THÈSE

présentée à

l'UFR des Sciences & Techniques de l'Université de Franche-Comté,

pour obtenir le

Grade de docteur de l'Université de Franche-Comté,
en Mathématiques & Applications.

Aspects constructifs de la théorie des corps valués

(précédée d'un chapitre sur la noetherianité constructive)

par

Hervé Perdry

Soutenue le 18 décembre 2001 devant la commission d'examen :

Directeur de thèse :	H. Lombardi	Maître de Conférences à l'Université de Franche-Comté
Présidente du jury :	F. Delon	Directrice de Recherche au CNRS (Paris 7)
Examinateurs :	V. Fleckinger	Professeur à l'Université de Franche-Comté
	A. Galligo	Professeur à l'Université de Nice Sophia-Antipolis
	G. Gras	Professeur à l'Université de France-Comté
	C. Quitté	Maître de Conférences à l'Université de Poitiers
Rapporteurs :	F.-V. Kuhlmann	Associate Professor, University of Saskatchewan
	F. Richman	Professor, Florida Atlantic University

MERCI

Rien n'est jamais perdu
tant qu'il reste quelque chose à trouver.
Pierre DAC.

Henri Lombardi, familièrement appelé «le boss» ou «chef», a accepté d'encadrer cette thèse ; on ne peut pas vraiment remercier quelqu'un qui vous a apporté autant, car les remerciements ne seront jamais suffisants. Je me contenterai donc de lui cirer un peu les pompes, une fois n'est pas coutume, en rendant grâce à son humeur égale, sa curiosité et son enthousiasme communicatifs, sa disponibilité et sa culture nonpareilles.

Je ne sais pas si l'argent est le nerf de quoi que ce soit, mais il est bien commode d'en avoir à dépenser de temps à autre : George Gras et Marie-Françoise Roy ont appuyé ma demande d'allocation de recherche alors que les vaches se faisaient maigres, merci à eux.

Franz-Viktor Kuhlmann ne m'a pas seulement fait l'honneur de lire très attentivement cette thèse, il m'a également invité à deux reprises à Saskatoon (dans le Saskatchewan !) : je le remercie pour sa gentillesse et son hospitalité — mes pensées vont aussi à Salma et à Murray.

J'ai également été très honoré par la lecture de Fred Richman, avec qui il fut passionant de débattre le temps de quelques e-mails. Françoise Delon, qui présidait le jury de thèse, et André Galligo ont montré leur intérêt pour mon travail, j'en ai été fort flatté ; George Gras (encore lui) a accepté de faire partie de ce jury, ainsi que Vincent Fleckinger (avec qui il a toujours été agréable de parler un peu boutique), ils ont toute ma gratitude. Claude Quitté mérite une mention spéciale : il a été et il sera très agréable de travailler en sa compagnie, à Luminy ou ailleurs, et sa pugnacité face aux problèmes mathématiques est un exemple stimulant.

La vie au sein du labo est rendue plus douce par Catherine — mais aussi par Catherine (ne m'en veux pas de t'avoir fait passer après l'autre !), qui s'acquittent de leurs tâches administratives avec le sourire et une efficacité sans reproche. Jacques Vernerey est le pape de la photocopieuse, que son nom soit béni ! Nathalie & Odile sont de joyeuses bibliothécaires, que les Saints Springer et Verlag veillent sur elles.

De nombreux co-bureaux successifs ont enduré mes excentricités sans broncher outre mesure, je ne peux que leur en rendre grâce. C'est le moment des amis, la coutume veut qu'on énumère quelques noms ; j'assure ici de mon indéfectible affection Eva, Jean-Yves, Caroline, Édouard, Stéphane, Jean-Nicolas, Flo, Maria.

Enfin, comme tout bon candidat de jeu télé, je salue mon papa et ma maman, que je ne pourrai jamais remercier assez de tout ce qu'ils m'ont apporté (et je promets de faire attention aux dinosaures).

SOMMAIRE

Introduction

Ce mémoire traite de mathématiques *constructives*; il pourrait être intéressant de tenter de définir ce terme. Cela pourrait nous entrainer dans une digression historique où faire preuve d'exactitude serait difficile (il est facile d'attribuer à Brouwer ou à Markov ses propres idées), et dont nous ne sortirions pas nécessairement plus amplement informés; cela pourrait aussi nous amener à définir un cadre logique strict, sans doute rebutant, et pas en rapport plus étroit avec la pratique des mathématiques constructives (du moins telle qu'elle est conçue dans ce mémoire) que la théorie des ensembles **ZF** ne l'est avec la pratique des mathématiques dites classiques. Je pense que les mathématiques constructives, comme les mathématiques classiques, sont avant tout une pratique, difficile à définir autrement qu'en l'illustrant. Nous nous contenterons donc de rappeler la formule connue, suivant laquelle « il existe » signifiera pour nous « on sait construire ».

Le premier chapitre est consacré à la noethérianité. Il n'est pas relié au reste du mémoire. Mon travail a été principalement orienté vers les corps valués, mais la noethérianité me semble un des points de l'algèbre classique les plus intéressants du point de vue constructif, et j'y ai consacré une part importante de mon temps. Du point de vue constructif, la définition classique de la noethérianité n'est (comme nous le verrons) vérifiée par aucun anneau $\mathbb{A}$ (et c'est bien dommage, car la preuve classique du transfert de la noethérianité de $\mathbb{A}$ à $\mathbb{A}[\mathrm{X}]$ est constructive !) Il convient donc de donner une autre définition de la noethérianité, équivalente à la définition classique, qui soit vérifiée constructivement par les anneaux noethériens usuels et qui passe (du point de vue constructif) de $\mathbb{A}$ à $\mathbb{A}[\mathrm{X}]$ (c'est le théorème de Hilbert).

Ceci peut être fait de plusieurs façons différentes; en effet, des résultats équivalents du point de vue classique peuvent ne pas l'être du point de vue constructif (c'est, pour la noethérianité, ce qui fait la richesse du sujet). Abraham Seidenberg et Fred Richman ont fourni en 1974 deux versions très proches de la noethérianité, ainsi qu'une preuve du théorème de Hilbert; une autre définition (plus forte, du point de vue constructif) a été proposée en 1991 par Carl Jacobson et Clas Löfwall (ainsi qu'une preuve du théorème de transfert).

Henri Lombardi et moi-même avons proposé en 1998 une preuve constructive directe de la noethérianité de $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, au sens de la définition de Richman. Cette preuve est à nouveau présentée ici. Je propose ensuite une autre définition de la noethérianité, (la *noethérianité forte*), plus forte (du point de vue constructif) que les autres définitions évoquées jusque là. J'en donne une preuve directe pour $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ (dans l'esprit de la preuve Lombardi/Perdry donnée en 1998) ; je prouve également constructivement que cette propriété passe de $\mathbb{A}$ à $\mathbb{A}[X]$, en utilisant certains lemmes dûs à Richman. En passant, je redémontre le théorème de transfert de Jacobson et Löfwall. Le chapitre se termine par une étude de la longueur des suites croissantes d'idéaux monomiaux dans $\mathbb{K}[X_1, \ldots, X_n]$.

Le chapitre II présente à la fois les outils de base que nous utilisons pour travailler de façon constructive dans les extensions de corps et quelques grands traits de la théorie classique des corps valués. Les idées de base pour les extensions de corps sont celles de *l'algèbre dynamique* introduite par Michel Coste, Henri Lombardi, et Marie-Françoise Roy, elles-mêmes héritières des évaluations dynamiques de Jean Della Dora, Claire Dicrescenzo et Dominique Duval.

Nous présentons également la transformation de Tschirnhaus et les polygones de Newton, deux outils crées au XVII^e siècle, et qui ont un rôle prépondérant dans notre travail. Nous évoquons aussi le lemme de Hensel et la théorie classique des corps henséliens. À bien des égards, le lemme de Hensel est aux corps valués ce que le théorème des valeurs intermédiaires est aux corps ordonnés : sous certaines conditions, il assure l'existence d'une racine d'un polynôme. Comme le théorème des valeurs intermédiaires, il est vrai dans les corps complets ; et on peut oublier la complétude pour étudier les corps qui vérifient le lemme de Hensel, les *corps henséliens*. La similitude n'est pas totale : la théorie des corps réels clos (c.-à-d. des corps ordonnés vérifiant le théorème des valeurs intermédiaires) admet une élimination des quantificateurs, pas celle des corps henséliens.

Le chapitre III est consacré à l'étude constructive des corps henséliens. Nous commençons par donner une construction (qui suit de près celle donnée par Franz-Viktor Kuhlmann et Henri Lombardi, publiée en 2000) du *hensélisé* d'un corps valué $\mathbb{K}$, c'est-à-dire de la plus petite extension algébrique valuée de $\mathbb{K}$ qui vérifie le lemme de Hensel. Cette extension est unique à unique isomorphisme près, c'est ce qui permet sa construction directe, *grosso modo* comme union d'une tour d'extensions algébriques de $\mathbb{K}$. Nous nous tournons ensuite vers la théorie générale des corps henséliens ; nous démontrons tout d'abord un critère de factorisation de polynômes (qui s'exprime également en termes de polygone de Newton).

Les preuves constructives mises en œuvre jusque là sont sans doute un peu surprenantes pour le mathématicien classique, à qui la théorie de Galois épargne bien des soucis pour arriver aux mêmes résultats. Les preuves qui interviennent ensuite, pour donner divers résultats classiques à propos des corps henséliens, sont particulièrement simples et concises, et intéresseront sans doute (nous l'espérons) même des mathématiciens pour qui l'effectivité n'est pas un souci prépondérant... nous montrons notamment le lemme de Krasner et l'unicité de l'extension de la valuation d'un corps hensélien à une de ses extensions algébriques.

Le chapitre se termine par une construction du corps d'inertie et du corps de ramification d'un corps valué.

Dans le chapitre IV, je donne une preuve (non constructive) d'une variante du lemme de Hensel, suivie d'une preuve constructive de ce résultat. Il s'agit d'étendre une reformulation du lemme de Hensel en terme de *valuation de Gauss* de polynômes à deux classes de valuation de $\mathbb{K}[X]$: les valuations *résiduellement transcendantes*, et *transcendantes relativement aux groupes de valuation*. Ce résultat avait déjà été prouvé dans des cas particuliers (valuation résiduellement transcendante et corps $\mathbb{K}$ complet de valuation discrète), en particulier par Sudesh Kaur Khanduja. J'ai également donné une interprétation « géométrique » de ce résultat (en termes de la géométrie ultramétrique du graphe des racines des polynômes qui interviennent), ainsi qu'une version multidimensionnelle.

J'ai introduit dans ces preuves des transformations simples qui permettent de relier entre elles les valuations résiduellement transcendantes, qui semblent n'avoir pas été remarquées par d'autres auteurs.

Le dernier chapitre porte le numéro V. Il s'agit d'un travail en commun avec Franz-Viktor Kuhlmann et Henri Lombardi. Dans un premier temps, nous donnons un analogue à l'algorithme D5 (évoqué plus haut, à la base des idées de l'algèbre dynamique) dans les corps valués. Cet algorithme permet, étant donné un polynôme P de degré n à coefficients dans un corps valué $\mathbb{K}$ et des polynômes $q_1, \ldots, q_k \in \mathbb{K}[X]$, de calculer les $k+1$-uplets de valuations $\left[v(\alpha_i), v(q_1(\alpha_i)), \ldots, v(q_k(\alpha_i))\right]$ (pour $i = 1, \ldots, n$) — où $\alpha_1, \ldots, \alpha_n$ sont (dans un ordre arbitraire) les racines de P dans la clôture algébrique de $\mathbb{K}$.

Ceci permet de donner ensuite une procédure de décision pour les problèmes existentiels à une variable (du type $\exists x \Phi(x)$, où $\Phi(x)$ exprime des conditions sur x) dans un corps valué algébriquement clos; cette procédure de décision est suffisament souple pour fournir, si on tente de l'appliquer à un problème où sont présents des paramètres (dans les conditions exprimées par $\Phi(x)$...), une condition équivalente sans quantificateur. Ainsi, on a obtenu un algorithme d'élimination des quantificateurs dans les corps valués algébriquement clos, très différent de celui donné par Volker Weispfenning en 1984. La géométrie ultramétrique du graphe des racines des polynômes qui interviennent dans les conditions joue à nouveau un rôle majeur.

Nous espérons que ce mémoire, malgré un certain nombre de défauts et d'inachèvements, pourra donner une bonne idée de la vision constructive en algèbre, de ses faiblesses comme de ses points forts, et présentera de l'intérêt pour les constructivistes comme pour les mathématiciens classiques.

Chapitre I

Noethérianité constructive

Introduction

La noethérianité est sans doute, parmi les notions classiques en algèbre, celle dont le traitement constructif est le plus délicat — et provoque le plus grand étonnement des mathématiciens classiques. Cela tient sans doute au fait que c'est une notion du *second ordre* :

« Toute suite croissante d'idéaux de $\mathbb{A}$ est ultimement constante. »

La quantification se fait sur l'ensemble des suites d'idéaux de $\mathbb{A}$, et non sur des éléments de $\mathbb{A}$. Il est impossible de se ramener à un énoncé équivalent du premier ordre. L'énoncé plus raisonnable

« Toute suite croissante d'idéaux de type fini de $\mathbb{A}$ est ultimement constante. »

n'est pas plus facile à manipuler : « ultimement constante » pose des problèmes insurmontables. L'expérience prouve que les énoncés du second ordre sont les plus difficiles à manier en mathématiques constructives ; cependant ils sont rares en algèbre. Ainsi Henri Lombardi et Thierry Coquand ont récemment traité la dimension de Krull par des schémas d'énoncés du premier ordre (cf [Lom, CoqLom_1, CoqLom_2]). La noethérianité, elle, est réellement et profondément une notion du second ordre.

C'est en examinant les exigences des mathématiques constructives sur la noethérianité qu'on prend conscience qu'il ne s'agit pas simplement de fournir des algorithmes ; encore faut-il que leur preuve de terminaison soit constructive. Il s'agit là d'une exigence qui touche à l'épistémologie, et qui est difficile à définir autrement que par la pratique.

Espérons que l'exposé qui va suivre illustrera l'objet de cette exigence.

1 Ensembles ordonnés & anneaux noethériens

1.1 Définitions, exemples

Une relation binaire $\leq$ sur un ensemble E est un *ordre* si elle est transitive, réflexive, et antisymétrique. Si pour tous $a, b \in \mathrm{E}$, on a $a \leq b$ ou $b \leq a$ l'ordre est dit *total;* dans le cas contraire il est dit *partiel.* La relation d'ordre strict associée est définie par $a < b$ ssi $a \leq b$ et $a \neq b$ (nous supposons que l'égalité est décidable dans E ; de façon générale, exception faite des exemples, nous ne traitons que le cas des ensembles où l'égalité est décidable).

Exemples – L'ordre usuel de $\mathbb{N}$ est un ordre total ;

- la relation de divisibilité dans $\mathbb{N}$: $a|\ b$ ssi $\exists c\ :\ b = ac$. Il s'agit d'un ordre partiel ;
- soit X un ensemble quelconque. La relation d'inclusion $\subseteq$ est un ordre partiel sur $\mathrm{E} = \mathcal{P}(\mathrm{X})$, l'ensemble des parties de X ;
- soit $\mathbb{A}$ un anneau. La relation d'inclusion est un ordre partiel sur $\mathcal{J}_{\mathbb{A}}$, l'ensemble des idéaux de $\mathbb{A}$;
- si $(\mathrm{E}, \leq_{\mathrm{E}})$ et $(\mathrm{F}, \leq_{\mathrm{F}})$ sont deux ensembles ordonnés, on peut ordonner $\mathrm{E} \times \mathrm{F}$ par *l'ordre produit* :

$$(a, b) \leq_{\mathrm{E}\times\mathrm{F}} (a', b') \iff (a \leq_{\mathrm{E}} a') \wedge (b \leq_{\mathrm{F}} b')$$

  C'est un ordre partiel sauf dans des cas triviaux. L'ordre produit sur le produit d'un nombre quelconque d'ensembles ordonnés se définit par récurrence sur le nombre d'ensembles, de manière évidente. L'ordre produit sur E^d sera noté $\leq_d$;
- si $(\mathrm{E}, \leq_{\mathrm{E}})$ et $(\mathrm{F}, \leq_{\mathrm{F}})$ sont deux ensembles ordonnés, on peut ordonner $\mathrm{E} \times \mathrm{F}$ par *l'ordre lexicographique* :

$$(a, b) \leq_{\mathrm{lex}} (a', b') \iff \begin{cases} a <_{\mathrm{E}} a' \\ \text{ou} \\ a = a' \wedge b \leq_{\mathrm{F}} b' \end{cases}$$

  Si E et F sont totalement ordonnés, il s'agit d'un ordre total. L'ordre lexicographique sur un produit d'un nombre quelconque d'ensemble ordonnés se définit à nouveau par récurrence sur le nombre d'ensembles, de manière évidente ;
- soit $\mathrm{E} = \mathbb{N}^d$. On a déjà donné deux ordres sur E, l'ordre produit $\leq_d$ et l'ordre lexicographique $\leq_{\mathrm{lex}}$. *L'ordre lexicographique gradué* en est un troisième, défini comme suit :

$$(a_1, \ldots, a_d) \leq_{\mathrm{deglex}} (b_1, \ldots, b_d)$$
$$\iff$$
$$\begin{cases} a_1 + \cdots + a_d < b_1 + \cdots + b_d \\ \text{ou} \\ a_1 + \cdots + a_d = b_1 + \cdots + b_d \wedge (a_1, \ldots, a_d) \leq_{\mathrm{lex}} (b_1, \ldots, b_d) . \end{cases}$$

Remarques – On sera amené à privilégier les ordres décidables, c.-à-d. ceux pour lesquels un algorithme prenant en entrée deux éléments a, b décide en un temps fini si $a \leq b$ ou non. Cette condition sera souvent implicite. Parmi les exemples qui précèdent, on remarquera par exemple que l'inclusion sur $\mathcal{P}(\mathrm{X})$ n'est pas décidable quand X n'est pas un ensemble fini (on identifie ici $\mathcal{P}(\mathrm{X})$ à $\mathbf{2}^{\mathrm{X}}$, l'ensemble des fonctions caractéristiques de X ; du point de vue des mathématiques classiques cette identification est naturelle, par contre du point de constructif, $\mathbf{2}^{\mathrm{X}}$ est un ensemble beaucoup plus simple que $\mathcal{P}(\mathrm{X})$) ;

– si $(\mathrm{E}, \leq)$ est un ensemble ordonné, on notera $(\mathrm{E}, \geq)$ l'ensemble ordonné par $x \geq y \iff y \leq x$. On utilisera souvent cette notation pour raccourcir les énoncés.

Définitions Une *application croissante* entre $(\mathrm{E}, \leq)$ et $(\mathrm{F}, \preceq)$ est une application $\phi\ : \mathrm{E} \longrightarrow \mathrm{F}$ telle que $a \leq b \Longrightarrow \phi(a) \preceq \phi(b)$. Un *isomorphisme d'ordre* est une application croissante bijective, dont l'inverse est également une application croissante.

Une autre notion importante est celle d'*application strictement croissante* : il s'agit d'une application $\phi : \mathrm{E} \longrightarrow \mathrm{F}$ telle que $a < b \Longrightarrow \phi(a) \prec \phi(b)$. Les isomorphismes d'ordre sont des applications strictement croissantes. Une *application strictement décroissante* $\phi : \mathrm{E} \longrightarrow \mathrm{F}$ vérifie $a < b \Longrightarrow \phi(a) \succ \phi(b)$

Exemples (Les preuves sont laissées à la lectrice et au lecteur, ainsi que la critique de leur caractère constructif ou non.)

– L'application constante de $(\mathrm{E}, \leq)$ vers $\{0\}$ est croissante ;
– il existe un isomorphisme d'ordre entre $(\mathbb{N}, \leq)$ et $(\mathbb{N}^d, \leq_{\text{deglex}})$;
– il en existe un entre $(\mathcal{J}_{\mathbb{Z}}, \supseteq)$ et $(\mathbb{N}, |)$;
– l'identité est strictement croissante de $(\mathbb{N}^\star, |)$ vers $(\mathbb{N}^\star, \leq)$; ce n'est pas un isomorphisme ;
– la même chose a lieu pour l'identité $\mathrm{Id}\ : (\mathbb{N}^d, \leq_d) \longrightarrow (\mathbb{N}^d, \leq_{\text{lex}})$ et pour $\mathrm{Id}\ : (\mathbb{N}^d, \leq_d) \longrightarrow (\mathbb{N}^d, \leq_{\text{deglex}})$;
– soit $\mathbb{K}$ un corps. Il existe une application strictement décroissante de $(\mathcal{J}_{\mathbb{K}[\mathrm{X}]}, \subseteq)$ vers $(\mathbb{N} \cup \{+\infty\}, \leq)$.

Notez bien dans les exemples ci-dessus la différence entre $(\mathcal{J}_{\mathbb{A}}, \subseteq)$ et $(\mathcal{J}_{\mathbb{A}}, \supseteq)$. L'élément $+\infty$ qu'on ajoute à $\mathbb{N}$ dans les deux exemples faisant intervenir des ensembles d'idéaux s'explique par le fait que nous considérons le singleton $\{0\}$ comme un idéal ; l'image de $\{0\}$ par notre application strictement croissante sera $+\infty$.

1.2 Ordres noethériens, artiniens, & Cie

Un ensemble ordonné $(\mathrm{E}, \leq)$ est *noethérien* (resp. *artinien*) si il satisfait à la condition de chaîne ascendante **CCA**(resp. descendante **CCD**) :

CCA : Toute suite $(a_i)_{i \in \mathbb{N}}$ de E croissante pause, c.-à-d. il existe n tel que $a_n = a_{n+1}$.

CCD : Toute suite de E décroissante pause.

Remarquons que $(E, \leq)$ est noethérien ssi $(E, \geq)$ est artinien.

Les conditions utilisées de façon classique sont en fait les suivantes (*cf.* [Wae, II, Chap. XII]) :

CCA' : Toute suite $(a_i)_{i \in \mathbb{N}}$ de E croissante est ultimement constante, c.-à-d. il existe n tel que $a_n = a_{n+1} = a_{n+2} = \dots$

CCD' : Toute suite de E décroissante est ultimement constante.

Via le tiers-exclus, les conditions **CCA** et **CCA'** sont équivalentes : il est facile de voir que toutes deux signifient qu'il n'y a pas de suite infinie strictement croissante dans E. De même, on a **CCD** $\Longleftrightarrow$ **CCD'**.

Pourquoi alors préférer les deux premières conditions ? c'est que cette preuve d'équivalence n'est pas constructive. La condition **CCA** (resp. **CCD**) est plus faible que **CCA'** (resp. **CCD'**), de notre point de vue. La vision constructive rejoint ici le premier mouvement de l'intuition, pour qui **CCA'** est bien une condition plus forte que **CCA**. L'utilisation des conditions **CCA** et **CCD** est due, semble-t-il, à Seidenberg (*cf.* [S_1]).

Il se trouve que du point de vue constructif **CCD'** n'est pas vraie dans $(\mathbb{N}, \leq)$: étant donné une suite décroissante d'entiers on ne sait pas donner sa limite *a priori*. En effet, même si on trouve dans une suite décroissante un grand nombre de termes consécutifs égaux, on ne sait pas si il n'y en a pas d'autres plus petits qui apparaissent plus loin.

Plus précisément si Pr_{sde} est l'ensemble des procédures primitives récursives $u : n \mapsto u_n$ qui produisent des suites décroissantes d'entiers, il n'existe pas de procédure récursive $\Phi : \mathrm{Pr}_{sde} \longrightarrow \mathbb{N}$ qui calcule la limite $\Phi(u)$ de la suite $(u_n)_{n \in \mathbb{N}}$. Si une telle procédure existait, elle pourrait être utilisée pour résoudre récursivement le problème de la halte, ce qui est impossible (pour ces notions, voir Cori & Lascar, [CorLas, Chap. 5]).

Pour illustrer ce propos, voici un exercice intéressant (et difficile) :

Exercice Soit la suite $(u_n)_{n \in \mathbb{N}}$ définie par $u_0 = 1$, et

$$u_{n+1} = \begin{cases} u_n & \begin{array}{l} \text{si } 2n+1 \text{ n'est pas parfait} \\ \text{(c.-à-d. somme de ses diviseurs stricts)} ; \end{array} \\ 0 & \text{sinon.} \end{cases}$$

Calculer la limite de cette suite.

Il ne s'agit pas d'insinuer que cet exercice n'a pas de solution, mais simplement qu'il n'y pas de méthode générale pour résoudre ce type d'exercice. Signalons qu'une conjecture connue de théorie des nombres suppose que la limite de la suite ci-dessus est 1.

Par contre, avec notre définition, on a les résultats suivants :

Lemme 1 $(\mathbb{N}, \leq)$ *est artinien.*

Démonstration Soit $(u_i)_{i\in\mathbb{N}}$ une suite décroissante de $\mathbb{N}$. Soit $n = u_0$. Alors si $u_n = 0$, on a $u_{n+1} = u_n = 0$; et si $u_n > 0$, alors il existe $k < n$ tel que $u_k = u_{k+1}$. □

Lemme 2 *Un produit fini d'ensembles noethériens (resp. artiniens), ordonné par l'ordre produit, est noethérien (resp. artinien).*

Démonstration Nous faisons la preuve dans le cas du produit de deux ensembles noethériens E et F. Le cas général s'en déduit par récurrence.

Soit $(u_n, v_n)_{n\in\mathbb{N}}$ une suite croissante de $\mathrm{E} \times \mathrm{F}$; montrons que cette suite pause. La suite $(u_n)_{n\in\mathbb{N}}$ est croissante dans E qui est noethérien, donc il existe $n_1 < n_2 < \cdots$ tels que, pour tout i, $u_{n_i} = u_{n_i+1}$. La suite $(v_{n_i})_{i\in\mathbb{N}}$ est croissante dans F, ensemble noethérien ; il existe donc i tel que $v_{n_i} = v_{n_{i+1}}$. Mais $v_{n_i} \leq v_{n_i+1} \leq v_{n_{i+1}}$, et donc $v_{n_i} = v_{n_i+1}$. On a $(u_{n_i}, v_{n_i}) = (u_{n_i+1}, v_{n_i+1})$. □

Corollaire 3 $(\mathbb{N}^d, \leq_d)$ *est artinien.*

1.3 Anneaux

Définition Un anneau $\mathbb{A}$ est dit *noethérien* si $(\mathcal{I}_\mathbb{A}, \subseteq)$ est noethérien, où $\mathcal{I}_\mathbb{A}$ **désigne l'ensemble des idéaux de $\mathbb{A}$ *de type fini***, par opposition à $\mathcal{J}_\mathbb{A}$ qui était l'ensemble de tous les idéaux. La raison de cette restriction apparaît dans la preuve du lemme suivant :

Lemme 4 *Soit $\mathbb{K}$ un corps. L'anneau $\mathbb{K}[\mathrm{X}]$ est noethérien.*

Démonstration Rappelons tout d'abord que les idéaux de $\mathbb{K}[\mathrm{X}]$ sont principaux. En mathématiques classiques ceci est vrai pour tout idéal, en mathématiques constructives cela n'est vrai que pour les idéaux de type fini, d'où la nécessité de se restreindre à ceux-ci.

C'est l'algorithme d'Euclide, utilisant la division des polynômes, qui permet d'associer à $f_1, \ldots, f_n \in \mathbb{K}[\mathrm{X}]$ un unique polynôme unitaire $g \in \mathbb{K}[\mathrm{X}]$ tel que $f_1 \cdot \mathbb{K}[\mathrm{X}] + \cdots + f_n \cdot \mathbb{K}[\mathrm{X}] = g \cdot \mathbb{K}[\mathrm{X}]$.

Notons $\deg_\mathrm{X} g = \Phi(f_1, \ldots, f_n)$. Il est facile de vérifier que si

$$f_1 \cdot \mathbb{K}[\mathrm{X}] + \cdots + f_n \cdot \mathbb{K}[\mathrm{X}] = g_1 \cdot \mathbb{K}[\mathrm{X}] + \cdots + g_m \cdot \mathbb{K}[\mathrm{X}],$$

alors $\Phi(f_1, \ldots, f_n) = \Phi(g_1, \ldots, g_m)$. L'application Φ va de $\mathcal{I}_{\mathbb{K}[\mathrm{X}]}$ vers $\mathbb{N} \cup \{+\infty\}$; on pose $\Phi(\{0\}) = +\infty$. C'est une application strictement décroissante de $(\mathcal{I}_{\mathbb{K}[\mathrm{X}]}, \supseteq)$ vers $(\mathbb{N} \cup \{+\infty\}, \leq)$.

Il est clair que $\mathbb{N}$ artinien entraîne $\mathbb{N} \cup \{+\infty\}$ artinien. Le lemme suivant (que nous isolons pour souligner son caractère général) affirme qu'alors $(\mathcal{I}_{\mathbb{K}[\mathrm{X}]}, \supseteq)$ est artinien. Donc $(\mathcal{I}_{\mathbb{K}[\mathrm{X}]}, \subseteq)$ est noethérien, et l'anneau $\mathbb{K}[\mathrm{X}]$ est noethérien. □

Lemme 5 *Soit* $\Phi\ : (\mathrm{E}, \leq) \longrightarrow (\mathrm{F}, \preceq)$ *une application strictement croissante. Si* $(\mathrm{F}, \preceq)$ *est noethérien (resp. artinien), alors* $(\mathrm{E}, \leq)$ *est noethérien (resp. artinien).*

Démonstration Un cas suffira : supposons que $(\mathrm{F}, \preceq)$ est noethérien. Soit $(u_i)_{i\in\mathbb{N}}$ une suite croissante de E. Alors $u_i \le u_{i+1} \Longrightarrow \Phi(u_i) \preceq \Phi(u_{i+1})$: la suite $(\Phi(u_i))$ est croissante. Or F est noethérien, donc il existe n tel que $\Phi(u_n) = \Phi(u_{n+1})$. On conclut en utilisant que si Φ est une application strictement croissante, on a :

$$(a \le b \wedge \Phi(a) = \Phi(b)) \Longrightarrow a = b\,.$$

□

Lemme 6 *L'anneau $\mathbb{Z}$ est noethérien.*

Démonstration On utilise l'isomorphisme d'ordre entre $(\mathcal{I}_{\mathbb{Z}}, \supseteq)$ et $(\mathbb{N}, |)$, puis l'application strictement croissante de $(\mathbb{N}^\star, |)$ vers $(\mathbb{N}^\star, \le)$, pour donner une application strictement décroissante de $(\mathcal{I}_{\mathbb{Z}}, \subseteq)$ vers $(\mathbb{N} \cup \{+\infty\}, \le)$. On conclut grâce au lemme précédent. □

Malheureusement la preuve utilisée ici pour $\mathbb{K}[\mathrm{X}]$ se généralise mal au cas de $\mathbb{A}[\mathrm{X}]$ (où $\mathbb{A}$ est un anneau), ou de $\mathbb{K}[\mathrm{X}, \mathrm{Y}]$: la division euclidienne des polynômes y manque cruellement.

Diverses approches ont été utilisées pour régler cette question, notament par Abraham Seidenberg (*cf.* [S_1]) et Fred Richman (*cf.* [Ric_1]). On trouvera dans le cours d'algèbre constructive de Mines, Richman et Ruitenburg [MRR, Chap. VIII] le théorème suivant :

Théorème 7 (Richman/Seidenberg) *Si l'anneau $\mathbb{A}$ est cohérent et noethérien, alors $\mathbb{A}[\mathrm{X}]$ est cohérent et noethérien. De plus si $\mathbb{A}$ est fortement discret, alors $\mathbb{A}[\mathrm{X}]$ est fortement discret.*

Définition Un anneau $\mathbb{A}$ est *cohérent* si, pour tout idéal de type fini $\mathrm{I} = f_1 \cdot \mathrm{A} + \cdots + f_n \cdot \mathrm{A}$, le module des syzygies de I, c.-à-d. le noyau de l'application

$$\begin{array}{ccc} \mathbb{A}^n & \longrightarrow & \mathbb{A} \\ (g_1, \ldots, g_n) & \mapsto & f_1 \cdot g_1 + \cdots + f_n \cdot g_n \end{array}$$

est de type fini.

Définition Un anneau $\mathbb{A}$ est *fortement discret* si, pour tout idéal de type fini $\mathrm{I} = f_1 \cdot \mathrm{A} + \cdots + f_n \cdot \mathrm{A}$, on a un test d'appartenance $g \overset{?}{\in} \mathrm{I}$. On dit que les idéaux de type fini de $\mathbb{A}$ sont *détachables*.

Du point de vue des mathématiques classiques tous les anneaux noethériens sont cohérents. En pratique, on s'aperçoit que la cohérence est très importante pour les preuves constructives. Avoir en outre l'hypothèse « fortement discret » est bien sûr bien plus confortable ; s'en passer veut dire se priver de l'instance suivante du tiers-exclus : « $\forall f,\ f \in \mathrm{I} \vee f \notin \mathrm{I}$ ». Il est tout à fait remarquable que les résultats de Richman & Seidenberg sont vrais sans cette hypothèse.

Remarquons que la preuve classique de ce théorème est constructive ; malheureusement l'hypothèse de noethérianité au sens classique du terme n'est satisfaite, du point de vue constructif, par aucun anneau non trivial (c.-à-d. autre que $\{0\}$).

Ce théorème permet en particulier de conclure que $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ est noethérien. Cependant, pour ce cas particulier, d'autres approches permettent d'aboutir. Henri Lombardi et moi-même avons utilisé les bases de Gröbner pour le traiter ([LP]); c'est l'objet de la section suivante. Avant de l'aborder, encore quelques considérations générales sur les ensembles ordonnés.

1.4 Parties initiales et terminales

Définition Soit $(\mathrm{E}, \preceq)$ un ensemble ordonné. Une partie A de E est dite *partie initiale* de E si

$$a \in \mathrm{A}, b \preceq a \Longrightarrow b \in \mathrm{A}\,.$$

A sera dite *partie terminale* de A si $a \in \mathrm{A}, a \preceq b \Longrightarrow b \in \mathrm{A}$.

Soient $a_1, \ldots, a_s \in \mathrm{E}$. La partie initiale engendrée par $a_1, \ldots, a_s$ est

$$\mathrm{A} = \langle a_1, \ldots a_s \rangle_{\mathbf{I}} = \{x \in \mathrm{E} \,:\, x \preceq a_1 \vee \cdots \vee x \preceq a_s\}.$$

Une telle partie initiale sera dite *de type fini*. De façon analogue, $a_1, \ldots, a_s$ engendrent une partie terminale :

$$\mathrm{A} = \langle a_1, \ldots a_s \rangle_{\mathbf{T}} = \{x \in \mathrm{E} \,:\, a_1 \preceq x \vee \cdots \vee a_s \preceq x\}$$

Un telle partie terminale sera également dite de type fini.

L'ensemble des parties initiales (resp. terminales) de type fini de E (y compris $\emptyset$, considéré comme étant engendré par la famille vide) sera noté $\mathbf{I}^\circ(\mathrm{E})$ (resp. $\mathbf{T}^\circ(\mathrm{E})$).

Lemme 8 *Tout* $\mathrm{A} \in \mathbf{T}^\circ(\mathrm{E})$ *est engendré par une unique famille minimale pour l'inclusion ; si* $\mathrm{A}, \mathrm{B} \in \mathbf{T}^\circ(\mathrm{E})$*, on peut décider si* $\mathrm{A} \subseteq \mathrm{B}$ *ou non.*

Démonstration Soient $a, \alpha^1, \ldots, \alpha^n \in \mathrm{E}$. On a

$$\langle\, a \,\rangle_{\mathbf{T}} \subseteq \langle \alpha^1, \ldots, \alpha^n \rangle_{\mathbf{T}} \Longleftrightarrow a \in \langle \alpha^1, \ldots, \alpha^n \rangle_{\mathbf{T}} \Longleftrightarrow \alpha^1 \preceq a \vee \cdots \vee \alpha^n \preceq a$$

Donc si $\mathrm{A} = \langle \alpha^1, \ldots, \alpha^n \rangle_{\mathbf{T}}$, la famille génératrice $\alpha^1, \ldots, \alpha^n$ est minimale pour l'inclusion ssi les α^i sont deux à deux incomparables. Pour extraire une famille minimale de $\alpha^1, \ldots, \alpha^n$, il suffit de garder, parmi cette famille, les éléments minimaux pour $\preceq$. Nous laissons le lecteur écrire la procédure de décision pour la question « $\mathrm{A} \subseteq \mathrm{B}$? ». □

2 Noethérianité et bases de Gröbner

Nous allons utiliser les bases de Gröbner pour prouver la noethérianité de $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_d] = \mathbb{K}[\underline{\mathrm{X}}] = \mathbb{A}$. La preuve s'articule ainsi :

- Preuve constructive du lemme de Dickson, qui assure la noethérianité de l'ensemble $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$ des *idéaux monomiaux* de $\mathbb{A} = \mathbb{K}[\underline{\mathrm{X}}]$ ordonné par inclusion ;
- reprise de l'exposé classique de la théorie des bases de Gröbner : le lemme de Dickson prouve la terminaison de l'algorithme de Buchberger ;
- les bases de Gröbner permettent définir constructivement l'application

$$\begin{array}{cccc} \textsc{lm} : & \mathcal{I}_{\mathbb{A}} & \longrightarrow & \mathcal{IM}_{\mathbb{A}} \\ & \mathrm{I} & \mapsto & \textsc{lm}(\mathrm{I}) \end{array}$$

qui à un idéal associe l'idéal de ses *monômes de tête*. Φ est une application strictement croissante ;
- on conclut en invoquant le lemme 5.

2.1 Lemme de Dickson

On considère $\mathbb{N}^d$ muni de l'ordre produit $\leq_d$. Si $\alpha \in \mathbb{N}^d$, on note $\underline{\mathrm{X}}^\alpha$ le monôme $\mathrm{X}_1^{\alpha_1} \cdots \mathrm{X}_d^{\alpha_d}$. Un idéal monomial de type fini de $\mathbb{A} = \mathbb{K}[\underline{\mathrm{X}}]$ est par définition un idéal engendré par une famille finie de monômes ; on note leur ensemble $\mathcal{IM}_{\mathbb{A}}$. On considère que $\{0\} \in \mathcal{IM}_{\mathbb{A}}$, et que ce singleton est engendré par la famille vide.

Lemme 9 *Il y a un isomorphisme d'ordre entre* $(\mathbf{T}^\circ(\mathbb{N}^d), \subseteq)$ *et* $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$.

Démonstration Laissons la lectrice prouver que l'application

$$\begin{array}{ccc} \mathbf{T}^\circ(\mathbb{N}^d) & \longrightarrow & \mathcal{IM}_{\mathbb{A}} \\ \varnothing & \mapsto & \{0\} \\ \langle \alpha^1, \ldots, \alpha^n \rangle_{\mathbf{T}} & \mapsto & \underline{\mathrm{X}}^{\alpha^1} \cdot \mathbb{A} + \cdots + \underline{\mathrm{X}}^{\alpha^n} \cdot \mathbb{A} \end{array}$$

est bien un isomorphisme d'ordre. □

Proposition 10 *L'ensemble ordonné* $(\mathbf{T}^\circ(\mathbb{N}^d), \subseteq)$ *est noethérien.*

Démonstration La preuve se fait par récurrence sur d. Le cas $d = 1$ est clair.

Soit $d \geq 2$, soit $(\mathrm{A}^m)_{m \in \mathbb{N}}$ une suite croissante dans $\mathbf{T}^\circ(\mathbb{N}^d)$. On peut supposer sans perte de généralité que $\mathrm{A}^0 \neq \varnothing$; soit $a = (a_1, \ldots, a_d) \in \mathrm{A}^0$ (par exemple, un des générateurs de A^0).

Pour tout $i \in \{1, \ldots, d\}$ et $r \in \mathbb{N}$, posons

$$\mathrm{H}^r_{i,d} = \{(x_1, \ldots, x_d) \ : x_i = r\} \subset \mathbb{N}^d.$$

Il y a un isomorphisme d'ordre entre $(\mathrm{H}^r_{i,d}, \leq_d)$ et $(\mathbb{N}^{d-1}, \leq_{d-1})$, donné par

$$(x_1, \ldots, x_d) \mapsto (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_d).$$

Donc les $(\mathbf{T}^\circ(\mathrm{H}^r_{i,d}), \subseteq)$ sont noethériens par hypothèse de récurrence.

D'autre part, $\mathbb{N}^d \setminus \langle\, a \,\rangle_{\mathbf{T}}$ est une union finie d'ensembles $\mathrm{H}^r_{i,d}$:

$$\mathbb{N}^d \setminus \langle\, a \,\rangle_{\mathbf{T}} \;=\; \bigcup_{i=1}^{d} \bigcup_{r<a_i} \mathrm{H}^r_{i,d}.$$

Appelons-les $\mathcal{H}_1, \ldots, \mathcal{H}_k$, de manière à ce que : $\mathbb{N}^d \setminus \langle\, a \,\rangle_{\mathbf{T}} = \cup_{j=1}^{k} \mathcal{H}_j$, où chaque $\mathcal{H}_j$ est un des $\mathrm{H}^r_{i,d}$ dans la formule ci-dessus.

Étant donné $\mathrm{A} = \langle \alpha^1, \ldots, \alpha^n \rangle_{\mathbf{T}} \in \mathbf{T}^\circ(\mathbb{N}^d)$ et $\mathcal{H} = \mathrm{H}^r_{i,d}$, on peut donner explicitement $\mathcal{H} \cap \mathrm{A}$ comme élément de $\mathbf{T}^\circ(\mathcal{H})$:

Tout d'abord, si $\beta \in \mathbb{N}^d$, on a :

$$\langle \beta \rangle_{\mathbf{T}} \cap \mathrm{H}^r_{i,d} = \begin{cases} \varnothing & \text{si } r < \beta_i \\ \langle (\beta_1, \ldots, \beta_{i-1}, r, \beta_{i+1}, \ldots, \beta_d) \rangle_{\mathbf{T}} & \text{si } \beta_i \le r. \end{cases}$$

puis $\mathcal{H} \cap \mathrm{A} = \bigcup_{i=1,\ldots,n} \big(\langle \alpha^i \rangle_{\mathbf{T}} \cap \mathcal{H} \big)$.

Donc pour tout $j \in \{1, \ldots, k\}$ on peut considérer la suite croissante $(\mathrm{A}^m \cap \mathcal{H}_j)_{m\in\mathbb{N}}$ de $\mathbf{T}^\circ(\mathcal{H}_j)$. Puisque chaque $(\mathbf{T}^\circ(\mathcal{H}_j), \subseteq)$ est noethérien, en vertu du lemme 2, il existe i tel que $\mathrm{A}^i \cap \mathcal{H}_j = \mathrm{A}^{i+1} \cap \mathcal{H}_j$ pour tout $j \in \{1, \ldots, k\}$. Alors, puisque pour tout m

$$\mathrm{A}^m = \langle\, a \,\rangle_{\mathbf{T}} \;\cup\; \Big(\bigcup_{j=1,\ldots,k} (\mathrm{A}^m \cap \mathcal{H}_j) \;\Big)$$

on a $\mathrm{A}^i = \mathrm{A}^{i+1}$. La suite $(\mathrm{A}^m)_{m\in\mathbb{N}}$ pause, et $\mathbf{T}^\circ(\mathbb{N}^d)$ est noethérien. □

En utilisant l'isomorphisme d'ordre entre $(\mathbf{T}^\circ(\mathbb{N}^d), \subseteq)$ et $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$, cette proposition se reformule comme suit :

Proposition 11 (Lemme de Dickson) $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$ *est noethérien.*

2.2 Bases de Gröbner

Le matériel de cette section est classique ; voir par exemple le livre de Cox, Little et O'Shea [CLO]. Les bases de Gröbner ont été crées en 1965 par Bruno Buchberger (*cf.* [Buc$_1$], [Buc$_2$]).

Ordres monomiaux et division

On l'a vu, une généralisation de l'algorithme de division euclidienne des polynômes à $\mathbb{K}[\underline{\mathrm{X}}]$ serait la bienvenue. Il faut pour cela donner un ordre sur les monômes, c.-à-d. sur $\mathbb{N}^d$.

Un ordre total $\preceq$ sur $\mathbb{N}^d$ est dit *acceptable* si :
- $0 \preceq \alpha$ pour tout $\alpha \in \mathbb{N}^d$;
- si $\alpha \le_d \beta$, alors $\alpha \preceq \beta$;
- si $\alpha \preceq \beta$, alors $\alpha + \gamma \preceq \beta + \gamma$;
- $\preceq$ est décidable.

On notera naturellement $\underline{\mathrm{X}}^\alpha \preceq \underline{\mathrm{X}}^\beta$ quand $\alpha \preceq \beta$.

Exemple Les ordres $\leq_{\text{lex}}$ et $\leq_{\text{deglex}}$ donnés dans la première section sont des ordres acceptables.

Lemme 12 *Si $\preceq$ est un ordre acceptable sur $\mathbb{N}^d$, alors $(\mathbb{N}^d, \preceq)$ est artinien.*

Démonstration Si $(\alpha_n)_{n\in\mathbb{N}}$ est une suite décroissante de $(\mathbb{N}^d, \preceq)$, alors en posant $\mathrm{A}^n = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbf{T}}$, on obtient une suite croissante de $\mathbf{T}^\circ(\mathbb{N}^d)$. On a $\mathrm{A}^{n+1} = \mathrm{A}^n$ si et seulement si $\alpha_{n+1} = \alpha_n$; or $\mathbf{T}^\circ(\mathbb{N}^d)$ est noethérien donc la suite $(\mathrm{A}^n)_{n\in\mathbb{N}}$ pause, et ainsi $(\alpha_n)_{n\in\mathbb{N}}$ pause également. □

Nous fixons un ordre acceptable $\preceq$ sur $\mathbb{N}^d$. Soit $f = \sum_{\alpha\in\mathbb{N}^d} a_\alpha \underline{\mathrm{X}}^\alpha \in \mathbb{A}$ un polynôme non nul. Le multidegré de f est

$$\operatorname{mdeg} f = \max_{\preceq}\{\alpha \in \mathbb{N}^d \ : \ a_\alpha \neq 0\}.$$

Si $\alpha = \operatorname{mdeg} f$, le *monôme de tête* de f est $\mathrm{LM}(f) = \underline{\mathrm{X}}^\alpha$, le *coefficient dominant* de f est $\mathrm{LC}(f) = a_\alpha$, et le *terme dominant* de f est $\mathrm{LT}(f) = a_\alpha \underline{\mathrm{X}}^\alpha$. On parlera des monômes de f pour désigner les $\underline{\mathrm{X}}^\alpha$ pour lesquels $a_\alpha \neq 0$.

Proposition 13 *Soient $f_1, \ldots, f_s$ dans $\mathbb{A} = \mathbb{K}[\underline{\mathrm{X}}]$. Tout $f \in \mathbb{A}$ peut être écrit (de manière effective)*

$$f = a_1 \cdot f_1 + \cdots + a_s \cdot f_s + r$$

où $a_1, \ldots, a_s, r \in \mathbb{A}$, $\operatorname{mdeg} a_i \cdot f_i \preceq \operatorname{mdeg} f$, et aucun des monômes de r n'est divisible par un des $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s)$.

On appelle r le ***reste de la division de f par*** *$\mathcal{F} = (f_1, \ldots, f_s)$. On notera $r = \overline{f}^{\mathcal{F}}$.*

Démonstration Si l'algorithme suivant s'arrête, le résultat répond clairement aux exigences de l'énoncé.
<u>Entrée</u> : $f_1, \ldots, f_s, f$.
<u>Sortie</u> : $a_1, \ldots, a_s, r$.

$a_1 := 0, \ldots, a_s := 0, \ r := 0, \ p := f$
Tant que $p \neq 0$**, faire**
  $i := 1$ **;**
  $div :=$ **faux ;**
  Tant que ($i \leq s$ **et** $div =$**faux**) **faire**
    Si $\mathrm{LM}(f_i) | \mathrm{LM}(p)$ **alors** $a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ **;**
      $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$ **;**
      $div :=$**vrai.**
    sinon $i := i + 1$.
  Si $div =$**faux, alors** $r := r + \mathrm{LT}(p)$**,** $p := p - \mathrm{LT}(p)$**.**

Considérons la suite des valeurs successives prises par $\mathrm{LM}(p)$. C'est une suite décroissante pour $\preceq$ qui est un ordre artinien, donc elle pause ; mais, vu l'algorithme, elle ne pause que si $p = 0$ et l'algorithme s'arrête. □

Remarques – C'est le lemme de Dickson qui prouve que l'algorithme de division est correct ; il va également prouver la correction de l'algorithme de Buchberger. Il apparaît donc comme la clef de voûte de toute la théorie des bases de Gröbner ;

– il n'y a pas *a priori* de réel résultat d'unicité du reste pour cette division. En particulier, si on permute les $f_1, \ldots, f_s$, la valeur de $\overline{f}^{\mathcal{F}}$ peut très bien changer. D'autre part il se peut que $f \in f_1 \cdot \mathbb{A} + \cdots + f_s \cdot \mathbb{A}$ et que $\overline{f}^{\mathcal{F}} \neq 0$. Cette généralisation est donc très imparfaite.

Algorithme de Buchberger

Définitions – Si $\alpha, \beta \in \mathbb{N}^d$, on appelle $\sup_{\leq_d}(\alpha, \beta)$ l'élément $\gamma = (\gamma_1, \ldots, \gamma_d)$ de $\mathbb{N}^d$ défini par $\gamma_i = \max(\alpha_i, \beta_i)$ pour tout i. Ceci correspond bien à la définition usuelle du sup pour un ordre quelconque ;

– soient $f, g \in \mathbb{K}[\underline{X}]$. Si $\alpha = \operatorname{mdeg} f$, $\beta = \operatorname{mdeg} g$, et $\gamma = \sup_{\leq_d}(\alpha, \beta)$, le *S-polynôme de* f, g est

$$\mathrm{S}(f, g) = \frac{\underline{X}^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{\underline{X}^\gamma}{\mathrm{LT}(g)} \cdot g.$$

La proposition suivante définit les bases de Gröbner. Pour sa preuve, se reporter à [CLO].

Proposition 14 (Buchberger) *Soit une famille* $\mathcal{G} = (g_1, \ldots, g_s)$ *de* $\mathbb{A} = \mathbb{K}[\underline{X}]$. *Soit* $\mathrm{I} = g_1 \cdot \mathbb{A} + \cdots + g_s \cdot \mathbb{A}$. *Les propriétés suivantes sont équivalentes :*

– *Pour tout* $f \in \mathrm{I}$, *le reste* $\overline{f}^{\mathcal{G}}$ *de la division de* f *par* $\mathcal{G}$ *est nul;*

– *pour tout* $f \in \mathrm{I}$, $\mathrm{LM}(f) \in \mathrm{LM}(g_1) \cdot \mathbb{A} + \cdots + \mathrm{LM}(g_s) \cdot \mathbb{A}$*;*

– *pour tous* i, j, $\overline{\mathrm{S}(g_i, g_j)}^{\mathcal{G}} = 0$.

On dit que $\mathcal{G}$ *est une base de Gröbner (ou base standard) de* I.

Nous pouvons maintenant donner l'algorithme de Buchberger.

Théorème 15 (Algorithme de Buchberger) *Soit* $\mathrm{I} = (f_1, \ldots, f_s)$ *un idéal non nul de* $\mathbb{A}$. *Une base de Gröbner de* I *est donnée par l'algorithme suivant :*
<u>*Entrée*</u> *:* $(f_1, \ldots, f_s)$ *une base de* I.
<u>*Sortie*</u> *:* $\mathcal{G}$ *une base de Gröbner de* I.

$\mathcal{G} := (f_1, \ldots, f_s)$
Répète
$\mathcal{H} = \mathcal{G}$
Pour toutes les paires $p, q \in \mathcal{H}$ ***faire***
Si $\overline{\mathrm{S}(p, q)}^{\mathcal{H}} \neq 0$ ***alors*** $\mathcal{G} := \mathcal{G} \cup \left\{\overline{\mathrm{S}(p, q)}^{\mathcal{H}}\right\}$.
Jusqu'à ce que $\mathcal{H} = \mathcal{G}$.

Démonstration De la proposition précédente, on déduit que si l'algorithme s'arrête, $\mathcal{G}$ est bien une base de Gröbner de I. À chaque étape de l'algorithme, on considère l'idéal monomial $\text{LM}(\mathcal{G})$ engendré par les monômes de tête des polynômes présents dans $\mathcal{G}$: on montre facilement que c'est une suite strictement croissante tant que l'algorithme ne s'arrête pas.

Le lemme de Dickson permet donc de conclure à l'arrêt de l'algorithme. Pour plus de détails, voir [CLO]. □

2.3 Conclusion

Du deuxième point de la proposition 14 découle facilement le lemme suivant :

Lemme 16 *Soit* I *un idéal de type fini de* $\mathbb{A}$. *Soit* $\mathcal{G} = (g_1, \dots, g_s)$ *une base de Gröbner de* I. *Alors l'idéal* $\text{LM}(\mathrm{I})$ *des monômes de tête de* I, *défini par*

$$\text{LM}(\mathrm{I}) = \langle \text{LM}(f) \ : \ f \in \mathrm{I} \rangle$$

est de type fini, et engendré par $\text{LM}(\mathcal{G}) = (\text{LM}(g_1), \dots, \text{LM}(g_s))$.

Lemme 17 *L'application*

$$\begin{array}{rccc} \text{LM} : & \mathcal{I}_{\mathbb{A}} & \longrightarrow & \mathcal{IM}_{\mathbb{A}} \\ & \mathrm{I} & \mapsto & \text{LM}(\mathrm{I}) \end{array}$$

est une application strictement croissante pour l'ordre de l'inclusion.

Démonstration Clairement $\mathrm{I} \subseteq \mathrm{J} \Longrightarrow \text{LM}(\mathrm{I}) \subseteq \text{LM}(\mathrm{J})$. Montrons que si $\mathrm{I} \subseteq \mathrm{J}$ et $\text{LM}(\mathrm{I}) = \text{LM}(\mathrm{J})$, alors $\mathrm{I} = \mathrm{J}$. Soit $p \in \mathrm{J}$. On a $\text{LM}(p) \in \text{LM}(\mathrm{J}) = \text{LM}(\mathrm{I})$, donc il existe $f \in \mathrm{I}$ tel que $\text{LM}(f) = \text{LM}(\mathrm{P})$.

Posons $p' = p - f \in \mathrm{J}$. On a $\operatorname{mdeg} p' < \operatorname{mdeg} p$. En utilisant cet argument récursivement, grâce au lemme 12, on conclut que $p \in \mathrm{I}$. □

Nous pouvons maintenant conclure :

Théorème 18 *L'anneau* $\mathbb{A} = \mathbb{K}[\mathrm{X}_1, \dots, \mathrm{X}_d]$ *est noethérien.*

Démonstration On applique le lemme 5 à l'application $\text{LM} : \mathcal{I}_{\mathbb{A}} \longrightarrow \mathcal{IM}_{\mathbb{A}}$. L'ensemble ordonné $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$ étant noethérien (prop. 11), $(\mathcal{I}_{\mathbb{A}}, \subseteq)$ est noethérien. □

Conséquences Tout ceci n'est pas sans avoir d'autres conséquences d'importance sur les idéaux de type fini de $\mathbb{A}$.

Proposition 19 *Soit* $\mathbb{A} = \mathbb{K}[\mathrm{X}_1, \dots, \mathrm{X}_d]$.
– $\mathbb{A}$ *est fortement discret ;*
– *l'ordre de l'inclusion est décidable dans* $\mathcal{I}_{\mathbb{A}}$.

Démonstration Pour décider si $f \in \mathrm{I}$, il faut commencer par calculer une base de Gröbner $\mathcal{G}$ de I, puis calculer $\overline{f}^{\mathcal{G}}$; et pour que I soit inclus dans J, il faut et il suffit que tous les polynômes d'une famille génératrice de J soient dans I. □

Théorème 20 *L'anneau $\mathbb{A}$ est cohérent.*

Rappelons que la notion de cohérence d'un anneau a été définie à la fin de la section précédente. Avant tout prouvons la proposition suivante :

Proposition 21 *Soient $(f_1, \ldots, f_s)$ et $(g_1, \ldots, g_t)$ deux familles génératrices d'un même idéal; c'est-à-dire qu'on sait exprimer les f_i en fonction des g_j, et réciproquement. Alors si on connaît une base du module des relations entre les f_i, on sait calculer une base du module des relations entre les g_j.*

Démonstration Soient $\mathrm{F} \in \mathbb{A}^{s\times 1}$ et $\mathrm{G} \in \mathbb{A}^{t\times 1}$ les vecteurs colonnes constitués respectivement des f_i et des g_j.

Par hypothèse, on dispose de matrices $\mathrm{P} \in \mathbb{A}^{s\times t}$ et $\mathrm{Q} \in \mathbb{A}^{t\times s}$ telles que

$$\mathrm{F} = \mathrm{P} \cdot \mathrm{G} \text{ et } \mathrm{G} = \mathrm{Q} \cdot \mathrm{F}.$$

On connait une base $\mathrm{R}_1, \ldots, \mathrm{R}_n \in \mathbb{A}^{1\times s}$ du module des relations entre les F_i, exprimée en vecteurs lignes. On a donc $\mathrm{R}_1 \cdot \mathrm{F} = 0, \ldots, \mathrm{R}_n \cdot \mathrm{F} = 0$, et si $[a_1, \ldots, a_s] \cdot \mathrm{F} = 0$, alors il existe $q_1, \ldots, q_n \in \mathbb{A}$ tels que $[a_1, \ldots, a_s] = \sum q_i \cdot \mathrm{R}_i$.

De $\mathrm{R}_i \cdot \mathrm{F} = 0$, on déduit $\mathrm{R}_i \cdot \mathrm{P} \cdot \mathrm{G} = 0$; soient donc

$$\mathrm{S}_1 = \mathrm{R}_1 \cdot \mathrm{P}, \ldots, \mathrm{S}_n = \mathrm{R}_n \cdot \mathrm{P} \in \mathbb{A}^{1\times t}$$

les vecteurs lignes associés à ces relations entre les g_j.

Une autre famille de relations est donnée par l'égalité qui découle des changements de base : $\mathrm{G} = \mathrm{Q}\cdot\mathrm{P}\cdot\mathrm{G}$. Soient $\mathrm{T}_1, \ldots, \mathrm{T}_t$ les t lignes de la matrice $\mathrm{Id}_t - \mathrm{Q}\cdot\mathrm{P}$. Alors pour tout i, $\mathrm{T}_i \cdot \mathrm{G} = 0$.

La famille $\{\mathrm{S}_1, \ldots, \mathrm{S}_n, \mathrm{T}_1, \ldots, \mathrm{T}_t\}$ est une famille génératrice pour le module des relations entre les g_j. En effet, si $[b_1, \ldots, b_t]\cdot\mathrm{G} = 0$, on a $[b_1, \ldots, b_t]\cdot\mathrm{Q}\cdot\mathrm{F} = 0$, et donc $[b_1, \ldots, b_t] \cdot \mathrm{Q} = \sum q_i \cdot \mathrm{R}_i$. Alors $[b_1, \ldots, b_t] \cdot \mathrm{Q} \cdot \mathrm{P} = \sum q_i \cdot \mathrm{S}_i$; et donc $[b_1, \ldots, b_t] = \sum q_i \cdot \mathrm{S}_i + b_1 \cdot \mathrm{T}_1 + \cdots + b_t \cdot \mathrm{T}_t$. □

Nous allons avoir besoin du lemme suivant :

Lemme 22 *Soient $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^d$. On va s'intéresser aux relations (syzygies) des monômes $\underline{\mathrm{X}}^{\alpha_i}$. Elles sont engendrées par les relations $\mathrm{S}(\underline{\mathrm{X}}^{\alpha_i}, \underline{\mathrm{X}}^{\alpha_j}) = 0$.*

Plus précisément, soit $\gamma_{ij} = \sup_{\leq_d}(\alpha_i, \alpha_j)$. Soit $\mathrm{R}_{ij} \in \mathbb{A}^s$ le vecteur de polynômes correspondant à la relation

$$\underline{\mathrm{X}}^{\gamma_{ij}-\alpha_i} \cdot \underline{\mathrm{X}}^{\alpha_i} - \underline{\mathrm{X}}^{\gamma_{ij}-\alpha_j} \cdot \underline{\mathrm{X}}^{\alpha_j} = 0$$

c.-à-d. $$\mathrm{R}_{ij} = (0, \ldots, \underbrace{\underline{\mathrm{X}}^{\gamma_{ij}-\alpha_i}}_{i^{\text{e}}\ position}, \ldots, \underbrace{-\underline{\mathrm{X}}^{\gamma_{ij}-\alpha_j}}_{j^{\text{e}}\ position}, \ldots, 0).$$

Alors pour toute relation $p_1 \cdot \underline{\mathrm{X}}^{\alpha_1} + \cdots + p_s \cdot \underline{\mathrm{X}}^{\alpha_s} = 0$*, il existe des polynômes* q_{ij}*, pour* $i < j \in \{1, \ldots, s\}$*, tels que*

$$(p_1, \ldots, p_s) = \sum_{i<j} q_{ij} \cdot \mathrm{R}_{ij}.$$

De plus si $\operatorname{mdeg}(p^k \cdot \underline{\mathrm{X}}^{\alpha_k}) \preceq \delta$ *pour tout* k*, on a peut supposer* $\operatorname{mdeg} q_{ij} \preceq \delta - \gamma_{ij}$*.*

Démonstration La preuve est une récurrence finie descendante sur s.

On écrit la division de p_s par la famille $(\underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s})_{k=1,\ldots,s-1}$.

$$p_s = \sum_{k=1}^{s-1} q_k \cdot \underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s} + r_s$$

où $\operatorname{mdeg} q_k \cdot \underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s} \preceq \operatorname{mdeg} p_s$ (et donc $\operatorname{mdeg} q_k \preceq \delta - \gamma_{ks}$), et aucun des monômes de r_s n'est divisible par un des $\underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s}$. Alors on a

$$p_1 \cdot \underline{\mathrm{X}}^{\alpha_1} + \cdots + p_{s-1} \cdot \underline{\mathrm{X}}^{\alpha_{s-1}} + \left(\sum_{k=1}^{s-1} q_k \cdot \underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s} \right) \cdot \underline{\mathrm{X}}^{\alpha_s} = -r_s \cdot \underline{\mathrm{X}}^{\alpha_s}.$$

Si $r_s \neq 0$, $\alpha_s + \operatorname{mdeg} r_s$ est le multidegré d'un des termes de gauche. Si c'est un des $q_k \cdot \underline{\mathrm{X}}^{\gamma_{ks}}$, on a $\underline{\mathrm{X}}^{\gamma_{ks}-\alpha_s}$ qui divise $\textsc{lm}(r_s)$. Si c'est un des $p_i \cdot \underline{\mathrm{X}}^{\alpha_i}$, alors $\underline{\mathrm{X}}^{\alpha_i}$ divise $\textsc{lm}(r_s) \cdot \underline{\mathrm{X}}^{\alpha_s}$ et $\underline{\mathrm{X}}^{\gamma_{is}-\alpha_s}$ divise $\textsc{lm}(r_s)$. La seule possibilité est donc $r_s = 0$.

En posant $p'_i = p_i + q_i \cdot \underline{\mathrm{X}}^{\gamma_{is}-\alpha_s}$, on obtient une nouvelle relation

$$(p'_1, \ldots, p'_{s-1}, 0) = (p_1, \ldots, p_s) + \sum_{k=1}^{s-1} q_k \cdot \mathrm{R}_{ks}.$$

Notons que $\operatorname{mdeg} p'_i \cdot \underline{\mathrm{X}}^{\alpha_i} \preceq \delta$ Il reste à répéter cette opération (en tout s fois) pour obtenir le résultat. □

Proposition 23 *Soit* $\mathrm{I} \in \mathcal{I}_{\mathrm{A}}$ *un idéal de base de Gröbner* $\mathcal{G} = (g_1, \ldots, g_s)$*. Le module de syzygies* $\{(p_1, \ldots, p_s) \in \mathbb{A}^s \ : \ p_1 \cdot g_1 + \cdots + p_s \cdot g_s = 0\}$ *de* I *est de type fini, et il est engendré par les relations qui expriment que* $\overline{\mathrm{S}(g_i, g_j)}^{\mathcal{G}} = 0$*.*

Démonstration On garde les notations du lemme précédent, en posant $\alpha_i = \operatorname{mdeg} g_i$. On appelle T_{ij} le vecteur associé à la relation

$$\mathrm{X}^{\gamma_{ij}-\alpha_i} \cdot g_i - \underline{\mathrm{X}}^{\gamma_{ij}-\alpha_j} \cdot g_j = \sum_{k=1}^{s} p_k^{ij} \cdot g_k.$$

Ce vecteur est $\mathrm{T}_{ij} = \mathrm{R}_{ij} - (p_1^{ij}, \cdots, p_s^{ij})$.

Soient $p_1, \ldots, p_s$ tels que $p_1 \cdot g_1 + \cdots + p_s \cdot g_s = 0$. Soit $\delta_i = \operatorname{mdeg} p_i \cdot g_i$ et $\delta = \max\{\delta_1, \ldots, \delta_s\}$. On a

$$\sum_{k\,:\,\delta_k=\delta} \textsc{lt}(p_k) \cdot \underline{\mathrm{X}}^{\alpha_k} = 0$$

et cette relation s'exprime en fonction des R_{ij}.

Soit μ le vecteur des $\mu_k = \begin{cases} 0 & \text{si } \delta_k \prec \delta, \\ \mathrm{LT}(p_k) & \text{si } \delta_k = \delta. \end{cases}$ On a $\mu = \sum_{i<j} q_{ij} \cdot \mathrm{R}_{ij}$.

On obtient

$$\sum_{k\,:\,\delta_k=\delta} \mathrm{LT}(p_k) \cdot g_k = \sum_{i<j} q_{ij} \cdot \left(\mathrm{X}^{\gamma_{ij}-\alpha_i} \cdot g_i - \underline{\mathrm{X}}^{\gamma_{ij}-\alpha_j} \cdot g_j\right).$$

On reconnaît le terme de gauche de la relation qui définit les T_{ij}. On utilise cette relation pour obtenir

$$\sum_{k\,:\,\delta_k=\delta} \mathrm{LT}(p_k) \cdot g_k = \sum_{i<j} q_{ij} \cdot \left(\sum_{k=1}^{s} p_k^{ij} \cdot g_k\right).$$

puis $\displaystyle\sum_{k\,:\,\delta_k=\delta} (p_k - \mathrm{LT}(p_k)) \cdot g_k + \sum_{k\,:\,\delta_k<\delta} p_k \cdot g_k + \sum_{i<j} q_{ij} \cdot \left(\sum_{k=1}^{s} p_k^{ij} \cdot g_k\right) = 0.$

Cette nouvelle relation est $p'_1 \cdot g_1 + \cdots + p'_s \cdot g_s = 0$, avec

$$(p'_1, \cdots, p'_s) = (p_1, \ldots, p_s) - \sum_{i<j} q_{ij} \cdot \mathrm{T}_{ij}.$$

Ce nouveau vecteur a son multidegré maximal $\prec \delta$. En itérant cette opération, on finit par arriver au vecteur nul. □

Preuve du théorème 20 Il suffit de mettre bout à bout les deux propositions précédentes. □

Définitions – Soit $\mathrm{I} \in \mathcal{I}_{\mathbb{A}}$. Le r^{e} idéal d'élimination de I est, par définition, l'idéal $\mathrm{I}_r = \mathrm{I} \cap \mathbb{K}[\mathrm{X}_{r+1}, \ldots, \mathrm{X}_d]$ de $\mathbb{K}[\mathrm{X}_{r+1}, \ldots, \mathrm{X}_d]$;
– le quotient $\mathrm{I} : \mathrm{J}$ de deux idéaux est l'idéal $\{f : f \cdot \mathrm{J} \subseteq \mathrm{I}\}$.

Théorème 24 *Soit* $\mathrm{I} \in \mathcal{I}_{\mathbb{A}}$. *On sait calculer les idéaux d'élimination de* I. *Soit* $\mathrm{J} \in \mathcal{I}_{\mathbb{A}}$. *On sait calculer* $\mathrm{I} \cap \mathrm{J}$ *et* $\mathrm{I} : \mathrm{J}$.

Démonstration Pour calculer les idéaux d'élimination de I, il faut choisir comme ordre admissible $\preceq$ l'ordre lexicographique $\leq_{\mathrm{lex}}$. Alors si $\mathcal{G}$ est une base de Gröbner pour cet ordre, $\mathcal{G}_r = \mathcal{G} \cap \mathbb{K}[\mathrm{X}_{r+1}, \ldots, \mathrm{X}_d]$ est une base de Gröbner pour I_r. Pour plus de détails, voir [CLO].

Il y a différentes manières bien connues de calculer l'intersection de deux idéaux $\mathrm{I} = f_1 \cdot \mathbb{A} + \cdots + f_s \cdot \mathbb{A}$ et $\mathrm{J} = g_1 \cdot \mathbb{A} + \cdots + g_t \cdot \mathbb{A}$. Par exemple on peut remarquer que donner un élément

$$a_1 \cdot f_1 + \cdots + a_s \cdot f_s = b_1 \cdot g_1 + \cdots + b_t \cdot g_t$$

de $\mathrm{I} \cap \mathrm{J}$ revient à calculer un vecteur de relations $(a_1, \ldots, a_s, b_1, \ldots, b_t)$ entre les polynômes $(f_1, \ldots, f_s, -g_1, \ldots, -g_t)$. On calcule donc une base finie du module des syzygies de ce système.

Si, à nouveau, $\mathrm{I} = f_1 \cdot \mathbb{A} + \cdots + f_s \cdot \mathbb{A}$ et $\mathrm{J} = g_1 \cdot \mathbb{A} + \cdots + g_t \cdot \mathbb{A}$, on s'aperçoit que

$$f \in (\mathrm{I} \;:\mathrm{J}) \Longleftrightarrow (f \cdot g_1 \in \mathrm{I} \wedge \cdots \wedge f \cdot g_t \in \mathrm{I})$$

et donc
$$\mathrm{I} \;:\mathrm{J} = (\mathrm{I} \;: g_1 \cdot \mathbb{A}) \cap \cdots \cap (\mathrm{I} \;: g_t \cdot \mathbb{A})$$

Il suffit de calculer $(\mathrm{I} \;: g \cdot \mathbb{A})$ pour g arbitraire. Soit une base finie $h_1, \ldots, h_u$ de $\mathrm{I} \cap g \cdot \mathbb{A}$; alors $h_1/g, \ldots, h_u/g$ est une base de $(\mathrm{I} \;: g \cdot \mathbb{A})$. □

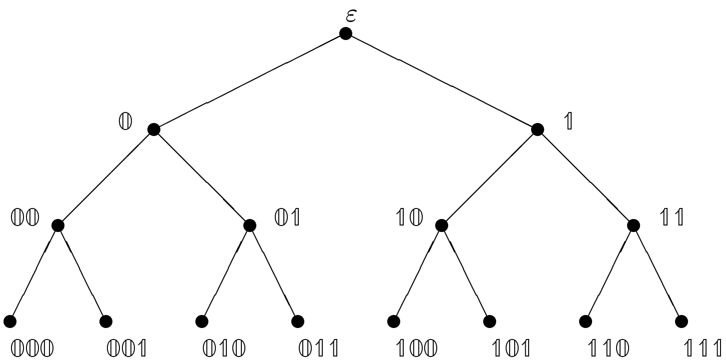
Remarque : les $\mathbb{A}$-modules libres Terminons cette section en signalant que, suivant par exemple un rapport de André Galligo ([Gal]), la technique des bases de Gröbner peut être étendue aux $\mathbb{A}$-modules de $\mathbb{A}^n$. Alors la preuve constructive du lemme de Dickson permet de conclure constructivement à la noethérianité et à la cohérence de $\mathbb{A}^n$ (*cf.* [LP]).

3 Ensembles ordonnés, suite

Je me suis attaché dans cette partie à décrire la démarche heuristique qui conduit à une nouvelle version de la noethérianité constructive. J'espère que le lecteur pressé ne m'en tiendra pas rigueur.

Arbres Soit $\mathbb{T}_2$ l'ensemble des mots sur l'alphabet $\{\mathbb{0}, \mathbb{1}\}$, y compris le mot vide, noté ε. On munit $\mathbb{T}_2$ de la relation d'ordre suivante : $a \preceq b$ si a est un préfixe de b, c.-à-d. il existe un mot c tel que $ac = b$.

On représente habituellement $\mathbb{T}_2$ ainsi :



Un *arbre binaire* T est une partie initiale de $\mathbb{T}_2$. Les parties initiales de type fini de $\mathbb{T}_2$ sont de cardinal fini ; on les appellera arbres finis.

Soit $(\mathrm{E}, \leq)$ un ensemble ordonné. Un *arbre binaire strictement croissant (resp. décroissant)* dans E, (T, ϕ), est un arbre T muni d'une application strictement croissante $\phi \,:\, (\mathrm{T}, \preceq) \longrightarrow (\mathrm{E}, \leq)$ (resp. $\phi \,:\, (\mathrm{T}, \preceq) \longrightarrow (\mathrm{E}, \geq)$).

Le symbole ¶ signale un résultat non constructif.

¶ **Théorème 25** *Si* $(\mathrm{E}, \leq)$ *est noethérien (resp. artinien), alors tout arbre binaire strictement croissant (resp. décroissant) dans* E *est fini.*

Pour prouver ce théorème nous avons besoin du théorème suivant.

¶ **Théorème 26 (Lemme de König)** *Si* T *est un arbre binaire infini, alors* T *a une branche infinie, c'est-à-dire qu'il existe une suite strictement croissante* $(a_n)_{n\in\mathbb{N}}$ *de sommets de* T.

Démonstration Plaçons un personnage omniscient à la racine $a_0 = \varepsilon$ de l'arbre. Devant lui s'ouvrent deux sous-arbres : l'un des deux au moins est infini. Ce personnage choisit d'avancer sur le sommet a_1 de ce sous-arbre infini, et recommence. Le personnage parcourt un chemin infini. □

Remarquons que les personnages omniscients ne sont pas constructifs. Plus précisément, étant donné une énumération des sommets d'un arbre, il n'y a pas d'algorithme qui peut en trouver une branche infinie. Kleene a construit un arbre récursif infini dont aucune branche infinie n'est récursive ; on peut également montrer que le lemme de König entraine le « principe d'omniscience » **LLPO** (*cf.* [MRR, Chap. I]), et est donc non constructif.

Preuve du théorème 25 Si on a un arbre binaire strictement croissant dans E, (T, ϕ) infini, choisissons-en une branche infinie $(a_n)_{n\in\mathbb{N}}$. La suite $\phi(a_n)$ est une suite strictement croissante de E. Ceci contredit la noethérianité de E. □

Il est difficile de produire une preuve constructive du théorème 25. Pourtant il peut être nécessaire de disposer d'une version de ce théorème pour des arbres croissants dans les idéaux de type fini d'un anneau ; la question arrive naturellement quand on utilise les méthodes dynamique à la [CLR].

En tentant de montrer ce résultat pour les idéaux de $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, j'ai été conduit à formuler une condition de noethérianité plus forte (au point de vue constructif) que la condition **CCA**, dont la vérité entraine le théorème 25.

Avant tout, remarquons qu'il y a des choses faciles à prouver.

Lemme 27 *Tout arbre binaire strictement décroissant dans* $\mathbb{N}$ *est fini.*

Démonstration Soit (T, ϕ) un tel arbre. La preuve se fait par récurrence sur $\phi(\varepsilon)$. Si $\phi(\varepsilon) = 0$, alors clairement $\mathrm{T} = \{\varepsilon\}$.

Si c'est vrai $\forall k < n$ pour $\phi(\varepsilon) = k$, alors tout arbre dont la racine est étiquetée par $\phi(\varepsilon) = n$ est étiqueté en $\mathbb{0}$ et $\mathbb{1}$ par $\phi(\mathbb{0}), \phi(\mathbb{1}) < n$, et est donc « l'union » de (au plus) deux arbres finis ; il est donc fini. □

Lemme 28 *Tout arbre binaire strictement croissant dans* $\mathcal{I}_{\mathbb{K}[\mathrm{X}]}$ *est fini.*

Démonstration Soit (T, ϕ) un arbre binaire strictement croissant dans $\mathcal{I}_{\mathbb{K}[\mathrm{X}]}$. Souvenons-nous de la preuve du lemme 4 : il y a une application strictement décroissante Φ de $(\mathcal{I}_{\mathbb{K}[\mathrm{X}]}, \subseteq)$ vers $(\mathbb{N} \cup \{+\infty\}, \leq)$. Donc $(\mathrm{T}, \Phi \circ \phi)$ est un arbre binaire strictement décroissant dans $\mathbb{N} \cup \{+\infty\}$. Il est fini grâce au lemme précédent. □

Lemme 29 *Tout arbre binaire strictement croissant dans $\mathcal{I}_{\mathbb{Z}}$ est fini.*

Démonstration Cette fois ci, on utilise l'application strictement croissante $(\mathcal{I}_{\mathbb{Z}}, \supseteq)$ vers $(\mathbb{N} \cup \{+\infty\}, \leq)$, comme dans la preuve du lemme 6. □

On voit que la récurrence joue un grand rôle ici.

3.1 Ensembles bien fondés, bien ordonnés

Ensembles bien fondés

Soit $(\mathrm{E}, \leq)$ un ensemble ordonné. Une partie H de E est *héréditaire* si

$$\forall x, \ \big(\{y \ : \ y < x\} \subseteq \mathrm{H} \Longrightarrow x \in \mathrm{H}\big)\,.$$

Un ensemble *bien fondé* est un ensemble ordonné $(\mathrm{E}, \leq)$ tel que la seule partie héréditaire H de E soit $\mathrm{H} = \mathrm{E}$. D'un point de vue pratique, c'est un ensemble qui permet les preuves par récurrence ; cette propriété est très clairement une propriété du second ordre.

Les deux lemmes suivants nous seront utiles plus loin.

Lemme 30 *Soient* $(\mathrm{E}, \leq_{\mathrm{E}})$ *et* $(\mathrm{F}, \leq_{\mathrm{F}})$ *deux ensembles bien fondés. Alors* $(\mathrm{E} \times \mathrm{F}, \leq_{\mathrm{E}\times\mathrm{F}})$ *et* $(\mathrm{E} \times \mathrm{F}, \leq_{\mathrm{lex}})$ *sont bien fondés.*

Démonstration On va faire la preuve pour l'ordre produit $\leq_{\mathrm{E}\times\mathrm{F}}$. Soit H une partie héréditaire de $\mathrm{E} \times \mathrm{F}$. Soit $\mathrm{H_E}$ la partie de E définie par

$$\mathrm{H_E} = \{x \in \mathrm{E} \ : \ \forall y \in \mathrm{F}, (x, y) \in \mathrm{H}\}.$$

Soit x dans E ; supposons que tous les $x' <_{\mathrm{E}} x$ sont dans $\mathrm{H_E}$. Définissons une partie de F comme suit :

$$\mathrm{H}_x = \{y \in \mathrm{F} \ : \ (x, y) \in \mathrm{H}\}.$$

Montrons que H_x est héréditaire. Soit y tel que pour tout $y' <_{\mathrm{F}} y$ on ait $y' \in \mathrm{H}_x$. On a donc $(x, y') \in \mathrm{H}$ pour tout $y' <_{\mathrm{F}} y$, et d'autre part $(x', y') \in \mathrm{H}$ dès que $x' <_{\mathrm{E}} x$ (hypothèse faite sur x). Donc $(x', y') <_{\mathrm{E}\times\mathrm{F}} (x, y) \Longrightarrow (x', y') \in \mathrm{H}$. L'hérédité de H entraîne $(x, y) \in \mathrm{H}$ et donc $y \in \mathrm{H}_x$. La partie H_x est bien une partie héréditaire de F, donc $\mathrm{H}_x = \mathrm{F}$. Ceci entraîne $x \in \mathrm{H_E}$, et donc $\mathrm{H_E}$ héréditaire.

On a donc $\mathrm{H_E} = \mathrm{E}$, puis $\mathrm{H} = \mathrm{E} \times \mathrm{F}$. L'ensemble $\mathrm{E} \times \mathrm{F}$ est bien-fondé. □

Remarque Cette preuve permet également de conclure que $(\mathrm{E} \times \mathrm{F}, \leq_{\mathrm{lex}})$ est bien fondé.

Lemme 31 *Soit* $\phi \ : (\mathrm{E}, \leq_{\mathrm{E}}) \longrightarrow (\mathrm{F}, \leq_{\mathrm{F}})$ *une application strictement croissante. Si* F *est bien fondé, alors* E *est bien fondé.*

Démonstration Soit H une partie héréditaire de E. Soit

$$\mathrm{H}' = \{y \in \mathrm{F} \,:\, \phi(x) \leq_{\mathrm{F}} y \Longrightarrow x \in \mathrm{H}\}.$$

H' est héréditaire : supposons que y est tel que $y' <_{\mathrm{F}} y \Longrightarrow y' \in \mathrm{H}'$. Soit $x \in \mathrm{E}$ tel que $\phi(x) \leq_{\mathrm{F}} y$. Si $\phi(x) <_{\mathrm{F}} y$, alors soit $y' = \phi(x) < y$, y' est dans H' et donc $\phi(x) \leq_{\mathrm{F}} y'$ implique $x \in \mathrm{H}$. Si $\phi(x) = y$, alors pour tout $x' <_{\mathrm{E}} x$, on a $\phi(x') <_{\mathrm{F}} \phi(x) = y$, et comme avant $x' \in \mathrm{H}$; par hérédité de H, on a également $x \in \mathrm{H}$. Donc y est dans H'.

Alors F étant bien fondé, $\mathrm{H}' = \mathrm{F}$, et par suite $\mathrm{H} = \mathrm{E}$. Donc E est bien fondé. □

Théorème 32 *Si* $(\mathrm{E}, \leq)$ *est bien fondé, alors tout arbre binaire strictement décroissant dans* E *est fini.*

Démonstration Soit

$$\mathrm{H} = \{x \,:\, \text{tout arbre } (\mathrm{T}, \phi) \text{ tel que } \phi(\varepsilon) = x \text{ est fini}\}.$$

Alors H est une partie héréditaire : si tous les $y < x$ sont dans H, tout arbre étiqueté à la racine par x est étiqueté en $\mathbb{0}$ et $\mathbb{1}$ (si ils font partie de l'arbre) par $y_{\mathbb{0}}, y_{\mathbb{1}} < x$; il est donc « l'union » de deux arbres (au plus) finis, donc il est fini.

□

En particulier un ensemble bien fondé satisfait la condition **CCD** : il est artinien. D'un point de vue non constructif, la réciproque est vraie :

¶ **Proposition 33** *Si* $(\mathrm{E}, \leq)$ *vérifie* ***CCD****, alors* E *est bien fondé.*

Démonstration Soit H une partie héréditaire tel que $\mathrm{E} \setminus \mathrm{H} \neq \varnothing$. Soit $x_0 \in \mathrm{E} \setminus \mathrm{H}$. Alors $\{y \,:\, y < x_0\} \setminus \mathrm{H}$ est non vide ; soit x_1 dans cet ensemble. En itérant cette opération on obtient une suite infinie décroissante. □

Jacobsson & Löfwall ont montré constructivement (*cf.* [JL]) que si $\mathbb{A}$ est un anneau cohérent à idéaux détachables,

$$(\mathcal{I}_{\mathbb{A}}, \supseteq) \text{ bien fondé} \Longrightarrow (\mathcal{I}_{\mathbb{A}[\mathrm{X}]}, \supseteq) \text{ bien fondé},$$

et de plus $\mathbb{A}[\mathrm{X}]$ est cohérent à idéaux détachables (comparer ce résultat avec le théorème 7). Un résultat analogue est montré en théorie des types par Coquand & Persson, sans l'hypothèse de détachabilité des idéaux (*cf.* [CP]).

Ce beau résultat est néanmoins un peu difficile à appréhender pour l'esprit. Que signifie exactement cette propriété de fondation, d'un point de vue constructif ? Qu'on peut faire des preuves par récurrence. Mais c'est ce qu'on a fait pour $\mathbb{K}[\mathrm{X}]$ et $\mathbb{Z}$, sans parler d'ensemble bien fondé.

Ce que je veux suggérer, c'est qu'il est plus facile et plus intuitif de faire des preuves par récurrence sur le degré que sur l'ordre $\supseteq$. On peut penser que c'est parce que le degré vit dans un ensemble totalement ordonné.

Ensembles bien ordonnés

Un ensemble *bien ordonné* est un ensemble bien fondé totalement ordonné.

Lemme 34 *Soient* $(\mathrm{E}, \leq_{\mathrm{E}})$ *et* $(\mathrm{F}, \leq_{\mathrm{F}})$ *deux ensembles bien ordonnés. Alors* $(\mathrm{E}\times\mathrm{F}, \leq_{\mathrm{lex}})$ *est bien ordonné.*

Démonstration On pourrait renvoyer à la preuve du lemme 30, mais nous préférons, afin d'appuyer notre affirmation selon laquelle les preuves sont plus concrètes dans les ensembles bien ordonnés, présenter les choses comme une récurrence double classique. Soit H une partie héréditaire de $\mathrm{E} \times \mathrm{F}$.

Pour $x \in \mathrm{E}$, soit $\mathrm{P}(x)$ la propriété suivante : pour tout y dans F, $(x, y) \in \mathrm{H}$. Montrons par récurrence que $\mathrm{P}(x)$ est vraie pour tout x.

Appelons $\mathbb{0}_{\mathrm{E}}$ et $\mathbb{0}_{\mathrm{F}}$ les plus petits éléments de E et F. Alors $(\mathbb{0}_{\mathrm{E}}, \mathbb{0}_{\mathrm{F}})$ est le plus petit élément de $(\mathrm{E} \times \mathrm{F})$. En tant que tel, d'après la définition d'une partie héréditaire, il est dans H. Puis, par récurrence dans F, pour tout $y \in \mathrm{F}$, $(\mathbb{0}_{\mathrm{E}}, y) \in \mathrm{H}$. Donc $\mathrm{P}(\mathbb{0}_{\mathrm{E}})$ est vraie.

Si $\mathrm{P}(y)$ est vraie pour tout $y < x$, alors clairement $(x, \mathbb{0}_{\mathrm{E}}) \in \mathrm{H}$ d'après l'hérédité de H. Puis par récurrence dans F, $(x, y) \in \mathrm{H}$ pour tout y dans F. Donc $\mathrm{P}(x)$ est vraie. Par récurrence dans E, elle est vraie pour tout x.

On conclut qu'on a bien $\mathrm{H} = \mathrm{E} \times \mathrm{F}$. □

3.2 Ensembles fortement artiniens et noethériens

Définition Un ensemble ordonné $(\mathrm{E}, \leq)$ sera dit *fortement artinien* (resp. *fortement noethérien*) si on dispose d'un ensemble bien ordonné $(\mathrm{F}, \preceq)$ et d'une application strictement croissante (resp. une application strictement décroissante) de $(\mathrm{E}, \leq)$ vers $(\mathrm{F}, \preceq)$.

Un anneau $\mathbb{A}$ sera dit fortement noethérien si $(\mathcal{I}_{\mathbb{A}}, \subseteq)$ est fortement noethérien.

Exemple On l'a vu (lemmes 4, 6, 28, 29), $\mathbb{Z}$ et $\mathbb{K}[\mathrm{X}]$ sont des anneaux fortements noethériens.

Théorème 35 *Un ensemble fortement artinien est bien fondé. En particulier il est artinien.*

Démonstration Soit $\phi : (\mathrm{E}, \leq) \longrightarrow (\mathrm{F}, \preceq)$ une application strictement croissante vers un ensemble bien ordonné. Soit H une partie héréditaire de $(\mathrm{E}, \leq)$. On montre que pour tout $x \in \mathrm{F}$, $\{a \in \mathrm{E} : \phi(a) = x\}$ est dans H, par récurrence sur x; cela se fait facilement par récurrence dans F. On conclut par $\mathrm{H} = \phi^{-1}(\mathrm{F}) = \mathrm{E}$. □

Lemme 36 *Les arbres strictement croissants (resp. décroissants) dans un ensemble fortement noethérien (resp. fortement artinien) sont finis.*

Démonstration On peut utiliser le fait que c'est vrai pour les ensembles bien fondés ; on peut refaire la preuve de 27 en la traduisant en une récurrence sur $\phi(\varepsilon)$, où ϕ est comme dans la preuve précédente. □

Nos conditions fortes sont, du point de vue constructifs, plus fortes que les autres conditions évoquées (et c'est heureux). Du point de vue classique, une fois de plus, tout est équivalent.

¶ **Théorème 37** *Soit* $(\mathrm{E}, \leq)$ *un ensemble bien fondé. Alors il existe un ensemble bien ordonné* $(\mathrm{F}, \preceq)$ *et une application strictement croissante* $\phi : \mathrm{E} \longrightarrow \mathrm{F}$.

Démonstration La preuve est une récurrence transfinie. Pour cette notion et la notion d'ordinaux, voir [Kri].

Soit $\mathrm{E}_\varnothing = \varnothing$. Pour tout ordinal α, on définit

$$\mathrm{E}_{\alpha+1} = \{x \in \mathrm{E} \;:\; y < x \Longrightarrow y \in \mathrm{E}_\alpha\}.$$

Pour un ordinal limite $\beta = \bigcup_{\alpha<\beta} \alpha$, on pose $\mathrm{E}_\beta = \bigcup_{\alpha<\beta} \mathrm{E}_\alpha$.

Les E_α forment une suite tout d'abord strictement croissante pour l'inclusion, puis constante dès qu'on a atteint γ tel que $\mathrm{E}_\gamma = \mathrm{E}$. L'application

$$\begin{array}{ccc} \mathrm{E} & \longrightarrow & \gamma \\ x & \mapsto & \min\{\alpha < \gamma \;:\; x \in \mathrm{E}_\alpha\} \end{array}$$

est une application strictement croissante. □

Nous pouvons considérer la noethérianité forte de l'anneau $\mathbb{A} = \mathbb{K}[\underline{\mathrm{X}}]$, puis celle de $\mathbb{Z}[\mathrm{X}]$.

4 Noethérianité forte

4.1 Noethérianité forte et bases de Gröbner

Nous allons démontrer une nouvelle version du lemme de Dickson. On réutilise ici les notations de la section 2. En particulier l'anneau $\mathbb{A}$ est $\mathbb{A} = \mathbb{K}[\underline{\mathrm{X}}] = \mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$.

Un sous-espace de dimension $d-k$ de $\mathbb{N}^d$ est, par définition, un espace du type

$$\mathrm{H}^{\overline{r}}_{\overline{\imath},d} = \{(x_1, \ldots, x_d) \;:\; x_{i_1} = r_1 \wedge \cdots \wedge x_{i_k} = r_k\}\,,$$

où $1 \leq i_1 < \cdots < i_k \leq d$, et $r_1, \ldots, r_k \in \mathbb{N}$. Les sous-espaces de dimension 0 sont des singletons.

Proposition 38 *L'ensemble ordonné* $(\mathbf{T}^\circ(\mathbb{N}^d), \subseteq)$ *est fortement noethérien.*

Démonstration Soit $\mathrm{A} \in \mathbf{T}^\circ(\mathbb{N}^d) \setminus \{\varnothing\}$. On va s'intéresser au complémentaire de A : notons-le C_1. On compte les sous-espaces de dimension $d-1$ qui sont inclus dans C_1. Ils sont en nombre fini ψ_1 (peut-être nul) ; ils ne sont pas nécessairement disjoints. Notons maintenant C_2 l'ensemble C_1 privé de ces ψ_1 hyperplans. On compte les sous-espaces de dimension $d-2$ qui sont inclus dans C_2. Ils sont en nombre fini ψ_2. On poursuit ainsi jusqu'à C_d qui est une union finie de ψ_d singletons.

Notons $\Psi_d(A) = (\psi_1, \dots, \psi_d) \in \mathbb{N}^d$. Alors

$$\begin{array}{rcccc} \Psi_d & : & (\mathbf{T}^\circ(\mathbb{N}^d), \subseteq) & \longrightarrow & (\mathbb{N}^d \cup \{+\infty\}, \leq_{\text{lex}}) \\ & & \varnothing & \mapsto & +\infty \\ & & A & \mapsto & \Psi_d(A) \end{array}$$

est une application strictement décroissante vers un ensemble bien ordonné. □

Remarque À des fins de calcul efficace, cette fonction peut être définie par récurrence. Si $A \in \mathbf{T}^\circ(\mathbb{N})$, A s'écrit $A = \langle\, a \,\rangle_{\mathbf{T}}$ avec $a \in \mathbb{N}$, et $\Psi_1(A) = a$.

Soient $\pi_1, \dots \pi_d$ les d projections canoniques de $\mathbb{N}^d$ vers $\mathbb{N}^{d-1}$. Il est facile de calculer $\pi_i(A)$ de façon effective : si $A = \langle a_1, \dots, a_n \rangle_{\mathbf{T}}$, alors $\pi_i(A) = \langle \pi_i(a_1), \dots, \pi_i(a_n) \rangle_{\mathbf{T}}$. Posons

$$(\phi_1, \dots, \phi_{d-1}) = \Psi_{d-1} \circ \pi_1(A) + \cdots + \Psi_{d-1} \circ \pi_d(A)\,.$$

Alors on peut poser $\psi_1 = \dfrac{\phi_1}{d-1}, \dots, \psi_{d-2} = \dfrac{\phi_{d-2}}{2}, \psi_{d-1} = \phi_{d-1}$.

Il est plus difficile de calculer ψ_d. Nous n'entrerons pas dans les détails, la calculabilité de cet entier à partir de la données des générateurs de A nous semblant tout à fait intuitive ; nous allons cependant donner une esquisse d'algorithme, sans en prouver la correction.

Appelons *pavé* de $\mathbb{N}^d$ une partie $\mathfrak{P}(a, b)$ définie, pour $a <_d b$, comme suit :

$$\mathfrak{P}(a, b) = \{x \in \mathbb{N}^d \ : \ a \leq_d x <_d b\}$$

On clôt la famille $(a_1, \dots, a_n)$ par les opérations $\sup_{\leq_d}$ et $\inf_{\leq_d}$. On obtient une famille finie $\mathcal{A}$.

On considère les pavés $\mathfrak{P}_1, \dots, \mathfrak{P}_\ell$ définis par les doublets d'éléments $a <_d b$ de $\mathcal{A}$. Cette famille est fermée pour l'intersection. On en extrait la famille $\mathfrak{P}_1, \dots, \mathfrak{P}_k$ des pavés minimaux pour l'inclusion. Ces pavés sont disjoints. Chacun de ces $\mathfrak{P}_i$ $(i \leq k)$ est soit inclus dans C_d, soit inclus dans le complémentaire de C_d ; si un pavé $\mathfrak{P}$ n'est pas inclus dans A, mais que pour tout i, $\pi_i(\mathfrak{P}) \subseteq \pi_i(A)$, alors $\mathfrak{P} \subseteq C_d$. D'autre part C_d est l'union des $\mathfrak{P}_i$ qui le coupent, ce qui permet de calculer ψ_d qui est le cardinal de C_d.

Exemples En dimension 2 et 3 on peut faire quelques dessins.

La figure 1 représente $A = \langle (2,7), (4,5), (6,4), (9,2) \rangle_{\mathbf{T}}$.

Les points noircis sont bien entendu les éléments de A. On lit facilement $\Psi_2(A) = (4, 22)$: pour « compléter » A de façon à obtenir $\mathbb{N}^2$, il faut lui ajouter 4 « droites » et 22 points. Il est très clair que si $B \supseteq A$, alors soit B coupe (au moins) une des 4 droites en question, soit B contient (au moins) un des 22 points ; si $\psi_2(B) = (\psi_1, \psi_2)$, ceci signifie que soit $\psi_1 < 4$, soit $\psi_2 < 22$, c'est-à-dire $\Psi_2(B) \leq_{\text{lex}} \Psi_2(A)$.

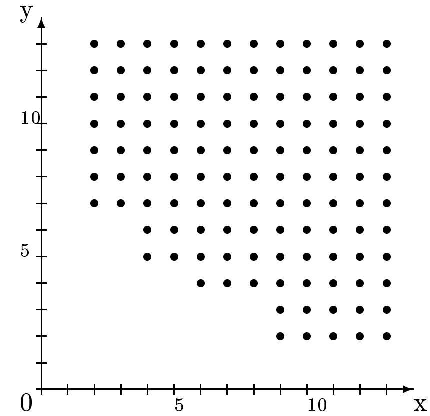


Figure 1 : Un idéal monomial pour $d = 2$.

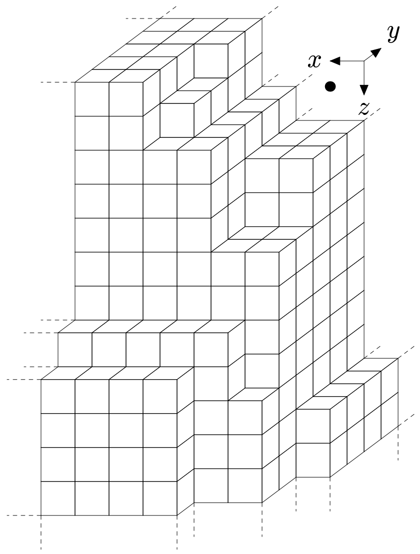


Figure 2 : Un idéal monomial pour $d = 3$.

La figure 2 représente une partie terminale A de $\mathbb{N}^3$. Le petit disque marque l'origine de $\mathbb{N}^3$; les axes ne sont pas dessinés pour des raisons de lisibilité, nous avons juste indiqué un trièdre direct. L'orientation est inhabituelle, c'est encore pour améliorer la lisibilité. Voici la liste des 10 points qui engendrent A, classés par coordonnées en z croissantes :

$$\begin{aligned} \mathrm{A} = \langle &(6,7,1),\ (7,4,1),\ (6,5,2),\ (5,4,3),\ \ (3,6,4), \\ &(3,4,6),\ (4,3,8),\ (5,2,9),\ (3,3,10),\ (2,6,11)\rangle_{\mathbf{T}} \end{aligned}$$

Ils correspondent aux 20 « sommets saillants » du dessin. Les cubes représentés sont ceux dont les 8 sommets sont dans A. Il est facile de lire sur la liste des coordonnées qu'il faut d'abord ajouter à A 5 « plans » pour pouvoir ensuite le compléter par des droites et des points en $\mathbb{N}^3$. En lisant sur le dessin, on trouve qu'il faut encore ajouter 35 « droites » (15 parallèles à l'axe des x, 15 à l'axe des y, 5 à l'axe des z) et 14 points. On a $\Psi_3(\mathrm{A}) = (5, 35, 14)$.

À nouveau l'isomorphisme d'ordre entre $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$ et $(\mathbf{T}^\circ(\mathbb{N}^d), \subseteq)$ permet de reformuler cette proposition comme suit :

Proposition 39 $(\mathcal{IM}_{\mathbb{A}}, \subseteq)$ *est fortement noethérien.*

Le lemme 17, qui donne un morphisme d'ordre strict entre $\mathcal{I}_{\mathbb{A}}$ et $\mathcal{IM}_{\mathbb{A}}$, permet d'énoncer le théorème suivant :

Théorème 40 *L'anneau* $\mathbb{A} = \mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ *est fortement noethérien.*

4.2 Anneaux de polynômes sur un anneau

Théorème de transfert

Définition Un anneau $\mathbb{A}$ est *fortement cohérent* si il est cohérent et fortement discret.

Nous allons utiliser plusieurs résultats issus de [MRR] : la proposition 41 est issue de III.2.5 & III.2.7, la proposition 45 est issue de VIII.1.2 & VIII.1.5, et le lemme 46 est le lemme VIII.1.4.

Proposition 41 *Soit* M *un* $\mathbb{A}$*-module et* N *un sous* $\mathbb{A}$*-module de type fini de* M*. Alors* M *est (fortement) cohérent si et seulement si* N *et* M/N *sont (fortement) cohérents.*

Si M est un $\mathbb{A}$-module de type fini, on note $\mathcal{I}_{\mathrm{M}}$ l'ensemble des sous $\mathbb{A}$-modules de type fini de M. On dira que M est *fortement noethérien* si $(\mathcal{I}_{\mathrm{M}}, \subseteq)$ est fortement noethérien.

Lemme 42 *Soit* $\mathbb{A}$ *un anneau cohérent. Soit* M *un* $\mathbb{A}$*-module et* N *un sous* $\mathbb{A}$*-module de* M*. Il existe une application strictement croissante de* $\mathcal{I}_{\mathrm{M}}$ *dans* $\mathcal{I}_{\mathrm{M/N}} \times \mathcal{I}_{\mathrm{N}}$ *(ordonné par l'ordre produit).*

Démonstration Soit

$$\begin{array}{cccc} \psi : & \mathcal{I}_{\mathrm{M}} & \longrightarrow & \mathcal{I}_{\mathrm{M/N}} \times \mathcal{I}_{\mathrm{N}} \\ & \mathrm{A} & \mapsto & (\mathrm{A/N}, \mathrm{A} \cap \mathrm{N}). \end{array}$$

Cette application est bien définie car M est cohérent. On ordonne $\mathcal{I}_{\mathrm{M/N}} \times \mathcal{I}_{\mathrm{N}}$ par l'ordre produit des ordres $\subseteq$. Alors Ψ est une application strictement croissante : d'une part en effet si $\mathrm{A} \subseteq \mathrm{B}$ alors $\mathrm{A/N} \subseteq \mathrm{B/N}$ et $\mathrm{A} \cap \mathrm{N} \subseteq \mathrm{B} \cap \mathrm{N}$. D'autre part supposons que $\mathrm{A} \subseteq \mathrm{B}$, $\mathrm{A/N} = \mathrm{B/N}$ et $\mathrm{A} \cap \mathrm{N} = \mathrm{B} \cap \mathrm{N}$. Soit $b \in \mathrm{B}$. Il existe $a \in \mathrm{A}$ tel que $a + \mathrm{N} = b + \mathrm{N}$, et donc $b - a \in \mathrm{B} \cap \mathrm{N} = \mathrm{A} \cap \mathrm{N}$. Donc $b - a \in \mathrm{A}$ et $b \in \mathrm{A}$; on a $\mathrm{A} = \mathrm{B}$. □

Proposition 43 *Soit* $\mathbb{A}$ *un anneau cohérent. Soit* M *un* $\mathbb{A}$*-module et* N *un sous* $\mathbb{A}$*-module de* M*.*

- $(\mathcal{I}_{\mathrm{M}}, \supseteq)$ *est bien fondé si et seulement si* $\mathcal{I}_{\mathrm{N}}$ *et* $\mathcal{I}_{\mathrm{M/N}}$ *sont bien fondés (pour l'ordre* $\supseteq$*) ;*
- M *est fortement noethérien si et seulement si* N *et* M/N *sont fortement noethériens.*

Démonstration – Il est facile de trouver une application strictement croissante de $\mathcal{I}_{\mathrm{N}}$ dans $\mathcal{I}_{\mathrm{M}}$ et de $\mathcal{I}_{\mathrm{M/N}}$ dans $\mathcal{I}_{\mathrm{M}}$. Si $\mathcal{I}_{\mathrm{M}}$ est bien fondé, le lemme 31 montre alors que $\mathcal{I}_{\mathrm{N}}$ et $\mathcal{I}_{\mathrm{M/N}}$ sont bien fondés. Réciproquement, si $\mathcal{I}_{\mathrm{N}}$ et $\mathcal{I}_{\mathrm{M/N}}$ sont bien fondés, le lemme 30 montre que $\mathcal{I}_{\mathrm{N}} \times \mathcal{I}_{\mathrm{M/N}}$ est bien fondé, et l'application strictement croissante du lemme précédent permet à nouveau de conclure ;

– soient $\phi_1 : \mathcal{I}_{\mathrm{M/N}} \longrightarrow \mathcal{E}_1$ et $\phi_2 : \mathcal{I}_{\mathrm{N}} \longrightarrow \mathcal{E}_2$. Les ensembles $(\mathcal{E}_1, \leq_1)$ et $(\mathcal{E}_2, \leq_2)$ sont bien ordonnés.

Soit
$$\begin{array}{cccc} \Psi & : & \mathcal{I}_{\mathrm{M}} & \longrightarrow & \mathcal{E}_1 \times \mathcal{E}_2 \\ & & \mathrm{A} & \mapsto & \big(\phi_1(\mathrm{A/N}), \phi_2(\mathrm{A} \cap \mathrm{N})\big) . \end{array}$$

On ordonne $\mathcal{E}_1 \times \mathcal{E}_2$ par l'ordre lexicographique $\leq_{\mathrm{lex}}$. Alors $\Psi : (\mathcal{I}_{\mathrm{M}}, \subseteq) \longrightarrow (\mathcal{E}_1 \times \mathcal{E}_2, \leq_{\mathrm{lex}})$ est une application strictement décroissante vers un ensemble bien ordonné (lemme 34).

Nous laissons l'autre implication à la lectrice et au lecteur. □

On en déduit par récurrence le corollaire suivant :

Corollaire 44 *Soit $\mathbb{A}$ un anneau (fortement) cohérent. Soit $n \in \mathbb{N}$; le $\mathbb{A}$-module libre $\mathbb{A}^n$ est (fortement) cohérent. De plus :*

- *Si $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé, $(\mathcal{I}_{\mathbb{A}^n}, \supseteq)$ est bien fondé.*
- *Si $\mathbb{A}$ est un anneau fortement noethérien, $\mathbb{A}^n$ est un $\mathbb{A}$-module fortement noethérien.*

Soit $n \in \mathbb{N}$. On note $\mathbb{A}[x]_n$ l'ensemble des polynômes de degré $< n$. C'est un $\mathbb{A}$-module libre de dimension n.

Proposition 45 *L'anneau $\mathbb{A}$ est (fortement) cohérent et noethérien.*

- *Soit $\mathrm{I} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$. Alors $\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_n$ est un $\mathbb{A}$-module de type fini ;*
- *L'anneau $\mathbb{A}[\mathrm{X}]$ est (fortement) cohérent.*

Si $\mathbb{A}$ est cohérent et noethérien, soit $\mathrm{I} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$. On pose

$$\textsc{lc}(\mathrm{I}) = \{a \in \mathbb{A} \, : \, \exists n, a_0, \ldots, a_{n-1}, \; a \cdot \mathrm{X}^n + a_{n-1} \cdot \mathrm{X}^{n-1} + \cdots + a_0 \in \mathrm{I}\} .$$

Lemme 46 *Si $\mathbb{A}$ est cohérent et noethérien, alors pour tout $\mathrm{I} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$, $\textsc{lc}(\mathrm{I})$ est de type fini. Si $\mathrm{I} \subseteq \mathrm{J}$ et $\textsc{lc}(\mathrm{I}) = \textsc{lc}(\mathrm{J})$, alors*

$$\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_n \textit{ engendre } \mathrm{I} \textit{ comme idéal} \Longrightarrow \mathrm{J} \cap \mathbb{A}[\mathrm{X}]_n \textit{ engendre } \mathrm{J}.$$

Définition Si $\mathbb{A}$ est fortement cohérent et noethérien, on peut définir, pour tout $\mathrm{I} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$, l'entier $n(\mathrm{I})$ tel que $\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{I})}$ engendre I, et tel que c'est le plus petit entier qui a cette propriété. D'une part, $n(\mathrm{I})$ est plus petit que le degré maximal des générateurs $(f_1, \ldots, f_s)$ de I ; d'autre part, pour savoir si $n \geq n(\mathrm{I})$, on calcule les générateurs de $\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_n$ et on teste si les f_i appartiennent à l'idéal qu'ils engendrent. C'est ici qu'on a réellement besoin de l'hypothèse de cohérence forte.

Le deuxième point du lemme précédent se relit ainsi :

Lemme 47 *Soit $\mathbb{A}$ fortement cohérent et noethérien. Soient* $\mathrm{I}, \mathrm{J} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$. *Si* $\mathrm{I} \subseteq \mathrm{J}$ *et* $\mathrm{LC}(\mathrm{I}) = \mathrm{LC}(\mathrm{J})$, *alors* $n(\mathrm{I}) \geq n(\mathrm{J})$.

Définition Soit $(\mathcal{E}_i, \leq_i)_{i \in \mathbb{N}}$ une famille d'ensembles ordonnés indexée par $\mathbb{N}$. On note $\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i$ (resp. $\overleftarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i$) l'union disjointe des $\mathcal{E}_i$ ordonnée par

$$x \in \mathcal{E}_i \preceq y \in \mathcal{E}_j \iff \begin{cases} i < j \text{ (resp. } j < i). \\ i = j \wedge x \leq_i y\,. \end{cases}$$

La définition la plus naturelle est celle de $\overrightarrow{\bigoplus} \mathcal{E}_i$; la distinction n'est pas essentielle, car si $(\mathcal{E}'_i, \leq'_i) = (\mathcal{E}_i, \geq_i)$, on a $(\overrightarrow{\bigoplus} \mathcal{E}'_i, \preceq) = (\overleftarrow{\bigoplus} \mathcal{E}_i, \succeq)$. C'est ce qui a motivé la deuxième définition qui va s'appliquer à des ensembles $(\mathcal{E}_i, \leq_i)$ tels que c'est $(\mathcal{E}_i, \geq_i)$ qui est bien fondé.

Lemme 48 *Si les ensembles $(\mathcal{E}_i, \leq_i)_{i\in\mathbb{N}}$ sont bien fondés (resp. bien ordonnés), l'ensemble $(\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i, \preceq)$ est bien fondé (resp. bien ordonné).*

Démonstration Nous faisons la preuve dans le cas « bien fondé » ; elle est bien entendu valide dans le cas « bien ordonné », mais on pourrait préférer, dans ce dernier cas, une preuve qui ressemble (encore) plus à une récurrence classique.

Soit H une partie héréditaire de $(\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i, \preceq)$. Soit $\mathcal{H}_0 = \mathrm{H} \cap \mathcal{E}_0$ (on considère que les $\mathcal{E}_i$ sont inclus dans leur union disjointe). Alors $\mathcal{H}_0$ est une partie héréditaire de $\mathcal{E}_0$: soit $x \in \mathcal{E}_0$ tel que tout $x' \in \mathcal{E}_0$ qui vérifie $x' <_0 x$ est dans $\mathcal{H}_0$. Tout $y \in \overrightarrow{\bigoplus} \mathcal{E}_i$ tel que $y < x$ est dans $\mathcal{E}_0$, donc dans $\mathcal{H}_0 \subseteq \mathrm{H}$; on en déduit, par l'hérédité de H, que $x \in \mathrm{H}$ et donc $x \in \mathcal{H}_0$. $\mathcal{H}_0$ est bien une partie héréditaire ; on a donc $\mathcal{H}_0 = \mathcal{E}_0$.

Soit maintenant $\mathcal{H}_1 = \mathrm{H} \cap \mathcal{E}_1$. Montrons que $\mathcal{H}_1$ est héréditaire. Soit $x \in \mathcal{E}_1$ tel que tout $x' <_1 x$ est dans $\mathcal{H}_1$. Soit $y \in \overrightarrow{\bigoplus} \mathcal{E}_i$, $y < x$. Alors $y \in \mathcal{E}_0$ ou $y \in \mathcal{E}_1$; dans le premier cas, comme $\mathcal{E}_0 = \mathcal{H}_0$, $y \in \mathrm{H}$ et dans le deuxième cas, $y <_1 x$ et donc $y \in \mathcal{H}_1 \subseteq \mathrm{H}$. Par hérédité de H, on a $x \in \mathrm{H}$ et donc $x \in \mathcal{H}_1$. $\mathcal{H}_1$ est héréditaire ; on a $\mathcal{H}_1 = \mathcal{E}_1$.

On a par récurrence : $\forall i$, $\mathrm{H} \cap \mathcal{E}_i = \mathcal{E}_i$. Donc $\mathrm{H} = \overrightarrow{\bigoplus} \mathcal{E}_i$. □

Corollaire 49 *Soit $\mathbb{A}$ un anneau cohérent.*
- *Si $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé, alors $(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \succeq)$ est bien fondé ;*
- *si $\mathbb{A}$ est fortement noethérien, alors $(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \preceq)$ est fortement noethérien.*

Démonstration Le premier point est clair : si $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé, alors chacun des $(\mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \supseteq)$ est bien fondé (corollaire 44), et on applique le lemme précédent.

Pour le second point. Si on dispose d'applications strictement décroissantes

$$\begin{array}{rlcl} \phi_1 : & \mathcal{I}_{\mathbb{A}[\mathrm{X}]_1} & \longrightarrow & \mathcal{E}_1 \\ \phi_2 : & \mathcal{I}_{\mathbb{A}[\mathrm{X}]_2} & \longrightarrow & \mathcal{E}_2 \\ \vdots & & & \end{array}$$

vers des ensembles bien ordonnés $\mathcal{E}_0, \mathcal{E}_1, \ldots$ On peut définir

$$\begin{array}{rccc} \Phi \ : & \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n} & \longrightarrow & \overrightarrow{\bigoplus_{n\geq 1}} \mathcal{E}_n \\ & \mathrm{M} \subseteq \mathbb{A}[\mathrm{X}]_n & \mapsto & \phi_n(\mathrm{M}). \end{array}$$

C'est une application strictement décroissante de $(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \preceq)$ vers l'ensemble bien ordonné $(\overrightarrow{\bigoplus_{n\geq 1}} \mathcal{E}_n, \preceq)$. □

Soit Θ l'application suivante :

$$\begin{array}{rccc} \Theta \ : & \mathcal{I}_{\mathbb{A}[\mathrm{X}]} & \longrightarrow & \mathcal{I}_{\mathbb{A}} \times \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n} \\ & \mathrm{I} & \mapsto & \big(\textsc{lc}(\mathrm{I}), \mathrm{I} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{I})}\big) \ . \end{array}$$

C'est une application strictement croissante (en ordonnant l'ensemble d'arrivée par l'ordre lexicographique). En effet si $\mathrm{I} \subsetneq \mathrm{J}$ alors $\textsc{lc}(\mathrm{I}) \subseteq \textsc{lc}(\mathrm{J})$; et si $\textsc{lc}(\mathrm{I}) = \textsc{lc}(\mathrm{J})$, alors soit $n(\mathrm{I}) < n(\mathrm{J})$, soit $n(\mathrm{I}) = n(\mathrm{J})$ et dans ce cas

$$\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{I})} \subseteq \mathrm{J} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{J})}.$$

D'autre part si $\mathrm{I} \subseteq \mathrm{J}$, $\textsc{lc}(\mathrm{I}) = \textsc{lc}(\mathrm{J})$, $n(\mathrm{I}) = n(\mathrm{J})$ et $\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{I})} = \mathrm{J} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{J})}$, ces deux derniers sous-modules engendrant respectivement I et J comme idéal, on a $\mathrm{I} = \mathrm{J}$.

On peut maintenant énoncer le théorème suivant :

Théorème 50 *Soit $\mathbb{A}$ un anneau fortement cohérent. Alors :*
- *si $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé, $(\mathcal{I}_{\mathbb{A}[\mathrm{X}]}, \supseteq)$ est bien fondé ;*
- *si $\mathbb{A}$ est fortement noethérien, $\mathbb{A}[\mathrm{X}]$ est fortement noethérien.*

Dans les ceux cas, $\mathbb{A}[\mathrm{X}]$ est fortement cohérent.

Démonstration Pour le premier point, on a presque tout dit : si $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé, il en est de même de $(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \succeq)$ et donc de $(\mathcal{I}_{\mathbb{A}} \times \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n}, \geq_{\mathrm{lex}})$. L'application strictement croissante et le lemme 31 permettent de conclure.

Pour le deuxième point, si $\mathbb{A}$ est fortement noethérien, on dispose d'une application strictement croissante $\phi : \mathcal{I}_{\mathbb{A}} \longrightarrow \mathcal{E}$ où $\mathcal{E}$ est bien fondé ; et, d'après le corollaire précédent, d'une application strictement croissante

$$\Phi : \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{\mathbb{A}[\mathrm{X}]_n} \longrightarrow \mathcal{F}.$$

L'ensemble $\mathcal{F}$ est bien fondé. On peut composer Θ avec $\phi \times \Phi$, comme suit :

$$\begin{array}{rccc} \Psi & : & \mathcal{I}_{\mathbb{A}[\mathrm{X}]} & \longrightarrow & \mathcal{E} \times \mathcal{F} \\ & & \mathrm{I} & \mapsto & \big(\phi(\textsc{lc}(\mathrm{I})), \Phi(\mathrm{I} \cap \mathbb{A}[\mathrm{X}]_{n(\mathrm{I})})\big) \end{array} .$$

On ordonne $\mathcal{E} \times \mathcal{F}$ par l'ordre lexicographique. Ψ est une application strictement croissante de $(\mathcal{I}_{\mathbb{A}[\mathrm{X}]}, \supseteq)$ vers $(\mathcal{E} \times \mathcal{F}, \leq_{\mathrm{lex}})$ qui est un ensemble bien ordonné. □

Quelques commentaires

On aurait pu ajouter à notre exposé le cas où $\mathbb{A}$ est noethérien et fortement cohérent, et montrer que ces propriétés se transfèrent à $\mathbb{A}[\mathrm{X}]$ grâce à cette même application strictement croissante, mais cela ne nous a pas semblé nécessaire.

Le premier point du théorème 50 est celui prouvé par Jacobson et Löfwall dans [JL]. À cette fin, ils utilisaient des bases de Gröbner pour des polynômes à coefficients dans un anneau. Il serait très intéressant de comparer ces bases à celles définies dans [AL], et de voir si ce qui est fait n'est pas au bout du compte équivalent aux calculs associés implicitement aux preuves constructives de Richman et Seidenberg.

En effet, il est possible de calculer des bases de Gröbner à l'aide des algorithmes sous-jacents aux preuves de Richman ; esquissons-en le principe. Le lemme 46 indique en effet que si $\mathrm{I} \in \mathcal{I}_{\mathbb{A}[\mathrm{X}]}$, l'idéal $\textsc{lc}(\mathrm{I})$ est de type fini. On peut donc en calculer une famille génératrice $a_1, \ldots, a_s$, et pour tout i on a un polynôme $f_i \in \mathbb{A}[\mathrm{X}]$ dont a_i est le coefficient dominant. Alors la famille $(f_1, \ldots, f_s)$ est une base de Gröbner. On peut faire la même chose dans l'anneau $\mathbb{A}[\mathrm{X}, \mathrm{Y}]$ en le considérant comme un anneau de polynômes en X à coefficients dans $\mathbb{A}[\mathrm{Y}]$: on obtient une base de Gröbner pour l'ordre lexicographique.

Les bases de Gröbner seraient peut-être préférables pour la forme car elles permettent d'ajouter n indéterminées en une seule fois (au lieu de le faire par récurrence finie, une indéterminée après l'autre). Il reste de plus très possible que les algorithmes de calculs de base de Gröbner présentés dans [JL] et [AL] soient réellement conceptuellement différents, et permettent de fournir une preuve constructive plus performante.

Un cas particulier

Corollaire 51 *L'anneau $\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$ est fortement noethérien et fortement cohérent.*

Si on suit la preuve, la taille de l'ensemble bien ordonné qui certifie la forte noethérianité augmente fortement à chaque étape. De plus la structure de l'ensemble se complique. Cependant, dans certains cas particuliers, il est possible d'exprimer des choses plus simples.

Lemme 52 *Soient $k, d \in \mathbb{N}$; soit $(\mathrm{E}, \leq) = (\mathbb{N}^k, \leq_{\mathrm{lex}})$. Alors il existe une application strictement croissante de $(\mathrm{E}^d, \leq_d)$ (ordonné par l'ordre produit) vers $(\mathrm{E}, \leq)$.*

Démonstration Fred Richman, un des rapporteurs de cette thèse, m'a fait remarquer que la preuve que je proposais pour ce lemme était inutilement compliquée. Je l'ai laissée ci-dessous en petits caractères ; voici la preuve proposée par Fred Richman, traduite en français.

– Il suffit clairement de prouver le lemme dans le cas $d = 2$; en effet, s'il y a une application strictement croissante de $(\mathrm{E}^d, \leq_d)$ vers $(\mathrm{E}, \leq)$, il y en a un de $(\mathrm{E}^{d+1}, \leq)$ vers $(\mathrm{E}^2, \leq_2)$, et on conclut par récurrence.

– Considérons la classe des ensembles ordonnés α tels qu'il existe une application strictement croissante de $\alpha \times \alpha$ vers α. Cette classe est close pour le produit lexicographique : notons $\alpha\beta$ le produit lexicographique de α et β, et le produit ordinaire $\alpha \times \beta$; l'application naturelle

$$\alpha\beta \times \gamma\delta \longrightarrow (\alpha \times \gamma)(\beta \times \delta)$$

est une application strictement croissante. Ainsi on obtient une application strictement croissante

$$\alpha\beta \times \alpha\beta \longrightarrow (\alpha \times \alpha)(\beta \times \beta),$$

et donc de $\alpha\beta \times \alpha\beta$ dans $\alpha\beta$.

Il suffit d'exhiber une application strictement croissante de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$ (*cf.* ci-dessous, dans la preuve en petits caractères) pour conclure.

Voici maintenant la preuve que j'avais proposée.

Supposons tout d'abord que $d = 2$. On définit un ordre $\trianglelefteq$ sur $\mathrm{E} \times \mathrm{E} = \mathbb{N}^{2k}$:

$$(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}) \trianglelefteq (b_1, \ldots, b_k, b_{k+1}, \ldots, b_{2k})$$

$$\Longleftrightarrow$$

$$\begin{cases} (a_1 + a_{k+1}, \ldots, a_k + a_{2k}) <_{\mathrm{lex}} (b_1 + b_{k+1}, \ldots, b_k + b_{2k}) \\ \text{ou} \begin{cases} (a_1 + a_{k+1}, \ldots, a_k + a_{2k}) = (b_1 + b_{k+1}, \ldots, b_k + b_{2k}) \\ \text{et} \\ (a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}) \leq_{\mathrm{lex}} (b_1, \ldots, b_k, b_{k+1}, \ldots, b_{2k}). \end{cases} \end{cases}$$

L'identité est une application strictement croissante entre $(\mathrm{E}^2, \leq_2)$ et $(\mathrm{E}^2, \trianglelefteq)$. En effet

$$(a_1, \ldots, a_k, a_{k+1}, \ldots, a_{2k}) \leq_2 (b_1, \ldots, b_k, b_{k+1}, \ldots, b_{2k})$$

$$\Longrightarrow \begin{cases} (a_1, \ldots, a_k) \leq_{\mathrm{lex}} (b_1, \ldots, b_k) \\ \text{et} \\ (a_{k+1}, \ldots, a_{2k}) \leq_{\mathrm{lex}} (b_{k+1}, \ldots, b_{2k}) \end{cases}$$

Si $(a_1, \ldots, a_{2k}) <_2 (b_1, \ldots, b_{2k})$, une des deux inégalités pour $\leq_{\mathrm{lex}}$ ci-dessus est stricte, et dans ce cas on a

$$(a_1 + a_{k+1}, \ldots, a_k + a_{2k}) <_{\mathrm{lex}} (b_1 + b_{k+1}, \ldots, b_k + b_{2k}).$$

Ouvrons une parenthèse sur le cas où $k = 1$. Dans ce cas, l'ordre $\trianglelefteq$ est l'ordre gradué $\leq_{\mathrm{deglex}}$ donné dans les exemples de la première section. Il est facile de voir qu'il y a un isomorphisme d'ordre entre $(\mathbb{N}, \leq_{\mathrm{lex}}) = (\mathbb{N}, \leq)$ et $(\mathbb{N}^2, \leq_{\mathrm{deglex}})$: on peut en effet énumérer les éléments de $\mathbb{N}^2$ dans l'ordre croissant pour $\leq_{\mathrm{deglex}} = \trianglelefteq$, comme suit.

$$\begin{array}{ccccccccccccc} (0,0) & \triangleleft & (0,1) & \triangleleft & (1,0) & \triangleleft & (0,2) & \triangleleft & (1,1) & \triangleleft & (2,0) & \triangleleft & \\ (0,3) & \triangleleft & (1,2) & \triangleleft & (2,1) & \triangleleft & (3,0) & \triangleleft & (0,4) & \triangleleft & (1,3) & \triangleleft & \ldots \end{array}$$

Il suffit alors de considérer l'application suivante :

$$\begin{array}{ccc}
\mathbb{N} & \longrightarrow & \mathbb{N}^2 \\
0 & \mapsto & (0,0) \\
 & & \\
1 & \mapsto & (0,1) \\
2 & \mapsto & (1,0) \\
 & & \\
3 & \mapsto & (0,2) \\
4 & \mapsto & (1,1) \\
5 & \mapsto & (2,0) \\
\vdots & & \vdots \\
\dfrac{n(n+1)}{2} & \mapsto & (0,n) \\
\dfrac{n(n+1)}{2}+1 & \mapsto & (1,n-1) \\
\vdots & & \vdots
\end{array}$$

C'est bien un isomorphisme d'ordre.

Ceci se généralise à k quelconque : écrivons-le pour $k=2$, en espérant convaincre le lecteur que le cas général n'est pas plus difficile.

Pour chaque $(x,y) \in \mathrm{E} = \mathbb{N}^2$, on peut énumérer dans l'ordre croissant les éléments $[(a,b),(a',b')]$ de $\mathrm{E} \times \mathrm{E}$ tels que $(a+a',b+b') = (x,y)$; ils sont en nombre fini. En faisant cette énumération « dans l'ordre croissant des (x,y) » on obtient l'isomorphisme désiré.

$$\begin{array}{cccccc}
\mathrm{E} & \longrightarrow & \mathrm{E}\times\mathrm{E} & & & \\
 & & & & & \\
(0,0) & \mapsto & [(0,0),(0,0)] & (1,0) & \mapsto & [(0,0),(1,0)] \\
 & & & (1,1) & \mapsto & [(1,0),(0,0)] \\
(0,1) & \mapsto & [(0,0),(0,1)] & & & \\
(0,2) & \mapsto & [(0,1),(0,0)] & (1,2) & \mapsto & [(0,0),(1,1)] \\
 & & & (1,3) & \mapsto & [(0,1),(1,0)] \\
(0,3) & \mapsto & [(0,0),(0,2)] & (1,4) & \mapsto & [(1,0),(0,1)] \\
(0,4) & \mapsto & [(0,1),(0,1)] & (1,5) & \mapsto & [(1,1),(0,0)] \\
(0,5) & \mapsto & [(0,2),(0,0)] & & & \\
 & & & (1,6) & \mapsto & [(0,0),(1,2)] \\
(0,6) & \mapsto & [(0,0),(0,3)] & (1,7) & \mapsto & [(0,1),(1,1)] \\
(0,7) & \mapsto & [(0,1),(0,2)] & (1,8) & \mapsto & [(0,2),(1,0)] \\
(0,8) & \mapsto & [(0,2),(0,1)] & (1,9) & \mapsto & [(1,0),(0,2)] \\
(0,9) & \mapsto & [(0,3),(0,0)] & (1,10) & \mapsto & [(1,1),(0,1)] \\
 & & & (1,11) & \mapsto & [(1,2),(0,0)] \\
\vdots & & \vdots & \vdots & & \vdots
\end{array}$$

Nous avons fait apparaître des blocs qui correspondent aux énumérations finies des $[(a,b),(a',b')]$ de $\mathrm{E}\times\mathrm{E}$ à $(a+a',b+b')$ constant.

Le cas $d=2$, k quelconque fonctionne de la même manière. Pour le cas d quelconque il faut remplacer les sommes

$$(a_1,\ldots,a_{2k}) \mapsto (a_1+a_{k+1},\ldots,a_k+a_{2k})$$

par des sommes

$$(a_1,\ldots,a_{dk}) \mapsto (a_1+a_{k+1}+\cdots+a_{(d-1)k+1},\ldots,a_k+a_{2k}+\cdots+a_{dk})$$

La démarche reste la même, espérons que la lectrice est convaincue. $\square$

Remarque Ce lemme peut être vu comme un résultat concernant certains ordinaux, les ω^k ; il peut sans doute être étendu à d'autres ordinaux.

Lemme 53 *Soit* $\mathbb{A}$ *un anneau et* ϕ *une application strictement croissante de* $\mathcal{I}_{\mathbb{A}}$ *vers* $\mathrm{E} = \mathbb{N}^k$ *ordonné lexicographiquement. Alors il existe une application strictement croissante de* $\mathcal{I}_{\mathbb{A}^n}$ *vers* $(\mathbb{N}^k, \leq_{\mathrm{lex}})$.

Démonstration La preuve que nous avons donnée fourni une application strictement croissante vers $(\mathrm{E}^n, \leq_n)$; il suffit d'appliquer le lemme précédent. □

Lemme 54 *Si pour tout* i, $(\mathcal{E}_i, \leq_i) = (\mathbb{N}^k, \leq_{\mathrm{lex}})$, *alors il a un isomorphisme d'ordre entre* $(\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i, \preceq)$ *et* $(\mathbb{N}^{k+1}, \leq_{\mathrm{lex}})$.

Démonstration On envoie $(a_0, a_1, \ldots, a_k) \in \mathbb{N}^{k+1}$ sur $(a_1, \ldots, a_k) \in \mathcal{E}_{a_0} \subseteq \overrightarrow{\bigoplus} \mathcal{E}_i$. □

Le corollaire suivant est alors clair, au vu de la preuve du théorème 50.

Corollaire 55 *Soit* $\mathbb{A}$ *un anneau et* ϕ *une application strictement croissante de* $\mathcal{I}_{\mathbb{A}}$ *vers* $\mathrm{E} = \mathbb{N}^k$ *ordonné lexicographiquement. Alors il existe un morphisme d'ordre strict de* $(\mathcal{I}_{\mathbb{A}[\mathrm{X}]}, \supseteq)$ *vers* $(\mathbb{N}^{2k+1}, \leq_{\mathrm{lex}})$.

Proposition 56 *Soit* $\mathbb{A} = \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. *Il existe une application strictement croissante de* $(\mathcal{I}_{\mathbb{A}}, \supseteq)$ *vers* $(\mathbb{N}^k, \leq_{\mathrm{lex}})$, *où* $k = 2^{n+1} + 2^n - 1$.

Démonstration Pour $\mathbb{A} = \mathbb{Z}$, on a une application strictement croissante de $\mathcal{I}_{\mathbb{A}}$ vers $\mathbb{N} \cup \{+\infty\}$ et il est donc facile d'en construire une de $\mathcal{I}_{\mathbb{A}}$ vers $(\mathbb{N}^2, \leq_{\mathrm{lex}})$. On applique ensuite le résultat précédent récursivement. □

Remarque On peut voir le plus petit ordinal α associé à un ensemble bien fondé E (dans le sens où il existe une application strictement croissante de E dans α) comme «mesurant la complexité de E» ; ce que nous venons de faire pour $\mathbb{A} = \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, dans cette optique, revient à donner une borne à la complexité de $(\mathcal{I}_{\mathbb{A}}, \supseteq)$. Nous avons réussi à donner une borne meilleure que celle fournie par la preuve du théorème 50 ; mais rien ne dit qu'elle est optimale. Il est probable que cette manière de voir les ensembles bien fondés a déjà été utilisée ailleurs, mais nous n'avons pas trouvé de référence.

4.3 Un petit bilan

En mettant de côté la notion d'arbres croissants qui est un peu à part (de par son côté «les suites sont finies»), on a utilisé trois notions de noethérianité qui sont, par ordre décroissant de force :

$\mathbb{A}$ est fortement noethérien.
$(\mathcal{I}_{\mathbb{A}}, \supseteq)$ est bien fondé.
$\mathbb{A}$ est noethérien.

Pour les deux conditions les plus fortes, nous avons montré un théorème de transfert de $\mathbb{A}$ à $\mathbb{A}[\mathrm{X}]$ sous l'hypothèse additionnelle de forte cohérence de $\mathbb{A}$.

Ceci était connu pour la seconde condition (*cf.* [JL]), cependant notre preuve est différente.

La notion la plus faible passe de $\mathbb{A}$ à $\mathbb{A}[X]$ (*cf.* [MRR]) avec seulement l'hypothèse de cohérence, ce qui est beaucoup plus spectaculaire. Il est cependant normal que nous ayons besoin de la forte cohérence pour des conditions où les inégalités strictes sont importantes. La question de savoir si les anneaux cohérents non fortement cohérents relèvent ou non du cas pathologique est un débat ouvert...

5 Longueur des suites croissantes d'idéaux

Une des caractéristiques des preuves constructives est qu'elles permettent de calculer des bornes ; dans ce cas précis, nous avons même la chance de pouvoir calculer des bornes optimales. Nous allons en effet donner la longueur maximale d'une suite strictement croissante d'idéaux monomiaux, sous certaines conditions.

Dans [S$_2$], Abraham Seidenberg a montré constructivement l'existence de telles bornes, sans toutefois les exhiber. Guillermo Moreno-Socìas a fait une étude de ce type, par des moyens différents, dans [M-S$_1$] et [M-S$_2$].

5.1 Suites décroissantes pour l'ordre lexicographique, première manière

On va s'intéresser ici à la longueur maximale des suites strictement décroissantes pour l'ordre lexicographique, telles que le degré des termes est donné par une fonction strictement croissante $f : \mathbb{N} \longrightarrow \mathbb{N}$. Plus précisément soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une application strictement croissante ; on cherche la longueur maximale ℓ d'une suite $u_1 >_{\text{lex}} u_2 >_{\text{lex}} u_3 >_{\text{lex}} \cdots >_{\text{lex}} u_\ell$ de $\mathbb{N}^d$ telle que $\deg u_k = f(k)$.

Exemple : dimension 2

Posons $d = 2$ et $f(k) = k + 2$; c'est-à-dire qu'on va s'intéresser aux suites de $\mathbb{N}^2$, strictement décroissantes pour l'ordre lexicographiques, dont le premier terme est de degré 3, et dont le degré augmente de 1 à chaque étape.

Si on commence par $u_1 = (0, 3)$, il n'est pas possible de trouver u_2 tel que $u_2 <_{\text{lex}} u_1$ et $\deg u_2 = 4$.

Si on commence par $u_1 = (1, 2)$, un terme de degré 4 qui soit $<_{\text{lex}}$ ne peut pas être de la forme $(1, \cdot)$, il faut donc prendre $u_2 = (0, 4)$, et c'est terminé.

En raisonnant de la même façon, on trouve deux autres suites :

$$(2,1) >_{\text{lex}} (1,3) >_{\text{lex}} (0,5)$$

et

$$(3,0) >_{\text{lex}} (2,2) >_{\text{lex}} (1,4) >_{\text{lex}} (0,6).$$

La plus longue est la dernière.

Exemple : dimension 3

Prenons maintenant $d = 3$, et $f(k) = k+1$. En suivant le même raisonnement il est facile de voir qu'il faut commencer par $u_1 = (2, 0, 0)$ pour obtenir la suite la plus longue ; on se retrouve avec $u_2 = (1, a, b)$ où (a, b) doit être de degré 2. le terme suivant sera (si possible) $u_3 = (1, a', b')$ avec $(a, b) >_{\mathrm{lex}} (a', b')$ et $\deg\,(a', b') = 3$. Pour pouvoir faire ça le plus longtemps possible il faut prendre $(a, b) = (2, 0)$. On trouve la suite suivante :

$$\begin{array}{lll}
u_1 = (2,0,0) & u_2 = (1,2,0) & u_5 = (0,6,0) \\
 & u_3 = (1,1,2) & u_6 = (0,5,2) \\
 & u_4 = (1,0,4) & u_7 = (0,4,4) \\
 & & u_8 = (0,3,6) \\
 & & u_9 = (0,2,8) \\
 & & u_{10} = (0,1,10) \\
 & & u_{11} = (0,0,12).
\end{array}$$

Le cas général

On va définir un entier $\ell(d, f)$ qui correspond à la longueur maximale ℓ d'une suite $u_1 >_{\mathrm{lex}} u_2 >_{\mathrm{lex}} u_3 >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} u_\ell$ de $\mathbb{N}^d$ telle que $\deg u_k = f(k)$.

Dimension 2 On prend $d = 2$, et f une fonction strictement croissante quelconque. Le même raisonnement qu'avec notre exemple conduit à la suite suivante :

$$\begin{array}{rrcl}
 & u_1 & = & \big(f(1)\,,\, 0 \big) \\
>_{\mathrm{lex}} & u_2 & = & \big(f(1)-1\,,\, f(2)-f(1)+1\big) \\
>_{\mathrm{lex}} & u_3 & = & \big(f(1)-2\,,\, f(3)-f(1)+2\big) \\
 & & \vdots & \\
>_{\mathrm{lex}} & u_{f(1)+1} & = & \big(0\,,\, f(f(1)+1) \big)
\end{array}$$

qui est de longueur $f(1) + 1$.

On pose donc $\ell(2, f) = f(1) + 1$.

Dimension d On suppose que $\ell(d-1, g)$ est défini, pour toute fonction g strictement croissante. On va voir comment définir $\ell(d, f)$.

Le raisonnement qui conduit à l'exemple donné en dimension 3 reste valable, f étant strictement croissante. Voici donc à quoi ressemble la suite de longueur maximale pour une fonction f donnée :

$$
\begin{array}{lll}
\text{degré} & \text{terme...} & \\
f(1) & u_1 & = (\ f(1),\quad 0\ ,\ldots,0\quad) \\
f(2) & u_2 & = (\ f(1)-1,\ v_1^1,\ldots,\ v_{d-1}^1) \\
f(3) & u_2 & = (\ f(1)-1,\ v_1^2,\ldots,\ v_{d-1}^2) \\
\vdots & \vdots & \qquad\qquad\qquad \vdots \\
f(\mathrm{N}_1) & u_{\ell_1} & = (\ f(1)-1,\ v_1^{\ell_1},\ldots,\ v_{d-1}^{\ell_1})
\end{array}
$$

Où la suite $v^1, v^2, \ldots$ de $\mathbb{N}^{d-1}$ est une suite strictement décroissante pour l'ordre lexicographique, dont les termes successifs sont de degré $f(2)-f(1)+1, f(3)-f(1)+1, \ldots$ On la choisit de longueur maximale $\ell_1 = \ell(d-1, g_1)$, où $g_1(k) = f(1+k)-f(1)+1$. On est alors arrivé, pour la suite u, au terme d'indice $\mathrm{N}_1 = 1 + \ell(d-1, g_1)$.

Voici comment continue notre suite :

$$
\begin{array}{lll}
f(\mathrm{N}_1+1) & u_{\mathrm{N}_1+1} & = (\ f(1)-2,\ w_1^1,\ldots,\ w_{d-1}^1) \\
\vdots & \vdots & \qquad\qquad\qquad \vdots \\
f(\mathrm{N}_2) & u_{\mathrm{N}_2} & = (\ f(1)-2,\ w_1^{\ell_2},\ldots,\ w_{d-1}^{\ell_2})
\end{array}
$$

Où la suite $w^1, w^2, \ldots$ de $\mathbb{N}^{d-1}$ est une suite strictement décroissante pour l'ordre lexicographique, dont les termes successifs sont de degré $f(\mathrm{N}_1+1)-f(1)+2, f(\mathrm{N}_1+2)-f(1)+2, \ldots$ On la choisit de longueur maximale $\ell_2 = \ell(d-1, g_2)$, où $g_2(k) = f(\mathrm{N}_1+k)-f(1)+2$. On est alors arrivé, pour la suite u, au terme d'indice $\mathrm{N}_2 = \mathrm{N}_1 + \ell(d-1, g_1)$.

On voit donc comment définir $\ell(d, f)$:

on pose $\mathrm{N}_0 = 1$, et pour tout $i > 0$,

$$\mathrm{N}_i = \mathrm{N}_{i-1} + \ell(d-1, g_i),$$

où
$$g_i(k) = f(\mathrm{N}_{i-1}+k) - f(1) + i.$$

On pose pour finir
$$\ell(d, f) = \mathrm{N}_{f(1)}.$$

Proposition 57 *Soit $f : \mathbb{N} \longrightarrow \mathbb{N}$ une fonction strictement croissante. L'entier $\ell(d, f)$ est la longueur maximale ℓ atteinte par les suites $u_1 >_{\mathrm{lex}} u_2 >_{\mathrm{lex}} \cdots >_{\mathrm{lex}} u_\ell$ de $\mathbb{N}^d$, telles que $\deg u_k = f(k)$.*

5.2 Suites décroissantes pour l'ordre lexicographique, deuxième manière

Si les termes de la suite $(u_i)_{i\in\mathbb{N}}$ sont fournis par un algorithme qui calcule u_{i+1} en fonction des termes précédents (et plus généralement d'un contexte qui évolue au fil du calcul), il est naturel d'imaginer que le degré de u_{i+1} puisse dépendre du degré des termes qui l'ont précédé. C'est la raison qui pousse à formuler les problèmes ci-dessous, en particulier le deuxième problème (le premier n'est qu'un cas particulier de ce qui précède).

Premier problème : Déterminer la longueur maximale des suites de $\mathbb{N}^d$ strictement décroissantes pour l'ordre lexicographique, telles que le degré des termes *est contrôlé par une fonction* $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$. Plus précisément, soit γ :

$\mathbb{N} \longrightarrow \mathbb{N}$ telle que $\gamma(k) > k$; on cherche la longueur maximale ℓ d'une suite $u_1 >_{\text{lex}} u_2 >_{\text{lex}} u_3 >_{\text{lex}} \cdots >_{\text{lex}} u_\ell$ telle que $\deg u_{i+1} = \gamma(\deg u_i)$ et $\deg u_1 = n$.

Deuxième problème : Déterminer la longueur maximale d'une suite $u_1 >_{\text{lex}} u_2 >_{\text{lex}} u_3 >_{\text{lex}} \cdots$ tel que $\deg u_i \leq \gamma(\max_{k<i}\{\deg u_k\})$.

Le premier problème :

Il s'agit d'un cas particulier de ce qui est traité à la section précédente ; il suffit de poser $f_n(k) = \gamma^{k-1}(n)$ (où la notation exponentielle est naturellement à comprendre comme itération de la composition). On prend donc $f_n(k) = \gamma^{k-1}(n)$ dans toute cette section.

La longueur maximale ℓ atteinte par une suite $u_1 >_{\text{lex}} u_2 >_{\text{lex}} \cdots >_{\text{lex}} u_\ell$ de $\mathbb{N}^d$ telle que $\deg u_{i+1} = \gamma(\deg u_i)$, est

$$\ell = \ell'(d, \gamma, n) = \ell(d, f_n)$$

Ainsi les exemples donnés en dimensions $d = 2$ et $d = 3$ correspondent à $\gamma(n) = n + 1$, avec pour valeur pour n respectivement 3 et 2. Nous allons les utiliser à nouveau, pour mieux comprendre ce qui se passe pour le **deuxième problème**.

Le deuxième problème, exemples

Nous savons donc régler le cas $\deg u_i = \gamma(\deg u_{i-1})$. Et si on veut $u_i \leq \gamma(\max_{k<i}\{\deg u_k\})$?

La dimension 2 Revenons au cas $d = 2$, avec $n = 3$ et $\gamma(i) = i + 1$.

Il est facile de voir qu'on peut intercaler des termes, comme ceci :

$$\begin{array}{lllllllllll}
 & (3,0) & >_{\text{lex}} & (2,2) & >_{\text{lex}} & (2,1) & >_{\text{lex}} & (2,0) & & \\
>_{\text{lex}} & (1,4) & >_{\text{lex}} & (1,3) & >_{\text{lex}} & (1,2) & >_{\text{lex}} & (1,1) & >_{\text{lex}} & (1,0) \\
>_{\text{lex}} & (0,6) & >_{\text{lex}} & (0,5) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (0,1) & >_{\text{lex}} & (0,0).
\end{array}$$

Le degré maximal atteint ne change pas. Cela est dû à la présence du $\max\{\deg u_k\}$; si on avait posé comme condition $\deg u_i \leq f(i)$ (ou $\deg u_i \leq \gamma^{i-1}(\deg u_1)$) cela n'aurait pas été le cas.

La condition que nous avons choisie est un contrôle du degré plus naturel dans l'hypothèse où la suite des u_i est produite par un algorithme : à chaque étape cet algorithme manipule les termes déjà calculés pour en produire un nouveau ; son analyse permettra sans doute de donner une fonction γ convenable, si sa preuve de terminaison est constructive.

La dimension 3 Ré-examinons l'exemple précédent pour $d = 3$. Voici comment s'intercalent les nouveaux termes :

$$\begin{array}{llllllllllll}
(2,0,0) & >_{\text{lex}} & (1,2,0) & >_{\text{lex}} & (1,1,2) & >_{\text{lex}} & (1,1,1) & >_{\text{lex}} & (1,1,0) & >_{\text{lex}} & & \\
(1,0,4) & >_{\text{lex}} & (1,0,3) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (1,0,0) & >_{\text{lex}} & & & & \\
(0,6,0) & >_{\text{lex}} & (0,5,2) & >_{\text{lex}} & (0,5,1) & >_{\text{lex}} & (0,5,0) & >_{\text{lex}} & \cdots & & & \\
(0,4,4) & >_{\text{lex}} & (0,4,3) & >_{\text{lex}} & & >_{\text{lex}} & (0,4,0) & >_{\text{lex}} & & & & \\
(0,3,6) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (0,3,0) & >_{\text{lex}} & (0,2,8) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (0,2,0) & >_{\text{lex}} \\
(0,1,10) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (0,1,0) & >_{\text{lex}} & (0,0,12) & >_{\text{lex}} & \cdots & >_{\text{lex}} & (0,0,0). &
\end{array}$$

On observe le même phénomène. Le nombre de termes intercallés est **la somme des dernières coordonnées des éléments de la suite du premier problème**. Ici c'est $0+0+2+4+0+2+4+6+8+10+12 = 48$, comme on peut le lire sur la liste complète des termes écrite plus haut.

Il est clair que ceci est vrai quelque soit la fonction γ choisie, et que cela ne depend pas non plus de la valeur de d. La description détaillée de la suite de longueur maximale du **premier problème** permet de décrire celle du **deuxième problème**.

Le cas général

On pose $f_n(k) = \gamma^{k-1}(n)$.

Il suffit donc de savoir calculer, pour la suite de longueur maximale $(u_i)_{i \in \mathbb{N}}$ décrite dans la section précédente, la somme $\mathcal{V}(n, d)$ des dernières coordonnées des u_i.

En revenant à la description de cette suite, on écrit facilement :

$$\mathcal{V}(2, f_n) = \sum_{i=2}^{f_n(1)+1} f_n(i) + \sum_{i=1}^{f_n(1)} (i - f_n(1))$$

$$\mathcal{V}(2, f_n) = \sum_{i=2}^{f_n(1)+1} f_n(i) + \frac{f_n(1)(1 - f_n(1))}{2}$$

Puis, en reprenant les notations g_i et N_i introduites à la section précédente, ainsi que la description de la suite qui y est donnée, on voit qu'il faut poser :

$$\mathcal{V}(d, f_n) = \mathcal{V}(d-1, g_1) + \mathcal{V}(d-1, g_2) + \cdots + \mathcal{V}(d-1, g_{f_n(1)}).$$

La longueur maximale L atteinte par une suite $u_1 >_{\text{lex}} u_2 >_{\text{lex}} \cdots >_{\text{lex}} u_{\mathrm{L}}$ telle que $\deg u_1 = n$ et $\deg u_i \leq \gamma(\max_{k<i}\{\deg u_k\})$, est

$$\mathrm{L} = \mathrm{L}(d, \gamma, n) = \ell(d, f_n) + \mathcal{V}(d, f_n)$$

où $f_n(k) = \gamma^{k-1}(n)$.

5.3 Suites croissantes d'idéaux dans $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_d]$

On va s'intéresser aux suites croissantes d'idéaux monomiaux dont les générateurs successifs sont contrôlés en degré par une fonction γ, de façon analogue à ce que nous avons appelé la « deuxième manière » ; on peut sans difficulté adapter nos arguments pour s'intéresser à un contrôle « première manière ».

Soit $\mathbb{A} = \mathbb{K}[X_1, \ldots, X_d]$. On fixe comme auparavant une fonction $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$ telle que $\gamma(k) > k$. Nous abuserons de la correspondance entre $\mathbf{T}^\circ(\mathbb{N}^d)$ et $\mathcal{IM}_\mathbb{A}$; en particulier, si $a = (a_1, \ldots, a_d) \in \mathbb{N}^d$, nous écrirons $\deg a$ pour la quantité $a_1 + \cdots + a_d$. On parlera d'idéaux monomiaux pour désigner des éléments de $\mathbf{T}^\circ(\mathbb{N}^d)$, et de monômes pour les éléments de $\mathbb{N}^d$.

On s'intéresse à la longueur maximale que peut avoir une suite strictement croissante d'idéaux monomiaux de la forme $A_n = \langle u_1, \ldots u_n, \rangle_\mathbf{T}$ avec $\deg u_1$ fixé et $\deg u_{i+1} = \gamma(\deg u_i)$: c'est le **problème A**. On s'intéresse également à la même question mais avec comme contrôle du degré $\deg u_{i+1} \leq \gamma(\max_{k<i}\{\deg u_k\})$. C'est le **problème B**.

Comme auparavant, il suffit de répondre au **problème A** pour connaître la réponse à la question du **problème B** : en effet, si on a une suite qui satisfait aux hypothèses de **problème B**, on peut suprimer les monômes u_i dont le degré est trop faible pour obtenir une suite (plus courte) satisfaisant aux hypothèses du **problème A** ; d'autre part, une telle suite de longueur maximale finit nécessairement par un terme A_N tel que $\Psi_d(A_N) = (0, \ldots, M)$. On peut ensuite remettre les monômes qu'on a enlevés, dans l'ordre où on les a enlevés ; on obtient toujours une suite strictement croissante ; ces monômes étaient en nombre $\leq M$, et égal à M si la suite de départ était de longueur maximale. Il suffit donc de connaître une suite qui répond au **problème A**, et de connaître $\Psi_d(A_N)$, pour résoudre le **problème B**.

Des suites déjà bien longues

Observons qu'à chaque suite de $\mathbb{N}^d$ strictement décroissante pour l'ordre lexicographique, de degré contrôlé par γ, on peut associer une suite strictement croissante d'idéaux monomiaux : si $u_1 >_{\text{lex}} u_2 >_{\text{lex}} \cdots >_{\text{lex}} u_r$ alors en posant $A_n = \langle u_1, \ldots, u_n \rangle_\mathbf{T}$, on obtient une suite strictement croissante $A_1 \subset A_2 \subset \cdots \subset A_r$. Appelons $\mathfrak{a}_1, \ldots, \mathfrak{a}_N$ la suite strictement décroissante de longueur maximale. La suite associée $\mathfrak{A}_1, \ldots, \mathfrak{A}_N$ est fort longue. Nous allons montrer qu'en fait sa longueur est maximale.

Exemple Reprenons la suite de $\mathbb{N}^3$, $\mathfrak{a}_1 >_{\text{lex}} \cdots >_{\text{lex}} \mathfrak{a}_{11}$ de longueur maximale avec $\deg \mathfrak{a}_1 = 2$ et $\gamma(n) = n + 1$. La figure 3 représente, avec les mêmes conventions que plus haut, certains des $\mathfrak{A}_i$.

Rappelons les valeurs prises par les $\mathfrak{a}_i$.

$$\begin{array}{llll} \mathfrak{a}_1 = (2,0,0) & \mathfrak{a}_2 = (1,2,0) & \mathfrak{a}_3 = (1,1,2) & \mathfrak{a}_4 = (1,0,4) \\ \mathfrak{a}_5 = (0,6,0) & \mathfrak{a}_6 = (0,5,2) & \mathfrak{a}_7 = (0,4,4) & \mathfrak{a}_8 = (0,3,6) \\ \mathfrak{a}_9 = (0,2,8) & \mathfrak{a}_{10} = (0,1,10) & \mathfrak{a}_{11} = (0,0,12). & \end{array}$$

On s'aperçoit que la dernière composante de $\Psi_d(\mathfrak{A}_n)$ correspond à l'évolution de la valeur de $L_3^\gamma(2)$ au fil de la suite $(\mathfrak{a}_i)$; c'est-à-dire qu'à l'étape n, il est égal au nombre de termes de degré $\leq \gamma^{n-1}(n)$ qu'on peut intercaller dans la suite $\mathfrak{a}_1 >_{\text{lex}} \cdots >_{\text{lex}} \mathfrak{a}_n$. Tout à fait logiquement, $\Psi_d(\mathfrak{A}_{11})$ donne le volume de $\mathbb{N}^3 \setminus \mathfrak{A}_{11}$, qui est le nombre de termes de degré inférieur à $\gamma^{10}(n) = 12$ qu'on peut intercaller dans la suite $\mathfrak{a}_1, \ldots, \mathfrak{a}_{11}$. Par contre les $d - 1$ premières composantes de $\Psi_d(\mathfrak{A}_n)$ coïncident avec celles de $\mathfrak{a}_n$. Ceci se reproduira, en toute dimension,

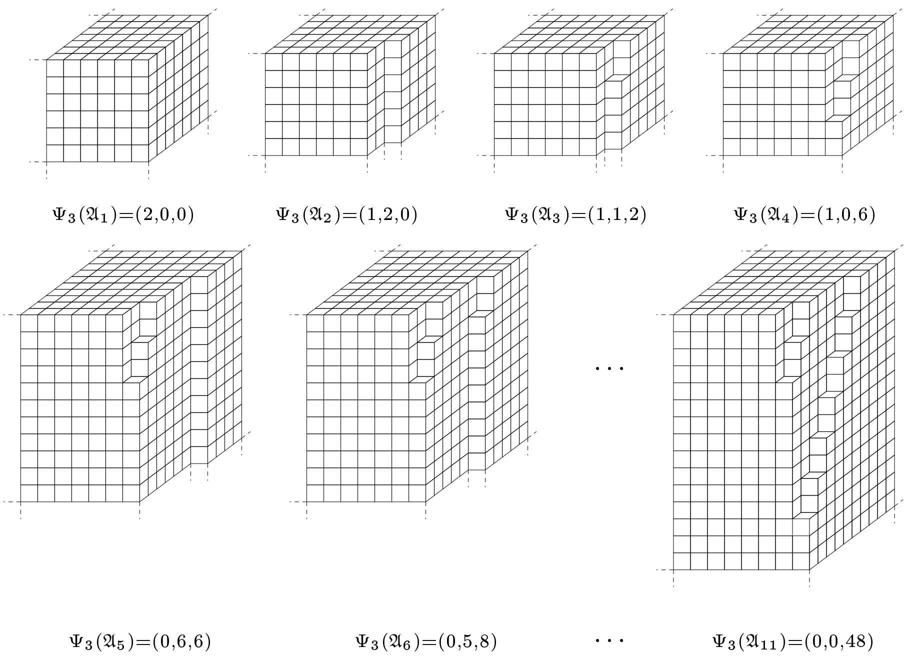


Figure 3 : Une suite déjà bien longue

chaque fois qu'on prendra la suite $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\mathrm{N}}$ construite avec la suite de longueur maximale $\mathfrak{a}_1, \ldots, \mathfrak{a}_{\mathrm{N}}$ associée aux conditions $\deg \mathfrak{a}_i = \gamma(\deg u_{i-1})$ et $\deg \mathfrak{a}_0 = n$.

Heuristique

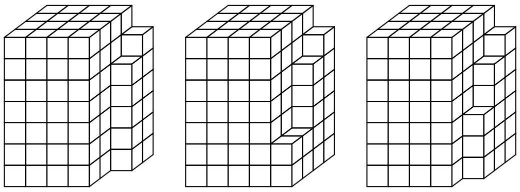
Si $\mathrm{A}_i \subset \mathrm{A}_{i+1}$, alors $\Psi_d(\mathrm{A}_i) >_{\mathrm{lex}} \Psi_d(\mathrm{A}_{i+1})$. Si le degré des générateurs ajouté croît strictement à chaque étape, il n'est pas possible d'avoir $\Psi_d(\mathrm{A}_i) = (x_1, \ldots, x_{d-1}, x_d)$ et $\Psi_d(\mathrm{A}_{i+1}) = (x_1, \ldots, x_{d-1}, x_d{}')$ avec $x_d{}' < x_d$: pour cela, il faut ajouter aux générateurs de A_i un monôme qui est de degré plus petit que celui d'un de ces générateurs. Donc la suite $\Psi'_d(\mathrm{A}_i) \in \mathbb{N}^{d-1}$ des $d-1$ premières composantes de $\Psi_d(\mathrm{A}_i) \in \mathbb{N}^d$ est strictement décroissante pour l'ordre lexicographique.

Il aurait été agréable que le degré des $\Psi'_d(\mathrm{A}_i)$ soit suffisament bien contrôlé pour qu'on puisse affirmer reconstruire à partir de cette suite une suite u_i telle que $u_i >_{\mathrm{lex}} u_{i+1}$ et $\deg u_{i+1} = \gamma(\deg u_i)$.

Malheureusement, on peut très bien trouver des suites d'idéaux monomiaux (A_i) satisfaisant notre condition mais dont la suite associée $\Psi'_d(\mathrm{A}_i)$ a son degré qui croît trop vite pour pouvoir être complété en une suite u_i. Nous affirmons que ce cas peut-être évité : on peut les «rectifier», c'est-à-dire les modifier pour construire une suite de même longueur, qui ne présente pas cet inconvénient. Faisons la preuve en dimension 3.

Rectification On a toujours $\mathrm{A}_n = \langle u_1, \ldots, u_n \rangle_{\mathrm{T}}$ et $\mathrm{A}_{n+1} = \langle u_1, \ldots, u_{n+1} \rangle_{\mathrm{T}}$, avec $\deg u_1 < \cdots < \deg u_n < \deg u_{n+1}$.

Soit $\Psi'_3(\mathrm{A}_n) = (a, b)$, avec $a, b > 0$. Si $\Psi'_3(\mathrm{A}_{n+1}) = (a, b')$, avec $b' < b - 1$, alors on peut remplacer u_{n+1} par un u'_{n+1} de même degré, tel que, si A'_{n+1} est le nouvel idéal associé, $\Psi'_3(\mathrm{A}'_{n+1}) = (a, b - 1)$: voir la figure 4.

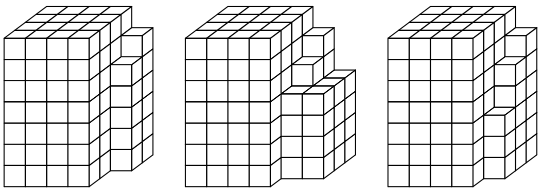


A_n A_{n+1} A'_{n+1}

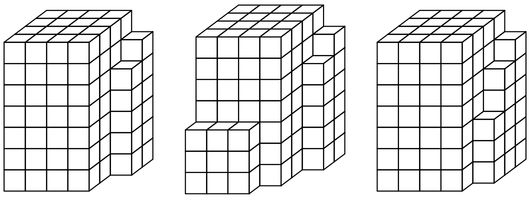
Figure 4 : Rectification, 1.

On a $\mathrm{A}_n \subset \mathrm{A}'_{n+1} \subset \mathrm{A}_{n+1}$: en remplaçant A_{n+1} par A'_{n+1}, on a construit une suite de la même longueur, telle que $\Psi'_d(\mathrm{A}_i)$ est bien contrôlé.

Si $\Psi'_3(\mathrm{A}_{n+1}) = (a', b')$ avec $a' < a$, on peut faire une rectification du même genre : voir la figure 5.



A_n A_{n+1} A'_{n+1}



A_n A_{n+1} A'_{n+1}

Figure 5 : Rectification, 2.

C'est surtout ce cas qui est important, car ici $\Psi'_d(\mathrm{A}_i)$ a vu son degré augmenter brutalement ; mais c'est au détriment de la longueur finale de la suite. **C'est la condition de croissance du degré** ($\gamma(k) > k$) qui fait que nos dessins représentent le cas général. Si on ne l'avait pas, il ne serait pas toujours possible de rectifier la suite.

Reste le cas $\Psi'_3(\mathrm{A}_n) = (a, 0)$ avec $a > 0$. Soit $\Psi'_3(\mathrm{A}_{n+1}) = (a', b')$; à nouveau comme avant on peut imposer $a' = a - 1$, car sinon on trouve une suite plus longue. Quelle va être la valeur de b' ? si on tient compte du fait qu'une suite de longueur maximale commence par un idéal monogène, on s'aperçoit, de proche en proche, que b' est bien tel que $\deg \Psi'_3(\mathrm{A}_{n+1}) \leq \deg \mathfrak{a}_{n+1}$. Nous allons encore une fois nous contenter d'un exemple.

Pour $d = 3$, on démarre avec un monôme de degré 2, la fonction γ étant une fois de plus $\gamma(n) = n + 1$. On pose $u_1 = (1, 1, 0)$ et $\mathrm{A}_1 = \langle\, u_1 \,\rangle_{\mathbf{T}}$. On a

$\Psi_3(\mathrm{A}_1) = (2,0,0)$. D'après ce qui précède, il faut « remplir » les deux plans de $\mathbb{N}^3 \setminus \mathrm{A}_1$ l'un après l'autre, et chacun de ces deux plans « une droite à la fois ». Cela nous laisse quand-même une certaine liberté pour choisir $u_2, u_3, \ldots$; on pose bien sûr $\mathrm{A}_n = \langle u_1, \ldots, u_n \rangle_{\mathbf{T}}$. Cependant on voit que la suite $\Psi_3(\mathrm{A}_n)$ est égale à la suite $\Psi_3(\mathfrak{A}_n)$. Voir figure 6.

Les monômes choisis sont les suivants :

$u_1 = (1,1,0)$ $u_2 = (0,2,1)$ $u_3 = (0,1,3)$ $u_4 = (0,5,0)$ $u_5 = (3,0,2)$
$u_6 = (0,5,2)$ $u_7 = (2,0,6)$ $u_8 = (1,0,8)$ $u_9 = (9,0,1)$ $u_{10} = (11,0,0)$
$u_{11} = (0,0,12)$

Nous espérons avoir convaincu le lecteur ou la lectrice du résultat suivant :

Théorème 58 *Soit $\gamma : \mathbb{N} \longrightarrow \mathbb{N}$ telle que $\gamma(k) > k$ pour tout k. Alors la longueur maximale d'une suite strictement croissante d'idéaux monomiaux $\mathrm{A}_n = \langle u_1, \ldots, u_n \rangle_{\mathbf{T}}$ telle que $\deg u_1 = n$ et pour tout i $\deg u_i = \gamma(\deg u_{i-1})$, est la fonction $\ell'(d, \gamma, n)$ de la section 5.2. La longueur maximale d'une suite $\mathrm{A}_n = \langle u_1, \ldots, u_n \rangle_{\mathbf{T}}$ strictement croissante pour l'inclusion, telle que $\deg u_1 = n$ et pour tout i $\deg u_i \leq \gamma(\max_{k<i}\{\deg u_k\})$, est la fonction $\mathrm{L}(d, \gamma, n)$ de la section 5.2.*

5.4 Un cas particulier

Guillermo Moreno-Socìas a étudié, dans [M-S$_1$], le cas où $\gamma(n) = n + 1$, par des méthodes différentes ; un théorème de Macaulay concernant les fonctions de Hilbert-Samuel joue un grand rôle dans sa preuve. Nous allons redémontrer son résultat, qui, avec nos notations, se traduit comme ceci :

$$\ell_d(n) := \ell'(d, \gamma, n) = \mathrm{A}_d(n-1) - n,$$

où $\mathrm{A}_d(n)$ est la fonction d'Ackermann définie par

$$\left\{ \begin{array}{rcl} \mathrm{A}_0(n) & = & n+1 \\ \mathrm{A}_{d+1}(0) & = & \mathrm{A}_d(1) \\ \mathrm{A}_{d+1}(n+1) & = & \mathrm{A}_d \circ \mathrm{A}_{d+1}(n). \end{array} \right.$$

La fonction d'Ackermann On a $\mathrm{A}_{d+1}(n) = \mathrm{A}_d \circ \mathrm{A}_{d+1}(n-1) = \ldots = \mathrm{A}_d^n \circ \mathrm{A}_{d+1}(0) = \mathrm{A}_d^{n+1}(1)$.

On en déduit assez facilement les valeurs de $\mathrm{A}_d(n)$ pour $d = 1, 2, 3, 4$:

$$\begin{aligned} \mathrm{A}_1(n) &= n+2 \\ \mathrm{A}_2(n) &= 2n+3 = 2 \cdot (n+3) - 3 \\ \mathrm{A}_3(n) &= 2^{n+3} - 3 \\ \mathrm{A}_4(n) &= \underbrace{2^{2^{\cdot^{\cdot^{2}}}}}_{n+3} - 3 \end{aligned}$$

Récurrence Soit f_n la fonction définie par $f_n(k) = \gamma^{k-1}(n)$, c'est-à-dire $f_n(k) = n + k - 1$.

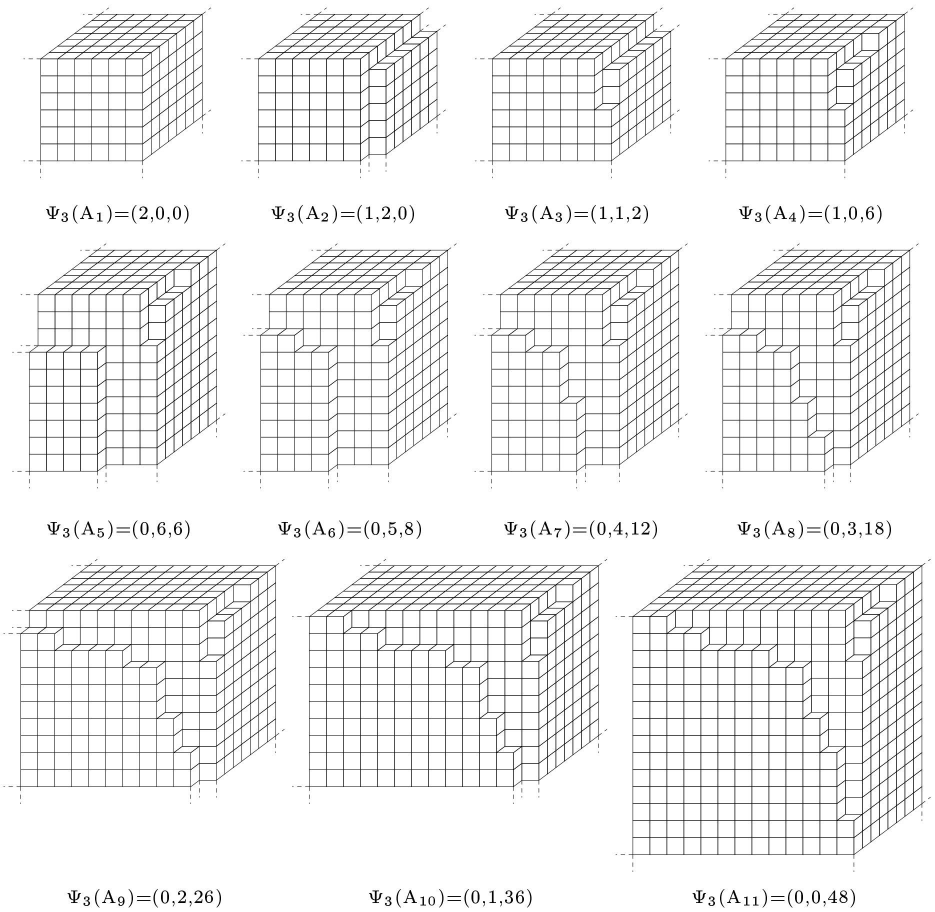


Figure 6 : Une suite de longueur maximale

On a $\ell_d(n) = \ell'(d, \gamma, n) = \ell(d, f_n)$.

On a d'après nos définitions $\ell_2(n) = \ell(2, f_n) = f_n(1) + 1 = n + 1$, et donc $\ell_2(n) = \mathrm{A}_2(n-1) - n$.

Posons l'hypothèse de récurrence suivante :

$$\ell_d(n) = \mathrm{A}_d(n-1) - n.$$

On l'a vérifié pour $d = 2$. Supposons que c'est vérifié pour $d - 1$, montrons le pour d.

On pose $\mathrm{N}_0 = 1$ et pour $i > 0$, $\mathrm{N}_i = \mathrm{N}_{i-1} + \ell(d-1, g_i)$,
où $g_i(k) = f_n(\mathrm{N}_{i-1} + k) - f_n(1) + i$.

On a $\ell_d(n) = \ell(d, f_n) = \mathrm{N}_{f_n(1)} = \mathrm{N}_n$.
On a $g_1(k) = f_n(1+k) - f_n(1) + 1 = k + 1$, d'où $g_1 = f_2$ (par définition $f_n(k) = n + k - 1$).
On en déduit $\mathrm{N}_1 = \mathrm{N}_0 + \ell(d-1, g_1) = 1 + \ell_{d-1}(2)$,
et donc $\mathrm{N}_1 = \mathrm{A}_{d-1}(1) - 1$.
Puis $g_2(k) = f_n(\mathrm{N}_1 + k) - f_n(1) + 2 = \mathrm{N}_1 + k + 1$ d'où $g_2 = f_{\mathrm{N}_1+2}$.
et donc $\ell(d-1, g_2) = \ell(d-1, f_{\mathrm{N}_1+2}) = \mathrm{A}_{d-1}(\mathrm{A}_{d-1}(1)) - \mathrm{N}_1 - 2$,
d'où $\mathrm{N}_2 = \mathrm{A}_{d-1}^2(1) - 2$.

De proche en proche on trouve $\mathrm{N}_k = \mathrm{A}_{d-1}^k(1) - n$, et donc $\mathrm{N}_n = \mathrm{A}_{d-1}^n(1) - n$;
d'où $\ell_d(n) = \mathrm{N}_n = \mathrm{A}_d(n-1) - n$; ce qui conclut l'étape de récurrence.

On retrouve bien le résultat annoncé. La longueur de ces suites simples à décrire est réellement très surprenante ; on peut écrire à la main la suite qui commence par $(1, 0, 0, 0)$, et aussi, si on fait un usage judicieux des points de suspension, celle qui commence par $(2, 0, 0, 0)$. Il est tout à fait vain de s'essayer à trouver la longueur de $(3, 0, 0, 0)$ sans faire de preuve par récurrence. Par contre il est possible de prouver directement la relation de récurrence suivante :

$$\ell_2(n) = n + 1, \quad \ell_{d+1}(n+1) = \ell_d(\ell_{d+1}(n) + 2).$$

5.5 Complexité de certains algorithmes

On peut toujours trouver une borne à la complexité d'un algorithme si sa preuve de terminaison est constructive. Les calculs que nous venons de développer peuvent être vus comme un outil pour borner la complexité d'algorithmes dont la terminaison dépend de l'arrêt d'une suite de $\mathbb{N}^d$ strictement décroissante pour l'ordre lexicographique, ou de l'arrêt d'une suite d'idéaux monomiaux de $\mathbb{K}[\underline{\mathrm{X}}]$ strictement croissante pour l'inclusion.

L'algorithme de Buchberger est concerné ; nous allons donner une borne au nombre d'itérations de la boucle principale. Nous ne chercherons pas à estimer le nombre d'opérations arithmétiques élémentaires qui peut être nécessaire pour réaliser cette boucle.

L'algorithme de Rosenfeld-Gröbner dû à François Boulier (*cf.* [Boul], [BLOP]) est lui aussi contrôlé par le lemme de Dickson, mais nous n'avons pas pris le temps de l'analyser.

La borne fournie est bien entendu exécrable : au vu du cas particulier précédent il est certain qu'elle ne sera jamais primitive récursive. En fait il est très intuitif (au vu du calcul précédent) que les fonctions $\ell(d,n) = \ell'(d,\gamma,n)$ et $\mathrm{L}(d,n) = \mathrm{L}(d,\gamma,n)$ ne seront jamais primitives récursives ; en particulier puisqu'on a pour tout n $\gamma(n) > n$, alors $\gamma(n) \geq n+1$ et donc $\ell(d,\gamma,n) \geq \mathrm{A}_d(n-1) - n$. Le principal intérêt est donc l'existence d'une borne ; sa valeur sera inutile en pratique, car trop élevée ($\mathrm{A}_4(2) = 2^{65\,536} - 3$ dépasse très largement la grandeur connue sous le nom « d'âge de l'univers » — même exprimée en femtosecondes). Nous nous contenterons donc de majorations grossières.

Nous nous restreignons au cas d'un ordre monomial dominé par le degré total, comme $\leq_{\mathrm{deglex}}$. Supposons que tous les monômes présents dans la famille $\mathcal{G}_i$, à la i^e étape de calcul, sont de degré total $\leq n$. Alors à l'étape $i+1$, on a ajouté des polynômes du style $\overline{\mathrm{S}(f,g)}^{\mathcal{G}_i}$, avec $f, g \in \mathcal{G}_i$. Le degré total de $\mathrm{S}(f,g)$ est $\leq 2n$; et la division n'augmente pas le degré *grâce au choix d'un ordre dominé par le degré total*. Il convient donc de poser $\gamma(k) = 2 \cdot k$. On va donner une majoration brutale de $\ell'(d,\gamma,n)$ et $\mathrm{L}(d,\gamma,n)$; le nombre de boucles après lequel l'algorithme s'arrête, pour un idéal de $\mathrm{K}[\mathrm{X}_1,\ldots,\mathrm{X}_d]$ engendré par des polynômes de degré total inférieur à n, est majoré par $\mathrm{L}_d(n) = \mathrm{L}(d,\gamma,n)$.

Notre souci sera d'obtenir un résultat compact, et non pas une valeur proche de la vraie valeur. En fait il est très difficile de mener des calculs plus précis, le cas $\gamma(n) = n+1$ est un vrai miracle.

Voici quelques faits que nous utiliserons dans le calcul : pour $r \geq 4$ on a
- A_r strictement croissante ;
- $2^{\mathrm{A}_r(k)} < \mathrm{A}_r(k+1)$;
- $2^{\mathrm{A}_r^n(k)} < \mathrm{A}_r^n(k+1)$;
- $\mathrm{A}_r(k) + \mathrm{A}_r \circ \mathrm{A}_r(k) < \mathrm{A}_r \circ \mathrm{A}_r(k+1)$;
- $\mathrm{A}_r^n(k) + \mathrm{A}_r^{n+1}(k) < \mathrm{A}_r^{n+1}(k+1)$;
- $\mathrm{A}_r(k^2) < \mathrm{A}_{r+1}(k)$;
- $\mathrm{A}_r(k^2 + \lambda \cdot k) < \mathrm{A}_{r+1}((\lambda+1) \cdot k)$.

(la notation exponentielle désigne une fois encore l'itération de la composition).

Lemme 59 *Soit $\gamma(k) = 2 \cdot k$. On pose note $\ell_d(n) = \ell'(d,\gamma,n)$ et $\mathcal{V}_d(n) = \mathcal{V}(d,\gamma,n)$. Si il exite $\lambda \in \mathbb{N}$ et $r \geq 4$ tels que $\ell_d(n) < \mathrm{A}_r(\lambda \cdot n)$ et $\mathcal{V}_d(n) < \mathrm{A}_r(\lambda \cdot n)$, alors il existe $\mu \in \mathbb{N}$ tel que $\ell_{d+1}(n) < \mathrm{A}_{r+1}(\mu \cdot n)$ et $\mathcal{V}_{d+1}(n) < \mathrm{A}_{r+1}(\mu \cdot n)$.*

Démonstration Une fois encore on pose $f_n(k) = \gamma^{k-1}(n)$, ce qui produit $f_n(k) = 2^{k-1} \cdot n$. De façon générale, on note $f_m(k) = 2^{k-1} \cdot m$.

On pose $\mathrm{N}_0 = 1$ et pour $i > 0$, $\mathrm{N}_i = \mathrm{N}_{i-1} + \ell(d, g_i)$,

où $g_i(k) = f_n(\mathrm{N}_{i-1} + k) - f_n(1) + i$.

On a $\ell_{d+1}(n) = \ell(d+1, f_n) = \mathrm{N}_{f_n(1)} = \mathrm{N}_n$.

La fonction $g_1(k) = f_n(1+k) - f(1) + 1 = (2^k - 1)\cdot n + 1$ est majorée par $f_{2n}(k) = 2^{k-1}\cdot(2n)$, donc $\ell(d, g_1) < \ell(d, f_{2n}) = \ell_d(2n) < \mathrm{A}_r(2n)$;

puis $\mathrm{N}_1 = 1 + \ell(d, g_1) \leq \mathrm{A}_r(2n)$.

Ensuite $g_2(k) = f_n(\mathrm{N}_1 + k) - f_n(1) + 2 \leq 2^{\mathrm{A}_r(2\lambda\cdot n_0)+k-1}\cdot n < f_{2^{\mathrm{A}_r(2\lambda\cdot n)}\cdot n}$;

d'où $\ell(d, g_2) < \ell(d, f_{2^{\mathrm{A}_r(2\lambda\cdot n)}\cdot n}) = \ell_d(2^{\mathrm{A}_r(2\lambda\cdot n)}\cdot n)$

$\ell(d, g_2) < \mathrm{A}_r(\lambda\cdot 2^{\mathrm{A}_r(2\lambda\cdot n)}\cdot n)$

$\ell(d, g_2) < \mathrm{A}_r(\lambda\cdot \mathrm{A}_r(2\lambda\cdot n + 1)\cdot n)$

$\ell(d, g_2) < \mathrm{A}_r^2((2\lambda+1)\cdot n + \lambda + 1)$.

et donc $\mathrm{N}_2 = \mathrm{N}_1 + \ell(d, g_2) < \mathrm{A}_r^2((2\lambda+1)\cdot n + \lambda + 2)$.

Ensuite $g_3(k) = f_n(\mathrm{N}_2 + k) - f_n(1) + 3 < 2^{\mathrm{A}_r^2((2\lambda+1)\cdot n+\lambda+2)+k-1}\cdot n$,

$g_3(k) < 2^{k-1}\cdot \mathrm{A}_r^2((2\lambda+2)\cdot n + \lambda + 3)$

et $\ell(d, g_3) < \ell_d(\mathrm{A}_r^2((2\lambda+2)\cdot n + \lambda + 3)$,

$\ell(d, g_3) < \mathrm{A}_r^3((2\lambda+2)\cdot n + 2\lambda + 3)$

et donc $\mathrm{N}_3 = \mathrm{N}_2 + \ell(d, g_3) < \mathrm{A}_r^3((2\lambda+2)\cdot n + 2\lambda + 4)$.

De proche en proche $\mathrm{N}_i < \mathrm{A}_r^i((2\lambda+i-1)\cdot n + (i-1)\lambda + 2(i-1))$;

d'où $\mathrm{N}_n < \mathrm{A}_r^n((3\lambda+1+n)\cdot n)$

$\ell_{d+1}(n) = \mathrm{N}_n < \mathrm{A}_r^{n-1}\circ \mathrm{A}_r((3\lambda+1+n)\cdot n)$

$\ell_{d+1}(n) < \mathrm{A}_r^{n-1}\circ \mathrm{A}_{r+1}((3\lambda+2)\cdot n)$

$\ell_{d+1}(n) < \mathrm{A}_{r+1}((3\lambda+3)\cdot n)$.

Reste à s'occuper de $\mathcal{V}(d, g_i)$ afin d'obtenir une majoration de $\mathcal{V}(d+1, f_n)$.

D'après ce qui précède, pour tout i, $g_i < f_{m_i}$,

avec $m_i = \mathrm{A}_r^{i-1}((2\lambda+i)\cdot n + (i-1)\lambda + 2i - 1)$,

et donc $\mathcal{V}(d, g_i) < \mathcal{V}_d(m_i) < \mathrm{A}_r(\lambda\cdot m_i)$;

d'où $\mathcal{V}(d, g_i) < \mathrm{A}_r^{i+1}((2\lambda+i)\cdot n + i\lambda + 2i - 1)$.

On obtient $\mathcal{V}(d+1, f_n) = \sum_i \mathcal{V}(d, g_i) < \mathrm{A}_{r+1}((3\lambda+3)\cdot n)$. □

Remarque Nos majorations ont été plus que brutales; cependant il en est une à laquelle il est impossible d'échapper, c'est la dernière, celle qui permet d'écrire un résultat en A_{r+1}. Quoiqu'on fasse, $\ell_{d+1}(n)$ est une somme dans laquelle le terme le plus gros (de loin) est $\ell(d, g_n)$, qui est en fait grosso modo un empilement de n itérations de ℓ_d ; on change « d'étage » dans la fonction d'Ackerman. La valeur r de cet « étage » nous paraît beaucoup plus importante que le contenu des parenthèses dans l'expression $\mathrm{A}_r(\cdots)$.

Proposition 60 *On a* $\mathrm{L}_d(n) < \mathrm{A}_{d+2}(\lambda_d\cdot n)$ *où* $\lambda_d \in \mathbb{N}$.

Démonstration Il est très facile de vérifier que $\ell_2(n)$ et $\mathcal{V}_2(n)$ sont majorés par $\mathrm{A}_4(\lambda \cdot n)$ pour un λ bien choisi ; on applique le lemme précédent. □

Remarque L'algorithme de Buchberger naïf tel que nous l'avons décrit n'est pas vraiment celui qui est utilisé en pratique ; en particulier dans le cas de polynômes homogènes il y a des méthodes qui permettent d'accélérer les calculs et de borner la taille du calcul à partir de la taille du résultat final. Nous n'avons trouvé nulle part dans la littérature d'analyse de l'algorithme de Buchberger général tel que nous l'avons présenté ; des bornes sont connues sur le degré final d'une base de Gröbner : obtenues par des moyens abstraits, elles sont, avec nos notations, de l'ordre de n^{2^d}, ce qui est nettement plus raisonnable (c'est primitif récursif). Pour plus de détails sur ce sujet, on pourra se reporter à [M], [BW], [Giu].

CHAPITRE II

POLYNÔMES ET CORPS (VALUÉS)

Introduction

1 Les outils de base

Nous allons tout d'abord donner des outils concernant la manipulation des corps et des polynômes, dans le cas non valué. Il s'agit d'outils élémentaires : *la transformation de Tschirnhaus*, d'une part, et d'autre part nous donnons un bref exposé d'une méthode algorithmique permettant le calcul dans le corps de rupture d'un polynôme donné, y compris en l'absence d'algorithme de factorisation des polynômes.

Après des généralités sur les corps valués, nous définirons un outil propre aux corps valués, *le polygone de Newton d'un polynôme.*

1.1 Transformée de Tschirnhaus

Ici $\mathbb{K}$ est un corps quelconque, et $\mathbb{K}^{ac}$ est sa clôture algébrique. Le lemme suivant remonte au XVII^{e} siècle (*cf.* [KK]).

Lemme 1 *Soient* P, Q *deux polynômes de* $\mathbb{K}[\mathrm{X}]$*, et soient* $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^{ac}$ *les racines de* P *; alors le polynôme*

$$\mathrm{T}_{\mathrm{P},\mathrm{Q}}(\mathrm{X}) = \prod_{i=1}^{n} \big(\mathrm{X} - \mathrm{Q}(\alpha_i)\big)$$

est dans $\mathbb{K}[\mathrm{X}]$*, et on peut le calculer à partir des coefficients de* P *et* Q*. On appelle* $\mathrm{T}_{\mathrm{P},\mathrm{Q}}$ *la transformée de Tschirnhaus de* P *par* Q*.*

Démonstration On peut se contenter de remarquer que $\mathrm{T}_{\mathrm{P},\mathrm{Q}}$ est invariant par toute permutation des α_i, et que donc ses coefficients sont des expressions polynomiales en les fonctions symétriques élémentaires des α_i, c.-à-d. (ce sont les relations de Viète) en les coefficients de P si P est unitaire.

Cependant nous donnons la recette suivante : soit M_P la matrice compagnon de P. Alors $\mathrm{T}_{\mathrm{P},\mathrm{Q}}$ est le polynôme caractéristique de $\mathrm{Q}(\mathrm{M}_\mathrm{P})$. □

Remarque Les déterminants n'existaient pas en 1684. On calculait $\mathrm{T}_{\mathrm{P},\mathrm{Q}}(\mathrm{X})$ en éliminant Y entre les deux équations

$$\begin{aligned} \mathrm{P}(\mathrm{Y}) &= 0, \\ \mathrm{X} - \mathrm{Q}(\mathrm{Y}) &= 0. \end{aligned}$$

C'est ainsi que procède Lagrange dans [Lag]. Cette méthode peut être encore utilisée aujourd'hui, en faisant l'élimination avec un calcul de résultant.

Notation Nous utiliserons la notation suivante :

$$\prod_{\alpha\,:\,\mathrm{P}} \big(\mathrm{X} - \mathrm{Q}(\alpha)\big) = \prod_{i=1}^{n} \big(\mathrm{X} - \mathrm{Q}(\alpha_i)\big)$$

Ainsi placé en indice, $\alpha\ :\ \mathrm{P}$ signifie « α décrit les racines de P ».

La généralisation suivante est naturelle :

Lemme 2 *Soient* $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ *de degré* n *et* $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^{ac}$ *ses racines. Soit* $\mathrm{T}(\mathrm{Y}_1, \ldots, \mathrm{Y}_n)(\mathrm{X}) \in \mathbb{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_n][\mathrm{X}]$*. On note* $\mathfrak{S}_n$ *le groupe des permutations de* $\{1, \ldots, n\}$*. Si*

$$\forall \sigma \in \mathfrak{S}_n,\ \ \mathrm{T}(\mathrm{Y}_{\sigma 1}, \ldots, \mathrm{Y}_{\sigma n})(\mathrm{X}) = \mathrm{T}(\mathrm{Y}_1, \ldots, \mathrm{Y}_n)(\mathrm{X}),$$

alors le polynôme $\mathrm{T}(\alpha_1, \ldots, \alpha_n)(\mathrm{X})$ *est dans* $\mathbb{K}[\mathrm{X}]$*, et on peut expliciter ses coefficients comme des éléments de* $\mathbb{K}$*, à partir des coefficients de* P*.*

Le lemme suivant pourra donner une première idée de l'utilité de la transformation de Tschirnhaus.

Lemme 3 *Si on a une factorisation de* $\mathrm{T}_{\mathrm{P},\mathrm{Q}}$ *en* $\mathrm{T} = \mathrm{T}_1 \cdots \mathrm{T}_k$ *dans* $\mathbb{K}[\mathrm{X}]$*, avec les* T_i *premiers deux à deux, alors on peut trouver une factorisation* $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_k$ *de* $\mathrm{P}(\mathrm{X})$ *dans* $\mathbb{K}[\mathrm{X}]$*, avec* $\deg \mathrm{P}_i = \deg \mathrm{T}_i$*, les* P_i *étant premiers deux à deux et vérifiant* $\mathrm{T}_{\mathrm{P}_i,\mathrm{Q}} = \mathrm{T}_i$*.*

Démonstration Pour tout i on pose $\mathrm{P}_i = \mathrm{pgcd}(\mathrm{T}_i \circ \mathrm{Q}, \mathrm{P})$. Alors

$$\{\alpha \in \mathbb{K}^{ac}\ :\ \mathrm{P}_i(\alpha) = 0\} = \{\alpha \in \mathbb{K}^{ac}\ :\ \mathrm{P}(\alpha) = 0 \text{ et } \mathrm{Q}(\alpha) \text{ racine de } \mathrm{T}_i\}$$

Il est clair que ces ensembles sont deux à deux disjoints (car les T_i sont premiers deux à deux) et que leur réunion est l'ensemble de toutes les racines de P.

On peut imposer tous les P_i unitaires, sauf par exemple P_1 auquel on impose d'avoir le même coefficient dominant que P, et on a obtenu la factorisation désirée. □

Remarque Ce lemme peut se ré-interpréter en termes d'action du groupe de Galois sur l'ensemble des racines de P ; les lecteurs habitués à ce point de vue y verront sans doute une justification intuitive de sa véracité.

Le lemme suivant est élémentaire mais utile.

Lemme 4 *Soient* $\mathrm{P}_1, \ldots, \mathrm{P}_n \in \mathbb{K}[\mathrm{X}]$. *On peut calculer une liste de polynômes premiers entre eux deux à deux* Q_j *pour* $j = 1, \ldots, m$, *et des entiers positifs* n_{ij} *pour* $i = 1, \ldots, n$ *et* $j = 1, \ldots, m$, *tels que* $\mathrm{P}_i = a_i \prod_{j=1,\ldots,m} \mathrm{Q}_j^{n_{ij}}$ *avec* $a_i \in \mathbb{K}$ *(on peut imposer que les* Q_j *soient unitaires, et dans ce cas* a_i *est le coefficient dominant de* P_i*).*

Démonstration On applique répétitivement l'algorithme d'Euclide et la division euclidienne. □

1.2 Calcul dans un corps de rupture

La méthode exposée ici est *grosso modo* issue des évaluation dynamiques introduites dans l'article de Michel Coste, Henri Lombardi, et Marie-Françoise Roy, [CLR] ; cette conception est elle-même héritière de l'algorithme D5 dû à Jean Della Dora, Claire Dicrescenzo et Dominique Duval (*cf.* [D5],[DD]).

Définition En mathématiques constructives un *corps discret* $\mathbb{K}$ est un corps tel que :
- les opérations $+$ et $\times$ sont explicites dans $\mathbb{K}$;
- le calcul de l'inverse d'un élément non nul également ;
- on dispose d'un test $x \stackrel{?}{=} 0$.

Ce terme est un peu ambigu dans la mesure où il a déjà un autre sens en mathématiques classiques ; cependant il paraît très intuitif qu'un corps discret dans notre sens *doit* être dénombrable — au moins du point de vue classique. Du point de vue des mathématiques classiques, tous les corps sont discrets ; en particulier, le troisième point correspond à l'instance suivante du tiers-exclu : « $x = 0 \vee x \neq 0$ ». La mathématicienne et le mathématicien classique pourront lire les preuves constructives comme des preuves élémentaires où on a limité les utilisations du tiers-exclus ; elles sont bien sûr valables du point de vue classique.

Soit $\mathrm{P}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ un polynôme *pas nécessairement irréductible.* Alors on peut « calculer » dans un corps de rupture de P, dans le sens suivant :

Soit ζ une racine de P ; on représente les éléments de $\mathbb{K}[\zeta]$ par des expressions polynomiales formelles $q(\zeta)$, avec $q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ et $\deg q < \deg \mathrm{P}$. On dit que ζ est *codé par* P, ce qu'on notera parfois « ζ : P ».

Les opérations + et $\times$ sont explicites dans $\mathbb{K}[\zeta]$: on pose $q_1(\zeta) + q_2(\zeta) = (q_1 + q_2)(\zeta)$, et pour multiplier $q_1(\zeta)$ par $q_2(\zeta)$, on commence par calculer $q_1 \cdot q_2$ et on prend le reste de la division par P.

Le test $q(\zeta) \stackrel{?}{=} 0$ d'égalité à zéro peut avoir une réponse ambiguë : on calcule $r(\mathrm{X}) = q(\mathrm{X}) \wedge \mathrm{P}(\mathrm{X})$. Si r est constant, $q(\zeta) \neq 0$. Si r est non constant, on calcule

P_1 et P_2 tels que $P = P_1 \cdot P_2$, avec $P_1 \wedge P_2 = 1$, $P_1 \wedge q = 1$, et P_2 divise une puissance de r. Ainsi P_2 est le facteur de P qui contient toutes les racines de P qui sont aussi des racines de Q. Alors la réponse au test dépend de la question « la racine ζ de P est-elle racine de P_1 ou de P_2 ? ». Si on cherche simplement à calculer dans un corps de rupture de P, on peut répondre de façon arbitraire (par exemple en choisissant de P_1 ou de P_2 celui qui a le plus petit degré). Si on s'intéresse aux propriétés de tous les zéros de P, on pourra ouvrir deux branches de calcul.

On remplace donc le code de définition de ζ (qui était P) par P_1 ou P_2. Si on a choisi P_2, alors $q(\zeta) = 0$. Si on a choisi P_1, alors $q(\zeta) \neq 0$.

Ainsi pour un polynôme non irréductible, on aura à choisir en cours de route de quel facteur de P notre α est réellement une racine. Remarquons qu'en caractéristique nulle on peut se limiter au cas où P est séparable, ce qui simplifie le problème.

Dans la suite on sera amené à utiliser cet algorithme en disposant en outre d'un test « étant donné un facteur de P, ζ en est-il racine ? ». Dans ce cas, si une factorisation de P apparaît au cours du test précédent, le choix du facteur à conserver pour la définition de ζ ne sera plus arbitraire, et le test d'égalité à zéro ne sera plus ambigu.

Le calcul de l'inverse d'un élément non nul est un sous-produit de ce calcul de pgcd par l'algorithme d'Euclide : si $q(\zeta) \neq 0$, on vient d'expliquer qu'on peut toujours supposer, modulo le choix d'une nouvelle définition P pour ζ, que $q(X) \wedge P(X) = 1$. Alors on calcule $u(X), v(X) \in \mathbb{K}[X]$ tels que $u(X) \cdot q(X) + v(X) \cdot P(X) = 1$. L'inverse de $q(\zeta)$ est $u(\zeta)$.

Nombre de théorèmes classiques peuvent être ré-écrits dans ce cadre, en particulier le théorème de l'élément primitif (voir [Wae], par exemple), qui nous sera utile dans la suite.

Théorème 5 (Théorème de l'élément primitif) *On suppose que* $\mathbb{K}$ *est infini et que* $\mathcal{F}$ *est une partie infinie de* $\mathbb{K}$. *Soit* α *défini comme étant un des zéros de* $P(X) \in \mathbb{K}[X]$. *On suppose que* P *est séparable, c.-à-d. que* $P(X) \wedge P'(X) = 1$. *Soit* $Q(X, Y) \in \mathbb{K}[X, Y]$; *on note* $Q_\alpha(X)$ *le polynôme de* $\mathbb{K}[\alpha][X]$ *défini par* $Q_\alpha(X) = Q(\alpha, X)$. *On suppose que* $Q_\alpha(X)$ *est unitaire. Soit* β *défini comme étant un des zéros de* $Q_\alpha(X)$.

On peut calculer un polynôme $T(X) \in \mathbb{K}[X]$, *tel que si on prend* ζ *une de ses racines, on a* $\mathbb{K}[\zeta] = \mathbb{K}[\alpha][\beta]$; *concrètement,* α *et* β *s'expriment comme des éléments* $a(\zeta)$ *et* $b(\zeta)$ *de* $\mathbb{K}[\zeta]$. *Les polynômes* $P(a(X))$ *et* $Q(a(X), b(X))$ *sont donc divisibles par* $T(X)$.

On peut imposer $\zeta = u \cdot \alpha + \beta$ *avec* $u \in \mathcal{F}$. *On a alors*

$$T(X) = \prod_{\alpha\,:\,P} \ \prod_{\beta\,:\,Q_\alpha} \big(X - (u \cdot \alpha + \beta)\big) \,;$$

si on fixe α *une racine de* P *et* β *une racine de* Q, u *est tel que* $\mathbb{K}[\alpha, \beta] = \mathbb{K}[u \cdot \alpha + \beta]$.

Démonstration On prend u un élément de $\mathcal{F}$. Posons

$$\mathrm{S}^u_\alpha(\mathrm{X}) = \prod_{\beta\,:\,\mathrm{Q}} \big(\mathrm{X} - (u\cdot\alpha + \beta)\big).$$

C'est un polynôme de $\mathbb{K}[\alpha][\mathrm{X}]$; en fait on a $\mathrm{S}^u_\alpha(\mathrm{X}) = \mathrm{Q}_\alpha(\mathrm{X} - u\cdot\alpha)$. On pose ensuite

$$\mathrm{T}^u(\mathrm{X}) = \prod_{\alpha\,:\,\mathrm{P}} \mathrm{S}^u_\alpha(\mathrm{X}) = \prod_{\substack{\alpha\,:\,\mathrm{P}\\ \beta\,:\,\mathrm{Q}}} \big(\mathrm{X} - (u\cdot\alpha + \beta)\big).$$

On a $\mathrm{T}^u(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$. Quelles sont les racines de T^u ? Soient $n = \deg \mathrm{P}$ et $m = \deg_{\mathrm{Y}} \mathrm{Q}$. On a $\deg \mathrm{T}^u = n\cdot m$. Notons $\alpha_1, \ldots, \alpha_n$ les racines de P. Pour chaque α_i, le polynôme $\mathrm{Q}_{\alpha_i}(\mathrm{X})$ a m racines (on l'a supposé unitaire, donc il n'y a pas de risque de chute de degré). On les note $\beta_{i1}, \ldots, \beta_{im}$. Les racines de T^u sont les $\zeta^u_{ij} = u\cdot\alpha_i + \beta_{ij}$.

Soit $\widetilde{\mathrm{Q}}(\mathrm{X}) = \prod_{\alpha\,:\,\mathrm{P}} \mathrm{Q}_\alpha(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$. Les racines de $\widetilde{\mathrm{Q}}$ sont les β_{ij}.

Soit ζ^u une racine formelle de T^u.

La racine α vérifie

$$\begin{cases} \mathrm{P}(\alpha) &= 0 \\ \widetilde{\mathrm{Q}}(\zeta^u - u\cdot\alpha) &= 0. \end{cases}$$

Une racine α_k de $\mathrm{P}(\mathrm{X})$ n'est racine de $\widetilde{\mathrm{Q}}(\zeta^u_{ij} - u\cdot\mathrm{X})$ que si il existe ℓ tel que $\zeta^u_{ij} - u\cdot\alpha_k = \beta_\ell$, c.-à-d. $u\cdot\alpha_k + \beta_\ell = u\cdot\alpha_i + \beta_j$.

Choisissons $u_0 \in \mathcal{F}$ tel que

$$\forall i, j, k, \ell \text{ avec } i \neq k,\ \ u_0 \neq \frac{\beta_j - \beta_\ell}{\alpha_i - \alpha_k}.$$

Il existe de tels u_0 car d'une part si $i \neq k$, $\alpha_i - \alpha_k \neq 0$ (grâce à la séparabilité de P), et d'autre part $\mathcal{F}$ est infini, alors que seules un nombre fini de valeurs pour u sont proscrites. Nous allons voir dans peu de temps comment en choisir un de façon effective.

Posons $\mathrm{T} = \mathrm{T}^{u_0}$, et $\zeta = \zeta^{u_0}$.

On peut calculer dans $\mathbb{K}[\zeta]$ le pgcd suivant : $\mathrm{P}(\mathrm{X}) \wedge \widetilde{\mathrm{Q}}(\zeta - u_0\cdot\mathrm{X})$. D'après ce qui précède c'est un polynôme linéaire (c.-à-d. de degré 1) si u_0 est tel qu'on l'a choisi ; ceci est donc un moyen de choisir u_0 dans $\mathcal{F}$ par essais successifs.

Ce polynôme linéaire a pour unique racine α; il permet donc d'exprimer α sour la forme $a(\zeta)$. On a ensuite $\beta = \zeta - u\cdot\alpha = b(\zeta)$. □

Discussion Cette démonstration est un peu déroutante ; quelle est cette racine formelle non précisée ? au début c'est n'importe quelle racine. Si $\mathrm{P}(\mathrm{X})$ et $\mathrm{Q}_\alpha(\mathrm{X})$ sont irréductibles, ce théorème est exactement le théorème classique, tel qu'il est démontré par exemple dans [Wae], à quelques détails inessentiels près. Dans le cas général, il peut arriver que T ne soit pas irréductible.

Si on tient à identifer les racines par les indices, on a

$$\begin{array}{r} a(\zeta_{ij}) = \alpha_i \\ b(\zeta_{ij}) = \beta_{ij} \end{array}$$

Si P est unitaire on a $\prod_{\zeta\,:\,\mathrm{T}}\big(\mathrm{X}-a(\zeta)\big) = \mathrm{P}(\mathrm{X})^m$. On a aussi $\prod_{\zeta\,:\,\mathrm{T}}\big(\mathrm{X}-b(\zeta)\big) = \prod_{\alpha\,:\,\mathrm{P}} \mathrm{Q}_\alpha(\mathrm{X})$.

Si $\mathrm{T} = \mathrm{T}_1 \cdot \mathrm{T}_2$, calculons les polynômes suivants :

$$\begin{array}{l} p_1 = \prod_{\zeta\,:\,\mathrm{T}_1}\big(\mathrm{X} - a(\zeta)\big), \\ q_1 = \prod_{\zeta\,:\,\mathrm{T}_1}\big(\mathrm{X} - b(\zeta)\big), \end{array}$$

Un calcul de pgcd de p_1 et de P produira dans certains cas une factorisation de P. Si ça n'est pas le cas, on a $p_1 = \mathrm{P}^k$ avec $k < m$. Les racines de T_1 sont parmi les ζ_{ij} :

$$\begin{array}{ccc} \zeta_{11} & \cdots & \zeta_{1m} \\ \vdots & & \vdots \\ \zeta_{n1} & \cdots & \zeta_{nm} \end{array}$$

Il y en a k exactement dans chaque ligne du tableau ci-dessus. Alors le pgcd $q_1 \wedge \mathrm{Q}_\alpha$, calculé dans $\mathbb{K}[\alpha]$, fournit un facteur de degré k de Q_α.

Ainsi une factorisation de T produit une factorisation de P ou (non exclusif) de Q_α. Si on sait choisir quel facteur de ces deux polynômes on veut conserver, on sait choisir quel facteur de T nous intéresse.

Toute la théorie classique des extensions de corps peut être ré-écrite de cette façon, avec des polynômes non irréductibles.

2 Corps valués

Nous allons parcourir rapidement quelques notions classiques. Voici quelques références : [E], [Gou], [Kuh_2].

2.1 Premières définitions

En écrivant « groupe ordonné » nous sous-entendons toujours « groupe totalement ordonné ».

Soient $\mathbb{K}$ un corps et Γ un groupe ordonné abélien. Une application $v : \mathbb{K}^\times \longrightarrow \Gamma$ est une valuation si :
- $\forall x, y \in \mathbb{K}^\times,\ v(x \cdot y) = v(x) + v(y)$;
- $v(x + y) \geq \min(v(x), v(y))$.

On convient d'ajouter à Γ un nouvel élément noté ∞, de poser $v(0) = \infty$, et d'ordonner $\Gamma \cup \{\infty\}$ par $\gamma \leq \infty$ pour tout γ dans Γ. On pose également $\gamma + \infty = \infty$, de sorte que les propriétés ci-dessus restent valables.

L'application v est appelée une valuation, et (K, v) est un corps valué.

On vérifie facilement que si $v(x) < v(y)$, alors $v(x+y) = v(x) = \min(v(x), v(y))$.

Anneau des entiers

On note $\mathfrak{V}_{\mathbb{K}}$ ou simplement $\mathfrak{V}$ l'anneau suivant :

$$\mathfrak{V}_{\mathbb{K}} = \{x \in \mathrm{K} \,:\, v(x) \geq 0\}.$$

Le fait que c'est un anneau se déduit des axiomes donnés sur v. On en déduit également que

$$\mathfrak{M}_{\mathbb{K}} = \{x \in \mathrm{K} \,:\, v(x) > 0\}.$$

(noté plus simplement $\mathfrak{M}$) est un idéal maximal de $\mathfrak{V}_{\mathbb{K}}$; en outre, son complémentaire est $\mathfrak{V}^{\times}$, l'ensemble des inversibles de $\mathfrak{V}$: $\mathfrak{M}$ est donc l'unique idéal maximal de $\mathfrak{V}$.

Anneaux de valuation et anneaux locaux

Il est temps d'ouvrir une courte parenthèse sur ce sujet.

Définition Un anneau intègre qui vérifie la propriété suivante est un *anneau de valuation* :

$$\forall x\, \forall y\, \exists a \quad x = a \cdot y \lor y = a \cdot x.$$

On abrège $\exists a\ x = a \cdot y$ en $y|x$ (« *y divise x* »). La propriété devient

$$\forall x, y \quad x|y \lor y|x.$$

Il est facile de vérifier que $\mathfrak{V}_{\mathbb{K}}$ est un anneau de valuation. Inversement si $\mathbb{A}$ est un anneau de valuation, soit $\mathbb{K} = \operatorname{Frac} \mathbb{A}$ son corps de fractions ; soit Γ le groupe quotient $\mathbb{K}^{\times}/\mathbb{A}^{\times}$ et v l'application quotient canonique $\mathbb{K}^{\times} \longrightarrow \mathbb{K}^{\times}/\mathbb{A}^{\times} = \Gamma$. On ordonne Γ par $v(x) < v(y)$ si $x|y$ (c.-à-d. $y/x \in \mathfrak{V}$) ; alors $(\mathbb{K}, v)$ est un corps valué.

Définition Un anneau $\mathfrak{V}$ qui a la propriété d'avoir un unique idéal maximal $\mathfrak{M}$ est appelé un *anneau local*. Il est facile de vérifier (en maths classiques) que le complémentaire $\mathfrak{V} \setminus \mathfrak{M}$ de cet idéal maximal est l'ensemble $\mathfrak{V}^{\times}$ des éléments inversibles (les unités) de l'anneau. En effet si x n'est pas inversible, alors le lemme de Zorn permet de montrer qu'il existe un idéal maximal contenant x ; on conclut que $x \in \mathfrak{M}$.

Remarque L'anneau trivial $\{0\}$ ne satisfait pas la définition ci-dessus ; cependant, par convention, on le considèrera comme un anneau local.

Tout anneau de valuation est local, mais la réciproque n'est pas vraie, comme nous le verrons plus loin. Être un anneau local est en fait également une propriété du premier ordre :

$$\forall x\, \exists a \quad a \cdot x = 1 \lor a \cdot (1 + x) = 1.$$

L'anneau trivial vérifie cette propriété (ce qui justifie la convention mentionnée ci-dessus). Il est facile de vérifier que tout anneau local non trivial doit également vérifier cette propriété : en effet si x et $1+x$ ne sont pas inversibles, ils doivent être tous deux dans $\mathfrak{M}$ et donc $1 \in \mathfrak{M}$, ce qui contredit $\mathrm{V} \setminus \mathfrak{M} = \mathfrak{V}^{\times}$.

Inversement, si cette propriété est vérifiée dans un anneau non trivial $\mathfrak{V}$, il faut montrer que

$$\mathfrak{M} = \{x \in \mathfrak{V} \ : \ x \text{ non inversible}\}$$

est un idéal maximal. Si c'est un idéal, il est clairement maximal ; le seul point délicat est

$$x, y \in \mathfrak{M} \Longrightarrow x + y \in \mathfrak{M}.$$

Tout d'abord constatons que dans un tel anneau on a

$$a + b = 1 \Longrightarrow a \text{ inversible} \vee b \text{ inversible} ;$$

ceci découle naturellement de $a = 1 - b$: on a $-b$ ou $1 - b$ inversible. Soient alors x, y tels que $x + y \notin \mathfrak{M}$; notons $(x + y)^{-1}$ l'inverse de $x + y$. Posons $a = x \cdot (x + y)^{-1}$ et $b = y \cdot (x + y)^{-1}$. On a $a + b = 1$ et donc a ou b inversible.

Si a inversible, alors soit a^{-1} son inverse ; on a $x \cdot (x + y)^{-1} \cdot a^{-1} = 1$ et donc x est inversible. De même, si b inversible, alors y est inversible.

Nous avons prouvé

$$x + y \in \mathfrak{V}^{\times} \Longrightarrow x \in \mathfrak{V}^{\times} \vee y \in \mathfrak{V}^{\times},$$

ce qui est équivalent au résultat annoncé.

Corps résiduel

Le *corps résiduel* d'un anneau local $\mathfrak{V}$, d'idéal maximal $\mathfrak{M}$, est $\mathfrak{V}/\mathfrak{M}$. Dans le cas de l'anneau de valuation $\mathfrak{V}_{\mathbb{K}}$ d'un corps valué $(\mathbb{K}, v)$, on notera le corps résiduel $\Bbbk = \mathfrak{V}_{\mathbb{K}}/\mathfrak{M}_{\mathbb{K}}$. On désignera l'application canonique de $\mathfrak{V}_{\mathbb{K}}$ dans $\Bbbk$ par $x \mapsto \overline{x}$. La classe $\overline{x}$ de x modulo $\mathfrak{M}$ est appelée *résidu de x*.

2.2 Quelques exemples

Anneaux locaux

« Y a-t-il des anneaux locaux qui ne sont pas des anneaux de valuation ? » L'expert répond sans hésitation : « le localisé d'une courbe algébrique en un point non régulier », ou bien : « le localisé d'une surface algébrique en un point ». Nous allons en donner un exemple explicite, afin de clarifier (un tout petit peu) le sens de cette formule.

Localisé Soit S une partie multiplicative d'un anneau $\mathbb{A}$, c.-à-d. $x, y \in \mathrm{S} \Longrightarrow x \cdot y \in \mathrm{S}$. On note $\mathrm{S}^{-1}\mathbb{A}$ l'anneau suivant :

$$\mathrm{S}^{-1}\mathbb{A} = \left\{ \frac{x}{s} \ : \ x \in \mathbb{A}, \ s \in \mathrm{S} \right\}.$$

On considère bien entendu que

$$\frac{x}{s} = \frac{y}{t} \iff \exists s' \in \mathrm{S},\ \big(x \cdot t - y \cdot s\big) \cdot s' = 0.$$

Les lois d'addition et de multiplication sont intuitives :

$$\frac{x}{s} + \frac{y}{t} = \frac{x \cdot t + y \cdot s}{t \cdot s}, \text{ et } \frac{x}{s} \cdot \frac{y}{t} = \frac{x \cdot y}{t \cdot s}.$$

Soit maintenant $\mathfrak{P}$ un idéal premier de $\mathbb{A}$. Alors $\mathrm{S} = \mathbb{A} \setminus \mathfrak{P}$ est une partie multiplicative de $\mathbb{A}$; on note $\mathbb{A}_{\mathfrak{P}}$ l'anneau $\mathrm{S}^{-1}\mathbb{A}$, qu'on appelle *le localisé de* $\mathbb{A}$ *en* $\mathfrak{P}$.

L'idéal $\mathfrak{P}$ donne naissance à un idéal $\mathrm{S}^{-1}\mathfrak{P}$, qui est précisément l'ensemble des éléments non inversibles de $\mathbb{A}_{\mathfrak{P}}$, et qui est son unique idéal maximal.

Un exemple Soit le polynôme $\mathrm{P}(x, y) = x \cdot y \in \mathbb{Q}[x, y]$. L'anneau de fonctions de la courbe algébrique associée (l'union des deux droites $x = 0$ et $y = 0$) est

$$\mathbb{A} = \mathbb{Q}[x, y] \Big/ \langle \mathrm{P}(x, y) \rangle \cdot$$

Un bon système exact de représentant des classes pour ce quotient est l'ensemble des expressions $p(x) + q(y)$, où la multiplication se fait avec la convention $x \cdot y = 0$. Dans le but qui nous anime, on les écrira encore mieux sous la forme $a + x \cdot p(x) + y \cdot q(y)$ où $a \in \mathbb{Q}$, $p(x) \in \mathbb{Q}[x]$ et $q(y) \in \mathbb{Q}[y]$.

L'idéal associé au point non lisse $(0, 0)$ est celui des fonctions qui s'annulent en ce point :

$$\mathfrak{P} = \{x \cdot p(x) + y \cdot q(y) \ : \ p(x) \in \mathbb{Q}(x),\ q(y) \in \mathbb{Q}(y)\}.$$

L'anneau qui nous intéresse est

$$\mathbb{A}_{\mathfrak{P}} = \left\{ \frac{a + x \cdot p(x) + y \cdot q(y)}{b + x \cdot r(x) + y \cdot s(y)} \ : \ b \neq 0 \right\}$$

muni des lois naturelles.

Si un élément α de $\mathbb{A}_{\mathfrak{P}}$ est non inversible, c'est que son dénominateur est de la forme $x \cdot p(x) + y \cdot q(y)$; il est alors facile de vérifier que ce n'est pas le cas de $1 + \alpha$ qui est donc inversible. Ainsi l'anneau $\mathbb{A}_{\mathfrak{P}}$ est bien local ; par contre ce n'est pas un anneau de valuation car x ne divise pas y plus que y ne divise x.

Un autre exemple Soit $\mathbb{A} = \mathbb{Q}[x, y]$ (l'anneau de fonctions du plan) et

$$\mathfrak{P} = \{\mathrm{P}(x, y) \ : \ \mathrm{P}(0, 0) = 0\}.$$

Le localisé au point lisse $(0, 0)$ est $\mathbb{A}_{\mathfrak{P}}$; on vérifie de même que x ne divise pas y et y ne divise pas x.

Corps valués

Il est très utile d'avoir divers modèles en tête afin de mieux comprendre les énoncés relatifs aux corps valués.

Quelques valuations discrètes Soit $\Bbbk$ un corps quelconque. On peut munir $\Bbbk[\mathrm{X}]$ d'une valuation de diverses façons. Ainsi on peut poser

$$v_\infty(f) = -\deg f$$

On étend bien sûr v_∞ à $\mathbb{K} = \Bbbk(\mathrm{X})$ par $v(f/g) = v(f) - v(g)$.

Ceci fait de $\mathbb{K}$ un corps valué, de groupe de valuation $\mathbb{Z}$ (on parle alors de *valuation discrète*), et de corps résiduel $\Bbbk$. On a

$$\mathfrak{V}_{\mathbb{K}} = \left\{ \frac{f(x)}{g(x)} \ : \ \lim_{x\to\infty} \frac{f(x)}{g(x)} < \infty \right\} ;$$

et l'application canonique de $\mathfrak{V}_{\mathbb{K}}$ dans $\Bbbk$ est

$$\frac{f(x)}{g(x)} \mapsto \lim_{x\to\infty} \frac{f(x)}{g(x)}.$$

Cette valuation est appelée *la valuation à l'infini* de $\mathbb{K} = \Bbbk[\mathrm{X}]$.

Une autre valuation classique est la *valuation en* 0 :

$$v_0\left(\sum_i a_i \cdot \mathrm{X}^i\right) = \min\{i \ : \ a_i \neq 0\}.$$

Cette fois-ci l'anneau de valuation est celui des fractions rationnelles définies en $\mathrm{X} = 0$; le corps résiduel est $\Bbbk$, et l'application canonique de $\mathfrak{V}_{\mathbb{K}}$ dans $\Bbbk$ est l'évaluation en 0.

Plus généralement, si $\mathrm{P(X)} \in \Bbbk[\mathrm{X}]$ est un polynôme irréductible, on peut définir

$$v_{\mathrm{P}}(f) = \max\{i \ : \ \mathrm{P}^i \mid f\}.$$

On remarque que v_0 coïncide avec v_{X}.

Si $\mathrm{P(X)} = \mathrm{X} - a$, on note la valuation associée v_a et on l'appelle *valuation en a* ; le corps résiduel est dans ce cas encore une fois $\Bbbk$, $\mathfrak{V}_{\mathbb{K}}$ est l'anneau des fractions définies en a, et le passage au quotient est l'évaluation en a.

Si P est de degré strictement plus grand que 1, soit $\Bbbk[\alpha]$ un corps de rupture de P (on pose $\mathrm{P}(\alpha) = 0$) ; le corps résiduel de $\mathbb{K}$ pour la valuation v_{P} est naturellement isomorphe à $\Bbbk[\alpha]$. L'anneau de valuation est cette fois constitué des fractions rationnelles « définies en α » et l'application quotient est l'évaluation en α.

Le corps $\mathbb{K} = \Bbbk((\mathrm{X}))$ des séries de Laurent à coefficients dans $\Bbbk$ peut être muni de la valuation v_0 :

$$v_0\left(\sum_{i>n} a_i \cdot \mathrm{X}^i\right) = \min\{i > n \ : \ a_i \neq 0\}.$$

Tout se passe comme pour $\Bbbk(\mathrm{X})$. On pourra bien sûr faire la même chose pour les séries de Puiseux. Le corps des séries de Laurent est le complété de $\mathbb{K}(\mathrm{X})$ pour la métrique associée à la valuation v_0.

Quelques valuations non discrètes Nous nous intéresserons plus particulièrement aux énoncés du premier ordre (par nécessité, car ce sont ceux là qui sont naturellement accessibles aux méthodes constructives). Or « être un corps de valuation discrète » n'est pas une propriété du premier ordre. Il est donc utile de connaître quelques exemples de valuations non discrètes.

Soit Γ un groupe ordonné abélien. On note $\Gamma^{>0}$ l'ensemble des élements positifs de Γ. On peut généraliser la notion de polynôme : soit $\Bbbk[\Gamma]$ l'ensemble des sommes finies de la forme

$$a_1 \cdot \mathrm{X}^{\gamma_1} + \cdots + a_n \cdot \mathrm{X}^{\gamma_n},\ \forall i\ a_i \in \Bbbk,\ \gamma_i \in \Gamma^{>0}.$$

Les règles d'addition et de multiplication sont intuitives : on a en particulier $a \cdot \mathrm{X}^{\gamma} + b \cdot \mathrm{X}^{\gamma} = (a+b) \cdot \mathrm{X}^{\gamma}$ et $(a \cdot \mathrm{X}^{\gamma}) \times (b \cdot \mathrm{X}^{\lambda}) = (ab \cdot \mathrm{X}^{\gamma+\lambda})$. On étend ces règles pour faire de $(\mathbb{K}[\Gamma], +, \times)$ un anneau.

On pose $v(\sum_{i=1}^{n} a_i \cdot \mathrm{X}^{\gamma_i}) = \min\{\gamma_i\ :\ a_i \neq 0\}$, en supposant que les γ_i sont deux à deux distincts. Cette valuation s'étend de façon naturelle à $\Bbbk(\Gamma)$, le corps des fractions de $\Bbbk[\Gamma]$; son groupe de valuation est Γ.

Caractéristique mixte : les nombres p-adiques

Dans les exemples précédents, la caractéristique du corps valué $\mathbb{K}$ et de son résidu $\Bbbk$ sont égales; mais il est possible que la caractéristique de $\mathbb{K}$ soit nulle tandis que celle de $\Bbbk$ est p (un nombre premier).

Les nombres p-adiques L'exemple le plus simple et le plus classique est constitué par $\mathbb{K} = \mathbb{Q}$ muni de la valuation p-adique v_p. Pour $a \in \mathbb{Z} \setminus \{0\}$ on pose

$$v_p(a) = \max\{i\ :\ p^i | a\}\,;$$

et on prolonge cette valuation à $\mathbb{Q}^{\times}$ tout entier en posant $v(a/b) = v(a) - v(b)$.

C'est une valuation discrète. On vérifie que le corps résiduel est $\mathbb{F}_p$.

Le complété de $(\mathbb{Q}, v_p)$ pour la métrique induite par v_p est le *corps des nombres p-adiques*. Son anneau d'entiers est noté $\mathbb{Z}_p$, et l'idéal maximal en est $p\mathbb{Z}_p$. On peut le présenter *ex nihilo* comme suit :

$$\mathbb{Z}_p = \big\{a_0 + a_1 \cdot p + \cdots + a_i \cdot p^i + \cdots\ :\ \forall i,\ a_i \in \{0, \ldots, p-1\}\big\}\,;$$

il s'agit de « séries formelles en p ». On munit $\mathbb{Z}_p$ de lois *ad hoc* pour en faire un anneau. On pose

$$\sum_i a_i \cdot p^i + \sum_i b_i \cdot p^i = \sum_i c_i \cdot p^i$$

où les c_i sont obtenus de la façon suivante :
- on pose $r_0 = 0$;
- si $a_i + b_i + r_i < p$, $c_i = (a_i + b_i) + r_i$ et $r_{i+1} = 0$;
- si $a_i + b_i + r_i \geq p$, $c_i = (a_i + b_i - p) + r_i$ et $r_{i+1} = 1$.

Il s'agit en fait de faire une addition (en base p) en « propageant la retenue vers la droite ». Pour la multiplication, l'intuition est la même, mais c'est un peu plus compliqué à écrire : pour $a \in \{0, \dots, p-1\}$, on pose

$$a \cdot \sum_i b_i \cdot p^i = \sum_i c_i \cdot p_i$$

où les c_i sont obtenus de la façon suivante :
- on pose $r_0 = 0$;
- on écrit $a \cdot b_i + r_i = c_i + r_{i+1} \cdot p$, où $c_i, r_{i+1} \in \{0, \dots, p-1\}$.

Puis on écrit

$$\left(\sum_i a_i \cdot p^i\right) \cdot \left(\sum_i b_i \cdot p^i\right) = a_0 \cdot \left(\sum_i a_i \cdot p^i\right) + a_1 \cdot \left(\sum_i a_i \cdot p^{i+1}\right) + \cdots$$

Cette somme infinie a bien un sens, car seul un nombre fini de termes participent à un coefficient donné du résultat.

On vérifie que ces lois font de $\mathbb{Z}_p$ un anneau. $\mathbb{N}$ s'injecte dans $\mathbb{Z}_p$ en envoyant $a \in \mathbb{N}$ sur sa représentation en base p ; l'image de $\mathbb{N}$ est alors constitué des « séries finies ». L'addition et la multiplication de $\mathbb{Z}_p$, restreintes à l'image de $\mathbb{N}$ correspondent aux opérations usuelles. On peut ensuite injecter $\mathbb{Z}$ dans $\mathbb{Z}_p$ en remarquant que -1 est représenté naturellement par la série suivante :

$$-1 = (p-1) + (p-1) \cdot p + (p-1) \cdot p^2 + \cdots$$

Il est facile de vérifier que les unités de $\mathbb{Z}_p$ sont les $a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots$ avec $a_0 \neq 0$. On pose

$$v_p\left(\sum_i a_i \cdot p^i\right) = \min\{i \ : \ a_i \neq 0\}.$$

On pose ensuite $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$. On a $\mathbb{Q}_p = \bigcup_{k \in \mathbb{N}} p^{-k} \cdot \mathbb{Z}_p$.

Il est assez facile de vérifier que $\mathbb{Q}_p$ est un corps complet (pour v_p) qui contient $\mathbb{Q}$, et que tout élément de $\mathbb{Q}_p$ est limite (pour la topologie de v_p) d'une suite de Cauchy de rationnels. C'est donc bien le complété de $\mathbb{Q}$.

Extensions de $\mathbb{Q}_p$ Le moyen le plus simple de fournir quelques autres exemples de valuations de caractéristique mixte consiste à prendre des extensions algébriques ou transcendantes de $\mathbb{Q}_p$. On se contentera ici de parler très brièvement du cas transcendant.

Ainsi on peut définir une valuation w sur $\mathbb{Q}_p(\mathrm{X})$ en posant

$$w(a_i \cdot \mathrm{X}^i + a_{i+1} \cdot \mathrm{X}^{i+1} + \cdots + a_n \cdot \mathrm{X}^n) = (i, v_p(a_i)) \in \mathbb{Z} \times \mathbb{Z}$$

pour $a_i \neq 0$, et $w(f/g) = w(f) - w(g)$. On ordonne le groupe $\mathbb{Z} \times \mathbb{Z}$ par l'ordre lexicographique ; w est bien une valuation.

Plus généralement si $\mathbb{Z}$ est vu comme plongé dans un autre groupe ordonné Γ, et si $\gamma \in \Gamma \setminus \mathbb{Z}$, on peut poser

$$w\left(\sum a_i \cdot \mathrm{X}^i\right) = \min\{v_p(a_i) + i \cdot \gamma\}$$

et on obtient une valuation dans le sous groupe de Γ engendré par $\mathbb{Z}$ et γ.

2.3 Autour des valuations

Voici quelques notions en rapport direct avec les valuations.

Extensions algébriques

Si $(\mathbb{K}, v)$ est un corps valué, et $\mathbb{L}$ une extension algébrique de $\mathbb{K}$, soit w une valuation sur $\mathbb{L}$; on dit que w est une extension de v si pour tout $x \in \mathbb{K}$, $v(x) \geq 0 \Longrightarrow w(x) \geq 0$. En terme d'anneaux de valuation, si $\mathfrak{V}_{\mathbb{K}}$ est l'anneau d'entiers associé à v et $\mathfrak{V}_{\mathbb{L}}$ est celui associé à w, cela s'écrit $\mathfrak{V}_{\mathbb{K}} = \mathfrak{V}_{\mathbb{L}} \cap \mathbb{K}$.

On peut prouver le théorème suivant :

¶ **Théorème 6 (Clôture algébrique valuée)** *Soit $(\mathbb{K}, v)$ un corps valué. La valuation v peut être étendue en une valuation w de $\mathbb{K}^{ac}$.*

En général, l'extension de v à $\mathbb{K}^{ac}$ n'est pas unique.

Dans sa version classique ce théorème est non constructif; une autre version, plus faible du point de vue constructif (mais équivalente du point de vue classique, via le théorème de compacité de la théorie des modèles) est prouvée dans [CLR] : il s'agit de la cohérence relative de la théorie des corps valués algébriquement clos et de la théorie des corps valués.

Places

Le vocabulaire des *places* est un autre point de vue sur les corps valués. Une place P d'un corps $\mathbb{K}$ vers $\Bbbk$ est une application $\mathrm{P} : \mathbb{K} \longrightarrow \Bbbk \cup \{\infty\}$, qui vérifie les propriétés suivantes :

– $\mathrm{P}(x+y) = \mathrm{P}x + \mathrm{P}y$ et $\mathrm{P}(x \cdot y) = \mathrm{P}x \cdot \mathrm{P}y$ (pour $\mathrm{P}x, \mathrm{P}y \neq \infty$) ;
– pour $x \neq 0$, $\mathrm{P}x = \infty \Longleftrightarrow \mathrm{P}(x^{-1}) = 0$.

Alors $\mathrm{P}^{-1}(\Bbbk)$ est un anneau de valuation de $\mathbb{K}$, d'idéal maximal $\mathrm{P}^{-1}(\{0\})$, et de corps résiduel $\Bbbk$.

Inversement, étant donné un corps valué, l'application quotient de son anneau de valuation $\mathfrak{V}$ vers $\mathfrak{V}/\mathfrak{M}$ est une place (on pose $\mathrm{P}x = \infty$ pour tout $x \notin \mathfrak{V}$).

Métrique & topologie associées

On présente souvent les valuations au moyen des valeurs absolues. Si $(\Gamma, +, \leq)$ est un sous-groupe de $(\mathbb{R}, +, \leq)$, on peut en effet poser

$$|x| = 2^{-v(x)}$$

(avec la convention $2^{-\infty} = 0$) afin d'obtenir une valeur absolue sur $\mathbb{K}$ (ce que le lecteur vérifiera sans mal). On obtient ainsi une distance $d(x, y) = |x - y|$. L'inégalité triangulaire est vérifiée, et on a même une inégalité beaucoup plus forte :

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}.$$

Cette distance fait de $\mathbb{K}$ un espace *ultramétrique* (terminologie due à Krasner). Les propriétés en sont inhabituelles :

- tout triangle est isocèle ;
- pour $a \in \mathbb{R}$ et $x \in \mathbb{K}$ on pose $\mathrm{D}^\circ(x,a) = \{y \in \mathbb{K} \ : \ d(x,y) < a\}$; c'est le *disque ouvert de centre x et de rayon a*. Alors dès que $y \in \mathrm{D}^\circ(x,a)$, on a $\mathrm{D}^\circ(y,a) = \mathrm{D}^\circ(x,a)$: tout point d'un disque ouvert est en est le centre ! On a également, pour $a \leq b \in \mathbb{R}$, $\mathrm{D}^\circ(x,a) \cap \mathrm{D}^\circ(x,b) = \varnothing$ ou $\mathrm{D}^\circ(x,a) \subseteq \mathrm{D}^\circ(y,b)$: deux disques sont disjoints ou emboîtés.

Ces faits sont faciles à prouver : nous les laissons à la lectrice. Des propriétés analogues sont vraies pour les disques fermés. La figure 1 représente les diverses configurations possibles pour les triangles et les disques (ouverts ou fermés).

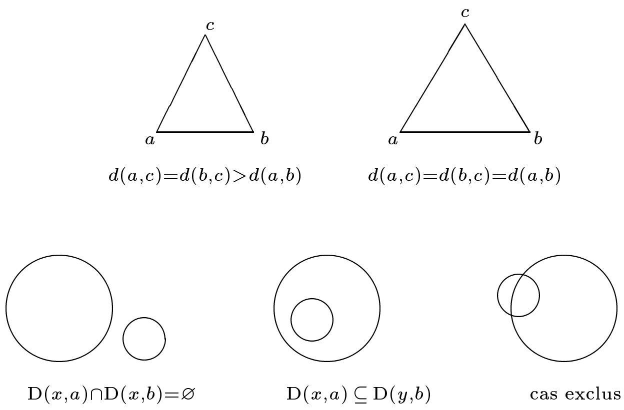


Figure 1 : Triangles & disques.

Même si Γ ne peut pas être plongé comme groupe ordonné dans $\mathbb{R}$, on peut définir une topologie sur $\mathbb{K}$ en considérant les disques ouverts de centre x : $\mathrm{B}^\circ_{x,\alpha} = \{y \in \mathbb{K} \ : \ v(x-y) > \alpha\}$, pour $\alpha \in \Gamma$, comme une base de voisinages de x. De manière générale, on pourra penser à la valuation comme à une distance, au détail près que « grande valuation » signifie « petite distance ».

Décomposition du disque fermé Un disque fermé

$$\mathrm{B}_{a,\alpha} = \{x \ : \ v(x-a) \geq \alpha\}$$

dans $(\mathbb{K}, v)$ peut être décrit comme une union de disques ouverts de même rayon ; les disques de cette union sont indicés par $\Bbbk$, le corps résiduel de $\mathbb{K}$.

Nous allons détailler cette construction dans le cas $\mathfrak{V} = \mathrm{B}_{0,0} = \{x : v(x) \geq 0\}$. La relation binaire $x \equiv y$ définie par $v(x-y) > 0$ est une relation d'équivalence sur $\mathbb{K}$ tout entier, et sur $\mathfrak{V}$. Les classes d'équivalence de cette relation sont des disques ouverts $\mathrm{B}^\circ_{a,0} = \{x \ : \ v(x-a) > 0\}$; si $a \in \mathfrak{V}$, alors $\mathrm{B}^\circ_{a,0} \subseteq \mathfrak{V}$. Ceci montre que $\mathfrak{V}$ est une union de disques $\mathrm{B}^\circ_{a,0}$; nous allons donner une bijection entre l'ensemble de ces disques et $\Bbbk$.

Pour tout $\xi \in \Bbbk$ soit $\phi(\xi)$ une unité de $\mathfrak{V}$ de résidu ξ. On envoie $\xi \in \Bbbk$ sur la classe de $\phi(\xi)$. Il est facile de vérifier que cette classe ne dépend pas du choix de $\phi(\xi)$: en effet si $x, y \in \mathfrak{V}$ ont même résidu $\overline{x} = \overline{y} = \xi$, alors $v(x-y) > 0$ et $\mathrm{B}^\circ_{x,0} = \mathrm{B}^\circ_{y,0}$. L'application obtenue est bien une bijection.

Soit $\mathrm{B} = \mathrm{B}_{a,\delta}$ un disque fermé quelconque ; soit d de valuation δ ; l'application $\phi \,:\, x \mapsto \dfrac{x-a}{d}$ est une bijection de $\mathrm{B}_{a,\delta}$ vers $\mathfrak{V}$.

Le choix de ϕ n'est pas canonique : tout point de B en est un centre et d est défini à une unité près. Elle permet d'écrire $\mathrm{B}_{a,\delta}$ comme union de boules ouvertes $\mathrm{B}^\circ_{x,\delta}$; ces boules ouvertes sont indépendantes du choix de a et d : ce sont les classes d'équivalence de la relation $x \sim y \iff v(x-y) > \delta$. Par contre la bijection de $\Bbbk$ vers les membres de cette union n'est pas canonique, et dépend du choix de a et d.

Nous retrouverons cette décomposition en IV.3.

Groupes ordonnés abéliens

Rappelons que les groupes ordonnés que nous considérons sont toujours totalement ordonnés.

L'exemple le plus simple est $\Gamma = \mathbb{Z}$ avec la loi + usuelle et l'ordre usuel ; mais tous les sous-groupes additifs de $\mathbb{R}$ sont des groupes ordonnés abéliens. Il y a des groupes ordonnés qui ne peuvent pas être plongés dans $\mathbb{R}$, car ils ne sont pas archimédiens, comme $\mathbb{Z} \times \mathbb{Z}$ (avec la loi + composante par composante et l'ordre lexicographique).

Sous-groupes convexes et valuations Soit Γ un groupe ordonné abélien ; soit $\Delta \subseteq \Gamma$ un sous-groupe de Γ. On dit que Δ est un *sous-groupe convexe* de Γ si

$$\forall \delta \in \Delta,\ \delta > 0,\ -\delta < \gamma < \delta \Longrightarrow \gamma \in \Delta.$$

Dans ce cas, la relation d'ordre de Γ passe naturellement au quotient $\Gamma/_{\Delta}$.

Soit $v : \mathbb{K}^\times \longrightarrow \Gamma$ une valuation sur un corps $\mathbb{K}$ et Δ un sous-groupe convexe de Γ. Il y a une manière naturelle de définir une valuation $v_\Delta : \mathbb{K}^\times \longrightarrow \Gamma/_{\Delta}$:

$$v_\Delta \,:\, x \mapsto v(x) + \Delta \in \Gamma/_{\Delta}.$$

Si $(\mathfrak{V}_\mathbb{K}, \mathfrak{M}_\mathbb{K})$ et $(\mathfrak{V}'_\mathbb{K}, \mathfrak{M}'_\mathbb{K})$ sont les anneaux de valuations associés à v et v_Δ, on a

$$\mathfrak{V}_\mathbb{K} \subseteq \mathfrak{V}'_\mathbb{K} \text{ et } \mathfrak{M}'_\mathbb{K} \subseteq \mathfrak{M}_\mathbb{K}.$$

Inversement, tout anneau $\mathbb{A}$ tel que $\mathfrak{V}_\mathbb{K} \subseteq \mathbb{A} \subseteq \mathbb{K}$ est un anneau de valuation, et il lui correspond un sous-groupe convexe Δ de Γ tel que la valuation v' associée à $\mathbb{A}$ soit précisément la valuation v_Δ.

La valuation v_Δ est *plus grossière* que la valuation v. Le corps résiduel de v_Δ admet naturellement une valuation w dans le groupe Δ : pour $a \in \mathfrak{V}'_\mathbb{K} \setminus \mathfrak{M}'_\mathbb{K}$, on pose $w(a + \mathfrak{M}'_\mathbb{K}) = v(a)$; c'est bien un élément de Δ car $v_\Delta(a) = 0$ est équivalent à $v(a) \in \Delta$.

Nous donnerons plus bas (composition de places) plus de détails sur cette situation ; pour l'instant nous voulons parler du rang des groupes ordonnés.

Rang Il est facile de vérifier que si Δ et Δ' sont deux sous-groupes convexes d'un groupe totalement ordonné Γ, distincts, alors $\Delta \subset \Delta'$ ou $\Delta' \subset \Delta$; ainsi l'ensemble des sous-groupes convexes stricts de Γ est totalement ordonné. Le rang de Γ est le type de l'ordre de cet ensemble. En particulier (et c'est le cas classique), cela peut-être un entier supérieur ou égal à 1.

On peut montrer que les propriétés suivantes sont équivalentes :
- Γ est de rang 1 ;
- Γ est archimédien (c.-à-d. si $0 < \gamma < \lambda \in \Gamma$, il existe $n \in \mathbb{N}$ tel que $n \cdot \gamma > \lambda$) ;
- Γ est isomorphe à un sous groupe de $(\mathbb{R}, +, \leq)$.

Ceci fournit un grand nombre d'exemples de groupes de rang 1. Si Γ_1, Γ_2 sont des groupes ordonnés de rang $r_1, r_2 \in \mathbb{N}$, le produit $\Gamma_1 \times \Gamma_2$ ordonné par l'ordre lexicographique est de rang $r_1 + r_2$.

Ainsi $\mathbb{Z} \times \mathbb{Z}$ et $\mathbb{Q} \times \mathbb{Z}$ sont de rang 2. On peut généraliser le produit lexicographique de groupes ordonnés pour obtenir des groupes de rang α où α est un ordinal quelconque : si pour tout $\beta < \alpha$, Γ_β est un groupe de rang 1, le groupe $\prod_{\beta<\alpha} \Gamma_\beta$, muni de l'ordre

$$(\gamma_\beta)_{\beta<\alpha} < (\lambda_\beta)_{\beta<\alpha} \iff \begin{cases} \beta_0 = \min\{\beta \ : \gamma_\beta \neq \lambda_\beta\} \\ \gamma_{\beta_0} < \lambda_{\beta_0} \end{cases}$$

est un groupe de rang α.

Composition de places

Soit $\mathrm{P} \ : \ \mathbb{K} \longrightarrow \Bbbk$ une place et $\mathrm{P}' \ : \ \Bbbk \longrightarrow \mathbb{l}$ une autre place ; il est naturel d'examiner la composition $\mathrm{P}'\mathrm{P} \ : \ \mathbb{K} \longrightarrow \mathbb{l}$. Ceci correspond à la situation où le corps résiduel d'un corps valué est lui-même muni d'une valuation.

Soient $\mathfrak{V}_\mathbb{K}$ et $\mathfrak{V}'_\mathbb{K}$ les anneaux de valuation de $\mathbb{K}$ associés respectivement à P et P′P. L'anneau de valuation de $\Bbbk$ associé à P′ est $\mathfrak{V}_\Bbbk$.

Nous allons nous contenter de relier les groupes de valuation $\Gamma_\mathbb{K} = \mathbb{K}^\times / \mathfrak{V}_\mathbb{K}^\times$, $\Gamma'_\mathbb{K} = \mathbb{K}^\times / \mathfrak{V}'^\times_\mathbb{K}$ et $\Gamma_\Bbbk = \Bbbk^\times / \mathfrak{V}_\Bbbk^\times$.

On note $1 + \mathfrak{M}_\mathbb{K}$ le groupe multiplicatif $\{1 + \nu \ : \ \nu \in \mathfrak{M}_\mathbb{K}\}$ (c'est *le groupe des* 1-*unités*). Le groupe multiplicatif $\Bbbk^\times$ est naturellement isomorphe au quotient de groupes multiplicatifs suivant :

$$\mathfrak{V}_\mathbb{K}^\times / 1 + \mathfrak{M}_\mathbb{K}.$$

On a la chaîne d'inclusions de groupes multiplicatifs suivante :

$$1 + \mathfrak{M}_\mathbb{K} \subseteq 1 + \mathfrak{M}'_\mathbb{K} \subseteq \mathfrak{V}'^\times_\mathbb{K} \subseteq \mathfrak{V}^\times_\mathbb{K} \subseteq \mathbb{K}^\times.$$

D'autre part l'image de $\mathfrak{V}_\mathbb{K}^\times$ par P est $\Bbbk^\times$, alors que celle de $\mathfrak{V}'_\mathbb{K}$ est $\mathfrak{V}_\Bbbk^\times$; P est dans les deux cas un morphisme de groupes multiplicatifs, de noyau $1 + \mathfrak{M}_\mathbb{K}$. On a les suites exactes suivantes entre groupes multiplicatifs :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 + \mathfrak{M}_\mathbb{K} & \longrightarrow & \mathfrak{V}_\mathbb{K}^\times & \xrightarrow{\mathrm{P}} & \Bbbk^\times & \longrightarrow & 1 \\ 1 & \longrightarrow & 1 + \mathfrak{M}_\mathbb{K} & \longrightarrow & \mathfrak{V}'^\times_\mathbb{K} & \xrightarrow{\mathrm{P}} & \mathfrak{V}_\Bbbk^\times & \longrightarrow & 1 \end{array}$$

et donc

$$\mathfrak{V}_{\mathbb{K}}^{\times}/\mathfrak{V}_{\mathbb{K}}'^{\times} \cong \mathfrak{V}_{\mathbb{K}}^{\times}/1+\mathfrak{M}_{\mathbb{K}} \Big/ {\mathfrak{V}_{\mathbb{K}}'^{\times}/1+\mathfrak{M}_{\mathbb{K}}} \cong \Bbbk^{\times}/\mathfrak{V}_{\Bbbk}^{\times} = \Gamma_{\Bbbk}.$$

Alors l'isomorphisme

$$\mathbb{K}^{\times}/\mathfrak{V}_{\mathbb{K}}^{\times} \cong \mathbb{K}^{\times}/\mathfrak{V}_{\mathbb{K}}'^{\times} \Big/ {\mathfrak{V}_{\mathbb{K}}^{\times}/\mathfrak{V}_{\mathbb{K}}'^{\times}}$$

permet de conclure que $\Gamma_{\mathbb{K}} \cong \Gamma'_{\mathbb{K}}/\Gamma_{\Bbbk}$. La façon dont $\Gamma_{\Bbbk}$ se plonge dans $\Gamma'_{\mathbb{K}}$ est naturelle : si $\xi = x + \mathfrak{M}_{\mathbb{K}} \in \Bbbk^{\times}$, on identifie $v_{\Bbbk}(\xi) \in \Gamma_{\Bbbk}$ à $v'_{\mathbb{K}}(x) \in \Gamma'_{\mathbb{K}}$. Ceci est sans amiguïtué : si $x + \mathfrak{M}_{\mathbb{K}} = y + \mathfrak{M}_{\mathbb{K}}$ avec $x, y \in \mathfrak{V}_{\mathbb{K}} \setminus \mathfrak{M}_{\mathbb{K}}$, alors $\dfrac{x}{y} \in 1 + \mathfrak{M}_{\mathbb{K}} \subseteq 1 + \mathfrak{M}'_{\mathbb{K}}$ et donc $v'_{\mathbb{K}}\left(\dfrac{x}{y}\right) = 0$, et $v'_{\mathbb{K}}(x) = v'_{\mathbb{K}}(y)$.

Ainsi la valuation $v_{\mathbb{K}}$ associée à $\mathfrak{V}_{\mathbb{K}}$ est plus grossière que la valuation $v'_{\mathbb{K}}$ associée à $\mathfrak{V}'_{\mathbb{K}}$; ce fait est tout à fait intuitif, le groupe des unités de $v_{\mathbb{K}}$ étant plus gros que celui de $v'_{\mathbb{K}}$.

Nous avons retrouvé la situation décrite dans la section précédente (groupes ordonnés abéliens).

$$\left.\begin{array}{c}\Gamma/\Delta\;\left[\begin{array}{c}\mathbb{K}\\ \Big\downarrow\ \mathrm{P}\\ \Bbbk\end{array}\right.\\ \Delta\;\left[\begin{array}{c}\Bbbk\\ \Big\downarrow\ \mathrm{P}'\\ \mathbb{l}\end{array}\right.\end{array}\right]\;\Gamma$$

Ici $\Gamma = \Gamma'_{\mathbb{K}}$, $\Delta = \Gamma_{\Bbbk}$ et $\Gamma/\Delta = \Gamma_{\mathbb{K}}$.

Encore quelques exemples : la composition des places

Ce qui vient d'être fait sur la composition des places permet d'enrichir sans grands efforts notre bestiaire de corps valués. Nous utiliserons ici les notations introduites immédiatement ci-dessus.

Si on ne prend que des exemples simples, on se retrouve dans la situation où $\Gamma'_{\mathbb{K}}$ est le produit lexicographique de $\Gamma_{\mathbb{K}}$ et de $\Gamma_{\Bbbk}$. Ainsi, on peut poser $\mathbb{K} = \mathbb{Q}_p(\mathrm{X})$ avec la valuation v_0 ; le corps résiduel est $\Bbbk = \mathbb{Q}_p$, qu'on considère muni de la valuation v_p ; son corps résiduel est $\mathbb{l} = \mathbb{F}_p$. Alors la valuation de $\mathbb{K}$ associée à la composition des places correspondantes (qui produit une place de $\mathbb{Q}_p(\mathrm{X})$ dans $\mathbb{F}_p$) coïncide avec la valuation w définie plus haut par :

$$w(a_i \cdot \mathrm{X}^i + a_{i+1} \cdot \mathrm{X}^{i+1} + \cdots + a_n \cdot \mathrm{X}^n) = (i, v_p(a_i)) \in \mathbb{Z} \times \mathbb{Z}$$

pour $a_i \neq 0$, et $w(f/g) = w(f) - w(g)$; cette valuation est à valeur dans $\mathbb{Z} \times \mathbb{Z}$ ordonné lexicographiquement.

Il paraît important de produire un exemple où ça n'est pas le cas ; ne serait-ce que pour montrer que le groupe de valuation associé à la place $\mathrm{P}'\mathrm{P}$ ne dépend pas uniquement de ceux associés à P et P'.

Il importe avant tout de donner un groupe ordonné Γ et un sous-groupe convexe Δ de Γ, tel que que Γ ne soit pas isomorphe au produit lexicographique $\Gamma/\Delta \times \Delta$. Nous verrons ensuite à y associer des corps valués.

Nous introduisons quelques notions qui ne sont pas indispensables ici, mais notre exemple permettant de les illustrer dans une certaine mesure, il nous a semblé bon de les nommer.

Groupes divisibles Un groupe Γ est dit divisible si pour tout $\gamma \in \Gamma$ et tout $n \in \mathbb{N}$, il existe $\gamma' \in \Gamma$ tel que $n \cdot \gamma' = \gamma$.

Être un groupe divisible est équivalent au *schéma* $(\mathrm{D}_n)_{n\geq 1}$ d'énoncés du premier ordre (dans le langage des groupes) suivant :

$$\mathrm{D}_n : \qquad \forall \gamma\ \exists \gamma',\ \underbrace{\gamma' + \cdots + \gamma'}_{n \text{ fois}} = \gamma.$$

Tout groupe Γ admet une clôture divisible; dans le cas d'un groupe sans torsion (et c'est le cas d'un groupe ordonné), la clôture divisible de Γ est :

$$\overline{\Gamma} = \mathbb{Q} \otimes_{\mathbb{Z}} \Gamma = \left\{ \frac{\gamma}{n} \ :\ \gamma \in \Gamma,\ n \in \mathbb{N}^\star \right\}.$$

Si Γ est un groupe ordonné, $\overline{\Gamma}$ sera un groupe ordonné également. Si $(\mathbb{K}, v)$ est un corps valué de groupe de valuation Γ, alors quelle que soit l'extension w de v à $\mathbb{K}^{ac}$ (la clôture algébrique de $\mathbb{K}$), le groupe de valuation de w est $\overline{\Gamma}$.

$\mathbb{Z}$-groupes Si dans un groupe Γ il y a un plus petit élément positif, noté 1, alors $\mathbb{Z}$ se plonge naturellement dans Γ en envoyant $1 \in \mathbb{Z}$ sur $1 \in \Gamma$; c'est un sous-groupe convexe de Γ. Un *$\mathbb{Z}$-groupe* est un groupe ordonné Γ dans lequel il y a un plus petit élément positif et tel que $\Gamma/\mathbb{Z}$ est un groupe divisible.

De manière équivalente, c'est un groupe ordonné satisfaisant à la théorie du premier ordre de $(\mathbb{Z}, +, <)$, ce qui s'axiomatise comme suit, dans le langage $\mathcal{L} = \{1, +, <\}$:
- axiomes de groupe totalement ordonné;
- $\forall x,\ x > 0 \Longrightarrow (x = 1 \vee x > 1)$;
- pour tout n, un axiome C_n :

$$\mathrm{C}_n : \qquad \forall x,\ \exists y,\ \big(n \cdot y = x \vee n \cdot y = x - 1 \vee \cdots \vee n \cdot y = x - (n-1)\big).$$

Les $\mathbb{Z}$-groupes de rang 1 Ils sont tous isomorphes à $\mathbb{Z}$.

Un $\mathbb{Z}$-groupe de rang 2 L'exemple le plus simple est $\mathbb{Q} \times \mathbb{Z}$ ordonné par l'ordre lexicographique. Cependant il ne sont pas tous isomorphes à celui-ci! Avant de donner un autre exemple, il faut parler de $\widehat{\mathbb{Z}}$.

«$\mathbb{Z}$ **chapeau**» **:** $\widehat{\mathbb{Z}}$ En langage savant, c'est le «complété profini des groupes $\mathbb{Z}/n\mathbb{Z}$». Nous allons en donner une description tout ce qu'il y a de terre à terre. Soit S un système infini de congruences de la forme suivante :

$$\mathrm{S}(\underline{c}) = \begin{cases} x \equiv c_2 \mod 2 \\ x \equiv c_3 \mod 3 \\ \vdots \\ x \equiv c_i \mod i \\ \vdots \end{cases}$$

$\underline{c} = (c_i)_{i\geq 2}$ est une suite d'entiers. On suppose que ces équations sont compatibles deux à deux :

$$\forall i, j,\ c_i \equiv c_j \mod i \wedge j,$$

où $i \wedge j$ est le p.g.c.d. de i et j. Cette hypothèse permet d'assurer que tous les sous-systèmes finis de S admettent une solution dans $\mathbb{Z}$ (c'est *grosso modo* le théorème des restes chinois). Il n'est cependant pas difficile de donner de tels systèmes qui n'ont pas de solution dans $\mathbb{Z}$.

Le groupe $\widehat{\mathbb{Z}}$ est constitué des solutions formelles de tels systèmes S ; plus simplement, c'est l'ensemble de ces systèmes, muni de la loi + suivante :

$$\mathrm{S}(\underline{c}) + \mathrm{S}(\underline{d}) = \mathrm{S}(\underline{c} + \underline{d}),$$

où $\underline{c} + \underline{d}$ est la suite $(c_i + d_i)_{i\geq 2}$. Bien entendu, on considère que $\mathrm{S}(\underline{c}) = \mathrm{S}(\underline{d})$ ssi $c_i \equiv d_i \mod i$ pour tout i (et donc chaque système S a une solution unique dans $\widehat{\mathbb{Z}}$).

On plonge naturellement $\mathbb{Z}$ dans $\widehat{\mathbb{Z}}$ en envoyant a sur $\mathrm{S}(a)$, le système

$$\mathrm{S}(a) = \begin{cases} x \equiv a \mod 2 \\ x \equiv a \mod 3 \\ \vdots \end{cases}$$

C'est bien une injection, car si $a, b \in \mathbb{Z}$ vérifient pour tout $i \in \mathbb{N}^\star$, $a \equiv b \mod i$, on a $a = b$.

On peut identifier naturellement $\widehat{\mathbb{Z}}$ au produit $\prod_p \mathbb{Z}_p$. Notons que $\widehat{\mathbb{Z}}$ est le groupe de Galois absolu de $\mathbb{F}_p$ (pour n'importe quel p premier).

Un autre $\mathbb{Z}$-groupe de rang 2 Fixons un élément $\mathrm{S}(\underline{c}) \in \widehat{\mathbb{Z}} \setminus \mathbb{Z}$.

Soient $\omega_1, \omega_2, \ldots, \omega_i, \ldots$ des symboles pour l'instant purement formels ; on forme l'ensemble suivant :

$$\Gamma = \{a + b \cdot w_i \ :\ a, b \in \mathbb{Z},\ i \in \mathbb{N}^\star\}.$$

On introduit une première règle de calcul dans Γ :

$$i \cdot \omega_i = \underbrace{w_i + \cdots + w_i}_{i \text{ fois}} = w_1 - c_i \text{ pour } i \geq 2$$

et on pose

$$(a + b \cdot \omega_i) + (c + d \cdot \omega_j) = e + (j \cdot b + i \cdot d) \cdot \omega_{ij}$$

où
$$e = a + c + b \cdot \frac{c_{ij} - c_i}{i} + d \cdot \frac{c_{ij} - c_j}{j}.$$
e est bien un entier, grâce aux conditions de compatibilité entre les c_i. La loi $+$ ci-dessus est obtenue en utilisant la règle de calcul sur les ω_i.

C'est bien une loi de groupe, à condition de considérer que $a+b\cdot\omega_i = c+d\cdot\omega_j$ ssi
$$\begin{cases} j \cdot b - i \cdot d & = & 0 \\ a - c + b \cdot \dfrac{c_{ij} - c_i}{i} - d \cdot \dfrac{c_{ij} - c_j}{j} & = & 0. \end{cases}$$
Ainsi $a + b \cdot w_i$ n'est pas une écriture unique dans Γ (de même que p/q dans $\mathbb{Q}$).

On ordonne enfin Γ par
$$a + b \cdot w_i \geq 0 \Longleftrightarrow \begin{cases} b \geq 0 \\ \text{ou} \\ b = 0 \wedge a \geq 0 \end{cases}$$

Alors Γ est un $\mathbb{Z}$-groupe de rang 2. On y plonge $\mathbb{Z}$ par $a \in \mathbb{Z} \mapsto a + 0 \cdot w_1 \in \Gamma$.

Soit l'application $\Phi : \begin{cases} \Gamma & \longrightarrow & \mathbb{Q} \\ a + b \cdot \omega_i & \mapsto & \dfrac{b}{i} \end{cases}$. C'est un morphisme de groupes ordonnés ; son noyau est précisément $\mathbb{Z}$. On a donc $\Gamma/\mathbb{Z} \cong \mathbb{Q}$.

Cependant Γ n'est pas isomorphe à $\mathbb{Q} \times \mathbb{Z}$: dans $\mathbb{Q} \times \mathbb{Z}$ aucun élément ne vérifie : pour tout i, $x \equiv c_i \bmod i$; plus précisément, pour $(a, b) \in \mathbb{Q} \times \mathbb{Z}$, on a pour tout i : $(a, b) \equiv b \bmod i$. Le choix de $\mathrm{S}(\underline{c}) \in \widehat{\mathbb{Z}} \setminus \mathbb{Z}$ était donc crucial.

Des corps valués associés à cette situation On fixe un corps $\Bbbk$ avec une valuation discrète, de corps résiduel $\mathbb{l}$; la place associée est P'. Prenons (par exemple) $\Bbbk = \mathbb{Q}_p$ et $\mathbb{l} = \mathbb{F}_p$; la valuation est notée v_p selon l'usage.

• Pour $\mathbb{Q} \times \mathbb{Z}$, soit $\mathbb{K} = \Bbbk((\mathrm{X}))^\wedge$ le corps des séries de Puiseux à coefficients dans $\Bbbk$, muni de la valuation v_0 :
$$v_0 \left(\sum_{n \geq k} a_n \cdot \mathrm{X}^{\frac{n}{i}} \right) = \frac{k}{i} \in \mathbb{Q} \quad (a_k \neq 0).$$
La place associée $\mathrm{P} : \mathbb{K} \longrightarrow \Bbbk \cup \{\infty\}$ est « l'évaluation en $\mathrm{X} = 0$ ».

Et la valuation $w : \mathbb{K}^\times \longrightarrow \mathbb{Q} \times \mathbb{Z}$ associée à la composition de place $\mathrm{P}'\mathrm{P}$ est
$$w \left(\sum_{n \geq k} a_n \cdot \mathrm{X}^{\frac{n}{i}} \right) = \left(\frac{k}{i}, v_p(a_k) \right) \in \mathbb{Q} \times \mathbb{Z} \quad (a_k \neq 0).$$

• Pour le groupe Γ que nous venons de décrire, la construction est un peu plus compliqué. Soit $\mathbb{K} = \Bbbk((\mathrm{X}))^{\wedge(\underline{c})}$ le « corps de pseudo séries de Puiseux » suivant : on ajoute des indéterminées $\mathrm{X}_1, \mathrm{X}_2, \ldots, \mathrm{X}_i, \ldots$; l'intention est d'obtenir un corps où $w(\mathrm{X}_i) = \omega_i$. On considère l'ensemble des « séries de Laurent » en une de ces indéterminées :

$$\sum_{n \geq k} a_n \cdot \mathrm{X}_i^n\,; \quad (k \in \mathbb{Z}).$$

Pour sommer ou multiplier deux éléments, on utilise l'égalité $\mathrm{X}_i = p^{\frac{c_{ij}-c_i}{i}} \cdot \mathrm{X}_{ij}^j$ de façon à faire une « réduction au même dénominateur des exposants » ; on peut vérifier que c'est compatible avec la loi + de Γ. On pose

$$w\left(\sum_{n \geq k} a_n \cdot \mathrm{X}_i^n\right) = v_p(a_k) + n \cdot \omega_i \in \Gamma \quad (a_k \neq 0).$$

Ceci fait de $\mathbb{K}$ un corps valué dans Γ. On voit que si on avait choisi $c_i = 0$ pour tout i ce serait exactement le corps des séries de Puiseux.

L'autre valuation sur $\mathbb{K}$ est

$$v\left(\sum_{n \geq k} a_n \cdot \mathrm{X}_i^n\right) = \frac{n}{i} \in \mathbb{Q} \quad (a_k \neq 0)\,;$$

la place P associée va dans $\Bbbk \cup \{\infty\}$ (ici $\Bbbk = \mathbb{Q}_p$), et correspond une nouvelle fois à « l'évaluation en $\mathrm{X}_i = 0$ (pour tout i) ».

2.4 Corps henséliens

Soit (K, v) un corps valué, Γ son groupe de valuation, $\mathfrak{V}$ son anneau d'entiers, $\mathfrak{M}$ l'idéal maximal ; si $\mathrm{P}(\mathrm{X}) = a_0 \cdot \mathrm{X}^n + \cdots + a_n \in \mathfrak{V}[\mathrm{X}]$, on note $\overline{\mathrm{P}}(\mathrm{X})$ le polynôme de $\Bbbk[\mathrm{X}]$ suivant : $\overline{a_0} \cdot \mathrm{X}^n + \cdots + \overline{a_n}$.

Définition Un corps $\mathbb{K}$ est dit *hensélien* si il vérifie le lemme formulé ci-dessous (*cf.* [E], par exemple) :

Lemme 7 (Lemme de Hensel) *Soit* $\mathrm{P}(\mathrm{X}) \in \mathfrak{V}(\mathrm{X})$ *un polynôme à coefficients entiers. Si* $\overline{\mathrm{P}}(\mathrm{X}) \in \Bbbk[\mathrm{X}]$ *admet une racine simple* $\zeta \in \Bbbk$*, alors il existe* $z \in \mathfrak{V}$ *une racine de* P *telle que* $\overline{z} = \zeta$*.*

C'est Hensel qui a le premier formulé cette propriété, au sujet des corps p-adiques.

Exemple

Le corps des p-adiques $\mathbb{Q}_p$ est hensélien ; c'est le cas de tous les corps complets de valuation discrète (c.-à-d. dont le groupe de valuation est isomorphe à $\mathbb{Z}$).

En effet, soit $\mathrm{P}(\mathrm{X}) \in \mathfrak{V}[\mathrm{X}]$ un polynôme de degré d ; soit $z_0 \in \mathfrak{V}$ tel que que $\overline{z_0} = \zeta$, une racine simple de $\overline{\mathrm{P}}(\mathrm{X}) \in \Bbbk[\mathrm{X}]$; on a $v(\mathrm{P}(z_0)) > 0$ et $v(\mathrm{P}'(z_0)) = 0$. Définissons par récurrence une suite $(z_n)_{n \in \mathbb{N}}$:

$$z_{n+1} = z_n - \frac{\mathrm{P}(z_n)}{\mathrm{P}'(z_n)}.$$

Alors, par récurrence, $\overline{z_n} = \zeta$ pour tout n ; d'autre part, le développement de Taylor

$$\mathrm{P}(x+h) = \mathrm{P}(x) + h \cdot \mathrm{P}'(x) + h^2 \cdot \frac{\mathrm{P}''(x)}{2} + \cdots + h^d \cdot \frac{\mathrm{P}^{(d)}(x)}{d!}$$

produit

$$\mathrm{P}(z_{n+1}) = \left(\frac{-\mathrm{P}(z_n)}{\mathrm{P}'(z_n)}\right)^2 \cdot \frac{\mathrm{P}''(x)}{2} + \cdots + \left(\frac{-\mathrm{P}(z_n)}{\mathrm{P}'(z_n)}\right)^d \cdot \frac{\mathrm{P}^{(d)}(x)}{d!}\,;$$

or chaque $\frac{\mathrm{P}^{(i)}(\mathrm{X})}{i!}$ est un polynôme de $\mathfrak{V}[\mathrm{X}]$; on en déduit facilement que $v(\mathrm{P}(z_{n+1})) \geq 2 \cdot v(\mathrm{P}(z_n))$. Alors $v(z_{n+1} - z_n)$ est une suite strictement croissante de $\mathbb{Z}$; il en découle que $(z_n)_{n \in \mathbb{N}}$ est une suite de Cauchy.

Si z est sa limite, il est clair que $\mathrm{P}(z) = 0$ et que $\zeta = \overline{z}$.

Remarque Cette démonstration est basée sur une utilisation « savante » de la formule de Newton ; dans le cas de $\mathbb{Q}_p$ par exemple, on pourrait être encore plus élémentaire en montrant que la condition $\overline{\mathrm{P}'}(\zeta) \neq 0$ permet de calculer, de proche en proche, des approximations de z modulo p^2, p^3,... (*cf.* [Gou]). La méthode de Newton permet une convergence plus rapide (le nombre de « décimales » correctes double à chaque étape) ; il est remarquable que cette méthode, vouée à l'origine à être utilisée sur des fonctions réelles, est valable dans $\mathbb{Q}_p$, alors que le dessin qui la justifie dans $\mathbb{R}$ ne peut pas être transposé à $\mathbb{Q}_p$.

Développement hensélien Soit $(\mathbb{K}, v)$ un corps de valuation discrète. Soit $\Omega = \{\omega_x \ : \ x \in \Bbbk\} \subseteq \mathfrak{V}_{\mathbb{K}}$ un système exact de représentant des classes de $\mathfrak{V}_{\mathbb{K}}$ modulo $\mathfrak{M}_{\mathbb{K}}$; soit $\pi \in \mathfrak{V}$ tel que $v(\pi) = 1 \in \mathbb{Z} = v(\mathbb{K})$. On peut écrire les éléments de $\mathfrak{V}_{\mathbb{K}}$ comme des sommes infinies de la forme

$$\omega_0 + \omega_1 \cdot \pi + \cdots + \omega_i \cdot \pi^i + \cdots$$

où les ω_i sont dans Ω. Si toutes cls sommes infinies de ce type sont dans $\mathfrak{V}_{\mathbb{K}}$, le corps est complet.

Définition Le *hensélisé* de $(\mathbb{K}, v) \subset (\mathbb{K}^{ac}, w)$ est la plus petite extension algébrique $\mathbb{L}$ de $\mathbb{K}$ qui vérifie le lemme de Hensel.

Une extension w de la valuation v de $\mathbb{K}$ étant fixée dans $\mathbb{K}^{ac}$, cette extension $\mathbb{L}$ est unique. De manière générale, si w_1 et w_2 sont deux extensions de v à $\mathbb{K}^{ac}$, on a deux hensélisés $\mathbb{L}_1$ et $\mathbb{L}_2$ de $\mathbb{K}$ qui y correspondent ; il existe alors un **unique** $\mathbb{K}$-isomorphisme de corps valués entre $\mathbb{L}_1$ et $\mathbb{L}_2$.

Du point de vue classique, voici comment on peut définir le hensélisé de $\mathbb{K}$: soit $(\mathbb{K}^{sep}, w)$ la clôture séparable de $\mathbb{K}$ munie d'une extension w de v. Soit $\mathrm{Aut}(\mathbb{K}^{sep}/\mathbb{K})$ le groupe de Galois absolu de $\mathbb{K}$. Soit

$$\mathrm{G} = \{\sigma \in \mathrm{Aut}(\mathbb{K}^{sep}/\mathbb{K}) \ : \ \forall x \in \mathbb{K}^{sep}, \ w(\sigma x) = w(x)\}.$$

Soit $\mathbb{K}^h$ le corps fixé de G : $\mathbb{K}^h = \{x \in \mathbb{K}^{sep} \ : \ \forall \sigma \in \mathrm{G},\ \sigma x = x\}$. La valuation w de $\mathbb{K}^{sep}$ restreinte à $\mathbb{L}$ est encore notée w ; $(\mathbb{K}^h, w)$ est le hensélisé de $\mathbb{K}$.

Dans la suite, on notera toujours $(\mathbb{K}^h, w)$, et par abus $(\mathbb{K}^h, v)$, le hensélisé de $(\mathbb{K}, v)$. On a la propriété suivante :

$$\forall \sigma \in \mathrm{Aut}(\mathbb{K}^{sep}/\mathbb{K}^h),\ \forall \alpha \in \mathbb{K}^{sep},\ w(\sigma\alpha) = w(\alpha).$$

Propriété universelle Le hensélisé possède la propriété suivante : si $\mathbb{L}$ est un corps hensélien et que $\phi : \mathbb{K} \longrightarrow \mathbb{L}$ est un morphisme de corps valués, il existe une unique façon de prolonger ϕ en un morphisme de corps valués $\Phi : \mathbb{K}^h \longrightarrow \mathbb{L}$.

Cette propriété universelle caractérise le hensélisé : si une extension algébrique $(\widetilde{\mathbb{K}}, v)$ de $(\mathbb{K}, v)$ la possède, alors il existe un unique isomorphisme de corps valués entre $\mathbb{K}^h$ et $\widetilde{\mathbb{K}}$.

Le chapitre suivant est pour la plus grande part consacré à la construction du hensélisé et à la démonstration constructive des résultats classiques qui concernent les corps henséliens. Un outil essentiel sera alors le polygone de Newton, que nous présentons dans la section suivante.

3 Polygone de Newton

Ici $\mathbb{K}$ est un corps valué, et $v \ : \ \mathbb{K} \longrightarrow \Gamma$ est la valuation associée ; Γ est le groupe de valuation de $\mathbb{K}$. On note $\overline{\Gamma} = \left\{ \frac{\gamma}{n} \ : \ \gamma \in \Gamma,\ n \in \mathbb{N}^* \right\}$ la clôture divisible de Γ.

Soit w une extension de v à $\mathbb{K}^{ac}$, la clôture algébrique de $\mathbb{K}$. Le groupe de valuation de w est $\overline{\Gamma}$.

Définition Soit $\mathrm{P(X)} = a_0 \cdot \mathrm{X}^n + \cdots + a_n$ un polynôme de $\mathbb{K}[\mathrm{X}]$; on note $\mathfrak{p}_i = (i, v(a_i)) \in \mathbb{N} \times \Gamma$. On dit que le *segment* $[\mathfrak{p}_i, \mathfrak{p}_j]$ (où $i < j$) est dans le *polygone de Newton* de P si

$$\begin{array}{rrcl} \forall k, & v(a_k) & \geq & \dfrac{v(a_j) - v(a_i)}{j - i} \cdot k + \dfrac{j \cdot v(a_i) - i \cdot v(a_j)}{j - i}, \\ \text{si } k < i \text{ ou } j < k, & v(a_k) & > & \dfrac{v(a_j) - v(a_i)}{j - i} \cdot k + \dfrac{j \cdot v(a_i) - i \cdot v(a_j)}{j - i}. \end{array}$$

Dans ce cas on appelle *pente* du segment $[\mathfrak{p}_i, \mathfrak{p}_j]$ l'élément de $\overline{\Gamma}$ suivant :

$$\frac{v(a_j) - v(a_i)}{j - i}.$$

La largeur de $[\mathfrak{p}_i, \mathfrak{p}_j]$ est, par définition, $j - i$. On note $\mathcal{PN}(\mathrm{P})$ la liste (ordonnée) des pentes des segments du polygone de Newton de P, *avec multiplicité*, c.-à-d. la pente d'un segment de largeur ℓ est répétée ℓ fois (voir exemple plus bas).

Dans le cas particulier où Γ est de rang 1 (c.-à-d. peut-être vu comme un sous-groupe de $(\mathbb{R}, +)$), la définition abstraite du polygone de Newton donnée ci-dessus revient à dire que les segments du polygone de Newton de P sont les segments de l'enveloppe convexe inférieure des points $\mathfrak{p}_i$ dans $\mathbb{N} \times \mathbb{R} \subseteq \mathbb{R} \times \mathbb{R}$, et les pentes en sont bien les pentes géométriques « traditionnelles ».

Penchons-nous sur un exemple :

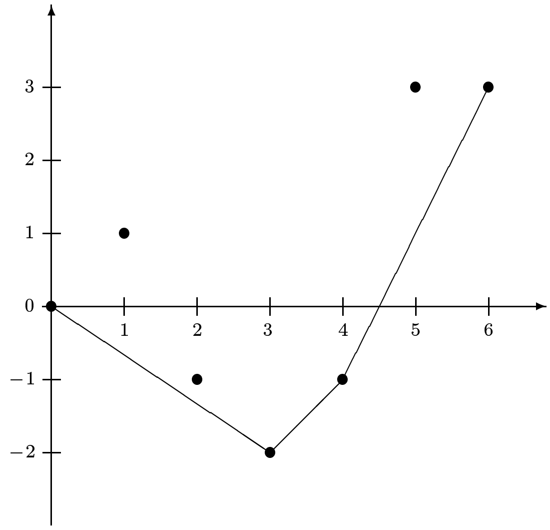


Figure 2 : Polygone de Newton de $\mathfrak{A}[\mathrm{X}]$

$\mathfrak{A}(\mathrm{X}) = \mathrm{X}^6 + 3 \cdot \mathrm{X}^5 + \frac{2}{3} \cdot \mathrm{X}^4 + \frac{5}{9} \cdot \mathrm{X}^3 - \frac{1}{6} \cdot \mathrm{X}^2 + 27 \cdot \mathrm{X} + 54 \in \mathbb{Q}_{(3)}(\mathrm{X})$

Le corps considéré est $\mathbb{Q}_{(3)}$, c.-à-d. $\mathbb{Q}$ muni de la valuation 3-adique v_3. Soit $\mathfrak{A}(\mathrm{X}) = \mathrm{X}^6 + 3\mathrm{X}^5 + \frac{2}{3}\mathrm{X}^4 + \frac{5}{9}\mathrm{X}^3 - \frac{1}{6}\mathrm{X}^2 + 27x + 54 \in \mathbb{Q}_{(3)}(\mathrm{X})$; son polygone de Newton est représenté figure 2. Ici $\mathcal{PN}(\mathfrak{A})$ est la liste $\left[-\frac{2}{3} ; -\frac{2}{3} ; -\frac{2}{3} ; 1 ; 2 ; 2\right]$, ce qui au vu du théorème 8 ci-dessous signifie concrètement que parmi les racines de $\mathfrak{A}$ dans $\mathbb{Q}^{ac}$ muni d'un prolongement w de v_3, il y en a trois de valuation $-\frac{2}{3}$, une de valuation 1 et deux de valuation 2.

Ce théorème suivant est très classique (*cf.*[Gou], chap. 6) ; néanmoins nous en donnons la preuve.

Théorème 8 (Le polygone de Newton) *Soit* $(\mathbb{K}, v)$ *un corps valué et soit* $(\mathbb{K}^{ac}, w)$ *sa clôture algébrique munie d'un prolongement* w *de* v*. Soit* $\mathrm{P}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ *un polynôme de degré* n*, et* $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^{ac}$ *ses racines. Alors la liste (ordonnée) des valuations* $w(\alpha_i)$ *coïncide avec la liste* $\mathcal{PN}(\mathrm{P})$*.*

Démonstration On peut supposer que P est unitaire : $v(a_0) = 0$; en effet la multiplication de P par une constante non nulle ne change pas la liste $\mathcal{PN}(\mathrm{P})$. On suppose que les racines sont classées par ordre de valuation croissante $v(\alpha_1) \leq \cdots \leq v(\alpha_n)$.

Pour tout $k \leq n$, nous notons $\mathrm{I}_1^k, \mathrm{I}_2^k, \ldots$ les parties à k éléments de $\{1, \ldots, n\}$, avec la convention $\mathrm{I}_1^k = \{1, \ldots, k\}$.

Soit $k \geq 1$ tel que $\gamma = v(\alpha_1) = \cdots = v(\alpha_k) < v(\alpha_{k+1})$.

On a

$$a_k = \alpha_1 \cdots \alpha_k + \sum_{i>1} \prod_{j\in \mathrm{I}_i^k} \alpha_j.$$

Or $v(\alpha_1 \cdots \alpha_k) = k \cdot \gamma$, et pour tout $i > 1$, $v(\prod_{j\in \mathrm{I}_i^k} \alpha_j) > k \cdot \gamma$; on a donc $v(a_k) = k \cdot \gamma$.

Pour $k' \neq k$, on a $a_{k'} = \sum_{i\geq 1} \prod_{j\in \mathrm{I}_i^{k'}} \alpha_j$. Si $0 < k' < k$, chacun des termes de cette somme est de valuation supérieure à $k' \cdot \gamma$, donc $v(a_{k'}) \geq k' \cdot \gamma$; si $k' > k$, chacun des termes est de valuation strictement supérieure à $k' \cdot \gamma$, et $v(a_{k'}) > k' \cdot \gamma$.

On a ainsi prouvé que le segment $[\mathfrak{p}_0, \mathfrak{p}_k]$ est dans le polygone de Newton de P ; il est de pente γ et de largeur k.

On peut poursuivre ainsi ; soit ℓ tel que $\delta = v(\alpha_{k+1}) = \cdots = v(\alpha_\ell) < v(\alpha_{\ell+1})$.

On a

$$v(a_\ell) = v(\alpha_1 \cdots \alpha_\ell + \sum_{i>1} \prod_{j\in \mathrm{I}_i^k} \alpha_j) = v(\alpha_1 \cdots \alpha_\ell) = k \cdot \gamma + (\ell - k) \cdot \delta$$

et pour k' tel que $k < k' < \ell$,

$$v(a_{k'}) = v(\sum_{i\geq 1} \prod_{j\in \mathrm{I}_i^{k'}} \alpha_j) \geq k \cdot \gamma + (k' - k) \cdot \delta\,;$$

quand $k' > \ell$, de même, $v(a_{k'}) > k \cdot \gamma + (k' - k) \cdot \delta$.

On a prouvé que le segment $[\mathfrak{p}_k, \mathfrak{p}_\ell]$, de largeur $\ell - k$ et de pente δ, est dans le polygone de Newton de P.

La preuve peut se terminer par récurrence. $\square$

Dans le cas d'un corps $\mathbb{K}$ hensélien, il y a beaucoup plus de choses à dire : on va utiliser la propriété classique suivante :

$$\forall \sigma \in \mathrm{Aut}(\mathbb{K}^{ac} \;/\; \mathbb{K}),\ \ \forall \alpha \in \mathbb{K}^{ac},\ \ w(\sigma\alpha) = w(\alpha).$$

On rappelle que w est une extension de v à $\mathbb{K}^{ac}$; dans le cas hensélien il n'y en a qu'une mais ce n'est pas notre propos pour l'instant.

Soit $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$. Si $\mathcal{PN}(\mathrm{P})$ présente la valeur γ avec la multiplicité k, soient $\alpha_1, \ldots, \alpha_k$ les k racines de P de valuation γ. Alors tout $\sigma \in \mathrm{Aut}(\mathbb{K}^{ac} \;/\; \mathbb{K})$ envoie α_i $(1 \leq i \leq k)$ sur un α_j $(1 \leq j \leq k)$; le polynôme $(\mathrm{X} - \alpha_1) \cdots (\mathrm{X} - \alpha_k)$ est invariant par l'action de $\mathrm{Aut}(\mathbb{K}^{ac} \;/\; \mathbb{K})$, il est donc dans $\mathbb{K}[\mathrm{X}]$. En particulier si $k = 1$, $\alpha_1 \in \mathbb{K}$. Nous avons montré le théorème suivant (de façon non constructive, ce qui est signalé par le symbole ¶).

¶ **Théorème 9** *Soit* $\mathbb{K}$ *un corps valué hensélien. Soit* $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ *un polynôme unitaire. À chaque segment de largeur* ℓ *et de pente* γ *dans le polygone de Newton de* P *correspond un facteur de* P, $\mathrm{Q} \in \mathbb{K}[\mathrm{X}]$, *avec* $\deg \mathrm{Q} = \ell$ *et toutes les racines de* Q *(dans* $\mathbb{K}^{ac}$*) sont de valuation* γ *(donc* $\mathcal{PN}(\mathrm{Q}) = [\gamma, \ldots, \gamma]$*).*

Ainsi le polynôme $\mathfrak{A}(\mathrm{X})$ de notre exemple admet, dans $\mathbb{Q}_3[\mathrm{X}]$ (car $\mathbb{Q}_3$ est hensélien), une racine de valuation 1, un facteur de degré 2 dont les racines sont de valuation 2, et un facteur de degré 3 dont les racines sont de valuation $-\frac{2}{3}$.

CHAPITRE III

CORPS HENSÉLIENS

1 Construction du hensélisé

La section 1 concerne la construction du hensélisé et établit de façon effective un théorème classique très puissant : le théorème du polygone de Newton (13). Ce théorème assure qu'un polynôme à coefficients dans un corps hensélien se factorise en un produit de polynômes dont toutes les racines ont même valuation ; nous donnons un algorithme permettant de calculer ces polynômes.

Dans la suite nous utilisons ce résultat pour démontrer, de façon très simple, l'unicité de l'extension de la valuation d'un corps hensélien à une extension algébrique (16), le fait que toute extension algébrique est hensélienne, le lemme de Krasner (18).

1.1 Notations et définitions

Nous donnons ici une liste de notations valables pour la totalité du chapitre.

$(\mathbb{K}, v)$	un corps valué ;
$\mathfrak{V} = \{x \in \mathbb{K} \,:\, v(x) \geq 0\}$	son anneau de valuation ;
$\mathfrak{M} = \{x \in \mathfrak{V} \,:\, v(x) > 0\}$	l'unique idéal maximal de $\mathfrak{V}$;
$\Gamma = v(\mathbb{K})$	le groupe de valuation de $\mathbb{K}$;
$\overline{\Gamma} = \{\gamma/n \,:\, \gamma \in \Gamma,\ n \in \mathbb{N}^*\}$	sa clôture divisible ;
$\Bbbk = \mathfrak{V} \,/\, \mathfrak{M}$	le corps résiduel de $\mathbb{K}$;
$\mathfrak{V} \longrightarrow \Bbbk,\ a \mapsto \overline{a}$	la projection canonique ;
$(\mathbb{K}^{ac}, w)$ ou $(\mathbb{K}^{ac}, v)$	la clôture algébrique de $\mathbb{K}$ munie d'un prolongement de la valuation v ;
$\Bbbk^{ac}$	la clôture algébrique de $\Bbbk$ **et** le corps résiduel de $\mathbb{K}^{ac}$;
$\mathfrak{V}^{ac}, \mathfrak{M}^{ac}$	l'anneau de valuation de $\mathbb{K}^{ac}$ et son idéal maximal ;
$(\mathbb{K}^h, w)$ ou $(\mathbb{K}^h, v)$	le *hensélisé* de $\mathbb{K}$ (*cf. infra*) ;
$\mathfrak{V}^h, \mathfrak{M}^h$	l'anneau de valuation de $\mathbb{K}^h$ et son idéal maximal ;
$\mathbb{K}^{sh}, \mathfrak{V}^{sh}, \mathfrak{M}^{sh}$	le *hensélisé strict* de $\mathbb{K}$ (*cf. infra*), son anneau de valuation, l'idéal maximal de cet anneau k ;

$\Bbbk^{sep}$ .... la clôture séparable de $\Bbbk$ **et** le corps résiduel de $\mathbb{K}^{sh}$ (*cf. infra*).

On appellera aussi $\mathfrak{V}$ *l'anneau des entiers* de $\mathbb{K}$.

En outre, si $\mathrm{P}(\mathrm{X}) = a_0\mathrm{X}^n + \cdots + a_n \in \mathfrak{V}[\mathrm{X}]$, on note $\overline{\mathrm{P}}(\mathrm{X})$ le polynôme de $\Bbbk[\mathrm{X}]$ suivant : $\overline{a_0}\mathrm{X}^n + \cdots + \overline{a_n}$.

Une extension de corps valués $\mathbb{K} \subseteq \mathbb{L}$ est dite *immédiate* si le groupe de valuation de $\mathbb{L}$ et son corps résiduel sont égaux à ceux de $\mathbb{K}$. Un élément ζ de $\mathbb{K}^{ac}$ admet $z \in \mathbb{K}$ comme *présentation immédiate* si $\zeta = z \cdot (1+\nu)$ avec $\nu \in \mathfrak{M}^{ac}$. Il est clair qu'une extension est immédiate si et seulement si tous ses éléments admettent une présentation immédiate.

Un corps $\mathbb{K}$ est dit *hensélien* si il vérifie le lemme de Hensel :

Lemme 1 (Lemme de Hensel) *Soit* $\mathrm{P}(\mathrm{X}) \in \mathfrak{V}(\mathrm{X})$ *un polynôme à coefficients entiers. Si* $\overline{\mathrm{P}}(\mathrm{X}) \in \Bbbk[\mathrm{X}]$ *admet une racine simple* $z \in \Bbbk$*, alors il existe* $\zeta \in \mathfrak{V}$ *une racine de* P *telle que* $\overline{\zeta} = z$.

Le *hensélisé* de $(\mathbb{K}, v) \subset (\mathbb{K}^{ac}, w)$ est la plus petite extension algébrique $\mathbb{L}$ de $\mathbb{K}$ qui vérifie le lemme de Hensel.

Une extension w de la valuation v de $\mathbb{K}$ étant fixée dans $\mathbb{K}^{ac}$, cette extension $\mathbb{L}$ est unique. De manière générale, si w_1 et w_2 sont deux extensions de v à $\mathbb{K}^{ac}$, on a deux hensélisés $\mathbb{L}_1$ et $\mathbb{L}_2$ de $\mathbb{K}$ qui y correspondent ; il existe alors un **unique** $\mathbb{K}$-isomorphisme de corps valués entre $\mathbb{L}_1$ et $\mathbb{L}_2$.

On note $(\mathbb{K}^h, w)$, et par abus $(\mathbb{K}^h, v)$, le hensélisé de $(\mathbb{K}, v)$.

1.2 Extensions henséliennes finies

Nous reprenons ici la construction du hensélisé telle qu'elle figure dans [KL]. Notre preuve du théorème principal (4) est légèrement plus simple que celle qu'on pouvait y trouver.

Nous supposons pour toute cette section que $(\mathbb{K}, v)$ est plongé dans $(\mathbb{K}^{ac}, v)$, sa clôture algébrique valuée ; l'existence d'une telle clôture valuée est non constructive, mais on peut prouver constructivement (*cf.* [CLR]) que supposer son existence n'introduit pas de contradiction.

Les corps henséliens admettent une autre caractérisation que nous appelons « lemme de Hensel-Newton » (ce nom n'a rien de général dans la littérature) :

Lemme 2 (Lemme de Hensel-Newton) *Soit* $(\mathbb{K}, v)$ *un corps valué.* $\mathbb{K}$ *est hensélien si, et seulement si, étant donné* $\mathrm{P}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ *un polynôme tel que la liste* $\mathcal{PN}(\mathrm{P})$ *présente une valeur isolée* $\gamma \in \overline{\Gamma}$ *(le polygone de Newton de* P *a un segment de largeur* 1*, de pente* γ*), il existe une unique racine de P,* $\zeta \in \mathbb{K}$*, telle que* $v(\zeta) = \gamma$.

Remarque Dans ce cas, il est clair qu'on a en fait $\gamma \in \Gamma$.

Démonstration Nous commençons par prouver que si $\mathbb{K}$ est hensélien, le lemme est vérifié. Soit donc $\mathrm{P}(\mathrm{X}) = a_0\mathrm{X}^n + \ldots + a_n \in \mathbb{K}[\mathrm{X}]$ dont le polygone de Newton a une pente de largeur 1, entre les points $\big(i, v(a_i)\big)$ et $\big(i+1, v(a_{i+1})\big)$. La pente γ correspondante est $\gamma = v(a_{i+1}) - v(a_i)$.

Soit
$$\mathrm{Q}(\mathrm{X}) = \frac{a_i^{n-i-1}}{a_{i+1}^{n-i}} \mathrm{P}\left(-\frac{a_{i+1}}{a_i}\mathrm{X}\right).$$

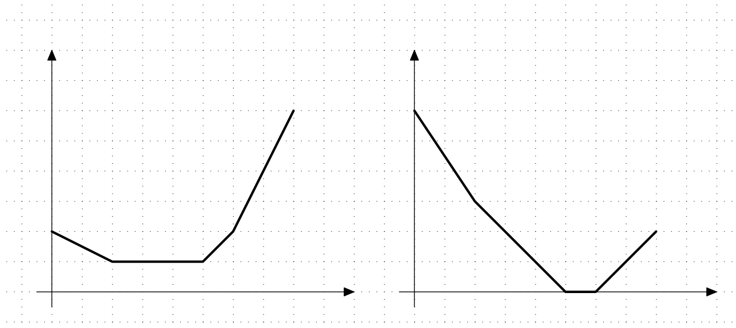


Figure 1 : Silhouette possible des polygones de Newton de P et Q.

On vérifie facilement que $\mathrm{Q}(\mathrm{X})$ vérifie les hypothèses du lemme de Hensel, $\overline{\mathrm{Q}}(\mathrm{X})$ admettant $1 \in \Bbbk$ comme racine simple. Alors il existe $\xi \in \mathbb{K}$ tel que $\mathrm{Q}(\xi) = 0$ et $\overline{\xi} = 1$. Alors $\zeta = -\dfrac{a_{i+1}}{a_i}\xi$ est une racine de P, de valuation γ. La figure 1 illustre la façon dont le polygone de Newton de Q dépend de celui de P : le segment isolé considéré (ici, de pente 1) est transformé par le changement de variable en un segment isolé de pente 0.

Montrons maintenant que si ce lemme est vrai dans un corps $\mathbb{K}$, alors $\mathbb{K}$ est hensélien. Soit donc $\mathrm{P} \in \mathfrak{V}[\mathrm{X}]$ et $a \in \mathfrak{V}$ tel que $\overline{a} \in \Bbbk$ est un zéro simple de $\overline{\mathrm{P}}$.

Soit $\mathrm{Q}(\mathrm{X}) = \mathrm{P}(\mathrm{X} - a)$. Alors $0 \in \Bbbk$ est un zéro simple de $\overline{\mathrm{Q}}$, ce qui se traduit par $v(\mathrm{Q}(0)) > 0$ et $v(\mathrm{Q}'(0)) = 0$. Il est clair que le polygone de Newton de Q admet une pente isolée *strictement positive*, tout à droite du dessin. Alors Q admet un zéro de valuation strictement positive, et donc P un zéro de résidu $\overline{a}$. □

Ajouter une racine à la Hensel-Newton

L'idée de la construction est de pouvoir ajouter à $\mathbb{K}$, au fur et à mesure des calculs, les racines de polynômes qui satisfont aux hypothèses du lemme 2.

Définition Un corps valué $(\mathbb{K}, v)$ est *discret* si :
- les opérations $+$ et $\times$ sont explicites dans $\mathbb{K}$;
- le calcul de l'inverse d'un élément non nul également;
- on dispose d'un test $x \stackrel{?}{=} 0$;
- on dispose de tests $x \stackrel{?}{\in} \mathfrak{V}$ et $x \stackrel{?}{\in} \mathfrak{M}$.

Remarquons que ceci suffit à «calculer» dans $\Bbbk$ et Γ, sans vraiment les connaître : pour $a, b \in \mathfrak{V}$, $\overline{a} = \overline{b}$ s'écrit $a - b \in \mathfrak{M}$, et des conditions du type $2v(a) \leq v(b)$ ou $v(a) > 2(b) + v(c)$ s'écrivent $b \,/\, a^2 \in \mathfrak{V}$ et $a \,/\, b^2c \in \mathfrak{M}$.

Étant donné $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ ceci suffit à calculer la liste $\mathcal{PN}(\mathrm{P})$ définie en II.3 ; les éléments de $\overline{\Gamma}$ sont représentés par un entier n et un élément de $a \in \mathbb{K}$, (n, a) symbolisant $v(a) \,/\, n \in \overline{\Gamma}$.

Soit $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ un polynôme satisfaisant aux hypothèses du lemme 2 et $\gamma \in \Gamma$ une valeur isolée de $\mathcal{PN}(\mathrm{P})$. On appelle le couple (P, γ) un *code à la Hensel-Newton* ; il y correspond une unique racine de P, soit $\zeta \in \mathbb{K}^h$. On va montrer comment calculer formellement dans $\mathbb{K}[\zeta]$, et surtout comment y effectuer les tests $x \overset{?}{\in} \mathfrak{V}$ et $x \overset{?}{\in} \mathfrak{M}$: $\mathbb{K}[\zeta]$ sera donc un corps valué discret.

En itérant cette construction un nombre fini de fois, on calcule dans $\mathbb{K}^h$, sans l'avoir jamais construit en entier ; on construit en fait une tour d'extensions algébriques finies, «coincée» entre $\mathbb{K}$ et $\mathbb{K}^h$. Nous verrons comment présenter de manière simple «l'union» de toutes ces extensions, qui est $\mathbb{K}^h$.

Pour les opérations $+$ et $\times$, le test $x \overset{?}{=} 0$ et le calcul de l'inverse d'un élément non nul, on utilise les techniques décrites dans la section II.1.2 pour le calcul dans un corps de rupture de P. Cette fois ci, si un test $q(\zeta) \overset{?}{=} 0$ fournit une factorisation $\mathrm{P} = \mathrm{P}_1 \cdot \mathrm{P}_2$ de P, alors un seul des $\mathcal{PN}(\mathrm{P}_i)$ contient la valeur γ, par exemple $\mathcal{PN}(\mathrm{P}_1)$. On remplace donc (P, γ) par (P_1, γ). La réponse au test d'égalité à zéro n'est donc pas ambiguë.

Il reste à savoir répondre dans $\mathbb{K}[\zeta]$ aux questions $q(\zeta) \overset{?}{\in} \mathfrak{V}^h$ et $q(\zeta) \overset{?}{\in} \mathfrak{M}^h$. On va faire encore mieux : on va montrer comment, étant donné $q(\zeta) \in \mathbb{K}[\zeta]$, calculer $z \in \mathbb{K}$ qui soit une présentation immédiate de $q(\zeta)$: $q(\zeta) = z \cdot (1 + \nu)$ avec $\nu \in \mathfrak{M}^h$.

Si on est dans une situation particulière où Γ ou $\Bbbk$ sont explicitement connus, on bénéficie du fait que $v(q(\zeta)) = v(z)$ et $\overline{q(\zeta)} = \overline{z}$. Dans le cas général, on a simplement

$$\begin{array}{rcl} q(\zeta) \in \mathfrak{V}^h & \iff & z \in \mathfrak{V}, \text{ et} \\ q(\zeta) \in \mathfrak{M}^h & \iff & z \in \mathfrak{M}. \end{array}$$

Lemme 3 *Soit* (P, γ) *un code à la Hensel-Newton. Alors on calcule (de manière uniforme) une présentation immédiate dans* $\mathbb{K}$ *de la racine* ζ *correspondante.*

Démonstration On reprend la démonstration du lemme 2 : ζ s'écrit $\zeta = -\dfrac{a_{i+1}}{a_i}\xi$, où $\overline{\xi} = 1$, c.-à-d. $\xi = 1 + \nu$, $\nu \in \mathfrak{M}^h$. Donc $-\dfrac{a_{i+1}}{a_i}$ est une présentation immédiate de ζ. □

Théorème 4 *Soit* (P, γ) *un code à la Hensel-Newton, définissant une racine* ζ *de* P. *Soit* $q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ *un polynôme de degré* $\deg q < \deg \mathrm{P}$. *On sait calculer (de manière uniforme) une présentation immédiate de* $q(\zeta)$ *dans* $\mathbb{K}$.

Démonstration On suppose que ζ est défini par le code (P, γ). Soient $\zeta_1 = \zeta, \zeta_2, \ldots, \zeta_n$ les racines de P dans $\mathbb{K}^{ac}$.

On calcule tout d'abord la liste $\mathcal{L} = \mathcal{PN}(\mathrm{P})$ des valuations $v(\zeta_i)$. La valeur γ y est présente une seule fois.

Soit
$$\mathrm{T}_0(\mathrm{X}) = \mathrm{T}_{\mathrm{P},q}(\mathrm{X}) = \prod_{i=1}^{n}(\mathrm{X} - q(\zeta_i)).$$
On calcule la liste $\mathcal{L}_0$ des valuations $v\big(q(\zeta_i)\big)$: c'est $\mathcal{L}_0 = \mathcal{PN}(\mathrm{T}_0)$. On a $v\big(q(\zeta)\big)$ dans cette liste, mais on ne sait pas précisément où.

Soit
$$\mathrm{T}_k(\mathrm{X}) = \prod_{i=1}^{n}(\mathrm{X} - \zeta_i^k q(\zeta_i)).$$
La liste $\mathcal{L}_k = \mathcal{PN}(\mathrm{T}_k)$ est celle des valuations $v\big(\zeta_i^k q(\zeta_i)\big) = k \cdot v(\zeta_i) + v\big(q(\zeta_i)\big)$.

Il existe $k \in \mathbb{N}$ tel que $k \cdot v(\zeta) + v\big(q(\zeta)\big)$ soit isolé parmi cette liste, c.-à-d.
$$k \cdot v(\zeta_1) + v\big(q(\zeta_1)\big) \neq k \cdot v(\zeta_i) + v\big(q(\zeta_i)\big) \qquad \forall\, i > 1.$$
En effet cela revient à dire que
$$k\big(v(\zeta_1) - v(\zeta_i)\big) \neq v\big(q(\zeta_i)\big) - v\big(q(\zeta_1)\big) \qquad \forall\, i > 1.$$
Or $v(\zeta_1) - v(\zeta_i) \neq 0$, et donc ces inéquations n'excluent qu'un nombre fini de valeurs pour k.

On peut trouver un tel k en imposant
$$k \cdot (\gamma - \gamma') \neq \delta_1 - \delta_2 \qquad \forall\, \gamma' \in \mathcal{L} \text{ tel que } \gamma' \neq \gamma \text{ et } \forall\, \delta_1, \delta_2 \in \mathcal{L}_0.$$

Alors dans le polygone de Newton de T_k la racine $\zeta^k q(\zeta)$ correspond à une pente isolée. On peut trouver laquelle en faisant le test $\delta - k \cdot \gamma \overset{?}{\in} \mathcal{L}_0$ pour les $\delta \in \mathcal{L}_k$: la condition imposée sur k assure qu'il n'y ait qu'un seul $\delta \in \mathcal{L}_k$ pour lequel ce test soit positif, et c'est $\delta = k \cdot \gamma + v(q(\zeta))$.

En utilisant le lemme précédent, on trouve une présentation immédiate z_1 de $\zeta^k q(\zeta)$. Si z est une présentation immédiate de ζ, alors $\dfrac{z_1}{z^k}$ en est une de $q(\zeta)$.□

Remarque Dans [KL], un théorème analogue est démontré sans l'utilisation de ce dernier test, en utilisant un changement de variable pour se ramener au cas où P est un polynôme spécial (*cf.* section 1.4). L'utilisation de ce test ouvre la voie à un résultat plus général qui se peut démontrer de la même façon : si γ est présent avec la multiplicité k dans $\mathcal{PN}(\mathrm{P})$, soient $\zeta_1, \ldots, \zeta_k$ les racines de P de valuation γ; si $q(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$, on sait calculer la liste $\gamma_1, \ldots, \gamma_k$ des valuations $v(q(\zeta_1)), \ldots, v(q(\zeta_k))$. Nous reformulerons ce résultat plus tard, de façon plus précise (*cf.* l'algorithme **SimVal**, en V.2.2, où la preuve est légèrement différente; cependant une preuve suivant de plus près celle-ci peut être donnée).

Théorème 5 *Soit* $(\mathbb{K}, v)$ *un corps valué discret, et soit* Γ *son groupe de valuation ; soit* $\mathrm{P}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ *et* $\gamma \in \Gamma$ *tels que* γ *est une valeur isolée de* $\mathcal{PN}(\mathrm{P})$. *Alors il existe une (unique) extension immédiate* $(\mathbb{K}[\zeta], v)$ *de* $\mathbb{K}$ *avec* $\mathrm{P}(\zeta) = 0$ *et* $v(\zeta) = \gamma$. *C'est un corps valué discret.*

Ce dernier théorème rassemble les résultats de cette section (à condition de lire l'énoncé au sens constructif, où « extension immédiate » signifie « étant donné un élément, on sait en trouver une présentation immédiate »).

Définition Une extension algébrique du type $\mathbb{K} \subseteq \mathbb{K}[\zeta]$ sera appelée *extension hensélienne finie.*

Avant d'exprimer exactement la construction de $\mathbb{K}^h$ on va donner deux résultats qui le concernent ; nous considérons dans un premier temps de façon abstraite que $\mathbb{K}^h$ est l'union de toutes les tours d'extensions henséliennes finies, vues comme plongées dans $\mathbb{K}^{ac}$.

Corollaire 6 *Le hensélisé $\mathbb{K}^h$ de $\mathbb{K}$ est une extension immédiate de $\mathbb{K}$.*

Le corollaire suivant correspond au classique *développement Hensélien* dans le cas où Γ est le groupe $(\mathbb{Z}, +)$.

Corollaire 7 *Soit $\zeta \in \mathbb{K}^h$. On peut calculer une suite de présentations immédiates $(z_n)_{n\in\mathbb{N}}$, avec $\zeta = z_n \cdot (1 + \nu_n)$, telle que, pour tout n, $v(\nu_{n+1}) > v(\nu_n)$.*

Démonstration On calcule d'abord une présentation immédiate : $\zeta = z_0 \cdot (1 + \nu_0)$.

On procède par récurrence. Supposons que $z_0, z_1, \ldots, z_n$ et $\nu_0, \ldots, \nu_n$ soient construits.

Alors ν_n est un élément de $\mathbb{K}[\zeta]$. On en calcule une présentation immédiate $\nu_n = a_n \cdot (1 + \mu_n)$ (avec $\mu_n \in \mathfrak{M}$).

On a alors

$$\zeta = z_n \cdot (1 + \nu_n) = (z_n + z_n \cdot a_n) \cdot \left(1 + \frac{a_n}{1 + a_n}\mu_n\right) ,$$

on peut donc prendre $z_{n+1} = z_n + z_n \cdot a_n$ et $\nu_{n+1} = \dfrac{a_n}{1 + a_n}\mu_n$. Il est facile de vérifier qu'on a bien $v(\nu_{n+1}) > v(\nu_n)$. □

Remarque Dans le cas où $\Gamma = \mathbb{Z}$, on a $v(\nu_n) > n$; on en déduit que les n premiers termes du développement hensélien de ζ coïncident avec les n premiers termes de celui de z_{n-1}.

1.3 Le hensélisé

On sait construire des tours d'extensions henséliennes de $\mathbb{K}$, mais comment atteindre $\mathbb{K}^h$? On pourrait se contenter de ceci, considérant qu'on a un objet dynamique qui grossit au fur et à mesure du « besoin ». Cependant il n'est pas très difficile de construire $\mathbb{K}^h$; nous allons donner les grandes lignes d'une telle construction. Nous avons délibérément choisi une présentation de type «informatique», qui rend très concrètes des considérations classiques du style «limite inductive».

Soient $\llbracket$, $\fatsemi$, $\star$, $\dagger$, $\rrbracket$ des symboles pour l'instant vides de sens (considérés comme de simples lettres). Soit $\mathcal{E}$ le plus petit ensemble clos sous les propriétés suivantes :

– $\mathbb{K} \subseteq \mathcal{E}$ (c'est en fait de l'ensemble support de $\mathbb{K}$ qu'il s'agit) ;
– si $a, b \in \mathcal{E}$, alors $\llbracket a \dagger b \rrbracket \in \mathcal{E}$ et $\llbracket a \star b \rrbracket \in \mathcal{E}$;
– si $a_0, \ldots, a_n, b \in \mathcal{E}$, alors $\llbracket a_0 \fatsemi \cdots \fatsemi a_n \fatsemi b \rrbracket \in \mathcal{E}$.

On convient que $\dagger$ et $\star$ vont représenter, une fois la construction terminée, des lois d'addition et de multiplication ; et que si $v(b)$ est une valeur isolée dans la liste $\mathcal{PN}(a_0 \cdot \mathrm{X}^n + \cdots + a_n)$, le terme $\llbracket a_0 \fatsemi \cdots \fatsemi a_n \fatsemi b \rrbracket \in \mathcal{E}$ représentera l'unique racine de $a_0 \cdot \mathrm{X}^n + \cdots + a_n$ de valuation $v(b)$ (si $v(b)$ n'a pas cette propriété, on peut convenir que ce terme représente 0).

On peut facilement adapter l'algorithme de calcul de présentation immédiate que nous avons donné pour obtenir un algorithme qui s'applique à $\mathcal{E}$. En voici une esquisse. À tout élément t de $\mathcal{E}$ on associe de manière naturelle une tour d'extensions henséliennes $\mathbb{K} \subseteq \mathbb{K}[\zeta_1] \subseteq \mathbb{K}[\zeta_1, \zeta_2] \subseteq \cdots \subseteq \mathbb{K}[\zeta_1, \ldots, \zeta_{n(t)}] = \mathbb{L}_t$ et un élément $\overline{t}$ de $\mathbb{L}_t$, donné par un polynôme en les ζ_i : $\overline{t} = \mathrm{P}(\zeta_1, \ldots, \zeta_{n(t)}) \in \mathbb{L}_t$. Une présentation immédiate de $\overline{t}$ sera par définition *une présentation immédiate de* t.

Pour un terme t de $\mathcal{E}$ notons $\mathcal{L}(t)$ la liste $[\zeta_1, \ldots, \zeta_{n(t)}]$ et $\mathrm{P}_t \in \mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_{n(t)}]$ le polynôme associés ; ils se définissent par récurrence comme suit :

– si $a \in \mathbb{K}$, $\mathcal{L}(a) = \varepsilon$ (la suite vide), et $\overline{a} = a$;
– si $a, b \in \mathcal{E}$, soient $u = \llbracket a \dagger b \rrbracket$ et $v = \llbracket a \star b \rrbracket$.
Alors $n(u) = n(v) = n(a) + n(b)$, et $\mathcal{L}(u) = \mathcal{L}(v) = \mathcal{L}(a) \sqcup \mathcal{L}(b)$; on considère de façon naturelle que $\mathbb{L}_u, \mathbb{L}_v \subseteq \mathbb{L}_t$, et on pose $\overline{a \dagger b} = \overline{a} + \overline{b}$ et $\overline{a \star b} = \overline{a} \cdot \overline{b}$.
– si $t = \llbracket a_0 \fatsemi \cdots \fatsemi a_n \fatsemi b \rrbracket \in \mathcal{E}$; si $v(\overline{b})$ n'est pas une valeur isolée de $\mathcal{PN}(\overline{a_0} \cdot \mathrm{X}^n + \cdots + \overline{a_n})$ on pose $\mathcal{L}(t) = \varepsilon$, $\overline{t} = 0$; dans le cas contraire $n(t) = n(a_0) + \cdots + n(a_n) + 1$, et $\mathcal{L}(t) = \mathcal{L}(a_0) \sqcup \cdots \sqcup \mathcal{L}(a_n) \sqcup [\xi]$, où ξ est l'unique racine de valuation $v(\overline{b})$ de $\overline{a_0} \cdot \mathrm{X}^n + \cdots + \overline{a_n}$. On pose $\overline{t} = \xi$.

On note $u - v$ le terme $\llbracket u \dagger \llbracket (-1) \star v \rrbracket \rrbracket$. Considérons $\mathcal{E}$ quotienté par la relation $u \sim v \iff \overline{u - v} = 0$; les opérateurs $\dagger$ et $\star$ passent au quotient, et en font un corps ; et l'application $t \in \mathcal{E} \mapsto v(\overline{t}) \in \Gamma$ passe au quotient, et en fait un corps valué. $\mathbb{K}$ se plonge de manière naturelle dans ce corps que nous notons $\mathbb{K}^h$. Le schéma d'applications de $\mathcal{E}^{n+2}$ dans $\mathcal{E}$

$$(a_0, \ldots, a_n, b) \in \mathcal{E}^{n+2} \mapsto \llbracket a_0 \fatsemi \cdots \fatsemi a_n \fatsemi b \rrbracket \in \mathcal{E}$$

passe au quotient, et le schéma d'applications

$$\mathcal{H}_n \ : \ a_0, \ldots, a_n, b \in (\mathbb{K}^h)^{n+2} \mapsto \mathcal{H}_n(a_0, \ldots, a_n, b)$$

qui en résulte permet d'exhiber concrètement les racines à la Hensel-Newton du lemme 2 : si $\mathrm{P}(\mathrm{X}) = a_0 \cdot \mathrm{X}^n + \cdots + a_n$ est tel que $\mathcal{PN}(\mathrm{P})$ présente une valeur isolée $v(b)$, alors $\zeta = \mathcal{H}_n(a_0, \ldots, a_n, b)$ est l'unique racine de P de valuation $v(\zeta) = v(b)$. Donc $\mathbb{K}^h$ est hensélien, et c'est bien le hensélisé de $\mathbb{K}$: nous montrerons plus tard la propriété universelle qui le caractérise.

La preuve du lemme 2 permet d'utiliser les applications $\mathcal{H}_n$ pour rendre explicite le lemme de Hensel dans $\mathbb{K}^h$.

Pertinence de la construction Notre construction, pour être exacte, n'en est pas moins peu pertinente d'un point de vue strictement informatique ; si on voulait réellement programmer ceci, il conviendrait de compliquer un peu la définition des termes, afin de diminuer leur complexité « en machine ». En effet, si on suit notre définition à la lettre, la somme de deux éléments d'une même extension se trouve associée à une liste où la description de cette extension se trouve redoublée. On peut par exemple imaginer une routine qui élimine les éléments superflus de cette liste. Cependant, il y a lieu de craindre que même avec une programmation soigneuse, la complexité des termes décrivant des éléments de $\mathbb{K}^h$ croisse très vite même lors de calculs simples en apparence ; ceci étant dû à la récursivité de notre définition.

Correction de la construction Pourquoi cette construction est-elle correcte ? Qu'est-ce qui prouve que le résultat est bien un corps ?

Du point de vue platonicien, si on considère comme acquis le fait que la valuation de $\mathbb{K}$ peut être étendue à $\mathbb{K}^{ac}$, on fixe une telle extension, et on voit le hensélisé comme une certaine sous-extension de $\mathbb{K}^{ac}$; il est alors clair que notre construction explicite cette extension. Les différents éléments de $\mathcal{E}$ équivalents modulo $\sim$ sont différentes manières de décrire un même élément de $\mathbb{K}^{ac}$.

Du point de vue constructif, on va simplement utiliser l'article [CLR] qui prouve constructivement la cohérence relative de la théorie des corps valués algébriquement clos et de la théorie des corps valués : en utilisant cette preuve, si nos calculs en supposant l'existence de $(\mathbb{K}^{ac}, v)$ comme nous l'avons fait mènent à une identité algébrique contradictoire (si l'objet construit manque à satisfaire les axiomes de corps valué), on en déduit une identité algébrique contradictoire dans $\mathbb{K}$.

Signalons enfin qu'il suffirait de prouver :

– premièrement, que l'algorithme qui « choisit » un facteur de P en cas de factorisation en cours de calcul « choisit toujours le même facteur » ; concrètement, si ζ est codé par (P, γ) et si $\mathrm{P} = \mathrm{P}_1 \cdot \mathrm{P}_2 = \mathrm{P}_3 \cdot \mathrm{P}_4$, notre test va renvoyer par exemple $\gamma \in \mathcal{PN}(\mathrm{P}_1)$ et $\gamma \in \mathcal{PN}(\mathrm{P}_3)$; on doit avoir alors $\deg(\mathrm{P}_1 \wedge \mathrm{P}_3) > 0$, et $\gamma \in \mathcal{PN}(\mathrm{P}_1 \wedge \mathrm{P}_3)$. Tout ceci découle naturellement d'un résultat de nature combinatoire sur les polygones de Newton : à savoir, $\mathcal{PN}(\mathrm{P} \cdot \mathrm{Q}) = \mathcal{PN}(\mathrm{P}) \sqcup \mathcal{PN}(\mathrm{Q})$ (à l'ordre près bien sûr ; ici $\sqcup$ est en fait la concaténation des listes). Ainsi $\mathbb{K}[\zeta]$ est bien un corps ;

– deuxièmement, que l'algorithme de calcul de présentation immédiate en fait bien un corps valué. Cela semble également être un résultat combinatoire sur les polygones de Newton.

Ces résultats peuvent être vus comme des conséquences des deux résultats cités plus haut ; cependant ces résultats très concrets doivent pouvoir être prouvés directement de façon constructive ; mais peut-être la preuve naturelle en est-elle quasiment identique à la preuve du théorème de [CLR] évoqué plus haut.

Univers de Herbrand Notons enfin brièvement que le hensélisé de $\mathbb{K}$, tel que nous l'avons présenté, est relié à *l'univers de Herbrand* de la théorie purement équationnelle de $\mathbb{K}$ augmentée du schéma d'axiomes qui correspond au lemme de Hensel ; c'est-à-dire que c'est la plus petite construction qui satisfait cette théorie ; on l'obtient par itération de l'application des axiomes.

Proposition 8 (Propriété universelle) *Soit* $(\mathbb{K}, v)$ *un corps valué. Si* $\Phi : \mathbb{K} \longrightarrow \mathbb{L}$ *est un morphisme de corps valués de* $\mathbb{K}$ *dans* $\mathbb{L}$ *où* $\mathbb{L}$ *est hensélien, alors il y a une manière unique de prolonger* Φ *à* $\mathbb{K}^h$.

Démonstration Soit $u \in \mathbb{K}^h$; par construction, il existe une tour d'extensions henséliennes finies $\mathbb{K} \subseteq \mathbb{K}[\zeta_1] \subseteq \cdots \subseteq \mathbb{K}[\zeta_1, \ldots, \zeta_n] = \mathbb{K}_1$ telle que u est un élément de $\mathbb{K}_1$.

On va construire l'extension de Φ à $\mathbb{K}_1$, de manière unique ; on aura ainsi $\Phi(u)$ l'image de u. L'élément ζ_1 est l'unique racine de valuation γ_1 d'un polynôme $\mathrm{P}_1(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$; $\mathbb{L}$ étant hensélien, il existe un unique $\xi_1 \in \mathbb{L}$ tel que $v(\xi_1) = \gamma_1$ et $\mathrm{P}_1(\xi_1) = 0$. Alors pour prolonger Φ il n'y a pas d'autre choix que de poser $\Phi(\zeta_1) = \xi_1$. On recommence cette opération n fois, et on a construit une extension de Φ à $\mathbb{K}_1$ qui est la seule possible.

Le point délicat est qu'il n'y pas unicité de la tour d'extensions finies $\mathbb{K} \subseteq \mathbb{K}[\zeta_1] \subseteq \cdots \subseteq \mathbb{K}[\zeta_1, \ldots, \zeta_n] = \mathbb{K}_1$ telle que $u \in \mathbb{K}_1$; soit $\mathbb{K} \subseteq \mathbb{K}[\zeta'_1] \subseteq \cdots \subseteq \mathbb{K}[\zeta'_1, \ldots, \zeta'_m] = \mathbb{K}_2$ avec $u \in \mathbb{K}_2$ et $\xi'_1, \ldots, \xi'_m \in \mathbb{L}$ les images naturelles des ζ'_i.

On a $u = \mathrm{P}(\zeta_1, \ldots, \zeta_n) \in \mathbb{K}_1$ et $u = \mathrm{Q}(\zeta'_1, \ldots, \zeta'_m) \in \mathbb{K}_2$; on se place dans $\mathbb{K}[\zeta_1, \ldots, \zeta_n, \zeta'_1, \ldots, \zeta'_m] = \mathbb{K}_1\mathbb{K}_2$ où on a $\mathrm{P}(\zeta_1, \ldots, \zeta_n) = \mathrm{Q}(\zeta'_1, \ldots, \zeta'_m)$. La seule manière d'étendre Φ à $\mathbb{K}_1\mathbb{K}_2$ est de poser $\Phi(\zeta_i) = \xi_i$ et $\Phi(\zeta'_i) = \xi'_i$, et on a $\mathrm{P}(\xi_1, \ldots, \xi_n) = \mathrm{Q}(\xi'_1, \ldots, \xi'_m) = \Phi(u)$.

C'est essentiellement la correction de la construction qui a été utilisée ici ; en effet les différentes tours associées à u sont étroitement liées aux différents termes de $\mathcal{E}$ qui représentent u. □

1.4 Éléments primitifs

On va montrer que toutes les extensions de degré fini, intermédiaires entre $\mathbb{K}$ et $\mathbb{K}^h$, admettent un élément primitif.

Définition Soit $\mathrm{S}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$. On dit que S est un *polynôme spécial* si il est de la forme $\mathrm{S}(\mathrm{X}) = \mathrm{X}^n - \mathrm{X}^{n-1} + c_2 \cdot \mathrm{X}^{n-2} + \cdots + c_n$, avec $c_i \in \mathfrak{M}$ pour $i = 2, \ldots, n$. Dans ce cas $(\mathrm{S}, 0)$ est un code à la Hensel-Newton, correspondant à un élément σ de $\mathbb{K}^h$ de résidu $\overline{\sigma} = 1$, le *zéro spécial* de $\mathrm{S}(\mathrm{X})$.

Lemme 9 *Soit* (P, γ) *un code à la Hensel-Newton,* ζ *l'élément de* $\mathbb{K}^h$ *associé. Alors il existe un polynôme spécial* $\mathrm{S}(\mathrm{X})$*, tel que le zéro* σ *associé à* $(\mathrm{S}, 0)$ *engendre le même corps que* ζ *:* $\mathbb{K}[\zeta] = \mathbb{K}[\sigma]$.

Démonstration Soit $P(X) = a_0 \cdot X^n + \ldots + a_n \in \mathbb{K}[X]$. On suppose que le polygone de Newton de P a une pente de largeur 1, entre les points $\big(i, v(a_i)\big)$ et $\big(i+1, v(a_{i+1})\big)$. On a $\gamma = v(a_{i+1}) - v(a_i)$.

Comme dans la démonstration du lemme 2, on pose

$$Q(X) = \frac{a_i^{n-i-1}}{a_{i+1}^{n-i}} P\left(-\frac{a_{i+1}}{a_i} X\right).$$

Le polynôme $\overline{Q}(X) \in \Bbbk[X]$ admet 1 comme racine simple.

On pose alors $R(X) = Q(X+1) = b_0 \cdot X^n + \cdots + b_n$. On a $v(b_n) > 0$ et $v(b_{n-1}) = 0$. Si $b_n = 0$, alors $\zeta = -\dfrac{a_{i+1}}{a_i} \in \mathbb{K}$, et $\mathbb{K}[\zeta] = \mathbb{K}$. Si $b_n \neq 0$, soit $T(X) = \dfrac{1}{b_n} R(\dfrac{b_n}{b_{n-1}} X)$ et $S(X) = X^n T(1 \,/\, X)$.

On vérifie que S est un polynôme spécial. Si σ est l'élément associé au code $(S, 0)$, on peut écrire ζ sous la forme $\zeta = \dfrac{a\sigma + b}{c\sigma + d}$, avec $a, b, c, d \in \mathfrak{V}$, $c\sigma + d \neq 0$ et $ad - bc \neq 0$.

On a donc bien $\mathbb{K}[\zeta] = \mathbb{K}[\sigma]$. □

On déduit de ce lemme qu'une extension $\mathbb{K} \subset \mathbb{K}[\zeta_1, \ldots, \zeta_k] \subset \mathbb{K}^h$ peut se réécrire $\mathbb{K}[\zeta_1, \ldots, \zeta_k] = \mathbb{K}[\sigma_1, \ldots, \sigma_k]$ où chaque σ_i est codé par $(S_i, 0)$, où $S_i \in \mathbb{K}[\sigma_1, \ldots, \sigma_{i-1}]$ est un polynôme spécial.

Théorème 10 *A tout moment de la construction de $\mathbb{K}^h$, une extension $\mathbb{K} \subset \mathbb{K}[\zeta_1, \ldots, \zeta_k] \subset \mathbb{K}^h$ peut se réécrire sous la forme $\mathbb{K}[\zeta_1, \ldots, \zeta_k] = \mathbb{K}[\xi]$, où ξ est donné par un code à la Newton-Hensel.*

Démonstration Il suffit de considérer des extensions successives par des polynômes spéciaux, et par récurrence le cas $k = 2$ suffit.

Soit donc une extension $\mathbb{K} \subset \mathbb{K}[\alpha, \beta]$, où α, β sont définis par des polynômes spéciaux $P(X) \in \mathbb{K}[X]$, et $Q_\alpha(X) \in \mathbb{K}[\alpha][X]$.

• La preuve est proche de celle du théorème II.5 — nous allons l'utiliser, le lecteur est prié de s'y référer. On va d'abord construire un polynôme spécial de $R(X) \in \mathbb{K}[X]$ dont le zéro spécial sera γ, tel que $\mathbb{K}[\alpha, \beta] = \mathbb{K}[\alpha, \gamma]$.

Soient $\alpha_1 = \alpha, \ldots, \alpha_n$ les racines de P. Les racines des polynômes Q_{α_i} sont notées comme suit.

$$\begin{array}{cccc} \text{racines de } Q_{\alpha_1} : & \beta_{11} & \cdots & \beta_{1m} \\ \vdots & \vdots & & \vdots \\ \text{racines de } Q_{\alpha_n} : & \beta_{n1} & \cdots & \beta_{nm} \end{array}$$

On pourra supposer que $\beta_{11} = \beta$. C'est la seule racine parmi les racines de Q_α, $\beta_{11}, \ldots, \beta_{1m}$, à être de valuation nulle.

Soit

$$S_{\alpha_i}^k(X) = \prod_{j=1}^{m} \big(X - {\alpha_i}^k \cdot \beta_{ij}\big),$$

qui est un polynôme de $\mathbb{K}[\alpha_i][\mathrm{X}]$. On peut calculer $\widetilde{\mathrm{S}}^k(\mathrm{X}) = \prod_{i=1}^n \mathrm{S}^k_{\alpha_i}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$.

Les racines de $\widetilde{\mathrm{S}}^k$ sont les $(\alpha_i)^k \cdot \beta_{ij}$, pour $i = 1, \ldots, n$ et $j = 1, \ldots, m$.

Pour chaque valeur de k, le polygone de Newton de $\widetilde{\mathrm{S}}^k$ présente au moins une fois la valeur 0 : en effet $(\alpha_1)^k \cdot \beta_{11}$ a toujours valuation 0. De plus on peut trouver k tel que cette valeur soit isolée ; en effet,

$$k \cdot v(\alpha_i) + v(\beta_{ij}) = 0 \iff \begin{cases} i = 1\,, & \text{et } j = 1 \\ \text{ou bien} & \\ i > 1\,, & \text{et } j \text{ est tel que } k \cdot v(\alpha_i) = -v(\beta_{ij})\,. \end{cases}$$

Il n'y a clairement qu'un nombre fini de valeurs de k pour lesquelles la valeur 0 n'est pas isolée dans $\mathcal{PN}(\widetilde{\mathrm{S}}^k)$. On peut en trouver une par essais successifs $(k = 0, 1, \ldots)$.

Soit donc un tel k, et soit $\gamma_0 = \alpha^k \cdot \beta = (\alpha_1)^k \cdot \beta_{11}$. On pose $\mathrm{R}_0(\mathrm{X}) = \widetilde{\mathrm{S}}^k(\mathrm{X})$. On a bien $\mathbb{K}[\alpha, \beta] = \mathbb{K}[\alpha, \gamma_0]$, et d'autre part $(\mathrm{R}_0, 0)$ est un code à la Hensel-Newton pour γ_0. Le lemme précédent nous permet de trouver un polynôme spécial $\mathrm{R}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ dont le zéro spécial γ vérifie $\mathbb{K}[\gamma_0] = \mathbb{K}[\gamma]$, et donc $\mathbb{K}[\alpha, \beta] = \mathbb{K}[\alpha, \gamma]$.

- La suite est identique à ce qui a été fait pour le théorème II.5. On calcule

$$\mathrm{T}(\mathrm{X}) = \prod_{\substack{\alpha\,:\,\mathrm{P} \\ \gamma\,:\,\mathrm{R}}} (\mathrm{X} - (\alpha + u \cdot \gamma))$$

pour une valeur de u bien choisie ; en plus des conditions de la preuve de II.5 sur u, nous avons d'autres exigences. Nous ne répéterons pas les conditions sur u pour que $\alpha + u \cdot \gamma$ soit élément primitif, ni la manière de les vérifier.

Soient $\gamma_1 = \gamma, \ldots, \gamma_\ell$ les racines de R.

On a $\overline{\gamma_1} = 1$ et, pour tout $i > 1$, $v(\gamma_i) > 0$. On va utiliser également le fait que $\overline{\alpha_1} = 1$ et que pour tout $i > 1$, $v(\alpha_i) > 0$.

Premier cas : $\Bbbk \neq \mathbb{F}_2$.

Soit $\mu \in \Bbbk^\times$ tel que $\mu + 1 \neq 0 \in \Bbbk$.

On va choisir un élément primitif de la forme $\xi = \alpha + u \cdot \gamma$, en imposant de plus que $\overline{u} = \mu$ (il y a un nombre infini de u qui vérifient cette condition). On obtient un polynôme $\mathrm{T}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ dont les racines sont les $\xi_{ij} = \alpha_i + u \cdot \gamma_j$.

Il suffit de pouvoir identifier parmi les racines de T la racine ξ_{11} comme une racine à la Newton-Hensel. Or les racines de T ont pour résidu possible les valeurs 0, 1, et $1 + \mu$. On a $\overline{\xi_{11}} = 1 + \mu$ et c'est la seule des racines de T qui vérifie ceci ; le polygone de Newton du polynôme $\mathrm{T}(\mathrm{X} - (1 + \mu))$ présente donc une seule valeur strictement positive, qui de plus est isolée.

Deuxième cas : $\Bbbk = \mathbb{F}_2$.

D'après le corollaire 7, il existe une infinité de présentations immédiates d'un élément donné.

On considère une présentation immédiate u de $-\dfrac{\alpha}{\gamma}$:

$$-\frac{\alpha}{\gamma} = u \cdot (1+\nu)$$

telle que $\alpha + u \cdot \gamma$ soit un élément primitif pour $\mathbb{K}[\alpha, \gamma]$.

On obtient un polynôme $\mathrm{T}_u(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ dont les racines sont les $\xi_{ij} = \alpha_i + u \cdot \gamma_j$.

Alors

$$\begin{cases} \xi_{11} & = & \alpha_1 + u \cdot \gamma_1 & = & \alpha_1 \dfrac{\nu}{1+\nu} \\ \text{et} & & & & \\ \xi_{ij} & = & \alpha_i + u \cdot \gamma_j & = & \alpha_1 \dfrac{\nu}{1+\nu} \left(\dfrac{\gamma_j}{\gamma_1} + \dfrac{1+\nu}{\nu} \left(\dfrac{\alpha_i}{\alpha_1} - \dfrac{\gamma_j}{\gamma_1} \right) \right) . \end{cases}$$

C'est ξ_{11} qui nous intéresse. Sa valuation est $v(\nu)$.

Le corollaire 7 nous permet également de choisir u et ν tels que

$$v(\nu) \neq v \left(\frac{\alpha_i}{\alpha_1} - \frac{\gamma_j}{\gamma_1} \right) \quad \forall (i,j) \neq (1,1) .$$

On vérifie alors que dans ce cas $v(\xi_{ij}) \neq v(\xi_{11})$ dès que $(i,j) \neq (1,1)$. Donc le polygone de Newton de T_u présente une valeur isolée qui correspond à ξ_{11}.

En pratique, on essaiera pour u les différentes valeurs fournies par le corollaire 7, une à une : toutes sauf un nombre fini font de $\alpha + u \cdot \gamma$ un élément primitif, et parmi celles-ci, seul un nombre fini est exclu par cette dernière condition. Il suffit de calculer $\mathcal{PN}(\mathrm{T}_u)$ pour vérifier que le u choisi convient. $\square$

Le corollaire suivant est immédiat.

Corollaire 11 *Toute sous extension de degré fini* $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}^h$ *peut être écrite* $\mathbb{L} = \mathbb{K}[\alpha]$ *où* α *est la racine d'un polynôme spécial* $\mathrm{S}(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$.

2 Les corps henséliens

Nous présentons nos résultats pour un corps $(\mathbb{L}, v)$ hensélien; c'est-à-dire pour nous un corps satisfaisant de façon explicite la condition décrite par le lemme 2; en utilisant la preuve de ce lemme, on sait rendre explicite le lemme de Hensel. D'autre part cette même preuve indique que dans un corps $\mathbb{L}$ où le lemme de Hensel est explicite, alors cette condition est satisfaite. On dispose donc d'un schéma d'applications $\mathcal{H}_n : \mathbb{L}^{n+2} \longrightarrow \mathbb{L}$ (partiellement définies) telles que si $\mathrm{P}(\mathrm{X}) = a_0 \cdot \mathrm{X}^n + \cdots + a_n \in \mathbb{L}[\mathrm{X}]$ est un polynôme dont le polygone de Newton présente une valeur isolée $v(b)$, $\mathcal{H}_n(a_0, \ldots, a_n, b) \in \mathbb{L}$ est la racine de P de valuation $v(b)$.

En pratique, $\mathbb{L}$ pourra être un corps donné explicitement comme hensélien, ou étant donné un corps valué $\mathbb{K}$, $\mathbb{K}^h$ ou une de ses extensions algébriques (*cf. infra*). L'anneau de valuation de $\mathbb{L}$ est $\mathfrak{V}_{\mathbb{L}} = \mathfrak{V}$, son corps résiduel est $\mathbb{l}$, de clôture algébrique $\mathbb{l}^{ac}$; la clôture algébrique de $\mathbb{L}$ est $\mathbb{L}^{ac}$, munie d'une extension de v, la valuation de $\mathbb{L}$.

Nous allons montrer la plupart des conséquences classiques du lemme de Hensel.

2.1 Le polygone de Newton

Le lemme de Newton

Il n'est pas facile de baptiser correctement tous les lemmes équivalents au lemme de Hensel, car les noms varient au fil de la littérature ; il n'est pas facile non plus de choisir lesquels prouver, car ils sont nombreux ; le suivant nous a semblé digne d'intérêt car il est souvent utilisé. Il est sans doute possible d'en trouver une preuve constructive dans la littérature, peut-être même la nôtre.

Proposition 12 (Lemme de Newton) *Soit* $\mathrm{P}(\mathrm{X}) \in \mathfrak{V}[\mathrm{X}]$ *et soit* $a \in \mathfrak{V}$ *tel que* $v(\mathrm{P}(a)) > 2 \cdot v(\mathrm{P}'(a))$. *Alors il existe une racine* $\zeta \in \mathfrak{V}$ *de* P *telle que* $v(\zeta - a) > v(\mathrm{P}'(a))$.

Démonstration Soit $\mathrm{Q}(\mathrm{X}) = \mathrm{P}(\mathrm{X}+a) \in \mathfrak{V}[\mathrm{X}]$. On a $v(\mathrm{Q}(0)) > 2 \cdot v(\mathrm{Q}(0))$. On écrit $\mathrm{Q}(\mathrm{X}) = a_0 \cdot \mathrm{X}^n + \cdots + a_n$. Soient les points $\mathfrak{p}_i = (i, v(a_i))$ qui servent à construire le polygone de Newton. Les hypothèses se traduisent par $\forall i\ v(a_i) \geq 0$ et $v(a_n) > 2 \cdot v(a_{n-1})$. On en déduit facilement que le segment $[\mathfrak{p}_{n-1}, \mathfrak{p}_n]$ est dans le polygone de Newton de Q, qui possède donc une racine ξ de valuation $v(a_n) - v(a_{n-1}) = v(\mathrm{P}(a)) - v(\mathrm{P}'(a))$.

Alors $\zeta = \xi + a$ est une racine de P. On a $v(\zeta - a) = v(\mathrm{P}(a)) - v(\mathrm{P}'(a)) > v(\mathrm{P}'(a))$. □

Le polygone de Newton

Cette fois-ci c'est le théorème que nous avons donné de façon non constructive plus haut (th. II.9) que nous allons prouver.

Théorème 13 *Soit* $\mathrm{P} \in \mathbb{L}[\mathrm{X}]$ *un polynôme unitaire. À chaque segment de largeur* ℓ *et de pente* γ *dans le polygone de Newton de* P *correspond un facteur de* P, $\mathrm{Q} \in \mathbb{L}[\mathrm{X}]$, *avec* $\deg \mathrm{Q} = \ell$ *et toutes les racines de* Q *(dans* $\mathbb{L}^{ac}$*) sont de valuation* γ *(donc* $\mathcal{PN}(\mathrm{Q}) = [\gamma, \ldots, \gamma]$*). Les coefficients de* Q *sont décrits par un calcul uniforme comme éléments de* $\mathbb{L}$.

Démonstration Soient α_i, $(i = 1, \ldots, n)$, les zéros de P dans $\mathbb{L}^{ac}$, classés par valuations croissantes.

On va montrer comment calculer le facteur $\mathrm{Q}(\mathrm{X}) = \mathrm{X}^\ell + a_1\mathrm{X}^{\ell-1} + \cdots + a_\ell = \prod_{i=1\ldots\ell}(\mathrm{X} - \alpha_i)$ correspondant au premier segment du polygone de Newton de P, de largeur $\ell < n$ et de pente γ (γ est donc le plus petit élément de $\mathcal{PN}(\mathrm{P})$, et il y est présent avec multiplicité ℓ).

On calcule tout d'abord le terme constant de Q : soient $\mathrm{I}_1, \ldots, \mathrm{I}_k$ les parties à ℓ éléments de $\{1, \ldots, n\}$. On pose $\delta_i = \prod_{j \in \mathrm{I}_i} \alpha_j$.

On peut supposer $\mathrm{I}_1 = \{1, \dots, \ell\}$, et donc $\delta_1 = (-1)^\ell a_\ell = \alpha_1 \cdots \alpha_\ell$. Alors $v(\delta_1) = \ell \cdot \gamma < v(\delta_j)$ pour tout $j > 1$, car $v(\alpha_i) = \gamma < v(\alpha_j)$ pour tout $i \leq \ell$ et $j > \ell$.

En utilisant le lemme II.2, on calcule le polynôme $\mathrm{R} = \prod_{i=1,\dots,k}(\mathrm{X} - \delta_i)$.

Le polygone de Newton de R présente donc une pente isolée, de pente $\ell \cdot \gamma$, ce qui explicite a_ℓ comme élément de $\mathbb{L}$. On trouve également dans $\mathcal{PN}(\mathrm{R})$ la liste des valuations $v(\delta_i)$ pour $i > 1$.

On peut maintenant déterminer les autres a_i : soit $m < \ell$ fixé. On calcule

$$a_m = (-1)^m \sum_{1 \leq i_1 < \cdots < i_m \leq \ell} \alpha_{i_1} \cdots \alpha_{i_m}.$$

Comme dans ce qui précède on pose, pour i variant de 1 à k,

$$\Delta_i = \sum_{\substack{j_1 < \cdots < j_m \\ j_1, \dots, j_m \in \mathrm{I}_i}} \alpha_{j_1} \cdots \alpha_{j_m}.$$

Notons que $a_m = (-1)^m \Delta_1$.

On calcule $\mathrm{S}_0(\mathrm{X}) = \prod(\mathrm{X} - \Delta_i)$. Son polygone de Newton nous fournit la liste $\mathcal{L}$ des valuations des Δ_i. Ici on ne sait pas séparer *a priori* Δ_1 des autres éléments de $\mathcal{L}$: il n'est pas nécessairement isolé.

On pose $\widetilde{\Delta}_i^k = (\delta_i)^k \Delta_i$ et bien sûr $\mathrm{S}_k(\mathrm{X}) = \prod(\mathrm{X} - \widetilde{\Delta}_i^k)$. Ce polynôme est à nouveau calculable à partir des coefficients de P. On pose $\mathcal{L}_k = \mathcal{PN}(\mathrm{S}_k)$.

Maintenant, on peut choisir k tel que $v(\widetilde{\Delta}_1^k) \neq v(\widetilde{\Delta}_i^k)$ pour $i > 1$: il suffit de remarquer que c'est équivalent à

$$k \cdot (v(\delta_1) - v(\delta_i)) \neq (v(\Delta_i) - v(\Delta_1)).$$

Or les $v(\delta_1) - v(\delta_i)$ sont tous non nuls, donc un tel k existe ; on peut en calculer un à l'aide la liste $\mathcal{L}$, en imposant $k \cdot (v(\delta_1) - v(\delta_i)) \neq (\varepsilon_1 - \varepsilon_2)$ pour tous les $i > 1$ et tous les $\varepsilon_1, \varepsilon_2 \in \mathcal{L}$.

Alors pour un tel k, $\mathcal{L}_k$ présente une valeur isolée $v(\nu)$ qui correspond à la racine $\widetilde{\Delta}_1^k$.

Si on sait déterminer laquelle, on explicite $\widetilde{\Delta}_1^k = (\delta_1)^k \cdot \Delta_1$ comme élément du hensélisé, donc Δ_1. Or, même si $\mathcal{L}_k$ présente plusieurs valeurs isolées $\varepsilon_1, \varepsilon_2, \dots$, une seule d'entre elles satisfait au test $\varepsilon - k \cdot v(\delta_1) \overset{?}{\in} \mathcal{L}$, d'après la condition sur k, et c'est celle qui correspond à la racine $\widetilde{\Delta}_1^k$ de S_k.

Ainsi on a calculé Q, un facteur de P ; on fait la division euclidienne de P par Q, et on recommence. □

2.2 Autres résultats classiques ou non.

Ici les preuves constructives, jusqu'alors élémentaires dans leurs outils mais un peu complexes dans leur déroulement, deviennent réellement des preuves élémentaires extrèmement agréables. Nous pensons qu'utiliser, comme nous allons le faire, le théorème 13 pour donner des preuves effectives d'une série de résultats équivalents au lemme de Hensel, est une approche élégante de la théorie des corps henséliens. L'enchaînement logique qui se fait entre les divers résultats présentés nous paraît naturel et instructif.

Un critère de factorisation

Le théorème suivant est une généralisation du théorème 13. C'est en fait lui qui va servir à montrer presque tous les résultats classiques.

Théorème 14 *Soit* $\mathrm{P(X)} \in \mathbb{L}[\mathrm{X}]$ *et soient* $\alpha_1, \ldots, \alpha_n$ *ses racines dans* $\mathbb{L}^{ac}$*. Si on a* $\mathrm{Q(X)} \in \mathbb{L}[\mathrm{X}]$ *tel que la liste des valuations* $v\big(\mathrm{Q}(\alpha_i)\big)$ *—qui est* $\mathcal{PN}(\mathrm{T_{P,Q}})$*— comporte plusieurs valeurs distinctes, alors* $\mathrm{P(X)}$ *se factorise dans* $\mathbb{L}(\mathrm{X})$*.*

De plus si les valeurs distinctes présentes dans $\mathcal{PN}(\mathrm{T_{P,Q}})$*,* $\gamma_1, \ldots, \gamma_k$*, le sont avec multiplicités respectives* $n_1, \ldots, n_k$*, alors* $\mathrm{P(X)}$ *se factorise en* k *facteurs* $\mathrm{P}_1, \ldots, \mathrm{P}_k$ *de degrés respectifs* $n_1, \ldots, n_k$*, et* $\mathcal{PN}(\mathrm{T}_{\mathrm{P}_i,\mathrm{Q}})$ *est la liste* $[\underbrace{\gamma_i, \ldots, \gamma_i}_{n_i\ \textit{fois.}}]$*.*

Les P_i *sont premiers deux à deux.*

Démonstration On considère donc le polygone de Newton de $\mathrm{T_{P,Q}}$. On peut le factoriser en k facteurs unitaires $\mathrm{T}_1, \ldots, \mathrm{T}_k$, avec $\deg \mathrm{T}_i = n_i$ et $\mathcal{PN}(\mathrm{T}_i) = [\gamma_i, \ldots, \gamma_i]$.

Les T_i sont clairement premiers deux à deux : on applique le lemme II.3 et on conclut. □

Un cas particulier est $\mathrm{Q(X)} = \mathrm{X}$: c'est le théorème 13. Ce théorème peut se démontrer très directement à partir de la propriété classique

$$\forall \sigma \in \mathrm{Aut}(\mathbb{L}^{ac} \,/\, \mathbb{L}),\ \forall \alpha \in \mathbb{L}^{ac},\ v(\sigma\alpha) = v(\alpha).$$

Il permettra en fait dans la suite de remplacer cette propriété.

Relever des factorisations

Théorème 15 *Soit* $\mathrm{P(X)} \in \mathfrak{V}_{\mathbb{L}}[\mathrm{X}]$*. On suppose qu'il existe deux polynômes* $q(\mathrm{X}), r(\mathrm{X}) \in \mathbb{l}(\mathrm{X})$ *premiers entre eux, tels que* $\overline{\mathrm{P}} = q \cdot r$*. Alors cette factorisation se relève de manière unique dans* $\mathfrak{V}_{\mathbb{L}}[\mathrm{X}]$ *—c.-à-d. qu'il existe* $\mathrm{Q(X)}, \mathrm{R(X)} \in \mathfrak{V}_{\mathbb{L}}[\mathrm{X}]$*, uniques si on impose* Q*,* q *unitaires et* $\deg \mathrm{Q} = \deg q$*, tels que* $\mathrm{P} = \mathrm{Q} \cdot \mathrm{R}$ *et* $\overline{\mathrm{Q}} = q$*,* $\overline{\mathrm{R}} = r$*.*

Démonstration Il est clair que P a nécessairement dans $\mathbb{L}^{ac}$ des racines de valuation positive ou nulle. Si P a également des racines de valuation strictement négative, on peut utiliser le théorème 13 pour factoriser P en $\mathrm{P}_1 \cdot \mathrm{P}_2$, où les racines de P_1 sont de valuation positive, et ce sont toutes les racines de P de valuation positive. On peut supposer $\overline{\mathrm{P}}(\mathrm{X}) = \overline{\mathrm{P}_1}(\mathrm{X})$ et $\overline{\mathrm{P}_2}(\mathrm{X}) = 1$. Si on a une factorisation $\mathrm{P}_1 = \mathrm{Q} \cdot \mathrm{R}$ avec $\deg \mathrm{Q} = \deg q$, $\overline{\mathrm{Q}} = q$ et $\overline{\mathrm{R}} = r$, on a alors $\mathrm{P} = \mathrm{Q} \cdot (\mathrm{R} \cdot \mathrm{P}_2)$, qui est la factorisation de P voulue.

Soient $n = \deg \mathrm{P}_1$ et $m = \deg q$. On appelle $\alpha_1, \ldots, \alpha_n$ les racines de $\mathrm{P}_1(\mathrm{X})$ dans $\mathbb{L}^{ac}$, avec $\overline{\alpha_1}, \ldots, \overline{\alpha_m}$ les racines de q dans $\mathbb{L}^{ac}$. Comme q et r sont premiers entre eux, on a $q(\overline{\alpha_i}) \neq 0$ pour $i > m$.

Soit $\mathrm{Q}_0(\mathrm{X}) \in \mathbb{L}[\mathrm{X}]$ un relèvement unitaire de $q(\mathrm{X})$. On a $\overline{\mathrm{Q}_0(\alpha_i)} = q(\overline{\alpha_i})$, et donc $v\big(\mathrm{Q}_0(\alpha_i)\big) > 0$ pour $i = 1, \ldots, m$ et $v\big(\mathrm{Q}_0(\alpha_i)\big) = 0$ pour $i > m$.

On peut donc factoriser $\mathrm{T}_{\mathrm{P}_1,\mathrm{Q}_0}$; on utilise le théorème précédent pour obtenir une factorisation $\mathrm{P}_1 = \mathrm{Q} \cdot \mathrm{R}$, avec $\deg \mathrm{Q} = m$, où $\mathcal{PN}(\mathrm{T}_{\mathrm{Q},\mathrm{Q}_0})$ ne comporte que des valeurs strictement positives, et $\mathcal{PN}(\mathrm{T}_{\mathrm{R},\mathrm{Q}_0})$ est une liste de zéros.

On a donc $\overline{\mathrm{Q}} = \overline{\mathrm{Q}_0} = q$ et par conséquent $\overline{\mathrm{R}} = r$. Si on impose Q(X) unitaire, l'unicité découle du fait qu'on a nécessairement $\mathrm{Q}(\mathrm{X}) = (\mathrm{X} - \alpha_1) \cdots (\mathrm{X} - \alpha_m)$.

□

Calculs dans les extensions algébriques d'un corps hensélien

Même en l'absence de test d'irréducibilité dans $\mathbb{L}[\mathrm{X}]$, on peut calculer dans les extensions algébriques de $\mathbb{L}$.

On dira qu'un polynôme $\mathrm{P}(\mathrm{X}) \in \mathbb{L}[\mathrm{X}]$ est *présumé irréductible* si il n'y a pas de valeurs distinctes dans $\mathcal{PN}(\mathrm{P})$. On supposera en outre que si sa dérivée n'est pas nulle (ce qui peut arriver en caractéristique positive) il est premier avec celle-ci. En caractéristique $p > 0$, si $\mathrm{P}(\mathrm{X}) = \mathrm{Q}(\mathrm{X}^{p^k})$, avec $\mathrm{Q}'(\mathrm{X}) \neq 0$, il sera naturel d'imposer que Q soit premier avec Q′. On calcule dans un corps de rupture de P : l'idée reste la même, on fait comme si P était irréductible, et s'il ne l'est pas on est amené à le remplacer par un de ses facteurs, sans que la validité des calculs qui précèdent cette substitution soit en cause. En l'absence d'un moyen de choisir un facteur de P plutôt qu'un autre, on peut être amené à ouvrir plusieurs branches de calcul différentes, chacune correspondant à un des nouveaux facteurs, de façon à connaître le résultat pour toutes les racines de P.

Le théorème suivant est une version effective de l'unicité de l'extension de la valuation v de $\mathbb{L}$ à une extension algébrique.

Théorème 16 (Valuation et résidu d'un élément) *Soit* $\mathrm{P}(\mathrm{X}) \in \mathbb{L}[\mathrm{X}]$ *un polynôme présumé irréductible de degré n. Soit $\alpha \in \mathbb{L}^{ac}$ une de ses racines. Soit* $q(\mathrm{X}) \in \mathbb{L}[\mathrm{X}]$ *un polynôme de degré strictement inférieur à n. Alors il y a un algorithme qui calcule $v\big(q(\alpha)\big) \in \overline{\Gamma}$: une seule valeur est possible,* ***ou bien*** *on produit une factorisation de* $\mathrm{P}(\mathrm{X})$ *dans* $\mathbb{L}[\mathrm{X}]$.

Si $q(\alpha)$ est de valuation 0, on produit un polynôme $r(\mathrm{X}) \in \mathbb{I}(\mathrm{X})$ dont $\overline{q(\alpha)}$ est racine. Si $r(\mathrm{X})$ s'avère ne pas être irréductible (ou une puissance d'un irréductible), on obtient une factorisation de $\mathrm{P}(\mathrm{X})$ *dans* $\mathbb{L}[\mathrm{X}]$.

Démonstration Il s'agit en fait d'une relecture du théorème 14 : pour calculer $v\big(q(\alpha)\big)$, on calcule $\mathcal{PN}(\mathrm{T}_{\mathrm{P},q})$. Si il n'y a qu'une valeur dans cette liste, c'est

$v\big(q(\alpha)\big)$, et si il y a des valeurs distinctes, on peut factoriser $\mathrm{P(X)}$ dans $\mathbb{L}[\mathrm{X}]$.

Si $q(\alpha)$ est de valuation nulle, on peut prendre $r(\mathrm{X}) = \overline{\mathrm{T}_{\mathrm{P},q}}(\mathrm{X})$. Si on a une factorisation de $r(\mathrm{X})$ en deux facteurs premiers entre eux dans $\mathbb{l}[\mathrm{X}]$, on en déduit (théorème 15) une factorisation de $\mathrm{T}_{\mathrm{P},q}$ en deux facteurs premiers entre eux, $\mathrm{T}_{\mathrm{P},q} = \mathrm{R} \cdot \mathrm{S}$. On peut alors utiliser à nouveau le lemme II.3 pour factoriser P.
$\square$

Remarque Dans le cas où P est irréductible, on retombe sur le résultat classique

$$\forall \beta \in \mathbb{L}[\alpha],\ \ v(\beta) = \frac{v(\mathrm{N}(\beta))}{n}.$$

Théorème 17 *Soit* $\mathrm{P(X)} \in \mathbb{L}[\mathrm{X}]$ *un polynôme présumé irréductible et* $\alpha \in \mathbb{L}^{ac}$ *une de ses racines. Le théorème du polygone de Newton (théorème 13) est vrai dans* $\mathbb{L}[\alpha]$ *: soit* $\mathrm{Q}_\alpha(\mathrm{X}) = q(\alpha, \mathrm{X}) \in \mathbb{L}[\alpha][\mathrm{X}]$ *; alors on peut calculer* $\mathcal{PN}(\mathrm{Q}_\alpha)$ *et, si il y a plusieurs pentes, factoriser* $\mathrm{Q}_\alpha(\mathrm{X})$ *dans* $\mathbb{L}[\alpha](\mathrm{X})$*. Éventuellement, au cours du calcul, il peut apparaître une factorisation de* P *; dans ce cas, on obtient un résultat (différent) pour chacun des facteurs de* P*.*

Démonstration Pour calculer le polygone de Newton de Q_α, il s'agit juste de calculer la valuation de certains éléments de $\mathbb{L}[\alpha]$ — éventuellement, en cours de route, apparaît une factorisation de P, qu'on peut alors remplacer par un de ses facteurs.

On suppose que $\mathcal{PN}(\mathrm{Q}_\alpha)$ est composé des valeurs distinctes $\gamma_1, \dots, \gamma_k$, présentes avec les multiplicités respectives $n_1, \dots, n_k$.

Soient $\alpha = \alpha_1, \dots, \alpha_n$ les racines de P. On pose

$$\widetilde{\mathrm{Q}}(\mathrm{X}) = \prod_{\alpha\,:\,\mathrm{P}} \mathrm{Q}_\alpha(\mathrm{X}) = \prod_{i=1}^{n} \mathrm{Q}_{\alpha_i}(\mathrm{X})$$

D'après le lemme II.2, $\widetilde{\mathrm{Q}}(\mathrm{X})$ est dans $\mathbb{L}[\mathrm{X}]$. Le polygone de Newton de $\widetilde{\mathrm{Q}}$ est composé des valeurs $\gamma_1, \dots, \gamma_k$, avec multiplicités $n \cdot n_1, \dots, n \cdot n_k$.

On peut donc factoriser $\widetilde{\mathrm{Q}}$ dans $\mathbb{L}[\mathrm{X}]$, en $\widetilde{\mathrm{Q}} = \mathrm{R}_1 \cdots \mathrm{R}_k$, avec $\deg \mathrm{R}_i = n \cdot n_i$ et $\mathcal{PN}(\mathrm{R}_i) = [\gamma_i, \dots, \gamma_i]$.

On pose $\mathrm{R}_{i,\alpha}(\mathrm{X}) = r_i(\alpha, \mathrm{X}) = \mathrm{pgcd}_{\mathbb{L}[\alpha][\mathrm{X}]}\big(\mathrm{R}_i(\mathrm{X}), q(\alpha, \mathrm{X})\big)$. Ce calcul nécessite d'inverser des éléments de $\mathbb{L}[\alpha]$ et peut donc éventuellement conduire à une factorisation de P, et à son remplacement par un de ses facteurs.

On a alors $\deg \mathrm{R}_{i,\alpha} = n_i$ et $\mathrm{Q}_\alpha = \mathrm{R}_{1,\alpha} \cdots \mathrm{R}_{k,\alpha}$ avec $\mathcal{PN}(\mathrm{R}_{i,\alpha}) = [\gamma_i, \dots, \gamma_i]$.
$\square$

Remarque Ceci nous autorise, en pratique, étant donné un corps valué $\mathbb{K}$, à prendre comme corps hensélien $\mathbb{L}$ dans les théorèmes que nous donnons ici, $\mathbb{K}^h$ ou une extension algébrique de $\mathbb{K}^h$.

Le lemme de Krasner

Le lemme de Krasner apparaît comme une conséquence naturelle de ce dernier théorème.

Théorème 18 (lemme de Krasner) *Soit* $\mathbb{L}$ *un corps hensélien. Soient* $\mathrm{P}, \mathrm{Q} \in \mathbb{L}[\mathrm{X}]$ *deux polynômes présumés irréductibles,* α *une racine de* P *et* β *une racine de* Q *(dans la clôture algébrique de* $\mathbb{L}$*). On suppose que* $v(\beta - \alpha) > v(\alpha - \alpha')$*, pour tout* $\alpha' \neq \alpha$ *tel que* $\mathrm{P}(\alpha') = 0$.

Alors α *est purement inséparable au-dessus de* $\mathbb{L}[\beta]$*. En particulier si* P *est séparable, alors* $\alpha \in \mathbb{L}[\beta]$.

Démonstration Soient $\alpha_1, \ldots, \alpha_n$ les racines de P. Si α est une racine de multiplicité k, on suppose que $\alpha = \alpha_1 = \cdots = \alpha_k$.

On se place dans $\mathbb{L}[\beta]$, où on pose $\mathrm{P}_1(\mathrm{X}) = \mathrm{P}(\mathrm{X} + \beta)$. Ses racines sont les $\beta - \alpha_i$, pour $i = 1, \ldots, n$. Les hypothèses montrent que le polygone de Newton de P_1 présente un segment de largeur k, de pente $v(\beta - \alpha)$, qui correspond aux racines $\beta - \alpha_1, \ldots, \beta - \alpha_k$.

On peut utiliser le théorème 17 pour factoriser $\mathrm{P}_1(\mathrm{X})$ et donc $\mathrm{P}(\mathrm{X})$ dans $\mathbb{L}[\beta][\mathrm{X}]$: soit $\mathrm{R}(\mathrm{X})$ le facteur de $\mathrm{P}(\mathrm{X})$ obtenu en considérant ce segment de largeur k. Les racines de R sont clairement $\alpha_1, \ldots, \alpha_k$, et donc $\mathrm{R}(\mathrm{X}) = (\mathrm{X} - \alpha)^k \in \mathbb{L}[\beta][\mathrm{X}]$.

Si P est séparable, on a $k = 1$ et donc $\alpha \in \mathbb{L}[\beta]$. □

3 Le corps d'inertie

Le *corps d'inertie* ou *hensélisé strict* $\mathbb{K}^{sh}$ de $\mathbb{K}$ est sa plus grande extension non ramifiée. Pour nous, c'est simplement le corps obtenu en ajoutant à $\mathbb{K}^h$ le relèvement de racines simples dans $\Bbbk^{ac}$ (c.-à-d. d'éléments de $\Bbbk^{sep}$), et non plus simplement dans $\Bbbk$. Plus précisément, $\mathbb{K}^{sh}$ doit vérifier la propriété suivante : soit $\mathrm{P}(\mathrm{X}) \in \mathbb{K}^{sh}[\mathrm{X}]$ tel que $\overline{\mathrm{P}}(\mathrm{X})$ admet une racine simple $z \in \Bbbk^{sep}$. Alors il existe $\zeta \in \mathbb{K}^{sh}$ une racine de P telle que $\overline{\zeta} = z$.

En particulier le corps résiduel de $\mathbb{K}^{sh}$ est $\Bbbk^{sep}$. Par contre nous allons montrer que le groupe de valuation reste Γ.

Soit $p(\mathrm{X}) \in \Bbbk[\mathrm{X}]$ un polynôme qui admet une racine simple $z \in \Bbbk^{ac}$ (donc, en fait, $z \in \Bbbk^{sep}$). On peut se ramener facilement au cas où p et sa dérivée p' sont premiers entre eux.

Soit $\mathrm{P} \in \mathbb{K}^h[\mathrm{X}]$ tel que $\overline{\mathrm{P}}(\mathrm{X}) = p(\mathrm{X})$. On peut voir (P, z) comme un moyen de coder une racine ζ de P. Nous allons voir comment calculer dans $\mathbb{K}^h[\zeta]$; de même que pour $\mathbb{K}^h$, l'itération de cette construction permet le calcul dans $\mathbb{K}^{sh}$. Le choix du polynôme P qui « remonte » p est sans importance, comme le montre la proposition suivante :

Lemme 19 *Soit* $p(\mathrm{X}) \in \Bbbk[\mathrm{X}]$ *un polynôme qui admet une racine simple* $z \in \Bbbk^{ac}$, *et soient* $\mathrm{P(X)}, \mathrm{Q(X)} \in \mathbb{K}^h(\mathrm{X})$ *tels que* $\overline{\mathrm{P}}(\mathrm{X}) = \overline{\mathrm{Q}}(\mathrm{X}) = p(\mathrm{X})$*. Soient* $\zeta, \xi \in \mathbb{K}^{ac}$ *les racines de* P *et* Q *dont les résidus sont* $\overline{\zeta} = \overline{\xi} = z$*.*

Alors on a $\mathbb{K}^h[\zeta] = \mathbb{K}^h[\xi]$*.*

Démonstration Il suffit d'appliquer le lemme de Krasner.

Si $\zeta' \neq \zeta$ est une racine de P, alors $v(\zeta - \zeta') \leq 0$. D'autre part $v(\zeta - \xi) > 0$. Alors on a bien $v(\zeta - \xi) > v(\zeta - \zeta')$, et donc $\zeta \in \mathbb{K}[\xi]$.

La situation étant symétrique on a aussi $\xi \in \mathbb{K}[\zeta]$, et donc $\mathbb{K}[\zeta] = \mathbb{K}[\xi]$. □

Tous les calculs peuvent se faire à l'aide des théorèmes 16 et 17 ; cependant, nous allons donner une variante du théorème 16, mieux adaptée à ce cas particulier. Bien sûr, si P(X) n'est pas irréductible, au cours des calculs, on peut être amené à en « découvrir » une factorisation ; auquel cas, dans la définition de ζ par (P, z), on peut remplacer P par celui de ses facteurs dont le résidu admet z comme racine.

Notons qu'on peut supposer que toutes les racines de P dans $\mathbb{K}^{ac}$ sont de valuation nulle.

Théorème 20 *Soit* $\mathbb{L}$ *un corps hensélien ; dans le cadre qui nous intéresse ici,* $\mathbb{L}$ *est* $\mathbb{K}^h$ *ou une extension algébrique de* $\mathbb{K}^h$ *telle que* $\mathbb{K}^h \subseteq \mathbb{L} \subseteq \mathbb{K}^{sh}$*. Soit* $(\mathrm{P}, z) \in \mathbb{L}[\mathrm{X}] \times \Bbbk^{sep}$ *un code pour* ζ *tel que défini ci-dessus ; on pose* $n = \deg \mathrm{P}$*. Soit* $\mathrm{Q(X)} \in \mathbb{L}[\mathrm{X}]$ *un polynôme de degré strictement inférieur à* n*. Alors on sait calculer un élément de* $\mathbb{L}$ *qui a même valuation que* $\mathrm{Q}(\zeta)$*.*

Démonstration On commence par factoriser Q(X) à l'aide du théorème 13 : $\mathrm{Q} = \mathrm{Q}_1 \cdots \mathrm{Q}_k$, où chaque $\mathcal{PN}(\mathrm{Q}_i)$ est formé d'une répétition de la même valeur. On a $v\big(\mathrm{Q}(\alpha)\big) = v\big(\mathrm{Q}_1(\alpha)\big) + \cdots + v\big(\mathrm{Q}_k(\alpha)\big)$.

Il suffit donc de traiter le cas où $\mathcal{PN}(\mathrm{Q}) = [\gamma, \ldots, \gamma]$.

On pose $\mathrm{Q(X)} = a_0\mathrm{X}^m + \cdots + a_m$. Si $\gamma > 0$, on a $v\big(\mathrm{Q}(\alpha)\big) = v(a_0)$; si $\gamma < 0$, $v\big(\mathrm{Q}(\alpha)\big) = v(a_m)$.

Si $\gamma = 0$, en supposant Q(X) unitaire, on peut considérer le polynôme $\overline{\mathrm{Q}}(\mathrm{X}) \in \mathbb{l}[\mathrm{X}]$ ($\mathbb{l}$ étant le corps résiduel de $\mathbb{L}$) : son degré est $m < n$. Alors si $\overline{\mathrm{Q}}(z) \neq 0$, $v(\mathrm{Q}(z)) = 0$; et si $\overline{\mathrm{Q}}(z) = 0$, on en déduit une factorisation de $\overline{\mathrm{P}}$ dans $\mathbb{l}[\mathrm{X}]$, en deux facteurs premiers entre eux (car z est racine simple de $\overline{\mathrm{P}}$), qui se remonte donc en une factorisation de P. On peut remplacer P par celui de ses facteurs dont le résidu admet z comme racine. □

Le hensélisé strict de $\mathbb{K}$ se construit par application répétée de ce lemme, avec pour point de départ $\mathbb{K}^h$.

Corollaire 21 *Le groupe de valuation de* $\mathbb{K}^{sh}$ *est* Γ*, le groupe de valuation de* $\mathbb{K}$*.*

4 Le corps de ramification

C'est la plus grande extension totalement ramifiée de $\mathbb{K}^{sh}$. Il s'agit pour nous d'ajouter à $\mathbb{K}^{sh}$ les racines $n^{\rm e}$ d'éléments de $\mathbb{K}^{sh}$, avec, si le corps résiduel est de caractéristique $p > 0$, n premier à p.

Remarques – Notons que si $v(a) = 0$, le polynôme $\mathrm{X}^n - a$ (pour n vérifiant l'hypothèse ci-dessus) étant scindé *en racines distinctes* dans $\Bbbk^{sep}$, il l'est également dans $\mathbb{K}^{sh}$. Toutes les racines $n^{\rm e}$ de a sont donc dans $\mathbb{K}^{sh}$. En particulier, c'est le cas pour les racines $n^{\rm e}$ de l'unité.

– Si $v(a) = n \cdot \gamma$, avec $\gamma \in \Gamma$, soit b de valuation γ ; on a $v\left(\dfrac{a}{b^n}\right) = 0$, et toutes les racines $n^{\rm e}$ de $\dfrac{a}{b^n}$, et donc celles de a, sont dans $\mathbb{K}^{sh}$. Il s'agit donc de se soucier des racines $n^{\rm e}$ d'éléments de $\mathbb{K}^{sh}$ dont la valuation n'est pas un multiple de n.

Supposons que nous disposions d'un test de divisibilité dans Γ : étant donné $\gamma \in \Gamma$ et $n \in \mathbb{N}^\star$, on sait répondre à la question

$$\exists ? \lambda \in \Gamma,\ \ n \cdot \lambda = \gamma.$$

Si la réponse est affirmative, on dit que n divise γ dans Γ. On suppose que dans ce cas, on sait trouver λ tel que $n \cdot \lambda = \gamma$; concrètement, on obtient un élément de $\mathbb{K}$ de valuation λ.

Définition Soit $\delta \in \overline{\Gamma}$, la clôture divisible de Γ. Soient $\gamma \in \Gamma$ et $n \in \mathbb{N}$ tels que $n \cdot \delta = \gamma$; si tout diviseur m de n (dans $\mathbb{N}$) ne divise pas γ (dans Γ) on dit que (γ, n) est un *représentant irréductible* de δ, ou encore que $\frac{\gamma}{n}$ est *irréductible.*

Lemme 22 (Lemme de Gauss) *Soient $\gamma \in \Gamma$ et $n, m \in \mathbb{N}$. Si n divise $m \cdot \gamma$ dans Γ et n, m sont premiers entre eux, alors n divise γ.*

Démonstration Soient $u, v \in \mathbb{Z}$ tels que $u \cdot n + v \cdot m = 1$, et soit λ tel que $n \cdot \lambda = m \cdot \gamma$. Alors $n \cdot (v \cdot \lambda + u \cdot \gamma) = \gamma$, donc n divise γ. □

Comme en arithmétique classique, le lemme de Gauss permet de montrer que si $\dfrac{\gamma}{n}$ est irréductible, dès que $\dfrac{\gamma'}{n'} = \dfrac{\gamma}{n}$ on a $n' = k \cdot n$ et $\gamma' = k \cdot \gamma$ avec $k \in \mathbb{Z}$.

Lemme 23 *Si on dispose d'un test de divisiblité dans Γ, et si $\dfrac{\gamma}{n}$ est irréductible, alors on dispose d'un test de divisibilité dans*

$$\Gamma + \frac{\gamma}{n} \cdot \mathbb{Z} = \left\{ \lambda + i \cdot \frac{\gamma}{n}\ :\ \lambda \in \Gamma,\ 0 \leq i < n \right\}.$$

Démonstration Soit $k \in \mathbb{N}^\star$ et $\lambda + i \cdot \frac{\gamma}{n} \in \Gamma + \frac{\gamma}{n} \cdot \mathbb{Z}$. Existe-t-il $\varepsilon + j \cdot \frac{\gamma}{n} \in \Gamma + \frac{\gamma}{n} \cdot \mathbb{Z}$ tel que

$$k \cdot \varepsilon + kj \cdot \frac{\gamma}{n} = \lambda + i \cdot \frac{\gamma}{n}\,?$$

Il faut tout d'abord choisir, si c'est possible, j tel que $0 \le j < n$ et $kj \equiv i\ [n]$. Il y a un nombre fini de tels j ; pour chacun d'entre eux, on écrit $kj = i + \ell \cdot n$, et on est ramené à poser la question : existe-t-il $\varepsilon \in \Gamma$ tel que

$$k \cdot \varepsilon + \ell \cdot \gamma + i \cdot \frac{\gamma}{n} = \lambda + i \cdot \frac{\gamma}{n}\ ?$$

c.-à-d. k divise-t-il $\lambda - \ell \cdot \gamma$? Il suffit donc effectuer ce test de divisibilité (pour toutes les valeurs de j envisageables). □

Lemme 24 *Soit* $(\mathbb{L}, v)$ *un corps hensélien de groupe de valuation* $\Gamma_{\mathbb{L}}$ *; soient* $a \in \mathbb{L}$ *de valuation* $v(a) = \gamma$ *et* $n \in \mathbb{N}$ *tel que* $\frac{\gamma}{n}$ *soit irréductible dans* $\Gamma_{\mathbb{L}}$*. Alors le polynôme* $\mathrm{P(X)} = \mathrm{X}^n - a$ *est irréductible dans* $\mathbb{L}[\mathrm{X}]$*. Si* α *est une racine de* P*, le groupe de valuation de* $\mathbb{L}_1 = \mathbb{L}[\alpha]$ *est* $\Gamma_{\mathbb{L}_1} = \Gamma_{\mathbb{L}} + \frac{\gamma}{n} \cdot \mathbb{Z}$*. Le corps résiduel de* $\mathbb{L}_1$ *est* $\mathbb{l}$*, le corps résiduel de* $\mathbb{L}$*.*

Démonstration Si $\mathrm{P} = \mathrm{P}_1 \cdot \mathrm{P}_2$, les polygones de Newton de P_1 et P_2 fournissent des représentations γ'/n' de γ/n avec $n' < n$, ce qui contredit l'irréductibilité de γ/n.

Un élément de $\mathbb{K}[\alpha]$ est de la forme $\sum_{i=0}^{n-1} a_i \cdot \alpha^i$; si $v(a_i \cdot \alpha^i) = v(a_j \cdot \alpha^j)$ avec $i \neq j$, on a

$$\frac{v(a_i) - v(a_j)}{j - i} = \frac{\gamma}{n},$$

ce qui contredit à nouveau l'irréductibilité de $\frac{\gamma}{n}$; donc

$$v\left(\sum_{i=0}^{n-1} a_i \cdot \alpha^i\right) = \min_i v(a_i \cdot \alpha^i) = v(a_k) + k \cdot \frac{\gamma}{n} \in \Gamma + \frac{\gamma}{n} \cdot \mathbb{Z}$$

le min étant atteint une seule fois ; et donc $\Gamma_{\mathbb{L}_1} = \Gamma_{\mathbb{L}} + \frac{\gamma}{n} \cdot \mathbb{Z}$.

De plus si $v\left(\sum_{i=0}^{n-1} a_i \cdot \alpha^i\right) = 0$, on sait que le min des valuations est atteint en $i = 0$, et donc le résidu de $\sum_{i=0}^{n-1} a_i \cdot \alpha^i$ est $\overline{a_0}$, et le corps résiduel est bien $\mathbb{l}$. □

Lemme 25 *Soit* $\mathbb{L}$ *un corps hensélien dont le corps résiduel* $\mathbb{l}$ *est séparablement clos. On suppose en outre qu'on dispose dans* $\Gamma_{\mathbb{L}}$ *d'un test de divisibilité. Soit* $a \in \mathbb{L}$ *; soit* $n \in \mathbb{N}^\star$*, tel que si la caractéristique* $\mathbb{l}$ *est* $p > 0$*,* p *ne divise pas* n*. Alors on sait construire une extension de* $\mathbb{L}$ *dans laquelle sont présentes toutes les racines* n^{e} *de* a *; son corps résiduel est* $\mathbb{l}$ *et son groupe de valuation est une extension de* $\Gamma_{\mathbb{L}}$ *où on dispose à nouveau d'un test de divisibilité.*

Démonstration À l'aide du test de divisibilité, on produit $b \in \mathbb{L}$ et $m \in \mathbb{N}$ tel que

$$\frac{v(a)}{n} = \frac{v(b)}{m}$$

et $v(b)/m$ est irréductible. On pose $\mathrm{P(X)} = \mathrm{X}^m - b$ et on construit l'extension associée $\mathbb{L}_1 = \mathbb{L}[\beta]$ à l'aide du lemme ci-dessus. Son corps résiduel est $\mathbb{l}$ et son groupe de valuation est $\Gamma_{\mathbb{L}_1} = \Gamma_{\mathbb{L}} + \frac{v(b)}{m} \cdot \mathbb{Z}$, où le test de divisibilité est donné par le lemme 23.

Dans $\Gamma_{\mathbb{L}_1}$, $v(a)$ est divisible par n, car $v(a) = n \cdot v(\beta)$; alors, comme on l'a fait remarquer en début de section, les racines n^{e} de a sont dans $\mathbb{L}_1$. $\square$

Par application répétée de ce lemme, en partant de $\mathbb{K}^{sh}$, on construit le corps de ramification de $\mathbb{K}$.

CHAPITRE IV

UNE GÉNÉRALISATION DU LEMME DE HENSEL

Introduction

Ce chapitre contient un article en anglais — je commence donc par m'en excuser auprès des lecteurs et lectrices francophones. Il s'agit de démontrer une variante du lemme de Hensel, vraie dans tous les corps henséliens, qui n'avait été démontrée par Sudesh Kaur Khanduja et Jayanti Saha ([KS]) que dans le cas des corps complets de valuation discrète.

Il s'agit d'un critère de factorisation ; les conditions sont exprimées au moyen d'une extension de la valuation v de $\mathbb{K}$ (hensélien) au corps $\mathbb{K}(\mathrm{X})$. Quand il s'agit de la valuation de Gauss

$$v^{\mathrm{G}}\left(\sum c_i \cdot \mathrm{X}^i\right) = \min\{v(c_i)\}$$

il s'agit d'un énoncé classique du lemme de Hensel, équivalent à III.15.

Par contre, cet énoncé est également valable pour des valuations w de $\mathbb{K}(\mathrm{X})$, définies sur $\mathbb{K}[\mathrm{X}]$ par

$$w\left(\sum c_i \cdot (\mathrm{X}-a)^i\right) = \min\{v(c_i) + i \cdot \delta\}$$

où δ est un élément d'un groupe ordonné Λ qui contient $\overline{\Gamma}$; si δ est dans $\overline{\Gamma}$, la valuation w est *résiduellement transcendante* (ou *transcendante relativement aux corps résiduels* , sinon elle est *transcendante relativement aux groupes de valuation.* Dans ces deux cas, l'énoncé reste valable ; la preuve donnée est non constructive.

Nons donnons une interprétation géométrique de ce lemme qui est à notre avis de nature à rendre plus intéressante son énoncé brut. Nous donnons également un analogue de ce résultat pour des systèmes d'équations polynomiales à plusieurs variables.

En retournant à la langue française, nous donnons une preuve constructive du lemme ; puis vient une section consacrée à une utilisation des valuations résiduellement transcendantes, en connexion avec l'interprétation géométrique de la section 3 (mais pas avec le théorème).

1 Definitions, notations & statements

Let $\mathbb{K}$ be a Henselian field, and $\mathbb{K}^{ac}$ be its algebraic closure. The value group of $\mathbb{K}$ is denoted by Γ, and the one of $\mathbb{K}^{ac}$ by $\overline{\Gamma}$, the divisible closure of Γ. The valuation on $\mathbb{K}^{ac}$ is always denoted by v; the valuation ring of $\mathbb{K}$ is denoted by $\mathfrak{V}$, the one of $\mathbb{K}^{ac}$ by $\mathfrak{V}^{ac}$. The residue fields of $\mathbb{K}$ and $\mathbb{K}^{ac}$ are denoted by $\Bbbk$ and $\Bbbk^{ac}$. The galois group of $\mathbb{K}$ is denoted by $\mathcal{G}\mathrm{al}(\mathbb{K})$. For all $\alpha \in \mathbb{K}^{ac}$ and all $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$, we have $v(\sigma\alpha) = v(\alpha)$. For general definitions and statements, cf [E].

Let Λ be an ordered abelian group which contains $\overline{\Gamma}$. Take $(a,\delta) \in \mathbb{K}^{ac} \times \Lambda$. We use it to define an extension of v to a simple transcendental extension $\mathbb{K}^{ac}(\mathrm{X})$ of $\mathbb{K}^{ac}$:

$$w_{a,\delta}\left(\sum_i c_i(\mathrm{X}-a)^i\right) = \min_i \{vc_i + i\delta\}.$$

If $\delta \in \overline{\Gamma}$, the valuation $w_{a,\delta}$ defines a *residually transcendental extension* of v (cf. [PP] or [Bour], §10). The residue fields of $\mathbb{K}(\mathrm{X})$ and $\mathbb{K}^{ac}(\mathrm{X})$ for such a valuation are $\Bbbk'(t)$ and $\Bbbk^{ac}(t)$, where $\Bbbk'$ is a finite extension of $\Bbbk$ and t is transcendental over $\Bbbk$; this property is the definition of a residually transcendental extension. For every residually transcendental extension w on $\mathbb{K}(\mathrm{X})$, there exists (a,δ) such that w is defined by the above formula (cf. [APZ]). This pair (a,δ) is not unique; we shall later see exactly when $w_{a,\delta} = w_{a',\delta'}$.

The pair $(0,0)$ defines the so-called *Gaussian extension* v^{G} of v; we have $v^{\mathrm{G}}(\sum_i c_i\mathrm{X}^i) = \min_i vc_i$.

A *value transcendental valuation* w is defined by a pair (a,δ) where $a \in \mathbb{K}^{ac}$ and δ is defined by a cut in $\overline{\Gamma}$: we have two subsets of $\overline{\Gamma}$, $\overline{\Gamma}^{<\delta}$ and $\overline{\Gamma}^{>\delta}$ such that $\overline{\Gamma} = \overline{\Gamma}^{<\delta} \cup \overline{\Gamma}^{>\delta}$ and for all $a \in \overline{\Gamma}^{<\delta}$ and $b \in \overline{\Gamma}^{>\delta}$, we have $a < b$. We consider more over that in that case we have $a < \delta < b$, and this is sufficient to give an order on $\overline{\Gamma} + \mathbb{Z}\cdot\delta$. The residue field of $\mathbb{K}(\mathrm{X})$ for this valuation is $\Bbbk'$, a finite extension of $\Bbbk$, and the value group is contained in $\overline{\Gamma} + \mathbb{Z}\cdot\delta$.

One of the classical versions of Hensel's Lemma is as follows (cf. [Rib]). We denote by $\mathrm{lc}(f)$ the leading coefficient of the polynomial f.

Theorem 1.1 (Classical Hensel's Lemma) *Let f, g_0, h_0 be polynomials in $\mathbb{K}[\mathrm{X}]$ such that the conditions $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ are satisfied:*

- H_1 $v^{\mathrm{G}}(f - g_0 \cdot h_0) > v^{\mathrm{G}}(f)$
- H_2 $v(\mathrm{lc}(g_0)) = v^{\mathrm{G}}(g_0)$
- H_3 $\exists a, b \in \mathbb{K}[\mathrm{X}]$ *such that* $v^{\mathrm{G}}(a \cdot g_0) \geq 0$, $v^{\mathrm{G}}(b \cdot h_0) \geq 0$ *and* $v^{\mathrm{G}}(a \cdot g_0 + b \cdot h_0 - 1) > 0$.

Then there exist $g, h \in \mathbb{K}[\mathrm{X}]$ *such that the following conditions* $\mathrm{H}_a, \mathrm{H}_b, \mathrm{H}_c$ *are satisfied; moreover, these polynomials are unique.*

- H_a $f = g \cdot h$
- H_b $\deg g = \deg g_0$ *and* $\mathrm{lc}(g) = \mathrm{lc}(g_0)$
- H_c $v^{\mathrm{G}}(g - g_0) > v^{\mathrm{G}}(g_0)$.

As soon as the conditions $\mathrm{H}_a, \mathrm{H}_b, \mathrm{H}_c$ *are satisfied, we have* $v^{\mathrm{G}}(h - h_0) > v^{\mathrm{G}}(h_0)$.

Remark 1 *We denote by* $a \mapsto \overline{a}$ *the canonical map from* $\mathfrak{V}$ *to* $\mathbb{k}$. *If* $v^{\mathrm{G}}(f) = v^{\mathrm{G}}(g_0) = v^{\mathrm{G}}(h_0) = 0$, *the hypotheses can be reformulated as follows:*

- H_1 $\overline{f} = \overline{g_0} \cdot \overline{h_0}$
- H_2 $\deg \overline{g_0} = \deg g_0$
- H_3 $\overline{g_0}$ *and* $\overline{h_0}$ *are relatively prime.*

And the conclusion becomes:

- H_a $f = g \cdot h$
- H_b $\deg g = \deg g_0$ *and* $\mathrm{lc}(g) = \mathrm{lc}(g_0)$
- H_c $\overline{g} = \overline{g_0}$.

If the conditions of the conclusion are verified, we have clearly $\overline{h} = \overline{h_0}$.

The following theorem, in the case of a residually transcendental extension $w_{a,\delta}$ of v (with the additional assumption that the valuation v has rank 1), is exactly the generalization given by Sudesh K. Khanduja and Jayanti Saha in [KS].

Theorem 1.2 (Generalized Hensel's Lemma) *Let* $w_{a,\delta}$ *be either a residually transcendental valuation or a value transcendental extension of* v. *Let* f, g_0, h_0 *be polynomials in* $\mathbb{K}[\mathrm{X}]$ *such that the conditions* $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$ *are satisfied:*

- GH_1 $w_{a,\delta}(f - g_0 \cdot h_0) > w_{a,\delta}(f)$
- GH_2 $v(\mathrm{lc}(g_0)) + \deg(g_0) \cdot \delta = w_{a,\delta}(g_0)$
- GH_3 $\exists a, b \in \mathbb{K}[\mathrm{X}]$ *such that* $w_{a,\delta}(a \cdot g_0) \geq 0$, $w_{a,\delta}(b \cdot h_0) \geq 0$ *and* $w_{a,\delta}(a \cdot g_0 + b \cdot h_0 - 1) > 0$,

Then there exists $g, h \in \mathbb{K}[\mathrm{X}]$ *such that the following conditions* $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$ *are satisfied; moreover, these polynomials are unique.*

- GH_a $f = g \cdot h$
- GH_b $\deg g = \deg g_0$ *and* $\mathrm{lc}(g) = \mathrm{lc}(g_0)$
- GH_c $w_{a,\delta}(g - g_0) > w_{a,\delta}(g_0)$.

As soon as the conditions $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$ *are satisfied, we have* $w_{a,\delta}(h - h_0) > w_{a,\delta}(h_0)$.

This generalization is very natural; the only point where there might be a problem is the second hypothesis, denoted by H_2 in the Classical Lemma, and by GH_2 in the Generalized Lemma. Where does this $-\deg(g_0)\cdot\delta$ come from? We shall see that this is in fact as natural as the other modifications.

We are going to prove that every Henselian field satisfies this Generalized Hensel's Lemma.

2 The residually transcendental case

A residually transcendental valuation $w_0 = w_{a,\delta}$, defined by $(a,\delta) \in \mathbb{K}^{ac} \times \overline{\Gamma}$ is fixed throughout this section.

Let $\mathbb{L}$ be an algebraic extension of $\mathbb{K}[a,d]$ where $d \in \mathbb{K}^{sep}$ is such that $v(d) = \delta$ (if $\delta = v(a)/n$ with a in $\mathbb{K}$, take e.g. d to be one of the roots of $\mathrm{X}^n + a\cdot\mathrm{X} + a$). Being an algebraic extension of a Henselian field, $\mathbb{L}$ is Henselian.

We denote by $f \mapsto \hat{f}$ and $f \mapsto \check{f}$ the following automorphisms of $\mathbb{L}[\mathrm{X}]$:

$$f(\mathrm{X}) \mapsto \hat{f}(\mathrm{X}) = f(d\cdot\mathrm{X} + a) \qquad f(\mathrm{X}) \mapsto \check{f}(\mathrm{X}) = f(\frac{1}{d}(\mathrm{X}-a)).$$

These automorphisms are obviously inverse of each other.

- Fact 1: For every $f(\mathrm{X}) \in \mathbb{L}[\mathrm{X}]$ we have $w_{a,\delta}\left(f(\mathrm{X})\right) = v^{\mathrm{G}}\left(\hat{f}(\mathrm{X})\right)$.
- Fact 2: Let $f, g_0, h_0, g, h \in \mathbb{L}[\mathrm{X}]$. We have the following equivalences:

$$f, g_0, h_0 \text{ satisfy } \mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3 \iff \hat{f}, \hat{g_0}, \hat{h_0} \text{ satisfy } \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3.$$

$$f, g, h \text{ satisfy } \mathrm{H}_a, \mathrm{H}_b, \mathrm{H}_c \iff \check{f}, \check{g}, \check{h} \text{ satisfy } \mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c.$$

Of course, we have other such equivalences using the fact the two transformations "hat" ($f \mapsto \hat{f}$) and "check" ($f \mapsto \check{f}$) are inverse of each other. The proofs are straightforward and left to the reader. Note that fact 1 allows to prove in a short way that w_0 is a valuation on $\mathbb{K}^{ac}[\mathrm{X}]$; from fact 2, one understands better why one must have $v(\mathrm{lc}(g_0)) = -\deg(g_0)\cdot\delta + w_{a,\delta}(g_0)$ in the hypotheses GH_2 of the generalized lemma.

Before starting the proof, there is still a bit of preparation: we said that two different pairs (a,δ) and (a',δ') in $\mathbb{K}^{ac} \times \overline{\Gamma}$ may define the same valuation $w_{a,\delta} = w_{a',\delta'}$. How can we characterize such pairs? The answer of this question can be found in [AP]; this is the first point of the next lemma.

Lemma 2 *We write* $\mathrm{B}_{a,\delta} = \{\alpha \in \mathbb{K}^{ac} : v(a-\alpha) \geq \delta\}$.

- *Let* (a,δ) *and* (a',δ') *be in* $\mathbb{K}^{ac} \times \overline{\Gamma}$. *We have* $w_{a,\delta} = w_{a',\delta'}$ *iff* $\mathrm{B}_{a,\delta} = \mathrm{B}_{a',\delta'}$.
- *If* $g_0 \in \mathbb{K}[\mathrm{X}]$ *is a polynomial such that the hypothesis* GH_2 *holds, then all roots of* g_0 *are in* $\mathrm{B}_{a,\delta}$.
- *In this case, we can choose* $b \in \mathbb{K}^{sep}$ *such that we have* $w_{a,\delta} = w_{b,\delta} = w_{\sigma b,\delta}$, *for all* $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$.

Proof Note that given (a, δ), we have $\mathrm{B}_{a,\delta} = \mathrm{B}_{a',\delta'}$ iff $\delta' = \delta$ and $a' \in \mathrm{B}_{a,\delta}$.

Now note that $w_{a,\delta}$ and $w_{a',\delta'}$ coincide on the field $\mathbb{K} \subseteq \mathbb{K}[\mathrm{X}]$; thus as soon as they have the same valuation ring, they are equal. Using fact 1 we write the following equivalences, where d, d' are elements of $\mathbb{K}^{sep}$ such that $v(d) = \delta$ and $v(d') = \delta'$.

$$\forall f \in \mathbb{L}[\mathrm{X}] \quad w_{a,\delta}(f) = w_{a',\delta'}(f) \quad \Leftrightarrow$$

$$\left[\forall f \in \mathbb{L}[\mathrm{X}] \quad f(d\mathrm{X}+a) \in \mathfrak{V}[\mathrm{X}] \Longleftrightarrow f(d'\mathrm{X}+a') \in \mathfrak{V}[\mathrm{X}]\right] \quad \Leftrightarrow$$

$$\left[\forall f \in \mathbb{L}[\mathrm{X}] \quad f(d\mathrm{X}+a) \in \mathfrak{V}[\mathrm{X}] \Longleftrightarrow f\left(d \cdot (\frac{d'}{d}\mathrm{X} + \frac{a'-a}{d}) + a\right) \in \mathfrak{V}[\mathrm{X}]\right] \quad \Leftrightarrow$$

$$\left[\forall g \in \mathbb{L}[\mathrm{X}] \quad g(\mathrm{X}) \in \mathfrak{V}[\mathrm{X}] \Longleftrightarrow g\left(\frac{d'}{d}\mathrm{X} + \frac{a'-a}{d}\right) \in \mathfrak{V}[\mathrm{X}]\right] \quad \Leftrightarrow$$

$$v\left(\frac{d'}{d}\right) = 0 \text{ and } v\left(\frac{a'-a}{d}\right) \geq 0$$

The second assertion of the lemma is very simple to prove. Note that $\hat{g_0} \in \mathbb{K}^{ac}[\mathrm{X}]$ has leading coefficient with valuation $v^{\mathrm{G}}(\hat{g_0})$; hence its roots are in $\mathfrak{V}^{ac}$. Now if ζ is a root of g_0, $\dfrac{\zeta - a}{d}$ is a root of $\hat{g_0}$. From $v\left(\dfrac{\zeta-a}{d}\right) \geq 0$ follows $\zeta \in \mathrm{B}_{a,\delta}$.

Before proving the third assertion, note that if we replace $g_0(\mathrm{X})$ by $g_0(\mathrm{X}) + c \cdot x$, with $v(c)$ large enough, the hypotheses of the lemma are still satisfied; hence one can suppose that g_0 is separable, and so the roots of g_0 are in $\mathbb{K}^{sep}$.

Now for a root ζ of g_0 as above, we have $\mathrm{B}_{a,\delta} = \mathrm{B}_{\zeta,\delta}$; we have $\sigma\zeta \in \mathrm{B}_{\zeta,\delta}$ for all $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$. Thus we can take b equal to a root of g_0, and by first asserstion we have $w_{a,\delta} = w_{b,\delta} = w_{\sigma b,\delta}$, for all $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$. □

We are now going to prove the generalized lemma. We assume that f, g_0, h_0 are polynomials satisfying the hypotheses $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$. In this situation, the previous lemma allows us to assume that $w_{\sigma a,\delta} = w_{a,\delta}$, for all $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$.

We first prove a uniqueness statement, which will be useful in the proof of existence.

Lemma 3 (Uniqueness statement) *In a Henselian field $\mathbb{L}$ such that $a, d \in$ L, let f, g_0, h_0 be polynomials satisfying the hypotheses $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$ of the generalized Hensel's lemma. If there are polynomials g, h satisfying its conclusion $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$ then they are unique.*

Proof We use the unicity of Classical Hensel's lemma: $\hat{f}, \hat{g_0}, \hat{h_0}$ satisfy the hypotheses $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ of the classical lemma, and $\hat{g}, \hat{h}$ satisfy its conclusion H_a, $\mathrm{H}_b, \mathrm{H}_c$. But there are no other polynomials than $\hat{g}, \hat{h}$ satisfying this conclusion, hence there are no other polynomials than g, h satisfying $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$. □

Proof [Existence proof] Of course the idea is to put $\mathbb{L} = \mathbb{K}[a, d] \subseteq \mathbb{K}^{sep}$, and to say that if f, g_0, h_0 satisfy $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$, then $\hat{f}, \hat{g_0}, \hat{h_0}$ satisfy $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$, to use the Classical Hensel's lemma in $\mathbb{L}$ to find (unique) polynomials g_1, h_1 satisfying $\mathrm{H}_a, \mathrm{H}_b, \mathrm{H}_c$, and then just do the reverse transformation to obtain $g = \check{g_1}$, and $h = \check{h_1}$ satisfying $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$. But now these polynomials are in $\mathbb{L}[\mathrm{X}]$!

It suffices to show that g, h are fixed by every element σ of $\mathcal{G}\mathrm{al}(\mathbb{K})$, so that they are in $\mathbb{K}[\mathrm{X}]$. Using the uniqueness statement (in $\mathbb{L}$), it suffices to show that for all $\sigma \in \mathrm{Aut}(\mathbb{L}|\mathbb{K})$, σg and σh satisfy the conclusion $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$.

This is clear for GH_a and GH_b. Now let $g_0 = \sum_i r_i(a)(\mathrm{X}-a)^i$ and $g = \sum_i \rho_i(a,d)(\mathrm{X}-a)^i$, with $r_i \in \mathbb{K}[\mathrm{X}]$ and $\rho_i \in \mathbb{K}[\mathrm{X},\mathrm{Y}]$. We have

$$g_0(\mathrm{X}) - g(\mathrm{X}) = \sum_i (r_i(a) - \rho_i(a,d))(\mathrm{X}-a)^i$$

and

$$g_0(\mathrm{X}) - \sigma g(\mathrm{X}) = \sigma g_0(\mathrm{X}) - \sigma g(\mathrm{X}) = \sum_i (r_i(\sigma a) - \rho_i(\sigma a, \sigma d))(\mathrm{X}-\sigma a)^i.$$

$\mathbb{K}$ being Henselian, we have $v(r_i(\sigma a) - \rho_i(\sigma a, \sigma d)) = v(r_i(a) - \rho_i(a,d))$, hence $w_{\sigma a,\delta}(\sigma g_0 - \sigma g) = w_{a,\delta}(g_0 - g)$. But we said that one can assume that $w_{\sigma a,\delta} = w_{a,\delta}$. Then we have $w_{a,\delta}(\sigma g_0 - \sigma g) = w_{a,\delta}(g_0 - g) > w_{a,\delta}(g_0)$. This proves that g and h are in $\mathbb{K}[\mathrm{X}]$.

From $v^{\mathrm{G}}(h_0 - h_1) > v^{\mathrm{G}}(h_0)$ we conclude that $v^{\mathrm{G}}(\hat{h_0} - h_1) > v^{\mathrm{G}}(\hat{h_0})$. This concludes the proof. □

3 Geometric interpretation

We give here a geometric interpretation of the previous result.

For any $\zeta \in \mathbb{K}^{ac}$ we denote by $\mathrm{B}^{\circ}_{\zeta,0} = \{\alpha \in \mathbb{K}^{ac} : v(\alpha - \zeta) > 0\}$ the open ball of center ζ; the closed ball $\mathfrak{V}^{ac} = \mathrm{B}_{0,0}$ is a disjoint union of such open balls. Note that there is bijection between the set of open balls $\mathrm{B}^{\circ}_{\alpha,0} \subseteq \mathrm{B}_{0,0}$ and the residue field of $\mathbb{K}^{ac}$ (given by $\mathrm{B}^{\circ}_{\alpha,0} \mapsto \overline{\alpha}$).

Let f, f_0, g_0 be polynomials satisfying the hypotheses of the Classical Hensel's Lemma. As soon as there are roots of f in a ball $\mathrm{B}^{\circ}_{\alpha,0} \subseteq \mathrm{B}_{0,0}$, then there are roots of g_0 or h_0. If there are some roots of g_0 (resp. h_0) in a ball $\mathrm{B}^{\circ}_{\alpha,0}$, then there are exactly the same number of roots of f. All the roots of g_0 are in $\mathrm{B}_{0,0}$. Moreover, in any ball $\mathrm{B}^{\circ}_{\alpha,0} \subseteq \mathrm{B}_{0,0}$ there can not be roots of g_0 together with roots of h_0.

These geometric conditions are equivalent to $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$.

If g, h are the factors of f provided by the conclusion of the lemma, the roots of g are exactly the roots of f which are in the open balls $\mathrm{B}^{\circ}_{\alpha,0}$ where the roots of g_0 can be found; the same holds for integral roots of h, and the non-integral roots of f (the roots not in $\mathrm{B}_{0,0}$) are exactly the non-integral roots of h.

Now for the Generalized Lemma, in the case of a residually transcendantal valuation $w_{a,\delta}$, almost the same holds: just replace $\mathrm{B}_{0,0}$ by $\mathrm{B}_{a,\delta}$, and the open balls $\mathrm{B}^{\circ}_{\alpha,0}$ by open balls $\mathrm{B}^{\circ}_{\alpha,\delta} \subseteq \mathrm{B}_{a,\delta}$. We think that these geometric interpretations are of some interest for a better understanding of the proof given in the previous section; they are certainly useful for the proof given in the next section.

The following lemma gathers all these results in a very formal manner.

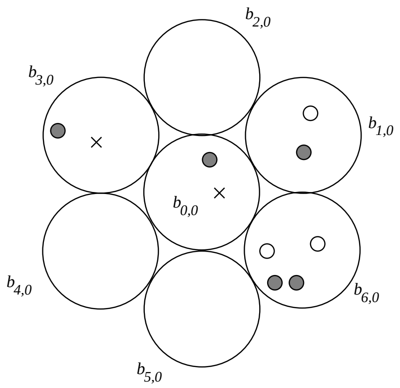
Lemma 4 *Let $w_{a,\delta}$ be a residually transcendental valuation.*

- *For $p(\mathrm{X}) = \sum_i c_i \cdot (\mathrm{X} - a)^i \in \mathbb{K}[\mathrm{X}]$, write $\mathrm{M}_{a,\delta}(p) = \max\{i : v(c_i) + i \cdot \delta = w_{a,\delta}(p)\}$, and $\mathrm{m}_{a,\delta}(p) = \min\{i : v(c_i) + i \cdot \delta = w_{a,\delta}(p)\}$. Then, in $\mathbb{K}^{ac}$, there are exactly (counted with multiplicities) $\mathrm{M}_{a,\delta}(p)$ roots of $p(\mathrm{X})$ in $\mathrm{B}_{a,\delta}$ and $\mathrm{m}_{a,\delta}(p)$ in $\mathrm{B}^\circ_{a,\delta}$.*
- *For $p, q \in \mathbb{K}[\mathrm{X}]$, we have $\mathrm{M}_{a,\delta}(p \cdot q) = \mathrm{M}_{a,\delta}(p) + \mathrm{M}_{a,\delta}(q)$, and $\mathrm{m}_{a,\delta}(p \cdot q) = \mathrm{m}_{a,\delta}(p) + \mathrm{m}_{a,\delta}(q)$. If $w_{a,\delta}(f - g_0 \cdot h_0) > w_{a,\delta}(f)$, then $\mathrm{M}_{a,\delta}(f) = \mathrm{M}_{a,\delta}(g_0 \cdot h_0)$ and $\mathrm{m}_{a,\delta}(f) = \mathrm{m}_{a,\delta}(g_0 \cdot h_0)$.*
- *If there are $a, b \in \mathbb{K}[\mathrm{X}]$ such that $w_{a,\delta}(a \cdot g_0) \geq 0$, $w_{a,\delta}(b \cdot h_0) \geq 0$ and $w_{a,\delta}(a \cdot g_0 + b \cdot h_0 - 1) > 0$, then $\min(\mathrm{m}_{a,\delta}(g_0), \mathrm{m}_{a,\delta}(h_0)) = 0$.*

Proof It's easy to verify all this in the case where $w_{a,\delta} = w_{0,0} = v^{\mathrm{G}}$ — it comes from the fact that if $v(c) = v^{\mathrm{G}}(p)$, then we can write $\overline{p(\mathrm{X})/c} = \overline{c'_{\mathrm{M}}} \cdot \mathrm{X}^{\mathrm{M}} + \cdots + \overline{c'_{\mathrm{m}}} \cdot \mathrm{X}^{\mathrm{m}} \in k[\mathrm{X}]$. For the general case use the case of the Gaussian extension and the "hat" and "check" transformations ($f \mapsto \hat{f}$ and $f \mapsto \check{f}$). □

Remark 5 *If $\mathrm{B}_{a,\delta} = \mathrm{B}_{b,\delta}$, we don't necessarily have $\mathrm{B}^\circ_{a,\delta} = \mathrm{B}^\circ_{b,\delta}$; hence the value of $\mathrm{m}_{a,\delta}(p)$ for a polynomial p depends not only on the choice of $w_{a,\delta}$, but on the choice of the pair (a, δ), whereas the value of $\mathrm{M}_{a,\delta}(p)$ is the same for each pair defining the same valuation.*

Exemple 6 *In $\mathbb{K} = \mathbb{Q}_7$, this figure describes the situation for the polynomials $f = 7\mathrm{X}^6 + \mathrm{X}^5 + 5\mathrm{X}^4 + 3\mathrm{X}^3 + 9\mathrm{X}^2 - 4\mathrm{X} + 7$, $g_0 = \mathrm{X}^3 + \mathrm{X}^2 - \mathrm{X} + 6$, $h_0 = \mathrm{X}^2 + 4\mathrm{X} + 7$. The gray disks are the roots of f in $\mathrm{B}_{0,0}$, the white ones the roots of g_0 and the crosses the roots of h_0. We have $\mathrm{B}_{0,0} = \mathrm{B}^\circ_{0,0} \cup \mathrm{B}^\circ_{1,0} \cup \ldots \cup \mathrm{B}^\circ_{6,0}$.*



4 The value transcendental case

We prove Theorem 1.2 in the case where $w_{a,\delta}$ is a value transcendental valuation. In that case δ defines a cut in $\overline{\Gamma}$ as stated in the first part of the paper.

Proof [Proof of theorem 1.2] Consider a value transcendental valuation $w_{a,\delta}$.

Suppose that f, g_0, h_0 in $\mathbb{K}[\mathrm{X}]$ verify the hypotheses $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$. We write

$$g_0 \cdot h_0 = \sum_{i=0}^{n} c_i \cdot (\mathrm{X} - a)^i \quad \text{and} \quad f = \sum_{i=0}^{k} a_i \cdot (\mathrm{X} - a)^i,$$

$$g_0 = \sum_{i=0}^{m} r_i \cdot (\mathrm{X} - a)^i \quad \text{and} \quad h_0 = \sum_{i} s_i \cdot (\mathrm{X} - a)^i.$$

Note that GH_2 implies that $v(r_m) + m \cdot \delta = w_{a,\delta}(g_0)$.

Since we have $\delta \notin \overline{\Gamma}$, there exists a *unique* $\ell \leq k$ such that $w(f) = v(a_\ell) + \ell \cdot \delta$. With the notations of lemma 4, we have $\ell = \mathrm{M}_{a,\delta}(f) = \mathrm{m}_{a,\delta}(f)$. Now GH_1 is equivalent to

$$\begin{cases} v(a_\ell - c_\ell) & > & v(a_\ell) \\ \delta & > & \dfrac{v(a_\ell) - v(a_i - c_i)}{i - \ell} & \text{for } i > \ell \\ \delta & < & \dfrac{v(a_\ell) - v(a_i - c_i)}{i - \ell} & \text{for } i < \ell. \end{cases}$$

An equivalence with other systems of strict inequalities can be written for GH_2, GH_3. We conclude that there exist $\varepsilon_1, \varepsilon_2$ in $\overline{\Gamma}$ such that for all $\delta' \in (\varepsilon_1, \varepsilon_2) := \{\delta' \in \overline{\Gamma} : \varepsilon_1 < \delta' < \varepsilon_2\}$, the hypotheses $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$ hold for the residually transcendental valuation $w_{a,\delta'}$. In the case where $\overline{\Gamma}^{<\delta} = \varnothing$ we can even take $\varepsilon_1 = -\infty$, and in the case where $\overline{\Gamma}^{>\delta} = \varnothing$ we can take $\varepsilon_2 = +\infty$.

Take $\delta_1 < \delta_2 \in (\varepsilon_1, \varepsilon_2)$, denote w_{a,δ_1} and w_{a,δ_2} the associated residually transcendental valuations.

Following the geometric interpretation given in the previous section, we see that all roots of g_0 are in $\mathrm{B}_{a,\delta_1} \subseteq \mathrm{B}^\circ_{a,\delta_2}$. Then we see that all roots of g_0 are in $\mathrm{B}^\circ_{a,\delta'}$ for all $\delta' \in (\varepsilon_1, \varepsilon_2)$.

In the case $\overline{\Gamma}^{>\delta} = \varnothing$, that proves that g has no roots in $\mathrm{B}^\circ_{a,\delta'}$, for all $\delta' \in (\varepsilon_1, +\infty)$, that is $\mathrm{m}_{a,\delta'} = 0$. Hence, by definition of $\mathrm{m}_{a,\delta'}$, for all $\delta' \in (\varepsilon_1, +\infty)$, we have $w_{a,\delta'}(g_0) = v(r_0)$, and that is true for δ as well. Since we have also $v(lc(g_0)) + \deg(g_0) \cdot \delta = w_{a,\delta}(g_0)$, we have $\deg g_0 = 0$ and the theorem is trivial. We can then assume $\overline{\Gamma}^{>\delta} \neq \varnothing$

Still using the geometric interpretation, we see also that h_0 has not roots in $\mathrm{B}^\circ_{a,\delta_2}$ (for roots of g_0 are in it) which contains B_{a,δ_1}.

Then for all $\delta' \in (\varepsilon_1, \varepsilon_2)$, h_0 has no roots in $\mathrm{B}_{a,\delta'}$. That is $\mathrm{M}_{a,\delta'}(h_0) = 0$, for all $\delta' \in (\varepsilon_1, \varepsilon_2)$. We conclude that $v(s_0) = w_{a,\delta'}(h_0)$ for all $\delta' \in (\varepsilon_1, \varepsilon_2)$, and now it's easy to show that $v(s_0) = w_{a,\delta}(h_0)$.

In the case $\overline{\Gamma}^{<\delta} = \varnothing$, that proves that $\deg h_0 = 0$. Moreover, from GH_1 you can now conclude that $\deg g_0 = \deg g$ and the theorem is trivial. We can then assume that $\overline{\Gamma}^{<\delta} \neq \varnothing$.

Now take $\delta_1 \in (\varepsilon_1, \delta)$ and $\delta_2 \in (\delta, \varepsilon_2)$.

Applying the residually transcendental case, we get unique polynomials g_1, h_1 and g_2, h_2 satisfying the conclusion of the theorem, for w_{a,δ_1} and w_{a,δ_2} respectively.

We write $g_2 = \sum_{i=0}^{m} r'_i \cdot (\mathrm{X}-a)^i$. Now $w_{a,\delta_2}(g_2 - g_0) > w_{a,\delta_2}(g_0)$ is equivalent to

$$\left\{ v(r_m - r'_m) \quad > \quad v(r_m) \quad \delta_2 \quad < \quad \frac{v(r'_i - r_i) - v(r_m)}{m-i}, \quad \forall\, i < m. \right.$$

(Remember that $v(r_m) + m \cdot \delta' = w_{a,\delta'}(g_0)$ for all $\delta' \in (\varepsilon_1, \varepsilon_2)$.) For we have $\delta_1 < \delta < \delta_2$, the same system of inequalities remains true if we replace δ_2 by δ or δ_1, and we conclude that $w_{a,\delta}(g_2 - g_0) > w_{a,\delta}(g_0)$ and $w_{a,\delta_1}(g_2 - g_0) > w_{a,\delta_1}(g_0)$.

Now g_2, h_2 satisfy the conditions $\mathrm{GH}_a, \mathrm{GH}_b, \mathrm{GH}_c$ for the valuation w_{a,δ_1}, and by unicity we have $g_1 = g_2$ and $h_1 = h_2$.

We take $g = g_1 = g_2$ and $h = h_1 = h_2 = \sum_i s'_i \cdot (\mathrm{X}-a)^i$. Of course GH_a and GH_b hold, and we just proved that GH_c holds. It remains to show that $w_{a,\delta}(h - h_0) > w_{a,\delta}(h_0)$.

The inequality $w_{a,\delta_1}(h - h_0) > w_{a,\delta_1}(h_0)$ holds, and, since we have $w_{a,\delta_1}(h_0) = v(s_0)$, is equivalent to

$$\left\{ \begin{array}{rcl} v(s'_0 - s_0) & > & v(s_0) \\ \delta_1 & > & \dfrac{v(s_0) - v(s'_i - s_i)}{i}, \quad \forall\, i > 0. \end{array} \right.$$

From $\delta > \delta_1$ we conclude that $w_{a,\delta}(h - h_0) > w_{a,\delta}(h_0)$, and this ends the proof. $\square$

Remark 7 *During the proof, we have proved that if we keep the definitions of lemma 4 for* $\mathrm{M}_{a,\delta}$ *and* $\mathrm{m}_{a,\delta}$*, for all* $p(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$*, we have* $\mathrm{M}_{a,\delta}(p) = \mathrm{m}_{a,\delta}(p)$*; we proved that the three statements of lemma 4 were still true. Thus if* f, g_0, h_0 *satisfy* $\mathrm{GH}_1, \mathrm{GH}_2, \mathrm{GH}_3$*, then* $\deg h_0 = 0$ *and* $\deg g_0 = \mathrm{M}_{a,\delta}(f)$.

5 A multidimensional lemma

We thank Sudesh Kaur Khanduja for suggesting us to try to state a multivariate version of this result; we will do this now. Here we consider only residually transcendental extensions of v.

It was an abuse to speak of *the* Classical Hensel's Lemma: there is another very classical statement of Hensel's Lemma about zeros of a polynomial (cf. [Rib]). There is a well-known equivalent form, the *multi-dimensional Hensel Lemma* dealing with zeros of systems of polynomials (cf. [Kuh$_1$]). We restate these two results below.

For a system $(f) = (f_1, \ldots, f_n)$ of polynomials in $\mathfrak{V}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, we denote by J_f the Jacobian matrix $\left(\dfrac{\partial f_i}{\partial \mathrm{X}_j}\right)_{ij}$.

Theorem 5.1 (Another Classical Hensel's Lemma) *In a Henselian field, the following statements hold:*

1. *Let $f(\mathrm{X}) \in \mathfrak{V}[\mathrm{X}]$ and $\zeta_0 \in \mathfrak{V}$, such that $v(f(\zeta_0)) > 0$ and $v(f'(\zeta_0)) = 0$. Then there exists a unique $\zeta \in \mathfrak{V}$ such that $f(\zeta) = 0$ and $v(\zeta - \zeta_0) > 0$.*

2. *Let $(f) = (f_1, \ldots, f_n)$ be polynomials in $\mathfrak{V}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, and $\zeta^0 \in \mathfrak{V}^n$ be a n-tuple $(\zeta_1^0, \ldots, \zeta_n^0)$ of integers such that $v(f_i(\zeta^0)) > 0$ for all i. We assume moreover that $v(\det \mathrm{J}_f(\zeta^0)) = 0$. Then there exists a unique $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathfrak{V}^n$ such that $f_i(\zeta) = 0$ for all i, and $v(\zeta_j - \zeta_j^0) > 0$ for all j.*

Remark 8 *The geometric interpretation of the multi-dimensional lemma is that there is one and only one root of (f) in $\mathrm{B}^\circ_{\zeta_1^0,0} \times \cdots \times \mathrm{B}^\circ_{\zeta_n^0,0}$. The conclusion asserts that this root is in $\mathbb{K}^n$.*

We fix a n-tuple $\overline{a} = (a_1, \ldots, a_n)$ of $(\mathbb{K}^{ac})^n$ and $\overline{\delta} = (\delta_1, \ldots, \delta_n) \in \overline{\Gamma}^n$. We extend the valuation v of $\mathbb{K}^{ac}$ by a valuation $w_{\overline{a},\overline{\delta}}$ of $\mathbb{K}^{ac}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$: first we extend v to $\mathbb{K}[\mathrm{X}_1]$ using the pair (a_1, δ_1), and then to $\mathbb{K}[\mathrm{X}_1, \mathrm{X}_2]$ using (a_2, δ_2), and so on.

For each δ_i, we fix a $d_i \in \mathbb{K}^{sep}$ such that $v(d_i) = \delta_i$. We denote by $\mathcal{D}$ the *closed polydisk* $\mathrm{B}_{a_1,\delta_1} \times \ldots \times \mathrm{B}_{a_n,\delta_n}$.

Theorem 5.2 (Another Generalized Hensel's Lemma) *In a Henselian field, the following statements hold:*

1. *Let $f(\mathrm{X})$ be of non-negative $w_{a,\delta}$-value and $\xi_0 \in \mathrm{B}_{a,\delta} \cap \mathrm{K}$, such that $v(f(\xi_0)) > 0$ and $v(f'(\xi_0)) = -\delta$. Then there exists a unique $\xi \in \mathrm{B}_{a,\delta} \cap \mathrm{K}$ such that $f(\xi) = 0$, and $v(\xi - \xi_0) > \delta$.*

2. *Let $(f) = (f_1, \ldots, f_n)$ be polynomials in $\mathbb{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ with non-negative $w_{\overline{a},\overline{\delta}}$-value. Let $\xi^0 = (\xi_1^0, \ldots, \xi_n^0) \in \mathcal{D} \cap \mathbb{K}^n$ be such that $v(f_i(\xi^0)) > 0$ for all i. We assume moreover that $v(\det \mathrm{J}_f(\xi^0)) = -\sum_i \delta_i$. Then there exists a unique $\xi = (\xi_1, \ldots, \xi_n) \in \mathcal{D} \cap \mathbb{K}^n$ such that $f_i(\xi) = 0$ for all i, and $v(\xi_j - \xi_j^0) > \delta_j$ for all j.*

Remark 9 *Now, the geometric interpretation for this modified hypotheses is that there is one and only one root of (f) in $\mathrm{B}^\circ_{\xi_1^0,\delta} \times \cdots \times \mathrm{B}^\circ_{\xi_n^0,\delta}$.*

Proof We prove the second statement (the first is a particular case, or could be deduced from Theorem 1.2).

We note that $\mathcal{D} \cap \mathbb{K}^n$ being non-empty, we can assume w.l.o.g. that $a_i \in \mathrm{K}$ for all i. We set $g_i = f_i(d_1\mathrm{X}_1 + a_1, \ldots, d_n\mathrm{X}_n + a_n) \in \mathbb{K}^{sep}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ for all i and $\zeta_j^0 = \dfrac{\xi_j^0 - a_j}{d_j}$. The hypothesis $w_{\overline{a},\overline{\delta}}(f_i) \geq 0$ leads to $g_i \in \mathfrak{V}^{sep}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. The tuple $\zeta^0 = (\zeta_1^0, \ldots, \zeta_n^0)$ is in $\mathfrak{V}^n$, and we have that $v(g_i(\zeta^0)) > 0$ for all i.

The Jacobian matrix J_g is obtained from J_f simply by multiplying the j-th column by d_j, hence $\det \mathrm{J}_g(\zeta^0) = d_1 \cdots d_n \cdot \det \mathrm{J}_f(\xi^0)$ has value 0.

We apply the Classical Lemma to get $\zeta \in (\mathfrak{V}^{sep})^n$, and we set $\xi_j = d_j\zeta_j + a_j$. We have $f_i(\xi) = 0$ for all i and $\xi \in \mathcal{D}$. The inequality $v(\zeta_j - \zeta_j^0) > 0$ leads to

$v(\xi_j - \xi_j^0) > \delta_j$. As in the previous section, the unicity in the statement of the Classical Lemma leads to the unicity of such a tuple ξ in $\mathbb{K}^{sep}$. Then we show that for all $\sigma \in \mathcal{G}\mathrm{al}(\mathbb{K})$, we have $\sigma\xi_j = \xi_j$, just by remarking that the tuple $\sigma\xi$ is another solution; we conclude that $\xi \in \mathbb{K}^n$. □

One could call these generalizations *De-centralized Hensel's Lemmas*, because they replace the classical ball $\mathrm{B}_{0,0} = \mathfrak{V}$ by any other ball.

6 Une version constructive

Revenant à la langue de Giono, nous allons donner une brève preuve constructive du théorème 1.2, dans le cas d'une valuation résiduellement transcendante $w_{a,\delta}$.

Nous allons utiliser l'interprétation géométrique qui a été donnée (section 3) des hypothèses du théorème. Soient f, g_0, h_0 qui vérifient les hypothèses GH_1, $\mathrm{GH}_2, \mathrm{GH}_3$ du lemme 1.2 ; et soit $\mathrm{T(X)} = \mathrm{T}_{f,g_0}(\mathrm{X})$ la transformation de Tschirnhaus de f par g_0.

L'interprétation géométrique nous dit que certaines racines de f sont dans $\mathrm{B}_{a,\delta}$; que c'est le cas de toutes les racines de g_0 ; et qu'à chaque racine β de g_0 on peut associer (pas forcément de façon unique) une racine α de f telle que $v(\beta - \alpha) > \delta$. Soient donc $\beta_1, \ldots, \beta_k$ les racines de g_0, et $\alpha_1, \ldots, \alpha_k$ les racines de f associées. Pour tout $i, j \leq k$, on a $v(\alpha_i - \beta_j) \geq \delta$ et d'autre part on a $v(\alpha_i - \beta_i) > \delta$.

Soient $\alpha_{k+1}, \ldots, \alpha_n$ les autres racines de f (si $\deg f = k$, la factorisation cherchée est $g = f$ et $h = 1$) ; on sait également que si α_i $(i > k)$ est l'une d'entre elles, $v(\alpha_i - \beta_j) \leq \delta$ pour $j = 1, \ldots, k$.

On a

$$v(g_0(\alpha_i)) = v(\mathrm{lc}\, g_0) + \sum_j v(\alpha_i - \beta_j)\,;$$

alors pour $i > k$, $v(g_0(\alpha_i)) \leq v(\mathrm{lc}\, g_0) + k \cdot \delta$, tandis que pour $i \leq k$, $v(g_0(\alpha_i)) > v(\mathrm{lc}(g_0) + k \cdot \delta$.

Nous sommes dans les conditions d'utilisation du théorème III.14 ; on en déduit une factorisation de f, dont un facteur correspond aux racines $\alpha_1, \ldots, \alpha_k$, et est le facteur g cherché.

La comparaison entre les deux preuves est instructive ; on voit que le théorème III.14 permet (ainsi que nous l'avions annoncé) de remplacer le recours au groupe de Galois. L'interprétation géométrique est vitale pour comprendre le sens de ce résultat ; il semble que c'est plus le cas encore pour la preuve constructive que pour la preuve classique, mais c'est un choix de présentation, car on aurait pu travailler sur $\mathrm{T}_{f,g_0}(\mathrm{X})$ et $\mathrm{T}_{\hat{f},\hat{g_0}}(\mathrm{X})$ sans faire cette interprétation.

À condition de donner un sens constructif au choix d'une coupure de $\overline{\Gamma}$, la preuve donnée dans la section 4 pour le cas d'une valuation w qui est transcendante relativement aux groupes de valuation est tout-à-fait constructive.

Si on considère le lemme de Hensel multidimensionnel comme acquis, la généralisation qui en est donnée dans la section 5 est prouvée de façon constructive.

7 Une application de l'interprétation géométrique

Ici $\mathbb{K}$ n'est pas nécessairement un corps hensélien. Le théorème suivant assure la continuité des racines d'un polynôme relativement à ses coefficients.

Théorème 10 *Soit $f(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ de degré n et soient $\alpha_1, \dots, \alpha_n \in \mathbb{K}^{ac}$ ses racines. Soit $\delta > 0$ un élément de Γ. Soit $g(\mathrm{X}) \in \mathbb{K}[\mathrm{X}]$ de degré n, tel que $v^{\mathrm{G}}(f-g) > \Delta$, où*

$$\Delta = v(\mathrm{lc}\, f) + n \cdot \left[\delta + v(\mathrm{lc}\, f) - v^{\mathrm{G}}(f)\right]$$

($\mathrm{lc}\, f$ est le terme dominant de f); alors les racines de g, $\beta_1, \dots, \beta_n$, peuvent être ordonnées de telle façon que $v(\alpha_i - \beta_i) > \delta$ pour tout i.

Remarque Ce résultat est classique, cependant on ne trouve pas en général dans la littérature de valeur pour Δ en fonction de δ. La valeur donné ici n'est pas loin d'être optimale.

Démonstration Voici ce que dit l'interprétation géométrique (section 3) :

$$w_{a,\delta}(f-g) > w_{a,\delta}(f)$$
$$\iff \begin{cases} f \text{ et } g \text{ ont le même nombre de racines} \in \mathrm{B}_{a,\delta}\,; \\ \text{soient } \alpha_1, \dots, \alpha_m \text{ et } \beta_1, \dots, \beta_m \text{ ces racines}; \\ \text{on peut les ordonner de façon à ce que } v(\alpha_i - \beta_i) > \delta. \end{cases}$$

Soit f de degré n et soient $\alpha_1, \dots, \alpha_n \in \mathbb{K}^{ac}$ ses racines. Soit $\delta > 0$; on veut trouver Δ tel que si $v^{\mathrm{G}}(f-g) > \Delta$, on peut ordonner les racines de g en $\beta_1, \dots, \beta_n$ de sorte que $v(\alpha_i - \beta_i) > \delta$ pour tout i.

Cette condition peut s'écrire également : pour tout $a \in \mathbb{K}^{ac}$, $w_{a,\delta}(f-g) > w_{a,\delta}(f)$. Mais il suffit clairement que ça soit vrai pour $a = \alpha_1, \dots, \alpha_n$.

Inégalités entre la valuation de Gauss et $w_{a,\delta}$ Rappelons qu'on suppose $\delta > 0$, ce qui simplifie le travail;. Soit $d \in \mathbb{K}^{ac}$ tel que $v(d) = \delta$. Soit $\phi = \sum_{i=0}^{n} c_i (x-a)^i$. On a $w_{a,\delta}(\phi) = v^{\mathrm{G}}(\phi(dx+a))$.

Or $\phi(dx+a) = \sum_i (c_i d^i) x^i$, et comme $\delta > 0$, $v(c_i d^i) \geq v(c_i)$. On en déduit

$$w_{a,\delta}(\phi) \geq w_{a,0}(\phi).$$

D'autre part $v(c_i d^i) \leq v(c_i) + n\delta$, d'où on déduit

$$w_{a,\delta}(\phi) \leq w_{a,0}(\phi) + n\delta.$$

Bilan, si $\delta > 0$, on a :

$$w_{a,0}(\phi) \leq w_{a,\delta}(\phi) \leq w_{a,0}(\phi) + n\delta.$$

Supposons temporairement que ϕ est unitaire. On écrit $\phi(\mathrm{X}) = \prod_{i=1}^{n}(\mathrm{X}-\alpha_i)$. Alors

$$v^{\mathrm{G}}(\phi) = \sum_{i=1}^{n} \min(0, v(\alpha_i))$$

$$w_{a,0}(\phi) = v^{\mathrm{G}}(\phi(x+a)) = \sum_{i=1}^{n} \min(0, v(\alpha_i - a))$$

Alors, si $v(a) \geq 0$, on a $w_{a,0}(\phi) = v^{\mathrm{G}}(\phi)$.

Et si $v(a) < 0$, on a :

- Si $v(\alpha_i) > v(a)$, alors $v(\alpha_i - a) = v(a)$;
- si $v(\alpha_i) = v(a)$, alors $v(\alpha_i - a) \geq v(a)$;
- si $v(\alpha_i) < v(a)$, alors $v(\alpha_i - a) = v(\alpha_i)$.

Dans les trois cas, on vérifie que $\min(0, v(\alpha_i - a)) \geq \min(0, v(\alpha_i)) + v(a)$.

On en déduit que, pour ϕ unitaire et $v(a) < 0$, on a :

$$0 \geq w_{a,0}(\phi) \geq v^{\mathrm{G}}(\phi) + n \cdot v(a).$$

Pour ϕ de coefficient dominant $\mathrm{lc}\,\phi$ et $v(a) < 0$, on a :

$$v(\mathrm{lc}\,\phi) \geq w_{a,0}(\phi) \geq v^{\mathrm{G}}(\phi) + n \cdot v(a).$$

On a donc les inégalités suivantes :

$$\begin{array}{ll} \text{si } v(a) < 0 & v^{\mathrm{G}}(\phi) + nv(a) \leq w_{a,\delta}(\phi) \leq v(\mathrm{lc}\,\phi) + n \cdot \delta \\ \text{si } v(a) \geq 0 & v^{\mathrm{G}}(\phi) \leq w_{a,\delta}(\phi) \leq v^{\mathrm{G}}(\phi) + n \cdot \delta \leq v(\mathrm{lc}\,\phi) + n \cdot \delta \end{array}$$

Notre condition suffisante Revenons à notre problème. On veut, pour tout i, $w_{\alpha_i,\delta}(f-g) > w_{\alpha_i,\delta}(f)$.

Or $w_{\alpha_i,\delta}(f) \leq v^{\mathrm{G}}(f) + n \cdot \delta$, pour tout i; donc une condition suffisante est :

$$\forall i,\ w_{\alpha_i,\delta}(f-g) > v(\mathrm{lc}\,f) + n \cdot \delta.$$

On vérifie facilement que si α_i est une racine de f, on a $v(\alpha_i) \geq v^{\mathrm{G}}(f) - v(\mathrm{lc}\,f)$. D'autre part on a $v^{\mathrm{G}}(f) - v(\mathrm{lc}\,f) \leq 0$, et cette quantité est nulle si, et seulement si, $v(\alpha_i) \geq 0$ pour tout i.

On a donc, pour tout i : $v^{\mathrm{G}}(f-g) + n \cdot (v^{\mathrm{G}}(f) - v(\mathrm{lc}\,f) \leq w_{\alpha_i,\delta}(f-g)$. La condition suivante est donc une condition suffisante pour que pour tout i, $w_{\alpha_i,\delta}(f-g) > w_{\alpha_i,\delta}(f)$:

$$v^{\mathrm{G}}(f-g) > v(\mathrm{lc}\,f) + n \cdot (\delta + v(\mathrm{lc}\,f) - v^{\mathrm{G}}(f)).$$

□

Remarque Si on n'impose pas $\deg g = n$, la condition $v^{\mathrm{G}}(f-g) > \Delta$ implique simplement que $\deg g \geq n$ et que parmi les racines de g, il y en a n, $\beta_1, \dots, \beta_n$, telles que $v(\alpha_i - \beta_i) > \delta$.

Chapitre V

Corps valués algébriquement clos

Ce chapitre contient également un article en anglais. Je réïtère donc mes excuses. Il s'agit ici d'un travail en commun avec Franz-Viktor Kuhlmann et Henri Lombardi.

On présente une méthode de calcul dynamique dans un corps valué ; une fois de plus l'algorithme du polygone de Newton est au cœur des calculs. Les algorithmes ainsi produits sont ensuite utilisés pour décrire une élimination effective des quantificateurs pour la théorie des corps valués algébriquement clos.

Je n'ai pas modifié la définition du polygone de Newton telle qu'elle apparaissait dans cet article ; notez qu'elle est légèrement différente de celle donnée au chapitre II (il faut ici prendre l'opposé des pentes du polygone de Newton de P pour obtenir la valuation de ses racines).

Introduction

We consider a valued field $\mathbb{K}$ with $\mathbb{V}$ its valuation ring and $\mathbb{S}$ a subring of $\mathbb{V}$ such that $\mathbb{K}$ is the quotient field of $\mathbb{S}$. We assume that $\mathbb{S}$ is an explicit ring and that divisibility inside $\mathbb{V}$ is testable for two arbitrary elements of $\mathbb{S}$. By explicit ring we mean a ring where algebraic operations and equality test are explicit. These are our minimal assumptions of computability. If we want more assumptions in certain cases we shall explicitly state them.

We let $\mathbb{K}^{\mathrm{ac}}$ denote the algebraic closure of $\mathbb{K}$ with $\mathbb{V}^{\mathrm{ac}}$ a valuation ring that extends $\mathbb{V}$. Our general purpose is the discussion of computational problems in $(\mathbb{K}^{\mathrm{ac}}, \mathbb{V}^{\mathrm{ac}})$ under our computability assumptions on $(\mathbb{K}, \mathbb{V})$.

Each computational problem we shall consider has as input *a finite family* $(c_i)_{i=1,\dots,n}$ *of parameters* in the ring $\mathbb{S}$. We call them the *coefficients of our computational problem.* Algorithms with the previous minimal computability assumptions work uniformly. This means that some computations are made that give polynomials of $\mathbb{Z}[\mathrm{C}_1, \ldots, \mathrm{C}_n]$, and that all our tests are of the two following types:

Is $\mathrm{P}(c_1, \ldots, c_n) = 0$? Does $\mathrm{Q}(c_1, \ldots, c_n)$ divide $\mathrm{P}(c_1, \ldots, c_n)$ in $\mathbb{V}$?

We are not interested in the way the answers to these tests are made. We may imagine these answers given either by some oracles or by some algorithms.

We shall denote the unit group by $\mathcal{U}_{\mathbb{V}}$ or $\mathbb{V}^{\times}$, $\mathcal{M}_{\mathbb{V}} = \mathbb{V} \setminus \mathcal{U}_{\mathbb{V}}$ will be the maximal ideal and $\mathcal{U}_{\mathbb{V}}^1 = 1 + \mathcal{M}_{\mathbb{V}}$ is the group of units whose residue is equal to 1. We denote the value group $\mathbb{K}^{\times}/\mathcal{U}_{\mathbb{V}}$ by $\Gamma_{\mathbb{K}}$. We consider $\Gamma_{\mathbb{K}^{\mathrm{ac}}}$ as the divisible hull $\Gamma_{\mathbb{K}}^{dh}$ of $\Gamma_{\mathbb{K}}$, and the valuation $v_{\mathbb{K}^{\mathrm{ac}}}$ as an extension of $v_{\mathbb{K}}$. We shall denote the residue field $\mathbb{V}/\mathcal{M}_{\mathbb{V}}$ of $(\mathbb{K}, \mathbb{V})$ by $\overline{\mathbb{K}}$. By convention, $v(0) = \infty$ (this is not an element of $\Gamma_{\mathbb{K}}$).

We say that the value of some element x belonging to $\mathbb{K}^{\mathrm{ac}}$ is well determined if we know an integer m and two elements F and G of $\mathbb{Z}[\mathrm{C}_1, \ldots, \mathrm{C}_n]$ such that, setting $f = \mathrm{F}(c_1, \ldots, c_n)$, with $f \neq 0$, and $g = \mathrm{G}(c_1, \ldots, c_n)$, there exists a unit u in $\mathbb{V}^{\mathrm{ac}}$ such that:

$$f x^m = u g$$

(a particular case is given by infinite value, i.e., when $x = 0$.)

We call $v(x)$ the value of x and we read the previous formula as:

$$m\, v(x) = v(g) - v(f)\,.$$

We shall use the notation $x \preceq y$ for $v(x) \leq v(y)$.

Example 1 Let us for example explain the computations that are necessary to compare $3v(x_1) + 2v(x_2)$ to $7v(x_3)$ when the values are given by

$$f_1 x_1^{m_1} = u_1 g_1,\ f_2 x_2^{m_2} = u_2 g_2,\ f_3 x_3^{m_3} = u_3 g_3, \quad (g_1, g_2, g_3 \neq 0)\,.$$

We consider the LCM $m = m_1 n_1 = m_2 n_2 = m_3 n_3$ of m_1, m_2, m_3. We have that

$$f_1^{n_1} x_1^m = u_1^{n_1} g_1^{n_1},\ f_2^{n_2} x_2^m = u_2^{n_2} g_2^{n_2},\ f_3^{n_3} x_3^m = u_3^{n_3} g_3^{n_3}\,.$$

So $3v(x_1) + 2v(x_2) \leq 7v(x_3)$ iff $g_1^{3n_1} g_2^{2n_2} f_3^{7n_3} \preceq f_1^{3n_1} f_2^{2n_2} g_3^{7n_3}$.

The reader can easily verify that computations we shall run in the value group are always meaningful under our computability asumptions on the ring $\mathbb{S}$.

In the same way, elements of the residue field will be in general defined from elements of $\mathbb{V}$. So computations inside the residue field are given by computations inside $\mathbb{S}$.

The constructive meaning of the existence of an algebraic closure $(\mathbb{K}^{\mathrm{ac}}, \mathbb{V}^{\mathrm{ac}})$ of $(\mathbb{K}, \mathbb{V})$ is that computations inside $(\mathbb{K}^{\mathrm{ac}}, \mathbb{V}^{\mathrm{ac}})$ never produce contradictions. The constructive proof of this constructive meaning can be obtained by considering classical proofs (of the existence of an algebraic closure) from the viewpoint of dynamical theories (see [CLR]).

The present paper can be read from a classical point of view as well as from a constructive one. Our results give a uniform way for computing inside $(\mathbb{K}^{\mathrm{ac}}, \mathbb{V}^{\mathrm{ac}})$ when we know how to compute inside $(\mathbb{K}, \mathbb{V})$.

In the first section we give some basic material for computation inside algebraically closed valued fields. The most important is the Newton Polygon Algorithm.

In section 2, we explain how the Newton Polygon Algorithm can be used in order to make explicit computations inside the algebraic closure of a valued field, even in the case where there is no factorisation algorithm for one variable polynomials. It is sufficient to take the point of view of dynamic evaluations as in [D5].

To conclude the paper, we give in section 3 a new quantifier elimination algorithm for the theory of algebraically closed valued fields (with fixed characteristic and residue field characteristic). The geometric idea for this algorithm is simple. It can be easily implemented after the work done in section 2.

1 Basic material

1.1 Multisets

A *multiset* is a set with (nonnegative) multiplicities, or equivalently a list defined up to permutation. E.g., the roots of a polynomial P(X) form a multiset in the algebraic closure of the base field. We shall use the notation $[x_1, \ldots, x_d]$ for the multiset corresponding to the list $(x_1, \ldots, x_d)$. The *cardinality* of a multiset is the length of a corresponding list, i.e., the sum of multiplicities occurring in the multiset.

We shall use the natural (associative commutative) additive notation for "disjoint unions" of multisets, e.g.,

$$[b, a, c, b, b, a, b, d, a, c, b] = 3[a, b] + [b, b, d] + 2[c] = 3[a] + 5[b] + 2[c] + [d] .$$

We call *a pairing between two multisets* what remains of a bijection between two corresponding lists when one forgets the ordering of the lists. E.g., if we consider the two lists

$$(a, a, a, a', a', a', a'') = (a_i)_{i=1,\ldots,7}, \quad (b, b, b', b', b'', b'', b'') = (b_i)_{i=1,\ldots,7}$$

corresponding to the multisets

$$3[a] + 3[a'] + [a''] \quad \text{and} \quad 2[b] + 2[b'] + 3[b'']$$

and the bijection

$$a_1 \mapsto b_3,\ a_2 \mapsto b_4,\ a_3 \mapsto b_1,\ a_4 \mapsto b_6,\ a_5 \mapsto b_5,\ a_6 \mapsto b_7,\ a_7 \mapsto b_2 ,$$

then what remains can be described as

$$2[a \mapsto b'] + [a \mapsto b] + 3[a' \mapsto b''] + [a'' \mapsto b] ,$$

or equivalently as

$$2[(a,b')] + [(a,b)] + 3[(a',b'')] + [(a'',b)]\ .$$

This is a multiset of pairs that gives by the canonical projections the initial multisets $3[a]+3[a']+[a'']$ and $2[b]+2[b']+3[b'']$.

This notion can be extended to r multisets $\mathrm{M}_1,\ldots,\mathrm{M}_r$ with same cardinality k: a pairing between the M_i's is a multiset of r-tuples that gives by the canonical projections the initial multisets $\mathrm{M}_1,\ldots,\mathrm{M}_r$.

The notion of multisets is a natural one when dealing with roots of a polynomial in an abstract setting. Multiplicity is relevant, but in general there is no canonical ordering of the roots.

Dynamic evaluation in [D5, DD] can be understood as a way of computing with root multisets.

1.2 The Newton Polygon

Here we recall the well known Newton Polygon Algorithm.

The Newton polygon of a polynomial $\mathrm{P}(\mathrm{X}) = \sum_{i=0,\ldots,d} p_i \mathrm{X}^i \in \mathbb{K}[\mathrm{X}]$ (where $p_d \neq 0$) is obtained from the list of pairs in $\mathbb{N}\times(\Gamma_{\mathbb{K}}\cup\{\infty\})$

$$((0,v(p_0)),(1,v(p_1)),\ldots,(d,v(p_d)))\ .$$

The Newton polygon is "the bottom convex hull" of this list. It can be formally defined as the extracted list $((0,v(p_0)),\ldots,(d,v(p_d)))$ verifying: two pairs $(i,v(p_i))$ and $(j,v(p_j))$ are two consecutive vertices of the Newton polygon iff:

$$\begin{array}{lcl}
\text{if } 0\le k<i \text{ then } (v(p_j)-v(p_i))/(j-i) & > & (v(p_i)-v(p_k)/(i-k)) \\
\text{if } i<k<j \text{ then } (v(p_k)-v(p_i))/(k-i) & \geq & (v(p_j)-v(p_i))/(j-i) \\
\text{if } j<k\le d \text{ then } (v(p_k)-v(p_j))/(k-j) & > & (v(p_j)-v(p_i))/(j-i)
\end{array}$$

Let $\mathrm{P}(\mathrm{X}) = p_d\prod_{i=1}^d(\mathrm{X}-x_i)$ in $\mathbb{K}^{\mathrm{ac}}[\mathrm{X}]$. It is easily shown that if $(i,v(p_i))$ and $(j,v(p_j))$ are two consecutive vertices in the Newton polygon of the polynomial P, then the zeros of P in $\mathbb{K}^{\mathrm{ac}}$ whose value in $\Gamma_{\mathbb{K}}^{dh}$ equals $(v(p_i)-v(p_j))/(j-i)$ form a multiset with cardinality $j-i$.

Proof Order the x_i's in non-decreasing order of the values $v(x_i)$. We give the proof for an example. Assume for instance that

$$\nu_1 = v(x_1) = v(x_2) < \nu_3 = v(x_3) = v(x_4) = v(x_5) < \nu_6 = v(x_6)\cdots$$

Let us express p_{d-j}/p_d as a symmetric function of the roots. We see immediately that

$$\begin{array}{lcl}
v(p_{d-1}) & \geq & v(p_d)+\nu_1 \\
v(p_{d-2}) & = & v(p_d)+2\nu_1 \\
v(p_{d-3}) & \geq & v(p_d)+2\nu_1+\nu_3 > v(p_d)+3\nu_1 \\
v(p_{d-4}) & \geq & v(p_d)+2\nu_1+2\nu_3 \\
v(p_{d-5}) & = & v(p_d)+2\nu_1+3\nu_3 \\
v(p_{d-6}) & \geq & v(p_d)+2\nu_1+3\nu_3+\nu_6 > v(p_d)+2\nu_1+4\nu_3
\end{array}$$

So the two last edges of the Newton polygon are $((d-2, v(p_{d-2})), (d, v(p_d)))$ with slope $-2\nu_1$ and $((d-5, v(p_{d-5})), (d-2, v(p_{d-2})))$ with slope $-3\nu_3$, giving the wanted result. □

Now we can answer to the following problem.

Computational problem 2 (Multiset of values of roots of polynomials)
Input: *A polynomial* $\mathrm{P} \in \mathbb{K}[\mathrm{X}]$ *over a valued field* $(\mathbb{K}, \mathbb{V})$*.*
Output: *The multiset* $[v(x_1), \ldots, v(x_n)]$ *where* $[x_1, \ldots, x_n]$ *is the multiset of roots of* P *in* $\mathbb{K}^{\mathrm{ac}}$*.*

This problem is solved by the following algorithm, which is widely used in the sequel.

Proof [Newton Polygon Algorithm] The number n_∞ of roots equal to 0 (i.e., with infinite value) is read off from P. Let $\mathrm{P}_0 := \mathrm{P}/\mathrm{X}^{n_\infty}$. Compute the Newton polygon of P_0, compute the slopes and output the answer. □

1.3 Generalized Tschirnhausen transformation

We recall here the well known (generalized) Tschirnhausen transformation, which we will use freely in our computations.

Let $\mathbb{K}$ be a field, $(\mathrm{P}_j)_{j=1,\ldots,m}$ be a family of monic polynomials in $\mathbb{K}[\mathrm{X}]$, and

$$\mathrm{P}_j(\mathrm{X}) = (\mathrm{X} - x_{j,1}) \times \cdots \times (\mathrm{X} - x_{j,d_j})$$

their factorizations in $\mathbb{K}^{\mathrm{ac}}[\mathrm{X}]$.

Let $\mathrm{Q}(\mathrm{Y}_1, \ldots, \mathrm{Y}_m)$ be a polynomial of $\mathbb{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_m]$. Then the polynomial

$$\mathrm{T}_\mathrm{Q}(\mathrm{Z}) = (\mathrm{Z} - \mathrm{Q}(x_{1,1}, \ldots, x_{m,1})) \times \cdots \times (\mathrm{Z} - \mathrm{Q}(x_{1,d_1}, \ldots, x_{m,d_m}))$$

is the characteristic polynomial of A_Q where A_Q is the matrix of the multiplication by $\mathrm{Q}(y_1, \ldots, y_m)$ inside the d-dimensional $\mathbb{K}$-algebra

$$\mathbb{K}[y] := \mathbb{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_m]/\langle \mathrm{P}_1(\mathrm{Y}_1), \ldots, \mathrm{P}_m(\mathrm{Y}_m)\rangle$$

$(d = d_1 \cdots d_m)$.

Let $\mathrm{R} \in \mathbb{K}[\mathrm{Y}_1, \ldots, \mathrm{Y}_m]$ with $\mathrm{R}(x) \neq 0$ for all m-tuples $x = (x_{1,r_1}, \ldots, x_{m,r_m})$. So A_R is an invertible matrix. Let $\mathrm{F} = \mathrm{Q}/\mathrm{R}$, then the polynomial

$$\mathrm{T}_\mathrm{F}(\mathrm{Z}) = (\mathrm{Z} - \mathrm{F}(x_{1,1}, \ldots, x_{m,1})) \times \cdots \times (\mathrm{Z} - \mathrm{F}(x_{1,d_1}, \ldots, x_{m,d_m}))$$

is the characteristic polynomial of $\mathrm{A}_\mathrm{Q}(\mathrm{A}_\mathrm{R})^{-1}$.

2 Dynamic computations in the algebraic closure

Dynamic computations in the algebraic closure of a valued field are an extension of dynamic computations in the algebraic closure of a field as explained in [D5, DD]. First let us recall these.

2.1 Dynamic algebraic closure

The following algorithms tell us how to compute dynamically in the algebraic closure of $\mathbb{K}$ when we do not want to (or we cannot) use factorisation algorithms in $\mathbb{K}[\mathrm{X}]$.

First we examine the problem of adding one root of a monic polynomial without factorisation algorithm. If we are able to compute in the field so created, then we are able to compute recursively in any finite extension given by adding one after the other roots of several polynomials. In fact, since there is a priori an ambiguity about what root we have introduced (distinct roots give in general non-isomorphic fields), we have to compute all possible cases.

Computational problem 3 (computational problem à la D5)

Input: *Let* P *(of degree* ≥ 2*) and* Q *be polynomials in* $\mathbb{K}[\mathrm{X}]$.
Output: *Give correct answers to the following questions:*

(1) *Is* Q *zero at each root of* P *in* $\mathbb{K}^{\mathrm{ac}}$ *?*

(2) *Is* Q *nonzero at each root of* P *in* $\mathbb{K}^{\mathrm{ac}}$ *?*

(3) *If the two answers are "No", compute two factors* P_1 *and* P_2 *of* P *and two polynomials* U_1, U_2 *such that:*
— Q *is zero at each root of* P_1 *in* $\mathbb{K}^{\mathrm{ac}}$,
— Q *is nonzero at each root of* P_2 *in* $\mathbb{K}^{\mathrm{ac}}$,
— P_1 *and* P_2 *are coprime,* $\mathrm{P}_1\mathrm{U}_1 + \mathrm{P}_2\mathrm{U}_2 = 1$,
— *each root of* P *in* $\mathbb{K}^{\mathrm{ac}}$ *is a root of* $\mathrm{P}_1\mathrm{P}_2$.

We give two natural solutions of the previous problem.

Proof [Algorithm SquarefreeD5] *(solving computational problem 3 when* P *is a squarefree polynomial)*
Assume that P is squarefree.

Compute the monic GCD P_1 of P and Q.

If $\mathrm{P}_1 = 1$ then answer Yes to the second question.

else if $\mathrm{lcof}(\mathrm{P})\mathrm{P}_1 = \mathrm{P}$ then answer Yes to the first question.

else return P_1, $\mathrm{P}_2 := \mathrm{P}/\mathrm{P}_1$ and polynomials U_1, U_2 s.t. $\mathrm{P}_1\mathrm{U}_1+\mathrm{P}_2\mathrm{U}_2 = 1$.
□

Proof [Algorithm BasicD5] *(solving computational problem 3)*
Compute the monic GCD P_1 of P and Q.

If $\mathrm{P}_1 = 1$ then answer Yes to the second question.

else compute the monic polynomial P_2 such that:

P_2 divides P, $\mathrm{GCD}(\mathrm{P}_1, \mathrm{P}_2) = 1$ and P divides $\mathrm{P}_1^m\mathrm{P}_2$ (for some m),

if $\mathrm{P}_2 = 1$ then answer Yes to the first question and replace P by P_1.

else return P_1, P_2 and polynomials U_1, U_2 s.t. $P_1U_1 + P_2U_2 = 1$. □

Remark 4 We may assume w.l.o.g. that $\deg(Q) < \deg(P)$ and we can easily see that $P_2 = P/\gcd(P_1^k, Q) = P/\gcd(P^k, Q)$ where $k = 1 + \deg(Q) - \deg(P_1)$. We can also get P_2 by iteration of the process: replace R by $R/\gcd(R, Q)$ (here $\gcd(R, Q)$ means the monic GCD of R and Q) beginning with $R = P$, until the GCD is 1.
If P is monic and the ring $\mathbb{S}$ is normal then P_1 and P_2 are inside $\mathbb{S}[X]$ but it is not always easy to make this result explicit. Nevertheless we can always compute P_1 and P_2 using coefficients in the quotient field of $\mathbb{S}$: the GCD computation may use pseudo divisions instead of divisions. The use of subresultant polynomials may improve the efficacy of the algorithm.

We can understand the previous algorithms as breaking the set of roots of a polynomial in distinct subsets anytime that some objective distinction may be done between the roots.

The simplicity and efficiency of the previous algorithms make it hard to understand how they are not quoted as soon as algebraic extensions of fields are concerned.

Remark 5 If we see the roots of P as a multiset, and if we want to keep the information concerning multiplicities, the output:

- (P_1, P_2) with P_1, P_2 coprime and each root of P in $\mathbb{K}^{ac}$ is a root of P_1P_2.

is not the good one. We need in this case one of the two following outputs:

- (P_1, P_2) with P_1, P_2 coprime and $P_1P_2 = P$.

or in a more economic way for future computations:

- (P_1, P_2) with P_1, P_2 coprime, $P_1P_2 = P$ and a decomposition of each P_i as a product of powers of coprime polynomials.

The computational problem corresponding to the first output can be solved by the following slight variant of **BasicD5**.

Proof [Algorithm MultisetD5] *(solving a multiset variant of computational problem 3).*

Input: Let P (of degree ≥ 2) and Q be polynomials in $\mathbb{K}[X]$.
Output: (P_1, P_2) with P_1, P_2 coprime, $P_1P_2 = P$, Q is zero at each root of P_1 in $\mathbb{K}^{ac}$, Q is nonzero at each root of P_2 in $\mathbb{K}^{ac}$.

Compute the monic GCD R_1 of P and Q.

If $R_1 = 1$ then return $P_1 = 1$, $P_2 = P$

else compute the monic polynomial P_2 such that:

P_2 divides P, $\mathrm{GCD}(R_1, P_2) = 1$ and P divides $R_1^m P_2$ (for some m).

return P_2, $P_1 = P/P_2$ and polynomials U_1, U_2 such that $P_1U_1 + P_2U_2 = 1$. □

We now explain the recursive use of algorithms **SquarefreeD5** and **BasicD5**.

Definition 6 *Take a system of polynomials*

$$\overline{P} = (P_1, \ldots, P_n) \quad \textit{where} \;\; P_1(X_1) \in K[X_1],$$
$$P_2(X_1, X_2) \in K[X_1, X_2], \ldots, P_k(X_1, \ldots, X_k) \in K[X_1, \ldots, X_k]\,.$$

This system is called a triangular system *if each* P_i *is monic in* X_i*.*
A vector $\overline{x} = (x_1, \ldots, x_k) \in (K^{\mathrm{ac}})^k$ *is called a* root vector of $\overline{P}$ *(or* a solution of $\overline{P}$*) if*

$$P_1(x_1) = P_2(x_1, x_2) = \ldots = P_k(x_1, \ldots, x_k) = 0\,.$$

Two systems with the same variables are called coprime systems *if they have no common root vector.*

Note that root vectors of a triangular system $\overline{P}$ form a multiset with cardinality $d = \prod_i \deg_{X_i}(P_i)$.

Computational problem 7 (computing in extensions generated by several successive algebraic elements)
Input:

- *A triangular system of polynomials* $\overline{P} = (P_1, \ldots, P_n)$*:*

$$P_1(X_1) \in K[X_1],\, P_2(X_1, X_2) \in K[X_1, X_2], \ldots$$
$$P_k(X_1, \ldots, X_k) \in K[X_1, \ldots, X_k]\,.$$

- *A finite list of polynomials* $Q_1, \ldots, Q_r$ *in* $K[X_1, \ldots, X_k]$.

Output:

- *A list of coprime triangular systems* $\overline{S^{(1)}}, \ldots, \overline{S^{(\ell)}}$ *whose root vectors give a partition of the set of all solutions of the initial triangular system* $\overline{P}$*.*
- *For each triangular system* $\overline{S^{(j)}}$ *the (fixed)* r*-tuple of signs for the tuple* $(Q_1(\overline{x}), \ldots, Q_r(\overline{x}))$ *(the sign of* y *is either* 0 *if* $y = 0$ *or* 1 *if* $y \neq 0$*), where* $\overline{x} = (x_1, \ldots, x_k)$ *is any root vector of* $\overline{S^{(j)}}$ *.*

In the general case, we can solve the previous problem in the following way.

Proof [Algorithm TriangularBasicD5] *(solving computational problem 7)*

Use **BasicD5** recursively. More precisely consider that Q and P_k are polynomials with variable X_k and parameters $(x_1, \ldots, x_{k-1})$. When making the computations of **BasicD5** we have to solve some tests

$$\text{“ Is } \mathrm{R}(x_1, \ldots, x_{k-1}) = 0 \text{ or not ? ”}$$

for some polynomials R given by the computation. So we have to solve the same kind of problem with one variable less. So a recursive computation ends with the good type of answer. □

In the case of a perfect field, we can use **SquarefreeD5** recursively. To see why this works, we have to recall how to compute the squarefree part of a one variable polynomial in this case.

Proof [Algorithm SquarefreePart] *(compute the squarefree part of a one variable polynomial in the case of a perfect field)*

We assume that K is a perfect field. In the characteristic p case we assume that getting p-th roots is explicit inside S.

Input: A polynomial $\mathrm{P} \in S[\mathrm{X}]$.

Output: P_1 the squarefree part of P.

If the characteristic is zero then $\mathrm{P}_1 = \mathrm{P}/\gcd(\mathrm{P}, \mathrm{P}')$.

If the characteristic is p then let $\mathrm{P}_1 = 1$ and:

Iterate the following process:

Beginning with $\mathrm{R} = \mathrm{P}$ iterate the following process:

If $\mathrm{R} = \mathrm{Q}(\mathrm{X}^p)$ then replace R by $\mathrm{R}^{1/p}$ else replace R by $\mathrm{R}/\gcd(\mathrm{R}, \mathrm{R}')$

until you find $\gcd(\mathrm{R}, \mathrm{R}') = 1$.

Replace P_1 by $\mathrm{P}_1 \times \mathrm{R}$

Iterate the following process:

Replace P by $\mathrm{P}/\gcd(\mathrm{P}, \mathrm{R})$

until you find $\gcd(\mathrm{P}, \mathrm{R}) = 1$

until $\mathrm{P} = 1$. □

Proof [AlgorithmPerfectTriangularD5] *(solving computational problem 7 in the case of a perfect field)*

We assume that K is a perfect field. In the characteristic p case we assume that getting p-th roots is explicit inside S.

In a first big step we replace the initial system by a disjunction of coprime systems that are “squarefree”.

For each polynomial in the triangular system, we use **SquarefreePart** and (recursively) **SquarefreeD5** to replace it by a “squarefree” one.

More precisely, first we replace P_1 by its squarefree part S_1.

Then we try to apply **SquarefreePart** to the polynomial P_2 as if the quotient algebra $K[\mathrm{X}_1]/\mathrm{S}_1(\mathrm{X}_1)$ were a field. If this is not possible, **SquarefreeD5** produces a splitting of S_1. In each branch so created the computation is possible and we can replace P_2 by its squarefree part.

E.g., we get three branches. In the first one, the polynomial $\mathrm{P}_{1,1}$ replaces P_1, and P_2 is coprime with its derivative, so that $\mathrm{P}_{2,1} = \mathrm{P}_2$. In the second one, the polynomial $\mathrm{P}_{1,2}$ replaces P_1, and the squarefree part of P_2 is given by $\mathrm{P}_{2,2}$ with degree $\deg(\mathrm{P}_2) - 1$. In the third one, $\mathrm{P}_{1,3}$ replaces P_1 and the squarefree part of P_2 is given by $\mathrm{P}_{2,3}$ with degree $\deg(\mathrm{P}_2) - 4$. Then we introduce P_3 in any branch previously created and try to apply **SquarefreePart** to the polynomial P_3 as if the corresponding quotient algebra $K[\mathrm{X}_1, \mathrm{X}_2]/\langle \mathrm{R}_1(\mathrm{X}_1), \mathrm{R}_2(\mathrm{X}_1, \mathrm{X}_2)\rangle$ were a field. If this is not possible, **SquarefreeD5** produces a splitting of R_1 or R_2.

And so on.

When we have introduced all P_i's, we get a tree. Each leaf of the tree corresponds to a new triangular system where all successive polynomials replacing the P_i's are "strongly squarefree" (the squarefreeness is certified by a Bezout identity in the suitable quotient algebra). Distinct leaves correspond to coprime triangular systems. So the set of root vectors of $\overline{\mathrm{P}}$ is partitioned into distinct subsets, each one corresponding to a leaf of the tree.

Now we describe the second "big step". At each leaf of the previous tree we search for the signs of the Q_j's using **SquarefreeD5** as if the corresponding quotient algebra were a field. If this is not possible, new splittings are produced. □

Remark 8 Slight variants of the previous algorithms give a partition of the *multiset* of solutions of the triangular system $\overline{\mathrm{P}}$ in disjoint multisets that are defined by coprime triangular systems $\overline{\mathrm{S}'^{(j)}}$, each Q_i having a constant sign at the zeros of each $\overline{\mathrm{S}'^{(j)}}$.

Remark 9 The previous algorithms can be generalized in order to search systematically for solutions of any system of sign conditions: equalities need not be in a triangular form. So they can be seen as quantifier elimination algorithms in the first order theory of algebraically closed extensions of some explicitly given field K.

In the following subsection we show that the same kind of computations are allowed in the case of valued fields.

2.2 Dynamic algebraic closure of a valued field

Roots of one polynomial

The valued algebraic closure of (K, V) is well determined up to isomorphism. So the following computational problem makes sense.

Computational problem 10 (Simultaneous valuations)
Input: *polynomials* P *(monic) and* $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *in* $K[\mathrm{X}]$. *Call* $[x_1, \ldots, x_d]$ *the multiset of roots of* P *in* K^{ac}.

Output: *The multiset* $[(v(x_i), v(\mathrm{Q}_1(x_i)), \ldots, v(\mathrm{Q}_r(x_i)))]_{i=1,\ldots,d}$ *of* $(r+1)$*-tuples of values.*

This problem is solved by the following algorithm.

Proof [Algorithm SimVal] *(solving computational problem 10)*

Assume w.l.o.g. that $\mathrm{P}(0) \neq 0$. The multiset $[\nu_i]_{i=1,\ldots,d}$ of (finite) values of the x_i's is given by the Newton Polygon Algorithm for P.

For $m, n \in N$, the polynomial

$$\mathrm{S}_{m,n}(\mathrm{X}) = (\mathrm{X} - x_1^m \mathrm{Q}_1(x_1)^n) \cdots (\mathrm{X} - x_d^m \mathrm{Q}_1(x_d)^n)$$

is the characteristic polynomial of the matrix $\mathrm{A}^m(\mathrm{Q}_1(\mathrm{A}))^n$ where A is the companion matrix of P.

So, using the Newton polygon of $\mathrm{S}_{m,n}$ we know the multiset

$$[m\, v(x_i) + n\, v(\mathrm{Q}_1(x_i))]_{i=1,\ldots,d} = [m\, \nu_i + n\, \nu_{1,i}]_{i=1,\ldots,d}$$

for any (m, n).

We compute first the multiset $[\nu_{1,i}]_{i=1,\ldots,d}$.

We want to compute the correct pairing between the two multisets $[\nu_i]_{i=1,\ldots,d}$ and $[\nu_{1,i}]_{i=1,\ldots,d}$.

Assume first that no $\nu_{1,i}$ is infinite.

Let us call a *bad coincidence for* n_1 an equality

$$\nu_i + n_1\, \nu_{1,h} = \nu_j + n_1\, \nu_{1,k} \quad \text{with} \quad \nu_i \neq \nu_j, \quad i, j, h, k \in \{1, \ldots, d\}\ .$$

If there is no bad coincidence for some n_1 then we can state this fact by considering the two sets $\{\nu_i\ : i = 1, \ldots, d\}$ and $\{\nu_{1,i}\ : i = 1, \ldots, d\}$. Note also that there are at most $(d(d-1)/2)^2$ "bad values" of n_1. So we can find a "good" n_1 by a finite number of computations. Fix a "good" n_1. From the multisets $[\nu_i]_{i=1,\ldots,d}$ and $[\nu_{1,i}]_{i=1,\ldots,d}$ we deduce the multiset $[\nu_i + n_1\, \nu_{1,j}]_{i=1,\ldots,d, j=1,\ldots,d}$. Now, n_1 being "good", the multiset $[\nu_i + n_1\, \nu_{1,i}]_{i=1,\ldots,d}$ (obtained by the Newton Polygon Algorithm applied to S_{1,n_1}) can be read as a submultiset of $[\nu_i + n_1\, \nu_{1,j}]_{i=1,\ldots,d, j=1,\ldots,d}$. This gives us the pairing between the multisets $[\nu_i]_{i=1,\ldots,d}$ and $[\nu_{1,i}]_{i=1,\ldots,d}$.
For example, assume that

$$[\nu_i]_{i=1,\ldots,9} = 3[\alpha_1] + 4[\alpha_2] + 2[\alpha_3], \qquad [\nu_{1,i}]_{i=1,\ldots,9} = 2[\beta_1] + 2[\beta_2] + 2[\beta_3] + 3[\beta_4]$$

and that the number 5 is good, i.e., the twelve values $\alpha_i + 5\beta_k$ are distinct. Computing the multiset $[\nu_i + 5\, \nu_{1,i}]_{i=1,\ldots,9}$, we find e.g.,

$$\begin{gathered}[\alpha_1 + 5\beta_1] + 2[\alpha_1 + 5\beta_4] + [\alpha_2 + 5\beta_4] + 2[\alpha_2 + 5\beta_2] + \\ + [\alpha_2 + 5\beta_3] + [\alpha_3 + 5\beta_1] + [\alpha_3 + 5\beta_3],\end{gathered}$$

and we get the pairing

$$[(\alpha_1, \beta_1)] + 2[(\alpha_1, \beta_4)] + [(\alpha_2, \beta_4)] + 2[(\alpha_2, \beta_2)] + [(\alpha_2, \beta_3)] + [(\alpha_3, \beta_1)] + [(\alpha_3, \beta_3)]\,.$$

Comment: the multiset $[x_i]_{i=1,\ldots,d}$ is, as a root multiset, made of "indiscernible elements". The knowledge of the multiset $[\nu_i]_{i=1,\ldots,d}$ introduces some distinction between the roots (if the ν_i's are not all equal). The knowledge of the multiset $[\nu_i + n_1\,\nu_{1,i}]_{i=1,\ldots,d}$ (with a "good" n_1) induces a finer distinction between the roots.

We remark that the case where some $\mathrm{Q}_1(x_i)$'s equal zero can also be done correctly by a slight modification of the previous algorithm. Nevertheless, when such a case appears, it seems more natural to use the technique of dynamical evaluation (see [D5] and section 2.1). If not all $\mathrm{Q}_1(x_i)$'s equal zero (which is a trivial case), then one can compute a factorisation of P in a product of two coprime polynomials P_1 and P_2 by applying algorithm **BasicD5** to P and Q_1. And we can study separately the roots of these two polynomials. Moreover, the following steps of the algorithm are clearer if all $\mathrm{Q}_1(x_i)$'s are distinct from zero.

Next we show that analogous arguments work for the general case. It will be sufficient to show how the case $r = 2$ works. Set $\nu_{2,i} = v(\mathrm{Q}_2(x_i))$. We have computed the correct pairing $[(\nu_1, \nu_{1,1}), (\nu_2, \nu_{1,2}), \ldots, (\nu_d, \nu_{1,d})]$ between the multisets $[\nu_i]_{i=1,\ldots,d}$ and $[\nu_{1,i}]_{i=1,\ldots,d}$. We know also a "good" integer n_1. We can assume w.l.o.g. that all $\nu_{1,i}$'s and $\nu_{2,i}$'s are finite. We compute first the multiset $[\nu_{2,i}]_{i=1,\ldots,d}$. Let us call a *bad coincidence for* n_2 an equality

$$\nu_i + n_1\,\nu_{1,i} + n_2\,\nu_{2,h} = \nu_j + n_1\,\nu_{1,j} + n_2\,\nu_{2,k} \quad \text{with} \quad \nu_i + n_1\,\nu_{1,i} \neq \nu_j + n_1\,\nu_{1,j}\,.$$

If there is no bad coincidence for some n_2 then we can state this fact by considering the two sets $\{\nu_i + n_1\,\nu_{1,i}\ : i = 1, \ldots, d\}$ and $\{\nu_{2,i}\ : i = 1, \ldots, d\}$. We choose such an integer n_2. And so on. □

Remark 11 Assume that P is a squarefree polynomial, so the x_i's are in the separable closure K^{sep} of (K, V). Assume that algorithm **SimVal** has shown that some list of values $(\nu_i, \nu_{1,i}, \ldots, \nu_{r,i})$ corresponds to only one root of P. It is clear from the abstract definition of the henselization that such a "discernible" element over (K, V) is inside the henselization K^{h} of (K, V). A perhaps surprising computational consequence is that, since the henselization is an immediate extension, when algorithm **SimVal** isolates (or discerns) some root of P, then the corresponding list of values is made only of "integer values", i.e., values of elements of K "without integer denominator". We can prove this constructively:

First, using computations in the henselization K^{h} as defined in [KL], we proved (this is theorem III.14) the following lemma:

Lemma 12 *If the polynomial* $\mathrm{P} \in K^{\mathrm{h}}[\mathrm{X}]$ *has roots* $x_1, \ldots, x_d$ *and if the* d*-tuple* $[v(\mathrm{Q}(x_1)), \ldots, v(\mathrm{Q}(x_d))]$ *(provided by* **SimVal** *applied to* P, Q *or by any other way) is equal to* $d_1[\alpha_1] + \ldots + d_k[\alpha_k]$*, with* $\alpha_i \neq \alpha_j$ *(for* $i \neq j$*), then one can factorize* $\mathrm{P} = \mathrm{P}_1 \ldots \mathrm{P}_k$ *in* $K^{\mathrm{h}}[\mathrm{X}]$ *(*$\deg \mathrm{P}_i = d_i$*), such that, if the roots of* P_i *are* $y_1, \ldots, y_{d_i}$ *the* d_i*-tuple* $[v(\mathrm{Q}(y_1), \ldots, v(\mathrm{Q}(y_{d_i}))]$ *is equal to* $d_i[\alpha_i]$.

Then if some list of values $(\nu_i, \nu_{1,i}, \ldots, \nu_{r,i})$ corresponds to only one root of P, we let
$n_0 = \#\{j : \nu_j = \nu_i\}$,
$n_1 = \#\{j : \nu_j = \nu_i \text{ and } \nu_{1,j} = \nu_{1,i}\}$,

...
$n_r = \#\{j : \nu_j = \nu_i \text{ and } \nu_{k,j} = \nu_{k,i} \quad k = 1, \ldots, r\} = 1$

The previous result applied to $\mathrm{P}(\mathrm{X})$ and $\mathrm{Q}(\mathrm{X}) = \mathrm{X}$ provides a factor P_0 of P, with degree n_0; then applied to $\mathrm{P}_0(\mathrm{X})$ and $\mathrm{Q}_1(\mathrm{X})$, it provides a factor P_1 with degree n_1, and so on. Finally, we obtain a factor P_r of degree $n_r = 1$. So the corresponding root is in K^{h}. The computations in K^{h} prove that the list of values is made only of "integer values"; one can compute explicitly elements of K having the same value. More precisely, one can compute $z_0, z_1, \ldots, z_r \in K$, such that $x_i = z_0(1 + \nu_0), \mathrm{Q}_1(x_i) = z_1(1 + \nu_1), \ldots, \mathrm{Q}_r(x_i) = z_r(1 + \nu_r)$, with $v(\nu_i) > 0$ for all i.

Root vectors of triangular systems

The algorithm **SimVal** says that "we can compute in $K[x]$" where x is a root of P satisfying certain "compatible value conditions". We know how many roots of P correspond to a system of compatible value conditions. Computing in $K[x]$ means that we can get "any brute information concerning the valuation in this field", more precisely, we can decide, for any new polynomial Q, if the value of $\mathrm{Q}(x)$ is well determined or not. And we can compute the value(s). When several possibilities for $v(\mathrm{Q}(x))$ appear, choosing one possible value, we refine our description of $K[x]$.

So even if $K[x]$ is not a priori a completely well determined valued field, we can nevertheless always do as if it was completely well determined. And we get recursively the following computations, exactly as in section 2.1.

More precisely, our computational problem is the following.

Computational problem 13
(computing in extensions generated by several successive algebraic elements)

Input:

- *A triangular system of polynomials* $\overline{\mathrm{P}} = (\mathrm{P}_1, \ldots, \mathrm{P}_n)$*:*

$$\mathrm{P}_1(\mathrm{X}_1) \in K[\mathrm{X}_1],\ \mathrm{P}_2(\mathrm{X}_1, \mathrm{X}_2) \in K[\mathrm{X}_1, \mathrm{X}_2],\ \ldots,$$
$$\mathrm{P}_k(\mathrm{X}_1, \ldots, \mathrm{X}_k) \in K[\mathrm{X}_1, \ldots, \mathrm{X}_k]\,.$$

- *A finite list of polynomials* $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *in* $K[\mathrm{X}_1, \ldots, \mathrm{X}_k]$.

Output:

- *The multiset of* $(k + r)$*-tuples of values*

$$[(v(x_1), \ldots, v(x_k), v(\mathrm{Q}_1(\overline{x})), \ldots, v(\mathrm{Q}_r(\overline{x})))]_{\overline{x}=(x_1,\ldots,x_k)\in \mathrm{R}}$$

where R *is the multiset of root vectors of* $\overline{\mathrm{P}}$ *(this multiset has cardinality* $d = \prod_i \deg_{\mathrm{X}_i}(\mathrm{P}_i)$*).*

This problem is solved by the following algorithm.

Proof [Algorithm TriangularSimVal] Use recursively algorithm **SimVal**. □

Graph of roots

The following algorithm can be seen as a particular case of the previous one. We denote by $\mu(\mathrm{P}, a)$ the multiplicity of a as root of the univariate polynomial P (if $\mathrm{P}(a) \neq 0$ we let $\mu(\mathrm{P}, a) = 0$).

Computational problem 14
(computing the ultrametric graph of roots of a family of univariate polynomials)

Input:

- *A finite family of univariate polynomials* $\overline{\mathrm{P}} = (\mathrm{P}_1, \ldots, \mathrm{P}_s)$ *in* $K[\mathrm{X}]$.

Output:

- *The number* N *of distinct roots of* $\mathrm{P}_1 \cdots \mathrm{P}_n$.
- *For some ordering* $(x_1, \ldots, x_\mathrm{N})$ *of these roots the finite family*

$$\big((\mu(\mathrm{P}_i, x_j))_{i\in[1,s],j\in[1,\mathrm{N}]}, (v(x_j - x_\ell))_{1\leq j<\ell\leq \mathrm{N}}\big) \ .$$

Note that there are many possible answers, by changing the order of the roots. All correct answers are isomorphic.

Proof [Algorithm GraphRoots] First a recursive use of **BasicD5** allows to find a finite multiset of pairwise coprime polynomials $(\mathrm{R}_1, \ldots, \mathrm{R}_r)$ such that each P_i is a product of some R_k's. So we can assume w.l.o.g. that the P_i's are pairwise coprime. If $\deg(\mathrm{P}_i) = n_i$ we introduce the roots $x_{i,1}, \ldots, x_{i,n_i}$ of P_i through the triangular system

$$\begin{array}{rcl}
\mathrm{P}_{i,1}(\mathrm{X}_{i,1}) & = & \mathrm{P}_i(\mathrm{X}_{i,1}) \\
\mathrm{P}_{i,2}(\mathrm{X}_{i,1}, \mathrm{X}_{i,2}) & = & \frac{\mathrm{P}_{i,1}(\mathrm{X}_{i,2}) - \mathrm{P}_{i,1}(\mathrm{X}_{i,1})}{\mathrm{X}_{i,2} - \mathrm{X}_{i,1}} \\
\mathrm{P}_{i,3}(\mathrm{X}_{i,1}, \mathrm{X}_{i,2}, \mathrm{X}_{i,3}) & = & \frac{\mathrm{P}_{i,2}(\mathrm{X}_{i,1}, \mathrm{X}_{i,3}) - \mathrm{P}_{i,2}(\mathrm{X}_{i,1}, \mathrm{X}_{i,2})}{\mathrm{X}_{i,3} - \mathrm{X}_{i,2}} \\
\vdots & \vdots & \vdots \\
\mathrm{P}_{i,n_i}(\mathrm{X}_{i,1}, \ldots, \mathrm{X}_{i,n_i}) & = & \frac{\mathrm{P}_{i,n_i-1}(\mathrm{X}_{i,1}, \ldots, \mathrm{X}_{i,n_i-2},, \mathrm{X}_{i,n_i}) - \mathrm{P}_{i,n_i-1}(\mathrm{X}_{i,1}, \ldots, \mathrm{X}_{i,n_i-2},, \mathrm{X}_{i,n_i-1})}{\mathrm{X}_{i,n_i} - \mathrm{X}_{i,n_i-1}}
\end{array}$$

$$\begin{array}{rcl}
\mathrm{P}_{i,1}(x_{i,1}) & = & 0 \\
\mathrm{P}_{i,2}(x_{i,1}, x_{i,2}) & = & 0 \\
\mathrm{P}_{i,3}(x_{i,1}, x_{i,2}, x_{i,3}) & = & 0 \\
\vdots & \vdots & \vdots \\
\mathrm{P}_{i,n}(x_{i,1}, \ldots, x_{i,n_i}) & = & 0
\end{array}$$

The $\mathrm{P}_{i,k}$'s give all together a triangular system and we can apply **Triangular-SimVal** for finding the values $v(x_{i,k} - x_{i',k'})$. In particular we get the multiplicity of each root. We remark that we can use a simplified form of **TriangularSimVal** since all possible results are isomorphic and we need only one of these results. E.g., in the first step we compute the multiset $[(v(x_{1,k} - x_{1,k'})_{1\leq k<k'\leq n_1}]$ but we select arbitrarily one value as the good one w.r.t. some ordering of the roots, and so on. □

Remark 15 There are probably some shortcuts allowing to give this ultrametric graph in a quicker way: for example, for a single polynomial, it is easy to compute the multiset of values $[v(x_i - x_j)]_{i\neq j}$ *without* knowing exactly to which edge each value corresponds; there might be a way (at least in a great number of cases) to reconstruct the graph (up to isomorphism).

3 Quantifier elimination

The aim of this section is to give a transparent proof of the following well known theorem (cf. [Wei]).

Theorem 3.1 *The theory of algebraically closed valued fileds (with fixed characteristics) admits quantifier elimination.*

First we give a sketch of the proof of this theorem. Our algorithm is a kind of "cylindric algebraic decomposition" (in the real closed case see e.g. [BCR]). Given a finite set of multivariate polynomials, we choose a variable as beeing the main variable and we consider the other ones as parameters.

We settle in subsection 3.2 an existential decision procedure for a quantifier free formula with only one variable: given a finite set S of univariate polynomials, we give a complete description of the "valued line K^{ac}" w.r.t. S.

More precisely we give first a formal name to each root of each polynomial in S, and we compute the ultrametric distance between each pair of these roots. We compute also the multiplicities of these roots and all the valuations $v(\mathrm{P}_i(x_j))$ for each root x_j and each polynomial P_i. All this job is done by algorithm **GraphRoots**.

Next, from these datas, we are able to test if a given conjunction of elementary assertions concerning the $v(\mathrm{P}_i(\xi))$'s is realizable by some ξ of the line K^{ac}. In order to make this test we need a key geometric lemma, concerning *ultrametric graphs*. We explain this lemma in section 3.1.

The structure of our existential univariate decision procedure is very simple. This implies a kind of uniformity in such a way that the algorithm can be performed "with parameters", exactly as **BasicTriangularD5** is nothing but a parameterized version of **Basic D5**. This gives a good way for eliminating the quantifier in a formula with only one existential quantifier. So the work of final section 3.3 is a carefull verification of uniformity for the algorithms used in section 3.2.

Finally the general elimination procedure follows by usual tricks.

We now give general explanations about notations and technical buisiness needed in the algorithms.

As in [Wei] we use a two-sorted language, $\mathrm{L} = (\mathrm{L_F}, \mathrm{L_\Gamma}, v)$. The language of fields $\mathrm{L_F} = \{0, 1, +, -, .\}$ is the F-sort. The language $\mathrm{L_\Gamma}$ is the Γ-sort. There is one more symbol, v, which is an function-symbol for the valuation. The language $\mathrm{L_\Gamma}$ consists of the language $\mathrm{L}'_\Gamma = \{0, \infty, +, -, <\}$ of ordered Abelian groups with top element ∞ together with a family of symbols $\{\frac{\cdot}{q} : q \in N^*\}$.

By convention $a - \infty = 0$ for all $a \in \Gamma$. But there are some ambiguities as $a - (b - c)$ possibly not equal to $a - b + c$. In fact it is possible to avoid the sign $-$ for Γ-formulas, using case by case distinctions. E.g. we can replace $a - b = c$ by $(b = \infty \wedge c = 0) \vee a = b + c$. So any quantifier free formula Φ is equivalent to a formula written without the Γ-sign $-$. In the sequel we assume w.l.o.g. that Γ-terms are always written without using the Γ-sign $-$.

Remark also that we have no function symbol for the inverse of a nonzero element inside the field. This is not a restriction. The introduction of this function symbol would imply some troubles as the necessity of some strange convention as $x/0 = 0$ for any x.

The theory of algebraically closed, non-trivial valued fields is $\mathbf{ACVF}(\mathrm{L})$. Recall that the formal theory specifies the characteristic of the field and of the residue field. In our formulas there are F-variables and Γ-variables, F-terms and Γ-terms, and, more important, F-quantifiers and Γ-quantifiers.

The rules of building terms are the natural ones. We see that the F-terms are formal polynomials in $Z[x_1, \cdots, x_n]$. For the Γ-terms, we avoid the Γ-sign $-$. Set $r_1, \ldots, r_k \in Q^{>0}$, and let $f_1, \ldots, f_\ell$ (with $\ell \leq k$) be F-terms, then

$$r_1 \cdot v(f_1) + \cdots + r_\ell \cdot v(f_\ell) + r_{\ell+1} \cdot a_{\ell+1} + \cdots + r_k \cdot a_k \tag{V.1}$$

(where each a_i is a Γ-variable or a Γ-constant) is a general Γ-term. Moreover we remark that such a Γ-term can be easily rewritten as an equal term

$$\frac{1}{\mathrm{N}} \left(v(f) + s_{\ell+1} \cdot a_{\ell+1} + \cdots + s_k \cdot a_k \right)$$

where $\mathrm{N}, s_j \in Z^{>0}$.

When we want to make computations inside the algebraic closure of some explicitly given valued field (K, V) we have to use the theory $\mathbf{ACVF}(K, V)$ where the elements of K and Γ_K are added as constants and the diagram of the valued field (K, V) is added as a set of axioms.

The theory $\mathbf{DOAG}_\infty$ of divisible ordered Abelian groups with top element ∞ admits quantifier elimination; hence it is sufficient to eliminate the F-quantifiers from an L-formula ϕ: we obtain an F-quantifier free L-formula ϕ' (most of the time, this formula has more Γ-quantifiers than ϕ), and we can conclude using the quantifier elimination of $\mathbf{DOAG}_\infty$.

This strategy allows us to get a new algorithmic proof of theorem 3.1, which is the topic of the third section of [Wei]: *The theory* $\mathbf{ACVF}(\mathrm{L})$ *admits quantifier elimination.*

3.1 Ultrametric Graphs

To prove theorem 3.1, we will need a lemma about *ultrametric graphs.* Let Γ be the divisible ordered Abelian group $\Gamma_{K^{\mathrm{ac}}}$. A graph of vertices $p_1, \ldots, p_n$ is a subset G of $\{p_1, \ldots, p_n\}^2$ such that if $(p_i, p_j) \in \mathrm{G}$, then $(p_j, p_i) \in \mathrm{G}$. If $(p_i, p_j) \in \mathrm{G}$, then it is an *edge* of G. This graph will be called *complete* if every pair (p_i, p_j) is an edge.

We consider graphs labelled by elements of $\Gamma \cup \{\infty\}$: to each edge (p_i, p_j) we associate an element $\varepsilon_{ij} \in \Gamma \cup \{\infty\}$, and we impose that $\varepsilon_{ij} = \varepsilon_{ji}$. Such a graph is called *ultrametric* if every triangle in it is an *ultrametric triangle*, that is, has two vertices labelled by the same element of Γ, and the third one is labelled by a greater or equal element. We can put $\varepsilon_{ii} = \infty$ as a convention, so that degenerated triangles are ultrametric.

If we set $t(\varepsilon_{ij}, \varepsilon_{ik}, \varepsilon_{jk})$ in the following way

$$t(\varepsilon_{ij}, \varepsilon_{ik}, \varepsilon_{jk}) \ : \ (\varepsilon_{ij} = \varepsilon_{ik}) \wedge (\varepsilon_{ij} \leq \varepsilon_{jk}) \,,$$

then

$$\mathrm{T}(\varepsilon_{ij}, \varepsilon_{ik}, \varepsilon_{jk}) \ : \ t(\varepsilon_{ij}, \varepsilon_{ik}, \varepsilon_{jk}) \vee t(\varepsilon_{ik}, \varepsilon_{jk}, \varepsilon_{ij}) \vee t(\varepsilon_{jk}, \varepsilon_{ij}, \varepsilon_{ik})$$

is the formula asserting that (p_i, p_j, p_k) is an ultrametric triangle inside the graph G.

The complete graph of vertices $p_1, \ldots, p_n$ with edges labelled by ε_{ij} is ultrametric if the following formula is true:

$$\bigwedge_{i<j<k} \mathrm{T}(\varepsilon_{ij}, \varepsilon_{ik}, \varepsilon_{jk}) \,.$$

In an algebraically closed valued field, let $a_1, \ldots, a_n$ be fixed elements. Let $\varepsilon_{ij} = v(a_i - a_j)$. Then the complete graph of vertices $a_1, \ldots, a_n$ and of edges (a_i, a_j) labelled by ε_{ij} is ultrametric.

Lemma 16 (Ultrametric graphs) *In any formal theory of valued fields implying that the residue field is infinite, the assertion*

$$\exists_{\mathrm{F}} x \bigwedge_{i=1,\ldots,n} v(x - a_i) = \beta_i$$

is equivalent to the formula expressing that the complete graph of vertices $a_1, \ldots, a_n$ and x, with edges (a_i, x) labelled by β_i, is ultrametric. The triangles (a_i, a_j, a_k) being ultrametric, this is equivalent to $\bigwedge_{i<j} \mathrm{T}_{ij}$ where T_{ij} is $\mathrm{T}(\varepsilon_{ij}, \beta_i, \beta_j)$.

Proof Let $\mathrm{S}_i(x)$ be the formula $v(x - a_i) = \beta_i$. We prove that

$$\left(\exists_{\mathrm{F}} x \bigwedge_i \mathrm{S}_i(x) \right) \Longleftrightarrow \bigwedge_{i<j} \mathrm{T}_{ij} \,.$$

The implication $\Longrightarrow$ is clear.

For the reverse implication $\Longleftarrow$, we first note that

$$(\mathrm{T}_{ij} \wedge (\beta_j < \beta_i)) \Longrightarrow \beta_j = \varepsilon_{ij} ,$$

and that

$$(\beta_j = \varepsilon_{ij} \wedge (\beta_j < \beta_i) \wedge \mathrm{S}_i(x)) \Longrightarrow \mathrm{S}_j(x) .$$

Thus we have the following implication:

$$(\mathrm{T}_{ij} \wedge (\beta_j < \beta_i) \wedge \mathrm{S}_i(x)) \Longrightarrow \mathrm{S}_j(x) . \tag{V.2}$$

Hence we can keep only the indices i for which β_i is maximal among $\beta_1, \dots, \beta_n$. Let $\beta = \max\{\beta_1, \dots, \beta_n\}$ and $\mathrm{I}_1 = \{i \in \{1, \dots, n\} : \beta_i = \beta\}$. Assume w.l.o.g. that $1 \in \mathrm{I}_1$. We have

$$\bigwedge_{i<j} \mathrm{T}_{ij} \wedge \bigwedge_{i\in \mathrm{I}_1} \mathrm{S}_i(x) \Longrightarrow \bigwedge_{1=1,\dots,n} \mathrm{S}_i(x)$$

Note that for $i, j \in \mathrm{I}_1$, T_{ij} is equivalent to $\varepsilon_{ij} \geq \beta$ and that $\mathrm{S}_i(x)$ is the formula $v(x - a_i) = \beta$. We show that

$$\bigwedge_{i<j,\ i,j\in \mathrm{I}_1} \mathrm{T}_{ij} \Longrightarrow \exists_{\mathrm{F}} x \bigwedge_{i\in \mathrm{I}_1} v(x - a_i) = \beta .$$

If $\beta = \infty$, we have $\mathrm{T}_{ij} \Longrightarrow (a_i = a_j)$ for all $i, j \in \mathrm{I}_1$, and in this case we take $x = a_i$ for any $i \in \mathrm{I}_1$. Now assume that $\beta < \infty$. If $\varepsilon_{ij} > \beta$, we obtain $(\mathrm{S}_i(x) \wedge \mathrm{T}_{ij}) \Longrightarrow \mathrm{S}_j(x)$. We make the following case distinction:

• If $\varepsilon_{ij} > \beta$ for all $i, j \in \mathrm{I}_1$ then $\left(\bigwedge_{i<j\ i,j\in \mathrm{I}_1} \mathrm{T}_{ij} \wedge \mathrm{S}_1(x)\right) \Longrightarrow \bigwedge_{i\in \mathrm{I}_1} \mathrm{S}_i(x)$. The formula $\exists_{\mathrm{F}} x\ \mathrm{S}_1(x)$ being always true, we have $\bigwedge_{i<j} \mathrm{T}_{ij} \Longrightarrow \exists_{\mathrm{F}} x\ \bigwedge_i \mathrm{S}_i(x)$.

• Else, we take in I_1 a subset I_2 which is maximal for the property that $\varepsilon_{ij} = \beta$ for all indices $i, j \in \mathrm{I}_2$. It suffices to show that $\bigwedge_{i<j\in \mathrm{I}_2} \mathrm{T}_{ij} \Longrightarrow \exists_{\mathrm{F}} x \bigwedge_{i\in \mathrm{I}_2} \mathrm{S}_i(x)$, since from the definition of I_2 we have

$$\left(\bigwedge_{i<j\ i,j\in \mathrm{I}_1} \mathrm{T}_{ij} \wedge \bigwedge_{i\in \mathrm{I}_2} \mathrm{S}_i(x)\right) \Longrightarrow \bigwedge_{i\in \mathrm{I}_1} \mathrm{S}_i(x) .$$

We can assume w.l.o.g. that $1 \in \mathrm{I}_2$. We denote the natural map from V^{ac} to $V^{\mathrm{ac}}/\mathcal{M}_{V^{\mathrm{ac}}} = \overline{K^{\mathrm{ac}}}$ by $x \mapsto \operatorname{res} x$. We fix $z \in K^{\mathrm{ac}}$ such that $v(z) = \beta$. The field $\overline{K^{\mathrm{ac}}}$ is infinite since it is algebraically closed; thus we can choose $x \in K^{\mathrm{ac}}$ such that $v(x - a_1) = \beta$ and

$$\bigwedge_{i\in \mathrm{I}_2\setminus\{1\}} \operatorname{res}\left(\frac{x - a_1}{z}\right) \neq \operatorname{res}\left(\frac{a_i - a_1}{z}\right) .$$

This x verifies $v(x - a_i) = \beta$, for all $i \in \mathrm{I}_2 \setminus \{1\}$. This concludes the proof. □

Remark 17 We can give a geometric description of the set

$$\mathrm{S} = \{x \in K^{\mathrm{ac}} : \bigwedge_{i=1,\dots,n} v(x - a_i) = \beta_i\} .$$

We use the notations of the proof. Set $\mathrm{C}_\beta(a) = \{x : v(x-a) = \beta\}$. We have

$$\mathrm{S} = \bigcap_{i=1,\dots,n} \mathrm{C}_{\beta_i}(a_i) = \bigcap_{i\in \mathrm{I}_1} \mathrm{C}_\beta(a_i)\,.$$

If $\beta = \infty$, S is reduced to one element in K. Now suppose $\beta < \infty$. If $\varepsilon_{ij} > \beta$ for all $i, j \in \mathrm{I}_1$, then $\mathrm{S} = \mathrm{C}_{\beta_i}(a_i)$ for all $i \in \mathrm{I}_1$. If for some $i, j \in \mathrm{I}_1$, $\varepsilon_{ij} = \beta$, take I_2 as in the proof. We have $\mathrm{S} = \bigcap_{i\in\mathrm{I}_2} \mathrm{C}_\beta(a_i)$. Suppose that $1 \in \mathrm{I}_2$. The set $\mathrm{C}_\beta(a_1)$ is an infinite disjoint union of open disks $\mathrm{B}^\circ_\beta(\zeta) = \{x : v(x-\zeta) > \beta\}$, where $v(\zeta - a_1) = \beta$. There is a bijection between the disks $\mathrm{B}^\circ_\beta(\zeta)$ and the residue field of K^{ac}, given by

$$\mathrm{B}^\circ_\beta(\zeta) \mapsto f(\zeta) = \mathrm{r}es\, \frac{\zeta - a_1}{z}\,\cdot$$

We have the following equality:

$$\mathrm{S} = \bigcap_{i\in\mathrm{I}_2} \mathrm{C}_{\beta_i}(a_i) = \bigcup_{\substack{v(\zeta-a_1)=\beta \\ \forall i\in\mathrm{I}_2\setminus\{1\}\ f(\zeta)\neq f(a_i)}} \mathrm{B}^\circ_\beta(\zeta)\,.$$

This union is nonempty because there are infinitely many values possible for $f(\zeta)$, but only finitely many for $f(a_i)$.

Remark 18 Another formulation of lemma 16 is that we have a quantifier elimination for *linear formulas* in $\mathbf{ACVF}(\mathrm{L})$: given a formula

$$\exists_{\mathrm{F}} x\ \bigwedge_i v(x - x_i) = \beta_i$$

we put $\varepsilon_{ij} = v(x_i - x_j)$, and the above formula is equivalent to

$$\bigwedge_{i<j} \mathrm{T}(\varepsilon_{ij}, \beta_i, \beta_j)\,.$$

An easy consequence is the following lemma:

Lemma 19 *Take any complete ultrametric graph of vertices $p_1, \dots, p_n$, with edges labelled by $\varepsilon_{ij} \in \Gamma \cup \{\infty\}$, and elements $x_1, \dots, x_l \in K^{\mathrm{ac}}$ (with $l < n$), such that $v(x_i - x_j) = \varepsilon_{ij}$ for all $i, j \le l$. Then there exist $x_{l+1}, \dots, x_n \in K^{\mathrm{ac}}$ such that $v(x_i - x_j) = \varepsilon_{ij}$ for all i, j.*

3.2 Univariate existential decision procedure

We are going to prove that existential problems in a single variable x can be solved in $(K^{\mathrm{ac}}, V^{\mathrm{ac}})$.

Definition 20 *We define* univariate F-conditions *by*

- **(i)** *For any $\mathrm{P}(\mathrm{X}) \in K[\mathrm{X}]$, the condition $\Phi(x)\ :\ \mathrm{P}(x) = 0$ is a univariate* F*-condition.*

(ii) *Take any* $\gamma, \delta \in \Gamma_K$, $q, r \in Q^{>0}$, *and any* $\mathrm{P(X)}, \mathrm{Q(X)} \in K[\mathrm{X}]$. *The condition* $\Phi(x)\ :\ v(\mathrm{P}(x)) + q \cdot \gamma \ \square\ v(\mathrm{Q}(x)) + r \cdot \delta$, *where* $\square$ *is either* $=$ *or* $<$, *is a univariate* F*-condition.*

(iii) *Take any* $\mathrm{P(X)} \in K[\mathrm{X}]$. *The condition* $\Phi(x)\ :\ v(\mathrm{P}(x)) < \infty$ *is a univariate* F*-condition.*

(iv) *If* $\Phi(x), \Psi(x)$ *are univariate* F*-conditions, then* $\Phi(x) \wedge \Psi(x)$ *and* $\Phi(x) \vee \Psi(x)$ *are univariate* F*-conditions.*

Conditions of the form **(i)**, **(ii)** *and* **(iii)** *are called* atomic F-conditions.

Definition 21 *We define* Γ-conditions *by*

(i) *For any* $\delta \in \Gamma_K \cup \{\infty\}$, $q_1, \ldots, q_n \in Q^{>0}$, $r \in \{1, n\}$ *the condition* $\Phi(\bar{a})\ :\ q_1 \cdot a_1 + \cdots + q_r \cdot a_r \ \square\ q_{r+1} \cdot a_{r+1} + \cdots + q_n \cdot a_n + \delta$, *where* $\square$ *is either* $=$, $>$ *or* $<$, *is a* Γ*-condition on* $\bar{a}$.

(ii) *If* $\Phi(\bar{a}), \Psi(\bar{a})$ *are* Γ*-conditions on* $\bar{a}$, *then so are* $\Phi(\bar{a}) \wedge \Psi(\bar{a})$ *and* $\Phi(\bar{a}) \vee \Psi(\bar{a})$.

Conditions of the form **(i)** *are called* atomic Γ-conditions.

It is well known that such conditions are equivalent to some condition of the following form, which is by definition a *disjunctive normal form*:

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m_i} \Phi_{ij}\ ,$$

where the Φ_{ij} are atomic conditions. Moreover, given any univariate condition $\Phi(x)$, there is an algorithm which computes a disjunctive normal form for $\Phi(x)$.

We say that $\xi \in K^{\mathrm{ac}}$ satisfies a univariate F-condition $\Phi(x)$ if $\Phi(\xi)$ holds in K^{ac}, and that $\alpha_1, \ldots, \alpha_n \in \Gamma_{K^{\mathrm{ac}}}$ satisfy a Γ-condition $\Phi(\bar{a})$ if $\Phi(\bar{\alpha})$ holds in $\Gamma_{K^{\mathrm{ac}}}$.

We recall the following result without proof.

Proposition 22 (Existential Decision Procedure in DOAG$_\infty$) *Let* $\Phi(\bar{a})$ *be a* Γ*-condition. Then there is an algorithm to decide whether there are some* $\alpha_1, \ldots, \alpha_n \in \Gamma_{K^{\mathrm{ac}}}$ *satisfying* $\Phi(\bar{a})$ *or not. If the answer is yes, the algorithm provides such a n-tuple. We call it a* witness *of the condition.*

We now prove the following theorem:

Theorem 3.2 Univariate Existential Decision Procedure in ACVF *Let* $\Phi(x)$ *be a univariate condition. Then we have an algorithm to decide whether there is some* $\xi \in K^{\mathrm{ac}}$ *satisfying* $\Phi(x)$ *or not. If the answer is yes, the algorithm gives a description of a witness* $\xi \in K^{\mathrm{ac}}$ *such that* $\Phi(\xi)$ *holds; the algorithm decides whether* ξ *is unique or not, and if this is the case then* ξ *is in* K^{h}.

Proof We give an existential decision procedure for a conjunction

$$\Phi(x)\ :\ \bigwedge_{i=1}^{n} \Phi_i(x)$$

where the Φ_i's are atomic conditions. It suffices to use it several times to obtain an existential decision procedure for a univariate condition put in a disjunctive normal form, and hence for every univariate condition.

• **First case:** One of the $\Phi_i(x)$ (let's say $\Phi_1(x)$) is of the form $\mathrm{P}(x) = 0$. Let $k = \deg \mathrm{P}$, and $\xi_1, \ldots, \xi_k$ be the roots of P. Let $\mathrm{Q}_1(x), \ldots, \mathrm{Q}_r(x) \in \mathrm{K}[x]$ be the polynomials appearing in the other $\Phi_i(x)$'s. We can use **SimVal** to obtain the multiset of $(r+1)$-tuples of values $[(v(\xi_i), v(\mathrm{Q}_1(\xi_i)), \ldots, v(\mathrm{Q}_r(\xi_i)))]_{i=1,\ldots,k}$.

It suffices now to check, for each $(\nu, \nu_1, \ldots, \nu_r)$ in this list, whether the conditions $\Phi_1, \ldots, \Phi_n$ are verified:

- for a Φ_k of the form $\mathrm{Q}_i(x) = 0$, test whether $\nu_i = \infty$,
- for a Φ_k of the form $v(\mathrm{Q}_i(x)) + q \cdot \gamma \ \Box \ v(\mathrm{Q}_j(x)) + r \cdot \delta$, test whether $\nu_i + q \cdot \gamma \ \Box \ \nu_j + r \cdot \delta$ (where $\Box$ is either $=$, $>$ or $<$).
- for a Φ_k of the form $v(\mathrm{Q}_i(x)) < \infty$, test whether $\nu_i < \infty$.

If there are no $(r+1)$-tuples in this multiset such that these conditions are verified, then there is no $\xi \in K^{\mathrm{ac}}$ satisfying $\Phi(x)$; if there are $m \leq k$ of these multisets satisfying these conditions, we know that m of the roots of P can be chosen for ξ.

If $m = 1$, then remark 11 shows that the corresponding root of P is in K^{h}.

• **Second case:** Assume now that there is no condition $\Phi_i(x)$ of the form $\mathrm{P}(x) = 0$ among the $\Phi_i(x)$. For each i, let $\mathrm{P}_i(x)$ and $\mathrm{Q}_i(x)$ be the polynomials appearing in atomic formulas $\Phi_i\ :\ v(\mathrm{P}_i(x)) + q_i \cdot \gamma_i \ \Box_i \ v(\mathrm{Q}_i(x)) + r_i \cdot \delta_i$ (where $\Box_i$ is either $=$, $>$ or $<$), and $\Phi_i\ :\ v(\mathrm{P}_i(x)) < \infty$ (in that case, set $\mathrm{Q}_i = 1$, $q_i = r_1 = 1$, $\gamma_i = 0$ and $\delta_i = \infty$ for the sequel).

We construct the following formulas:

$$\Phi'(x, \bar{c}, \bar{d})\ :\ \left(\bigwedge_{i=1}^{n} v(\mathrm{P}_i(x)) = c_i \wedge v(\mathrm{Q}_i(x)) = d_i\right)$$

$$\Phi''(\bar{c}, \bar{d})\ :\ \left(\bigwedge_{i=1}^{n} c_i + q_i \cdot \gamma_i \ \Box_i \ d_i + r_i \cdot \delta_i\right) .$$

The variables $\bar{c} = c_1, \ldots, c_n$ and $\bar{d} = d_1, \ldots, d_n$ stand for elements of $\Gamma_{K^{\mathrm{ac}}}$. We have

$$\exists x \in K^{\mathrm{ac}}\ \Phi(x) \Longleftrightarrow \exists \bar{c}, \bar{d} \in \Gamma_{K^{\mathrm{ac}}}\ \exists x \in K^{\mathrm{ac}}\ \Phi'(x, \bar{c}, \bar{d}) \wedge \Phi''(\bar{c}, \bar{d}) .$$

Consider a problem of the following form:

$$\Psi(x, \bar{b})\ :\ \exists x \in K^{\mathrm{ac}}\ \bigwedge_{i=1}^{m} v(\mathrm{R}_i(x)) = b_i ,$$

where each $\mathrm{R}_i(\mathrm{X})$ is a polynomial of $K[x]$, and the b_i's are indeterminates.

We introduce all the roots $r_1, \dots, r_\mathrm{N}$ of the polynomials $\mathrm{R}_1, \dots, \mathrm{R}_m$. We can compute N with the algorithm **GraphRoots**, as well as the values $\varepsilon_{ij} = v(r_i - r_j)$, for all i, j, and the multiplicity μ_{jk} of r_k as a root of R_j. We have an equivalence

$$\Psi(x, \bar{b}) \Longleftrightarrow \exists\, x \in K^{\mathrm{ac}}\ \exists a_1 \cdots a_\mathrm{N} \in \Gamma_{K^{\mathrm{ac}}}\ \bigwedge_{i=1}^{\mathrm{N}} v(x - r_i) = a_i \wedge \Psi_1(\bar{a}, \bar{b})\ ,$$

where Ψ_1 is a conjuction of formulas of the form $b_j = \sum_k \mu_{jk} \cdot a_k$.

From the ultrametric graph lemma we have

$$\exists x \in K^{\mathrm{ac}}\ \bigwedge_{i=1}^{\mathrm{N}} v(x - r_i) = a_i \Longleftrightarrow \bigwedge_{i<j} \mathrm{T}(\varepsilon_{ij}, a_i, a_j)\ .$$

Hence we can write that $\Psi(x, \bar{b})$ is equivalent to a problem in $\Gamma_{K^{\mathrm{ac}}}$:

$$\Psi(x, \bar{b}) \Longleftrightarrow \exists \bar{a} \in \Gamma_{K^{\mathrm{ac}}}\ \bigwedge_{i<j} \mathrm{T}(\varepsilon_{ij}, a_i, a_j) \wedge \Psi_1(\bar{a}, \bar{b})\ .$$

Now we can do that for $\Psi = \Phi'$. We obtain that $\exists x \in K^{\mathrm{ac}} \Phi'(x, \bar{c}, \bar{d})$ is equivalent to $\exists \bar{a} \in \Gamma_{K^{\mathrm{ac}}}\ \Phi'''(\bar{a}, \bar{c}, \bar{d})$, where $\Phi'''(\bar{a}, \bar{c}, \bar{d})$ is a Γ-condition. We have proved

$$\exists x \in K^{\mathrm{ac}}\ \Phi(x) \Longleftrightarrow \exists \bar{a}, \bar{c}, \bar{d} \in \Gamma_{K^{\mathrm{ac}}}\ \Phi'''(\bar{a}, \bar{c}, \bar{d}) \wedge \Phi''(\bar{c}, \bar{d})\ .$$

Now we can apply the existential decision procedure for $\mathbf{DOAG}_\infty$ to this formula. If there is no solution, then there is no $\xi \in K^{\mathrm{ac}}$ satisfying $\Phi(x)$. Is there is a solution, we can use it and lemma 16 to describe an element $\xi \in K^{\mathrm{ac}}$ satisfying $\Phi(x)$. Of course, there is no unicity in that case. □

Remark 23 The first case of our proof can in fact be treated as a particular case of the second, replacing $\mathrm{P}(x) = 0$ by $v(\mathrm{P}(x)) = \infty$: in that case the existential decision procedure in $\mathbf{DOAG}_\infty$ will give $a_i = \infty$ for some i, and then $v(x - r_i) = \infty$ implies $\xi = r_i$. However, the proof is clearer with this distinction. Moreover, it would be less easy to show that in the case of unicity, the witness is in K^{h}.

3.3 Quantifier Elimination

Quantifier elimination algorithms come very often from existential decision procedures in the one variable case. If such a decision procedure is "uniform" it can be performed "with parameters". This gives a good way for eliminating the quantifier in a formula with only one existential quantifier. For the real algebraic case see e.g. [BCR] chapter 1. We do this job in the present section for the case of algebraically closed valued fields.

Definition 24 *Take $n \in N$, and denote by $\bar{y}$ an n-tuple $(y_1, \dots, y_n)$ of* F-*variables. Let $\mathrm{C}_1(\bar{y}), \dots, \mathrm{C}_m(\bar{y})$ be atomic* L-*formulas with $y_1, \dots, y_n$ as sole free variables.*

1. *We say that* $\bigvee_i \mathrm{C}_i(\bar{y})$ *is a* finite exclusive disjunction *if*

$$\forall_{\mathrm{F}} \bar{y} \quad \bigvee_{i=1}^{m} \mathrm{C}_i(\bar{y}) \ \wedge \ \bigwedge_{i \neq j} \neg \mathrm{C}_i(\bar{y}) \vee \neg \mathrm{C}_j(\bar{y})$$

holds. In that case we write

$$\mathfrak{C}_i = \{\bar{y} \in K^n : \mathrm{C}_i(\bar{y})\} \ .$$

Then K^n *is the disjoint union of* $\mathfrak{C}_1, \ldots, \mathfrak{C}_m$. *The family* $\mathfrak{C}_i$ *is a* definable partition of the space K^n. *Note that we allow that some* $\mathfrak{C}_i$ *may be empty.*

2. *Let* $\mathrm{D}_{ij}(\bar{y})$, *for* $i = 1, \ldots, m$ *and* $j = 1, \ldots, \ell_i$, *be atomic* L*-formulas such that* $\bigvee_{ij} \mathrm{D}_{ij}(\bar{y})$ *is a finite exclusive disjunction. We say that* $\bigvee_{ij} \mathrm{D}_{ij}$ *is a refinement of* $\bigvee_i \mathrm{C}_i$ *if for all* i, *we have*

$$\mathrm{C}_i(\bar{y}) \Longleftrightarrow \bigvee_{j=1}^{\ell_i} \mathrm{D}_{ij}(\bar{y}) \ ,$$

or, equivalently

$$\mathfrak{C}_i = \bigcup_{j=1}^{\ell_i} \mathfrak{D}_{ij} \ ,$$

where $\mathfrak{D}_{ij} = \{\bar{y} \in K^n : \mathrm{D}_{ij}(\bar{y})\}$. *Note that this union is a disjoint union.*

We denote by $\bar{\mathrm{Y}}$ a n-tuple of indeterminates $\mathrm{Y}_1, \ldots, \mathrm{Y}_n$. The ring $K\left[\bar{\mathrm{Y}}\right]$ is $K[\mathrm{Y}_1, \ldots, \mathrm{Y}_n]$. We can apply the algorithms given in the previous section to polynomials with parameters. Consider $\mathrm{P}(\bar{\mathrm{Y}}, \mathrm{X}) \in K\left[\bar{\mathrm{Y}}, \mathrm{X}\right]$ as a polynomial in X with parameters $\bar{\mathrm{Y}}$.

Proposition 25 (Algorithms with parameters)

1. *The Newton Polygon Algorithm applied to* P *provides*

(i) *a finite exclusive disjunction* $\bigvee_i \mathrm{C}_i(\bar{y})$,

(ii) *for each* i, *an integer* k_i *and a multiset* $[t_1(\bar{y}), \ldots, t_{k_i}(\bar{y})]$, *where each* $t_j(\bar{y})$ *is a* L_Γ*-term,*

such that for all $\bar{y} \in \mathfrak{C}_i$, $k_i = \deg_{\mathrm{X}} \mathrm{P}(\bar{y}, \mathrm{X})$, *and if* $[\xi_1, \ldots \xi_{k_i}]$ *denotes the multiset of roots of* $\mathrm{P}(\bar{y}, \mathrm{X})$, *then* $[t_1(\bar{y}), \ldots, t_{k_i}(\bar{y})]$ *is* $[v(\xi_1), \ldots, v(\xi_{k_i})]$. *In other words, in each case of the above exclusive disjunction, the algorithm computes the values of the roots of* $\mathrm{P}(\bar{y}, \mathrm{X})$.

2. *Keep the notation of the previous statement. Let* $\mathrm{Q}_1, \ldots, \mathrm{Q}_r \in K\left[\bar{\mathrm{Y}}, \mathrm{X}\right]$ *be polynomials in* X *with parameters* $\bar{\mathrm{Y}}$. *The algorithm* **SimVal** *applied to* $\mathrm{P}, \mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *provides*

(i) *a refinement* $\bigvee_{ij} \mathrm{D}_{ij}(\bar{y})$ *of* $\bigvee_i \mathrm{C}_i(\bar{y})$,

(ii) *for each case* i, j *(with* $j \in \{1, \ldots, \ell_i\}$*) a multiset of* $(r+1)$*-tuples of* L_Γ*-terms* $\left[\left(t_s(\bar{y}), u_s^1(\bar{y}), \ldots, u_s^r(\bar{y})\right)\right]_{s=1,\ldots,k_i}$, *such that for all* $\bar{y} \in \mathfrak{D}_{ij}$*, if* $[\xi_1, \dots \xi_{k_i}]$ *is the multiset of roots of* $\mathrm{P}(\bar{y}, \mathrm{X})$*, then* $\left[\left(t_s(\bar{y}), u_s^1(\bar{y}), \dots, u_s^r(\bar{y})\right)\right]_{s=1,\dots,k_i}$ *is* $[(v(\xi_s), v(\mathrm{Q}_1(\xi_s), \dots, v(\mathrm{Q}_r(\xi_s)))]_{s=1,\dots,k_i}$.

3. *Set* $\mathrm{P}_1, \dots, \mathrm{P}_s \in K\left[\bar{\mathrm{Y}}, \mathrm{X}\right]$*. The algorithm* **GraphRoots** *applied to* $\mathrm{P}_1, \dots, \mathrm{P}_s$ *provides*

- **(i)** *a finite exclusive disjunction* $\bigvee_i \mathrm{C}_i(\bar{y})$*,*
- **(ii)** *for each* i*, an integer* N_i*, a finite family*

$$\left((\mu_{jk})_{j\in[1,s],k\in[1,\mathrm{N}_i]}, (t_{k,\ell}(\bar{y}))_{1\le j<\ell\le \mathrm{N}}\right)$$

where the μ_{jk} *are integers and the* $t_{k,\ell}(\bar{y})$ *are* L_Γ *terms,*

such that for all $\bar{y} \in \mathfrak{C}_i$*,* N_i *is the number of roots of* $\mathrm{P}_1 \cdot \ldots \cdot \mathrm{P}_s$*, and for some ordering* $(\xi_1, \dots, \xi_{\mathrm{N}_i})$ *of these roots,* μ_{jk} *is the multiplicity of* ξ_k *as a root of* P_j*, and* $t_{k,\ell}(\bar{y})$ *is* $v(\xi_k - \xi_\ell)$*.*

Proof For the first statement, write $\mathrm{P}(\bar{\mathrm{Y}}, \mathrm{X}) = q_n(\bar{y})\cdot\mathrm{X}^n + \cdots + q_0(\bar{y})$. Consider the exclusive disjunction

$$\left(q_0(\bar{y}) = \ldots = q_n(\bar{y}) = 0\right) \vee \bigvee_{i=0}^{n} \left(v(q_i(\bar{y})) < \infty \wedge \bigwedge_{j=i+1}^{n} q_{n-j}(\bar{y}) = 0\right).$$

In each case of this disjunction the degree in X of $\mathrm{P}(\bar{y}, \mathrm{X})$ is fixed. We are going to refine it to obtain the desired disjunction. Apply the Newton Polygon Algorithm in any fixed case of this disjunction: its result depends naturally on a new disjunction, each case of it expressing a different shape for the Newton Polygon of P. More precisely, if $m > 0$ is $\deg_{\mathrm{X}} \mathrm{P}(\bar{y}, \mathrm{X})$, for each $\ell \le m + 1$ and each ℓ-tuple $(k_1, \dots, k_\ell)$ of non-negative integers such that $0 = k_1 < \cdots < k_\ell = m$, we can write a formula $\mathrm{C}_{m,\ell,k_1,\dots,k_\ell}(\bar{y})$ expressing that $(k_1, v(q_{k_1}(\bar{y}))), \dots, (k_\ell, v(q_{k_ell}(\bar{y})))$ are the consecutive vertices of the Newton Polygon of P. In each fixed case $\mathrm{C}_{m,\ell,k_1,\dots,k_\ell}$, the values of the roots are the L_Γ-terms $\frac{1}{k_{i+1}-k_i}(v(q_{k_i}(\bar{y})) - v(q_{k_{i+1}}(\bar{y})))$.

Example: Set $\mathrm{R}(\bar{\mathrm{Y}}, \mathrm{X}) = a(\bar{\mathrm{Y}})\mathrm{X}^2 + b(\bar{\mathrm{Y}})\mathrm{X} + c(\bar{\mathrm{Y}})$; we omit the parameters $\bar{\mathrm{Y}}$ in the sequel: a stands for $a(\bar{\mathrm{Y}})$, and so on.

- If $v(a) < \infty$, and $2v(b) \ge v(a) + v(c)$, then $\xi_1, \xi_2 \in K^{\mathrm{ac}}$, the roots of R considered as a polynomial in X, have both value $\frac{1}{2}(v(c) - v(a))$.
- If $v(a) < \infty$, and $2v(b) < v(a) + v(c)$, then there is one root of value $v(b) - v(a)$ and the other of value $v(c) - v(b)$.
- If $a = 0$ and $v(b) < \infty$, then there is a single root, of value $v(c) - v(b)$.
- If $a = 0$ and $b = 0$ and $v(c) < \infty$, then there is no root.
- If $a = b = c = 0$, then $\forall x \in K^{\mathrm{ac}}$, $\mathrm{R}(\bar{y}, x) = 0$.

Now turn to the second statement. The algorithm **SimVal** applies the Newton Polygon Algorithm to P: this is our first disjunction. Then it computes some Tschirnhausen transformation of P. The degree of P being fixed in each case of the disjunction, this can be done without refining it. The results of this computations are new polynomials in $\mathrm{K}\left[\bar{\mathrm{Y}}, \mathrm{X}\right]$. We apply the Newton Polygon Algorithm to each of these polynomials, after refining the disjunction. We obtain some lists of L_Γ-terms, from which we can construct the list we want, under a few conditions to eliminate "bad coincidences" (cf. 10); these conditions give rise to a new refinement of the disjunction.

For the third statement, just note that **GraphRoots** uses **SimVal** iteratedly; then the result comes from the second statement. □

Now we are able to prove theorem 3.1

Proof [Proof of theorem 3.1] We recall that there are classical and easy arguments ([Wei]) showing that it suffices to eliminate an F-quantifier $\exists_{\mathrm{F}} x$ in a formula such that $\exists_{\mathrm{F}} x \ \bigwedge_{k=1,\ldots,n} \Phi_k(\bar{y}, x)$, where each $\Phi_k(\bar{y}, x)$ is either an atomic F-formula like $\mathrm{P}(\bar{y}, x) = 0$ with $\mathrm{P}(\bar{y}, x) \in Z[\bar{y}, x]$, or an atomic Γ-formula. Note that an atomic F-formula $(\mathrm{P}(\bar{y}, x) \neq 0)$ can be replaced by the Γ-formula $v(\mathrm{P}(\bar{y}, x)) < \infty$. So we are done if we prove the following proposition. □

Proposition 26 *There is an algorithmic procedure that computes, from a formula* $\exists_{\mathrm{F}} x \ \bigwedge_{k=1,\ldots,n} \Phi_k(\bar{y}, x)$, *(where each* $\Phi_k(\bar{y}, x)$ *is either an atomic* F*-formula like* $\mathrm{P}(\bar{y}, x) = 0$ *with* $\mathrm{P}(\bar{y}, x) \in Z[\bar{y}, x]$, *or an atomic* Γ*-formula), an equivalent quantifier free formula* $\Psi(\bar{y})$.

A geometric form of this proposition is the following one (for the real algebraic case see e.g. [BCR] theorem 2.2.1).

Proposition 27 *Let L be an algebraically closed valued field, and K be a subfield. Let us call a* basic v-constructible set defined over K *inside* L^n *a set defined as* $\{\bar{x} \in L^n : \Phi(\bar{x})\}$ *where* $\Phi(\bar{x})$ *is either an atomic* F*-formula like* $\mathrm{P}(\bar{x}) = 0$ *with* $\mathrm{P}(\bar{x}) \in K[\bar{x}]$, *or an atomic* Γ*-formula (which is built by using only constants in* K *and* $v(K)$*). Let us call a* v-constructible set defined over K *inside* L^n *any boolean combination of basic* v*-constructible sets defined over* K. *Then the canonical projection from* L^n *onto* L^{n-1} *maps any* v*-constructible set* S *defined over* K *in another one* $\pi(\mathrm{S})$. *Moreover, there is an algorithmic procedure that uses only computations inside* K *for getting a description of* $\pi(\mathrm{S})$ *from a description of* S.

Proof [Proof of proposition 26]

We can apply our univariate decision procedure (theorem 3.2) with parameters in order to eliminate x. This procedure uses **SimVal** and **GraphRoots** with parameters: it will provide an exclusive disjunction $\bigvee_i \mathrm{C}_i(\bar{y})$, and in each case of this exclusive disjunction, a formula $\Psi_i(\bar{y})$ without F-quantifiers (but perhaps with some new Γ-quantifiers if for $\bar{y} \in \mathfrak{C}_i$ we are in the second case of the proof of 3.2) such that

$$\forall \bar{y} \in \mathfrak{C}_i,\ \exists_{\mathrm{F}} x \bigwedge_{k=1,\ldots,n} \Phi_k(\bar{y}, x) \Longleftrightarrow \Psi_i(\bar{y})\,.$$

Thus we have

$$\exists_{\mathrm{F}} x \bigwedge_{k=1,\ldots,n} \Phi_k(\bar{y}, x) \Longleftrightarrow \bigvee_i \mathrm{C}_i(\bar{y}) \wedge \Psi_i(\bar{y})\,.$$

This concludes the proof. □

Remark 28 The strategy used in [Wei] was first to give an elimination for linear formulas, and then a procedure which decreases the degrees of polynomials. There was no geometric ideas at first sight, although there may be a geometric content hidden in the proof. We think that the two procedures are in fact different.

When we use this quantifier elimination with the theory $\mathbf{ACVF}(K, V)$ we get as a particular case a decision procedure for a closed formula with coefficients in a valued field K given as in the introduction.

Theorem 3.3 *Take a formula*

$$\Theta(\bar{y})\ :\ \mathrm{Q}^1_{\mathrm{F}} x_1 \ldots \mathrm{Q}^n_{\mathrm{F}} x_n\ \Phi(\bar{\alpha}, \bar{y}, \bar{x})$$

where each $\mathrm{Q}^i_{\mathrm{F}}$ is $\forall_{\mathrm{F}}$ or $\exists_{\mathrm{F}}$ and $\bar{\alpha} = \alpha_1, \ldots, \alpha_m$ are elements of K. We have an algorithm for computing a quantifier free formula $\Psi(\bar{y})$ equivalent to $\Theta(\bar{y})$. As a particular case, when $\bar{y}$ is the empty sequence, we can decide whether the formula $\Theta(\bar{y})$ is true in K^{ac} or not. Moreover, if the formula is purely existential, i.e. $\mathrm{Q}^1_{\mathrm{F}}, \ldots, \mathrm{Q}^n_{\mathrm{F}}$ are existential quantifiers $\exists_{\mathrm{F}}$, then the algorithm provides a witness $\bar{\xi} \in (K^{\mathrm{ac}})^n$ such that $\Phi(\bar{\xi})$ is true. If we have a result of unicity such as

$$\forall_{\mathrm{F}} \bar{x}, \bar{y}\ (\Phi(\bar{\alpha}, \bar{x}) \wedge (\Phi(\bar{\alpha}, \bar{y}) \Longrightarrow \bar{y} = \bar{x})\ ,$$

then this witness is in $(K^{\mathrm{h}})^n$.

Proof Let us explain how we get the test point. We apply the quantifier elimination procedure to

$$\mathrm{Q}^1_{\mathrm{F}} x_1 \ldots \mathrm{Q}^n_{\mathrm{F}} x_n\ \Phi(\bar{a}, \bar{x})$$

obtained after replacement of each α_i by a new indeterminate a_i. The result is a quantifier-free formula $\Psi(\bar{a})$, such that

$$\mathrm{Q}^1_{\mathrm{F}} x_1 \ldots \mathrm{Q}^n_{\mathrm{F}} x_n\ \Phi(\bar{a}, \bar{x}) \Longleftrightarrow \Psi(\bar{a})\,.$$

It suffices to test whether $\Psi(\bar{\alpha})$ is true or not.

If all quantifiers $\mathrm{Q}^i_{\mathrm{F}}$ are existential, we can find formulas $\Psi_k(\bar{a}, x_1, \ldots, x_k)$ for $k = 1$ to $n - 1$, such that

$$\begin{array}{cc}
 & \exists_{\mathrm{F}} x_1 \ldots \exists_{\mathrm{F}} x_n\ \Phi(\bar{a}, x_1, \ldots, x_n) \\
\Longleftrightarrow & \exists_{\mathrm{F}} x_1 \ldots \exists_{\mathrm{F}} x_{n-1}\ \Psi_{n-1}(\bar{a}, x_1, \ldots, x_{n-1}) \\
\vdots & \vdots \\
\Longleftrightarrow & \exists_{\mathrm{F}} x_1\ \Psi_1(\bar{a}, x_1) \\
\Longleftrightarrow & \Psi(\bar{a})
\end{array}$$

If $\Psi(\bar{\alpha})$ is true, applying the decision procedure of theorem 3.2 to the formula $\exists_{\mathrm{F}} x_1\ \Psi_1(\bar{\alpha}, x_1)$, we find $\xi_1 \in K^{\mathrm{ac}}$ such that $\Psi_1(\bar{\alpha}, \xi_1)$ holds; now we apply again the decision procedure to $\exists_{\mathrm{F}} x_2\ \Psi_2(\bar{\alpha}, \xi_1, x_2)$ and we find $\xi_2 \in K^{\mathrm{ac}}$ such that $\Psi_2(\bar{\alpha}, \xi_1, \xi_2)$ holds, and so on. And last we find $\xi_1, \ldots, \xi_n \in K^{\mathrm{ac}}$ such that $\Phi(\bar{\alpha}, \xi_1, \ldots, \xi_n)$ holds.

If the n-tuple $(\xi_1, \ldots, \xi_n)$ satisfying $\Phi(\bar{\alpha}, x_1, \ldots, x_n)$ is unique, then ξ_1 satisfying $\Psi_1(\bar{\alpha}, x_1)$ is unique and theorem 3.2 shows that $\xi_1 \in K^{\mathrm{h}}$. Repeating this argument n times, we conclude that, in this case, $\xi_1, \ldots, \xi_n \in K^{\mathrm{h}}$. $\square$

BIBLIOGRAPHIE

[AL] William W. ADAMS, Philippe LOUSTAUNAU. (1994). *An introduction to Groebner bases.* Vol. 3 de Graduate Studies in Mathematics, Amer. Math. Soc.

[AP] Victor ALEXANDRU et Nicolae POPESCU. Sur une classe de prolongements à K(X) d'une valuation sur un corps K, *Rev. Roumaine Math. Pures Appl.*, **33**(5): 393–400, 1988.

[APZ] Victor ALEXANDRU, Nicolae POPESCU et Alexandru ZAHARESCU. Minimal pairs of definition of a residual transcendental extension of a valuation, *J. Math. Kyoto Univ.* **30**(2): 207–225, 1990.

[BW] Thomas BECKER et Volker WEISPFENNING. (1993). *Groebner bases: a computational approach to commutative algebra.* Graduate Texts in Mathematics. Springer-Verlag, Berlin-Heidelberg-New York.

[BCR] Jacek BOCHNAK, Michel COSTE et Marie-Françoise ROY. (1987) Géométrie algébrique réelle. Springer-Verlag, Berlin-Heidelberg-New York.

[Boul] François BOULIER. (1994) *Étude et implantation de quelques algorithmes en algèbre différentielle.* Thèse d'informatique à université des sciences et technologies de Lille.

[BLOP] François BOULIER, Daniel LAZARD, François OLLIVIER et Michel PETITOT. (1998) *Computing representations for radical of finitely generated differentials ideals.* Publication interne IT-306 du LIFL.

[Bour] Nicolas BOURBAKI. (1964). *Algèbre commutative,* Ch. VI. Hermann, Paris.

[Buc$_1$] Bruno BUCHBERGER. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* Dissertation, Innsbruck Universität.

[Buc$_2$] Bruno BUCHBERGER. (1970). Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. Vol. 4 de *Aequationes Math.*, pages 374-383.

[CorLas] René CORI et Daniel LASCAR. (1993). *Logique mathématique. Cours et exercices.* (deux tomes). Masson, Paris.

[CoqLom$_1$] Thierry COQUAND et Henri LOMBARDI. (2001). *Constructions cachées en algèbre abstraite (3) : Dimension de Krull, Going Up, Going Down.* (Soumis).

[CoqLom$_2$] Thierry COQUAND et Henri LOMBARDI. (2001). *Krull's Principal Ideal Theorem.* (Soumis).

[CP] Thierry COQUAND et Henrik PERSSON. (1999). Gröbner bases in type theory. *Types for proofs and programs.* Vol 1657 de Lect. Notes Comput. Sci. pages 33-46. Springer-Verlag, Berlin-Heidelberg-New York.

[CLR] Michel COSTE, Henri LOMBARDI et Marie-Françoise ROY. (2001). Dynamical method in algebra: Effective Nullstellensätze. In *Annals of Pure and Applied Logic,* volume 111, pages 203–256.

[CLO] David COX, John LITTLE et Donal O'SHEA. (1992). *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, New York.

[D5] Jean DELLA DORA, Claire DICRESCENZO et Dominique DUVAL. (1985). About a new method for computing in algebraic number fields. In *Proceedings Eurocal'85.* volume 204 of *Lecture Notes in Computer Science,* pages 289–290, Springer-Verlag, Berlin-Heidelberg-New York.

[DD] Claire DICRESCENZO et Dominique DUVAL. (1989) Algebraic extensions and algebraic closure in Scratchpad. In *Symbolic and algebraic computation (ISSAC 88),* volume 358 of *Lecture Notes in Computer Science 358,* pages 440–446,Springer-Verlag, Berlin-Heidelberg-New York.

[E] Otto ENDLER. (1972) *Valuation Theory.* Springer-Verlag, Berlin-Heidelberg-New York.

[Gal] André GALLIGO. (1983). *Algorithmes de calcul de bases standard.* Rapport technique. Université de Nice.

[Giu] Marc GIUSTI. (1985). A note on the complexity of constructing standard bases. *Proceedings Eurocal'85*, Vol. 204 de *Lecture Notes in Computer Science*. Springer-Verlag, Berlin-Heidelberg-New York.

[Gou] Fernando Q. GOUVEA. (1997) *p-adic nombers : an introduction* 2^{e} édition. Springer-Verlag, Berlin-Heidelberg-New York.

[JL] Carl JACOBSSON et Clas LÖFWALL. (1991). Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. Vol. 12 de *J. Symbolic Comput.*, pages 337-371.

[KK] Manfred KRACHT et Erwin KREYSZIG. (1990). E. W. von Tschirnhaus: His role in early calculus and his work and impact on algebra. *Hist. Math. 17*, No.1, pages 16-35.

[Kri] Jean-Louis KRIVINE. (1969). *Théorie axiomatique des ensembles.* Presses Universitaires de France, Paris.

[KS] Sudesh K. KHANDUJA et Jayanti SAHA. (1999) Generalized Hensel's lemma, *Proc. Edimbourg Math. Soc.* **42**, 469-480 (1999).

[Kuh_1] Franz-Viktor KUHLMANN. A theorem about maps on spherically complete ultrametric spaces, and its applications, *preprint.*

[Kuh_2] Franz-Viktor KUHLMANN. *Valuation thory of fields, abelian groups and modules*, en préparation, à paraître dans la collection « Algebra, Logic and Applications » (Gordan and Breach), eds. A. Macintyre et R.Göbel.

[KL] Franz-Viktor KUHLMANN et Henri LOMBARDI. (2000). Construction du hensélisé d'un corps valué. In *Journal of Algebra,* volume 228, pages 624–632.

[Lag] Joseph-Louis LAGRANGE. (1770). Réflexions sur la résolution algébrique des équations. Première publication dans *Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin.* Repris dans *Oeuvres.* Vol 3., Gauthiers-Villard, Paris, 1869.

[Lom] Henri LOMBARDI. (2000). Dimension de Krull, Nullstellensätze et Évaluation Dynamique. *À paraître dans Math Zeitschrift.*

[LP] Henri LOMBARDI et Hervé PERDRY. (1998). The Buchberger algorithm as a tool for ideal theory of polynomial rings in constructive mathematics. *Proceedings of the Conference 33 Years of Gröbner Bases*, Cambridge University Press, Vol. 251 de London Mathematical Society Lecture Notes Series.

[M] Ernst W. MAYR. (1997). Some complexity results for polynomial ideals. *Journal of complexity*, No 3, pages 303-325.

[MRR] Ray MINES et Fred RICHMAN, Wim RUITENBURG. (1988). *A course in constructive algebra.* Springer-Verlag, Berlin-Heidelberg-New York.

[$\mathrm{M\text{-}S}_1$] Guillermo MORENO-SOCIÁS. (1991). *Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux)* (thèse), École Polytechnique.

[$\mathrm{M\text{-}S}_2$] Guillermo MORENO-SOCIÁS. (1991). An Ackermannian polynomial ideal. *Applied algebra, algebraic algorithms and error-correcting codes*, Lect. Notes Comput. Sci. 539, pages 269-280.

[PP] Liliana POPESCU et Nicolae POPESCU. (1989). Sur la définition des prolongements résiduels transcendents d'une valuation sur un corps K à K(X), *Bull. Math. Soc. Sci. Math. R. S. Roumanie (NS),* **33**(81)(3): pages 257–264.

[Rib] Paulo RIBENBOIM. (1985). Equivalent forms of Hensel's Lemma. *Exposition Math.*, **3**(1): 3–24,

[Ric_1] Fred Richman. (1974). Constructive aspects of Noetherian rings. Vol. 44 de *Proc. Amer. Mat. Soc.*, pages 436-441.

[Ric_2] Fred Richman. (2001). The ascending tree condition. Preprint.

[S_1] Abraham Seidenberg. (1974). What is Noetherian ? Vol. 44 de *Rend. Sem. mat. fis. Milano*, pages 55-61.

[S_2] Abraham Seidenberg. (1971). On the length of a Hilbert ascending chain. Vol. 29 de *Proc. Amer. Math. Soc.*, pages 443-450.

[Wae] Bartel Leendert van der Waerden. (1931). *Modern Algebra* (2 Vol.). Trad. Fred Blum. Frederick Ungar Publishing Co. New-York.

[Wei] Volker Weispfenning. (1984). Quantifier elimination and decision procedure for valued fields. In *Models and sets,* volume 1103 of *Lecture Notes in Math.,* pages 419–472, Springer-Verlag, Berlin-Heidelberg-New York.