfrak{p})$. Quelle que soit la relation radicale que l'on choisit sur A, on aura $P(a) \cap P(b) = P(d)$ donc $(A, \leq)$ sera $\cap$-stable. En particulier A lui-même est $\cap$-stable.

(2) On notera que le (d) du théorème 1 implique qu'un anneau booléen A est $\cap$-stable : quels que soient $a, b \in A$ il existe $c \in A$ tel que $W_A(c) = W_A(a) \cap W_A(b)$ et donc, puisque A est de Prüfer, $M(c) = M(a) \cap M(b)$.
(3) L'anneau $A := \mathbb{Q}[X, Y]$, muni de sa relation radicale associée n'est pas $\cap$-stable, et son TSUP résiduel est néanmoins un treillis. En effet, on sait que tout idéal premier de $\mathbb{Q}[X, Y]$ est égal à son radical de Jacobson, donc $\mathrm{Sp}(A, \leq_A) = \mathrm{Sp}(A)$. Tout élément f de $\mathbb{Q}[X, Y]$ s'écrit de manière unique comme produit d'éléments irréductibles, et il est clair que si f est lui-même irréductible, alors $P(f)$ est un atome de $\mathrm{L}(A, \leq_A)$. Tout élément de $\mathrm{L}(A, \leq_A)$ s'écrit donc comme réunion finie d'atomes. Il s'ensuit que $\mathrm{L}(A, \leq_A)$, en tant qu'ensemble ordonné, est un treillis distributif (il est même isomorphe à $\mathrm{L}(\mathbb{Z}, \leq_{\mathbb{Z}})$). Pourtant $\mathbb{Q}[X, Y]$ n'est pas $\cap$-stable, car par exemple $P(X) \cap P(Y) = \{(X, Y)\} \notin \mathrm{L}(A, \leq_A)$. En effet pour tout $f \in \mathbb{Q}[X, Y]$, ou bien f est inversible et $P(f) = \emptyset$, ou bien f possède au moins un facteur irréductible qui engendre un idéal premier $\mathfrak{p}$ non maximal de $\mathbb{Q}[X, Y]$ appartenant à $P(f)$, et dans les deux cas $P(f) \neq \{(X, Y)\}$. (Note : l'infimum de $P(X)$ et $P(Y)$ dans $\mathrm{L}(A, \leq_A)$ est $\mathbf{0}$.)

Les langages

Notations:

- $\mathrm{L_{ann}} := \{0, 1, +, -, .\}$ est le langage des anneaux ;
- $\mathrm{L_{rad}} := \mathrm{L_{ann}} \cup \{\leq\}$ celui des r-anneaux ;
- $\mathrm{L_{div}} := \mathrm{L_{ann}} \cup \{\,|\,\}$ où $|$ est une relation binaire ;
- $\mathrm{L_{lat}} := \{0, 1, \wedge, \vee\}$ le langage des treillis avec extrémités.

Si E est un ensemble ordonné quelconque, et si T est une théorie du langage $\mathrm{L_{lat}}$, on dit par abus de langage que E est un modèle de T si E, en tant qu'ensemble ordonné, est un treillis avec extrémités, et si une fois muni de cette $\mathrm{L_{lat}}$-structure naturelle qu'on peut lui attribuer, il est un modèle de T.

De même étant donné un anneau A, on le considère comme une $\mathrm{L_{ann}}$-structure en donnant aux symboles de $\mathrm{L_{ann}}$ leur interprétation évidente (0 est l'élément neutre de l'addition…etc) mais on peut aussi le munir d'une $\mathrm{L_{rad}}$-structure ou d'une $\mathrm{L_{div}}$-structure en interprétant :

- "$\leq$" par la relation radicale associée à A, notée $\leq_A$,
- "$|$" par la divisibilité usuelle sur A, notée $|_A$.

Par abus de langage, nous dirons d'un anneau A qu'il est un modèle d'une théorie T de $\mathrm{L_{rad}}$ (resp. $\mathrm{L_{div}}$), si $(A, \leq_A)$ (resp. $(A, |_A)$) est modèle de T.

On a, pour tout anneau A, et tous $a, b \in A$:

$$a \leq_A b \iff \forall c((b, c) = 1 \to (a, c) = 1),$$
$$a|_A b \iff \exists c(b = ac).$$

où l'expression "$(x, y) = 1$" abrège la formule "$\exists u \exists v(ux + vy = 1)$".

Autrement dit on peut traduire une théorie quelconque de l'un de ces langages dans l'autre, et cette traduction conserve la complétude ; la théorie d'un anneau A dans L est décidable si et seulement si la théorie du r-anneau associé $(A, \leq_A)$ est décidable, si et seulement si la théorie de $(A, |_A)$ est décidable. De même, si un anneau A est plongé élémentairement dans un anneau A', ce plongement respectera les structures additionnelles de $\mathrm{L_{rad}}$ et $\mathrm{L_{div}}$, et sera encore un plongement élémentaire de $(A, \leq_A)$ dans $(A', \leq_{A'})$, et de $(A, |_A)$ dans $(A', |_{A'})$.

Cependant, cette traduction ne conserve pas la quantification, aussi un plongement $\exists$-clos entre deux anneaux A et A' n'a-t-il aucune raison d'être encore un plongement de $(A, \leq_A)$ dans $(A', \leq_{A'})$, et même si c'était le cas, d'être encore $\exists$-clos au sens de $\mathrm{L_{rad}}$ (et de même pour les $\mathrm{L_{div}}$-structures associées). On a tout de même la propriété suivante :

Propriété 4
Soient R et R' deux anneaux de valuation, et σ un plongement de R dans R'. On identifie R à son image, et on suppose que $m(R) = m(R') \cap R$.
Alors σ est encore un plongement au sens de $\mathrm{L_{rad}}$ et de $\mathrm{L_{div}}$, et l'on a :

$$(R, \leq_R) \leq_\exists (R', \leq_{R'}) \quad \Longleftrightarrow \quad (R, |_R) \leq_\exists (R', |_{R'}).$$

Preuve: Pour tous $a, b \in R$, on a :

$$a \leq_R b \iff (a \notin m(R) \text{ ou } b \in m(R)) \iff (a \notin m(R') \text{ ou } b \in m(R')) \iff a \leq_{R'} b$$

Or $R' \cap \mathrm{Fr}(R)$ est un anneau de valuation contenant R donc l'hypothèse que $m(R) = m(R') \cap R$ implique que $R' \cap \mathrm{Fr}(R) = R$ d'où :

$$a|_R b \iff \frac{b}{a} \in R \iff \frac{b}{a} \in R' \cap \mathrm{Fr}(R) \iff \frac{b}{a} \in R' \iff a|_{R'} b$$

σ est donc bien un plongement au sens de $\mathrm{L_{rad}}$ ou de $\mathrm{L_{div}}$.

D'autre part on a pour tous $a, b \in R$:

$$a|_R b \iff \exists c(b = ac),$$
$$a \not|_R b \iff \exists c(a = bc \wedge c \not\leq_R 1).$$

Toute formule existentielle de $\mathrm{L_{div}}$ à paramètres dans R peut donc être traduite en une formule existentielle de $\mathrm{L_{rad}}$, avec les mêmes paramètres, d'où :

$$(R, \leq_R) \leq_\exists (R', \leq_{R'}) \implies (R, |_R) \leq_\exists (R', |_{R'}).$$

Inversement, $\leq_R$ est définissable sans quanteur dans $\mathrm{L_{div}}$ par :

$$a \leq_R b \iff a|_R 1 \vee b \not|_R 1.$$

L'autre implication en découle immédiatement.

■

N.B. Cela nous autorise à regarder les anneaux de valuations que nous utiliserons indifféremment comme des $\mathrm{L_{div}}$-structures ou des $\mathrm{L_{rad}}$-structures.

Rudiments de géométrie algébrique

Pour les objets dont l'usage est commun aux logiciens et aux géomètres, il n'existe pas de définitions universelles, c'est pourquoi je reprends ici toutes les définitions des objets de géométrie algébrique de base dont j'aurai l'usage. Fixons un corps algébriquement clos K et un corps k inclus dans K.

À toute partie E de $K[X]$ $(X = (X_1, \ldots, X_n))$ on associe l'ensemble $\mathcal{A}_E(K)$ des zéros de E dans K, c'est-à-dire : $\mathcal{A}_E(K) := \{x \in K^n / \forall f \in E, f(x) = 0\}$. Les ensembles de cette forme constituent une base de fermés d'une topologie sur K^n appelée **topologie de Zariski**. On sait que la trace de cette topologie sur $(k^a)^n$ coïncide avec la topologie de Zariski de $(k^a)^n$. Les fermés de Zariski de K^n sont appelés **ensembles**

algébriques (affines). Les ensembles algébriques irréductibles (au sens de la topologie de Zariski, c'est-à-dire ceux qui ne peuvent pas s'écrire comme réunion de deux parties propres fermées) sont plus brièvement appelés des **variétés (affines)**. Tout ensemble algébrique se décompose de manière unique en une réunion finie de variétés appelées ses **composantes irréductibles**.

Soit $\mathcal{A}$ un fermé de Zariski de K^n. Toute partie E de $K[X]$ telle que $\mathcal{A} = \mathcal{A}_E(K)$ est appelée un **système d'équations de $\mathcal{A}$**. Si $E \subseteq k[X]$ ce système est dit **à coefficients dans k**. On appelle **ensembles k-algébriques** les ensembles algébriques (dans un corps algébriquement clos contenant k quelconque) ayant un système d'équations à coefficients dans k. Soit E une partie quelconque de $k[X]$, et pour tout corps L contenant k soit J_L l'idéal engendré par E dans $L[X]$. On sait que E est un système d'équations de $\mathcal{A}$ (à coefficients dans k) si et seulement si $I_K(\mathcal{A}) = \sqrt{J_K}$. Cela ne dépend pas du choix de K (pourvu qu'il soit algébriquement clos) donc il est équivalent de requérir que $I_{k^a}(\mathcal{A}) = \sqrt{J_{k^a}}$. Si E est un système d'équations de $\mathcal{A}$ à coefficients dans k, il est dit **réduit sur k** si J_k et un idéal réduit *i.e.* si $J_k = \sqrt{J_k}$, et **absolument réduit** s'il est réduit sur k^a (ou sur K, ou sur toute extension de k, c'est équivalent). Il est dit **irréductible** (sur k) si $\sqrt{J_k}$ est un idéal premier de $k[X]$, et **absolument irréducible** s'il est irréductible sur k^a (ou sur toute extension de k).

$\mathcal{A}$ est lui-même dit **irréductible sur k** (resp. **absolument irréductible**) s'il admet un système d'équations irréductible sur k (resp. absolument irréductible). De même il est dit **réduit sur k** (resp. **absolument réduit**) s'il admet un système d'équations ayant ces propriétés. On sait que $\mathcal{A}$ est une variété si et seulement s'il est absolument irréductible, et dans ce cas tout système d'équations de $\mathcal{A}$ à coefficients dans k est absolument irréductible (de même si $\mathcal{A}$ est irréductible sur k tout système d'équations de $\mathcal{A}$ à coefficients dans k est irréductible). On appelle **variétés définies sur k** les ensembles k-algébriques absolument irréductibles et absolument réduits. On sait que si V est une variété définie sur k^a il existe une plus petite extension algébrique (finie) de k sur laquelle V est définie.

Soit $\mathcal{A}$ un ensemble k-algébrique. L'**idéal de $\mathcal{A}$ sur k** est $\boldsymbol{I_k(\mathcal{A})}$:$= \{f \in k[X] \ / \ \forall x \in \mathcal{A},\ f(x) = 0\}$. Nous le noterons simplement $I(\mathcal{A})$ chaque fois que la référence à k ne sera pas indispensable. $I_k(\mathcal{A})$ ne dépend pas du corps algébriquement clos considéré. On note $\boldsymbol{k[\mathcal{A}]}$:$= k[X]/I_k(\mathcal{A})$ et on l'appelle l'**anneau des fonctions** (k-rationnelles) de $\mathcal{A}$. On sait que $I_k(\mathcal{A})$ est un système d'équations de $\mathcal{A}$ réduit sur k (mais pas forcément absolument réduit). $\mathcal{A}$ est irréductible sur k si et seulement si $I_k(\mathcal{A})$ est premier *i.e.* si et seulement si $k[\mathcal{A}]$ est intègre, et dans ce cas on appelle **corps des fonctions** (k-rationnelles) de $\mathcal{A}$ le corps des fractions $\boldsymbol{k(\mathcal{A})}$ de $k[\mathcal{A}]$. Nous aurons souvent recours à la caractérisation suivante :

Théorème 5
Un ensemble k-algébrique $\mathcal{A}$ est une variété définie sur k si et seulement si $k[\mathcal{A}]$ est intègre et $k(\mathcal{A})$ est une extension régulière de k.

Soit $\mathcal{A}$ un ensemble k-algébrique, et B une k-algèbre. On appelle **point de $\mathcal{A}$ à coefficients dans B** tout $x \in B^n$ tel que quel que soit $f \in I_k(\mathcal{A})$ on ait $f(x) = 0$. Je note $\boldsymbol{\mathcal{A}(B)}$ l'ensemble des points de $\mathcal{A}$ à coordonnées dans B. Un point $x \in B^n$ sera dit **générique de $\mathcal{A}$ sur k** si quel que soit $f \in k[\mathcal{A}]$ on a $f(x) = 0 \iff f \in I_k(\mathcal{A})$.

La projection canonique de $k[X]$ dans $k[\mathcal{A}]$ envoie X sur un point générique de $\mathcal{A}$ sur k, que nous noterons souvent $x_{\mathcal{A}}$. Si x est un autre point générique de $\mathcal{A}$ sur k il existe un isomorphisme de k-algèbre (unique) envoyant x sur $x_{\mathcal{A}}$, ce qui autorise à parler **du** point générique de $\mathcal{A}$ sur k.

Soit V une variété définie sur k, et $E \in k[X]^m$ un système absolument réduit d'équations de V. La **dimension** de V est le degré de transcendance de $k(V)$ sur k. On sait que si $x \in V(B)$ (où B est une k-algèbre quelconque) le rang de la matrice jacobienne de E en x est inférieur ou égal à $n - \dim(V)$. Le point x sera dit **lisse** ou **régulier** si ce rang est égal à $n - \dim(V)$. Par exemple un point générique de V sur k est toujours lisse. Je note $\boldsymbol{V^\circ(B)}$ l'ouvert de lissité de V, c'est-à-dire l'ensemble des points lisses de V dans B.

Si V est une variété définie sur k^a ayant un système d'équations à coefficients dans k, et si $V^\circ(k) \neq \emptyset$, alors V est définie sur k : en effet la fonction d'évaluation $f \mapsto f(x)$ pour un certain $x \in V^\circ(k)$ définit une place de $k(V)$ dans k, ce qui garantit que l'extension $k(V)|k$ est régulière.

Remarque: Les géomètres distinguent les notions de points lisses et réguliers, mais quand leurs variétés sont absolument réduites (ce qui est toujours le cas pour nous) les deux notions coïncident. Avec nos conventions, la distinction est donc inutile.

Exemple de variété

Il nous faudra souvent déterminer si un système d'équations polynômiales est absolument réduit et absolument irréductible. Pour éviter de répéter des vérifications fastidieuses, nous donnons ici un type d'équations définissant des variétés, suffisamment général pour englober tous les cas particulier que nous rencontrerons.

Proposition 6
Soit V une variété définie sur k, d'idéal $I_k(V)$, et $f := (f_1, \ldots, f_m) \in k[X]^m$ ($X := (X_1, \ldots, X_n)$) un système absolument réduit d'équations de V.
Soient $g_0, \ldots, g_s, h_0, \ldots, h_s \in k[X]$ tels que :
- *h_0 est constant et non nul ;*
- *$g_0 \notin I(V)$;*
- *$\forall i \in [\![1, s]\!]$, $h_i \neq 0$, $g_i \notin I(V)$, et si $h_i \notin k^*$, alors $g_i | g_0$.*

Soit $Y := (Y_0, \ldots, Y_s)$ une nouvelle suite d'indéterminées, et pour tout $i \in [\![0, s]\!]$ soit $f_{m+i+1}(X, Y) := g_i(X)Y_i - h_i(X)$. Enfin, soit W l'ensemble k-algébrique d'équations $F = 0$, où $F := (f_1, \ldots, f_{m+s+1})$.
Alors W est une variété définie sur k, de même dimension que V, et F en est un système d'équations absolument réduit. De plus, si un point $x \in V^\circ(k)$ n'annule aucun des g_i, alors le point (x, y) défini par $y_i := h_i(x)/g_i(x)$ pour $i \in [\![0, s]\!]$, appartient à $W^\circ(k)$.

Preuve: L'idéal engendré par F dans $k^a[X, Y]$ contient celui engendré par f, et on a donc :

$$k^a[X, Y]_{/(F)} \simeq (k^a[x_V])[Y]_{/(F(x_V, Y))}.$$

Notons $A := k^a[x_V]$, et pour tout $i \in [\![0, s]\!]$, $u_i := g_i(x_V)$, $v_i := h_i(x_V)$. Nous allons vérifier que l'idéal I engendré dans $A[Y]$ par les $u_iY_i - v_i$ est premier.

Soit S la partie multiplicative de $A[Y]$ engendrée par les u_i. Par hypothèse les $g_i \notin I_k(V)$, donc les u_i sont non nuls, et comme $A[Y]$ est intègre, il s'ensuit que $0 \notin S$.

Soit $a \in A[Y]$ et $i \in [\![0,s]\!]$ tel que $u_i a \in I$. Il y a deux cas possibles :

- ou bien $h_i \in k^*$, alors $v_i \in A^*$, et $u_i a \in I \Longrightarrow u_i Y_i a \in I \Longrightarrow v_i a \in I \Longrightarrow a \in I$;
- ou bien $h_i \notin k^*$, et alors $g_i | g_0$, donc il existe $u'_i \in A$ tel que $u_0 = u_i u'_i$, et donc $u_i a \in I \Longrightarrow u_i u'_i a \in I \Longrightarrow u_0 a \in I$, et puisque $h_0 \in k^*$ on est ramené au premier cas, *i.e.* $a \in I$.

On voit donc que pour tout $s \in S$ et tout $a \in A[Y]$, si $sa \in I$ alors $a \in I$. On sait qu'alors $I = S^{-1}I \cap A[Y]$, où $S^{-1}I$ est l'idéal engendré par I dans $S^{-1}A$, et que $A/I = S^{-1}A/S^{-1}I$. Or dans $S^{-1}A$, les u_i sont inversibles, donc $S^{-1}I$ est l'idéal engendré par les $Y_i - v_i/u_i$, et il est donc clair que $S^{-1}A/S^{-1}I = A[v_0/u_0, \ldots, v_s/u_s]$.

On a montré que $k^a[X,Y]/(F) = A/I = A[v_0/u_0, \ldots, v_s/u_s]$, en particulier cet anneau est intègre, donc W est bien irréductible sur k ; et $k(W) = \mathrm{Fr}(k^a[X,Y]/(F)) = \mathrm{Fr}(A) = k(V)$ donc l'extension $k(W)|k$ est régulière, et W est bien une variété définie sur k dont F est un système d'équations absolument réduit. Enfin V et W, ayant même corps des fonctions, ont même dimension.

Soit $x \in V^\circ(k)$ n'annulant pas les g_i, et $(x,y) \in k^{n+s}$ défini par $y_i := h_i(x)/g_i(x)$ pour $i \in [\![0,s]\!]$. Il est clair que $F(x,y) = 0$, donc $(x,y) \in W(k)$. Le jacobien de F en (x,y) s'écrit :

$$J_F(x,y) = \begin{vmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} & & & \\ \vdots & & \vdots & & 0 & \\ \frac{\partial f_m}{\partial X_1} & \cdots & \frac{\partial f_m}{\partial X_n} & & & \\ & & & g_1(x) & & \\ & * & & & \ddots & \\ & & & & & g_s(x) \end{vmatrix} = \begin{vmatrix} J_f(x) & & 0 & \\ & g_1(x) & & \\ * & & \ddots & \\ & & & g_s(x) \end{vmatrix}$$

Les $g_i(x)$ étant non nuls cette matrice est de rang $rg(J_f(x)) + s$, et puisque $x \in V^\circ(k)$ $rg(J_f(x)) = n - \dim V$. On a donc :

$$(n+s) - rg(J_F(x,y)) = (n+s) - (n - \dim V + s) = \dim V = \dim W$$

et (x,y) est bien un point lisse de W.

■

Remarque: Si pour tout $i \in [\![1,s]\!]$, h_i ou g_i est élément de k^*, alors il est clair que le même résultat reste vrai quand on élimine l'équation $g_0 Y_0 - h_0$, ce que nous ne manquerons pas de faire. Nous laissons au lecteur le soin de vérifier, comme nous l'affirmons ici, que tous les systèmes d'équations considérés dans cette thèse dont nous dirons qu'ils sont absolument irréductibles et absolument réduits peuvent se mettre sous la forme ci-dessus (sans l'équation suplémentaire $g_0 Y_0 - h_0$ s'il y a lieu).

Le théorème des fonctions implicites

Prestel et Ziegler ont étudié dans [P-Z] la notion fondamentale suivante :

Définition

(1) Un corps topologique K est dit **t-hensélien**, relativement à une topologie τ non discrète, si (K,τ) satisfait le théorème des fonctions implicites (TFI) pour les variétés, c'est-à-dire si :

pour toute variété V définie sur K, de dimension $d \geq 1$, si V possède un point lisse $x := (x_1, \ldots, x_n)$ dans K, alors, quitte à renuméroter les coordonnées de x, il existe

un voisinage U_1 de $(x_1, \ldots, x_d)$ et un voisinage U_2 de $(x_{d+1}, \ldots, x_n)$ tels que pour tout $(y_1, \ldots, x_d) \in U_1$ il existe un unique $(y_{d+1}, \ldots, y_n) \in U_2$ tel que $(y_1, \ldots, x_n) \in V(K)$.
(2) Je dirais d'un anneau A qu'il est **t-hensélien** s'il est intègre et si son corps des fractions K est t-hensélien relativement à une topologie qui fait de A un ouvert de K.

D'après [P-Z], un corps t-hensélien (K, τ) est un corps V-topologique, c'est à dire, en vertu d'un théorème de Kowalsky-Dürbaum et Fleisher rappelé dans [P-Z], que l'on peut trouver un ordre ou une valuation sur K qui induise la topologie τ. Il s'ensuit que si A est un anneau t-hensélien, et B une extension élémentaire de A, on peut trouver une topologie qui prolonge celle de A et qui fasse de B un anneau t-hensélien.

Lemme 7
Soit $(\overline{R}, \tau)$ un anneau t-hensélien, de corps des fractions $\overline{F}$. Soit R un sous-anneau de $\overline{R}$, et V une variété de dimension $d \geq 1$, définie sur $F := \mathrm{Fr}(R)$. On suppose que V a un point lisse x dans R^n, et que le degré de transcendance de $\overline{F}$ sur F est supérieur ou égal à d.
Alors V possède un point générique (sur F) dans tout voisinage de x dans $\overline{F}^n$, et en particulier dans $\overline{R}^n$.

La preuve est une application du TFI, en notant que les éléments de $\overline{F}^d$ dont les coordonnées sont algébriquement indépendantes sur F sont denses dans $\overline{F}^d$ pour la topologie produit (l'argument est emprunté à la preuve de 3.3 (v*) p. 188 de [P-S 90]).

J'emploierai souvent ce lemme dans le contexte suivant :
R est un anneau t-hensélien, et $\overline{R}$ une extension élémentaire de R de cardinal strictement plus grand que $|R|$ (par exemple une ultra-puissance non triviale de R). Alors R est t-hensélien et le degré de transcendance de $\mathrm{Fr}(\overline{R})$ sur $\mathrm{Fr}(R)$ est infini. Je dirai alors :

"le TFI nous donne dans $\overline{R}$ un point générique de V sur $F\ldots$"

Notons que si A est un sous-anneau de R, tel que F soit algébrique sur $K := \mathrm{Fr}(A)$ et que V soit définie sur K, alors $K(x_V)$ est une extension régulière de K donc F et $K(x_V)$ sont K-linéairement disjoints (en notant x_V un point générique sur F de V, donné par le TFI dans une extension élémentaire $\overline{R}$ assez grande de R, l'indépendance linéaire étant vue dans $\mathrm{Fr}(\overline{R})$). Comme R et $K(x_V)$ sont des A-modules plats $A[x_V] \otimes_A R$ s'injecte dans $K(x_V) \otimes_A F = K(x_V) \otimes_K F \simeq F(x_V)$. Il s'ensuit que :

$$R[x_V] = AR[x_V] \simeq A[x_V] \otimes_A R.$$

Un autre application utile du théorème des fonctions implicites est donnée par le lemme suivant :

Lemme 8
Soit R un anneau t-hensélien, V une variété définie sur $\mathrm{Fr}(R)$, x un point lisse de V dans R, et f un polynôme à coefficients dans R n'appartenant pas à $I(V)$.
Alors on peut trouver dans tout voisinage de x un point $y \in V^\circ(R)$, tel que $f(y) \neq 0$.

Preuve: (idée) On commence par prendre une ultra-puissance non triviale R' de R. Le lemme 7 nous donne dans R' un point générique x_V de V sur $\mathrm{Fr}(R)$ aussi proche que l'on veut de x ; $f \notin I(V)$, donc $f(x_V) \neq 0$, et la propriété "il existe un point lisse de V dans tel voisinage fixé (à paramètre dans R) de x en lequel f ne s'annule pas" se dit par une formule existentielle du langage des anneaux, enrichi d'un prédicat pour l'ordre ou la valuation définissant la topologie de R (et de R'). Cette formule est satisfaite par x_V dans R', et puisque R est existentiellement clos dans R' (au sens de ce langage enrichi), il s'ensuit qu'elle est aussi satisfaite dans R, c.q.f.d.

■

Chapitre I
Passages du local au global

Résumé : Nous introduisons ici les notions qui forment la toile de fond de cette thèse, en insistant sur la forte signification logique des principes locaux-globaux du type du principe de Hasse. En particulier nous tirons du théorème de Moret-Bailly ses conséquences immédiates les plus utiles pour un théoricien des modèles.

§ 1. Principes locaux-globaux en théorie des modèles

Définitions

Ershov a introduit dans [E 92b] une notion de clôture régulière relative pour les corps, dont l'adaptation la plus littérale au cadre des anneaux intègres est la suivante :
un anneau intègre A de corps des fractions K, est **régulièrement clos relativement à une famille** $\mathcal{R}$ d'anneaux contenant A et inclus dans K^a (ce qu'on notera $A \in \mathrm{RC}(\mathcal{R})$) si et seulement si A est existentiellement clos dans tout anneau intègre B vérifiant :

- $A \subseteq B$ et l'extension $\mathrm{Fr}(B)|\mathrm{Fr}(A)$ est régulière ;
- $\forall R \in \mathcal{R}, \quad R \leq_{\exists} R \otimes_A B$.

Nous reprenons aussi de [E 92b] la notion suivante : si W est une famille d'anneaux de valuations de K, nous dirons que A est **régulièrement clos relativement à** W s'il l'est relativement à la famille $\mathcal{F} := \{H_R(K) \,/\, R \in W\}$. On le note $A \in \mathrm{RC}(W)$.

Remarque: Avec les notations de la définition, si tous les éléments de $\mathcal{R}$ sont des corps alors K lui-même est une extension régulière de $\mathrm{Fr}(A)$ et pour tout $R \in \mathcal{R}$ on a $R \otimes_A K = R$ donc trivialement $K \leq_{\exists} R \otimes_A K$. Si $A \in \mathrm{RC}(\mathcal{R})$ il s'ensuit que $A \leq_{\exists} K$ donc que $A = K$ *i.e.* que A est un corps. En particulier si $A \in \mathrm{RC}(W)$ alors A est un corps.

Exemples:
(1) Un corps K est dit **pseudo algébriquement clos** (en abrégé **PAC**) s'il est existentiellement clos dans toute extension régulière. On voit qu'un anneau intègre A est un corps PAC si et seulement si $A \in \mathrm{RC}(\emptyset)$.
(2) Un corps K est dit **pseudo réel clos** (en abrégé **PRC**) s'il est existentiellement clos dans toute extension régulière L telle que tout ordre de K se prolonge à L. On sait qu'un anneau intègre A est un corps PRC si et seulement si $A \in \mathrm{RC}(\mathcal{F})$, où $\mathcal{F}$ est l'ensemble des corps réels clos algébriques sur $\mathrm{Fr}(A)$.

(3) Rappelons qu'une ***p*-valuation de rang *d*** est une valuation v d'anneau R sur un corps K de caractéristique nulle telle que $p \in m(R)$ et $\dim(R/pR) = d$, où la dimension est à prendre au sens des $\mathbb{F}_p$-espaces vectoriels (*cf.* [P-R]). En particulier, v est de rang 1 si et seulement si son corps résiduel est $\mathbb{F}_p$ et si $v(p)$ est le plus petit élément strictement positif de son groupe des valeurs (noté additivement). Un corps K est dit ***p*-adiquement clos (de rang *d*)** s'il admet une valuation p-adiquement close (de rang d) c'est-à-dire une p-valuation (de rang d) henselienne dont le groupe des valeurs Γ soit un $\mathbb{Z}$-groupe (*i.e.* Γ noté additivement, en plus de posséder un plus petit élément strictement positif, vérifie $|\Gamma/n\Gamma| = n$ pour tout $n \in \mathbb{N}^*$). De manière équivalente, K est p-adiquement clos si et seulement s'il admet une p-valuation et si aucune extension algébrique propre de K n'admet de p-valuation de même rang la prolongeant.
Étant donné un ensemble M de couples (p, d) deux à deux distincts où p est un entier premier et $d \in \mathbb{N}^*$, pour tout corps K notons $\mathcal{F}_M$ l'ensemble des extensions algébriques de K p-adiquement closes de rang d pour (p, d) décrivant M. Alors K est dit $\mathbf{PC}_{\boldsymbol{M}}$ si et seulement si $K \in \mathrm{RC}(\mathcal{F}_M)$. Si M est réduit au seul couple $(p, 1)$ les corps PC_M sont dits aussi **pseudo *p*-adiquement clos** (en abrégé **P*p*C**).

Remarque: Les valuations p-adiquement closes de rang quelconque ont de bonnes propriétés (*cf.* [P-R]) mais au début de l'étude des corps PC_M il a paru nécessaire de se restreindre au cas des corps régulièrement clos relativement à l'ensemble des corps p-adiquement clos (de rang 1) les contenant (*cf.* [Kü 89]). C'est pourquoi les définitions varient d'un auteur à l'autre en fonction des objectifs visés, et c'est pourquoi aussi il est peu de références dans la littérature auxquelles nous puissions renvoyer le lecteur pour les corps PC_M.

Plus récemment a été introduite une notion de corps RC_π très générale ; même si nous n'y recourrons pas directement nous renvoyons le lecteur à la série d'articles de Ershov cités dans la bibliographie sur ce sujet : on y trouvera nombre de preuves généralisant aux RC_π (et donc aux PC_M) les propriétés connues des PpC. Il en reste malheureusement dont l'adaptation aux PC_M a été démontrée mais jamais publiée, et qu'on ne pourra déduire des articles de Ershov. Il s'agit notamment de résultats faisant intervenir la théorie de Galois des corps PC_M. Nous avons vérifié auprès de Pop que ces résultats étaient bien démontrés, et nous en appelons à l'indulgence du lecteur pour l'absence de référence ou de preuve (en cas de doute, on pourra toujours se restreindre au cas PpC et trouver les démonstrations dans [Kü 89]).

Pour tous les exemples ci-dessus on sait caractériser la propriété de clôture régulière à l'aide d'un principe local-global analogue au principe de Hasse non singulier, tel qu'on peut le trouver énoncé dans [Lan] p. 248. La notion suivante définit un cadre général dans lequel cette caractérisation est possible.

Définition
Je dirai qu'un anneau intègre A est **géométriquement clos** si pour toute variété non vide V définie sur $\mathrm{Fr}(A)$, on a : $\qquad V^\circ(A) \neq \emptyset \quad \Longleftrightarrow \quad A \leq_\exists A[V]$.

Remarque: Dans cette définition seule l'implication de gauche à droite est significative : l'autre est vérifiée par tout anneau intègre. En effet, si $f := (f_1, \ldots, f_m) \in A[X_1, \ldots, X_n]^m$ est un système absolument réduit d'équations de V et Δ un déterminant de taille $n - \dim V$ extrait du jacobien de f tel que $\Delta(x_V) \neq 0$ (où $x_V \in A[V]$ est un point générique de V sur $\mathrm{Fr}(A)$), on a : $A[V] \models \exists x(f(x) = 0 \wedge \Delta(x) \neq 0)$. Puisque

$A \leq_\exists A[V]$, A aussi satisfait cette formule existentielle, *i.e.* $V^\circ(A) \neq \emptyset$.

Propriété 1

(1) *Tout anneau t-henselien est géométriquement clos.*

(2) *Soit $\mathcal{R}$ une famille d'anneaux géométriquement clos contenant tous un même anneau intègre A et tous inclus dans une clôture algébrique de $K := \mathrm{Fr}(A)$. Si $A \in \mathrm{RC}(\mathcal{R})$ alors A est géométriquement clos.*

Preuve:

(1) Soit R un anneau t-henselien, et V une variété définie sur $F := \mathrm{Fr}(R)$ telle que $V^\circ(R) \neq \emptyset$. Soit $\overline{R}$ une ultra-puissance non triviale de R. Le théorème des fonctions implicites nous donne dans $\overline{R}$ un point x_V générique de V sur F (cf. le lemme 7 dans les prérequis). Comme $R \preceq \overline{R}$ on a $R \leq_\exists R[x_V]$, *i.e.* $R \leq_\exists R[V]$.

(2) Soit V une variété définie sur K telle que $V^\circ(A) \neq \emptyset$. L'extension $K(V)|K$ est régulière et pour tout $R \in \mathcal{R}$ on a $V^\circ(R) \supseteq V^\circ(A) \neq \emptyset$ donc $R \leq_\exists R[V]$ puisque R est géométriquement clos, et $R[V] \simeq R \otimes_A A[V]$ (suivant les commentaires accompagnant le lemme 7 des prérequis), donc la clôture régulière entraîne que $A \leq_\exists A[V]$.

■

Proposition 2

Soit A un anneau intègre de corps des fractions K et soit $\mathcal{R}$ une famille d'anneaux inclus dans une clôture algébrique de K et contenant tous A. Si tous les éléments de $\mathcal{R}$ sont géométriquement clos, alors les propriétés suivantes sont équivalentes :

(i) $A \in \mathrm{RC}(\mathcal{R})$;

(ii) *pour toute variété non vide V définie sur K, et pour tout polynôme g à coefficients dans A n'appartenant pas à $I(V)$, si V possède un point lisse dans tout $R \in \mathcal{R}$, alors V possède dans A un point n'annulant pas g.*

Preuve:

(i)$\Longrightarrow$(ii) Soit V une variété définie sur K et g un polynôme à coefficients dans A tels que $g \notin I(V)$ et pour tout $R \in \mathcal{R}$, $V^\circ(R) \neq \emptyset$. Soit x_V un point générique de V sur K^a ; quel que soit $R \in \mathcal{R}$ on a $R[x_V] \simeq R \otimes_A A[x_V]$ (car R est inclus dans K^a qui est K-linéairement disjoint de $K[x_V]$) et puisque $V^\circ(R) \neq \emptyset$ et que R est géométriquement clos on a $R \leq_\exists R[x_V]$. Le (i) entraîne donc que $A \leq_\exists A[x_V]$.

Soit $f := (f_1, \ldots, f_m) \in A[X_1, \ldots, X_n]^m$ un système absolument réduit d'équations de V. Tous les f_i s'annulent en x_V, et $g \notin I(V)$, donc $g(x_V) \neq 0$. Il s'ensuit que $A[x_V] \models \exists x(f(x) = 0 \wedge g(x) \neq 0)$. Puisque $A \leq_\exists A[x_V]$, cette formule existentielle est aussi satisfaite par A, *i.e.* il existe $a \in V(A)$ tel que $g(a) \neq 0$.

(ii)$\Longrightarrow$(i) Soit B une extension régulière de A (*i.e.* $A \subseteq B$ et $L := \mathrm{Fr}(B)$ est une extension régulière de K) telle que pour tout $R \in \mathcal{R}$ on ait $R \leq_\exists R \otimes_A B$. On considère $h_1, \ldots, h_s \in A[X]$ ($X = (X_1, \ldots, X_n)$) et $b \in B^n$ tels que $B \models \bigwedge\!\!\!\bigwedge_{i=1}^r h_i(b) = 0 \bigwedge\!\!\!\bigwedge_{i=r+1}^s h_i(b) \neq 0$. Puisque L est une extension régulière de K, $K[b]$ aussi, et donc b est le point générique d'une variété V définie sur K ; soit $I(V)$ son idéal dans $K[X]$ et $f \in A[X]^m$ un système absolument réduit d'équations de V. Soit Δ un déterminant de taille $n - \dim V$ extrait du Jacobien de f tel que $\Delta(b) \neq 0$, et posons $g := \prod_{i=r+1}^s h_i$.

Quel que soit $R \in \mathcal{R}$, la formule $\exists x(f(x) = 0 \wedge \Delta(x) \neq 0)$ est satisfaite (par b) dans B donc aussi dans $R \otimes_A B$, et puisque $R \leq_\exists R \otimes_A B$ elle est encore satisfaite dans R *i.e.* V a un point lisse dans R. Le polynôme $g := \prod_{i=r+1}^s h_i$ ne s'annulant pas en b on a $g \notin I(V)$, donc (ii) donne un point $a \in V(A)$ tel que $g(a) \neq 0$. Il vient :

- $\forall i \in [\![1, r]\!],\ h_i \in I(V) \Longrightarrow h_i(a) = 0$;
- $\forall i \in [\![r+1, s]\!],\ g(a) \neq 0$ et $h_i | g \Longrightarrow h_i(a) \neq 0$.

D'où $A \models \bigwedge_{i=1}^{r} h_i(a) = 0 \bigwedge_{i=r+1}^{s} h_i(a) \neq 0$ et A est donc bien existentiellement clos dans B.

■

§ 2. LGPH et LGP de Moret-Bailly

Moret-Bailly a démontré dans [MB 89] un résultat apparenté au principe de Hasse non singulier, généralisant ainsi un théorème de Rumely paru dans [Ru 86]. Nous en donnons ici une traduction non schématique, peut-être plus faible que le théorème originel, mais qui a l'avantage d'être compréhensible par un logicien algébriste (non géomètre).

Notations: Soit k un corps et v une valeur absolue de k. Le complété de k relativement à v est noté k_v. Le prolongement canonique de v à k_v est encore noté v. Si v est non archimédienne on note $\mathcal{O}_v$ l'anneau de v dans k_v, et $\mathcal{O}_v^s$ (resp. $\mathcal{O}_v^a$) l'unique prolongement de $\mathcal{O}_v$ à k_v^s (resp. k_v^a). Si v est archimédienne, on pose $\mathcal{O}_v := k_v$, et donc $\mathcal{O}_v^s := k_v^s$ et $\mathcal{O}_v^a := k^a$.

Théorème 1 (Moret-Bailly)
Soient k une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$, Σ un ensemble de valeurs absolues de k et Σ_0 une partie finie de Σ. Pour tout $v \in \Sigma_0$ on fixe une extension algébrique F_v de k_v. Soit V une variété définie sur k vérifiant :

- $\forall v \in \Sigma_0,\ V^\circ(\mathcal{O}_v^s \cap F_v) \neq \emptyset$;
- $\forall v \in \Sigma,\ V^\circ(\mathcal{O}_v^s) \neq \emptyset$.

Si k possède une valeur absolue (non triviale) v_0 n'appartenant pas à Σ, alors il existe $x \in V^\circ(k^a)$ tel que :

- *$\forall v \in \Sigma_0$, x et tous ses k-conjugués sont à coordonnées dans $\mathcal{O}_v^s \cap F_v$;*
- *$\forall v \in \Sigma$, x et tous ses k-conjugués sont à coordonnées dans $\mathcal{O}_v^s$.*

Remarques:
(1) Le théorème de Rumely correspond au cas particulier où Σ est l'ensemble des valeurs absolues non archimédiennes de $\mathbb{Q}$, $\Sigma_0 = \emptyset$ et v_0 la valeur absolue usuelle de $\mathbb{Q}$.
(2) On n'affaiblirait pas le théorème en remplaçant les hypothèses par :

- $\forall v \in \Sigma_0,\ V^\circ(R_v^s \cap F_v) \neq \emptyset$;
- $\forall v \in \Sigma,\ V^\circ(R_v^s) \neq \emptyset$;

en notant $R_v^s := \mathcal{O}_v^s \cap k^s$. Cela découle par exemple du théorème suivant (*cf.* [Lan], chapitre X, § 3, p. 259) en prenant $K = F_v \cap k^s$ (resp. $K = k_v \cap k^s$) et $L = F_v \cap k_v^s$ (resp. $L = k_v$) pour tout $v \in \Sigma_0$ (resp. tout $v \in \Sigma$) :

Théorème 2 (Lang)
Soit v une valeur absolue sur un corps L et K un sous-corps dense dans L tel que l'extension $L|K$ soit régulière. Soit $\mathcal{S}$ un système fini d'équations polynomiales à coefficients dans K.
Alors l'ensemble des solutions de $\mathcal{S}$ à coordonnées dans K est dense (pour la topologie produit) parmi celles à coordonnées dans L.

Pour déduire du théorème de Moret-Bailly ses conséquences les plus intéressantes pour nous, il est nécessaire de le formuler autrement (nous prenons aussi en compte la remarque précédente).

Notations: On reprend celles du théorème de Moret-Bailly, et si v est une valeur absolue de k on pose :

- $R_v := \mathcal{O}_v \cap k^s$;
- $H_v(k) := \mathrm{Fr}(R_v)$, et $R_v^s := \mathcal{O}_v^s \cap k^s$.

On sait que si v est non archimédienne alors $H_v(k)$ n'est autre que le hensélisé de k relativement à la valuation de v, ce qui justifie les notations.

Si $\mathcal{F}$ est une famille d'extensions algébriques de k on note :

$$k_{\mathcal{F}} := \bigcap \{\sigma[F \cap k^s] \,/\, \sigma \in G(k),\ F \in \mathcal{F}\}$$

Autrement dit, $k_{\mathcal{F}}$ est l'ensemble des éléments de k^s dont le polynôme minimal sur k est scindé sur tout $F \in \mathcal{F}$.

Définition

Soit Σ un ensemble de valeurs absolues sur un corps K. Je dis que K satisfait le **LGP de Moret-Bailly relativement à Σ** si pour toute variété V définie sur K on a :

$$V^\circ\left(\bigcap_{v\in\Sigma} R_v \cap K\right) \neq \emptyset \quad\iff\quad \forall v \in \Sigma,\ V^\circ(R_v) \neq \emptyset.$$

Le théorème de Moret-Bailly peut alors être reformulé ainsi :

Théorème 3 (Moret-Bailly bis)

Soit k une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$. Soit Σ un ensemble quelconque de valeurs absolues de k et Σ_0 une partie finie de Σ. Pour tout $v \in \Sigma_0$ soit F_v une extension algébrique de $H_v(k)$, et soit $\mathcal{F}$ l'ensemble des F_v quand v décrit Σ_0. Enfin soit Π (resp. Π_0) l'ensemble des valeurs absolues de $k_{\mathcal{F}}$ qui prolongent les éléments de Σ (resp. Σ_0). S'il existe dans k une valeur absolue non triviale $v_0 \notin \Sigma$, alors $k_{\mathcal{F}}$ satisfait le LGP de Moret-Bailly relativement à Π.

Remarque: On sait que si on oublie de laisser libre au moins une valeur absolue de k le théorème devient faux. Ainsi $\mathbb{Q}_{\{\mathbb{R}\}}$ ne satisfait-il pas le LGP de Moret-Bailly relativement à l'ensemble de toutes ses valeurs absolues.

Preuve: Nous n'en donnons que les grandes lignes. Pour alléger on pose $L := k_{\mathcal{F}}$. Il faut commencer par vérifier que :

- $\{H_w(L) \,/\, w \in \Pi_0\} = \{\sigma[F_v] \,/\, \sigma \in G(k),\, v \in \Sigma_0\}$;
- $\forall w \in \Pi \setminus \Pi_0$, $H_w(L) = L^s = k^s$.

Cela fait, on considère une variété V définie sur L telle que $V^\circ(R_w) \neq \emptyset$ pour tout $w \in \Pi$. Soit k' l'extension de k engendrée dans L par les coefficients d'un système absolument réduit d'équations de V. C'est donc une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$ sur laquelle V est définie. On note Σ' (resp. Σ'_0) l'ensemble des valeurs absolues de k' prolongeant les éléments de Σ (resp. Σ_0).

Toute valeur absolue v de k' admet un prolongement w_v à L tel que $H_v(k') \subseteq H_{w_v}(L)$, et donc $R_v^s \cap H_{w_v}(L) = R_{w_v}$. En particulier, si $v \in \Sigma'_0$ on a $V^\circ(R_v^s \cap H_{w_v}(L)) = V^\circ(R_{w_v}) \neq \emptyset$. Si $v \in \Sigma'$ on a aussi $V^\circ(R_v^s) = V^\circ(R_{w_v}) \neq \emptyset$. Le théorème de Moret-

Bailly nous donne donc un point $x \in V^\circ(k'^a)$ tel que :

– $\forall v \in \Sigma'_0$, x et tous ses k'-conjugués sont à coordonnées dans R_{w_v}. Or pour tout $w \in \Pi_0$, la restriction v' de w à k' appartient à Σ'_0 et $R_{w_{v'}}$ se plonge au-dessus de k' dans R_w, donc x est à coordonnées dans R_w.

– $\forall v \in \Sigma'$, x et tous ses k'-conjugués sont à coordonnées dans R^s_v. Or pour tout $w \in \Pi \setminus \Pi_0$, la restriction v' de w à k' appartient à Σ' et $R^s_{w_{v'}}$ est k'-isomorphe à R_w, donc x est à coordonnées dans R_w.

Il s'ensuit que les coordonnées de x sont dans :

$$\bigcap_{w\in\Pi} R_w = \bigcap_{w\in\Pi} R_w \cap \bigcap_{w\in\Pi_0} H_w(L) = \bigcap_{w\in\Pi} R_w \cap L$$

Ce qu'il fallait démontrer.

■

Introduction du LGPH

Définition

Un anneau A satisfait le **LGPH** si et seulement s'il est intègre et s'il vérifie les propriétés suivantes :

(LGPH1) $\forall a \in A \setminus \{0\}$, $M(a)^c$ est quasi-compact ;

(LGPH2) pour toute variété V définie sur $K := \mathrm{Fr}(A)$ on a :

$$V^\circ(A) \neq \emptyset \quad \Longleftrightarrow \quad \forall R \in W_A,\ V^\circ(R^h) \neq \emptyset.$$

Le LGPH2 sera aussi appelé **condition géométrique** du LGPH.
Il est commode d'introduire tout de suite une version très affaiblie de cette propriété. Un anneau A satisfait le **LGPH'** si et seulement s'il est intègre, vérifie (LGPH1) et :

(LGPH2 bis) pour toute variété V définie sur $\mathrm{Fr}(A)$ on a :

$$V^\circ(A) \neq \emptyset \quad \Longleftrightarrow \quad \forall R \in W_A,\ V^\circ(R^h) \neq \emptyset \ \text{ et } \ V^\circ(K) \neq \emptyset.$$

Remarque:

(1) Le "H" est là pour rappeler que les points locaux sont pris dans les henselisés (*cf.* variantes plus loin).

(2) On est en droit de penser qu'un anneau intègre satisfaisant (LGPH2) a suffisamment de propriétés intéressantes sans qu'il soit besoin de lui demander de vérifier en prime (LGPH1). De fait, j'ai cru plusieurs fois parvenir à éliminer cette hypothèse, dernier résidu d'une longue suite de simplification des LGP considérés, en la déduisant de (LGPH2). J'ai finalement dû y renoncer, et (LGPH1) restera donc pour nous une hypothèse nécessaire (bien que trivialement vérifiée dans tous les cas utiles : tout anneau de dimension 1, par exemple, la satisfait).

(3) Modulo la condition géométrique du LGPH, le (LGPH1) est équivalent à d'autres propriétés peut-être plus parlantes, comme la bonne factorisation (que nous introduisons au prochain paragraphe), la BAP ou le fait d'être localement booléen (des concepts que nous étudierons au prochain chapitre). J'ai choisi de le donner sous cette forme parce que le (LGPH1) est plus faible que toutes ces conditions.

Le lien entre LGPH (ou LGPH') et LGP de Moret-Bailly est résumé dans l'énoncé suivant :

Proposition 4
Soit A un anneau intègre et intégralement clos, tel que tout element de W_A definisse une valeur absolue. Notons K son corps des fractions et Σ_A l'ensemble des valeurs absolues de K associées aux éléments de W_A. Soit Σ_0 un ensemble quelconque de valeurs absolues de K tel que $\Sigma_0 \setminus \Sigma_A$ ne soit composé que de valeurs absolues archimédiennes. Enfin posons $\Sigma := \Sigma_0 \cup \Sigma_A$; alors :

(a) *A satisfait le LGPH si et seulement si K satisfait le LGP de Moret-Bailly relativement à Σ_A.*
(b) *Supposons que K satisfasse le LGP de Moret-Bailly relativement à Σ_0.*
Alors A satisfait le LGPH' si et seulement si K satisfait le LGP de Moret-Bailly relativement à Σ.

Remarque: On voit sur cet énoncé à quoi sert le LGPH' : c'est une astuce formelle qui permet d'isoler ce qui dans le LGP dépend des valeurs absolues archimediennes pour ne s'intéresser provisoirement qu'aux autres.

Preuve: Remarquons tout de suite que A vérifie (LGPH1). En effet par hypothèse tout $R \in W_A$ induit une valeur absolue donc n'a pas d'idéal premier autre que (0) et $m(R)$, et ceci valant pour tout $R \in W_A$ on voit que $\mathrm{Sp}(A)$ est réduit à $\mathrm{Spm}(A) \cup \{(0)\}$. Il s'ensuit que quel que soit $a \in A \setminus \{0\}$ on a $M(a)^c = D(a) \setminus \{(0)\}$ (où $D(a) = \{\mathfrak{p} \in \mathrm{Sp}(A) \;/\; a \notin \mathfrak{p}\}$) ensemble qu'on sait être quasi-compact.

Notons également que puisque A est intégralement clos $A = \cap W_A$, et puisque les valeurs absolues de $\Sigma_0 \setminus \Sigma_A$ sont toutes infinies on a :

$$\bigcap\{R_v \cap K \;/\; v \in \Sigma\} = \bigcap\{R_v \cap K \;/\; v \in \Sigma_A\} = \cap W_A = A.$$

Enfin avec nos hypothèses pour toute valuation v de K d'anneau $R \in W_A$ on a $R^h = \mathcal{O}_v \cap K^s = R_v$. Le (a) en découle immédiatement

Pour prouver (b) on suppose que K satisfait le LGP de Moret-Bailly relativement à Σ_0.

($\Longrightarrow$) Si K satisfait le LGP de Moret-Bailly relativement à Σ et si V est une variété définie sur K ayant un point lisse dans K et dans tout R^h pour R décrivant W_A, alors pour tout $v \in \Sigma$ on a :

- Si $v \notin \Sigma_A$ alors v est infinie donc $V^\circ(R_v) \supseteq V^\circ(K) \neq \emptyset$.
- Si $v \in \Sigma_A$ alors il existe $R \in W_A$ tel que v soit la valuation d'anneau R, donc $V^\circ(R_v) = V^\circ(R^h) \neq \emptyset$.

Le LGP de Moret-Bailly relativement à Σ donne donc un point lisse x de V à coordonnées dans $\bigcap\{R_v \cap K \;/\; v \in \Sigma\}$ *i.e.* à coordonnées dans A.

($\Longleftarrow$) Si A satisfait le LGPH' et si V est une variété définie sur K telle que $V^\circ(R_v) \neq \emptyset$ pour tout $v \in \Sigma$, alors le LGP de Moret-Bailly relativement à Σ_0 donne un point lisse de V à coordonnées dans K, d'où avec le LGPH' un point lisse x de V à coordonnées dans A *i.e.* dans $\bigcap\{R_v \cap K \;/\; v \in \Sigma\}$.

■

Le théorème de Moret-Bailly nous donne donc de nombreux exemples d'anneaux satisfaisant le LGPH ou le LGPH' et inclus dans la clôture algébrique de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$. Nous en énumérons maintenant quelques-uns.

Notations: $v_{\mathbb{R}}$ désigne la valeur absolue usuelle de $\mathbb{Q}$, et pour tout nombre premier p on note v_p sa valeur absolue p-adique.

Définition
Avec les notations du théorème 3, $\mathbb{Q}_{\{\mathbb{R}\}}$ est appelé le corps des **nombres algébriques absolument réels**, nous le noterons $\mathbb{Q}_{r-abs}$.
De même, si M est en ensemble fini de couples (p,d) où p est un entier premier et $d \in \mathbb{N}^*$, nous noterons $\mathbb{Q}_{\boldsymbol{M-abs}} := \mathbb{Q}_{\mathcal{F}}$ où $\mathcal{F}$ est l'ensemble des corps p-adiquement clos de rang d algébriques sur $\mathbb{Q}$.
Les éléments de $\mathbb{Q}_{M-abs}$ sont appelés les **nombres algébriques absolument M-adiques**.

Corollaire 5
(a) *La clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}^a$ satisfait le LGPH.*
(b) *Pour tout nombre premier p, la clôture intégrale de $\mathbb{F}_p[T]$ dans $\mathbb{F}_p(T)^s$ satisfait le LGPH.*
(c) *Pour toute famille finie M de couples (p,d) où p est un entier premier et $d \in \mathbb{N}^*$, $\mathbb{Q}_{M-abs}$ est PC_M et la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_{M-abs}$ satisfait le LGPH.*

Preuve:
(a) C'est le théorème de Rumely. On le retrouve à partir de Moret-Bailly bis en prenant pour Σ l'ensemble des valeurs absolues finies de $\mathbb{Q}$ (ce qui laisse libre la valeur absolue usuelle de $\mathbb{Q}$) et $\Sigma_0 = \emptyset$.

(b) C'est le théorème de Moret-Bailly bis avec pour Σ l'ensemble des valeurs absolues de $\mathbb{F}_p(T)$ associées aux anneaux de valuation contenant $\mathbb{F}_p[T]$ (ce qui laisse libre la place à l'infini) et $\Sigma_0 = \emptyset$.

(c) On pose $\mathcal{P} := \{p \in \mathbb{N} /\ \exists d \in \mathbb{N}^*,\ (p,d) \in M\}$, et pour tout $p \in \mathcal{P}$ on note F_{v_p} l'intersection de toutes les extensions algébriques de $\mathbb{Q}_p \cap \mathbb{Q}^a$ qui sont p-adiques de rang d, avec $(p,d) \in M$. Alors le théorème de Moret-Bailly bis en prenant pour Σ l'ensemble des valeurs absolues non archimédiennes de $\mathbb{Q}$ (ce qui laisse libre la valeur absolue usuelle de $\mathbb{Q}$), pour Σ_0 les valeurs absolues associées aux valuations p-adiques de $\mathbb{Q}$ pour p décrivant $\mathcal{P}$, et quelle que soit $v \in \Sigma_0$, F_v comme ci-dessus, nous donne la conclusion (*via* la proposition 4).

■

Pour les absolument réels, on introduit encore quelques notations :
- $\mathbb{Z}_{r-abs}$ est la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_{r-abs}$, et pour tout $a \in \mathbb{Z}_{r-abs} \setminus \{0\}$ on pose :
- $\mathbb{Z}_{r-abs}(a) := S_a^{-1}\mathbb{Z}_{r-abs}$ où $S_a := \mathbb{Z}_{r-abs} \setminus \cup M(a)$;
- $\mathbb{Z}^{\circ}_{r-abs}(a) := T_a^{-1}\mathbb{Z}_{r-abs}$ où $T_a := \mathbb{Z}_{r-abs} \setminus \cup M(a)^c$.

Corollaire 6
$\mathbb{Q}_{r-abs}$ est PRC et pour tout élément non nul a de $\mathbb{Z}_{r-abs}$ on a :
(a) *$\mathbb{Z}_{r-abs}(a)$ satisfait le LGPH';*
(b) *si a est non inversible alors $\mathbb{Z}^{\circ}_{r-abs}(a)$ satisfait le LGPH'.*

Preuve: Le fait que $\mathbb{Q}_{r-abs}$ soit PRC découle immédiatement du théorème de Moret-bailly bis, en prenant $\Sigma = \Sigma_0 = \{v_{\mathbb{R}}\}$.

Soit a un élément de $\mathbb{Z}_{r-abs} \setminus \{0\}$; posons $A := \mathbb{Z}_{r-abs}(a)$ (resp. $A := \mathbb{Z}^{\circ}_{r-abs}(a)$). Soit Σ_A l'ensemble de valeurs absolues de $\mathbb{Q}_{r-abs}$ associées aux éléments de W_A, et Σ_0 l'ensemble des valeurs absolues archimédiennes de $\mathbb{Q}_{r-abs}$. Dans les deux cas il existe une valeur absolue non archimédienne de $\mathbb{Q}(a)$ qui n'est pas la trace sur $\mathbb{Q}(a)$ d'un élément de Σ_A (prendre un anneau de valuation R de $\mathbb{Q}(a)$ tel que $a \notin m(R)$ pour (a) et tel que $a \in m(R)$ pour (b)) donc le théorème 3 montre que $\mathbb{Q}_{r-abs}$ satisfait le LGP de Moret-Bailly relativement à $\Sigma_A \cup \Sigma_0$.

Puisque $\mathbb{Q}_{r-abs}$ est PRC *i.e.* puisqu'il satisfait le LGP de Moret-Bailly relativement à Σ_0 la proposition 4 s'applique et entraîne que A satisfait le LGPH'.

■

Remarque: Le fait que $\mathbb{Q}_{r-abs}$ soit PRC était déjà connu (selon [FHV] ce résultat est demontré dans [Pop]).

§ 3. LGPH et anneaux de Rumely

Dans leur axiomatisation de l'anneau de tous les entiers algébriques van den Dries et Macintyre introduisent l'expression "Rumely domain" pour désigner les anneaux de Prüfer de corps des fractions algébriquement clos qui satisfont la condition géométrique du LGPH (*cf.* [VdD-M] (3.6)). Ils introduisent en outre la condition de "block factorisation" suivante :

Définition
Un anneau A a **bonne factorisation** (en abrégé BF) si et seulement si pour tout $b \in A \setminus \{0\}$, tout élément a de $A \setminus \{0\}$ se factorise sous la forme $a = a_1 a_2$ avec $M(a_1) = M(a) \cap M(b)$ et $M(a_2) = M(a) \setminus M(b)$.

Nous allons dans ce paragraphe montrer comment déduire cette propriété du LGPH' (c'est uniquement là qu'intervient la curieuse condition (LGPH1) de notre définition, qui est donc équivalente à la bonne factorisation modulo (LGPH2 bis) et *a fortiori* modulo (LGPH2)).

Remarque: La bonne factorisation paraît s'apparenter à la factorialité, mais l'analogie a ses limites :
(1) $\mathbb{Q}[X, Y]$, bien que factoriel, ne satisfait pas BF.
(2) Tout anneau local a bonne factorisation. En particulier BF n'implique pas la factorialité, ni Prüfer.
(3) Cependant, un anneau de Prüfer noethérien (*i.e.* de Dedekind) a bonne factorisation si et seulement s'il est factoriel, comme nous le vérifierons au prochain chapitre.

Proposition 1
Soit A un anneau satisfaisant le LGPH 2bis.
Alors A est de Bezout.

Preuve: Soient $a, b \in A \setminus \{0\}$. Le système d'équations $(X(aU+bV) = a, Y(aU+bV) = b)$ détermine une variété V définie sur $\mathrm{Fr}(A)$, non vide et lisse. V a un point dans chaque R appartenant à W_A (car R est de Bezout) et dans $\mathrm{Fr}(A)$, donc $V(A) \neq \emptyset$ (par le LGPH 2bis). Soit $(u, v, x, y) \in V(A)$, et $d := au + bv$. Par construction $d \in aA + bA$, et d'autre part $a = dx$ et $b = dy$, donc $aA + bA \subseteq dA$. D'où $aA + bA = dA$.

■

Définition
Une famille W d'anneaux de valuation sur un corps K est dite **indépendante** si deux

éléments quelconques $R \neq R' \in W$ sont indépendants, c'est-à-dire si $RR' = K$.
Un anneau intègre A est dit **indépendant** si et seulement si W_A est indépendante.

Lemme 2
Soit A un anneau satisfaisant le LGPH 2bis. Soient $a \in A \setminus \{0\}$, et $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Sp}(A)$.
Si $\mathfrak{p}_1$ et $\mathfrak{p}_2$ ne sont pas comparables pour l'inclusion, alors il existe $a_1, a_2 \in A$ tels que $a = a_1 a_2$, $a_1 \notin \mathfrak{p}_1$ et $a_2 \notin \mathfrak{p}_2$ i.e. *$a = a_1 a_2$ et $|a_1|_{\mathfrak{p}_1} = |a_2|_{\mathfrak{p}_2} = 1$.*

Preuve: Soient $c_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$ et $c_2 \in \mathfrak{p}_2 \setminus \mathfrak{p}_1$.
Quitte à remplacer c_i par $c'_i = c_i/d$ (i = 1,2) où d est un pgcd de c_1 et c_2 dans A, on peut supposer c_1 et c_2 étrangers.
Le système d'équations ($A_1A_2 = a$, $c_1Y_1 + A_1B_1 = 1$, $c_2Y_2 + A_2B_2 = 1$) est absolument irréductible et absolument réduit. La variété V associée est lisse, et pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ on a :

- si $c_1 \notin \mathfrak{m}$ alors $(a, 1, 0, 1, c_1^{-1}, 0) \in V(A_\mathfrak{m})$;
- sinon, $c_2 \notin \mathfrak{m}$, donc $(1, a, 1, 0, 0, c_2^{-1}) \in V(A_\mathfrak{m})$.

Le LGPH 2bis appliqué à V donne donc un point $(a_1, a_2, b_1, b_2, y_1, y_2) \in V(A)$. On a bien $a = a_1a_2$, et pour $i = 1$ ou 2 on a $c_iA + a_iA = A$, donc $a_i \notin \mathfrak{p}_i$ *i.e.* $|a_i|_{\mathfrak{p}_i} = 1$.
■

Proposition 3
Soit A un anneau satisfaisant le LGPH'.
Alors A est indépendant.

Preuve: Soient $R_1 \neq R_2 \in W_A$; A étant de Bezout donc de Prüfer d'après la proposition 1, ils sont de la forme $A_{\mathfrak{m}_1}$ et $A_{\mathfrak{m}_2}$, avec $\mathfrak{m}_1 \neq \mathfrak{m}_2 \in \mathrm{Spm}(A)$. Pour montrer que $R_1R_2 = K$ il suffit de montrer que tout idéal premier de A inclus dans $\mathfrak{m}_1 \cap \mathfrak{m}_2$ est nul. Par l'absurde supposons que non, et soit $\mathfrak{p}$ un tel idéal premier, et $a \in \mathfrak{p} \setminus \{0\}$. Soient a_1 et a_2 donnés par le lemme 2 appliqué à $a, \mathfrak{m}_1$ et $\mathfrak{m}_2$. On a :

- $|a_1|_{\mathfrak{m}_1} = 1 \Longrightarrow a_1 \notin \mathfrak{m}_1 \Longrightarrow a_1 \notin \mathfrak{p}$;
- $|a_2|_{\mathfrak{m}_2} = 1 \Longrightarrow a_2 \notin \mathfrak{m}_2 \Longrightarrow a_2 \notin \mathfrak{p}$.

Or $a = a_1a_2 \in \mathfrak{p}$, ce qui contredit $\mathfrak{p}$ premier.
■

Lemme 4
Soit A un anneau satisfaisant le LGPH 2bis. Soient $\mathcal{P}, \mathcal{Q} \subseteq \mathrm{Sp}(A)$ tels que :

- *$\mathcal{P}, \mathcal{Q}$ sont quasi-compacts ;*
- *$\mathcal{P} \cap \mathcal{Q} = \emptyset$;*
- *les éléments de $\mathcal{P} \cup \mathcal{Q}$ sont incomparables pour l'inclusion.*

Alors $\forall a \in A \setminus \{0\}, \exists b, c \in A \setminus \{0\}$ tels que :

$$\begin{cases} a = bc \\ \forall \mathfrak{p} \in \mathcal{P}, |b|_\mathfrak{p} = |a|_\mathfrak{p} \quad (\textit{donc } |c|_\mathfrak{p} = 1) \\ \forall \mathfrak{q} \in \mathcal{Q}, |c|_\mathfrak{q} = |a|_\mathfrak{q} \quad (\textit{donc } |b|_\mathfrak{q} = 1) \end{cases}$$

Preuve: Pour tout α dans A, je note $\mathcal{P}(\alpha) = \{\mathfrak{p} \in \mathcal{P} \ / \ \alpha \in \mathfrak{p}\}$, et idem pour $\mathcal{Q}(\alpha)$.

Fixons un élément $\mathfrak{p}$ de $\mathcal{P}$. Pour tout $\mathfrak{q} \in \mathcal{Q}$ le lemme 2 donne $b_{\mathfrak{p},\mathfrak{q}} \in A \setminus \{0\}$ tel que $b_{\mathfrak{p},\mathfrak{q}}$ divise a, $|b_{\mathfrak{p},\mathfrak{q}}|_\mathfrak{q} = 1$ et $|b_{\mathfrak{p},\mathfrak{q}}|_\mathfrak{p} = |a|_\mathfrak{p}$. La famille $(\mathcal{Q}(b_{\mathfrak{p},\mathfrak{q}}))_{\mathfrak{q} \in \mathcal{Q}}$ de fermés de $\mathcal{Q}$ est d'intersection vide (puisque $\forall \mathfrak{q} \in \mathcal{Q}, b_{\mathfrak{p},\mathfrak{q}} \notin \mathfrak{q}$). On peut donc, par quasi-compacité de $\mathcal{Q}$, trouver $\mathfrak{q}_1, \ldots, \mathfrak{q}_n \in \mathcal{Q}$ tels que $(\mathcal{Q}(b_{\mathfrak{p},\mathfrak{q}_i}))_{1 \leq i \leq n}$ soit d'intersection vide.

Soit $b_{\mathfrak{p}} = \sum_{i=1}^{n} \lambda_i b_{\mathfrak{p},\mathfrak{q}_i}$ un pgcd de $(b_{\mathfrak{p},\mathfrak{q}_1} \dots, b_{\mathfrak{p},\mathfrak{q}_n})$.

– $b_{\mathfrak{p}} | b_{\mathfrak{p},\mathfrak{q}_1}$ et $b_{\mathfrak{p},\mathfrak{q}_1} | a$, donc $b_{\mathfrak{p}} | a$.
– $b_{\mathfrak{p}} | a \Longrightarrow |b_{\mathfrak{p}}|_{\mathfrak{p}} \geq |a|_{\mathfrak{p}}$, or :

$$|b_{\mathfrak{p}}|_{\mathfrak{p}} \leq \max_{1\leq i\leq n} |\lambda_i b_{\mathfrak{p},\mathfrak{q}_i}|_{\mathfrak{p}} \leq \max_{1\leq i\leq n} |b_{\mathfrak{p},\mathfrak{q}_i}|_{\mathfrak{p}} = |a|_{\mathfrak{p}}$$

donc $|b_{\mathfrak{p}}|_{\mathfrak{p}} = |a|_{\mathfrak{p}}$.
– $\forall \mathfrak{q} \in \mathcal{Q}, \exists i \in [\![1,n]\!]$ tel que $b_{\mathfrak{p},\mathfrak{q}_i} \notin \mathfrak{q}$, or $b_{\mathfrak{p}} | b_{\mathfrak{p},\mathfrak{q}_i}$ donc $b_{\mathfrak{p}} \notin \mathfrak{q}$, *i.e.* $|b_{\mathfrak{p}}|_{\mathfrak{q}} = 1$.

On répète cette construction pour chaque $\mathfrak{p} \in \mathcal{P}$, et on pose $c_{\mathfrak{p}} := a/b_{\mathfrak{p}}$; $|b_{\mathfrak{p}}|_{\mathfrak{p}} = |a|_{\mathfrak{p}} \Longrightarrow |c_{\mathfrak{p}}|_{\mathfrak{p}} = 1$, *i.e.* $c_{\mathfrak{p}} \notin \mathfrak{p}$. $(\mathcal{P}(c_{\mathfrak{p}}))_{\mathfrak{p}\in\mathcal{P}}$ est donc une famille de fermés de $\mathcal{P}$ d'intersection vide. Puisque $\mathcal{P}$ est quasi-compact, il existe $\mathfrak{p}_1, \dots, \mathfrak{p}_m \in \mathcal{P}$ tels que $(\mathcal{P}(c_{\mathfrak{p}_i}))_{1\leq i\leq m}$ soit d'intersection vide.

Soit $c := \sum_{i=1}^{m} \mu_i c_{\mathfrak{p}_i}$ un pgcd de $(c_{\mathfrak{p}_1} \dots, c_{\mathfrak{p}_m})$.

– $c | c_{\mathfrak{p}_1}$ et $c_{\mathfrak{p}_1} | a$, donc $c|a$, et on pose $b := a/c$.
– $\forall \mathfrak{p} \in \mathcal{P}, \exists i \in [\![1,m]\!]$ tel que $c_{\mathfrak{p}_i} \notin \mathfrak{p}$, or $c | c_{\mathfrak{p}_i}$, donc $c \notin \mathfrak{p}$, *i.e.* $|c|_{\mathfrak{p}} = 1$,
d'où $|b|_{\mathfrak{p}} = |a/c|_{\mathfrak{p}} = |a|_{\mathfrak{p}}$.
– $\forall \mathfrak{q} \in \mathcal{Q}, c|a \Longrightarrow |c|_{\mathfrak{q}} \geq |a|_{\mathfrak{q}}$, or :

$$|c|_{\mathfrak{q}} \leq \max_{1\leq i\leq m} |\mu_i c_{\mathfrak{p}_i}|_{\mathfrak{q}} \leq \max_{1\leq i\leq m} |c_{\mathfrak{p}_i}|_{\mathfrak{q}} = \max_{1\leq i\leq m} |a/b_{\mathfrak{p}_i}|_{\mathfrak{q}} = |a|_{\mathfrak{q}}$$

donc $|c|_{\mathfrak{q}} = |a|_{\mathfrak{q}}$ et $|b|_{\mathfrak{q}} = \left|\frac{a}{c}\right|_{\mathfrak{q}} = 1$.

■

Remarque: Notons que dans les propositions précédentes nous n'avons utilisé que la conditition géométrique du LGPH' et jamais le LGPH1. C'est maintenant que cette hypothèse devient nécessaire. Par la suite, nous utiliserons seulement la bonne factorisation (ou la BAP, qui apparaîtra plus loin).

Proposition 5
Soit A un anneau satisfaisant le LGPH'.
Alors A a bonne factorisation.

Preuve: Soient $a, b \in A$, avec $a \neq 0$, et soit d un pgcd de a et b. On sait que $\mathcal{P} := M(a) \setminus M(b)$ est quasi-compact (en tant que fermé du quasi-compact $M(b)^c$) et $\mathcal{Q} := M(a) \cap M(b) = M(d)$ l'est aussi (en tant que fermé de $\mathrm{Spm}(A)$).

Le lemme 4 appliqué à $a, \mathcal{P}$ et $\mathcal{Q}$, donne $a_1, a_2 \in A$ tels que :

– $a = a_1 a_2$;
– $\forall \mathfrak{m} \in M(a) \setminus M(b), |a_1|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$ et $|a_2|_{\mathfrak{m}} = 1$,
donc $M(a_1) \supseteq M(a) \setminus M(b)$ et $M(a_2) \subseteq M(a) \cap M(b)$;
– $\forall \mathfrak{m} \in M(a) \cap M(b), |a_1|_{\mathfrak{m}} = 1$ et $|a_2|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$,
donc $M(a_1) \subseteq M(a) \setminus M(b)$ et $M(a_2) \supseteq M(a) \cap M(b)$.

D'où $a = a_1 a_2$ avec $M(a_1) = M(a) \setminus M(b)$ et $M(a_2) = M(a) \cap M(b)$.

■

Remarque:
(1) Il est facile de voir que si un anneau A a bonne factorisation alors toute partie constructible de $\mathrm{Spm}(A)$ est de la forme $M(a)$ ou $M(a)^c$ avec $a \in A \setminus \{0\}$. En effet,

pour tous $a, b \in A \setminus \{0\}$ on a, en notant a_1, a_2 les facteurs de a donnés par BF et b_1, b_2 les facteurs de b analogues (obtenus en inversant les rôles de a et b) :
- $M(a) \cap M(b) = M(a_1)$;
- $M(a) \cap M(b)^c = M(a_2)$;
- $M(a) \cup M(b) = M(ab)$;
- $M(a) \cup M(b)^c = \left(M(a)^c \cap M(b)\right)^c = M(b_2)^c$.

Et une récurrence facile donne la conclusion (on peut toujours remplacer $M(0)$ par $M(1)^c$, ce qui permet de supposer a et b non nuls).
(2) Ce qui précède explicite la relation entre les "good Rumely domains" de [VdD-M] et le LGPH : les premiers sont caractérisés par des conditions Ru1 à Ru6 ; Ru1 dit que le corps des fractions est algébriquement clos, Ru2 à Ru4 correspondent modulo Ru1 au LGPH, enfin Ru5 et Ru6 disent que cet anneau est un $\mathrm{r}_\circ$-domaine qui n'est pas un corps et dont le treillis résiduel est dense. La distinction faite dans [VdD-M] entre "Rumely domains" satisfaisant Ru1 à Ru3 et "good Rumely domains" satisfaisant Ru1 à Ru6 ne facilite pas la comparaison avec le LGPH, puisque ce sont à notre avis les conditions Ru2 à Ru4 qui ont une portée générale et les autres qui sont particulières aux anneaux considérés dans cet article ; la filiation entre les anneaux de Rumely (bons ou non) et le LGPH (qui les généralise) est cependant claire.

§ 4. LGPH et clôture régulière

On fixe pour la durée de ce paragraphe un anneau intègre A, et $K := \mathrm{Fr}(A)$.

Proposition 1
Si A satisfait le LGPH' alors pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ l'anneau A est dense dans $A^h_{\mathfrak{m}}$.

Preuve: Soit $\mathfrak{m}$ un idéal maximal de A.

On sait que $A_{\mathfrak{m}}$ est dense dans $A^h_{\mathfrak{m}}$ si et seulement si pour tout polynôme g à coefficients dans $A_{\mathfrak{m}}$, s'il existe un certain b dans $A_{\mathfrak{m}}$ tel que $g(b) \in \mathfrak{m}A_{\mathfrak{m}}$ et $g'(b) \in A^*_{\mathfrak{m}}$ alors 0 est adhérent à $g[A_{\mathfrak{m}}]$.

Il suffit donc de montrer que pour tout polynôme f à coefficients dans A, s'il existe un élément a de A tel que $f(a) \in \mathfrak{m}$ et $f'(a) \notin \mathfrak{m}$ alors 0 est adhérent à $f[A]$. En effet, cette propriété, appliquée d'abord pour tous $c, d \in A$ avec $d \notin \mathfrak{m}$, à $f(X) = dX - c$, montre que A est dense dans $A_{\mathfrak{m}}$, et il est clair qu'elle implique que le critère précédent est vérifié, donc que $A_{\mathfrak{m}}$ est dense dans $A^h_{\mathfrak{m}}$.

Soient, donc, $f \in A[X]$ et $a \in A$ tels que $f(a) \in \mathfrak{m}$ et $f'(a) \notin \mathfrak{m}$. Soit $\varepsilon \in \mathfrak{m} \setminus \{0\}$; la bonne factorisation donne $\varepsilon' \in A \setminus \{0\}$ tel que :
- $\forall \mathfrak{n} \in M(f'(a))^c, \quad |\varepsilon'|_{\mathfrak{n}} = |\varepsilon|_{\mathfrak{n}}$ et en particulier $\varepsilon' \in \mathfrak{m}$;
- $\forall \mathfrak{n} \in M(f'(a)), \quad |\varepsilon'|_{\mathfrak{n}} = 1$.

Soit α un pgcd de ε' et de $f(a)$ (donc $\alpha \in \mathfrak{m}$). On applique le LGPH' à la variété lisse V définie par les équations suivantes :

$$\begin{cases} \varepsilon Y = Zf(X) \\ \alpha U + TZ = 1 \end{cases}$$

- $V(\mathrm{Fr}(A))$ est non vide (prendre par exemple $(t, u, x, y, z) = (0, \alpha^{-1}, 0, 0, 0)$).
- Soit $\mathfrak{n} \in \mathrm{Spm}(A)$.
  - Si $\alpha \notin \mathfrak{n}, \quad (0, \alpha^{-1}, 0, 0, 0) \in V(A_{\mathfrak{n}})$.

– Sinon, par construction $f(a) \in \mathfrak{n}$ et $f'(a) \notin \mathfrak{n}$. Donc le lemme de Hensel s'applique dans $A^h_{\mathfrak{n}}$, et donne $x_{\mathfrak{n}} \in A^h_{\mathfrak{n}}$ tel que $f(x_{\mathfrak{n}}) = 0$. On prends alors $(t, u, x, y, z) = (1, 0, x_{\mathfrak{n}}, 0, 1)$.

Le LGPH' donne $(t, u, x, y, z) \in V(A)$, et on a donc :
– $\alpha u + tz = 1 \Longrightarrow M(z) \cap M(\alpha) = \emptyset \Longrightarrow z \notin \mathfrak{m}$,
– $\varepsilon y = zf(x) \Longrightarrow |f(x)|_{\mathfrak{m}} = \left|\frac{\varepsilon y}{z}\right|_{\mathfrak{m}} = |\varepsilon y|_{\mathfrak{m}} \leq |\varepsilon|_{\mathfrak{m}}$.

Ceci étant valable pour n'importe quel ε non nul, on a bien vérifié que 0 était adhérent à $f(A)$.

■

Lemme 2 (d'accessibilité)
Soient $R_0 \in W_A$ et $x_0 \in H_{R_0}(K)^n$. On suppose R_0 dense dans son hensélisé.
Alors pour tout $\varepsilon \in K \setminus \{0\}$ on peut trouver une partie constructible W_0 de W_A et un $x \in K^n$ tels que :
(i) *$R_0 \in W_0$ et $|x_0 - x|_{R_0} < |\varepsilon|_{R_0}$,*
(ii) *$\forall R \in W_0$, $\exists x_R \in H_R(K)^n$, K-conjugué de x_0, tel que $|x_R - x|_R < |\varepsilon|_R$.*

Preuve: On le démontre d'abord pour $n = 1$.

Fixons $\varepsilon \in K \setminus \{0\}$. Soit f le polynôme minimal de x_0 sur K, $u \in A \setminus \{0\}$ un dénominateur commun aux coefficients de f, et $g := uf$. La densité de K dans $H_{R_0}(K)$ nous donne donc $x \in K$ tel que :

$$|x_0 - x|_{R_0} < |\varepsilon|_{R_0} \tag{1}$$

On sait que $H_{R_0}(K)$ est séparable sur K donc $g'(x_0) \neq 0$. Par continuité des fonctions polynômiales on peut donc s'arranger pour que :

$$|g(x)|_{R_0} < \min\left(\left|g'(x)^2\right|_{R_0}, \left|\varepsilon g'(x)\right|_{R_0}\right) \tag{2}$$

Soit $W_0 := W\left(\frac{g(x)}{g'(x)^2}\right) \cap W\left(\frac{g(x)}{\varepsilon g'(x)}\right)$.
– Le (2) entraîne que $R_0 \in W_0$ ce qui, vu (1), donne (i).
– D'autre part $g \in A[X] \subseteq R^h[X]$, et pour tout $R \in W_0$, on a : $\left|\frac{g(x)}{g'(x)}\right|_R < |\varepsilon|_R$ et $|g(x)|_R < |g'(x)^2|_R$, donc d'après Hensel-Rychlik g possède une racine x_R dans $H_R(K)$, qui est donc un K-conjugué de x_0, telle que :

$$|x_R - x|_R = \left|\frac{g(x)}{g'(x)}\right|_R < |\varepsilon|_R$$

i.e. (ii).

Le cas où n est quelconque s'en déduit : le théorème de l'élément primitif appliqué à $K(x_0)$ nous donne $\theta_0 \in H_{R_0}(K)$ tel que $K(x_0) = K(\theta_0)$. Soit $f \in K[X]^n$ tel que $f(\theta_0) = x_0$. Soit $u \in A \setminus \{0\}$ tel que $g := uf \in A[X]^n$. Enfin soit $\varepsilon \in K \setminus \{0\}$.

Ce qui précède nous donne un élément θ de K et une partie constructible W_0 de W_A contenant R_0, tels que :
(i) $|\theta_0 - \theta|_{R_0} < |u\varepsilon|_{R_0}$,
(ii) $\forall R \in W_0$ il existe $\theta_R \in H_R(K)$, K-conjugué de θ_0, tel que $|\theta_R - \theta|_R < |u\varepsilon|_R$.

Posons $x := f(\theta)$ et pour tout $R \in W_0$, $x_R := f(\theta_R)$. Les coefficients de f étant pris dans K, $x \in K^n$ et pour tout $R \in W_0$, x_R est un élément de $H_R(K)^n$, K-conjugué de

x_0. Le multinôme g étant à coefficient dans $A \subseteq \cap W_0$, la formule de Taylor (appliquée à chaque coordonnée de g) nous garantit que :

(i) $|g(\theta_0) - g(\theta)|_{R_0} \leq |\theta_0 - \theta|_{R_0} < |u\varepsilon|_{R_0}$ donc $|x_0 - x|_{R_0} < |\varepsilon|_{R_0}$;

(ii) $\forall R \in W_0$, $|g(\theta_R) - g(\theta)|_R \leq |\theta_R - \theta|_R < |u\varepsilon|_R$ donc $|x_R - x|_R < |\varepsilon|_R$.

■

Proposition 3 (densité locale)

On suppose que A satisfait le LGPH (resp. le LGPH'). Soit V une variété définie sur K, ayant un point lisse dans chaque R^h (resp. et dans K) pour R décrivant W_A.
Alors pour tout $R \in W_A$, $V^\circ(A)$ est dense dans $V^\circ(R^h)$ (au sens de la topologie de R^h).

Preuve: Soit $f \in K[X]^p$, où $X = (X_1, \ldots, X_n)$, un système absolument réduit d'équations de V. Soit R_0 fixé dans W_A et $x_0 \in V^\circ(R_0^h)$. Enfin, soit $\varepsilon \in K^*$.

On peut toujours supposer que $\varepsilon \in A$. Le lemme d'accessibilité nous donne $x \in K^n$, une partie constructible W_0 de W_A contenant R_0, et pour chaque $R \in W_0$ un élément x_R de $H_R(K)^n$, K-conjugué de x_0, vérifiant : $|x_R - x|_R < |\varepsilon|_R$. En outre on peut prendre $x_{R_0} = x_0$.

Soit u un plus petit dénominateur commun des coordonnées de x. On a $x_0 \subseteq R_0^h$, et $|x_{R_0} - x|_{R_0} < |\varepsilon|_{R_0} \leq 1$, donc $x \subseteq R_0$, et donc $u \notin m(R_0)$. Pour tout $R \in W_0 \setminus W_A(u)$, on a : $x \subseteq R$, et $|x_R - x|_R < |\varepsilon|_R \leq 1$, donc $x_R \subseteq R^h$. La remarque clôturant le paragraphe 3 nous autorise à supposer que $W_0 \setminus W_A(u)$ est de la forme $W_A(\alpha)$ pour un certain α non nul appartenant à $m(R_0) \cap A$ (parce que $W_0 \setminus W_A(u)$ est constructible, donc de la forme $W(a)$ ou $W(a)^c$ d'après cette remarque et la correspondance entre les parties constructibles de $\mathrm{Spm}(A)$ et celles de W_A, et qu'on peut écarter le cas $W_A(a)^c$ en se restreignant à $W(b) \cap (W_0 \setminus W_A(u))$ pour un b quelconque dans $m(R_0) \cap A$). Pour tout $R \in W_A(\alpha)$ on a donc $u \notin m(R)$ d'où $x_R \subseteq R^h$.

On applique la bonne factorisation à ε : il vient $\varepsilon = \varepsilon_1\varepsilon_2$, avec $M(\varepsilon_1) = M(\varepsilon) \cap M(\alpha)$ et $M(\varepsilon_2) = M(\varepsilon) \setminus M(\alpha)$. En particulier, pour tout $R \in W_A(\alpha)$, on a $|\varepsilon|_R = |\varepsilon_1|_R$.
Soit V_1 la variété lisse définie sur K par :

$$\begin{cases} f(X) = 0 \\ X - x = \varepsilon_1 Y \end{cases}$$

où $Y = (Y_1, \ldots, Y_n)$.

• Soit $R \in W_A$.

– Si α n'appartient pas à $m(R)$, alors ε_1 non plus ne lui appartient pas puisque $M(\varepsilon_1) \subseteq M(\alpha)$. Soit x_R un élément quelconque de $V^\circ(R^h)$ (il en existe par hypothèse). ε_1 est inversible dans R^h donc on a : $(x_R, (x_R - x)/\varepsilon_1) \in V_1^\circ(R^h)$.

– Sinon $R \in W(\alpha)$ donc x_R, le K-conjugué de x_0 donné par la première partie, appartient à $V^\circ(R^h)$ et vérifie : $|x_R - x|_R < |\varepsilon|_R = |\varepsilon_1|_R$ d'où $(x_R, (x_R - x)/\varepsilon_1) \in V_1^\circ(R^h)$.

• Si A satisfait le LGPH ce qui précède suffit à nous donner un point de $V_1(A)$, sinon on a dans nos hypothèses un point $x_K \in V^\circ(K)$, d'où un point $(x_K, (x_K - x)/\varepsilon_1) \in V_1^\circ(K)$.

Dans les deux cas (LGPH ou LGPH') on a donc $V_1(A) \neq \emptyset$, d'où $a \in A^n$ tel que $(a, (a - x)/\varepsilon_1) \in V_1^\circ(A)$. On a alors :

– $f(a) = 0$, donc $a \in V(A)$;

– $(a-x)/\varepsilon_1 \subseteq A \subseteq R_0$, donc $|a-x|_{R_0} \leq |\varepsilon_1|_{R_0} = |\varepsilon|_{R_0}$, et donc :

$$|a-x_0|_{R_0} \leq \max(|a-x|_{R_0}, |x_0-x|_{R_0}) \leq |\varepsilon|_{R_0}.$$

■

Corollaire 4
On suppose que A satisfait le LGPH (resp. le LGPH') et que A n'est pas un corps. Soit V une variété définie sur K, ayant un point lisse dans chaque R^h, pour R décrivant W_A (resp. et un point lisse dans K).
Alors pour tout $g \in K[X] \setminus I_K(V)$, V a un point lisse dans A n'annulant pas g.

Preuve: C'est immédiat : A n'étant pas un corps, on peut prendre un anneau de valuation non trivial R appartenant à W_A ; R^h est t-henselien, donc le TFI donne un point $x_R \in V^\circ(R^h)$ tel que $g(x_R) \neq 0$. Par continuité de g, il suffit de prendre un point de $V^\circ(A)$ suffisamment proche de x_R.

■

Corollaire 5
On suppose que A satisfait le LGPH (resp. le LGPH'). Soit V une variété définie sur K telle que $\forall R \in W_A,\ V^\circ(H_R(K)) \neq \emptyset$ (resp. que $V^\circ(K) \neq \emptyset$).
Alors $\forall R \in W_A,\ V^\circ(K)$ est dense dans $V^\circ(H_R(K))$ (au sens de la topologie de R^h).

Preuve: Soit $f_1, \ldots, f_m \in A[X_1, \ldots, X_n]$ un système absolument réduit d'équations de V. On considère la variété V^* définie sur K par les homogénéisés $f_i^*(X,Y)$, (Y une nouvelle indéterminée). Pour tout $R \in W_A$ soit $x_R \in V^\circ(H_R(K))$; il s'écrit $x_R = a_R/u_R$, avec $(a_R, u_R) \in (V^*)^\circ(R^h)$ et $u_R \neq 0$. Soit R_0 fixé dans W_A. La densité locale appliquée à V^* nous donne un point $(a,b) \in V^*(A)$ arbitrairement proche de (a_{R_0}, b_{R_0}). En particulier $b \neq 0$ et $x := a/b \in V^\circ(K)$ est proche de x_{R_0}.

■

Corollaire 6
Supposons que quel que soit $a \in A$, $M(a)^c$ soit quasi-compact (i.e. *la condition (LGPH1) est réalisée). Alors sont équivalents :*
(i) *A satisfait le LGPH ;*
(ii) *A satisfait le LGPH' et $K \in \mathrm{RC}(W_A)$;*
(iii) *$A \in \mathrm{RC}(\mathcal{R})$, où $\mathcal{R} = \{R^h \ /\ R \in W_A\}$.*

Preuve:
(i) $\Longleftrightarrow$ (ii) Si A satisfait le LGPH il satisfait *a fortiori* le LGPH', et le corollaire 5 montre que $K \in \mathrm{RC}(W_A)$. La réciproque est triviale.
(i) $\Longleftrightarrow$ (iii) Si A satisfait le LGPH alors $A \in \mathrm{RC}(\mathcal{R})$ d'après le corollaire 4, et la réciproque est triviale (dans les deux sens on utilise la caractérisation de la clôture régulière de la proposition 1.2).

■

§ 5. Principe de spécialisation locale

Pour tout anneau de valuation R on note R^c le complété de R.

Lang a introduit dans [Lan], chapitre X, § 3, pp. 258-259, un “principe de spécialisation locale" pour les anneaux locaux qui n'est pas sans rapport avec notre étude, c'est pourquoi nous nous permettons maintenant une digression. Pour les anneaux de valuations ce principe peut s'énoncer ainsi :

Définition
Un anneau de valuation R satisfait le **principe de spécialisation locale** si et seulement si pour toute famille finie de polynômes $f \in R[X]^p$, avec $X = (X_1, \ldots, X_n)$, les solutions de $f(X) = 0$ à coordonnées dans R sont denses (pour la topologie produit de la valuation) parmi celles à coordonnées dans R^c.

Lang a montré que tout anneau de valuation henselien R sur un corps K dont le groupe des valeurs est plongé dans $\mathbb{R}$ (*i.e.* R est l'anneau d'une valeur absolue) satisfait le principe de spécialisation locale. On sait que pour un tel anneau de valuation, le complété de K relativement à R est une extension séparable de K. La proposition suivante montre qu'on peut généraliser ce résultat, pour en faire une condition nécessaire et suffisante.

Proposition 1
Soit R un anneau de valuation hensélien. Alors sont équivalents :
(i) *R satisfait le principe de spécialisation locale ;*
(ii) *$\mathrm{Fr}(R^c)$ est une extension séparable de $\mathrm{Fr}(R)$;*
(iii) *$\mathrm{Fr}(R^c)$ est une extension régulière de $\mathrm{Fr}(R)$;*
(iv) *R est $\exists$-clos dans R^c (dans $\mathrm{L}_{\mathrm{div}}$, ou $\mathrm{L}_{\mathrm{rad}}$).*

La démonstration de cette proposition passe par le lemme suivant :

Lemme 2
Soit R un anneau de valuation henselien, F son corps des fractions, F^c le complété de F relativement à la valuation de R et V une variété définie sur F.
Alors $V^\circ(F)$ est dense dans $V^\circ(F^c)$ (pour la topologie produit de la valuation).

Ce genre de résultat est paraît-il bien connu, mais de là à pouvoir en donner une référence publiée... De toutes façons nous aurons besoin, pour l'axiomatisation, du lemme un peu plus général suivant, dont celui-ci découle immédiatement :

Lemme 3
Soit R un anneau de valuation henselien, F son corps des fractions, et B une partie non vide de F^n telle que :
– $\exists M_B \in F,\ \forall x \in B,\ \ |x|_R \leq |M_B|_R$;
– $\exists m_B \in F \setminus \{0\},\ \forall x \in B,\ \forall y \in F^n,\ \ |x-y|_R \leq |m_B|_R \Longrightarrow y \in B$;
Soit V une variété non vide, de dimension d, définie sur F par un système absolument réduit d'équations $f := (f_1, \ldots, f_m) \in R[X]^m$ ($X = (X_1, \ldots, X_n)$). Soient enfin Δ un déterminant de taille $n-d$, extrait du Jacobien de f, et $\delta \in F \setminus \{0\}$ tels que :

$$\forall \varepsilon \in F \setminus \{0\},\ \exists x_\varepsilon \in B, \quad |f(x_\varepsilon)|_R \leq |\varepsilon|_R \wedge |\Delta(x_\varepsilon)|_R \geq |\delta|_R.$$

Alors V possède un point lisse dans B.

Remarque: On notera que $B = R^n$ a les propriétés ci-dessus avec $m_B = M_B = 1$.

Preuve: On considère le langage $\mathrm{L}_{\mathrm{div}}$, augmenté d'un symbole de prédicat n-aire, disons U, interprété dans F par B, de nouveaux symboles de constantes pour les éléments de F, (comme toujours pour les corps valués "|" est interpété dans F par

$x|_F y \iff |x|_R \geq |y|_R$). Notons $\mathcal{L}$ ce nouveau langage, soient $c_1, \ldots, c_n$ des symboles de constantes n'appartenant pas à $\mathcal{L}$. On considère la théorie :

$$\mathcal{T} := Th(F) \cup \{\text{“} \bigwedge_{i=1}^{m} \varepsilon|f_i(c) \wedge \Delta(c)|\delta \wedge U(c)\text{”} \;/\; \varepsilon \in F \setminus \{0\}\},$$

où $Th(F)$ est le diagramme élémentaire de $(F, B, |_F)$ en tant que $\mathcal{L}$-structure.

Il est clair que T est finiment satisfaisable : un fragment fini fait intervenir un nombre fini de ε, disons $\varepsilon_1, \ldots, \varepsilon_r$, donc se plonge dans :

$$\mathcal{T}_0 := Th(F) \cup \{\text{“} \bigwedge_{i=1}^{m} \varepsilon_j|f_i(c) \wedge \Delta(c)|\delta \wedge U(c)\text{”} \;/\; 1 \leq j \leq r\}.$$

Si l'on prend un $\varepsilon_0 \in F \setminus \{0\}$ tel que $|\varepsilon_0|_R \leq \min\{|\varepsilon_j|_R \;/\; 1 \leq j \leq r\}$, et qu'on interprète c par x_{ε_0}, alors $(F, B, |_F, x_{\varepsilon_0})$ est un modèle de $\mathcal{T}_0$.

Par le théorème de compacité, $\mathcal{T}$ possède donc un modèle F°, muni d'interprétations B° et $|^\circ$ de U et $|$, et d'un n-uplet x° d'éléments de F° tels que :

(a) $(F, B, |_F) \preceq (F^\circ, B^\circ, |^\circ)$;

(b) $x^\circ \in B^\circ$;

(c) $\forall \varepsilon \in F \setminus \{0\},\ \ |f(x^\circ)|_{R^\circ} \leq |\varepsilon|_{R^\circ}$ et $|\Delta(x^\circ)|_{R^\circ} \geq |\delta|_{R^\circ}$

Le (a) entraîne que $R^\circ := \{x \in F^\circ \;/\; 1|^\circ x\}$ est l'anneau d'une valuation henselienne de F°, prolongeant celle associée à R, et que B° vérifie relativement à m_B, M_B et R° les mêmes propriétés que B, puisque tout cela est du premier ordre.

Soit $\mathfrak{p} := \{m \in R^\circ \;/\; \forall \varepsilon \in F \setminus \{0\},\ |m|_{R^\circ} \leq |\varepsilon|_{R^\circ}\}$. Il est facile de voir que $\mathfrak{p}$ est un idéal premier de R°, donc le localisé $R' := R^\circ_{\mathfrak{p}}$ est encore un anneau de valuation henselien. Pour tout $y \in B^\circ$, on a $|y|_{R^\circ} \leq |M_B|_{R^\circ}$, donc $y \in R'^n$, *i.e.* $B^\circ \subseteq R'^n$, et en particulier $x^\circ \in R'^n$ d'après le (b). Le (c) entraîne que $f(x^\circ) \in \mathfrak{p}$ et $\Delta(x^\circ) \notin \mathfrak{p}$, donc par le lemme de Hensel, il existe $x^* \in R'^n$ tel que $f(x^*) = 0$, et $x^* - x^\circ \in m(R') = \mathfrak{p}$. Il s'ensuit que $|x^* - x^\circ|_{R^\circ} \leq |m_B|_{R^\circ}$, et donc $x^* \in B^\circ$. Δ est à coefficients dans $R \subseteq R^\circ$, donc $|\Delta(x^*) - \Delta(x^\circ)|_{R^\circ} \leq |x^* - x^\circ|_{R^\circ} < |\delta|_{R^\circ} \leq |\Delta(x^\circ)|_{R^\circ}$, donc $|\Delta(x^*)|_{R^\circ} = |\Delta(x^\circ)|_{R^\circ} \geq |\delta|_{R^\circ}$.

$(F^\circ, B^\circ, |^\circ) \models \exists x(f(x) = 0 \wedge \Delta(x)|\delta \wedge U(x))$ (le point x^* a ces propriétés), et puisque d'après le (a), $(F, B, |_F)$ est $\exists$-clos dans $(F^\circ, B^\circ, |^\circ)$, cette formule est encore satisfaite dans $(F, B, |_F)$, ce qu'il fallait démontrer.

■

Preuve: (du lemme 2).
Pour tout $x \in V^\circ(F^c)$ et tout $m \in R \setminus \{0\}$, soit $B := \{y \in F^n \;/\; |x - y|_{R^c} \leq |m|_{R^c}\}$ et Δ un déterminant de taille $n - d$ extrait d'un Jacobien de V tel que $\Delta(x) \neq 0$. Quel que soit $\varepsilon \in R \setminus \{0\}$, un point x_ε de R^n suffisamment proche de x vérifie par continuité de f et de Δ : $|f(x_\varepsilon)|_R \leq |\varepsilon|_R$ et $|\Delta(x_\varepsilon)|_R = |\Delta(x)|_R$. Le lemme 3 donne alors un point $y \in V^\circ(B)$ qui vérifie donc $|x - y|_{R^c} \leq |m|_{R^c}$.

■

Nous pouvons maintenant revenir à la proposition 1.

Preuve: (i)$\Longrightarrow$(iv) Il faut montrer que toute formule existentielle de $\mathrm{L_{div}}$ à paramètres dans R satisfaite dans R^c est satisfaite dans R. On sait qu'il suffit de le vérifier pour les formules du type $\exists x\varphi(x)$, où φ est une conjonction de formules négatomiques de $\mathrm{L_{div}}$. Soit donc :

$$\varphi(x) \equiv \bigwedge_{i=1}^{m} f_i(x) = 0 \wedge \bigwedge_{i=1}^{n} g_i(x) \neq 0 \wedge \bigwedge_{i=1}^{r} p_i(x)|q_i(x) \wedge \bigwedge_{i=1}^{r'} p'_i(x) \not| \, q'_i(x),$$

où les polynômes sont à coefficients dans R, une formule satisfaite dans R^c par un certain $b \subseteq R^c$. Si l'un des $p_i(b) = 0$, alors aussi $q_i(b) = 0$, donc quitte à modifier φ en remplaçant $p_i(x)|q_i(x)$ par $p_i(x) = q_i(x) = 0$, on peut supposer tous les $p_i(b)$ non nuls. Alors n'importe quelle solution de $\bigwedge_{i=1}^m f_i(x) = 0$ suffisamment proche de b satisfera aussi $\varphi(x)$, par continuité des fonctions polynomiales. (i) assure qu'une telle solution peut être prise dans R, donc $R \models \exists x \varphi(x)$, d'où (iv).

(iv)$\Longrightarrow$(iii) Si R est existentiellement clos dans R^c en tant que $\mathrm{L_{div}}$-structure, alors il l'est *a fortiori* en tant qu'anneau, et $\mathrm{Fr}(R^c)$ est une extension existentiellement close de $\mathrm{Fr}(R)$, donc régulière.

(iii) $\Longleftrightarrow$ (ii) C'est clair, puisqu'on sait qu'un corps valué henselien est séparablement clos dans son complété.

(iii)$\Longrightarrow$(i) Soit $h := (h_1, \ldots, h_p) \in R[X]^p$ ($X = (X_1, \ldots, X_n)$) un système d'équations polynomiales à coefficients dans R ayant une solution dans R^c. Soit $b \subseteq R^c$ une telle solution. $\mathrm{Fr}(R^c)$ est une extension régulière de $\mathrm{Fr}(R)$, donc aussi $\mathrm{Fr}(R)[b]$. Alors b est le point générique, donc lisse, d'une variété V définie sur $\mathrm{Fr}(R)$. D'après le lemme 2, V possède des points (lisses) dans R arbitrairement proches de b. Ces points sont aussi solutions de $h(X) = 0$, puisque $h(b) = 0 \Longrightarrow h \in I(V)$, ce qui démontre (i).

■

Remarque: Une conséquence immédiate de la proposition 1 est que pour un anneau de valuation hensélien R, son corps des fractions F est existentiellement clos dans son complété $F^c = \mathrm{Fr}(R^c)$ (pour le langage des anneaux) si et seulement si (F, R) est existentiellement clos dans (F^c, R^c) (pour le langage des corps munis d'un anneau de valuation). Cette indifférence au langage de la propriété de clôture existentielle relative dans ce cas particulier est assez surprenante, dans la mesure où R^c n'est en général pas définissable dans F^c.

Chapitre II
Axiomatisation

Résumé : Ce chapitre est consacré à l'axiomatisation du LGPH dans le langage des anneaux. Celle-ci passe par différentes étapes au cours desquelles d'autres propriétés sont introduites, discutées, puis axiomatisées. La première de ces notions, celle d'anneau localement booléen, généralise l'idée d'anneau booléen introduite par Ershov (dont l'influence a été déterminante dans le choix de l'approche que nous faisons dans ce chapitre) et fournit le cadre le plus général dans lequel les autres seront axiomatisées.

Nous avons procédé du général au particulier, aussi le lecteur pressé d'aller à l'essentiel est-il encouragé à sauter les étapes intermédiaires, quitte à y revenir plus tard, pour ne retenir que la notion la plus utile après le LGPH : celle d'approximation par bloc. Celle-ci n'est pas seulement une étape nécessaire pour l'axiomatisation, elle fournit aussi un outil incontournable (et d'ailleurs très classique) pour les prochains chapitres.

§ 1. r-anneaux localement booléens

Les familles booléennes d'anneaux de valuation ont de très belles propriétés, mais ce sont, comme on l'a vu sur les exemples (notamment sur les corps de nombres) des familles relativement "petites". Pour pouvoir traiter de plus grandes familles, il est tentant de définir une notion de "famille localement booléenne d'anneaux de valuation sur un corps K" par analogie avec Ershov, en appelant ainsi les familles W quasi-compactes telles que $\forall x \in K\setminus\{0\},\ \ W(x)$ est booléenne (comme le suggère l'exemple des corps de nombres). Mais cette notion ne se comporte pas bien : la famille W de tous les anneaux de valuations de $\mathbb{Q}(X)$ contenant $\mathbb{Q}$ (où X est une indéterminée) répond à cette définition, puisqu'elle est formée d'éléments deux à deux incomparables pour l'inclusion, et que, pour tout $x \in \mathbb{Q}(X)\setminus\{0\},\ \ W(x)$ est finie. Or $\mathrm{Fr}(\cap W) = \mathbb{Q} \neq \mathbb{Q}[X]$; on ne peut donc pas retrouver W à partir de son anneau d'holomorphie. Notons d'ailleurs qu'ici $\bigcap W$ est un corps, et *a fortiori* un anneau booléen.

C'est donc par les anneaux que va devoir passer notre généralisation, et pour cela on commence par revenir aux r-anneaux en introduisant à titre préliminaire la notion suivante.

Définition
Soit $(A, \leq)$ un r-anneau.
(1) $(A, \leq)$ est **complémenté** si :

$$\forall a \in A,\ \exists b \in A, \quad P(b) = P(a)^c.$$

(2) $(A, \leq)$ est **localement complémenté** si :

$$\forall a \in A \setminus \{0\},\ \forall b \in A,\ \exists c \in A, \quad P(a) \setminus P(b) = P(a) \cap P(c).$$

Remarques:
(1) Rappelons que suivant nos conventions un anneau A sera dit (localement) complémenté si $(A, \leq_A)$ l'est.
(2) Nous emploierons souvent la propriété de complémentation locale sous la forme symétrique : $\forall a \in A \setminus \{0\},\ \forall b \in A,\ \exists c \in A, \quad P(a) \cap P(b) = P(a) \cap P(c)^c$.
(3) Le lecteur se convaincra facilement par lui-même que pour un anneau intègre localement complémenté A les propriétés suivantes sont équivalentes :
(a) A est un corps ou $(A, \leq_A)$ n'est pas un $\mathrm{r}_\circ$-domaine ;
(b) A est un corps ou le radical de Jacobson de A n'est pas réduit à (0) ;
(c) A est un corps ou (0) n'est pas r-clos dans $(A, \leq_A)$;
(d) $\mathrm{L}(A, \leq_A)$ est stable par combinaisons booléennes ;
(e) A est complémenté.
(4) Toujours au chapitre des trivialités, nous utiliserons souvent que si $(A, \leq)$ est un r-anneau localement complémenté, $a \in A \setminus \{0\}$ et $\mathcal{C}$ est une partie constructible de $\mathrm{Sp}(A, \leq)$ alors il existe $b \in A \setminus \{0\}$ tel que :

$$P(a) \cap \mathcal{C} = P(a) \cap P(b).$$

(C'est un simple itération de la propriété de complémentation locale.)

Il s'ensuit que toute partie constructible $\mathcal{C}$ de $\mathrm{Sp}(A, \leq)$ est de la forme $P(a) \cap P(b)$ ou $P(a)^c \cup P(b)^c$ pour certains $a, b \in A \setminus \{0\}$ et qu'on peut choisir la première forme si et seulement si $\bigcap \mathcal{C} \neq \emptyset$, ce qui est toujours le cas si $(0) \notin \mathrm{Sp}(A, \leq)$. Notons que si le r-anneau est en outre $\cap$-stable alors on peut encore simplifier en mettant $\mathcal{C}$ sous la forme $P(a)$ ou $P(a)^c$.

Proposition 1
Dans un r-domaine localement complémenté, les idéaux premiers r-clos non nuls sont deux à deux incomparables pour l'inclusion.
En particulier, si A est un anneau intègre localement complémenté alors :
(a) $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Spm}(A) \cup \{(0)\}$;
(b) *toute partie constructible de* $\mathrm{Spm}(A)$ *est quasi-compacte.*

Preuve:
(1) Soit $(A, \leq)$ un r-domaine localement complémenté. Soient $\mathfrak{p}, \mathfrak{q}$ deux éléments distincts de $\mathrm{Sp}(A, \leq) \setminus \{(0)\}$ avec par exemple $\mathfrak{q} \not\subseteq \mathfrak{p}$, il faut montrer que $\mathfrak{p} \not\subseteq \mathfrak{q}$.

Soient $b \in \mathfrak{q} \setminus \mathfrak{p}$ et $a \in \mathfrak{p} \setminus \{0\}$; quitte à remplacer a par ab on peut supposer que $a \in \mathfrak{q}$. La complémentation locale donne $c \in A$ tel que $P(c) \cap P(a) = P(a) \setminus P(b)$. Par construction, $\mathfrak{p} \in P(a) \setminus P(b) = P(c) \cap P(a) \subseteq P(c)$, donc $\mathfrak{p} \in P(c)$. De même $\mathfrak{q} \notin P(a) \setminus P(b)$ donc $\mathfrak{q} \notin P(c) \cap P(a)$ or $\mathfrak{q} \in P(a)$ donc $\mathfrak{q} \notin P(c)$ et donc $c \in \mathfrak{p} \setminus \mathfrak{q}$.

(2) On suppose maintenant que $\leq$ est la relation radicale $\leq_A$ associée à A. Alors l'inclusion de $\mathrm{Spm}(A)$ dans $\mathrm{Sp}(A, \leq)$ résulte simplement de la définition de $\leq_A$, et l'autre inclusion découle immédiatement du (1).

Il s'ensuit que pour tout $a \in A \setminus \{0\}$ on a $P_{(A, \leq_A)}(a) = M(a)$ donc, en vertu des remarques précédentes, toute partie constructible $\mathcal{C}$ de $\mathrm{Spm}(A)$ est de la forme $M(a) \cap M(b)$ ou $M(a)^c \cup M(b)^c$ avec $a, b \in A \setminus \{0\}$. Dans le premier cas $\mathcal{C}$ est une partie fermée de $\mathrm{Spm}(A)$ donc est quasi-compacte, et dans le second il suffit de montrer que $M(a)^c$ est quasi-compact (car ce sera vrai aussi de $M(b)$, et $\mathcal{C}$ en tant que réunion de deux parties quasi-compactes de $\mathrm{Spm}(A)$ sera donc elle-même quasi-compacte). Supposons que la famille $(M(a_i))_{i\in I}$ soit d'intersection vide avec $M(a)^c$: $\bigcap_{i\in I} M(a_i) \cap M(a)^c = \emptyset$. On peut supposer les a_i non nuls, et prendre pour tout $i \in I$ un élément b_i de A tel que $M(a_i) \cap M(a)^c = M(a_i) \cap M(b_i)$. Les $M(a_i) \cap M(b_i)$ constituent alors une famille de fermés de $\mathrm{Spm}(A)$ d'intersection vide, et par quasi-compacité de $\mathrm{Spm}(A)$ on peut en extraire une sous-famille finie d'intersection vide, *i.e.* trouver $i_1, \ldots, i_n \in I$ tels que $M(a_{i_1}) \cap \ldots \cap M(a_{i_n}) \cap M(a)^c = \emptyset$ ce qui démontre la quasi-compacité de $M(a)^c$.

■

Proposition 2

(1) *Un anneau intègre A est localement complémenté si et seulement si :*

$$\forall a \in A \setminus \{0\},\ \forall b \in A,\ \exists c \in A, \quad M(a) \setminus M(b) = M(a) \cap M(c). \qquad (*)$$

Dans ce cas, pour tout $a \in A \setminus \{0\}$, on a $P(a) = M(a)$.

(2) *Un anneau intègre A est complémenté si et seulement si pour tout $a \in A$ il existe $b \in A$ tel que $M(b) = M(a)^c$. Dans ce cas, pour tout $a \in A$, on a $P(a) = M(a)$.*

Remarque: Contrairement aux apparences, cette proposition n'est pas un simple pléonasme : la relation radicale associée à un anneau A est définie par $\mathrm{Spm}(A)$, mais cela ne signifie pas que $\mathrm{Sp}(A, \leq) = \mathrm{Spm}(A)$ ($\mathbb{Q}[X, Y]$ est un contre-exemple). On n'a donc pas de relation, en général, entre une propriété portant sur les parties constructibles de $\mathrm{Sp}(A, \leq_A)$ et la propriété analogue sur celles de $\mathrm{Spm}(A)$.

Preuve:

(1) Un implication vient de ce que $\mathrm{Sp}(A, \leq_A) \setminus \{(0)\} = \mathrm{Spm}(A)$, comme nous venons de le voir. Réciproquement, si on a $(*)$, montrons que $\mathrm{Sp}(A, \leq_A) \setminus \{(0)\} = \mathrm{Spm}(A)$ (ce qui donnera la conclusion puisqu'on aura alors $P(a) = M(a)$ pour tout $a \in A \setminus \{0\}$, et $(*)$ sera donc la même chose que la complémentation locale). Une inclusion étant banale, il suffit de montrer que $\mathrm{Sp}(A, \leq_A) \setminus \{(0)\} \subseteq \mathrm{Spm}(A)$. Soit $\mathfrak{p}$ un idéal premier de A, non nul et non maximal. Alors $\mathfrak{p}$ se plonge dans $\mathfrak{m} \in \mathrm{Spm}(A)$, et il existe $m \in \mathfrak{m} \setminus \mathfrak{p}$. Soit $a \in \mathfrak{p} \setminus \{0\}$, et $b \in A$ tel que $M(a) \setminus M(m) = M(a) \cap M(b)$. Naturellement $b \notin \mathfrak{m}$, et *a fortiori* $b \notin \mathfrak{p}$, donc $bm \notin \mathfrak{p}$ (car $\mathfrak{p}$ est premier). Or $M(a) \subseteq M(bm)$, *i.e.* $a \leq_A bm$, donc $\mathfrak{p}$ n'est pas r-clos.

(2) A étant intègre, il est complémenté si et seulement s'il est localement complémenté et (0) n'est pas r-clos, donc la conclusion découle immédiatement du (1).

■

Proposition 3

Un anneau A est booléen si et seulement s'il est de Prüfer et complémenté.

Preuve: Si A est booléen, il est de Prüfer d'après Ershov. Pour vérifier que $(A, \leq_A)$ est complémenté, il suffit d'après la proposition 2 de montrer que pour tout $a \in A$, il existe $b \in A$ tel que $M(a)^c = M(b)$.

Soit $a \in A$; W_A étant booléenne, il existe un élément y de $\mathrm{Fr}(A)$ tel que $W_A(y) = W_A(a)^c$. D'après l'étude de Ershov, il existe $b \in A$ tel que $W_A(b) = W_A(y)$, et puisque A est de Prüfer on a alors $M(b) = M(a)^c$.

A étant de Prüfer, il est intègre et intégralement clos, donc $A = A_{W_A}$ et W_A est homéomorphe à $\mathrm{Spm}(A)$ (*cf.* "notations et conventions", la propriété 1), donc est quasi-compact. Il suffit donc de montrer que $\mathrm{L}(W_A)$ est stable par combinaisons booléennes, *i.e.* que toute partie constructible $\mathcal{C}$ de W_A appartient à $\mathrm{L}(W_A)$. Toujours d'après la propriété 1 de la partie "notations et conventions", l'application $R \mapsto m(R) \cap A$ établit une correspondance bijective entre les parties constructibles de W_A et celles de $\mathrm{Spm}(A)$ (c'est la réciproque de $\mathfrak{m} \mapsto A_{\mathfrak{m}}$). Or $(A, \leq_A)$ étant complémenté, toute partie constructible de $\mathrm{Spm}(A)$ est de la forme $M(a)$, avec $a \in A \setminus \{0\}$. On peut donc trouver a dans A tel que $\mathcal{C} = \{A_{\mathfrak{m}} \,/\, \mathfrak{m} \in M(a)\} = W_A(a)$, *i.e.* $\mathcal{C} \in \mathrm{L}(W_A)$.

■

Définition
Un r-anneau $(A, \leq)$ sera dit **localement booléen** (resp. **booléen**) s'il satisfait les conditions suivantes :
(a) A est de Prüfer ;
(b) $(A, \leq)$ est localement complémenté (resp. complémenté) ;
(c) la relation radicale de $(A, \leq)$ est celle associée à A, *i.e.* $(A, \leq) = (A, \leq_A)$.

Remarques:
(1) Comme toujours nous dirons d'un anneau A qu'il est (localement) booléen si et seulement si $(A, \leq_A)$ l'est, et il suffit pour cela que A soit de Prüfer et (localement) complémenté puisque la condition (c) est automatiquement satisfaite par $(A, \leq_A)$. On voit qu'inversement la définition ci-dessus entraîne que tout r-anneau (localement) booléen est de cette forme.
(2) La proposition 3 nous garantit qu'un anneau est booléen au sens de Ershov si et seulement s'il est booléen au sens ci-dessus.

Exemples d'anneaux localement booléens $\cap$-stables

Les anneaux booléens, dont nous avons déja donné des exemples, sont localement booléens. Il est facile de voir que des anneaux de Prüfer factoriels comme $\mathbb{Z}$ ou $\mathbb{F}_p[T]$ sont localement booléens sans être booléens. Plus généralement, nous verrons que tout anneau de Dedekind est localement booléen. Ce qui suit montre qu'il s'agit en fait d'une propriété extrêmement courante, au point qu'il est difficile de concevoir un anneau de Prüfer qui ne soit pas localement booléen. Il est probable qu'il en existe cependant : le lecteur curieux trouvera dans le commentaire (2.10) de [VdD-M] un exemple d'anneau de Bezout qui n'a pas bonne factorisation, et un tel anneau a peu de chance d'être localement booléen (nous préciserons plus loin la relation entre Bezout et bonne factorisation pour les anneaux localement booléens indépendants).

Proposition 4
Soit A un anneau de Dedekind, tel que $Pic(A)$ soit de torsion. Alors :
(a) *Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, il existe un élément $a_{\mathfrak{m}}$ de A tel que $P(a_{\mathfrak{m}}) = \{\mathfrak{m}\}$.*
(b) *$\mathrm{L}(A, \leq_A) \setminus \{P(0)\}$ est l'ensemble des parties finies de $\mathrm{Spm}(A)$.*
(c) *A est localement booléen et $\cap$-stable.*

Preuve: Puisque A est de dimension ≤ 1, on a $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Sp}(A) = \mathrm{Spm}(A) \cup \{0\}$, donc quel que soit $a \in A \setminus \{0\}$ on a $P(a) = M(a)$.
(a) Soit $\mathfrak{m} \in \mathrm{Spm}(A)$. Par hypothèse, il existe un entier $n \in \mathbb{N}$ que $\mathfrak{m}^n$ soit un idéal principal de A. Un générateur $a_{\mathfrak{m}}$ de $\mathfrak{m}^n$ convient manifestement.

(b) Soit a un élément non nul de A. A étant de Dedekind, on sait que a n'appartient qu'à un ensemble fini d'idéaux maximaux de A. D'après ce qui précède, $P(a)$ est donc une partie finie de $\mathrm{Spm}(A)$.

Inversement, soit $\mathcal{M} := \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ une partie finie de $\mathrm{Spm}(A)$. Alors, d'après le (a), $\mathcal{M} = P\Big(\prod_{1\le i\le n} a_{\mathfrak{m}_i}\Big)$ est un élément de $\mathrm{L}(A, \le_A) \setminus \{P(0)\}$.

(c) C'est immédiat, vu (b).

■

Proposition 5

Soit B un anneau intégralement clos inclus dans la clôture algébrique de $\mathbb{Q}$ ou de $\mathbb{F}_p(T)$. Alors B est localement booléen et $\cap$-stable.

Preuve: On sait que B est de Prüfer, donc il suffit de vérifier qu'il est localement complémenté et $\cap$-stable. En remarquant que quels que soient $a, b \in B$ on a $M(a) \cap M(b) = M(a) \setminus (M(a) \setminus M(b))$, cela revient à montrer que :

$$\forall b \in B \setminus \{0\},\ \forall b_1 \in B,\ \exists b_2 \in B \setminus \{0\} \text{ tel que } M(b_2) = M(b) \setminus M(b_1).$$

Si B est de caractéristique nulle, on pose $A = \mathbb{Z}$. S'il est caractéristique $p \neq 0$, on pose $A := \mathbb{F}_p[T]$. Ou bien B est un corps et la conclusion est trivialement vérifiée, ou bien il contient une copie de A, et est inclus dans la clôture algébrique de $\mathrm{Fr}(A)$. On peut donc supposer qu'on est dans ce dernier cas.

Soit $K := \mathrm{Fr}(A)$, et $L := \mathrm{Fr}(B)$. On sait que tout anneau intégralement clos dont le corps des fractions est une extension finie de K est un anneau de Dedekind, de groupe de Picard fini. Soient $b, b_1 \in B$, avec $b \neq 0$, et $A' := B \cap K(b, b_1)$. B est intégralement clos, donc A' aussi, donc la proposition 4 s'applique : il existe $a \in A'$ tel que $M_{A'}(a) = M_{A'}(b) \setminus M_{A'}(b_1)$.

Soit B' la clôture intégrale de A' dans L. B' est de dimension ≤ 1, et on sait que pour tout $\mathfrak{n}' \in \mathrm{Spm}(B')$, $\mathfrak{n}' \cap A' \in \mathrm{Spm}(A')$, donc :

$$a \in \mathfrak{n}' \iff a \in \mathfrak{n}' \cap A' \iff b \in \mathfrak{n}' \cap A' \text{ et } b_1 \notin \mathfrak{n}' \cap A' \iff b \in \mathfrak{n}' \text{ et } b_1 \notin \mathfrak{n}'$$

i.e. $M_{B'}(a) = M_{B'}(b) \setminus M_{B'}(b_1)$.

B est un sur-anneau de B' (*i.e.* compris entre B' et $\mathrm{Fr}(B')$), et B' est un anneau de Prüfer de dimension ≤ 1, B est donc lui-même un anneau de Prüfer de dimension ≤ 1, et pour tout idéal maximal $\mathfrak{n}$ de B, on a $\mathfrak{n} \cap B' \in \mathrm{Spm}(B')$ (cf [Gil], pp. 322-324, théorèmes 26.1 et 26.2). Comme précédemment, il s'ensuit que $M_B(a) = M_B(b) \setminus M_B(b_1)$.

■

§ 2. Axiomatisation des anneaux localement booléens

Définition

J'appelle **quasi-algèbre de Boole** les treillis distributifs L avec extrémités, tels que :

$$\forall e, e' \in L, \quad e \neq \mathbf{1}_L \implies \exists e'' \in L, \begin{cases} e' \wedge e'' = \mathbf{0}_L \\ e' \vee e'' = e' \vee e \end{cases}$$

Il est clair qu'un tel e'' est unique, on le notera $e \setminus e'$.

Un quasi-algèbre de Boole sera dite **propre** si ce n'est pas une algèbre de Boole.

Exemples:
(1) Toute algèbre de Boole est une quasi-algèbre de Boole.
(2) Le treillis résiduel de tout r-anneau $\cap$-stable et localement complémenté est une quasi-algèbre de Boole (*cf.* ci-dessous).

Propriété 1
Soit $(A, \leq)$ *un r-domaine* $\cap$*-stable.*
(1) $(A, \leq)$ *est localement complémenté* $\iff$ $\mathrm{L}(A, \leq)$ *est une quasi-algèbre de Boole.*
(2) $(A, \leq)$ *est complémenté* $\iff$ $\mathrm{L}(A, \leq)$ *est une algèbre de Boole.*

Preuve: Soient $a, b, c \in A$.
– Comme $\mathrm{L}(A, \leq)$ est stable par $\cup$ on a : $P(a) = P(b) \vee P(c)$ si et seulement si $P(a) = P(b) \cup P(c)$.
– Comme $(A, \leq)$ est $\cap$-stable on a : $P(a) = \inf(P(b), P(c))$ si et seulement si $P(a) = P(b) \cap P(c)$.
On a donc $P(a) = P(b) \setminus P(c)$ dans $\mathrm{L}(A, \leq)$, au sens défini ci-dessus des quasi-algèbres de Boole, si et seulement si $P(a) = P(b) \setminus P(c)$ au sens ensembliste c'est-à-dire $P(a) = P(b) \cap P(c)^c$. La conclusion en découle immédiatement.
■

Il est clair que la classe des quasi-algèbres de Boole est axiomatisable au premier ordre dans le langage des treillis, ou même dans celui des ensembles ordonnés. Comme le TSUP résiduel d'un r-domaine y est interprétable, il était tentant d'essayer d'axiomatiser les r-domaines localement complémentés en les identifiant aux r-domaines dont le TSUP résiduel est une quasi-algèbre de Boole. Malheureusement cette notion, si elle est bien du premier ordre, ne donne pas du tout les résultats voulus : $\mathbb{Q}[X, Y]$ est l'exemple typique d'un anneau dont le TSUP résiduel est une quasi-algèbre de Boole, sans que cet anneau soit localement complémenté (ceci montre en passant que l'hypothèse d'$\cap$-stabilité n'est pas superflue dans la propriété 1).

On aurait pu également essayer de se restreindre aux anneaux localement complémentés et $\cap$-stables ; mais toutes mes tentatives pour relier la complémentation locale et l'$\cap$-stabilité ont échoué : d'une part je ne connais pas d'exemple d'anneau localement complémenté qui ne soit pas $\cap$-stable, et d'autre part je ne vois aucune bonne raison de croire qu'il n'en existe pas. Or l'$\cap$-stabilité est une hypothèse suplémentaire gênante pour les diverses propriétés que nous axiomatiserons plus loin dans le cadre des anneaux localement booléens ; enfin et surtout j'ignore toujours si l'$\cap$-stabilité est axiomatisable au premier ordre dans le langage des anneaux.

Il est possible qu'il existe cependant pour les anneaux de Prüfer une solution autre que celle que nous présentons maintenant : pour axiomatiser les anneaux localement complémentés, nous allons passer par leurs localisés.

Lemme 2
Soit $(A, \leq)$ *un r-anneau complémenté. Alors sont équivalents :*
(i) *Pour tout* $a \in A$, $(a \leq 1 \Longrightarrow a \in A^*)$.
(ii) $\mathrm{Sp}(A, \leq) = \mathrm{Spm}(A)$.

Preuve: Si $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq)$, alors $\cup\mathrm{Sp}(A, \leq) = \cup\mathrm{Spm}(A)$, donc pour tout élément

a de A, on a :

$$a \leq 1 \iff a \in A \setminus \cup\mathrm{Sp}(A, \leq) = A \setminus \cup\mathrm{Spm}(A) = A^*.$$

L'implication (ii)$\Longrightarrow$(i) est donc claire (et générale).

Inversement, supposons (i). Puisque $(A, \leq)$ est complémenté, les éléments du spectre r-clos de $(A, \leq)$ sont deux à deux incomparables pour l'inclusion. Il suffit donc de montrer que tout élément de $\mathrm{Spm}(A)$ est r-clos.

Soit $\mathfrak{m}_0 \in \mathrm{Spm}(A)$ fixé, et supposons, par l'absurde, que $\mathfrak{m}_0$ ne soit pas r-clos. Pour tout $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$, $\mathfrak{m}_0 \not\subseteq \mathfrak{p}$ (sinon par maximalité $\mathfrak{m}_0 = \mathfrak{p}$ est r-clos), donc il existe $a_\mathfrak{p} \in \mathfrak{m}_0 \setminus \mathfrak{p}$. Les $(P(a_\mathfrak{p})^c)_{\mathfrak{p} \in \mathrm{Sp}(A, \leq)}$ constituent un recouvrement ouvert de $\mathrm{Sp}(A, \leq)$, d'où l'on peut extraire un recouvrement fini $(P(a_i)^c)_{1 \leq i \leq n}$ (avec les $a_i \in \mathfrak{m}_0$).

Puisque $(A, \leq)$ est complémenté, il existe $\beta_1 \in A$ tel que $P(\beta_1) = P(a_1)^c$. Pour tout $k \in [\![1, n-1]\!]$, si $\beta_1, \ldots, \beta_k$ ont été déjà construits, on prend $\beta_{k+1} \in A$ tel que $P(\beta_{k+1}) = P(a_{k+1})^c \setminus \cup_{1 \leq i \leq k} P(\beta_k)$. Il est clair que les $(P(\beta_i))_{1 \leq i \leq n}$ constituent une partition de $\mathrm{Sp}(A, \leq)$ et que pour chaque $i \in [\![1, n]\!]$, on a $P(\beta_i) \subseteq P(a_i)^c$. On pose alors :

- $\forall i \in [\![1, n]\!]$, $\alpha_i = \prod_{j \neq i} \beta_j$,
- $a := \sum_{i=1}^n \alpha_i a_i$.

Tous les a_i appartiennent à $\mathfrak{m}_0$, donc $a \in \mathfrak{m}_0$. D'autre part, pour tout $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$, il existe un unique $i_\mathfrak{p} \in [\![1, n]\!]$ tel que $\mathfrak{p} \in P(\beta_{i_\mathfrak{p}})$. On a $P(\beta_{i_\mathfrak{p}}) = P(\alpha_{i_\mathfrak{p}})^c \subseteq P(a_{i_\mathfrak{p}})^c$, donc $\alpha_{i_\mathfrak{p}} a_{i_\mathfrak{p}} \notin \mathfrak{p}$; et pour tout $i \in [\![1, n]\!] \setminus \{i_\mathfrak{p}\}$, $\beta_{i_\mathfrak{p}}$ divise α_i, donc $\alpha_i a_i \in \mathfrak{p}$. Il s'ensuit que $a \notin \mathfrak{p}$. Ceci étant valable pour tout $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$, on a $a \leq 1$ donc d'après (i) $a \in A^*$, ce qui contredit $a \in \mathfrak{m}_0$, et achève la démonstration.

■

Proposition 3

Soit A un anneau intègre localement complémenté, I un idéal tel que $(0) \neq I \neq A$, et $S_I := A \setminus \bigcup M(I)$ (où $M(I) = \{\mathfrak{m} \in \mathrm{Spm}(A) \,/\, I \subseteq \mathfrak{m}\}$). Alors :

(a) $\mathrm{Spm}(S_I^{-1}A) = \{S_I^{-1}\mathfrak{m} \,/\, \mathfrak{m} \in M(I)\}$;

(b) $S_I^{-1}A$ *est complémenté.*

En particulier, pour tout $a \in A \setminus \{0\}$ on a : $W_A(a) = W_{S_a^{-1}A}$ (rappelons que nous notons $S_a := A \setminus \bigcup M(a)$).

Preuve: I étant un idéal propre de A, $M(I) \neq \emptyset$ donc $0 \notin S_I$; on sait donc que $\{S_I^{-1}\mathfrak{m} \,/\, \mathfrak{m} \in M(I)\} \subseteq \mathrm{Spm}(S_I^{-1}A)$. Pour alléger les notations posons $A' := S_I^{-1}A$, $\mathcal{M}' := \{S_I^{-1}\mathfrak{m} \,/\, \mathfrak{m} \in M(I)\}$ et considérons la relation radicale $\leq'$ définie sur A' par $\mathcal{M}'$.

On commence par montrer que $\mathrm{Sp}(A', \leq') = \mathcal{M}'$. Soit $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$; on sait que $\mathfrak{p} := \mathfrak{p}' \cap A \in \mathrm{Sp}(A)$ et que $\mathfrak{p}' = S_I^{-1}\mathfrak{p}$ donc il suffit de montrer que $\mathfrak{p} \in M(I)$. Quel que soit $a \in I$ on a $0 \leq' a$, donc $a \in \mathfrak{p}' \cap A = \mathfrak{p}$, *i.e.* $I \subseteq \mathfrak{p}$. Comme A est localement complémenté on sait que $\mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Spm}(A) \cup \{0\}$, et comme $I \neq (0)$ *a fortiori* $\mathfrak{p} \neq (0)$ donc pour montrer que $\mathfrak{p}$ est maximal il suffit de vérifier qu'il est r-clos dans $(A, \leq_A)$.

Soient $a \in \mathfrak{p}$ et $b \in A$ tel que $a \leq_A b$. Quel que soit $\forall \mathfrak{M} \in \mathcal{M}'$, si $a \in \mathfrak{M}$ alors $a \in \mathfrak{m} := \mathfrak{M} \cap A \in M(I)$ donc $b \in \mathfrak{m} \subseteq S_I^{-1}\mathfrak{m} = \mathfrak{M}$ *i.e.* $a \leq' b$. Il s'ensuit que $b \in \mathfrak{p}'$ (par r-clôture de $\mathfrak{p}'$) et finalement que $b \in \mathfrak{p}$ *i.e.* $\mathfrak{p}$ est bien r-clos.

On vérifie ensuite que $(A', \leq')$ est complémenté. Soit $b' = b/s \in A'$, avec $b \in A$ et $s \in S_I$, et soient $\alpha \in I \setminus \{0\}$ et $c \in A$ tels que $P_A(\alpha) \cap P_A(c) = P_A(\alpha) \setminus P_A(b)$. Quel que soit $\mathfrak{m}' \in \mathcal{M}'$ on a $\mathfrak{m} := \mathfrak{m}' \cap A \in M(I) \subseteq M(\alpha)$, donc $b \in \mathfrak{m} \iff c \notin \mathfrak{m}$, *i.e.* $b/s \in \mathfrak{m}' \iff c \notin \mathfrak{m}'$ puisque s est inversible dans A'.

Enfin quel que soit $b' \in A'$ tel que $b' \leq' 1$ on l'écrit $b' = b/s$ avec $b \in A$ et $s \in S_I$; comme s est inversible dans A' on a $b = sb' \leq' s \leq' 1$, donc quel que soit $\mathfrak{m} \in M(I)$ on a $b' \leq' 1 \Longrightarrow b' \notin S_I^{-1}\mathfrak{m} \Longrightarrow b \notin \mathfrak{m}$, et il s'ensuit que $b \in A \setminus \cup M(I) = S_I$, *i.e.* $b' \in A'^*$. le lemme 2 entraîne alors que $\mathrm{Spm}(A') = \mathrm{Sp}(A', \leq')$, ce qui prouve à la fois (a) et (b).

En particulier, pour tout $a \in A \setminus \{0\}$ et tout $\mathcal{M} \in \mathrm{Spm}(S_a^{-1}A)$ on a $(S_a^{-1}A)_{\mathcal{M}} = A_{\mathfrak{m}}$ où $\mathfrak{m} := \mathcal{M} \cap A \in \mathrm{Spm}(A)$, donc $W_{S_a^{-1}A} \subseteq \{R \in W(a) /\ a \in m(R)\} = W_A(a)$, et l'inclusion inverse est banale (on sait que quel que soit $\mathfrak{m} \in \mathrm{Spm}(A)$, $S_a^{-1}\mathfrak{m}$ est un idéal maximal de $S_a^{-1}A$).

∎

Corollaire 4

Soit A un anneau intègre. Les assertions suivantes sont équivalentes :

(i) *A est localement complémenté.*

(ii) *Pour tout $a \in A$, non nul et non inversible, $S_a^{-1}A$ est complémenté.*

Preuve: (i)$\Longrightarrow$(ii). Soit a un élément non nul et non inversible de A. Par définition $S_a = A \setminus \cup P(a)$, et comme A est localement complémenté et que $a \neq 0$ on a $P(a) = M(a) = M((a)_{\leq})$. La proposition 3 appliqué à $I := (a)_{\leq}$ donne donc la conclusion.

(ii)$\Longrightarrow$(i). On montre d'abord que $\mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Spm}(A) \cup \{(0)\}$: soit $\mathfrak{p} \in \mathrm{Sp}(A)$, et supposons $\mathfrak{p} \notin \mathrm{Spm}(A) \cup \{(0)\}$; $\mathfrak{p}$ se plonge dans un $\mathfrak{m} \in \mathrm{Spm}(A)$ qui le contient strictement. Soit $a \in \mathfrak{p} \setminus \{0\}$, et $A' := S_a^{-1}A$. On a $a \in \mathfrak{p} \subseteq \mathfrak{m}$ donc $\mathfrak{m} \in P(a)$, et $\mathfrak{m} \cap S_a = \emptyset$. Il s'ensuit que $\mathfrak{p}' := S_a^{-1}\mathfrak{p}$ est strictement inclus dans $\mathfrak{m}' := S_a^{-1}\mathfrak{m}$, donc n'appartient pas à $\mathrm{Spm}(A')$. Pour tout $\mathfrak{n}' \in \mathrm{Spm}(A')$, on a donc un point $b_{\mathfrak{n}'} \in \mathfrak{n}' \setminus \mathfrak{p}'$. A' étant complémenté, il existe $c_{\mathfrak{n}'} \in A'$ tel que $M_{A'}(c_{\mathfrak{n}'}) = M_{A'}(b_{\mathfrak{n}'})^c$. Les $(M_{A'}(c_{\mathfrak{n}'})^c)_{\mathfrak{n}' \in \mathrm{Spm}(A')}$ recouvrent $\mathrm{Spm}(A')$, on peut donc en extraire un recouvrement fini $(M_{A'}(c_{\mathfrak{n}'_i})^c)_{1 \leq i \leq n}$.

Posons $b' := \prod_{i=1}^{n} b_{\mathfrak{n}'_i}$. Par construction $b' \notin \mathfrak{p}'$, et $M_{A'}(b') = \cup_{i=1}^{n} M_{A'}(c_{\mathfrak{n}'_i})^c = \mathrm{Spm}(A')$, donc $0 \leq_{A'} b'$. On peut écrire b' sous la forme b/s, avec $b \in A$ et $s \in S_a$, et comme s est inversible dans A' on a encore $b \notin \mathfrak{p}'$ et $0 \leq_{A'} b$. Pour tout $\mathfrak{n} \in M_A(a)$, on a $S^{-1}\mathfrak{n} \in \mathrm{Spm}(A')$, donc $b \in S^{-1}\mathfrak{n} \cap A = \mathfrak{n}$, *i.e.* $a \leq_A b$. Comme d'autre part $a \in \mathfrak{p}$ et $b \notin \mathfrak{p}$, il s'ensuit que $\mathfrak{p}$ n'est pas r-clos, et on a bien montré que $\mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Spm}(A) \cup \{(0)\}$.

Pour en déduire la complémentation locale, on prend $a \in A \setminus \{0\}$ et $b \in A$. Si a est inversible $P(a) \setminus P(b) = \emptyset = P(a) \cap P(1)$. On peut donc écarter ce cas et supposer a non inversible. Par hypothèse $A' := S_a^{-1}A$ est complémenté, donc il existe $c' = c/s \in A'$ tel que $M_{A'}(c') = M_{A'}(b)^c$. Comme s est inversible dans A', on a encore $M_{A'}(c) = M_{A'}(c') = M_{A'}(b)^c$. Pour tout $\mathfrak{m} \in P(a)$, $a \neq 0$ donc $\mathfrak{m} \in \mathrm{Spm}(A)$, et $\mathfrak{m} \cap S_a = \emptyset$, donc $S_a^{-1}\mathfrak{m} \in \mathrm{Spm}(A')$. On en déduit :

$$c \in \mathfrak{m} \iff S_a^{-1}\mathfrak{m} \in M_{A'}(c) \iff S_a^{-1}\mathfrak{m} \notin M_{A'}(b) \iff b \notin \mathfrak{m}$$

i.e. $P_A(a) \setminus P_A(b) = P_A(a) \cap P_A(c)$, et A est donc bien localement complémenté.

∎

Corollaire 5
Un anneau intègre A est localement booléen si et seulement si pour tout $a \in A$, non nul et non inversible, $S_a^{-1}A$ est localement booléen.

Preuve: C'est immédiat, d'après le corollaire 4 et le fait (connu) qu'un anneau intègre A est de Prüfer si et seulement si pour tout $a \in A$, non nul et non inversible, $S_a^{-1}A$ est de Prüfer.

■

Nous pouvons maintenant axiomatiser les anneaux localement complémentés et localement booléens, après avoir rappelé l'évidence suivante :

Propriété 6
Soit $\varphi(x)$ une formule du langage des anneaux, à n variables libres. Il existe des formules $\varphi^0(x), \varphi^1(x,t)$ et $\varphi^2(x,x',t)$, du même langage, respectivement à n, $n+1$ et $n+n+1$ variables libres, telles que tout anneau intègre A, tout $a \in A^n$, tout $\alpha \in A \setminus (A^* \cup \{0\})$ et tout $a' \in S_\alpha^n$ vérifient :

(a) $A \models \varphi^0(a) \iff \forall \beta \in A \setminus (A^* \cup \{0\}),\ S_\beta^{-1}A \models \varphi(a)$;

(b) $A \models \varphi^1(a, \alpha) \iff S_\alpha^{-1}A \models \varphi(a)$;

(c) $A \models \varphi^2(a, a', \alpha) \iff S_\alpha^{-1}A \models \varphi(a_1/a'_1, \ldots, a_n/a'_n)$.

En particulier, si T est une théorie d'anneaux, la classe des anneaux A tels que pour tout $a \in A \setminus (A^* \cup \{0\})$ le localisé $S_a^{-1}A$ soit modèle de T, est élémentaire.

Remarque: On aurait aussi bien pu autoriser la formule $\varphi(x)$ à être dans $\mathrm{L_{rad}}$ ou $\mathrm{L_{div}}$, puisque nous avons vu qu'une telle formule se "traduit" en une formule du langage des anneaux, les relations $\leq_A$ et $|_A$ étant (uniformément) interprétables dans la structure d'anneau. Nous ne nous priverons pas d'utiliser la propriété 6 sous cette forme un peu plus générale.

Preuve: Il suffit de montrer le (c), et de prendre ensuite $\varphi^1(x,t) \equiv \varphi^2(x,1,\ldots,1,t)$ et $\varphi^o(x) \equiv \forall t,\ (t \neq 0 \wedge \forall t',\ t't \neq 1) \to \varphi^1(x,t)$. Le "en particulier..." en découle immédiatement : si $(\varphi_n)_{n\in\mathbb{N}}$ est une énumération de T, l'ensemble des φ_n^0, pour $n \in \mathbb{N}$ axiomatise la classe en question.

On démontre (c) par récurrence sur la complexité de la formule $\varphi(x)$:

- $\varphi(x) \equiv f(x) = 0$, avec $f \in \mathbb{Z}[X_1, \ldots, X_n]$.
  On prend $\varphi^2(x,x',t) \equiv f^*(x,x') = 0$, où $f^* \in \mathbb{Z}[X_1,\ldots,X_n,X'_1,\ldots,X'_n]$ est défini par :
$$f^* = f\Big(\frac{X_1}{X'_1}, \ldots, \frac{X_n}{X'_n}\Big) \times \prod_{i=1}^{n} X_i'^{d^\circ_{X_i} f}.$$
- $\varphi(x) \equiv \neg\psi(x)$.
  On prend $\varphi^2(x,x',t) \equiv \neg\psi(x,x',t)$.
- $\varphi(x) \equiv \exists y \psi(x,y)$.
  On prend $\varphi^2(x,x',t) \equiv \exists y, \exists y'(y' \neq 0 \wedge (y',t) = 1 \wedge \psi^2(x,y,x',y',t))$, où la sous-formule "$(y',t) = 1$" abrège "$\exists u, \exists v(uy' + vt = 1)$".

La vérification que la formule $\varphi^2(x,x',t)$ ainsi construite a bien la propriété voulue est immédiate, et laissée au lecteur.

■

Proposition 7
Les propriétés suivantes sont axiomatisables dans le langage des anneaux :
(a) *être de Prüfer ;*
(b) *être localement complémenté ;*
(c) *être localement booléen.*

Remarque: On notera que les anneaux intègres complémentés (resp. booléens) étant exactement les anneaux localement complémentés (resp. booléens) dont le radical de Jacobson est nul, ou encore qui satisfont l'axiome (o) des $\mathrm{r}_\circ$-domaines, ceux-ci sont donc également axiomatisés par la proposition 7.

Incidemment, on obtient ainsi une axiomatisation des anneaux booléens différente de celle proposée par Ershov.

Preuve:
(a) C'est connu, voir par exemple [VdD-M].

(b) Le corollaire 4, combiné à la propriété 6 ci-dessus, montre qu'il suffit de vérifier que la classe des anneaux complémentés est élémentaire ; mais il est immédiat que pour tout anneau A et pour tous $a, b \in A$ on a :

$$M(a) = M(b)^c \iff 0 \leq_A ab \text{ et il existe } u, v \in A,\ au + bv = 1$$

donc la formule "$\forall a, \exists b,\ (0 \leq ab \wedge \exists u, \exists v(au + bv = 1))$" (ou plus exactement sa traduction dans le langage des anneaux) axiomatise la classe des anneaux complémentés.

(c) Un anneau est localement booléen si et seulement s'il est de Prüfer et localement complémenté, ce qui est du premier ordre vu (a) et (b).

■

§ 3. Approximation par blocs

La propriété suivante apparaît, sous une forme ou une autre, dans toutes les études modèle-théoriques sur les corps munis d'une famille de topologies.

Définition
Une famille W d'anneaux de valuation sur un corps K est dite avoir la propriété d'**approximation par blocs**, (en abrégé BAP) si et seulement si :
– pour toute partition constructible $W_1, \ldots, W_p$, de W,
– $\forall x_1, \ldots, x_p \in K,\ \ \forall \varepsilon_1, \ldots, \varepsilon_p \in K \setminus \{0\}$
il existe $x \in K$ tel que :

$$\forall i \in [\![1, p]\!],\ \forall R \in W_i, \quad |x - x_i|_R \leq |\varepsilon_i|_R.$$

Exemples:
(1) Il est bien connu qu'une famille finie d'anneaux de valuation a la BAP si et seulement si ces valuations sont deux à deux indépendantes (c'est le théorème d'approximation simultanée pour les valuations indépendantes).
(2) On trouvera dans [Mal], p.138, lemme 6.25, la preuve du fait suivant : si A est un anneau de Dedekind, alors W_A a la BAP.

Propriété 1
Une famille W d'anneaux de valuation sur un corps K a la BAP si et seulement si pour

toute partie constructible W_1 de W, pour tous $x_1, x_2 \in K$ et pour tous $\varepsilon_1, \varepsilon_2 \in K \setminus \{0\}$ il existe $x \in K$ tel que :

$$\begin{cases} \forall R \in W_1, & |x - x_1|_R \leq |\varepsilon_1|_R \\ \forall R \in W \setminus W_1, & |x - x_2|_R \leq |\varepsilon_2|_R. \end{cases}$$

Preuve: C'est une récurrence triviale.

■

Propriété 2

Soit W une famille d'anneaux de valuation sur un corps K. Si W a la BAP, alors pour tout $R \in W$, l'anneau d'holomorphie de W est dense dans R (au sens de la valuation de R).

Preuve: Soient $R_0 \in W$, $x \in R_0$ et $\varepsilon \in K \setminus \{0\}$. On veut trouver $a \in A_W = \cap W$ tel que $|a - x|_{R_0} \leq |\varepsilon|_{R_0}$. On peut bien sûr supposer que $x \notin A_W$, donc $x \neq 0$, et que $\varepsilon \in R_0$. Soit $W_1 := W(x^{-1})^c \cap W(\varepsilon^{-1})^c$ l'ensemble des $R \in W$ tel que $x, \varepsilon \in R$. La BAP donne un élément a de K tel que :

$$\begin{cases} \forall R \in W_1, & |a - x|_R \leq |\varepsilon|_R, \\ \forall R \in W \setminus W_1, & |a|_R \leq |1|_R. \end{cases}$$

Pour tout $R \in W$, si $R \in W_1$ alors $x \in R$ et $|a - x|_R \leq |\varepsilon|_R \leq 1$, donc $a \in R$, sinon $|a|_R \leq 1$, *i.e.* $a \in R$, et au total $a \in \cap W$. De plus $R_0 \in W_1$, donc $|x - a|_{R_0} \leq |\varepsilon|_{R_0}$.

■

Définitions

Un anneau A est **indépendant** si et seulement s'il est intègre et si W_A est indépendante, c'est à dire si :

$$\forall R, R' \in W_A,\ R \neq R' \Longrightarrow RR' = \mathrm{Fr}(A).$$

Il a la **BAP** si et seulement s'il est intègre, intégralement clos et si W_A a la BAP.

L'indépendance a peu de chance d'être une propriété axiomatisable au premier ordre en toute généralité. En revanche, nous allons montrer qu'elle l'est pour les anneaux localement booléens, tout simplement parce qu'elle coïncide pour ceux-ci avec la BAP. Encore faudra-t-il ensuite démontrer que la BAP est elle-même du premier ordre ! Nous le ferons en deux temps : d'abord dans ce paragraphe en vérifiant que la BAP est une propriété locale (*cf.* le corollaire final) puis en la reliant à la bonne factorisation.

Proposition 3

Tout anneau ayant la BAP est localement booléen et indépendant.

Preuve: Soit A un anneau ayant la BAP. L'indépendance de A est claire, et $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq_A)$ par définition, donc il suffit de vérifier que A est de Prüfer, et localement complémenté. Notons que, A étant intégralement clos, $A = \cap W_A$.

(a) A est de Prüfer.
Soit $\mathfrak{m} \in \mathrm{Spm}(A)$; $A_\mathfrak{m}$ est intégralement clos, donc $A_\mathfrak{m} = \cap W_{A_\mathfrak{m}}$. Si $W_{A_\mathfrak{m}}$ est réduite à un élément R, il s'ensuit que $A_\mathfrak{m} = R$, et donc $A_\mathfrak{m}$ est un anneau de valuation.

Par l'absurde, supposons que $W_{A_\mathfrak{m}}$ ne soit pas réduite à un seul élément, et prenons $R_1 \neq R_2 \in W_{A_\mathfrak{m}}$. Comme ils dominent tous les deux $A_\mathfrak{m}$, nécessairement $R_1 \not\subseteq R_2$ et

$R_2 \not\subseteq R_1$. Soient donc $x_1 \in R_1 \setminus R_2$ et $x_2 \in R_2 \setminus R_1$. La BAP donne $x \in K$ tel que :

$$\begin{cases} \forall R \in W_A\left(\dfrac{1}{x_2}\right), & \left|x - \dfrac{1}{x_2}\right|_R \leq \left|\dfrac{1}{x_2}\right|_R \\ \forall R \in W_A(x_1)^c \cap W_A\left(\dfrac{1}{x_2}\right)^c, & |x-1|_R \leq \left|\dfrac{1}{x_1}\right|_R \\ \forall R \in W_A(x_1) \cap W_A\left(\dfrac{1}{x_2}\right)^c, & |x|_R \leq 1 \end{cases}$$

Il s'ensuit que $\forall R \in W_A, |x|_R \leq 1$, et donc $x \in \cap W_A = A$. De plus :

- $R_1 \in W_A(\frac{1}{x_2}) \Longrightarrow |x|_{R_1} \leq \left|\frac{1}{x_2}\right|_{R_1} < 1 \Longrightarrow x \in m(R_1) \cap A = \mathfrak{m}$,
- $R_2 \in W_A(\frac{1}{x_2})^c \cap W_A(\frac{1}{x_1}) \Longrightarrow |x|_{R_2} = 1 \Longrightarrow x \notin m(R_2)$.

Comme $\mathfrak{m} \subseteq m(R_2)$, les deux informations apportent une contradiction, et $A_\mathfrak{m}$ est donc bien un anneau de valuation.

(b) $(A, \leq_A)$ est localement complémenté.
Soient $a \in A \setminus \{0\}$ et $b \in A$. La BAP donne $c \in K$ tel que :

$$\begin{cases} \forall R \in W_A(a) \setminus W_A(b), & |c-a|_R \leq |a|_R, \\ \forall R \in (W_A(a) \setminus W_A(b))^c, & |c-1|_R \leq |b|_R. \end{cases}$$

On a donc :

- $\forall R \in W_A(a) \setminus W_A(b), \quad |c|_R \leq |a|_R < 1$,
- $\forall R \in W_A(a) \cap W_A(b), \quad |c|_R = 1$,
- $\forall R \in W_A(a)^c, \quad |c|_R \leq 1$.

Il s'ensuit que $c \in \cap W_A = A$, et que $M(c) \cap M(a) = M(b)^c \cap M(a)$.

■

Nous avons cité le lemme 6.25 de [Mal] selon lequel tout anneau de Dedekind a la BAP. Le résultat suivant, que nous avions annoncé, découle donc immédiatement de la proposition 3.

Corollaire 4
Tout anneau de Dedekind est localement booléen.

Ershov a montré que pour un anneau booléen, W_A a la BAP si et seulement si A est indépendant. Sa démonstration utilise de façon cruciale le fait qu'un anneau booléen a un radical de Jacobson non nul, elle ne peut donc pas être recyclée pour les anneaux localement booléens. Nous proposons ici une preuve un peu différente, qui marche dans les deux cas.

Lemme 5
Soit A un anneau de Prüfer tel que, pour tous $\alpha, \varepsilon_0, \varepsilon_1 \in A \setminus \{0\}$, et pour tous $a_0, a_1 \in A$, on ait $a \in A$ tel que :

$$\forall \mathfrak{m} \in \mathrm{Spm}(A), \begin{cases} \alpha \notin \mathfrak{m} \Longrightarrow |a - a_0|_\mathfrak{m} \leq |\varepsilon_0|_\mathfrak{m} \\ \alpha \in \mathfrak{m} \Longrightarrow |a - a_1|_\mathfrak{m} \leq |\varepsilon_1|_\mathfrak{m} \end{cases}$$

Alors A a la BAP.

Preuve: On commence par montrer que A est localement complémenté. Soient $a, b \in A$, avec $a \neq 0$. Il existe $c \in A$ tel que :

$$\begin{cases} \forall \mathfrak{m} \in M(b), & |c-1|_\mathfrak{m} \ \leq |b|_\mathfrak{m} \\ \forall \mathfrak{m} \in M(b)^c, & |c-a|_\mathfrak{m} \ \leq |a^2|_\mathfrak{m} \end{cases}$$

Cet élément c de A nous est donné par l'hypothèse si $b \neq 0$, et sinon il suffit de prendre $c = 1$. Alors pour tout $\mathfrak{m} \in M(b)$, $|c-1|_\mathfrak{m} < 1$ donc $|c|_\mathfrak{m} = 1$, *i.e.* $M(c) \cap M(b) = \emptyset$. D'autre part pour tout $\mathfrak{m} \in M(a) \cap M(b)^c$, on a $|c-a|_\mathfrak{m} < |a|_\mathfrak{m}$, donc $|c|_\mathfrak{m} = |a|_\mathfrak{m}$, *i.e.* $M(c) \supseteq M(a) \cap M(b)^c$. Au total on a $M(a) \cap M(b)^c = M(a) \cap M(c)$, et A est bien localement complémenté d'après la proposition 1.2.

Il s'ensuit que pour toute partie constructible $\mathcal{M}$ de $\mathrm{Spm}(A)$ et pour tout $a \in A \setminus \{0\}$, on peut trouver $b \in A$ tel que $M(a) \cap \mathcal{M} = M(a) \cap M(b)$.

Soient W_1 une partie constructible de W, $x_1, x_2 \in K$ et $\varepsilon_1, \varepsilon_2 \in K \setminus \{0\}$. D'après la propriété 1, il suffit de trouver $x \in K$ tel que

$$\begin{cases} \forall R \in W_1, & |x-x_1|_R \ \leq |\varepsilon_1|_R \\ \forall R \in W \setminus W_1, & |x-x_2|_R \ \leq |\varepsilon_2|_R \end{cases}$$

Soient $a_1, a_2 \in A$, $\delta_1, \delta_2, u \in A \setminus \{0\}$ tels que $x_1 = a_1/u$, $x_2 = a_2/u$, $\varepsilon_1 = \delta_1/u$ et $\varepsilon_2 = \delta_2/u$. Posons $\alpha := \delta_1\delta_2 u$.

A étant de Prüfer, la propriété 1 de la partie "notations et conventions" entraîne que $\mathcal{M} := \{m(R) \cap A \,/\, R \in W_1\}$ est une partie constructible de $\mathrm{Spm}(A)$. On a donc $\beta \in A$ tel que $M(\alpha) \cap \mathcal{M} = M(\alpha) \cap M(\beta)$. L'hypothèse sur A nous donne $a \in A$ tel que :

$$\begin{cases} \forall \mathfrak{m} \in M(\beta), & |a-a_1|_\mathfrak{m} \leq |\alpha|_\mathfrak{m} \\ \forall \mathfrak{m} \in M(\beta)^c, & |a-a_2|_\mathfrak{m} \leq |\alpha|_\mathfrak{m} \end{cases}$$

Posons $x := a/u$.

– Pour tout $\mathfrak{m} \in \mathcal{M}$, ou bien α n'appartient pas à $\mathfrak{m}$, et alors u et δ_1 non plus, donc $|x-x_1|_\mathfrak{m} = |a-a_1|_\mathfrak{m} \leq 1 = |\varepsilon_1|_\mathfrak{m}$; ou bien α appartient à $\mathfrak{m}$, donc $\mathfrak{m} \in M(\alpha) \cap \mathcal{M} = M(\alpha) \cap M(\beta)$, et $\mathfrak{m} \in M(\beta)$, donc :

$$|x-x_1|_\mathfrak{m} = \left|\frac{a-a_1}{u}\right|_\mathfrak{m} \leq \left|\frac{\alpha}{u}\right|_\mathfrak{m} = |\delta_1\delta_2|_\mathfrak{m} = |u\varepsilon_1\delta_2|_\mathfrak{m} \leq |\varepsilon_1|_\mathfrak{m}.$$

– Pour tout $\mathfrak{m} \in \mathrm{Spm}(A) \setminus \mathcal{M}$, ou bien $\alpha \notin \mathfrak{m}$ et alors comme tout à l'heure $|x-x_2|_\mathfrak{m} = |a-a_2|_\mathfrak{m} \leq 1 = |\varepsilon_2|_\mathfrak{m}$; ou bien $\alpha \in \mathfrak{m}$, et alors $\mathfrak{m} \in M(\alpha) \cap \mathcal{M}^c = M(\alpha) \cap M(\beta)^c$, et donc

$$|x-x_2|_\mathfrak{m} = \left|\frac{a-a_2}{u}\right|_\mathfrak{m} \leq \left|\frac{\alpha}{u}\right|_\mathfrak{m} = |\delta_1\delta_2|_\mathfrak{m} \leq |\varepsilon_2|_\mathfrak{m}.$$

x a donc bien les propriétés cherchées.

■

Lemme 6

Soit A un anneau de Prüfer. Si $\forall \alpha_1, \alpha_2, \varepsilon_1, \varepsilon_2 \in A \setminus \{0\}$, $\exists \delta_1, \delta_2 \in A$, tels que :

$$\begin{cases} M(\delta_1) \cap M(\delta_2) = \emptyset \\ \forall \mathfrak{m} \in M(\alpha_1) \setminus M(\alpha_2), & |\delta_1|_\mathfrak{m} \leq |\varepsilon_1|_\mathfrak{m} \\ \forall \mathfrak{m} \in M(\alpha_1) \cap M(\alpha_2), & |\delta_2|_\mathfrak{m} \leq |\varepsilon_2|_\mathfrak{m} \end{cases}$$

alors A a la BAP.

Preuve: Soient $\alpha, \varepsilon_1, \varepsilon_2 \in A \setminus \{0\}$, et $a_1, a_1 \in A$.

On cherche $a \in A$ comme dans le lemme 5. L'hypothèse nous donne $\delta_1, \delta_2 \in A$ tels que :
- $M(\delta_1) \cap M(\delta_2) = \emptyset$;
- $\forall \mathfrak{m} \in M(\alpha\varepsilon_2) \cap M(\alpha) = M(\alpha), \quad |\delta_1|_{\mathfrak{m}} \leq |\varepsilon_1|_{\mathfrak{m}}$;
- $\forall \mathfrak{m} \in M(\alpha\varepsilon_2) \setminus M(\alpha) = M(\varepsilon_2) \setminus M(\alpha), \quad |\delta_2|_{\mathfrak{m}} \leq |\varepsilon_2|_{\mathfrak{m}}$.

Alors il existe $u_1, u_2 \in A$ tels que $u_1\delta_1 + u_2\delta_2 = 1$. Soit $a := a_2u_1\delta_1 + a_1u_2\delta_2$. Pour tout $\mathfrak{m} \in M(\alpha)$, on a :
- $|a_2u_1\delta_1|_{\mathfrak{m}} \leq |\delta_1|_{\mathfrak{m}} \leq |\varepsilon_1|_{\mathfrak{m}}$;
- $|a_1u_2\delta_2 - a_1|_{\mathfrak{m}} = |a_1(u_2\delta_2 - 1)|_{\mathfrak{m}} = |a_1u_1\delta_1|_{\mathfrak{m}} \leq |\delta_1|_{\mathfrak{m}} \leq |\varepsilon_1|_{\mathfrak{m}}$;

donc $|a - a_1|_{\mathfrak{m}} \leq \max(|a_2u_1\delta_1|_{\mathfrak{m}}, |a_1u_2\delta_2 - a_1|_{\mathfrak{m}}) \leq |\varepsilon_1|_{\mathfrak{m}}$.

De même, $\forall \mathfrak{m} \in M(\alpha)^c$, si $\mathfrak{m} \notin M(\varepsilon_2)$ alors trivialement $|a - a_2|_{\mathfrak{m}} \leq 1 = |\varepsilon_2|_{\mathfrak{m}}$, et sinon on a :
- $|a_1u_2\delta_2|_{\mathfrak{m}} \leq |\delta_2|_{\mathfrak{m}} \leq |\varepsilon_2|_{\mathfrak{m}}$;
- $|a_2u_1\delta_1 - a_2|_{\mathfrak{m}} = |a_2(u_1\delta_1 - 1)|_{\mathfrak{m}} = |a_2u_2\delta_2|_{\mathfrak{m}} \leq |\delta_2|_{\mathfrak{m}} \leq |\varepsilon_2|_{\mathfrak{m}}$;

et donc $|a - a_2|_{\mathfrak{m}} \leq \max(|a_1u_2\delta_2|_{\mathfrak{m}}, |a_2u_1\delta_1 - a_2|_{\mathfrak{m}}) \leq |\varepsilon_2|_{\mathfrak{m}}$.

■

Proposition 7

Un anneau A a la BAP si et seulement s'il est localement booléen et indépendant.

Preuve: L'implication (i)$\Longrightarrow$(ii) à été faite (c'est la proposition 3). Réciproquement, supposons que A soit localement booléen et indépendant. Alors A est de Prüfer, et en particulier intègre et intégralement clos. Montrons que A a la BAP.

Soient $\alpha_1, \alpha_2, \varepsilon_1, \varepsilon_2 \in A \setminus \{0\}$. On cherche δ_1, δ_2 comme dans le lemme 6. Quitte à remplacer ε_1 par $\varepsilon_1\alpha_1$, on suppose que $M(\alpha_1) \subseteq M(\varepsilon_1)$, et de même $M(\alpha_2) \subseteq M(\varepsilon_2)$.

Posons $\mathcal{M}_1 := M(\alpha_1) \setminus M(\alpha_2)$, $\mathcal{M}_2 := M(\alpha_1) \cap M(\alpha_2)$, et $W_i := \{A_{\mathfrak{m}} / \ \mathfrak{m} \in \mathcal{M}_i\}$, (i=1,2). A étant localement booléen, $\mathcal{M}_1$ et $\mathcal{M}_2$ quasi-compacts (car constructibles) d'après la proposition 1.1, et donc aussi W_1 et W_2 puisque A est de Prüfer.

(a) Soit $\mathfrak{n} \in \mathcal{M}_1^c$, fixé jusqu'au (b).
Pour chaque $\mathfrak{m} \in \mathcal{M}_1$, $A_{\mathfrak{m}}$ et $A_{\mathfrak{n}}$ sont indépendants, donc il existe $x_{\mathfrak{m}} \in K$ tel que :
- $|x_{\mathfrak{m}}|_{\mathfrak{m}} \leq |\varepsilon_1|_{\mathfrak{m}}$,
- $|x_{\mathfrak{m}} - 1|_{\mathfrak{n}} < 1$.

Soit $S_{\mathfrak{m},\mathfrak{n}} := A \setminus (\mathfrak{m} \cup \mathfrak{n})$.

Je dis que $S_{\mathfrak{m},\mathfrak{n}}^{-1}A = A_{\mathfrak{m}} \cap A_{\mathfrak{n}}$. En effet, tout idéal maximal $\mathfrak{M}$ de $S_{\mathfrak{m},\mathfrak{n}}^{-1}A$ est de la forme $S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{p}$, où $\mathfrak{p} = \mathfrak{M} \cap A$ ne rencontre pas $S_{\mathfrak{m},\mathfrak{n}}$. Donc $\mathfrak{p} \subseteq \mathfrak{m} \cup \mathfrak{n}$, et le lemme d'évitement des idéaux premiers entraîne que $\mathfrak{p} \subseteq \mathfrak{m}$ ou $\mathfrak{p} \subseteq \mathfrak{n}$, *i.e.* $\mathfrak{M} \subseteq S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{m}$ ou $\mathfrak{M} \subseteq S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{n}$, donc par maximalité $\mathfrak{M} = S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{m}$ ou $\mathfrak{M} = S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{n}$. Le spectre maximal de $S_{\mathfrak{m},\mathfrak{n}}^{-1}A$ est donc réduit à $\{S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{m}, S_{\mathfrak{m},\mathfrak{n}}^{-1}\mathfrak{n}\}$. Comme A est de Prüfer, $S_{\mathfrak{m},\mathfrak{n}}^{-1}A$ aussi, et on a donc $S_{\mathfrak{m},\mathfrak{n}}^{-1}A = \cap W_{S_{\mathfrak{m},\mathfrak{n}}^{-1}A} = A_{\mathfrak{m}} \cap A_{\mathfrak{n}}$.

Par construction, $x_{\mathfrak{m}} \in A_{\mathfrak{m}} \cap A_{\mathfrak{n}}$, donc $x_{\mathfrak{m}}$ s'écrit $a_{\mathfrak{m}}/b_{\mathfrak{m}}$, avec $a_{\mathfrak{m}} \in A$, et $b_{\mathfrak{m}} \in S_{\mathfrak{m},\mathfrak{n}}$. $|b_{\mathfrak{m}}|_{\mathfrak{m}} = |b_{\mathfrak{m}}|_{\mathfrak{n}} = 1$, donc il vient :
- $|a_{\mathfrak{m}}|_{\mathfrak{m}} = |b_{\mathfrak{m}}x_{\mathfrak{m}}|_{\mathfrak{m}} = |x_{\mathfrak{m}}|_{\mathfrak{m}} \leq |\varepsilon_1|_{\mathfrak{m}}$, donc $y_{\mathfrak{m}} := \varepsilon_1/a_{\mathfrak{m}} \notin m(A_{\mathfrak{m}})$, *i.e.* $A_{\mathfrak{m}} \in W_A(y_{\mathfrak{m}})^c$,
- $|a_{\mathfrak{m}}|_{\mathfrak{n}} = |b_{\mathfrak{m}}x_{\mathfrak{m}}|_{\mathfrak{n}} = |x_{\mathfrak{m}}|_{\mathfrak{n}} = 1$, donc $a_{\mathfrak{m}} \notin \mathfrak{n}$.

La famille $(W_A(y_{\mathfrak{m}})^c)_{\mathfrak{m} \in \mathcal{M}_1}$ constitue un recouvrement ouvert du quasi-compact W_1. On en extrait un sous-recouvrement fini $(W_A(y_i)^c)_{1 \leq i \leq p}$. Posons $c_{\mathfrak{n}} := \prod_{1 \leq i \leq p} a_i$, il vient :

- pour tout $\mathfrak{m} \in W_1$, il existe $i \in [\![1,p]\!]$ tel que $A_\mathfrak{m} \in W_A(y_i)^c$, donc $|a_i|_\mathfrak{m} \le |\varepsilon_1|_\mathfrak{m}$, et *a fortiori* $|c_\mathfrak{n}|_\mathfrak{m} \le |\varepsilon_1|_\mathfrak{m}$,
- $\forall i \in [\![1,p]\!],\ a_i \notin \mathfrak{n}$, et donc $c_\mathfrak{n} \notin \mathfrak{n}$.

(b) On procède ainsi pour chaque $\mathfrak{n} \in \mathcal{M}_1^c$, et on note I_1 l'idéal de A engendré par $\{c_\mathfrak{n} \,/\, \mathfrak{n} \in \mathcal{M}_1^c\}$. Il est clair que :

- tout élément d_1 de I_1 vérifie : $\forall \mathfrak{m} \in \mathcal{M}_1,\ |d_1|_\mathfrak{m} \le |\varepsilon_1|_\mathfrak{m}$;
- pour tout $\mathfrak{n} \in \mathcal{M}_1^c,\ I_1 \not\subseteq \mathfrak{n}$ car $c_\mathfrak{n} \in I_1$.

On fait de même avec $\mathcal{M}_2^c$, ça nous donne un idéal I_2 de A tel que :

- tout élément d_2 de I_2 vérifie : $\forall \mathfrak{m} \in \mathcal{M}_2,\ |d_2|_\mathfrak{m} \le |\varepsilon_2|_\mathfrak{m}$;
- $\forall \mathfrak{n} \in \mathcal{M}_2^c,\ I_2 \not\subseteq \mathfrak{n}$.

Alors, comme $\mathrm{Spm}(A) \subseteq \mathcal{M}_1^c \cup \mathcal{M}_2^c$, l'idéal $I_1 + I_2$ n'est inclus dans aucun idéal maximal de A, *i.e.* $I_1 + I_2 = A$. Donc il existe $\delta_1 \in I_1$ et $\delta_2 \in I_2$ tels que $\delta_1 + \delta_2 = 1$. Ce sont les deux éléments cherchés, et le lemme 6 donne la conclusion.

∎

Remarques:
(1) On voit sur sa démonstration que la proposition 7 clôt une chaîne d'implications circulaires, commençant à la proposition 3 et dont les deux lemmes intermédaires étaient les maillons. Il s'ensuit que les conditions suffisantes introduites dans ces lemmes étaient aussi des conditions nécessaires.
(2) Nous verrons plus loin comment la proposition 7 permet de montrer que la BAP se transmet par clôture intégrale dans une extension de corps.

Corollaire 8
Pour un anneau A, les propriétés suivantes sont équivalentes :
(i) *A a la BAP.*
(ii) *Pour tout $a \in A \setminus (A^* \cup \{0\})$, $S_a^{-1}A$ a la BAP.*

Preuve: Il est clair que (i) et (ii) entraînent chacun (par définition) que A est intègre.
(i)$\Longrightarrow$(ii) Quel que soit $a \in A \setminus (A^* \cup \{0\})$, (i) et le corollaire 2.4 assurent que $S_a^{-1}A$ est complémenté, et même booléen (on sait que la propriété de Prüfer est conservée par passage aux sur-anneaux). D'autre part la proposition 2.3 et (i) assurent que $W_{S_a^{-1}A} = W_A(a)$ est indépendante (car incluse dans W_A) donc d'après la proposition 7 $S_a^{-1}A$ a la BAP.
(ii)$\Longrightarrow$(i) Vu le corollaire 2.5, le (ii) entraîne que A est localement booléen. Quels que soient $\mathfrak{m} \neq \mathfrak{n} \in \mathrm{Spm}(A)$, un élément a de $\mathfrak{m} \cap \mathfrak{n} \setminus \{0\}$ nous donne que $A_\mathfrak{m}, A_\mathfrak{n} \in W_{S_a^{-1}A}$ donc sont indépendants, *i.e.* A lui-même est indépendant et donc satisfait la BAP.

∎

§ 4. Axiomatisation de la BAP et de la bonne factorisation

La formule suivante axiomatise la bonne factorisation :

$$\forall a \forall b,\ [b \neq 0 \to \exists a_1 \exists a_2,\ (a = a_1 a_2 \wedge \text{“}(b, a_2) = 1\text{”} \wedge a_1 \le b)]$$

où les sous-formules “$(b, a_2) = 1$” et “$a_1 \le b$,” dont la signification est claire, peuvent être considérées comme des abréviations des formules correspondantes du langage des anneaux. L'axiomatisation de la BAP est autrement plus délicate, mais par bonheur il s'avère que la bonne factorisation est en fait une sorte de version “locale” de la BAP, comme les anneaux booléens sont une version “locale” des anneaux localement booléens.

Proposition 1
Soit A un anneau de Prüfer. Sont équivalents :
(i) *A a bonne factorisation ;*
(ii) *A a la BAP et est de Bezout.*

Remarque: Il s'ensuit qu'un anneau de Prüfer noethérien (*i.e.* de Dedekind) a bonne factorisation si et seulement s'il est factoriel, puisqu'on sait qu'un anneau de Dedekind satisfait toujours la BAP, et qu'il est de Bezout si et seulement s'il est factoriel.

Preuve:
(i) $\Longrightarrow$ BAP.
Il est clair que BF entraîne la complémentation locale. A est donc localement booléen, et il suffit de vérifier que A est indépendant. Cela revient à montrer que :

$$\forall \mathfrak{p} \in \mathrm{Sp}(A),\ \forall \mathfrak{m}_1, \mathfrak{m}_2 \in \mathrm{Spm}(A), \quad \mathfrak{m}_1 \neq \mathfrak{m}_2 \text{ et } \mathfrak{p} \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2 \Longrightarrow \mathfrak{p} = (0).$$

Par l'absurde, supposons que non, et soit $a \in \mathfrak{p} \setminus \{0\}$ et $b \in \mathfrak{m}_1 \setminus \mathfrak{m}_2$. a et b sont différents de 0, donc la bonne factorisation s'applique. Elle donne $a_1, a_2 \in A$ tels que $a = a_1 a_2$, $M(a_1) = M(a) \cap M(b)$ et $M(a_2) = M(a) \setminus M(b)$. La relation radicale est celle définie par $\mathrm{Spm}(A)$, donc :

$$M(a_2) = M(a) \setminus M(b) \Longrightarrow \mathfrak{m}_1 \notin M(a_2) \Longrightarrow a_2 \notin \mathfrak{p},$$
$$M(a_1) = M(a) \cap M(b) \Longrightarrow \mathfrak{m}_2 \notin M(a_1) \Longrightarrow a_1 \notin \mathfrak{p}.$$

Or $a = a_1 a_2 \in \mathfrak{p}$, ce qui contredit l'hypothèse “$\mathfrak{p}$ premier”.

(i) $\Longrightarrow$ Bezout.
Soient $a, b \in A \setminus \{0\}$. Soit $W_0 := W_A(a) \cup W_A(b)$. La BAP donne c tel que :

$$\begin{cases} \forall R \in W_A\left(\dfrac{a}{b}\right) \cap W_0, & |c-b|_R \ \leq |ab|_R, \\ \forall R \in W_A\left(\dfrac{a}{b}\right)^c \cap W_0, & |c-a|_R \ \leq |ab|_R, \\ \forall R \in W_0^c, & |c|_R \ \leq 1. \end{cases}$$

On a donc $c \in \cap W_A$, *i.e.* $c \in A$ (car Prüfer $\Longrightarrow$ intégralement clos), et :

$$\forall \mathfrak{m} \in M(a) \cup M(b),\ \ |c|_\mathfrak{m} = \max(|a|_\mathfrak{m}, |b|_\mathfrak{m})$$

et en particulier $M(c) \cap M(ab) = M(a) \cap M(b)$. La bonne factorisation s'applique à c et ab : elle donne $d, e \in A$ tels que $c = de$, $M(d) = M(c) \cap M(ab)$, et $M(e) = M(c) \setminus M(ab)$. On a alors $M(d) = M(a) \cap M(b)$, et pour tout $\mathfrak{m} \in M(a) \cap M(b)$, $|d|_\mathfrak{m} = |c|_\mathfrak{m}$, d'où :

$$\forall \mathfrak{m} \in \mathrm{Spm}(A),\ \ |d|_\mathfrak{m} = \max(|a|_\mathfrak{m}, |b|_\mathfrak{m}).$$

Il s'ensuit que :
- pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, on a $|a|_\mathfrak{m} \leq |d|_\mathfrak{m}$, *i.e.* $a/d \in A_\mathfrak{m}$, donc $a/d \in \cap W_A = A$, *i.e.* d divise a dans A ;
- de même, d divise b dans A ;
- pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, on a $a' := a/d \in \mathfrak{m}$ si et seulement si $|a|_\mathfrak{m} < |b|_\mathfrak{m} < 1$, et $b' := b/d \in \mathfrak{m}$ si et seulement si $|b|_\mathfrak{m} < |a|_\mathfrak{m} < 1$, donc $M(a') \cap M(b') = \emptyset$.

On a donc $a'A + b'A = A$, d'où en multipliant par d, $aA + bA = dA$, et A est bien de Bezout.

(ii)$\Longrightarrow$(i)
Soient $a, b \in A \setminus \{0\}$. La BAP donne c tel que :

$$\begin{cases} \forall \mathfrak{m} \in M(a) \cap M(b), & |c-a|_{\mathfrak{m}} \le |a^2|_{\mathfrak{m}}, \\ \forall \mathfrak{m} \in ((M(a) \cap M(b))^c, & |c-1|_{\mathfrak{m}} \le |a|_{\mathfrak{m}} \end{cases}.$$

Soit d un pgcd de a et c. D'une part, pour tout $\mathfrak{m} \in M(a) \setminus M(b)$, on a $|c-1|_{\mathfrak{m}} \le |a|_{\mathfrak{m}} < 1$, d'où $|c|_{\mathfrak{m}} = 1$ et $c \notin \mathfrak{m}$, donc $d \notin \mathfrak{m}$. D'autre part, pour tout $\mathfrak{m} \in M(a) \cap M(b)$, on a $|c-a|_{\mathfrak{m}} \le |a^2|_{\mathfrak{m}} < |a|_{\mathfrak{m}}$, donc $|c|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$. Or $d \in aA + cA$, donc $|d|_{\mathfrak{m}} \le |a|_{\mathfrak{m}}$, et puisque d divise a on a $|d|_{\mathfrak{m}} \ge |a|_{\mathfrak{m}}$, d'où $|d|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$ et finalement $|a/d|_{\mathfrak{m}} = 1$, *i.e.* $a/d \notin \mathfrak{m}$. On voit donc que $a_1 := a/d$, et $a_2 := d$ fournissent la bonne factorisation cherchée.

■

Corollaire 2
(1) *Pour un anneau booléen, la bonne factorisation et la BAP coïncident, en particulier, tout anneau booléen indépendant est de Bezout.*
(2) *Un anneau A a la BAP si et seulement s'il est de Prüfer et si quel que soit $a \in A \setminus (A^* \cup \{0\})$, $S_a^{-1}A$ a bonne factorisation.*

Preuve:
(1) Un anneau booléen est de Prüfer, donc s'il a bonne factorisation il a aussi la BAP d'après la proposition 1.

Réciproquement, soit A un anneau booléen satisfaisant la BAP. Soient $a, b \in A \setminus \{0\}$, et $\alpha \in A \setminus \{0\}$ tel que $M(\alpha) = \mathrm{Spm}(A)$. La BAP nous donne $x \in A$ tel que :

$$\begin{cases} \forall \mathfrak{m} \in M(b)^c, & |x-a|_{\mathfrak{m}} \le |\alpha a|_{\mathfrak{m}}, \\ \forall \mathfrak{m} \in M(b), & |x-1|_{\mathfrak{m}} \le |\alpha|_{\mathfrak{m}}. \end{cases}$$

Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, si $\mathfrak{m} \in M(a) \setminus M(b)$ on a donc $|x|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$, et sinon $|x|_{\mathfrak{m}} = 1$. Il s'ensuit que $M(x) = M(a) \setminus M(b)$, que $a/x \in \cap W_A = A$, et que pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, si $\mathfrak{m} \in M(a) \setminus M(b)$ alors $|a/x|_{\mathfrak{m}} = 1$, et si $\mathfrak{m} \in M(a) \cap M(b)$ alors $|a/x|_{\mathfrak{m}} = |a|_{\mathfrak{m}}$. D'où, en posant $a_1 = x$ et $a_2 = a/x$ la bonne factorisation cherchée.

En particulier, un anneau booléen indépendant, puisqu'il a la BAP, a bonne factorisation d'après ce qui précède, et donc est de Bezout d'après la proposition 1.

(2) C'est la conséquence directe de la proposition 1 et du corollaire 3.8.

■

Corollaire 3
La classe des anneaux ayant la BAP élémentaire.

Preuve: C'est immédiat, d'après le corollaire 2, le fait que la bonne factorisation (et la propriété de Prüfer) soient élémentaires, et la propriété 2.6.

■

Remarque: On aurait pu déduire l'axiomatisabilité de la BAP directement du corollaire 3.8 du fait, démontré par Ershov, que la classe des anneaux booléens ayant la BAP est élémentaire (nous pouvions réutiliser son résultat pour les anneaux booléens, mais pas adapter sa démonstration au cas localement booléen car elle utilise de façon cruciale qu'un anneau booléen a un radical de Jacobson non nul). Cependant la relation simple existant entre la bonne factorisation et la BAP nous paraissait mériter d'être explicitement formulée, d'autant plus qu'elle nous donne le corollaire suivant :

Corollaire 4
Tout anneau qui satisfait le LGPH' a la BAP.

Preuve: Nous avons en effet démontré précédemment qu'un tel anneau était de Bezout, donc de Prüfer, et avait bonne factorisation (*cf.* la proposition I.3.5).
■

§ 5. Axiomatisation du LGPH et du LGPH'

Il sera commode au cours de ce paragraphe (et aussi parfois dans d'autres chapitres) de recourir à des abus de langages afin d'éviter de répéter certaines vérifications aussi élémentaires que fastidieuses : je veux parler des arguments de compacité.
Supposons que nous soient donnés :
- un anneau localement booléen A ;
- une partie quasi compacte $\mathcal{M}$ de $\mathrm{Spm}(A)$ telle que $\bigcap \mathcal{M} \neq 0$;
- pour chaque $\mathfrak{m} \in \mathcal{M}$ un élément $\alpha_{\mathfrak{m}} \in \mathfrak{m} \setminus \{0\}$.

Alors nous dirons systématiquement :

"on peut extraire de $(M(\alpha_{\mathfrak{m}}))_{\mathfrak{m}\in\mathcal{M}}$ une partition finie $(M(\alpha_i))_{1\leq i\leq n}$ de $\mathcal{M}$".

Nous entendrons par là la chose suivante : il existe par hypothèse un élément non nul $\alpha \in \bigcap \mathcal{M}$ donc pour tout $\mathfrak{m} \in \mathcal{M}$ la complémentation locale donne un élément $\beta_{\mathfrak{m}}$ de A tel que $M(\alpha) \cap M(\alpha_{\mathfrak{m}}) = M(\alpha) \cap M(\beta_{\mathfrak{m}})^c$ donc tel que $M(\alpha_{\mathfrak{m}}) \cap \mathcal{M} = M(\beta_{\mathfrak{m}})^c \cap \mathcal{M}$. Comme $\alpha_{\mathfrak{m}} \in \mathfrak{m}$ la famille $(M(\beta_{\mathfrak{m}})^c)_{\mathfrak{m}\in\mathcal{M}}$ constitue un recouvrement ouvert de $\mathcal{M}$, dont on peut extraire un recouvrement fini $(M(\beta_{\mathfrak{m}_i})^c)_{1\leq i\leq n}$ par quasi-compacité de $\mathcal{M}$.

La famille $(M(\alpha_{\mathfrak{m}_i}))_{1\leq i\leq n}$ recouvre donc $\mathcal{M}$; pour en déduire une partition on procède comme suit :
- quitte à remplacer $\alpha_{\mathfrak{m}_1}$ par α on peut supposer $\alpha_{\mathfrak{m}_1}$ non nul, on pose alors $\gamma_1 := \alpha_{\mathfrak{m}_1}$;
- si $\gamma_1, \ldots, \gamma_k$ on été déja construits, tous non nuls, tels que les $M(\gamma_i) \cap M(\alpha)$ soient deux à deux disjoints et que $\bigcup_{i=1}^k M(\alpha_{\mathfrak{m}_i}) \cap M(\alpha) \subseteq \bigcup_{i=1}^k M(\gamma_i) \cap M(\alpha)$, alors on prend $\gamma_{k+1} \in A \setminus \{0\}$ tel que :
$$M(\alpha) \cap M(\gamma_{k+1}) = M(\alpha) \cap \left[M(\alpha_{\mathfrak{m}_{k+1}}) \setminus \bigcup_{i=1}^{k} M(\gamma_i) \right].$$
Les $\mathcal{M} \cap M(\gamma_i)$ constituent un partition de $\mathcal{M}$. On peut en outre éliminer les éléments triviaux *i.e.* supposer les γ_k non inversibles (quitte à réduire n).

Pour économiser des lettres et des explications, nous poserons $\alpha_i := \gamma_i$ pour tout $i \in [\![1, n]\!]$, et étendrons ces notations à toute autre donnée indexée sur $\mathcal{M}$ qui nous aura été fournie au départ ; et c'est là que se situe l'abus de langage ! Imaginons par exemple que nous aient été donnés pour chaque $\mathfrak{m} \in \mathrm{Spm}(A)$ en même temps que $\alpha_{\mathfrak{m}}$:
- un élément $x_{\mathfrak{m}}$ de $A^h_{\mathfrak{m}}$;
- un $\varepsilon_{\mathfrak{m}} \in A \setminus \{0\}$;
- un élément $a_{\mathfrak{m}}$ de $\mathrm{Fr}(A)$;

tels que pour tout $\mathfrak{n} \in M(\alpha_{\mathfrak{m}}) \cap \mathcal{M}$, $x_{\mathfrak{m}}$ possède un conjugué $y_{\mathfrak{n},\mathfrak{m}}$ sur K qui appartienne à $A_{\mathfrak{n}}^h$ et vérifie $|a_{\mathfrak{m}} - y_{\mathfrak{n},\mathfrak{m}}|_{\mathfrak{n}} \leq |\varepsilon_{\mathfrak{m}}|_{\mathfrak{n}}$.

Alors il est clair que la façon dont nous avons choisi les α_i garantit que pour tout $i \in [\![1, n]\!]$ et pour tout $\mathfrak{n} \in M(\alpha_i) \cap \mathcal{M}$ il existe un K-conjugué $y_{\mathfrak{n},i}$ de x_i appartenant à $A_{\mathfrak{n}}^h$ tel que $|a_i - y_{\mathfrak{n},i}|_{\mathfrak{n}} \leq |\varepsilon_i|_{\mathfrak{n}}$ (ou toute autre relation additionnelle dépendant du contexte). Nous utiliserons cette propriété, mais pour éviter d'alourdir encore les démonstrations nous ne vérifierons pas à chaque fois qu'elle est bien satisfaite.

Proposition 1

Soit A un anneau de Prüfer, de corps des fractions K, $x \in K^n$ et $\sigma(u)$ une formule sans quanteur, à paramètres dans A, à n variables libres, dans le langage $\mathrm{L}_{\mathrm{rad}}$ (ou $\mathrm{L}_{\mathrm{div}}$). Alors l'ensemble des $\mathfrak{m} \in \mathrm{Spm}(A)$ tels que $x \in A_{\mathfrak{m}}$ et $A_{\mathfrak{m}} \models \sigma(x)$ est constructible.

Preuve: x est fixé dans K^n, et on démontre la proposition par récurrence sur les formules sans quanteur σ à n variables libres de $\mathrm{L}_{\mathrm{rad}}$ ou $\mathrm{L}_{\mathrm{div}}$, ou disons de $\mathrm{L}_{\mathrm{rad}} \cup \mathrm{L}_{\mathrm{div}}$.

Soit $\mathcal{M}_x := \{\mathfrak{m} \in \mathrm{Spm}(A) \,/\, x \in A_{\mathfrak{m}}\}$. L'ensemble W des anneaux de valuation de W_A contenant x est constructible : c'est $W_A(0)$ si $x = 0$, et $W_A(x^{-1})^c$ sinon. $\mathcal{M}_x$ est l'image de W par l'application $R \mapsto m(R) \cap A$; comme A est de Prüfer c'est donc une partie constructible de $\mathrm{Spm}(A)$ (*cf.* la propriété 1, "notations et conventions").

Notons $\mathcal{M}_x(\sigma) := \{\mathfrak{m} \in \mathcal{M} \,/\, A_{\mathfrak{m}} \models \sigma(x)\}$. Il est clair que $\mathcal{M}_x(\neg\sigma) = \mathcal{M}_x \setminus \mathcal{M}_x(\sigma)$ et que si τ est une autre formule sans quanteur à n variables, on a $\mathcal{M}_x(\sigma \vee \tau) = \mathcal{M}_x(\sigma) \cup \mathcal{M}_x(\tau)$. Les parties constructibles de $\mathrm{Spm}(A)$ étant stables par combinaisons booléennes, il suffit donc de montrer la proposition pour les formules atomiques. Il y a alors trois cas possibles (on note X un n-uplet d'indéterminées) :

– $\sigma(u) \equiv f(u) = 0$, avec $f \in A[X]$. Alors $\mathcal{M}_x(\sigma)$ égale $M(1)$ si $f(x) \neq 0$, et égale $M(0)$ sinon ;

– $\sigma(u) \equiv f(u)|g(u)$, avec $f, g \in A[X]$. Si $f(x) = 0$, $\mathcal{M}_x(\sigma) = \mathcal{M}_x(\tau)$, où $\tau \equiv g(u) = 0$ est du type précédent, donc $\mathcal{M}_x(\sigma)$ est constructible. Sinon, soit $y := g(x)/f(x)$; $\mathcal{M}_x(\sigma) = \mathcal{M}_y$ est une partie constructible de $\mathrm{Spm}(A)$.

– $\sigma(u) \equiv f(u) \leq g(u)$, avec $f, g \in A[X]$ $(X = (X_1, \ldots, X_n))$. Alors $\sigma(u) \equiv f(u)|1 \vee g(u) \not| 1$ et on est ramené au cas précédent.

■

Définition

Je dirais qu'une formule de $\mathrm{L}_{\mathrm{div}}$ (ou $\mathrm{L}_{\mathrm{rad}}$) $\varphi(x)$, à n variables libres, est **BAP-compatible** s'il existe une formule $\varphi^*(x)$ du langage des anneaux telle que tout anneau booléen indépendant A et tout $a \in A^n$ vérifient :

$$A \models \varphi^*(a) \iff \forall \mathfrak{m} \in \mathrm{Spm}(A) \;\; A_{\mathfrak{m}} \models \varphi(a).$$

Propriété 2

Si une formule $\varphi(x)$ de $\mathrm{L}_{\mathrm{div}}$ à n variables libres est BAP-compatible, alors il existe des formules $\varphi^o(x)$ et $\varphi^1(x, t)$ du langage des anneaux telles que pour tout anneau A ayant la BAP (i.e. localement booléen et indépendant), tout élément a de A^n et tout $\alpha \in A \setminus (A^* \cup \{0\})$ on ait :

(a) $A \models \varphi^o(a) \iff \forall \mathfrak{m} \in \mathrm{Spm}(A),\; A_{\mathfrak{m}} \models \varphi(a)$.

(b) $A \models \varphi^1(a, \alpha) \iff \forall \mathfrak{m} \in M(\alpha),\; A_{\mathfrak{m}} \models \varphi(a)$.

Preuve: Il suffit de montrer (b) et de poser $\varphi^o(x) \equiv \forall t,\; (t \neq 0 \wedge \forall t',\; t't \neq 1) \rightarrow \varphi^1(x, t)$ pour obtenir (a).

Soit $\varphi^*(x)$ la formule donnée par la BAP-compatibilité. La propriété 2.6, appliquée à $\varphi^*(x)$, nous donne une formule $\psi(x,t)$ telle que tout n-uplet a d'éléments d'un anneau A, localement booléen et indépendant, et tout $\alpha \in A \setminus (A^* \cup \{0\})$ vérifient :

$$A \models \psi(a,\alpha) \iff S_\alpha^{-1}A \models \varphi^*(a) \iff \forall R \in W_{S_\alpha^{-1}A},\ R \models \varphi(a). \tag{1}$$

Or d'après la proposition 2.3, $W_A(\alpha) = W_{S_\alpha^{-1}A}$, donc le dernier membre de (1) est équivalent à :

$$\forall \mathfrak{m} \in M(\alpha),\ A_\mathfrak{m} \models \varphi(a).$$

■

Lemme 3

Soit $\varphi(x,y)$ une formule BAP-compatible, à $m+n$ variables, et $\theta(x,y)$ une formule sans quanteur du langage des anneaux.
Alors la formule $\forall y(\theta(x,y) \to \varphi(x,y))$ est BAP-compatible.

Preuve: Par hypothèse, on a dans ce cas une formule $\varphi^*(x,y)$ telle que pour tout anneau booléen indépendant et tout $(a,b) \in A^{m+n}$ on ait :

$$A \models \varphi^*(a,b) \iff \forall \mathfrak{m} \in \mathrm{Spm}(A),\ A_\mathfrak{m} \models \varphi(a,b). \tag{1}$$

Soit A un anneau booléen indépendant et $a \in A^m$. Si tout $R \in W_A$ satisfait $\forall y(\theta(a,y) \to \varphi(a,y))$, alors pour tout $\alpha \in A \setminus (A^* \cup \{0\})$ et tout $b \in (S_\alpha^{-1}A)^n$, on a deux possibilités :

(a) $S_\alpha^{-1}A \models \neg\theta(a,b)$, et dans ce cas trivialement $S_\alpha^{-1}A \models \theta(a,b) \to \varphi^*(a,b)$.

(b) $S_\alpha^{-1}A \models \theta(a,b)$, et dans ce cas, comme θ est sans quanteur, tout $R \in W_{S_\alpha^{-1}A}$ satisfait aussi $\theta(a,b)$. Or $W_{S_\alpha^{-1}A} \subseteq W_A$, donc $R \models \theta(a,b) \to \varphi(a,b)$, d'où l'on déduit que $R \models \varphi(a,b)$. Ceci étant valable pour tout $R \in W_{S_\alpha^{-1}A}$, (1) appliqué à $S_\alpha^{-1}A$ entraîne que $S_\alpha^{-1}A \models \varphi^*(a,b)$, et en particulier $S_\alpha^{-1}A \models \theta(a,b) \to \varphi^*(a,b)$.

Dans les deux cas, $S_\alpha^{-1}A$ satisfait donc : $\forall y(\theta(a,y) \to \varphi^*(a,y))$.

Réciproquement, si pour tout $\alpha \in A \setminus (A^* \cup \{0\})$, le localisé $S_\alpha^{-1}A$ satisfait $\forall y(\theta(a,y) \to \varphi^*(a,y))$, montrons que tout $R \in W_A$ satisfait $\forall y(\theta(a,y) \to \varphi(a,y))$.
Soit $R \in W_A$ et $b \in R^n$, on a :

- b s'écrit b_0/u, pour un certain $u \in A \setminus (m(R) \cap A)$;
- $R \in W_A(\alpha_u) = W_{S_{\alpha_u}^{-1}A}$, pour un certain $\alpha_u \in A \setminus \{0\}$ tel que $M_A(\alpha_u) = M_A(u)^c$ (il en existe puisque A est booléen) ;
- $\alpha_u \neq 0$, et $u \notin m(R) \implies \alpha_u \in m(R) \cap A$, donc $\alpha_u \in A \setminus (A^* \cup \{0\})$ et $S_{\alpha_u}^{-1}A \models \forall y(\theta(a,y) \to \varphi(a,y))$;
- $u \in S_{\alpha_u}$ donc $b \in S_{\alpha_u}^{-1}A$, et $S_{\alpha_u}^{-1}A \models \theta(a,b) \to \varphi^*(a,b)$;
- comme θ est sans quanteur, $S_{\alpha_u}^{-1}A \models \theta(a,b)$ si et seulement si $R \models \theta(a,b)$.

Si $R \not\models \theta(a,b)$ alors trivialement $R \models \theta(a,b) \to \varphi(a,b)$. Sinon, $S_{\alpha_u}^{-1}A \models \theta(a,b)$, donc $S_{\alpha_u}^{-1}A \models \varphi^*(a,b)$, et tout $R' \in W_{S_{\alpha_u}^{-1}A}$ satisfait $\varphi(a,b)$. En particulier R satisfait $\varphi(a,b)$, et donc aussi $\theta(a,b) \to \varphi(a,b)$.

La propriété 2.6, appliquée à "$\forall y(\theta(x,y) \to \varphi^*(x,y))$," donne alors une formule $\psi(x,t)$ telle que tout anneau booléen indépendant, tout $a \in A^n$ et tout $\alpha \in A \setminus (A^* \cup \{0\})$ vérifient :

$$A \models \psi(a,\alpha) \iff S_\alpha^{-1}A \models \forall y \psi^*(a,y).$$

On a donc, pour tout anneau booléen A et tout $a \in A^m$:

$$\begin{aligned} A \models \forall\alpha(\alpha \neq 0 \wedge \forall\beta, (\alpha\beta \neq 1)) &\rightarrow \psi(a,\alpha) \\ &\iff \forall\alpha \in A \setminus (A^* \cup \{0\}), \quad S_\alpha^{-1}A \models \forall y(\theta(a,y) \rightarrow \varphi^*(a,y)) \\ &\iff \forall\alpha \in A \setminus (A^* \cup \{0\}), \ \forall\mathfrak{m} \in M_A(\alpha), \quad A_\mathfrak{m} \models \forall y(\theta(a,y) \rightarrow \varphi(a,y)), \\ &\iff \forall\mathfrak{m} \in \mathrm{Spm}(A), \quad A_\mathfrak{m} \models \forall y(\theta(a,y) \rightarrow \varphi(a,y)). \end{aligned}$$

C'est-à-dire que la formule $\forall y(\theta(x,y) \rightarrow \varphi(x,y))$ est BAP-compatible, comme annoncé.

■

Lemme 4

Soit $\psi(x,y,z) \equiv \bigvee\!\!\!\bigvee_{i\in I} \psi_i(x,y,z)$ une disjonction de formules à $m+n+p$ variables libres, du type suivant :

$$\psi_i(x,y,z) \equiv \bigwedge\!\!\!\bigwedge_{j\in J_i} f_{i,j} \neq 0 \bigwedge\!\!\!\bigwedge_{j\in K_i} 0 \neq p_{i,j}|q_{i,j} \bigwedge\!\!\!\bigwedge_{j\in K_i'} p'_{i,j} \nmid q'_{i,j}$$

où les $f_{i,j}, p_{i,j}, q_{i,j}, p'_{i,j}, q'_{i,j}$ sont des polynômes en x,y,z à coefficients dans $\mathbb{Z}$ (les variables sont sous-entendues dans ψ_i). Soit $\theta(x,y)$ une formule sans quanteur du langage des anneaux.
Alors la formule $\exists z\psi(x,y,z))$ est BAP-compatible.
Il s'ensuit que $\forall y(\theta(x,y) \rightarrow \exists z\psi(x,y,z))$ est elle aussi BAP-compatible.

Preuve: D'après le lemme 3, la seconde assertion découle immédiatement de la première. Il suffit donc de montrer que la formule $\varphi(x,y) \equiv \exists z\psi(x,y,z)$ est BAP-compatible.

Pour tout $i \in I$, posons $h_i := \prod_{j\in J_i} f_{i,j} \times \prod_{j\in K_i} p_{i,j} \times \prod_{j\in K_i'} q'_{i,j}$. Soit A un anneau booléen indépendant, et $(a,b) \in A^{m+n}$, tels que tout $R \in W_A$ vérifie $\exists z\psi(a,b,z)$. Soit $\mathfrak{m} \in \mathrm{Spm}(A)$; il existe $i_\mathfrak{m} \in I$, et $c_\mathfrak{m} \in A_\mathfrak{m}^p$ tels que $A_\mathfrak{m} \models \psi_{i_\mathfrak{m}}(a,b,c_\mathfrak{m})$. Notons qu'on a alors nécessairement $h_{i_\mathfrak{m}}(a,b,c_\mathfrak{m}) \neq 0$. D'après la proposition 1, l'ensemble des $\mathfrak{n} \in \mathrm{Spm}(A)$ tels que $c_\mathfrak{m} \in A_\mathfrak{n}^p$ et $A_\mathfrak{n} \models \psi(a,b,c_\mathfrak{m})$ est une partie constructible de $\mathrm{Spm}(A)$, donc (puisque A est booléen) de la forme $M(\alpha_\mathfrak{m})$, pour un certain $\alpha_\mathfrak{m} \in \mathfrak{m}\setminus\{0\}$.

La famille $(M(\alpha_\mathfrak{m}))_{\mathfrak{m}\in\mathrm{Spm}(A)}$ recouvre $\mathrm{Spm}(A)$, donc on peut en extraire une partition finie $(M(\alpha_k))_{1\leq k\leq q}$ de $\mathrm{Spm}(A)$. La BAP nous donne alors un point c de K^p vérifiant, pour tout $k \in [\![1,q]\!]$ et tout $\mathfrak{m} \in M(\alpha_k)$:

$$|c - c_k|_\mathfrak{m} \leq |\alpha_k h_{i_k}(a,b,c_k)|_\mathfrak{m}$$

En particulier $c \in A^p$.

Soit $k \in [\![1,q]\!]$; la formule de Taylor nous donne que pour tout $j \in J_k$ et tout $\mathfrak{m} \in M(\alpha_k)$ on a :

$$|f_{i_k,j}(a,b,c) - f_{i_k,j}(a,b,c_k)|_\mathfrak{m} \leq |c - c_k|_\mathfrak{m} < |f_{i_k,j}(a,b,c_k)|_\mathfrak{m}$$

donc $|f_{i_k,j}(a,b,c)|_\mathfrak{m} = |f_{i_k,j}(a,b,c_k)|_\mathfrak{m}$, et en particulier $f_{i_k,j}(a,b,c) \neq 0$.

De même, pour tout $j \in K_k$ et tout $\mathfrak{m} \in M(\alpha_k)$ on a $|p_{i_k,j}(a,b,c)|_\mathfrak{m} = |p_{i_k,j}(a,b,c_k)|_\mathfrak{m}$, donc $p_{i_k,j}(a,b,c) \neq 0$, et :

$$\begin{aligned} |q_{i_k,j}(a,b,c)|_\mathfrak{m} &\leq \max(|q_{i_k,j}(a,b,c) - q_{i_k,j}(a,b,c_k)|_\mathfrak{m}, |q_{i_k,j}(a,b,c_k)|_\mathfrak{m}) \\ &\leq \max(|c - c_k|_\mathfrak{m}, |q_{i_k,j}(a,b,c_k)|_\mathfrak{m}) \\ &\leq \max(|p_{i_k,j}(a,b,c_k)|_\mathfrak{m}, |q_{i_k,j}(a,b,c_k)|_\mathfrak{m}) \\ &\leq |p_{i_k,j}(a,b,c_k)|_\mathfrak{m} = |p_{i_k,j}(a,b,c)|_\mathfrak{m}, \end{aligned}$$

et donc $0 \neq p_{i_k,j}(a,b,c)|_{\mathfrak{m}} q_{i_k,j}(a,b,c)$.

Enfin pour tout $j \in K'_k$, on a de même $|q'_{i_k,j}(a,b,c)|_{\mathfrak{m}} = |q'_{i_k,j}(a,b,c_k)|_{\mathfrak{m}}$. Mais alors $|p'_{i_k,j}(a,b,c_k)|_{\mathfrak{m}} < |q'_{i_k,j}(a,b,c)|_{\mathfrak{m}}$, d'où :

$$\begin{aligned}|p'_{i_k,j}(a,b,c)|_{\mathfrak{m}} &\leq \max(|p'_{i_k,j}(a,b,c) - p'_{i_k,j}(a,b,c_k)|_{\mathfrak{m}}, |p'_{i_k,j}(a,b,c_k)|_{\mathfrak{m}})\\ &\leq \max(|c - c_k|_{\mathfrak{m}}, |p'_{i_k,j}(a,b,c_k)|_{\mathfrak{m}})\\ &< |q'_{i_k,j}(a,b,c)|_{\mathfrak{m}},\end{aligned}$$

et donc $p'_{i_k,j}(a,b,c) \not|_{\mathfrak{m}} q'_{i_k,j}(a,b,c)$.

Pour chaque $i \in I$, posons $\beta_i := \prod\{\alpha_k \ / \ k \in [\![1,q]\!] \text{ et } i_k = i\}$. D'après ce qui précède, pour tout $\mathfrak{m} \in M(\beta_i)$, le localisé $A_{\mathfrak{m}}$ satisfait $\psi_i(a,b,c)$. On en déduit, quel que soit $\mathfrak{m} \in M(\beta_i)$:

(a) Pour tout $j \in K_i \quad q_{i,j}(a,b,c)/p_{i,j}(a,b,c) \in A_{\mathfrak{m}}$. D'après le corollaire 4.2, A est de Bezout, donc on peut trouver $v_{i,j} \in A$ et $u_{i,j} \in A \setminus \{0\}$, étrangers, tels que $v_{i,j}/u_{i,j} = q_{i,j}(a,b,c)/p_{i,j}(a,b,c)$. On a donc $u_{i,j} \notin \cup M(\beta_i)$, i.e. $u_{i,j}$ est étranger à β_i.

(b) Pour tout $j \in K'_i$, $p'_{i,j}(a,b,c)/q'_{i,j}(a,b,c) \in m(A_{\mathfrak{m}})$, donc on peut mettre ce quotient sous la forme $u'_{i,j}/v'_{i,j}$, avec $v'_{i,j} \in A \setminus \cup M(\beta_i)$, *i.e.* $v'_{i,j}$ étranger à β_i, et $u'_{i,j} \in \cap M(\alpha_i)$, *i.e.* $\beta_i \leq u'_{i,j}$.

A satisfait donc la formule suivante :

$$\begin{aligned}&\exists c \exists (\beta_i)_{i\in I},\ Part(\beta_i)_{i\in I} \ \bigwedge_{i\in I} \Big[\bigwedge_{j\in J_i} f_{i,j}(a,b,c) \neq 0\\ &\bigwedge_{j\in K_i} \exists u_{i,j} \exists v_{i,j} \ (Prem(u_{i,j},\alpha_i) \wedge u_{i,j} \neq 0 \wedge u_{i,j} q_{i,j}(a,b,c) = v_{i,j} p_{i,j}(a,b,c))\\ &\bigwedge_{j\in K'_i} \exists u'_{i,j} \exists v'_{i,j} \ (Prem(v'_{i,j},\alpha_i) \wedge v'_{i,j} \neq 0 \wedge \beta_i \leq u'_{i,j}\\ &\qquad\qquad\qquad\qquad \wedge u'_{i,j} q'_{i,j}(a,b,c) = v'_{i,j} p'_{i,j}(a,b,c)) \Big]\end{aligned}$$

où $Prem(x,y)$ est la formule "$\exists u \exists v (ux + vy = 1)$" qui énonce que deux éléments sont étrangers, et "$Part(x_i)_{i\in I}$" est la formule "$\bigwedge_{i\neq j\in I}(x_i,x_j) = 1 \wedge 0 \leq \prod_{i\in I} x_i$" qui caractérise les partitions constructibles. Cette formule est de $\mathrm{L}_{\mathrm{rad}}$ et non pas du langage des anneaux, mais comme nous avons vu que, la relation radicale définie par le spectre maximal étant définissable, on peut la remplacer par une formule équivalente du langage des anneaux.

Réciproquement, si on note $\varphi^*(x,y)$ la formule ci-dessus, il est facile de vérifier (comme nous en laissons la joie au lecteur) que pour tout anneau booléen indépendant A et tout $(a,b) \in A^{m+n}$ satisfaisant $\varphi^*(a,b)$, tout $\mathfrak{m} \in \mathrm{Spm}(A)$ satisfait $\exists z \psi(a,b,z)$. La formule $\exists z \psi(x,y,z)$ est donc bien BAP-compatible.

■

Proposition 5

La classe des anneaux ayant la BAP et denses dans chacun de leurs henselisés, est élémentaire (dans le langage des anneaux).

Preuve: Un anneau de valuation R est dense dans son hensélisé si et seulement si pour tout polynôme $f \in R[X]$, s'il existe un élément a de R tel que $f(a) \in m(R)$ et $f'(a) \notin m(R)$, alors pour tout $\varepsilon \in R \setminus \{0\}$ il existe $b \in R$ tel que $|f(b)|_R \leq |\varepsilon|_R$. Autrement dit, la classe des anneaux de valuation denses dans leurs hensélisés est axiomatisée par les formules suivantes, pour tout $d \in \mathbb{N}^*$:

$$DH_d \equiv \forall c_0, \ldots, c_d \forall a \forall \varepsilon, \ \Big(\varepsilon \neq 0 \rightarrow \exists b, \ f(a)|1 \vee f'(a) \not| 1 \vee \varepsilon | f(b)\Big)$$

avec $f = \sum c_i X^i$. On voit que DH_d est BAP-compatible, d'après le lemme 4, donc un anneau localement booléen et indépendant A est dense dans ses hensélisés (c'est-à-dire dans les hensélisés de ses localisés) si et seulement si tout $R \in W_A$ satisfait pour tout $d \in \mathbb{N}^*$, DH_d (car on sait déja, par la BAP, que A est dense dans R) si et seulement si A satisfait DH_d^o, pour tout $d \in \mathbb{N}^*$ (DH_d^o nous est donnée par la propriété 2).

■

Proposition 6
Le LGPH et le LGPH' sont récursivement axiomatisables dans le langage des anneaux.

Preuve: Nous avons vu qu'un anneau satisfaisant le LGPH' était dense dans ses hensélisés et satisfaisait la BAP. Cette propriété (notons-la BAPH) étant élémentaire, il nous suffit d'axiomatiser le LGPH et le LGPH' modulo BAPH. En outre un anneau ayant la BAP est localement booléen, donc satisfait LGPH1, donc nous pouvons nous concentrer sur la condition géométrique de ces LGP.

L'élimination des quantificateurs dans les corps algébriquement clos donne une formule $Var_{m,n,e,d}(x)$ du langage des anneaux telle que si A est un anneau intègre quelconque, et c la liste (de taille $N = N(m,n,e)$) des coefficients d'un système $f = (f_1, \ldots, f_m)$ de m polynômes en n indéterminées, de degré au plus e, à coefficients dans A, alors $A \models Var_{m,n,e,d}(c)$ si et seulement si f est absolument réduit, absolument irréductible, et la variété associée est de dimension d. L'ensemble des déterminants de taille $n-d$ extraits du Jacobien de f, qui permettent de caractériser les points lisses de V, peut être décrit indépendamment des valeurs des coefficients de f, en fonction des entiers m, n, e et d, je le note $\mathcal{J}$. Le problème est d'exprimer au premier ordre que V a un point lisse dans R^h pour tout $R \in W_A$. Pour cela on considère la formule suivante :

$$ZH_{m,n,e,d}(x,t) \equiv \forall \varepsilon, \ (\varepsilon \neq 0 \rightarrow \exists y, \ \bigvee_{J \in \mathcal{J}} \bigwedge_{1 \leq i \leq N} \varepsilon | f_i(y) \wedge 0 \neq J(y)|t).$$

C'est une formule BAP-compatible, d'après le lemme 4, donc on peut trouver une formule $ZH^1_{m,n,e,d}(x,t,u)$ telle que tout anneau A indépendant et localement booléen, tout $c \in A^N$, tout $\mu \in A$ et tout $\alpha \in A \setminus (A^* \cup \{0\})$ vérifient :

$$A \models ZH^1_{m,n,e,d}(c,\mu,\alpha) \quad \Longleftrightarrow \quad \forall \mathfrak{m} \in M(\alpha), \ A_\mathfrak{m} \models ZH_{m,n,e,d}(c,\mu). \tag{1}$$

Soit A un anneau intégralement clos, ayant la BAP, et dense dans ses hensélisés. Soit $c \subseteq A$ tel que $A \models Var_{m,n,e,d}(c)$, soit f le système absolument réduit et absolument irréductible correspondant, et V la variété associée.

(a) Montrons que si V possède un point lisse dans R^h pour tout $R \in W_A$, alors quel que soit $\alpha \in A \setminus (A^* \cup \{0\})$ il existe $\mu \in A \setminus \{0\}$ tel que $A \models ZH^1_{m,n,e,d}(c,\mu,\alpha)$.

Si A est un corps, $A \setminus (A^* \cup \{0\})$ est vide, et il n'y rien à montrer. On suppose donc que A n'est pas un corps, et soit $\alpha \in A \setminus (A^* \cup \{0\})$. Pour tout $\mathfrak{m} \in M(\alpha)$, $V^\circ(A^h_\mathfrak{m}) \neq \emptyset$, donc il existe $x_\mathfrak{m} \in (A^h_\mathfrak{m})^n$ et $J_\mathfrak{m} \in \mathcal{J}$ tel que $f(x_\mathfrak{m}) = 0$ et $J_\mathfrak{m}(x_\mathfrak{m}) \neq 0$. Soit J un élément fixé de $\{J_\mathfrak{m} \mathbin{/} \mathfrak{m} \in M(\alpha)\}$ (il en existe puisque $\alpha \notin A^* \Longrightarrow M(\alpha) \neq \emptyset$). $J \notin I(V)$, donc quitte à appliquer le théorème des fonctions implicites (*cf.* le lemme 8 des prérequis) en chaque $x_\mathfrak{m}$ on peut supposer $J(x_\mathfrak{m}) \neq 0$ pour tout $\mathfrak{m} \in M(\alpha)$. Il s'agit de trouver une sorte de minorant commun à tous les $J(x_\mathfrak{m})$. Pour cela, on commence par se ramener à un nombre fini de points locaux.

Quel que soit $\mathfrak{m} \in M(\alpha)$, le lemme d'accessibilité (*i.e.* le lemme I.4.2) nous donne un $\alpha_\mathfrak{m} \in \mathfrak{m} \setminus \{0\}$ tel que pour tout $\mathfrak{n} \in M(\alpha_\mathfrak{m}) \cap M(\alpha)$, $A^h_\mathfrak{n}$ contienne un K-conjugué $x_{\mathfrak{m},\mathfrak{n}}$ de $x_\mathfrak{m}$. Quand $\mathfrak{m}$ décrit $M(\alpha)$, les $M(\alpha_\mathfrak{m})$ recouvrent $M(\alpha)$; on en déduit une partition finie $(M(\alpha_i) \cap M(\alpha))_{1\leq i\leq p}$ de $M(\alpha)$, telle que pour tout $i \in [\![1,p]\!]$, tout $\mathfrak{m} \in M(\alpha_i) \cap M(\alpha)$ contienne un K-conjugué $y_\mathfrak{m}$ de x_i.

Soit $i \in [\![1,p]\!]$; quitte à remplacer chaque $A^h_\mathfrak{m}$, pour $\mathfrak{m}$ décrivant $M(\alpha_i)$, par une de ses copies K-isomorphes, on peut supposer que $x_i \subseteq A^h_\mathfrak{m}$. On peut écrire $J(x_i)$ sous la forme μ_i/ν_i, avec μ_i, ν_i entiers sur A, et quitte à multiplier numérateur et dénominateur par les conjugués de μ_i, on peut supposer que $\mu_i \in A$. Comme $J(x_i) \neq 0$, on a $\mu_i \neq 0$.

Soit $\mu := \prod_{i=1}^p \mu_i$; c'est un élément non nul de A, et pour tout $i \in [\![1,p]\!]$ et tout $\mathfrak{m} \in M(\alpha) \cap M(\alpha_i)$ on a :

$$|\mu|_\mathfrak{m} \leq |\mu_i|_\mathfrak{m} \leq |J(x_i)|_\mathfrak{m}.$$

Quels que soient $i \in [\![1,p]\!]$ et $\mathfrak{m} \in M(\alpha) \cap M(\alpha_i)$, la densité de $A_\mathfrak{m}$ dans son hensélisé et la continuité des fonctions polynomiales nous donne alors, pour tout $\varepsilon_\mathfrak{m} \in A_\mathfrak{m} \setminus \{0\}$, un point $a_\mathfrak{m}$ de $A_\mathfrak{m}$ tel que $|f(a_\mathfrak{m})|_\mathfrak{m} \leq |\varepsilon_\mathfrak{m}|_\mathfrak{m}$ et $|\mu|_\mathfrak{m} \leq |J(a_\mathfrak{m})|_\mathfrak{m}$, c'est-à-dire que $A_\mathfrak{m} \models ZH_{m,n,e,d}(c,\mu)$. D'après (1), on a donc bien $A \models ZH^1_{m,n,e,d}(c,\mu,\alpha)$.

(b) Réciproquement, montrons que si A n'est pas un corps, et si pour tout $\alpha \in A \setminus (A^* \cup \{0\})$ il existe $\mu \in A \setminus \{0\}$ tel que $A \models ZH^1_{m,n,e,d}(c,\mu,\alpha)$, alors quel que soit $R \in W_A$, $V^o(R^h) \neq \emptyset$.

Soit $R \in W_A$, et α un élément non nul de $m(R) \cap A$ (il en existe puisque A, et donc R, n'est pas un corps). Par hypothèse on a un élément μ de $A \setminus \{0\}$ tel que $A \models ZH^1_{m,n,e,d}(c,\mu,\alpha)$, donc d'après (1) $R \models ZH_{m,n,e,d}(c,\mu)$, ie :

$$\forall \varepsilon \in R \setminus \{0\},\ \exists a_\varepsilon \in R^n,\ \exists J_\varepsilon \in \mathcal{J},\quad |f(a_\varepsilon)|_\mathfrak{m} \leq |\varepsilon|_\mathfrak{m} \text{ et } |\mu|_\mathfrak{m} \leq |J_\varepsilon(a_\varepsilon)|_\mathfrak{m}. \qquad (2)$$

L'ensemble $\mathcal{J}$ étant fini, il existe un élément J de $\mathcal{J}$, indépendant de ε, tel que (2) soit vérifié avec J à la place de J_ε. Le lemme I.5.3, appliqué à $B := (R^h)^n$ entraîne alors que $V^o(R^h) \neq \emptyset$.

On voit donc que si A n'est pas un corps les assertions suivantes sont équivalentes :
(i) $\forall R \in W_A,\ V^o(R^h) \neq \emptyset$;
(ii) $A \models \forall u \exists t,\ (u \neq 0 \to ZH^1_{m,n,e,d}(c,t,u))$.

Il s'ensuit que le LGPH est axiomatisé par la famille de formules suivante, pour toutes les valeurs de m,n,e,d :

$$NC \to \forall c,\ \Big[\Big(Var_{m,n,e,d}(c) \wedge \forall u \exists t (u \neq 0 \to ZH^1_{m,n,e,d}(c,t,u))\Big) \to \exists y,\ f(y) = 0\Big]$$

où $NC \equiv \exists a \forall a',\ a \neq 0 \wedge a'a \neq 1$ est la formule disant que l'anneau n'est pas un corps. Le LGPH' s'axiomatise de même, en rajoutant aux hypothèses la formule disant que $V^\circ(\mathrm{Fr}(A)) \neq \emptyset$ (ce qui s'écrit dans A grâce à une simple réduction de dénominateur).

∎

Chapitre III
LGPH et approximation

Résumé : On trouvera ici la preuve que le LGPH est conservé par clôture intégrale, et qu'il possède une propriété de clôture existentielle non seulement dans le langage des anneaux (comme nous le savons déja grâce à la clôture régulière) mais aussi dans le langage des r-anneaux. Ce dernier résultat marque le tournant entre l'étude générale du LGPH que nous avons menée jusqu'ici et les applications auxquelles nous consacrerons les chapitres suivants. En attendant, il nous permet de retrouver le LGP introduit par Prestel et Schmid dans [P-S 90] et [P-S 91] comme un cas particulier du LGPH'.
(Ces résultats ont pour point commun d'être tous basés sur l'une ou l'autre des propriétés d'approximation que nous avons déduites du LGPH, d'où notre titre.)

§ 1. Points constructibles

On peut donner de la BAP une interprétation en termes de densité. Fixons une famille W d'anneaux de valuation sur un corps K.

Définition
Un point ***W*-constructible** est un point x de K^W tel qu'il existe une partition constructible $(W_1, \ldots, W_p)$ de W et des points $(x_1, \ldots, x_p)$ de K tels que

$$\forall i \in [\![1, p]\!],\ \forall R \in W_i, \quad x(R) = x_i.$$

On notera $\boldsymbol{\mathcal{C}(W)}$ l'ensemble des points W-constructibles, et si W est de la forme W_A pour un certain anneau A on notera simplement $\boldsymbol{\mathcal{C}(A)}$ au lieu de $\mathcal{C}(W_A)$. Par extension, un n-uplet sera dit constructible si ses coordonnées le sont.

$\mathcal{C}(W)$ est un sous-anneau de K^W. On peut le munir d'une topologie, en posant :

$$\forall x, y \in \mathcal{C}(W), \quad |x|_W \leq |y|_W \iff \forall R \in W,\ |x(R)|_R \leq |y(R)|_R$$

et en prenant comme voisinages d'un point x de $\mathcal{C}(W)$ les parties X de $\mathcal{C}(W)$ pour lesquelles il existe $\varepsilon \in K^*$ tel que $\{y \in \mathcal{C}(W) \ /\ |x - y|_W \leq |\varepsilon|_W\} \subseteq X$. Le plongement diagonal fait de K un sous-anneau de $\mathcal{C}(W)$ et il est clair alors que :

$$W \text{ a la BAP} \iff \text{K est dense dans } \mathcal{C}(W).$$

N.B. Soit x un point constructible d'une variété V définie sur K. Avec la définition générale de la lissité que nous avons donnée au départ, x serait lisse si et seulement si on avait $\Delta(x) \neq 0$, pour un certain déterminant Δ extrait d'un Jacobien de V, donc si et seulement si l'un des $x(R)$ $(R \in W)$ était un point lisse de V. Il est clair qu'une telle notion de lissité risque d'être trop faible pour qu'on puisse en faire quelque chose, c'est pourquoi nous en changeons la définition pour le cas particulier des points constructibles :

Définition
Un point constructible x d'une variété V définie sur K sera dit **lisse** si et seulement si $x(R)$ est lisse quel que soit $R \in W$.
On notera encore $V^\circ(\mathcal{C}(W))$ l'ensemble des points lisses de V dans $\mathcal{C}(W)$.

Proposition 1 (densité dans les constructibles)
Soit A un anneau intègre, K son corps des fractions, et V une variété définie sur K. Si A satisfait le LGPH' (et a fortiori *le LGPH), alors $V^\circ(K)$ est dense dans $V^\circ(\mathcal{C}(A))$.*

Preuve: K est plongé dans $\mathcal{C}(A)$ par le plongement diagonal, donc si $V^\circ(\mathcal{C}(A)) = \emptyset$, on a aussi $V^\circ(K) = \emptyset$, et il n'y a rien à montrer. On peut donc supposer $V^\circ(\mathcal{C}(A)) \neq \emptyset$.

Soit $x \in V^\circ(\mathcal{C}(A))$, et $W_1, \ldots, W_p$ une partition constructible de W_A telle que la fonction $R \mapsto x(R)$ soit constante sur chaque W_i. Pour chaque $i \in [\![1,p]\!]$, soit $x_i := x(R)$, pour un R quelconque dans W_i, soit $u_i \in A \setminus \{0\}$ un dénominateur commun des coordonnées de x_i, soit u leur produit, et $y := ux$. Pour tout $R \in W_A$ on a donc $y(R) \in A$.

Soit $f \in K[T_1, \ldots, T_n]^r$ un système absolument réduit d'équations de V et $\varepsilon \in A\setminus\{0\}$. A satisfait la BAP, *i.e.* K est dense dans $\mathcal{C}(A)$, donc on peut trouver $y_0 \in K^n$ tel que $|y - y_0|_W \leq |u\varepsilon|_W$. Soit V' la variété définie sur K par :

$$\begin{cases} f(X/u) = 0 \\ X - y_0 = u\varepsilon Z \end{cases}$$

où Z est un n-uplet de nouvelles indéterminées.

Pour tout $R \in W_A$, on a $y(R) \in A^n \subseteq R^n$, et $|y(R)-y_0)|_R \leq |u\varepsilon|_R$, donc clairement : $(y(R), (y(R) - y_0)/u\varepsilon) \in V'^\circ(A)$. Le LGPH' donne alors $(a, (a - y_0)/u\varepsilon) \in V'^\circ(A)$ d'où $b := a/u \in V^\circ(K)$ et :

$$|b - x|_W \leq \max\left(\left|b - \frac{y_0}{u}\right|_W, \left|x - \frac{y_0}{u}\right|_W\right) \leq \max\left(\left|\frac{a - y_0}{u}\right|_W, \left|\frac{y - y_0}{u}\right|_W\right) \leq |\varepsilon|_W$$

■

L'essentiel de ce chapitre est consacré aux conséquences de cette propriété, éventuellement sous la forme plus précise suivante, conjuguée à la proposition I.4.3 de densité locale.

Corollaire 2
Soient V une variété définie sur K, h un polynôme à coefficients dans A, α un élément non nul de A et $\overline{x} \in V^\circ(\mathcal{C}(A))$ tels que :

$$\forall \mathfrak{m} \in \mathrm{Spm}(A), \quad \overline{x}(A_\mathfrak{m}) \in A_\mathfrak{m} \quad \textit{et} \quad h(\overline{x}(A_\mathfrak{m})) \leq_{A_\mathfrak{m}} \alpha.$$

Si A satisfait le LGPH' alors pour tout $\varepsilon \in A \setminus \{0\}$ on peut trouver $a \in V^\circ(A)$ tel que $h(a) \leq_A \alpha$ et $|a - \overline{x}|_{W_A} \leq |\varepsilon|_{W_A}$.

Preuve: Soit $\varepsilon \in A \setminus \{0\}$; soit $f := (f_1, \ldots, f_m) \in A[X_1, \ldots, X_n]^m$ un système absolument réduit d'équations de V, et I_V l'idéal engendré par f dans $K[X_1, \ldots, X_n]$. Si h appartient I_V les hypothèses entraînent que $M(\alpha) = \mathrm{Spm}(A)$, et le corollaire 2 se réduit à la densité dans les constructibles. On peut donc écarter ce cas et supposer

$h \notin I_V$.

La proposition 1 nous donne un point $b = (b_1, \dots, b_n) \in V^\circ(A)$ tel que $|b - \overline{x}|_{W_A} \leq |\varepsilon|_{W_A}$ et $h(b) \neq 0$. La bonne factorisation permet de trouver $\delta, \eta \in A \setminus \{0\}$ tels que $h(b) = \delta\eta$, $M(\delta) = M(h(b)) \cap M(\alpha)$ et $M(\eta) = M(h(b)) \setminus M(\alpha)$.

Soit W la variété définie sur K par :

$$\begin{cases} (1) \quad f(X) = 0 \\ (2) \quad (b - X) = \varepsilon Y \\ (3) \quad h(X)Z = \delta \end{cases}$$

avec $Y = (Y_1, \dots, Y_n)$ où Z et les Y_i sont de nouvelles indéterminées. Un point (x, y, z) de W vérifie $h(x) \neq 0$, et il est lisse si et seulement si x est un point lisse de V. Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ on a :

- si $\alpha \in \mathfrak{m}$ alors $\eta = h(b)/\delta \notin \mathfrak{m}$ donc $(b, 0, \eta^{-1}) \in W^\circ(A_\mathfrak{m})$;
- sinon, $x_\mathfrak{m} := \overline{x}(A_\mathfrak{m}) \in A_\mathfrak{m}^n$, et $y_\mathfrak{m} := (b - x_\mathfrak{m})/\varepsilon \in A_\mathfrak{m}^n$ car $|b - x_\mathfrak{m}|_\mathfrak{m} \leq |\varepsilon|_\mathfrak{m}$, et par hypothèse $h(x_\mathfrak{m}) \notin m(A_\mathfrak{m})$ donc $z_\mathfrak{m} := \delta/h(\overline{x}(A_\mathfrak{m})) \in A_\mathfrak{m}$, d'où $(x_\mathfrak{m}, y_\mathfrak{m}, z_\mathfrak{m}) \in W^\circ(A_\mathfrak{m})$.

Le LGPH' donne donc un point $(x, y, z) \in W^\circ(A)$. La relation (1) entraîne que $x \in V^\circ(A)$, et la (3) que $M(h(x)) \subseteq M(\delta) \subseteq M(\alpha)$. D'autre part, pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ on a :

$$|x - \overline{x}(A_\mathfrak{m})|_\mathfrak{m} \leq \max(|x - b|_\mathfrak{m}, |b - \overline{x}(A_\mathfrak{m})|_\mathfrak{m}) = \max(|y|_\mathfrak{m}, |y_\mathfrak{m}|_\mathfrak{m}) \leq |\varepsilon|_\mathfrak{m}$$

d'où $|x - \overline{x}|_{W_A} \leq |\varepsilon|_{W_A}$.

■

Remarque: Il est assez facile de définir de manière analogue une notion de **point adélique**, qui se réduit à la notion usuelle pour un corps de nombre. En combinant le théorème densité dans les constructibles et celui de densité locale (II.5), on obtient alors un sympatique théorème d'approximation des points adéliques.

Dans la pratique, les deux énoncés de densité que nous avons démontrés se sont avérés plus simples à utiliser que cette propriété d'approximation ; simplement parce qu'il est plus facile de remplacer d'abord des points locaux par des points dans le corps, puis ceux-ci par un point constructible, que de construire directement un point adélique à partir de points locaux. Nous épargnerons donc au lecteur une telle digression.

§ 2. Passage à la clôture intégrale

Notre première application des propriétés de densité que nous avons introduites, sera de démontrer que si un anneau A satisfait le LGPH ou le LGPH', alors sa clôture intégrale dans n'importe quelle extension de son corps des fractions le satisfait aussi.

On commence par évacuer le problème de la condition non géométrique ($M(a)^c$ quasi-compact) à l'aide de la proposition suivante :

Proposition 1

Soit A un anneau localement booléen, K son corps des fractions, L une extension algébrique de K, et B la clôture intégrale de A dans L. Alors B est localement booléen.

Remarque: Il s'ensuit immédiatement, vu la proposition II.3.7 que la BAP est elle aussi conservée par passage à la clôture intégrale dans une extension.

Preuve: On sait que la propriété de Prüfer est conservée par passage à la clôture intégrale, donc B est de Prüfer et il suffit de montrer qu'il est localement complémenté. Nous allons pour cela utiliser le critère donné par le corollaire II.2.4. Soit b un élément non nul et non inversible de B ; b étant entier sur A, sa norme sur K est un élément a de A, lui aussi non nul et non inversible. Pour alléger un peu l'écriture, posons :

- $S := A \setminus \bigcup M_A(a)$;
- $T := B \setminus \bigcup M_B(a)$;
- $U := B \setminus \bigcup M_B(b)$;
- $A' := S^{-1}A$;
- $B' := T^{-1}B$;
- $T' := B' \setminus \bigcup M_{B'}(b)$.

Il nous faut montrer que $U^{-1}B$ est complémenté. On sait que A' est localement booléen par le corollaire II.2.5. Nous allons vérifier que B' est la clôture intégrale de A' dans L (donc est booléen d'après Ershov), puis que $U^{-1}B = T'^{-1}B'$ (ce qui achèvera la démonstration car B' étant booléen $T'^{-1}B'$ le sera aussi d'après le corollaire II.2.5).

(a) B' est la clôture intégrale de A' dans L.

Soit L'' la clôture normale de L sur K, et A'' (resp. B'') la clôture intégrale de A' (resp. B') dans L'' ; $A'' \cap L$ est la clôture intégrale de A' dans L, et comme B' est intégralement clos (en tant que localisé de B qui est intégralement clos), $B' = B'' \cap L$. Il suffit donc de montrer que $A'' = B''$. Autrement dit, quitte à remplacer L par L'', on peut supposer que $L|K$ est une extension normale.

B' est intégralement clos, nous l'avons dit, et il contient manifestement A', donc la première inclusion est claire. Pour l'inclusion inverse, il suffit de montrer que B' est inclus dans tout anneau de valuation de L contenant A'.

Soit R un anneau de valuation de L contenant A', et $m(R)$ son idéal maximal. Soit $\mathfrak{q} := B \cap m(R)$, et $\mathfrak{p} := \mathfrak{q} \cap A$. $M_B(a)$ est stable par K-automorphisme de L, donc aussi $\bigcup M_B(a)$. Donc si par l'absurde, $\mathfrak{q} \not\subseteq \bigcup M_B(a)$, *i.e.* si on peut trouver $y \in \mathfrak{q} \cap T$, alors tout K-conjugué de y appartient à T, donc la norme x de y sur K appartient à T. Or x appartient à A (car y est entier sur A) et à $\mathfrak{q}$ (car y divise x dans B) donc $x \in (\mathfrak{q} \cap T) = \mathfrak{p} \cap S$ (car $T \cap A = S$). Mais alors $x \in m(R) \cap A'^{*}$, ce qui contredit $A' \subseteq R$; $\mathfrak{q}$ est donc inclus dans $\bigcup M_B(a) = B \setminus T$, *i.e.* $R = B_{\mathfrak{q}} \supseteq T^{-1}B = B'$.

(b) $U^{-1}B = T'^{-1}B'$.

L'inclusion $U^{-1}B \subseteq T'^{-1}B'$ est claire : pour tout $\mathfrak{n}' \in M_{B'}(b)$, l'idéal $\mathfrak{n}' \cap B$ de B est premier et contient b, donc est inclus dans $\bigcup M_B(b)$. Il s'ensuit que $B \cap (\bigcup M_{B'}(b))$ est inclus dans $\bigcup M_B(b)$, *i.e.* U est inclus dans $T' \cap B$, et donc dans T'. Comme $B \subseteq B'$, il vient $U^{-1}B \subseteq T'^{-1}B'$.

Inversement, soit $y' \in T'^{-1}B'$. On a :

- $y' = b'/t'$, avec $b' \in B'$ et $t' \in T'$;
- $b' = b_0/t_0$, avec $b_0 \in B$ et $t_0 \in T$;
- $t' = t/t_1$, avec $t \in B$ et $t_1 \in T$.

Donc $y' = \frac{t_1 b_0}{t_0 t}$, avec $t_1 b_0 \in B$, et il suffit de vérifier que $t_0 t \in U$, et pour cela que t_0 et t appartiennent à U (car U est stable par multiplication).

– b divise a dans B, donc $M_B(b) \subseteq M_B(a)$, *i.e.* $T \subseteq U$, et donc $t_0 \in U$.

– D'autre part, si par l'absurde, $t \notin U$, il existe $\mathfrak{n} \in M_B(b)$ tel que $t \in \mathfrak{n}$, donc $t \in T^{-1}\mathfrak{n}$, *i.e.* $t' = t/t_1 \in T^{-1}\mathfrak{n}$. Or $T^{-1}\mathfrak{n} \in \mathrm{Spm}(B')$ et $b \in T^{-1}\mathfrak{n}$, donc

$T^{-1}\mathfrak{n} \in M_{B'}(b) \subseteq B' \setminus T'$. Il vient $t' \in T' \cap T^{-1}\mathfrak{n} = \emptyset$, contradiction.
■

Remarque: Il s'ensuit d'après la proposition II.3.7 que si un anneau intègre A a la BAP alors sa clôture intégrale dans n'importe quelle extension de son corps des fractions a aussi la BAP.

La méthode de descente de Weil

On entend par là en général le procédé suivant : étant donnés un corps K, une extension algébrique finie et séparable L de K, de degré d, et une variété $V' \subseteq (K^a)^n$ définie sur L, on leur associe l'ensemble $\sigma_0(V'(L)) \times \ldots \times \sigma_{d-1}(V'(L))$, où $\sigma_0, \ldots, \sigma_{d-1}$ sont les différents K-plongements de L dans K^a.

Alors il existe une variété $V \subseteq (K^a)^{n\times d}$ définie sur K telle que cet ensemble soit la trace de V sur $\prod_{i=0}^{d-1}(\sigma_i(L))^n$. De plus, si θ est un élément de L donné par le théorème de l'élément primitif (*i.e.* tel que $L = K[\theta]$) alors l'isomorphisme K-linéaire de L dans K^d qui à un élément de L associe ses coordonnées sur K dans la base $(1, \theta, \ldots, \theta^{d-1})$ établit une correspondance bijective entre $V'(L)$ et $V(K)$ (une fois rangées correctement les différentes coordonnées), qui conserve la lissité.

Remarquons que si A est un anneau de corps des fractions K et B sa clôture intégrale dans L, il n'y a en général aucune raison pour que cette correspondance fonctionne encore entre $V'(B)$ et $V(A)$.

Cependant, si W est une famille d'anneaux de valuation sur K et W' l'ensemble des anneaux de valuation R' de L tels que $R' \cap K \in W$, l'étude de la théorie de Galois des corps valués henséliens, telle qu'on peut la trouver dans [End], montre qu'on peut tout de même étendre cette correspondance aux hensélisations de K et L relativement aux éléments de W et W' respectivement (*cf.* [H-P 84]). Précisément, ils ont montré que si W est finie et $K \in \mathrm{RC}(W)$ alors $L \in \mathrm{RC}(W')$. Plus généralement, leur méthode est connue pour marcher pour une famille booléenne.

Notre but dans ce paragraphe sera d'adapter la méthode de Weil, étendue par Heinemann et Prestel, aux cas du LGPH et du LGPH'. Cette adaptation ne se fait pas sans peine, puisque comme nous venons de le rappeler elle ne marche que pour les corps, et que dans nos LGP le fait que les points soient á coordonnées dans des anneaux est essentiel. Cependant, étant linéaire, la correspondance établie pour les corps est continue (relativement à n'importe quelle topologie de corps) ce qui va nous permettre de lever cette difficulté, grâce aux propriétés de densité que nous avons démontrées (en bonne partie dans ce but) et au fait qu'un anneau de valuation est ouvert pour la topologie qu'il définit.

Proposition 2
Soit A un anneau satisfaisant le LGPH (resp. LGPH'), K son corps des fractions, et L une extension finie de K, de degré d, séparable sur K. Alors la clôture intégrale B de A dans L satisfait le LGPH (resp. LGPH').

Preuve: La proposition 1 nous garantit déja que B est localement booléen, donc toute partie constructible de son spectre maximal est quasi-compacte et *a fortiori* B satisfait la condition non géométrique du LGPH (resp. LGPH') ; nous pouvons donc consacrer nos efforts à l'autre condition.

Le théorème de l'élément primitif nous donne $\theta \in L$, que l'on peut choisir entier sur A, tel que $L = K[\theta]$. Soient $\sigma_0, \ldots, \sigma_{d-1}$ les K-plongements de L dans K^a, avec $\sigma_0 = \mathrm{Id}_L$. Pour chaque $j \in [\![0, d[\![$, notons $\theta_j := \sigma_j(\theta)$, et soit $M := (\theta_j^i)_{0 \le i,j < d}$ la matrice de Van der Monde de $(\theta_0, \ldots, \theta_{d-1})$.

Soit $g := (g_1, \ldots, g_m) \in L[Y_1, \ldots, Y_n]^m$ un système absolument réduit d'équations d'une variété non vide V' définie sur L. Soit $f := (f_{i,j})_{\substack{1 \le i \le m \\ 0 \le j < d}} \in (K[X_{i,j}]_{\substack{1 \le i \le n \\ 0 \le j < d}})^{m \times d}$ défini par :

$$\forall i \in [\![1, n]\!], \quad g_i\left(\sum_{j=0}^{d-1} X_{1,j}\theta^j, \ldots, \sum_{j=0}^{d-1} X_{n,j}\theta^j\right) = \sum_{j=0}^{d-1} f_{i,j}(X_{1,0}, \ldots, X_{n,d-1})\theta^j.$$

La descente de Weil nous dit que f est un système absolument réduit d'équations d'une variété V, définie sur K. De plus, si l'on range les coordonnées des points de $V(K)$ (resp. $\prod_{0 \le i \le d-1} V'(K(\theta_i))$) sous la forme de matrices $n \times d$, l'endomorphisme Ψ de $M_{n,d}(K^a)$ défini par $\Psi : x \mapsto xM$ envoie $V^\circ(K)$ dans $\prod_{0 \le i \le d-1} V'^\circ(K(\theta_i))$, tandis que pour tout $y \in V'^\circ(L)$ (présenté en colonne) sa réciproque Θ envoie $(\sigma_0(y), \ldots, \sigma_{d-1}(y))$ dans $V^\circ(K)$.

En particulier, $\qquad V^\circ(K) \neq \emptyset \iff V'^\circ(L) \neq \emptyset. \qquad (*)$

On suppose que V' satisfait les hypothèses du LGPH (resp. LGPH') dans B. Nous allons montrer que V' a un point dans B. Notons que pour le LGPH', en vertu de $(*)$, $V^\circ(K) \neq \emptyset$.

Étape 1. $\forall \mathfrak{m} \in \mathrm{Spm}(A)$, V possède un point lisse dans L entier sur $A_\mathfrak{m}$.

Soit $\mathfrak{m} \in \mathrm{Spm}(A)$ fixé ; $\mathfrak{m}$ se relève en $\mathfrak{n}_1, \ldots, \mathfrak{n}_r$ dans $\mathrm{Spm}(B)$. Pour chaque $i \in [\![1, r]\!]$, notons $B_i := B^h_{\mathfrak{n}_i}$, et $L_i := \mathrm{Fr}(B_i)$. Pour chaque $j \in [\![0, d[\![$, soit $K_j := (H_\mathfrak{m}(K))(\theta_j)$, et A_j l'unique prolongement (et donc aussi la clôture intégrale) de $A^h_\mathfrak{m}$ dans K_j.

• On sait (voir [End]) que pour chaque $i \in [\![1, r]\!]$ il existe $j(i) \in [\![0, d[\![$ tel que B_i soit K-isomorphe à $A_{j(i)}$. Plus précisément, le polynôme minimal μ de θ sur K se décompose sur $H_\mathfrak{m}(K)$ en r facteurs irréductibles $\mu_1, \ldots, \mu_r$; pour chaque $i \in [\![1, r]\!]$, soit $\Omega_i := \{j \in [\![0, d[\![\ / \ \mu_i(\theta_j) = 0\}$ et $j(i)$ un élément quelconque de Ω_i, alors il existe un K-automorphisme τ_i de K^a tel que :

- $\tau_i[B_i] = A_{j(i)}$;
- $\tau_i(\theta) = \theta_{j(i)}$ donc $\tau_{i|L} = \sigma_{j(i)}$;
- $L_i = \tau_i^{-1}[H_\mathfrak{m}(K)](\theta)$.

$\forall i \in [\![1, r]\!]$, soit $y_i' \in V'^\circ(B_i)$ donné par les hypothèses du LGPH (resp. LGPH'). Remarquons que $\tau_i(y_i') \in V'^\circ(A_{j(i)})$.
$\forall j \in \Omega_i$, θ_j et $\theta_{j(i)}$ sont $H_\mathfrak{m}(K)$-conjugués, on a donc un plongement de $A_{j(i)}$ au dessus de $H_\mathfrak{m}(K)$ qui envoie $\theta_{j(i)}$ sur θ_j. Soit $x'_{j,\mathfrak{m}}$ l'image de $\tau_i(y_i')$ par ce plongement. On a :

$$x'_{j(i),\mathfrak{m}} = \tau_i(y_i') \subseteq A_{j(i)} \Longrightarrow x'_{j(i),\mathfrak{m}} \text{ est entier sur } A^h_\mathfrak{m}. \tag{1}$$

Enfin soit $x'_\mathfrak{m} := (x'_{0,\mathfrak{m}}, \ldots, x'_{d-1,\mathfrak{m}})$ (rangé sous forme de matrice $n \times d$).

• Ainsi qu'il est démontré dans [H-P 84], il s'ensuit que : $x_\mathfrak{m} := \Theta(x'_\mathfrak{m}) \in V^\circ(H_\mathfrak{m}(K))$.

Ceci étant valable pour tout $\mathfrak{m}' \in \mathrm{Spm}(A)$, le corollaire I.4.5 de densité locale s'applique (qu'on soit dans le cas du LGPH ou du LGPH', vu $(*)$) : $V^\circ(K)$ est dense dans $V^\circ(H_\mathfrak{m}(K))$. On peut donc trouver $x \in V^\circ(K)$ tel que $|x - x_\mathfrak{m}|_\mathfrak{m} \le 1$, *i.e.* $x - x_\mathfrak{m} = \varepsilon$, avec $\varepsilon \in M_{n,d}(A^h_\mathfrak{m})$.

Soit $x' := \Psi(x) = (x'_0, \ldots, x'_{d-1})$; on sait que $x' \in \prod_{0 \le i \le d-1} V'^{\circ}(K(\theta_i))$, *i.e.* que $x'_0 \in V'^{\circ}(L)$, et que $\forall j \in [\![0, d-1]\!]$, $x'_j = \sigma_i(x'_0)$. Le but est maintenant de montrer que x'_0 est entier sur $A_{\mathfrak{m}}$ *i.e.* que pour tout $i \in [\![1, r]\!]$ $x'_0 \in B_{\mathfrak{n}_i}$. Puisqu'on sait déja que $x'_0 \in L$, il suffit pour cela de montrer que pour tout $i \in [\![1, r]\!]$ $x'_0 \in B_i$.

Soit $i \in [\![1, r]\!]$; on a $\tau_{i|L} = \sigma_{j(i)}$, et $\tau_i[B_i] = A_{j(i)}$ donc :

$$x'_0 \in B_i \iff \tau_i(x'_0) \in A_{j(i)} \iff \sigma_{j(i)}(x'_0) \in A_{j(i)} \iff x'_{j(i)} \in A_{j(i)}.$$

Comme par définition $A_{j(i)}$ est la clôture intégrale de $A^h_{\mathfrak{m}}$ dans K_j, et que $x'_{j(i)} \in K(\theta_{j(i)}) \subseteq (H_{\mathfrak{m}}(K))(\theta_{j(i)}) = K_j$, il suffit de montrer que $x'_{j(i)}$ est entier sur $A^h_{\mathfrak{m}}$. Or on a :

$$x' - x'_{\mathfrak{m}} = \Psi(x) - \Psi(x_{\mathfrak{m}}) = \Psi(x - x_{\mathfrak{m}}) = \varepsilon M.$$

ε est à coefficients dans $A^h_{\mathfrak{m}}$ et M à coefficients entiers sur A donc *a fortiori* entiers sur $A^h_{\mathfrak{m}}$. La matrice $x' - x'_{\mathfrak{m}}$ est donc à coefficients entiers sur $A^h_{\mathfrak{m}}$, et en particulier les coordonnées de sa $j(i)$-ème colonne $x'_{j(i)} - x'_{j(i),\mathfrak{m}}$ sont entières sur $A^h_{\mathfrak{m}}$. Or $x'_{j(i),\mathfrak{m}}$ est à coordonnées entières sur $A^h_{\mathfrak{m}}$ d'après (1), donc aussi $x'_{j(i)}$.

Étape 2. $V(B) \neq \emptyset$.

Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, la première étape nous donne un point $y'_{\mathfrak{m}}$ de $V'^{\circ}(L)$ entier sur $A_{\mathfrak{m}}$. Soient $f_{\mathfrak{m},1}, \ldots, f_{\mathfrak{m},n}$ les polynômes minimaux sur K des coordonnées de $y'_{\mathfrak{m}}$. Soit $s_{\mathfrak{m}} \in A$ un plus petit dénominateur commun des coefficients des $f_{\mathfrak{m},i}$ $(1 \le i \le n)$. $y'_{\mathfrak{m}}$ étant entier sur $A_{\mathfrak{m}}$, on a $s_{\mathfrak{m}} \notin \mathfrak{m}$, *i.e.* $\mathfrak{m} \in M_A(s_{\mathfrak{m}})^c$, et pour tout $\mathfrak{m}' \in M_A(s_{\mathfrak{m}})^c$, $y'_{\mathfrak{m}}$ est entier sur $A_{\mathfrak{m}'}$. Les $(M_A(s_{\mathfrak{m}})^c)_{\mathfrak{m} \in \mathrm{Spm}(A)}$ recouvrent $\mathrm{Spm}(A)$, on peut donc en extraire un recouvrement fini $(M_A(s_0)^c, \ldots, M_A(s_p)^c)$. Posons $W_0 := W_A(s_0)^c$, et pour tout $i \in [\![1, p]\!]$:

- $W_i := W_A(s_i)^c \setminus \bigcup_{0 \le j < i} W_j$,
- $z'_i := (\sigma_0(y'_i), \ldots, \sigma_{d-1}(y'_i))$,
- $z_i := \Theta(z'_i) \in V'^{\circ}(K)$.

La famille $(W_i)_{0 \le i \le p}$ constitue une partition constructible de W_A, et pour tout $\mathfrak{m} \in W_i$, $s_i \notin \mathfrak{m}$ donc y'_i est entier sur $A_{\mathfrak{m}}$. On considère le point constructible z défini par $\forall i \in [\![0, p]\!]$, $\forall R \in W_i$, $z(R) = z_i$. C'est un point de $V^{\circ}(\mathcal{C}(A))$, donc la proposition 1.1 de densité dans les constructibles s'applique : il existe $x \in V^{\circ}(K)$ tel que $|x - z|_{W_A} \le 1$, *i.e.* quels que soient $i \in [\![1, p]\!]$ et $R \in W_i$, $x - z_i = \varepsilon_i$ avec $\varepsilon_i \in M_{n,d}(R)$.

Soit $x' := \Psi(x)$, et y' la première colonne de x'. On sait que $y' \in V'^{\circ}(L)$.
Soit $\mathfrak{m} \in \mathrm{Spm}(A)$, et $i \in [\![0, p]\!]$ tel que $A_{\mathfrak{m}} \in W_i$. On a :

- y'_i est entier sur $A_{\mathfrak{m}}$, donc aussi z'_i ;
- $x' - z'_i = \Psi(x - z_i) = \varepsilon_i M$ est à coefficients entiers sur $A_{\mathfrak{m}}$.

On en déduit que x' est entier sur $A_{\mathfrak{m}}$, et en particulier les coefficients de sa première colonne y' sont entiers sur $A_{\mathfrak{m}}$. Ceci étant valable pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, il s'ensuit que y' est entier sur A, et puisque $y' \subseteq L$, que $y' \in V'(B)$.

■

Proposition 3

Soit A un anneau satisfaisant le LGPH (resp. LGPH'), K son corps des fractions, et L une extension algébrique finie purement inséparable de K. Alors la clôture intégrale B de A dans L satisfait le LGPH (resp. LGPH').

Preuve: La preuve est beaucoup plus simple que dans le cas séparable. Soit V' une variété définie sur L, telle que quel que soit $\mathfrak{n} \in \mathrm{Spm}(B)$, $V'^{\circ}(B^h_{\mathfrak{n}}) \neq \emptyset$ (et s'il y a lieu $V'^{\circ}(L) \neq \emptyset$).

Par hypothèse, il existe un entier n tel que $L^{p^n} \subseteq K$. Soit $\varphi : x \mapsto x^{p^n}$ l'automorphisme de K^a correspondant. Alors on sait que pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ il existe un unique $\mathfrak{n} \in \mathrm{Spm}(B)$ qui relève $\mathfrak{m}$ dans B, et que $\varphi[B^h_{\mathfrak{n}}]$ est inclus dans $A^h_{\mathfrak{m}}$.

L'image de V' par φ est une variété V définie sur L^{p^n} et *a fortiori* sur K, ayant d'après ce qui précède un point lisse à coordonnées dans $A^h_{\mathfrak{m}}$ pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ (et s'il y a lieu un point lisse dans K). Le LGPH (ou le LGPH') donne alors un point $a \in V^{\circ}(A)$ que φ^{-1} envoie sur un point de V' à coordonnées dans B, c.q.f.d.

■

Corollaire 4

Soit A un anneau satisfaisant le LGPH (resp. LGPH'), K son corps des fractions, et L une extension algébrique de K. Alors la clôture intégrale B de A dans L satisfait le LGPH (resp. LGPH').

Preuve: Si L est une extension finie de K cela découle immédiatement des deux propositions précédentes : soit K' la clôture séparable relative de K dans L, d'après la proposition 2 la clôture intégrale A' de A dans K' satisfait le LGPH (resp. le LGPH') et d'après la proposition 3 la clôture intégrale de A' dans L, qui coïncide avec B, le satisfait aussi.

Pour le cas général, soit V une variété définie sur L, ayant pour tout $\mathfrak{n} \in \mathrm{Spm}(B)$ un point lisse $y_{\mathfrak{n}} \subseteq B_{\mathfrak{n}}$, (resp. et un point lisse $y_L \subseteq L$). Les coefficients dans L d'un système absolument réduit d'équations de V, (resp. plus les coordonnées de y_L) engendrent une extension finie K' de K. D'après ce qui précède la clôture intégrale A' de A dans K' satisfait le LGPH (resp. le LGPH'). Quitte à remplacer A par A' on peut donc supposer que V est définie sur K (et que $y_L \subseteq K$). L'argument du théorème 2.2 de [H-P 84] montre qu'il existe une sous-extension $K \subseteq L' \subseteq L$ telle que $[L' : K]$ soit fini et que la clôture intégrale B' de A dans L' vérifie : $\forall \mathfrak{n}' \in \mathrm{Spm}(B')$, $V^{\circ}(B'^h_{\mathfrak{n}'}) \neq \emptyset$. La conclusion suit.

■

§ 3. LGPH et clôture existentielle

Lemme 1

Soit A un anneau localement booléen $\cap$-stable, et $I_1, \ldots, I_n$ des idéaux de A propres et non nuls tels que les $M(I_k)$ soient deux à deux disjoints. Quel que soit $k \in [\![1, n]\!]$ soit $\alpha_k \in A \setminus \{0\}$ tel que $M(I_k) \subseteq M(\alpha_k)$.
Alors il existe $\beta_1, \ldots, \beta_n \in A \setminus \{0\}$ tels que :
- *$\forall k \in [\![1, n]\!],\ M(I_k) \subseteq M(\beta_k) \subseteq M(\alpha_k)$;*
- *$\forall k, l \in [\![1, n]\!],\ k \neq l \Longrightarrow M(\beta_k) \cap M(\beta_l) = \emptyset$.*

Remarque: Avec des données de ce genre, nous appliquerons le lemme 1 sans nous y référer en disant simplement :

"quitte à réduire les $M(\alpha_i)$ on peut les supposer deux à deux disjoints."

L'essentiel étant de conserver l'hypothèse utile, à savoir $M(I_k) \subseteq M(\alpha_k)$.

Preuve: On commence par construire $\beta_{1,2}$ tel que $M(I_1) \subseteq M(\beta_{1,2}) \subseteq M(\alpha_1)$ et $M(\beta_{1,2})$ disjoint de $M(I_2)$. Soit $\mathfrak{m} \in M(I_1)$; posons $S := A \setminus \bigcup M(I_2)$. On sait que $\mathrm{Spm}(S^{-1}A) = \{S^{-1}\mathfrak{n} \,/\, \mathfrak{n} \in M(I_2)\}$ (*cf.* la proposition II.2.3) et que tout idéal maximal de A qui ne rencontre pas S se relève en idéal maximal de $S^{-1}A$; il s'ensuit que $\mathfrak{m} \cap S \neq \emptyset$. Prenons donc un élément $c_{\mathfrak{m}}$ de $\mathfrak{m} \cap S$. La famille $(M(c_{\mathfrak{m}}))_{\mathfrak{m} \in M(I_1)}$ recouvre $M(I_1)$, on peut donc en extraire un recouvrement fini $(M(c_i))_{1 \leq i \leq r}$ (nous avons déjà justifié cet abus de langage au début du II.5). Le produit des c_i donne un élément c tel que $M(c) \supseteq \bigcup_{i=1}^{r} M(c_i) \supseteq M(I_1)$, de plus $c \in S = A \setminus \bigcup M(I_2)$ donc $M(c)$ ne rencontre pas $M(I_2)$. Il suffit alors de prendre pour $\beta_{1,2}$ un élément de A tel que $M(\beta_{1,2}) = M(\alpha_1) \cap M(c)$.

On répète cette construction pour $I_3, \ldots, I_n$ et on choisit un élément β_1 de A tel que $M(\beta_1) = M(\beta_{1,2}) \cap \cdots \cap M(\beta_{1,n})$. On a donc $M(I_1) \subseteq M(\beta_1) \subseteq M(\alpha_1)$ et $M(\beta_1)$ disjoint de $M(I_k)$ pour tout $k \neq 1$. Si $\beta_1, \ldots, \beta_{k-1}$ ont déja été construits, la même opération réalisée sur $M(I_k)$ et $M(\beta_1), \ldots, M(\beta_k), M(I_{k+1}), \ldots, M(I_n)$ nous donne un élément $\beta_k \in A$ tel que $M(I_k) \subseteq M(\beta_k) \subseteq M(\alpha_k)$ et $M(\beta_k)$ disjoint de $M(\beta_l)$ pour tout $l < k$ et de $M(I_l)$ pour tout $l > k$. Les $\beta_1, \ldots, \beta_n$ ainsi construits sont les éléments recherchés.

■

Lemme 2

*Soit A un anneau localement booléen $\cap$-stable ; on se donne des idéaux r-clos non nuls $I_1, \ldots, I_r$ de $(A, \leq_A)$ tels que les $M(I_k)$ soient non vides (*i.e. *I_k est un idéal propre de A) et deux à deux disjoints, et des idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ tous distincts. Posons $\mathcal{M} := \bigcup_{k=1}^{r} M(I_k) \cup \{\mathfrak{m}_1, \ldots, \mathfrak{m}_t\}$.*
Soient $\alpha \in \cap\mathcal{M} \setminus \{0\}$ et $x_0 \in A^n$.
Enfin pour tout $\mathfrak{m} \in M(\alpha)$ soient $\alpha_{\mathfrak{m}} \in \mathfrak{m} \setminus \{0\}$ et $x_{\mathfrak{m}}$ un point de A^n.

Alors il existe un point constructible $\overline{x} \in \mathcal{C}(W_A)$ tel que pour tout $\mathfrak{m} \in M(\alpha)^c$, $\overline{x}(A_{\mathfrak{m}}) = x_0$, et que quel que soit $\mathfrak{m} \in M(\alpha)$ il existe $\mathfrak{n} \in M(\alpha)$ vérifiant :

(a) *$\mathfrak{m} \in M(\alpha_{\mathfrak{n}})$ et $\overline{x}(A_{\mathfrak{m}}) = x_{\mathfrak{n}}$;*

(b) *$\forall k \in [\![1, r]\!]$, si $\mathfrak{m} \in M(I_k)$ alors $\mathfrak{n} \in M(I_k)$;*

(c) *$\forall j \in [\![1, t]\!]$, si $\mathfrak{m} = \mathfrak{m}_j$ alors $\mathfrak{n} = \mathfrak{m}_j$.*

Remarque: Ce qu'il faut comprendre dans l'énoncé ci-dessus, c'est qu'on remplace $(x_{\mathfrak{m}})_{\mathfrak{m} \in \mathrm{Spm}(A)}$ par un point $\overline{x}$ qui a les mêmes propriétés relativement à $I_1, \ldots, I_r$ et $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ et qui *en plus* est constructible. Ce n'est d'ailleurs qu'une indigeste trivialité.

Preuve:
Cas 1 : $r = 1$ et $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_t\} \subseteq M(I_1)$.

Quitte à restreindre les $M(\alpha_{\mathfrak{m}_j})$ $(1 \leq j \leq t)$ on peut les supposer deux à deux disjoints et inclus dans $M(\alpha)$.

Soit $\mathcal{N} := M(I_1) \setminus \bigcup_{j=1}^{t} M(\alpha_{\mathfrak{m}_j})$; c'est l'intersection d'une partie constructible, donc quasi-compacte, de $\mathrm{Spm}(A)$ avec $M(I_1)$, et ce dernier étant fermé $\mathcal{N}$ est lui-même quasi-compact. La famille des $M(\alpha_{\mathfrak{m}})$ recouvre $\mathcal{N}$ quand $\mathfrak{m}$ décrit $\mathcal{N}$, on peut donc en extraire une partition finie $M(\alpha_{\mathfrak{m}_{t+1}}), \ldots, M(\alpha_{\mathfrak{m}_u})$ de $\mathcal{N}$ (cet abus de langage a été justifié au début du II.5).

Quitte à remplacer chaque $\alpha_{\mathfrak{m}_j}$ $(1 \leq j \leq u)$ par un élément $\beta_{\mathfrak{m}_j}$ tel que :

$$M(\beta_{\mathfrak{m}_j}) = M(\alpha_{\mathfrak{m}_j}) \setminus \bigcup_{1\leq i<j} M(\alpha_{\mathfrak{m}_i})$$

(ce qu'on peut faire puisque A est localement complémenté et $\cap$-stable) on peut supposer les $M(\alpha_{\mathfrak{m}_j})$ deux à deux distincts. Le lecteur vérifiera alors sans peine que le point constructible défini ci-après a bien les propriétés annoncées :

$$\forall \mathfrak{m} \in \mathrm{Spm}(A), \qquad \overline{x}(A_\mathfrak{m}) = \begin{cases} x_{\mathfrak{m}_j} & \text{si } \mathfrak{m} \in M(\alpha_j) \quad 1 \leq j \leq u \\ x_0 & \text{sinon} \end{cases}$$

Le cas général : Pour tout $k \in [\![1, r]\!]$ soit $\mathcal{M}_k := \{\mathfrak{m}_{k,1}, \ldots, \mathfrak{m}_{k,s_k}\}$ une énumération de l'ensemble des $\mathfrak{m}_j$ appartenant à $M(I_k)$, et soit $\mathcal{M}_0 := (\mathfrak{m}_{0,1}, \ldots, \mathfrak{m}_{0,s_0})$ une énumération des $\mathfrak{m}_j$ restants, c'est-à-dire de $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_t\} \setminus \bigcup_{k=1}^r M(I_k)$. On déduit facilement du lemme d'évitement des idéaux premiers que $\mathcal{M}_0 = M(I_0)$ où $I_0 := \bigcap \mathcal{M}_0$.

Pour chaque $k \in [\![0, r]\!]$ soit $a_k \in I_k \setminus \{0\}$. Quitte à réduire les $M(a_k)$ on peut les supposer deux à deux disjoints. Le premier cas s'applique à I_k et $\mathcal{M}_k$, et nous donne un point constructible $\overline{x}_k$ correspondant à ces données. Il suffit alors, comme le lecteur pourra le vérifier aisément, de les combiner en posant :

$$\forall \mathfrak{m} \in \mathrm{Spm}(A), \qquad \overline{x}(A_\mathfrak{m}) = \begin{cases} \overline{x}_k(A_\mathfrak{m}) & \text{si } \mathfrak{m} \in M(\alpha_k) \quad 0 \leq k \leq r \\ x_0 & \text{sinon} \end{cases}$$

■

Proposition 3 (clôture existentielle)
Soit A un anneau de Prüfer, $\leq$ sa relation radicale associée et K son corps de fraction. On munit $(A, \leq)$ d'idéaux r-clos non nuls $I_1, \ldots, I_r$ tels que les $M(I_k)$ soient non vides et deux à deux disjoints.
Soit K' une extension régulière de K ; pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ on suppose donné un anneau de valuation $R(\mathfrak{m})$ de K' prolongeant $A_\mathfrak{m}$ tel que le plongement naturel de $A_\mathfrak{m}^h$ dans $R(\mathfrak{m})^h$ soit $\exists$-clos au sens de $\mathrm{L_{rad}}$ (ou $\mathrm{L_{div}}$). On note W' la famille d'anneaux de valuation de K' ainsi définie.
Soit $A' := \cap W'$, $\mathcal{P}' := \{m(R') \cap A' \,/\, R' \in W'\}$, et pour tout $k \in [\![1, r]\!]$, $I'_k := \cap\{m(R(\mathfrak{m})) \cap A' \,/\, \mathfrak{m} \in M(I_k)\}$. On munit A' de la relation radicale $\leq'$ définie par $\mathcal{P}' \cup \{0\}$ si $(A, \leq)$ est un $\mathrm{r}_\circ$-domaine et par $\mathcal{P}'$ sinon.

Alors $(A, \leq, I_1, \ldots, I_r)$ est une sous-$\mathrm{L^r_{rad}}$-structure de $(A', \leq', I'_1, \ldots, I'_r)$ (où $\mathrm{L^r_{rad}}$ est le langage obtenu en enrichissant $\mathrm{L_{rad}}$ de r prédicats unaires, interprétés par les I_k dans A et les I'_k dans A').
De plus si A satisfait le LGPH (resp. s'il satisfait le LGPH' et si $K \leq_\exists K'$) alors le plongement de $(A, \leq, I_1, \ldots, I_r)$ dans $(A', \leq', I'_1, \ldots, I'_r)$ est $\exists$-clos.

Remarque: Nous reviendrons plus tard sur les plongements de $\mathrm{L^r_{rad}}$-structures, mais disons tout de suite que la première affirmation signifie seulement que $I'_k \cap A = I_k$ pour tout $k \leq r$ et que la trace de $\leq'$ sur A coïncide avec $\leq$, ce qui est immédiat d'après le théorème 3 des prérequis. L'objet de cette proposition est donc le fait que ce plongement soit existentiellement clos au sens de $\mathrm{L^r_{rad}}$.

Preuve: La démonstration est un peu longue, mais suit un schéma très classique (nous l'avons déjà rencontré dans la démonstration de la proposition I.1.2) : on prend une formule $\varphi(x)$ de $\mathrm{L^r_{rad}}$ à n variables libres et à paramètres dans A, sans quanteur, telle que $(A', \leq', I'_1, \ldots, I'_r) \models \exists x \varphi(x)$. Dans en premier temps on modifie φ pour ramener sa satisfaction à un problème "local" (c'est-à-dire dans les R'^h et dans K'). Puis on transfère ces données aux structures locales de A en utilisant que $A^h_{\mathfrak{m}} \leq_\exists R(\mathfrak{m})^h$. Enfin le LGPH ou le LGPH' opère la synthèse de ces informations locales pour donner un point a de A^n tel que $(A, \leq, I_1, \ldots, I_r) \models \varphi(a)$.

Pour alléger un peu l'écriture, je note "$A \models \cdots$" au lieu de "$(A, \leq, I_1, \ldots, I_r) \models \cdots$", et de même pour A', et pour les structures locales.

Partie I : modification de φ.

• φ peut se mettre sous forme normale disjonctive, $\varphi(x) \equiv \bigvee\!\!\bigvee \varphi_i(x)$, où les φ_i sont des conjonctions de formules négatomiques de $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$, à paramètres dans A. Comme $A' \models \exists x \varphi(x)$, l'une au moins des $\varphi_i(x)$, disons φ_1 est satisfaite dans A'. Il suffit de prouver que $A \models \exists x \varphi_1(x)$ pour avoir $A \models \exists x \varphi(x)$. Quitte à remplacer φ par φ_1, on peut supposer que φ est de la forme suivante :

$$\varphi(x) \equiv \varphi_0(x) \wedge \varphi^+_{rad}(x) \wedge \varphi^-_{rad}(x) \wedge \bigwedge\!\!\!\bigwedge_{i=1}^{k} (\varphi^+_k(x) \wedge \varphi^-_k(x))$$

où :
- $\varphi_0(x) \equiv \bigwedge\!\!\bigwedge_{i=1}^m f_i(x) = 0 \bigwedge\!\!\bigwedge_{i=1}^{m'} f'_i(x) \neq 0$,
- $\varphi^+_{rad}(x) \equiv \bigwedge\!\!\bigwedge_{i=1}^s p_i(x) \leq q_i(x)$,
- $\varphi^-_{rad}(x) \equiv \bigwedge\!\!\bigwedge_{i=1}^{s'} p'_i(x) \not\leq q'_i(x)$,
- $\forall k \in [\![1, r]\!]$, $\varphi^+_k(x) \equiv \bigwedge\!\!\bigwedge_{i=1}^{l_k} I_k(g_{k,i}(x))$ et $\varphi^-_k(x) \equiv \bigwedge\!\!\bigwedge_{i=1}^{l'_k} \neg I_k(g'_{k,i}(x))$

où les $f_i, f'_i, p_i, q_i, p'_i, q'_i, g_{k,i}$ et $g'_{k,i}$ sont pris dans $A[X]$ $(X = (X_1, \ldots, X_n))$.
On fixe un élément a' de A'^n tel que $A' \models \varphi(a')$.

• Modification de φ_0.
Soit $\mathcal{I} := \{f \in A[X] \;/\; f(a') = 0\}$. Puisque l'extension $K'|K$ est régulière, $K(a')|K$ aussi, et $\mathcal{I}$ est l'idéal d'une variété V définie sur K, dont a' est un point générique (donc lisse). Soit $H \subseteq A[X]$ un système absolument réduit d'équations de V. Soit Δ un déterminant de taille $n - \dim V$ extrait du Jacobien de H tel que $\Delta(a') \neq 0$. Soit $f_0 := \Delta \times \prod_{i=1}^{m'} f'_i$.
$A' \models H(a') = 0 \wedge f_0(a') \neq 0$ et pour tout $a \in A^n$, si $A \models H(a) = 0 \wedge f_0(a) \neq 0$, on a :
- $H(a) = 0 \implies a \in V$, et $\forall i \in [\![1, m]\!]$, $f_i \in I(V) \Longrightarrow f_i(a) = 0$,
- $f_0(a) \neq 0 \implies \forall i \in [\![1, m']\!]$, $f'_i(a) \neq 0$,

et donc $A \models \varphi_0(a)$.
Quitte à remplacer $\varphi_0(x)$ par "$H(x) = 0 \wedge f_0(x) \neq 0$" on peut donc supposer que $f := (f_1, \ldots, f_m)$ est un système absolument réduit d'équations de V, et que $\varphi_0(x) \equiv f(x) = 0 \wedge f_0(x) \neq 0$.

• Modification de φ^+_{rad}.
Soit $I := \{i \in [\![1, s]\!] \;/\; p_i(a') \neq 0 \text{ ou } q_i(a') \neq 0\}$.

Cas 1. $(0) \notin \mathrm{Sp}(A, \leq)$. Soit $\alpha \in A \setminus \{0\}$ tel que $0 \leq \alpha$. Pour tout $i \in I$, on pose :

$$h_i(x) := \begin{cases} p_i(x) & \text{si } p_i(a') \neq 0, \\ \alpha & \text{sinon.} \end{cases}$$

Cas 2. $(0) \in \mathrm{Sp}(A, \leq)$. Alors, par construction, $(0) \in \mathrm{Sp}(A', \leq')$. Donc quel que soit $i \in [\![1, s]\!]$, si $p_i(a') = 0$ nécessairement $q_i(a') = 0$, ce qui implique que $i \notin I$. Pour tout $i \in I$, on a donc $p_i(a') \neq 0$, et on pose $h_i := p_i$.

Dans les deux cas, on a, pour tout $i \in I$: $h_i(a') \leq' q_i(a')$.

D'autre part quel que soit $a \in V(A)$ tel que $A \models \bigwedge\!\!\!\bigwedge_{i\in I} h_i(a) \leq q_i(a)$, on a pour tout $i \in [\![1, s]\!]$:

– Si $i \notin I$.
  $p_i(a') = q_i(a') = 0$, donc $p_i, q_i \in I(V)$, et donc $p_i(a) = q_i(a) = 0$, et *a fortiori* $p_i(a) \leq q_i(a)$.
– Si $i \in I$ et $p_i(a') \neq 0$.
  Dans les deux cas (1 et 2) $h_i = p_i$, donc trivialement $h_i(a) \leq q_i(a) \Longrightarrow p_i(a) \leq q_i(a)$.
– Si $i \in I$ et $p_i(a') = 0$.
  Cela implique, par définition de I, que $q_i(a') \neq 0$, donc on est dans le cas 1 ($0 \leq' q_i(a') \neq 0$). On a $h_i = \alpha$ et $0 \leq \alpha \leq q_i(a)$, donc $p_i(a) \leq q_i(a)$.

On voit que tout $a \in A^n$ qui satisfait $\varphi_0(x)$ et '$\bigwedge\!\!\!\bigwedge_{i\in I} h_i(x) \leq q_i(x)$" satisfait aussi $\varphi_0 \wedge \varphi^+_{rad}$. Quitte à remplacer φ^+_{rad} par "$\bigwedge\!\!\!\bigwedge_{i\in I} h_i(x) \leq q_i(x)$", on peut donc supposer que $\forall i \in [\![1, s]\!],\ \ p_i \notin I(V)$.

• Modification de φ^-_{rad}.
Soit $I := \{i \in [\![1, s']\!] \ /\ p'_i(a') \not\leq_{\mathcal{P}'} q'_i(a')\}$, et $J := [\![1, s']\!] \setminus I$. Notons que si la relation radicale $\leq'$ est définie par $\mathcal{P}'$ alors $I = [\![1, s']\!]$ et $J = \emptyset$.
Soit $h := \prod_{i\in J} q'_i$; quel que soit $i \in J$ on a $p'_i(a') \not\leq' q'_i(a')$, et en particulier $q'_i(a') \neq 0$, donc $h(a') \neq 0$, *i.e.* $A' \models \bigwedge\!\!\!\bigwedge_{i\in I} p'_i(a') \not\leq' q'_i(a') \wedge h(a') \neq 0$.
D'autre part, tout élément $a \in V(A)$ tel que $A \models \bigwedge\!\!\!\bigwedge_{i\in I} p'_i(a) \not\leq q'_i(a) \wedge h(a) \neq 0$, vérifie pour tout $i \in [\![1, s]\!]$:

– Si $i \in I$, $\ p'_i(a) \not\leq q'_i(a)$.
– Sinon, $i \in J$ donc $p'_i(a') \leq_{\mathcal{P}'} q'_i(a')$, et puisque $p'_i(a') \not\leq' q'_i(a')$ on est dans le cas où $\leq'$ est définie par $\mathcal{P}' \cup \{0\}$ (donc où $(A, \leq)$ est un r_o-domaine) et on a $p'_i(a') = 0$ et $q'_i(a') \neq 0$. Il s'ensuit que $p'_i \in I(V)$, et puisque $a \in V(A)$ on a $p'_i(a) = 0$. D'autre part q'_i divise h et $h(a) \neq 0$ donc $q'_i(a) \neq 0$, et puisque $(A, \leq)$ est un r_o-domaine il vient $p'_i(a) \not\leq q'_i(a)$.

On voit donc que $\forall a \in A^n$, si $A \models \varphi_0(a) \bigwedge\!\!\!\bigwedge_{i\in I} p'_i(a) \not\leq q'_i(a) \wedge h(a) \neq 0$, alors $A \models \varphi_0(a) \wedge \varphi^-_{rad}(a)$. Quitte à remplacer f_0 par $f_0 \times h$ dans φ_0, et φ^-_{rad} par $\bigwedge\!\!\!\bigwedge_{i\in I} p'_i(a) \not\leq q'_i(a)$, on peut supposer que pour tout $i \in [\![1, s']\!]$ on a $p'_i(a') \not\leq_{\mathcal{P}'} q'_i(a')$ *i.e.* il existe $\mathfrak{m} \in \mathrm{Spm}(A)$ tel que $p'_i(a') \in m(R(\mathfrak{m}))$ et $q'_i(a') \notin m(R(\mathfrak{m}))$.

Partie II : transfert et synthèse.

• Soit $\{h_1, \dots, h_N\}$ une énumération des $p_i, q_i, p'_i, q'_i, g_{k,i}$ et $g'_{k,i}$. Pour chaque $\mathfrak{m} \in \mathrm{Spm}(A)$ soit $\Omega_{\mathfrak{m}} := \{i \in [\![1, N]\!] \ /\ h_i(a') \in m(R(\mathfrak{m}))\}$ et $\Omega'_{\mathfrak{m}} := [\![1, N]\!] \setminus \Omega_{\mathfrak{m}}$. On considère la formule :

$$\varphi_{\mathfrak{m}}(x) \equiv \bigwedge\!\!\!\bigwedge_{1\leq i\leq s} p_i(x) \neq 0 \wedge \bigwedge\!\!\!\bigwedge_{i\in\Omega_{\mathfrak{m}}} 0 \leq h_i(x) \wedge \bigwedge\!\!\!\bigwedge_{i\in\Omega'_{\mathfrak{m}}} h_i(x) \leq 1.$$

$R(\mathfrak{m})^h \models \exists x(\varphi_0(x) \wedge \varphi_{\mathfrak{m}}(x))$ ($x = a'$ convient) or $A^h_{\mathfrak{m}} \leq_{\exists} R(\mathfrak{m})^h$ donc il existe $x_{\mathfrak{m}} \in (A^h_{\mathfrak{m}})^n$ tel que $A^h_{\mathfrak{m}} \models \varphi_0(x_{\mathfrak{m}}) \wedge \varphi_{\mathfrak{m}}(x_{\mathfrak{m}})$. Alors $f(x_{\mathfrak{m}}) = 0$ et $f_0(x_{\mathfrak{m}}) \neq 0$ donc $x_{\mathfrak{m}} \in V^\circ(A^h_{\mathfrak{m}})$ (car par construction f_0 est divisible par un déterminant Δ de taille $n - \dim V$ extrait du Jacobien de f), et par définition de $\Omega_{\mathfrak{m}}$:

$$\forall i \in [\![1, N]\!], \quad h_i(x_{\mathfrak{m}}) \in m(A^h_{\mathfrak{m}}) \iff h_i(a') \in m(R(\mathfrak{m})) \iff i \in \Omega_{\mathfrak{m}}. \qquad (1)$$

• La proposition I.4.3, de densité locale nous donne pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ un point $y_{\mathfrak{m}} \in V^\circ(A)$ tel que $|x_{\mathfrak{m}} - y_{\mathfrak{m}}|_{\mathfrak{m}} < 1$ et $f_0(x_{\mathfrak{m}})$ et les $p_i(x_{\mathfrak{m}})$ soient non nuls ($1 \leq i \leq s$).

Pour tout $i \in [\![1,N]\!]$ on aura $|h_i(x_\mathfrak{m}) - h_i(y_\mathfrak{m})|_\mathfrak{m} \leq |x_\mathfrak{m} - y_\mathfrak{m}|_\mathfrak{m} < 1$, (la première inégalité venant de la formule de Taylor) et donc $h_i(y_\mathfrak{m}) \in \mathfrak{m} \iff h_i(x_\mathfrak{m}) \in m(A^h_\mathfrak{m})$. Quitte à remplacer les $x_\mathfrak{m}$ par les $y_\mathfrak{m}$, on voit donc qu'on peut supposer tous les $x_\mathfrak{m}$ dans A.

Soit $\mathfrak{n} \in \mathrm{Spm}(A)$; l'ensemble $\mathcal{N}_\mathfrak{n} := \{\mathfrak{m} \in \mathrm{Spm}(A) \ / \ A_\mathfrak{m} \models \varphi_\mathfrak{n}(x_\mathfrak{n})\}$ est constructible et contient $\mathfrak{n}$, donc on peut trouver $\alpha_\mathfrak{n} \in \mathfrak{n} \setminus \{0\}$ tel que $M(\alpha_\mathfrak{n}) \subseteq \mathcal{N}_\mathfrak{n}$. Par définition de $\varphi_\mathfrak{n}$ pour tout $\mathfrak{m} \in M(\alpha_\mathfrak{n})$ on a :

$$\forall i \in [\![1,N]\!], \quad h_i(x_\mathfrak{n}) \in \mathfrak{n} \iff i \in \Omega_\mathfrak{n} = \Omega_\mathfrak{m} \iff h_i(x_\mathfrak{m}) \in \mathfrak{m}. \tag{2}$$

(Comme $\mathfrak{m} \in M(\alpha_\mathfrak{n}) \subseteq \mathcal{N}_\mathfrak{n}$, $A_\mathfrak{m} \models \varphi_\mathfrak{n}(x_\mathfrak{n})$ et c'est ce qui entraîne que $\Omega_\mathfrak{n} = \Omega_\mathfrak{m}$.)

• $\forall k \in [\![1,p]\!], \forall i \in [\![1,l'_k]\!]$, $g'_{k,i}(a') \notin I'_k$, donc $\exists \mathfrak{m} \in M(I_k)$ tel que $g'_{k,i}(a') \notin m(R(\mathfrak{m}))$ *i.e.* tel que $g'_{k,i}(x_\mathfrak{m}) \notin m(A^h_\mathfrak{m})$.

$\forall i \in [\![1,s']\!]$, $\exists \mathfrak{m} \in \mathrm{Spm}(A)$ tel que $p'_i(a') \in m(R(\mathfrak{m}))$ et $q'_i(a') \notin m(R(\mathfrak{m}))$, *i.e.* $p'_i(a') \in m(A^h_\mathfrak{m})$ et $q'_i(a') \notin m(A^h_\mathfrak{m})$.

La satisfaction de ces conditions fait intervenir un ensemble fini $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_t\}$ d'idéaux maximaux de A. Soit α un élément non nul de $\mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t \cap I_1 \cap \ldots \cap I_r$, et $x_0 \in \{x_\mathfrak{m} \ / \ \mathfrak{m} \in \mathrm{Spm}(A)\}$; les $p_i(x_0)$ sont tous non nuls $(1 \leq i \leq r)$ donc quitte à multiplier α par leur produit on peut supposer que $p_0(x_0) \leq \alpha$ (où $p_0 := p_1 \times \ldots \times p_s$).

Soit $\overline{x} \in \mathcal{C}(A)$ construit à partir de ces données à l'aide du lemme 2. Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ on a $\overline{x}(A_\mathfrak{m}) \in \{x_\mathfrak{n} \ / \ \mathfrak{n} \in M(\alpha)\} \cup \{x_0\}$ donc $\overline{x}(A_\mathfrak{m}) \in V^\circ(A)$ *i.e.* $\overline{x} \in V^\circ(\mathcal{C}(W_A))$. De plus si $\mathfrak{m} \in M(\alpha)$ alors $p_0(\overline{x}(A_\mathfrak{m}) \leq_{A_\mathfrak{m}} 0 \leq_{A_\mathfrak{m}} \alpha$ et sinon $p_0(\overline{x}(A_\mathfrak{m})) = p_0(x_0) \leq \alpha$ donc dans tous les cas $p_0(\overline{x}(A_\mathfrak{m})) \leq_{A_\mathfrak{m}} \alpha$.

Le corollaire 1.2 nous donne un point $a \in V^\circ(A)$ tel que $p_0(a) \leq_A \alpha$ et $|a - \overline{x}|_{W_A} \leq |\alpha|_{W_A}$, et quitte à approcher $\overline{x}$ suffisamment on peut en outre exiger que $f_0(a) \neq 0$. Pour tout $\mathfrak{m} \in M(\alpha)$ on a $|a - \overline{x}(A_\mathfrak{m})|_\mathfrak{m} < 1$ donc $|h_i(a) - h_i(\overline{x}(A_\mathfrak{m}))|_\mathfrak{m} < 1$ $(1 \leq i \leq N)$ d'où :

$$\forall i \in [\![1,N]\!], \quad h_i(a) \in \mathfrak{m} \iff h_i(\overline{x}(A_\mathfrak{m})) \in \mathfrak{m}. \tag{3}$$

• Il ne reste qu'à vérifier que a a bien les propriétés voulues, c'est-à-dire que $A \models \varphi(a)$.

– $a \in V(A)$ et $f_0(a) \neq 0$, donc $A \models \varphi_0(a)$.

– Soit $i \in [\![1,s]\!]$ et $\mathfrak{m} \in M(p_i(a))$. On a $p_i(a) \leq p_0(a) \leq \alpha$, donc $\mathfrak{m} \in M(\alpha)$; soit $\mathfrak{n} \in \mathrm{Spm}(A)$ tel que $\overline{x}(A_\mathfrak{m}) = x_\mathfrak{n}$ et $\mathfrak{m} \in M(\alpha_\mathfrak{n})$. D'après (3) on a $p_i(x_\mathfrak{n}) = p_i(\overline{x}(A_\mathfrak{m})) \in \mathfrak{m}$ donc d'après (2) $p_i(x_\mathfrak{n}) \in \mathfrak{n}$. Il s'ensuit d'après (1) que $p_i(a') \in m(R(\mathfrak{n}))$, et puisque $p_i(a') \leq' q_i(a')$ il vient $q_i(a') \in m(R(\mathfrak{n}))$ d'où d'après (1) $q_i(x_\mathfrak{n}) \in \mathfrak{n}$ et d'après (2) $q_i(\overline{x}(A_\mathfrak{m})) = q_i(x_\mathfrak{n}) \in \mathfrak{m}$. Enfin d'après (3) il vient $q_i(a) \in \mathfrak{m}$, et ceci valant pour tout $\mathfrak{m} \in M(p_i(a))$ on a donc $p_i(a) \leq_A q_i(a)$, pour tout $i \in [\![1,s]\!]$, *i.e.* $A \models \varphi^+_{rad}(a)$.

– Soit $k \in [\![1,r]\!]$, $i \in [\![1,l_k]\!]$ et $\mathfrak{m} \in M(I_k)$. Par construction de $\overline{x}$ il existe $\mathfrak{n} \in M(I_k)$ tel que $\mathfrak{m} \in M(\alpha_\mathfrak{n})$ et $x(A_\mathfrak{m}) = x_\mathfrak{n}$. Comme $\mathfrak{m} \in M(\alpha_\mathfrak{n})$ on a $A_\mathfrak{m} \models \varphi_\mathfrak{n}(x_\mathfrak{n})$, et comme $\mathfrak{n} \in M(I_k)$ on sait que $g_{i,k}(a') \in m(R(\mathfrak{n}))$ donc $\varphi_\mathfrak{n}(x)$ implique $0 \leq g_{i,k}(x)$. Il s'ensuit que $g_{i,k}(\overline{x}(A_\mathfrak{m})) = g_{i,k}(x_\mathfrak{n}) \in m(A_\mathfrak{m})$ et puisque $\mathfrak{m} \in M(I_k) \subseteq M(\alpha)$ (3) entraine que $g_{i,k}(a) \in \mathfrak{m}$. Ceci montre que $g_{i,k}(a) \in \cap M(I_k) = I_k$ (la dernière égalité venant du fait que I_k est r-clos et non nul) et puisque c'est vrai pour tout $k \in [\![1,r]\!]$ on a bien $A \models \varphi^+_k(a)$.

– Enfin quel que soit $j \in [\![1,t]\!]$ on a $\overline{x}(A_\mathfrak{m}) = x_{\mathfrak{m}_j}$ et $\alpha \in \mathfrak{m}_j$ donc quel que soit $i \in [\![1,N]\!]$ $h_i(a) \in \mathfrak{m}_j \iff h_i(x_{\mathfrak{m}_j}) \in \mathfrak{m}_j \iff h_i(a') \in m(R(\mathfrak{m}_j))$. Quel que soit $i \in [\![1,s']\!]$ il existe par construction $j \in [\![1,r]\!]$ tel que $p'_i(a') \in m(R(\mathfrak{m}_j))$ et $q'_i(a') \notin m(R(\mathfrak{m}_j))$, donc tel que $p'_i(a) \in \mathfrak{m}_j$ et $q'_i(a) \notin \mathfrak{m}_j$, *i.e.* $p'_i(a) \not\leq_A q'_i(a)$, et

on a bien $A \models \varphi^-_{rad}(a)$. De même, quel que soient $k \in [\![1, r]\!]$ et $i \in [\![1, l'_k]\!]$ il existe $j \in [\![1, t]\!]$ tel que $\mathfrak{m}_j \in M(I_k)$ et $g'_{k,i}(a') \notin m(R(\mathfrak{m}_j))$ donc tel que $g'_{k,i}(a) \notin \mathfrak{m}_j$, et puisque $I_k = \cap M(I_k)$ il s'ensuit que $g'_{k,i}(a) \notin I_k$ et on a bien $A \models \varphi^-_k(a)$.
∎

§4. LGPH et LGP de Prestel et Schmid

Notations: Rappelons que, pour tout anneau de valuation R sur un corps K, je note R^s l'unique prolongement de R^h à la clôture séparable K^s de K, et R^a son prolongement à la clôture algébrique K^a de K.

La proposition 3.3 bien que peu algébrique dans sa forme contient en puissance des versions affinées du LGPH faisant intervenir des conditions algébriques auxiliaires sur les points des variétés auxquelles on l'applique. Un exemple en est donné par le LGP de Prestel et Schmid introduit dans [P-S 90] et [P-S 91] afin d'axiomatiser la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$ et dans $\mathbb{R}$.

Définition
Un r-anneau intègre $(A, \leq)$ satisfait le **LGP de Prestel et Schmid** si pour tous $f_1, \ldots, f_m$, g, $p_1, \ldots, p_s$, $q_1, \ldots, q_s \in A[X_1, \ldots, X_n]$ tels que :
- les f_i forment un système absolument réduit d'équations d'une variété V ;
- V possède un point lisse dans K n'annulant pas g ;
- pour tout $\mathfrak{p} \in \mathrm{Sp}(A, \leq) \setminus \{(0)\}$, il existe un anneau de valuation R sur $\mathrm{Fr}(A)$ dominant $A_\mathfrak{p}$ tel que V possède un point lisse $x_\mathfrak{p}$ dans R^a vérifiant $g(x_\mathfrak{p}) \neq 0$ et pour tout $i \in [\![1, s]\!]$, $0 \neq p_i(x_\mathfrak{p}) \leq_{R^a} q_i(x_\mathfrak{p})$;

on a (en conséquence) un point lisse a de V dans A, tel que $g(a) \neq 0$ et pour tout $i \in [\![1, s]\!]$, $0 \neq p_i(a) \leq q_i(a)$.

Remarques:
(1) Le principe local-global de Prestel et Schmid est indépendant de la présence ou non de l'idéal nul dans le spectre r-clos : on n'y considère que les éléments de $\mathrm{Sp}(A, \leq) \setminus \{(0)\}$, et dans les conditions de la forme $a \leq b$, on suppose toujours $a \neq 0$. Il s'ensuit que pour un r-domaine quelconque $(A, \leq)$, si on note $\leq_0$ (resp. $\leq_1$) la relation radicale définie par $\mathrm{Sp}(A, \leq) \cup \{(0)\}$ (resp. $\mathrm{Sp}(A, \leq) \setminus \{(0)\}$) alors $(A, \leq_0)$ satisfait le principe local-global de Prestel-Schmid si et seulement si $(A, \leq_1)$ le satisfait.
(2) Si $(A, \leq)$ satisfait le LGP de Prestel-Schmid, la preuve du lemme 3.5 de [P-S 90] s'adapte sans problème pour montrer que $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq) \subseteq \mathrm{Spm}(A) \cup \{0\}$.

De ces deux remarques il suit qu'un r-domaine $(A, \leq)$ satisfait le LGP de Prestel et Schmid si et seulement si A le satisfait et $\leq$ est la relation radicale définie par $\mathrm{Spm}(A)$ ou par $\mathrm{Spm}(A) \cup \{0\}$. Nous perdons donc rien à ne considérer que les anneaux (et non les r-anneaux) satisfaisant le LGP de Prestel et Schmid (*i.e.* tels que $(A, \leq_A)$ le satisfait).

Il est commode d'introduire les définitions suivantes :

Définitions
Soit A un anneau intègre, de corps des fractions K.
(1) A satisfait le **LGPS** (resp. **LGPS'**) si et seulement si :
(LGPS1) $\forall a \in A \setminus \{0\}$, $M(a)^c$ est quasi-compact.

(LGPS2) (resp. **LGPS2bis**) Pour toute variété non vide V définie sur K on a :

$$V^\circ(A) \neq \emptyset \iff \forall R \in W_A,\ V^\circ(R^s) \neq \emptyset \text{ (resp. et } V^\circ(K) \neq \emptyset).$$

(2) A satisfait le **LGPA** (resp. **LGPA'**) si et seulement si :
(LGPA1) $\forall a \in A \setminus \{0\},\ M(a)^c$ est quasi-compact.
(LGPA2) (resp. **LGPA2bis**) Pour toute variété non vide V définie sur K on a :

$$V^\circ(A) \neq \emptyset \iff \forall R \in W_A, V^\circ(R^a) \neq \emptyset \text{ (resp. et } V^\circ(K) \neq \emptyset).$$

Lemme 1
Soit A un anneau intègre, de corps des fractions K. Si A satisfait le LGPS 2bis, alors pour tout $R \in W_A$, on a $R^h = R^s$.

Preuve: Il suffit de montrer que tout polynôme $f \in R[X]$, unitaire, séparable sur K, possède une racine dans R^h, pour tout $R \in W_A$. Soit donc f un tel polynôme, et $R_0 \in W_A$ fixé.

Soit $\varepsilon \in A \setminus \{0\}$; le polynôme $f(X) - \varepsilon Y$ est absolument irréductible, et absolument réduit. La variété V associée est donc définie sur K. Il est clair qu'elle est lisse.
- $(1, f(1)/\varepsilon) \in V(\mathrm{Fr}(A))$.
- Pour tout $R \in W_A$, f possède un zéro x_R dans R^s, donc $(x_R, 0) \in V(R^s)$.

Le LGPS 2bis donne $(a, b) \in V(A)$, et l'on a donc $|f(a)|_R = |\varepsilon b|_R \leq |\varepsilon|_R$. Ceci étant valable pour tout ε, on voit que 0 est adhérent à $f[A]$, et *a fortiori* à $f[R^h]$, ce qui entraîne (on sait que f séparable $\Longrightarrow$ $f[R^h]$ fermé) que $0 \in f[R^h]$, *i.e.* f a un zéro dans R^h.

■

Lemme 2
Soit R un anneau de valuation, alors pour toute variété non vide V définie sur $\mathrm{Fr}(R)$ *on a :* $V^\circ(R^s) \neq \emptyset \iff V^\circ(R^a) \neq \emptyset$.

Preuve: Seule l'implication de droite à gauche est non triviale. Quitte à remplacer, on peut supposer que $R = R^s$, *i.e.* que $F := \mathrm{Fr}(R)$ est séparablement clos.

Soit V une variété de dimension d, définie sur F, ayant un point x^a dans R^a. Si $d = 0$, la variété est réduite à un point, qui est dans F puisque V est définie sur F, *i.e.* $x^a \subseteq F \cap R^a = R$, et il n'y a plus rien à montrer. On peut donc supposer $d \geq 1$.

Soit $(\overline{F}, \overline{R})$ une ultra-puissance non triviale de (F^a, R^a). Le TFI nous donne un point $x \in V(\overline{R})$, générique de V sur F ; $R' := \overline{R} \cap F[x]$ est un prolongement de R à $F' := F[x]$, qui est isomorphe à $F[V]$, donc est une extension régulière de F.

On sait que (F, R) est existentiellement clos dans toute extension régulière (cela resulte, par exemple, du théorème énoncé page 4 de [De]), et en particulier dans (F', R'), et donc $V^\circ(R) \neq \emptyset$ (car cela se dit au premier ordre par une formule existentielle vérifiée dans (F', R') par le point générique, comme nous l'avons déja vu).

■

Proposition 3
Pour un anneau intègre A les assertions suivantes sont équivalentes :
(i) *A satisfait le LGPA 2 (resp. LGPA 2bis),*
(ii) *A satisfait le LGPS 2 (resp. LGPS 2bis),*
(iii) *A satisfait le LGPH 2 (resp. LGPH 2bis) et $\forall R \in W_A$, $R^h = R^s$.*

Preuve:
(i)$\Longrightarrow$(ii) C'est trivial.
(ii)$\Longrightarrow$(iii) C'est le lemme 1.
(iii)$\Longrightarrow$(i) C'est le lemme 2.
∎

Proposition 4
Soit A un anneau intègre, de corps des fractions K. Les assertions suivantes sont équivalentes :
(i) *A satisfait le LGP de Prestel et Schmid ;*
(ii) *A satisfait le* LGPA'.

Preuve:
(i)$\Longrightarrow$(ii) On a rappelé dans la remarque suivant la définition du LGP de Prestel-Schmid que si $(A,\leq)$ le satisfait alors $\mathrm{Sp}(A,\leq)\setminus\{(0)\} = \mathrm{Spm}(A)$, donc l'ensemble des anneaux de valuation R de K tels que $m(R)\cap A \in \mathrm{Sp}(A,\leq)\setminus\{(0)\}$ n'est autre que W_A, et LGPA 2bis est exactement le LGP de Prestel-Schmid sans les conditions radicales.

Il reste donc seulement à controler que tout a non nul appartenant à A vérifie que $M(a)^c$ est quasi-compact. Pour cela il suffit de montrer que quel que soit $b \in A\setminus\{0\}$, $M(a)^c \cap M(b)$ est quasi-compact. On applique le LGP de Prestel-Schmid à la variété V définie sur $\mathrm{Fr}(A)$ par $(B_1B_2 - b, B_1U_1 + aU_2 - 1)$ avec la condition radicale $0 \neq B_2 \leq a$. Cela nous donne $b_1, b_2, u_1, u_2 \in B$ tels que :
(a) $b_1b_2 = b$ donc $M(b_1)\cup M(b_2) = M(b)$;
(b) $b_1u_1 + au_2 = 1$ donc $M(b_1)\cap M(a) = \emptyset$, *i.e.* $M(b_1) \subseteq M(b)\setminus M(a)$;
(c) $b_2 \leq a$ donc $M(b_2) \subseteq M(a)$.
(a), (b) et (c) entraînent que $M(b_1) = M(b)\setminus M(a)$ et $M(b_2) = M(b)\cap M(a)$. En particulier $M(a)^c \cap M(b) = M(b_1)$ est bien une partie quasi-compacte de $\mathrm{Spm}(A)$.

(ii)$\Longrightarrow$(i) La preuve est la même que celle de 3.3 (v*), p. 188 de [P-S 90].

Soit V une variété définie sur K, et $f = (f_1,\ldots,f_m) \in A[X]^m$ ($X = (X_1,\ldots,X_n)$) un système absolument réduit d'équations de V. Soient g, $p_1,\ldots,p_s$, $q_1,\ldots,q_s \in A[X]$, et supposons que pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$ il existe $x_\mathfrak{m} \in V^\circ(A^a_\mathfrak{m})$ tel que $g(x_\mathfrak{m}) \neq 0$ et quel que soit $i \in [\![1,s]\!]$, $0 \neq p_i(x_\mathfrak{m}) \leq_{A^a_\mathfrak{m}} q_i(x_\mathfrak{m})$.

Quel que soit $\mathfrak{m} \in \mathrm{Spm}(A)$, soit $R(\mathfrak{m})$ une extension élémentaire de $A^a_\mathfrak{m}$, de degré de transcendance infini sur K. Le TFI donne dans $R(\mathfrak{m})$ un point générique $\theta_\mathfrak{m}$ de V sur K^a, que l'on peut prendre assez proche de $x_\mathfrak{m}$ pour que $p_i(\theta_\mathfrak{m}) \leq_{R(\mathfrak{m})} q_i(\theta_\mathfrak{m})$. Comme g et les p_i n'appartiennent pas à $I(V)$ (ils de s'annulent pas en $x_\mathfrak{m}$), $g(\theta_\mathfrak{m})$ et les $p_i(\theta_\mathfrak{m})$ sont non nuls. Les $K(\theta_\mathfrak{m})$ sont tous K-isomorphes, on peut donc les identifier et munir ainsi $K(\theta)$ (où θ est l'un quelconque des $\theta_\mathfrak{m}$) de la famille $W' := \{R(\mathfrak{m})\cap A \,/\, \mathfrak{m} \in \mathrm{Spm}(A)\}$. Soit $A' := \cap W'$, $\mathcal{P}' := \{m(R')\cap A' \,/\, R' \in W'\}$ et $\leq'$ est la relation radicale définie par $\mathcal{P}'\cup\{(0)\}$ si $(A,\leq_A)$ est un r_o-domaine et par $\mathcal{P}'$ sinon. Puisque V est définie sur K, l'extension $K(\theta)|K$ est régulière et la proposition 3.3 s'applique : $(A,\leq_A) \leq_\exists (A',\leq')$.

De plus quel que soit $i \in [\![1,s]\!]$ on a $0 \neq p_i(\theta) \leq_{\mathcal{P}'} q_i(\theta)$ donc $p_i(\theta) \leq' q_i(\theta)$. Soit Δ un déterminant de taille $n - \dim V$ extrait du Jacobien de f tel que $\Delta(\theta) \neq 0$, on a :

$$(A',\leq') \models \exists x\big(f(x) = 0 \wedge \Delta(x) \neq 0 \wedge g(x) \neq 0 \wedge \bigwedge_{i=1}^{s} 0 \neq p_i(x) \leq q_i(x)\big)$$

Cette formule existentielle à paramètres dans A est aussi satisfaite dans $(A,\leq_A)$ donc il existe $a \in A^n$ tel que $f(a) = 0$ et $\Delta(a) \neq 0$ *i.e.* $a \in V^\circ(A)$, $g(a) \neq 0$ et quel que soit

$i \in [\![1, r]\!],\ 0 \neq p_i(a) \leq_A q_i(a)$.

■

Chapitre IV
Anneaux PAC, PRC, PC_M

Résumé : Le LGP de Prestel et Schmid s'est avéré suffisant pour beaucoup d'applications, et nécessite un formalisme moins contraignant que le LGPH, car moins général. Nous avons donc préféré présenter dans ce chapitre les applications pour lesquelles le LGP de Prestel et Schmid était suffisant, et réserver au suivant celles pour lesquelles le LGPH était vraiment nécessaire.

Nous introduisons trois classes de r-domaines, inspirées des exemples traditionnels d'études modèle-théoriques de corps. Nous vérifions que toute l'information contenue dans ces structures, du point de vue de la logique, peut être ramenée à celle de leurs corps des fractions et de leurs treillis résiduels. En plus de retrouver les résultats de van den Dries-Macintyre et de Prestel-Schmid, nous obtenons ainsi la décidabilité de divers sous-anneaux de la clôture absolument réelle de $\mathbb{Q}$ et de la clôture séparable de $\mathbb{F}_p(T)$, et nous ramenons la décidabilité de l'anneau des entiers algébriques absolument p-adiques à celle de son corps des fractions. Une application purement algébrique est également donnée à la fin.

§ 1. Définitions, CDM-représentations

Définitions

Un anneau A sera dit **pseudo algébriquement clos**, (en abrégé **PAC**) s'il satisfait le LGPA.
Il sera dit **pseudo réel clos** (en abrégé **PRC**) s'il satisfait le LGPA' (*i.e.* le LGP de Prestel et Schmid) et si son corps des fractions est PRC (au sens usuel, rappelé au I.1).
Enfin il sera dit $\mathbf{PC}_M$ s'il satisfait le LGPA' et si son corps des fractions est PC_M au sens usuel.

Remarques:

(1) Ces définitions sont compatibles avec les notions usuelles, puisque si A est un corps il est PAC (resp. PRC, PC_M) au sens ci-dessus si et seulement s'il est PAC (resp. PRC, PC_M) au sens des corps.

(2) De même que pour les corps, les anneaux PAC sont donc un cas particulier des anneaux PRC ou PC_M : celui où le corps des fractions ne possède ni ordre ni valuation p-adique de rang d pour tout $(p,d) \in M$. Réciproquement un corps PRC (resp. PC_M) s'il n'est pas PAC est ordonnable (resp. possède une p-valuation de rang d pour un certain $(p,d) \in M$) et donc est de caractéristique nulle.

Nous dirons pourtant fréquemment : *"soit A un anneau PRC ou PC_M parfait"*.

L'hypothèse de perfection n'est ajoutée que pour englober dans un même énoncé les PRC et les PC_M "stricts" d'une part (ceux qui ne sont pas PAC et sont donc de caractéristique nulle), et les PAC parfaits de caractéristique quelconque d'autre part.

Définition
Un r-domaine sera dit PAC (resp. PRC, PC_M) s'il est de la forme $(A, \leq_A)$ où A est PAC (resp. PRC, PC_M).

Proposition 1
La classe des anneaux PAC (resp. PRC, PC_M) est récursivement axiomatisable dans le langage des anneaux. De même la classe des r-domaines PAC (resp. PRC, PC_M) l'est-elle dans le langage des r-anneaux.

Preuve: Prestel et Schmid ont donné un schéma d'axiomes pour le LGPA' (on peut d'ailleurs facilement en construire un autre à partir de celui que nous avons donné pour le LGPH') et on sait que la classe des corps PAC (resp. PRC) est récursivement axiomatisable. L'axiomatisabilité des anneaux PAC (resp. PRC) en découle immédiatement.

Pour en déduire la seconde affirmation, il suffit d'axiomatiser "la relation radicale est celle définie par le spectre maximal", ce qui se dit dans $\mathrm{L}_{\mathrm{rad}}$ par la formule :

$$a \leq b \quad \Longleftrightarrow \quad \forall c((b,c) = 1 \rightarrow (a,c) = 1)$$

où l'expression "$(x,y) = 1$" abrège la formule "$\exists u \exists v(ux + vy = 1)$" comme nous l'avons vu à la fin des prérequis.

■

CDM-représentation

Notations: Je note $G(K)$ le groupe de Galois absolu d'un corps K, c'est-à-dire le groupe de Galois de l'extension $K^s|K$.

La notion de "CDM-représentation", issue de [CDM], joue un rôle crucial dans l'étude modèle-théorique des corps PAC, PRC et PC_M. Rappelons brièvement ses principales propriétés, telles qu'elles sont exposées dans [E 84] par exemple.

Il existe une classe élémentaire Σ de structures, dans un langage multi-sorte $\mathcal{L}$, et une correspondance bijective, notée Φ, entre les éléments de cette classe et les groupes profinis, telle que :

- pour toute formule close $\varphi_{\mathcal{L}}$ de $\mathcal{L}$ il existe une formule close φ_{ann} du langage des anneaux telle qu'un corps K satisfait φ_{ann} si et seulement si $\Phi G(K)$ satisfait $\varphi_{\mathcal{L}}$;
- si un corps K est κ-saturé, alors $\Phi G(K)$ est κ-saturé ;
- tout épimorphisme $\psi : G \longrightarrow H$ de groupes profinis induit un plongement $\Phi\psi$ de ΦH dans ΦG, et réciproquement.

Si K est séparablement clos dans L, l'homomorphisme ρ de restriction de $G(L)$ sur $G(K)$ induit un plongement $\Phi\rho$ de $\Phi G(K)$ dans $\Phi G(L)$.

On notera plus simplement $(\Phi G(L), K)$ la structure $(\Phi G(L), \Phi\rho[\Phi G(K)])$.
Soient K_1, K_2 deux extensions régulières d'un même corps K, on a :

$$(K_1, K) \equiv (K_2, K) \quad \Longrightarrow \quad (\Phi G(K_1), K) \equiv (\Phi G(K_2), K).$$

L'intérêt de la notion de CDM-représentation vient de ce que si K_1 et K_2 sont tous les deux PAC (resp. PRC, PC_M) et de même degré d'imperfection alors l'implication réciproque est vraie aussi (rappellons que le degré d'imperfection d'un corps F est nul si ce corps est parfait, vaut p^n si F admet une p-base de n vecteurs, et est infini sinon).

Remarque: Nous n'avons trouvé nulle part de démonstration de ces théorèmes pour les corps PC_M en général, mais ils sont admis par tout le monde ; le lecteur sceptique pourra s'il le souhaite restreindre au seul cas PpC les résultats que nous énonçons pour les PC_M.

Lemme 2
Soient K' et K'' deux extensions régulières d'un même corps K. L'anneau $K' \otimes_K K''$ étant intègre, on peut plonger tous ces corps dans une clôture algébrique Ω de $\mathrm{Fr}(K' \otimes_K K'')$. Dans Ω, le composé $K'^s K''^s \simeq \mathrm{Fr}(K'^s \otimes_{K^s} K''^s)$ est une extension galoisienne de $K'K''$, dont le groupe de Galois est isomorphe à $G(K') \times_{G(K)} G(K'')$. On suppose qu'il existe un épimorphisme $\pi : G(K'') \longrightarrow G(K')$ commutant avec la restriction. Soit $G := \{\langle \pi(\tau), \tau \rangle \ / \ \tau \in G(K'')\}$, et $K^\circ := (K'^s K''^s)^G$ l'extension de $K'K''$ formée des éléments de $K'^s K''^s$ laissés fixes par tous les éléments de G.
(1) Alors pour toute extension algébrique séparable F'' de K'' telle que $F''K^s = F''^s$, il existe une extension algébrique séparable F' de K' telle que $F' \cap K^a = F'' \cap K^a$ et $G(F'') \simeq G(F') \simeq G(F)$ (en posant $F := F'' \cap K^a$).
(2) Si K'' est régulièrement clos relativement à une famille $\mathcal{F}$ de clôtures p-adiques et de clôtures réelles, alors il s'ensuit que $K'' \leq_\exists R^\circ$.

Preuve: La première partie de la conclusion est une simple remarque : comme $F''K^s = F''^s$ l'épimorphisme de restriction de $G(F'')$ sur $G(F)$ est injectif. De même la restriction de π à $G(F'')$ est injective donc il suffit de prendre $F' := K'^{\pi[G(F'')]}$.

Pour prouver la seconde partie, on commence par remarquer que si K'' est PAC, $K'' \leq_\exists K^\circ$ résulte simplement du fait que l'extension $K^\circ | K''$ est régulière. Nous pouvons donc écarter ce cas, et en particulier supposer qu'on est en caractéristique nulle, donc que tous les corps sont parfaits.

Soit $\mathcal{F}$ la famille d'extensions algébriques de K'', réelles closes ou p-adiquement closes, relativement à laquelle K'' est régulièrement clos. Pour tout $F'' \in \mathcal{F}$ on a $F''^a = F''\mathbb{Q}^a = F''K^a$; soient donc F' et F les corps donnés par la première partie.

- Si F'' est réel clos, $G(F'') = G(F') = G(F) = \mathbb{Z}/2\mathbb{Z}$, donc F et F' sont réel clos, d'où $F \preceq F'$ et $F \preceq F''$.
- Si F'' est p-adiquement clos, comme $G(F'') = G(F') = G(F)$ [K 95] nous assure de même que F' et F sont p-adiquement clos. De plus $F'' \cap \mathbb{Q}^a = F' \cap \mathbb{Q}^a$ donc $F \equiv F''$ et le plongement de F dans F'' est élémentaire (tout cela est particulier aux corps p-adiques, pour lesquels nous renvoyons à [P-R]) . Le même argument vaut pour F' donc $F \preceq F'$.

On sait amalgamer de façon linéairement disjointe deux extensions élémentaires d'un même corps dans une extension élémentaire commune, donc dans les deux cas ci-dessus $F'' \leq_\exists \mathrm{Fr}(F' \otimes_F F'') \simeq F'F''$. Pour tout $\sigma \in Gal(K'^a K''^a | F'F'')$ on a $(\pi(\sigma_{|K''^a}))_{|K^a} = (\sigma_{|K'^a})_{|K^a}$ or l'opération de restriction de $G(F')$ dans $G(F)$ est injective et $\pi(\sigma_{|K''^a}) \in G(F')$. Il s'ensuit que $\pi(\sigma_{|K''^a}) = \sigma_{|K'^a}$ *i.e.* $\sigma = \langle \pi(\sigma_{|K''^a}), \sigma_{|K''^a} \rangle$ et donc $\sigma \in G$. Ceci valant pour tout élément de $Gal(K'^a K''^a | F'F'')$ on en déduit que $K^\circ \subseteq F'F''$ et donc :

$$F'' \subseteq F''K^\circ \subseteq F'F'' \quad \Longrightarrow \quad F'' \leq_\exists F''K^\circ.$$

Ceci vaut pour tout $F'' \in \mathcal{F}$, et comme par hypothèse $K'' \in \mathrm{RC}(\mathcal{F})$ il s'ensuit que $K'' \leq_{\exists} K^{\circ}$.

■

§ 2. Morphismes de r-anneaux

On considère dans ce paragraphe certains aspects fonctoriels de la notion de relation radicale, et plus particulièrement le type de contrainte qu'apporte cette relation sur les morphismes.

Définition
Un **morphisme** $\varphi : (A, \leq) \longrightarrow (A', \leq')$ entre deux r-anneaux est un morphisme d'anneaux vérifiant, pour tous a, b dans A : $a \leq b \Longrightarrow \varphi(a) \leq' \varphi(b)$.

Propriété 1
Soient $(A, \leq)$ et $(A', \leq')$ deux r-anneaux, et soit $\varphi : A \longrightarrow A'$ un morphisme d'anneaux ; alors sont équivalents :
(i) *φ est un morphisme de r-anneaux de $(A, \leq)$ dans $(A', \leq')$;*
(ii) $\forall \mathfrak{p}' \in \mathrm{Sp}(A', \leq')$, $\varphi^{-1}[\mathfrak{p}'] \in \mathrm{Sp}(A, \leq)$;
(iii) *il existe une partie $\mathcal{P}'$ de $\mathrm{Sp}(A')$ telle que $\leq' = \leq_{\mathcal{P}'}$ et $\forall \mathfrak{p}' \in \mathcal{P}'$, $\varphi^{-1}[\mathfrak{p}'] \in \mathrm{Sp}(A, \leq)$.*

Preuve:
(i) $\Longrightarrow$ (ii) Supposons que φ soit un morphisme de r-anneaux, et soit $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$. On sait que $\varphi^{-1}[\mathfrak{p}'] \in \mathrm{Sp}(A)$ puisque φ est un morphisme d'anneaux. Il suffit donc de montrer qu'il est r-clos. Soient $a \in \varphi^{-1}[\mathfrak{p}']$ et $b \in A$, tels que $a \leq b$. Alors $\varphi(a) \leq' \varphi(b)$ et $\varphi(a) \in \mathfrak{p}'$, d'où $\varphi(b) \in \mathfrak{p}'$ et enfin $b \in \varphi^{-1}[\mathfrak{p}']$.
(ii) $\Longrightarrow$ (iii) C'est immédiat : il suffit de prendre $\mathcal{P}' := \mathrm{Sp}(A', \leq')$.
(iii) $\Longrightarrow$ (i) Soit $\mathcal{P}'$ une telle partie de $\mathrm{Sp}(A')$ et soient $a, b \in A$ tels que $a \leq b$. Pour tout $\mathfrak{p}' \in \mathcal{P}'$, si $\varphi(a) \in \mathfrak{p}'$ alors $a \in \varphi^{-1}[\mathfrak{p}']$ qui est r-clos, donc $b \in \varphi^{-1}[\mathfrak{p}']$ *i.e.* $\varphi(b) \in \mathfrak{p}'$, d'où $\varphi(a) \leq_{\mathcal{P}'} \varphi(b)$ et donc $\varphi(a) \leq' \varphi(b)$.

■

Notations: Étant donné $\varphi : (A, \leq) \longrightarrow (A', \leq')$ un morphisme de r-anneau, on considère :
– $\widehat{\varphi}$ l'application de $\mathrm{Sp}(A', \leq')$ dans $\mathrm{Sp}(A, \leq)$ définie par :

$$\forall \mathfrak{p}' \in \mathrm{Sp}(A', \leq'), \quad \widehat{\varphi}(\mathfrak{p}') := \varphi^{-1}[\mathfrak{p}'].$$

Cette application est bien à valeurs dans $\mathrm{Sp}(A, \leq)$ d'après la propriété 1.
– $\overline{\varphi}$ l'application de $\mathrm{L}(A, \leq)$ dans $\mathrm{L}(A', \leq')$ définie par :

$$\forall a \in A, \quad \overline{\varphi}(P(a)) = P(\varphi(a)).$$

Cette application est bien définie puisque si $P(a) = P(b)$ on a $a \leq b$ et $b \leq a$, donc $\varphi(a) \leq' \varphi(b)$ et $\varphi(b) \leq' \varphi(a)$, *i.e.* $P(\varphi(a)) = P(\varphi(b))$.

Propriété 2
Si $\varphi : (A, \leq) \longrightarrow (A', \leq')$ est un morphisme de r-anneaux alors l'application $\overline{\varphi}$ préserve les extrémités, l'inclusion, la réunion et s'il y a lieu l'intersection.
Si $\sigma : (A', \leq') \longrightarrow (A'', \leq'')$ est un second morphisme on a : $\overline{\sigma \circ \varphi} = \overline{\sigma} \circ \overline{\varphi}$ et $\widehat{\sigma \circ \varphi} = \widehat{\varphi} \circ \widehat{\sigma}$.

Remarque: De la première assertion ci-dessus il suit que $\overline{\varphi}$ est un morphisme de demi-treillis supérieur avec extrémités. Si de plus $(A, \leq)$ et $(A', \leq')$ sont $\cap$-stables, alors $\overline{\varphi}$ est un morphisme de treillis avec extrémités.

Preuve: Soient $a, b \in A$. Si $P(a) \subseteq P(b)$ alors $a \leq b$, donc $\varphi(a) \leq \varphi(b)$, *i.e.* $\overline{\varphi}(P(a)) = P(\varphi(a)) \subseteq P(\varphi(b)) = \overline{\varphi}(P(b))$. De même, $\overline{\varphi}(P(a) \cup P(b)) = \overline{\varphi}(P(ab)) = P(\varphi(ab)) = P(\varphi(a)\varphi(b)) = P(\varphi(a)) \cup P(\varphi(b)) = \overline{\varphi}(P(a)) \cup \overline{\varphi}(P(b))$. Enfin $P(\varphi(1)) = P(1)$ et $P(\varphi(0)) = P(0)$ donc $\overline{\varphi}$ préserve bien l'inclusion, la réunion et les extrémités.

Supposons maintenant qu'il existe $c \in A$ tel que $P(c) = P(a) \cap P(b)$. Alors $\overline{\varphi}$ étant croissante on a $\overline{\varphi}(P(c)) \subseteq \overline{\varphi}(P(a)) \cap \overline{\varphi}(P(b))$. D'autre part quel que soit $\mathfrak{p}' \in \overline{\varphi}(P(a)) \cap \overline{\varphi}(P(b))$ on a $\mathfrak{p} := \varphi^{-1}[\mathfrak{p}'] \in \mathrm{Sp}(A, \leq)$, $a \in \mathfrak{p}$ et $b \in \mathfrak{p}$ donc $c \in \mathfrak{p}$, *i.e.* $\varphi(c) \in \mathfrak{p}'$ et donc $\overline{\varphi}(P(a)) \cap \overline{\varphi}(P(b)) \subseteq P(\varphi(c)) = \overline{\varphi}(P(c))$ d'où la conclusion.

Quant à la dernière assertion, elle est immédiate.

■

Définition

Un **plongement** $\varphi : (A, \leq) \longrightarrow (A', \leq')$ entre deux r-anneaux est un plongement d'anneaux vérifiant, pour tous a, b dans A : $a \leq b \iff \varphi(a) \leq' \varphi(b)$.

Proposition 3

Soient $(A, \leq)$ et $(A', \leq')$ deux r-anneaux, φ un plongement d'anneaux de A dans A'.
(1) *S'il existe une partie $\mathcal{P}$ (resp. $\mathcal{P}'$) de $\mathrm{Sp}(A, \leq)$ (resp. $\mathrm{Sp}(A', \leq')$) définissant la relation radicale $\leq$ (resp. $\leq'$) remplissant les conditions suivantes :*
(a) $\forall \mathfrak{p}' \in \mathcal{P}',\ \mathfrak{p}' \cap A' \in \mathrm{Sp}(A, \leq_{\mathcal{P}})$;
(b) $\forall \mathfrak{p} \in \mathcal{P}, \exists \mathfrak{p}' \in \mathrm{Sp}(A', \leq_{\mathcal{P}'}),\ \widehat{\varphi}(\mathfrak{p}') = \mathfrak{p}$;
alors φ est un plongement de $(A, \leq)$ dans $(A', \leq')$.
(2) *Inversement, si φ est un plongement de r-anneaux de $(A, \leq)$ dans $(A', \leq')$, alors la relation radicale définie sur A par $\mathcal{P} := \{\widehat{\varphi}(\mathfrak{p}') \ /\ \mathfrak{p}' \in \mathrm{Sp}(A', \leq')\}$ coïncide avec $\leq$.*

Preuve:
(1) La condition (a) assure que φ est un morphisme de $(A, \leq_{\mathcal{P}})$ dans $(A', \leq_{\mathcal{P}'})$ d'après la propriété 1. Pour que ce soit un plongement il reste à vérifier que pour tous $a, b \in A$, si $a \not\leq_{\mathcal{P}} b$ alors $\varphi(a) \not\leq_{\mathcal{P}'} \varphi(b)$. Soient donc $a, b \in A$ tels que $a \not\leq_{\mathcal{P}} b$. Alors il existe $\mathfrak{p} \in \mathcal{P}$ tel que $a \in \mathfrak{p}$ et $b \notin \mathfrak{p}$. L'hypothèse (b) donne $\mathfrak{p}' \in \mathcal{P}'$ tel que $\widehat{\varphi}(\mathfrak{p}') = \varphi^{-1}[\mathfrak{p}] = \mathfrak{p}$, donc $\varphi(a) \in \mathfrak{p}'$ et $\varphi(b) \notin \mathfrak{p}'$, d'où $\varphi(a) \not\leq_{\mathcal{P}'} \varphi(b)$.

(2) Soient $a, b \in A$; on sait que $\mathcal{P} \subseteq \mathrm{Sp}(A, \leq)$ donc si $a \leq b$ on a clairement $a \leq_{\mathcal{P}} b$. Inversement supposons que $a \not\leq b$. Alors $\varphi(a) \not\leq \varphi(b)$ donc il existe $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$ tel que $\varphi(a) \in \mathfrak{p}'$ et $\varphi(b) \notin \mathfrak{p}'$. On a alors $\mathfrak{p} := \varphi^{-1}[\mathfrak{p}'] \in \mathcal{P}$, $a \in \mathfrak{p}$ et $b \notin \mathfrak{p}$, donc $a \not\leq_{\mathcal{P}} b$.

■

Corollaire 4

Soit $\varphi : (A, \leq) \longrightarrow (A', \leq')$ un plongement de r-anneaux.
Alors $\overline{\varphi}$ est un plongement de $\mathrm{L}(A, \leq)$ dans $\mathrm{L}(A', \leq')$.

Remarque: Dans ce corollaire, $\overline{\varphi}$ est un plongement au sens des demi-treillis supérieurs avec extrémités. Cependant, en vertu de la remarque précédente, si $(A, \leq)$ est $(A', \leq')$ sont $\cap$-stables alors $\overline{\varphi}$ est un plongement au sens des treillis avec extrémités.

Preuve: La propriété 2 montre qu'il suffit de vérifier que $\overline{\varphi}$ est injective, ce qui est immédiat : quels que soient $a, b \in A$ tels que $\overline{\varphi}(P(a)) = \overline{\varphi}(P(b))$, *i.e.* $P(\varphi(a)) = P(\varphi(b))$

on a $\varphi(a) \leq' \varphi(b)$ et $\varphi(b) \leq' \varphi(a)$ donc $a \leq_{\mathcal{P}} b$ et $b \leq_{\mathcal{P}} a$ où $\mathcal{P} := \{\widehat{\varphi}(\mathfrak{p}') \,/\, \mathfrak{p}' \in \mathrm{Sp}(A', \leq')\}$, d'où d'après la proposition 3 : $a \leq b$ et $b \leq a$ *i.e.* $P(a) = P(b)$.

■

Remarque: Il est facile de voir qu'en fait, si φ est un morphisme injectif de r-domaine, alors $\overline{\varphi}$ est un plongement si et seulement si φ en est un.

La proposition 3 suggère qu'un morphisme injectif φ entre deux r-domaines est un plongement si et seulement si $\widehat{\varphi}$ est surjective ; c'est malheureusement faux, nous donnerons plus loin un contre-exemple. On peut cependant énoncer un résultat partiel, suffisant pour les applications, dans le cas des r-domaines $\cap$-stables.

Définition

Étant donnés deux r-anneaux $\cap$-stables $(A, \leq)$ et $(A', \leq')$, et un morphisme σ de $\mathrm{L}(A, \leq)$ dans $\mathrm{L}(A', \leq')$ (au sens des treillis avec extrémités), on lui associe l'application $\boldsymbol{\widehat{\sigma}}$ définie par :

$$\forall \mathfrak{p}' \in \mathrm{Sp}(A', \leq'), \quad \widehat{\sigma}(\mathfrak{p}') := \{a \in A \,/\, \exists a' \in \mathfrak{p}',\ \sigma(P(a)) = P(a')\}.$$

Si φ est un morphisme de $(A, \leq)$ dans $(A', \leq')$ on peut prendre $\sigma = \overline{\varphi}$. Dans ce cas $\widehat{\sigma} = \widehat{\overline{\varphi}} = \widehat{\varphi}$, ce qui justifie les notations.

Proposition 5

Pour tout $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$, *on a :* $\quad \widehat{\sigma}(\mathfrak{p}') \in \mathrm{Sp}(A, \leq)$.

Preuve: Soient $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$ et $a, b \in A$.

– $0 \in \mathfrak{p}'$ et $\sigma(P(0)) = P(0)$ (σ préserve les extrémités) donc $0 \in \widehat{\sigma}(\mathfrak{p}')$.

– Pour tout $a' \in A'$ tel que $\sigma(P(1)) = P(a')$ on a $P(a') = P(1)$ donc $a' \notin \mathfrak{p}'$, *i.e.* $1 \notin \widehat{\sigma}(\mathfrak{p}')$.

– Si $a \in \widehat{\sigma}(\mathfrak{p}')$ et $a \leq b$, soient $a' \in \mathfrak{p}'$ et $b' \in A'$ tels que $\sigma(P(a)) = P(a')$ et $\sigma(P(b)) = P(b')$. On a $P(a) \subseteq P(b)$ donc $P(a') \subseteq P(b')$, *i.e.* $a' \leq' b'$ d'où $b' \in \mathfrak{p}'$ ce qui entraîne que b appartient à $\widehat{\sigma}(\mathfrak{p}')$ qui est donc r-clos.

– Si $b \in \widehat{\sigma}(\mathfrak{p}')$, alors $b \leq ab$ donc $ab \in \widehat{\sigma}(\mathfrak{p}')$.

– Si $a, b \in \widehat{\sigma}(\mathfrak{p}')$ soit $c \in A$ tel que $P(c) = P(a) \cap P(b)$. On a $c \leq a + b$, donc pour montrer que $a + b \in \widehat{\sigma}(\mathfrak{p}')$ il suffit de vérifier que $c \in \widehat{\sigma}(\mathfrak{p}')$. Soit $c' \in \mathfrak{p}'$ tel que $P(c') = \sigma(P(a)) \cap \sigma(P(b))$. Par hypothèse $\mathfrak{p}' \in \sigma(P(a)) \cap \sigma(P(b))$ donc $c' \in \mathfrak{p}'$. On a $\sigma(P(c)) = \sigma(P(a) \cap P(b)) = \sigma(P(a)) \cap \sigma(P(b)) = P(c')$ donc $c \in \widehat{\sigma}(\mathfrak{p}')$ et *a fortiori* $a + b \in \mathfrak{p}$.

– Si $ab \in \widehat{\sigma}(\mathfrak{p}')$, soit $c' \in \mathfrak{p}'$ tel que $\sigma(P(ab)) = P(c')$. Soient $a', b' \in A'$ tels que $\sigma(P(a)) = P(a')$ et $\sigma(P(b)) = P(b')$. On a $P(c') = \sigma(P(ab)) = \sigma(P(a)) \cup \sigma(P(b)) = P(a'b')$, donc $a'b' \in \mathfrak{p}'$. Comme $\mathfrak{p}'$ est premier il s'ensuit que a' ou b' appartient à $\mathfrak{p}'$ et donc que a ou b appartient à $\widehat{\sigma}(\mathfrak{p}')$.

■

Proposition 6

Soient $(A, \leq)$ *et* $(A', \leq')$ *deux r-anneaux* $\cap$*-stables, et* σ *un plongement de* $\mathrm{L}(A, \leq)$ *dans* $\mathrm{L}(A', \leq')$.

Alors quel que soit $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$ *maximal parmi les idéaux r-clos de* $(A, \leq)$, *il existe* $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$ *tel que* $\widehat{\sigma}(\mathfrak{p}') = \mathfrak{p}$. *En particulier, si* $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq)$ *et* $\mathrm{Spm}(A') \subseteq \mathrm{Sp}(A', \leq')$ *on a* $\mathrm{Spm}(A) \subseteq \widehat{\sigma}[\mathrm{Spm}(A')]$.

Remarque: Si φ est un plongement de $(A, \leq)$ dans $(A', \leq')$, ceci s'applique notamment à $\overline{\varphi}$ d'après le corollaire 4 et le commentaire accompagnant la définition de $\widehat{\sigma}$.

Preuve: Soit $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$ et posons $I' := \{a' \in A' \,/\, \exists a \in \mathfrak{p},\ \sigma(P(a)) \subseteq P(a')\}$. On commence par montrer que I' est un idéal r-clos propre de $(A', \leq')$.
Soient $a', b' \in A'$.

– $\sigma(P(0)) = P(0)$, donc $0 \in I'$.

– Si $a' \in I'$ et $a' \leq' b'$, alors il existe $a \in \mathfrak{p}$ tel que $\sigma(P(a)) \subseteq P(a')$. On a $P(a') \subseteq P(b')$, donc $\sigma(P(a)) \subseteq P(b')$ *i.e.* $b' \in I'$.

– Si $b' \in I'$ alors $b' \leq' a'b'$ donc $a'b' \in I'$.

– Si $a', b' \in I'$ alors il existe $a, b \in \mathfrak{p}$ tels que $\sigma(P(a)) \subseteq P(a')$ et $\sigma(P(b)) \subseteq P(b')$. Soit $c \in A$ tel que $P(c) = P(a) \cap P(b)$, comme $\mathfrak{p} \in P(a) \cap P(b)$ on a $c \in \mathfrak{p}$, et d'autre part $\sigma(P(c)) = \sigma(P(a)) \cap \sigma(P(b)) \subseteq P(a') \cap P(b') \subseteq P(a' + b')$, donc $a' + b' \in I'$.

– Enfin quel que soit $a \in \mathfrak{p}$, $P(a) \neq \emptyset$ *i.e.* $P(a) \not\subseteq P(1)$ et donc, puisque σ est strictement croissante et conserve les extrémités, $\sigma(P(a)) \not\subseteq P(1)$, d'où $1 \notin I'$.

I' étant un idéal r-clos propre de $(A', \leq')$ il se plonge dans un idéal premier r-clos $\mathfrak{p}'$ de $(A', \leq')$. On a :

$$\begin{aligned}\widehat{\sigma}(\mathfrak{p}') &\supseteq \{a \in A \,/\, \exists a' \in I',\ \sigma(P(a)) = P(a')\}\\ &\supseteq \{a \in A \,/\, \exists b \in \mathfrak{p},\ \sigma(P(b)) \subseteq \sigma(P(a))\}\\ &\supseteq \{a \in A \,/\, \exists b \in \mathfrak{p},\ b \leq a\} = \mathfrak{p}\end{aligned}$$

Comme $\widehat{\sigma}(\mathfrak{p}') \in \mathrm{Sp}(A, \leq)$, par maximalité de $\mathfrak{p}$ on en déduit que $\widehat{\sigma}(\mathfrak{p}') = \mathfrak{p}$.

Le “en particulier” en découle immédiatement : un élément quelconque $\mathfrak{m}$ de $\mathrm{Spm}(A)$ se relève *via* $\widehat{\sigma}$ en $\mathfrak{p}' \in \mathrm{Sp}(A', \leq')$, et tout idéal maximal $\mathfrak{m}'$ de A' contenant $\mathfrak{p}'$ vérifie $\widehat{\sigma}(\mathfrak{m}') = \mathfrak{m}$.

■

Exemple: Soit $A := \mathbb{C}[X]$, muni de la relation radicale $\leq$ définie par $\mathrm{Spm}(A)$. On sait que A est de Bezout et que son radical de Jacobson est nul, donc $(A, \leq)$ est $\cap$-stable et $(0) \in \mathrm{Sp}(A, \leq)$.

Pour tout $\lambda \in \mathbb{C}$, soit $\mathfrak{m}_\lambda$ (resp. $\mathfrak{n}_\lambda$) l'idéal maximal de $\mathbb{C}[X, Y]$ engendré par $X - \lambda$ et Y (resp. et $Y - 1$). Posons $\mathcal{M} := \{\mathfrak{m}_\lambda \,/\, \lambda \in \mathbb{C}\}$ et $\mathcal{N} := \{\mathfrak{n}_\lambda \,/\, \lambda \in \mathbb{C}\}$. On munit $A' := \mathbb{C}[X, Y]$ de la relation radicale $\leq'$ associée à $\mathcal{M} \cup \mathcal{N}$. Il n'est pas difficile de voir que $\mathrm{Sp}(A', \leq') = \mathcal{M} \cup \mathcal{N}$ et que $(A', \leq')$ est $\cap$-stable (en fait les éléments de $\mathrm{L}(A', \leq')$ sont de la forme $\mathcal{F}$, $\mathcal{M} \cup \mathcal{F}$, $\mathcal{N} \cup \mathcal{F}$ ou $\mathcal{M} \cup \mathcal{N}$, où $\mathcal{F}$ est une partie finie quelconque de $\mathrm{Sp}(A', \leq')$).

Quel que soit $\lambda \in \mathbb{C}$ on a $\mathfrak{m}_\lambda \cap A = \mathfrak{n}_\lambda \cap A = (X - \lambda)A \in \mathrm{Spm}(A)$ et tout élément de $\mathrm{Spm}(A)$ est de cette forme, donc d'après la proposition 3 l'injection de A dans A' est un plongement de r-domaine de $(A, \leq)$ dans $(A', \leq')$.

En revanche $(0) \in \mathrm{Sp}(A, \leq_A)$ et quel que soit $\mathfrak{p}' \in \mathrm{Sp}(A', \leq') = \mathcal{M} \cup \mathcal{N}$ on a $\mathfrak{p}' \cap A \neq (0)$. On voit donc qu'on ne peut espérer améliorer la proposition 6 en relevant dans $\mathrm{Sp}(A', \leq')$ tous les éléments dans $\mathrm{Sp}(A, \leq)$. Une vérification séparée pour l'idéal nul paraît en tout cas inévitable.

§ 3. Plongement : le cas parfait

Définition

Soit A un anneau intègre, K son corps des fractions, K' une extension de K, et

W' un prolongement de W_A (*i.e.* une famille d'anneaux de valuation de K' telle que l'application $R' \mapsto R' \cap K$ soit une bijection de W' sur W_A).
Le r-domaine $(A', \leq')$ obtenu en prenant pour A' l'anneau d'holomorphie de W' et pour $\leq'$ la relation radicale définie par $\mathcal{M}' := \{m(R') \cap A' \;/\; R' \in W'\}$ si $(0) \notin \mathrm{Sp}(A, \leq)$, et par $\mathcal{M} \cup \{(0)\}$ sinon, sera appelé **l'extension de $(A, \leq_A)$ associée à W'**.

Remarques: Avec les notations de la définition, si $(A', \leq')$ est l'extension de $(A, \leq_A)$ associée à W' alors l'injection de A dans A' est un plongement de $(A, \leq_A)$ dans $(A', \leq')$.

Si de plus A est PAC et l'extension $K'|K$ est régulière, alors $(A, \leq_A) \leq_\exists (A', \leq')$. En effet quel que soit $R \in W_A$ son hensélisé égale R^s, donc est $\exists$-clos dans tout prolongement à une extension séparable, et en particulier $R^s \leq_\exists R'^h$ (où R' est l'élément de W' prolongeant R). Il s'ensuit que W' est un prolongement $\exists$-clos de W à K', et la proposition III.3.3 donne donc la conclusion.

Lemme 1 (d'amalgamation)
Soient R, R', R'' trois anneaux de valuation, de corps des fractions respectifs K, K', K'', tels que K' et K'' soient des extensions régulières de K, et $R' \cap K = R'' \cap K = R$.
Alors il existe un anneau de valuation R°, sur $K^\circ := \mathrm{Fr}(K' \otimes_K K'')$ tel que $R^\circ \cap K' = R'$ et $R^\circ \cap K'' = R''$.

Preuve: On distingue deux cas.

Cas 1 : $R \neq K$. Alors *a fortiori* $R' \neq K'$ et $R'' \neq K''$. On sait que deux extensions élémentaires A' et A'' d'un anneau A peuvent être amalgamées dans une extension élémentaire commune B de telle sorte que le type sur A'' dans B de tout n-uplet d'éléments de A' soit un héritier de son type sur A dans A'. En particulier, $\mathrm{Fr}(A')$ est $\mathrm{Fr}(A)$-linéairement disjoint de $\mathrm{Fr}(A'')$ dans $\mathrm{Fr}(B)$.

Or la théorie des anneaux de valuation non triviaux de corps des fractions algébriquement clos est modèle-complète, donc $R^a \preceq R'^a$ et $R^a \preceq R''^a$ (au sens de $\mathrm{L_{div}}$ ou $\mathrm{L_{rad}}$). L'argument ci-dessus nous donne donc un anneau de valuation $\overline{R}$ sur un corps algébriquement clos $\overline{K}$ contenant K' et K'' tel que $\overline{R} \cap K'^a = R'^a$, $\overline{R} \cap K''^a = R''^a$ et le composé de K'^a et K''^a dans $\overline{K}$ est isomorphe à $\mathrm{Fr}(K'^a \otimes_{K^a} K''^a)$.

Les corps K' et K'' sont K-linéairement disjoints dans $\overline{K}$ (n éléments de K'' liés sur K' dans $\overline{K}$ le seraient *a fortiori* sur K'^a, donc sur K^a, et donc encore sur K puisque K'' et K^a sont K-linéairement disjoints, ce qui est impossible) donc $K'K'' \simeq \mathrm{Fr}(K' \otimes_K K'')$ et il suffit de prendre $R^\circ := \overline{R} \cap K'K''$.

Cas 2 : $R = K$. Soit $A^\circ := R'R''$ l'anneau engendré par R et R' dans K°, et $J := m(R')A + m(R'')A$ l'idéal engendré dans A° par $m(R')$ et $m(R'')$. L'anneau A° est K-isomorphe à $R' \otimes_K R''$, donc $A^\circ \cap K' = R'$ et $A^\circ \cap K'' = R''$. Il suffit de vérifier que J est un idéal propre de A°, car dans ce cas il se plonge dans un idéal maximal $\mathfrak{m}$, qui vérifie $m(R') \subseteq J \cap R' \subseteq \mathfrak{m} \cap R'$ et $1 \notin \mathfrak{m} \cap R'$, donc $m(R') = \mathfrak{m} \cap R'$ et donc $R' = A^\circ_\mathfrak{m} \cap K'$, et de même $R'' = A^\circ_\mathfrak{m} \cap K''$. On n'a plus alors qu'à prendre pour R° un anneau de valuation quelconque de K° qui domine $A^\circ_\mathfrak{m}$.

Pour montrer que $1 \notin J$, prenons une base $(m'_i)_{i \in I'}$ du K-espace vectoriel $m(R')$. Comme $1 \notin m(R')$, la famille $(m'_i)_{i \in I'} \cup \{1\}$ est libre (dans le K-espace vectoriel R'), et on peut la compléter en une base $\mathcal{B}'$ de R'. De même, soit $(m''_i)_{i \in I''}$ une base de $m(R'')$ sur K, et $\mathcal{B}''$ une base de R'' contenant $(m''_i)_{i \in I''} \cup \{1\}$. Comme $A^\circ \simeq R' \otimes_K R''$, on sait que $\mathcal{B} := \{b'b'' \;/\; b' \in \mathcal{B}' \text{ et } b'' \in \mathcal{B}''\}$ est une base de A° sur K. En particulier elle est libre et puisque $1 = 1.1 \in \mathcal{B}$ on a : $\forall b' \in \mathcal{B}' \setminus \{1\}, \forall b'' \in \mathcal{B}'',\ b'b'' \neq 1$. Notons E le K-espace vectoriel engendré dans A° par $\mathcal{B} \setminus \{1\}$.

Les éléments de $m(R')A^\circ = m(R')R'R'' = m(R')R''$ sont combinaisons linéaires sur K d'éléments de la forme $m'_i b''$ avec $i \in I'$ et $b'' \in \mathcal{B}''$, *i.e.* d'éléments de $\mathcal{B} \setminus \{1\}$ (car $m'_i \in \mathcal{B}' \setminus \{1\}$) donc $m(R')A \subseteq E$. De même $m(R'')A^\circ \subseteq E$ et donc $J = m(R')A^\circ + m(R'')A^\circ \subseteq E$. La famille $\mathcal{B}$ est libre donc $1 \notin Vect(\mathcal{B} \setminus \{1\}) = E$ et *a fortiori* $1 \notin J$.

■

Théorème 2 (de plongement régulier I)
Soient $(A', \leq')$ et $(A'', \leq'')$ deux r-domaines localement booléens et $\cap$-stables, extensions d'un même r-domaine $\cap$-stable $(A, \leq)$. Soient K, K', K'' leurs corps des fractions, et L, L', L'' leurs treillis résiduels. D'après le corollaire 2.4, on peut considérer L comme un sous-treillis commun à L' et L''. On suppose que :

- *K' et K'' sont parfaits ;*
- *les extensions $K'|K$ et $K''|K$ sont régulières ;*
- *$(0) \in \mathrm{Sp}(A', \leq')$ si et seulement si $(0) \in \mathrm{Sp}(A'', \leq'')$;*
- *$(A'', \leq'')$ est $|A'|^+$-saturé ;*
- *$(A'', \leq'')$ est PRC ou PC_M.*

On se donne un plongement $\sigma : L' \longrightarrow L''$ dont la restriction à L soit l'identité, et un épimorphisme $\pi : G(K'') \longrightarrow G(K')$ qui commute à l'opération de restriction à K^a.

Alors il existe un K^a-plongement $\psi : K'^a \longrightarrow K''^a$ tel que l'on ait :

(i) *K'' est une extension régulière de $\psi[K']$;*
(ii) *$\varphi := \psi_{|A'}$ est un plongement de $(A', \leq')$ dans $(A'', \leq'')$, et $\overline{\varphi} = \sigma$;*
(iii) *pour tout $\tau \in G(K'')$: $\tau \circ \psi = \psi \circ \pi(\tau)$.*

Preuve: Les extensions $K'|K$ et $K''|K$ étant régulières, l'anneau $K' \otimes_K K''$ est intègre. On regarde tous les corps comme plongés dans une clôture algébrique Ω de $\mathrm{Fr}(K' \otimes_K K'')$. C'est dans Ω que sont pris dans la suite tous les composés $A'A''$, $K'K''$... *etc.*

$K'^a K''^a$ est une extension galoisienne de $K'K''$, dont le groupe de Galois est isomorphe à $G(K') \times_{G(K)} G(K'')$. Soit $G := \{\langle \pi(\tau), \tau \rangle \ / \ \tau \in G(K'')\}$, et $K^\circ := (K'^a K''^a)^G$. On sait par le lemme 1.2 que $K'' \leq_\exists K^\circ$.

La proposition 2.6 montre que σ induit une application $\widehat{\sigma}$ de $\mathrm{Sp}(A'', \leq'')$ dans $\mathrm{Sp}(A', \leq')$ telle que $\mathrm{Spm}(A') \subseteq \widehat{\sigma}[\mathrm{Spm}(A'')]$ et pour tout $\mathfrak{p}'' \in \mathrm{Sp}(A'', \leq'')$ on a $\mathfrak{p}'' \cap A = \widehat{\sigma}(\mathfrak{p}'') \cap A$ (parce que $\sigma_{|L} = Id_L$). Quel que soit $\mathfrak{m}'' \in \mathrm{Spm}(A'')$ le lemme 1 donne donc un anneau de valuation de $K'K''$ (identifié à $\mathrm{Fr}(K' \otimes_K K'')$) que l'on peut prolonger en un anneau de valuation $R(\mathfrak{m}'')$ de K°, tel que $R(\mathfrak{m}'') \cap K'' = A''_{\mathfrak{m}''}$ et $R(\mathfrak{m}'') \cap K' = A'_{\widehat{\sigma}(\mathfrak{m}'')}$.

On pose $W^\circ := \{R(\mathfrak{m}'') \ / \ \mathfrak{m}'' \in \mathrm{Spm}(A'')\}$ et $(A^\circ, \leq^\circ)$ l'extension de $(A'', \leq'')$ associée à W°. En vertu de la remarque ouvrant ce paragraphe, $(A'', \leq'') \leq_\exists (A^\circ, \leq^\circ)$.

Quel que soit $\mathfrak{m}'' \in \mathrm{Spm}(A'')$, $A' \subseteq R(\mathfrak{m}'')$ donc $A' \subseteq A^\circ$; de plus :

– $\forall \mathfrak{m}'' \in \mathrm{Spm}(A'')$, $R(\mathfrak{m}'') \cap K' = A'_{\widehat{\sigma}(\mathfrak{m}'')}$ donc $m(R(\mathfrak{m}'')) \cap A' = \widehat{\sigma}(\mathfrak{m}'') \in \mathrm{Sp}(A', \leq')$.

– $\forall \mathfrak{m}' \in \mathrm{Spm}(A'), \exists \mathfrak{m}'' \in \mathrm{Spm}(A'')$ tel que $\widehat{\sigma}(\mathfrak{m}'') = \mathfrak{m}'$ donc il existe $\mathfrak{p} \in \mathrm{Sp}(A^\circ, \leq^\circ)$ tel que $\mathfrak{p} \cap A' = \mathfrak{m}'$ (prendre $\mathfrak{p} := m(R(\mathfrak{m}'')) \cap A^\circ$).

– $(0) \in \mathrm{Sp}(A^\circ, \leq^\circ) \iff (0) \in \mathrm{Sp}(A'', \leq'') \iff (0) \in \mathrm{Sp}(A', \leq')$.

La proposition 2.3 entraîne donc que l'injection de A' dans A° est un plongement de $(A', \leq')$ dans $(A^\circ, \leq^\circ)$.

Puisque $(A', \leq')$ est ainsi plongé dans une extension $(A^\circ, \leq^\circ)$ dans laquelle $(A'', \leq'')$ est existentiellement clos, et que par hypothèse $(A'', \leq'')$ est $|A'|^+$-saturé on sait qu'il existe un plongement φ de $(A', \leq')$ dans $(A'', \leq'')$ au dessus de A. Cependant, il n'y a aucune raison pour qu'un tel plongement vérifie $\overline{\varphi} = \sigma$ ni que K'' soit une extension régulière de $\mathrm{Fr}(\varphi[A'])$. Pour obtenir la conclusion il nous faut donc raffiner un peu.

Pour que $\overline{\varphi} = \sigma$ on introduit une sorte de section de σ en fixant, pour tout $a' \in A'$, un élément $a''_{a'} \in A''$ tel que $P_{A''}(a''_{a'}) = \sigma(P_{A'}(a'))$. Si $a' \in A$ on prend $a''_{a'} = a'$. Si $a' = 0$, il s'ensuit que $a''_{a'} = 0$, et on peut s'arranger pour avoir la réciproque : si $a' \in A'$ est tel que $\sigma(P_{A'}(a')) = P_{A''}(0)$, alors $P_{A'}(a') = \mathbf{1}_{L'}$, donc ou bien $a' = 0$ et il n'y a rien à changer, ou bien $a' \neq 0$ et alors $(0) \notin \mathrm{Sp}(A', \leq')$, donc par hypothèse $(0) \notin \mathrm{Sp}(A'', \leq'')$, *i.e.* $(0)_\leq$ n'est pas réduit à $\{0\}$, et on prend pour $a''_{a'}$ un élément de $(0)_\leq \setminus \{0\}$.
Pour tout $\mathfrak{m}'' \in \mathrm{Spm}(A'')$, on a en notant $R^\circ := R(\mathfrak{m}'')$:

$$R^\circ \cap K'' = A''_{\mathfrak{m}''} \text{ et } R^\circ \cap K' = A_{\widehat{\sigma}(\mathfrak{m}'')} \text{ donc } m(R^\circ) \cap A' = \widehat{\sigma}(m(R^\circ) \cap A'')$$

d'où :

$$\begin{aligned} a''_{a'} \in m(R^\circ) &\iff \mathfrak{m}'' = m(R^\circ) \cap A'' \in P_{A''}(a''_{a'}) = \sigma(P_{A'}(a')) \\ &\iff a' \in \widehat{\sigma}(\mathfrak{m}'') = m(R^\circ) \cap A' \\ &\iff a' \in m(R^\circ) \end{aligned}$$

De plus par construction $a''_{a'} \in (0) \iff a' \in (0)$. On a donc $a''_{a'} \leq^\circ a'$ et $a' \leq^\circ a''_{a'}$.

Soit $(e''_\alpha)_{\alpha<\beta}$ une base de K''^a sur K'' (au sens des K''-espaces vectoriels). L'extension $K^\circ|K''$ étant régulière, K° et K''^a sont K''-linéairement disjoints donc la famille $(e''_\alpha)_{\alpha<\beta}$ reste libre sur K°. De plus le groupe de Galois de $K'^aK''^a$ sur K° est isomorphe à $G = Gal(K''^a|K'')$ donc $K^\circ K''^a = K'^aK''^a$ *i.e.* $(e''_\alpha)_{\alpha<\beta}$ engendre $K'^aK''^a$ sur K° et en constitue donc une base. Tout $x' \in K'^a$ s'écrit de manière unique :

$$x' = \sum_{i=1}^{n(x')} \lambda_i(x') e''_{\alpha_i(x')}, \quad \text{avec les } \lambda_i(x') \in K^\circ \setminus \{0\}.$$

Par construction A° contient la clôture intégrale de $A'A''$ dans K°, et K° est algébrique sur $\mathrm{Fr}(A'A'')$ donc $\mathrm{Fr}(A^\circ) = K^\circ$ et on peut écrire chaque $\lambda_i(x')$ sous la forme $\lambda_i(x') = c_i(x')/d_i(x')$ avec $c_i(x'), d_i(x') \in A^\circ \setminus \{0\}$.

- Posons $\mathcal{C} := \{c_i(x'), d_i(x') \ / \ x' \in K'^a,\ i < n(x')\}$ et $\mathcal{D} := \{a''_{a'} \ / \ a' \in A'\}$.
- Soit K_0 une sous-extension élémentaire de K'' de cardinal $|A'|$ contenant $K(\mathcal{D})$, et soit $(A_0, \leq_0)$ la trace de $(A'', \leq'')$ sur K_0.
- Soit A_1 le sous-anneau de A° engendré par A', A_0 et $\mathcal{C}$. On le munit de la trace $\leq_1$ de $\leq^\circ$ et on pose $K_1 := \mathrm{Fr}(A_1)$ (remarque : on a donc $K'^a \subseteq K''^aK_1$).

A priori il n'y a aucune raison pour que K_1 et K'' soient linéairement disjoints sur K_0, mais nous allons nous y ramener. Supposons déja construites deux chaines d'extensions $K_0 \subseteq K_2 \subseteq \cdots \subseteq K_{2n} \subseteq K''$ et $K_1 \subseteq K_3 \subseteq \cdots \subseteq K_{2n+1} \subseteq K^\circ$ telles que pour tout $i \in [\![0, n]\!]$:
- $K_{2i} \subseteq K_{2i+1}$ et ils sont de cardinal $|K'|$;
- l'inclusion de K_{2i} dans K'' est élémentaire ;
- tout k-uplet d'éléments de K_{2i-1} lié sur K'' est encore lié sur K_{2i}, pour tout $k \in \mathbb{N}^*$

(on convient que $K_{-1} = K'$).

À tout k-uplet x d'éléments de K_{2n+1} lié sur K'' on associe un k-uplet ν_x de coefficients d'une relation de dépendance linéaire de x sur K''. L'ensemble $\mathcal{N}$ de tous les éléments de K'' intervenant dans ces ν_x quand x décrit $\bigcup_{k\in\mathbb{N}^*}\mathbb{N}$ est de cardinal au plus $|K'|$. On peut donc contruire un sous-corps K_{2n+2} de K'' de cardinal $|K'|$ tel que $K_{2n}(\mathcal{N}) \subseteq K_{2n+2} \preceq K''$, et on prend alors simplement $K_{2n+3} = K_{2n+2}K_{2n+1}$. La réunion K_0' des K_{2n} est un sous-corps de $K_1' := \bigcup_{n\in\mathbb{N}} K_{2n+1}$, ils sont tous deux de cardinal $|K'|$, l'inclusion de K_0' dans K'' est élémentaire, et cette fois par construction tout k-uplet d'éléments de K_1' lié sur K'' l'est sur K_0' *i.e.* K_1' et K'' sont K_0'-linéairement disjoints dans K°. Quitte à remplacer K_0 et K_1 par K_0' et K_1', on voit qu'on peut donc supposer K_1 et K'' linéairement disjoints sur K_0.

Le cardinal de A_1 est majoré par $|A'|$ donc par saturation de $(A'', \leq'')$ il existe un A_0-plongement de $(A_1, \leq_1)$ dans $(A'', \leq'')$. Celui-ci s'étend de manière canonique en un K_0-plongement de K_1 dans K'', et l'indépendance linéaire permet de le prolonger à son tour en un homomorphisme de K''-algèbres Θ_1 de $K''K_1$ dans K''. L'extension $K^\circ|K_0$ est régulière ($K_0 \preceq K''$ garantit que l'extension $K''|K_0$ est régulière, et par construction K° est une extension régulière de K'') donc K° et *a fortiori* $K_1'K''$ est linéairement disjoint de K''^a sur K'', d'où l'on déduit par tensorisation un homomorphisme Θ de K''^a-algèbre de K''^aK_1 dans K''^a prolongeant Θ_1.

Notons ψ la restriction de Θ à K'^a (nous avons vu plus haut que K'^a était inclus dans $K''^a(\mathcal{C})$ donc dans K''^aK_1) soit $\varphi := \psi_{A'}$; φ est la trace sur A' du A_0-plongement de $(A_1, \leq_1)$ dans $(A'', \leq'')$ donc c'est bien un plongement de r-domaine de $(A', \leq')$ dans $(A'', \leq'')$ au-dessus de A. De plus pour tout $a' \in A'$ on a :

$$(A^\circ, \leq^\circ) \models a' \leq a''_{a'} \leq a' \quad \Longrightarrow \quad (A'' \leq'') \models \varphi(a') \leq a''_{a'} \leq \varphi(a')$$

(car $\Theta(a''_{a'}) = a''_{a'}$) donc $P_{A''}(\varphi(a')) = P_{A''}(a''_{a'}) = \sigma(P_{A'}(a'))$, et donc $\overline{\varphi} = \sigma$ *i.e.* (ii).

ψ est injective puisque K'^a est un corps, donc ψ est un K^a-plongement de K'^a dans K''^a.

Soit $x' = \sum_{i=1}^{n(x')} \lambda_i(x')e''_{\alpha_i(x')} \in K'^a$. Pour tout $\tau \in G(K'')$, on a :

$$\begin{aligned}\Big(\pi(\tau)\Big)(x') &= \Big\langle \pi(\tau), \tau \Big\rangle (x') \\ &= \sum_{i=1}^{n(x')} \Big\langle \pi(\tau), \tau \Big\rangle (\lambda_i(x')).\Big\langle \pi(\tau), \tau \Big\rangle (e''_{\alpha_i(x')}) \\ &= \sum_{i=1}^{n(x')} \lambda_i(x')\tau(e''_{\alpha_i(x')})\end{aligned}$$

La dernière égalité vient de ce que $\langle \pi(\tau), \tau\rangle$ vaut l'identité sur K° par définition de K°, et vaut τ sur K''^a par définition du produit fibré. Il s'ensuit que :

$$\psi\Big(\pi(\tau)(x')\Big) = \Theta\Big(\pi(\tau)(x')\Big) = \sum_{i=1}^{n(x')} \Theta(\lambda_i(x'))\tau(e''_{\alpha_i(x')}) = \tau(\Theta(x')) = \tau(\psi(x'))$$

L'avant-dernière inégalité vient de ce que $\tau_{|K''}$ vaut l'identité et que les $\lambda_i(x')$ appartiennent à K_1 donc leur image par Θ est dans K''. Ceci prouve (iii). Il s'ensuit que

$\psi[K']$ est relativement algébriquement clos dans K'' *i.e.* (i) puisque K' est parfait.
■

§ 4. Plongement : le cas non parfait

Dans la démonstration du théorème 3.2 de plongement régulier I, juste avant d'utiliser l'hypothèse de saturation, on disposait de deux r-domaines $(A'', \leq'')$ et $(A_1, \leq_1)$, tous les deux inclus dans l'extension $(A^\circ, \leq^\circ)$ associée à un prolongement W° de $W_{A''}$ sur une extension régulière K° de $\mathrm{Fr}(A'')$. Le r-domaine $(A'', \leq'')$ était PAC (c'est le cas particulier d'anneau PRC qui nous intéresse ici) et $|A_1|^+$-saturé, ce qui permettait de plonger $(A_1, \leq_1)$ dans $(A'', \leq'')$ au-dessus d'un sous-anneau commun A_0.

Pour que ce plongement soit séparable, on avait supposé $\mathrm{Fr}(A')$ parfait. Ce paragraphe est consacré à l'élimination de cette hypothèse, moyennant certains raffinements empruntés à l'étude des corps PAC. Le lemme suivant est un analogue pour notre situation du lemme 10.11 de [F-J], dit "de Tamagawa".

Lemme 1
Soit $(A'', \leq'')$ un r-domaine PAC de caractéristique $p \neq 0$, $(A_0, \leq_0)$ un sous-r-domaine de $(A'', \leq'')$, K'' et K_0 leurs corps de fractions respectifs. Soit K° une extension régulière de K'', W° un prolongement de $W_{A''}$ à K°, et $(A^\circ, \leq^\circ)$ l'extension de $(A'', \leq'')$ associée à W°. Enfin soit K_1 un sous-corps de K° contenant K_0, et $(A_1, \leq_1)$ la trace de $(A^\circ, \leq^\circ)$ sur K_1.
On se donne une famille $(x'_i)_{i \in I'}$ d'éléments de K_1, p-libre sur $(K^\circ)^p$, et on suppose que :
- *$(A'', \leq'')$ est $|A_1|^+$-saturé.*
- *K'' possède une p-base de cardinal au moins égal à $|I'|$.*

Alors il existe un plongement de $(A_1, \leq_1)$ dans $(A'', \leq'')$, dont la restriction à A_0 soit l'identité et dont le prolongement à K_1 envoie $(x'_i)_{i \in I'}$ sur une famille p-libre d'éléments de K''.

Remarque: On sait déja que $(A'', \leq'') \leq_\exists (A^\circ, \leq^\circ)$, donc (par saturation) que $(A_1, \leq_1)$ se plonge au-dessus de A_0 dans $(A'', \leq'')$. Mais un tel plongement n'a *a priori* aucune raison de conserver la p-indépendance des x_i, et c'est là que réside la nouveauté.

Preuve: On commence par montrer le lemme sous l'hypothèse suplémentaire que $I' = \{1, \ldots, n\}$ et que K_1 est finiment engendré sur K_0 (cas finitaire). Le théorème de compacité permettra ensuite d'en déduire le cas général.

La démonstration faisant intervenir un nombre assez élevé de corps auxiliaires, un diagramme a été placé en fin de preuve pour récapituler leurs principales relations.

Le cas finitaire : méthode de Tamagawa. Sous ces nouvelles hypothèses, soient $K''_1 := K''K_1$ (le composé est pris dans K°) et $L := K''K_1^p(x'_1, \ldots, x'_n)$. On peut extraire de $(x'_i)_{1 \leq i \leq n}$ une p-base de L sur $K''K_1^p$. Quitte à renuméroter les x'_i, on peut supposer que $(x'_1, \ldots, x'_s)$ est une telle p-base (avec $s \leq n$). Soit $(x_i)_{i \in I}$ une p-base de K'' ; on a :

$$L = K''K_1^p[x'_1, \ldots, x'_s] = K_1''^p[(x_i)_{i \in I}, x'_1, \ldots, x'_s]$$

donc il existe $x_1, \ldots, x_r \in \{x_i \mid i \in I\}$ tel que $x'_{s+1}, \ldots, x'_n \in K_1''^p[x_1, \ldots, x_r, x'_1, \ldots, x'_s]$. Puisque par hypthèse $|I| \geq n$ on peut prendre $r \geq n$. Les x'_i sont p-indépendants sur $(K^\circ)^p$ et *a fortiori* sur $K_1''^p$, donc le lemme de l'échange nous donne (quitte à renuméroter les x_i) :

$$x_{r-(n-s)+1}, \ldots, x_r \in K_1''^p[x_1, \ldots, x_{r-(n-s)}, x'_1, \ldots, x'_n]. \tag{1}$$

Pour tout $i \in [\![1, s]\!]$ on pose $\eta_i := (x_{r-n+i}x'_i)^{1/p}$, et soit $K_2'' := K_1''[\eta_1, \ldots, \eta_s]$. La preuve du lemme de Tamagawa dont nous avons donné plus haut la référence montre que K_2'' est une extension régulière de K''. Pour la commodité du lecteur nous rappelons ici l'essentiel de son argument.

L'extension $K_2''|K''$ est séparable. L'extension $K_1''|K''$ est finiment engendrée (car K_1 est de type fini sur K_0) et séparable (car $K_1'' \subseteq K^\circ$). Il s'ensuit que $[K_1'' : K''K_1''^p] = p^t$ où t est le degré de transcendance de K_1'' sur K'' (cf. lemme 9.16, p. 114 de [F-J]). L'extension $K_2''|K''$ est de type fini, et comme K_2'' est algébrique sur K_1'' il a le même degré de transcendance sur K'', donc ce même lemme 9.16 entraîne qu'il suffit de montrer que $[K_2'' : K''K_2''^p] = [K_1'' : K''K_1''^p]$ pour en déduire que K_2'' est séparable sur K''.

$$K''K_2''^p = K''K_1''^p[\eta_i^p]_{1\leq i\leq s} = K''K_1''^p[x'_i]_{1\leq i\leq s} = K''K_1^p[x'_i]_{1\leq i\leq s} = L$$

d'où $[K''K_1''^p[\eta_i^p]_{1\leq i\leq s} : K''K_1''^p] = [L : K''K_1''^p] = p^s$, et la famille $(\eta_i^p)_{1\leq i\leq s}$ est donc p-indépendante sur $K''K_1''^p$. Il s'ensuit que $(\eta_i)_{1\leq i\leq s}$ est p-indépendante sur K_1'' (car une relation de p-dépendance sur K_1'' entre les η_i, élevée à la puissance p, donnerait une relation de p-dépendance sur $K_1''^p$ et *a fortiori* sur $K''K_1''^p$ entre les η_i^p) et donc $[K_2'' : K_1''] = p^s$.

$$[K_2'' : K''K_1''^p] = \begin{cases} [K_2'' : L][L : K''K_1''^p] = [K_2'' : L]p^s \\ \\ [K_2'' : K_1''][K_1'' : K''K_1''^p] = p^s[K_2'' : K''K_1''^p] \end{cases}$$

On en déduit $[K_2'' : K''K_2''^p] = [K_2'' : L] = [K_2'' : K''K_1''^p]$ et la conclusion suit.

K'' est relativement algébriquement clos dans K_2''. En effet, un élément y de K_2'' s'écrit :

$$y = \sum_{i\in I} u_i\eta_1^{i(1)}\ldots\eta_s^{i(s)} \quad \text{où} \quad I = [\![0, p-1]\!]^{[\![1,s]\!]} \quad \text{et les} \quad u_i \in K_1''. \tag{2}$$

Si y est algébrique sur K'' alors y^p aussi, et il appartient à $K_2''^p \subseteq K_1'' \subseteq K^\circ$. Comme l'extension $K''^\circ|K''$ est régulière il s'ensuit que $y^p \in K''$. L'équation (2) élevée à la puissance p nous donne alors une relation de p-dépendance sur K_1'' entre les η_i^p ce qui implique que tous les u_i sont nuls, sauf celui pour lequel i est constamment nul, c'est-à-dire que $y = u_0 \in K_1''$. Comme y est algébrique sur K il s'ensuit que $y \in K$, ce qu'il fallait démontrer.

Conclusion dans le cas finitaire. Soit $(A^\dagger, \leq^\dagger)$ l'extension de $(A'', \leq'')$ associée à un prolongement quelconque de W° sur $K^\circ[\eta_1, \ldots, \eta_s]$, et $(A_2'', \leq_2'')$ la trace de $(A^\dagger, \leq^\dagger)$ sur K_2''. Puisque K_2'' est une extension régulière de K'', on a $(A'', \leq'') \leq_\exists (A_2'', \leq_2'')$.

Pour tout $i \in [\![n - r + s + 1, r]\!]$ on a d'après (1), en posant $\mathcal{I} := [\![0, p-1]\!]^{[\![1,r+s]\!]}$:

$$x_i = \sum_{j\in\mathcal{I}} v_{i,j}^p x_1^{j(1)}\cdots x_{r-n+s}^{j(r-n+s)} x_1'^{j(r-n+s+1)} \cdots\cdots\cdots x_n'^{j(r+s)} \quad \text{où les} \quad v_{i,j} \in K_1''. \tag{3}$$

Soit K_2 l'extension de K_1 engendrée par ces coefficients $v_{i,j}$ et par $\eta_1, \ldots, \eta_s$. C'est une extension de type fini sur K_1, donc $|K_2| = |K_1|$. Enfin soit $(A_2, \leq_2)$ la trace de $(A_2'', \leq_2'')$ sur K_2. Par saturation de $(A'', \leq'')$ on a un A_0-plongement φ de $(A_2, \leq_2)$

dans $(A'', \leq'')$ (car $|A_2| = |A_1|$). Sa restriction à A_1 et son prolongement canonique en un K_0-plongement de K_2 dans K'' sont encore notés φ. Il ne reste qu'à vérifier que $(\varphi(x'_i))_{1\leq i\leq n}$ est p-indépendante (sur K''^p).

On a pour tout $i \in [\![n-r+s+1, r]\!]$, en conservant les notations de (3) :

$$x_i = \varphi(x_i) = \sum_{j\in\mathcal{I}} \varphi(v_{i,j})^p x_1^{j(1)} \cdots x_{r-n+s}^{j(r-n+s)} \varphi(x'_1)^{j(r-n+s+1)} \cdots \varphi(x'_n)^{j(r+s)}. \qquad (4)$$

Or pour tout $k \in [\![1, s]\!]$ on a : $x_{r-n+k} = \varphi(x_{r-n+k}) = \varphi(\eta_k^p x_k'^{-1}) = \varphi(\eta_k)^p \varphi(x_k'^{-1})$.
D'où, vu (4) :

$$x_1, \ldots, x_n \in K''^p(x_1, \ldots, x_{r-n}, \varphi(x'_1), \ldots, \varphi(x'_n)).$$

Or $x_1, \ldots, x_n$ sont p-indépendants sur K''^p, et la famille $(x_1, \ldots, x_{r-n}, \varphi(x'_1), \ldots, \varphi(x'_n))$ est donc nécessairement p-libre. Il s'ensuit que $\varphi(x'_1), \ldots, \varphi(x'_n)$ sont p-indépendants sur K''^p, ce qu'il fallait démontrer.

Le cas général : théorème de compacité. On reprends la famille $(x'_i)_{i\in I'}$ et les autres données de l'énoncé initial. Pour alléger l'écriture, notons $\mathcal{P}_\omega(I')$ l'ensemble des parties finies de I', et pour tout $I_0 \in \mathcal{P}_\omega(I')$:

– $\mathcal{I}_{I_0} :=$ l'ensemble des fonctions $j : I_0 \longrightarrow [\![0, p-1]\!]$:
– $b'_{I_0} \in A_1 \setminus \{0\}$ un dénominateur commun aux $\prod_{i\in I_0} x_i'^{j(i)}$ (pour $j \in I_0$) ;
– pour tout $j \in \mathcal{I}_{I_0}$, $a'_j := b'_{I_0} \prod_{i\in I_0} x_i'^{j(i)}$.

Démontrer la proposition revient à prouver que $(A'', \leq'')$ satisfait le diagramme sans quanteur de $(A_1, \leq_1)$ augmenté des formules suivantes, pour toute partie finie I_0 de I' :

$$\theta_{I_0} \equiv \forall\, (a_j)_{j\in\mathcal{I}_{I_0}} \Big[\sum_{j\in\mathcal{I}_{I_0}} a_j^p a'_j = 0 \longrightarrow \bigwedge_{j\in\mathcal{I}_{I_0}} a_j = 0 \Big].$$

Par saturation de $(A'', \leq'')$ il suffit de montrer que cette théorie est satisfaisable dans une extension élémentaire de $(A'', \leq'')$. Autrement dit il faut montrer que la théorie $T := \Delta(A'', \leq'') \cup D(A_1, \leq_1) \cup \{\theta_{I_0} \;/\; I_0 \in \mathcal{P}_\omega(I)\}$ du langage $\mathrm{L}_{\mathrm{rad}}(A'' \cup A_1)$ est consistante, où $\Delta(A'', \leq'')$ désigne le diagramme élémentaire de $(A'', \leq'')$ et $D(A_1, \leq_1)$ le diagramme sans quanteur de $(A_1, \leq_1)$.

Soit T_0 un fragment fini de T. Il fait intervenir un ensemble fini $\mathcal{C}$ d'éléments de A_1. Posons $K'_1 := K(\mathcal{C})$, et soit $(A'_1, \leq'_1)$ la trace de $(A_1, \leq_1)$ sur K_1. Puisque $\mathcal{C}$ est fini, il existe $I_0 \in \mathcal{P}_\omega(I)$ tel que $T_0 \subseteq \Delta(A'', \leq'') \cup D(A_1, \leq_1) \cup \{\theta_{J_0} \;/\; J_0 \subseteq I_0\}$.

Pour construire un modèle de T_0, il suffit donc de trouver un A-plongement de $(A_1, \leq_1)$ dans $(A'', \leq'')$ dont le prolongement à K_1 envoie $(x'_i)_{i\in I_0}$ sur une partie p-libre de K''. Or c'est exactement ce que nous avons démontré avec le cas finitaire : T est donc finiment satisfaisable, *i.e.* T est satisfaisable d'après le théorème de compacité, d'où la conclusion.

Récapitulatif :
$K''_1 = K''K_1 \qquad L = K''K_1''^p[x'_1, \ldots, x'_s] = K''K_2''^p \qquad K''_2 = K''_1[\eta_1, \ldots, \eta_s]$
Les x_i forment une p-base de K_1, et les x'_i une p-base de K''.
Les η_i sont construits à partir des x_i et des x'_i et on a : $\eta_i^p = x_{r-n+i} x'_i$.
K_2 est construit à partir de K_1, des η_i et de coefficients $v_{i,j}$ pris dans K''_1.
Le plongement de K'' dans K° est régulier.

Le diagramme commutatif suivant résume les positions relatives de tous ces corps (les flèches sont des inclusions) :

$$\begin{tikzcd}
 & & K^\circ & \\
K'' \arrow[r] & L \arrow[r] & K_1'' \arrow[r] \arrow[u] & K_2'' \\
K_0 \arrow[r] \arrow[u] & K_1^p \arrow[r] \arrow[u] & K_1 \arrow[r] \arrow[u] & K_2 \arrow[u]
\end{tikzcd}$$

■

Théorème 2 (de plongement régulier II)

Soient $(A', \leq')$ et $(A'', \leq'')$ deux r-domaines localement booléens et $\cap$-stables, extensions d'un même r-domaine $\cap$-stable $(A, \leq)$. Soient K, K', K'' leurs corps des fractions, et L, L', L'' leurs treillis résiduels. D'après le corollaire 2.4, on peut considérer L comme un sous-treillis commun à L' et L''. On suppose que :

- *K' et K'' sont des extensions régulières de K ;*
- *$(0) \in \mathrm{Sp}(A', \leq')$ si et seulement si $(0) \in \mathrm{Sp}(A'', \leq'')$;*
- *$[K' : K'^p] \leq [K'' : K''^p]$;*
- *$(A'', \leq'')$ est $|A'|^+$-saturé ;*
- *$(A'', \leq'')$ est PAC.*

On se donne un plongement $\sigma : L' \longrightarrow L''$ dont la restriction à L soit l'identité, et un épimorphisme $\pi : G(K'') \longrightarrow G(K')$ qui commute à l'opération de restriction à K^s.

Alors il existe un K^s-plongement $\psi : K'^s \longrightarrow K''^s$ satisfaisant les conditions suivantes :

(i) *K'' est une extension régulière de $\psi[K']$;*
(ii) *$\varphi := \psi_{|A'}$ est un plongement de $(A', \leq')$ dans $(A'', \leq'')$, et $\overline{\varphi} = \sigma$;*
(iii) *pour tout $\tau \in G(K'')$, on a : $\tau \circ \psi = \psi \circ \pi(\tau)$.*

Preuve: La preuve est presque identique à celle du théorème de plongement régulier I, jusqu'au moment où intervient l'argument de saturation (il faut seulement remplacer partout les clôtures algébriques par des clôtures séparables). On disposait alors de :

- un corps K°, extension régulière commune à K'' et K', et un prolongement W° de $W_{A''}$ à K° tel que l'extension $(A^\circ, \leq^\circ)$ de $(A'', \leq'')$ associée à W° soit aussi une extension de $(A', \leq')$;
- une famille $\{a''_{a'} \ / \ a' \in A'\}$ d'éléments de A'', telle que pour tout $a' \in A'$ on ait :
$$P_{A''}(a''_{a'}) = \sigma(P_{A'}(a')) \quad \text{et} \quad P_{A^\circ}(a''_{a'}) = P_{A^\circ}(a')$$
- une base $(e''_\alpha)_{\alpha < \beta}$ de K''^s, vu comme K''-espace vectoriel ;
- pour tout élément x' de K'^s, des éléments $c_i(x'), d_i(x') \in A^\circ \setminus \{0\}$ (avec $1 \leq i \leq n(x')$, pour un certain $n(x') \in \mathbb{N}$) tels que :
$$x' = \sum_{i=1}^{n(x')} \frac{c_i(x')}{d_i(x')} e''_{\alpha_i(x')}.$$

On pose encore $\mathcal{C} := \{c_i(x'), d_i(x') \ / \ x' \in K'^s, \ i < n(x')\}$ et $\mathcal{D} := \{a''_{a'} \ / \ a' \in A'\}$, et on considère :

- une p-base $\mathcal{B} := (x'_i)_{i \in I'}$ de K' ;
- une sous-extension élémentaire K_0 de K'' de cardinal $|A'|$ contenant $K(\mathcal{D})$, et $(A_0, \leq_0)$ la trace de $(A'', \leq'')$ sur K_0 ;

– A_1 le sous-anneau de A° engendré par A', A_0, $\mathcal{B}$ et $\mathcal{C}$, muni de la trace $\le_1$ de $\le^\circ$, et enfin $K_1 := \mathrm{Fr}(A_1)$.

Le r-domaine $(A_1, \le_1)$ est de cardinal $|A'|$ et, l'extension $K^\circ|K'$ étant régulière, $\mathcal{B}$ est encore p-libre sur $(K^\circ)^p$. Le lemme 1 donne donc un plongement Θ de $(A_1, \le_1)$ dans $(A'', \le'')$ dont la restriction à $A[\mathcal{D}]$ est l'identité, et dont le prolongement à K_1 envoie $\mathcal{B}$ sur une famille p-libre de K''. De même que dans la preuve du théorème de plongement régulier I on peut s'arranger pour que K_1 et K'' soient linéairement disjoints sur K_0, ce qui permet de prolonger ce plongement en un homomorphisme Θ de K''^a-algèbre de $K''^a K_1$ dans K''^a.

La démonstration reprend ensuite le cours de celle du théorème de plongement régulier I : on note ψ la restriction de Θ à K'^s (car K'^s est inclus dans $K''^s(\mathcal{C})$ donc dans $K''^a K_1$) et $\varphi := \psi_{A'}$. Ce plongement a toutes les propriétés déja vérifiées pour le théorème de plongement régulier I, de plus il envoie la p-base $\mathcal{B}$ sur une famille p-libre de K'' ce qui garantit que K'' est bien une extension séparable de $\psi[K']$, d'où la conclusion.

∎

§ 5. Un peu de théorie des modèles

Nous regroupons ici les principaux corollaires des théorèmes de plongement régulier I et II (le théorème 3.2 et le théorème 4.2) pour les r-domaines PAC, PRC et PC_M. Ces deux théorèmes constituent en fait les deux versions (cas parfait et cas non parfait) d'un unique énoncé que nous baptiserons désormais “*le* théorème de plongement régulier”.

Définition
Étant donné un anneau intègre A, je note $\mathbf{Alg}(\boldsymbol{A})$ la partie algébrique de A, c'est-à-dire l'ensemble des éléments de A algébriques sur le sous-corps premier de $\mathrm{Fr}(A)$.

Si A est muni d'un relation radicale $\le$, et $L := \mathrm{L}(A, \le)$, je note $\mathbf{Alg}(\boldsymbol{A}, \boldsymbol{\le})$ le r-domaine $\mathrm{Alg}(A)$ muni de la trace $\le_{alg}$ de la relation radicale de $(A, \le)$, et $\mathbf{Alg}(\boldsymbol{L}) := \mathrm{L}(\mathrm{Alg}(A), \le_{alg})$.

Remarque: Avec les notations de la définition, on voit que :

– l'injection de $\mathrm{Alg}(A)$ dans A est un plongement de r-domaine de $\mathrm{Alg}(A, \le)$ dans $(A, \le)$, qui induit donc, d'après le corollaire 2.4, un plongement (au sens des demi-treillis supérieurs avec extrémités) de $\mathrm{Alg}(L)$ dans L ;

– $K := \mathrm{Fr}(A)$ est une extension régulière de $\mathrm{Alg}(K) = \mathrm{Fr}(\mathrm{Alg}(A))$ (car $\mathrm{Fr}(Alg(A))$ est toujours un corps parfait, relativement algébriquement clos dans K) ;

– si $\mathrm{Alg}(A)$ est intégralement clos (c'est automatique si A l'est lui-même) alors la proposition II.1.5 s'applique à $\mathrm{Alg}(A)$, qui est donc localement booléen et $\cap$-stable, et comme $\mathrm{Alg}(A)$ est de dimension ≤ 1 on a $\mathrm{Sp}(\mathrm{Alg}(A, \le)) \subseteq \mathrm{Spm}(\mathrm{Alg}(A)) \cup \{0\}$ donc $\mathrm{Alg}(A, \le)$ est lui-même $\cap$-stable et localement booléen.

Propriété 1
Soit B un anneau intègre et intégralement clos. Notons $A := \mathrm{Alg}(B)$ et supposons que $(0) \in \mathrm{Sp}(B, \le_B)$ si et seulement si $(0) \in \mathrm{Sp}(A, \le_A)$.
Alors $\mathrm{Alg}(B, \le_B) = (A, \le_A)$.

Preuve: Il faut montrer que $\mathrm{Sp}(\mathrm{Alg}(B, \le_B)) = \mathrm{Sp}(A, \le_A)$. Le cas de l'idéal nul est réglé par hypothèse, et comme A est de dimension ≤ 1 on a forcément $\mathrm{Sp}(A, \leq_A) \subseteq \mathrm{Spm}(A)$. Comme par définition $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq_A)$ il reste donc á montrer que $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(\mathrm{Alg}(B, \leq_B))$. Or c'est immédiat puisqu'on sait relever tout idéal maximal de A en un idéal maximal de B.

■

Notations: Quand on a un langage $\mathcal{L}$, une $\mathcal{L}$-structure A et une partie B de A, on note $\mathcal{L}(B)$ le langage obtenu en ajoutant à $\mathcal{L}$ un ensemble de nouvelles constantes indexé sur B, et (A, B) la $\mathcal{L}(B)$-structure obtenue en interprétant dans A chaque nouvelle constante par l'élément de B qui la nomme. On a par exemple :

$$A \preceq A' \quad \iff \quad (A, A) \equiv (A', A).$$

Rappelons pour mémoire la propriété suivante :

Proposition 2

Soient $(A, \leq)$ et $(A', \leq')$ deux r-domaines de Bezout, de corps des fractions et de treillis résiduels respectifs K, L, K' et L'.
(1) *Si $(A, \leq) \leq_\exists (A', \leq')$, alors $K \leq_\exists K'$ et $L \leq_\exists L'$.*
(2) *Si $(A, \leq) \preceq (A', \leq')$, alors $K \preceq K'$ et $L \preceq L'$.*
(3) *Si $(A, \leq) \equiv (A', \leq')$, alors il existe un isomorphisme $\varphi : \mathrm{Alg}(A, \leq) \longrightarrow \mathrm{Alg}(A', \leq')$ tel que $(K, \mathrm{Alg}(K)) \equiv (K', \varphi^*[\mathrm{Alg}(K)]$ et $(L, \mathrm{Alg}(L)) \equiv (L', \overline{\varphi}[\mathrm{Alg}(L')])$ (en notant φ^* le prolongement naturel de φ à $\mathrm{Alg}(K)$).*
(4) *Si $(A, \leq)$ est κ-saturé alors L et K sont κ-saturés.*

Remarque: Si on ne précisait pas "de Bezout", le même résultat serait vrai, mais avec $L \leq_\exists L'$, $L \preceq L' \ldots$ *etc.* seulement en tant que demi-treillis supérieurs et non en tant que treillis comme c'est le cas ici.

Preuve:
(2) et (4) découlent immédiatement du fait que le corps des fractions et le treillis résiduel d'un r-domaine de Bezout sont uniformément interprétables dans ce r-domaine.
(3) Si $(A, \leq) \equiv (A', \leq')$ ils ont des extensions élémentaires isomorphes. On prend alors pour φ la restriction à $\mathrm{Alg}(A)$ d'un tel isomorphisme.
(1) L'argument de (2) peut s'appliquer, mais c'est plus délicat ici car seules les formules existentielles sont autorisées, aussi préférons-nous un argument moins syntaxique. Si $(A, \leq) \leq_\exists (A', \leq')$ il existe un A-plongement Φ de $(A', \leq')$ dans une extension élémentaire $(A'', \leq'')$ de $(A, \leq)$. Notons Φ^* le prolongement naturel de ce plongement à K', et soient $K'' := \mathrm{Fr}(A'')$ et $L'' := \mathrm{L}(A'', \leq'')$. Puisque A est de Bezout A'' aussi (contrairement à l'$\cap$-stabilité, nous savons que la propriété de Bezout est du premier ordre), donc $(A'', \leq'')$ est $\cap$-stable et l'on a :
– Φ^* est un K-plongement de K' dans K'', et $K \preceq K''$ d'après (2), donc $K \leq_\exists K'$;
– $\overline{\Phi}$ est un L-plongement de L' dans L'', et $L \preceq L''$ d'après (2), donc $L \leq_\exists L'$ (au sens des treillis puisque d'après le corollaire 2.4 tout ces plongement respectent l'intersection).

■

L'essentiel de nos résultats consiste à montrer que toute l'information logique contenue dans un r-domaine PAC (resp. PRC, PC_M) se réduit en fait á celle portée par les structures plus simples que sont son corps des fractions et son treillis résiduel, en renversant les implications (1), (2) et (3) ci-dessus.

Nous utiliserons constamment la remarque suivante :

Remarque: Soient $(A,\leq)$ et $(A',\leq')$ deux r-domaines $\cap$-stables et localement booléens qui ne sont pas des corps, et notons L et L' leurs treillis résiduels.

$$\text{Si} \quad L\equiv L' \quad \text{alors} \quad (0)\in \mathrm{Sp}(A,\leq) \iff (0)\in\mathrm{Sp}(A',\leq').$$

En effet comme A est $\cap$-stable on sait par la propriété II.2.1 que A est complémenté si et seulement si L est une algèbre de Boole. Or A n'est pas un corps, donc en vertu de la remarque suivant la définition des anneaux localement complémentés (II.1) on sait que $(0)\notin \mathrm{Sp}(A,\leq_A)$ si et seulement si L est une algèbre de Boole. Si $L\preceq L'$ l'un est une algèbre de Boole si et seulement si l'autre l'est, donc $(0)\in\mathrm{Sp}(A,\leq)$ si et seulement si $(0)\in\mathrm{Sp}(A',\leq')$, comme annoncé.

Corollaire 3
Soient $(A,\leq)\subseteq(A',\leq')$ deux r-domaines $\cap$-stables et localement booléens qui ne sont pas des corps, et notons K, K' leur corps de fractions et L, L' leur treillis résiduel respectif. Si $(A,\leq)$ est PAC (resp. PRC, PC_M) alors :

$$(A,\leq)\leq_\exists (A',\leq') \quad\iff\quad L\leq_\exists L' \ \ \text{et}\ \ K\leq_\exists K'.$$

Preuve: Une implication est banale, nous l'avons vu. Pour la réciproque, supposons que $L\leq_\exists L'$ et que $K\leq_\exists K'$. Soit $(A'',\leq'')$ une extension élémentaire $|A'|^+$-saturée de $(A,\leq)$, K'' son corps des fractions, et L'' son treillis résiduel.

- $(A,\leq)$ est $\cap$-stable (car de Bezout) et $(A'',\leq'')$ est PAC (resp. PRC, PC_M).
- $K\leq_\exists K'$ et $K\preceq K''$ donc les extensions $K''|K$ et $K'|K$ sont régulières.
- $(0)\in\mathrm{Sp}(A'',\leq'') \iff (0)\in\mathrm{Sp}(A,\leq)$ (par l'axiome (o)) $\iff (0)\in\mathrm{Sp}(A',\leq')$ (par la remarque précédente).
- Le plongement de L dans L'' est élémentaire, L'' est $|L'|^+$-saturée et $L\leq_\exists L'$, donc il existe un plongement σ de L' dans L'' au dessus de L.
- De même le plongement de K dans K'' est élémentaire, K'' est $|K'|^+$-saturé et $K\leq_\exists K'$, donc il existe un K-plongement de K' dans K''.

Si tous les corps sont parfaits, le plongement de K' dans K'' induit un épimorphisme $\pi : G(K'')\longrightarrow G(K')$ commutant à l'opération de restriction à K^a, et le théorème de plongement régulier (version I) s'applique : $(A',\leq')$ se plonge au-dessus de A dans $(A'',\leq'')$, et comme $(A,\leq)\preceq(A'',\leq'')$ on a bien $(A,\leq)\leq_\exists(A',\leq')$.

Sinon, c'est qu'on est en caractéristique positive et que $(A,\leq)$ (et donc aussi $(A'',\leq'')$) est PAC. Malheureusement, le théorème de plongement régulier (même en version II) ne permet pas d'obtenir directement la conclusion. Néanmoins si l'on regarde sa preuve, on voit que σ suffit à construire une extension $(A^\circ,\leq^\circ)$ commune à $(A',\leq')$ et $(A'',\leq'')$ telle que $(A'',\leq'')\leq_\exists(A^\circ,\leq^\circ)$ (ce n'est qu'au moment du plongement de $(A',\leq')$ dans $(A'',\leq'')$ que l'hypothèse suplémentaire $[K':K'^p]\leq[K'':K''^p]$ était nécessaire, afin de construire un plongement qui soit régulier). Puisque $(A,\leq)\preceq(A'',\leq'')$ il s'ensuit que $(A,\leq)\leq_\exists(A^\circ,\leq^\circ)$ et *a fortiori* $(A,\leq)\leq_\exists(A',\leq')$.

■

Proposition 4
Soient $(A',\leq')$ et $(A'',\leq'')$ deux r-domaines PAC (resp. PRC, PC_M) extensions d'un même r-domaine $\cap$-stable $(A,\leq)$. Notons K, K', K'' leurs corps des fractions, et L, L', L'' leurs treillis résiduels. On suppose que :

– *A' et A'' ne sont pas des corps ;*
– *K' et K'' sont des extensions régulières de K.*
Alors :

$$((A',\leq'),A)\equiv((A'',\leq''),A) \quad\Longleftrightarrow\quad (L',L)\equiv(L'',L) \text{ et } (K',K)\equiv(K'',K).$$

Preuve: Pour alléger l'écriture je sous-entends les relations radicales, en notant A pour $(A,\leq)$. L'implication de gauche à droite est banale, pour la réciproque nous devons montrer qu'il existe un A-isomorphisme entre des extensions élémentaires de A' et A''. Nous allons construire un tel isomorphisme par récurence.

• Initialisation : On pose $A_0 := A$, $A_1 := A'$ et $A_2 :=$ une extension élémentaire $|A'|^+$-saturée de A''. Comme le treillis résiduel L_2 de A_2 est une extension élémentaire de L'', on a encore $(L_2,L)\equiv(L',L)$. Les propriétés élémentaires de A'' sont conservées par A_2 ; en particulier (0) est r-clos dans A_2 si et seulement s'il l'est dans A'' (par l'axiome (o)) si et seulement s'il l'est dans $A'=A_1$ (parce que ce ne sont pas des corps), et A_2 est un r-domaine PAC (resp. PRC, PC_M). Enfin $K''\preceq K_2$ donc K_2 est une extension régulière de K'', donc aussi de K, et on a $(K_1,K)\equiv(K_2,K)$ ce qui entraîne que $(\Phi G(K_1),K)\equiv(\Phi G(K_2),K)$. Notons que $K_1\equiv K'\equiv K''\equiv K_2$ donc tous ces corps ont même degré d'imperfection.

• Itération : On dispose de trois r-domaines $\cap$-stables A_n, A_{n+1} et A_{n+2}, ayant respectivement pour corps des fractions K_n, K_{n+1}, K_{n+2} et pour treillis résiduels L_n, L_{n+1}, L_{n+2} tels que :
(i$_\mathrm{n}$) $\forall k\in[\![1,n]\!]$, $A_k\preceq A_{k+2}$;
(ii$_\mathrm{n}$) A_{n+2} est $|A_{n+1}|^+$-saturée ;
(iii$_\mathrm{n}$) A_n est un sous-r-domaine commun à A_{n+1} et A_{n+2} ;
(iv$_\mathrm{n}$) K_{n+1} et K_{n+2} sont des extensions régulières de K_n et ont même degré d'imperfection ;
(v$_\mathrm{n}$) $(L_{n+2},L_n)\equiv(L_{n+1},L_n)$.
(vi$_\mathrm{n}$) $(\Phi G(K_{n+1}),K_n)\equiv(\Phi G(K_{n+2}),K_n)$.
On prend pour A_{n+3} une extension élémentaire $|A_{n+2}|^+$-saturée de A_{n+1}, et on note $K_{n+3}=\mathrm{Fr}(A_{n+3})$ et $L_{n+3}=\mathrm{L}(A_{n+3},\leq_{n+3})$. Pour faire de A_{n+1} une sous-structure commune à A_{n+2} et A_{n+3} on va recourir au théorème de plongement régulier.

Comme A_{n+2} et A_{n+1} sont des extensions élémentaires de A' et A'', ce sont des r-domaines PAC (resp. PRC, PC_M) ; et comme la satisfaction de l'axiome (o) est conservée par extension élémentaire on a $(0)\in\mathrm{Sp}(A_{n+2},\leq)$ si et seulement si $(0)\in\mathrm{Sp}(A_{n+1},\leq)$. Par saturation de L_{n+2}, et par (v$_\mathrm{n}$), il existe un plongement élémentaire σ_n de L_{n+1} dans L_{n+2} au dessus de L_n. De même, par saturation de $\Phi G(K_{n+2})$ et par (vi$_\mathrm{n}$) il existe un plongement élémentaire de $\Phi G(K_{n+1})$ dans $\Phi G(K_{n+2})$ au dessus de $\Phi G(K_n)$, qui induit un épimorphisme $\pi_n : G(K_{n+2})\longrightarrow G(K_{n+1})$ compatible avec l'opération de restriction à K^s. Enfin K_{n+1} et K_{n+2} ont même degré d'imperfection, donc si on est en caractéristique p on a $[K_{n+2}^p : K_{n+2}]\geq[K_{n+1}^p : K_{n+1}]$ (si le degré d'imperfection est fini on a en fait une égalité, s'il est infini c'est l'hypothèse de saturation de K_{n+2} qui donne l'inégalité). Le théorème de plongement nous donne donc un A_n-plongement $\varphi_n : A_{n+1}\longrightarrow A_{n+2}$ qui fait de K_{n+2} une extension régulière de K_{n+1}, tel que $\overline{\varphi}_n=\sigma_n$ et que l'épimorphisme associé $\varphi_n^* : G(K_{n+2})\longrightarrow G(K_{n+1})$ coïncide avec π_n.

Les conditions (i_{n+1}) et (ii_{n+1}) sont satisfaites par définition de A_{n+3}, et (iii_{n+1}) l'est en identifiant A_{n+1} à son image.

L'extension $K_{n+3}|K_{n+2}$ est régulière par construction de φ_n, et d'autre part $K_{n+1} \preceq K_{n+3}$ donc l'extension $K_{n+3}|K_{n+1}$ est aussi régulière. De plus le degré d'imperfection de K_{n+3} est le même que celui de K_{n+1} et de K_{n+2}, d'où (iv_{n+1}).

$L_{n+1} \preceq L_{n+3}$ *i.e.* $(L_{n+3}, L_{n+1}) \equiv (L_{n+1}, L_{n+1})$ et, le plongement σ_n étant élémentaire, on a $L_{n+1} \preceq L_{n+2}$ *i.e.* $(L_{n+2}, L_{n+1}) \equiv (L_{n+1}, L_{n+1})$ d'où (v_{n+1}).

Enfin $K_{n+1} \preceq K_{n+3}$, *i.e.* $(K_{n+3}, K_{n+1}) \equiv (K_{n+1}, K_{n+1})$ donc $(\Phi G(K_{n+3}), K_{n+1}) \equiv (\Phi G(K_{n+1}), K_{n+1})$. D'autre part l'épimorphisme de restriction induit par φ_n de $G(K_{n+2})$ sur $G(K_{n+1})$ n'est autre que π_n, donc le plongement $\Phi\pi_n$ associé est élémentaire : $\Phi G(K_{n+1}) \preceq \Phi G(K_{n+2})$, *i.e.* $(\Phi G(K_{n+2}), K_{n+1}) \equiv (\Phi G(K_{n+1}), K_{n+1})$, d'où finalement (vi_{n+1}) ce qui achève la récurrence.

La construction ci-dessus nous donne deux chaînes élémentaires :

$$A_1 \preceq A_3 \preceq \cdots \preceq A_{2n+1} \preceq \cdots \quad \text{et} \quad A_2 \preceq A_4 \preceq \cdots \preceq A_{2n} \preceq \cdots$$

avec pour chaque entier non nul n un plongement φ_n de A_n dans A_{n+1}, tel que le diagramme représentant tous ces morphismes soit commutatif.
Posons $B' := \bigcup_{n\in\mathbb{N}} A_{2n+1}$, $B'' := \bigcup_{n\in\mathbb{N}} A_{2n}$, $\varphi' := \bigcup_{n\in\mathbb{N}} \varphi_{2n+1}$ et $\varphi'' := \bigcup_{n\in\mathbb{N}} \varphi_{2n}$.

Par construction, $A' = A_1 \preceq B'$, $A'' \preceq A_2 \preceq B''$, et φ' est un isomorphisme de B' dans B'', de réciproque φ''. Comme pour tout n, $\varphi_{n|A}$ est l'identité, on a $\varphi'_{|A} = Id_A$, et φ' est l'isomorphisme cherché.

■

Corollaire 5
Soient $(A, \leq) \subseteq (A', \leq')$ des r-anneaux PAC (resp. PRC, PC_M) qui ne sont pas des corps. Notons L, L' leurs treillis résiduels et K, K' leurs corps des fractions respectifs. Alors :

$$(A, \leq) \preceq (A', \leq') \qquad \Longleftrightarrow \qquad L \preceq L' \quad \textit{et} \quad K \preceq K'.$$

Preuve: Puisque $L \preceq L'$ on a $(L, L) \equiv (L', L)$, et de même $(K, K) \equiv (K', K)$, donc il suffit d'appliquer la proposition 4 en prenant $A'' = A$.
Il vient : $((A, \leq), A) \equiv ((A', \leq'), A)$ *i.e.* $(A, \leq) \preceq (A', \leq')$. La réciproque est banale.

■

Corollaire 6
Soient $(A, \leq), (A', \leq')$ des r-anneaux PAC (resp. PRC, PC_M) qui ne sont pas des corps. Notons L, L' leurs treillis résiduels et K, K' leurs corps de fractions .
Alors $(A, \leq) \equiv (A', \leq')$ si et seulement s'il existe un isomorphisme $\varphi : \mathrm{Alg}(A, \leq) \longrightarrow \mathrm{Alg}(A', \leq')$ tel que :

$$(L, \mathrm{Alg}(L)) \equiv (L', \overline{\varphi}[\mathrm{Alg}(L)]) \quad \textit{et} \quad (K, \mathrm{Alg}(K)) \equiv (K', \varphi^*[\mathrm{Alg}(K)])$$

où φ^* est le prolongement naturel de φ à $\mathrm{Alg}(K) = \mathrm{Fr}(\mathrm{Alg}(A))$.

Preuve: Les conditions de la CNS signifient précisément que quand $\mathrm{Alg}(A, \leq)$ est identifié à son image par φ, il devient une sous-structure commune à $(A, \leq)$ et $(A', \leq')$, donc un sous-r-domaine commun à $(A, \leq)$ et $(A', \leq')$, tel que $(L, \mathrm{Alg}(L)) \equiv (L', \mathrm{Alg}(L))$ et $(K, \mathrm{Alg}(K)) \equiv (K', \mathrm{Alg}(K))$. On peut donc appliquer la proposition 4 : il vient $(A, \mathrm{Alg}(A)) \equiv (A', \mathrm{Alg}(A))$, et *a fortiori* $(A, \leq) \equiv (A', \leq')$. La réciproque est immédiate.

■

Le cas particulier suivant mérite d'être isolé, car il permet de retrouver les résultats qui ont motivé cette thèse :

Corollaire 7 (le cas algébriquement clos)
Soient A, A' des anneaux intègres tels que :
- *A et A' sont PAC et ne sont pas des corps ;*
- *$\mathrm{Fr}(A)$ et $\mathrm{Fr}(A')$ sont algébriquement clos.*

Notons $L := \mathrm{L}(A, \leq_A)$, et $L' := \mathrm{L}(A', \leq_{A'})$. Alors :
(a) *Si $(A, \leq_A) \subseteq (A', \leq_{A'})$, on a : $(A, \leq_A) \preceq (A', \leq') \iff L \preceq L'$.*
(b) *$(A, \leq_A) \preceq (A', \leq_{A'})$ si et seulement s'il existe un isomorphisme φ de $\mathrm{Alg}(A, \leq_A)$ dans $\mathrm{Alg}(A', \leq_{A'})$ tel que $(L, \mathrm{Alg}(L)) \equiv (L', \overline{\varphi}(\mathrm{Alg}(L))$.*

Preuve: C'est le cas particulier des deux corollaires précédents quand les corps de fractions sont algébriquement clos.

■

Remarque: Dans le cas où les treillis résiduels sont denses on retrouve dans ce corollaire l'essentiel des résultats de [VdD-M] et [P-S 90].

Un autre cas particulier du corollaire 6 qui mérite notre attention, car il donne un critère significativement plus simple pour l'équivalence élémentaire (ce qui nous servira dans les applications), est celui de la caractéristique positive.

Corollaire 8
Deux anneaux PAC de même caractéristique positive qui ne sont pas des corps sont élémentairement équivalents si et seulement si leurs corps des fractions et leurs treillis résiduels respectifs sont élémentairement équivalents.

Preuve: Soient A, A' deux anneaux PAC de même caractéristique p, soient K, K' leurs corps des fractions et L, L' leurs treillis résiduels. On sait déjà que si $A \equiv A'$ alors $L \equiv L'$ et $K \equiv K'$, il suffit donc de vérifier la réciproque.

Puisque $K \equiv K'$ on a un isomorphisme φ^* de $\mathrm{Alg}(K)$ sur $\mathrm{Alg}(K')$ tel que $(K, \mathrm{Alg}(K)) \equiv (K', \varphi[\mathrm{Alg}(K)])$. La relation radicale de $(A, \leq)$ est définie par $\mathrm{Spm}(A)$ donc $1 \not\leq 0$, et ceci étant aussi vrai dans $\mathrm{Alg}(A, \leq)$ on a $\mathrm{Sp}(\mathrm{Alg}(A, \leq)) \neq \emptyset$. La caractéristique étant non nulle $\mathrm{Alg}(A)$ est un corps, donc $\mathrm{Sp}(\mathrm{Alg}(A, \leq)) = \{0\}$. Il en va de même pour A', et $\varphi = \varphi^*$ est donc en fait un isomorphisme de r-domaine de $\mathrm{Alg}(A, \leq)$ sur $\mathrm{Alg}(A', \leq')$. Enfin $\mathrm{Alg}(L)$ et $\mathrm{Alg}(L')$ sont réduits à leurs extrémités donc $L \equiv L'$ implique que $(L, \mathrm{Alg}(L)) \equiv (L', \mathrm{Alg}(L'))$.

Le corollaire 6 entraîne donc que $(A, \leq_A) \equiv (A', \leq_{A'})$ et *a fortiori* que $A \equiv A'$.

■

§6. Applications

De façon un peu arbitraire, nous avons isolé les applications les plus algébriques qui seront présentées au prochain paragraphe. Celui-ci est consacré aux propriétés modèle-théoriques de différents anneaux "classiques".

On reprend les notations du I.2 : si k est un corps de nombres et Σ un ensemble de places de k, on note $\mathcal{F}(\Sigma)$ l'ensemble des extensions algébriques de k qui sont k-isomorphes à $k_v \cap k^a$ avec $v \in \Sigma$, et $k(\Sigma) := \bigcap \mathcal{F}(\Sigma)$.

Lemme 1

Soit k un corps de nombre, Σ un ensemble fini de places de k, et $\mathcal{F} \subseteq \mathcal{F}(\Sigma)$.
Alors la clôture intégrale de $\mathbb{Z}$ dans $\cap\mathcal{F}$ est localement booléenne et $\cap$-stable, et son treillis résiduel est dense.

Preuve: Notons $\mathbb{Z}_{\mathcal{F}}$ la clôture intégrale de $\mathbb{Z}$ dans $\cap\mathcal{F}$. On sait d'après la proposition II.1.5 que $\mathbb{Z}_{\mathcal{F}}$ est localement booléen et $\cap$-stable, donc son treillis résiduel est une quasi-algèbre de Boole, et il suffit de montrer qu'il n'a pas d'atome. Il est facile de se convaincre que cela revient à vérifier que tout élément non inversible de $\mathbb{Z}_{\mathcal{F}}$ appartient à au moins deux idéaux maximaux de $\mathbb{Z}_{\mathcal{F}}$. L'argument est emprunté à [P-S 91].

Soit donc a un élément non inversible de $\mathbb{Z}_{\mathcal{F}}$. Posons $k' := k[a]$ et soit Σ' l'ensemble des places de k' prolongeant les éléments de Σ. On a clairement $k'(\Sigma') \subseteq k(\Sigma) \subseteq \cap\mathcal{F}$, et on pose $A := \mathbb{Z}_{\mathcal{F}} \cap k'$.

Comme a n'est pas inversible dans A il appartient à un idéal maximal $\mathfrak{m}$ de A. Notons $v_{\mathfrak{m}}$ la place de k' associée à $A_{\mathfrak{m}}$; k' est une extension finie de k donc Σ' est fini. Soit w une place finie de k' n'appartenant pas à $\Sigma' \cup \{v_{\mathfrak{m}}\}$, et soit b un élément de A qui ne soit pas un carré dans k'_w. Le théorème d'approximation simultanée pour les places indépendantes permet de trouver $x \in k'$, arbitrairement proche de b au sens de w et de 1 au sens des éléments de $\Sigma' \cup \{v_{\mathfrak{m}}\}$.

Il s'ensuit que x possède une racine carrée c dans chaque k'_v pour $v \in \Sigma' \cup \{v_{\mathfrak{m}}\}$, et pas dans k'_w, donc $c \in k'(\Sigma')$ et $k'[c]$ est une extension stricte de k'. Comme $c \in k'_{v_{\mathfrak{m}}}$, $v_{\mathfrak{m}}$ admet deux prolongements différents à $k'[c]$ *i.e.* $\mathfrak{m}$ se scinde dans $\mathbb{Z}_{\mathcal{F}} \cap k'[c]$ en deux idéaux distincts $\mathfrak{m}_1$ et $\mathfrak{m}_2$. Comme $k'[c] \subseteq k'(\Sigma')$ et que $\mathbb{Z}_{\mathcal{F}}$ est entier sur $\mathbb{Z}_{\mathcal{F}} \cap k'[c]$, $\mathfrak{m}_1$ et $\mathfrak{m}_2$ se relèvent en deux idéaux maximaux de $\mathbb{Z}_{\mathcal{F}}$ distincts et contenant a, ce qui achève la démonstration.

■

Lemme 2

Soit K une extension séparablement close de $\mathbb{F}_p(T)$, ou encore $K = \mathbb{F}_p[[T]]$.
Alors la clôture intégrale de $\mathbb{F}_p[T]$ dans K est localement booléen et $\cap$-stable, et son treillis résiduel est dense.

Preuve: La démonstration du lemme 1 s'adapte sans problème aux cas considérés.

■

Le lemme suivant est admis dans [P-S 90]. Ils y donnent l'idée de la preuve qui est de s'inspirer du résultat analogue sur les algèbres de Boole denses non triviales. Nous l'admettrons nous aussi pour l'instant, mais le lecteur exigeant trouvera en annexe une étude des quasi-algèbres de Boole incluant sa démonstration.

Lemme 3

Soit T la théorie des quasi-algèbres de Boole propres (dans le langage $\{\mathbf{0}, \mathbf{1}, \wedge, \vee\}$ des treillis avec extrémités).
La théorie T^* des quasi-algèbres de Boole propres et denses est complète et modèle-complète, c'est le modèle-compagnon de T.

Anneaux PAC

Proposition 4
Un anneau PAC de caractéristique positive est décidable si et seulement si son corps des fractions et son treillis résiduel sont décidables.

Preuve: Une implication est banale, pour la réciproque soit A un anneau PAC de caractéristique $p \neq 0$ ayant un corps des fractions et un treillis résiduel décidables. Si A est un corps, il est clairement décidable, sinon soit T_f (resp. T_l) la théorie complète de $\mathrm{Fr}(A)$ (resp. $\mathrm{L}(A, \leq_A)$). D'après le corollaire 5.8, un anneau B est élémentairement équivalent à A si et seulement si B satisfait les propriétés suivantes :

- B est PAC et n'est pas un corps ;
- $\mathrm{Fr}(B) \models T_f$ et $\mathrm{L}(B, \leq_B) \models T_l$.

Cette classe est élémentaire (seule l'axiomatisabilité de PAC est non triviale, mais nous l'avons démontrée précédemment) et puisque par hypothèse T_f et T_l sont décidables, elle est récursivement axiomatisable et complète, donc décidable.

■

Corollaire 5
La clôture intégrale de $\mathbb{F}_p[T]$ dans un corps séparablement clos quelconque est décidable.

Preuve: Cet anneau satisfait le LGPA, *i.e.* est PAC, en vertu du théorème de Moret-Bailly. Si on le munit de sa relation radicale associée, son treillis résiduel est une quasi-algèbre de Boole propres et denses (nous avons rappelé que la théorie des quasi-algèbres de Boole propre et dense était complète, et elle est clairement récursivement axiomatisable, donc décidable) et son corps des fractions est séparablement clos, de caractéristique p et de degré d'imperfection 0 ou 1 selon que le corps dans lequel est pris la clôture intégrale de $\mathbb{F}_p[T]$ est ou non algébriquement clos (et ces deux théories sont connues pour être décidables). C'est donc une conséquence directe de la proposition 4.

■

Remarque: Dans [VdD-M] était prouvée la décidabilité de la clôture intégrale de $\mathbb{F}_p[T]$ dans $\mathbb{F}_p(T)^a$. Plus exactement, en notant $\mathbb{F}_p[T]^a$ cet anneau, il était montré que pour toute partie multiplicative S de $\mathbb{F}_p[T]^a$ ne contenant pas 0, si le localisé de $\mathbb{F}_p[T]^a$ par S a pour treillis résiduel une quasi-algèbre de Boole propre et dense alors il est décidable.

Nous n'avons fait que généraliser ce résultat sous la forme d'une condition nécessaire et suffisante : $S^{-1}\mathbb{F}_p[T]^a$ est décidable si et seulement si son treillis résiduel est décidable (ce qui est le cas pour une quasi-algèbre de Boole propre et dense). En outre cela reste vrai en remplaçant la clôture algébrique par la clôture séparable.

Anneaux PRC

Notations: Le corps des nombres absolument réels est noté $\mathbb{Q}_{r-abs}$.
La clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_{r-abs}$ est notée $\mathbb{Z}_{r-abs}$.
Pour tout anneau intègre A et tout $a \in A \setminus \{0\}$, on notera $A(a) := S_a^{-1}A$ où $S_a := A \setminus \cup M(a)$, et $A^\circ(a) := S_a^{\circ\,-1}A$ où $S_a^\circ := A \setminus \cup M(a)^c$.

Le théorème de Moret-Bailly montre que $\mathbb{Q}_{r-abs}$ est pseudo réel clos et que quel que soit $a \in \mathbb{Z}_{r-abs}$ non nul et non inversible $\mathbb{Z}_{r-abs}(a)$ et $\mathbb{Z}^\circ_{r-abs}(a)$ satisfont le LGPH' et donc sont PRC' (c'est une conséquence directe du théorème I.2.3, en prenant

$k := \mathbb{Q}[a]$, pour Σ l'ensemble des places réelles de k plus celles associées aux éléments de $W_{\mathbb{Z}_{r-abs}(a)\cap k}$ ou $W_{\mathbb{Z}^\circ_{r-abs}(a)\cap k}$, et pour Σ_0 les places réelles de k, et en remarquant que le fait d'avoir supposé a non nul et non inversible garantit qu'en localisant par S_a ou S_a° on écarte bien de Σ au moins une place non triviale de k).

La propriété PRC est stable par clôture intégrale donc pour toute famille $\mathcal{F}$ de clôtures réelles de $\mathbb{Q}$ il vient, en notant $\mathbb{Z}_\mathcal{F}$ la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_\mathcal{F} := \cap\mathcal{F}$, que pour tout $a \in \mathbb{Z}_\mathcal{F}$ non nul et non inversible $\mathbb{Z}_\mathcal{F}(a)$ et $\mathbb{Z}^\circ_\mathcal{F}(a)$ sont PRC'.

Proposition 6

Soit a un entier non nul et $\mathcal{F}$ une famille quelconque de clôtures réelles de $\mathbb{Q}$. Avec les notations ci-dessus, soit $A := \mathbb{Z}^\circ_\mathcal{F}(a)$ (resp. $\mathbb{Z}_\mathcal{F}(a)$), et supposons que A satisfasse le LGPH' (comme nous l'avons rappelé, c'est toujours le cas si a n'est pas inversible).

(1) *Un r-domaine $(A', \leq')$ est élémentairement équivalent à $(A, \leq_A)$ si et seulement s'il vérifie les propriétés suivantes :*

- (a) *$(A', \leq')$ est PAC ;*
- (b) *$(A', \leq') \models (o)$ (resp. $\neg(o)$) ;*
- (c) *$\mathrm{L}(A', \leq')$ est dense et non réduit à un élément ;*
- (d) *$\mathrm{Fr}(A') \models \mathrm{Th}(\mathbb{Q}_\mathcal{F})$;*
- (e) *$A' \models \forall x f(x) \neq (0)$, pour tout $f \in \mathbb{Z}[X]$, irréductible, à coefficients globalement étrangers, dont le coefficient dominant possède d'autre facteurs premiers que ceux de a (resp. n'est pas étranger à a) ;*
- (f) *$A' \models \exists b(ab = 1)$ (resp. $0 \leq a$).*

(2) *Si $\mathrm{Th}(\mathbb{Q}_\mathcal{F})$ est modèle-complète, alors $\mathrm{Th}(A, \leq_A)$ aussi.*

(3) *A est décidable si et seulement si $\mathbb{Q}_\mathcal{F}$ est décidable.*

Preuve:

(1) Les propriétés (a) à (f) sont du premier ordre et sont vérifiées par $(A, \leq_A)$, donc tout r-anneau élémentairement équivalent à $(A, \leq_A)$ les satisfait aussi.

Inversement, soit $(A', \leq')$ un r-anneau vérifiant ces propriétés. Soient L, L', K et K' les treillis résiduels et les corps de fractions respectifs de $(A, \leq_A)$ et $(A', \leq')$.

Les conditions (d), (e) et (f) entraînent que $\mathrm{Alg}(A') \simeq A$. Après identification, la propriété 5.1 montre que $\mathrm{Alg}(A', \leq') = (A, \leq_A)$ puisque $(0) \in \mathrm{Sp}(A', \leq') \iff (0) \in \mathrm{Sp}(A, \leq_A)$ d'après (b).

Pour pouvoir appliquer le corollaire 5.6, il suffit donc de vérifier que $(L, L) \equiv (L', L)$ et $(K, K) \equiv (K', K)$. La première condition est vérifiée parce que $L \subseteq L'$ sont tous deux modèles, d'après (b) et (c), de la théorie des quasi-algèbres de Boole propres et denses (resp. des algèbres de Boole denses), et que cette théorie est modèle-complète, donc $L \preceq L'$, *i.e.* $(L, L) \equiv (L', L)$. D'autre part (c) entraîne que $K' \equiv K$, donc ils ont des ultrapuissances isomorphes. Cet isomorphisme conserve les parties algébriques, donc est un K-isomorphisme, d'où $(K, K) \equiv (K', K)$, et enfin $(A', \leq') \equiv (A, \leq_A)$.

(2) Supposons maintenant que $\mathrm{Th}(\mathbb{Q}_\mathcal{F})$ soit modèle-complète, et soient $(A', \leq') \subseteq (A'', \leq'')$ deux modèles $\mathrm{Th}(A, \leq_A)$. Ce sont tous les deux des $\mathrm{r}_\circ$-domaines (resp. des r-domaines) PRC' et leurs treillis résiduels sont denses, donc $\mathrm{L}(A', \leq') \preceq \mathrm{L}(A'', \leq'')$. D'autre part $\mathrm{Fr}(A')$ et $\mathrm{Fr}(A'')$ sont modèles de la théorie modèle-complète $\mathrm{Th}(\mathbb{Q}_\mathcal{F})$, donc $\mathrm{Fr}(A') \preceq \mathrm{Fr}(A'')$. Le corollaire 5.5 s'applique, et donne $(A', \leq') \preceq (A'', \leq'')$. La théorie complète de A est donc bien modèle-complète.

(3) Une implication est banale. Pour l'autre, on note que les conditions (a), (b), (c),

(e) et (f) sont récursivement axiomatisables (nous avons donné des schémas d'axiomes pour les premières, et c'est à peu près trivial pour la dernière). Si de plus $\mathrm{Fr}(A) = \mathbb{Q}_{\mathcal{F}}$ est décidable, on peut axiomatiser récursivement sa théorie, et donc la propriété (d). Il s'ensuit que les conditions (a) à (f) forment une axiomatisation récursive de la théorie de A qui, étant complète, est donc décidable.

■

On sait (cf [FHV]) que $\mathbb{Q}_{r-abs}$ est décidable. Cela nous fourni un joli cas d'application de la proposition 6. Les auteurs de [FHV], répondant à une question de [Rob 65], soulignaient que $\mathbb{Z}_{r-abs}$ est un exemple remarquable d'anneau indécidable dont le corps des fractions est tout de même décidable. Nous renchérissons en ajoutant que de nombreux sur-anneaux de $\mathbb{Z}_{r-abs}$ (en plus de son corps des fractions) sont eux-aussi décidables :

Corollaire 7
Pour tout entier $a \in \mathbb{N} \setminus \{0,1\}$ les anneaux $\mathbb{Z}^{\circ}_{r-abs}(a)$ et $\mathbb{Z}_{r-abs}(a)$ sont décidables.

On retrouve également par cette voie les résultats de [P-S 90] et [P-S 91] :

Corollaire 8
La clôture intégrale de $\mathbb{Z}$ dans $\mathbb{R}$ ou $\mathbb{C}$ est décidable, et sa théorie dans $\mathrm{L}_{\mathrm{rad}}$ est modèle-complète.

Preuve: La théorie d'une clôture réelle ou algébrique de $\mathbb{Q}$ étant décidable et modèle-complète, c'est un cas d'application de la proposition 6.

■

Anneaux PC'$_M$

Soit M un ensemble fini de couples (p,d) où p est un nombre premier et $d \in \mathbb{N}^*$. Soit K un corps et W_M l'ensemble des anneaux des p-valuations de rang d de K, pour (p,d) décrivant M. Nous rappelons que si K est PC_M alors $\cap W_M$ est appelé l'**anneau d'holomorphie** de K, et qu'il est définissable dans K (dans le langage de anneaux). On note $\mathbb{Q}_{M-abs}$ l'ensemble des nombres algébriques absolument M-adiques (*i.e.* l'intersection de l'ensemble des corps p-adiquement clos de rang d algébriques sur $\mathbb{Q}$, pour (p,d) décrivant M) et $\mathbb{Z}_{M-abs}$ la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_{M-abs}$.

Proposition 9
Soit K un corps PC_M algébrique sur $\mathbb{Q}$, a un entier non nul divisible par (resp. étranger à) tout p tel que $(p,d) \in M$, et soit A la clôture intégrale de $\mathbb{Z}^{\circ}(a)$ (resp. $\mathbb{Z}(a)$) dans K.

(1) *Un r-domaine $(A', \leq')$ est élémentairement équivalent à $(A, \leq_A)$ si et seulement s'il satisfait les propriétés suivantes :*
   (a) *$(A', \leq')$ est PC_M ;*
   (b) *$(A', \leq') \models (o)$ (resp. $\neg(o)$) ;*
   (c) *$\mathrm{L}(A', \leq')$ est dense et non réduit à un élément ;*
   (d) *$\mathrm{Fr}(A') \models \mathrm{Th}(K)$;*
   (e) *$A' \models \forall x (f(x) \neq 0)$, pour tout polynôme f à coefficients entiers globalement étrangers, dont le coefficient dominant possède d'autres facteurs premiers que ceux de a (resp. n'est pas étranger à a) ;*
   (f) *$\exists b(ab = 1)$ (resp. $0 \leq a$).*

(2) *Si $\mathrm{Th}(K)$ est modèle-complète, alors $\mathrm{Th}(A, \leq_A)$ aussi.*

(3) *A est décidable si et seulement si K est décidable.*

Preuve: Elle est identique à celle de la proposition 6. Notons que a est choisi de façon que tout $R \in W_A$ vèrifie $R^h = R^a$ (afin que A satisfasse bien le LGPA').

■

Corollaire 10
$\mathbb{Z}_{M-abs}$ est décidable si et seulement si $\mathbb{Q}_{M-abs}$ est décidable.

Preuve: Soit a le produit des p tels que $(p, d) \in M$, soit A la clôture intégrale de $\mathbb{Z}^\circ(a)$ dans $\mathbb{Q}_{M-abs}$ et soit B l'anneau d'holomorphie de $\mathbb{Q}_{M-abs}$. On sait par le théorème de Moret-Bailly que $\mathbb{Q}_{M-abs}$ est PC_M et que $\mathbb{Z}_{M-abs}$ satisfait le LGPH, donc A est PC_M (A satisfait le LGPH' en tant que localisé d'un anneau satisfaisant le LGPH, et $W_A \cap W_M = \emptyset$, or on sait que tout anneau de valuation d'un corps PC_M n'appartenant pas à W_M a un hensélisé séparablement clos, donc A satisfait le LGPA' par la proposition III.4.3). La proposition 9 s'applique : A est décidable si et seulement si $\mathbb{Q}_{M-abs}$ est décidable. D'autre part $\mathbb{Z}_{M-abs} = A \cap B$, et B est définissable dans $\mathbb{Q}_{M-abs}$ donc aussi dans A. Il s'ensuit que si A est décidable alors $\mathbb{Z}_{M-abs}$ l'est aussi. Donc si $\mathbb{Q}_{M-abs}$ est décidable, $\mathbb{Z}_{M-abs}$ l'est aussi, et la réciproque est banale.

■

Remarque: Un résultat assez récent de Pop élucide totalement la structure du groupe absolu de Galois de $\mathbb{Q}_{p-abs}$. Il m'a aimablement confirmé que son théorème impliquait que $\mathbb{Q}_{p-abs}$ était décidable, et que cette conséquence n'a malheureusement pas été publiée.

Corollaire 11
L'anneau $\mathbb{Z}_{p-abs}$ de tous les entiers algébriques absolument p-adiques est décidable.

§ 7. Le coin des algébristes

Proposition 1
Soit A un anneau intègre. Sont équivalents :
(i) *A est PAC ;*
(ii) *pour toute variété V définie sur $K := \mathrm{Fr}(A)$,*

$$V(A) \neq \emptyset \quad \iff \quad \forall R \in W_A,\ V(R^a) \neq \emptyset$$

(iii) *pour toute variété V définie sur $K := \mathrm{Fr}(A)$, $V(A) = \emptyset$ si et seulement s'il existe un polynôme f à coefficients dans A et un élément α de A, non inversible, tels que $\alpha f - 1 \in I(V)$.*

Remarque: L'équivalence (i) $\iff$ (ii), qui signifie que pour le LGPA il n'y a pas besoin de demander que les point locaux soient lisses, a été démontrée dans [Ru 86] et [VdD-M] par les voies de la géométrie algébrique, dans le cas où $\mathrm{Fr}(A)$ est algébriquement clos (on peut alors se ramener à un nombre fini de points locaux et, même s'ils ne sont pas lisses, tracer sur la variété une courbe lisse passant par ces points, on applique alors le LGPA à cette courbe). Il est permis de croire que leur méthode marche aussi dans ce cas plus général.

De même, on peut déduire (iii) de (i) dans le cas de la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$, et pour la clôture intégrale de $\mathbb{F}_p[T]$ dans un corps séparablement clos, par des voies plus classiques que celles de la logique (la preuve repose sur le fait que ces anneaux sont entiers sur des anneaux noethériens).

Dans les deux cas, ces démonstrations nécessitent quelques bonnes notions d'algèbre, et des hypothèses suplémentaires. La preuve que nous proposons ici, typique de l'esprit "théorie des modèles", donne le résultat général, et a l'avantage d'être nettement plus simple (à mon avis).

Preuve: Il est commode d'introduire une quatrième condition équivalente, moins algébrique :

(iv) A est existentiellement clos (pour le langage des anneaux) dans tout anneau intègre B contenant A, tel que $L := \mathrm{Fr}(B)$ soit une extension régulière de K et que tout $\mathfrak{m} \in \mathrm{Spm}(A)$ se relève en un $\mathfrak{n} \in \mathrm{Spm}(B)$.

(i) $\Longleftrightarrow$ (iv) La proposition I.1.2 entraîne que A est PAC, c'est-à-dire qu'il satisfait le LGPA, si et seulement si $A \in \mathrm{RC}(\mathcal{R})$ où $\mathcal{R} = \{R^a \ / \ R \in W_A\}$, c'est-à-dire si et seulement si A est $\exists$-clos dans tout anneau intègre A' tel que :

– $A \subseteq A'$ et l'extension $\mathrm{Fr}(A')|\mathrm{Fr}(A)$ est régulière ;

– $\forall R \in W_A,\ A'$ se plonge au-dessus de A dans une extension élémentaire de R^a.

Supposons (iv), et soit A' un anneau satisfaisant les deux hypothèses ci-dessus. Pour tout $\mathfrak{m} \in \mathrm{Spm}(A)$, A' se plonge au-dessus de A dans une extension élémentaire $R(\mathfrak{m})$ de $A_\mathfrak{m}$, donc $1 \notin m(R(\mathfrak{m})) \cap A' \supseteq \mathfrak{m}A'$, et donc $\mathfrak{m}$ se relève en un idéal maximal de A'. La propriété (iv) entraîne donc que $A \leq_\exists A'$.

Inversement, soit B un anneau intègre contenant A, tel que $L := \mathrm{Fr}(B)$ soit une extension régulière de K et que tout $\mathfrak{m} \in \mathrm{Spm}(A)$ se relève en un $\mathfrak{n} \in \mathrm{Spm}(B)$. Soit $R \in W_A$; l'idéal $\mathfrak{m} := m(R) \cap A \in \mathrm{Spm}(A)$ donc se plonge dans $\mathfrak{n} \in \mathrm{Spm}(B)$, et $B_\mathfrak{n}$ se plonge à son tour (avec domination) dans un anneau de valuation R' de L. Celui-ci vérifie $A_\mathfrak{m} \subseteq R' \cap K \subseteq R$, et, A étant de Prüfer, $R = A_\mathfrak{m}$, donc $R' \cap K = R$. On sait que le plongement de R^a dans R'^a est élémentaire, donc B est plongé au-dessus de A dans une extension élémentaire de R^a. L'extension $L|K$ étant régulière, la propriété de clôture régulière entraîne que $A \leq_\exists B$ ce qui achève de prouver l'équivalence (i) $\Longleftrightarrow$ (iv).

(iv)$\Longrightarrow$(iii) Soit V une variété définie sur K, d'idéal $I_K(V) \subseteq K[X]$, $(X := (X_1, \ldots, X_n))$ et supposons $V(A) = \emptyset$. Soit x_V un point générique de V, et $B := A[x_V]$; la variété V possède un point dans B et pas dans A, donc A n'est pas $\exists$-clos dans B. Comme $\mathrm{Fr}(B) = K[x_V]$ est une extension régulière de K, c'est donc qu'il existe $\mathfrak{m} \in \mathrm{Spm}(A)$ tel que $1 \in \mathfrak{m}B = \mathfrak{m}[x_V]$. D'après ce qui précède (iv)$\Longrightarrow$(i), donc A est PAC et *a fortiori* de Bezout. Soient $g \in \mathfrak{m}[X]$ tel que $g(x_V) = 1$ et $\alpha \in A$ un pgcd des coefficients de g ; on a d'une part $\alpha \in \mathfrak{m}$ et d'autre part $f := \alpha^{-1}g \in A[X]$ et $\alpha f(x_V) - 1 = g(x_V) - 1 = 0$ *i.e.* $\alpha f - 1 \in I(V)$.

(iii)$\Longrightarrow$(ii) Soit V une variété définie sur K, telle que quel que soit $R \in W_A$, $V(R^a) \neq \emptyset$. Alors pour tout $f \in A[X]$ $(X := (X_1, \ldots, X_n))$ et tout $\alpha \in A \setminus A^*$, il existe $\mathfrak{m} \in M(\alpha)$, et $x_\mathfrak{m} \in V(A^a_\mathfrak{m})$, d'où $\alpha f(x_\mathfrak{m}) \in m(A_\mathfrak{m})$ en particulier $\alpha f(x_\mathfrak{m}) \neq 1$, et donc $\alpha f(X) - 1 \notin I(V)$. Le (iii) donne alors un point de V dans A.

(ii)$\Longrightarrow$(i) C'est immédiat.

■

Prestel et Schmid ont montré dans [P-S 90] que tout $\mathrm{r}_\circ$-domaine $(A, \leq)$ se plonge dans un $\mathrm{r}_\circ$-domaine $(A', \leq')$ satisfaisant LGPA, de corps des fractions algébriquement clos, de treillis résiduel dense, tel que tout idéal premier r-clos de $(A, \leq)$ se relève en un idéal maximal de A'. Nous réutilisons ce fait dans la preuve suivante.

Théorème 2
Soit A un anneau satisfaisant le LGPA, de treillis résiduel dense, de radical de Jacobson nul et de corps des fractions algébriquement clos. Alors pour tous $f_1, \ldots, f_m \in A[X_1, \ldots, X_n, Y]$ les assertions suivantes sont équivalentes :

(i) *$\forall \alpha \in A^n$, les $f_i(\alpha, Y)$ ont un zéro commun dans A,*

(ii) *il existe $f \in A[X_1, \ldots, X_n, Y] \setminus \{1\}$, unitaire en Y, qui divise simultanément tous les f_i (dans $A[X_1, \ldots, X_n, Y]$).*

Preuve: L'implication (ii)$\Longrightarrow$(i) est banale : si un polynôme f unitaire en Y divise simultanément $f_1, \ldots, f_m$ dans $A[X_1, \ldots, X_n, Y]$, alors pour tout $\alpha \in A^n$, $f(\alpha, Y)$ est un polynôme unitaire non constant (f unitaire et $f \neq 1$), donc il a une racine β dans $\mathrm{Fr}(A)$ entière sur A, *i.e.* $\beta \in A$ puisque A est intégralement clos (car de Prüfer). Enfin pour tout $i \in [\![1, m]\!]$, f_i s'écrit fg_i, pour un certain $g_i \in A[X]$, donc $f_i(\alpha, \beta) = f(\alpha, \beta)g_i(\alpha, \beta) = 0$, *i.e.* β est une racine commune à tous les $f_i(\alpha, Y)$ dans A.

Réciproquement, soient $f_1, \ldots, f_m \in A[X_1, \ldots, X_n, Y]$ et $c \subseteq A$ la liste des coefficients des f_i. Soit $\varphi(c, x, y)$ la formule du langage des anneaux ($x := (x_1, \ldots, x_n)$ est une multivariable, y une variable simple) qui dit que "$\bigwedge\!\!\!\bigwedge_{i=1}^m f_i(x, y) = 0$."

Soit B la clôture intégrale de $A[X_1, \ldots, X_n]$ dans sa clôture algébrique. On sait que le radical de Jacobson de B est nul si et seulement si celui de A est nul. Comme nous l'avons rappelé juste avant l'énoncé du théorème, on peut plonger $(B, \leq_B)$ dans un r-domaine $(B', \leq')$, de treillis résiduel dense, PAC, tel que $(0) \in \mathrm{Sp}(B', \leq')$ si et seulement si $(0) \in \mathrm{Sp}(B, \leq_B)$ et que tout idéal premier r-clos de $(B, \leq_B)$ se relève en un élément de $\mathrm{Sp}(B', \leq')$. On peut exclure le cas où $\mathrm{L}(A, \leq_A)$ est réduit à un point puisqu'alors A est un corps algébriquement clos et que le résultat est trivial. On a donc $\mathrm{L}(A, \leq_A) \preceq \mathrm{L}(B', \leq')$, ce qui entraîne d'après le corollaire 5.7 que $(A, \leq_A) \preceq (B', \leq')$.

Alors les f_i vérifient (i) si et seulement si $(A, \leq) \models \forall x \exists y \varphi(c, x, y)$. Dans ce cas, $(B', \leq')$ satisfait aussi cette formule, et en particulier il existe $\theta \in B'$ tel que $(B', \leq') \models \varphi(c, X, \theta)$, c'est-à-dire tel que pour tout $i \in [\![1, m]\!]$, $f_i(X, \theta) = 0$. Un tel θ est nécessairement algébrique sur $A[X]$, donc dans $\mathrm{Fr}(B)$. Mais de plus tout idéal maximal de B se relève en un idéal maximal de B', donc $B' \cap \mathrm{Fr}(B) \subseteq \cap W_B = B$, et finalement $\theta \in B$.

Soit f le polynôme minimal de θ sur $A[X]$. Alors $f \in A[X, Y]$, est unitaire en Y, et pour tout $i \in [\![1, m]\!]$, $f_i(X, \theta) = 0$ implique que f divise f_i (vu comme polynôme en Y). ■

Remarque: Il semble qu'une démonstration purement algébrique du théorème 2 soit encore à trouver.

Chapitre V

LGPH et structures locales

Résumé : Nous montrons ici comment utiliser le LGPH pour obtenir des résultats similaires à ceux du chapitre précédent, mais cette fois avec des structures locales qui ne sont plus nécessairement des anneaux de valuations sur des corps séparablement clos.

En application on obtient de nouveaux résultats de décidabilité et de modèle-complétude, notamment pour la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_p$.

§ 1. Théories approximables

Définition

Soit T une théorie d'anneaux de valuation. Je dirais que T est **approximable** s'il existe une théorie T^* du langage des anneaux telle que pour tout anneau A booléen, indépendant, dense dans ses hensélisés, on ait :

$$A \models T^* \quad \Longleftrightarrow \quad \forall \mathfrak{m} \in \mathrm{Spm}(A),\ \ A^h_{\mathfrak{m}} \models T.$$

Remarques:

(1) La théorie T en question peut aussi bien être axiomatisée dans la langage des anneaux que dans $\mathrm{L}_{\mathrm{div}}$ ou $\mathrm{L}_{\mathrm{rad}}$, comme nous l'avons signalé au premier chapitre. Il est clair que cela ne change rien à l'approximabilité.

(2) Si une théorie T est approximable, alors la théorie $T' := T+$"le lemme de Hensel" l'est aussi, et vice-versa. En effet un anneau de valuation henselien R satisfait T si et seulement s'il satisfait T'.

Propriété 1

Une théorie d'anneaux de valuation est approximable si et seulement s'il existe une théorie T^{**} du langage des anneaux telle que, pour tout anneau A satisfaisant la BAP et dense dans chacun de ses hensélisés, on ait :

$$A \models T^{**} \quad \Longleftrightarrow \quad \forall \mathfrak{m} \in \mathrm{Spm}(A),\ \ A^h_{\mathfrak{m}} \models T.$$

Preuve: Soit T une théorie approximable, et T^* la théorie qui lui est associée dans la définition précédente. D'après la propriété II.2.6, la classe des anneaux intègres A tels que, pour tout $\alpha \in A \setminus (A^* \cup \{0\})$, $S_\alpha^{-1}A \models T^*$ est élémentaire. Sa théorie T^{**} a la propriété voulue, puisque d'après la proposition II.2.3, W_A est la réunion des $W_{S_\alpha^{-1}A}$, pour α décrivant $A \setminus (A^* \cup \{0\})$.

■

Propriété 2

Soit T une théorie d'anneaux de valuation telle que :

(a) *pour tout anneau de valuation R dense dans son hensélisé, $R \models T \iff R^h \models T$;*

(b) *T peut être axiomatisée par des formules BAP-compatibles.*

Alors T et $T' := T+$ "Hensel" sont approximables.

Preuve: En vertu de remarque précédente, il suffit de montrer que T est approximable.

Soit $\{\varphi_n\}_{n\in\mathbb{N}}$ une suite de formules BAP-compatibles axiomatisant T. La propriété II.5.2, nous donne une théorie d'anneaux $T^o := \{\varphi_n^o\}_{n\in\mathbb{N}}$ telle que tout anneau localement booléen et indépendant A vérifie :

$$A \models T^o \iff \forall R \in W_A,\ R \models T.$$

Si de plus A est dense dans ses hensélisés, on a donc, d'après (a) :

$$A \models T^o \iff \forall R \in W_A,\ R^h \models T$$

i.e. T est approximable.

■

Exemples de théories approximables

Proposition 3

Soient T_g une théorie de groupes abéliens linéairement ordonnés, T_c une théorie de corps, et $T(T_g, T_c)$ la théorie des anneaux de valuation henseliens dont le groupe des valeurs est modèle de T_g et le corps des restes modèle de T_c. Si les deux théories T_g et T_c sont inductives, alors $T(T_g, T_c)$ est approximable.

Preuve: Rappelons qu'une théorie inductive est une théorie axiomatisable par des formules $\forall\exists$.

Un axiome de T_c est de la forme $\forall x \exists y \varphi(x,y)$, où $\varphi(x,y)$ est une formule sans quanteur du langage des anneaux à $m+n$ variables libres :

$$\varphi(x,y) \equiv \bigvee_{i\in I} \bigwedge_{j\in J_i} f_{i,j}(x,y) = 0 \wedge g_i(x,y) \neq 0.$$

Elle se traduit par la formule $\forall x \exists y \varphi^*(x,y)$ de $\mathrm{L}_{\mathrm{div}}$ définie par :

$$\varphi^*(x,y) \equiv \bigvee_{i\in I} \bigwedge_{j\in J_i} f_{i,j}(x,y) \not| 1 \wedge g_i(x,y) | 1$$

au sens où un anneau de valuation R satisfait $\forall x \exists y \varphi^*(x,y)$ si et seulement si son corps des restes vérifie $\forall x \exists y \varphi(x,y)$. La formule $\forall x \exists y \varphi^*(x,y)$ est BAP-compatible, d'après le lemme II.5.4.

De même, on peut (c'est classique : il suffit de ramener la théorie du groupe à celle de sa partie positive) axiomatiser T_g modulo la théorie des groupes abéliens linéairement ordonnés par des formules $\forall x \exists y \psi(x,y)$ du type suivant :

$$\psi(x,y) \equiv \Big(\bigwedge_{1\le i\le m} x_i \geq 0\Big) \to$$
$$\Big[\bigwedge_{1\le j\le n} y_j \geq 0 \wedge \Big(\bigvee_{i\in I} \bigwedge_{j\in J_i} f_{i,j}(x,y) \geq f'_{i,j}(x,y) \bigwedge_{k\in K_i} g_{i,k}(x,y) \not\geq g'_{i,k}(x,y)\Big)\Big],$$

où $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_n)$ sont des multivariables, et les $f_{i,j}, f'_{i,j}, g_{i,j}, g'_{i,j}$ des combinaisons linéaires à coefficients dans $\mathbb{N}$. Tout anneau de valuation R, de groupe des valeurs Γ_R noté additivement, vérifie :

$$\Gamma_R \models \forall x \exists y \psi(x,y) \iff R \models \forall x \exists y \psi^*(x,y)$$

où $\psi^*(x,y)$ est la formule :

$$\psi^*(x,y) \equiv \Big(\bigwedge_{1\leq i\leq m} x_i \neq 0 \Big) \to$$
$$\Big[\bigwedge_{1\leq j\leq n} y_j \neq 0 \wedge \Big(\bigvee_{i\in I} \bigwedge_{j\in J_i} F'_{i,j}(x,y) | F_{i,j}(x,y) \bigwedge_{k\in K_i} G'_{i,k}(x,y) \nmid G_{i,k}(x,y) \Big) \Big],$$

dans laquelle, pour toute combinaison linéaire $h(z) := \sum n_i z_i$ à coefficients dans $\mathbb{N}$, on a posé $H(z) := \prod z_i^{n_i}$. Les x_i et y_i étant tous supposés non nuls, on peut remplacer les sous-formules $F'_{i,j}(x,y)|F_{i,j}(x,y)$ par $0 \neq F'_{i,j}(x,y)|F_{i,j}(x,y)$. On obtient ainsi une formule BAP-compatible (il suffit de déplacer le "$\exists y$" pour que la formule "$\forall x \exists y \psi^*(x,y)$" se retrouve sous la forme étudiée dans le lemme II.5.4).

On voit donc que $T(T_g, T_c)$ est axiomatisable par des formules BAP-compatibles, et il est clair qu'un anneau de valuation quelconque R est modèle de $T(T_g, T_c)$ si et seulement si son hensélisé R^h est modèle de $T(T_g, T_c)$ puisque R^h est une extension immédiate de R. La propriété 2 s'applique donc, et donne la conclusion.

■

Exemples: La proposition 3 nous donne, en vertu du théorème d'Ax-Kochen-Ershov, qu'un anneau de valuation henselien R a une théorie complète approximable au moins dans les cas suivants :

– R est l'anneau d'une valuation p-adique de rang d ;

– R est d'égale caractéristique nulle et les théories de ses structures résiduelles (groupe des valeurs et corps des restes) sont inductives.

Ce dernier cas s'applique notamment aux anneaux de valuation réels clos, *i.e.* les anneaux de valuation henséliens dont le corps résiduel est réel clos et le groupe des valeurs divisible.

Le dernier exemple utile est donné par la proposition suivante :

Proposition 4

La théorie des anneaux de valuation henseliens dont le corps des fractions est séparablement clos est approximable.

Preuve: Pour tout $d \in \mathbb{N}$, notons $\delta_d(c_0, \ldots, c_d)$ le discriminant du polynôme $X^{d+1} + \sum_{i=0}^{d} c_i X^i$. On sait que dans un anneau intègre quelconque A, tout $\alpha \in A^{d+1}$ vérifie : $A \models \delta_d(\alpha) \neq 0$ si et seulement si le polynôme $X^{d+1} + \sum_{i=0}^{d} \alpha_i X^i$ est séparable sur $\mathrm{Fr}(A)$.

Soit R un anneau de valuation henselien ; on sait que les propriétés suivantes sont équivalentes :

(i) $\mathrm{Fr}(R)$ est séparablement clos ;

(ii) tout polynôme séparable et unitaire à cefficients dans R a une racine dans R ;

(iii) $\forall f \in R[X]$, séparable et unitaire, 0 est adhérent à $f[R]$.

Il s'ensuit que pour un anneau de valuation R, dense dans son hensélisé, $\mathrm{Fr}(R^h)$ est séparablement clos si et seulement si $\forall f \in R[X]$, séparable et unitaire, 0 est adhérent à $f[R]$. Cette dernière propriété est axiomatisée par la famille de formules suivantes (d

décrivant $\mathbb{N}$) :

$$\forall c_0, \ldots, c_d \forall \varepsilon \left[\delta_d(c_0, \ldots, c_d)\varepsilon \neq 0 \rightarrow \exists a\Big(0 \neq \varepsilon \,\Big|\, a^{d+1} + \sum_{i=0}^{d} c_i a^i\Big)\right].$$

Ces formules sont BAP-compatibles, d'après le lemme II.5.4, donc la propriété 2 s'applique et donne la conclusion.

■

§ 2. Aspects fonctoriels, plongements locaux

Rappelons qu'un **filtre** d'un treillis distributif L est une partie F de L telle que :
- $F \neq \emptyset$;
- $\forall \alpha, \beta \in L$, si $\alpha \in F$ et $\alpha \leq \beta$ alors $\beta \in F$;
- $\forall \alpha, \beta \in F$, $\alpha \wedge \beta \in F$.

Un filtre F est **propre** s'il est différent de L, c'est un **filtre premier** s'il est propre et si quels que soient $\alpha, \beta \in L$ on a : $\alpha \vee \beta \in F \iff \alpha \in F$ ou $\beta \in F$ (notons que l'implication $\Longleftarrow$ est vraie pour tout filtre). Enfin on appelle **ultrafiltre** ou **filtre maximal** de L tout filtre propre de L qui n'est inclus strictement dans aucun filtre propre de L.

Nous admettrons (c'est classique) que tout filtre maximal est premier et que tout filtre propre est l'intersection de l'ensemble de filtres premiers qui le contiennent.

Propriété 1
Soit I un idéal r-clos d'un r-domaine $\cap$-stable $(A, \leq)$.
Notons $L := \mathrm{L}(A, \leq)$ et posons $I^* := \{P(a) \,/\, a \in I\}$.
(1) *I^* est un filtre de L, et $I = \{a \in A \,/\, P(a) \in I^*\}$.*
(2) *Tout filtre de L est de cette forme.*
(3) *I^* est premier si et seulement si I est premier.*
(4) *I^* est un ultrafiltre si et seulement si I est maximal parmi les idéaux r-clos de $(A, \leq)$.*

Preuve: c'est une suite de vérification triviales, nous ne faisons que celle que nous utiliserons, laissant les autres à l'amusement du lecteur.

(1) $I \neq \emptyset$ donc $I^* \neq \emptyset$. Soit $\alpha \in I^*$ et $a \in I$ tel que $\alpha = P(a)$.
- Soit $\beta \in L$ tel que $\alpha \leq \beta$ et soit $b \in A$ tel que $\beta = P(b)$. Alors $a \leq b$ et puisque I est r-clos $b \in I$, *i.e.* $\beta \in I^*$.
- Soient $\beta \in I^*$ et $b \in A$ tels que $\beta = P(b)$. Soit $c \in A$ tel que $P(c) = P(a) \cap P(b)$. On a $P(I) \subseteq P(a) \cap P(b)$ (car $a, b \in I$) donc $c \in \bigcap P(c) \subseteq \bigcap P(I) = I$ (car I est r-clos) et donc $\alpha \wedge \beta = P(c) \in I^*$.

I^* est donc bien un filtre de L. De plus I est inclus dans $J := \{b \in A \,/\, P(b) \in I^*\}$, et quel que soit $c \in J$ il existe $\beta \in I^*$ tel que $P(c) = \beta$ *i.e.* il existe $b \in I$ tel que $P(c) = P(b)$, en particulier $b \leq c$ donc $c \in I$, d'où $I = J$.

(2) Soit F un filtre de L ; posons $F_* := \{a \in A \,/\, P(a) \in L\}$.
- $F \neq \emptyset$ donc $F_* \neq \emptyset$.
- Soient $a, b \in F_*$, et $c \in A$ tel que $P(c) = P(a) \cap P(b)$. Alors $P(c) \subseteq P(a+b)$ et $P(c) \in F$, donc $P(a+b) \in F$ d'où $a + b \in F_*$.

– Soient $a \in A$ et $b \in F_*$, alors $P(b) \in F$ et $P(b) \subseteq P(ab)$ donc $P(ab) \in F$, *i.e.* $ab \in F_*$.
– Soient $a, b \in A$ tels que $a \leq b$ et $a \in F_*$. Alors $P(a) \subseteq P(b)$ et $P(a) \in F$ donc $P(b) \in F$ *i.e.* $b \in F_*$.

Il s'ensuit que F_* est un idéal r-clos de $(A, \leq)$, donc $(F_*)^*$ est un filtre de L, dont il est facile de voir qu'il est égal à F.

(3) Supposons que I soit premier ; alors $I \in \mathrm{Sp}(A, \leq)$ donc quel que soit $a \in A$ si $P(a) = \emptyset$ alors $a \notin I$, *i.e.* $\mathbf{0} \notin I^*$ et donc $I^* \neq L$. Quels que soient $\alpha, \beta \in L$ tels que $\alpha \vee \beta \in I^*$, soient $a, b \in A$ tels que $P(a) = \alpha$ et $P(b) = \beta$. On a $P(ab) = P(a) \cup P(b) \in I^*$ *i.e.* $ab \in I$, et puisque I est premier a ou b appartient à I, *i.e.* α ou β appartient à I^*, qui est donc bien un filtre premier de L. La réciproque est sans utilité pour nous

(4) Supposons que I soit maximal parmi les idéaux r-clos de $(A, \leq)$, et soit F un filtre de L contenant I^*. D'après le (2) F_* est un idéal r-clos de $(A, \leq)$, et il contient I donc est égal à I ou A. Or $F = (F_*)^*$ donc F est égal à I^* ou L et I^* est bien maximal. Nous ne démontrons pas la réciproque.

■

Notations: Si $(A, \leq, I_1, \ldots, I_r)$ est un r-domaine $\cap$-stable muni de r idéaux r-clos, je note $\mathrm{L}(A, \leq, I_1, \ldots, I_r)$ le treillis résiduel de $(A, \leq)$ muni des filtres $I_1^*, \ldots, I_r^*$. Je noterai I_k au lieu de I_k^* chaque fois que la distinction pourra se faire d'après le contexte.

Définitions

(1) Un **plongement** $\sigma : (L, F_1, \ldots, F_r) :\longrightarrow (L', F_1', \ldots, F_r')$ entre deux treillis distributifs munis d'extrémités et de r filtres, est un plongement de L dans L' au sens des treillis avec extrémités (*i.e.* σ est injective et conserve le sup., l'inf. et les extrémités) vérifiant en outre : $\forall k \in [\![1, r]\!]$, $\sigma^{-1}[F_k'] = F_k$.
(2) De même un **plongement** entre deux r-anneaux $(A, \leq, I_1, \ldots, I_r)$ et $(A', \leq', I_1', \ldots, I_r')$ munis de r idéaux r-clos est un plongement de r-domaines $\varphi : (A, \leq) \longrightarrow (A', \leq')$ tel que pour tout $k \in [\![1, r]\!]$ on a $\varphi^{-1}[I_k'] = I_k$.

Proposition 2

Soit $\varphi : (A, \leq, I_1, \ldots, I_r) \longrightarrow (A', \leq', I_1', \ldots, I_r')$ un plongement entre deux r-anneaux $\cap$-stables munis de r idéaux r-clos. Posons $L := \mathrm{L}(A, \leq, I_1, \ldots, I_r)$ et $L' := \mathrm{L}(A', \leq', I_1', \ldots, I_r')$.
Alors l'application $\overline{\varphi}$ définie au IV.2 est un plongement de L dans L'.

Preuve: C'est immédiat, en utilisant le corollaire IV.2.4.

■

Proposition 3

Soient $(A, \leq, I_1, \ldots, I_r)$ et $(A', \leq', I_1', \ldots, I_r')$ deux r-anneaux $\cap$-stables munis de r idéaux r-clos. Soit σ un plongement de $\mathrm{L}(A, \leq, I_1, \ldots, I_r)$ dans $\mathrm{L}(A', \leq', I_1', \ldots, I_r')$.
Alors quel que soit $k \in [\![1, r]\!]$ l'application $\widehat{\sigma} : \mathrm{Sp}(A', \leq') \longrightarrow \mathrm{Sp}(A, \leq)$ définie au IV.2 envoie $P(I_k')$ dans $P(I_k)$.

Preuve: Fixons un entier $k \in [\![1, r]\!]$ et notons $I := I_k$ et $I' := I_k'$.

Quel que soit $\mathfrak{p}' \in P(I')$, on sait que $\mathfrak{p} := \widehat{\varphi}(\mathfrak{p}') \in \mathrm{Sp}(A', \leq')$. De plus comme $\mathfrak{p}' \supseteq I'$, on a par définition de $\widehat{\sigma}$:

$$\mathfrak{p} \supseteq \{a \in A \,/\, \exists a' \in I',\ \sigma(P(a)) = P(a')\} = \{a \in A \,/\, P(a) \in \sigma^{-1}[I'^*] = I^*\} = I$$

d'où $\mathfrak{p} \in P(I)$.

■

Plongements locaux

Notations: Étant donnée une partie X d'un treillis L je note :

– $P(X) :=$ l'ensembles des filtres premiers de L contenant X, et quel que soit $\alpha \in L$, $P(\alpha) := P(\{\alpha\})$.

– $S_X := L \setminus \cup P(X)$.

Nous admettrons (c'est démontré dans n'importe quel livre sur les treillis) que dans un treillis distributif avec extrémités L on a pour tout $\alpha, \beta \in L$:

$$P(\alpha \wedge \beta) = P(\alpha) \cap P(\beta) \quad \text{et} \quad P(\alpha \vee \beta) = P(\alpha) \cup P(\beta)$$

Définition

(1) Un plongement $\sigma : (L, F_1, \ldots, F_r) :\longrightarrow (L', F'_1, \ldots, F'_r)$ entre deux treillis distributifs munis d'extrémités et de r filtres sera dit **local** si c'est encore un plongement de $(L, S_{F_1}, \ldots, S_{F_r})$ dans $(L', S_{F'_1}, \ldots, S_{F'_r})$ c'est-à-dire si quel que soit $k \in [\![1, r]\!]$ on a : $\sigma^{-1}[S_{F'_k}] = S_{F_k}$.

(2) De même un plongement φ entre deux r-anneaux $(A, \leq, I_1, \ldots, I_r)$ et $(A', \leq', I'_1, \ldots, I'_r)$ munis de r idéaux r-clos sera dit **local** si et seulement si $\overline{\varphi}$ l'est (ce qui a bien un sens d'après la proposition 2).

L'intèrêt des plongements locaux réside dans la propriété suivante :

Proposition 4

Soient $(A, \leq, I_1, \ldots, I_r)$ et $(A', \leq', I'_1, \ldots, I'_r)$ deux r-anneaux $\cap$-stables munis de r idéaux r-clos. Soit σ un plongement local de $\mathrm{L}(A, \leq, I_1, \ldots, I_r)$ dans $\mathrm{L}(A', \leq', I'_1, \ldots, I'_r)$.

Alors quel que soit $k \in [\![1, r]\!]$, pour tout $\mathfrak{p} \in \mathrm{Sp}(A, \leq)$ maximal parmi les éléments de $P(I_k)$ il existe $\mathfrak{p}' \in P(I_k)$ tel que $\widehat{\sigma}(\mathfrak{p}') = \mathfrak{p}$. En particulier, si $(A, \leq)$ est localement complémenté et si les I_k sont non nuls, $\widehat{\sigma}$ envoie surjectivement $M(I'_k)$ dans $M(I_k)$.

Preuve: Fixons un entier $k \in [\![1, r]\!]$ et notons $I := I_k$ et $I' := I'_k$.

Soit $\mathfrak{p} \in P(I)$; l'idéal I étant non nul on a $\mathfrak{p} \neq (0)$ et comme $(A, \leq)$ est localement complémenté $\mathfrak{p}$ est maximal dans $\mathrm{Sp}(A', \leq')$. La proposition IV.2.6 s'applique donc à $\mathfrak{p}$: sa preuve montre que $J' := \{a' \in A' \,/\, \exists a \in \mathfrak{p},\ \sigma(P(a)) \subseteq P(a')\}$ est un idéal r-clos propre de $(A', \leq')$, et il suffit donc de montrer que $P(J') \cap P(I') \neq \emptyset$, puisqu'on aura alors un élément $\mathfrak{p}'$ de $P(I')$ contenant J', et que la fin de la preuve de la proposition IV.2.6 montre que $\widehat{\sigma}(\mathfrak{p}') = \mathfrak{p}$.

Par l'absurde, supposons que $P(I') \cap P(J') = \emptyset$. Alors pour tout $\mathfrak{p}' \in P(I')$ il existe $a_{\mathfrak{p}'} \in J' \setminus \mathfrak{p}'$. On a $P(I') \subseteq \bigcup\{P(a_{\mathfrak{p}'})^c \,/\, \mathfrak{p}' \in P(I')\}$ et $P(I')$ est quasi-compact, en tant que fermé de $\mathrm{Sp}(A', \leq')$, donc on peut en extraire un recouvrement fini : $P(I') \subseteq \cup_{i=1}^n P(a_{\mathfrak{p}'_i})^c$. Soit $a' \in A'$ tel que $P(a') = \cap_{i=1}^n P(a_{\mathfrak{p}'_i})$, on a $P(J') \subseteq P(a)$ donc $a' \in \cap P(J') = J'$ (car J' est un idéal r-clos). Alors il existe $a \in \mathfrak{p}$ et $b' \in A'$ tels que $\sigma(P(a)) = P(b') \subseteq P(a')$, et puisque $a \in \cup P(I)$ et que le plongement σ est local

$b' \in \cup P(I')$, *i.e.* $P(b') \cap P(I') \neq \emptyset$ et puisque $P(b') \subseteq P(a')$ *a fortiori* $P(a') \cap P(I') \neq \emptyset$. Cela contredit la construction de a' puisque $P(I') \subseteq \cup_{i=1}^{n} P(a_{\mathfrak{p}'_i})^c = P(a)^c$.

■

Les principaux exemples de plongements locaux que nous rencontrerons sont donnés par les propositions suivantes.

Proposition 5

*Soit $\sigma : (L, F_1, \ldots, F_r) \longrightarrow (L', F'_1, \ldots, F'_r)$ un plongement entre deux quasi-algèbres de Boole munies de r filtres non triviaux (*i.e. *non réduits à $\{\mathbf{1}_L\}$).*

Si σ est un plongement existentiellement clos (au sens des treillis munis d'extrémités et de r filtres) alors :

(a) *σ est un plongement local ;*

(b) *si $(L'', F''_1, \ldots, F''_r)$ est une extension élémentaire $|L'|^+$-saturée de $(L, F_1, \ldots, F_r)$ alors il existe un plongement local de $(L', F'_1, \ldots, F'_r)$ dans $(L'', F''_1, \ldots, F''_r)$ au-dessus de $(L, F_1, \ldots, F_r)$*

Preuve: Notons $\mathcal{L}$ le langage des treillis avec extrémités augmenté de r symboles de prédicats (interprétés dans L par les F_k et dans L' par les F'_k) et $\mathcal{L}^*$ le langage $\mathcal{L}$ augmenté de r autres symboles de prédicats (interprétés dans L par les S_{F_k} et dans L' par les $S_{F'_k}$).

Soient $\alpha \in L$ et tout $k \in [\![1, r]\!]$.

(i) $\alpha \in S_{F_k} \iff \exists \beta \in F_k,\ \alpha \wedge \beta = \mathbf{0}_L$.
En effet il est facile de voir que $H := \{\gamma \in L \,/\, \exists \beta \in F_k,\ \alpha \wedge \beta \leq \gamma\}$ est le plus petit filtre de L contenant $F_k \cup \{\alpha\}$, et $H = L$ si et seulement si $\mathbf{0} \in H$ si et seulement s'il existe $\beta \in L$ tel que $\alpha \wedge \beta = \mathbf{0}_L$. Or si $\alpha \notin S_{F_k}$ alors α appartient à au moins un filtre premier contenant F_k, donc H est un filtre propre de L (il est inclus dans ce filtre premier). Et inversement si H est un filtre propre de L alors il se plonge dans un filtre maximal U de L, qui est donc premier et contient F_k, *i.e.* $\alpha \in U \in P(F_k)$ donc $\alpha \in \cup P(F_k) = L \setminus S_{F_k}$). D'où l'équivalence.

(ii) $\alpha \notin S_{F_k} \iff \exists \beta \in L \setminus F_k,\ \alpha \vee \beta \in F_k$.
On a $\alpha \notin S_{F_k}$ si et seulement si $P(\alpha) \cap P(F_k) \neq \emptyset$. Soit $\gamma \in F_k \setminus \{\mathbf{1}_L\}$, et $\beta := \gamma \setminus \alpha$. On a $P(\beta) = P(\gamma) \setminus P(\alpha)$, et $P(F_k) \subseteq P(\gamma)$, donc si $P(\alpha) \cap P(F_k) \neq \emptyset$ alors $P(F_k) \not\subseteq P(\beta)$, donc $\beta \notin \cap P(F_k) = F_k$, et d'autre part $\beta \vee \alpha = \alpha \vee \gamma \in F_k$, d'où une implication. Inversement, s'il existe $\beta \in L \setminus F_k$ tel que $\alpha \vee \beta \in F_k$, alors $P(F_k)$ est inclus dans $P(\alpha) \cup P(\beta)$ et pas dans $P(\beta)$ donc $P(F_k) \cap P(\alpha) \neq \emptyset$.

On voit donc que toute formule existentielle de $\mathcal{L}^*$ se traduit par une formule existentielle de $\mathcal{L}$. Il s'ensuit que σ est un plongement existentiellement clos au sens de $\mathcal{L}^*$, et que $(L'', F''_1, \ldots, F''_r)$ est une extension élémentaire $|L'|^+$-saturée au sens de $\mathcal{L}^*$. En particulier σ est un plongement au sens de $\mathcal{L}^*$ *i.e.* est un plongement local, d'où (a) ; et puisqu'il est $\exists$-clos au sens de $\mathcal{L}^*$ il s'injecte dans L'' au-dessus de L par un plongement respectant la $\mathcal{L}^*$-structure *i.e.* un plongement local, d'où (b).

■

Proposition 6

Soient $(L, F_1, \ldots, F_r)$ et $(L', F'_1, \ldots, F'_r)$ deux treillis distributifs munis d'extrémités et de r filtres. Si les F_k sont des ultrafiltres deux à deux distincts alors tout plongement *de* $(L, F_1, \dots, F_r)$ *dans* $(L', F'_1, \dots, F'_r)$ *est local.*

Preuve: C'est immédiat.

■

§ 3. Maximalité intégrale

Notations: Je désigne par $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$ le langage de r-anneaux augmenté de r nouveaux symboles de prédicat unaires $I_1, \dots, I_r$.

Propriété 1

On considère la classe Σ *des* $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$*-structures* $(A, \leq, I_1, \dots, I_r)$ *telles que :*

(a) $(A, \leq)$ *est un r-domaine ;*

(b) $\leq$ *est la relation radicale induite par* $\mathrm{Spm}(A)$ *;*

(c) $\forall k \in [\![1, r]\!]$, I_k *est interprété dans* A *par un idéal r-clos propre et non nul de* $(A, \leq)$ *;*

(d) $\forall k \neq l \in [\![1, r]\!]$, $M(I_k) \cap M(I_l) = \emptyset$.

La classe Σ *est élémentaire dans* $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$.

Preuve: (a) est axiomatisé par les axiomes des r-domaines donnés par Prestel et Schmid, et (b) par l'axiome suplémentaire :

$$\forall a \forall b, (a \leq b \leftrightarrow \forall c((b, c) = 1 \rightarrow (a, c) = 1))$$

où "$(x, y) = 1$" est une abréviation pour la formule "$\exists u \exists v(ux + vy = 1)$".
(c) est axiomatisé par les formules suivantes :

- $\neg I_k(1) \wedge \exists a(a \neq 0 \wedge I_k(a))$;
- $\forall a, b(I_k(a) \wedge I_k(b) \rightarrow I_k(a + b))$;
- $\forall a, b(I_k(b) \rightarrow I_k(ab))$;
- $\forall a, b(I_k(a) \wedge a \leq b \rightarrow I_k(b))$.

Enfin (d) est axiomatisé par :

- $\bigwedge\!\!\!\bigwedge_{1 \leq k < l \leq r} \exists a, b, u, v(I_k(a) \wedge I_l(b) \wedge au + bv = 1)$.

■

Notations: $\mathcal{T}^r :=$ la théorie de la classe Σ ci-dessus.
Si $(A, \leq, I_1, \dots, I_r)$ est un modèle de $\mathcal{T}^r$, $\forall k \in [\![1, r]\!]$, $S_k := A \setminus \cup M(I_k)$.

Remarque: Si $r \neq 0$ la condition (c) de la propriété 1 implique qu'un modèle de $\mathcal{T}^r$ ne peut pas être un corps.

Proposition 2

Soient $T_1, \dots, T_r$ *des théories approximables.*
Soit Σ *la classe des* $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$*-structures* $(A, \leq, I_1, \dots, I_r)$ *telles que :*

(a) $(A, \leq, I_1, \dots, I_r) \models \mathcal{T}^r$ *;*

(b) A *satisfait la BAP et est dense dans ses hensélisés ;*

(c) $\forall k \in [\![1, r]\!]$, $\forall \mathfrak{m} \in M(I_k)$, $A^h_{\mathfrak{m}} \models T_k$,

(d) $\forall \mathfrak{m} \in \mathrm{Spm}(A) \setminus \bigcup_{1 \leq k \leq r} M(I_k)$, $\mathrm{Fr}(A^h_{\mathfrak{m}})$ *est séparablement clos.*

Alors Σ *est élémentaire.*

Remarque: Si un modèle de $\mathcal{T}(\emptyset)$ est un corps (c'est possible puisqu'ici $r = 0$) il est séparablement clos (la valuation triviale est henselienne).

Preuve: On vient d'axiomatiser (a), et (b) l'a été avec la proposition II.5.5. Soit T_0 la théorie des anneaux de valuation séparablement clos. Pour tout $k \in [\![0, r]\!]$, la théorie T_k est approximable, donc on peut lui associer une théorie T_k^* telle qu'un anneau booléen B, indépendant et dense dans ses hensélisés vérifie T_k^* si et seulement si pour tout $\mathfrak{n} \in \mathrm{Spm}(B)$, $B_\mathfrak{n}^h \models T_k$. Les éléments de Σ sont les modèles $(A, \leq, I_1, \dots, I_r)$ de $\mathcal{T}^r$ tels que A soit localement booléen, indépendant, dense dans ses hensélisés, et que :
- $\forall k \in [\![1, r]\!], \ \ S_k^{-1}A \models T_k^*$;
- $\forall a \in A \setminus A^*, \ \ \bigwedge\!\!\!\bigwedge_{1 \leq k \leq r} \neg I_k(a) \to S_a^{-1}A \models T_0^*$.

Ces deux propriétés sont clairement du premier ordre (la première parce que, I_k étant dans le langage, $S_k^{-1}A$ est uniformément interprétable dans A ; et la seconde parce que S_a est uniformément définissable dans A comme l'ensemble des éléments étrangers à a).

■

Notations: Je désigne par $\mathcal{T}(T_1, \dots, T_r)$ la théorie de la classe Σ ci-dessus.

Propriété 3

Soient $T_1, \dots, T_r$ des théories d'anneaux de valuation henséliens, modèle-complètes et approximables. Soient $(A, \leq, I_1, \dots, I_r) \subseteq (A', \leq', I'_1, \dots, I'_r)$ deux modèles de $\mathcal{T}(T_1, \dots, T_r)$, supposés $\cap$-stables, $W_0 := \{A_\mathfrak{m} \,/\, \mathfrak{m} \in \cup_{k=1}^r M(I_k)\}$ et W'_0 l'analogue pour A'. Notons $K := \mathrm{Fr}(A)$, et $K' := \mathrm{Fr}(A')$.

Si l'injection de A dans A' est un plongement local, alors W_0 possède sur K' un prolongement $\exists$-clos W' inclus dans W'_0.

En particulier, si $r \neq 0$, alors l'extension $K'|K$ est séparable.

Preuve: Si $W_0 = \emptyset$ il n'y a rien à montrer, sinon soit $R \in W_0$. A est localement booléen, donc $R = A_\mathfrak{m}$, où $\mathfrak{m} := m(R) \cap A$ appartient à l'un des $M(I_k)$. L'injection de A dans A' étant un plongement local, $\mathfrak{m}$ se relève en $\mathfrak{m}' \in M(I'_k)$, d'où un élément $R' = A'_{\mathfrak{m}'}$ de W'_0 tel que $R^h \preceq R'^h$ (par modèle-complétude de T_k). L'opération, répétée pour tous les éléments de W_0, donne la famille W' cherchée.

Si $r \neq 0$ alors W_0 est non vide, et la remarque faite au III.3, juste après la définition des prolongements $\exists$-clos entraîne que l'extension $K'|K$ est séparable.

■

Définition

Un modèle $(A, \leq, I_1, \dots, I_r)$ de $\mathcal{T}^r$ est **intégralement maximal** si et seulement si pour toute extension algébrique propre K' de $K := \mathrm{Fr}(A)$, la famille W_A n'admet aucun prolongement $\exists$-clos à K'.

Propriété 4

Soient $T_1, \dots, T_r$ des théories d'anneaux de valuation henseliens, modèle-complètes et approximables. Soient $(A, \leq, I_1, \dots, I_r) \subseteq (A', \leq', I'_1, \dots, I'_r)$ des modèles $\cap$-stables et intégralement maximaux de $\mathcal{T}(T_1, \dots, T_r)$.

Si $r \neq 0$ et si l'injection de A dans A' est un plongement local, alors $K' := \mathrm{Fr}(A')$ est une extension régulière de $K := \mathrm{Fr}(A)$. Si de plus A satisfait le LGPH alors $K \leq_\exists K'$.

Preuve: La propriété 3 donne un prolongement $\exists$-clos W'_0 de $W_0 = \{A_\mathfrak{m} \,/\, \mathfrak{m} \in$

$\cup_{k=1}^r M(I_k)\}$ à K'. Il suffit d'étendre W_0' en un prolongement $\exists$-clos de W_A.

Quel que soit $R \in W_A \setminus W_0$, $\mathfrak{m} := m(R) \cap A \in \mathrm{Spm}(A)$ et $R = A_{\mathfrak{m}}$. La proposition IV.2.6 nous donne $\mathfrak{m}' \in \mathrm{Spm}(A')$ tel que $\mathfrak{m}' \cap A = \mathfrak{m}$. Pour alléger, notons $R' := A'^h_{\mathfrak{m}'}$. Comme $R \notin W_0$, son corps de fractions est séparablement clos, donc on sait que $(R^h, |_{R^h})$ est $\exists$-clos dans toute extension $(R'', |_{R''})$ telle que $\mathrm{Fr}(R'')$ soit un extension séparable de $\mathrm{Fr}(R)$. Or l'extension $K'|K$ étant séparable, R' vérifie précisément cette condition, donc $(R^h, |_{R^h}) \leq_\exists (R'^h, |_{R'^h})$, et d'après la propriété 4 des prérequis $(R^h, \leq_{R^h}) \leq_\exists (R'^h, \leq_{R'^h})$.

Si de plus A satisfait le LGPH alors on a vu que $K \in \mathrm{RC}(W_A)$, et on vient de construire un prolongement $\exists$-clos de W_A à K', donc $K \leq_\exists K'$.

■

Proposition 5

Soient $T_1, \ldots, T_r$ des théories approximables. Un modèle $(A, \leq, I_1, \ldots, I_r)$ de la théorie $\mathcal{T}(T_1, \ldots, T_r)$ est intégralement maximal si et seulement si tout polynôme à coefficients dans A, unitaire et irréductible sur $K := \mathrm{Fr}(A)$, ayant un racine dans R^h pour tout $R \in W_A$, a une racine dans A.

Preuve: Soit $(A, \leq, I_1, \ldots, I_r)$ un modèle de $\mathcal{T}(T_1, \ldots, T_r)$.

Soit f un polynôme à coefficients dans A, unitaire et irréductible sur K, ayant une racine dans R^h pour tout $R \in W_A$. Alors f possède une racine x, algébrique sur K, telle que pour tout $R \in W_A$, $H_R(K)$ contient un K-conjugué de x ; donc $K' := K(x)$ est inclus dans un corps K'_R, image de $H_R(K)$ par un K-automorphisme σ_R de K^a. La famille $W' := (\sigma_R(R^h) \cap K')_{R \in W_A}$ constitue donc un prolongement $\exists$-clos de W sur K'. Si A est intégralement maximal, on a donc nécessairement $K' = K$, *i.e.* $x \in K$. Comme f est unitaire et que A, étant de Prüfer, est intégralement clos, $x \in A$ *i.e.* f a bien une racine dans A.

Inversement, si A n'est pas intégralement maximal, alors on peut trouver une extension algébrique propre K' de K et un prolongement $\exists$-clos W' de W_A à K'. Pour tout $R' \in W'$, le K-plongement de $H_{R' \cap K}(K)$ dans $H_{R'}(K')$ est $\exists$-clos, et comme le second est algébrique sur le premier, il s'ensuit que ce plongement est un isomorphisme. Soit $x \in K' \setminus K$, entier sur A, et f son polynôme minimal sur K. Pour tout $R \in W_A$, x possède, en vertu de ce qui précède, un K-conjugué x_R dans $H_R(K)$, entier sur R^h puisque f est unitaire et à coefficients dans $A \subseteq R^h$, donc $x_R \in R^h$ puisque R^h est intégralement clos. On a donc une racine de f dans R^h, pour tout $R \in W_A$, alors que f n'a pas de de racine dans K, ni *a fortiori* dans A.

Corollaire 6

Soient $T_1, \ldots, T_r$ des théories approximables. Alors la classe des modèles intégralement maximaux de $\mathcal{T}(T_1, \ldots, T_r)$ est élémentaire.

Preuve: Soit R un anneau de valuation dense dans son hensélisé, et $f \in R[X]$, unitaire et irréductible sur $\mathrm{Fr}(R)$. Alors f possède une racine dans R^h si et seulement s'il existe un $a \in R$ tel que $|f(a)|_R \leq |f'(a)|_R^2$, *i.e.* si et seulement si R satisfait la formule $ZpolH_d(c)$, où $d = d^o f$ et $c = (c_0, \ldots, c_{d-1})$ est la liste des coefficients de f ($f = X^d + \sum c_i X^i$) et la formule $ZpolH_d(c) \equiv \exists y,\ 0 \neq f'(y)^2 | f(y)$. Cette formule est BAP-compatible d'après le lemme II.5.4, donc il existe une formule $ZpolH_d^o(x)$ telle que pour tout anneau A

indépendant et localement booléen, et tout élément c de A^d, on ait :

$$A \models ZpolH_d^o(c) \iff \forall \mathfrak{m} \in \mathrm{Spm}(A),\ A_\mathfrak{m} \models ZpolH_d(c).$$

Si de plus A est dense dans ses hensélisés, on aura donc :

$$A \models ZpolH_d^o(c) \iff \forall \mathfrak{m} \in \mathrm{Spm}(A),\ f := X^d + \sum_{i=0}^{d-1} c_i X^i \ \text{ a une racine dans } A_\mathfrak{m}^h.$$

Pour tout $d \in \mathbb{N}$, il est facile de construire une formule $Irr_d(x)$, où x est un d-uplet de variables, telle que pour tout anneau intègre A et tout $c \in A^d$, on ait $A \models Irr_d(c)$ si et seulement si le polynôme $X^d + \sum c_i X^i$ est irréductible sur $\mathrm{Fr}(A)$.

On déduit alors de la proposition 5 qu'un modèle $(A, \leq, S_1, \ldots, S_p)$ de $\mathcal{T}(T_1, \ldots, T_p)$ est intégralement maximal si et seulement s'il satisfait le schéma d'axiomes suivant (pour $d \in \mathbb{N}$) :

$$IntMax_d \equiv \forall x \Big((Irr_d(x) \wedge ZpolH_d^o(x)) \rightarrow \exists t,\ t^d + \sum_{i=0}^{d-1} x_i t^i = 0 \Big).$$

■

§ 4. Plongement existentiellement clos

Lemme 1 (d'amalgamation)
Soient R, R', R'' trois anneaux de valuation, de corps des fractions respectifs K, K', K'', tels que K' et K'' soient des extensions régulières de K, et $R' \cap K = R'' \cap K = R$. On suppose de plus que l'une au moins des conditions suivantes est remplie :
(a) *les $\mathrm{L_{rad}}$-plongements naturels de R^h dans R'^h et R''^h sont élémentaires,*
(b) *$H_{R''}(K'')$ est séparablement clos, et $R'' \neq K''$.*
Alors il existe un anneau de valuation R°, sur $K^\circ := \mathrm{Fr}(K' \otimes_K K'')$ vérifiant :
– *$R^\circ \cap K' = R'$,*
– *$R^\circ \cap K'' = R''$,*
– *le $\mathrm{L_{rad}}$-plongement naturel de R''^h dans $R^{\circ h}$ est $\exists$-clos.*

Preuve:
(a) On sait que deux extensions élémentaires A' et A'' d'un anneau A peuvent être amalgamées dans une extension élémentaire commune B de telle sorte que $\mathrm{Fr}(A')$ et $\mathrm{Fr}(A'')$ soient linéairement disjoints dans $\mathrm{Fr}(B)$ au-dessus de $\mathrm{Fr}(A)$. On applique cela à R^h, R'^h, R''^h : on obtient un anneau de valuation henselien $\overline{R}$, extension élémentaire commune à R'^h et R''^h telle que K° se plonge au-dessus de K dans $\mathrm{Fr}(\overline{R})$. Il suffit alors de prendre $R^\circ := \overline{R} \cap K^\circ$.

(b) On sait qu'un anneau de valuation non trivial de corps des fractions séparablement clos est existentiellement clos dans tout prolongement à une extension régulière. $K'|K$ étant régulière, $K^\circ|K''$ est régulière, donc il suffit de construire un prolongement commun à R' et R'' sur K°. C'est ce qui a été fait dans le lemme IV.3.1.

■

Théorème 2 (de plongement)
Soient $T_1, \ldots, T_r$ des théories d'anneaux de valuation, modèle-complètes et approximables. Considérons deux modèles $\cap$-stables $(A', \leq', I'_1, \ldots, I'_r)$ et $(A'', \leq'', I''_1, \ldots, I''_r)$

de $\mathcal{T}(T_1,\dots,T_r)$, et une sous-$\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure $(A,\leq,I_1,\dots,I_r)$ commune vérifiant les conditions suivantes :

– *A est de Prüfer et $\mathrm{Spm}(A)\subseteq\mathrm{Sp}(A,\leq)$;*

– *$(A,\leq)$ est $\cap$-stable et localement complémenté ;*

– *$\forall k\in[\![1,r]\!]$, $\forall\mathfrak{m}\in M(I_k)$, $A^h_{\mathfrak{m}}\models T_k$;*

– *$(0)\in\mathrm{Sp}(A',\leq')$ si et seulement si $(0)\in\mathrm{Sp}(A'',\leq'')$.*

Notons K, K', K'' les corps de fractions respectifs de A, A', A'', et L, L', L'' leurs treillis résiduels (munis des filtres associés aux I_k). Notons φ' l'injection de A dans A', φ'' celle de A dans A'', et $\overline{\varphi}'$, $\overline{\varphi}''$ les plongements induits, de L dans L' et L'', donnés par la proposition 2.2.

On se donne un plongement σ de L' dans L'' tel que $\overline{\varphi}''=\sigma\circ\overline{\varphi}'$, et on suppose que :

– *K' et K'' sont des extensions régulières de K ;*

– *le K-plongement naturel de K'' dans $K^\circ:=\mathrm{Fr}(K'\otimes_K K'')$ est $\exists$-clos (dans le langage des anneaux) ;*

– *σ, φ' et φ'' sont locaux ;*

– *$(A'',\leq'',I''_1,\dots,I''_r)$ est $|A'|^+$-saturé et A'' satisfait le LGPH'.*

Alors il existe un plongement local φ de $(A',\leq',I'_1,\dots,I'_r)$ dans $(A'',\leq'',I''_1,\dots,I''_r)$, dont la restriction à A soit l'identité, et tel que $\overline{\varphi}=\sigma$.

Preuve: σ est un plongement local, on en déduit une application, que nous noterons encore $\widehat{\sigma}$, de $W_{A''}$ dans $W_{A'}\cup\{K\}$ définie par : $\forall R''\in W_{A''},\ \ \widehat{\sigma}(R''):=A'_{\widehat{\sigma}(m(R'')\cap A'')}$.
On a alors $\widehat{\sigma}(R'')\cap K=R''\cap K$.
Soit $R''\in W_{A''}$, $R':=\widehat{\sigma}(R'')$, et $R:=R''\cap K=R'\cap K$. Il y a deux cas possibles :

Cas 1. $m(R'')$ appartient à l'un des $M(I''_k)$, et alors $\widehat{\sigma}(m(R'')\cap A'')\in M(I'_k)$ et $m(R'')\cap A\in M(I_k)$. Les hensélisés R^h, R'^h, R''^h sont donc tous trois modèles de T_k, qui est modèle-complète, et le lemme 1 s'applique : on est dans le cas (a).

Cas 2. $m(R'')\notin\cup_{k=1}^r M(I_k)$, et alors $R''^h=R''^s$, et cette fois c'est le cas (b) du lemme 1 qui s'applique.

Le lemme 1 nous permet ainsi de construire un prolongement $\exists$-clos W° de $W_{A''}$ à K°, tel que :

$$\forall R^\circ\in W^\circ,\ \ R^\circ\cap K'=\widehat{\sigma}(R^\circ\cap K'').$$

D'où, comme dans la proposition III.3.3, une extension $\exists$-close $(A^\circ,\leq^\circ,I^\circ_1,\dots,I^\circ_r)$ de $(A'',\leq'',I''_1,\dots,I''_r)$. Il est facile de vérifier que c'est aussi une extension de $(A',\leq',I'_1,\dots,I'_r)$, en se rappelant qu'on a supposé que $(0)\in\mathrm{Sp}(A',\leq')$ si et seulement si $(0)\in\mathrm{Sp}(A'',\leq'')$ (donc si et seulement si $(0)\in\mathrm{Sp}(A^\circ,\leq^\circ)$), et que d'après la proposition IV.2.6, $\widehat{\sigma}$ atteint tout $\mathrm{Spm}(A)$ (resp. $\widehat{\sigma}$ restreinte à I''_k atteint tout $M(I'_k)$ d'après la proposition 2.4).

Nous allons maintenant utiliser la propriété de saturation de A'' pour construire un A-plongement φ de A' dans A''. Mais si on l'utilise telle quelle, rien ne garantit qu'on aura $\overline{\varphi}=\sigma$. Pour y remédier il nous faut raffiner un peu en faisant intervenir une section de σ comme dans la preuve du théorème IV.3.2. Pour tout $a'\in A'$, on prend $a''_{a'}\in A''$ tel que :

– $P_{A''}(a''_{a'})=\sigma(P_{A'}(a'))$

– si $a'\in A$ on prend $a''_{a'}=a'$;

– $a''_{a'}=0$ si et seulement si $a'=0$;

et on a alors $a''_{a'}\leq^\circ a'\leq^\circ a''_{a'}$.

L'ensemble $(a''_{a'})_{a' \in A'}$ est de cardinal inférieur ou égal à celui de A', donc par saturation il existe un plongement de r-domaine $\widetilde{\varphi}$, de $A'[a''_{a'}]_{a' \in A'}$, muni de la trace de la $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure de $(A^\circ, \leq^\circ, I_1^\circ, \ldots, I_r^\circ)$ dans $(A'', \leq'', I_1'', \ldots, I_r'')$, dont la restriction à $(a''_{a'})_{a' \in A'}$ soit l'identité. Il ne reste qu'à vérifier que $\varphi := \widetilde{\varphi}_{|A'}$ a bien les propriétés voulues.

φ est un plongement de $(A', \leq', I_1', \ldots, I_r')$ dans $(A'', \leq'', I_1'', \ldots, I_r'')$, puisque la $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure de A' est la trace de celle de A°, donc aussi de celle de $A'[a''_{a'}]_{a' \in A'}$. Par construction $A \subseteq (a''_{a'})_{a' \in A'}$ donc $\varphi_{|A}$ est l'identité. Enfin, pour tout $a' \in A'$, on a :

$$\begin{aligned} a' \leq^\circ a''_{a'} \leq^\circ a' &\Longrightarrow \varphi(a') \leq'' \varphi(a''_{a'}) = a''_{a'} \leq'' \varphi(a') \\ &\Longrightarrow P_{A''}(\varphi(a')) = P_{A''}(a''_{a'}) = \sigma(P_{A'}(a')) \end{aligned}$$

i.e. $\overline{\varphi} = \sigma$.

■

§ 5. Conséquences modèle-théoriques

Nous regroupons ici les résultats analogues à ceux du IV.5.

Corollaire 1
Soient $T_1, \ldots, T_r$ des théories d'anneaux de valuation, approximables et modèle-complètes. Soient $(A, \leq, I_1, \ldots, I_r) \subseteq (A', \leq', I_1', \ldots, I_r')$ des modèles $\cap$-stables de $\mathcal{T}(T_1, \ldots, T_r)$, tels que $(0) \in \mathrm{Sp}(A, \leq)$ si et seulement si $(0) \in \mathrm{Sp}(A', \leq')$. Notons K, K' leurs corps de fractions et L, L' leurs treillis résiduels respectifs (munis de leurs filtres).
(a) *Si $A \models$ LGPH', alors :*

$$(A, \leq, I_1, \ldots, I_r) \leq_\exists (A', \leq', I_1', \ldots, I_r') \quad \Longleftrightarrow \quad L \leq_\exists L' \ \text{ et } \ K \leq_\exists K'.$$

(b) *Si $A \models$ LGPH, et si l'extension $K'|K$ est régulière, alors :*

$$(A, \leq, I_1, \ldots, I_r) \leq_\exists (A', \leq', I_1', \ldots, I_r') \quad \Longleftrightarrow \quad L \leq_\exists L'.$$

Preuve:
(a) Une implication est banale. Pour la réciproque, supposons que $L \leq_\exists L'$ et que $K \leq_\exists K'$. Nous allons réaliser les hypothèses du théorème de plongement.

Soit $(A'', \leq'', I_1'', \ldots, I_r'')$ une extension élémentaire $|A'|^+$-saturée de $(A, \leq, I_1, \ldots, I_r)$, K'' son corps des fractions, et L'' son treillis résiduel (muni de ses filtres).
- A satisfait le LGPH', donc A'' aussi (c'est du premier ordre).
- A', A et A'' sont $\cap$-stables et localement booléens (le premier par hypothèse, et les deux autres parce qu'ils satisfont le LGPH', donc sont localement booléens et de Bezout).
- $(0) \in \mathrm{Sp}(A'', \leq'') \iff (0) \in \mathrm{Sp}(A, \leq)$ (par l'axiome (o)) $\iff (0) \in \mathrm{Sp}(A', \leq')$.
- $K \preceq K''$, donc l'extension $K''|K$ est régulière.
- Le plongement de L dans L'' est élémentaire, donc local d'après la proposition 2.5 ; L'' est $|L'|^+$-saturée et $L \leq_\exists L'$, donc il existe un L-plongement σ de L' dans L'' au-dessus de L, que l'on peut prendre local d'après la proposition 2.5.

Il ne reste qu'à vérifier que $K'' \leq_\exists K' \otimes_K K''$. Or $K \leq_\exists K'$, donc K' se plonge (au-dessus de K) dans une extension élémentaire F' de K. Puisque $K \preceq K''$ et $K \preceq F'$, on peut amalgamer F' et K'' au dessus de K de façon K-linéairement disjointe dans une extension élémentaire F commune à F' et K''. On a donc un K''-plongement de $K' \otimes_K K''$ dans F (car $K'K'' \simeq K' \otimes_K K''$), qui fait de $K' \otimes_K K''$ une extension existentiellement close de K''.

Le théorème de plongement donne donc un monomorphisme de $(A', \leq', I'_1, \dots, I'_r)$ dans $(A'', \leq'', I''_1, \dots, I''_r)$ au-dessus de A, *i.e.* $(A', \leq', I'_1, \dots, I'_r)$ est bien une extension existentiellement close de $(A, \leq, I_1, \dots, I_r)$.

(b) On se ramène au (a) en observant que l'hypothèse $L \leq_\exists L'$ entraîne que le plongement est local, donc $W_0 := \{A_\mathfrak{m} \,/\, \mathfrak{m} \in \cup_{k=1}^r M(I_k)\}$ admet un prolongement $\exists$-clos à K' d'après la propriété 3.3. De plus tout $R \in W_A \setminus W_0$ admet un prolongement R' à K', et $R^h = R^s \leq_\exists R'^h$ (au sens de $\mathrm{L_{rad}}$ ou $\mathrm{L_{div}}$) car l'extension $K'|K$ est régulière donc $H_{R'}(K')|K^s$ aussi. C'est donc tout W_A qui admet un prolongement $\exists$-clos à K', et puisque A satisfait le LGPH on a $K \in \mathrm{RC}(W_A)$, donc exiger que l'extension $K'|K$ soit régulière revient à supposer que $K \leq_\exists K'$.

■

Lemme 2

Soient $T_1, \dots, T_r$ des théories d'anneaux de valuation henseliens, modèle-complètes et approximables, avec $r \neq 0$. Soient $(A', \leq', I'_1, \dots, I'_r)$ et $(A'', \leq'', I''_1, \dots, I''_r)$ deux modèles intégralement maximaux de $\mathcal{T}(T_1, \dots, T_r)$ satisfaisant le LGPH, et considérons une sous-$\mathrm{L^r_{rad}}$-structure $(A, \leq, I_1, \dots, I_r)$ commune à $(A', \leq', I'_1, \dots, I'_r)$ et $(A'', \leq'', I''_1, \dots, I''_r)$. Notons K, K', K'' leurs corps de fractions respectifs. On suppose que :

- *A est de Prüfer et $\mathrm{Spm}(A) \subseteq \mathrm{Sp}(A, \leq)$;*
- *$(A, \leq)$ est $\cap$-stable et localement complémenté ;*
- *$\forall k \in [\![1, r]\!]$, $\forall \mathfrak{m} \in M(I_k)$, $\mathfrak{m} \neq (0)$ et $A^h_\mathfrak{m} \models T_k$;*
- *$(0) \in \mathrm{Sp}(A', \leq')$ si et seulement si $(0) \in \mathrm{Sp}(A'', \leq'')$;*
- *les extensions $K'|K$ et $K''|K$ sont régulières ;*
- *les plongements de A dans A' et dans A'' (les $\mathrm{L^r_{rad}}$-structures étant sous-entendues) sont locaux.*

Notons L, L', L'' leurs treillis résiduels (munis de leurs filtres). Alors :

$$((A', \leq', I'_1, \dots, I'_r), A) \equiv ((A'', \leq'', I''_1, \dots, I''_r), A) \quad \iff \quad (L', L) \equiv (L'', L).$$

Preuve: Pour simplifier l'écriture, je note A au lieu de $(A, \leq, I_1, \dots, I_r)$, et de même pour les autres $\mathrm{L^r_{rad}}$-structures.

L'implication de droite à gauche est banale, puisque les treillis résiduels sont interprétables dans les r-anneaux.

Inversement, supposons que $(L', L) \equiv (L'', L)$. Nous allons construire par récurence un A-isomorphisme entre des extensions élémentaires de A' et A''.

• Initialisation : On pose $A_0 := A$, $A_1 := A'$ et $A_2 :=$ une extension élémentaire $|A'|^+$-saturée de A''. Comme le treillis résiduel L_2 de A_2 est une extension élémentaire de L'', on a encore $(L_2, L) \equiv (L', L)$, et les autres propriétés de A'' (maximalité, LGPH,… *etc.*), étant élémentaires, sont conservées par A_2. Enfin $K'' \preceq K_2$ donc K_2 est une extension régulière de K'', et donc aussi de K. De même $L'' \preceq L_2$, donc le plongement de A'' dans A_2 est local, et donc aussi celui de A dans A_2.

• Itération : étant donné $n \in \mathbb{N}$, on suppose construits A_n, A_{n+1} et A_{n+2}, $\cap$-stables et localement booléens, de treillis résiduels respectifs L_n, L_{n+1}, L_{n+2}, et de corps des fractions K_n, K_{n+1} et K_{n+2}, tels que :
($\mathrm{i_n}$) $\forall k \in [\![1, n]\!]$, $A_k \preceq A_{k+2}$;
($\mathrm{ii_n}$) A_{n+2} est $|A_{n+1}|^+$-saturée ;
($\mathrm{iii_n}$) A_n est une sous-$\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure commune à A_{n+1} et A_{n+2} ;
($\mathrm{iv_n}$) les plongements de A_n dans A_{n+1} et A_{n+2} sont locaux ;
($\mathrm{v_n}$) les extensions $K_{n+1}|K_n$ et $K_{n+2}|K_n$ sont régulières ;
($\mathrm{vi_n}$) $(L_{n+2}, L_n) \equiv (L_{n+1}, L_n)$.

On prends alors pour A_{n+3} une extension élémentaire $|A_{n+2}|^+$-saturée de A_{n+1} (ainsi ($\mathrm{i_{n+1}}$) et ($\mathrm{ii_{n+1}}$) sont vérifiés). On note $K_{n+3} := \mathrm{Fr}(A_{n+3})$, et $L_{n+3} := \mathrm{L}(A_{n+3}, \leq_{n+3}, I_{1,n+3}, \ldots, I_{p,n+3})$.
Pour faire de A_{n+1} une sous-structure commune à A_{n+2} et A_{n+3}, on utilise le théorème de plongement. Comme A_{n+2} et A_{n+1} sont des extensions élémentaires de A' et A'', ce sont des modèles algébriquement maximaux de $\mathcal{T}(T_1, \ldots, T_r)$, satisfaisant le LGPH ; et comme la satisfaction de l'axiome (o) est conservée par extension élémentaire, on a $(0) \in \mathrm{Sp}(A_{n+2}, \leq_{n+2})$ si et seulement si $(0) \in \mathrm{Sp}(A_{n+1}, \leq_{n+1})$. Par saturation de L_{n+2}, et par ($\mathrm{vi_n}$), il existe un plongement local σ_n de L_{n+1} dans L_{n+2} au dessus de L_n. Le théorème de plongement nous donne donc un plongement local $\varphi_n : A_{n+1} \longrightarrow A_{n+2}$, tel que $\overline{\varphi}_n = \sigma_n$. On identifie comme toujours A_{n+1} à son image, et les conditions ($\mathrm{iii_{n+1}}$) et ($\mathrm{iv_{n+1}}$) sont ainsi satisfaites.

Comme $K_{n+1} \preceq K_{n+3}$, l'extension $K_{n+3}|K_{n+1}$ est régulière. Et comme A_{n+1} est algébriquement maximal et que le plongement de A_{n+1} dans A_{n+3} est local, la propriété 3.4 assure que l'extension $K_{n+2}|K_{n+1}$ est aussi régulière, d'où ($\mathrm{v_{n+1}}$).

Enfin $L_{n+1} \preceq L_{n+3}$, *i.e.* $(L_{n+3}, L_{n+1}) \equiv (L_{n+1}, L_{n+1})$ et, le plongement σ_n étant élémentaire, on a $L_{n+1} \preceq L_{n+2}$, *i.e.* $(L_{n+2}, L_{n+1}) \equiv (L_{n+1}, L_{n+1})$, d'où ($\mathrm{vi_{n+1}}$), ce qui achève la récurrence.

La construction ci-dessus nous donne deux chaînes élémentaires :

$$A_1 \preceq A_3 \preceq \cdots \preceq A_{2n+1} \preceq \cdots \quad \text{et} \quad A_2 \preceq A_4 \preceq \cdots \preceq A_{2n} \preceq \cdots$$

avec pour chaque entier non nul n un plongement φ_n de A_n dans A_{n+1}, tel que le diagramme représentant tous ces morphismes soit commutatif.
Posons $B' := \bigcup_{n \in \mathbb{N}} A_{2n+1}$, $B'' := \bigcup_{n \in \mathbb{N}} A_{2n}$, $\varphi' := \bigcup_{n \in \mathbb{N}} \varphi_{2n+1}$ et $\varphi'' := \bigcup_{n \in \mathbb{N}} \varphi_{2n}$.

Par construction, $A' = A_1 \preceq B'$, $A'' \preceq A_2 \preceq B''$, et φ' est un isomorphisme de B' dans B'', de réciproque φ''. Comme pour tout n, $\varphi_{n|A}$ est l'identité, on a $\varphi'_{|A} = Id_A$, et φ' est l'isomorphisme cherché.

■

Corollaire 3
Soient $T_1, \ldots, T_r$ des théories d'anneaux de valuation henséliens, modèle-complètes et approximables, avec $r \neq 0$. Soient $(A, \leq, I_1, \ldots, I_r) \subseteq (A', \leq', I'_1, \ldots, I'_r)$ deux modèles intégralement maximaux de $\mathcal{T}(T_1, \ldots, T_r)$, satisfaisant le LGPH, tels que $(0) \in \mathrm{Sp}(A', \leq')$ si et seulement si $(0) \in \mathrm{Sp}(A'', \leq'')$. Notons L, L'' leurs treillis résiduels (munis de leurs filtres). Alors :

$$(A, \leq, I_1, \ldots, I_r) \preceq (A', \leq', I'_1, \ldots, I'_r) \iff L \preceq L'.$$

Preuve: Puisque $L \preceq L'$, le plongement de A dans A' est local, et la propriété 3.4 assure que l'extension $K'|K$ est régulière. On a $(L, L) \equiv (L', L)$, donc il suffit d'appliquer le lemme 2, en prenant $A'' = A$. Il vient (en sous-entendant les relations radicales et les idéaux r-clos) : $(A, A) \equiv (A', A)$, *i.e.* $A \preceq A'$. La réciproque est triviale.

∎

Corollaire 4

Soient $T_1, \ldots, T_r$ des théories d'anneaux de valuation henseliens, modèle-complètes et approximables, avec $r \neq 0$. Soient $(A, \leq, I_1, \ldots, I_r)$, $(A', \leq', I'_1, \ldots, I'_r)$ deux modèles intégralement maximaux de $\mathcal{T}(T_1, \ldots, T_r)$ tels que :

– *$(0) \in \mathrm{Sp}(A, \leq)$ si et seulement si $(0) \in \mathrm{Sp}(A', \leq')$;*

– *A et A' satisfont le LGPH.*

Notons K, K' leurs corps de fractions respectifs, et L, L' leurs treillis résiduels (munis de leurs filtres). Si les plongements de $\mathrm{Alg}(A, \leq, I_1, \ldots, I_r)$ dans $(A, \leq, I_1, \ldots, I_r)$ et de $\mathrm{Alg}(A', \leq', I'_1, \ldots, I'_r)$ dans $(A', \leq', I'_1, \ldots, I'_r)$ sont locaux alors :
$(A, \leq, I_1, \ldots, I_r) \equiv (A', \leq', I'_1, \ldots, I'_r)$ si et seulement si il existe un isomorphisme $\varphi : \mathrm{Alg}(A, \leq, I_1, \ldots, I_r) \longrightarrow \mathrm{Alg}(A', \leq', I'_1, \ldots, I'_r)$ tel que $(L, \mathrm{Alg}(L)) \equiv (L', \overline{\varphi}(\mathrm{Alg}(L))$.

Preuve: $(L, \mathrm{Alg}(L)) \equiv (L', \overline{\varphi}(\mathrm{Alg}(L))$ signifie que quand on identifie $\mathrm{Alg}(A)$ (les I_k sont sous-entendus) à son image par φ, il devient une sous-structure $\cap$-stable commune à A et A', telle que $(L, \mathrm{Alg}(L)) \equiv (L', \mathrm{Alg}(L))$. On peut donc appliquer le lemme 2 : il vient $(A, \mathrm{Alg}(A)) \equiv (A', \mathrm{Alg}(A))$, et *a fortiori* $A \equiv A'$. La réciproque est banale (prendre pour φ la restriction à $\mathrm{Alg}(A)$ d'un isomorphisme entre deux extensions élémentaires de $(A, \leq, I_1, \ldots, I_r)$ et $(A', \leq', I'_1, \ldots, I'_r)$).

∎

§ 6. Applications

On fixe pour la durée de ce paragraphe un ensemble fini $\mathcal{P} := \{p_1, \ldots, p_r\}$ d'entiers premiers, et pour tout $k \in [\![1, r]\!]$:

– un entier naturel non nul d_k ;

– $T_k :=$ la théorie des corps p_k-adiquement clos de rang d_k.

On pose $M := \{(p_1, d_1), \ldots, (p_r, d_r)\}$; nous dirons qu'un corps K est ***M*-maximal** s'il admet pour tout $(p, d) \in M$ une valuation p-adique de rang inférieur ou égal à d, et si aucune extension algébrique propre de K n'a cette propriété. On peut montrer que le henselisé d'un tel corps relativement à n'importe quelle valuation indépendante de celles énumérées par M est algébriquement clos.

Un corps M-maximal contient $\mathbb{Q}_{M-abs}$, donc la clôture intégrale $\widetilde{\mathbb{Z}} \cap K$ de $\mathbb{Z}$ dans K satisfait le LGPH (parce que c'est la clôture intégrale de $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_{M-abs}$ dans K, que $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_{M-abs}$ satisfait le LGPH d'après le corollaire I.2.5, et que le LGPH est stable par cloture intégrale d'après le corollaire III.2.4). Si K est algébrique sur $\mathbb{Q}$ le corollaire I.4.6 entraîne que $K \in \mathrm{RC}(W_{\widetilde{\mathbb{Z}} \cap K})$ et donc K est PC_M. Si on munit $\widetilde{\mathbb{Z}} \cap K$ de sa relation radicale associée, et de l'idéal I_k associé à la p_k-valuation de K pour tout $k \in [\![1, r]\!]$, on obtient donc un modèle algébriquement maximal de $\mathcal{T}(T_1, \ldots, T_r)$.

De plus on sait que dans un corps PC_M, l'anneau d'holomorphie de chaque famille de valuation p_k-adique de rang d_k est définissable (on suppose les couples (p_k, d_k) deux à deux distincts, *cf.* [Kü 89]). Toute la $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure additionnelle de $\widetilde{\mathbb{Z}} \cap K$ est donc définissable dans l'anneau, d'où il suit que $\widetilde{\mathbb{Z}} \cap K$ est décidable si et seulement si $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$ est décidable.

Enfin le treillis résiduel de $\widetilde{\mathbb{Z}} \cap K$ est une quasi-algèbre de Boole propre et dense d'après le lemme IV.6.1, et on admettra (c'est démontré en annexe) que la théorie des quasi-algèbres de Boole propres et denses munies de r ultrafiltres distincts est complète et modèle-complète.

Proposition 1
Soit K un corps M-maximal algébrique sur $\mathbb{Q}$. Notons $\widetilde{\mathbb{Z}} \cap K$ la clôture intégrale de $\mathbb{Z}$ dans K, munie de sa $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure définie comme ci-dessus, et soit L son treillis résiduel, muni de ses r ultrafiltres.
Les propriétés suivantes caractérisent les $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structures $(A', \leq', I'_1, \ldots, I'_r)$ élémentairement équivalentes à $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$:
(a) *$(A', \leq')$ est un r_o-domaine satisfaisant le LGPH ;*
(b) *$(A', \leq', I'_1, \ldots, I'_r)$ est un modèle algébriquement maximal de $\mathcal{T}(T_1, \ldots, T_r)$;*
(c) *$\mathrm{L}(A', \leq', I'_1, \ldots, I'_r)$ est une quasi-algèbre de Boole propre et dense munie de r ultrafiltres distincts ;*
(d) *"$\forall x, f(x) \neq 0$" pour tous les polynômes f à coefficients entiers globalement étrangers, irréductibles sur $\mathbb{Q}$ et non unitaires ;*
(e) *$\mathrm{Alg}(\mathrm{Fr}(A')) \simeq K$.*

Preuve: Soit $(A', \leq', I'_1, \ldots, I'_r)$ une $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure. Les propriétés (a) à (d) sont satisfaites par $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$ et sont du premier ordre, donc si $(A', \leq', I'_1, \ldots, I'_r)$ est élémentairement équivalent à $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$, il les satisfait nécessairement aussi. De plus, si $A \equiv A'$ ils ont de ultrapuissances isomorphes, et l'isomorphisme en question envoie les parties algébriques l'une sur l'autre, d'où (e).

Inversement, si $(A', \leq', I'_1, \ldots, I'_r)$ vérifie ces propriétés, on peut vu (e) identifier $\mathrm{Fr}(A') \cap \mathbb{Q}^a$ à K. Le (d) entraîne alors que $A' \cap \mathbb{Q}^a$ est entier sur $\mathbb{Z}$, et donc que $A' \cap \mathbb{Q}^a = \widetilde{\mathbb{Z}} \cap K$. Le même argument que dans la proposition IV.6.6 entraîne que $(\widetilde{\mathbb{Z}} \cap K, \leq) \simeq \mathrm{Alg}(A', \leq')$.

Pour tout $k \in [\![1, r]\!]$, $A'_{I'_k}$ est l'anneau d'une p_k-valuation de rang d_k d'après (b), donc sa trace sur K est de rang $\leq d_k$, or K n'a qu'une seule p_k-valuation de rang $\leq d_k$: c'est celle d'anneau A_{I_k}. On a donc $A'_{I'_k} \cap K = A_{I_k}$ *i.e.* $I'_k \cap A = I_k$, et ceci valant pour tout k il suit que $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r) = \mathrm{Alg}(A', \leq', I'_1, \ldots, I'_r)$.

La proposition 2.2 donne donc un plongement de L dans $L' := \mathrm{L}(A', \leq', I'_1, \ldots, I'_r)$. Mais L' et L sont tous deux modèles de $\mathrm{Th}(L)$ et cette théorie est modèle-complète. On a donc $L \preceq L'$ et le corollaire 5.3 s'applique : $(A, \leq, I_1, \ldots, I_r) \preceq (A', \leq', I'_1, \ldots, I'_r)$. En particulier, ils sont élémentairement équivalents.

■

Corollaire 2
Avec les notations ci-dessus, $\widetilde{\mathbb{Z}} \cap K$ est décidable si et seulement si K est décidable. Dans tous les cas la théorie complète de $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$ est modèle-complète.
En particulier la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_p$ est décidable (dans le langage des anneaux) et sa théorie complète dans le langage des r-anneaux est modèle-complète.

Preuve: La théorie complète de $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$ est axiomatisée par les conditions (a) à (e) de la proposition 1. Les quatre premières sont récursivement axiomatisables :

on a donné des schémas d'axiomes pour (a) et (b), et c'est assez trivial pour (c) et (d). Si K est décidable la condition (e) sera aussi récursivement axiomatisable, et la théorie complète de $(\widetilde{\mathbb{Z}} \cap K, \leq, I_1, \ldots, I_r)$, et *a fortiori* de $\widetilde{\mathbb{Z}} \cap K$ sera donc décidable (car complète et récursivement axiomatisée). La réciproque (si $\widetilde{\mathbb{Z}} \cap K$ est décidable alors K est décidable) est banale, puisque $K = \mathrm{Fr}(\widetilde{\mathbb{Z}} \cap K)$.

Si $(A', \leq') \subseteq (A'', \leq'')$ sont deux modèles de la théorie complète de $(\widetilde{\mathbb{Z}} \cap K, \leq)$, leurs corps des fractions respectifs sont munis pour chaque $k \in [\![1, r]\!]$ d'une unique p_k-valuation, donc la trace de la p_k-valuation de $K'' := \mathrm{Fr}(A'')$ sur $K' := \mathrm{Fr}(A')$ coïncide avec la p_k-valuation de K'. Si on munit A' et A'' de la $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure définie en interprétant chaque symbole I_k par la trace de l'idéal maximal de la p_k-valuation de leur corps de fractions, on obtient deux $\mathrm{L}^{\mathrm{r}}_{\mathrm{rad}}$-structure $(A', \leq', I'_1, \ldots, I'_r) \subseteq (A'', \leq'', I''_1, \ldots, I''_r)$ satisfaisant les conditions (a) à (e) de la proposition 1. On a donc, en notant L' et L'' leurs treillis résiduels (munis de leurs ultrafiltres) $L' \subseteq L''$ et même $L' \preceq L''$ puisque la théorie des quasi-algèbres de Boole propres et denses munies de r ultrafiltres distincts est modèle-complète, donc le corollaire 5.3 entraîne que $(A', \leq', I'_1, \ldots, I'_r) \preceq (A'', \leq'', I''_1, \ldots, I''_r)$ et *a fortiori* $(A', \leq') \preceq (A'', \leq'')$.
∎

Remarque: La décidabilité de la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_p$ avait été annoncée par Prestel et Schmid dans [P-S 91] mais leur démonstration comportait une erreur : ils utilisaient leur LGP, dont nous avons montré qu'il était équivalent au LGPA, pour axiomatiser cet anneau, alors que celui-ci n'est manifestement pas PAC. L'observation de cette anomalie a été la motivation initiale pour introduire le LGPH.

On notera d'ailleurs que l'astuce qui a permis au précédent chapitre de démontrer la décidabilité de $\mathbb{Z}_{p-abs}$ sans utiliser le LGPH ne peut pas marcher ici : le point crucial était que $\mathbb{Z}_{p-abs}$ est l'intersection d'un anneau PAC et de l'anneau d'holomorphie de $\mathbb{Q}_{p-abs}$; et ceci est faux pour $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_p$ (parce que l'idéal maximal associé à la valuation p-adique est recouvert par les autres idéaux maximaux de $\widetilde{\mathbb{Z}} \cap \mathbb{Q}_p$).

Annexe A
Quasi-algèbres de Boole

Nous démontrons ici les propriétés modèle-théoriques des quasi-algèbres de Boole denses que nous avons utilisées dans les applications. Cette étude est semblable à celle des algèbres de Boole denses (dont on sait que leur théorie est complète et modèle-complète), telle qu'on peut la trouver par exemple dans [Mo].

Rappelons que si L est un treillis distributif avec extrémités et x un élément de L, on note $\mathrm{Sp}(L)$ l'ensemble des filtres premiers de L, $\mathrm{Spm}(L)$ l'ensemble des éléments de $\mathrm{Sp}(L)$ maximaux pour l'inclusion (*i.e.* les ultrafiltres sur L) et :

$$P_L(x) := \{\mathfrak{p} \in \mathrm{Sp}(L) \,/\, x \in \mathfrak{p}\}.$$

Les parties constructibles de L sont les combinaisons booléennes de parties du type $P_L(x)$, pour $x \in L$. On omet l'indice L chaque fois que cette précision est rendue superflue par le contexte. Il est classique que pour tous $x, y \in L$ on a :

$$x \leq y \iff P(x) \subseteq P(y).$$

Nous avons appelé **quasi-algèbres de Boole** les treillis distributifs L avec extrémités tels que :

$$\forall \alpha \in L \setminus \{\mathbf{1}_L\},\ \forall \beta \in L,\ \exists \gamma \in L,\ \begin{cases} \beta \vee \gamma = \alpha \vee \beta \\ \beta \wedge \gamma = \mathbf{0}_L \end{cases}$$

Il est facile de voir qu'un tel γ est alors unique et qu'il vérifie $P(\gamma) = P(\alpha) \setminus P(\beta)$. Pour cette raison on le note $\alpha \setminus \beta$.

Remarques:
(1) Il est important de noter que dans ce paragraphe nous n'imposons pas aux extrémités d'un treillis d'être forcément distinctes, comme c'est souvent le cas. En particulier, un filtre premier ne pouvant pas contenir $\mathbf{0}$ par définition, le spectre de l'algèbre de Boole à un élément est vide.
(2) Un treillis distributif avec extrémités L est une quasi-algèbre de Boole si et seulement si pour tous $\alpha, \beta \in L$ on a :

$$\alpha \neq \mathbf{1}_L \quad \Longrightarrow \quad \exists \gamma \in L,\ P(\gamma) = P(\alpha) \setminus P(\beta).$$

L'élément γ en question est bien entendu égal à $\alpha \setminus \beta$.
(3) Un ensemble ordonné avec extrémités L est une quasi-algèbre de Boole si et seulement si quel que soit $e \in L \setminus \{\mathbf{1}_L\}$, l'ensemble des éléments de L plus petits que e est

une algèbre de Boole. En particulier toute algèbre de Boole est une quasi-algèbre de Boole (on a dans ce cas, pour tous $\alpha, \beta \in L$: $\alpha \setminus \beta = \alpha \wedge \overline{\beta}$).

Exemple: Si B est une algèbre de Boole donnée, et qu'on lui ajoute un nouvel élément plus grand que tous les autres, on obtient une quasi-algèbre de Boole qui n'est pas une algèbre de Boole (sauf dans le cas trivial où B n'a qu'un seul élément). Les quasi-algèbres de Boole L de cette forme sont caractérisées par le fait que $L \setminus \{\mathbf{1}_L\}$ possède un maximum.

Définitions
Une quasi-algèbre de Boole L est dite :
(a) **propre** si ce n'est pas une algèbre de Boole ;
(b) **fausse** si $L \setminus \{\mathbf{1}_L\}$ possède un élément maximum ;
(c) **vraie** si elle n'est pas fausse.

Propriété 1
Soit L une quasi-algèbre de Boole.
(1) $\mathrm{Sp}(L) \subseteq \mathrm{Spm}(L) \cup \{\mathbf{1}_L\}$, *et* $\{\mathbf{1}_L\} \in \mathrm{Sp}(L)$ *si et seulement si L est propre ou n'a que deux éléments.*
(2) *Soit $\mathcal{P}$ une partie constructible de* $\mathrm{Sp}(L)$, *alors il existe $e \in L \setminus \{\mathbf{1}_L\}$ tel que $\mathcal{P} = P(e)$ ou $\mathcal{P} = P(e)^c$. S'il existe $x \in L \setminus \{\mathbf{1}_L\}$ tel que $\mathcal{P} \subseteq P(x)$, alors on peut mettre $\mathcal{P}$ sous la première forme.*

Preuve: La démonstration est élémentaire, et semblable à celle des propriétés analogues sur le spectre r-clos d'un r-domaine $\cap$-stable et localement complémenté.
∎

Notations: Soit L un treillis distributif avec extrémités ; pour toute partie $\mathcal{P}$ de $\mathrm{Sp}(L)$, soit $L_0(\mathcal{P}) := \{e \in L \ / \ P(e) \subseteq \mathcal{P}\}$, et $L(\mathcal{P})$ définie comme suit :

$$L(\mathcal{P}) := \begin{cases} L_0(\mathcal{P}) & \text{si } L_0(\mathcal{P}) \text{ a un plus grand élément,} \\ L_0 \cup \{\mathbf{1}_L\} & \text{sinon.} \end{cases}$$

Il est clair que $L(\mathcal{P})$ est stable par $\vee$ et $\wedge$, et que c'est donc un treillis distributif. Il contient $\mathbf{0}_L$, qui est donc son minimum. Il possède aussi un élément maximum, par construction, mais celui-ci peut différer de celui de L.
Pour tout $x := (x_1, \ldots, x_n)$, et toute partie I de $[\![1, n]\!]$ posons :

$$\mathcal{P}_I(x) := \Big(\bigcap_{i \in I} P(x_i)\Big) \cap \Big(\bigcap_{i \in [\![1,n]\!] \setminus I} P(x_i)^c\Big).$$

On notera $L_I(x) := L(\mathcal{P}_I(x))$. Si $n = 0$, on aura alors $\mathcal{P}_\emptyset(\emptyset) = \mathrm{Sp}(L)$ et $L_\emptyset(\emptyset) = L(\mathrm{Sp}(L)) = L$ (ne pas confondre avec $L(\emptyset)$, qui est réduit à $\{\mathbf{0}_L\}$).
Enfin pour tout $e \in L$, on posera :

$$L(e) := L(P(e)) \quad \text{et} \quad L(e^\dagger) := L(P(e)^c).$$

On peut remarquer qu'avec ces notations, L est une quasi-algèbre de Boole si et seulement si pour tout $e \neq \mathbf{1}_L$, $L(e)$ est une algèbre de Boole ; et que si en outre il existe $e \neq \mathbf{1}_L$ tel que $L(e^\dagger)$ soit une algèbre de Boole alors L lui-même est une algèbre de Boole.

Notons enfin que pour tout $\mathcal{P} \subseteq \mathrm{Sp}(L)$ et tout $e \in L(\mathcal{P})$, on a :

$$L(\mathcal{P})(e) = L(\mathcal{P} \cap P(e)) \quad \text{et} \quad L(\mathcal{P})(e^\dagger) = L(\mathcal{P} \cap P(e)^c).$$

Propriété 2
Soit L une quasi-algèbre de Boole.
(1) *Soient $x := (x_1, \ldots, x_n) \in L^n$ et I une partie de $[\![1,n]\!]$. Si $L_0(\mathcal{P}_I(x))$ n'a pas de maximum alors L est propre, vraie, $I \subsetneq \{i \in [\![1,n]\!] \;/\; x_i = \mathbf{1}_L\}$, et $\mathcal{P}_I(x)$ est de la forme $P(e)^c$ avec e différent de $\mathbf{0}_L$ et de $\mathbf{1}_L$.*
(2) *Soit $\mathcal{P}$ une partie constructible de $\mathrm{Sp}(L)$ telle que $|L(\mathcal{P})| = 1$. Alors $L(\mathcal{P}) = \{\mathbf{0}_L\}$, et $\mathcal{P}$ est réduit à $\emptyset$ ou à $\{\mathbf{1}_L\}$, le second cas ne pouvant se produire que si L est fausse, a strictement plus de deux éléments (*i.e.* est propre et fausse), et si $\mathcal{P} = P(e)^c$ avec $e = \max L \setminus \{\mathbf{1}_L\}$.*

Preuve: C'est élémentaire.

■

Propriété 3
Soit L un treillis distributif avec extrémités, et $x = (x_1, \ldots, x_n)$ un n-uplet d'éléments de L.
(1) *$(\mathcal{P}_I(x))_{I \subseteq [\![1,n]\!]}$ forme une partition de $\mathrm{Sp}(L)$.*
(2) *Pour tous $i, j \in [\![1,n]\!]$, on a :*

$$x_i \leq x_j \quad \Longleftrightarrow \quad \forall I \subseteq [\![1,n]\!],\ (i \in I \text{ et } j \notin I \Longrightarrow \mathcal{P}_I(x) = \emptyset).$$

Preuve: On peut écarter le cas $n = 0$ où tout est trivial.
(1) Soient $I \neq J$ deux parties de $[\![1,n]\!]$ distinctes, par exemple $I \not\subseteq J$. Soit $i \in I \setminus J$; alors $\mathcal{P}_I(x) \subseteq P(x_i)$ et $\mathcal{P}_J(x) \subseteq P(x_i)^c$, donc $\mathcal{P}_I(x) \cap \mathcal{P}_J(x) = \emptyset$.

D'autre part pour tout $\mathfrak{p} \in \mathrm{Sp}(L)$, on a $\mathfrak{p} \in \mathcal{P}_I(x)$ où $I = \{i \in [\![1,n]\!] \;/\; x_i \in \mathfrak{p}\}$, donc $\mathrm{Sp}(L) \subseteq \bigcup_{I \subseteq [\![1,n]\!]} \mathcal{P}_I(x)$.

(2) D'après (1), $(\mathcal{P}_I(x))_{I \subseteq [\![1,n]\!]}$ partitionne $\mathrm{Sp}(L)$, donc pour toute partie $\mathcal{P}$ de $\mathrm{Sp}(L)$ on a :

$$\mathcal{P} = \bigcup_{I \subseteq [\![1,n]\!]} \mathcal{P} \cap \mathcal{P}_I(x).$$

En particulier, si $i, j \in [\![1,n]\!]$, on a :

$$\begin{aligned} x_i \leq x_j &\Longleftrightarrow P(x_i) \subseteq P(x_j) \Longleftrightarrow P(x_i) \cap P(x_j)^c = \emptyset \\ &\Longleftrightarrow \bigcup_{I \subseteq [\![1,n]\!]} \mathcal{P}_I(x) \cap P(x_i) \cap P(x_j)^c = \emptyset \end{aligned}$$

Or pour toute partie I de $[\![1,n]\!]$ on a :
- ou bien ($i \notin I$ ou $j \in I$), et alors trivialement $\mathcal{P}_I(x) \cap P(x_i) \cap P(x_j)^c = \emptyset$;
- ou bien non, et alors $P(x_i) \cap P(x_j)^c \supseteq \mathcal{P}_I(x)$, donc :

$$\mathcal{P}_I(x) \cap P(x_i) \cap P(x_j)^c = \emptyset \Longleftrightarrow \mathcal{P}_I(x) = \emptyset$$

d'où l'équivalence annoncée.

■

Définitions
J'appelle **relation de Vaught** toute relation binaire $\mathcal{R}$ entre quasi-algèbres de Boole, réflexive et symétrique, telle que pour toutes quasi-algèbres de Boole L et L' vérifiant $L \mathrel{\mathcal{R}} L'$ on ait :
(i) L est propre si et seulement si L' est propre ;

(ii) L et L' ont même cardinal ;
(iii) pour tout $x \in L$, il existe $x' \in L'$ tel que :

$$L(P(x)) \mathcal{R} L'(P(x')) \quad \text{et} \quad L(P(x)^c) \mathcal{R} L'(P(x')^c).$$

Remarque: Les relations de Vaught tirent leur nom du lemme 9.47, p. 154 de [Mo], attribué à Vaught. Le but de ce qui suit est de démontrer un résultat analogue à ce lemme : si $\mathcal{R}$ est une relation de Vaught et L, L' deux quasi-algèbres de Boole dénombrables telles que $L \mathcal{R} L'$, alors L et L' sont isomorphes.
Ce résultat requiert un dernier préliminaire.

Propriété 4
Soit $\mathcal{R}$ une relation de Vaught, et L, L' deux quasi-algèbres de Boole telles que $L \mathcal{R} L'$. Alors L est vraie si et seulement si L' est vraie.

Preuve: Si L est fausse, ou bien L a deux éléments, et dans ce cas L' aussi donc L' est fausse ; ou bien non, et dans ce cas L est propre et fausse, donc L' aussi est propre, et on a un élément $e := \max(L \setminus \{\mathbf{1}_L\})$ tel que $L(e)$ soit une algèbre de Boole tandis que $L(e^\dagger) = \{\mathbf{0}_L\}$. Puisque $L \mathcal{R} L'$ il existe $e' \in L'$ tel que $L(e) \mathcal{R} L'(e')$ et $L(e^\dagger) \mathcal{R} L'(e'^\dagger)$. Mais alors $L'(e')$ est une algèbre de Boole, donc $e' \neq \mathbf{1}_{L'}$ (car L' est propre) *i.e.* $P(e')^c \neq \emptyset$, et on a dans le même temps $|L'(e'^\dagger)| = |L(e^\dagger)| = 1$. D'après la propriété 2 il s'ensuit que L' est fausse et que $e' = \max(L' \setminus \{\mathbf{1}_{L'}\})$. Ceci démontre une implication, et la symétrie de $\mathcal{R}$ achève de prouver l'équivalence.
∎

Proposition 5
Soit $\mathcal{R}$ une relation de Vaught et L, L' deux quasi-algèbres de Boole finies ou dénombrables vérifiant $L \mathcal{R} L'$. Soient $x := (x_1, \ldots, x_n) \in L^n$ et $x' := (x'_1, \ldots, x'_n) \in L'^n$ tels que :

$$\forall k \in [\![0, n]\!],\ \forall I \subseteq [\![1, k]\!], \quad L_I(x_1, \ldots, x_k) \mathcal{R} L'_I(x'_1, \ldots, x'_k). \qquad (*)$$

Alors on peut compléter x et x' en deux suites $(x_k)_{k \in \mathbb{N}}$ et $(x'_k)_{k \in \mathbb{N}}$ telles que l'application $\varphi : x_k \longmapsto x'_k$ soit un isomorphisme de L sur L', et :

$$\forall k \in \mathbb{N},\ \forall I \subseteq [\![1, k]\!], \quad L_I(x_1, \ldots, x_k) \mathcal{R} L'_I(x'_1, \ldots, x'_k). \qquad (**)$$

Remarques:
(1) Si $L \mathcal{R} L'$ alors l'hypothèse $(*)$ est vérifiée avec $n = 0$ et $x = x' = \emptyset$, donc cette proposition montre que deux algèbres de Boole liées par une relation de Vaught sont isomorphes; on retrouve ainsi le lemme 9.47 de [Mo].
(2) Inversement l'hypothèse $(*)$ avec $k = 0$ entraîne que $L \mathcal{R} L'$.

Preuve: On peut distinguer trois étapes.

Étape 1 : On montre que si L (et donc aussi L') est propre ou fausse, alors pour tout $k \in [\![1, n]\!]$, $x_k = \mathbf{1}_L \iff x'_k = \mathbf{1}_{L'}$.

La seule quasi-algèbre de Boole qui soit fausse sans être propre est l'algèbre de Boole à deux éléments. Ce cas trivial est laissé au lecteur, et nous supposons ici que L est propre, donc que quel que soit $e \in L \setminus \{\mathbf{1}_L\}$, $L(e^\dagger)$ est propre (et $L(e)$ ne l'est pas, cette dernière propriété étant commune à toutes les quasi-algèbres de Boole).

Pour $k = 0$ on a $L \mathcal{R} L'$ et il n'y a rien d'autre à montrer.

Soit $k \in [\![1,n]\!]$ tel que $x_k = \mathbf{1}_L$, et supposons que pour tout $i < k$ on ait montré que $x_i = \mathbf{1}_L \iff x'_i = \mathbf{1}_{L'}$. Soient $I_k := \{i \in [\![1,k-1]\!] \,/\, x_i = \mathbf{1}_L\}$, $I'_k := I_k \cup \{k\}$, et $J_k := [\![1,k-1]\!] \setminus I_k$.

Par l'absurde, si $x'_k \neq \mathbf{1}_{L'}$, alors :

$$L'_{I'_k}(x'_1,\ldots,x'_k) = L'\Big(\bigcap_{j\in J_k} P(x'_j)^c \cap P(x'_k)\Big) = L'\Big(x'_k \setminus \bigvee_{j\in J_k} x'_j\Big).$$

On a $x'_k \setminus \bigvee_{j\in J_k} x'_j \in L' \setminus \{\mathbf{1}_{L'}\}$, donc $L'_{I'_k}(x'_1,\ldots,x'_k)$ est une algèbre de Boole.
D'autre part :

$$L_{I_k}(x_1,\ldots,x_k) = L\Big(\bigcap_{j\in J_k} P(x_j)^c \cap P(x_k)\Big) = L\Big(\bigcap_{j\in J_k} P(x_j)^c\Big) = L\Big(\Big(\bigvee_{j\in J_k} x_j\Big)^{\dagger}\Big)$$

Quel que soit $j \in J_k$ on a $x_j \neq \mathbf{1}_L$, et comme $\{\mathbf{1}_L\}$ est premier (car L est propre), il s'ensuit que $\bigvee_{j\in J_k} x_j \neq \mathbf{1}_L$ donc que $L((\bigvee_{j\in J_k} x_j)^{\dagger})$ n'est pas une algèbre de Boole. Or l'hypothèse $(*)$ entraîne que $L_{I_k}(x_1,\ldots,x_k)\ \mathcal{R}\ L'_{I'_k}(x'_1,\ldots,x'_k)$ donc l'une est propre si et seulement si l'autre est propre, d'où une contradiction.
Ceci démontre une implication, et l'équivalence en découle par symétrie.

Étape 2 : Pour tout $x_{n+1} \in L$, il existe $x'_{n+1} \in L'$ tel que pour tout $k \in [\![0,n+1]\!]$ et tout $I \subseteq [\![1,k]\!]$ on ait $L_I(x_1,\ldots,x_k)\ \mathcal{R}\ L'_I(x'_1,\ldots,x'_k)$.

Soit $x_{n+1} \in L$; vu $(*)$ il suffit de trouver $x'_{n+1} \in L'$ tel que pour tout $I \subseteq [\![1,n+1]\!]$ on ait $L_I(x_1,\ldots,x_{n+1})\ \mathcal{R}\ L'_I(x'_1,\ldots,x'_{n+1})$. Si $x_{n+1} = \mathbf{1}_L$ il est clair que $x'_{n+1} = \mathbf{1}_{L'}$ convient, on écarte donc ce cas en supposant que $x_{n+1} \neq \mathbf{1}_L$.

Soit I une partie de $[\![1,n]\!]$; comme $x_{n+1} \neq \mathbf{1}_L$ on peut trouver $e_I \in L$ tel que $P(e_I) = \mathcal{P}_I(x) \cap P(x_{n+1})$. On notera que e_I appartient à $L_I(x)$, puisque $P(e_I) \subseteq \mathcal{P}_I(x)$. On a $L_I(x)\ \mathcal{R}\ L'_I(x')$ donc il existe $e'_I \in L'_I(x')$ tel que :

$$L_I(x)(e_I)\ \mathcal{R}\ L'_I(x')(e'_I) \quad \text{et} \quad L_I(x)(e_I^{\dagger})\ \mathcal{R}\ L'_I(x')(e_I'^{\dagger})$$

On commence par vérifier que $P(e'_I) \subseteq \mathcal{P}_I(x')$.

Par l'absurde, supposons que ce ne soit pas le cas. Alors $e'_I \notin L'_0(\mathcal{P}_I(x'))$, et comme par ailleurs $e'_I \in L'_I(x') \subseteq L'_0(\mathcal{P}_I(x')) \cup \{\mathbf{1}_{L'}\}$, c'est donc que $e'_I = \mathbf{1}_{L'}$ et que $\mathbf{1}_{L'} \in L'_I(x') \setminus L'_0(\mathcal{P}_I(x'))$, donc que $L'_0(\mathcal{P}_I(x'))$ n'a pas de maximum. Par la propriété 2 on en déduit que L' est vraie, propre, et que $I \subseteq \{i \in [\![1,n]\!] \,/\, x'_i = \mathbf{1}_{L'}\} = \{i \in [\![1,n]\!] \,/\, x_i = \mathbf{1}_L\}$ (la dernière égalité venant de l'étape 1). On a donc : $L'_I(x')(e_I'^{\dagger}) = L'_I(x')(\emptyset) = \{\mathbf{0}_{L'}\}$, et il s'ensuit que $L_I(x)(e_I^{\dagger})$ n'a elle aussi qu'un seul élément. Or d'après la propriété 4, L est vraie $\Longrightarrow$ L' est vraie ; comme $L(\mathcal{P}_I(x) \cap P(e_I)^c) = L_I(x)(e^{\dagger}) = \{\mathbf{0}_{L'}\}$ la propriété 2 entraîne que $\mathcal{P}_I(x) \cap P(e_I)^c = \emptyset$, *i.e.* que $\mathcal{P}_I(x) \subseteq P(e_I)$. L'inclusion inverse est vérifiée par construction, donc $\mathcal{P}_I(x) = P(e_I)$.

Or quel que soit $i \in I$ on a $x_i = \mathbf{1}_L$, donc en notant $J := [\![1,n]\!] \setminus I$ il vient : $\mathcal{P}_I(x) = \cap_{j\in J} P(x_j)^c = P(\bigvee_{j\in J} x_j)^c$. Puisque L est propre, $P(e_I) = P(\bigvee_{j\in J} x_j)^c$ n'est possible que si $e_I = \mathbf{1}_L$ et $\bigvee_{j\in J} x_j = \mathbf{0}_L$ ou l'inverse. Mais si on avait $\bigvee_{j\in J} x_j = \mathbf{1}_L$, il s'ensuivrait que $L_I(x) = L(\emptyset) = \{\mathbf{0}_L\}$, donc que $L'_I(x') = \{\mathbf{0}_{L'}\}$, donc enfin que $L'_0(\mathcal{P}_I(x')) = \{\mathbf{0}_{L'}\}$, ce qui est exclu puisque $L'_0(\mathcal{P}_I(x'))$ n'a pas de maximum. On a donc bien $e_I = \mathbf{1}_L$, et puisque $e_I \le x_{n+1}$, il vient $x_{n+1} = \mathbf{1}_L$. Mais on a supposé dès le départ $x_{n+1} \neq \mathbf{1}_L$, et nous tombons encore dans une contradiction, d'où la conclusion : $P(e'_I) \subseteq \mathcal{P}_I(x')$.

Il reste à vérifier que $x'_{n+1} := \bigvee_{I \subseteq [\![1,n]\!]} e'_I$ convient.
Notons que pour tout $I \subseteq [\![1,n]\!]$ on a :
– $P(e_I) = \mathcal{P}_I(x) \cap P(x_{n+1})$, par définition de e_I.
– $P(e'_I) = \mathcal{P}_I(x') \cap P(x'_{n+1})$, parce que les $\mathcal{P}_J(x')$ partitionnent $\mathrm{Sp}(L')$ (quand J décrit l'ensemble des parties de $[\![1,n]\!]$), et qu'on a vérifié que $P(e'_I) \subseteq \mathcal{P}_I(x')$.

Soit $J \subseteq [\![1,n+1]\!]$; il nous faut distinguer deux cas :

Cas 1. $n+1 \in J$. Alors $J = I \cup \{n+1\}$, où $I \subseteq [\![1,n]\!]$, et il vient :

$$\begin{aligned}\mathcal{P}_J(x_1,\ldots,x_{n+1}) &= \Big(\bigcap_{i\in I} P(x_i)\Big) \cap \Big(\bigcap_{i\in[\![1,n]\!]\setminus I} P(x_i)^c\Big) \cap P(x_{n+1})\\ &= \mathcal{P}_I(x) \cap P(x_{n+1})\\ &= P(e_I).\end{aligned}$$

Comme $P(e_I) \subseteq \mathcal{P}_I(x)$, on a $L(e_I) = L_I(x)(e_I)$ et donc $L_J(x_1,\ldots,x_{n+1}) = L(e_I) = L_I(x)(e_I)$.
De même $L'_J(x'_1,\ldots,x'_{n+1}) = L'_I(x')(e'_I)$, d'où $L_J(x_1,\ldots,x_{n+1}) \;\mathcal{R}\; L'_J(x'_1,\ldots,x'_{n+1})$.

Cas 2. $n+1 \notin J$. Alors $J \subseteq [\![1,n]\!]$, et il vient :

$$\begin{aligned}\mathcal{P}_J(x_1,\ldots,x_{n+1}) &= \Big(\bigcap_{i\in J} P(x_i)\Big) \cap \Big(\bigcap_{i\in[\![1,n]\!]\setminus J} P(x_i)^c\Big) \cap P(x_{n+1})^c\\ &= \mathcal{P}_J(x) \cap P(x_{n+1})^c\\ &= \mathcal{P}_J(x) \cap P(e_I)^c\end{aligned}$$

Comme dans le cas 1, on en déduit que $L_J(x_1,\ldots,x_{n+1}) = L_J(x)(e^\dagger_J)$, et de même $L'_J(x'_1,\ldots,x'_{n+1}) = L'_J(x')(e'^\dagger_J)$, d'où là encore $L_J(x_1,\ldots,x_{n+1}) \;\mathcal{R}\; L'_J(x'_1,\ldots,x'_{n+1})$.

Étape 3 : Construction de l'isomorphisme par va-et-vient.

Soient $(y_k)_{k\in\mathbb{N}}$ et $(y'_k)_{k\in\mathbb{N}}$ des énumérations de L et L' respectivement. On peut itérer, pour tout $m \in \mathbb{N}$, la construction de l'étape 2 :

- si $(x_i)_{1\le i\le n+2m}$ et $(x'_i)_{1\le i\le n+2m}$ sont déja construits, on prend $x_{n+2m+1} = y_l$ où $l = \min\{k \in \mathbb{N} /\ y_k \notin \{x_i /\ 1 \le i \le n+2m\}\}$ (si cet ensemble est vide on prend $x_{n+2m+1} = \mathbf{1}_L$) et soit x'_{n+2m+1} l'élément correspondant de L' donné par l'étape 2 ;
- si $(x_i)_{1\le i\le n+2m+1}$ et $(x'_i)_{1\le i\le n+2m+1}$ sont déja construits, on prend de même $x'_{n+2m+2} = y'_l$ où $l = \min\{k \in \mathbb{N} /\ y_k \notin \{x'_i /\ 1 \le i \le n+2m+1\}\}$ (si cet ensemble est vide on prend $x'_{n+2m+2} = \mathbf{1}_L$) et soit x_{n+2m+2} l'élément de L donné par l'étape 2 (en inversant les rôles de L et L', ce qu'on peut faire puisque tout est symétrique).

Ceci nous définit deux suites $(x_i)_{i\in\mathbb{N}^*}$ et $(x'_i)_{i\in\mathbb{N}^*}$ satisfaisant la condition $(**)$ telles que $L = \{x_i /\ i \in \mathbb{N}^*\}$ et $L' = \{x'_i /\ i \in \mathbb{N}^*\}$. Il ne reste qu'à vérifier que l'application $\varphi : x_k \longmapsto x'_k$ est bien définie, et qu'elle est strictement croissante. Il suffit pour cela de démontrer que :

$$\forall i,j \in \mathbb{N}^*, \quad x_i \le x_j \iff x'_i \le x'_j \tag{1}$$

Par symétrie, il suffit de montrer une implication. Soient $i,j \in \mathbb{N}^*$ tels que $x_i \le x_j$, et posons $m := \max(i,j)$, $y := (x_1,\ldots,x_m)$ et $y' := (x'_1,\ldots,x'_m)$. D'après la propriété 3, il suffit de montrer que quel que soit $I \subseteq [\![1,m]\!]$, si $i \in I$ et $j \notin I$, alors $\mathcal{P}_I(y') = \emptyset$.

Soit donc $I \subseteq [\![1,m]\!]$ tel que $i \in I$ et $j \notin I$. On a $\mathcal{P}_I(y) = \emptyset$, et $L(\mathcal{P}_I(y)) \mathcal{R} L'(\mathcal{P}_I(y'))$, donc $|L'_I(y')| = |L_I(y)| = 1$, donc $\mathcal{P}_I(y')$ est vide ou réduit à $\{\mathbf{1}_{L'}\}$. Mais si par l'absurde $\mathcal{P}_I(y') = \{\mathbf{1}_L\}$ c'est que L' (et donc L) est fausse, et que pour tout $k \in I$, $x'_k = \mathbf{1}_{L'}$. En particulier $x'_i = \mathbf{1}_{L'}$, et l'étape 1 entraîne que $x_i = \mathbf{1}_L$. Comme $x_i \leq x_j$ il s'ensuit que $x_j = \mathbf{1}_L$, et donc par l'étape 1 que $x'_j = \mathbf{1}_{L'}$, d'où $x'_i \leq x'_j$, ce qui contredit $\mathcal{P}_I(y') \neq \emptyset$. On a donc bien $\mathcal{P}_I(y') = \emptyset$, d'où la conclusion.

■

Corollaire 6
La théorie des quasi-algèbres de Boole propres et denses est complète et modèle complète.

Preuve: C'est le cas particulier où $p = 0$ de l'énoncé suivant.

■

Corollaire 7
Soit p un entier fixé, et Σ la classe des structures $(L, F_1, \ldots, F_p)$ telles que :
(i) *L est une quasi-algèbre de Boole propre ;*
(ii) *L est dense et $\mathbf{0}_L \neq \mathbf{1}_L$;*
(iii) *$\forall k \in [\![1,p]\!]$, F_k est un ultrafiltre de L ;*
(iv) *les F_k sont deux à deux distincts.*
Alors Σ est élémentaire, et sa théorie est complète et modèle-complète.

Preuve:
(a) Σ est axiomatisée par :
• la théorie des treillis distributifs avec extrémités, complétée de l'axiome "$\mathbf{0} \neq \mathbf{1}$" ;
• $\forall e \forall e' \exists e''$, $e \neq \mathbf{1} \to (e' \wedge e'' = \mathbf{0}$ et $e' \vee e'' = e \vee e')$
(*i.e.* L est une quasi-algèbre de Boole) ;
• $\exists e \forall e'(e \wedge e' = \mathbf{0} \to e \vee e' \neq \mathbf{1})$
(*i.e.* L n'est pas une algèbre de Boole) ;
• $\forall e \forall e' \exists e''(e < e' \to e < e'' < e')$
(densité) ;
• pour chaque $k \in [\![1,p]\!]$:
 – $\neg F_k(\mathbf{0})$ et $F_k(\mathbf{1})$
 – $\forall e \forall e'((F_k(e')$ et $F_k(e)) \to F_k(e \wedge e'))$
 – $\forall e \forall e'(F_k(e \vee e') \leftrightarrow (F_k(e)$ ou $F_k(e')))$
 – $\exists e(F_k(e)$ et $e \neq \mathbf{1})$
(*i.e.* F_k est un filtre premier de $\mathrm{Sp}(L)$ non réduit à $\{\mathbf{1}_L\}$) ;
• pour chaque $k \neq l \in [\![1,p]\!]$, $\exists e(F_k(e)$ et $\neg F_l(e))$
(*i.e.* (iv)).

(b) Pour montrer que cette théorie, disons T, est complète, on vérifie à l'aide de la proposition 5 qu'elle est $\aleph_0$-catégorique. Soit Γ la classe des treillis finis ou dénombrables $(L, F_1, \ldots, F_p)$ munis de p prédicats unaires tels que :
(i) L est une quasi-algèbre de Boole ;
(ii) L est dense ;
(iii) $\forall k \in [\![1,p]\!]$, ou bien $F_k = \emptyset$, ou bien F_k est un ultrafiltre de L ;
(iv) les F_k sont deux à deux disjoints.

Notons que par densité si $(L, F_1, \ldots, F_p) \in \Gamma$ est fini alors il n'a qu'un seul élément ;

et si $F_k \neq \emptyset$ alors $F_k \neq \{\mathbf{1}_L\}$ (car F_k est maximal et que puisqu'il est non vide L n'est pas réduit à un seul élément).

Si L est un treillis distributif dense avec extrémités et F un ultrafiltre de L, alors pour tout $e \in L$, $L(e)$ (resp. $L(e^\dagger)$) est dense, et $F \cap L(e)$ (resp. $F \cap L(e^\dagger)$) est soit vide, soit un ultrafiltre de $L(e)$ (resp. $L(e^\dagger)$). Donc si $(L, F_1, \ldots, F_p) \in \Gamma$, pour toute partie constructible $\mathcal{P}$ de $\mathrm{Sp}(L)$, $L(\mathcal{P})$ muni de la trace des F_k appartient encore à Γ.

Pour tout $L \in \Gamma$ posons $\mathcal{I}(L) := \{k \in [\![1,p]\!] \;/\; F_k \neq \emptyset\}$. Soit $\mathcal{R}$ la relation définie sur Γ par $L \,\mathcal{R}\, L'$ si et seulement si :

- L est propre $\iff$ L' est propre ;
- $|L| = |L'|$;
- $\mathcal{I}(L) = \mathcal{I}(L')$.

Pour montrer que $\mathcal{R}$ est une relation de Vaught il ne reste qu'à vérifier qu'elle satisfait la propriété (iii) de ces relations. Soient donc $L, L' \in \Gamma$ tels que $L \,\mathcal{R}\, L'$, et x un élément de L. Il nous faut trouver $x' \in L'$ tel que $L(x) \,\mathcal{R}\, L'(x')$ et $L(x^\dagger) \,\mathcal{R}\, L'(x'^\dagger)$.

Cas 1. $x = \mathbf{0}_L$. On prend $x' = \mathbf{0}_{L'}$.

Cas 2. $x = \mathbf{1}_L$. On prend $x' = \mathbf{1}_{L'}$.

Cas 3. $x \notin \{\mathbf{0}_L, \mathbf{1}_L\}$. Alors $L(x)$ et $L(x^\dagger)$ ne sont pas des singletons, et sont encore des éléments de Γ, en outre $\mathcal{I}(L(x))$ est exactement l'ensemble des $k \in [\![1,p]\!]$ tels que $x \in F_k$, et $\mathcal{I}(x^\dagger) = \mathcal{I}(L) \setminus \mathcal{I}(L(x^\dagger))$. Comme $\mathcal{I}(L) = \mathcal{I}(L')$, pour tout $k \in \mathcal{I}(L)$ on a $F'_k \neq \emptyset$ donc $F'_k \neq \{\mathbf{1}_L\}$ et on peut trouver un élément $e'_k \in F'_k \setminus \bigcup\{F'_l \;/\; l \in \mathcal{I}(L) \text{ et } l \neq k\}$ (cela parce que les F'_k, pour $k \in \mathcal{I}(L)$, sont deux à deux incomparables pour l'inclusion ; e'_k s'obtient en prenant pour tout $l \neq k$ un élément $e'_{k,l} \in F'_k \setminus F'_l$ et $e'_k := \bigwedge\!\!\!\bigwedge_{l \neq k} e'_{k,l}$). On prend alors $x' := \sup\{e'_k \;/\; k \in \mathcal{I}(L) \text{ et } x \in F_k\}$, et il vient :

- $\mathcal{I}(L(x)) = \{k \in \mathcal{I}(L) \;/\; x \in \mathfrak{m}_k\} = \{k \in \mathcal{I}(L') \;/\; x' \in \mathfrak{m}_k\} = \mathcal{I}(L'(x'))$ d'où $L(x) \,\mathcal{R}\, L'(x'))$;
- $\mathcal{I}(L(x^\dagger)) = \mathcal{I}(L) \setminus \mathcal{I}(L(x)) = \mathcal{I}(L') \setminus \mathcal{I}(L'(x')) = I(L'(x'^\dagger))$ d'où $L(x^\dagger) \,\mathcal{R}\, L'(x'^\dagger)$.

La proposition 5 nous donne alors des suites $x := (x_n)_{n\in\mathbb{N}^*}$ et $x' = (x'_n)_{n\in\mathbb{N}^*}$ énumérant tous les éléments de L et L' respectivement, vérifiant :

$$\forall n \in \mathbb{N},\ \forall I \subseteq [\![1,n]\!], \quad L_I(x_1, \ldots, x_n) \,\mathcal{R}\, L'_I(x'_1, \ldots, x'_n)$$

et telles que l'application $\varphi : x_k \longmapsto x'_k$ soit un isomorphisme de L sur L'. Mais alors pour tout $n \in \mathbb{N}^*$ et tout $k \in [\![1,p]\!]$ on a, en prenant $I := \{i \in [\![1,n-1]\!] \;/\; x_i \in F_k\} \cup \{n\}$:

$$x_n \in F_k \iff F_k \in \mathcal{P}_I(x_1, \ldots, x_n) \iff k \in \mathcal{I}(L_I(x_1, \ldots, x_n))$$

et de même pour x'_n. Comme par construction $L_I(x_1, \ldots, x_n) \;\mathcal{R}\; L_I(x'_1, \ldots, x'_n)$, et que cela implique que $\mathcal{I}(L_I(x_1, \ldots, x_n)) = \mathcal{I}(L'_I(x'_1, \ldots, x'_n))$, on en déduit que $x_n \in F_k \iff x'_n = \varphi(x_n) \in F'_k$. Par récurrence sur n on a donc :

$$\forall x \in L, \quad x \in F_k \iff \varphi(x) \in F'_k$$

On voit que φ respecte les ultrafiltres, c'est donc un isomorphisme de $(L, F_1, \ldots, F_p)$ sur $(L', F'_1, \ldots, F'_p)$.

Enfin deux modèles dénombrables de T sont en relation par $\mathcal{R}$, donc sont isomorphes, *i.e.* T est $\aleph_0$-catégorique, et *a fortiori* complète.

(c) La démonstration de la modèle-complétude de T est presque identique : on prend deux modèles $L \subseteq L'$ de T (les ultrafiltres sont sous-entendus pour alléger l'écriture), et ψ une formule à r variables libres sans quanteurs, à paramètres $x := (x_1, \ldots, x_q)$ dans L, satisfaite dans L' par $y := (y'_1, \ldots, y'_r)$.

Quitte à remplacer L par une sous-structure élémentaire dénombrable L_0 contenant $x_1, \ldots, x_q$, et L' par une sous-structure élémentaire dénombrable L'_0 de L' contenant $L_0 \cup \{y'_1, \ldots, y'_r\}$, on peut supposer L et L' dénombrables. Comme pour tout $k \in [\![1, p]\!]$, on a $F_k = F'_k \cap L$, il vient, en notant $x := (x_1, \ldots, x_q)$:

$$\forall n \leq q,\ \forall I \subseteq [\![1, n]\!], \quad L_I(x_1, \ldots, x_q)\ \mathcal{R}\ L'_I(x_1, \ldots, x_q).$$

La proposition 5 donne alors un isomorphisme $f : L \longrightarrow L'$ dont la restriction à x soit l'identité. Posons $y := f^{-1}(y') \in L^r$; l'argument du (b) vaut pour montrer que cet isomorphisme respecte les ultrafiltres, et on a donc : $(L, F_1, \ldots, F_p) \models \psi(y)$. Le plongement de L dans L' est donc $\exists$-clos, et T est bien modèle-complète.

■

Corollaire 8

Soit Σ la classe des structures (L, F) telles que :

(i) *L est une quasi-algèbre de Boole propre ;*

(ii) *L est dense, et $\mathbf{0}_L \neq \mathbf{1}_L$;*

(iii) *il existe $\alpha \in L \setminus \{\mathbf{1}_L, \mathbf{0}_L\}$ tel que $F = L \setminus \cup P(\alpha)$.*

Alors Σ est élémentaire, et sa théorie est complète et modèle-complète.

Preuve:

(a) L'axiomatisation de (i) et (ii) a été vue pour le corollaire 7. La formule suivante axiomatise (iii) :

$$\exists \alpha \forall \beta\ (F(\beta) \iff \alpha \leq \beta)$$

On note T la théorie de Σ.

(b) Soit Γ la classe des treillis distributifs avec extrémités finis ou dénombrables (L, F) munis d'un prédicat unaire, tels que :

(i) L est une quasi-algèbre de Boole ;

(ii) L est dense ;

(iii) il existe $\alpha \in L$ tel que $F = L \setminus \cup P(\alpha)$ (on peut vérifier qu'un tel α est unique, on le notera α_F).

Comme dans le corollaire 7, il est facile de vérifier que si $(L, F) \in \Gamma$, alors pour tout $e \in L$, $(L(e), F \cap L(e))$ et $(L(e^\dagger), F \cap L(e^\dagger))$ appartiennent aussi à Γ, et que la relation $\mathcal{R}$ définie sur Γ par $(L, F)\ \mathcal{R}\ (L', F')$ si et seulement si :

- L est propre $\iff$ L' est propre ;
- $|L| = |L'|$;
- $\alpha_F = \mathbf{1}_L \iff \alpha_{F'} = \mathbf{1}_{L'}$;
- $\alpha_F = \mathbf{0}_L \iff \alpha_{F'} = \mathbf{0}_{L'}$;

est une relation de Vaught. Si (L, F) et (L', F') sont des modèles dénombrables de T on a clairement $[(L(\alpha_F), F \cap L(\alpha_F))\ \mathcal{R}\ (L'(\alpha_{F'}), F' \cap L'(\alpha_{F'})]$, et $[L(\alpha_F^\dagger), F \cap L(\alpha_F^\dagger)]\ \mathcal{R}$ $[L'(\alpha_{F'}^\dagger), F' \cap L'(\alpha_{F'}^\dagger)]$, d'où un isomorphisme φ de L dans L' qui envoie α_F sur $\alpha_{F'}$, *i.e.* respecte les filtres. T est $\aleph_0$-catégorique, donc complète.

(c) Soient $(L, F) \subseteq (L', F')$; comme $F = F' \cap L$ on a $\alpha_F = \alpha_{F'}$ (le lecteur me fera grâce des détails). La théorie des algèbres de Boole propres et denses étant modèle-complète il s'ensuit que $L \preceq L'$, et même que $(L, \alpha_F) \preceq (L', \alpha_{F'})$ (au sens du langage des treillis avec extrémités enrichi d'un nouveau symbole de constante interprété par α_F). Or les filtres de L et L' sont interprétables dans ce nouveau langage :

$$(L, F) \models \forall e,\ (F(e) \leftrightarrow \alpha \leq e)$$

et de même pour F', donc $(L, F) \preceq (L', F')$ et T est bien modèle-complète.

■

Bibliographie

[CDM] G. Cherlin, L. van den Dries, A. Macintyre, *The elementary theory of regularly closed fields*, preprint 1982.

[C-D 80] G. Cherlin, M. A. Dickmann, *Anneaux réels clos et anneaux de fonctions continues*, C. R. Acad. Sc. Paris **290** (1980) 1-4.

[C-D 83] G. Cherlin, M. A. Dickmann, *Real closed rings II. Model theory*, Annals of pure and applied logic **25** (1983) 213-231.

[De] F. Delon, *Quelques propriétés des corps valués en théorie des modèles*, Thèse de doctorat d'état, Université de Paris VII.

[VdD 88] L. van den Dries, *Elimination theory for the ring of all algebraic integers*, J. reine angew. Math. **388** (1988) 181-194.

[VdD 89] L. van den Dries, *Dimension of definable sets, algebraic boundedness and henselian fields*, Annals of pure and applied logic **45** (1989) 189-209.

[VdD-M] L. van den Dries, A. Macintyre, *The logic of Rumely's local-global principle*, J. reine angew. Math. **407** (1990) 33-56.

[E 82] Y. L. Ershov, *Totally real field extensions*, Soviet. Math. Dokl. **25** (1982) 477-479.

[E 84] Y. L. Ershov, *Two theorems on regularly r-closed fields*, J. reine angew. Math. **347** (1984) 154-167.

[E 91] Y. L. Ershov, *Characterisation of Kochen rings of PC_M-fields*, Soviet. Math. Dokl. **43** (1991) 26-29.

[E 92a] Y. L. Ershov, *Boolean families of valuation rings*, Algebra and Logic **31** (1992) 170-181.

[E 92b] Y. L. Ershov, *Relative regular closeness and π-valuations*, Algebra and Logic **31** (1992) 342-360.

[E 94a] Y. L. Ershov, *Relatively regularly closed fields*, Russian Acad. Sci. Dokl. Math. **48** (1994) 300-303.

[E 94b] Y. L. Ershov, *RC^*-Fields*, Algebra and Logic **33** (1994) 205-215.

[E 94c] Y.L.Ershov, *Fields with continuous local elementary properties. I*, Algebra and Logic **33** (1994) 342-360.

[End] O.Endler, *Valuation theory*, Springer 1972.

[FHV] M.D.Fried, D.Haran, H.Völklein, *Real hilbertianity and the field of totally real numbers*, Contemporary Mathematics **74** (1994) 1-34.

[F-J] M.D.Fried, M.Jarden, *Field arithmetic*, Ergebnisse der Mathematik.

[Gil] R.Gilmer, *Multiplicative ideal theory*, Dekker inc. publishers.

[H-P 84] B.Heinemann A.Prestel, *fields regularly closed with respect to finitely many valuations and orderings*, Quadratic and hermitian forms, Hamilton, Canadian Mathematical Society Conference Proceedings, Vol 4, 1984.

[K 95] J. Koenigsmann, *From p-rigid elements to valuations*, J. reine angew. Math. **465** (1995) 165-182.

[Kü 89] U.M.Künzi, *Decidable theories of pseudo p-adic closed fields*, Algebra and Logic **28** (1989) 421-438.

[Lan] S.Lang, *Number Theory* III, Encyclopedia of Mathematical Sciences, Vol 60, Springer-Verlag.

[Mal] M.-P.Malliavin, *Algèbre commutative*, Masson.

[MB 89] L.Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Ann. scien. Ec. Norm. Sup. (4) **22** (1989) 181-194.

[Mo] J.D.Monk, *Mathematical logic*, Graduate Texts in Mathematics, Berlin-Heidelberg-New York, Springer-Verlag.

[Pop] F.Pop, *Fields of totally Σ-adic numbers*, Preprint 1992.

[P-R] A.Prestel, P.Roquette, *Formally p-adic fields*, LNM **1050** Berlin-Heidelberg-New York-Tokyo 1984.

[Pr 81] A.Prestel, *Pseudo real closed fields, Set theory and model theory*, LNM **872** Berlin-Heidelberg-New York 1981, 127-156.

[P-S 90] A.Prestel, J.Schmid, *Existentially closed domains with radical relations, An axiomatisation of the ring of algebraic integers*, J. reine angew. Math. **407** (1990) 178-201.

[P-S 91] A.Prestel, J.Schmid, *Decidability of the rings of real algebraic and p-adic algebraic integers*, J. reine angew. Math. **414** (1991) 141-148.

[P-Z] A.Prestel, M.Ziegler, *Model theoretic methods in the theory of topological fields*, J. reine angew. Math. **299/300** (1978) 318-341.

[Rob 65] J.Robinson, *The decision problem for fields*, Symposium on the Theory of Models, North-Holland 1965

[Ru 86] Rumely, *Arithmetic over the ring of all algebraic integers*, J. reine angew. Math. **368** (1986) 127-133.

Résumé

Les principes locaux-globaux (LGP) du type du principe de Hasse non singulier ont une longue histoire en théorie des modèles appliquée à l'algèbre (corps pseudo algébriquement clos (PAC), pseudo réel clos (PRC), pseudo p-adiquement clos et leurs généralisations à un ensemble fini M d'entiers premiers (PC_M)...*etc.*). Nous commençons par dégager et étudier un principe local-global assez général pour englober non seulement ces LGP de corps mais aussi d'autres approches plus récentes sur les anneaux intègres, et en même temps assez raisonnable pour rester axiomatisable au premier ordre dans le langage des anneaux.

Après avoir caractérisé les principales propriétés modèle-théoriques des anneaux PAC, PRC ou PC_M (généralisation immédiate des notions homonymes sur les corps), nous obtenons ainsi des conditions nécessaires et suffisantes de décidabilité sur divers anneaux "naturels". Nous montrons notamment que la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}_p$ ou dans le corps de nombres algébriques absolument p-adiques est décidable. De même la clôture intégrale de $\mathbb{F}_p[T]$ dans tout corps séparablement clos est décidable.

Une contribution à l'algèbre est également fournie, lorsque nous étudions les familles de polynômes en $n+1$ indéterminées possédant un zéro commun entier sur $\mathbb{Z}$ pour toute valeur entiere sur $\mathbb{Z}$ des n premiers paramètres : nous montrons qu'alors il existe un polynôme unitaire en la dernière indéterminée qui divise simultanément tous ces polynômes.

Mots-clés : logique, principe de Hasse, pseudo algébriquement clos, pseudo réel clos, pseudo p-adiquement clos, décidabilité, modèle-complétude.